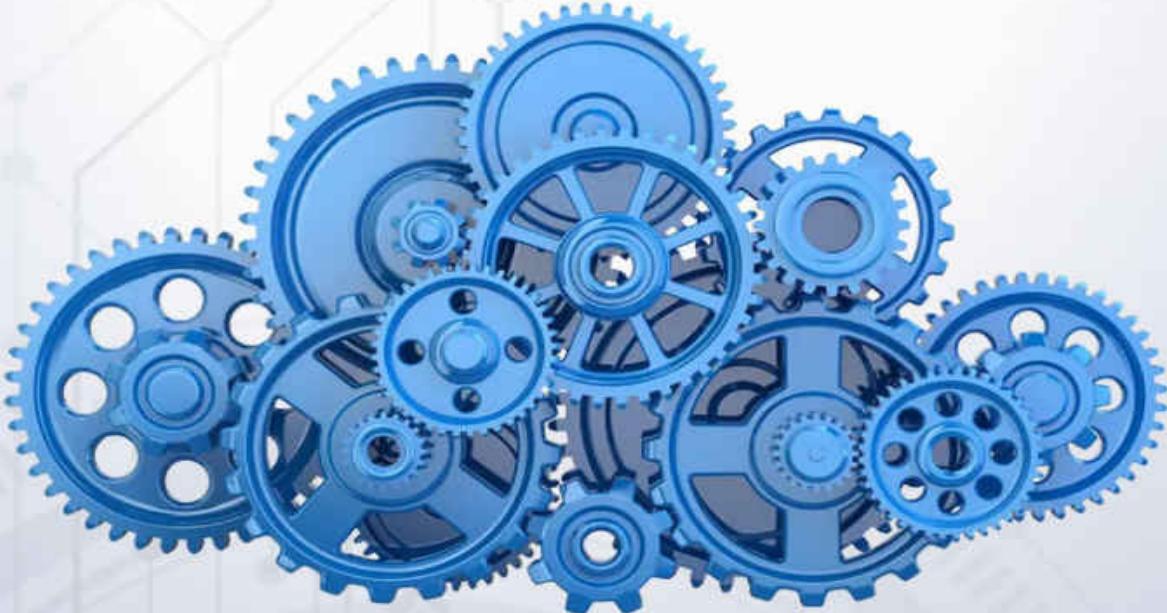


SECOND EDITION

AZ-500

MICROSOFT AZURE SECURITY TECHNOLOGIES

TECHNOLOGY WORKBOOK



UP TO DATE EXAM BLUEPRINT

LATEST EXAM QUESTIONS AND REGULARLY
REFRESHED CONTENT FOR YOU TO MASTER
YOUR EXAM CERTIFICATION.



ACE EXAMS WITH CONFIDENCE:

OUR PRECISE AND COMPREHENSIVE STUDY
MATERIAL ENSURES PASSING GRADES.

AZ-500: Microsoft Azure Security Technologies

Technology Workbook

www.ipspecialist.net

Document Control

Proposal Name : Microsoft Azure Security Technologies
Document Version : Version 2
Document Release Date : 5th May 2021
Reference : AZ-500

Copyright © 2018 IPSpecialist LTD.

Registered in England and Wales

Company Registration No: 10883539

Registration Office at: Office 32, 19-21 Crawford Street, London W1H 1PJ, United Kingdom

www.ipspecialist.net

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without the written permission from IPSpecialist LTD, except for the inclusion of brief quotations in a review.

Feedback:

If you have any comments regarding the quality of this book, or otherwise alter it to better suit your needs, you can contact us

through email at info@ipspecialist.net

Please make sure to include the book's title and ISBN in your message.

About IPSpecialist

[IPSPECIALIST](#) LTD. IS COMMITTED TO EXCELLENCE AND DEDICATED TO YOUR SUCCESS.

Our philosophy is to treat our customers like family. We want you to succeed, and we are willing to do everything possible to help you make it happen. We have the proof to back up our claims. We strive to accelerate billions of careers with great courses, accessibility, and affordability. We believe that continuous learning and knowledge evolution are the most important things to keep re-skilling and up-skilling the world.

Planning and creating a specific goal is where IPSpecialist helps. We can create a career track that suits your visions as well as develop the competencies you need to become a professional Network Engineer. We can also assist you with the execution and evaluation of your proficiency level, based on the career track you choose, as they are customized to fit your specific goals.

We help you STAND OUT from the crowd through our detailed IP training content packages.

Course Features:

Self-Paced Learning

- Learn at your own pace and in your own time

Covers Complete Exam Blueprint

- Prep-up for the exam with confidence

Case Study Based Learning

- Relate the content with real-life scenarios

Subscriptions that Suits You

- Get more and pay less with IPS subscriptions

Career Advisory Services

- Let the industry experts plan your career journey

Virtual Labs to test your skills

- With IPS vRacks, you can evaluate your exam preparations

Practice Questions

- Practice questions to measure your preparation standards
- On Request Digital Certification
- On request digital certification from IPSpecialist LTD.

About the Authors:

This book has been compiled with the help of multiple professional engineers who specialize in different fields, e.g., Networking, Security, Cloud, Big Data, IoT, etc. Each engineer develops content in his/her own specialized field, which is then compiled to form a comprehensive certification guide.

About the Technical Reviewers:

Nouman Ahmed Khan

AWS-Architect, CCDE, CCIEX5 (R&S, SP, Security, DC, Wireless), CISSP, CISA, CISM, Nouman Ahmed Khan is a Solution Architect working with a major telecommunication provider in Qatar. He works with enterprises, mega-projects, and service providers to help them select the best-fit technology solutions. He also works as a consultant to understand customer business processes and helps select an appropriate technology strategy to support business goals. He has more than fourteen years of experience working in Pakistan/Middle-East & the UK. He holds a Bachelor of Engineering Degree from NED University, Pakistan, and an M.Sc. in Computer Networks from the UK.

Abubakar Saeed

Abubakar Saeed has more than twenty-five years of experience managing, consulting, designing, and implementing large-scale technology projects, extensive experience heading ISP operations, solutions integration, heading Product Development, Pre-sales, and Solution Design. Emphasizing adhering to Project timelines and delivering as per customer expectations, he always leads the project

in the right direction with his innovative ideas and excellent management skills.

Uzair Ahmed

Uzair Ahmed is a computer science graduate working professionally as a product manager. He started his carrier as a technical content developer. He has been a part of a team of professionals operating in the implementation of SIEM. He holds a Bachelor's Degree in Computer Sciences from PAF-KIET, Pakistan. He has completed his training as AWS Solutions Architect and CCNA. He has both technical knowledge and industry-sounding information and has done international cloud-based projects. He previously worked as a professional developer and obtained good experience in software and backend development.

Syed Hanif Wasti

Syed Hanif Wasti is a Computer Science graduate working professionally as a Technical Content Developer. He is a part of a team of professionals operating in the E-learning and digital education sector. He holds a Bachelor's Degree in Computer Sciences from PAF-KIET, Pakistan. He has completed training of MCP and CCNA. He has both the technical knowledge and industry sounding information, which he uses efficiently in his career. He previously worked as a Database and Network administrator and obtained a good experience in software development.

Afreen Moin

Afreen Moin is a professional Technical Content Developer. She holds a Degree in Bachelor of Engineering in Telecommunications from Dawood University of Engineering and Technology. She has great knowledge of computer networking, cloud computing and has attended several training programs. She possesses a keen interest in research and design related to computers, which reflects in her professional career.

Hareem Khan

Hareem Khan is currently working as a Technical Content Developer, having command over networking and security. She has completed training of CCNA and Cybersecurity. She holds a B.E in Telecommunications Engineering from NED University of Engineering and Technology. She has strong knowledge of all the basics of IP and Security Networks and Routing and Switching Protocols.

Free Resources:

With each workbook purchased, IPSpecialist offers free resources to our valuable customers.

Once you buy this book, you will have to contact us at support@ipspecialist.net or tweet @ipspecialistnet to get this limited-time offer without any extra charges.

Free Resources Include:

For Free Resources: Please visit our website and register to access your desired Resources Or contact us at: info@ipspecialist.net

Career Report: This report is a step-by-step guide for a novice who wants to develop his/her career in the field of computer networks. It

answers the following queries:

- What are the current scenarios and future prospects?
- Is this industry moving towards saturation, or are new opportunities knocking at the door?
- What will the monetary benefits be?
- Why get certified?
- How to plan, and when will I complete the certifications if I start today?
- Is there any career track that I can follow to accomplish specialization level?

Furthermore, this guide provides a comprehensive career path towards being a specialist in networking and highlights the tracks needed to obtain certification.

IPS Personalized Technical Support for Customers: Good customer service means helping customers efficiently, in a friendly manner. It is essential to be able to handle issues for customers and do your best to ensure they are satisfied. Providing good service is one of the most important things that can set our business apart from the others of its kind.

Excellent customer service will result in attracting more customers and attain maximum customer retention.

IPS offers personalized TECH support to its customers to provide better value for money. If you have any queries related to technology and labs, you can simply ask our technical team for assistance via Live Chat or Email.

Our Products

Technology Workbooks

IPSpecialist Technology workbooks are the ideal guides to developing the hands-on skills necessary to pass the exam. Our workbooks cover the official exam blueprint and explain the technology with real-life case study-based labs. The content covered in each workbook consists of individually focused technology topics presented in an easy-to-follow, goal-oriented, step-by-step approach. Every scenario features detailed breakdowns and thorough verifications to help you completely understand the task and associated technology.

We extensively used mind maps in our workbooks to visually explain the technology. Our workbooks have become a widely used tool to learn and remember information effectively.

vRacks

Our highly scalable and innovative virtualized lab platforms let you practice the IPSpecialist Technology Workbook at your own time and your own place as per your convenience.

Quick Reference Sheets

Our quick reference sheets are a concise bundling of condensed notes of the complete exam blueprint. It is an ideal and handy document to help you remember the most important technology concepts related to the certification exam.

Practice Questions

IP Specialists' Practice Questions are dedicatedly designed from a certification exam perspective. The collection of these questions from our technology workbooks is prepared keeping the exam blueprint in mind, covering not only important but necessary topics as well. It's an ideal document to practice and revise your certification.

Content at a glance

- [**Chapter 01: Introduction to Azure**](#)
- [**Chapter 02: Configuration and Management of Azure AD for Workloads**](#)
- [**Chapter 03: Azure Tenant Security**](#)
- [**Chapter 04: Network Security**](#)
- [**Chapter 05: Securing VMs and Other Azure Resources**](#)
- [**Chapter 06: Container Security**](#)
- [**Chapter 07: Configuring Security Services**](#)
- [**Chapter 08: Security Policies and Alerts**](#)
- [**Chapter 09: Data Management & Security for Data Infrastructure**](#)
- [**Chapter 10: Security for Application Delivery**](#)
- [**Chapter 11: Encryption for Data at Rest**](#)
- [**Chapter 12: Final Steps**](#)
- [**Answers:**](#)
- [**Acronyms:**](#)
- [**References:**](#)
- [**About Our Products**](#)

Table of Contents

Chapter 01: Introduction to Azure

Introduction:

What is Cloud Computing?

Benefits of Cloud Computing

The Economy of Cloud Computing

Technical Terms

Types of Cloud Computing

Cloud Computing Deployments Models

What is Azure?

Azure Market Place

Global Footprint

Azure Resource Manager (ARM)

Azure Services

How to Interact with Azure

Practice Questions:

Chapter 02: Configuration and Management of Azure AD for Workloads

Azure AD Users

Lab 2-01: Creating an Azure AD User

1. Write these commands in Azure CLI; it will create your new Azure AD user account.

Azure AD Groups

1. Open PowerShell and write the following command to create your new Azure AD group.

1. Write the following command to create your new Azure AD group.

App Registrations, Permissions, Scopes, and Consent

Azure AD Connect

Azure AD Connect Authentication Methods

Federation Method:

Multi-factor Authentication

Conditional Access

Azure AD Identity Protection

Types of risk events

Azure AD Identity Protection Configuration Steps

AD PIM Overview and Activation

PIM Activation

Azure AD Roles

PIM Security Wizard

Administrative Units

Manage Administrative Units

Configure Workflow Automation by using Azure Security Center

Creating a Logic App and Defining Automatically Running Process

Manually Trigger a Logic App

Configure a Playbook Workflow Automation by using Azure Sentinel

Create a Playbook

Prepare the Playbook and Logic App

Choose the Trigger

Practice Questions:

Chapter 03: Azure Tenant Security

Introduction:

Transferring an Azure Subscription

Transferring Billing Ownership of an Azure Subscription

Transfer a Subscription to Another Azure AD Tenant

Steps After Transferring Billing Ownership

Transfer Visual Studio and Partner Network Subscriptions

Supported Subscription Types

[Transfer Account Ownership to Another Country/Region](#)

[Recipient Must Accept the Billing Information](#)

[Recipient Must Have an Azure Account](#)

[Mind Map](#)

[Practice Questions:](#)

[Chapter 04: Network Security](#)

[Introduction:](#)

[Virtual Network \(VNet\)](#)

[VNet Contains](#)

[VNet Peering](#)

[VNets Connection](#)

[Network Security Groups \(NSGs\)](#)

[Overview](#)

[Application Security Groups \(ASGs\)](#)

[Azure Firewall](#)

[Firewall Benefits](#)

[Firewall Configuration](#)

[Azure Firewall Limitations](#)

[Resource Firewall](#)

[Mind Map](#)

[Lab 4-01: Securing a Virtual Network with Azure Firewall](#)

[Lab 4-02: Configuring an Azure VNet-to-VNet VPN Gateway \(v2\)](#)

[Practice Questions](#)

[Chapter 05: Securing VMs and other Azure Resources](#)

[Introduction](#)

[Host Security: VM Endpoint Security](#)

[Features includes:](#)

[Pros:](#)

[Cons:](#)

[Antimalware: Single VM Deployment](#)

[Antimalware: Multiple VM Deployment](#)

[Host Security: Update Management](#)

[Role-Based Access Control \(RBAC\)](#)

[Managed Identities](#)

[Azure Resources Locks](#)

[Azure Management Groups](#)

[Azure Policies](#)

[Lab 5-01](#)

[Create a Tag for Each Virtual Network](#)

[Create a Policy](#)

[Practice Question](#)

[Chapter 06: Container Security](#)

[Introduction:](#)

[Azure Container Registry Security](#)

[Creating a Container Registry](#)

[Container Registry Authentication](#)

[Pushing an Image to the Registry](#)

[Lock/VNet/Firewall](#)

[Configuring Instance Security](#)

[ACR Tasks](#)

[Security Considerations](#)

[Create a Container Instance](#)

[Content Trust](#)

[Container Groups](#)

[Container Vulnerability Management](#)

[Azure Kubernetes Service \(AKS\)](#)

[Security Concepts](#)

[Best Practices](#)

[Authenticating to ACR from AKS](#)

[Mind Map](#)

Practice Questions

Chapter 07: Configuring security services

Introduction:

Microsoft Azure Monitor

Log Analytics

Diagnostic Logging and Log Retention

Tenant logs:

Resource logs

Logging Options

Mind Map

Practice Questions

Chapter 08: Security policies and Alerts

Introduction

Configuring Azure Policies: Just In Time VM Access Using Azure Security Center

To enable a user to request JIT access to a VM, assign these actions to the user:

Reviewing and Responding to Alerts and Recommendations

Security Alerts

Microsoft Azure Security Center Playbooks

Practice Questions

Chapter 09: Data Management & Security for Data Infrastructure

Data Classification Using Azure Information Protection

What is AIP?

Storage Analytics Data Retention Policies

Data Sovereignty with Azure Policy

Azure Key Vault

Managing Access to Key Vault, Secrets, Certificates, and Keys

[Managing Certificates and Secrets](#)

[Lab 9-01: Azure Key Vault](#)

[Database Authentication and Auditing](#)

[SQL Database Authentication with Azure AD](#)

[SQL Database Auditing](#)

[Azure SQL Database Threat Protection](#)

[Managing Access Control and Keys for Storage Accounts](#)

[Security for HDInsight](#)

[Security for Cosmos DB](#)

[Security for Microsoft Azure Data Lake](#)

[Practice Questions](#)

[Chapter 10: Security for application delivery](#)

[Introduction](#)

[Implementing Security Validations for Application Development](#)

[Best Practices](#)

[Synthetic Security Transactions](#)

[SSL/TLS Certificates](#)

[Protecting Web Apps](#)

[Mind Map](#)

[Practice Questions](#)

[Chapter 11: Encryption for Data at Rest](#)

[Introduction:](#)

[Microsoft Azure SQL Database Always Encrypted](#)

[Database Encryption](#)

[Storage Service Encryption](#)

[Disk Encryption](#)

[Supported Operating Systems](#)

[Backup Encryption](#)

[Lab 11-01: Enabling Always Encrypted in Azure SQL](#)

[Mind Map](#)

[Practice Questions](#)

[Chapter 12: Final Steps](#)

[Introduction](#)

[Course Completion and How to Prepare for the Exam](#)

[Register for the Exam](#)

[Preparing for the Exam](#)

[Mind Map](#)

[Answers:](#)

[Acronyms:](#)

[References:](#)

[About Our Products](#)

Microsoft Certifications

Microsoft Azure Certifications are industry-recognized credentials that validate your technical Cloud skills and expertise while assisting you in your career growth. These are one of the most valuable IT certifications right now since Azure has established an overwhelming growth rate in the public cloud market. Even with the presence of several tough competitors such as Amazon Web Services, Google Cloud Engine, and Rackspace, Azure is going to be the dominant public cloud platform today, with an astounding collection of proprietary services that continues to grow.

In this certification, we will discuss cloud concepts where we will learn the core benefits of using Azure like high availability, scalability, etc. We will talk about the Azure Architecture in which cloud resources are put together to work at best; Azure Compute where you will learn how to run applications in Azure; Networking in which the discussion is on how Azure resources communicate with each other; Storage, where you put all of your data and have different ways of storing it. We will also be covering Databases that are used for storage of data, its efficient retrieval as per demand, and to make sure that the users have the right access to the resources. Also, we will counter some complex scenarios with their solutions. We will have discussions on important topics like; Security, which makes Azure the best secure choice for your applications and functions; Privacy, Compliance and Trust that make sure how services ensure privacy and how you stay compliant with standards; As well as, Pricing in Azure to stay ahead on cost.

AZ-900 is the first certification of Microsoft Azure, which is the foundational certificate in Azure. After this certification, you can prove to the world that you are proficient and have the credibility to reach the highest point of your professional life.

Value of Azure Certifications

Microsoft places equal emphasis on sound conceptual knowledge of its entire platform, as well as on hands-on experience with the Azure

infrastructure and its many unique and complex components and services.

For Individuals

- Demonstrate your expertise in designing, deploying, and operating highly available, cost-effective, and secured applications on Microsoft Azure.
- Gain recognition and visibility of your proven skills and proficiency with Azure.
- Earn tangible benefits such as access to the Microsoft Certified Community, get invited to Microsoft Certification Appreciation Receptions and Lounges, obtain Microsoft Certification Practice Exam Voucher and Digital Badge for certification validation, Microsoft Certified Logo usage.
- Foster credibility with your employer and peers.

For Employers

- Identify skilled professionals to lead IT initiatives with Cloud technologies.
- Reduce risks and costs to implement your workloads and projects on the Azure platform.
- Increase customer satisfaction.

Types of Certification

Role-based Certification

- *Fundamental* - Validates overall understanding of the Azure Cloud.
- *Associate*- Technical role-based certifications. No pre-requisite required.
- *Expert*- Highest level technical role-based certification.

About Microsoft Azure Security Technologies

Exam Questions	Case study, short answer, repeated answer, MCQs

Number of Questions	40-60
Time to Complete	150 minutes
Exam Fee	165 USD
Languages	English, Japanese, Chinese (Simplified), Korean

The AZ-500: Microsoft Azure Security Technologies exam validates manage identity and access; implement platform protection; manage security operations; and secure data and applications. Example concepts you should understand for this exam include:

- Manage identity and access (30 - 35%)
- Implement platform protection (15 – 20%)
- Manage security operations (25 – 30%)
- Secure data and applications (20 – 25%)

Recommended Knowledge

- Configure security for service principals
- Manage Azure AD directory groups
- Manage Azure AD users
- Configure password writeback
- Configure authentication methods including password hash and Pass Through Authentication (PTA), OAuth, and passwordless
- Transfer Azure subscriptions between Azure AD tenants
- Secure the connectivity of virtual networks (VPN authentication, Express Route encryption)
- Configure Network Security Groups (NSGs) and Application Security Groups (ASGs)
- Create and configure Azure Firewall
- Implement Azure Firewall Manager
- Configure Azure Front Door service as an Application Gateway
- Configure a Web Application Firewall (WAF) on Azure Application Gateway
- Configure Azure Bastion

- Configure a firewall on a storage account, Azure SQL, KeyVault, or App Service
- Implement Service Endpoints
- Implement DDoS protection etc.

All the required information is included in this technology workbook.

	Domain
Domain 1	Manage Identity and Access
Domain 2	Implement Platform Protection
Domain 3	Manage Security Operations
Domain 4	Secure Data and Applications

Chapter 01: Introduction to Azure

Introduction:

Azure, like Google and Amazon Cloud Platforms, is Microsoft's Cloud Platform. It is typically a platform that allows us to use Microsoft tools. We need tremendous amount of money, energy, physical space, etc. to set up the huge IT infrastructure. In such circumstances, Microsoft Azure comes to our rescue. It offers us virtual machines, fast data processing, analytical tools, and monitoring instruments to simplify our work. Azure pricing is also simpler and cheaper. It is commonly referred to as "Pay as You Go", meaning you only pay for the services when you are using them. Microsoft launched Azure's Windows at the beginning of October 2008 but it became live in 2010. Microsoft later changed the name to Microsoft Azure in 2014, from Windows Azure. It has become one of the leading cloud services used today and is only growing bigger by the day.

What is Cloud Computing?

Cloud Computing is basically storing data and accessing the computers over the internet. It is the delivery of different computing services like servers, software, analytics, databases, and storage via the internet. Computing resources are delivered on-demand through a cloud service platform with pay-as-you-go pricing. The companies that are providing services termed as “Cloud Providers”. There are numbers of cloud providers like Amazon, Google and Azure.

Benefits of Cloud Computing

We all know that Cloud Computing has brought a major change in the traditional business thinking for IT resources. There are many benefits of using Cloud Computing. Some of which are:

1. Cost

Cloud computing eliminates the capital cost of buying hardware and software and of building and running in-house datacenters – server racks, 24 hours' electricity for power and cooling, etc.

2. Scale Globally

Cloud computing services have the capacity to scale with elasticity. In cloud, it means that IT resources are provided more or less computing power, storage, bandwidth – as per requirement and from the right place.

3. Increase Speed and Agility

New IT resources are readily available so that resources can be scaled up infinitely according to demand. This leads to a dramatic increase in agility for organizations.

4. Reliability

Cloud computing allows data backup, disaster recovery and business continuity as data can be replicated in the network of the cloud supplier on multiple redundant sites.

5. Security

The protection of their data is one of the main problems for any organization regardless of its size and industry. Infringements of

data and other cyber-crimes can devastate the revenue, customer loyalty, and positioning of a company. Cloud provides many advanced security features to strengthen the security of the overall company. It also helps in protecting your data, application, and infrastructure.

The Economy of Cloud Computing

In the traditional environment of organizations, as there is a need for large investments on CapEx, Cloud is the best way to switch to the pay-as-you-go model. Cloud reduces the Capital Expenditure (CapEx) cost and also gives some other benefits. With Cloud Computing, you should move toward Operational Expenditure (OpEx).

Mostly in Azure, the pricing is based on an hourly basis like VMs, App Services, etc. There is also consumption based pricing which is on the basis of per execution of function, per second use of resource, or both. An example of consumption based pricing is Azure Function.



EXAM TIP

Capital Expenditure (CapEx) is the expenditure to maintain or acquiring fixed assets by spending money. This includes land, equipment, etc.

Operational Expenditure (OpEx) is the cost of a product or a system that is running on a day-to-day basis like electricity, printer papers, etc.

Technical Terms

In order to understand Cloud Computing, you need to understand some technical terms.

- **High Availability (HA)** - It is the core of cloud computing. As we know that in traditional server environments, companies own a number of hardware and the workload is limited to this hardware capacity. In case of extra load, capacity cannot be increased whereas, sometimes this hardware seems extra for the workload. In cloud, you do not own any of the hardware and addition in servers is just a click away. This way, you get high

availability for your servers by replacing instantly the failed server with the new one. HA depends on the number of VMs that you set up to eventually cover in case one goes down

- **Fault Tolerance** - For resilience in the cloud, fault tolerance is also an important factor. Fault tolerance gives you zero down time. Fault tolerance means that if there is any fault from the Azure side, then it is immediately mitigated by Azure itself
- **Disaster Recovery (DR)** - In case of any catastrophic disaster like cyber-attack. There is a plan in DR to recover your business from these critical systems or in normal operation if such an event occurs. DR has designated time to recover and a recovery point
- **Scalability** - In cloud computing, scalability means addition or removal of the resources in an easy and quick way as per demand. It is important in such a situation where you do not know the actual number of resources that are needed. Auto-scaling is an approach for scalability depending on your requirement by defining the threshold
- **Elasticity** - Elasticity is the capacity to dynamically extend or minimize network resources to respond to autonomous working load adjustments and optimize the use of resources. This can contribute to overall cost savings for services
- **Agility** - Agility is the capability to adapt quickly and efficiently to changes in the business environment. Agility also refers to the ability to quickly develop, test and deploy business-led software applications. Instead of providing and managing services, Cloud Agility lets them concentrate on other issues such as security, monitoring, and analysis.



EXAM TIP

From the Exam perspective, one must be familiar with all the terms like HA, Fault Tolerance, DR, Elasticity, Scalability, and Agility.

Types of Cloud Computing

The cloud computing services are divided into four broad categories: IaaS, PaaS, Serverless, and SaaS. These are also known as a stack

in cloud computing because each of them is built on top of another. Let's discuss each of them.

1. Infrastructure as a Service (IaaS)

It gives you a basic IT infrastructure for Cloud IT like VMs, Data Storage, Networks, OS on a pay-as-you-go model.

2. Platform as a Service (PaaS)

Cloud computing platforms that provide an on-demand environment to build, test, deliver and manage software applications are referred to as Platform as a Service. PaaS is designed to facilitate the fast development of web or mobile apps for developers without the concern of setting or maintaining the underlying server, storage, network, and database infrastructure that are needed for development.

3. Serverless

Overlapping PaaS, serverless computing concentrates on creating application functionality, without continually spending time maintaining the required server and infrastructure. The cloud provider is responsible for the configuration, capacity planning, and server governance. The highly scalable and event-based serverless architectures only use resources when a particular task or trigger takes place.

4. Software as a Service (SaaS)

Both servers and code are taken over by cloud providers. Cloud providers are hosting and maintaining the applications and underlying infrastructure for SaaS and handling updates such as software upgrades, and security patches. Users link the app over the Internet, usually through their phone, tablet or PC through their web browser.

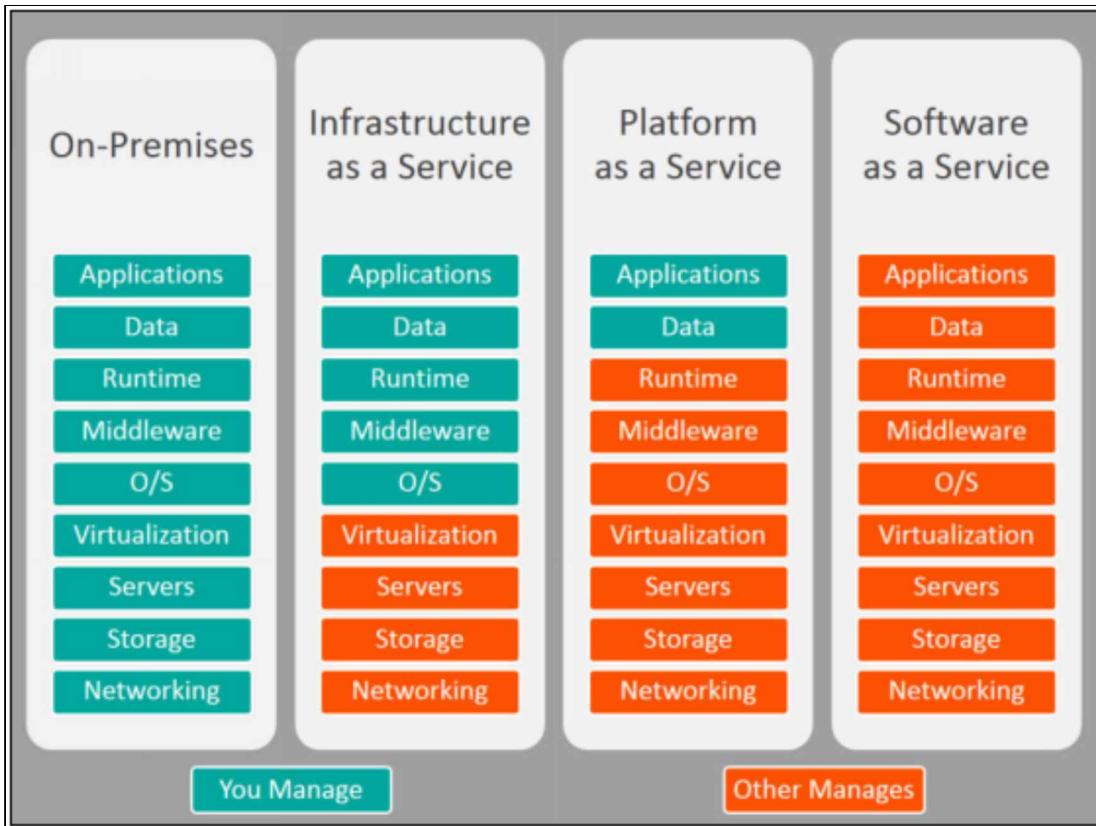


Figure 1-01: IaaS, PaaS and SaaS Overview



EXAM TIP

IaaS- servers, storage, and networking

PaaS-servers, storage, networking, management tools

SaaS- a complete application like Office 365

Serverless- no need of server; there is a single function that is hosted, deployed and managed on its own

Cloud Computing Deployments Models

We know that all clouds are not the same and not every business requirement for cloud computing is the same. So, in order to meet the requirements; different models, types and services have been used. Firstly, you have to decide how the cloud service is being applied by finding out the cloud deployment type or Architecture. There are three different types of Cloud Computing: Public, Private and Hybrid.

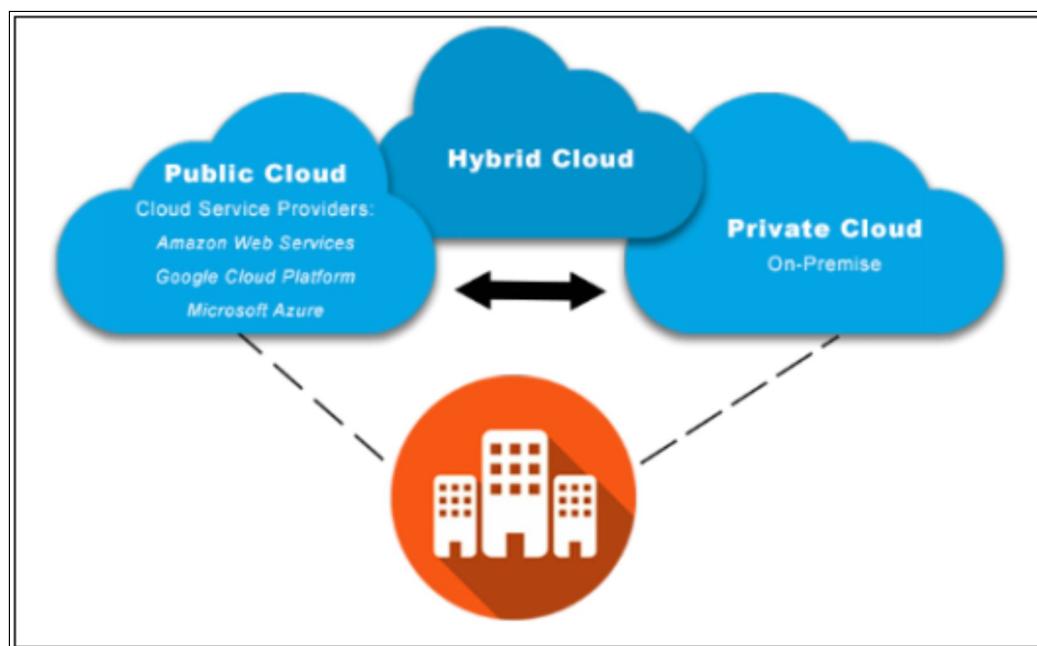


Figure 1-02: Public, Private and Hybrid Cloud



What is Azure?

Microsoft Azure is known as Windows Azure and it is a Public Cloud. We have already learned in the above discussion about Public Cloud. As for Azure, it is an expanding cloud service that helps the companies to meet their challenges. It is free to build, manage and deploy applications with your favorite tools and frames in a huge, global network. Azure is considered for offering both IaaS and PaaS. Azure offers over 100 services, from the execution of existing applications on virtual machines to exploration of new tech paradigms like smart bots and mixed reality.

In order to use Azure, you first need to setup an Azure account directly by going to “Azure.com” or with the help of a representative. You can sign-up to Azure as a Free account with free USD 200 credit and 25+ free services.

Azure, for example, offers AI and machine learning tools that can communicate with your customers through vision, hearing, and speech. It also offers solutions for the storage of massive amounts of data, which are increasing rapidly. Azure services give solutions that without Cloud resources, are much expensive.

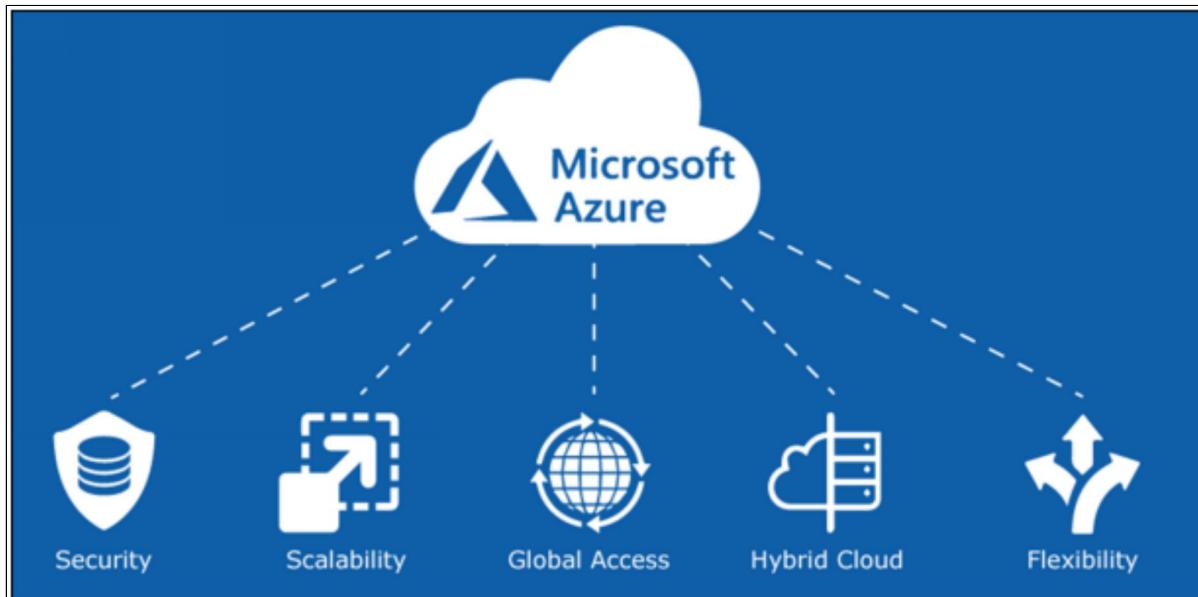


Figure 1-03: Azure Benefits

Azure Market Place

The Azure market place offers technical solutions and services from Microsoft and partners to build and extend Azure products and services. It has all kinds of services and applications like VMs, Templates, apps, and Azure managed services etc. There is an Azure App Store in your mobile for buying cloud services, where you have a variety of solutions including base OS, database, security, networking and developer tools. For accessing all of these you can either go directly to the website of market place or use Azure CLI or integrate with Powershell. From the catalog, you can add anything to subscription. Some services are free and some are charged. In order to publish your own product in the Market Place, you need to become partner with Microsoft so that it becomes a distribution channel for your business.

Global Footprint

Azure has more global regions than any other cloud provider — which offers the scale required to bring users around the world closer to applications, preserve residency and provide customers with comprehensive compliance and resilience options. There are 58 regions of Azure that are available around the world with 140 available in 140 countries.

Regions

Regions are geographical areas where Azure is present to deploy the Azure resources. It is a set of data centers with latency-defined perimeter connected via a dedicated regional low-latency network. There are region specific services but some core services like storage and VMs are by default live in all regions.



EXAM TIP

Dedicated Regional Low Latency network means there is a fiber connection between data centers in the region.

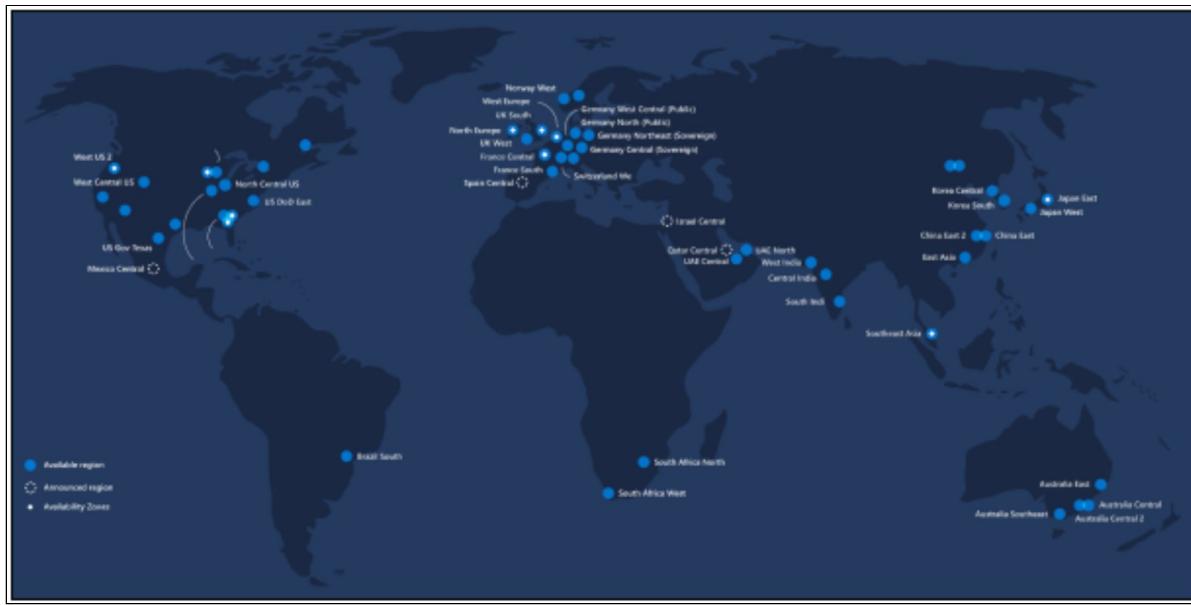


Figure 1-04: Azure Geographical Region

How to Choose a Region?

When you are choosing a region, you need to think about three things mainly:

- **Location-** in order to reduce the latency, choose a region closest to the user
- **Features-** all features are not available in all regions, so select a region where your specific feature is available
- **Price-** service prices in Azure vary from region to region

Geographies/Paired Regions

Geography is a distinct market that usually conserves data residence and compliance boundaries with two or more regions within the same geographic area.

Geographies enable customers with particular data residency needs to maintain their data and apps in close proximity. Geographical areas are fault tolerant to whole failures in the field by linking them to Azure's dedicated networking infrastructure. So if the primary region goes down, it failovers to the secondary region. In the paired region, only one region is updated at a time. For some services, paired regions are used as replications.

Availability Set

An Availability Set is a logical grouping function that can be used to separate VM resources from each other. Azure must ensure that your VMs are operating across several physical servers, device tables, storage units and network switches within an availability set. If a hardware or software failure occurs, only the VMs will be impacted, and the overall solution will remain operational.

Availability Zone

Availability Zones (AZ) are locations within an Azure region that are physically separate. An availability zone is composed of one or more independently operating power, and network data centers. Each region has a minimum of three zones.

Availability zones allow clients to run high-availability and low-latency mission-critical applications.

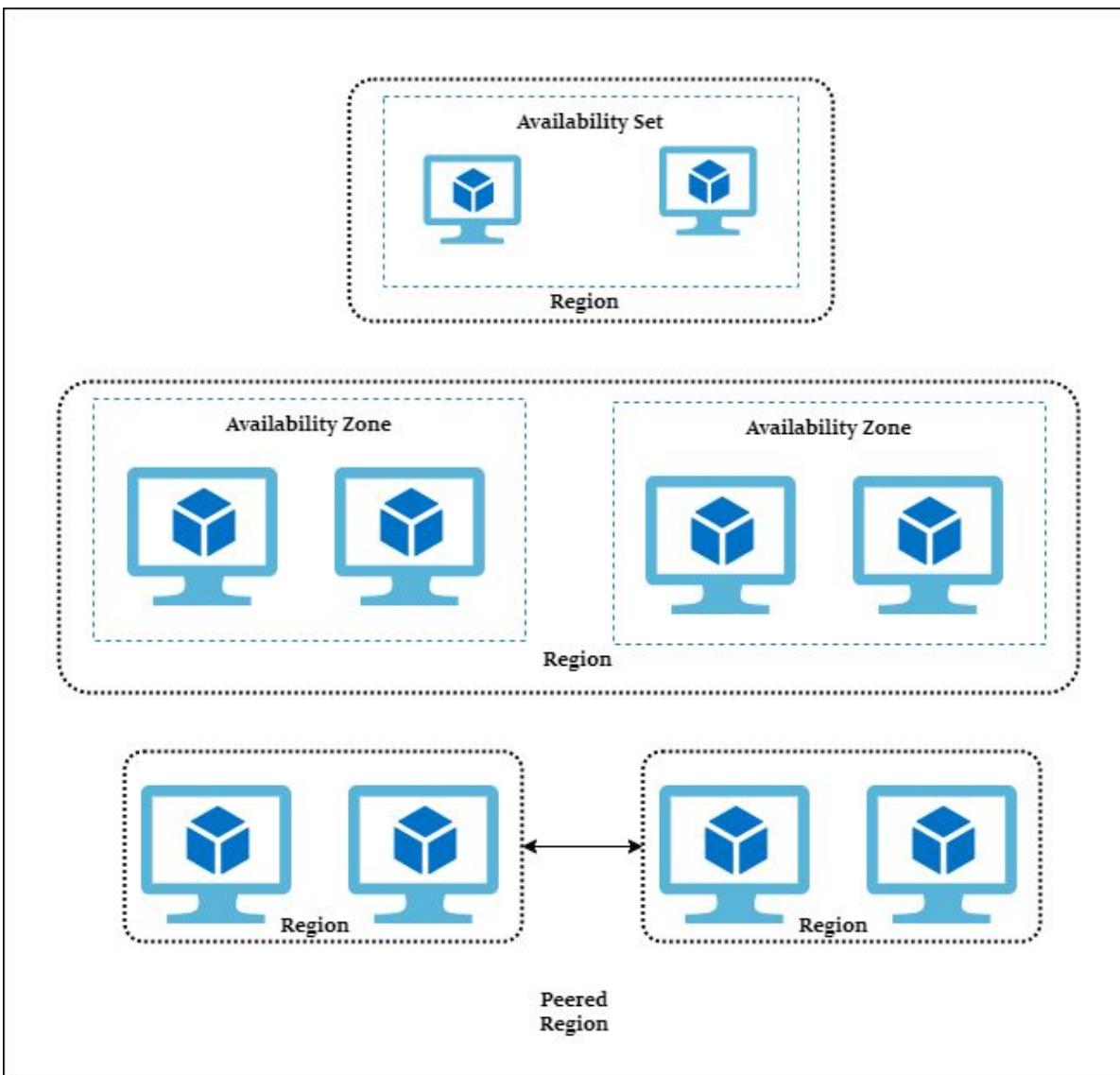


Figure 1-05: Region, AZ, and Paired Region



Azure Resource Manager (ARM)

It is an underlying service where the Azure resource deployment and management is done. It provides a management layer, which lets you create, upgrade, and uninstall your Azure subscription tools. You use management features such as access control, locks, or tags to ensure that your resources are protected and organized after deployment.

- **A Resource** is a manageable item that is available in Azure like VM, storage, databases, etc. Each resource can reside only in one resource group
- **Resource Groups** are the place where you deploy your resources. Here, you need to identify which resource group you want to deploy a resource. It is like a container where all resources of a solution or the resources that you want to manage in a group reside. The resource from the resource group can be added or removed at any time. You can move your resources from one group to another and the resource from multiple regions can be in one resource group as well. With the resource group, you have access control to the resource. The resources in different resource groups can interact with each other
- **Resource Provider** is a service that supplies the resources that you can deploy for a manageable resource for the resource manager
- **Resource Manager Template** is a JavaScript Object Notation (JSON) file that defines the resources deployed in the resource group. It also defines the dependencies between the deployed resources. With this template, resources can be deployed in a consistent and repeatable way

ARM Benefits

- You have group resource handlings like deploying, management, and monitoring
- You get consistency; For example, when you deploy resources, it will be happening in the same way as every time

- Define the dependencies between resources in the right order.
- Access Control, which is built-in to assign access to the users
- Tagging, which makes it easier to identify the resource in the future
- For billing, you can use tagging to stay on top



EXAM TIP

The resource group itself is not a resource, it helps in the structure of Azure Architecture.

Azure Services

There is a number of available services and features in Azure. The most commonly used categories are:

- Compute
- Networking
- Storage
- Mobile
- Databases
- Web
- Internet of Things
- Big Data
- Artificial Intelligence
- Security and Identity
- Monitoring and Management

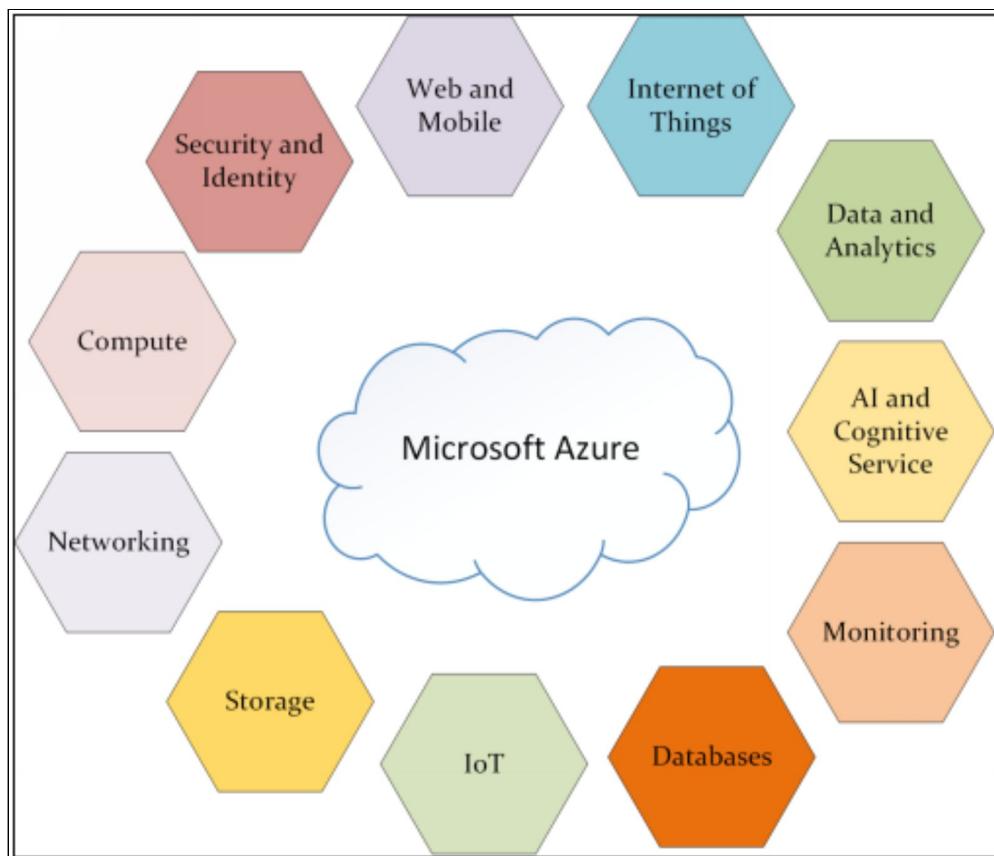


Figure 1-06: Azure Services

Compute

In Azure, there is a number of options that are available for application and service hosting. Azure Compute provides you an infrastructure where you can run your applications.

- **Azure Virtual Machine**- These are Linux and Windows VMs on demand with your desired configuration hosted in Azure. The supported Linux distributions are CentOS, Oracle Linux, RHEL, Debian, openSUSE, SUSE LES, and Ubuntu. There are 6 types of VMs with 28 families. There is a set amount of Memory, vCPUs and Temporary Storage. You can also attach additional data disks to these VMs. Pricing is based on per minute billing. Reserved VMs are also available for significant discounts, like you can get discounts up to 72% on a pay-as-you-go model
- **App Service** - It is a PaaS that provides a fully managed platform for creating cloud applications for web and mobile. It is used to host web applications, mobile app back ends, RESTful

APIs and automated business processes. The programming languages that are supported by App Service are .NET, .NET Core, Ruby, Java, PHP, Node.js and Python

- **Azure Function** – A serverless compute that enables you to automatically run code on demand. Azure Function is an event driven service for accelerating app development. It is FaaS that executes the code in response to an event or trigger. Its billing is done when code is executed; in the idle state, it is not charged. Its supported languages are C#, F# and JavaScript, and currently Java is in preview state. Azure Function is a part of App Services that can run in App Service Plans (from free to isolated plan). In free account, the first 1 million executions/month are free
- **Azure Batch** - A managed service for batch processing jobs like for running large-scale parallel and High-Performance Computing (HPC) applications. It has the ability to scale to tens, hundreds, or thousands of virtual machines as per requirement. It supports both windows and Linux compute nodes. This service is free and you only need to pay for the resource that are used in your task
- **Azure Kubernetes Service** - A managed Kubernetes Container Orchestration for simplifying the deployment, management, and operations of Kubernetes. It gives you automatic upgrades and patching. Azure Kubernetes Service enables you to manage the cluster of VMs on which containerized app is running. It also supports other orchestration like DC/OS, Docker, and Unmanaged Kubernetes, but these are not managed. Here, you only need to pay for agent nodes not for the master node
- **Azure Container Instance** - A containerized service that is used to run an application on Azure without provisioning the VMs and servers. You can easily run the container with a single command. It gives you an individual container as a service. Azure Container Instance is the fastest and easiest way to run a container in Azure. It is good for applications that run in an isolated container. The applications are publically addressable

and the container spec can be designed by you. The billing is per-second based

- **Service Fabric** - A distributed network framework that is capable of operating in various environments, Azure and on-site. It creates Windows and Linux micro services and orchestrates containers. Service Fabric is used by multiple Azure and Microsoft services like Skype, CosmosDB, Cortana, etc. It supports both stateful and stateless micro services. Its supported community is .NET but it also supports other languages and containers
- **Cloud Services** - A managed service for cloud applications. It is actually a PaaS offered by Azure. It is similar to App Services but with the difference that you can remote it into VMs. It creates highly available, flexible cloud applications and APIs to concentrate on software rather than hardware. It has two types of services: Web Roles that are websites and web apps, and Worker Roles that are for asynchronous processing

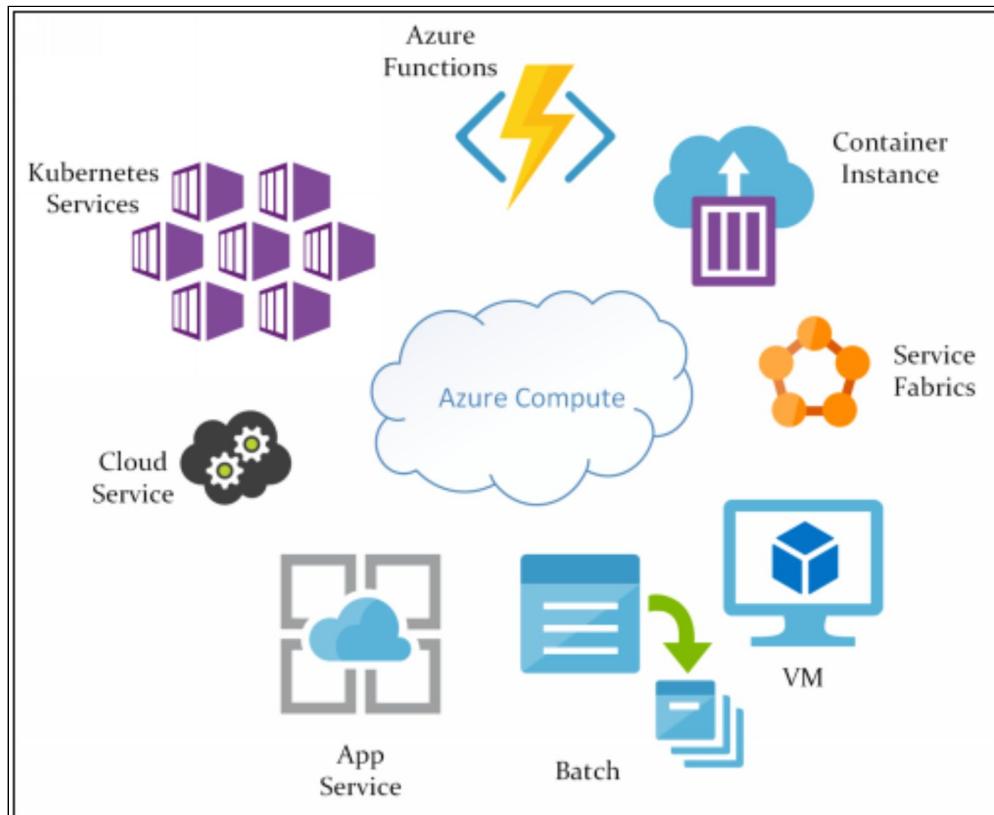


Figure 1-07: Azure Compute

Networking

The key function of Azure networking is the relation of compute resources and access to applications. In Azure, a network interface includes a number of options in global Microsoft Azure data centers that link the outside world to services and apps. There are various networking services in Azure that can be used individually or together. Azure networking provides you the most secure environment for your data as compared to any other Cloud Platform.

- **Virtual Networks** – This allows your Azure resources to communicate with each other over the internet or on-premises network, in a secure way. It is also known as VNET and is an isolated network where you host your VMs, VM Scale Sets and App Service environments. Virtual Networks are composed of subnets with user defined routes where you define the route to send the traffic and the destination from where it comes in. With Virtual Network, you can add Security Groups and outbound internet access to the resources. In Virtual Network, you have the capability of VNET Peering, where you connect two VNETs together. VNET peering can be done within the same region or across the region for global coverage. However, across-region VNET peering is supported in only a few regions currently. There is also a Service Endpoint feature that enables you to access the services within your VNET by creating a private connection to that resource rather than using the internet. This endpoint feature is only available in Storage account and SQL databases
- **Azure Load Balancer** – This balances the incoming and outgoing traffic to and from the application resources and service endpoints. It gives basic load balancing features to your VMs and operates at layer 4 (Transport layer of the OSI model). It has a public or internal load balancer. A public load balancer is internet facing while internal load balancer is used within the VNET. Azure Load Balancer provides regional load balancing by routing traffic over availability zones and into your VNets. It provides internal load balancing by routing traffic across and

from your local resources within VNET. It has HTTP or TCP based probes for health checks and availability. It uses hash based load balancing to balance the load inside the VMs that are behind your load balancer

- **Application Gateway** – This is a cloud load balancing device to handle web app traffic. It is Layer 7 load balancing that uses HTTP based Round robin. It optimizes application server delivery while increasing security for applications with a web application firewall. It also offers some other features like SSL Offloading, stickiness for some cookies based session affinity at the backend to maintain the state for the user between the connection of user with a single VM. It also provides support for client connected applications by Web Socket. It has internal and external load balancing, similar to the public and internal load balancer but they are at higher level
- **VPN Gateway** – This sends encrypted traffic across the public internet between an Azure virtual network and an on-site location. Azure Virtual Networks are accessed through high performance VPN Gateways in a secure way over the internet. VPN Gateway supports both Site-to-Site VPN and Point-to-Site VPN. You have one VPN gateway per VNET then you have the ability to have multiple connections per VPN Gateway. In that, you can perform Static or Dynamic Routing
- **Azure DNS** – This hosts DNS domains with the same credentials of Microsoft Azure infrastructure to provide name resolution with fast DNS response and high domain availability. In Azure DNS, you cannot purchase the Domain name. For DNS, you pay per zone, per month, and then per million queries. The pricing of per zone changes depending upon the zone. Private domain support currently is in preview state
- **Traffic Manager** – This is a global traffic router that distributes DNS-based traffic to services across the Azure region in order to get the best available endpoint, providing high availability and responsiveness. It supports 4 routing methods: priority, weighted, geographic and performance. Depending on the routing method and health checks, the traffic will be sent. It can

be used to build multi-region architecture like web applications

- **Content Delivery Network (CDN)** – This provides users with high bandwidth content. To reduce latency, CDNs save cached content on edge servers at POP locations near to end users. Edge servers are the smaller data centers. It is mainly used for static assets like media, images, etc. It also supports Dynamic Site Acceleration by optimizing the route between the requester and the origin for dynamic content because it does not cache the dynamic content on the edge servers. In Azure, CDN is actually provided by Akamai and Verizon. The billing is based per Gb outbound per month and the rates can change on zone basis
- **Express Route** - ExpressRoute allows you to extend your on-premises networks to Microsoft Cloud by a connectivity provider's private connection. This is a private connection. There is no traffic going on the internet. Connections to cloud services such as Microsoft Azure, Office 365, and Dynamics 365 can be built with ExpressRoute through stable high bandwidth connections. The dedicated link is up to 10Gbps. With that, you have two options: either you have connectivity to MPLS or to the on-premises network. This is good for DR or hybrid cases

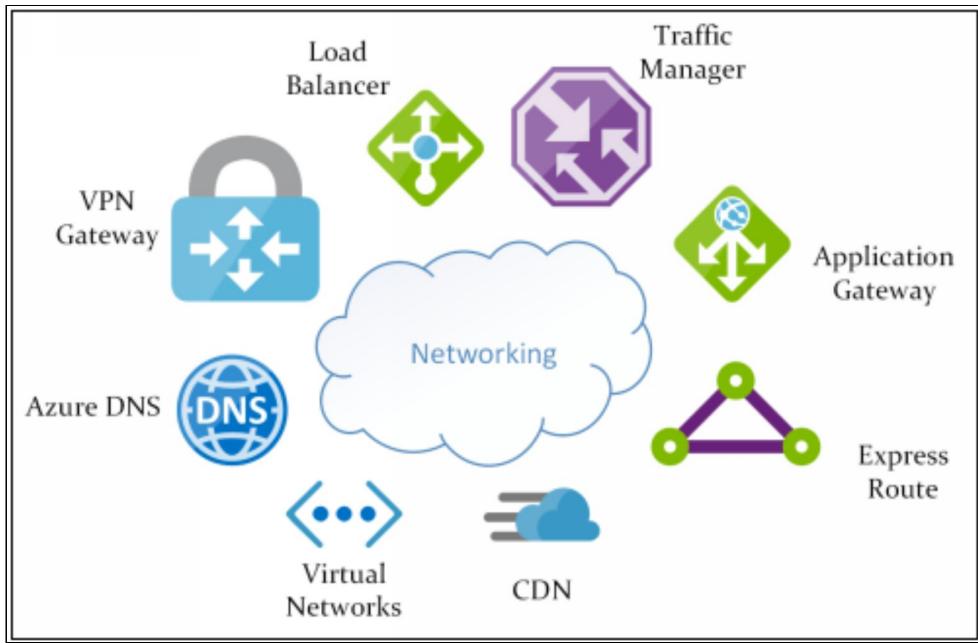


Figure 1-08: Azure Networking

Storage

Azure Storage is a cloud storage system from Microsoft that helps to store up-to-date files. Azure Storage offers an extremely scalable data object store, a cloud file system service, a reliable message store, and a NoSQL store. Azure Storage is secure, highly available and durable, scalable, managed and accessible. You must first create an account in Azure to use any kind of storage there, the storage account is the parent object. You can move your data to and from your storage account after your account has been established. You can also build a storage account for up to 500TB of cloud data because it has a limit of 500TB per storage account. To manage your expenses, use a Blob storage account and hot or cold access tiers depending on how often the object data is accessed. A storage account can be of two types: Standard and Premium accounts.

In Azure Storage, there are multiple types of replication: Locally Redundant Storage (LRS), Zone Redundant Storage (ZRS), Geo-Redundant Storage (GRS) and Read Access Geo-Redundant Storage (RA-GRS). In Azure Storage, there are also various tiers of Storage: Archive (for Blob only), Cool Storage (for infrequently accessed data) and Hot Storage (for frequently accessed data).

- **Blob Storage** - Azure Blob Storage is Microsoft's cloud object storage solution. Blob storage is for storage of large volumes of unstructured data, like text or binary data. It is an internet accessible Object Store via HTTP or HTTPS. In that, you have an option to make your data either public or private. The hierarchy is like: Storage Account -> Containers -> Blobs. A blob is an object which is in the container. It also has an archiving tier available
- **Queue Storage** – Azure Queue Storage is a data store for queuing and for the reliable provisioning of messages. It is a managed queuing service through which you get secure storage for communication between apps based on the message. Messages in the queue can be up to 64 KB and millions of messages can be stored in a single queue. A queue is generally used to store asynchronous lists of messages. It is useful for decoupling applications. The life time of a message in the queue is 7 days
- **File Storage**- Azure File Storage makes the use of a regular SMB (Server Message Block), to set up a highly available network of file shares. You also can read files via the REST interface or libraries for the storage client. The cloud or on-site implementations of Windows, Linux, Mac OS installs Azure file shares concurrently. Azure file shares can also be cached with Azure file sync on Windows Servers for easy access close to the data point. You can also use it as a shared file system for the apps that lift and shift into the cloud. The maximum file share size is 5TB
- **Table Storage**- Azure Table Storage is a service that stores NoSQL unstructured data in the cloud and offers a schema less design for providing a key/attribute database. Since table storage is schema less, the development of your application will make it easy for you to adapt your data. In table storage, there can be as many entity and tables as you like. The maximum entity size can be up to 1MB. Access to table storage data for many types of applications is fast and cost effective and is typically lower than conventional SQL for similar data volumes.

It has now become a part of Cosmos DB. A new Azure Cosmos DB Table API is introduced in addition to the Azure Table storage service, which offers optimized throughput tables, global distribution and automated secondary indexes

- **Disk Storage** – Azure Disk Storage provides a managed or unmanaged disk for your VMs. Managed disk takes care of the storage account and disks for you, and you pay for what you provisioned while in un-managed disk, as you have to manage the disk itself but you only have to pay for what you use. It has 99.999% availability with three replicas. The available types of disk storage are Ultra-Disks, Premium Solid-State Drives (SSDs), Standard SSDs, and Standard Hard Disk Drives (HDDs). In premium, you have an option of disk IOPS that are provisioned and these are mapped on disks not on VMs. However, not all VM families support the premium disk type. In Standard disk, the IOPS are not provisioned via disk so it varies with VMs. The size for the disk storage is from 32 GB to 4 TB, but you can attach multiple disks to a VM

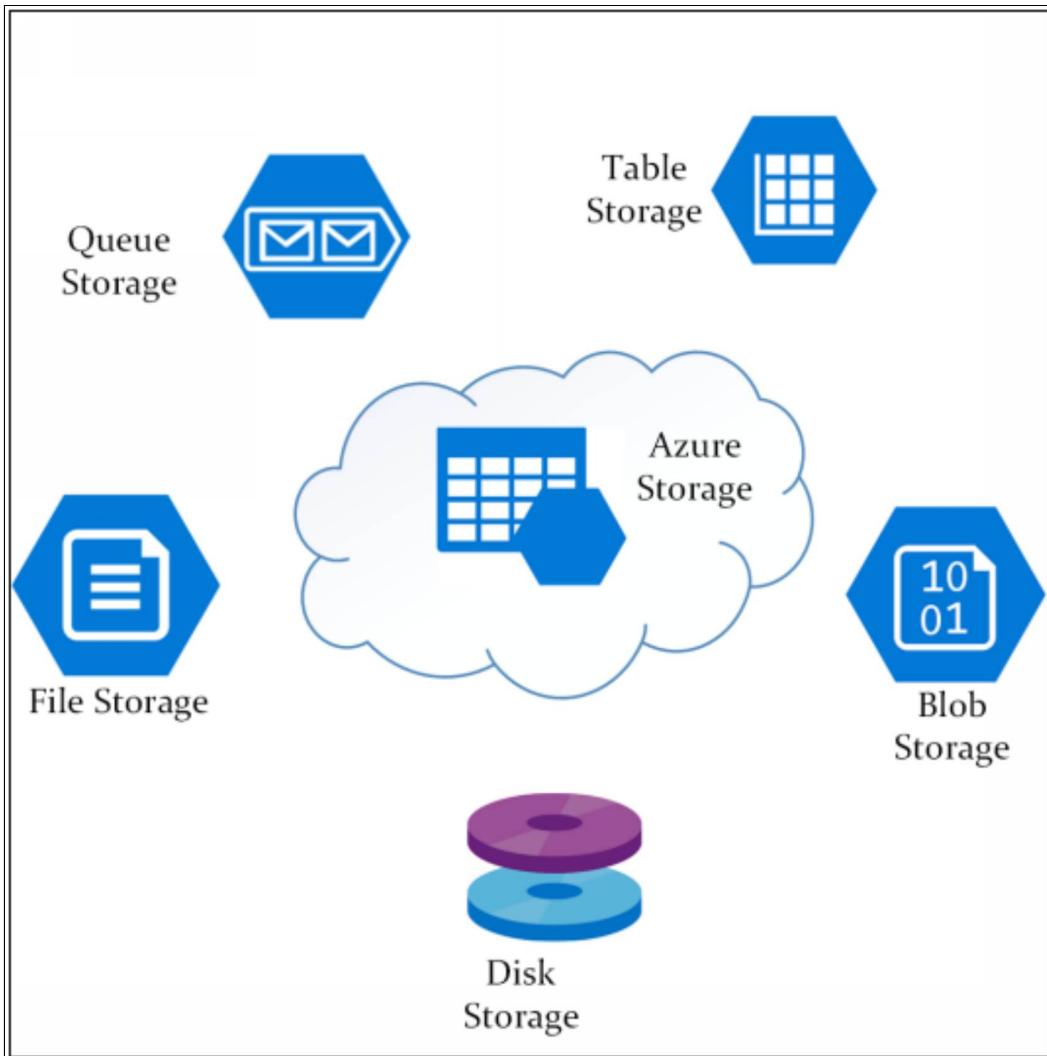


Figure 1-09: Azure Storage

Data and Analytics

Data is available in all sizes and formats. When they speak about Big Data, it means they refer to large volumes of information. Like, producing hundreds of gigabytes of data from weather systems, communications systems, genome analysis, imagery platforms, and many other scenarios. The volume of data makes it difficult to interpret and determine. It often is so large that it is no longer appropriate for traditional methods of processing and analysis.

To cope with these large data sets, Open Source cluster technologies have been developed. Microsoft Azure offers a wide range of Big Data and analytics tools and services.

- **HDInsight** – It is an open source fully managed analytic service. It processes huge amounts of data in the cloud with managed Hadoop clusters. The 99.9 percent SLA for your business is given by this. It is basically a Hadoop component from HDP (Hortonworks Data Platform). It is used for running streaming and historical data analytics. The open framework for HDInsight includes hive, spark, Kafka, storm, etc. The use cases for this service are batch processing, data science, and many more
- **Event Hub** – It is a large scale telemetry ingestion that allows you to run millions of events per second. You can use it to load a large amount of data in to the cloud in real time. It captures data into the Azure Blob or Data Lake and then publishers send this data into the event hub. Then from these hubs, the consumer reads data. The retention period of an item in hub is 7 days
- **Data Lake Store and Analytics** - Azure Data Lake provides all the capabilities to make the storage of data of any scale, shape and speed, and all types of processing and analytics across platforms and languages simple for developers, data scientists, and analysts. This eliminates the complexity of ingesting and processing all your data and makes the process of batching, uploading and immersive analysis easier. Data Lake Store is a repository for the analytics workload and it is HDFS compatible and can integrate with HDInsight. It has no limit for data storage. Data Lake Analytics is a completely managed pay-per-job analysis service with corporate security, auditing and support. It uses U-SQL language that is specifically designed for Data Lake Analytics that combine SQL and uses C# code to perform analytics. Data Lake Analytics can work with Data Lake Store and others
- **Data Factory** – It is a fully managed cloud based data integration service. Big data demands for the service to organize and operationalize processes and refine these huge raw data stores into operational business insights. This is an integrated cloud service for complex hybrid Extract-Transform-Load (ETL), Extract-Load-Transform (ELT), and data integration

projects. It is a service that automates the data movement along its process through various systems. SQL Server Integration Service built-in V2 of Data Factory is in preview, which is the transformation process of ETL

- **Azure Analysis Service** – It is an analytic engine as a service for enterprise grade. It uses advanced computing and mashup to combine data from several data sources, set metrics, and secure data in an advanced single table of the semantic data model for query purpose. The data model makes searching vast volumes of data for ad hoc data analysis easier and quicker for users. It supports hybrid network and it has built-in SQL Server Analysis Service

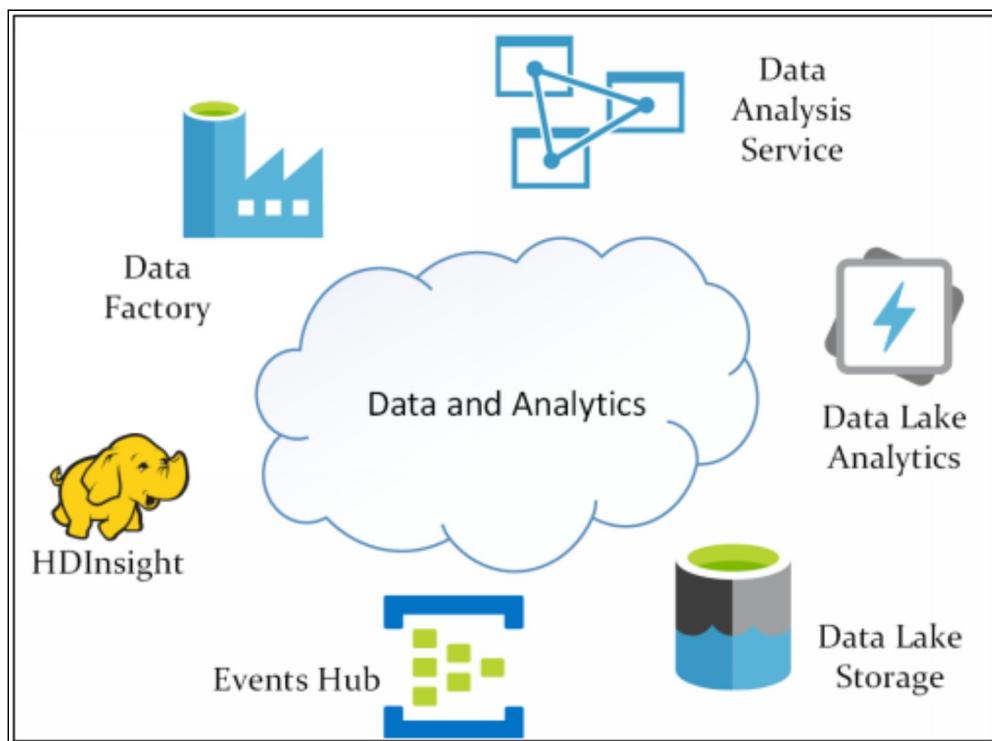


Figure 1-10: Data and Analytics

Databases

Azure Database is a fully managed service. It has business-grade efficiency with integrated high availability that ensures you can easily scale and hit global distribution without needing to pay attention to costly downtime.

- **SQL DB** – It is a fully managed relation database with high availability and performance data storage for applications. In that, you have two deployment options: Single DB and Elastic Pools. In Single DB, you pick a single service and scale it up or down in a single database while in Elastic Pools, a pool of resources is shared across number of databases. With Elastic Pool, you get better optimization. It has Database Transaction Unit (DTU) purchasing model. The purchasing model DTU provides a mixture of computing, storage and I/O services in three levels, supporting light to large databases. SQL DB shares its code base with MS SQL server, which means that SQL DB gets updated first before rolling out to the MS SQL server, this way, it will be up to date with the feature of an SQL server. It has built-in intelligence via auto tuning
- **Azure DB for MySQL and Postgre SQL** - Both of the databases are fully managed and relational databases. They both are scalable databases with security and high availability. They both have a pay-as-you-go pricing model
- **SQL Data Warehouse** – It is a managed petabyte data warehouse with complete security at all levels without additional costs. It uses massively parallel processing technique to run complex queries along with these data. The data is imported into the Data Warehouse by Polybase. The data storage is in Columnar storage in relational database that reduces the query time as well as storage. The billing is on compute Data Warehouse Unit (cDWU). In this, there are two performance tiers; one is Elasticity, which is for short burst and peak activity. The other is Compute Optimized performance, which is used SDD for frequently accessed data and recommended for fat performance requirements. With SQL Data Warehouse, you can map any type of data on it
- **Cosmos DB** – It is a non-relational database with low latency and high availability. It is a globally distributed and multi-model service which includes SQL, MongoDB, Cassandra, Table and Germlin (raph). It gives you a guaranteed throughput and within a single region, it gives you 99.99% availability. It offers you

turnkey global replication. Cosmos DB replicates your data transparently wherever your users are so that they can interact with a replica of the data closest to them. It offers you five consistency models, from Strong SQL to relax NoSQL (the models include strong, bounded staleness, session, consistent prefix, and eventual consistency). It also automatically indexes all of your data

- **Redis Cache** - It is managed in-memory cache service with quick, scalable, open-source compatible data store for applications. It frequently uses caches and static data to minimize storage and latency of the application. It comes in three tiers: basic tier that is with a single node and used for test and dev, and non-critical workloads with volume of up to 350GB. Standard tier is two replicated nodes in primary and secondary configurations with a high-availability SLA (99.9%) and is managed by Microsoft. Premium tier offers caches with more functionality and with lower latencies and higher throughput. Premium tier caches are used on more powerful hardware that performs better than the basic or standard tier. It is useful for snapshots and VNET integration. Its size can be up to 530GB

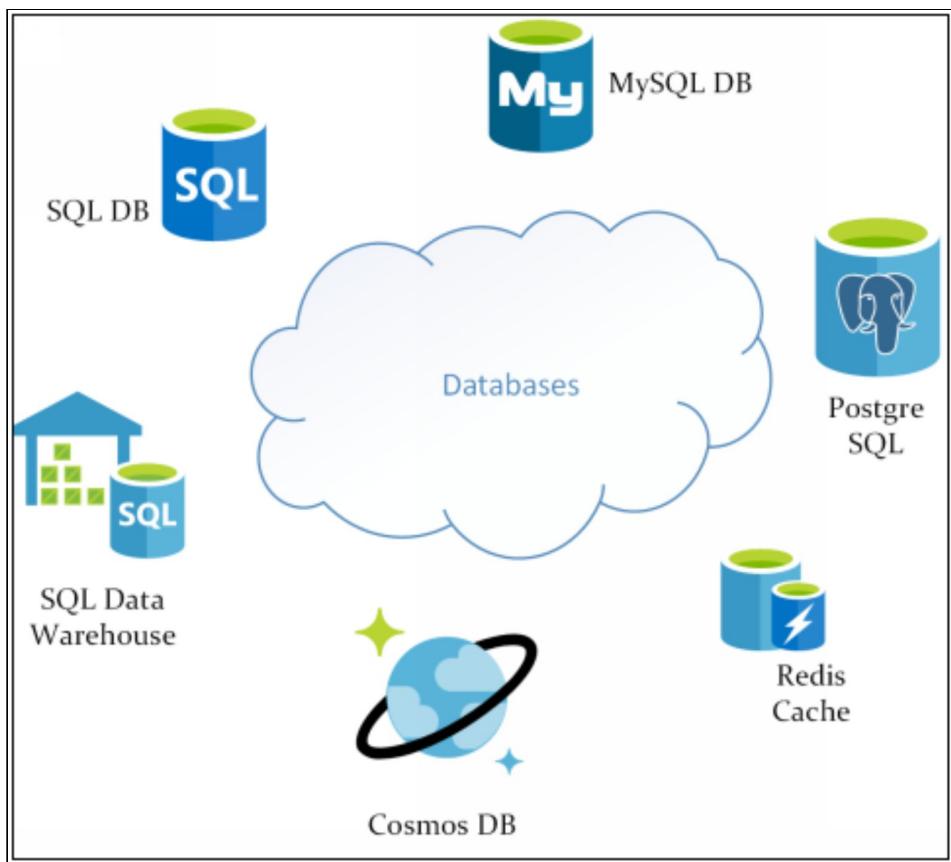


Figure 1-11: Azure Databases

Web and Mobile

Great web experience in today's business is important. Azure provides premium support for the creation and management of web applications and HTTP-based web services. Azure build engaging cross platforms for Android, iOS and Windows applications without any compromises that suit your business needs and reach to your customers everywhere. You can power your apps with smart back-end services and simplify your development cycle faster and more confidently.

- **App Service** - It is PaaS in Azure. It allows you to create and host web apps, mobile back ends and RESTful APIs without network maintenance in the programming language of your choice. It supports both Windows and Linux, automatic deployment from GitHub, Azure DevOps and any Git repo. It offers high availability and auto scaling. The supported

languages are .NET, .NET Core, Ruby, Java, PHP, Node.js and python. App Service runs in various “App Service Plans” from free to isolated

- **API Management** - API Management (APIM) is a way of creating reliable and functional back-end API gateways. API Management enables companies to publish APIs to external, partner, and internal developers to unlock their data and service potential. API Management consist of the following components:
 1. API Gateway has a tunnel feature that accepts the API calls and routes it to the backend. API gateway offers authorization and caching.
 2. Developer Portal is for developers that are used for developing the API. It is provided with documentation and different level of access requirements.
 3. Azure Portal is for the user to develop the API. Users can import existing APIs and create API products.
- **Media Services** - Cloud-based media workflow platforms allow you to build solutions requiring encoding, packaging, content protection and live broadcasting of events. The protection of the content is done via encryption. It also has streaming URLs that you provide to the user to download the streaming asset
- **Notifications Hub** – This gives you an ability to send mobile push notifications from any back-end (cloud or on-site) to any platform (iOS, Android, Windows, Kindle, Baidu, etc). For both corporate and customer applications, the Notification Hubs work well. You can also segment the user notification on the basis of tags so that certain notifications are sent to a certain group of users. You can also tailor your notification using user's language and their location. Scheduling of notification is also available. With this, you can also send silent push notifications to your application
- **Azure Search** - Azure Cognitive Search is the only cloud search service that has built-in AI capabilities, enriching all kinds of information for easy content recognition and discovery. It also performs a full text search using simple or lucene query syntax. The data uploaded is in JSON format. It also has the ability to

auto crawl various Azure services to get the data automatically. The supported services are Azure SQL DB, Cosmos DB and Azure Blob Storage. It supports filter, paging, and sort for the searches. It also has the ability for geo-based search.

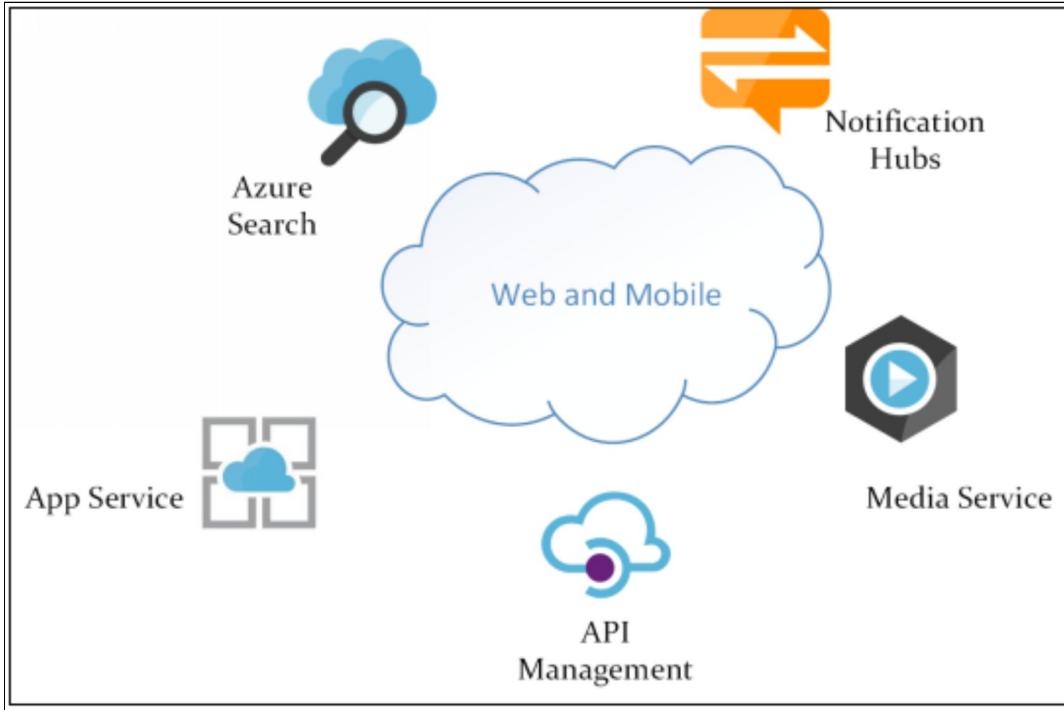


Figure 1-12: Web and Mobile

Security and Identity

We know that safety is one thing in the cloud and it is very important to have accurate and timely Azure Security information. Azure has a wide range of security tools and features that make it the best reason to use for your applications and services. Integrated Azure security services protect data, applications, and infrastructure quickly, this includes unparalleled security intelligence to help in identifying rapidly changing threats earlier, so you can react faster.

You can protect Azure identity and access management solutions for your applications and data on the front door. Defend malicious login attempts and secure passwords through risk-based access controls, identification security tools, and efficient authentication options, without interrupting productivity.

- **Azure Active Directory** – This is a cloud-based identity and access management service in Azure. It is one of the core services of Azure. With this service, the user can sign in and access the internal or external resources. The access can be role based and controlled access on various resources. With this, you can SSO for multiple clouds based SaaS applications with your company credentials. You can also authenticate your own applications by integrating it with this. You can also integrate your on-premises Windows AD
- **Azure Active Directory B2C** – This gives consumer identity and access management for your consumer based application. Your consumers can use their favorite social, company or local identity accounts to access your apps and APIs in an SSO interface. It is different from normal AD as it uses consumers to login and authenticate. It supports multiple languages
- **Azure Active Directory Domain Service** - Azure Active Directory Domain Services (Azure AD DS) offer fully Windows Server Active Directory-compatible, managed domain services such as Domain Join, Group policy, Lightweight Directory Access Protocol (LDAP) and Kerberos. There is no need of installing, maintaining and patching domain controllers in the cloud. You can use these domain services without a domain controller. It can be used in Cloud Only and Hybrid as well
- **Key Vault**- is a security service that can be used for key management in an encrypted form. When you deploy an application in the cloud, there are secrets and keys that are needed to access the DB or third party systems. So you need some service to store these and key vault is the most secure place for that. Keys in the key vault are protected by HSMs. For your own keys, it uses FIPS 140-2 Level 2 validated HSMs. With this, you can get real time usage logs of keys
- **Security Center** – This is a centralized network security management system that improves the security position of your data centers and provides advanced threat safety through your hybrid cloud workloads–whether in Azure or on site. It continuously checks your resources against the policy in order

to inform you about any incident at its earliest. If it finds any incident, it gives you a recommended action in order to resolve the issue. It also gives you a prioritized alert functionality as well. It comes in two tiers: free or standard. The standard is \$15 per server/month

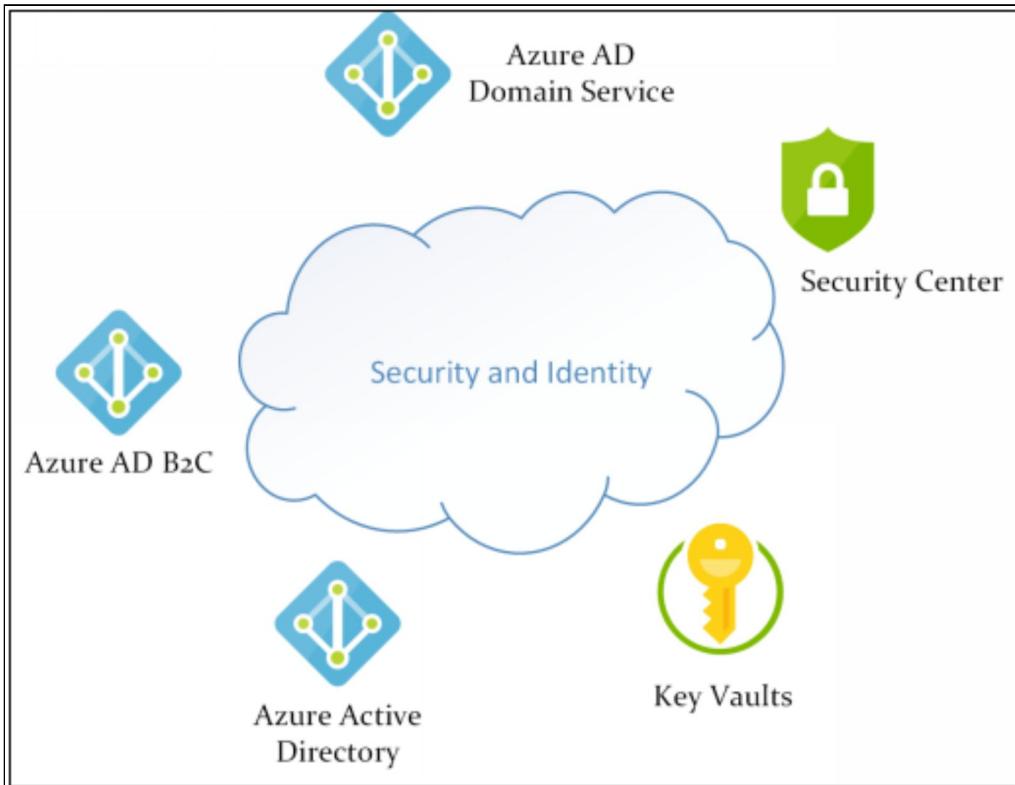


Figure 1-13: Security and Identity

Monitoring and Management

Azure management and governance tools help system managers and developers to secure and compliant the resources, both in-house and on the cloud. It monitors the infrastructure, software, system provision and set-up, app-updating, vulnerability detection, backup resources, disaster recovery, policy implementation, process automation, and even the management of costs— during the IT cycle.

- **Azure Policy** - Through this you can set and manage policies across the resources and monitor compliance
- **Azure Monitor** – This provides basic monitoring of Azure resources. It helps you understand how your applications work and recognize challenges and tools that impact them

proactively. With this, you can monitor metrics, activity log and diagnostic log

- **Application Insights** – This is a feature of Azure Monitor, is a robust APM (Application Performance Management) tool for Developer and Technical DevOps. You can use it for live application monitoring. This operates with applications on a wide range of different platforms, including. NET, Node.js and Java EE, hosting on site, hybrid, and other public clouds
- **Log Analytics** – This collects data from various sources and visualizes the data from sources like on premise and cloud. Log Analytics is the primary tool for collecting interactive analysis of log queries within the Azure portal
- **Azure-Site Recovery** – This is a service used for business continuity and DR. It gives highly available and built-in DR solutions. It has failover and fallback capability as well
- **Azure Backup** – This is a service in Azure that provides backup against data loss in cloud and on-premises. For backup, you have multiple options available

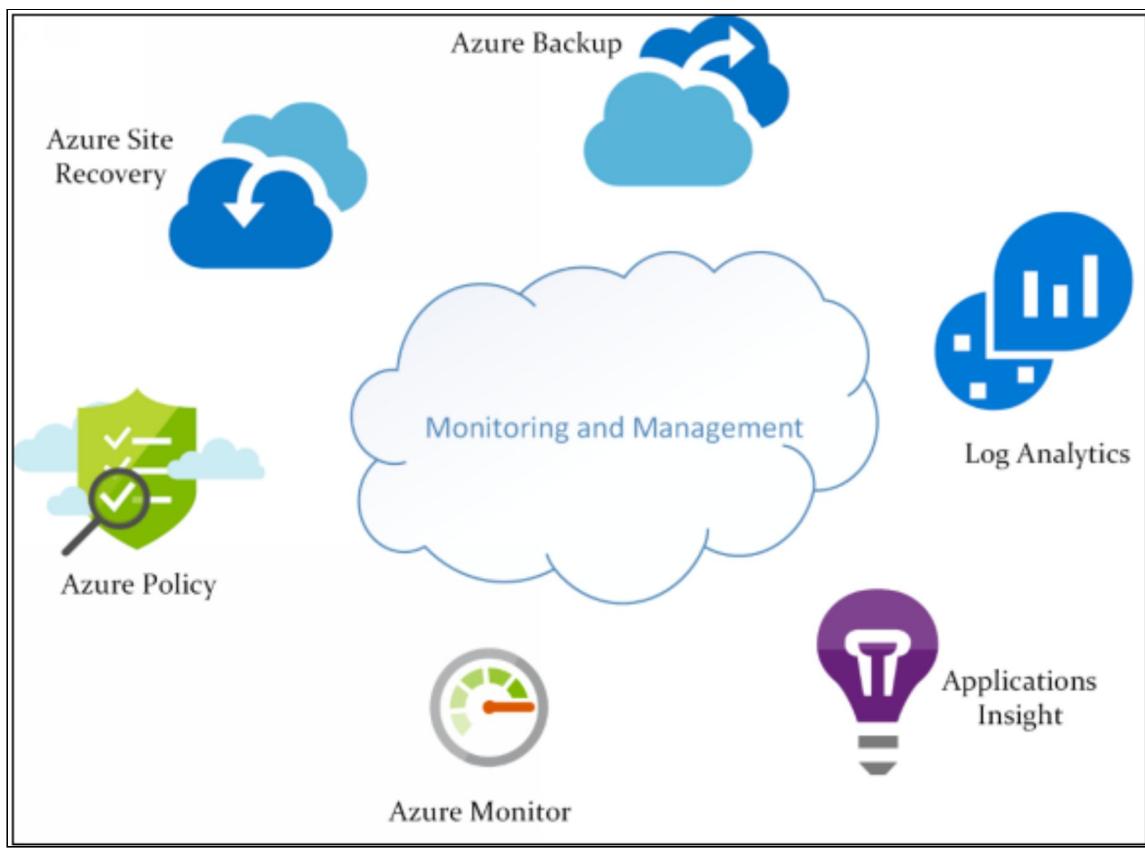


Figure 1-14: Monitoring and Management

MindMap

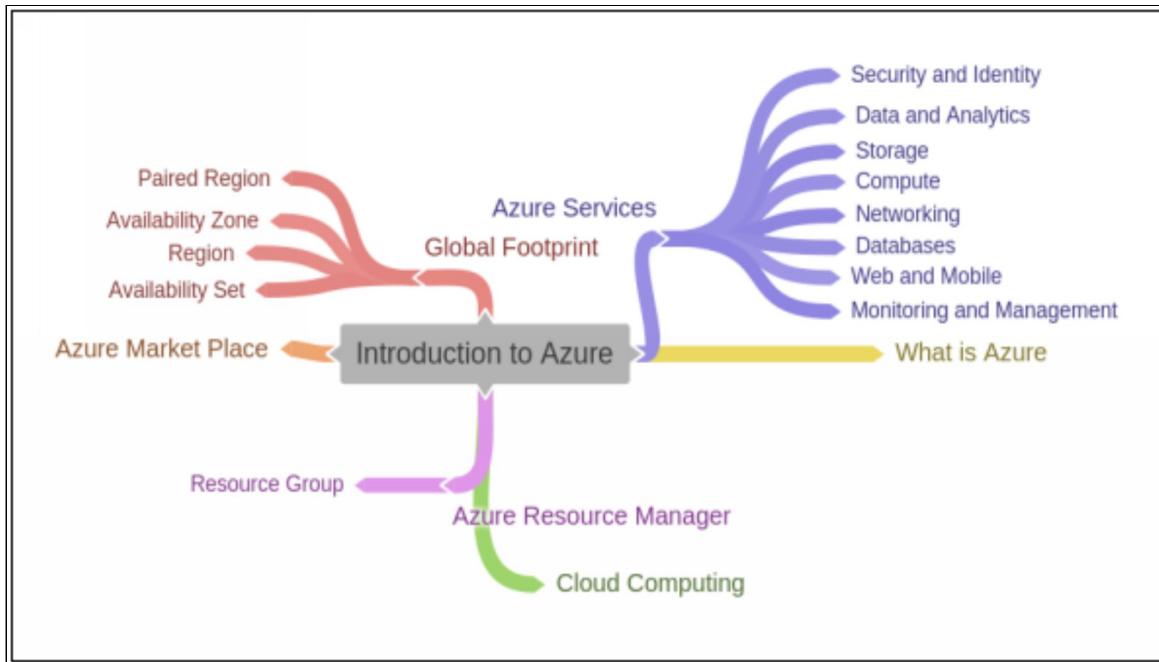


Figure 1-15: Mindmap

How to Interact with Azure

Azure Portal

In order to interact with Azure, Azure Portal is the most common way. Portal is just a website, where you fill your Microsoft account ID and password and login to Azure. With the portal, you get access to all the resources in Azure as well as on all its features. With the Azure portal, you can build, manage, and monitor everything like from simple apps to complex apps in a single console.

There are many benefits of using the Azure portal. Some of which are:

- You can personalize your Azure dashboard, layout, and workflow with colors
- With great accuracy, you can choose an access control on all resources that make your management and governance easier
- Cost management keeps an eye on the current and projected cost of resources
- It is like a One Stop shop where you have a single portal, single login for all of your Azure assets
- It has quick feature updates on products

- It has multi-platforms; it is available on the web and many other mobile devices

Azure CLI

Azure CLI is another tool that helps to interact with Azure services and features. It is only a text entry tool. In CLI, you need to enter a command to perform any action. Most Azure professionals use it frequently. Azure CLI can be downloaded from the website. The benefits of using Azure CLI are:

- It is stable, meaning commands do not change and can be used reliably
- The commands are structured in a logical way and all will follow the same pattern
- It is cross-platform, so it can work on Windows, Mac, and Linux
- As the command changes rarely in CLI, you can automate the commands for future purposes
- With CLI, you can keep track of who did what with the CLI command

You can always test the CLI that you installed to see if it has the proper version by running az --version. The CLI is designed to simplify scripting, query details, long term operations and more. The current version in use is 2.0.79. To login to azure, the first thing you need to do is write the “az login” command. A browser window will open asking you for login credentials. After logging in, you will see a list of all subscriptions associated with your account.

In order to install Azure CLI, write “Invoke-WebRequest -Uri <https://aka.ms/installazurecliwindows> -OutFile .\AzureCLI.msi; Start-Process msiexec.exe -Wait -ArgumentList '/I AzureCLI.msi /quiet” in Windows PowerShell.

You can also use the following link to download the CLI:
<https://docs.microsoft.com/en-us/cli/azure/install-azure-cli-windows?view=azure-cli-latest>

Azure PowerShell

It is just like Azure Command Line Interface (CLI). PowerShell is pre-installed in your windows machine and if it is not, then simply install it from the internet. PowerShell lets you use cmdlet that are small light weight groups of command through which you can perform simple tasks by calling a script, like to create a VM, you use command “New-AzVm”. With PowerShell, you can also use Azure Resource Manager just like the Azure portal. It can be used for any other tasks as well. PowerShell version 5.1 or higher can work on Windows while PowerShell core6.x and later versions can work on any other platforms. In order to check PowerShell version, type: \$PSVersionTable.PSVersion:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\a> 

PS C:\Users\a> $PSVersionTable.PSVersion

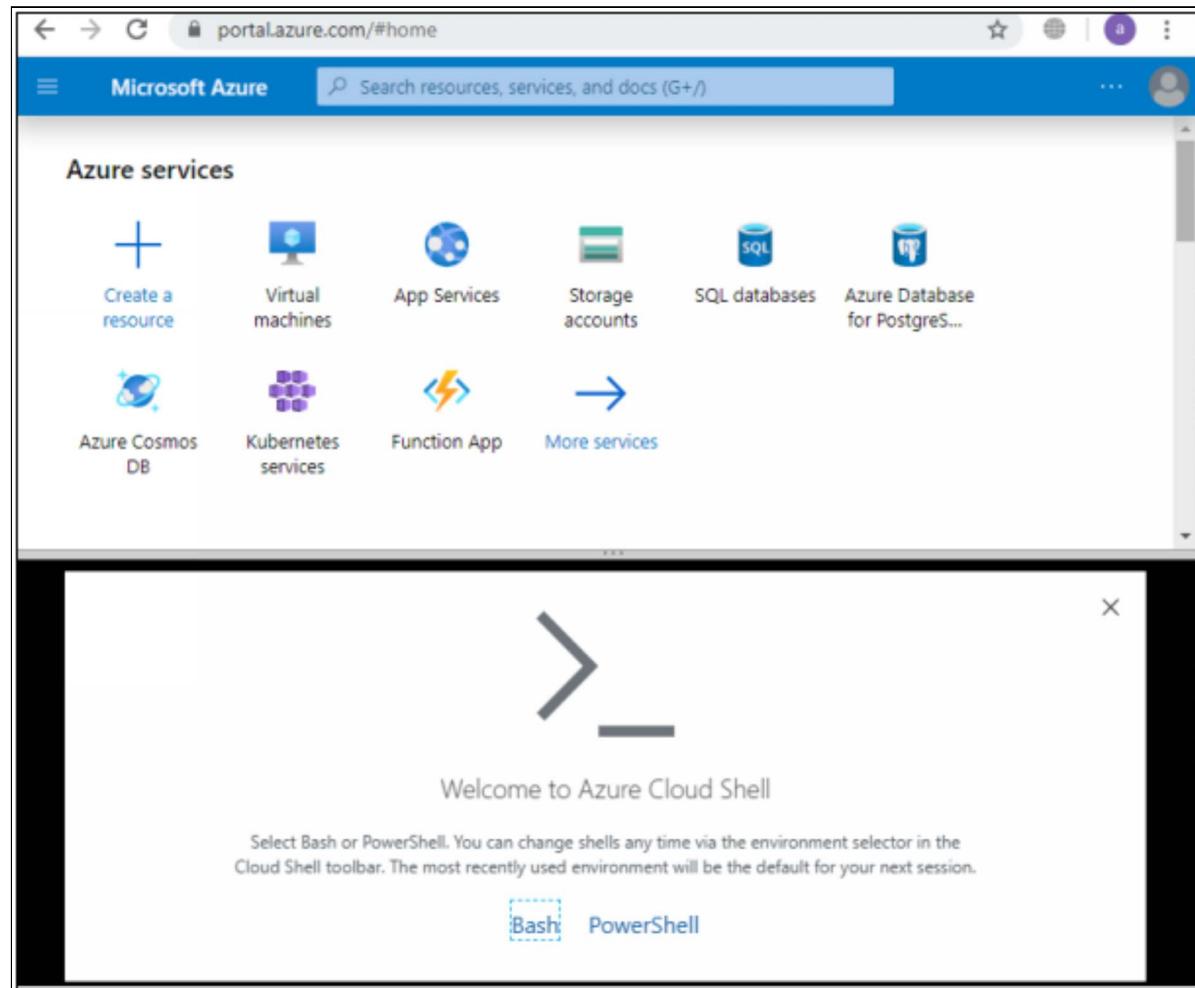
Major  Minor  Build  Revision
-----  -----  -----  -----
5       1       18362  145

PS C:\Users\a>
```

Azure Cloud Shell

An interactive browser-accessible shell for managing Azure resources. The shell experience is the best option, whether you work Bash or PowerShell as it offers flexibility. With Cloud Shell, you can either use a fully stand-alone browser or use the portal component to experience bash, which is similar to Azure CLI or PowerShell. With Cloud Shell, you get authenticated and secure access to the

resources using any web or mobile app from anywhere. Choose between Bash (CLI) or PowerShell. Tools included are interpreter, Azure tools, modules and different language support like Node.js, Python or .NET. In order to persist the data between sessions, it has its own dedicated storage. It also has integrated file editor.

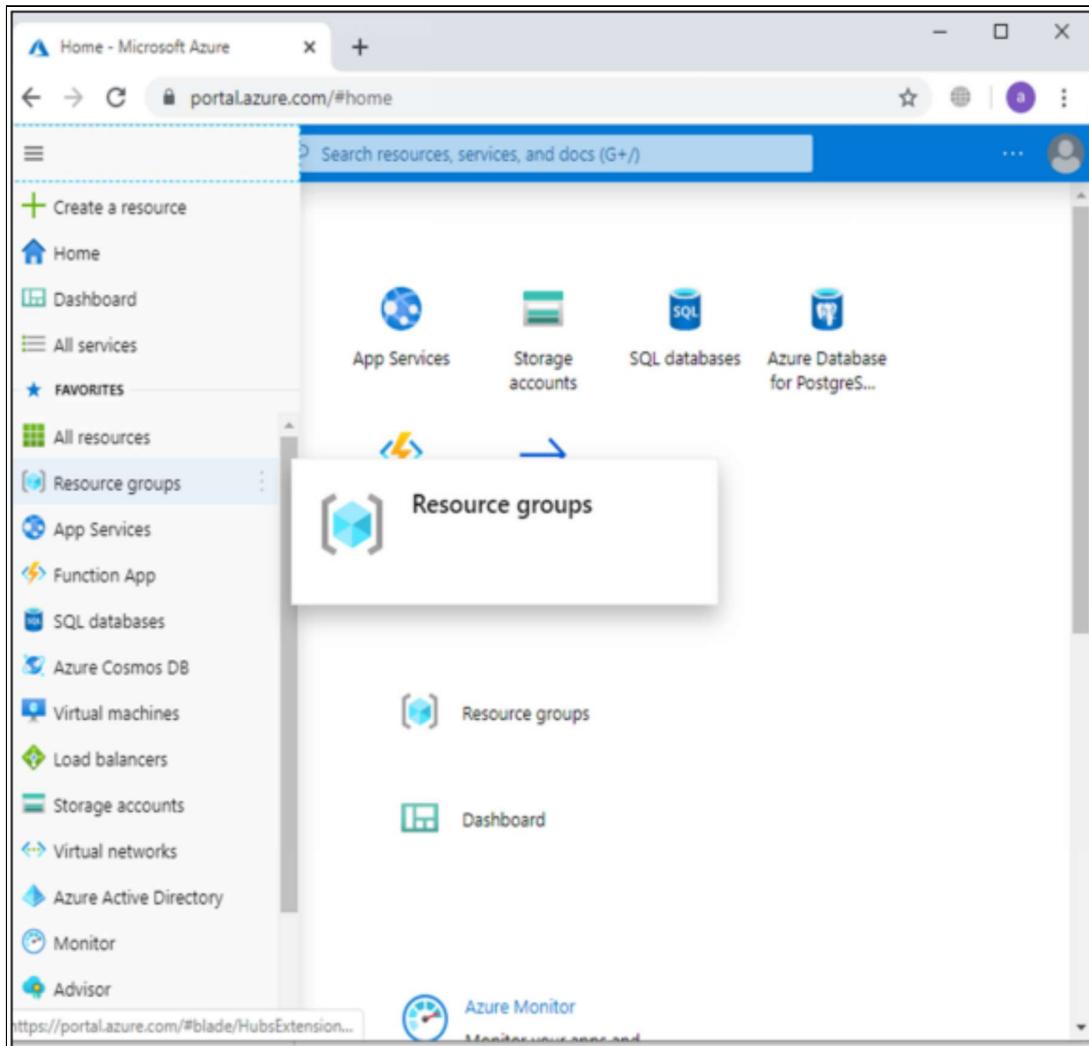


Creating an Account on Azure

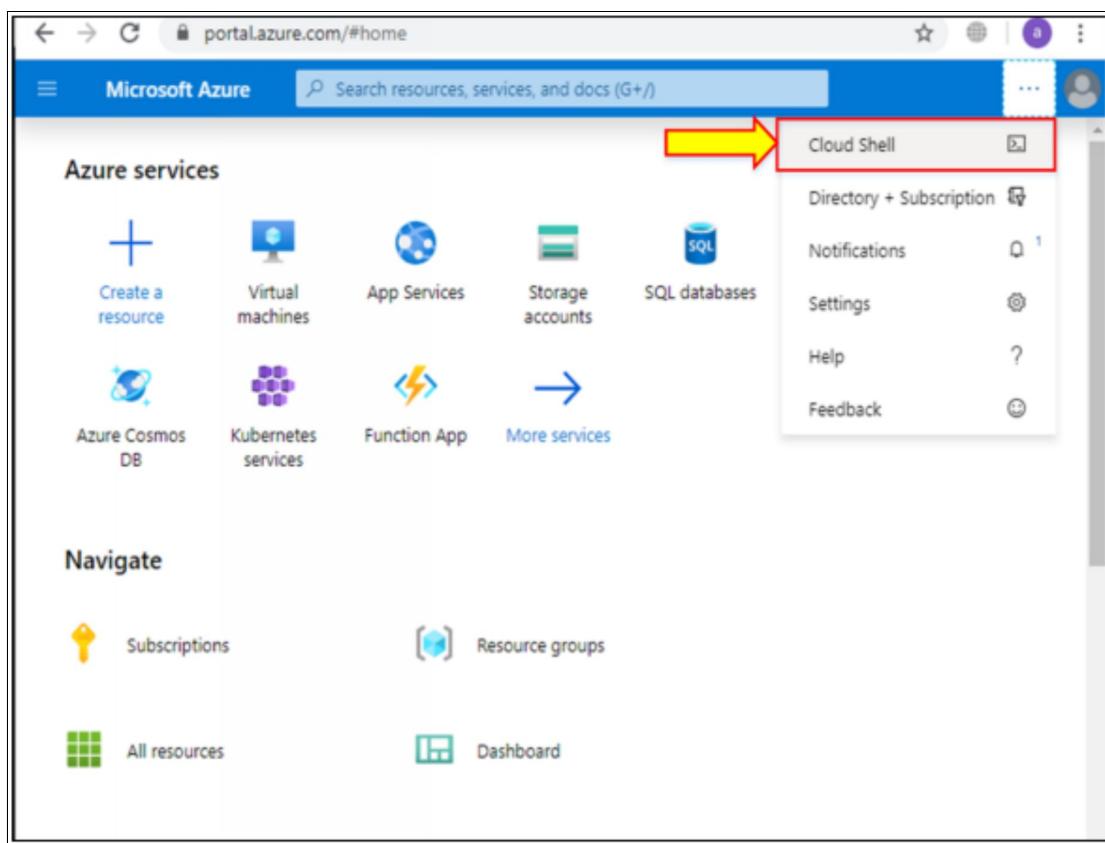
1. Create an account on Microsoft using your email address then go to "Azure.com".
2. Click on "Start free". Now Sign-in with the email address.
3. Go to the window of the sign-up process for creating a new account. In "About You" page, enter all the required details for sign-up then click "Next".
4. Now in "Identity verification by phone", enter the number with country code. Then you will get a message or call option to get the

verification code.

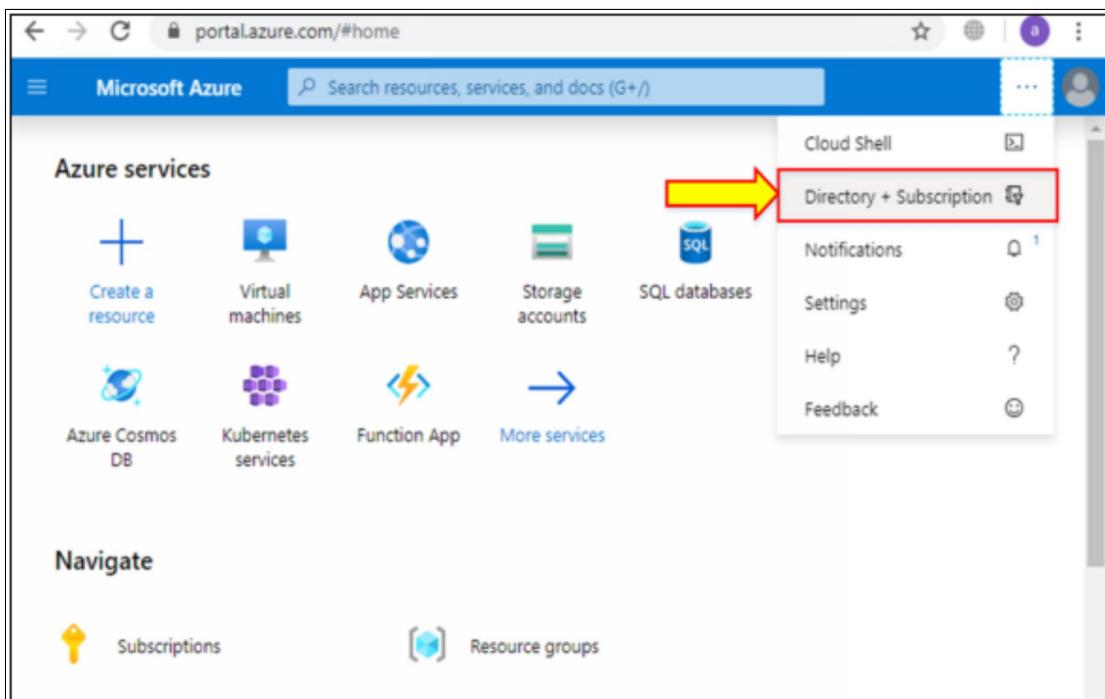
5. After verifying the code, enter the card information in “Identity verification by card”.
6. Click “Next”.
7. Then you have an agreement. Select the agreement then select “Sign-up”.
8. After signing up, click on “Go to Portal”. You will now get a pop-up window of Welcome to Azure with “start tour” or “maybe later” options.



9. In the top corner, you also have the “Cloud Shell” button.



10. You also have the “Directory and Subscription” filter on the top corner.



Note: The limitation of the free Azure Account is that you get free services for 12 months with credit expiration after 30 days.

Practice Questions:

1. Any service you use on Azure has a consumption component as part of the pricing is known as consumption-based pricing. True or false?
 - A. True
 - B. False
2. What does Infrastructure-as-a-Service mean?
 - A. Services on Azure that are updated automatically to provide a stable infrastructure for your applications
 - B. The layer of services that enable a complete cloud infrastructure for your business
 - C. Any hardware service provided by Azure such as Virtual Machines and Virtual Networks
 - D. Any service on Azure that you can rent and do not have to buy upfront
3. Which Azure service should you use to correlate events from multiple resources into a centralized repository?
 - A. Azure Log Analytics
 - B. Azure Monitor
 - C. Azure Events Hub
 - D. Azure Analysis Service
4. What is Cloud Agility?
 - A. To automatically improve the fidelity of resource usage and utilize the platform better
 - B. Quickly scale resource as per demand

- C. Focus on business rather than provisioning and maintaining the resources
 - D. Using cloud elasticity to increase the return on investment
5. As resource demand increases, Azure can split the demand over more resources and scale the application. True or false?
- A. True
 - B. False
6. In case any resource goes down, then instantly replacing it with a new one is known as_____.
- A. Scalability
 - B. Elasticity
 - C. Fault Tolerance
 - D. High Availability
7. What is the difference between OPEX and CAPEX?
- A. OPEX is the cost for acquiring or maintaining assets. CAPEX is an ongoing cost for running a business
 - B. OPEX has a better return on investment in the short term. CAPEX has a better return on investment in the long term
 - C. OPEX is an ongoing cost for running a business. CAPEX is the cost of acquiring or maintaining assets
 - D. OPEX is a cost on services you do not own, such as cloud computing. CAPEX is a cost of ownership
8. What is an Availability Zone?
- A. One or more datacenters equipped with independent power, cooling, and networking

- B. A collection of software that can enable high scalability at short notice
 - C. A set of data centers close together
 - D. One or more datacenters that are close together to provide backup
9. How many zones must each region have?
- A. 2
 - B. 3
 - C. 5
 - D. 6
10. What is Azure Region?
- A. One or more datacenters equipped with independent power, cooling, and networking
 - B. A collection of software that can enable high scalability at short notice
 - C. A set of datacenters close together
 - D. One or more datacenters that are close together to provide backup
11. A cloud server is being migrated to Azure. External users can access the web application. To reduce the administrative effort needed to manage the web application, which would you suggest from the following?
- A. IaaS
 - B. SaaS
 - C. FaaS
 - D. PaaS

12. Azure VM resource is a PaaS. True or false?
- A. True
 - B. False
13. For daily operations, Azure resources are needed for every business unit. The same form of Azure services is expected for all businesses. To automate the development of Azure resources, which solution would you suggest?
- A. Azure API Management Service
 - B. Resource Manager Template
 - C. Management Groups
 - D. None of the above
14. What is the limit of the amount of storage in Azure Storage?
- A. 30TB
 - B. 500GB
 - C. 500TB
 - D. 10TB
15. Which Azure Service is relevant to the AWS IAM service?
- A. Azure VM
 - B. Azure Blob
 - C. Azure MySQL DB
 - D. Azure Active Directory
16. From the following option, which is the best reason to use the Azure CLI?

- A. It makes it cheaper to use Azure, as you do not have to pay for the Azure Portal
 - B. You can use products and services that are not available in the Azure Portal
 - C. It rarely changes, and the commands stay the same for the most part
 - D. You can use Azure CLI with more than one cloud provider
17. Why would you prefer to use Cloud Shell rather than CLI or PowerShell?
- A. The Cloud Shell can be used entirely in a web browser and can be used across multiple devices
 - B. The Cloud Shell gets new features first
 - C. The Cloud Shell is free for 12 months
 - D. You can update the Cloud Shell independently of Azure CLI and Azure PowerShell
18. What is the limitation of Azure free account?
- A. Azure free accounts are valid only for certain times of promotion such as the launch of new services
 - B. Credit will expire after 30 days and free resources expire after 12 months
 - C. Free account resources can only be created when using the USA address
 - D. You are only allowed to create resources for 30 days
19. What is a PowerShell cmdlet?
- A. A PowerShell scripting language specifically for Azure
 - B. A piece of advice from Microsoft about PowerShell updates

C. A lightweight version of PowerShell that can run on mobile devices

D. A small lightweight group of commands to perform an action

20. Only products that are available globally can be accessed through Azure Portal. True or false?

A. True

B. False

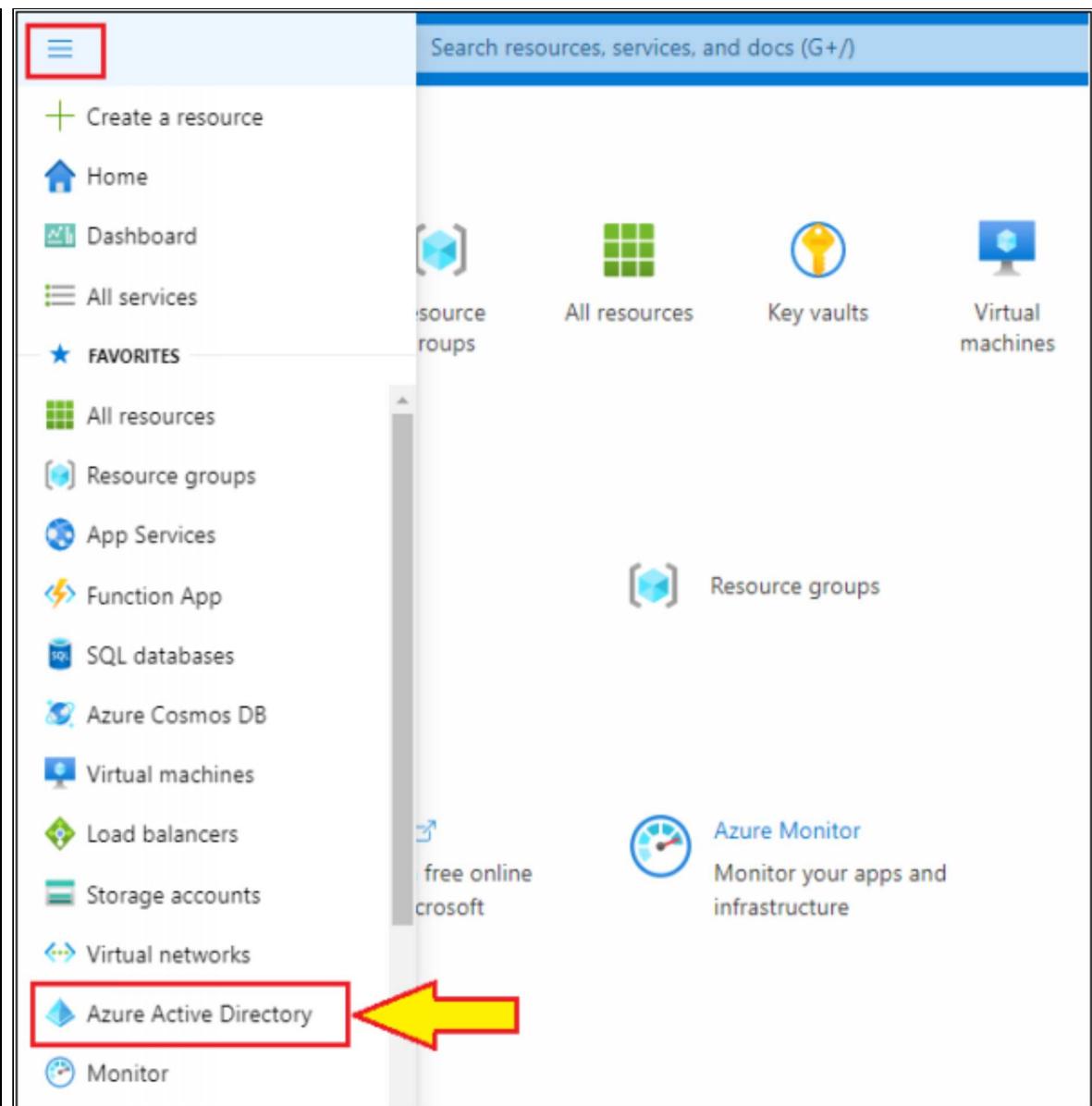
Chapter 02: Configuration and Management of Azure AD for Workloads

Azure AD Users

Azure AD is a Microsoft cloud based identity and access management service, which helps your employees sign in and access external resources such as Microsoft 365, Azure portal and thousands of other software and applications. You can also access internal resources such as apps on your corporate network and internet. A user is an account that requires access to Azure resources. User accounts can be of many types; it can be a work or school account or a cloud or guest account. You can manage Azure AD users through Azure portal, Azure PowerShell, and Azure CLI.

Lab 2-01: Creating an Azure AD User

You can create an Azure AD user account with Azure portal.
Sign in to your Azure portal and click on “Azure Active Directory”.



Now click on “Users”.

The screenshot shows the Azure Active Directory (Azure AD) portal. At the top, there are navigation links: 'Switch tenant', 'Delete tenant', '+ Create a tenant', 'What's new', and 'Preview features'. Below this, a message states: 'Azure Active Directory can help you enable remote work for your employees and partners. Learn more'. The main area is titled '(Default Directory)'. On the left, a sidebar titled 'Manage' lists several options: 'Overview', 'Getting started', 'Preview hub', 'Diagnose and solve problems', 'Users' (which is highlighted with a red box and has a yellow arrow pointing to it), 'Groups', 'External identities', 'Roles and administrators', 'Administrative units', and 'Enterprise applications'. To the right of the sidebar is a 'Tenant information' section and an 'Azure AD Connect' section. The 'Tenant information' section includes fields for 'Your role' (Global administrator), 'License' (Azure AD for Office 365), and 'Tenant ID'. The 'Azure AD Connect' section includes 'Status' (Enabled) and 'Last sync' (More than 1 day ago).

After that, you will see a list of active users.

Now, create a new user account by clicking on “New user”.

The screenshot shows the 'Users' page in the Azure portal. At the top, there are several buttons: '+ New user' (highlighted with a red box), '+ New guest user', 'Bulk operations', 'Refresh', 'Reset password', 'Multi-Factor Authentication', and 'Delete user'. Below these buttons, a message says: 'This page includes previews available for your evaluation. View previews →'. There is also a search bar labeled 'Search users' and a 'Add filters' button. At the bottom, it says '10 users found'.

Enter the required fields and click on Create. This will create your Azure AD user account in Azure portal.

Identity

User name ***** ⓘ Example: chris @ . ↘ The domain name I need isn't shown here

Name ***** ⓘ Example: 'Chris Green'

First name

Last name

Groups and roles

Groups 0 groups selected

Create

Now, create an Azure AD user account in PowerShell.

1. Write these commands in PowerShell; it will create your new Azure AD user account.

```

PowerShell v | ⌂ ? ⌂ ⌂ ⌂ ⌂ ⌂ ⌂ ⌂ ⌂ ⌂ ⌂
PS /home/ > $SecureStringPassword = ConvertTo-SecureString -String "Password.1" -AsPlainText -Force
PS /home/ >> New-AzADUser -DisplayName "Test User2" -UserPrincipalName "testuser2@.domain.com" -Password $SecureStringPassword -MailNickname testuser2
UserPrincipalName : testuser2@.domain.com
ObjectType : User
UsageLocation :
GivenName :
Surname :
AccountEnabled : True
MailNickname : testuser2
Mail :
DisplayName : Test User2
  
```

Activate Windows
Go to Settings to activate Windows.

Create an Azure AD user account in Azure CLI.

1. Write these commands in Azure CLI; it will create your new Azure AD user account.

```
Azure:~$ azure ad user create --display-name "Test User3" --password "Password.1" --user-principal-name testuser3
```

Azure AD Groups

Groups work similarly to the on-premises environment like in Azure active directory. These groups granted access to data or applications. In Azure, there are two different types of groups.

1. Security Groups

It is used to manage member and device access to shared resources. With security groups, you can give a set of permissions to all the members at once instead of having to individually add permissions to each member.

2. Office 365 Group

It provides collaboration by giving members access to a shared mailbox, calendar, SharePoint site, files, and more.

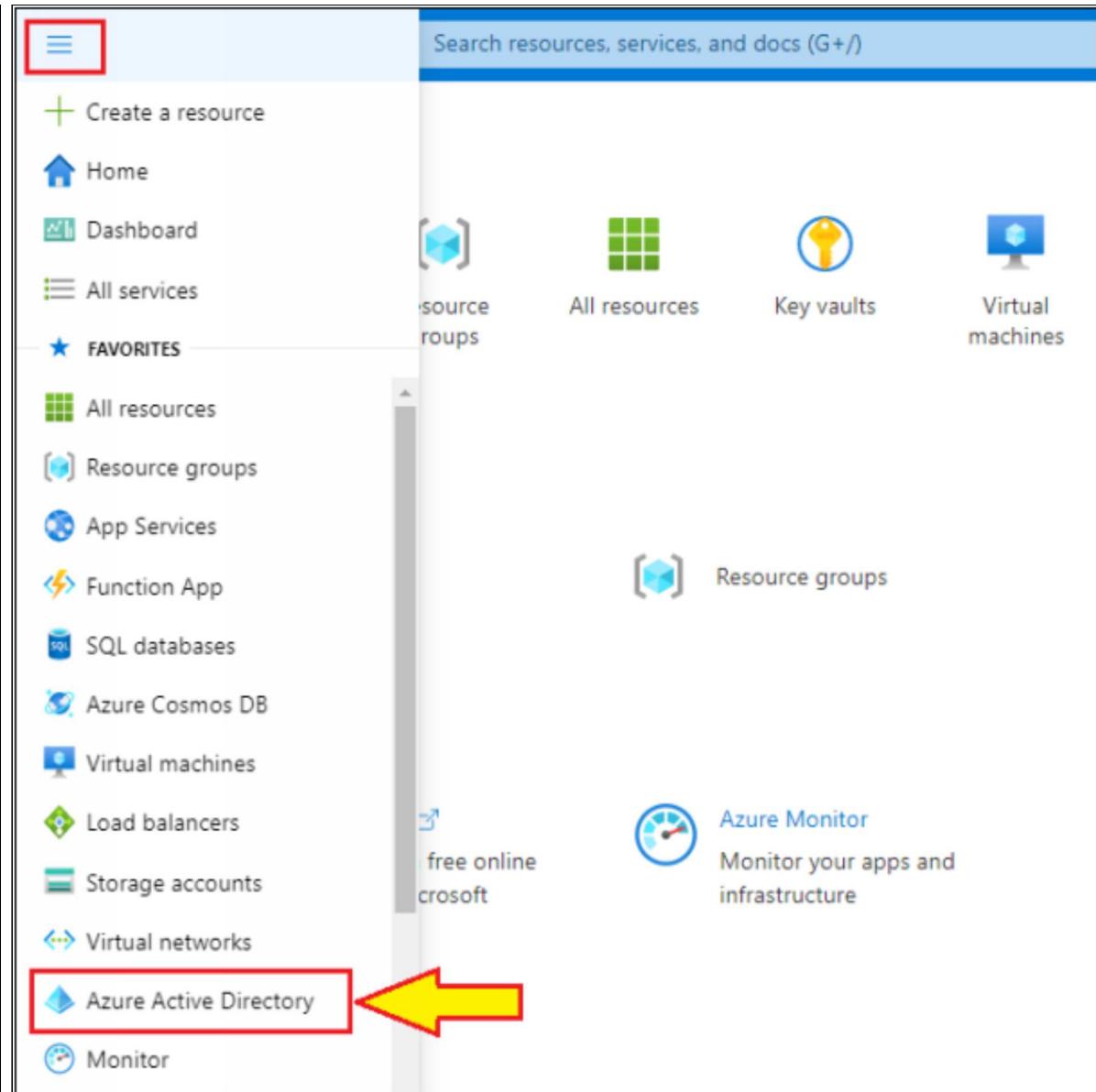
When you create a group, you will see three membership types:

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

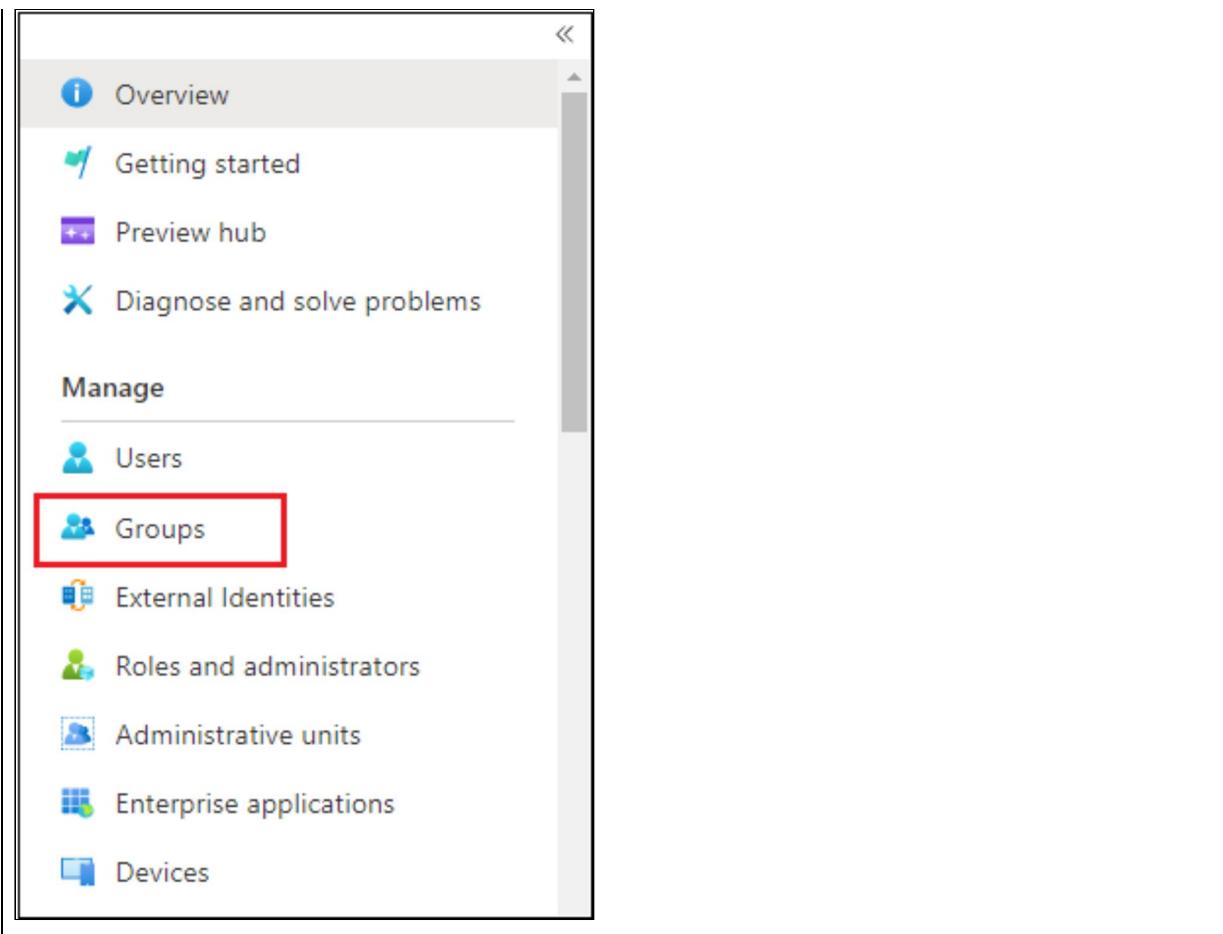
You can create groups through Azure portal, Azure PowerShell, and Azure CLI.

Let's create a group by using Azure portal.

Sign in to your Azure portal and click on “Azure Active Directory”.



Click on “Groups”.



Now, click on “New group”.

[+ New group](#) [Download groups](#) [Delete](#) [Refresh](#) | [Columns](#) [Preview features](#) [Got feedback?](#)

Enter the following parameters and click on “Create”. This will create your Azure AD group.

New Group

Group type * ⓘ

Security

Group name * ⓘ

Enter the name of the group

Group description ⓘ

Enter a description for the group

Membership type ⓘ

Assigned

Owners

No owners selected

Members

No members selected

Create



Now, create an Azure AD group using PowerShell.

1. Open PowerShell and write the following command to create your new Azure AD group.

```
PS /home/hanif> New-AzADGroup -DisplayName "Group" -MailNickname "Group"
```

```
SecurityEnabled : True
MailNickname    : Group
ObjectType      : Group
Description     :
DisplayName     : Group
Id              : d3b3b6e7-d29b-49e3-96cd-d999e6be0b2a
Type            :
```

Now, create an Azure AD group using Azure CLI.

1. Write the following command to create your new Azure AD group.

```
hanif@Azure:~$ az ad group create --display-name "Group" --mail-nickname "Group"
```

You have created Azure AD Groups using three different methods; Azure portal, Azure PowerShell, and Azure CLI.

App Registrations, Permissions, Scopes, and Consent

Users can use existing credentials to access applications with no more secondary logins. Microsoft identity providers based on complete authorization. Permissions are used to safeguard third party exposures. Access token is granted when you try to login to your account. First, you have to register and specify the application you want to use. Then, you can check the allow box for particular applications. Scopes are a group of information used to define what actions and applications are needed to be performed on behalf of the user against the set of resources. Scopes are basically a collection of permissions for the user. In order for an application to perform a task, users have to agree to a set of rules based on the particular applications. There are different types of consents like individual consent, administrator consent, etc.

Azure AD Connect

Azure AD connect is a tool to provide hybrid identity. Hybrid identity is simply an identity that exists on premises as well as on the cloud. You can use same credentials to access both on-premises applications and the cloud. The prerequisite of AD connect is the domain names server that you specify in your account.

Azure AD Connect Authentication Methods

You can use a single sign-on for all your accounts with Azure AD Connect. You have to choose the right authentication methods based on your usage of applications.

Federation Method:

It is one of the Azure AD connect authentication method. Federation is a collection of domains that establish trust. When an on-premises activity is federated with Azure AD, the trust is established; providing authentication, confirming who you say you are, and providing authorization to whether you are allowed to access or not. With the federation method, all user's identity is authorized on premises. It also supports smart card authentication. It is the only authentication solution that allows to display password authentication. Federation requires much more infrastructure and handles all your login requests inside your corporate network.

Password Hash Synchronization Method (PHS):

PHS synchronizes the hash of a user's on-premises password to Azure Active Directory. Using Azure AD connect, we can configure PHS so all cloud user authentication occurs in Azure AD. It can optionally be configured as a backup for federation method.

Pass-through Authentication Method (PTA):

PTA provides same seamless single sign on experience as PHS, but offers some additional security benefits. It does not require password hashes to be stored in the cloud. It only requires outbound connectivity from the on-premises authentication agents.

Multi-factor Authentication

Multi-factor authentication is simply logging into Azure AD using more than one form of authentication. It provides additional security for user accounts by requiring a second form of authentication. Typical authentication methods are a password, a device, and biometrics. It delivers strong authentication via a range of easy to use authentication methods. For example, text message, phone calls, authentication request via app, and authentication code via app and hard tokens. Multi-factor authentication can be bypassed based on the configuration of the product.

There are different types of multi-factor authentication available to meet organizational security requirements:

- Azure Cloud Multi-Factor Authentication
- Multi-factor authentication server
 - It is used to secure on premises resources like Remote desktop, Web apps, etc.
- RADIUS Integration
 - It is used for integration with VPN.
- Global Administrators

Sign in to your Azure portal. Click on “Azure Active Directory”. Now, click on “user” and then on “Multi-factor Authentication”.



You can enable or disable your multi-factor authentication status for every user.

MULTI-FACTOR AUTH
STATUS

Disabled

Disabled

Disabled

Disabled

Disabled

Disabled

You can also configure different services for multi-factor authentication by clicking on service settings.

multi-factor authentication

users service settings

Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. [Learn more about how to license other users.](#)
Before you begin, take a look at the [multi-factor auth deployment guide](#).

Choose the desired options and click on “Save”.

multi-factor authentication

users service settings

app passwords

- Allow users to create app passwords to sign in to non-browser apps
- Do not allow users to create app passwords to sign in to non-browser apps

verification options

Methods available to users:

- Call to phone
- Text message to phone
- Notification through mobile app
- Verification code from mobile app or hardware token

remember multi-factor authentication on trusted device

- Allow users to remember multi-factor authentication on devices they trust (between one to 365 days)

Number of days users can trust devices for

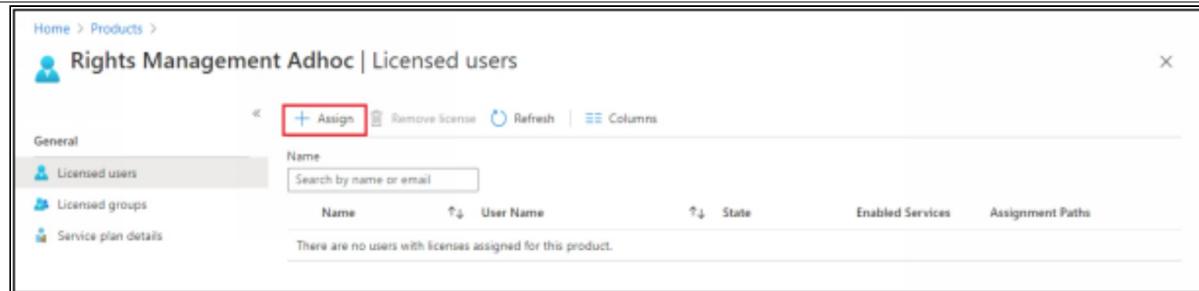
NOTE: For the optimal user experience, we recommend using Conditional Access sign-in frequency to extend risk sessions as an alternative to 'Remember MFA on a trusted device' settings. If using 'Remember MFA on a t more days.

save

Conditional Access

Conditional Access is automated access control that strengthens user sign-in and access to cloud applications. It is not used as a first factor authentication; passwords are still required for conditional access. It can be used to require multi-factor authentication. Access policies are the focus of conditional access. Policies are based on conditional and access controls. If you fail to carefully execute conditional access policies, it could have catastrophic consequences.

You can add a license to the user account by clicking on the “Assign” button.



The screenshot shows a user interface titled "Rights Management Adhoc | Licensed users". At the top, there is a navigation bar with "Home > Products >" followed by the main title. Below the title, there are three tabs: "General", "Licensed users" (which is selected and highlighted in grey), "Licensed groups", and "Service plan details". On the right side, there is a search bar labeled "Search by name or email" and a table header with columns: "Name", "User Name", "State", "Enabled Services", and "Assignment Paths". A red box highlights the "Assign" button, which is located just above the search bar. The table body below the header contains the message: "There are no users with licenses assigned for this product."

You can now add conditional access by clicking on the conditional access box.

SECURITY (22)

-  Security Center
-  Azure Information Protection
-  Application security groups
-  Extended Security Updates
-  Azure AD Identity Protection
-  Azure AD Authentication methods
-  Azure AD Conditional Access
-  Azure AD Risky sign-ins
-  Azure AD Named locations
-  Azure AD Privileged Identity Management
-  User settings
-  Key vaults
-  Azure Active Directory
-  Azure Sentinel
-  Azure AD Security
-  Azure AD Identity Secure Score
-  Multi-Factor Authentication
-  Azure AD Risky users
-  Azure AD Risk detections
-  Azure AD Password protection
-  Disk Encryption Sets
-  Azure Defender for IoT

By clicking on Azure AD conditional access, you will see a list of all the policies. You can also create a new policy by clicking on the “New Policy” box.

Conditional Access | Policies

Azure Active Directory

+ New policy  What if  Got feedback?

 Policies  Create your own policies and target specific conditions like Cloud apps, Sign-in risk, and Device platforms with Azure AD Premium →

 Insights and reporting

 Diagnose and solve problems

 Manage

 Named locations

 Custom controls (Preview)

 Terms of use

What is conditional access?

Conditional Access gives you the ability to enforce access requirements when specific conditions occur. Let's take a few examples

Conditions	Controls
When any user is outside the company network	They're required to sign in with multi-factor authentication
When users in the 'Managers' group sign-in	They are required to be on an Intune compliant or domain-joined device

If you want to create a new location in Azure AD conditional access policies, click on “Named locations” and then on “New location”.

Conditional Access | Named locations

Azure Active Directory

Policies + New location Configure MFA trusted IPs

This view will soon be replaced with the 'Named locations (preview)' view. Try it out.

Named locations are used by Azure AD security reports to reduce false positives and Azure AD conditional access policies. Learn more

Search locations.

Name	Trusted
No named locations found.	

Enter the required fields and click on “Create”.

All services > Conditional Access >

New named location

Upload Download

Name *

Example: 'Redmond office'

Define the location using:

IP ranges
 Countries/Regions

Mark as trusted location ⓘ

IP ranges

Add a new IP range (ex: 40.77.182.32/27) ***

No IP ranges

Create

Azure AD Identity Protection

Stolen user identities are the number one cause of security breaches. Attackers leverage phishing attacks and malware to gain access to systems. Even low-level user accounts can be used to gain access to a majority of network resources. Administrators must protect all identities, no matter the privilege level and ensure that compromised identities do not gain access. This typically involves full time awareness and monitoring of all user identities. The administrative effort is huge, and most of the time completely reactive in nature. Azure AD identity protection removes much of this effort by providing a comprehensive solution that:

- Proactively prevents compromised identities from accessing resources.
- Provides recommendations to improve security by analyzing vulnerabilities, such as user and sign-in risk levels and risk events, as well as environmental factors.
- Notifies administrators of risk events.
- Allows administrators to create policies to automatically mitigate risk events.

Azure AD identity protection is designed to mitigate two types of risks.

1. Sign-in Risk

- This type of risk represents the likelihood a given authentication request is not authorized by the identity owner.
- Sign-in risk can be evaluated in two ways:
 - Sign-in risk (Real time)
 - Sign-in risk (Aggregate)

2. User Risk

- This type of risk represents the likelihood a given identity is compromised.
- It is calculated by:
 - All risky sign-ins
 - All risky events not linked to a sign-in
 - The current user risk

- Any risk remediation or dismissal actions

Types of risk events

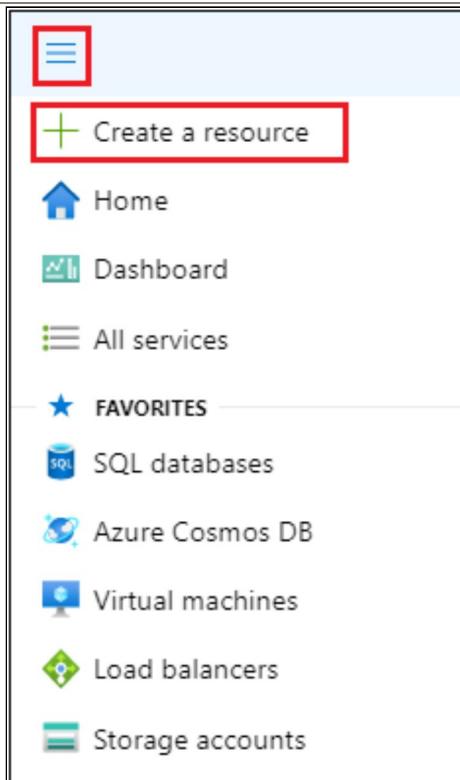
- Anonymous IP Addresses
- Unfamiliar sign-in properties
- IP addresses link to malware
- Leaked credentials

Azure AD Identity Protection Configuration Steps

- License users
- Onboard Azure AD Identity Protection
- Configure MFA policy (optional but recommended)
- Configure user risk policy
- Configure sign-in risk policy
- Test the configurations

Now, let's create Azure AD identity protection.

1. Sign in to your Azure portal and click on “Create a resource”.



2. Click on Azure AD identity protection, and then click on

“Create”.

The screenshot shows the 'SECURITY (22)' section of the Azure Security Center. On the left, there's a list of security features: Security Center, Azure Information Protection, Application security groups, Extended Security Updates, Azure AD Identity Protection (which is highlighted with a red box), Azure AD Authentication methods, and Azure AD Conditional Access. On the right, there are several preview features: Key vaults, Azure Active Directory, Azure Sentinel, Azure AD Security, Azure AD Identity Secure Score, Multi-Factor Authentication, and Azure AD Risky users.

3. First, configure MFA registration policy by clicking on the MFA registration policy box and then click on “Save”.

The screenshot shows the 'Identity Protection | MFA registration policy' configuration page. On the left, there's a sidebar with 'Overview', 'Protect' (User risk policy, Sign-in risk policy, MFA registration policy - highlighted with a red box), 'Report' (Risky users, Risky sign-ins, Risk detections), and 'Notify' (Users at risk detected alerts, Weekly digest). The main area shows the 'Policy Name' as 'Multi-factor authentication registration policy' and 'Assignments' for 'Users' (All users). There are two informational cards: one about MFA registration policy affecting cloud-based Azure MFA and another for Azure AD Premium P2 customers. At the bottom, there's an 'Enforce policy' switch (On) and a 'Save' button (highlighted with a red box).

4. Configure the user risk policy by clicking on “User risk policy” and then click on “Save”.

Identity Protection | User risk policy

Search (Ctrl+ /) <

Policy Name
User risk remediation policy

Assignments

Users
All users

User risk ⓘ
Low and above

This view is for Azure AD Premium P2 customers to setup user risk policy. Other customers can only disable.

Enforce policy
On Off

Save

5. For the last step, you will need to configure the sign-in risk policy by clicking on “Sign-in risk policy” and then click on “Save”.

Identity Protection | Sign-in risk policy

Search (Ctrl+ /) <

Policy Name
Sign-in risk remediation policy

Assignments

Users
All users

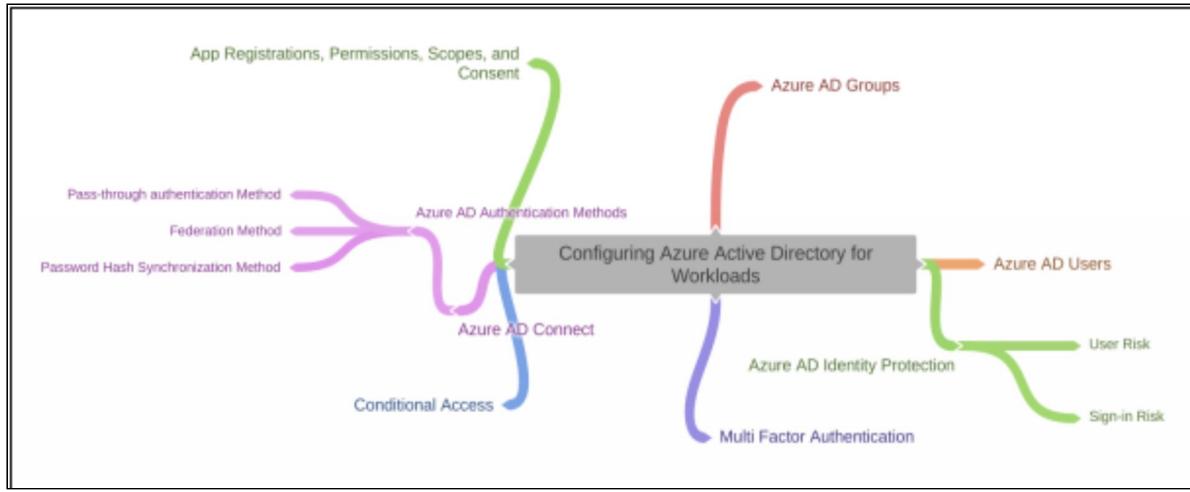
Sign-in risk ⓘ
Low and above

This view is for Azure AD Premium P2 customers to setup sign-in risk policy. Other customers can only disable.

Enforce policy
On Off

Save

Finally, you have configured Azure AD identity protection management.



AD PIM Overview and Activation

Azure Active Directory Privileged Identity Management (PIM) provides privileged access to Azure AD and Azure resources. It also provides Time-bound (expiring) access to resources, Approval requirements to activate privileged roles and Multi factor authentication enforcement to activate any role. It also shows pop-up Notifications when privileged roles are activated, and Downloadable history for internal or external audit.

In addition to management of AD directory roles, PIM allows for on-demand management of members for Azure resource rules. These include:

- Owner
- Contributor
- User Access Administrator
- Security Admin

Subscription-level roles and Azure Management Groups can be managed with PIM.

There are some relevant terms used in PIM architecture. You should review these to better understand PIM management of AD roles and Azure resources.

- Eligible
- Active
- Activate
- Activated
- Assigned
- Permanent Eligible
- Permanent Active
- Expire Eligible
- Expire Active
- Just-in-time (JIT) Access
- Principle of Least Privilege Access

PIM Activation

To activate PIM, you must be a Global Administrator. You must use an organizational account (not a personal account). Upon activation, you are automatically assigned the Security Administrator and Privileged Role Administrator roles in Azure AD.

To activate PIM, click on the security tab and then on “Azure AD privileged Identity Management”.

The screenshot shows the Azure Security blade with the title "SECURITY (22)". Below the title is a list of security-related services. The "Azure AD Privileged Identity Management" service is highlighted with a red rectangular box and a large yellow arrow pointing to it. Other services listed include Security Center, Key vaults, Azure Information Protection, Azure Active Directory, Application security groups, Azure Sentinel, Extended Security Updates (marked as PREVIEW), Azure AD Security, Azure AD Identity Protection, Azure AD Identity Secure Score, Azure AD Authentication methods, Multi-Factor Authentication, Azure AD Conditional Access, Azure AD Risky users, Azure AD Risky sign-ins, Azure AD Risk detections, Azure AD Named locations, Azure AD Password protection, Disk Encryption Sets, and Azure Defender for IoT.

SECURITY (22)	
Security Center	Key vaults
Azure Information Protection	Azure Active Directory
Application security groups	Azure Sentinel
Extended Security Updates PREVIEW	Azure AD Security
Azure AD Identity Protection	Azure AD Identity Secure Score
Azure AD Authentication methods	Multi-Factor Authentication
Azure AD Conditional Access	Azure AD Risky users
Azure AD Risky sign-ins	Azure AD Risk detections
Azure AD Named locations	Azure AD Password protection
Azure AD Privileged Identity Management	Disk Encryption Sets
User settings	Azure Defender for IoT

The portal of Azure AD Privileged Identity Management will open up. You will be able to explore many options in your PIM portal.

Privileged Identity Management | Quick start

You are using the updated Privileged Identity Management experience for Azure AD roles.

What's new Get started

Manage your privileged access

Use Privileged Identity Management to manage the lifecycle of role assignments, enforce just-in-time access policy, and discover who has what roles. [Learn more](#)

Azure AD Roles

You can use Azure AD roles to add an eligible member to a privileged group. You can also convert eligible assignments to permanent or vice-versa.

Privileged Identity Management

Azure AD PIM is a Premium feature that enables you to limit standing admin access to privileged roles and much more. [Learn more](#)

Assign

Assign users or current admins as eligible admins for specific Azure AD roles, so that they only have access when necessary

Activate

Activate your eligible admin roles so that you can get limit standing access to the privileged identity

Approve

View and approve all activation request for specific Azure AD roles that you are configured to approve

Assign Eligibility Activate your role Approve requests

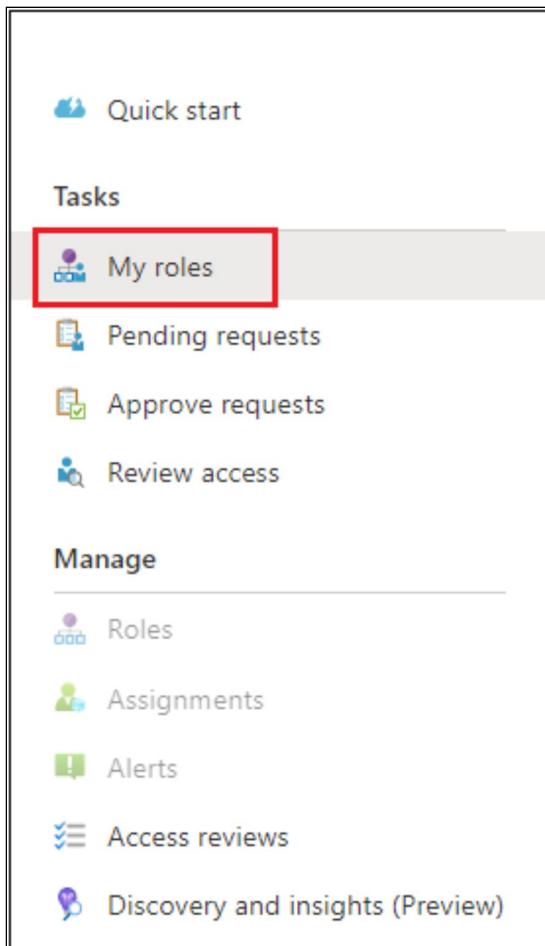
PIM Security Wizard

Use the Security Wizard to determine the current membership of all high-privileged AD Security roles. You can then use the wizard to reduce the number of permanently assigned role holders by converting those to eligible role assignments.

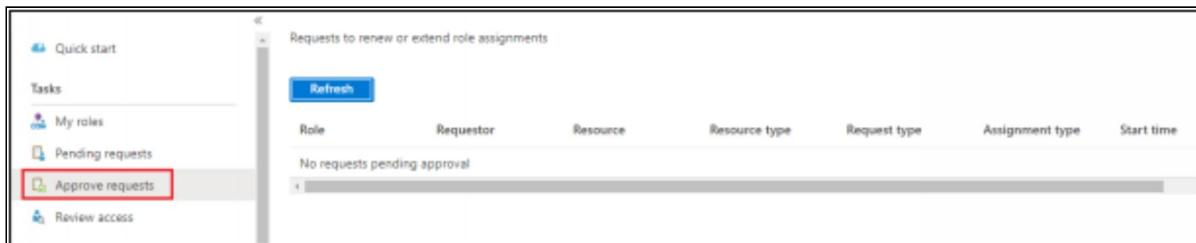
You can choose not to act on any security assignments at the time and instead perform the changes later. If you choose to modify the

security assignments, make sure the changes are announced to all administrators and business units ahead of time. At least one organizational account (not a personal account) must hold permanent Global Administrator and Privileged Role Administrator rights. If there is only one Privileged Role Administrator in the organization, the organization will not be able to manage PIM if that account is deleted.

Use “My roles” option to view and activate any Azure AD or Azure resource privilege elevation.



Use “Approve requests” to view and approve any requests for Azure AD or Azure resource privilege elevation.



Administrative Units

This section defines administrative units in Azure Active Directory (Azure AD). An administrative unit is an Azure AD resource that can be a container for other Azure AD resources. Only users and groups may be part of an administrative unit.

Permissions in a role are restricted by administrative units to any portion of the company that you identify. For example, you might use administrative units to delegate the Helpdesk Administrator role to regional support specialists so that they can only manage users in the region they support.

Manage Administrative Units

The Azure portal, PowerShell cmdlets and scripts, and Microsoft Graph can all be used to manage administrative units.

You may delegate users to an Azure AD role with a scope limited to one or more administrative units for more granular administrative control in Azure Active Directory (Azure AD).

Add an Administrative Unit

You can add an administrative unit by using either the Azure portal or PowerShell.

Use the Azure Portal

1. In the Azure portal, go to Azure AD. Then, on the left pane, select **Administrative units**.

The screenshot shows the Azure Active Directory Overview page. At the top left is a blue circular icon with a white 'i'. To its right is the word 'Overview' in large black font, followed by 'Azure Active Directory' in smaller gray font. Below this is a search bar with a magnifying glass icon and the placeholder 'Search (Ctrl+ /)'. To the right of the search bar is a 'Switch' button with a gear icon. On the left side, there's a vertical navigation menu with several items: 'Overview' (selected), 'Getting started', 'Diagnose and solve problems', 'Manage' (selected), 'Users', 'Groups', 'Organizational relationships', 'Roles and administrators', and 'Administrative units' (which is highlighted with a red rectangular border). On the right side, there's a sidebar with a blue circular icon and the word 'Azure'. Below it are sections for 'Overview' (underlined in blue), 'Tenant ID', 'Find' (underlined in blue), and a 'Users' button.

2. Select the **Add** button at the upper part of the pane, and then, in the **Name** box, enter the name of the administrative unit. Optionally, add a description of the administrative unit.
3. Select the blue **Add** button to finalize the administrative unit.

Add administrative unit

[+ Add](#) [Delete](#) | [Got feedback?](#)

Name	Description
<input type="text"/> Search administrative units	
Display Name	Description
<input type="checkbox"/> Mexico IT department	
<input type="checkbox"/> Redmond security org	
<input type="checkbox"/> UK Manufacturing	This unit is fo
<input type="checkbox"/> Seattle Operations	

Name *
Enter the name of the administrative unit

Description
Enter the description of the administrative unit

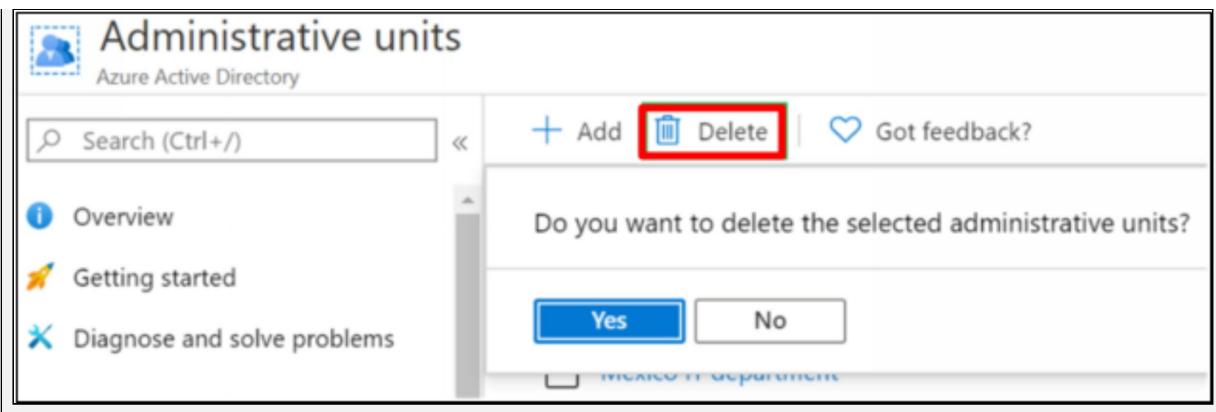
Add

Remove an Administrative Unit

In Azure AD, you can remove an administrative unit that you no longer need as a unit of scope for administrative roles.

Use the Azure Portal

1. In the Azure portal, go to **Azure AD** and then select **Administrative units**.
2. Select the administrative unit to be deleted, and then select **Delete**.
3. To confirm that you want to delete the administrative unit, select **Yes**. The administrative unit will be deleted.

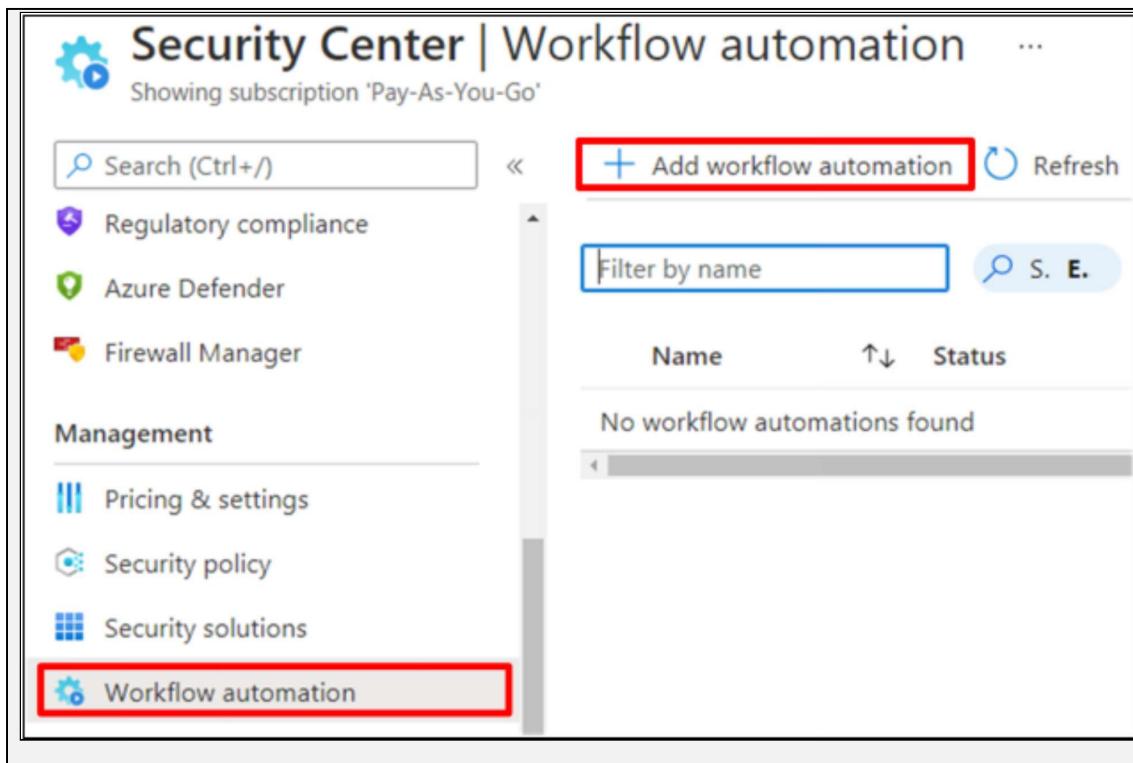


Configure Workflow Automation by using Azure Security Center

In this tutorial, we will learn and understand the workflow automation feature of Azure Security Center. This feature allows Logic Apps to be enabled in response to security alerts and recommendations. Every security software, on the other hand, requires several incident response workflows. Notifying relevant stakeholders, initiating a change management process, and implementing specific remediation measures are examples of these processes. Security professionals recommend that you automate as many steps of such procedures as possible. That is to say; automation lowers overhead while also increasing security by ensuring that process steps are completed consistently and according to requirements.

Creating a Logic App and Defining Automatically Running Process

1. Firstly, from Security Center's sidebar, select **Workflow automation**.



Here, on this page, you can create new automation rules, as well as enable, disable, or delete existing ones.

2. To define a new workflow, click **Add workflow automation**.

A pane appears with the options for your new automation. Here, you can enter:

- a. A name and description for the automation.
- b. The triggers that will initiate this automatic workflow. For example, you might want your Logic App to run when a security alert that contains "SQL" is generated.
- c. The Logic App that will run when your trigger conditions are met.

Add workflow automation

General

Name *

Description

Trigger conditions ⓘ

Choose the trigger conditions that will automatically trigger the configured action.

Select Security Center data types *

 Threat detection alerts

Alert name contains ⓘ

Actions

Configure the Logic App that will be triggered.

Choose an existing Logic App or [visit the Logic Apps page](#) to create a new one

Show Logic App instances from the following subscriptions *

 Pay-As-You-Go

Logic App name ⓘ

 No Logic Apps available

[Refresh](#)

Create

Cancel

3. From the Actions section, click **Create a new one** to begin the Logic App creation process.

You will be taken to Azure Logic Apps.

4. Enter a name, resource group, and location, and click **Create**.

The screenshot shows the 'Logic App' creation page. At the top, there's a breadcrumb navigation: Home > Logic App. Below it, the title 'Logic App' and a 'Create' button. The form fields are as follows:

- Name ***: A text input field.
- Subscription ***: A dropdown menu showing 'Pay-As-You-Go'.
- Resource group ***: A dropdown menu. The 'Create new' option is selected (indicated by a blue circle), and the 'Use existing' option is available.
- Location ***: A dropdown menu.
- Log Analytics**: A toggle switch with 'On' and 'Off' options, currently set to 'Off'. A tooltip below it says: 'You can add triggers and actions to your Logic App after creation.'

At the bottom right of the form are two buttons: a red-bordered 'Create' button and a 'Automation options' link.

5. In your new logic app, you can choose from built-in, predefined templates from the security category. Or, you can define a custom flow of events to occur when this process is triggered.

The logic app designer supports these Security Center triggers:

- When an Azure Security Center Recommendation is created or triggered
- When an Azure Security Center Alert is created or triggered
- When a Security Center regulatory compliance assessment is created or triggered.

6. After you have defined your logic app, return to the workflow automation definition pane ("Add workflow automation").
7. Click **Refresh** to ensure your new Logic App is available for selection.

Actions

Configure the Logic App that will be triggered.

Choose an existing Logic App or [visit the Logic Apps page](#) to create a new one

Show Logic App instances from the following subscriptions *

Pay-As-You-Go ▾

Logic App name ⓘ

No Logic Apps available ▾

Refresh

8. Select your logic app and save the automation. Note that the Logic App dropdown only shows Logic Apps with supporting Security Center connectors mentioned above.

Manually Trigger a Logic App

You can also run Logic Apps manually when viewing any security alert or recommendation.

To manually run a Logic App, open an alert or a recommendation and click **Trigger Logic App**:

PREVIEW - Role binding to the cluster-admin role detected

[Learn more](#)

General information

DESCRIPTION	Kubernetes audit log analysis detected a role binding to the cluster-admin role which gives administrative access to all namespaces.
ACTIVITY TIME	Tuesday, 12:00 PM UTC
SEVERITY	Low
STATE	Active
ATTACKED RESOURCE	View details
SUBSCRIPTION	View details
DETECTED BY	 Microsoft
ACTION TAKEN	View details

Was this useful? Yes No

[Trigger Logic App](#)

Configure a Playbook Workflow Automation by using Azure Sentinel

Playbooks are sets of procedures that Azure Sentinel can run in response to an alert or incident. By being attached to an analytics rule or an automation rule, a playbook can help automate and orchestrate the response. It can also be set to run automatically when specific alerts or incidents are generated. It can also be manually executed on request.

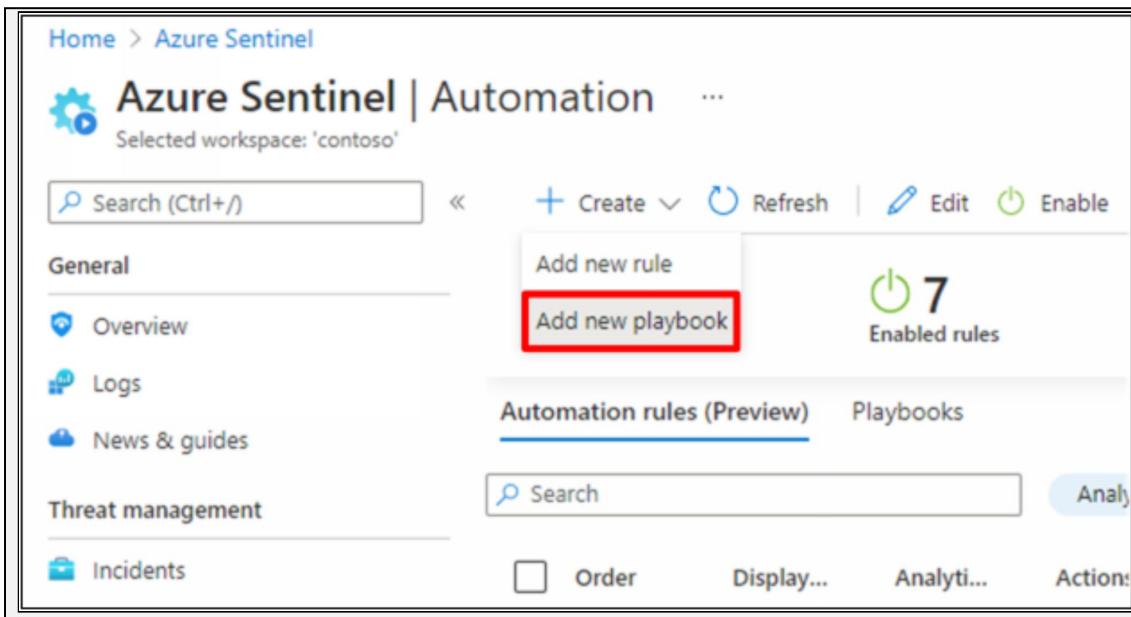
Playbooks in Azure Sentinel are based on Azure Logic Apps workflows, which means you get all of Logic Apps' power, customizability, and built-in templates. Each playbook is personalized to the subscription to which it belongs, but the Playbooks tab displays all of the playbooks available across all subscriptions.

Create a Playbook

Follow these steps to create a new playbook in Azure Sentinel:

Prepare the Playbook and Logic App

1. From the **Azure Sentinel** navigation menu, select **Automation**.
2. On the top menu, select **Create** and **Add new playbook**.



A new browser tab will open and take you to the **Create a logic app** wizard.

Create a logic app

Instance details

Logic app name *

Region *

Associate with integration service environment ⓘ

Integration service environment *

Enable log analytics ⓘ

Review + create

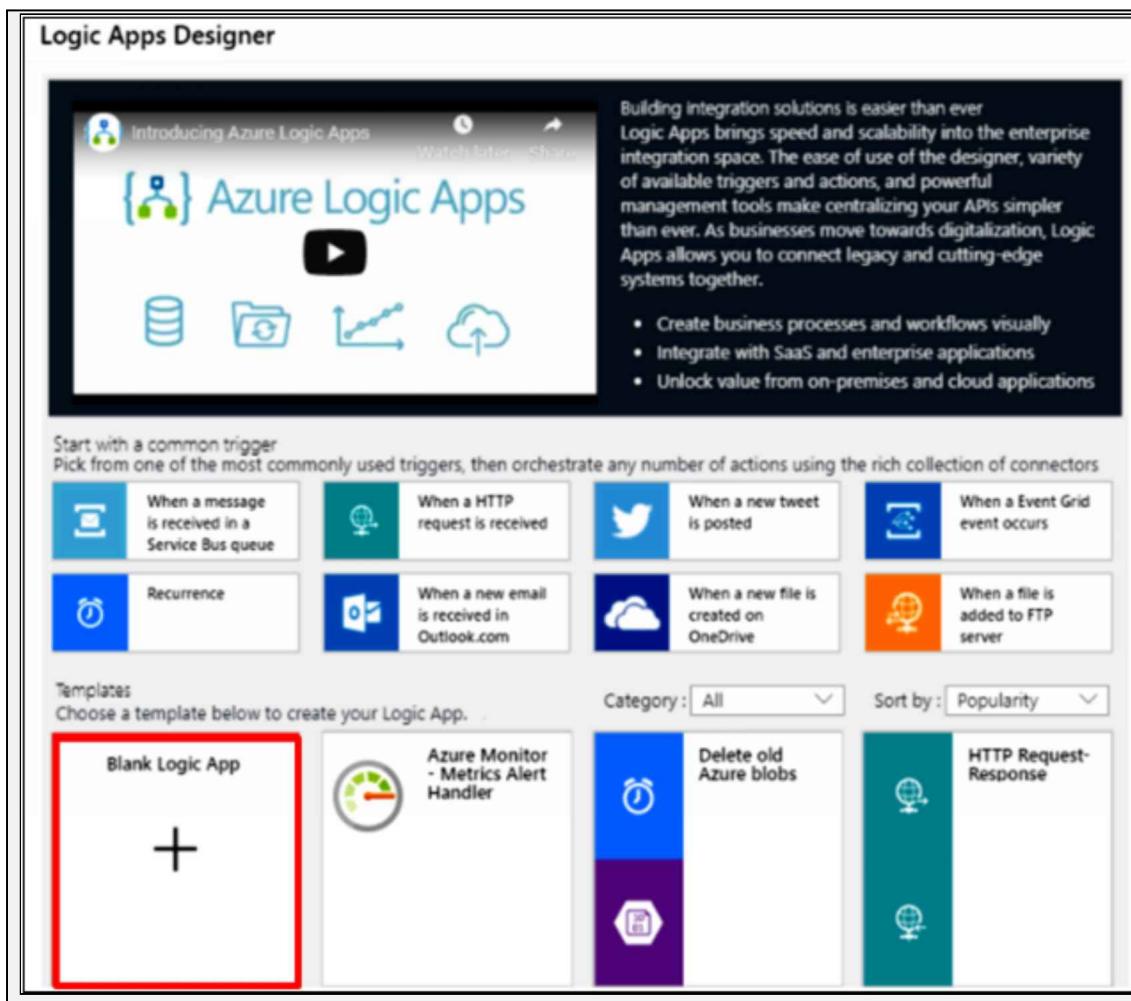
< Previous : Basics

Next : Tags >

This screenshot shows the 'Create a logic app' wizard. It's the first step, titled 'Instance details'. It asks for a 'Logic app name' (with a red asterisk), which is currently empty. It also asks for a 'Region' (set to 'East US 2'), and has an optional checkbox for 'Associate with integration service environment'. Below these are two more optional checkboxes: 'Integration service environment' and 'Enable log analytics'. At the bottom are three buttons: a red 'Review + create' button, a grey '< Previous : Basics' button, and a grey 'Next : Tags >' button.

3. Enter your **Subscription** and **Resource group**, and give your playbook a name under **Logic app name**.
4. For **Region**, select the Azure region where your Logic App information is to be stored.
5. If you want to monitor this playbook's activity for diagnostic purposes, mark the **Enable log analytics** check box, and enter your **Log Analytics workspace** name.
6. If you want to apply tags to your playbook, click **Next : Tags**. Otherwise, click **Review + Create**. Confirm the details you provided, and click **Create**.
7. While your playbook is being created and deployed (this will take a few minutes), you will be taken to a screen called **Microsoft.EmptyWorkflow**. When the "Your deployment is complete" message appears, click **Go to resource**.

- You will be taken to your new playbook's Logic Apps Designer, where you can start designing the workflow. You will see a screen with a short introductory video and some commonly used Logic App triggers and templates.
- Select the **Blank Logic App** template.

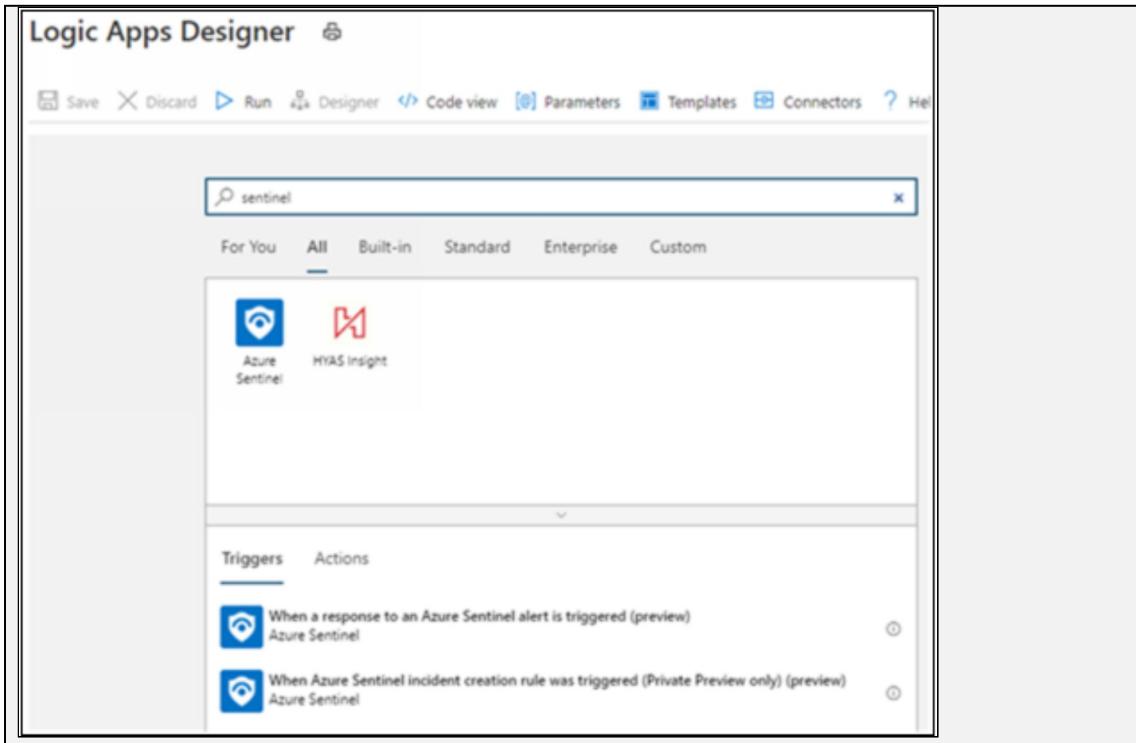


Choose the Trigger

Every playbook must start with a trigger. The trigger defines the action that will start the playbook and the schema that the playbook will expect to receive.

- In the search bar, look for Azure Sentinel. Select **Azure Sentinel** when it appears in the results.

2. In the resulting **Triggers** tab, you will see the two triggers offered by Azure Sentinel:
- When a response to an Azure Sentinel Alert is triggered
 - When the Azure Sentinel incident creation rule was triggered
 - Choose the trigger that matches the type of playbook you are creating.



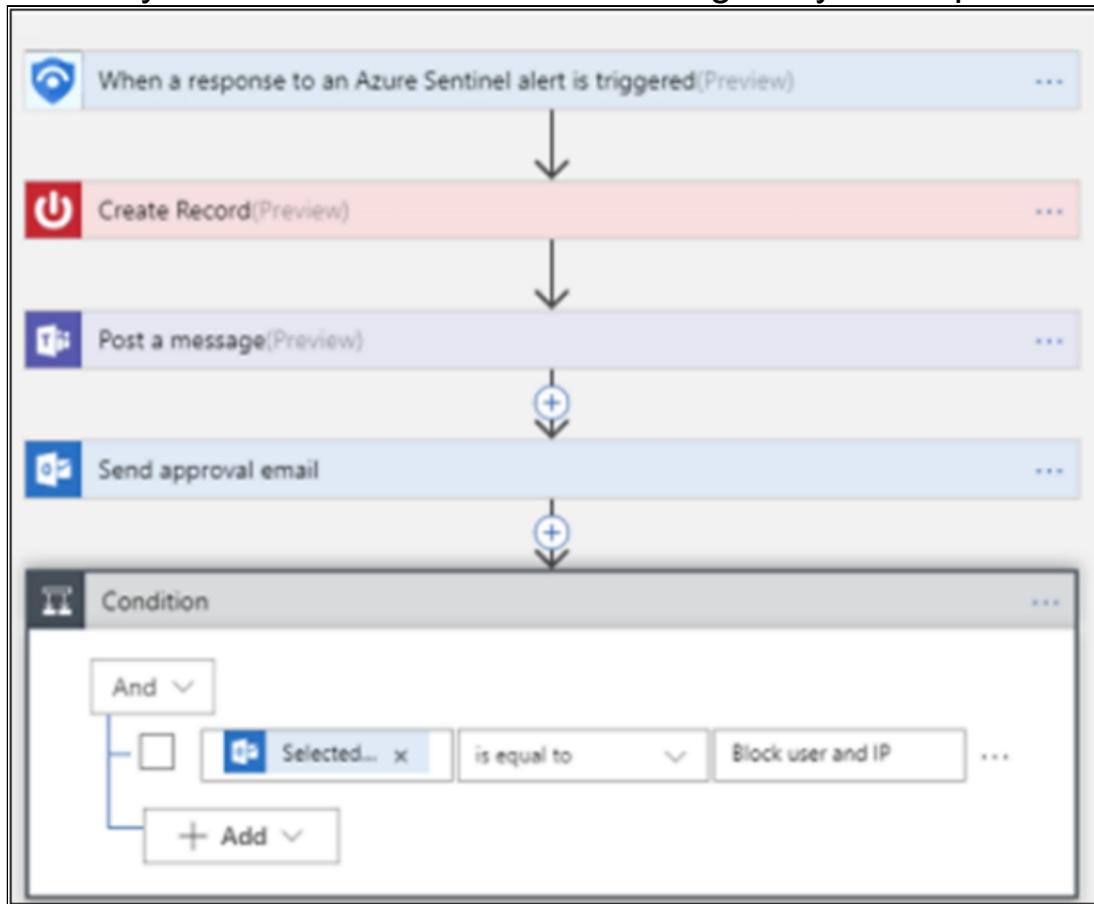
Add Actions

- Now you can define what happens when you call the playbook. You can add actions, logical conditions, loops, or switch case conditions, all by selecting **New step**.
- This selection opens a new frame in the designer, where you can choose a system or an application to interact with or a condition to set.
- Enter the name of the system or application in the search bar at the top of the frame, and then choose from the available results.
- In every one of these steps, clicking on any field displays a panel with two menus: **Dynamic content** and **Expression**.

From the **Dynamic content** menu, you can add references to the attributes of the alert or incident that was passed to the

playbook, including the values and attributes of all the entities involved.

From the **Expression** menu, you can choose from a large library of functions to add additional logic to your steps.



Practice Questions:

1. You can manage your Azure AD users account by using _____.
 - a. Azure Portal
 - b. Azure PowerShell
 - c. Azure CLI
 - d. All of the above

2. Which one from the following is something you cannot edit while creating your Azure AD user account in Azure portal?
 - a. User name
 - b. Domain name
 - c. First name
 - d. Last name

3. When creating a group, how many types of membership will you see?
 - a. One
 - b. Two
 - c. Three
 - d. Four

4. Which of the following is only used for security groups?
 - a. Assigned
 - b. Dynamic User
 - c. Dynamic Device
 - d. None of the above

5. Azure AD Connect is a tool that provides:
 - a. Individual identity
 - b. Group identity

- c. Hybrid identity
- d. Management identity

6. Which is the only authentication solution that allows to display password authentication?

- a. PHS
- b. Federation
- c. PTA
- d. None of the above

7. Which of the following supports smart card authentication?

- a. Federation
- b. PTA
- c. PHS
- d. All of the above

8. Typical multi-factor authentication methods are:

- a. Password
- b. Biometrics
- c. Device
- d. All of the above

9. Access policies are a focus of

- a. Access control
- b. Conditional access
- c. Conditional control
- d. Control statement

10. Which is the main cause of security breaches?

- a. Attackers leverage
- b. Stolen user identity

- c. Both of them
- d. None of them

11. Azure AD identity protection is designed to mitigate how many types of risks?

- a. One
- b. Two
- c. Three
- d. Four

12. Types of risk events include _____.

- a. Anonymous IP Addresses
- b. Unfamiliar sign-in properties
- c. IP addresses link to malware
- d. All of the above

13. Sign-in risk can be evaluated by _____.

- a. Real time
- b. Aggregate
- c. Both of them
- d. None of them

14. In Azure AD Identity Protection Configuration Steps, which configuration is optional but recommended?

- a. MFA
- b. User risk policy
- c. Sign-in risk policy
- d. None of the above

15. The last step of the Azure AD Identity Protection configuration is the _____.

- a. Configuration of user risk policy
- b. Configuration of Sign-in risk policy
- c. Configuration of MFA
- d. None of them

16. To activate PIM, you must be a _____.

- a. Local administrator
- b. Global administrator
- c. Administrator
- d. None of the above

17. To add an eligible member to the privilege group, you will need to use Azure AD _____.

- a. Members
- b. Roles
- c. Both of them
- d. None of them

18. To view or approve any requests in Azure AD, you will need to use _____.

- a. Access reviews
- b. Approve requests
- c. Request permissions
- d. All of the above

19. For PIM Activation, you must use your _____.

- a. Personal account
- b. Group account
- c. Organizational account

d. None of the above

20. Subscription-level roles and Azure Management Groups can be managed with _____.

- a. Roles
- b. Members
- c. Azure AD Users
- d. Privileged Identity Management

21. To activate PIM, click on _____.

- a. Security tab
- b. Identity tab
- c. Group tab
- d. Administrator tab

Chapter 03: Azure Tenant Security

Introduction:

One of the things you may want to do from time to time is transfer your Azure subscription to someone else; maybe the billing contact over a particular Azure subscription in your company is no longer with you and you need to transfer billing ownership to another account. This is where transferring an Azure subscription would be deployed.

Transferring an Azure Subscription

When you sign up for Azure, an Azure Active Directory (AD) tenant is created for you. Your account represents the tenant. To control access to your subscriptions and services, you use the tenant.

When you create a new subscription, it is hosted on the Azure AD tenant of your account. You ought to allow them to join your tenant, whether you wish to give others access to your subscription or its services. Doing so lets you manage access to your resources and subscriptions.

Transferring Billing Ownership of an Azure Subscription

This section helps you understand the things you should know before you transfer billing ownership of an Azure subscription to another account.

If you are leaving the company, you may want to transfer billing control of your Azure subscription, or you want your subscription to be billed to another account. Transferring billing ownership to another account provides authorization for billing activities to the administrators of the new account. They can change the mode of payment, view charges, and cancel the subscription.

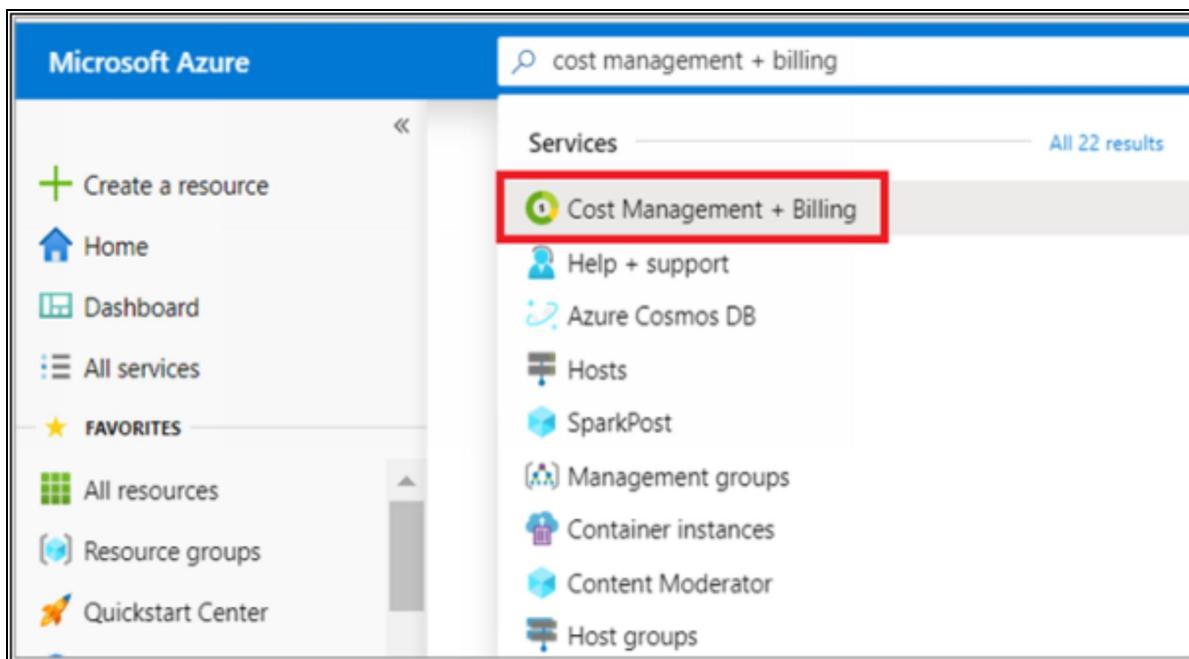


Figure 3-01: Cost Management and Billing Section

When transferring an Azure subscription, you can do it in the cost management and billing section of the Azure portal also known as the account center by taking a look at the subscription itself and then clicking on manage and it would take you the account center itself.

Transfer a Subscription to Another Azure AD Tenant

When you transfer billing ownership of your subscription to an account in another Azure AD tenant, you can transfer the subscription to the new tenant account. If you do so, all users, groups, or service principals that had Azure role assignments to manage subscriptions and its resources lose their access. Only the user in the new account who accepts your transfer request will have access to manage the resources. The new owner must manually add these users to the subscription to provide access to the user who lost it. Azure role-based access control (Azure RBAC) is the authorization system you use to manage access to Azure resources. To grant access, you assign roles to users, groups, service principals, or managed identities at a particular scope.

Steps After Transferring Billing Ownership

If you have accepted the billing ownership of an Azure subscription, it is recommended that you review these steps:

Update credentials related with this subscription's services containing:

- Management certificates that grant the user admin rights to subscription resources
- Access keys for services like Storage
- Remote Access credentials for services like Azure Virtual Machines

Transfer Visual Studio and Partner Network Subscriptions

Subscriptions to Visual Studio and Microsoft Partner Network have monthly recurring Azure credit associated with them. When you transfer these subscriptions, the destination billing account does not have the credit available. The subscription uses the credit in the

billing account. For example, John transfers a Visual Studio Enterprise subscription to Mike's account on September 9 and Mike accepts the transfer. After the transfer is completed, the subscription starts using credit in Mike's account. Each ninth day of the month, the credit will reset.

Supported Subscription Types

Subscription transfer in the Azure portal is available for the following subscription types:

- Microsoft Partner Network
- Enterprise Agreement (EA)
- Visual Studio Enterprise (MPN) subscribers
- MSDN Platforms
- Pay-As-You-Go
- Pay-As-You-Go Dev/Test
- Visual Studio Enterprise
- Visual Studio Enterprise: BizSpark
- Visual Studio Professional
- Visual Studio Test Professional
- Microsoft Azure Plan2

Presently, transfer is not supported for Free Trial or Azure in Open (AIO) subscriptions.

Transfer Account Ownership to Another Country/Region

You cannot transfer subscriptions across countries or regions using the Azure portal, unfortunately. However, they can be transferred if you open an Azure support request.

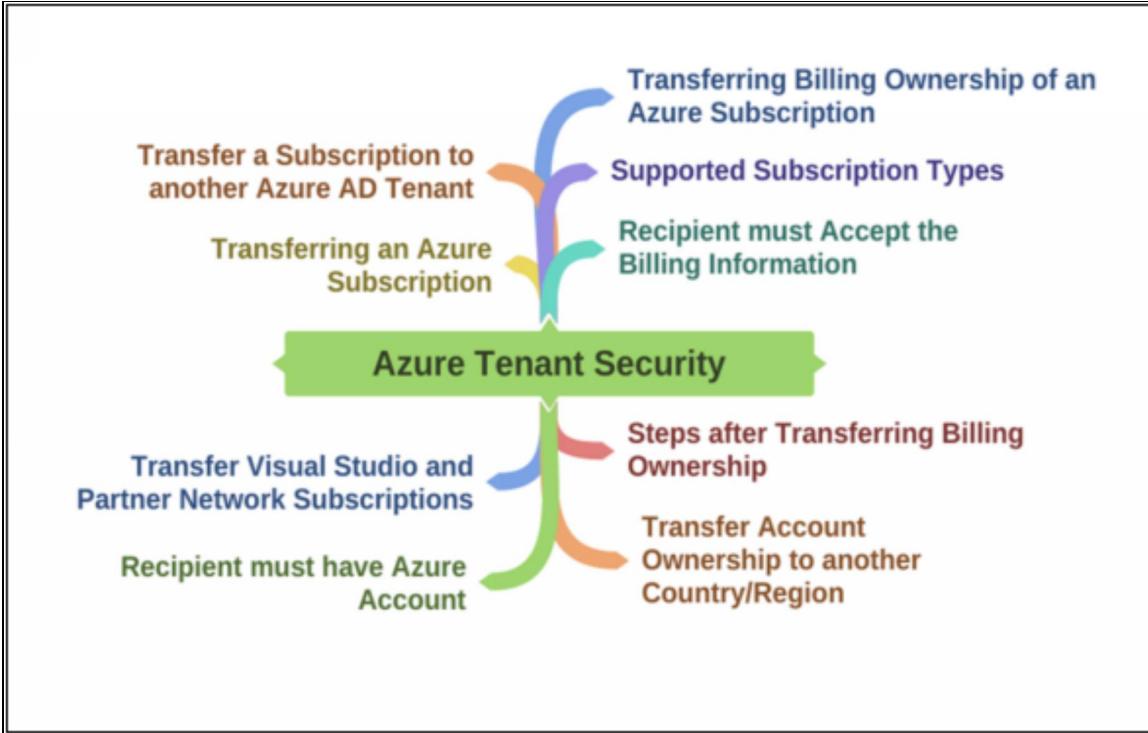
Recipient Must Accept the Billing Information

In order to complete the transfer, the recipient must accept the billing ownership and provide payment details.

Recipient Must Have an Azure Account

If the recipient does not have an Azure account, they must create one to accept the transfer.

Mind Map



Practice Questions:

1. When you sign up for Azure, an _____ is created for you.
 - A. Azure Resource Group
 - B. Azure Active Directory (AD) tenant
 - C. Azure Container
 - D. Azure Database

2. Transferring billing ownership to another account provides _____ for billing activities to the administrators of the new account.
 - A. Subscription
 - B. Authorization
 - C. Authentication
 - D. All of the above

3. When you transfer billing ownership of your subscription to an account in another Azure AD tenant, what will happen to the resources?
 - A. Resources lose their access
 - B. Resources get their access
 - C. Both
 - D. No change will occur to the resources

4. If you have accepted the billing ownership of an Azure subscription, what will be recommended?
 - A. Management certificates that grant the user admin rights to subscription resources
 - B. Access keys for services like Storage
 - C. Remote Access credentials for services like Azure Virtual Machines
 - D. All of the above

5. Subscriptions to Visual Studio and Microsoft Partner Network have _____ recurring Azure credit associated with them.
- A. Yearly
 - B. Monthly
 - C. Quarterly
 - D. Bi-monthly
6. Presently, transfer is not supported for Free Trial or Azure in Open (AIO) subscriptions. True or false?
- A. True
 - B. False
7. You cannot transfer subscriptions across countries or regions using the Azure portal, unfortunately. True or false?
- A. True
 - B. False
8. What should be necessary for accepting the subscription?
- A. Azure Subscription
 - B. Azure Account
 - C. Azure Portal
 - D. All of the above
9. You cannot transfer subscriptions across countries or regions using the Azure portal. True or false?
- A. True
 - B. False
10. Which authorization system should you use to manage access to Azure resources?
- A. Discretionary Access Control (DAC)
 - B. Mandatory Access Control (MAC)
 - C. Role Based Access Control (RBAC)
 - D. Attribute Based Access Control (ABAC)

Chapter 04: Network Security

Introduction:

In this lesson of az-500 course discusses about the platform protection through the Network security. Network security may be described by adding controls to network traffic, as the method of protecting resources against unwanted access or attack. The aim is to make sure that only authorized traffic is approved. To support the application and service access needs, Azure provides a comprehensive networking framework. Connectivity to the network is available between resources stored in Azure, between resources hosted on-premise and Azure, and to and from the internet and Azure.

Virtual Network (VNet)

The basic building block for your private network in Azure is the Azure Virtual Network (VNet). VNet helps several types of Azure services to connect safely with each other, the internet, and on-premise networks, such as Azure Virtual Machines (VM). VNet is similar to a conventional network where you can run in your own data centre, but carries with it additional advantages such as size, availability, and isolation from Azure's infrastructure.

VNet Contains

- The VNet has an internal address space like 10.1.0.0/16
- Resources connect to subnets within a Azure VNet to gain network access
- Subnets within the VNet must exist within the same address space
- All the subnets within a specific virtual network can communicate with each other
- Default routing can be modified with either BGP or user-defined route tables

VNet Peering

Through VNet Peering, Azure resources communicate securely. You can connect virtual networks to each other by using virtual network peering, allowing resources in each virtual network to communicate with each other. You will connect to virtual networks in the same, or different, Azure regions.

VNets Connection

VNets can also be connected with your on-premises networks as well as other virtual network by using

Site-to-site VPN: Created between your on-premises VPN device and the virtual network deployed by the Azure VPN Gateway. This form of connection allows any on-premises resource to access a virtual network that you allow. Connection between your on-premises VPN device and an Azure VPN gateway is transmitted over the Internet through an encrypted tunnel.

ExpressRoute: Developed by an ExpressRoute partner between your network and Azure. Such connection is confidential. Traffic is not linked to the internet.

The both routing connection requires Virtual Network Gateways to facilitate routing.



EXAM TIP: The three sections VNet Routing, VNet Peering, VPN Gateways that included in the AZ-300 course, recommended looking in a more detail to get solid foundation of the Network security.

Network Security Groups (NSGs)

Network security groups are used to filter network traffic to and from Azure services on an Azure virtual network. A Network security group includes security rules that allow or deny different forms of Azure services to inbound or outbound network traffic from a network. You must define the source and destination, the port, and the protocol for each rule.

Overview

- The best practice is to block all traffic except for contact that is necessary. Occasionally, this is called "default deny".
- Only a Network Interface Card (NIC), a subnet, or both may be applied to NSGs.

Rules from both are evaluated as NSGs are assigned to both.

- The rules of NSGs are stateful, so reply traffic is allowed instantly irrespective of other rules.
- NSGs contain 'Default rules' that can not be deleted; to overcome them, you need higher priority rules.
- No more rules are processed until once a rule is matched.

Application Security Groups (ASGs)

An Application Security Groups (ASGs) is a logical collection of virtual machines, specifically their Network Interface Cards (NICs). You join the ASG virtual machines and then use the application security group in the NSG rules as a source or destination.

Application security groups allow you to configure network security as a logical extension of the application structure, allowing virtual machines to be grouped and network security policies based on those groups to be defined. Without manual maintenance of explicit IP addresses, you will reuse your security policies on scale. The framework manages the difficulty of various rule sets and explicit IP addresses, helping you to focus on your business logic.

Consider the following example, to better understand the application security groups:

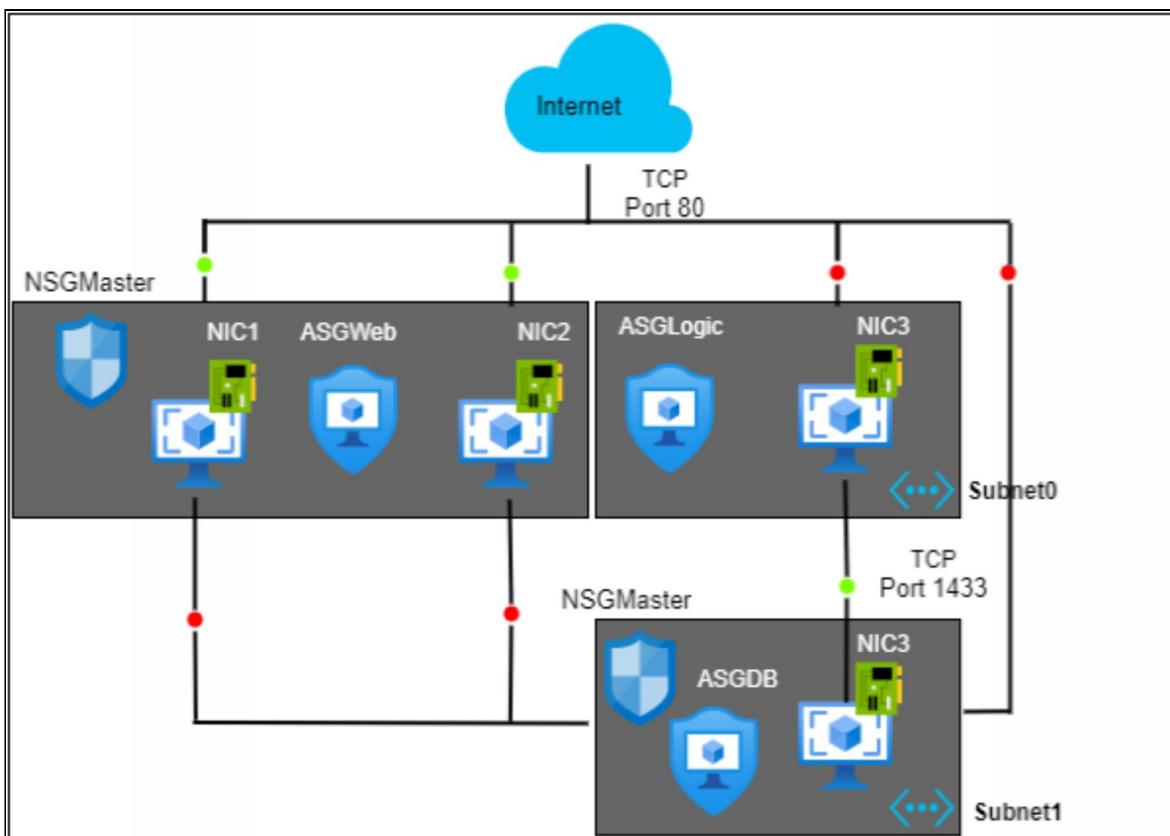


Figure 4-01: Application Security Groups

In the above picture, NIC1 and NIC2 are members of the security group for the AsgWeb application. NIC3 is a member of the security group for the AsgLogic application. NIC4 is a member of the security group for the AsgDb application. While each network interface in this example is a member of only one network security group, up to the Azure limits, a network interface may be a member of several security groups of applications. None of the network interfaces provide an associated security group for the network. Both subnets are connected to NSG1 and include the following rules:

Allow-HTTP-Inbound-Internet

To allow traffic from the internet to the web servers, this rule is required. Since the DenyAllInbound default security rule denies inbound traffic from the internet, no additional rules are needed for the AsgLogic or AsgDb application security groups.

ALLOW-HTTP-INBOUND-INTERNET

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
100	Internet	*	AsgWeb	80	TCP	Allow

Table 4-02: Allow-HTTP-Inbound-Internet

Azure Firewall

There are a few other network layer Azure offerings in addition to NSGs that we can introduce to harden network security. These were usually third-party products called Network Virtual Appliances (NVAs), used to examine all inbound and outbound network traffic to an entire virtual network.

Azure Firewall as-a-service was recently launched by Microsoft, planning it to be an alternative to third party NVAs. Microsoft, designed the Azure Firewall for the Cloud, specifically Azure.

Firewall Benefits

Azure Firewall includes the following features:

- A stateful firewall as a service
- Built-in high availability with unrestricted cloud scalability
- FQDN filtering and tags
- Rules for filtering network traffic
- Outbound SNAT support
- Inbound DNAT support (port forwarding)
- A central place to create, enforce, and log application and network connectivity policies across Azure subscription and VNETs.
- Full integration with Azure Monitor for logging and analytics

Firewall Configuration

The standard Azure Firewall implementation is inside a central virtual network. Other virtual networks are then peered to it in a hub-and-spoke manner. The default routes from the virtual peer networks point to the virtual network of the central firewall. You must all have a firewall, subnet, VNet, and public IP address in the same resource group.

Global VNet peering is supported, but because of potential performance and latency issues across regions, it is not recommended. Deploy one firewall per region for optimal outcomes.

The benefit of this model is the ability to centrally monitor activities through various subscriptions on several spoke VNETs.

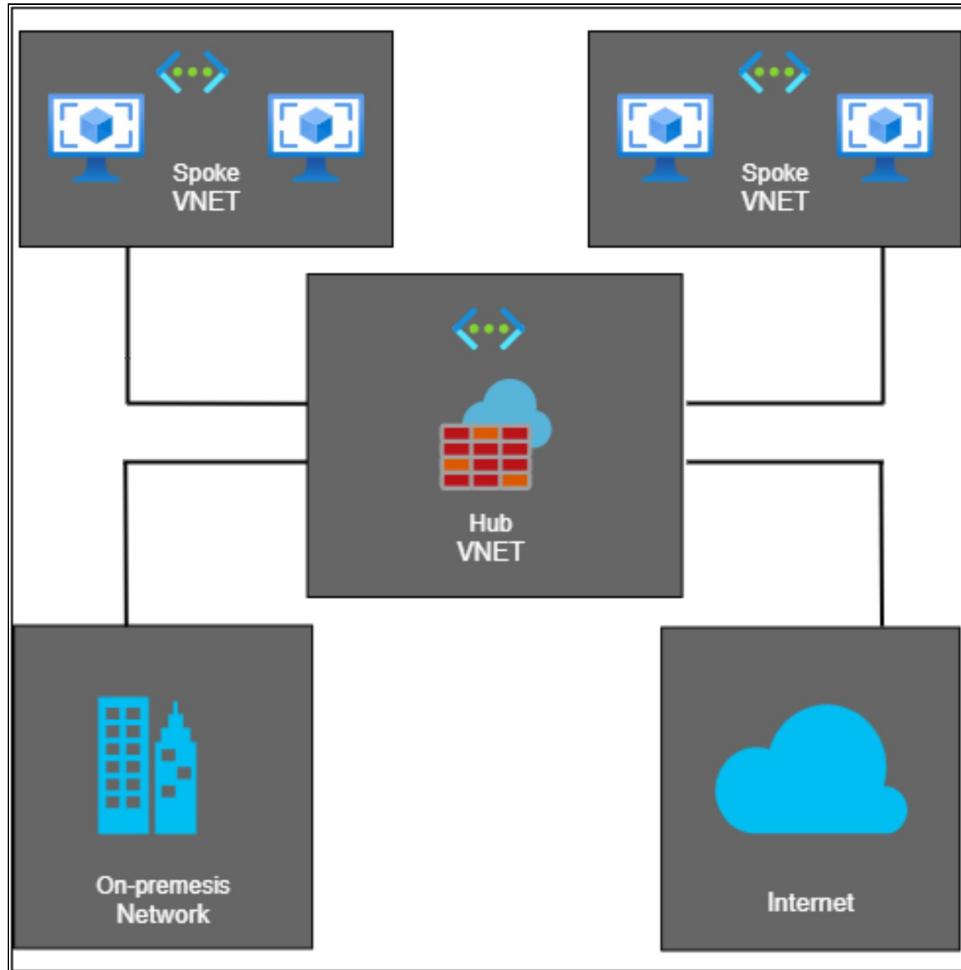


Figure 4-03: Azure Firewall Implementation

Azure Firewall Limitations

- Network filtering rules for non TCP/IP protocols such as ICMP do not work for Internet-bound traffic
- You cannot move Azure Firewall to a different resource group or subscription
- Limited port range
- No custom DNS support
- No SNAT/DNAT for private IP destinations

Resource Firewall

Single Azure resources also maintain their own set of firewall rules. Access to Azure virtual networks can be allowed or denied under these rules. Azure services such as backup and SQL, including Internet hosts.

Inside the Azure resources themselves, these access rules are configured. Azure Storage Accounts and Azure SQL server databases are the most common resources with this enhanced protection.

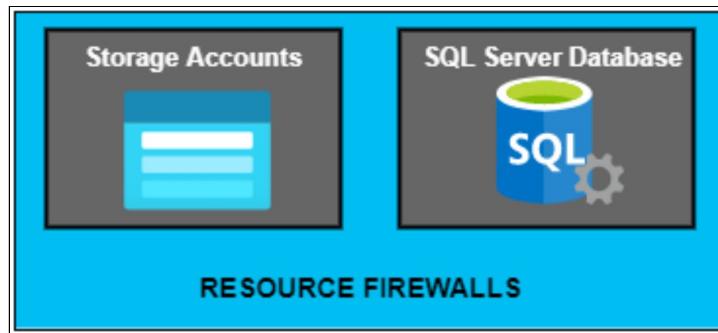
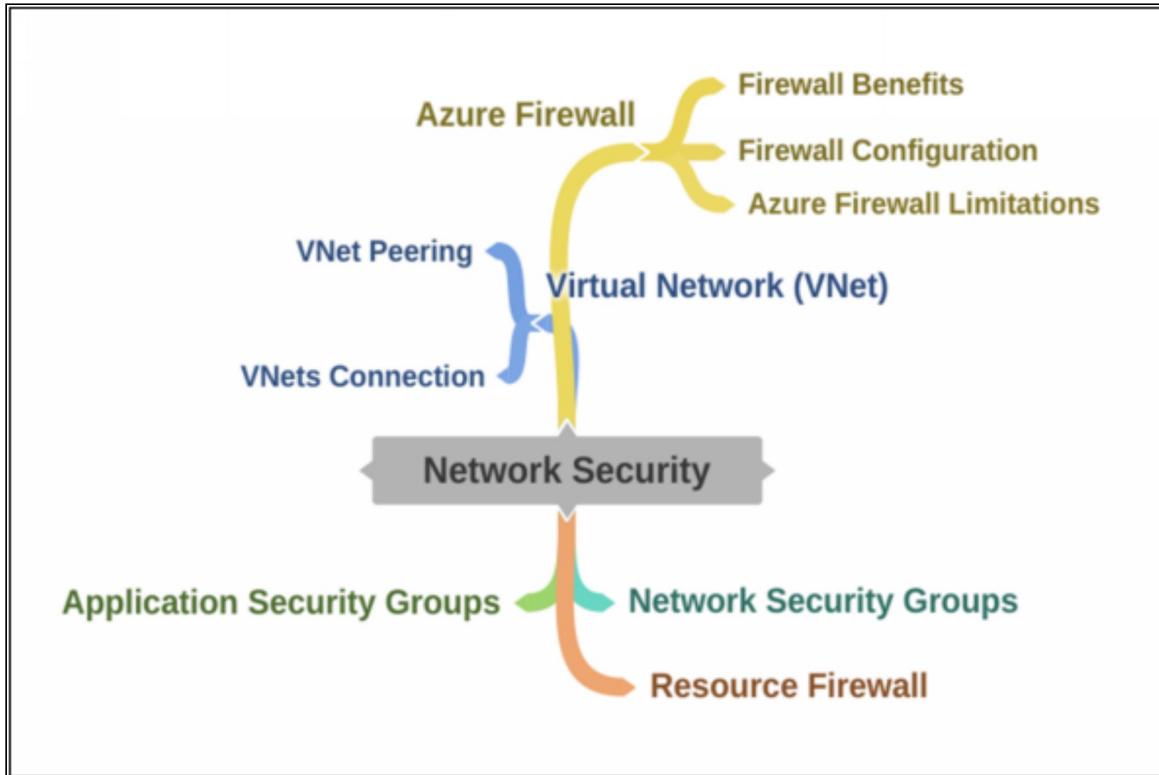


Figure 4-04: Resource Firewall

Mind Map



Lab 4-01: Securing a Virtual Network with Azure Firewall

Introduction

Securing a network's perimeter is one of the most important aspects of a cloud engineer's role, and this lab will demonstrate a common, real-world experience regarding this task. Candidates will build a network topology and then experience configuring and deploying Azure Firewall, before navigating it from the internet using a real-world scenario of Network Address Translation.

Solution

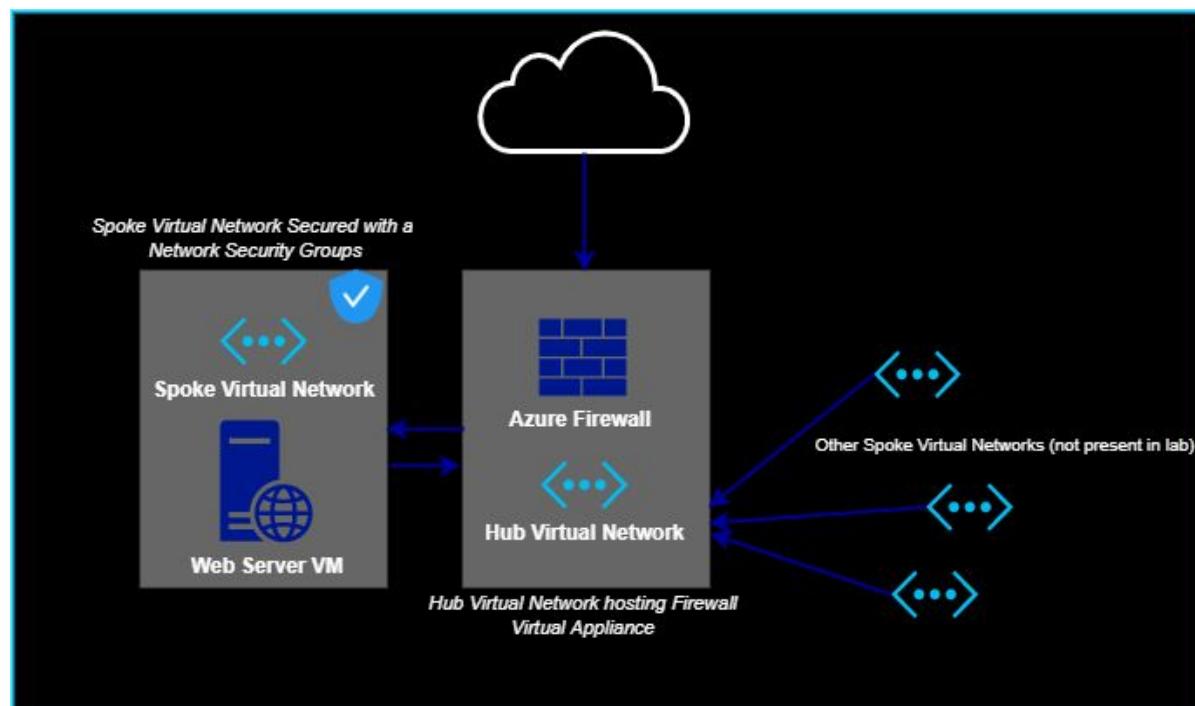


Figure 4-01-1: Securing a Virtual Network with Azure Firewall

Log in to the Azure Portal using the credentials.

Step#01

Create a Virtual Network and Network Security Group

Navigate to Resource groups in the left-hand menu to create a resource group.

Create a resource group

Basics Tags Review + create

Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more](#)

Project details

Subscription * ⓘ Pay-As-You-Go

Resource group * ⓘ secure_vnet_azure_firewall

Resource details

Region * ⓘ (US) South Central US

Navigate to Virtual networks in the left-hand menu and click Create virtual network.

Virtual networks

ipspecialist (Default Directory)

+ Add Manage view Refresh Export to CSV Open query ...

Filter by name... Subscription == all Add filter More (2)

Showing 1 to 1 of 1 records. No grouping List view

Name ↑ Resource group ↑ Location ↑ Subscription ↑

Set the following values:

- Name: SpokeVnet1

Create virtual network

Basics IP Addresses Security Tags Review + create

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. [Learn more about virtual network](#)

Project details

Subscription * Pay-As-You-Go

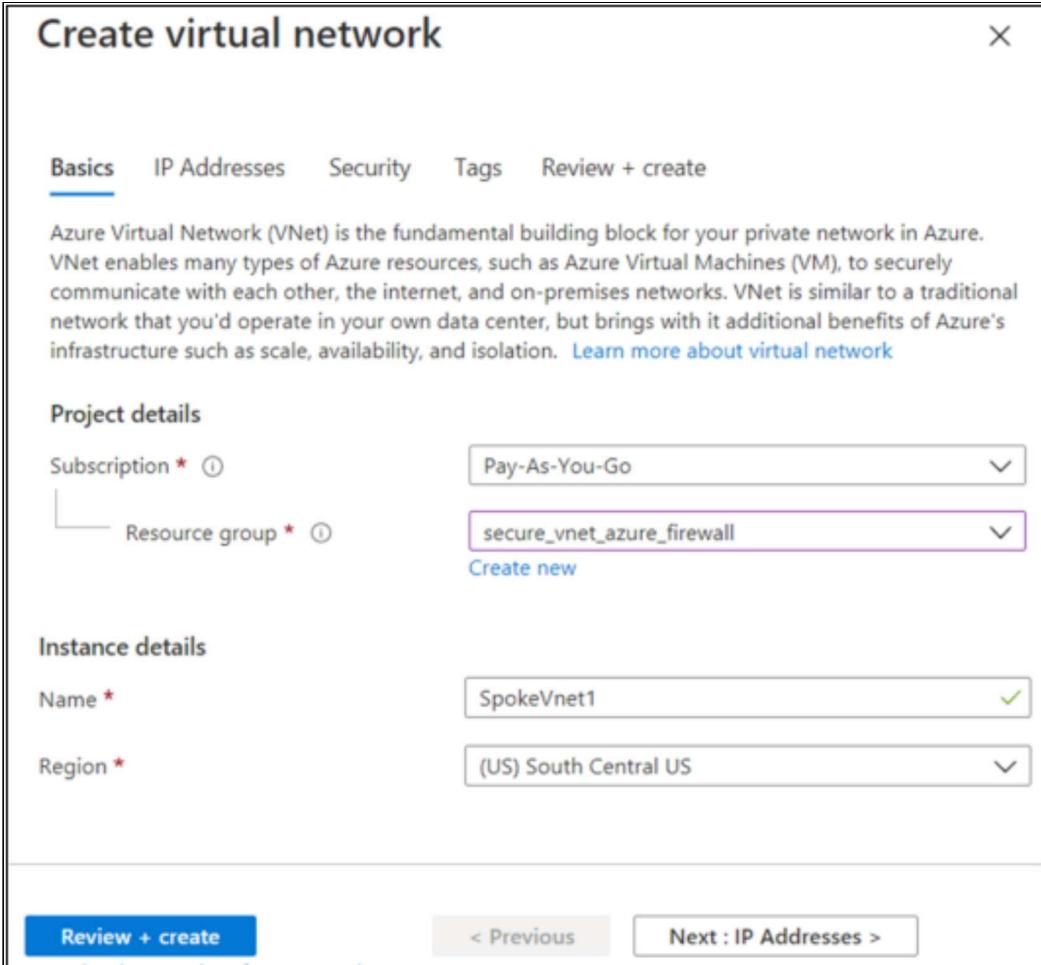
Resource group * secure_vnet_azure_firewall
[Create new](#)

Instance details

Name * SpokeVnet1

Region * (US) South Central US

[Review + create](#) < Previous Next : IP Addresses >



- Address space: 10.10.10.0/24
- Resource group: Select the one listed in the dropdown
- Location: The location we just noted
- Address range: 10.10.10.0/26
- Click Create.

Basics **IP Addresses** Security Tags Review + create

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

IPv4 address space

✓ [edit]

Add IPv6 address space (i)

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

+ Add subnet [edit] Remove subnet

Subnet name Subnet address range

default 10.10.10.0/26

Security

BastionHost
Disabled

DDoS protection plan
Basic

Firewall
Disabled

Create < Previous Next > Download a template for

Navigate to All services > Network security groups.

Click add network security group.

The screenshot shows the 'Network security groups' blade in the Azure portal. At the top, there's a header with the title 'Network security groups' and a 'Subscriptions' section. Below the header are several buttons: '+ Add' (highlighted with a red box), 'Edit columns', 'Refresh', 'Try preview', and 'Assign tags'. There are also filters for 'Filter by name...', 'All resource ...', 'All locations', 'All tags', and 'No gro...'. A message says '0 items'. Below the filters, there are sorting options: 'Name ↑↓', 'Resource group ↑↓', 'Location ↑↓', and 'Subscript'. The main area is currently empty.

Set the following values:

- Name: Anything you like (e.g., "SpokeNSG1")
- Resource group: Select the one listed in the dropdown
- Location: The same location as before

Click Create.

The screenshot shows the 'Create Network security group' wizard in the 'Basics' step. The 'Subscription' dropdown is set to 'Pay-As-You-Go'. The 'Resource group' dropdown is set to 'secure_vnet_azure_firewall'. The 'Name' field is set to 'SpokeNSG1'. The 'Region' dropdown is set to '(US) South Central US'. At the bottom, there are buttons for 'Review + create', '< Previous', 'Next : Tags >', and 'Download a'.

Once it is deployed, click the name of the NSG.

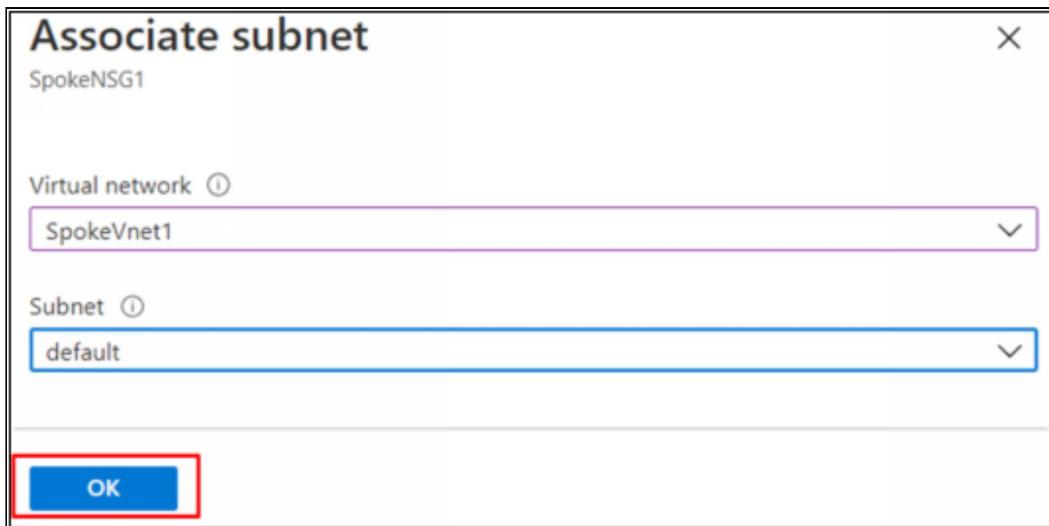
Click Subnets

Click Associate.

Click Virtual network and select our listed virtual network.

Click Subnet and select default.

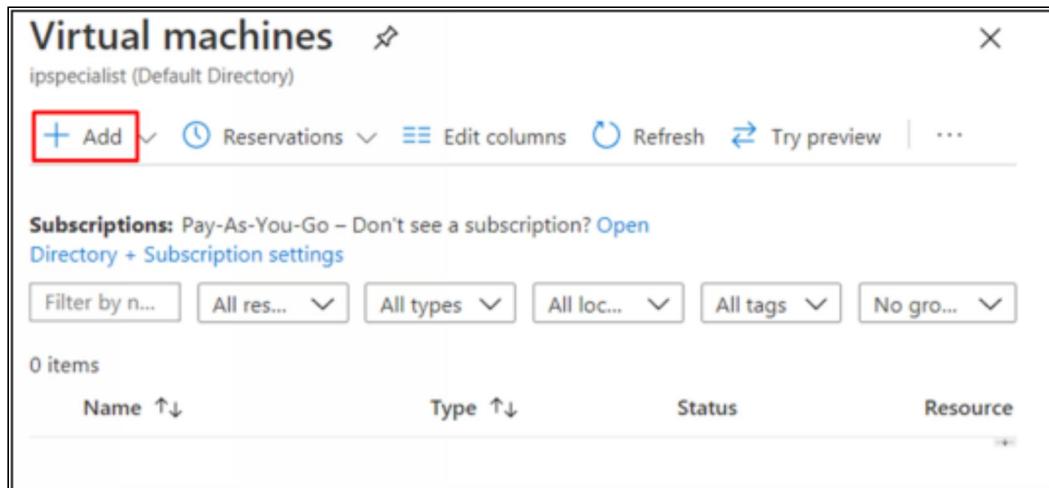
Click OK.



Step#02

Create a Virtual Machine

Click Virtual machines in the left-hand menu.



Click Create virtual machine, and set the following values:

- Resource group: Select the one listed in the dropdown
- Virtual machine name: Anything you like (e.g., "SpokeServer1")
- Region: Select the one listed in the dropdown

Basics [Disks](#) [Networking](#) [Management](#) [Advanced](#) [Tags](#) [Review + create](#)

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

Project details

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

Subscription * ⓘ Pay-As-You-Go

Resource group * ⓘ secure_vnet_azure_firewall
[Create new](#)

Instance details

Virtual machine name * ⓘ SpokeServer1

Region * ⓘ (US) South Central US

Availability options ⓘ No infrastructure redundancy required

- Image: Windows Server 2019
- Size: B2s Standard
- Username: Anything you'd like (e.g., "mythicaladmin")
- Password: Anything you'd like (e.g., "RUBYmountain135")

Image * ⓘ

Windows Server 2019 Datacenter - Gen1

See all images

Azure Spot instance ⓘ

Size * ⓘ

Standard_B2s - 2 vcpus, 4 GiB memory (\$42.27/m...)

See all sizes

Administrator account

Username * ⓘ

mythicaladmin

Password * ⓘ

Confirm password * ⓘ

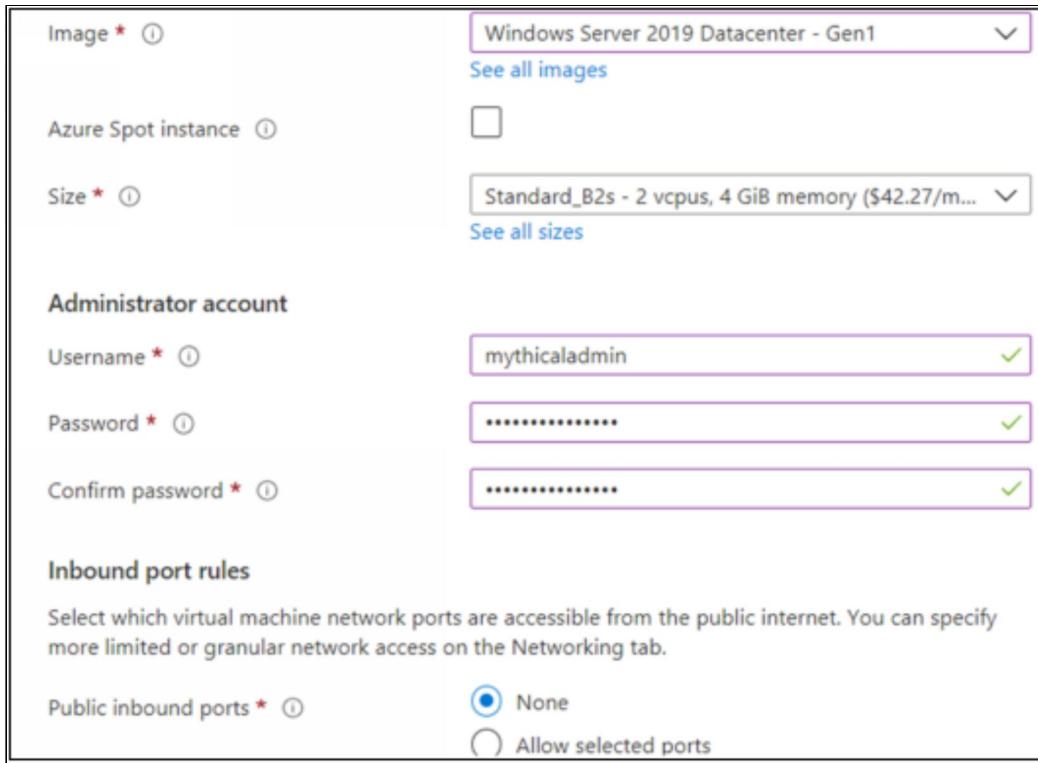
Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ

None

Allow selected ports



Click Next: Disks.

Leave settings as-is and click Next: Networking.

- Set the Virtual network to the one we previously created.
- Set Public IP to None.

Basics Disks **Networking** Management Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more](#)

Network interface

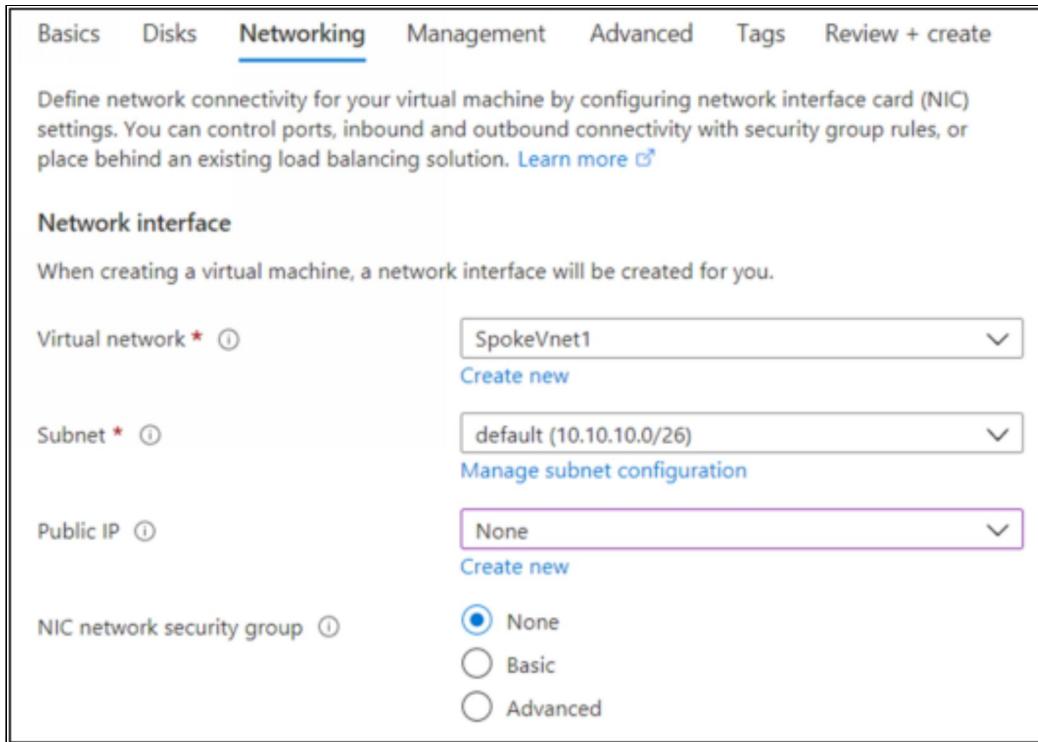
When creating a virtual machine, a network interface will be created for you.

Virtual network * ⓘ

Subnet * ⓘ

Public IP ⓘ

NIC network security group ⓘ None
 Basic
 Advanced



Click Next: Management.

- Set Boot Diagnostics to Off.

Basics Disks Networking **Management** Advanced Tags Review + create

Configure monitoring and management options for your VM.

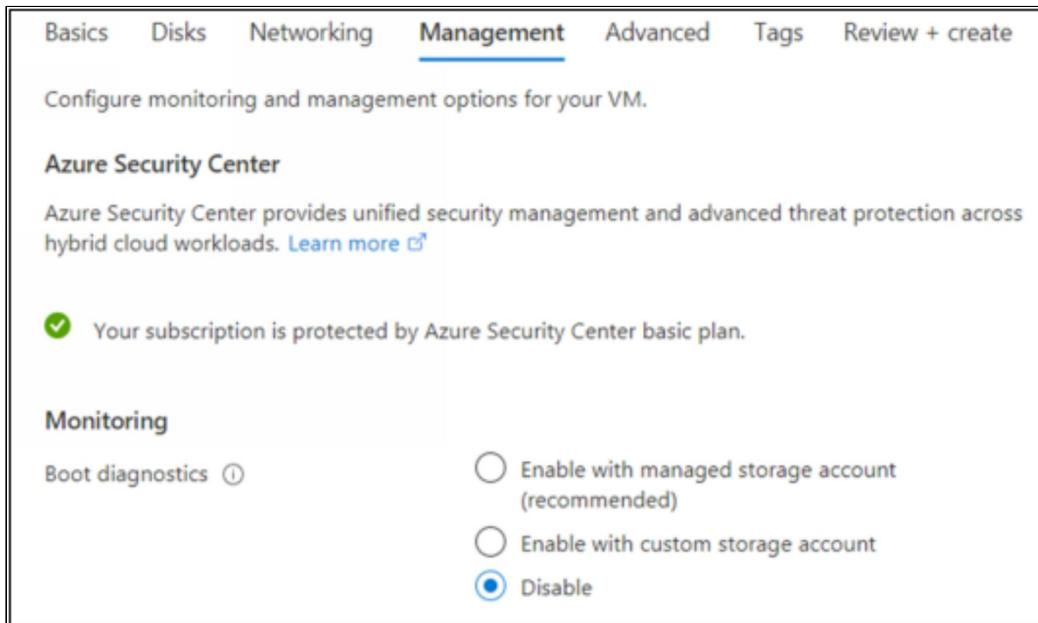
Azure Security Center

Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads. [Learn more](#)

 Your subscription is protected by Azure Security Center basic plan.

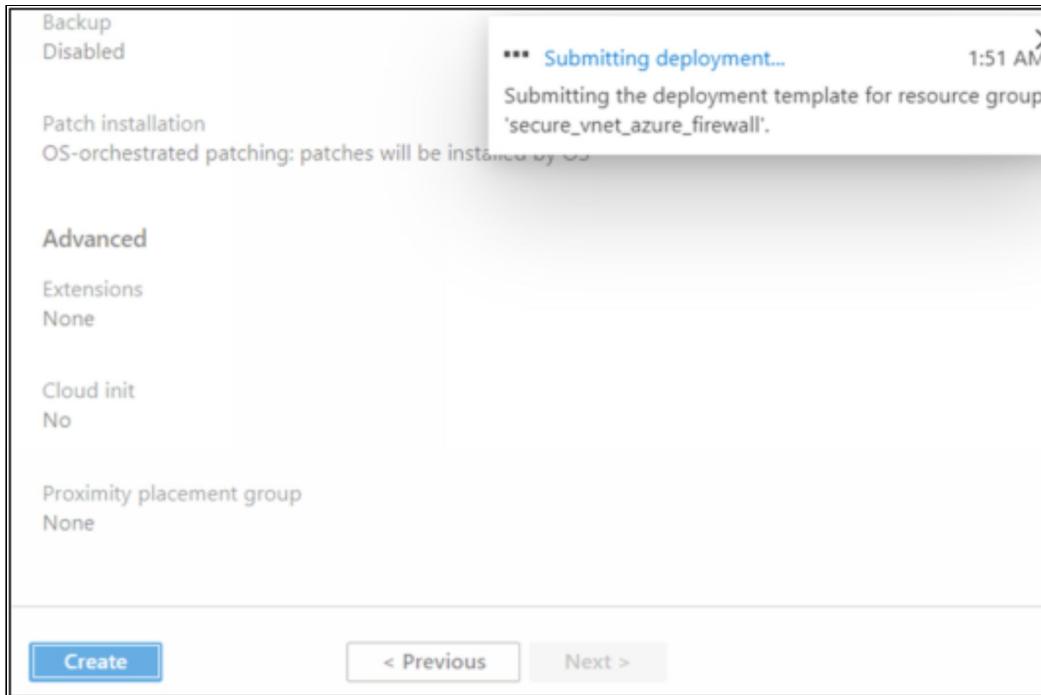
Monitoring

Boot diagnostics ⓘ Enable with managed storage account (recommended)
 Enable with custom storage account
 Disable



Click Next: Advanced > Next: Tags > Next: Review + create.

Click Create.



Step #03

Create a Second Virtual Network and Azure Firewall

Navigate to Virtual networks in the left-hand menu and click add virtual network.

The screenshot shows the "Virtual networks" blade in the Azure portal. At the top, there is a header with the user's name ("ipspecialist (Default Directory)"). Below the header, there is a toolbar with buttons for "Add" (which is highlighted with a red box), "Manage view", "Refresh", "Export to CSV", "Open query", and more. There is also a search bar labeled "Filter by name..." and a dropdown for "Subscription == all". Below the toolbar, there are buttons for "Add filter" and "More (2)". Underneath, there is a summary message "Showing 1 to 1 of 1 records." and two dropdown menus: "No grouping" and "List view". The main table lists one record: "SpokeVnet1" under "Name", "secure_vnet_azure_fire..." under "Resource group", "South Central US" under "Location", and "Pay-As-You-Go" under "Subscription".

Set the following values:

- Name: HubVnet1
- Resource group: Select the one listed in the dropdown
- Location: The same location as before

Basics IP Addresses Security Tags Review + create

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. [Learn more about virtual network](#)

Project details

Subscription *	Pay-As-You-Go
Resource group *	secure_vnet_azure_firewall
	Create new

Instance details

Name *	HubVnet1
Region *	(US) South Central US

- Address space: 10.10.200.0/24
- Address range: 10.10.200.0/26

Basics **IP Addresses** Security Tags Review + create

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

IPv4 address space

10.10.200.0/24	<input checked="" type="checkbox"/>	<input type="button" value="Delete"/>
<input type="text"/>		

Add IPv6 address space ⓘ

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

<input type="checkbox"/> Subnet name	Subnet address range
<input type="checkbox"/> default	10.10.200.0/26

- Firewall: Enabled
- Firewall name: Anything you like (e.g., "Firewall1")
- Firewall subnet address space: 10.10.200.64/26

Basics IP Addresses **Security** Tags Review + create

BastionHost ⓘ Disable Enable

DDoS Protection Standard ⓘ Disable Enable

Firewall ⓘ Disable Enable

Firewall name * Firewall1

Firewall subnet address space * 10.10.200.64/26
10.10.200.64 - 10.10.200.127 (64 addresses)

Public IP address * (New) azureFirewalls-ip
[Create new](#)

Click Create.

Tags
None

Security

BastionHost
Disabled

DDoS protection plan
Basic

Firewall
Enabled

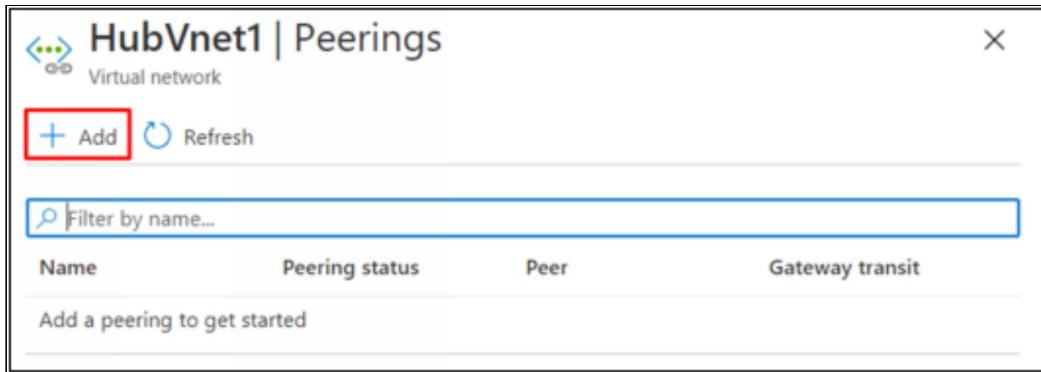
*** Initializing deployment... 2:08 AM
Initializing template deployment to resource group 'secure_vnet_azure_firewall'.

[Create](#) [< Previous](#) [Next >](#) [Download a template for](#)

Step#04

Peer the Virtual Networks Together and Create a Route Table

- Click HubVnet1.
- Click Peerings > Add.

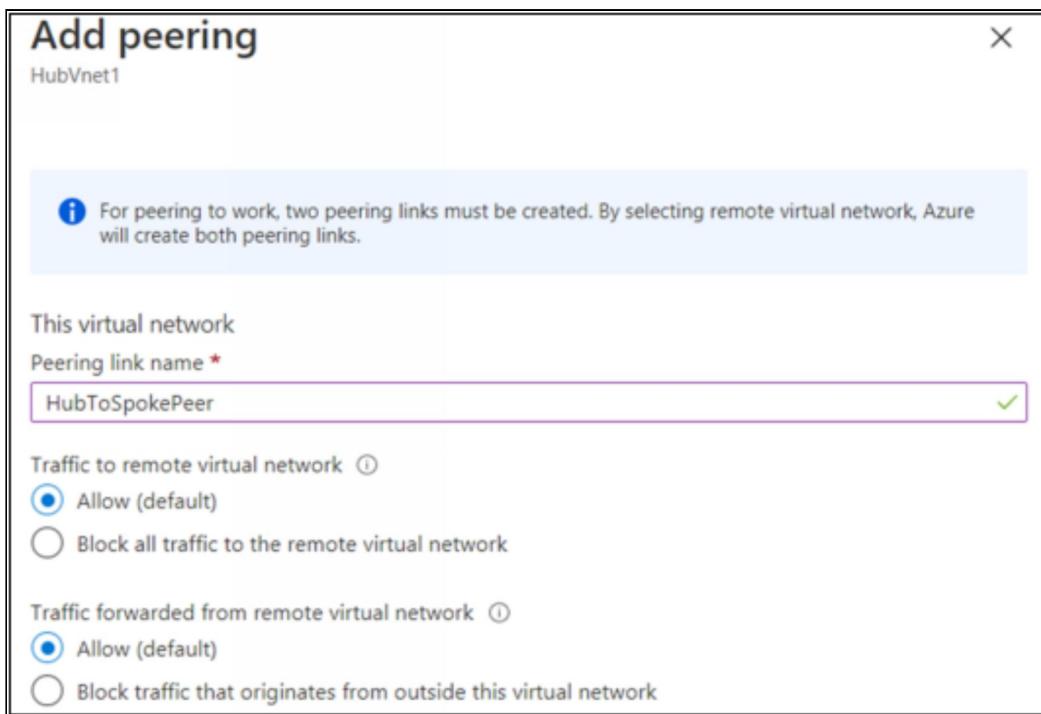


The screenshot shows the 'HubVnet1 | Peerings' page in the Azure portal. At the top left is a blue icon with three dots and lines. To its right is the text 'HubVnet1 | Peerings'. Below that is the word 'Virtual network'. Underneath are two buttons: a red-bordered 'Add' button with a plus sign and a 'Refresh' button with a circular arrow. A search bar with a magnifying glass icon and the placeholder 'Filter by name...' is positioned below the buttons. A table header follows with columns: 'Name', 'Peering status', 'Peer', and 'Gateway transit'. Below the header, a message says 'Add a peering to get started'. The entire interface is contained within a light gray box with a black border.

Set the following values:

- Name of the peering from HubVnet1 to remote virtual network: HubToSpokePeer
- Virtual network: SpokeVnet1
- Name of the peering from SpokeVnet1 to HubVnet1: SpokeToHubPeer
- Enable every peering option except gateway transit.

Click Add.



The screenshot shows the 'Add peering' dialog box. At the top left is a blue info icon with a white 'i'. To its right is the text 'For peering to work, two peering links must be created. By selecting remote virtual network, Azure will create both peering links.' Below this is a section titled 'This virtual network'. It contains a 'Peering link name *' label with a red asterisk and a text input field containing 'HubToSpokePeer', which has a green checkmark to its right. Below this are two sections: 'Traffic to remote virtual network' and 'Traffic forwarded from remote virtual network', each with two radio button options: 'Allow (default)' (selected) and 'Block all traffic to the remote virtual network' or 'Block traffic that originates from outside this virtual network'. The entire dialog box is contained within a light gray box with a black border.

Virtual network gateway ⓘ

Use this virtual network's gateway

Use the remote virtual network's gateway

None (default)

Remote virtual network

Peering link name *

SpokeToHubPeer ✓

Virtual network deployment model ⓘ

Resource manager

Classic

I know my resource ID ⓘ

Subscription *

Pay-As-You-Go

Virtual network *

SpokeVnet1

Virtual network *

SpokeVnet1

Traffic to remote virtual network ⓘ

Allow (default)

Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network ⓘ

Allow (default)

Block traffic that originates from outside this virtual network

Virtual network gateway ⓘ

Use this virtual network's gateway

Use the remote virtual network's gateway

None (default)

Add

Navigate to All services > Route tables.

The screenshot shows the 'Route tables' blade in the Azure portal. At the top left, it says 'ipspecialist (Default Directory)'. Below that is a toolbar with buttons for 'Add' (highlighted with a red box), 'Edit columns', 'Refresh', 'Try preview', and 'Assign tags'. A message 'Subscriptions: Pay-As-You-Go – Don't see a subscription? Open Directory + Subscription settings' is displayed. Below the toolbar are filters for 'Filter by name...', 'All resource ...', 'All locations', 'All tags', and 'No gro...'. It shows '0 items' and a header row with columns: Name ↑↓, Resource group ↑↓, Location ↑↓, and Subscript. The entire blade is enclosed in a large rectangular border.

Click Create route table, and set the following values:

- Name: Anything you like (e.g., "DefaultRoute")
- Resource group: Select the one listed in the dropdown
- Location: The same location as before

Click Create.

The screenshot shows the 'Create route table' wizard in the 'Basics' step. It has three tabs: 'Basics' (selected), 'Tags', and 'Review + create'. Under 'Project details', it says 'Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.' It shows a 'Subscription' dropdown set to 'Pay-As-You-Go' and a 'Resource group' dropdown set to 'secure_vnet_azure_firewall' with a 'Create new' link. Under 'Instance details', it shows a 'Region' dropdown set to 'South Central US' and a 'Name' input field containing 'DefaultRoute' with a green checkmark. It also shows a 'Propagate gateway routes' section with 'Yes' selected (radio button checked). The entire form is enclosed in a large rectangular border.

Once it is deployed, click its name.

Click Routes > Add.

The screenshot shows the 'Route tables' blade in the Azure portal. At the top, there are buttons for '+ Add', 'Edit columns', 'Refresh', 'Try preview', and 'Assign tags'. Below this, a message says 'Subscriptions: Pay-As-You-Go – Don't see a subscription? Open Directory + Subscription settings'. There are four filter dropdowns: 'Filter by name...', 'All resource ...', 'All locations', 'All tags', and 'No gro...'. A table header row shows columns for Name, Resource group, Location, and Subscription. The table contains one item: 'DefaultRoute' under 'Name', 'secure_vnet_azure_fire...' under 'Resource group', 'South Central US' under 'Location', and 'Pay-As-You' under 'Subscription'.

Set the following values:

- Route name: Anything you'd like (e.g., "DefaultRoute1")
- Address prefix: 0.0.0.0/0
- Next hop type: Virtual appliance
- Next hop address: 10.10.200.68

Click OK.

The screenshot shows the 'Add route' dialog box. It has a title 'Add route' and a subtitle 'DefaultRoute'. The form contains the following fields:

- Route name *: DefaultRoute1
- Address prefix *: 0.0.0.0/0
- Next hop type: Virtual appliance
- Next hop address *: 10.10.200.68

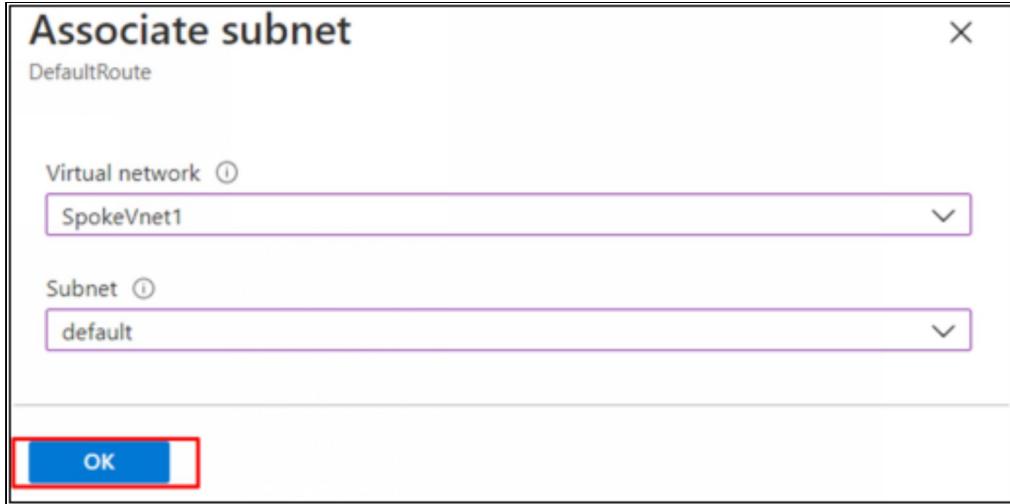
Each field has a green checkmark icon to its right, indicating validation status.

Click Subnets.

Click Associate.

- Select Virtual network and select SpokeVnet1.
- Select Subnet and select default.

Click OK.



Step#05

Allow Remote Desktop Protocol Traffic through the Azure Firewall and the Network Security Group

Navigate to All services > Firewalls.

Click the firewall we created earlier.

Click Public IP Configuration, and copy and paste its listed public IP address into a text editor since you need it in a bit for configuration.

Click Rules.

Click Add NAT rule collection, and set the following values for the rule collection:

A screenshot of the 'Firewall1 | Rules' interface. It shows a header with a briefcase icon and the text 'Firewall1 | Rules'. Below it is a 'Refresh' button and a note: 'This firewall can be managed by Azure Firewall Manager.' A navigation bar at the top includes tabs for 'NAT rule collection' (which is underlined), 'Network rule collection', and 'Application rule collection'. A red rectangular box highlights the 'Add NAT rule collection' button. Below this is a table with columns: Priority, Name, Action, and Rules. The table displays the message 'No results'.

- Name: Anything you like (e.g., "RDPForward")
- Priority: Any number between 100 and 50000
- In the Rules section, set the following values:
- Name: Anything you'd like (e.g., "RDPToSPOKE")
- Protocol: TCP and UDP
- Source Addresses: Can be a wildcard (*) or your public IPv4 address (which you can get by querying Google)
- Destination Addresses: The public IP address of the firewall we copied earlier
- Destination Ports: 3389
- Translated Address: 10.10.10.4
- Translated Port: 3389
- Click Add.

Add NAT rule collection

Name *	RDPForward		
Priority *	1000		
Action	Destination Network Address Translation (DNAT).		
Rules			
name	Protocol	Source type	Source
RDPtoSpoke ✓	2 selected ✓	IP address ✓	202.163.81.106 ✓
	0 selected ✓	IP address ✓	*, 192.168.10.1, 192...
Destination Addr...	Destination Ports	Translated address	Translated port
40.119.7.179 ✓	3389 ✓	10.10.10.4 ✓	3389 ✓

Navigate to All services > Network security groups.

Click the network security group we created earlier.

Click Inbound security rules.

Click Add

SpokeNSG1 | Inbound security rules

Network security group

+ Add Default rules Refresh

Priority	Name	Port	Protocol	Source IP addresses/CIDR ranges
65000	AllowVnetInBound	Any	Any	Virtual network
65001	AllowAzureLoadBalancing	Any	Any	Azure Load Balancer
65500	DenyAllInBound	Any	Any	Any

Set the following values:

- Source: IP Addresses
- Source IP addresses/CIDR ranges: 10.10.200.64/26
- Source port ranges: *
- Destination: IP Addresses
- Destination IP addresses/CIDR ranges: 10.10.10.4
- Destination port ranges: 3389
- Name: Anything you'd like (e.g., "RDPtoSpoke")
- Click Add.

Add inbound security rule

SpokeNSG1

Basic

Source * ⓘ

IP Addresses

Source IP addresses/CIDR ranges * ⓘ

10.10.200.64/26

Source port ranges * ⓘ

*

Destination * ⓘ

IP Addresses

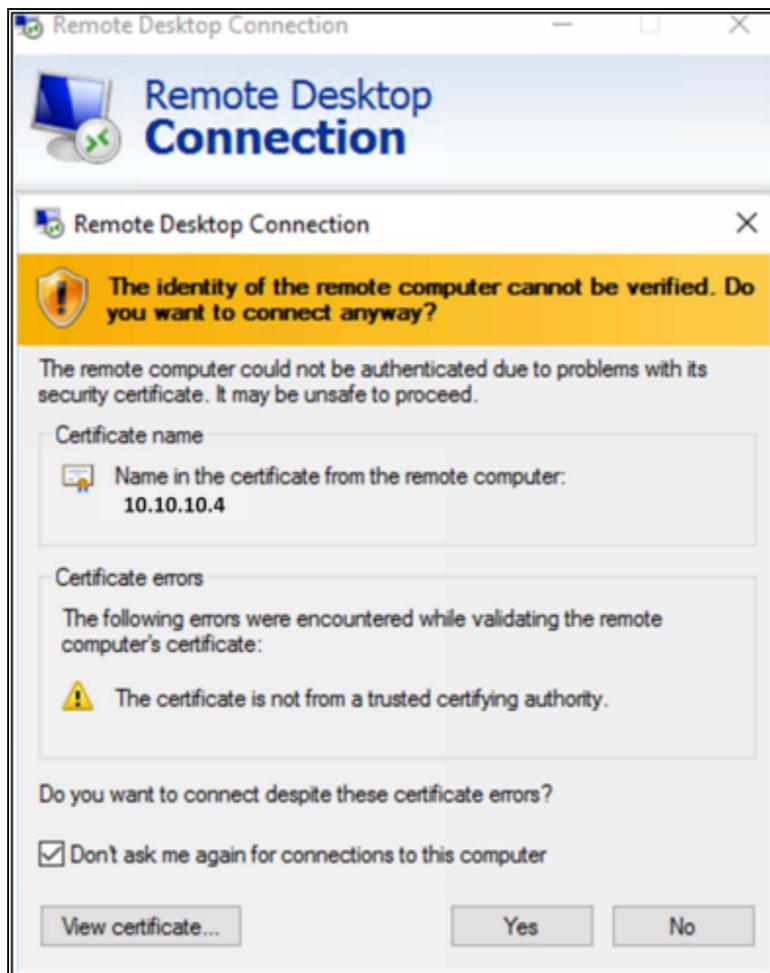
Destination IP addresses/CIDR ranges * ⓘ

10.10.10.4

Step#06

Test Azure Firewall

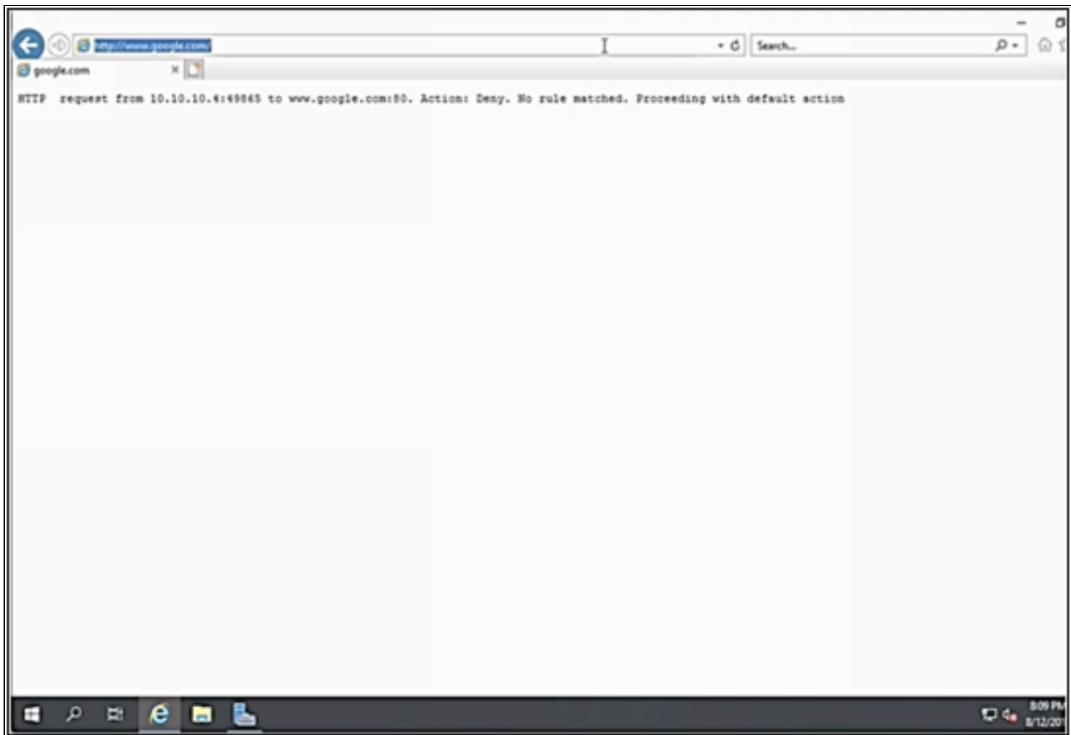
Open RDP to connect to the public IP address of the Azure Firewall.



If it is working correctly, a standard Windows credential pop-up should be presented.

Provide the username and password of the virtual machine, and then click Continue.

Once connected, open an Internet Explorer window and browse to Google.com. The response should be similar to:



HTTP request from 10.10.10.4:50626 to www.google.com:80. Action: Deny. No rule matched. Proceeding with default action

This is exactly what should be expected, as no internet-bound rules were created in the firewall, while the NSG has default rules allowing all internet-bound traffic to pass, proving the firewall is working as intended.

Conclusion

Congratulations on successfully completing this lab!

Lab 4-02: Configuring an Azure VNet-to-VNet VPN Gateway (v2)

Introduction

Virtual network gateways allow us to connect our on-premises network to an Azure data center. We can then extend our IT presence into the cloud by integrating Azure resources with our local Active Directory. A VPN gateway is a fast, secure way to start our organization's transfer to the cloud. In this lab, we connect one virtual network (VNet) to another in an Azure resource group. We then test connectivity between virtual machines located in each VNet. However, this lab is completely limited in Azure, the procedure and concepts can be used for local network-to-Azure connectivity as well.

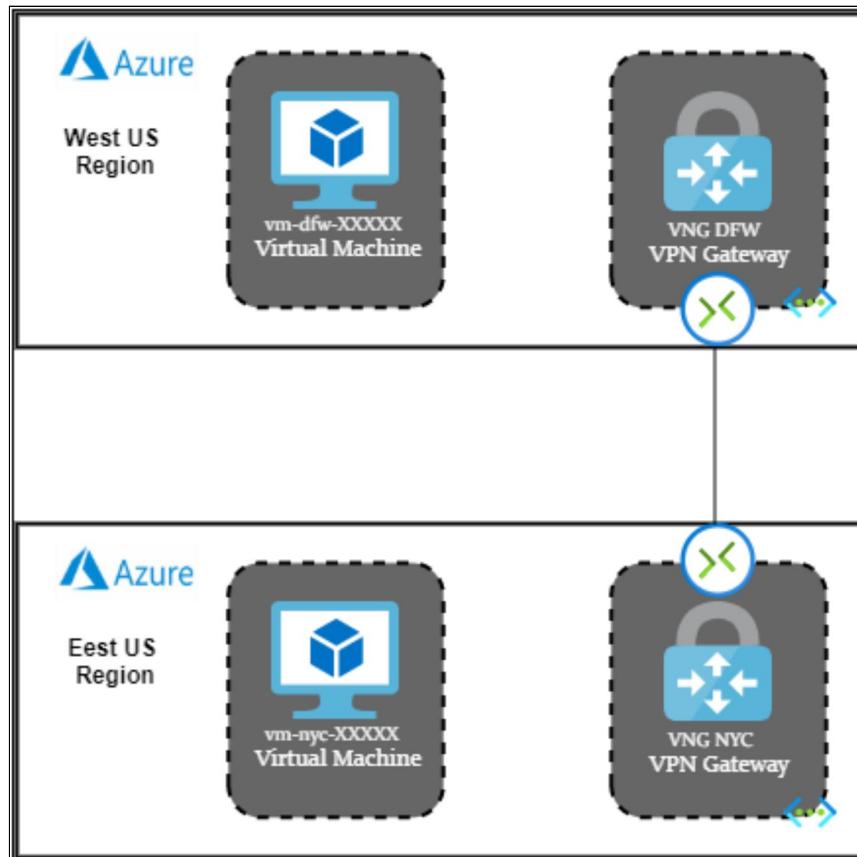


Figure 4-05: Configuring an Azure VNet-to-VNet VPN Gateway

Note: The lab has been updated with pre-deployed Azure virtual network gateways.

Solution

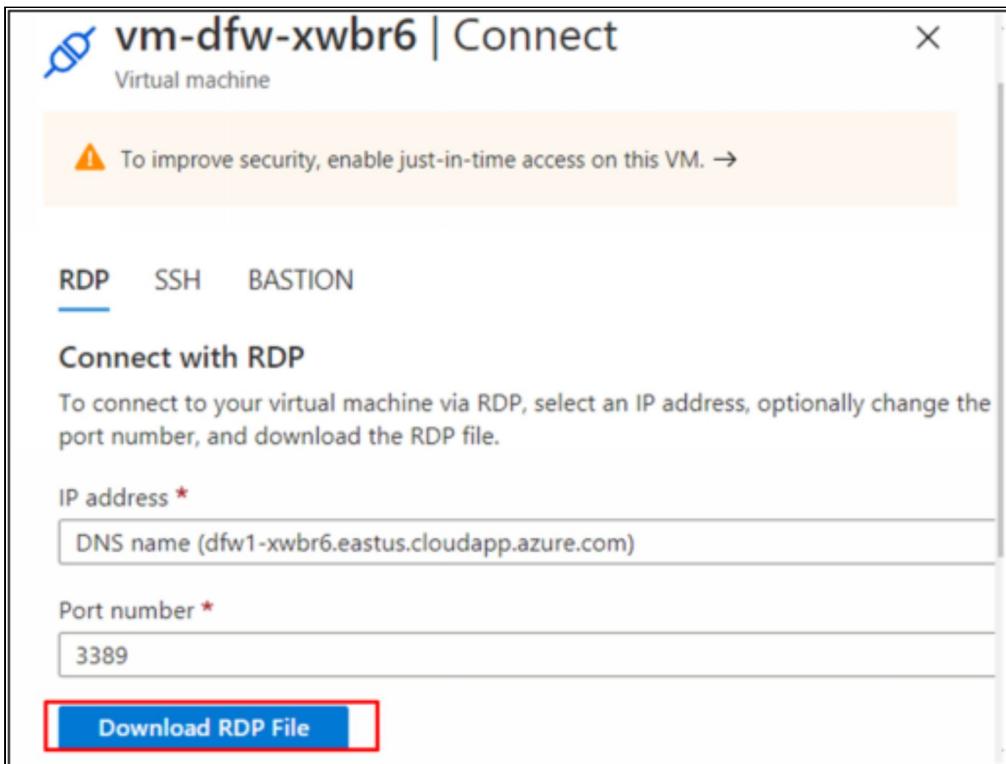
Log in to the Azure Portal using the credentials and follow below steps.

Step#01

Click on the virtual machine named vm-dfw-XXXXXX

Inside the virtual machine blade, click Connect.

Click Download RDP File.



Open the RDP file to connect to the virtual machine.

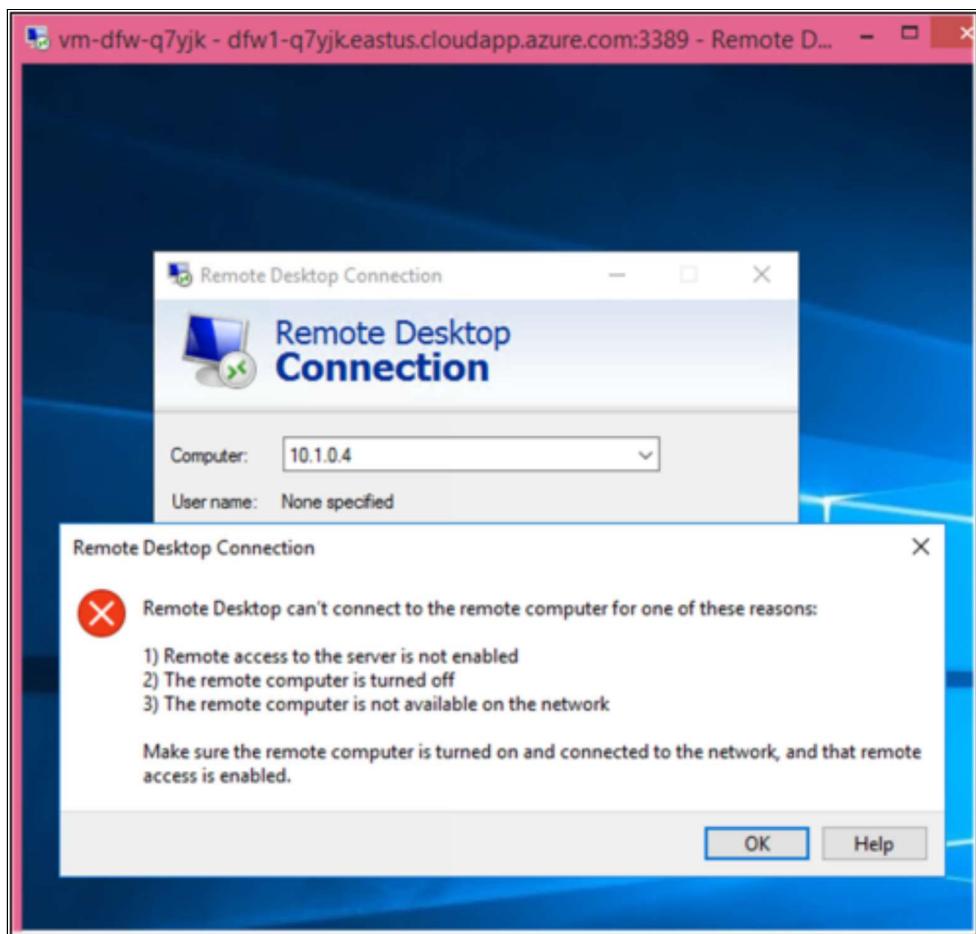
Log in to the virtual machine using the following credentials:

Username: *

Password: *

In the DFW VM, open the Remote Desktop Connection application.

In the Computer field, enter the IP address of the virtual machine in NYC: 10.1.0.4. Verify that we are unable to connect.



Note: Optionally, we can test connectivity from the NYC virtual network by performing the previous steps using the VM in NYC. Log in to the VM in NYC and try to connect to the VM in DFW using its IP: 10.0.0.4.

Step#02

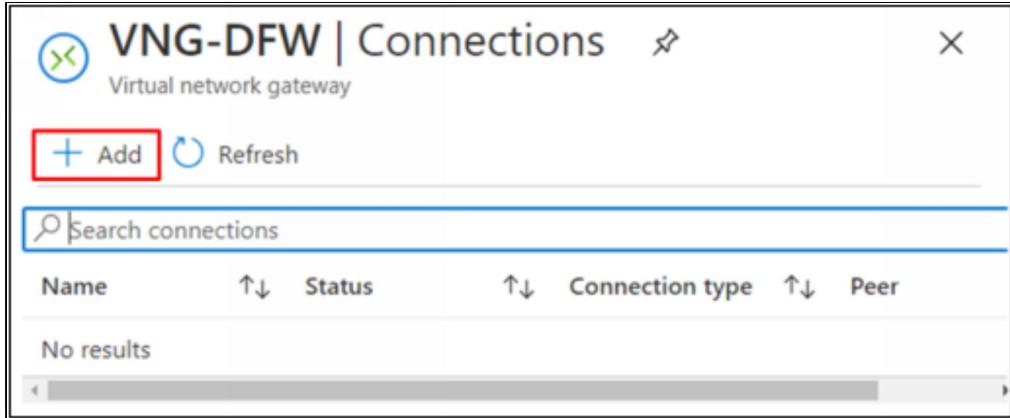
Create VPN Connections

In the Azure Portal, navigate to All resources.

Click VNG-DFW.

Once in the blade for the gateway, click Connections.

Click + Add.



Use the following settings, leaving all other settings at their default values:

- Name: DFW-NYC
- Second virtual network gateway: VNG-NYC
- Shared key (PSK): abc123
- Click OK to create the connection.

A screenshot of a "Add connection" dialog box for "VNG-DFW".

- Name ***: DFW-NYC
- Connection type**: VNet-to-VNet
- *First virtual network gateway**: VNG-DFW
- *Second virtual network gateway**: VNG-NYC
- Shared key (PSK) ***: abc123

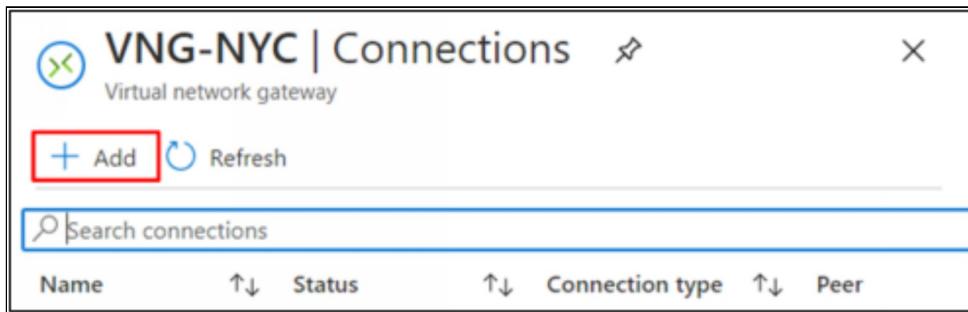
The "Name" field is highlighted with a purple border. The "Second virtual network gateway" dropdown shows "VNG-NYC" with a right-pointing arrow. The "Shared key (PSK)" field contains "abc123" and has a green checkmark icon.

Click > All resources.

Click VNG-NYC.

Once in the blade for the gateway, click Connections.

Click + Add.

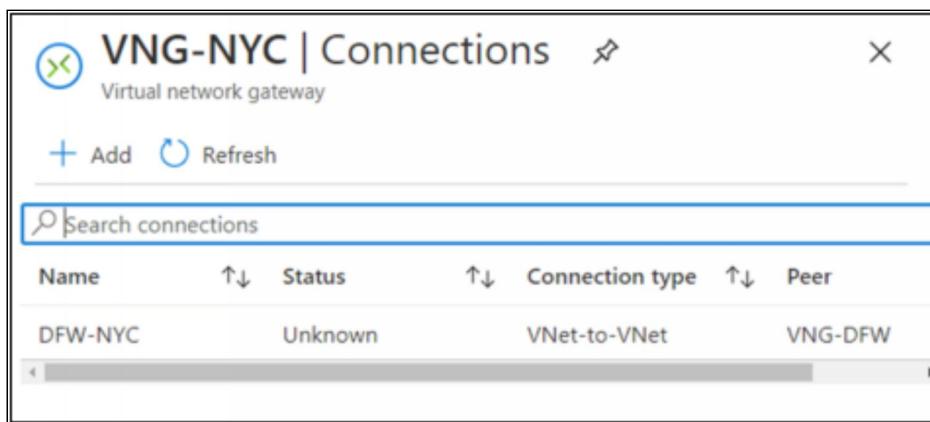


Use the following settings, leaving all other settings at their default values:

- Name: NYC-DFW
- Second virtual network gateway: VNG-DFW
- Shared key (PSK): abc123
- IKE Protocol: IKEv2
- Click OK to create the connection.

Wait for Connections to Become Connected

Once the connections are created, the status for each connection initializes to Unknown.



They will both change to Updating, then Connecting, and finally Connected. Once both connections are Connected, proceed to the next step.

The screenshot shows the 'VNG-DFW | Connections' page. At the top, there's a green circular icon with a white 'X' and the text 'Virtual network gateway'. Below that are buttons for '+ Add' and 'Refresh'. A search bar with a magnifying glass icon and the placeholder 'Search connections' is present. A table lists the connections:

Name	Status	Connection type	Peer
DFW-NYC	Connected	VNet-to-VNet	VNG-NYC
NYC-DFW	Connected	VNet-to-VNet	VNG-NYC

Step#03

Verify Connectivity between Virtual Machines

In the NYC VM, open Remote Desktop Connection.

Attempt to connect to 10.0.0.4. Verify that we are now able to connect.

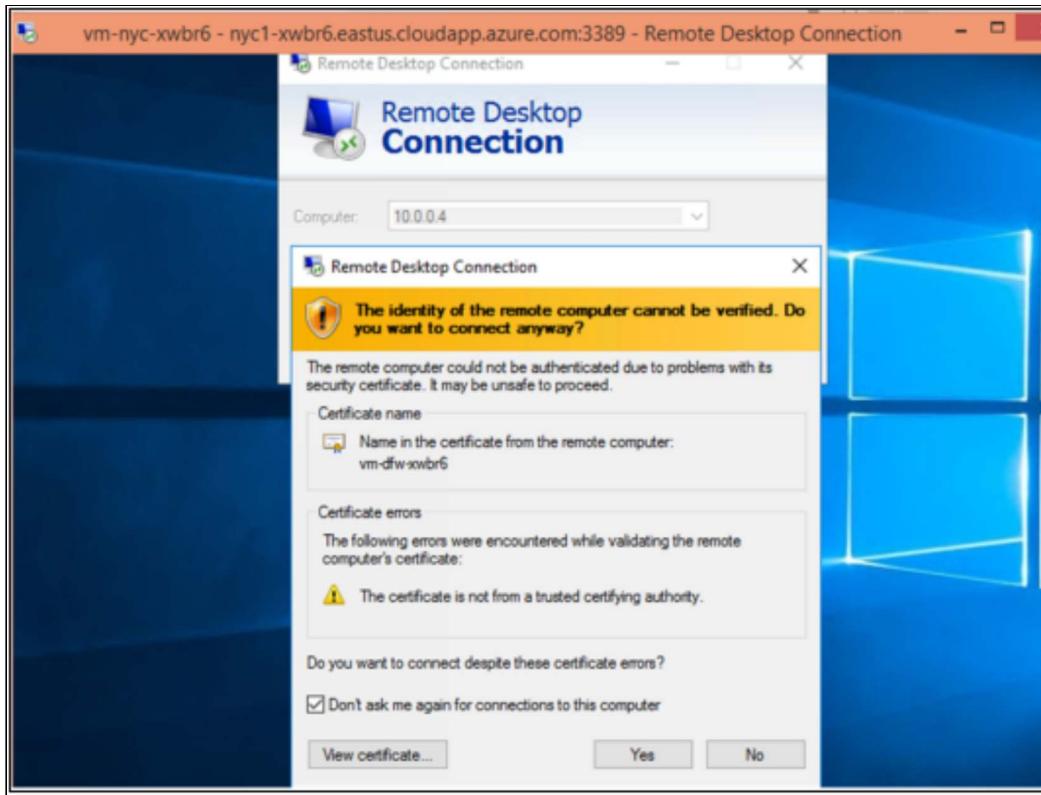
Use the same login credentials we used to log in to the virtual machine:

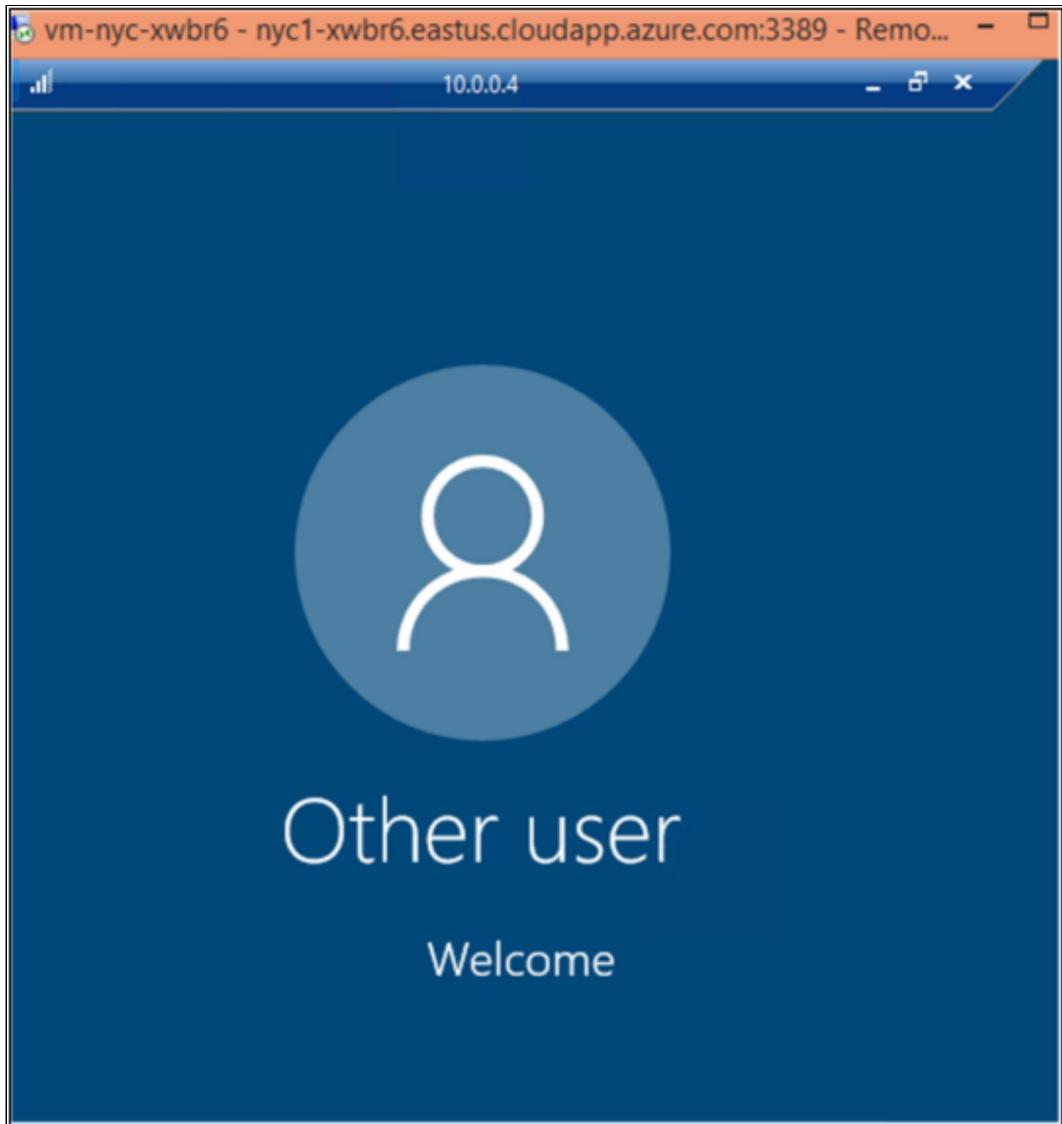
Username: *

Password: *

In the dialog asking us to verify the certificate, click Yes.

We should then be logged in to the DFW VM.





Note: Optionally, in the DFW VM, we can open Remote Desktop Connection again, attempt to connect to 10.1.0.4, and verify we are now able to connect.

Conclusion

Congratulations on successfully completing this lab!

Practice Questions

1. The basic building block for your private network in Azure is the _____.
 - A. VPN gateway
 - B. Azure Resource Groups
 - C. Network Security Group (NSG)
 - D. Azure Virtual Networks (VNs)

2. VNet is _____ to a conventional network.
 - A. Private
 - B. Public
 - C. Similar
 - D. Different

3. The VNet has an _____ address space.
 - A. Internal
 - B. External
 - C. Private
 - D. Public

4. Which routing connection is created between your on-premises VPN device and the virtual network deployed by the Azure VPN Gateway?
 - A. Express Route
 - B. Site-to-site VPN
 - C. BGP
 - D. Route Tables

5. Which routing connection is developed by a partner between your network and Azure. Such connection is confidential.
 - A. Express Route
 - B. Site-to-site VPN
 - C. BGP
 - D. Route Tables

6. Site-to-site VPN and Express Route routing connection requires _____ to facilitate routing.
- A. VPN Gateway
 - B. Virtual Network
 - C. VNet Peering
 - D. VNet Tunnel
7. Which are used to filter network traffic to and from Azure services on an Azure virtual network.
- A. VPN gateway
 - B. Azure Resource Groups
 - C. Network Security Group (NSG)
 - D. Azure Virtual Networks (VNets)
8. Network Security Group (NSG) is based on a _____ that allow or deny different forms of Azure services to inbound or outbound network traffic from a network.
- A. Security rules
 - B. Priority levels
 - C. Port numbers
 - D. Protocols
9. In Network Security Group (NSG), you must define _____ for each security rule.
- A. Source
 - B. Destination
 - C. Port
 - D. Protocol
 - E. All of the above
10. On which of the following, NSGs can be applied to?
- A. Network Interface Cards (NIC)
 - B. Subnet
 - C. Both
 - D. None

11. _____ is a logical collection of virtual machines, specifically their Network Interface Cards (NICs).
- A. Application Security Groups (ASGs)
 - B. VPN gateway
 - C. Azure Resource Groups
 - D. Network Security Group (NSG)
12. You join the ASG virtual machines and then use the application security group in the _____ rules as a source or destination.
- A. Inbound
 - B. Outbound
 - C. NSG
 - D. All of the above
13. VPN Gateway is designed for _____ connectivity.
- A. Public
 - B. VNet-to-VNet
 - C. Hybrid
 - D. Private
14. Which connectivity supports cross-region VNet connectivity?
- A. VPN Gateway
 - B. VNet Peering
 - C. Both
 - D. Neither
15. Which network security group service tag represents all CIDR ranges defined for the virtual network?
- A. Virtual Network
 - B. Gateway Manager
 - C. Internet
 - D. Azure Cloud
16. What is the name of the subnet that must be created in order to deploy Azure Firewall?

- A. default
- B. FirewallSubnet
- C. AzureFirewallSubnet
- D. DMZsubnet

17. _____ are the most common resources of Resource Firewall.

- A. Azure Storage Accounts
- B. Azure SQL server databases
- C. Both
- D. Azure Backup

Chapter 05: Securing VMs and Other Azure Resources

Introduction

This chapter explains how you can protect your systems from any malware or virus attacks. Microsoft offers several different services that we can use to protect our virtual machines including a free service, which will be covered in this chapter.

Host Security: VM Endpoint Security

Microsoft Antimalware for Azure is a free real-time protection service that helps identify and remove viruses, spyware, and other malicious software. It generates alerts when known malicious or unwanted software tries to install itself or run on your Azure systems.

Features includes:

1. **Real-time protection:** It monitors activity in Cloud Services and on Virtual Machines to detect and block malware execution.
2. **Malware remediation:** It automatically takes action on detected malware, such as deleting or quarantining malicious files and cleaning up malicious registry entries.
3. **Signature updates:** It automatically installs the latest protection signatures (virus definitions) to ensure protection is up-to-date on a pre-determined frequency.
4. **Antimalware engine updates:** It automatically updates the Microsoft Antimalware engine.
5. **Antimalware platform updates:** It automatically updates the Microsoft Antimalware platform.
6. **Active protection:** It reports telemetry metadata about detected threats and suspicious resources to Microsoft Azure to ensure rapid response to the evolving threat landscape, as well as enabling real-time synchronous signature delivery through the Microsoft Active Protection System (MAPS).
7. **Sample reporting:** It provides report samples to the Microsoft Antimalware service to help refine the service and enable troubleshooting .
8. **Exclusions:** It allows application and service administrators to configure exclusions for files, processes, and drives.
9. **Antimalware event collection:** It records the antimalware service health, suspicious activities, and remediation actions taken in the operating system event log and collects them into the customer's Azure Storage account.
10. **Schedule scanning:** It scans periodically to detect malware, including actively running programs.

Pros:

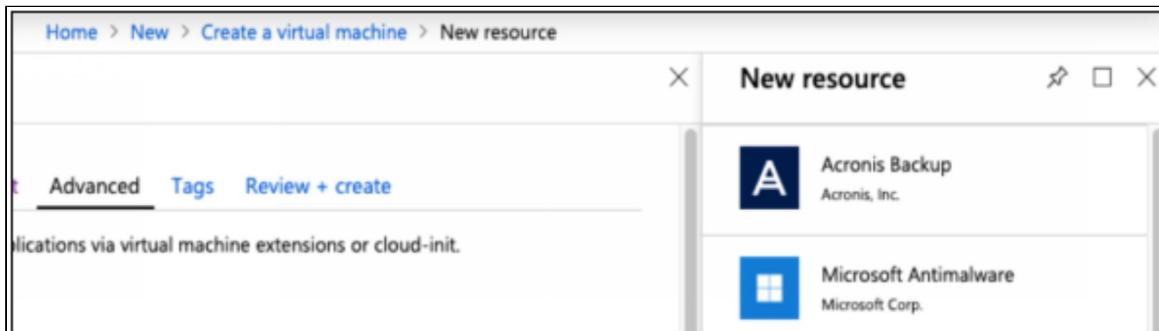
1. **Free:** VM Endpoint Security is free to use. Every user can use it without any subscription.
2. **Easy to deploy:** You can easily deploy VM Endpoint Security.
3. **Fully featured:** It has all the features you need in order to protect your data.

Cons:

1. **Not easy to modify:** You cannot modify this VM Endpoint Security easily because it has some security features and deployment tools that cannot be modified easily.
2. **Limited client availability:** It provides access to a limited number of users.
3. **No centralized management:** Everyone cannot manage it. Only the user with administrative rights can manage and update it.

Antimalware: Single VM Deployment

You can configure and deploy Microsoft Antimalware using Azure extensions. This can be performed on new VM deployments as well as existing VMs.



You can set and specify exclusions and protection parameters at deployment.

Install extension

Excluded files and locations 

Excluded file extensions 

Excluded processes 

Real-time protection 

Run a scheduled scan 

Scan type 

Scan day 

Saturday

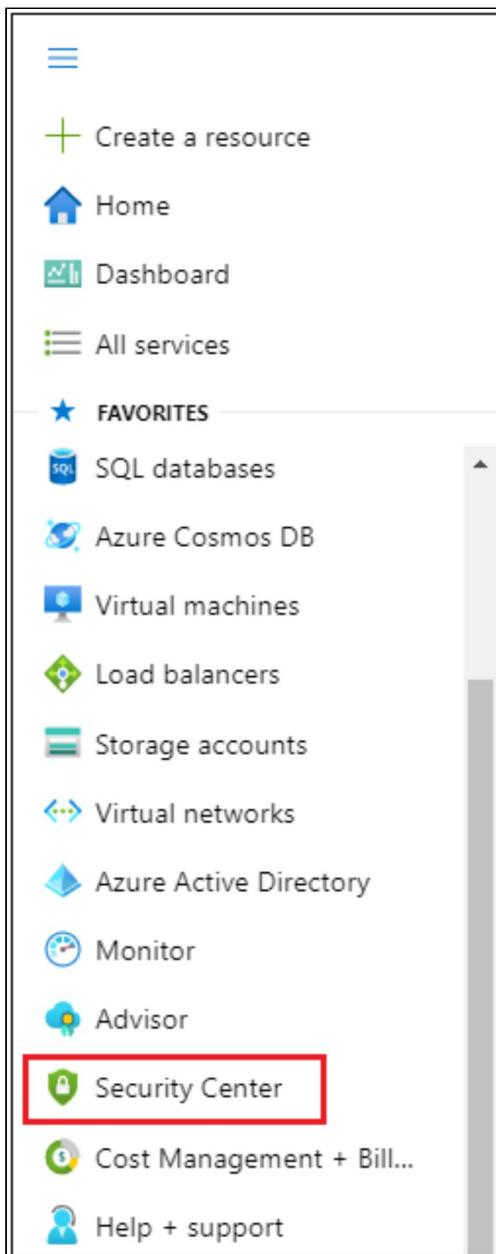
Scan time 

120

Antimalware: Multiple VM Deployment

You can also configure and deploy Microsoft Antimalware using Azure Policy of Azure Security Center. The preferred way to deploy multiple VMs is by Azure Security Center.

First, click on Azure Security Center.



This will give you a brief overview of Azure Security Center. You can then deploy multiple VMs. Security Center will enable all the Antimalware single or multiple VMs.

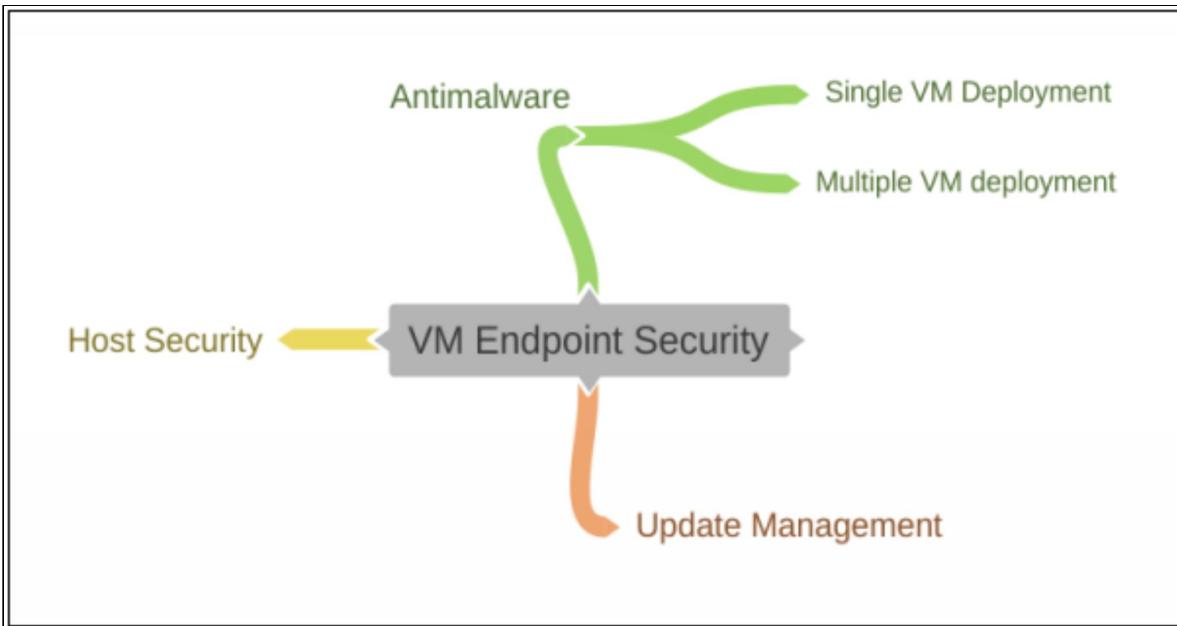
The screenshot shows the Azure Security Center Overview page. At the top left is the 'Home' link. The main title is 'Security Center | Overview' with a shield icon. Below it says 'Showing subscription 'Pay-As-You-Go''. A search bar with 'Search (Ctrl+I)' placeholder text is followed by 'Subscriptions' and 'What's new' buttons. On the left, a sidebar under 'General' has 'Overview' selected, along with links for 'Getting started', 'Recommendations', 'Security alerts', 'Inventory', and 'Community'. Under 'Cloud Security', there is a 'Secure Score' link. The main content area has a message: 'You're seeing limited information. For tenant-wide visibility, click here →'. It displays three metrics: 'Azure subscriptions' (1), 'Active recommendations' (0), and 'Security alerts' (--). Below these is a large 'Secure score' section with a shield icon and a progress bar.

Host Security: Update Management

Azure provides the update management solution to allow you to manage updates and patches for your Windows VMs. This solution requires Azure Log Analytics and an Azure Automation Account. If these are not available at deployment, they can be provisioned for you. You can then deploy updates for your new or existing VMs through update management.

The screenshot shows the Azure portal interface for configuring Update Management on a virtual machine. On the left, a sidebar lists various management options under three main categories: Configuration, Operations, and Monitoring. The 'Update management' option is highlighted with a blue selection bar. The main pane is titled 'Update Management' and contains the following information:

- A brief description: "Enable consistent control and compliance of this VM with Update Management."
- A note: "This service is included with Azure virtual machines. You only pay for logs stored in Log Analytics."
- A note: "This service requires a Log Analytics workspace and an Automation account. You can use your existing workspace and account or let us configure the nearest workspace and account for use."
- Two radio button options:
 - Enable for this VM
 - Enable for VMs in this subscription
- Location dropdown: East US
- Log Analytics workspace dropdown: defaultworkspace
- Automation account subscription dropdown: Microsoft Azure
- Automation account dropdown: Automate
- A large blue 'Enable' button at the bottom.



Role-Based Access Control (RBAC)

Azure RBAC is an authorization system built on Azure Resource Manager that provides fine-grained access management of resources in Azure. With Azure RBAC, you can grant the exact access that users need to do their jobs. For example, you can use Azure RBAC to let one employee manage virtual machines in a subscription while another manages SQL databases within the same subscription.

While Conditional Access and Identity Protection are used to control access to Azure AD managed resources, RBAC is used to provide granular access to Azure resources.

These roles can be assigned at the subscription, resource group, or resource level.

- Azure includes a range of over 70 built-in roles for controlling access to Azure resources. Some examples are:
 - **Owner:** Includes full access to the assigned resource(s) like rights to grant access to others.
 - **Contributor:** Provides full access to the assigned resource(s) except for rights to change permissions.
 - **Reader:** Provides full view access to the assigned resource(s) but no ability to make changes.

If the built-in roles are not sufficient, custom roles can be created.

- For roles to take effect, they must be assigned.
 - Roles are assigned to an azure AD user, group, or service principal.
 - They must be assigned to something: a subscription, resource group, or resource.

Managed Identities

Managed identities provides a secure method for authenticating Azure resources against other Azure services without needing to include credentials. Managed Identities is a feature of Azure AD which specifically provides an Azure resource with a managed identity within Azure AD.

This feature provides the ability to authenticate an Azure resource “behind-the-scenes”. This does not provide any implicit permissions (authorization) though. Those must be configured separately.

- It avoids the need for application credentials to be stored in code (e.g. Client ID and secrets).
- It is fully managed by Microsoft, so credentials no longer need to be rotated by developers.
- It automates the creation and registration of an application within Azure AD, Service Principal, and Client ID.
- It includes built-in functionality for Azure resources to securely obtain an authentication token.
- It does not imply any authorization, since the identity must still be granted whatever permissions desired.

Azure Resources Locks

We can use Azure resource locks to prevent other users in our organization from accidentally deleting or modifying critical resources such as subscriptions, resource groups, or resources.

There are two types of resource locks:

- **CanNotDelete:** It means authorized users can read and modify a resource, but they cannot delete that resource.
- **ReadOnly:** It means authorized users can read a resource, but they cannot delete or update it. Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.

When a resource lock is used at a parent scope, such as a subscription or resource group, all resources within that scope inherit the same lock. Resources added later inherit the lock from the parent. When a resource inherits multiple locks, the most restrictive lock in the inheritance takes precedence.

Unlike role-based access control, resource locks apply a restriction across all users and roles.

You must have access to Microsoft.Authorization/* or Microsoft.Authorization/locks/* actions to create or delete management locks. Owner and User Access Administrator are the only built-in roles granted those actions.

First, click on “Locks” and then click on “Add”.

A screenshot of the Azure portal interface. On the left, there's a sidebar with icons for Overview, Activity log, Access control (IAM), Tags, Events, Settings (with Deployments, Policies, and Properties), and Locks. The 'Locks' icon is highlighted with a yellow arrow. At the top, there's a search bar, a '+ Add' button (highlighted with a red box), a 'Subscription' dropdown, and a 'Refresh' button. The main content area shows a table with columns for Lock name, Lock type, Scope, and Notes. A message at the top of the table says, 'This resource has no locks.'

Choose the lock type, add a lock name and click on “Ok”.

A screenshot of the 'Add lock' dialog box. It has a header with '+ Add', 'Subscription', and 'Refresh' buttons. The main title is 'Add lock'. There are two input fields: 'Lock name' and 'Notes'. To the right of 'Lock name' is a 'Lock type' dropdown menu (highlighted with a blue box) which is currently open, showing 'Read-only' and 'Delete' options. At the bottom are 'OK' and 'Cancel' buttons, with 'OK' being highlighted with a blue box.

Azure Management Groups

Azure management groups allow us to group subscriptions to manage access, policies, and compliance. Think of them as one level above subscriptions, but only for management. Billing responsibility is still handled on the subscription level.

Subscriptions within a management group inherit the access, policies, and other compliance factors applied to it. A management group may contain individual subscriptions or other management groups in a nested hierarchy.

You can create management groups and apply a policy requiring all Azure resources to be created in a particular Azure region for compliance purposes. Another management group can be used to determine access to multiple subscriptions (via RBAC), as opposed to granting access on the subscription level.

When using management groups, the first group is called the Tenant Root Group and is used to manage all subscriptions. If you are a Global Administrator, you can elevate your access to allow you to manage access to the root group.

Azure Policies

Azure Policy is a service in Azure you use to create, assign, and manage policies. These policies enforce different rules and effects over your resources so those resources stay compliant with your corporate, technical, or government standards.

For example, you can define the policy to allow only a certain SKU size of virtual machines in your environment. If an Azure administrator attempts to deploy a virtual machine outside one of your defined SKU sizes, the deployment will fail validation and will not be deployed.

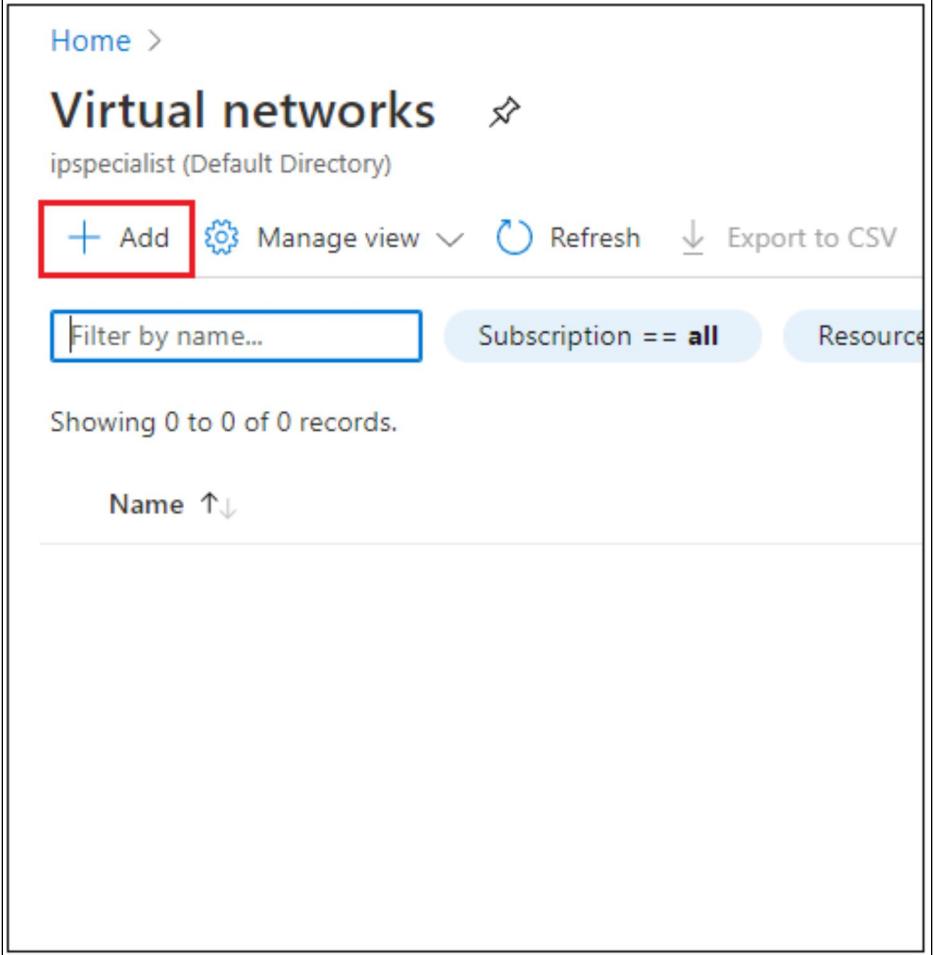
Also, existing resources found to be non-compliant can be remediated.

Policy definitions outline the specific criteria to be evaluated. Assignments determine where these policies are applied. They can be applied to Azure subscriptions and optionally to child resource groups. Child resources inherit the policy settings applied to their parents.

Policy initiatives are collections of policy definitions designed to accomplish a singular goal, such as the overall compliance of corporate standards. They are assigned in the same manner as individual definitions.

Lab 5-01

1. Navigate to Resource groups in the left-hand menu to verify the region your resource group is located in.
2. Navigate to Virtual networks in the left-hand menu and click “Create virtual network”.



The screenshot shows the Azure portal interface for managing Virtual networks. At the top, there's a breadcrumb navigation from Home > Virtual networks. Below that, it says 'ipspecialist (Default Directory)'. There are several buttons at the top: '+ Add' (which is highlighted with a red box), 'Manage view', 'Refresh', and 'Export to CSV'. Below these are search/filter fields for 'Filter by name...', 'Subscription == all', and 'Resource'. A message below the filters says 'Showing 0 to 0 of 0 records.' At the bottom, there's a header 'Name ↑' followed by a blank table area.

3. Set the following values:
 - a. Name: PolicyVnet1
 - b. Address space: 10.0.0.0/24
 - c. Resource group: Select the one listed in the dropdown
 - d. Location: The location you just noted

e. Address range: 10.0.0.0/26

Create virtual network

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. [Learn more about virtual network](#)

Project details

Subscription * ⓘ Pay-As-You-Go

Resource group * ⓘ (New) azresourcegroup
Create new

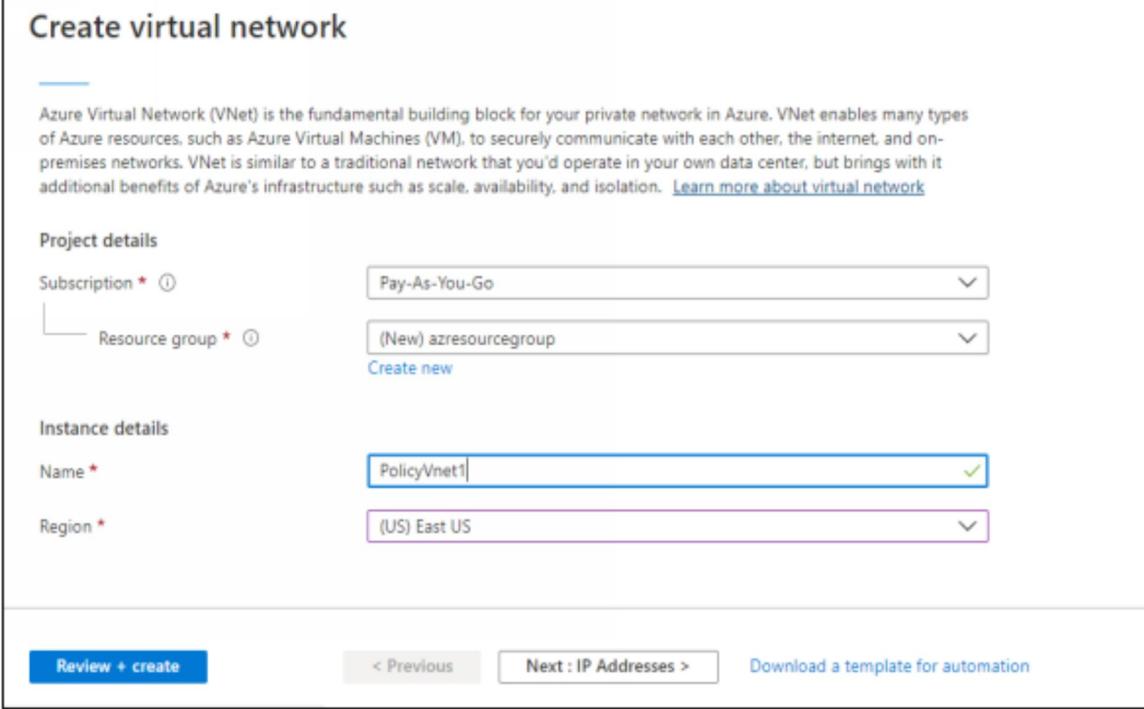
Instance details

Name * PolicyVnet1

Region * (US) East US

Actions

Review + create < Previous Next : IP Addresses > Download a template for automation



4. Click “Create”.

Create virtual network

Basics IP Addresses Security Tags Review + create

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

IPv4 address space

10.0.0.0/16 10.0.0.0 - 10.0.255.255 (65536 addresses)



Add IPv6 address space ⓘ

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

+ Add subnet ⌂ Remove subnet

Subnet name

Subnet address range

default

10.0.0.0/24

Review + create

< Previous

Next : Security >

Download a template for automation

5. Click “Add”.

6. Create the first virtual network and set the following values:

- a. Name: PolicyVnet2
- b. Address space: 10.10.10.0/24
- c. Resource group: Select the one listed in the dropdown
- d. Location: The location we just noted
- e. Address range: 10.10.10.0/26.

Create virtual network

Basics IP Addresses Security Tags Review + create

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. [Learn more about virtual network](#)

Project details

Subscription * ⓘ

Pay-As-You-Go

Resource group * ⓘ

(New) azresourcegroup

[Create new](#)

Instance details

Name *

PolicyVnet2

Region *

(Asia Pacific) Australia East

[Review + create](#)

< Previous

Next : IP Addresses >

[Download a template for automation](#)

7. Click “Create”.

Create virtual network

Basics IP Addresses Security Tags Review + create

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

IPv4 address space

10.0.0.0/16 10.0.0.0 - 10.0.255.255 (65536 addresses)



Add IPv6 address space ⓘ

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

+ Add subnet (i) Remove subnet

Subnet name

Subnet address range

default

10.0.0.0/24

Review + create

< Previous

Next : Security >

Download a template for automation

Create a Tag for Each Virtual Network

1. Click “PolicyVnet1”.
2. Click “Tags” and use the following settings:
 - a. Name: Audit
 - b. Value: Yes

Search (Ctrl+F) Delete all

Overview Activity log Access control (IAM) Tags Events Settings

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. Tag names are case insensitive, but tag values are case sensitive. [Learn more about tags](#)

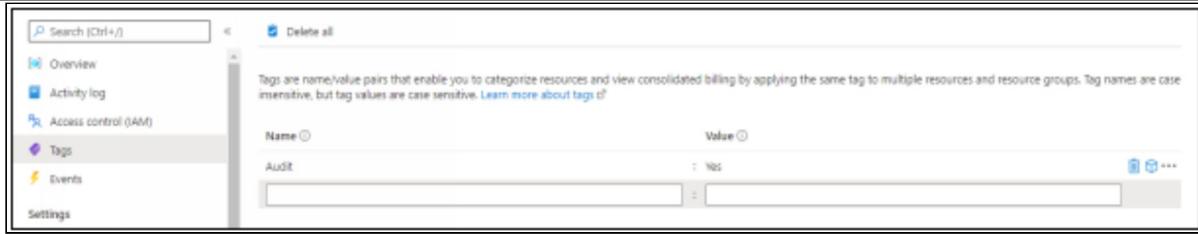
Name ⓘ	Value ⓘ
Audit	: Yes

3. Click “Save”.
4. Click “PolicyVnet2”.

5. Click “Tags” and use the following settings:

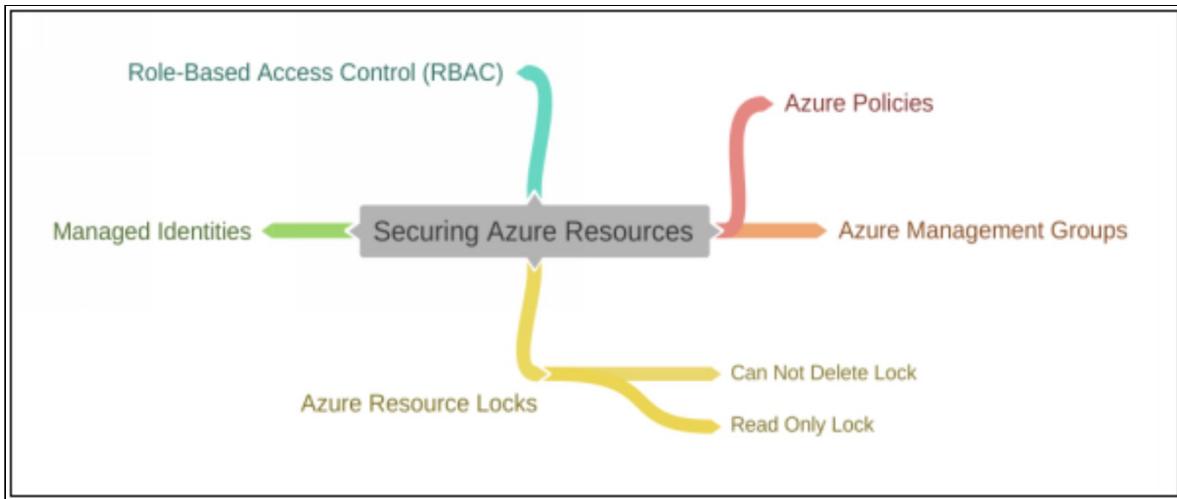
a. Name: Audit

b. Value: No



Create a Policy

1. Navigate to All services > Policy.
2. Click Compliance.
3. Click Assign policy.
4. Next to Scope, click the little blue square.
5. Click the dropdown for Resource Group and choose our listed resource group.
6. Click Select.
7. Next to Policy definition, click the little blue square.
8. Search "Tag" in the available policy definitions list.
9. Choose Require a tag and its value on resources.
10. Click Select.
11. In the Parameters section, use the following settings:
 - a. Tag Name: Audit
 - b. Tag Value: Yes
12. Click Review + Create -> Create.
13. After 15–30 minutes, click the little blue square next to the Scope.
14. Set the Resource Group to listed resource group.
15. Click Select. It should be refreshed to show the policy as non-compliant: 50 %.



Practice Question

- 1. Microsoft Antimalware for Azure removes _____.**
 - a. Viruses
 - b. Spyware
 - c. Malicious software
 - d. All of the above

- 2. Microsoft Antimalware for Azure is _____.**
 - a. Free
 - b. Easy to deploy
 - c. Fully featured
 - d. All of the above

- 3. You can configure and deploy Microsoft Antimalware using Azure**
 - a. Extensions
 - b. Deployments
 - c. Portal
 - d. None of the above

- 4. You can use Azure update management to deploy _____.**
 - a. New VMs
 - b. Existing VMs
 - c. Both of them
 - d. None of them

- 5. You can configure and deploy Microsoft Antimalware using Azure _____.**
 - a. Data Center
 - b. Security Center
 - c. Update Management

d. Configuration Center

6. Role-Based Access Control (RBAC) is used to provide _____ access to Azure resources.

- a. Granular
- b. Control
- c. Both of them
- d. None of them

7. These roles can be assigned at the _____.

- a. Subscription
- b. Resource Group
- c. Resource Level
- d. All of the above

Answer

All of them (d)

Explanation

These roles can be assigned at the subscription, resource group, or resource level.

8. Roles are assigned to an Azure AD _____.

- a. User
- b. Group
- c. Service Principal
- d. All of the above

Answer

All of the above (d)

Explanation

Roles are assigned to an Azure AD user, group, or service principal.

9. How many types of Azure resource locks are there?

- a. One
- b. Two
- c. Three
- d. Four

10. In which type of Azure resource lock can you only read a resource?

- a. CanNotDelete
- b. ReadOnly
- c. Both of them
- d. None of them

11. Resource locks apply a restriction across all _____.

- a. Users
- b. Roles
- c. Both of them
- d. None of them

12. Azure management groups allow to group subscriptions to manage _____.

- a. Access
- b. Policies
- c. Compliance
- d. All of the above

13. The first group in the management group is called _____.

- a. Tenant Root Group
- b. Single Root Group

- c. Root Group
- d. New Root Group

14. Azure Policy is a service in Azure you use to _____.

- a. Create policies
- b. Assign policies
- c. Manage policies
- d. All of the above

15. Assignments determine where to apply the _____.

- a. Policies
- b. Resources
- c. Roles
- d. None of the above

Chapter 06: Container Security

Introduction:

Container security is the use of security technologies and policies, to secure the container as well as its application and performance including storage, application supply chain, system tools, system libraries, and framework against malicious security attacks.

In this lesson, container security is going to be discussed. In the next sections of container security ranging from Azure container registry security all the way to Azure kubernetes service security will be discussed.

Azure Container Registry Security

Microsoft Azure has its own container registry and it is available for you to safely store and retrieve your container images; this is known as Container Registry.

Azure Container Registry is a containerized service that allows us to build, store, and manage images for all types of container deployment. It is a managed Docker registry service based on an open-source Docker Registry.

Creating a Container Registry

Azure Container Registry is a managed, private Docker container registry service for creating, storing, and serving Docker container images. You can create a container registry with Azure portal, Azure CLI, and Azure PowerShell.

Creating a Container Registry using Azure Portal

For creating a Container registry using Azure portal, there is a simple procedure.

1. Sign in to Azure

Sign in to the Azure portal at <https://portal.azure.com>.

2. Create a container registry

Select “Create a resource” > “Containers” > “Container Registry”.

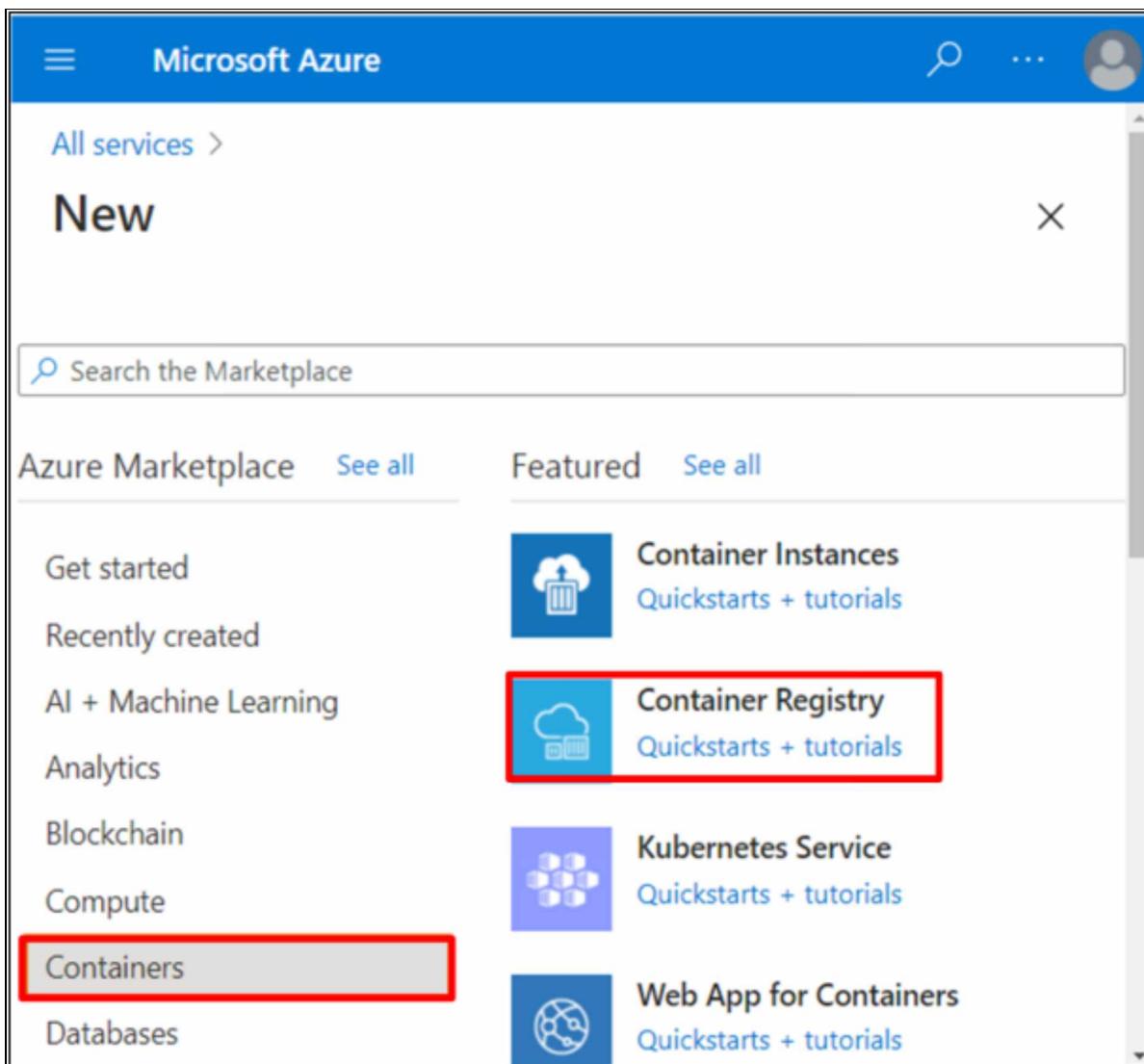


Figure 6-01: Navigate to Container Registry in Portal

In the Basics tab, set the following values for Resource group and Registry name. For example:

- Resource Group: myresourcegroup
- Registry Name: mycontainerregistry
- Location: West US
- SKU: Basic

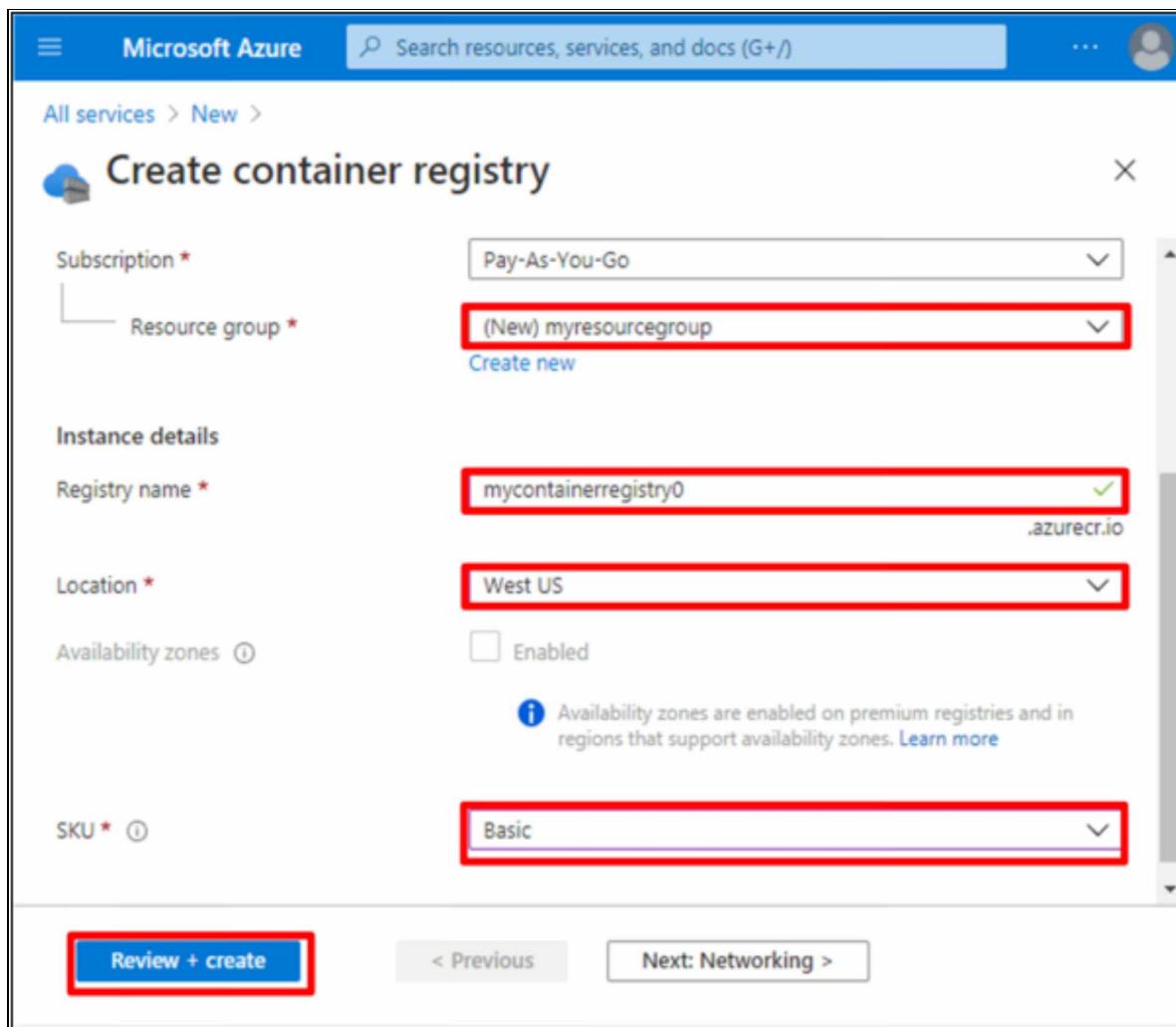


Figure 6-02: Create Container Registry in the Portal

Agree to default values for the remaining settings. Then select Review + create. After reviewing the settings, select Create.

Create an Azure container registry using PowerShell

In this section, you learn how to create an Azure container registry using Azure PowerShell. Follow the below steps.

Create Resource Group

A resource group is a logical container in which you manage and deploy your Azure resources. Once you are log in with Azure, create a resource group named [New-AzResourceGroup](#).

PowerShell

```
New-AzResourceGroup -Name myResourceGroup -Location EastUS
```

Create Container registry

Then, create a container registry in new resource group by using [New-AzContainerRegistry](#) command.

PowerShell

```
$registry = New-AzContainerRegistry -ResourceGroupName "myResourceGroup" -Name "myContainerRegistry007" -EnableAdminUser -Sku Basic
```

Container Registry Authentication

In order to use container registry as it is a private registry, you must authenticate against it to either push or pull container images from the registry. There are several ways to authenticate with an Azure container registry, each of which is applicable to one or more registry usage scenarios.

Azure AD

When working with your registry directly, such as pulling images to and pushing images from a development workstation to a created registry, authenticate by using your individual Azure identity.

Use Azure role-based access control (Azure RBAC), or configure other Azure users with specific Azure roles and permissions that could be assigned in order to retrieve or push an image.

The three main available roles for a container registry include:

1. **AcrPull**: This allows you to pull an image from a private registry
2. **AcrPush**: This allows you to pull and push images to the registry
3. **Owner**: This allows you to pull, push, and assign roles to other users

Service Principal

To control the container register, you can also use Service Principal. Your application or service can use it for headless authentication if

you attach a service principal to your registry. Service principals allow a registry to provide Azure role-based access control and you can allocate a registry to several service principals. For various apps, multiple service principals allow you to specify different access.

The three main available roles for a container registry include:

1. **AcrPull**: This allows you to pull an image from a private registry
2. **AcrPush**: This allows you to pull and push images to the registry
3. **Owner**: This allows you to pull, push, and assign roles to other users

Admin Account

An admin user account is included with each container registry, which is disabled by default. You can allow and manage an admin user's credentials via the Azure portal, Azure CLI, or other Azure tools. Full registry permissions are available for the admin user.

Two keys are provided to the admin account, each of which can be regenerated. By using one password while regenerating the other, two passwords allow you to retain a connection to the register. If the admin account is enabled, you can transfer a username and either password to the docker login command when requested for simple authentication to the registry.

For Example:

You can enable the admin user in the Azure portal by navigating your registry, selecting **Access keys > Settings > Enable > Admin user**.

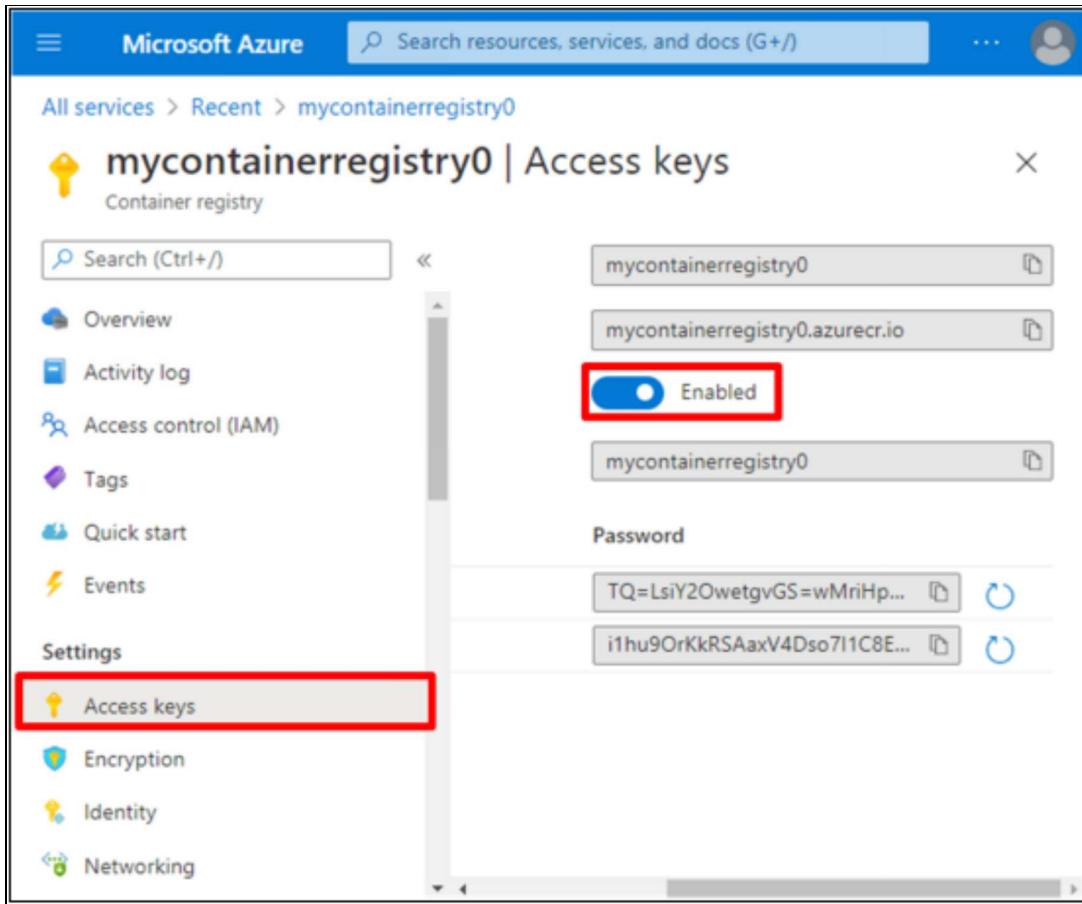


Figure 6-03: Enable Admin User

Pushing an Image to the Registry

To push an image to an Azure Container registry, you must first have an image. Run the following docker pull command to pull an existing file from the Docker Hub if you do not have any local container images yet.

For this example, pull the hello-world image.

Log in to the registry

```
docker login myregistry.azurecr.io
```

Push image to the registry

```
docker pull hello-world
```

Before you can push an image to your registry, you must tag it with the fully qualified name of your registry login server.

```
docker tag hello-world mycontainerregistry.azurecr.io/hello-world:v1
```

Finally, use docker push to push the image to the registry instance.

```
docker push hello-world mycontainerregistry.azurecr.io/hello-world:v1
```

Run image

```
docker run hello-world mycontainerregistry.azurecr.io/hello-world:v1
```

Lock/VNet/Firewall

There are several ways to secure our registries, some of them are:

Locks

Locks are just like any other Azure resource locks such as Storage Account or SQL server locks. You can prevent access to the container registry altogether or prevent update access to the registry.

VNet/Firewall

VNet and Firewall rules also works similarly as they for other Azure resources by allowing and denying access to virtual networks and specific IPs to the container registry.

To enable VNet/Firewall secure feature, we have to change the SKUs of our container registry from basic to premium.

Configuring Instance Security

Containers have been the standard way for cloud applications to be packaged, deployed, and managed. The fastest and easiest way to run a container in Azure is provided by Azure Container Instances, without having to manage any virtual machines and without attempting to adopt a higher-level service.

ACR Tasks

ACR Tasks is a collection of features within Azure Container Registry. It provides cloud-based container image building for Linux, Windows, and ARM. It can also automate OS and framework patching for Docker containers.

ACR tasks can do on-demand container image builds, and enables automated builds on source code commit or when a container's base image is updated.

Security Considerations

Security considerations are those best practices that should be adopted to ensure your container instances remain secure.

Use Private Registry

A publicly accessible image of a container does not guarantee security.

The Docker Trusted Registry is a private registry, which can be installed on-premises Docker configuration or in a virtual private cloud.

You can also use cloud-based private container registry services, like Azure Container Registry.

Monitor and Scan Container Images

Security monitoring and image scanning solutions are available through the Azure Marketplace.

Reap the benefits of solutions to scan container images in a private registry and identify potential vulnerabilities.

Always scan before pushing.

Protect Credentials

Always inventory all credential secrets.

Needs developers to use emerging secrets-management tools that are designed for container platforms.

Azure Key Vault is a cloud service that allow you to store credentials and secrets.

Create a Container Instance

In this section, you will learn how to create a container instance with the Azure CLI by using Service principal ID and password to authenticate with Container registry from container instances.

Create a Service Principal

```
#1/bin/bash
ACR_NAME= mycontainerregistry
SERVICE_PRINCIPAL_NAME=acr-service-principal
ACR_REGISTRY_ID=$(az acr show --name $ACR_NAME --query id --output tsv)
SP_PASSWD=$(az ad sp create-for-rbac --name http://\$SERVICE\_PRINCIPAL\_NAME --scopes $ACR_REGISTRY_ID --role acrpull --query password --output tsv)
SP_APP_ID=$(az ad sp show --id http://\$SERVICE\_PRINCIPAL\_NAME --query appId --output tsv)
echo "Service principal ID: $SP_APP_ID"
echo "Service principal password: $SP_PASSWD"
```

Create a Container Instance

```
az container create \
--resource-group myResourceGroup \
--name mycontainer \
--image mycontainerregistry.azureacr.io/myimage:v1 \
--registry-login-server mycontainerregistry.azureacr.io \
```

```
--registry-username <service-principal-ID> \  
--registry-password <service-principal-password>  
--dns-name-label az-acr-tasks-$ACR_NAME \  
az container show --resource-group myResourceGroup --name  
mycontainer --query "{FQDN:ipAddress.fqdn}" \  
--output table
```

Content Trust

Docker's content trust model is implemented by the Azure Container Registry, which allows signed images to be pushed and pulled.

Note: Content trust is a feature of the Premium SKU of Azure Container Registry.

Content trust helps you to sign the images that you are pushing into your registry. Your image consumers (people or systems who pull images from your registry) will configure their customers to pull signed images only. When an image consumer pulls a signed image, the integrity of the image is verified by their Docker client.

Container Groups

A container group is a gathering of containers that are planned on the same host machine. The containers in a container group share a lifecycle, resources, local network, and storage volumes. In concept, it is identical to a pod at Kubernetes.

A container group is useful when building an application sidecar for logging, monitoring, or any other configuration where a service needs a second attached process.

Container groups

- Are deployed on a single VM
- Only support Linux VMs
- Can sit behind a public IP with optional exposed ports
- Can be deployed by Azure Resource Manager (ARM) template or YAML file

Container Vulnerability Management

As mentioned in the Security Considerations lesson, vulnerability management is a vital part of container security. You must scan containerized images for vulnerabilities of bad configurations crucial to maintain secure container instances.

You can get security monitoring and scanning solutions like Twistlock and Aqua Security from the Azure Marketplace. These can be used in a private registry to scan container images and find possible vulnerabilities.

Azure Kubernetes Service (AKS)

This section introduces the core concepts that secure your applications in AKS:

Security Concepts

Master Security

In AKS, the master components of Kubernetes are part of the managed service offered by Microsoft. Each AKS cluster has its own single-tenanted, dedicated Kubernetes master to provide the API Server, Scheduler, etc.

Microsoft is responsible to manage and maintain this master security.

By default, the Kubernetes API server uses a public IP address and a fully qualified domain name (FQDN). You can control access to the API server by using Kubernetes role-based access control (Kubernetes RBAC) and Azure AD.

Node Security

AKS nodes are virtual Azure machines, which are managed and maintained by you.

Using the Moby container runtime, Linux nodes run an optimized Ubuntu distribution.

Windows Server nodes run an optimized release of Windows Server 2019 and use the runtime of Moby containers as well.

The nodes are automatically deployed with the latest OS security patches and configurations when an AKS cluster is created or scaled up.

Kubernetes Secrets

A Kubernetes Secret is used to inject sensitive data into pods, such as access credentials or keys.

Best Practices

- Secure access
- Secure container access to resources

- Regularly upgrade to the latest version of Kubernetes
- Process Linux node updates and reboots using kured

Authenticating to ACR from AKS

Let's take Azure Container Registry as an example. There are couple of ways to use this; both of them can be done via Command line.

1. Grant AKS access to ACR

First one is to grant the AKS access to ACR by using the manage instances of the AKS cluster and then granting the role assignment with ACR pull right to the container registry.

```
#!/bin/bash

AKS_RESOURCE_GROUP= myAKSResourceGroup
AKS_CLUSTER_NAME= myAKSCluster
ACR_RESOURCE_GROUP= myACResourceGroup
ACR_NAME= myACRRegistry

# Get the id of the service principal configured for AKS
CLIENT_ID=$(az aks show --resource-group $AKS_RESOURCE_GROUP --name $AKS_CLUSTER_NAME --query "servicePrincipalProfile.clientId" --output tsv)

# Get the ACR registry resource id
ACR_ID=$(az acr show --name $ACR_NAME --resource-group $ACR_RESOURCE_GROUP --query "id" --output tsv)

# Create role assignment
az role assignment create --assignee $CLIENT_ID --roleacrpull --scope $ACR_ID
```

If you do not have rights with an Azure AD to perform this role or task, you can do this task. We can do so with the Kubernetes secrets

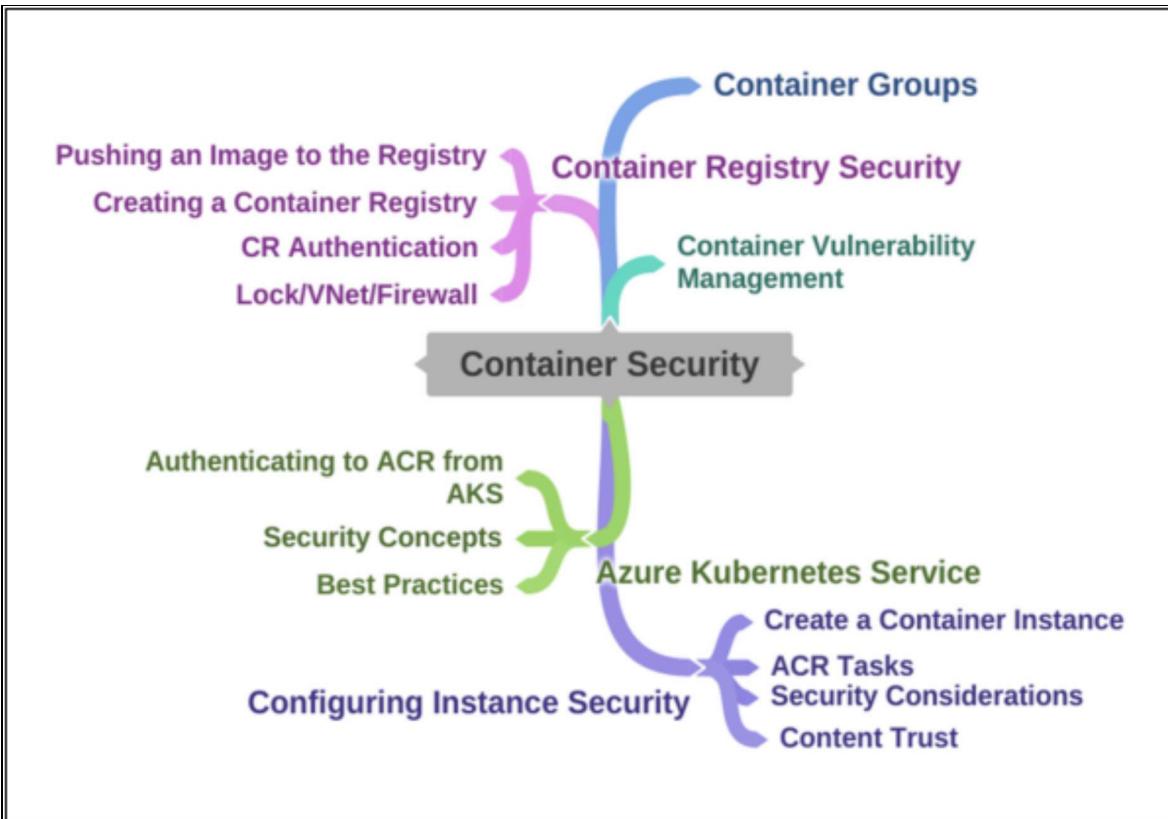
2. Access with Kubernetes Secrets

We can create a service principal and the add acr pull role rights to the registry id. We can then use the kube control command line interface to store the secret within the kubernetes service.

```
#!/bin/bash

ACR_NAME=myacrinstance
SERVICE_PRINCIPAL_NAME=acr-service-principal
# Populate the ACR login server and resource id.
ACR_LOGIN_SERVER=$(az acr show --name $ACR_NAME --query loginServer --output tsv)
ACR_REGISTRY_ID=$(az acr show --name $ACR_NAME --query id --output tsv)
# Create acrpull role assignment with a scope of the ACR resource.
SP_PASSWD=$(az ad sp create-for-rbac --name http://$SERVICE_PRINCIPAL_NAME --role acrpull --scopes $ACR_REGISTRY_ID --query password --output tsv)
# Get the service principal client id.
CLIENT_ID=$(az ad sp show --id http://$SERVICE_PRINCIPAL_NAME --query appId --output tsv)
# Output used when creating Kubernetes secret.
echo "Service principal ID: $CLIENT_ID"
echo "Service principal password: $SP_PASSWD"
```

Mind Map



Practice Questions

1. What types of resource locks are available in Azure?
 - A. CanNotDelete
 - B. ReadOnly
 - C. AllowAll
 - D. CanNotCreate

2. Which of the following is the Azure CLI command used to log in to an Azure Container Registry?
 - A. echo FROM hello-world > Dockerfile
 - B. az acr login --name <acrName>
 - C. az group create --name myResourceGroup --location eastus
 - D. -azLogin --AcrLogin

3. Which is a managed Docker registry service based on an open-source Docker Registry?
 - A. Azure DevOps
 - B. Azure Container Registry (ACR)
 - C. Azure Kubernetes Service (AKS)
 - D. Network Security Group (NSG)

4. You can create a container registry with _____.
 - A. Azure portal
 - B. Azure CLI
 - C. Azure PowerShell
 - D. All of the above

5. What are the main Azure RBAC roles available for a container registry?
 - A. AcrPull
 - B. AcrPush
 - C. Owner
 - D. All of the above

6. Which Azure RBAC roles allow you to pull and push images to the registry?
- A. AcrPull
 - B. AcrPush
 - C. Owner
 - D. All of the above
7. How many keys are provided to the admin account?
- A. One
 - B. Two
 - C. Three
 - D. Four
8. To enable VNet/Firewall secure feature of container registry, we have to change the SKUs of our container registry from basic to premium. True or false?
- A. True
 - B. False
9. Which is the fastest and easiest way to run a container in Azure?
- A. Azure Container Instance
 - B. Azure Container Registry (ACR)
 - C. Azure Kubernetes Service (AKS)
 - D. Network Security Group (NSG)
10. Which of the following provides cloud-based container image building for Linux, Windows, and ARM?
- A. Azure Kubernetes Service (AKS)
 - B. Azure Container Instance
 - C. ACR Tasks
 - D. Network Security Group (NSG)
11. Which of the following allows signed images to be pushed and pulled?
- A. Azure Key Vault

- B. Content Trust
 - C. Azure Container Instance
 - D. ACR Tasks
12. Which of the following will be used to create a container in Azure?
- A. Hostname
 - B. Fully Qualified Domain Name
 - C. Domain Name
 - D. None of the Above
13. Which of the following is the atomic unit of software that packages up a code and configuration for specific applications?
- A. Container
 - B. Virtual Machine
 - C. Virtual Network
 - D. Pod
14. Which of the following is the open-source platform that is used for working with a large number of containers?
- A. Azure Storage
 - B. Azure Kubernetes
 - C. Azure Data Lake
 - D. Azure Key Vault
15. Which security components of Kubernetes is managed and maintained by Microsoft?
- A. Master
 - B. Node
 - C. Kubernetes Secrets
 - D. All of the above

Chapter 07: Configuring Security Services

Introduction:

Securing the cloud efficiently is a formidable challenge for both developers and administrators. Microsoft Azure provides you with tools to overcome the problem and strengthen your security infrastructure. In this chapter, you will learn how to leverage Azure services such as Azure Monitor and Diagnostics logs to assess the security posture of your environment, remediate discovered issues, and monitor Azure resources on a continual basis.

Microsoft Azure Monitor

Monitoring is the process of collecting and analyzing data in order to evaluate your business application's performance, health, and availability as well as the resources it depends upon.

Azure Monitor lets you maximize your applications and services' availability and efficiency. It offers a comprehensive solution for telemetry collection, review, and intervention from your cloud and on-premises environments. This data allows you to understand how your applications perform and to proactively recognize problems that affect them and the services on which they depend.

Monitoring in Azure is mainly supported by Azure Monitor, which provides common stores to store monitoring data known as workspaces for log analytics. Multiple data sources are available to collect data from different levels that help our applications, such as networking, computing, and storage resources, and features to analyze and respond to data collected such as query and alert functionality.



EXAM TIP: Azure Monitor, Log Analytics, and Log Search are present in the AZ-300 course in more detail. It is recommended for you to go through that so you can answer all type of questions regarding them.

Log Analytics

Log Analytics is an Azure Portal tool used to edit and execute data log queries in Azure Monitor Logs. You can write a simple query that returns a set of records and then sort, filter, and analyze them using the Log Analytics features.

Diagnostic Logging and Log Retention

Diagnostic logs provide data about the procedure of Azure resources. There are two different types of diagnostic logs.

Tenant logs: Logs originating from tenant-level services such as Azure Active Directory. These logs span multiple subscriptions and multiple resources within those subscriptions. They are typically found in the Azure Active Directory portion of the Azure portal.

Resource logs: Logs originating from individual resources by themselves within an Azure subscription, such as Virtual machines, Network security groups, or Storage accounts.

These do not include the Azure Activity Log or any OS-level logging.

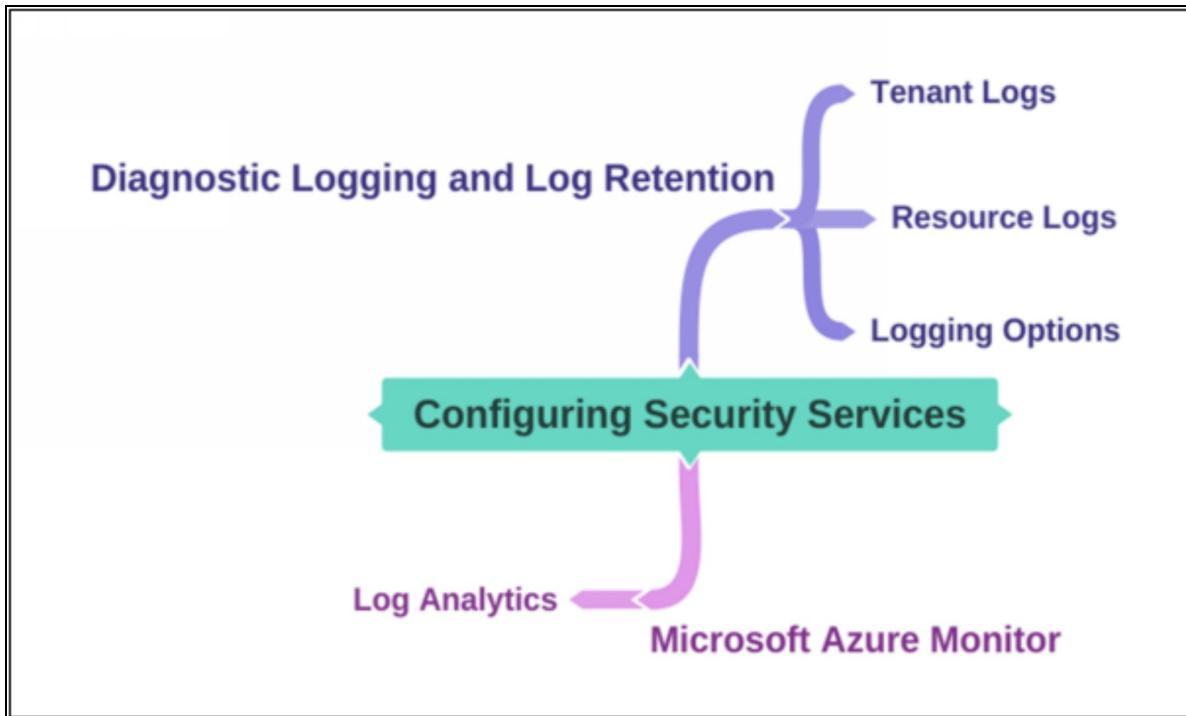
Logging Options

We can export these logs to different Azure services so that we can do other things with them.

We have a few options available for working with diagnostic logs:

- Save them to your Storage account for auditing or manual inspection of your Diagnostic logs.
- Stream them to event hubs for ingestion by a custom analytics solution such as Power BI that can determine security trends or anomaly existing in the environment.
- Analyze them with Azure Monitor. It would be the perfect solution because Azure monitor is a centralized logging and monitoring stations.

Mind Map



Practice Questions

1. Which Azure solution collects, analyzes, and acts on telemetry from our cloud and on-premises environments?
 - A. Azure Media Services
 - B. Azure Boot Diagnostics
 - C. Azure Application Insights
 - D. Azure Monitor
2. Which one of the following is the process of collecting and analyzing data in order to evaluate our business application's performance, health, and availability and the resources it depends upon?
 - A. Monitoring
 - B. Log diagnostics
 - C. Application Insights
 - D. None of the above
3. How many types of diagnostic logs are there?
 - A. One
 - B. Two
 - C. Three
 - D. Five
4. Which type of logs originate from services such as Azure Active Directory?
 - A. Diagnostics logs
 - B. Tenant logs
 - C. Resource logs
 - D. All of the above
5. Which type of logs originate within an Azure subscription, such as Virtual machines, Network security groups, or Storage

- accounts?
- A. Diagnostics logs
 - B. Tenant logs
 - C. Resource logs
 - D. All of the above
6. From the few options available for working with diagnostic logs, which would be the best one?
- A. Save them to your Storage account for auditing or manual inspection.
 - B. Stream them to event hubs for ingestion by a custom analytics.
 - C. Analyze them with Azure Monitor.
 - D. All of the above
7. What can we configure to ensure that we are notified when an alert occurs in Azure Monitor?
- A. Logic Apps
 - B. Application Insights
 - C. Action Group
 - D. Azure Playbooks

Chapter 08: Security Policies and Alerts

Introduction

In this chapter, we will discuss Just In Time VM Access that allows you to lock down the administrative ports of your VM such as remote desktop and requires your system administrator to request access to these remote ports. This feature reduces your attack servers by not allowing full time access to these administrative ports.

Configuring Azure Policies: Just In Time VM Access Using Azure Security Center

Just In Time (JIT) Virtual Machine Access lets you lock down access to your Azure virtual machines, allowing access only when required by the support personnel or other users.

Azure Security Center standard is required to configure this feature.

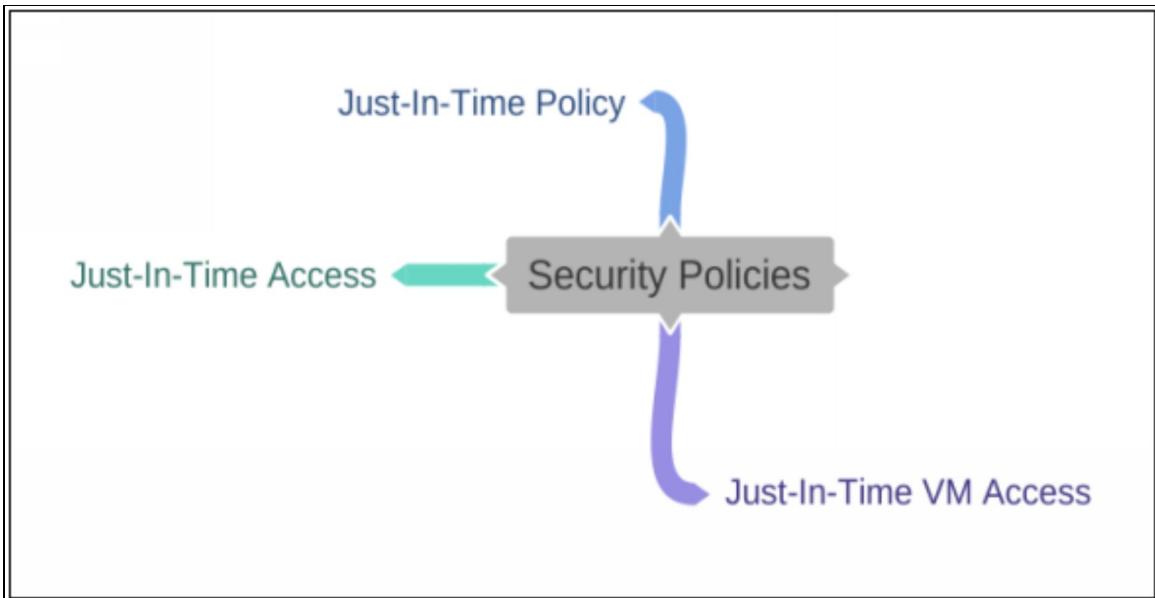
Security Center JIT VM access currently supports only VMs deployed through Azure Resource Manager.

To enable a user to create or edit a JIT Policy for a VM, assign these actions to the role:

- On the scope of a subscription or resource group that is associated with the VM: Microsoft.Security/locations/jitNetworkAccessPolicies/write
- On the scope of a subscription or resource group of VM: Microsoft.Compute/virtualMachines/write (subscription, resource group, or VM)

To enable a user to request JIT access to a VM, assign these actions to the user:

- On the scope of a subscription or resource group that is associated with the VM: Microsoft.Security/locations/{the_location_of_the_VM}/jitNetworkAccessPolicies/initiate/action
- On the scope of a subscription or resource group or VM: Microsoft.Compute/virtualMachines/read



Reviewing and Responding to Alerts and Recommendations

Security Alerts

Based on data collected by Azure Security Center, threats are detected. For each threat, an alert is generated.

A list of alerts is shown in the Security Center along with the information we need to quickly investigate the problem as well as recommendations for how to remediate an attack.

Recommendations

Recommendations are actions in order to take to secure resources. The recommendations are based on best practices and trusted security advisories.

Each recommendation provides the following:

- A description
- Remediation steps
- Affected resources
- Secure score impact

To view Security Alerts, click on “Security Center” and then on “Security Alerts”. Here, you will see a list of all the alerts that have been generated.

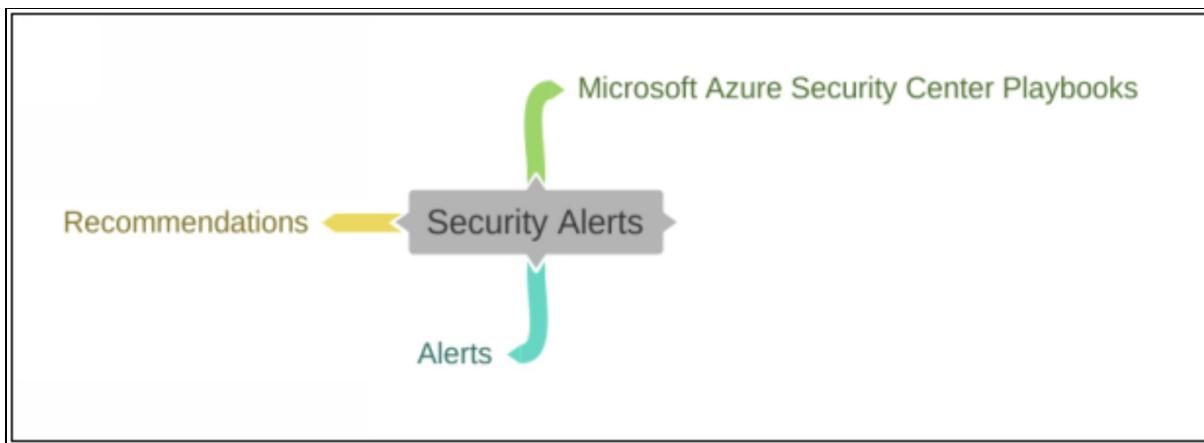
The screenshot shows the Azure Security Center interface. At the top left, there's a breadcrumb navigation: Home > Security Center. The main title is "Security Center | Security alerts". Below the title, there's a search bar labeled "Search (Ctrl+I)" and several action buttons: "Filter", "Download CSV report", "Suspension rules", and "Security alerts map (Preview)". On the left, there's a sidebar with a tree view of categories: General (Overview, Getting started), Recommendations (Security alerts, Inventory, Community), and Cloud Security (Secure Score, Regulatory compliance, Azure Defender). The "Security alerts" item is highlighted with a yellow arrow. The main content area has a heading "What is Advanced Threat Detection?" followed by a description: "A list of prioritized security alerts along with the information you need to quickly investigate the problem and remediate an attack." Below that is another section heading "How does it work?" with a detailed description: "Our threat detection engine processes a vast amount of data about cloud network activity and uses advanced machine learning algorithms, behavior and anomaly analysis to detect threats targeting your Azure deployments." At the bottom of this section, there's a link "For more information go to documentation >".

Microsoft Azure Security Center Playbooks

A security playbook is simply a collection of procedures that are executed when a playbook is triggered. Security alerts are the triggers that start playbook running.

Playbooks can help you craft and execute automated responses to security alerts, helping us manage our Azure environment with little administrative effort.

Security playbooks in the Security Center are based on Azure Logic Apps.



Practice Questions

1. Which of the following allows to lock down access to Azure VM?

- a. Just-In-Time Policy
- b. Just-In-Time Access
- c. Just-In-Time VM Access
- d. None of the above

Answer

Just-In-Time VM Access (b)

Explanation

Just In Time (JIT) Virtual Machine Access allows you to lock down access to your Azure virtual machines.

2. Which of the following is required to access JIT feature?

- a. Access Center
- b. Security Center
- c. Both of them
- d. None of them

Answer

Security Center (b)

Explanation

Azure Security Center standard is required to configure this JIT feature.

3. Security Center JIT VM access currently supports only VMs deployed through _____.

- a. Resource Manager
- b. Security Center
- c. Azure VM
- d. None of them

Answer

Resource Manager (b)

Explanation

Security Center JIT VM access currently supports only VMs deployed through Azure Resource Manager.

4. Which of the following notifies you of potential anomalies in Azure environment?

- a. Alerts
- b. Recommendations
- c. Both of them
- d. None of them

Answer

Alerts (a)

Explanation

Alerts notify you of potential anomalies in Azure environment.

5. Which of the following is based on best practices and trusted security advisories?

- a. Alerts
- b. Recommendations
- c. None of them
- d. Both of them

Answer

Recommendations (b)

Explanation

The recommendations are based on best practices and trusted security advisories.

6. Which of the following can help you craft and execute automated responses to security alerts?

- a. Playbooks
- b. Security Center
- c. Tools
- d. None of the above

Answer

Playbooks (a)

Explanation

Playbooks can help you craft and execute automated responses to security alerts.

Chapter 09: Data Management & Security for Data Infrastructure

Data Classification Using Azure Information Protection

What is AIP?

Azure Information Protection (AIP) is a cloud-based rights management solution that helps your organization classify and protect documents and email.

Classification is achieved by applying labels. Labels determine the confidentiality of the data based on conditions that can be set by administrators or optionally by end users. AIP can also recommend certain labels be applied to documents and emails based on the type of data created.

Azure Active Directory Premium P1 or P2 licenses are required to use AIP.

Permissions

AIP includes several built-in permission sets for access to labeled data. These roles can be applied to members of our Azure Active Directory as well as external recipients (specified by internet domain name).

- Co-Owner
- Co-Author
- Reviewer
- Viewer
- Custom

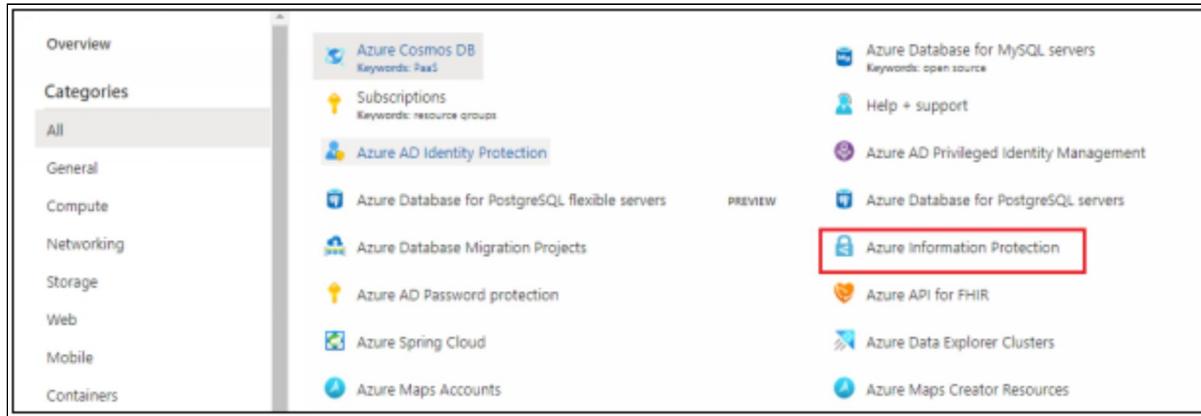
Labelling

In AIP, labels determine the classification of a piece of data. Data labelled ‘General’ is not protected and can be distributed inside and outside of an organization, whereas data labelled ‘Confidential’ cannot. Labels can be applied manually to a piece of data or can be applied automatically based on conditions, such as the data format.

AIP contains 100 preconfigured conditions, or we can create our own based upon a regular expression.

Applying conditions to a label requires Azure Active Directory P2 licensing.

To configure AIP, click on “All resources” and then on “Azure Information Protection”.



Storage Analytics Data Retention Policies

We can configure the retention settings on Azure Storage Accounts. If you wish to retain your storage analytics logging data, then there are few points you should take note of:

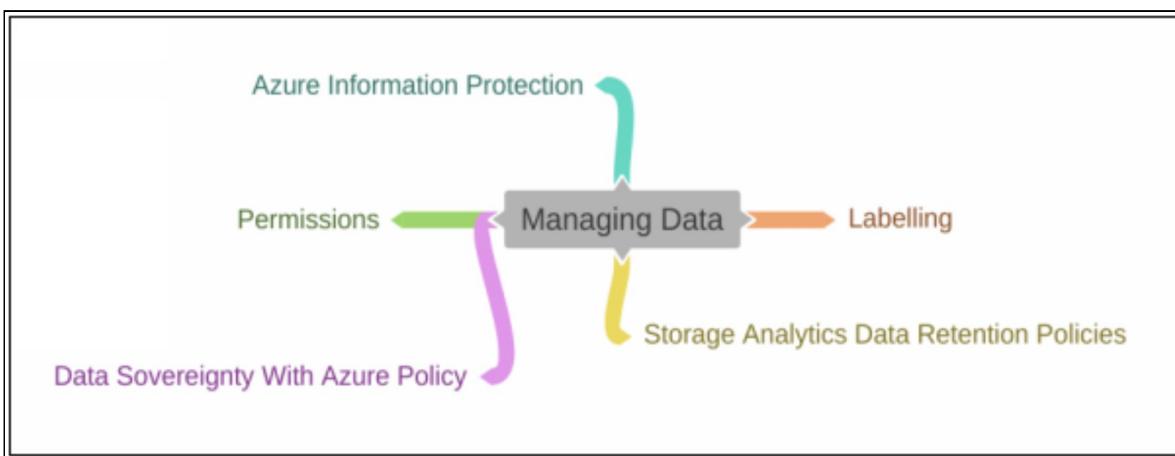
- By default, Storage Analytics will not delete any logging or metrics data.
- Blobs and data entries will continue to be written until the shared 20TB limit is reached.
- Once the 20TB limit is reached, Storage Analytics will stop writing new data and will not resume until free space is available.

To better manage this data, you can create a retention policy. Retention policies can be created via the REST API or in the Azure Portal.

Data Sovereignty with Azure Policy

Sometimes, due to governmental or other regulations, it is necessary to ensure the organizational data resides in a particular country of origin. In Azure, you are able to create Azure resources in regions located all over the world. To enforce data sovereignty, we can use Azure Policy to enforce where Azure resources and the data contained therein are located.

Azure Policy contains many preconfigured policies to assist you with your compliance goals. One of these determines allowed locations where Azure resources can be deployed.



Azure Key Vault

Azure Key Vault helps safeguard and manage keys for cryptography and secrets used by Azure applications and services.

With Azure Key Vault, you can perform the following tasks:

- Securely store and tightly control access to tokens, passwords, certificates, API Keys, and other secrets.
- Create and control the encryption keys used to encrypt data.
- Provision, manage, and deploy public and private Secure Socket Layer/Transport Layer Security (SSL/TLS) certificates for use with internal connected resources.
- Azure Resource Manager templates can access secrets and keys stored in key vault during deployment of other Azure resources.

Managing Access to Key Vault, Secrets, Certificates, and Keys

Because Azure Key Vault data is sensitive and business critical, you need to secure access to your key vaults by allowing only authorized applications and users.

Access to Azure Key Vault is controlled by an access policy. Access policies determine what privileges are granted for keys, secrets, and certificates stored in Key Vault.

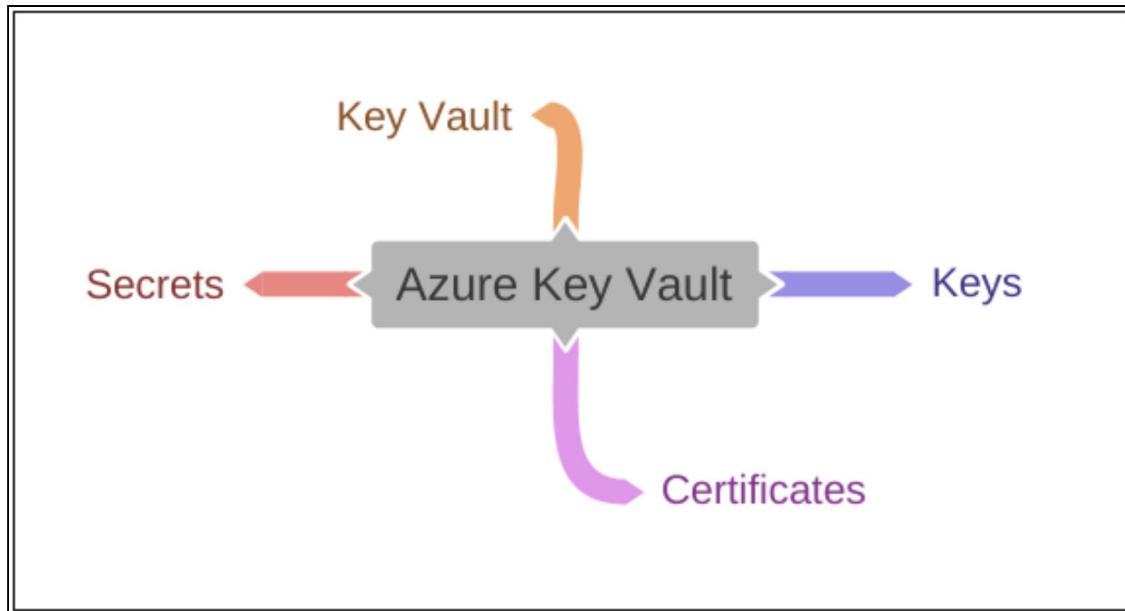
RBAC is also used to determine access to the Key Vault resource.

You can create an Azure Key Vault by clicking “Key Vault” and then on “Create Key Vault”. Click on “Review+Create” to create your new Azure Key Vault.

The screenshot shows the 'Create key vault' wizard in the Azure portal. The top navigation bar includes 'All services > Key vaults >' and the page title 'Create key vault'. Below the title is a navigation bar with tabs: Basics (underlined), Access policy, Networking, Tags, and Review + create. The 'Basics' tab is active. A descriptive text block explains that Azure Key Vault is a cloud service used to manage keys, secrets, and certificates. It highlights features like centralizing application secrets, secure storage of secrets and keys backed by Hardware Security Modules (HSMs), and audit logs for compliance. The 'Project details' section asks for a subscription and a resource group. A 'Subscription *' dropdown is set to 'Pay-As-You-Go'. A 'Resource group *' dropdown has an empty field and a 'Create new' link. The 'Instance details' section is partially visible at the bottom. At the bottom of the screen are three buttons: 'Review + create' (highlighted in blue), '< Previous', and 'Next : Access policy >'.

Managing Certificates and Secrets

You can use the Azure Portal, PowerShell, and the CLI to set and retrieve both secrets and certificates from Azure Key Vault.



Lab 9-01: Azure Key Vault

Azure Key Vault is a tool that allows IT personnel to securely store and access items such as API keys, passwords, access keys to Azure storage accounts, certificates, and more. Application developers can also reference the Key Vault in their code to access these secrets, as opposed to hard-coding them into their applications.

Log in to the Azure portal using the provided credentials.

Once you are logged in to the portal, make a note of the unique five-character code at the end of your lab-provisioned resources (e.g., upcbt). You may want to copy this into a text file, as you will be using it throughout the lab.

Also, note the region your storage account is located in as you will have to use this value when creating resources in the lab.

Set up Azure Key Vault

1. In the lab resource group pane, click “Add”.
2. Search for and click on “Key Vault”.
3. Click “Create”.
4. Set the following values:
 - a. Subscription: Leave as-is
 - b. Resource group: Leave as-is
 - c. Key vault name: kv-XXXXX, where XXXXX represents the five-character code you noted earlier
 - d. Region: Same as your lab-provided resources
 - e. Pricing tier: Standard
5. Click “Next: Access policy”.
6. Under Enable Access to, select Azure Resource Manager for template deployment.
7. Click “Next: Networking”. Leave it as the default.
8. Click “Review + create”.
9. Click “Create”.
10. Click “Go to resource” when it appears.

Create a Secret in the Key Vault for the VM Password

1. Click “Secrets” in the left-hand menu.

2. Click “Generate/Import”.
3. Configure the secret with the following settings:
 - a. Upload options: Manual
 - b. Name: VMKey
 - c. Value: Something memorable and unique (e.g., P@sswOrd). Make sure you note this password as you will be using it later.
 - d. Content type: password
4. Click “Create”.
5. Click “Properties” in the left-hand menu.
6. Click the copy icon next to the Resource ID.
7. Paste this value in a text file.

Create and Download a Virtual Machine ARM Template

1. Click “Home” at the top.
2. Click “Virtual Machines”.
3. Click “Add > Virtual machine”.
4. On the Basics page:
 - a. Subscription: Leave as-is
 - b. Resource group: Select the one in the dropdown
 - c. Virtual machine name: vm-XXXXX, where XXXXX represents the five-character code you noted earlier
 - d. Region: Same as your lab-provided resources
 - e. Availability options: No infrastructure redundancy required
 - f. Image: CentOS-based 8.2 (or the most recent version of it)
 - g. Size: Standard_B1s (or the least expensive option available)
 - h. Authentication type: Password
 - i. Username: azureid
 - j. Password: Enter a unique password
 - k. Confirm password: Repeat the password
 - l. Inbound port rules: Leave as-is
5. Click “Next: Disks”, and set the following values:
 - a. OS disk type: Standard HDD
 - b. Leave everything else as-is.
6. Click “Next: Networking”, and set the following values:

- a. Virtual network: Select the lab-provided VNet
 - b. Subnet: default (10.0.0.0/24)
 - c. Public IP: Select the lab-provisioned pip-XXXXX option in the dropdown
 - d. Leave all other settings as their defaults.
7. Click “Next: Management”, and set the following values:
 - a. Boot diagnostics: Disable
 - b. Leave all other settings as their defaults.
 8. Click “Review + create”.
 9. Do not click to create the VM.

Click the link to Download a template for automation.

Database Authentication and Auditing

SQL Database Authentication with Azure AD

By default, Azure SQL databases, managed instances, and data warehouses use local user accounts for authentication. When one of the above mentioned resources is initially deployed, a SQL server account is created for administration.

Azure Active Directory can be configured to simplify authentication to any of these resources. Benefits of Azure AD authentication are:

- Single user account for DB authentication
- Password strength based on Azure AD policies
- Support for ADFS authentication
- Support for MFA
- Use of SQL management tools with Azure AD authentication

In order to integrate with Azure AD, an Azure AD administrator must be assigned to the SQL database, managed instance, or data warehouse. This can be either a user or group object. The user or group can assign other Azure AD users and groups to SQL resources.

SQL Database Auditing

Auditing SQL databases and data warehouses helps you maintain compliance and gain insight into the activity in these critical Azure resources.

We can use SQL auditing to retain auditing data of events pertaining to the SQL, create reports on database activity, and analyze these reports with Azure Monitor to discover unusual events and activities.

SQL audit logs can be configured for the SQL server as a whole or at the individual database level. If you define server-level auditing, database-level auditing will be enabled as well. If you audit both server-level and database-level components, then some audit data will be captured twice. Be careful when doing this, as you could deplete the space allocated for auditing data in your Azure storage account.

Auditing logs can be sent to Azure storage accounts, Log analytics (to be used by Azure Monitor), or Event Hub (to be ingested by a third-party solution or Power BI).

Logging can be configured using the Azure Portal, PowerShell, the REST API, or ARM templates.

- | |
|--------------------------------|
| 1. First, create SQL Database. |
| |

All services > SQL databases >

Create SQL Database

Microsoft

Basics Networking Additional settings Tags Review + create

Create a SQL database with your preferred configurations. Complete the Basics tab then go to Review + Create to provision with smart defaults, or visit each tab to customize. [Learn more](#)

Project details

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

Subscription * ⓘ Pay-As-You-Go

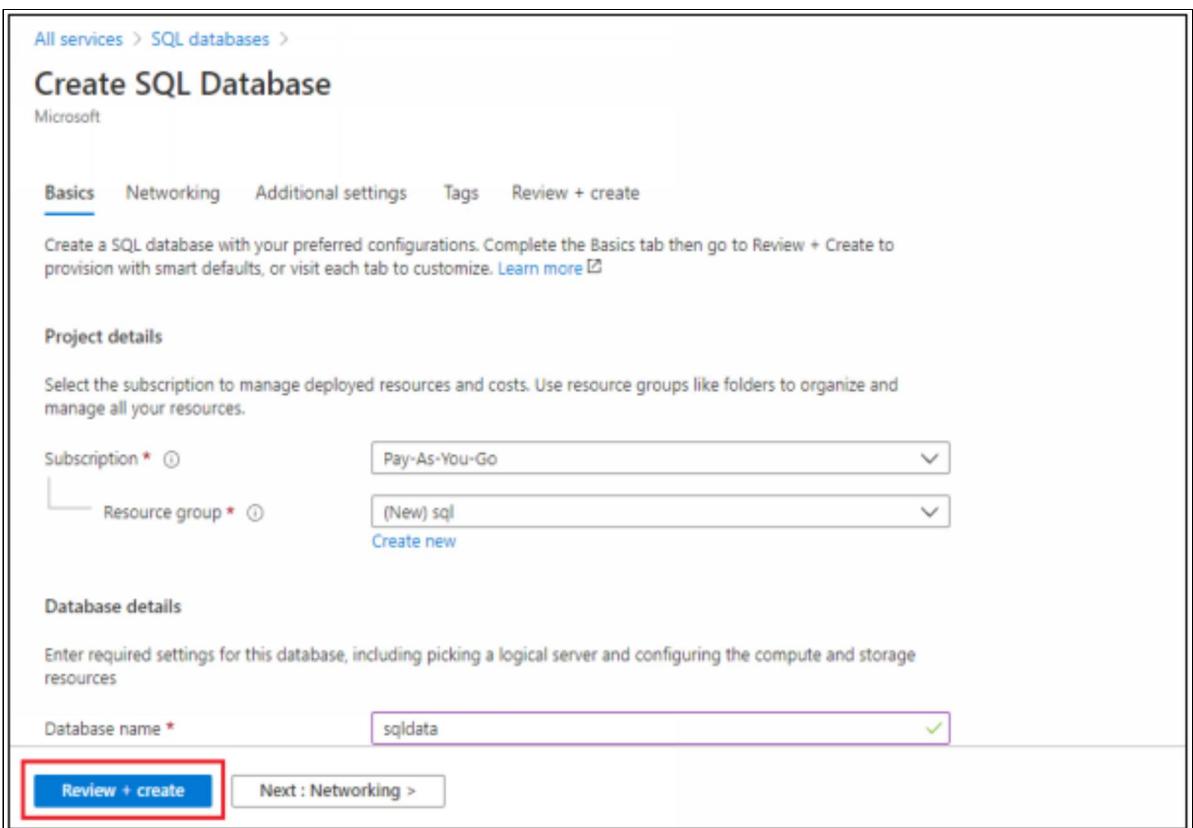
Resource group * ⓘ (New) sql [Create new](#)

Database details

Enter required settings for this database, including picking a logical server and configuring the compute and storage resources

Database name * sqldata

Review + create [Next : Networking >](#)



2. Now, click on server name.

Home > SQL databases >

sqluse/sqldata (sqluse/sqldata)

SQL database

Search (Ctrl+F)

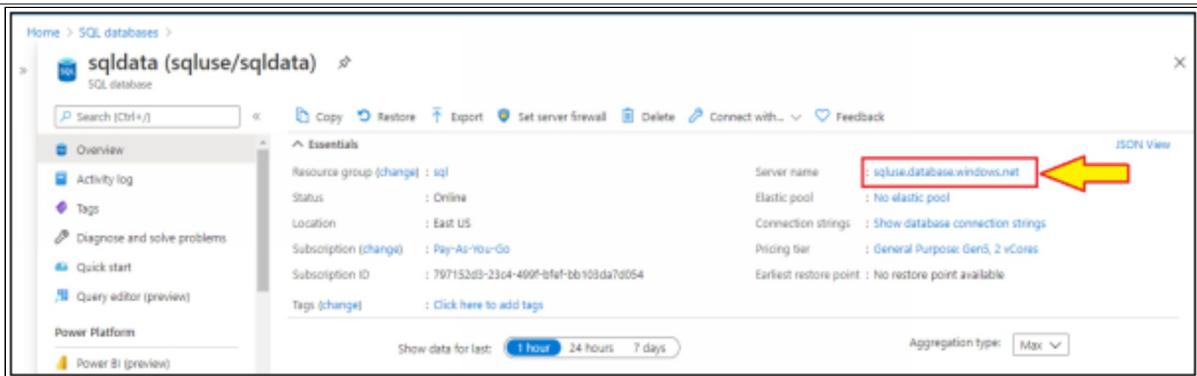
Copy Restore Export Set server firewall Delete Connect with... Feedback

Overview Activity log Tags Diagnose and solve problems Quick start Query editor (preview) Power Platform Power BI (preview)

Essentials

Resource group (change) : sql	Server name : sqluse.database.windows.net
Status : Online	Elastic pool : No elastic pool
Location : East US	Connection strings : Show database connection strings
Subscription (change) : Pay-As-You-Go	Pricing tier : General Purpose Gen3, 2 vCores
Subscription ID : 797152d5-23c4-469f-bfef-bb103da7d054	Earliest restore point : No restore point available
Tags (change) : Click here to add tags	Show data for last: 1 hour 24 hours 7 days Aggregation type: Max

JSON View



3. Click on “Active Directory Admin”.

The screenshot shows the Azure portal interface for managing a SQL database named 'sqluse'. On the left, there's a navigation sidebar with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Quick start, Failover groups, Manage Backups), and SQL databases. The main panel displays 'Essentials' information such as Resource group (sql), Status (Available), Location (East US), Subscription (Pay-As-You-Go), Subscription ID (797152d3-23d4-499f-bfe6-bb103da7d054), and Tags (Click here to add tags). Below this is a 'Notifications (1)' section with 'Info (1)' and 'Recommendations (0)'. A prominent yellow arrow points to the 'Active Directory admin' button, which is highlighted with a red box.

4. Set admin rules by clicking on “Set admin”.

This screenshot shows a modal dialog titled 'Set admin'. It includes three buttons: 'Set admin' (highlighted with a red box), 'Remove admin', and 'Save'. Below the buttons is a section with a green and blue icon representing users, followed by the text: 'Azure Active Directory authentication allows you to centrally manage identity and access to your Azure SQL Database V12.' There is also a 'Learn more' link. At the bottom of the dialog, there are two status indicators: 'Active Directory admin ⓘ' and 'No Active Directory admin ⓘ'.

5. Click on “Auditing” to enable Azure SQL Auditing and click on “Save”.

sqluse | Auditing

SQL server

Save Discard Feedback

Azure SQL Auditing

Azure SQL Auditing tracks database events and writes them to an audit log in your Azure storage account, Log Analytics workspace or Event Hub. [Learn more about Azure SQL Auditing](#)

Enable Azure SQL Auditing

Audit log destination (choose at least one):

Storage
 Log Analytics (Preview)
 Event Hub (Preview)

Auditing of Microsoft support operations (Preview)

Auditing of Microsoft support operations tracks Microsoft support engineers' (DevOps) operations on your server and writes them to an audit log in your Log Analytics workspace or Event Hub. [Learn more about Auditing of Microsoft support operations](#)

Enable Auditing of Microsoft support operations (Preview)

Search (Ctrl+ /)

Properties
Locks
Security
Auditing 
Firewalls and virtual networks
Private endpoint connections
Security Center
Transparent data encryption
Intelligent Performance
Automatic tuning
Recommendations
Monitoring
Logs

Azure SQL Database Threat Protection

Advanced Threat Protection is a part of Advanced Data Security in SQL databases that can help protect your Azure SQL infrastructure by detecting and alerting on activities including unusual and potentially harmful attempts to access or exploit databases.

Advanced Threat Protection can identify potential SQL injections, access from an unusual location or data center, access from an unfamiliar principal or potentially harmful applications, and brute force SQL credentials.

Notifications or alerts can be viewed in the Azure Portal or emailed.

Advanced data security is a premium service that entails additional cost.

Managing Access Control and Keys for Storage Accounts

Azure storage accounts are the repositories for data accessed by users, applications, and other Azure services. Locking down these storage accounts is a critical component of Azure security.

You can use several different methods for securing storage accounts. You can utilize access keys, which grant the user full control to the entire storage account.

You can also use Shared Access Signatures (SAS), which grant fine-grained access to storage account services. For example, you can apply a SAS to grant read-only access to a blob container within a storage account.

Security for HDInsight

Enterprise Security Package (ESP) clusters provide multi-user access on Azure HDInsight clusters. HDInsight clusters with ESP are connected to a domain so domain users can use their domain credentials to authenticate the clusters and run big data jobs.

In order to create an HDInsight cluster with ESP, Azure Active Directory Domain Services (Azure AD DS) must be deployed in your Azure tenant.

Once enabled, a managed identity for the HDInsight cluster must be created and assigned the HDInsight Domain Services Contributor role in the AD DS instance.

Once these prerequisites are complete, the HDInsight cluster with ESP can be deployed in Azure.

Security for Cosmos DB

Azure Cosmos DB uses two types of keys to authenticate users and provide access to its data and resources:

- Master Keys: It is used for administrative resources such as database accounts, databases, users, and permissions.
- Resource Tokens: It is used for application resources such as containers, documents, attachments, stored procedures, triggers, and UDFs.

Each account consists of two master keys: a primary key and a secondary key. The purpose of dual keys is so that keys can be regenerated or rolled, providing continuous access to your account and data.

You can use a resource token (by creating Cosmos DB users and permissions) when required to provide access to resources in your Cosmos DB account to a client that cannot be trusted with a master key.

1. First, create an Azure Cosmos DB account by clicking on “Review+create”.

Home > Azure Cosmos DB >

Create Azure Cosmos DB Account

For a limited time, create a new Azure Cosmos DB account with multi-region writes in any region, and receive up to 33% off for the life of your account.

Basics Networking Backup Policy Encryption Tags Review + create

Azure Cosmos DB is a globally distributed, multi-model, fully managed database service. Try it for free, for 30 days with unlimited renewals. [Learn more](#)

Project Details

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

Subscription * Pay-As-You-Go

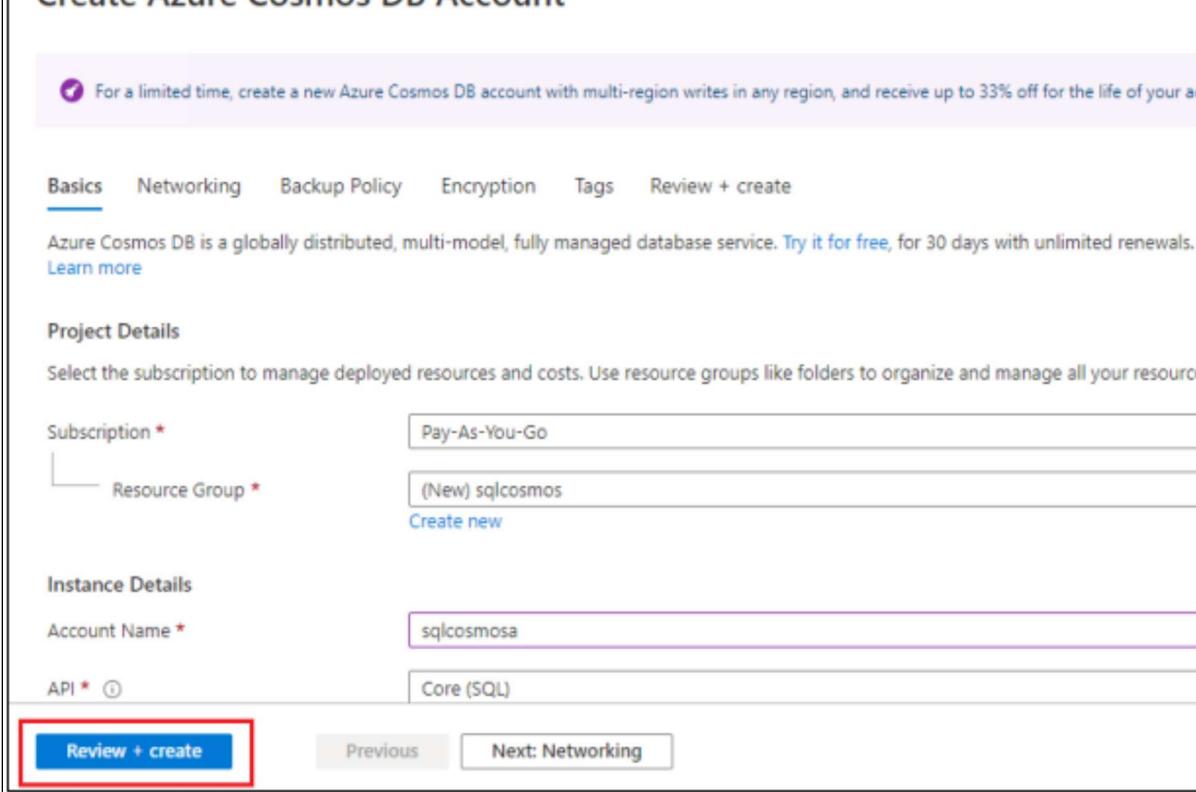
Resource Group * (New) sqcosmos
Create new

Instance Details

Account Name * sqcosmosa

API * Core (SQL)

Review + create Previous Next: Networking



2. Now, click on “Keys” to view all the generated keys.

sqlcosmosa | Keys

Azure Cosmos DB account

Search (Ctrl+I)

Features

Replicate data globally

Default consistency

Backup & Restore

Firewall and virtual networks

Private Endpoint Connections

CORS

Keys

Add Azure Cognitive Search

Add Azure Function

Advanced security (preview)

Locks

Read-write Keys Read-only Keys

(R) https://sqcosmosa.documents.azure.com:443/

PRIMARY KEY YwECHCAi...4rKClci...brsQeKQMcZ8g==

SECONDARY KEY BH1wE7KA...qY7qSeM4MB...md90/Onic...P0E...k...R...T...M...o...2...y...3...P...H...T...8...v...d...4...e...8...0...9...C...W...z...g...I...O...N...b...y...T...A...9...Q...=

PRIMARY CONNECTION STRING AccountEndpoint=https://sqcosmosa.documents.azure.com:443/AccountKey=YwECHCAi...4rKClci...brsQeKQMcZ8g==

SECONDARY CONNECTION STRING AccountEndpoint=https://sqcosmosa.documents.azure.com:443/AccountKey=BH1wE7KA...qY7qSeM4MB...md90/Onic...P0E...k...R...T...M...o...2...y...3...P...H...T...8...v...d...4...e...8...0...9...C...W...z...g...I...O...N...b...y...T...A...9...Q...=



Security for Microsoft Azure Data Lake

Securing data in Azure Data Lake Storage uses a combination of Azure AD role-based permissions and access control lists within the Data Lake file system.

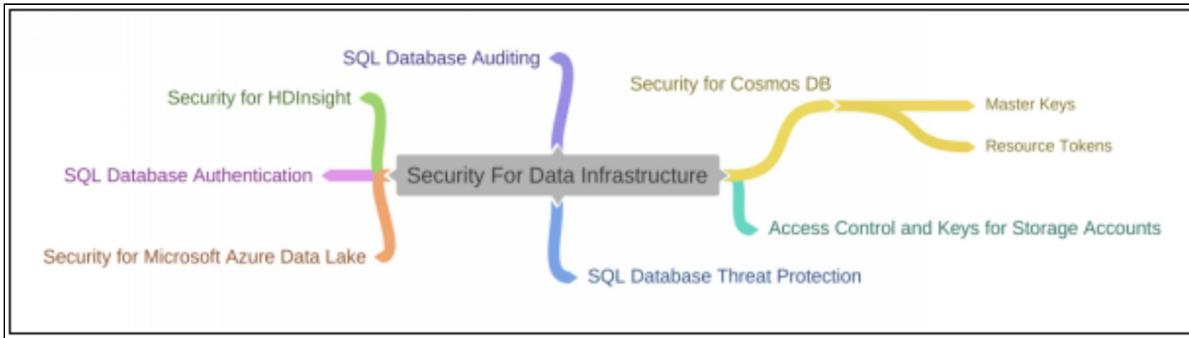
- AAD security principals control access to the Data Lake Storage GEN1 account from the portal and management operations from the portal or through APIs.
- These principals also regulate access control on the data stored in Data Lake Storage GEN1.
- You can lock down access to the Data Lake at the network level by using a resource firewall.

You can create your Data Lake Storage GEN1 account by clicking on “Review+create”.

The screenshot shows the 'New Data Lake Storage Gen1' creation page. At the top, there's a breadcrumb navigation: Home > Data Lake Storage Gen1 >. Below it is the title 'New Data Lake Storage Gen1'. A purple banner at the top right informs users that 'Azure Data Lake Storage Gen2 is now GA. Click here to read more about how you can migrate to Azure Data Lake Storage Gen2.' The main form is divided into sections: 'Project details' and 'Instance details'. In 'Project details', fields include 'Subscription *' (Pay-As-You-Go), 'Resource group *' (sqlcosmos, with a 'Create new' link), and 'Location *' (East US 2). In 'Instance details', the 'Name *' field is filled with 'azcosmos', which is highlighted with a blue border and a checkmark icon, indicating it's a valid name. Below the name is the generated URL: 'azcosmos.azuredatalakestore.net'. At the bottom of the form are three buttons: 'Review + create' (highlighted with a red box), 'Previous', and 'Next: Pricing >'.

Now, click on “Access Control (IAM)” to view access, roles, and role assignments of the account.

The screenshot shows the "azcosmos | Access control (IAM)" blade in the Azure portal. The left sidebar includes options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Events, Settings (Encryption, Firewall and virtual networks, Pricing tier, Properties, Locks), Data Lake Storage Gen1, and Quick start. The main area has tabs for Check access, Role assignments, Roles, Deny assignments, and Classic administrators. Under "Check access", there's a "My access" section with a "View my access" button, and a "Check access" section for users, groups, or service principals. To the right, there are sections for "Grant access to this resource" (with "Add role assignments" and "Learn more" buttons), "View access to this resource" (with "View" and "Learn more" buttons), and a "Classic administrators" section.



Practice Questions

1. Which of the following is a cloud-based rights management solution that helps your organization classify and protect documents and emails?
 - a. AIP
 - b. Permissions
 - c. Labelling
 - d. All of them

Answer

AIP (a)

Explanation

AIP is a cloud-based rights management solution that helps your organization classify and protect documents and emails.

2. Classification is achieved by applying _____,
 - a. Labels
 - b. Permissions
 - c. Both of them
 - d. None of them

Answer

Labels (a)

Explanation

Classification is achieved by applying Labels.

3. Azure Active Directory Premium P1 or P2 licenses are required to use _____.
 - a. Playbooks
 - b. AIP
 - c. Labels
 - d. All of the above

Answer

AIP (a)

Explanation

Azure Active Directory Premium P1 or P2 licenses are required to use AIP.

4. Which data label can be distributed inside and outside of an organization?

- a. Confidential
- b. General
- c. Both of them
- d. None of them

Answer

General (b)

Explanation

Data labelled ‘General’ is not protected and can be distributed inside and outside of an organization.

5. Labels can be applied _____.

- a. Manually
- b. Automatically
- c. Both of them
- d. None of them

Answer

Both of them (c)

Explanation

Labels can be applied manually to a piece of data or can be applied automatically based on conditions, such as the data format.

6. Which of the following helps safeguard and manage keys for cryptography and secrets?

- a. Azure Key Vault
- b. Labelling

- c. Resource Manager
- d. None of them

Answer

Azure Key Vault (a)

Explanation

Azure Key Vault helps safeguard and manage keys for cryptography and secrets.

7. Access to Azure Key Vault is controlled by an _____.

- a. Access Center
- b. Access Policy
- c. Access Manager
- d. All of the above

Answer

Access Policy (b)

Explanation

Access to Azure Key Vault is controlled by an access policy.

8. Which of the following can also be used to determine access to the Key Vault resource?

- a. Keys
- b. Securities
- c. Certificates
- d. RBAC

Answer

RBAC (d)

Explanation

RBAC is also used to determine access to the Key Vault resource.

9. Which of the following uses local user accounts for authentication?

- a. Azure SQL Databases

- b. Managed Instances
- c. Data Warehouses
- d. All of the above

Answer

All of the above (d)

Explanation

Azure SQL databases, managed instances, and data warehouses use local user accounts for authentication.

10. Logging can be configured using _____.
- a. Azure Portal
 - b. PowerShell
 - c. REST API
 - d. All of the above

Answer

All of the above (d)

Explanation

Logging can be configured using the Azure Portal, PowerShell, the REST API, or ARM templates.

11. Azure Cosmos DB uses how many types of keys?
- a. One
 - b. Two
 - c. Three
 - d. Four

Answer

Two (b)

Explanation

Azure Cosmos DB uses two types of keys to authenticate users and provide access to its data and resources.

Chapter 10: Security for Application Delivery

Introduction

Security for Application Delivery is the final subsection of the AZ-500 Microsoft Azure Security Technologies (LA) course. Security is one of the most important aspects of any application, and it is not an easy thing to manage. Fortunately, Azure offers a number of services that allow you to protect your cloud application. In this lesson, we are going to discuss practises that you can introduce to make your application more secure for the delivery.

Implementing Security Validations for Application Development

Implementing security validations for application development is an impressive way of saying how to secure your Platform-as-a-Service (PaaS) applications. We know that application development is typically done in the Platform-as-a-Service model using Azure web services. Application development using PaaS resources enables easier deployment of web and mobile applications. As the end user, we are no longer responsible for managing objects such as physical infrastructure and networking.

This does not mean that security is no longer of importance when developing and deploying PaaS based applications. Precautions must be taken when securing these applications, which by design are more vulnerable than on-premises applications.

Best Practices

Some best practices for securing PaaS applications are:

Adopting a policy of identity as the primary security perimeter: Azure Active Directory, a robust cloud solution for identity and access management, helps secure access to data in on-premises and cloud applications and simplifies user and group management. It integrates core directory services, advanced identity management, authentication, and access management for applications, making it easier for developers to create identity management based on policy into their applications.

Securing your keys and credentials to secure your PaaS deployment: Azure Key Vault protects keys and secrets by encrypting authentication keys, storage account keys, data encryption keys, certificates, and access credentials.

Managing your PaaS resources directly whenever possible: Protect your VM management interfaces on hybrid PaaS and IaaS services by using a management interface that enables you to remote manage these VMs directly. VM access can be done by remote management protocols such as SSH, RDP, and PowerShell remoting.

Using strong authentication and authorization: Azure AD conditional access allows us to implement additional security measures based on

your location and sign-in risk. It might require users to implement something like Multi-factor authentication to access resources.

Using a Web Application Firewall: Web Application Firewall is a great way to frontend web app resources in Azure and protect against vulnerability.

Monitoring app performance: Use Azure Application Insights to monitor availability, performance, and usage of our application, whether it is hosted in the cloud or on-premises.

Performing penetration testing whenever possible: Make penetration testing a standard part of the design and deployment process. Microsoft Security Risk Detection is a cloud-based tool that we can use to look for bugs and other security vulnerabilities in the software before deploying it to Azure.

Synthetic Security Transactions

Azure Application Insights is an extensible Application Performance Management (APM) service for web developers on multiple platforms. Application insights can be used to monitor App Service by running recurring tests to monitor availability and responsiveness.

Performance and availability issues could be a result of underlying security problems. It is recommended to run these tests often and further investigate if any performance and availability issues may arise.

There are three types of availability tests:

- URL Ping Test
- Multi-step Web Test
- Custom Track Availability Tests

SSL/TLS Certificates

We can use private and public SSL certificates to secure communication on Azure Web Apps. By combining them with custom domains that matches the name listed within the certificate, we can give our applications a vanity namespace for user access.

App services hosted on App service plans using the Basic, Standard, Premium, or isolated tiers are required to use custom SSL certificates, and the free tier is not eligible to do so. Certificates can be managed with the Azure Portal, CLI, or PowerShell.

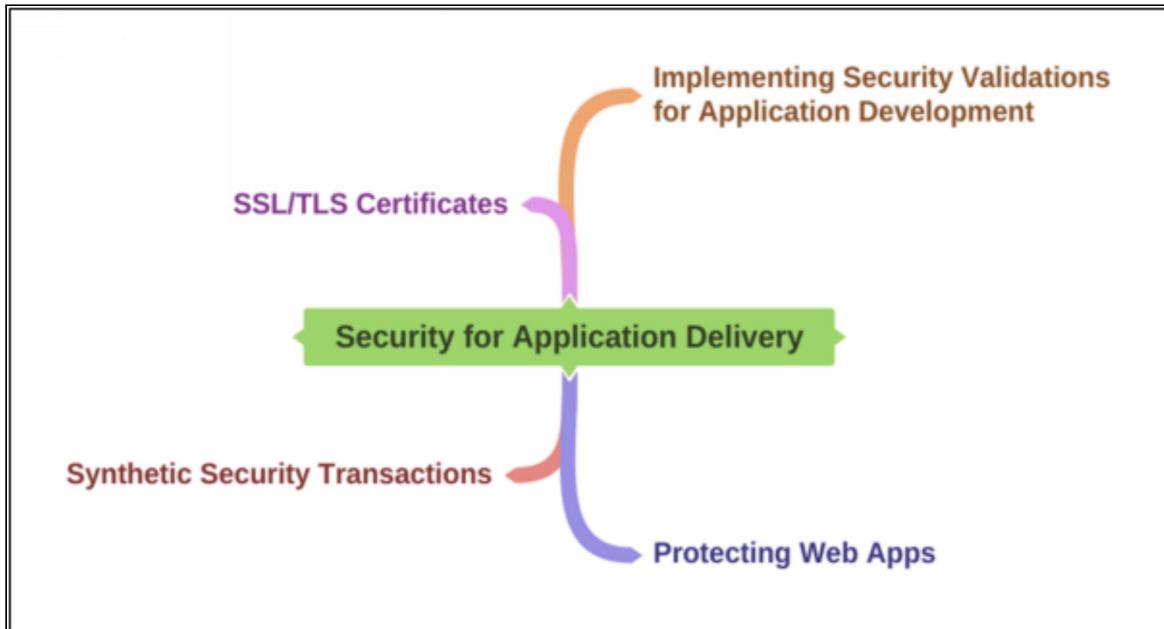
Protecting Web Apps

Azure Web Apps can be protected by deploying other Azure resources such as Application Gateway and Web App Firewall in front of the web apps.

Application Gateways provide network load balancing and traffic management for Azure virtual machines, virtual machine scale sets, and app services. With an application gateway, we can configure URL-based routing and multi-site hosting, along with other functionality to improve the availability of web applications.

Web Application Firewall (WAF) is an Application Gateway feature that provides web applications with centralized protection against common exploits and vulnerabilities. WAF is based on rules from the Open Web Application Security Project (OWASP) core rule sets 3.0 or 2.2.9.

Mind Map



Practice Questions

1. What feature of Application Gateway provides Web App protection from common exploits?
 - A. Azure Traffic Manager
 - B. Azure Antimalware
 - C. Web Application Firewall
 - D. Application Gateway

2. Implementing security validations for application development is an impressive way to secure _____ applications.
 - A. IaaS
 - B. PaaS
 - C. SaaS
 - D. None of the above

3. Adopting a policy of identity as the primary security perimeter can be done through _____.
 - A. Azure Key Vault
 - B. Azure Monitor
 - C. Azure Active Directory
 - D. Azure AD Conditional Access

4. Using strong authentication and authorization is a best practice for securing PaaS applications and can be done with _____.
 - A. Azure Key Vault
 - B. Azure Monitor
 - C. Azure Active Directory
 - D. Azure AD Conditional Access

5. Monitor app performance is a best practice for securing PaaS applications and can be done through _____.
 - A. Azure Monitor
 - B. Azure Application Insights
 - C. Azure Active Directory
 - D. Azure AD Conditional Access

6. Performing penetration testing whenever possible is a best practice for securing PaaS applications and can be implemented through _____.
- A. Microsoft Security Risk Detection
 - B. Azure Application Insights
 - C. Azure Active Directory
 - D. Azure AD Conditional Access
7. Which of the following types of availability tests are included in Synthetic Security Transactions?
- A. URL ping test
 - B. Multi-step web test
 - C. Custom Track Availability Tests
 - D. All of the above
8. To secure communication from Azure web apps to client browsers, what must be configured in the Azure Web App?
- A. SSL Certificate
 - B. Enforce TLS versions
 - C. App Service plan tier
 - D. All of the above
9. To improve the availability of web applications, what must be configured in the application gateway?
- A. URL-based routing
 - B. Multi-site hosting
 - C. OWASP core rule sets 3.0 or 2.2.9
 - D. All of the above
10. Which Azure resource provides network load balancing and traffic management?
- A. Azure Traffic Manager
 - B. Azure Antimalware
 - C. Web Application Firewall
 - D. Application Gateway

Chapter 11: Encryption for Data at Rest

Introduction:

Encryption at Rest is a standard security prerequisite. In Azure, companies can encrypt data at rest without the expense or cost of a custom key management solution. Organizations have the option to allow Azure at Rest to fully manage encryption. In addition, there are different ways for companies or individuals to closely manage encryption or encryption keys.

Microsoft Azure SQL Database Always Encrypted

In the Azure SQL Database and SQL Server, Always Encrypted is a data protection technology that helps secure, confidential data at rest on the server, during the transition between client and server, and when the data is in use. Always Encrypted promises that within the database system, confidential data never appears as plaintext. Only client applications or app servers with access to the keys will access plaintext data after we configure data encryption.

Always Encrypted is a client-level feature; it is configured using the Always Encrypted Wizard in the SQL Server Management Studio (SSMS). For encrypting entire databases or particular columns and rows inside the database, we can use Always Encrypted.

Database Encryption

Database encryption is available for Azure SQL Server, SQL Database, SQL Data Warehouse, Cosmos DB, and Data Lake using various technologies.

For Microsoft-managed service-side and client-side encryption scenarios, Azure SQL Database officially supports encryption at rest.

At present, the SQL feature called Transparent Data Encryption (TDE) offers support for server encryption. Once the TDE key is enabled by an Azure SQL Database customer, it is automatically generated and managed for them. Encryption at rest can be enabled at the database and server levels. Transparent Data Encryption (TDE) has been enabled by default on newly developed databases since June 2017.



EXAM TIP: In Microsoft Azure Exam DP-200- Implementing an Azure Data Solution course explains how encryption is achieved for each type of Azure database solution. It is recommended that you go through it to answer all types of questions regarding this topic.

Storage Service Encryption

Azure Storage automatically encrypts your data with 256-bit AES encryption, one of the strongest block ciphers available. Data in Azure Storage is transparently encrypted and decrypted. Azure Storage encryption is enabled by default for all new and existing storage accounts, including Resource Manager and classic storage accounts. Azure Storage encryption cannot be disabled.

All Azure Storage accounts, irrespective of performance tier (standard or premium), access tier (hot or cool), or deployment model (Azure Resource Manager or classic), are encrypted. Azure customers have an option between using Microsoft to handle the encryption key for storage accounts, or we can have our own key and manage the key using Azure Key Vault.

The Azure Portal, PowerShell, and the Azure CLI can be used to configure customer-managed keys.

Disk Encryption

We have a couple of options for disk encryption depending upon the operating system being used. Azure customers can choose to encrypt their Virtual Machine-managed disks to protect data. Azure uses BitLocker disk encryption for Windows managed disks, and DM-Crypt disk encryption for Linux managed disks.

It does not matter for running Standard and premium disks; both can benefit from disk encryption. We can use Azure Security Center to be alerted of any virtual machines that are not utilizing disk encryption and view instructions on how to encrypt these disks.

Azure Key Vault can be used to manage keys used to encrypt disks. Azure Disk Encryption requires your key vault and VMs to reside in the same Azure region and Azure subscriptions.

Supported Operating Systems

Following are the supported Operating systems that can benefit from Disk Encryption.

Windows:

- Workstation: Windows 8 and later
- Server: Windows Server 2008 R2 and later

Linux:

- Ubuntu: 14.04.5, 16.04, 18.04
- RHEL: 6.7, 6.8, 7.2n, 7.3, 7.6
- openSUSE: 42.3
- SLES: 12-SP3, SP4

Backup Encryption

Backups in Azure are encrypted with AES-256 encryption and are transmitted to the Azure Backup vault using secure HTTPS communication. Azure backups are encrypted at rest by default. There is no configuration required to enable the feature.

There are a couple of things that we need to be aware of regarding backup encryption.

- On-premise backups use the passphrase configured when installing the Azure Backup client. When you have installed the backup client or backup server and registered your connection with the Recovery Services vault, a passkey is generated that is required to restore or decrypt the data
- Azure VMs are encrypted at rest using Storage Service Encryption

If the passphrase generated at client installation is lost, then the backup data is unrecoverable. Azure Key Vault can be used to store Azure backup passphrases as secrets.

Lab 11-01: Enabling Always Encrypted in Azure SQL

Introduction

In this hands-on lab, candidates will employ one of the most important and popular "data at rest" protection mechanisms: Always Encrypted SQL data. We will create a SQL Server, populate a database with sample data, and then connect and encrypt a targeted portion of that data.

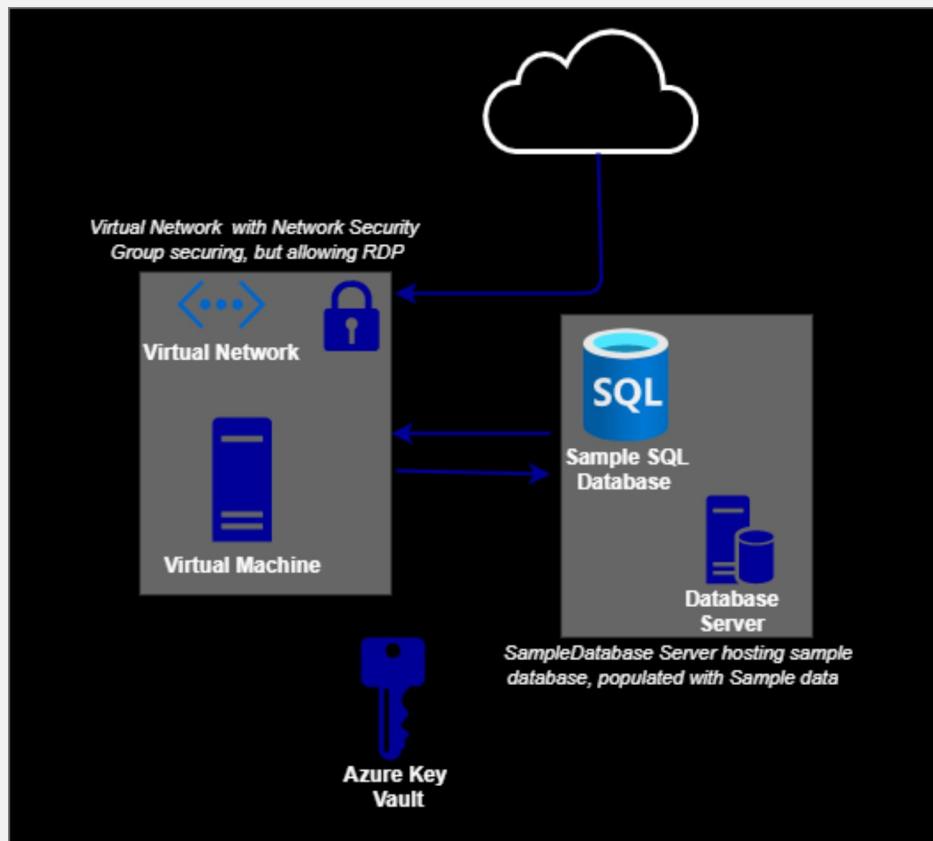


Figure15-01: Enabling Always Encrypted in Azure SQL

Solution

Log in to the Azure Portal using the credentials.

Step#01

Create a Virtual Network and Network Security Group

1. Navigate to **All services**; create a resource group.

Microsoft Azure

Home > Resource groups >

Create a resource group

Basics Tags Review + create

Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more](#)

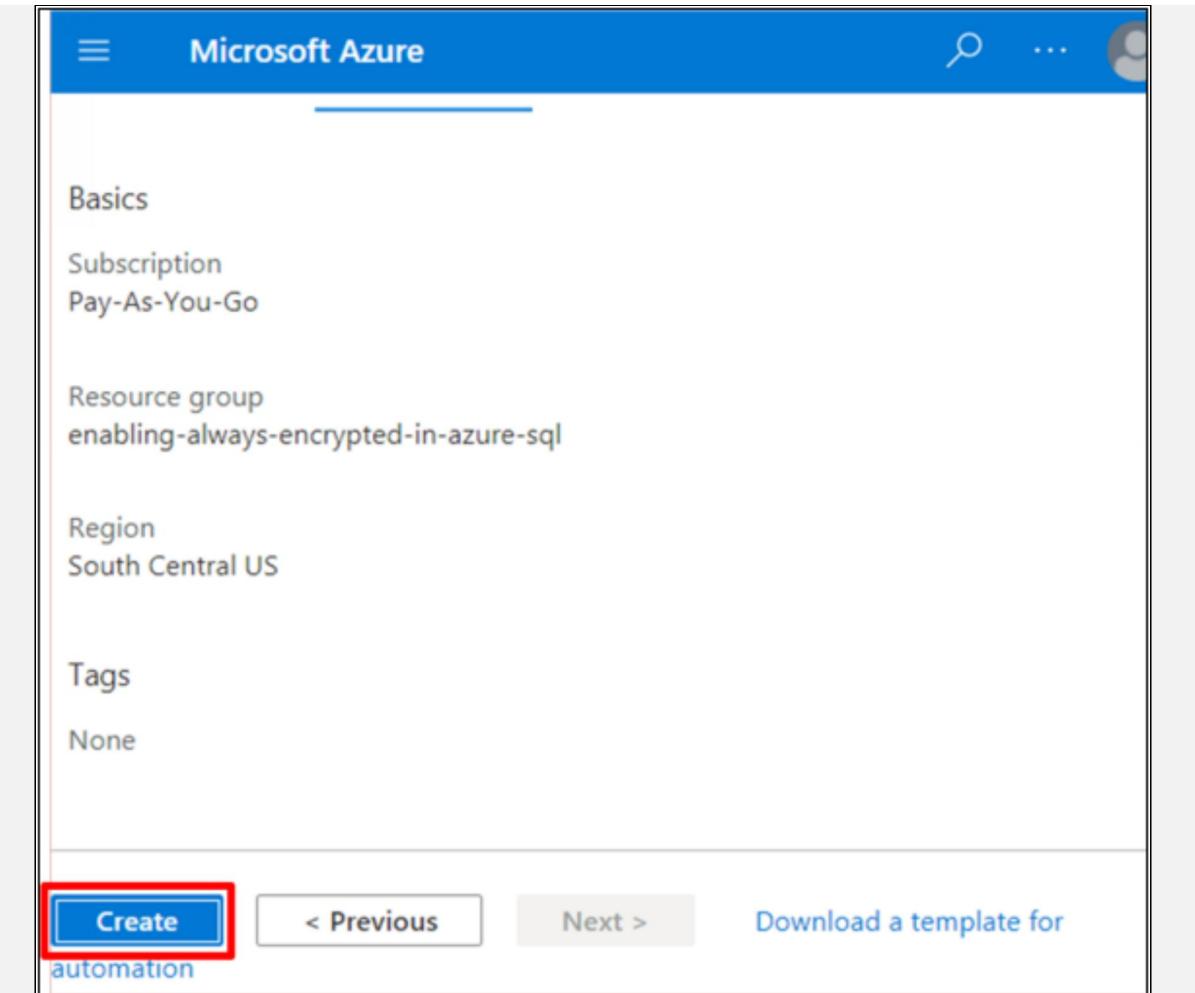
Project details

Subscription * ⓘ Pay-As-You-Go

Resource group * ⓘ enabling-always-encrypted-in-azure-sql ✓

Resource details

Region * ⓘ (US) South Central US



2. Navigate to **Virtual networks** in the left-hand menu and click **Create virtual network**.

 Microsoft Azure

List view

Name ↑↓ Resource group ↑↓ Location ↑↓

No virtual networks to display

Create a virtual network to securely connect your Azure resources to each other. Connect your network to your on-premises network using an Azure VPN Gateway or ExpressRoute

[Learn more](#)

[Create virtual network](#)

3. Set the following values:

- *Name*: Anything you would like (e.g., "SSMSVnet1")

Microsoft Azure Search resources, services, and docs (G/) ...

to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation.

[Learn more about virtual network](#)

Project details

Subscription * ⓘ Pay-As-You-Go

Resource group * ⓘ enabling-always-encrypted-in-azure-sql

Create new

Instance details

Name * SSMSVnet1

Region * (US) South Central US

Review + create < Previous

Next : IP Addresses > Download a template for automation

- **Address space:** **10.0.0.0/24**
- **Resource group:** Select the one listed in the dropdown
- **Location:** The location we just noted
- **Address range:** **10.0.0.0/26**

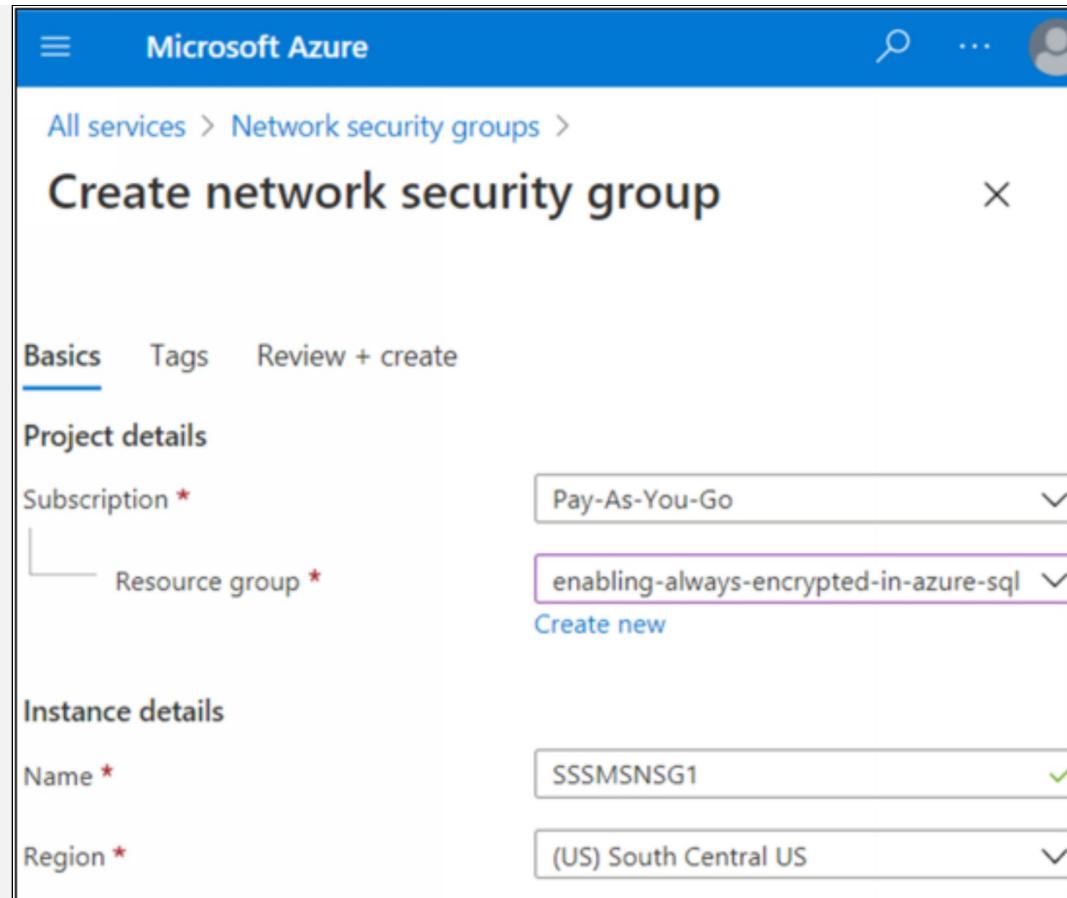
4. Click **Create**.

The screenshot shows the Microsoft Azure portal interface for creating a virtual network. The top navigation bar includes the Microsoft Azure logo, a search icon, and a user profile icon. Below the navigation, the breadcrumb trail shows 'Home > Virtual networks >'. The main title is 'Create virtual network' with a close button ('X'). The navigation tabs at the top of the form are 'Basics', 'IP Addresses' (which is underlined, indicating it's selected), 'Security', 'Tags', and 'Review + create'. A descriptive text below the tabs states: 'The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).'
IPv4 address space
A text input field contains '10.0.0.0/24' with a green checkmark icon to its right.

<input type="checkbox"/> Subnet name	Subnet address range
<input type="checkbox"/> default	10.0.0.0/26

At the bottom of the form are three buttons: 'Review + create' (highlighted with a red border), '< Previous', and 'Next : Security >'.

5. Navigate to **All services > Network security groups**.
6. Click **Create network security group**.
7. Set the following values:
 - **Name:** Anything you would like (e.g., "SSSMSNSG1")
 - **Resource group:** Select the one listed in the dropdown
 - **Location:** The same location as before
8. Click **Create**.



9. Once it is deployed, click the name of the NSG.
10. Click **Inbound security rules**.
11. Click **Add**.

The screenshot shows the Microsoft Azure portal interface. At the top, it says "Microsoft Azure" with a search bar and user icon. Below that, the navigation path is "All services > NoMarketplace-20210104222741 > SSSMSNSG1". The main title is "SSSMSNSG1 | Inbound security rules". Underneath, it says "Network security group". There are three buttons at the top: "Add" (highlighted with a red box), "Default rules", and "Refresh". A table below lists the current inbound security rules:

Priority	Name	Port	Protocol
65000	AllowVnetInBound	Any	Any
65001	AllowAzureLoadBala...	Any	Any
65500	DenyAllInBound	Any	Any

12. Set the following values:

- *Destination port ranges: 3389*
- *Name: Port_3389*

13. Click **Add**.

Microsoft Azure

3389

Protocol *

Any TCP UDP ICMP

Action *

Allow Deny

Priority *

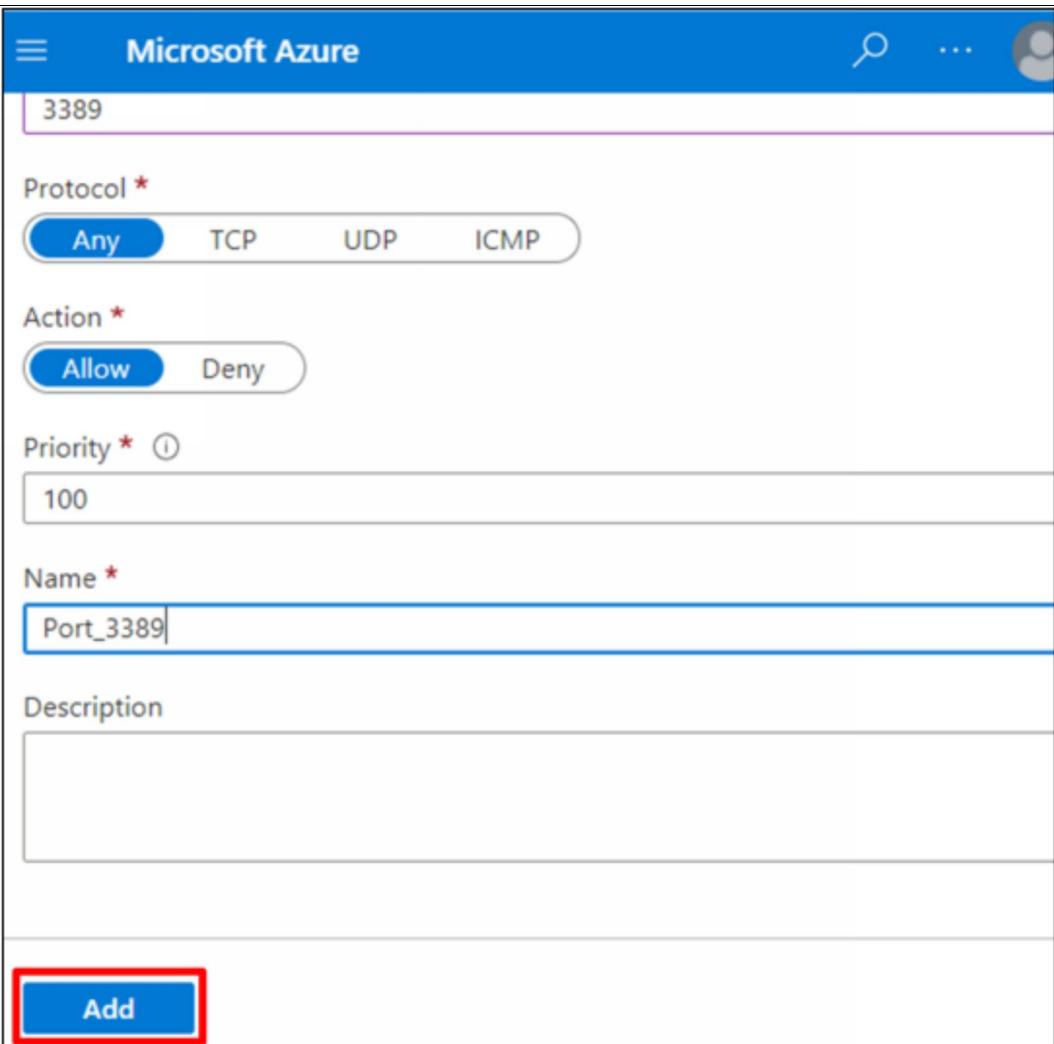
100

Name *

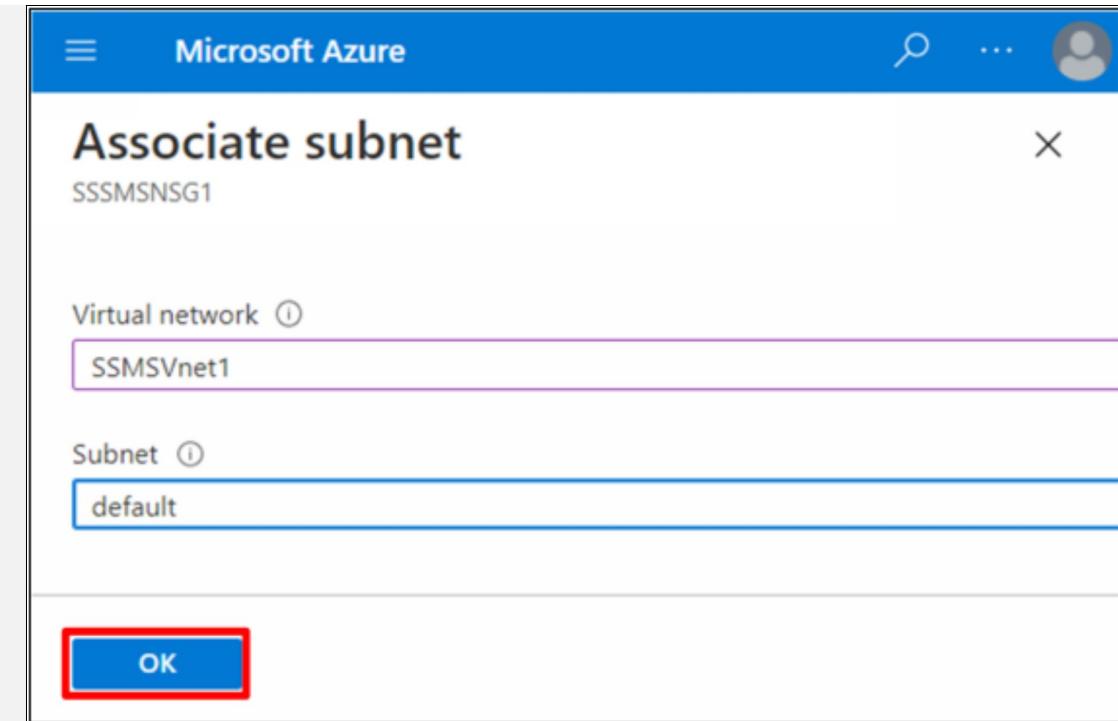
Port_3389

Description

Add



14. Click **Subnets**
15. Click **Associate**
16. Click **Virtual network** and select the listed virtual network.
17. Click **Subnet** and select **Default**.
18. Click **OK**



Step#02

Create a Virtual Machine

1. Click **Virtual machines** in the left-hand menu.
2. Click **Create virtual machine**, and set the following values:
 - *Resource group*: Select the one listed in the dropdown
 - *Virtual machine name*: Anything you'd like (e.g., "SSMSServer1")
 - *Region*: Select the one listed in the dropdown
 - *Image*: **Windows Server 2019**
 - *Size*: **B2s Standard**
 - *Username*: Anything you would like
 - *Password*: Anything you would like

Microsoft Azure

Instance details

Virtual machine name * ⓘ SSMServer1 ✓

Region * ⓘ (US) South Central US

Availability options ⓘ No infrastructure redundancy required

Image * ⓘ Windows Server 2019 Datacenter - Ge... ✓
See all images

Azure Spot instance ⓘ

Size * ⓘ Standard_B2s - 2 vcpus, 4 GiB memory... ✓
See all sizes

Administrator account

Username * ⓘ sqlserveradmin ✓

Password * ⓘ ✓

Confirm password * ⓘ ✓

This screenshot shows the 'Instance details' section of the Azure VM creation wizard. It includes fields for the virtual machine name (SSMServer1), region (South Central US), image (Windows Server 2019 Datacenter), size (Standard_B2s), and administrator account (sqlserveradmin). The 'Azure Spot instance' checkbox is unchecked. The 'Confirm password' field is identical to the 'Password' field.

3. Click **Next: Disks**.
4. Leave settings as-is and click **Next: Networking**.
5. Set the *Virtual network* to the one we previously created.

The screenshot shows the Microsoft Azure interface for configuring the networking settings of a virtual machine. The top navigation bar includes 'Microsoft Azure' with a search icon and user profile, and tabs for 'Basics', 'Disks', 'Networking' (which is underlined), 'Management', and 'Advanced'. Below the tabs, a descriptive text explains how to define network connectivity by configuring network interface card (NIC) settings, mentioning ports, security group rules, and load balancing. A 'Learn more' link is provided.

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * (i) SSMSVnet1

Subnet * (i) default (10.0.0.0/26)

Public IP (i) (new) SSMServer1-ip

NIC network security group (i) None Basic Advanced

6. Click **Next: Management**.
7. Set *Boot Diagnostics* to **Off**.

Microsoft Azure

Basics Disks Networking Management Advanced ...

Configure monitoring and management options for your VM.

Azure Security Center

Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads. [Learn more ↗](#)

Your subscription is protected by Azure Security Center basic plan.

Monitoring

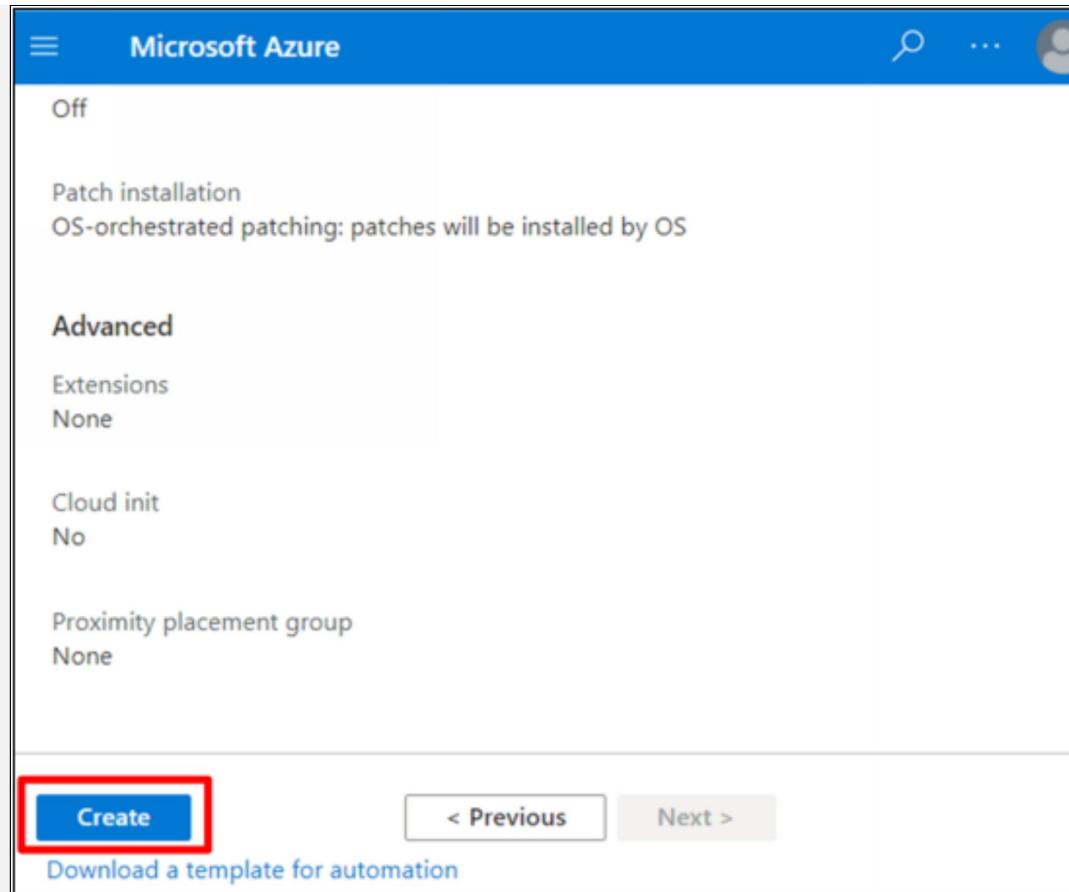
Boot diagnostics ⓘ

Enable with managed storage account (recommended)

Enable with custom storage account

Disable

8. Click **Next: Advanced > Next: Tags > Review + create.**
9. Click **Create.**



Step#03

Create a SQL Server and SQL Database

1. Navigate to **All services** > **Azure SQL**.
2. Click **Create Azure SQL resource**.
3. In the **SQL databases** card, with *Resource type* set to **Single database**, click **Create**.

All services > Azure SQL >

Select SQL deployment option

Microsoft

Feedback

How do you plan to use the service?

SQL databases

Best for modern cloud applications. Hyperscale and serverless options are available.

Resource type

Single database

Create

SQL managed instances

Best for most migrations to the Lift-and-shift read

Resource type

Single instance

Create

4. Set the following values:

- *Resource group*: Select the one listed in the dropdown
- *Database name*: Anything you'd like (e.g., "sampleDB1")
- **Server: Create new**

Server name: Anything unique you would like (e.g., "sampleserver" with five or six random numbers appended at the end)

Server admin login: Anything you would like

Password: Anything you would like

Location: The same location as before

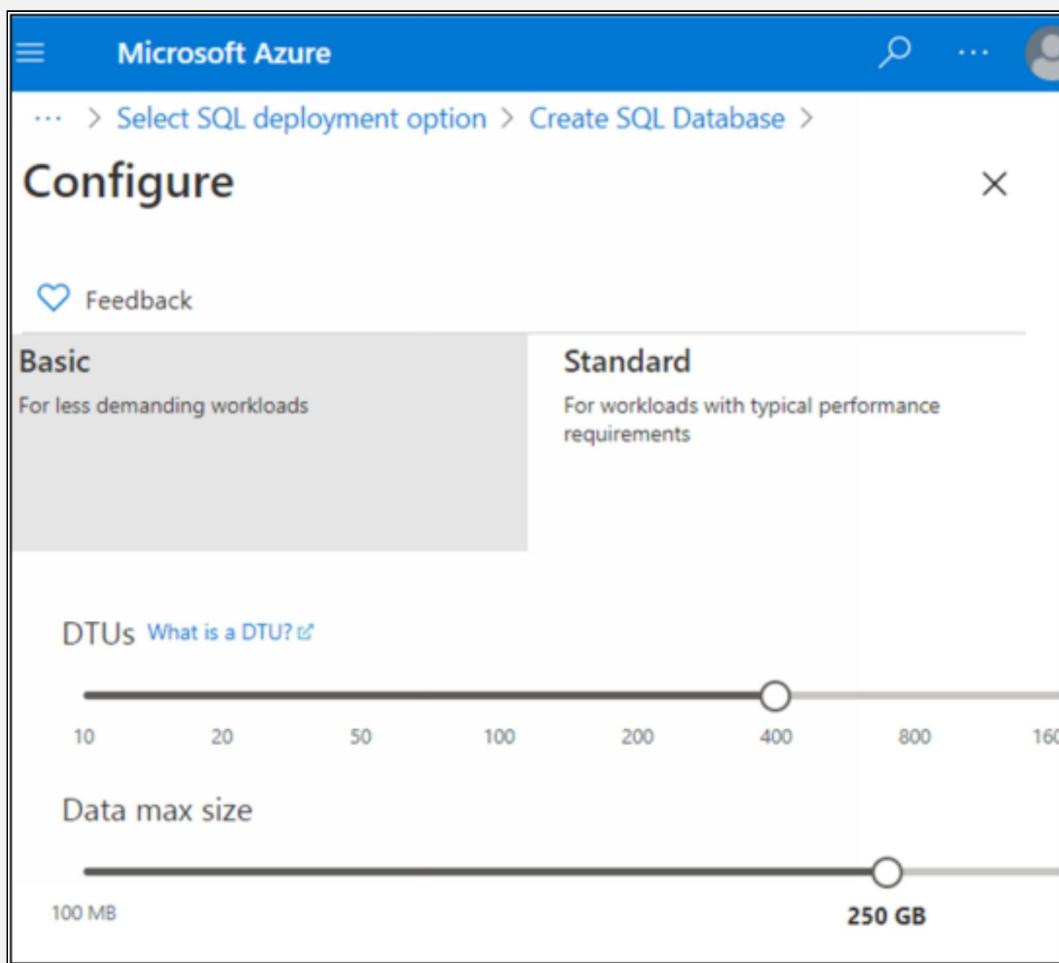
Allow Azure services to access server: Check

Click **OK**.

Compute + storage: Configure database

Select **Standard** and set it to **200 DTUs** (i.e., a Standard S04 server).

Click **Apply**.



5. Click **Next: Additional settings**, and set the following values:

- *Use existing data:* **Sample**
- *Enable Advanced Data Security:* **Not now**

6. Click **Next: Tags > Review + create**.

The screenshot shows the Microsoft Azure portal interface for creating a new SQL database. The top navigation bar includes the Microsoft Azure logo, a search icon, and a user profile icon. Below the navigation, a breadcrumb trail shows the path: ... > Azure SQL > Select SQL deployment option >. The main title is "Create SQL Database" with a close button (X) to its right. The Microsoft logo is present below the title.

The "Additional settings" tab is selected, indicated by an underline. Other tabs include Basics, Networking, Tags, and Review + create.

The "Additional settings" section contains the following content:

- Data source**: A note stating "Start with a blank database, restore from a backup or select sample data to populate your new database."
- Use existing data ***: A dropdown menu with three options: None, Backup, and Sample. The "Sample" option is highlighted with a purple background.
- A note below the dropdown states: "AdventureWorksLT will be created as the sample database."
- Azure Defender for SQL**: A note stating "Protect your data using Azure Defender for SQL, a unified security package including vulnerability assessment and advanced threat protection for your server." It includes a "Learn more" link and a checkbox.
- A note below the security section states: "Get started with a 30 day free trial period, and then 15 USD/server/month."
- Enable Azure Defender for SQL ***: A checkbox followed by a help icon (info symbol).
- Buttons for "Start free trial" and "Not now".

At the bottom of the page are three navigation buttons: "Review + create" (highlighted with a red border), "< Previous", and "Next : Tags >".

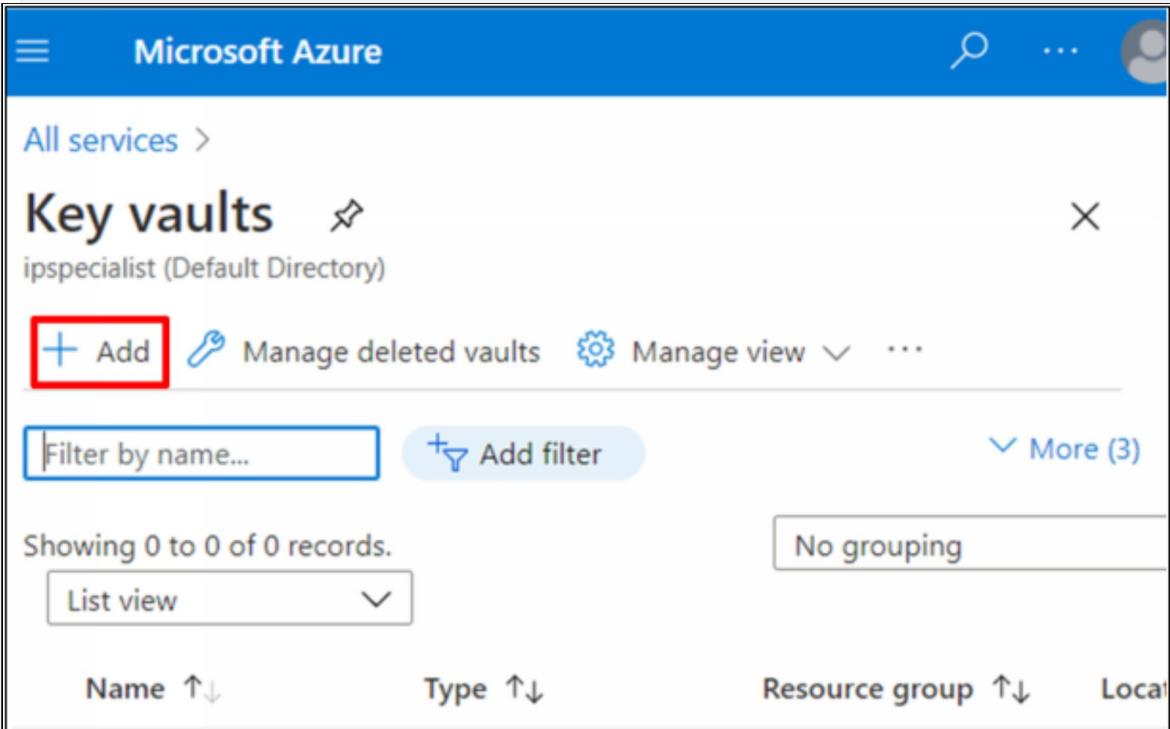
7. Click **Create**.

Step#04

Create an Azure Key Vault

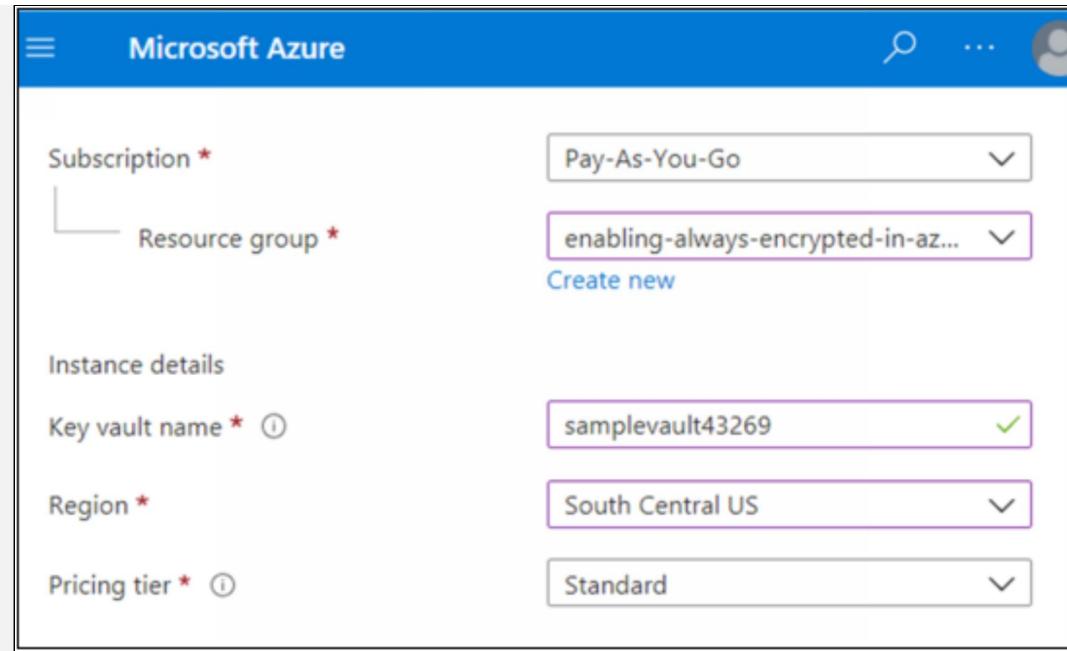
Note: Unless otherwise stated, select the default options or, in the case of the subscriptions and resource groups, the only available option.

1. Navigate to **All services > Key vaults**.
2. Click **Create key vault**.



The screenshot shows the Microsoft Azure Key vaults interface. At the top, there's a blue header bar with the Microsoft Azure logo and a search icon. Below it, the navigation path is "All services > Key vaults". The main title is "Key vaults" with a refresh icon. Underneath, it says "ipspecialist (Default Directory)". On the left, there's a "Add" button with a plus sign, which is highlighted with a red box. To its right are "Manage deleted vaults" and "Manage view" options. Below these are search and filter fields: "Filter by name..." and "Add filter". There's also a "More (3)" link. In the center, it says "Showing 0 to 0 of 0 records." Below this are sorting options: "List view" (with a dropdown arrow), "Name ↑↓", "Type ↑↓", "Resource group ↑↓", and "Loca↑". To the right, there's a "No grouping" button.

3. Set the following values:
 - **Resource group:** Select the one listed in the dropdown
 - **Key vault name:** Anything unique you'd like (e.g., "samplevault" with five or six random numbers appended at the end)
 - **Region:** Select the one listed in the dropdown



4. Click **Next: Access policy**.
5. In the *Key Permissions* column, click **Select all** for the logged-in lab user.
6. Click **Next: Virtual network > Next: Tags > Review + create**.
7. Click **Create**.

The screenshot shows the Microsoft Azure Access Policies interface. At the top, there's a blue header bar with the Microsoft Azure logo and a search icon. Below the header, there are two radio button options for the Permission model: "Vault access policy" (selected) and "Azure role-based access control (preview)". A link "+ Add Access Policy" is located below these options. The main section is titled "Current Access Policies" and contains a table with three columns: Name, Email, and Key Permissions. The table has a header row and a single data row for a user named "USER". The data row includes a small profile icon, the name "Hanif", the email "hanifwasti@nomykha...", and a dropdown menu showing "9 selected". Below the table is a navigation bar with buttons for "Review + create" (which is highlighted with a red box), "< Previous", and "Next : Networking >".

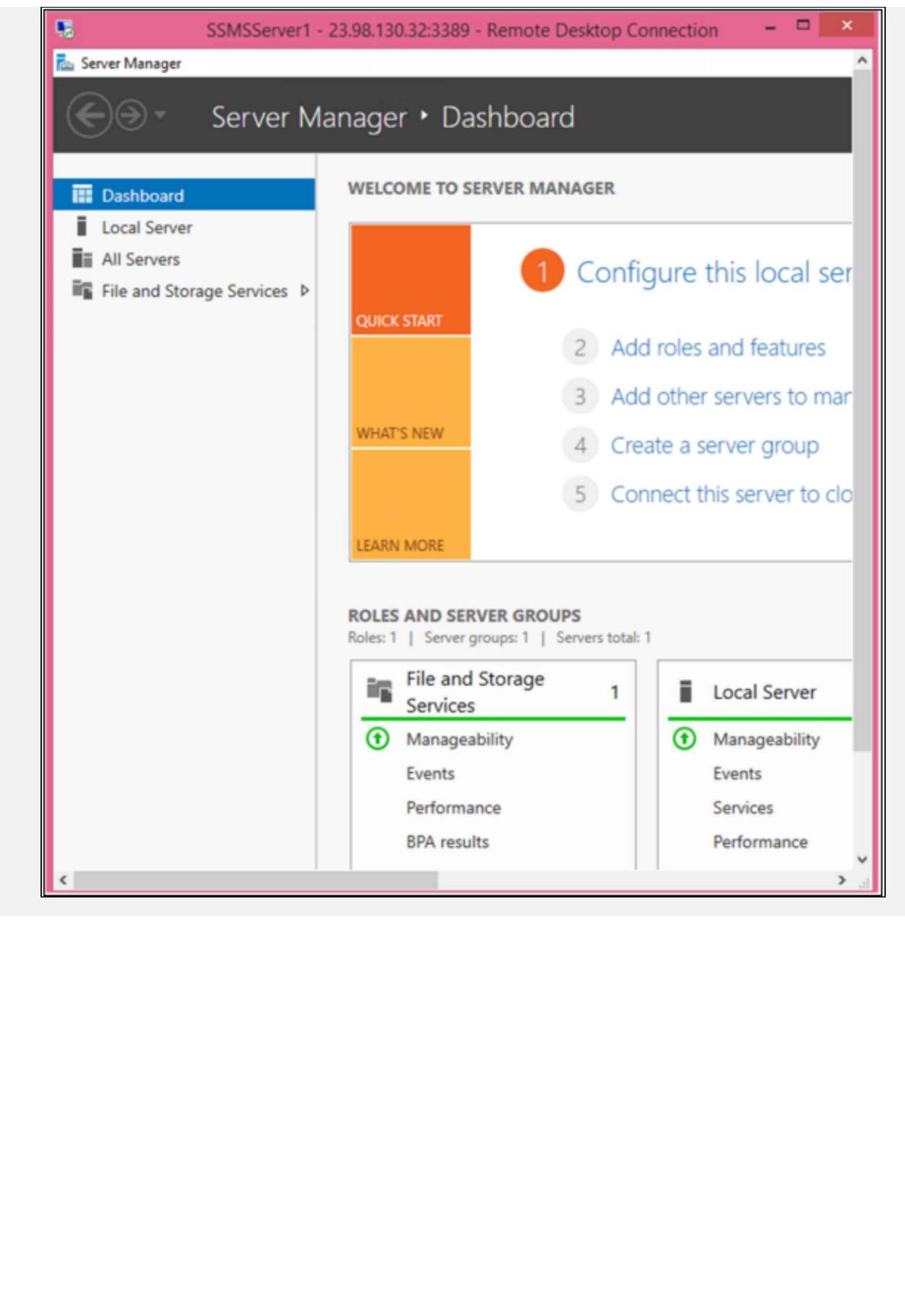
Step#05

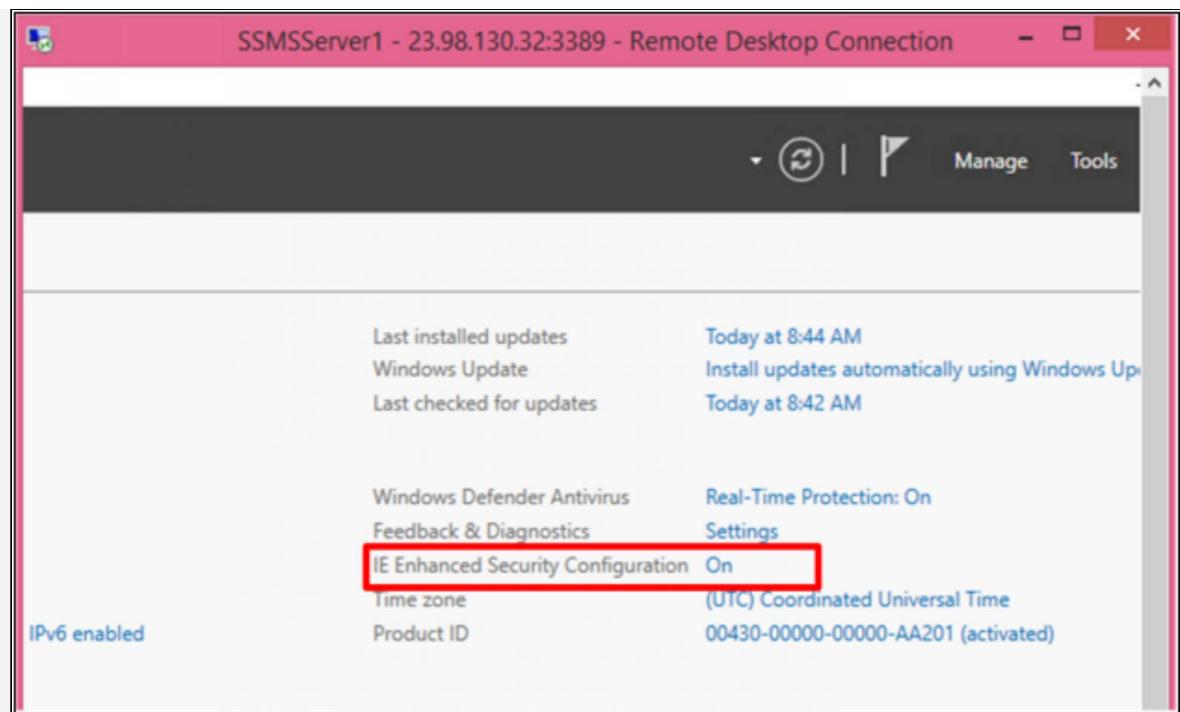
Use RDP to Connect to the Virtual Machine and Install SQL Server Management Studio

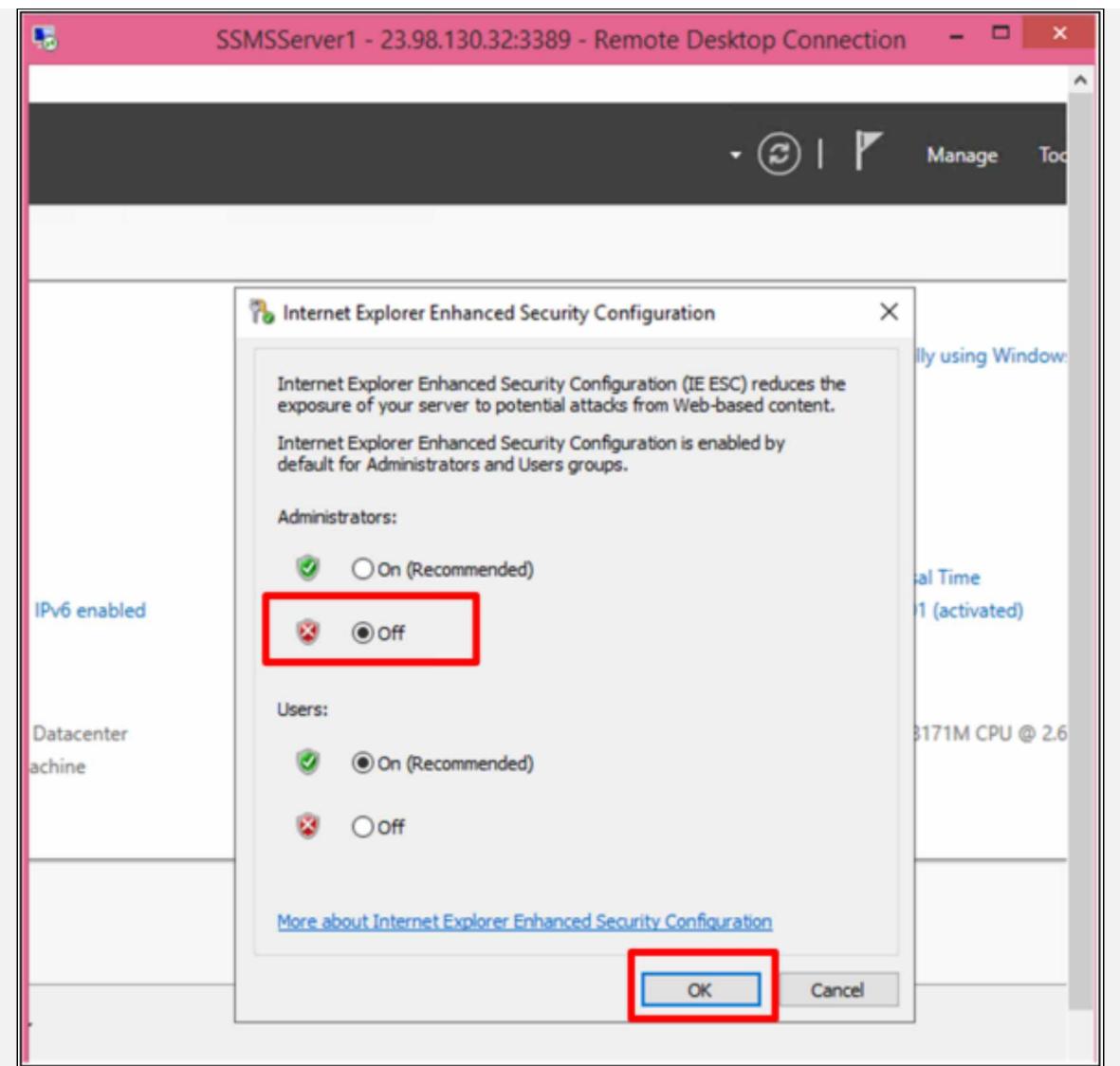
1. Navigate to **Virtual machines** in the left-hand menu, and click the listed VM.
2. Connect to the server via RDP, logging in with the credentials assigned above.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header bar with the 'Microsoft Azure' logo, a search icon, and a user profile icon. Below the header, a card for a virtual machine named 'SSMServer1 | Connect' is displayed. The card includes a blue link icon and the text 'Virtual machine'. A yellow warning box contains the message: '⚠ To improve security, enable just-in-time access on this VM. →'. Below the warning, there are three connection options: 'RDP' (underlined), 'SSH', and 'BASTION'. Under the 'RDP' section, the heading 'Connect with RDP' is followed by the instruction: 'To connect to your virtual machine via RDP, select an IP address, optionally change the port number, and download the RDP file.' Two input fields are present: 'IP address *' containing 'Public IP address (23.98.130.32)' and 'Port number *' containing '3389'. A red rectangular box highlights the 'Download RDP File' button, which is located at the bottom of the RDP connection section.

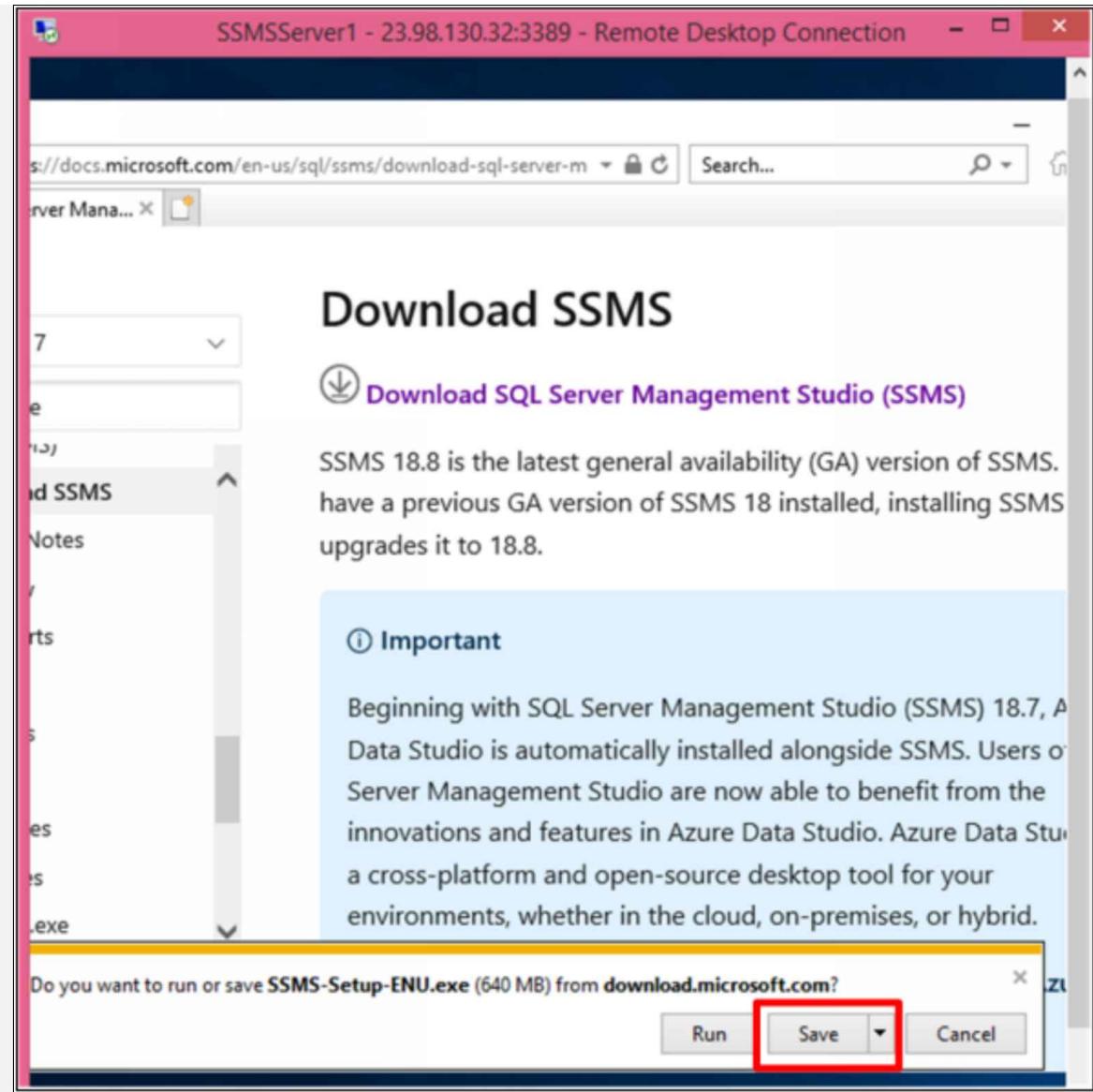
- Once connected, turn off *IE Enhanced Security Configuration*.

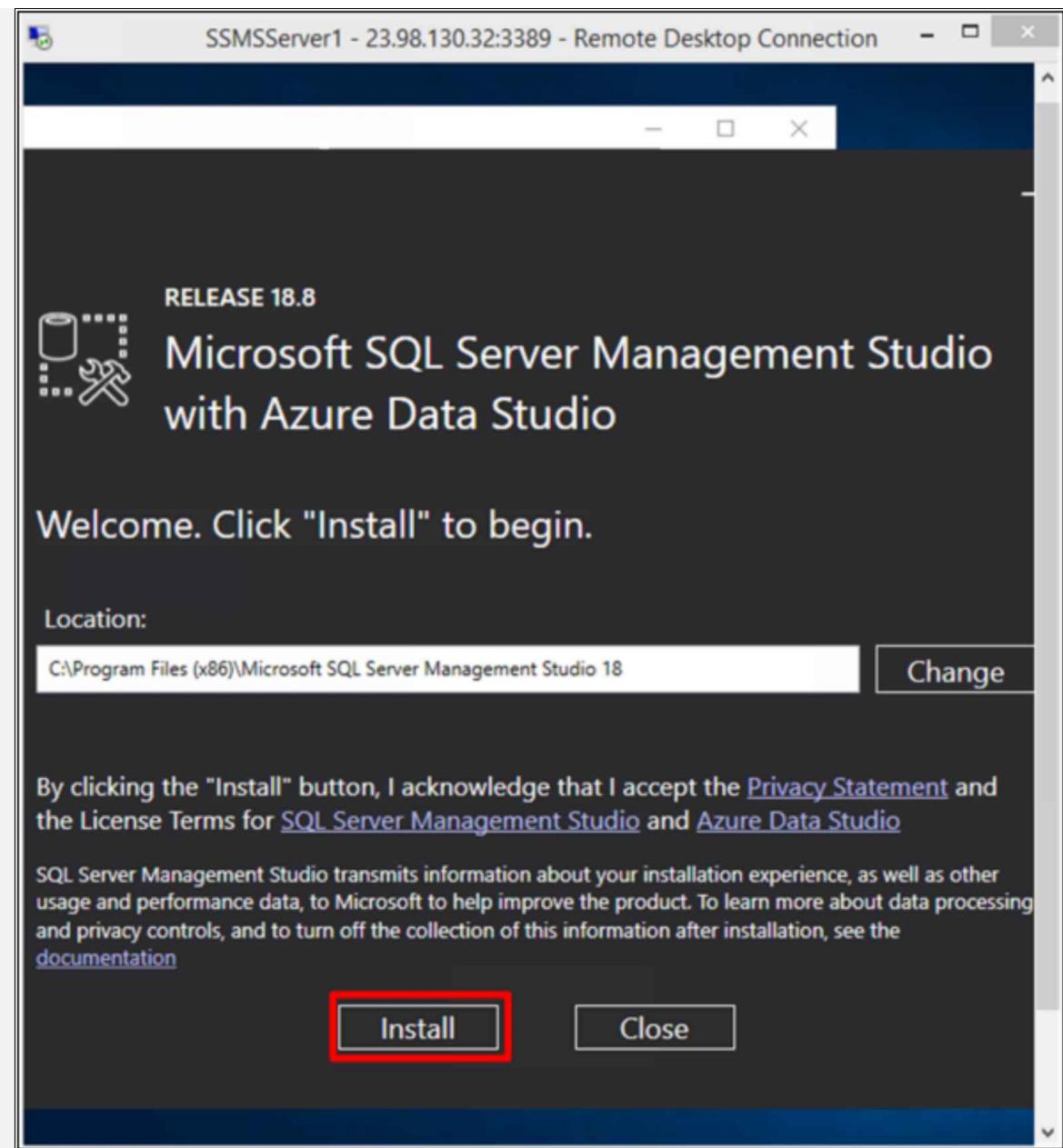






4. Open Internet Explorer, and browse to [this link](#) to download the latest version of SSMS.
5. Once it is saved to the Remote Desktop client desktop, click to open and install it.





Step#06

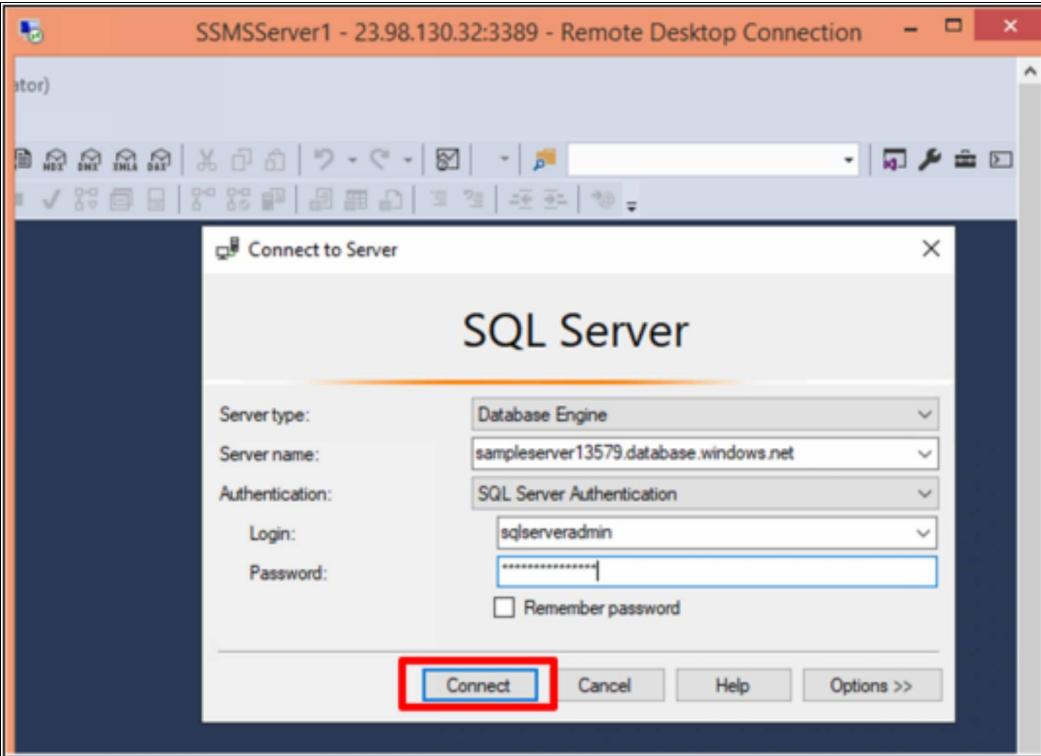
Connect to the SQL Server and Encrypt Some Data

1. In the Azure browser window, navigate to **Azure SQL resources > Overview**.
2. Copy the server name listed for it.

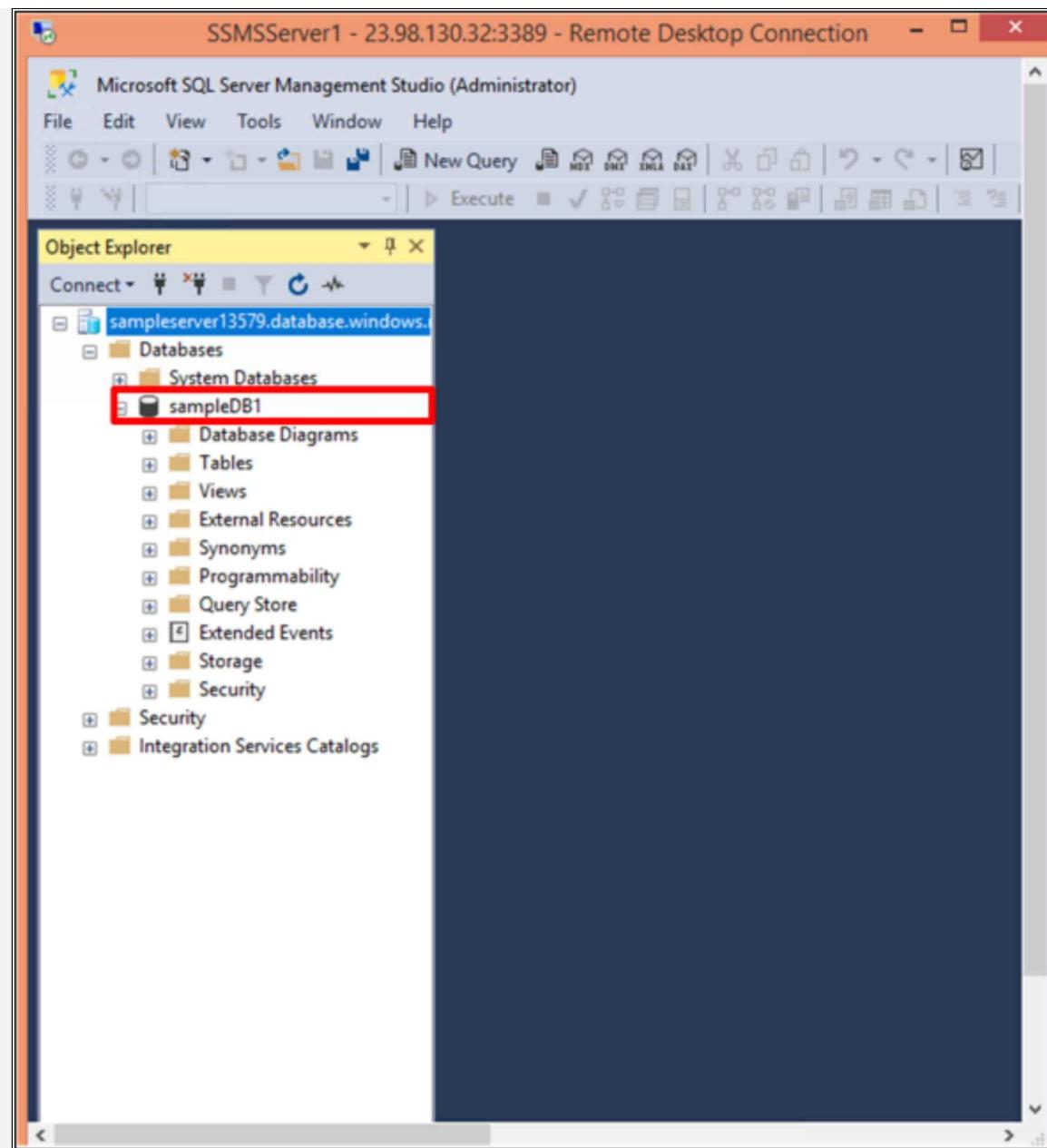
The screenshot shows the Microsoft Azure portal interface. At the top, it says "Microsoft Azure" with a search bar and user icon. Below that, it shows "All services > All resources >". The main title is "sampleDB1 (sampleserver1357...)" with a "SQL database" icon. Below the title are actions: "Copy", "Restore", "Export", "Set server firewall", and "...". A "JSON V" link is also present. Under the "Essentials" section, there are several properties listed:

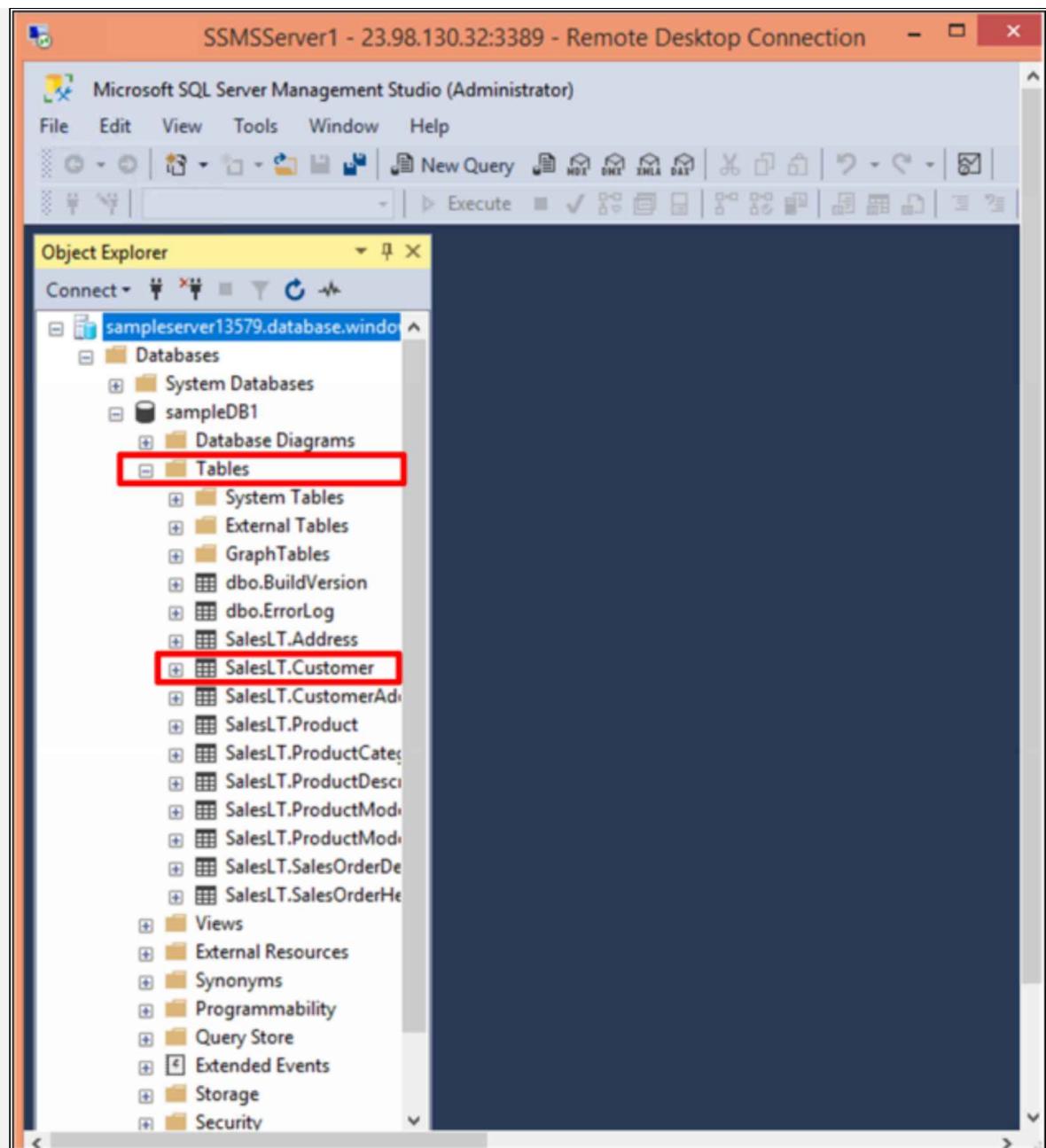
Property	Value
Resource group (change)	: enabling-always-encrypted-in-azure-sql
Status	: Online
Location	: South Central US
Subscription (change)	: Pay-As-You-Go
Subscription ID	: 797152d3-23c4-499f-bfef-bb103da7d054
Server name	sampleserver13579.database.windows.net
Elastic pool	: No elastic pool
Connection strings	: Show database connection strings
Pricing tier	: Standard S4: 200 DTUs
Earliest restore point	: 2021-01-05 08:49 UTC

3. Back in the Remote Desktop client, paste the server name into the SQL Server pop-up.
4. Change the *Authentication* to **SQL Server Authentication**.
5. Enter the login credentials you created for the server earlier
6. Click **Connect**.

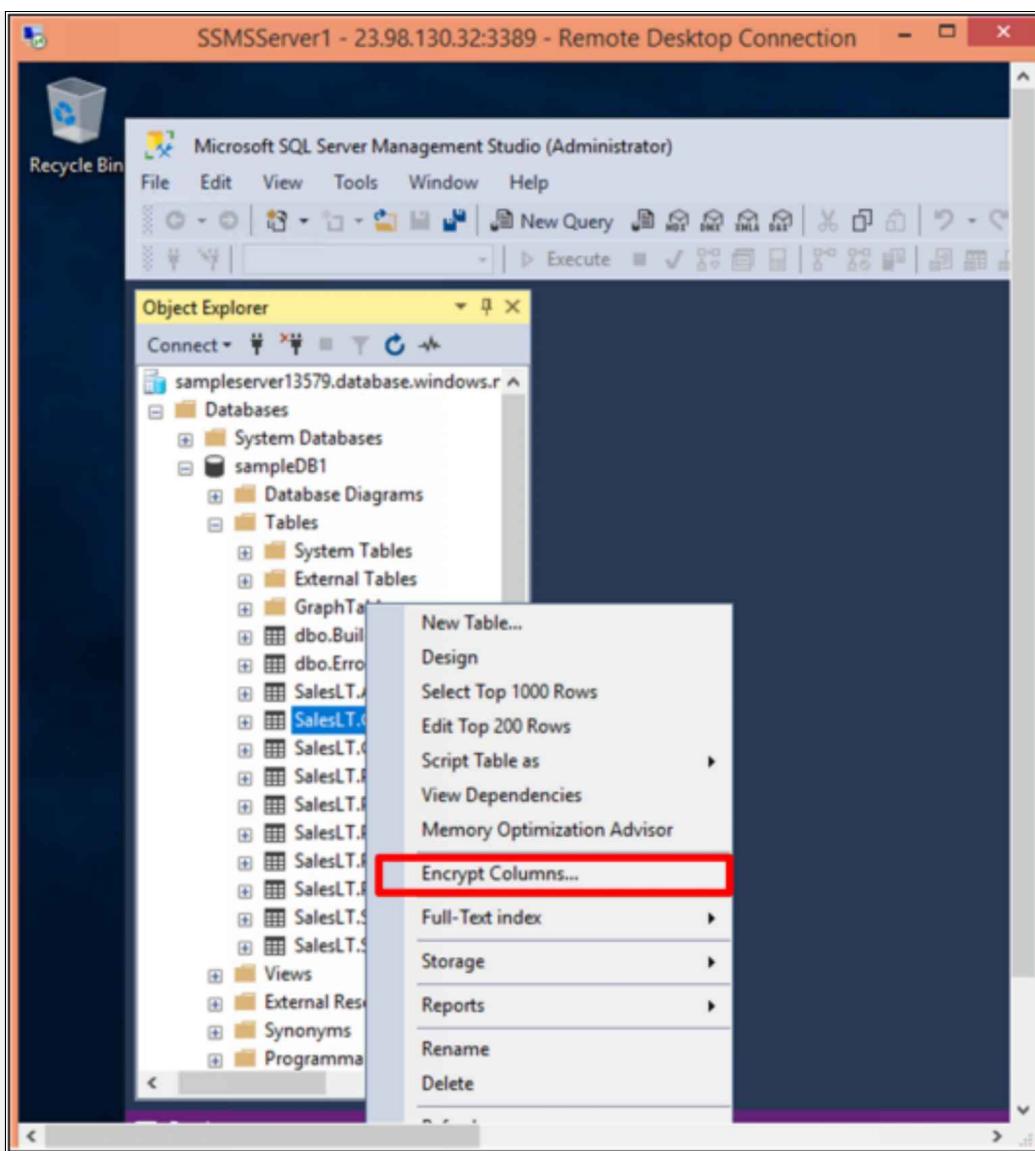


7. Browse to **Databases** > **sampledb1** > **Tables** > and right-click on **SalesLT.Customer**.

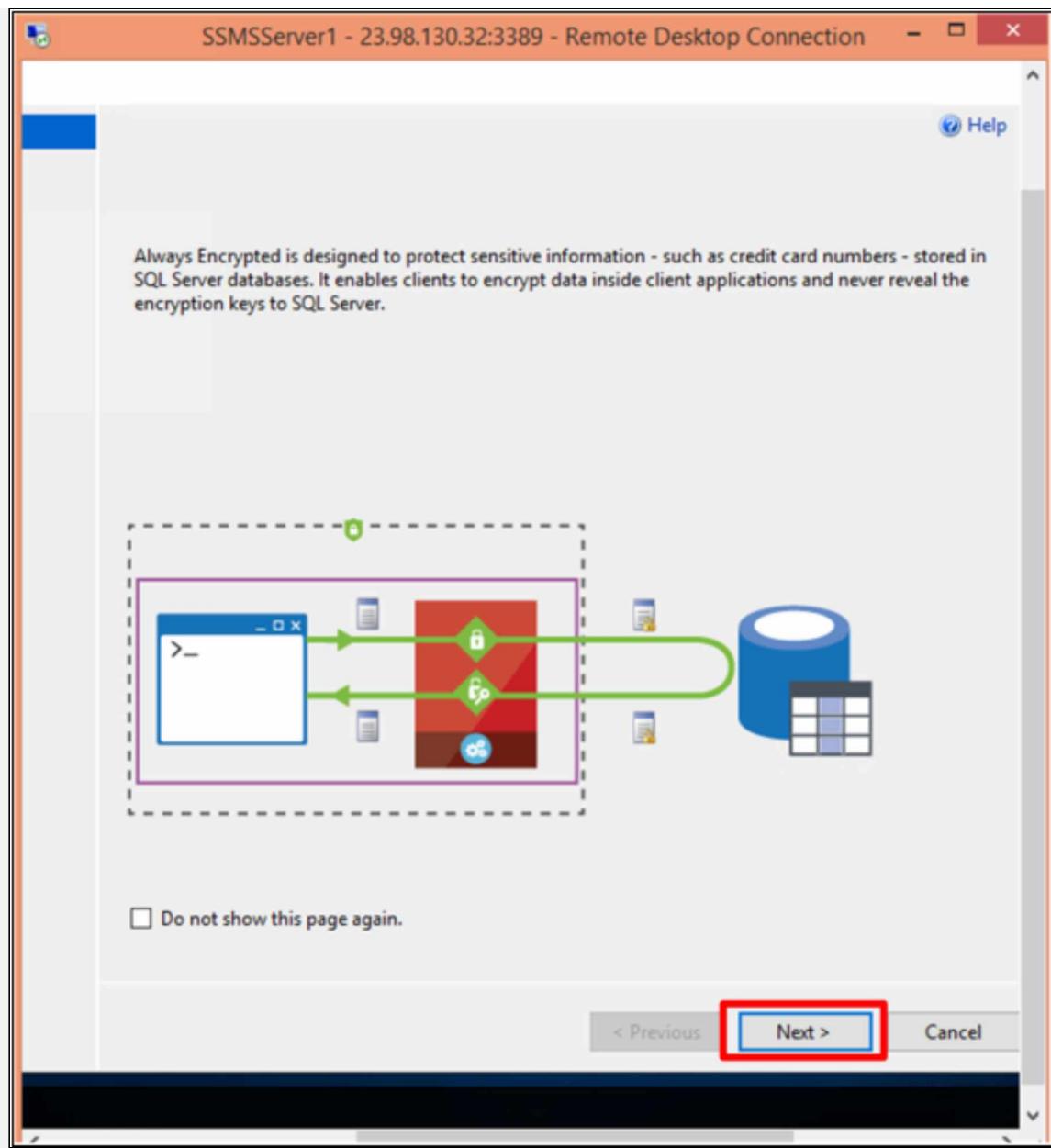




8. Select **Encrypt Columns**.



9. Click **Next**.



10. On the *Column Selection* screen, select **FirstName**, **MiddleName**, and **LastName**.

SSMSServer1 - 23.98.130.32:3389 - Remote Desktop Connection

Always Encrypted

Column Selection

Introduction

Column Selection

Master Key Configuration

Run Settings

Summary

Results

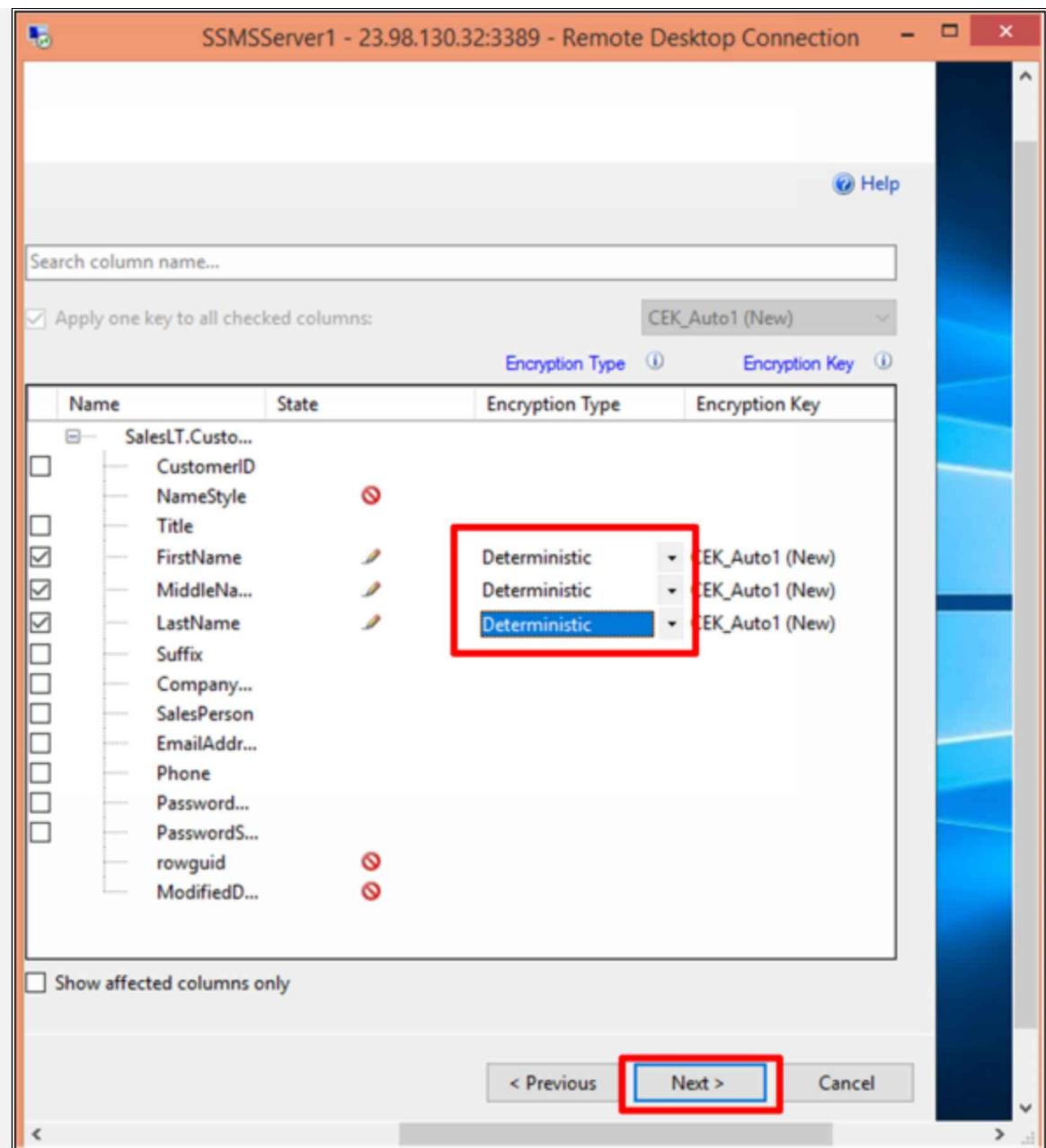
Search column name...

Apply one key to all checked columns:

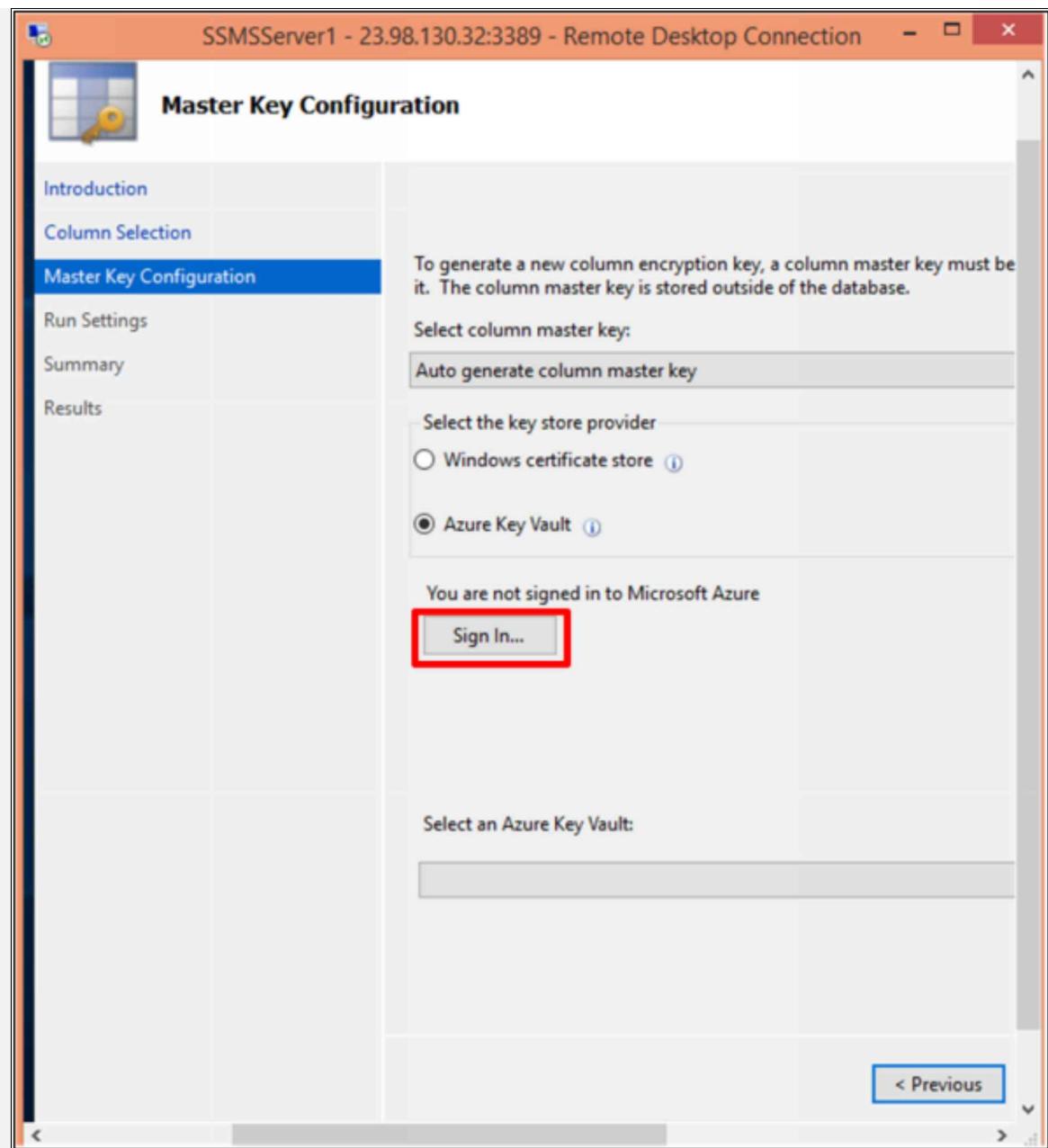
Name	State	Encryption Type
SalesLT.Custo...		
CustomerID		
NameStyle		🚫
Title		
<input checked="" type="checkbox"/> FirstName	*	Choose Type...
<input checked="" type="checkbox"/> MiddleNa...	*	Choose Type...
<input checked="" type="checkbox"/> LastName	*	Choose Type...
Suffix		
Company...		
SalesPerson		
EmailAddr...		
Phone		
Password...		
PasswordS...		
rowguid		🚫
ModifiedD...		🚫

Show affected columns only

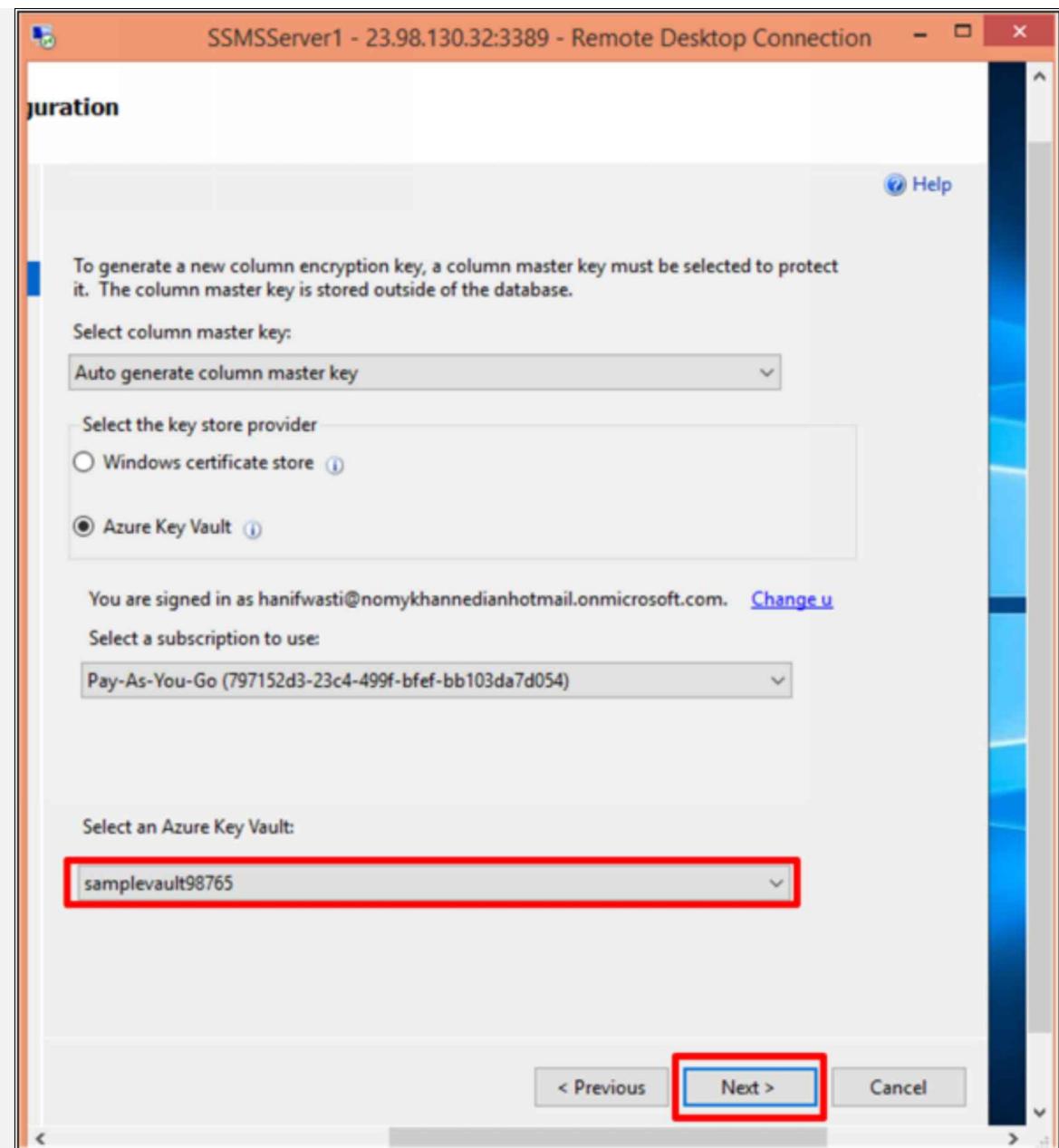
11. In the **Encryption Type** column, click the **Choose Type** dropdown for each and set them to **Deterministic** encryption.
12. Click **Next**.



13. On the *Master Key Configuration* screen, select **Azure Key Vault**.
14. Click to **Sign in** to Azure and use the credentials provided on the lab page.



15. Once signed in, the key vault should auto-populate.



16. Click **Next >** **Next >** **Finish**.
17. Click to select the logged-in Azure user account.
18. The results should be fully encrypted columns.

The screenshot shows the 'Results' page of the Always Encrypted Wizard. The left sidebar lists steps: Introduction, Column Selection, Master Key Configuration, Run Settings, Summary, and Results. The 'Results' step is selected. The main area displays a summary table:

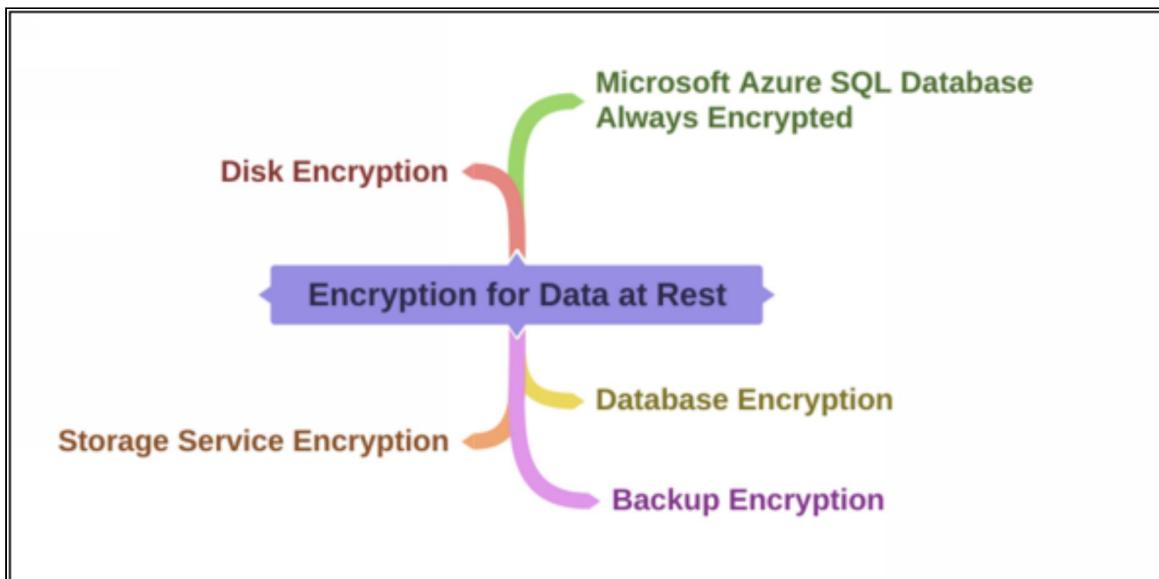
Task	Details
Generate new column master key CMK_Auto1 in Azure Key Vault samplevault9...	Passed
Generate new column encryption key CEK_Auto1	Passed
Performing encryption operations	Passed

A red box highlights the entire table. At the bottom of the main area, there is a link: [Always Encrypted Wizard Log Report](#).

Conclusion

Congratulations on successfully completing this hands-on lab!

Mind Map



Practice Questions

8. In which situation can we use Always Encrypted data protection technology to secure confidential data?
 - A. At rest on the server
 - B. During the transition between client and server
 - C. When the data is in use
 - D. All of the above
9. Always Encrypted is a _____ feature that is configured using the Always Encrypted Wizard in the SQL Server Management Studio (SSMS).
 - A. Client-level
 - B. Server-level
 - C. Administrator-level
 - D. All of the above
10. For encrypting entire databases or particular columns and rows inside the database, we can use Always Encrypted. True or false?
 - A. True
 - B. False
11. Which acronym is correct for TDE?
 - A. Transfer Data Encryption
 - B. Transparent Data Encryption
 - C. Transparent Database Encryption
 - D. Transit Database Encryption
12. Transparent Data Encryption (TDE) has been enabled by default on newly developed databases since June 2019. True or false?
 - A. True
 - B. False
13. Azure Storage automatically encrypts your data with _____.
 - A. Enable Always Encryption
 - B. Transparent Data Encryption
 - C. AES 256-bit Encryption
 - D. DES 56-bit Encryption

14. All Azure Storage account are encrypted irrespective of _____.
- A. Performance tier (standard or premium)
 - B. Access tier (hot or cool)
 - C. Deployment model (Azure Resource Manager or classic)
 - D. All of the above
15. Azure uses BitLocker disk encryption for Linux-managed disks and DM-Crypt disk encryption for Windows-managed disks. True or false?
- A. True
 - B. False
16. Backups in Azure are encrypted with _____.
- A. Enable Always Encryption
 - B. Transparent Data Encryption
 - C. DES 56-bit Encryption
 - D. AES 256-bit Encryption
17. Which Azure resource encryption requires a key vault and VMs to reside in the same Azure region and Azure subscriptions?
- A. Azure Disk Encryption
 - B. Database Encryption
 - C. Storage Service Encryption
 - D. Backup Encryption

Chapter 12: Final Steps

Introduction

This is the final chapter of the AZ-500 Microsoft Azure Security Technologies (LA) course. There is a lot of material that was covered in this course. Security may not always be very interesting thing but you did it and you should be very proud to have completed this course. Now, you should be ready to take the exam.

But before that, you should go through this lesson to understand the exam guidelines and practice the Exam Questions.

Course Completion and How to Prepare for the Exam

About the Exam

Length: 3 hours

Number of Questions: 40

Questions Type: Case study, Drag and drop, Exhibit, True or False, and Multiple choice

Exam Cost: \$165.00 USD

Register for the Exam

You can register for the exam through the following link.

<https://docs.microsoft.com/en-us/learn/certifications/exams/az-500>

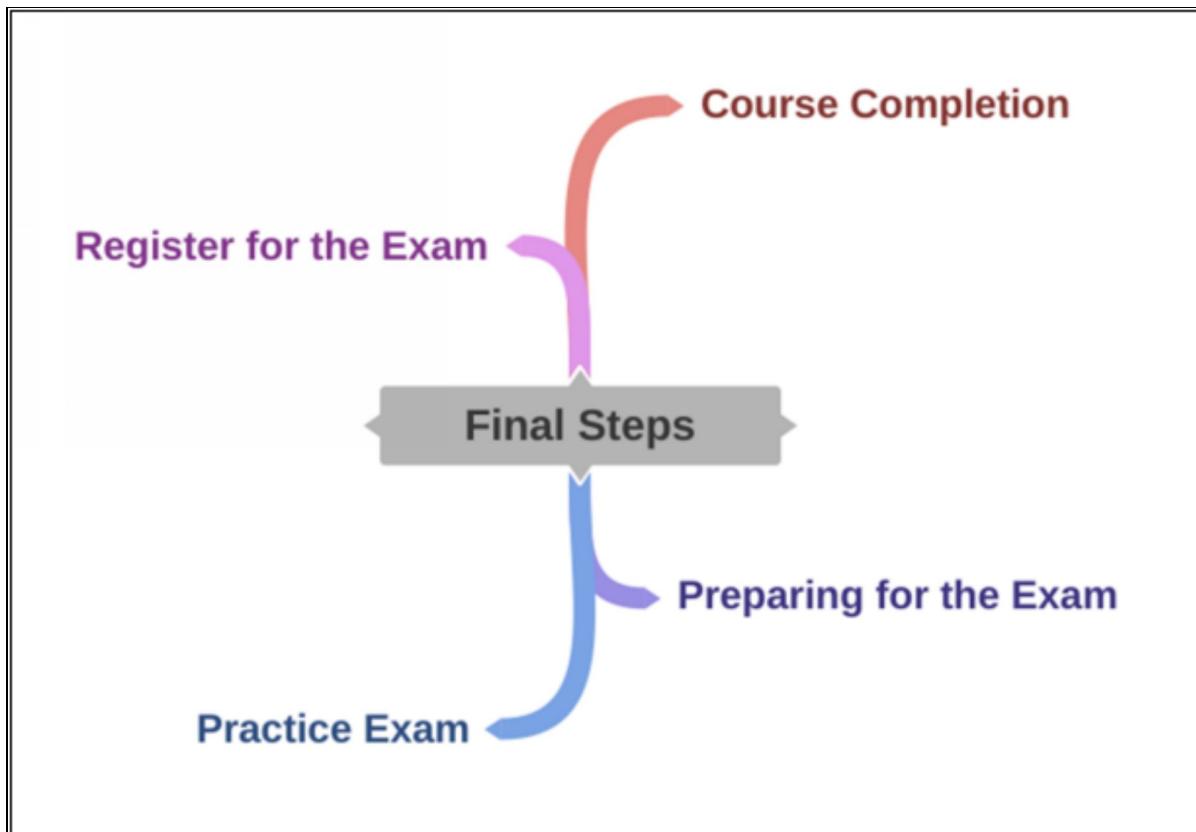
The exam can be taken at a local test center, at home, office, or a Pearson VUE test center. If you want to take a test at your own premises, you must have the requirements mentioned in the following link.

<https://docs.microsoft.com/en-us/learn/certifications/exams/az-500#certification-exams>

Preparing for the Exam

- Read and understand each and every thing present on all the lessons carefully
- Complete every hands-on lab at least twice
- Take the Practice exam questions that are present at the end of every lessons
- Memorize all the topics and create your own notes to increase memorization
- Review all the Exam tips and references mentioned in every lesson
- Participate in the Microsoft's expert forums related to AZ-500 exam
- Interact with the fellow candidates and share your knowledge

Mind Map



Answers:

Chapter 01: Introduction to Azure

1. **Answer: B (False)**

Explanation:

Consumption-based pricing is pricing based on usage of resource and it is not time based. It is not limited to free accounts and the services are not necessarily consumed all the time.

2. **Answer: C (Any hardware service provided by Azure such as Virtual Machines and**

Virtual Networks)

Explanation:

IaaS is the backbone of cloud computing, and in some way, all Azure services depend on IaaS. IaaS Azure services must never be purchased in advance, but may be used as required.

3. **Answer: A (Azure Log Analytics)**

Explanation:

It collects data from various sources and visualizes the data from sources like on-premise and cloud.

4. **Answer: C (Focus on business rather than provisioning and maintaining the resources)**

Explanation:

Instead of providing and managing services, Cloud Agility lets them concentrate on other issues such as security, monitoring, and analysis.

5. **Answer: A (True)**

Explanation:

In Azure, this is called Scalability, which means adding or removing the resources in an easy and quick way as per demand. It is important in such situations where you do not know the actual amount of the resource that is needed.

6. **Answer: D (High Availability)**

Explanation:

In this way, you get high availability for your servers by replacing the failed server instantly with the new one. HA depends on the number of VMs that you setup to eventually cover in case one goes down.

7. **Answer: C (OPEX is an ongoing cost for running a business. CAPEX is the cost of acquiring or maintaining assets)**

Explanation:

Capital Expenditure (CapEx) is the expenditure to maintain or acquiring fixed assets by spending money. This includes land, equipment, etc.

Operational Expenditure (OpEx) is the cost of a product or a system that is running on a day to day basis like electricity, printer papers, etc.

8. **Answer: A (One or more datacenters equipped with independent power, cooling, and networking)**

Explanation:

Availability Zones are locations within an Azure region that are physically separate. It is composed of one or more independently operating power, and network datacenters.

9. **Answer: B (3)**

Explanation:

Each region has a minimum of three zones.

10. **Answer: C (A set of datacenters close together)**

Explanation:

Regions are geographical areas where Azure is present to deploy the Azure resources. It is a set of data centers with latency-defined perimeter connected via a dedicated regional low-latency network.

11. **Answer: D (PaaS)**

Explanation:

PaaS is designed to facilitate the fast development of web or mobile apps for developers without the need to take concern over the setting or maintaining the underlying server, storage, network, and database infrastructure needed for development.

12. **Answer: B (False)**

Explanation:

VMs are Linux and Windows VM on demand with your desired configuration hosted in Azure. It is an IaaS resource.

13. **Answer: B (Resource Manager Template)**

Explanation:

Resource Manager Template is a JavaScript Object Notation (JSON) file that defines the resources deployed in the resource group. It also defines the dependencies between the deployed resources. With this template, resources can be deployed in a consistent and repeatable way.

14. **Answer: B (500GB)**

Explanation:

In Azure Storage, you can build a storage account for up to 500 TB of cloud data because it has a limit of 500TB per storage account.

15. **Answer: D (Azure Active Directory)**

Explanation:

It is a cloud based identity and access management service in Azure. It is one of the core services of Azure. With this service, the user can sign in and access the internal or external resources.

16. Answer: C (It rarely changes, and the commands stay the same for the most part)

Explanation:

In CLI, command changes rarely, so you can automate the commands for future purposes.

17. Answer: A (The Cloud Shell can be used entirely in a web browser and can be used across multiple devices)

Explanation:

An interactive browser, accessible shell for managing Azure resources. The shell experience is the best option, whether you work with Bash or PowerShell as it offers flexibility.

18. Answer: B (Credit will expire after 30 days and free resources expire after 12 months)

Explanation:

The limitation of free Azure Account is that you get free services for 12 months with credit expiration after 30 days.

19. Answer: D (A small lightweight group of commands to perform an action)

Explanation:

Most Azure features for PowerShell are made up of cmdlets. This simplifies the interaction with Azure resources to be consistent and efficient. It is a small lightweight group of commands to perform actions.

20. Answer: B (False)

Explanation:

You can use the Azure portal with any form of subscription to access all generally available Azure products and services.

Chapter 02: Configuration & Management of Azure AD for Workloads

1. **Answer: D** (All of the above)

Explanation:

You can manage your Azure AD user account by all three of them; Azure portal, Azure PowerShell and Azure CLI.

2. **Answer: B** (Domain name)

Explanation:

You cannot edit or modify your domain name. It is already created when you create your Microsoft Azure account.

3. **Answer: C** (Three)

Explanation:

You will see three types of membership when you create a group; Assigned, Dynamic User, and Dynamic Device.

4. **Answer: C** (Dynamic Device)

Explanation:

Dynamic Device is a type of membership which is only used for security group.

5. **Answer: C** (Hybrid identity)

Explanation:

Azure AD connect is a tool that provides hybrid identity. Hybrid identity is simply identity that exists on premises as well as on the cloud.

6. **Answer: B** (Federation)

Explanation:

Federation is the only authentication solution that allows to display password authentication

7. **Answer: A** (Federation)

Explanation:

Federation is the only authentication method which supports smart card authentication.

8. **Answer: D** (All of the above)

Explanation:

You can add all of the methods; password, biometrics, and device for multi-factor authentication.

9. **Answer: B** (Conditional access)

Explanation:

Access policies are the focus of conditional access. Policies are based on conditional and access controls.

10. **Answer: B** (Stolen user identity)

Explanation:

Stolen user identity is the main cause of security breaches.

11. Answer: B (Two)

Explanation:

Azure AD identity protection is designed to mitigate two types of risks; sign-in risk and user risk.

12. Answer: D (All of the above)

Explanation:

Types of risk events include Anonymous IP Addresses, Unfamiliar sign-in properties, and IP addresses link to malware.

13. Answer: C (Both of them)

Explanation:

Sign-in risk can be evaluated by two types; Sign-in risk (real time and aggregate).

14. Answer: A (MFA)

Explanation:

In Azure AD Identity Protection Configuration Steps, MFA configuration is optional but recommended.

15. Answer: B (Configuration of sign-in risk policy)

Explanation:

The last step in Azure AD Identity Protection configuration step is configuration of sign-in risk policy.

16. Answer: B (Global administrator)

Explanation:

To activate PIM, you must be a global administrator.

17. Answer: B (Roles)

Explanation:

You use Azure AD roles to add an eligible member to a privileged group

18. Answer: B (Approve requests)

Explanation:

Use Approve Requests to view and approve any requests for Azure AD or Azure resource privilege elevation.

19. Answer: C (Organizational account)

Explanation:

For PIM Activation, you must use an organizational account (not a personal account).

20. Answer: D (Privileged Identity Management)

Explanation:

Subscription-level roles and Azure Management Groups can be managed with PIM.

21 . Answer: A (Security tab)

Explanation:

To activate PIM, click on the Security tab.



Chapter 03: Azure Tenant Security

1. **Answer: B** (Azure Active Directory AD tenant)

Explanation: When you sign up for Azure, an Azure Active Directory (AD) tenant is created for you. Your account represents the tenant. To control access to your subscriptions and services, you use the tenant.

2. **Answer: B** (Authorization)

Explanation: Transferring billing ownership to another account provides authorization for billing activities to the administrators of the new account. They can change the mode of payment, view charges, and cancel the subscription.

3. **Answer: A** (Resources lose their access)

Explanation: When you transfer billing ownership of your subscription to an account in another Azure AD tenant, you can transfer the subscription to the new tenant account. If you do so, all users, groups, or service principals that had Azure role assignments to manage subscriptions and its resources lose their access.

4. **Answer: D** (All of the above)

Explanation: If you have accepted the billing ownership of an Azure subscription, it is recommended that you review these steps:

Update credentials related with this subscription's services containing:

- Management certificates that grant the user admin rights to subscription resources
- Access keys for services like Storage
- Remote Access credentials for services like Azure Virtual Machines

5. **Answer: B** (Monthly)

Explanation: Subscriptions to Visual Studio and Microsoft Partner Network have monthly recurring Azure credit associated with them.

6. **Answer: A** (True)

Explanation: Subscription transfer in the Azure portal is available for the following subscription types.

- Microsoft Partner Network
- Enterprise Agreement (EA)
- Visual Studio Enterprise (MPN) subscribers
- MSDN Platforms
- Pay-As-You-Go
- Pay-As-You-Go Dev/Test
- Visual Studio Enterprise
- Visual Studio Enterprise: BizSpark
- Visual Studio Professional
- Visual Studio Test Professional
- Microsoft Azure Plan2

Presently transfer is not supported for Free Trial or Azure in Open (AIO) subscriptions.

7. **Answer: A** (True)

Explanation: You cannot transfer subscriptions across countries or regions using the Azure portal, unfortunately. However, they can be transferred if you open an Azure

support request.

8. **Answer: B** (Azure Account)

Explanation: If the recipient does not have an Azure account, they must create one to accept the transfer.

9. **Answer: A** (True)

Explanation: You cannot transfer subscriptions across countries or regions using the Azure portal, unfortunately. However, they can be transferred if you open an Azure support request.

10. **Answer: C** (Role Based Access Control (RBAC))

Explanation: Azure Role Based Access Control (Azure RBAC) is the authorization system you use to manage access to Azure resources. To grant access, you assign roles to users, groups, service principals, or managed identities at a particular scope.

Chapter 04: Network Security

1. Answer: D (Azure Virtual Network)

Explanation: The basic building block for your private network in Azure is the Azure Virtual Network (VNet). VNet helps several types of Azure services to connect safely with each other, the internet, and on-premise networks, such as Azure Virtual Machines (VM). VNet is similar to a conventional network where you can run in your own data centre, but carries with it additional advantages such as size, availability, and isolation from Azure's infrastructure.

2. Answer: C (Similar)

Explanation: VNet is similar to a conventional network where you can run in your own data centre, but carries with it additional advantages such as size, availability, and isolation from Azure's infrastructure.

3. Answer: A (internal)

Explanation: The VNet has an internal address space like 10.1.0.0/16

4. Answer: B (Site-to-site VPN)

Explanation: Site-to-site VPN is created between your on-premises VPN device and the virtual network deployed by the Azure VPN Gateway. This form of connection allows any on-premises resource to access a virtual network that you allow.

5. Answer: A (Express Route)

Explanation: Developed by an ExpressRoute partner between your network and Azure. Such connection is confidential. Traffic is not linked to the internet.

6. Answer: A (VPN Gateway)

Explanation: Site-to-site VPN and Express Route routing connection requires Virtual Network Gateways to facilitate routing.

7. Answer: C (Network Security Group NSG)

Explanation: Network security groups are used to filter network traffic to and from Azure services on an Azure virtual network.

8. Answer: A (Security rules)

Explanation: A Network security group includes security rules that allow or deny different forms of Azure services to inbound or outbound network traffic from a network. You must define the source and destination, the port, and the protocol for each rule.

9. Answer: E (All of the above)

Explanation: A Network security group includes security rules that allow or deny different forms of Azure services to inbound or outbound network traffic from a network. You must define the source and destination, the port, and the protocol for each rule.

10. Answer: C (Both)

Explanation: NSGs can be applied to either a Network Interface Cards (NIC), a subnet, or both.

11. Answer: A (Application Security Groups)

Explanation: An Application Security Groups (ASGs) is a logical collection of virtual machines, specifically their Network Interface Cards (NICs). You join the ASG virtual

machines and then use the application security group in the NSG rules as a source or destination.

12. Answer: C (NSG rules)

Explanation: An Application Security Groups (ASGs) is a logical collection of virtual machines, specifically their Network Interface Cards (NICs). You join the ASG virtual machines and then use the application security group in the NSG rules as a source or destination.

13. Answer: B (VNet-to-VNet)

Explanation: VPN Gateway is designed for VNet-to-VNet connectivity.

14. Answer: C (Both)

Explanation: VPN Gateway and VNet Peering connectivity supports cross-region VNet connectivity

15. Answer: A (Virtual Network)

Explanation: This tag defines all CIDR ranges in the virtual network.

16. Answer: C (AzureFirewallSubnet)

Explanation: The "default" subnet name is the default name of the first subnet in a virtual network. It is not used for Azure Firewall. This subnet name is required for the deployment of the Azure Firewall.

17. Answer: C (Both)

Explanation: Azure Storage Accounts and Azure SQL server databases are the most common resources with this enhanced protection.

Chapter 5: Securing VMs & Other Azure Resources

1. **Answer: D (All of the above)**

Explanation:

Microsoft Antimalware for Azure is a free real-time protection service that helps identify and remove viruses, spyware, and other malicious software.

2. **Answer: D (All of the above)**

Explanation:

Microsoft Antimalware for Azure is free, easy to deploy, and fully featured.

3. **Answer: A (Extensions)**

Explanation:

You can configure and deploy Microsoft Antimalware using Azure extensions.

4. **Answer: C (Both of them)**

Explanation:

You can use your Azure update management portal to deploy and update new or existing VMs.

5. **Answer: B (Security Center)**

Explanation:

You can configure and deploy Microsoft Antimalware using Azure Security Center.

6. **Answer: A (Granular)**

Explanation:

Role-based access control (RBAC) is used to provide granular access to Azure resources.

7. **Answer: D (All of them)**

Explanation:

These roles can be assigned at the subscription, resource group, or resource level.

8. **Answer: D (All of the above)**

Explanation:

Roles are assigned to an Azure AD user, group, or service principal.

9. **Answer: B (Two)**

Explanation:

There are two types of Azure resource locks: CanNotDelete and ReadOnly.

10. **Answer: B (ReadOnly)**

Explanation:

ReadOnly means authorized users can read a resource, but they cannot delete or update it.

11. Answer: C (Both of them)**Explanation:**

Unlike role-based access control, resource locks apply a restriction across all users and roles.

12. Answer: D (All of the above)**Explanation:**

Azure management groups allow us to group subscriptions to manage access, policies, and compliance.

13. Answer: A (Tenant Root Group)**Explanation:**

When using management groups, the first group is called the Tenant Root Group and is used to manage all subscriptions.

14. Answer: D (All of the above)**Explanation:**

Azure Policy is a service in Azure you use to create, assign, and manage policies

15. Answer: A (Policies)**Explanation:**

Assignments determine where policies are applied. It can be applied to Azure subscriptions and optionally to child resource groups.

Chapter 6: Container Security

1. Answer: A & B (CanNotDelete & ReadOnly)

Explanation: CanNotDelete is one of the resource locks available. CanNotDelete allows changes, but not deletions, to an Azure resource.

ReadOnly is one of the resource locks available in Azure. ReadOnly prohibits all changes to an Azure resource.

2. Answer: B (az acr login --name <acrName>)

Explanation: az acr login --name <acrName> is the required CLI command to authenticate against an Azure Container Registry.

3. Answer: B (Azure Container Registry)

Explanation: Azure Container Registry is a containerized service that allows us to build, store, and manage images for all types of container deployment. It is a managed Docker registry service based on an open-source Docker Registry.

4. Answer: D (All of the above)

Explanation: You can create a container registry with Azure portal, Azure CLI, and Azure PowerShell.

5. Answer: D (All of the above)

Explanation: The three main available roles for a container registry include:

AcrPull: This allows you to pull an image from a private registry

AcrPush: This allows you to pull and push images to the registry

Owner: This allows you to pull, push, and assign roles to other users

6. **Answer: B & C (AcrPush & Owner)**

Explanation: The three main available roles for a container registry include:

AcrPull: This allows you to pull an image from a private registry

AcrPush: This allows you to pull and push images to the registry

Owner: This allows you to pull, push, and assign roles to other users

7. **B (Two)**

Explanation: Two keys are provided to the admin account, each of which can be regenerated. By using one password while regenerating the other, two passwords allow you to retain a connection to the register.

8. **Answer: A (True)**

Explanation: To enable VNet/Firewall secure feature, we have to change the SKUs of our container registry from basic to premium.

9. **Answer: A (Azure Container Instances)**

Explanation: The fastest and easiest way to run a container in Azure is provided by Azure Container Instances, without having to manage any virtual machines and without attempting to adopt a higher-level service.

10. **Answer: C (ACR Tasks)**

Explanation: ACR Tasks is a collection of features within Azure Container Registry. It provides cloud-based container image building for Linux, Windows, and ARM. It can also automate OS and framework patching for Docker containers.

11. **Answer: B (Content Trust)**

Explanation: The Azure Container Registry allows signed images to be pushed and pulled implements Docker's content trust model.

12. **Answer: B (Fully qualified domain name (FQDN))**

Explanation: When you create a container instance in Azure, the fully qualified domain name (FQDN) identifies the exact location of your container in the Domain Name System (DNS).

13. **Answer: A (Container)**

Explanation: Container is the standardized unit of software that contains the package of code and configurations for a specific application. The container allows us to break the unchanged applications into several parts of the service that make up the solution. This approach enables you to manage, develop, and deploy these parts of the service using a container.

14. **B (Azure Kubernetes)**

Explanation: Kubernetes is the open-source platform for working with containers. It gives you the means to do deployments, an easy way to scale, and monitoring of the containerized workloads. With Kubernetes, there is no need to configure the complex containers. The Kubernetes service allows you to use a global configuration method to organize the container in different computing environments.

15. A (Master)

Explanation: The master components of Kubernetes are part of the managed service offered by Microsoft. Each AKS cluster has its own single-tenanted, dedicated Kubernetes master to provide the API Server, Scheduler, etc. Microsoft is responsible to manage and maintain this master security.

Chapter 7: Configuring Security Services

1. Answer: D (Azure Monitor)

Explanation: Azure Monitor is designed to collect, analyze, and act on telemetry from our cloud and on-premises resources.

2. Answer: A (Monitoring)

Explanation: Monitoring is the process of collecting and analyzing data in order to evaluate our business application's performance, health, and availability and the resources it depends upon.

3. Answer: B (Two)

Explanation: There are two different types of diagnostic logs; Tenant logs and Resource logs.

4. Answer: B (Tenant logs)

Explanation: Tenant logs originate from tenant-level services such as Azure Active Directory.

5. Answer: C (Resource logs)

Explanation: Resource logs originate from individual resources by themselves within an Azure subscription, such as Virtual machines, Network security groups, or Storage accounts.

6. Answer: C (Analyze them with Azure Monitor)

Explanation: Analyzing them with Azure Monitor would be the perfect solution because Azure Monitor is a centralized logging and monitoring station.

7. Answer: C (Action Groups)

Explanation: Azure Monitor sends out its alerts to Action Groups.

Chapter 8: Security Policies & Alerts

- Answer: B (Just-In-Time VM Access)**

Explanation:

Just In Time (JIT) Virtual Machine Access allows you to lock down access to your Azure virtual machines.

- Answer: B (Security Center)**

Explanation:

Azure Security Center standard is required to configure this JIT feature.

- Answer: A (Resource Manager)**

Explanation:

Security Center JIT VM access currently supports only VMs deployed through Azure Resource Manager.

- Answer: A (Alerts)**

Explanation:

Alerts notify you of potential anomalies in Azure environment.

- Answer: B (Recommendations)**

Explanation:

The recommendations are based on best practices and trusted security advisories.

- Answer: A (Playbooks)**

Explanation:

Playbooks can help you craft and execute automated responses to security alerts.

Chapter 09: Data Management & Security for Data Infrastructure

1. Answer: A (AIP)

Explanation:

AIP is a cloud-based rights management solution that helps your organization classify and protect documents and emails.

2. Answer: A (Labels)

Explanation:

Classification is achieved by applying Labels.

3. Answer: B (AIP)

Explanation:

Azure Active Directory Premium P1 or P2 licenses are required to use AIP.

4. Answer: B (General)

Explanation:

Data labelled 'General' is not protected and can be distributed inside and outside of an organization.

5. Answer: C (Both of them)

Explanation:

Labels can be applied manually to a piece of data or can be applied automatically based on conditions, such as the data format.

6. Answer: A (Azure Key Vault)

Explanation:

Azure Key Vault helps safeguard and manage keys for cryptography and secrets.

7. Answer: B (Access Policy)

Explanation:

Access to Azure Key Vault is controlled by an access policy.

8. Answer: D (RBAC)

Explanation:

RBAC is also used to determine access to the Key Vault resource.

9. Answer: D (All of the above)

Explanation:

Azure SQL databases, managed instances, and data warehouses use local user accounts for authentication.

10. Answer: D (All of the above)

Explanation:

Logging can be configured using the Azure Portal, PowerShell, the REST API, or ARM templates.

11. Answer: B (Two)

Explanation:

Azure Cosmos DB uses two types of keys to authenticate users and provide access to its data and resources.

1. Answer: C (Web Application Firewall)

Explanation: Web Application Firewall (WAF) is an Application Gateway feature that provides web applications with centralized protection against common exploits and vulnerabilities. WAF is based on rules from the Open Web Application Security Project (OWASP) core rule sets 3.0 or 2.2.9.

2. Answer: B (PaaS Application)

Explanation: Implementing security validations for application development is an impressive way of explaining how to secure your Platform-as-a-Service or PaaS applications.

3. C (Azure Active Directory)

Explanation: Azure Active Directory, a robust cloud solution for identity and access management, helps secure access to data in on-premises and cloud applications and simplifies user and group management.

4. Answer: D (Azure AD conditional access)

Explanation: Azure AD conditional access allows us to implement additional security measures based on location and sign-in risk.

5. Answer: B (Azure Application Insights)

Explanation: Azure Application Insights can be used to monitor availability, performance, and usage of your application, whether it is hosted in the cloud or on-premises.

6. Answer: A (Microsoft Security Risk Detection)

Explanation: Make penetration testing a standard part of our design and deployment process. Microsoft Security Risk Detection is a cloud-based tool that we can use to look for bugs and other security vulnerabilities in the software before deploying it to Azure.

7. Answer: D (All of the above)

Explanation: There are three types of availability tests included in Synthetic Security Transactions:

- URL ping test
- Multi-step web test
- Custom Track Availability Tests

8. Answer: A & C (SSL certificates) & (App Service plan tier)

Explanation: We can use private and public SSL certificates to secure communication on Azure Web Apps. App services hosted on App service plans using the Basic, Standard, Premium, or isolated tiers are required to use custom SSL certificates, and the free tier is not eligible to do so.

9. Answer: A & B (URL-based) & (Multi-site hosting)

Explanation: With an application gateway, we can configure URL-based routing and multi-site hosting, along with other functionality to improve the availability of web applications.

10. Answer: D (Application Gateway)

Explanation: Application Gateways provide network load balancing and traffic management for Azure virtual machines, virtual machine scale sets, and app services.

Chapter 11: Encryption for Data at Rest

1. D (All of the above)

Explanation: In the Azure SQL Database and SQL Server, Always Encrypted is a data protection technology that helps secure confidential data at rest on the server, during the transition between client and server, and when the data is in use.

2. A (Client-level)

Explanation: Always Encrypted is a client-level feature; it is configured using the Always Encrypted Wizard in the SQL Server Management Studio (SSMS).

3. A (True)

Explanation: Always Encrypted is a client-level feature; it is configured using the Always Encrypted Wizard in the SQL Server Management Studio (SSMS). For encrypting entire databases or particular columns and rows inside the database, we can use Always Encrypted.

4. B (Transparent Data Encryption)

Explanation: At present, the SQL feature called Transparent Data Encryption (TDE) offers support for server encryption.

5. B (False)

Explanation: Transparent Data Encryption (TDE) has been enabled by default on newly developed databases by June 2017.

6. C (AES 256-bit Encryption)

Explanation: Azure Storage automatically encrypts your data with 256-bit AES encryption, one of the strongest block ciphers available.

7. D (All of the above)

Explanation: All Azure Storage accounts irrespective of performance tier (standard or premium), access tier (hot or cool), or deployment model (Azure Resource Manager or classic) are encrypted.

8. B (False)

Explanation: Azure uses BitLocker disk encryption for Windows managed disks and DM-Crypt disk encryption for Linux-managed disks.

9. D (AES 256-bit Encryption)

Explanation: Backups in Azure are encrypted with AES-256 encryption and are transmitted to the Azure Backup vault using secure HTTPS communication.

10. A (Azure Disk Encryption)

Explanation: Azure Disk Encryption requires that your key vault and VMs reside in the same Azure region and Azure subscriptions.

Acronyms:

AAD	Additional Authenticated Data
ACL	Access Control List
ACM PCA	AWS Certificate Manager Private Certificate Authority
ACM	AWS Certificate Manager
AD	Active Directory
ADM	Amazon Device Messaging
AMI	Amazon Machine Image
API	Application Program Interface
APN	AWS Partner Network
APNS	Apple Push Notification Service
ARN	Amazon Resource Name
ASN	Autonomous System Number
AUC	Area Under a Curve
AWS	Amazon Web Service
AZ	Availability Zone
BGP	Border Gateway Protocol
BLOB	Binary Large Object
CDN	Content Delivery Network
CGW	Customer Gateway
CIDR	Classless Inter-Domain Routing
CIFS	Common Internet File System
CLI	Command Line Interface
CMK	Customer Master Key
CNAME	Canonical Name
CPU	Central Processing Unit
DB	Database
DBA	Database Administrator
DDoS	Distributed Denial of Service
DKIM	DomainKeys Identified Mail
DNS	Domain Name System
DoS	Denial of Service
DR	Disaster Recovery
DRT	DDoS Response Team
EBS	Elastic Block Store
EC2	Elastic Cloud Compute
ECR	Elastic Container Registry
ECS	Elastic Container Service
EFS	Elastic File Storage
ELB	Elastic Load Balancer
EMR	Elastic Map Reduce
ENA	Elastic Network Adapter
ES	Elasticsearch Service

ETL	Extract, Transform, and Load
FBL	Feedback Loop
FIM	Federated Identity Management
FS	Federation Service
GCM	Google Cloud Messaging
GUI	Graphical User Interface
HMAC	Hash-based Message Authentication Code
HPC	High Performance Computing
HSM	Hardware Security Module
HTTP	Hyper Text Transfer Protocol
I/O	Input/output
IAM	Identity and Access Management
IdP	Identity Provider
IDS	Intrusion Detection System
IGW	Internet Gateway
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
ISP	Internet Service Provider
JCE	Java Cryptography Extensions
JDBC	Java Database Connectivity
JSON	JavaScript Object Notation
KMS	Key Management Service
LAN	Local Area Network
MFA	Multi Factor Authentication
MIME	Multipurpose Internet Mail Extensions
MPNS	Microsoft Push Notification Service for Windows Phone
MTA	Mail Transfer Agent
MTU	Maximum Transmission Unit
NACL	Network Access Control List
NAS	Network Attached Storage
NFS	Network File System
OCID	Open ID Connect
ODBC	Open Database Connectivity
OLAP	Online Analytical Processing
OS	Operating System
OU	Organizational Unit
PPS	Packets Per Second
Pub/Sub	Publisher/Subscriber
RDS	Relational Database Service
RI	Reserved Instance
RTMP	Real Time Messaging Protocol
S3	Simple Storage Service
SAML	Security Assertion Markup Language
SAN	Storage Are Network
SCP	Service Control Policies
SDK	Software Development Kit

SES	Simple Email Service
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SNI	Server Name Indication
SNS	Simple Notification Service
SOAP	Simple Object Access Protocol
SOC	Security Operations Center
SQS	Simple Queue Service
SRE	Site Reliability Engineers
SR-IOV	Single Root I/O Virtualization
SSD	Solid State Drive
SSE	Server Side Encryption
SSL	Secure Sockets Layer
SSO	Single Sign-On
STS	Security Token Service
SWF	Simple Workflow Service
TB	TeraByte
TLS	Transport Layer Security
TTL	Time to Live
URL	Uniform Resource Locator
VERP	Variable Envelope Return Path
VFI	Virtual Function Interface
VPC	Virtual Private Cloud
VPG	Virtual Private Gateway
VPN	Virtual Private Network
WAF	Web Application Firewall
WAM	WorkSpaces Application Manager
WPNS	Windows Push Notification Service
WSDL	Web Services Description Language

References:

- <https://azure.microsoft.com/en-gb/global-infrastructure/regions/>
- <https://docs.microsoft.com/en-us/learn/paths/azure-fundamentals/>
- <https://searchcloudcomputing.techtarget.com/definition/Windows-Azure>
- <https://searchcloudcomputing.techtarget.com/definition/cloud-computing>
- <https://azure.microsoft.com/en-us/global-infrastructure/locations/>
- <http://www.azurespeed.com/Information/AzureRegions>
- <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/overview>
- <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/resource-providers-and-types>
- <https://azure.microsoft.com/en-us/product-categories/compute/>
- <https://docs.microsoft.com/en-us/learn/modules/welcome-to-azure/3-tour-of-azure-services>
- <https://azure.microsoft.com/en-us/product-categories/networking/>
- <https://www.dataversity.net/key-cloud-agility/>
- <https://docs.microsoft.com/en-us/azure/storage/common/storage-introduction#types-of-storage-accounts>
- <https://docs.microsoft.com/en-us/cli/azure/get-started-with-azure-cli?view=azure-cli-latest>
- <https://docs.microsoft.com/en-us/cli/azure/install-azure-cli?view=azure-cli-latest>
- <https://docs.microsoft.com/en-us/azure/app-service/security-baseline>
- <https://docs.microsoft.com/en-us/azure/security/develop/secure-deploy>
- <https://docs.microsoft.com/en-us/azure/security/fundamentals/overview>

<https://docs.microsoft.com/en-us/azure/security/fundamentals/paas-deployments>

<https://docs.microsoft.com/en-us/azure/azure-monitor/overview>

<https://www.pluralsight.com/courses/microsoft-azure-configuring-security-services-policies>

<https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/log-analytics-overview>

<https://www.mcafee.com/enterprise/en-us/security-awareness/cloud/what-is-a-container.html>

<https://docs.microsoft.com/en-us/azure/container-registry/container-registry-intro>

<https://docs.microsoft.com/en-us/azure/container-registry/container-registry-get-started-portal>

<https://docs.microsoft.com/en-us/azure/container-registry/container-registry-get-started-powershell>

<https://docs.microsoft.com/en-us/azure/container-registry/container-registry-authentication>

<https://docs.microsoft.com/en-us/azure/container-instances/container-instances-overview>

<https://docs.microsoft.com/en-us/azure/container-instances/container-instances-container-groups>

<https://docs.microsoft.com/en-us/azure/aks/concepts-security>

<https://docs.microsoft.com/en-us/azure/container-registry/container-registry-tasks-overview>

<https://docs.microsoft.com/en-us/azure/container-registry/container-registry-auth-service-principal>

<https://learn.acloud.guru/course/6ca00157-fca5-4cfa-b6ec-1c749a1d359f/learn/73a13bc7-0e3b-49a6-af9a-269425724ac7/7206ea7d-12c1-44c4-a5a0-3de89ec10ba6/watch>

<https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/billing-subscription-transfer>

<https://docs.microsoft.com/en-us/azure/cost-management-billing/understand/subscription-transfer>

About Our Products

Other products from IPSpecialist LTD regarding AWS technology are:



AWS Certified Cloud Practitioner Technology Workbook



AWS Certified SysOps Admin - Associate Workbook



AWS Certified Solution Architect - Associate Technology Workbook



AWS Certified Developer Associate Technology Workbook



AWS Certified Advance Networking – Specialty Technology Workbook



AWS Certified Security – Specialty Technology Workbook



AWS Certified Big Data – Specialty Technology Workbook



Microsoft Certified: Azure Fundamentals



Microsoft Certified: Azure Administrator



Microsoft Certified: Azure Solution Architect



Microsoft Certified: Azure IoT Developer



Microsoft Certified: Azure DevOps Engineer

Note from the Author:

Reviews are gold to authors! If you have enjoyed this book and it has helped you along your certification, would you consider rating and reviewing it?

Link to Product Page: