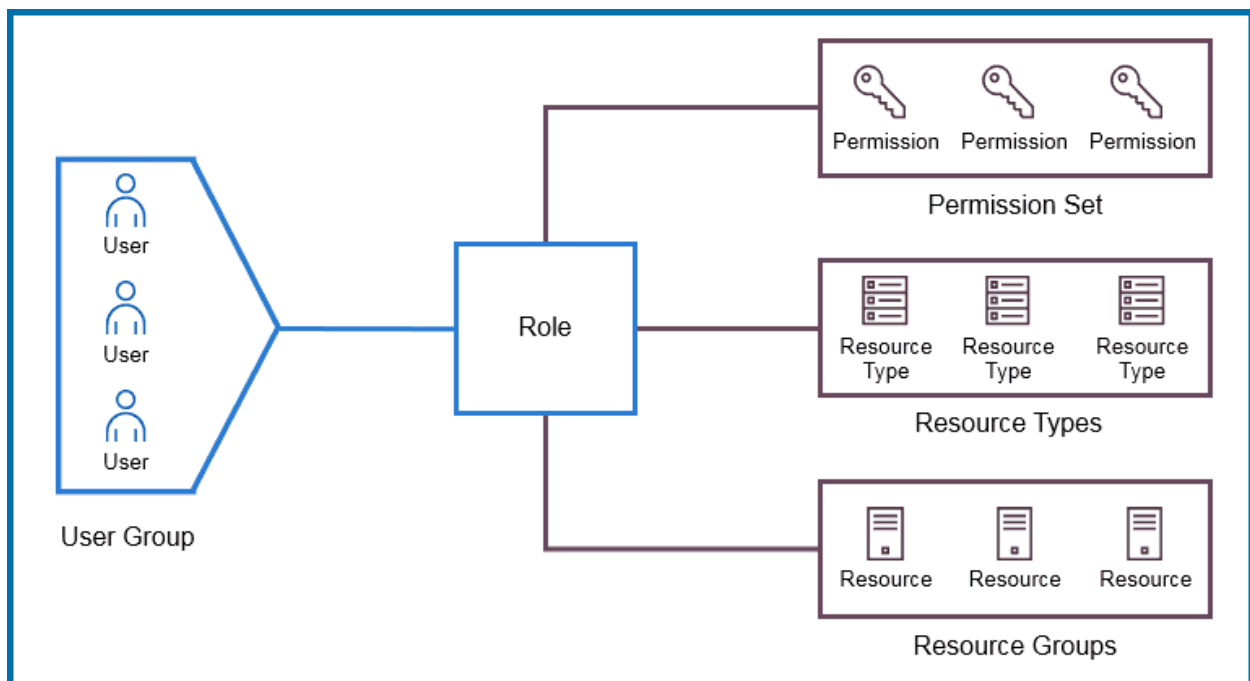


# Microsoft Azure Security Technologies: Step By Step Activity Guides (Hands-On Labs)

Activity Guides:

## 1) Role-Based Access Control

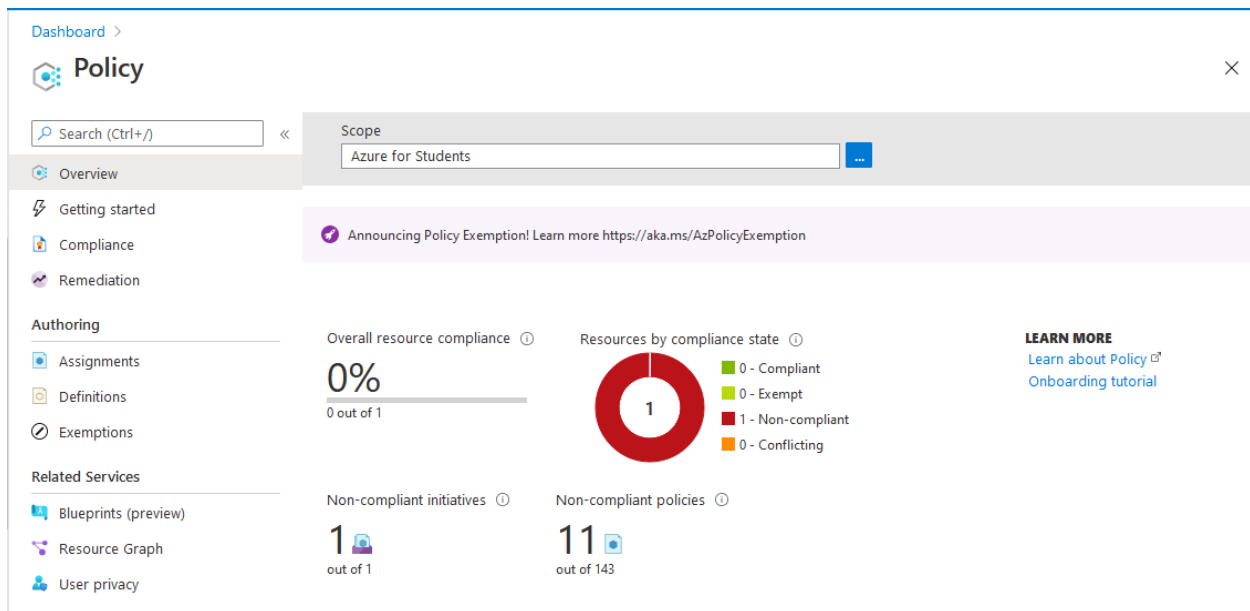
Here, you need to create a user group and users and provide role-based access to specific users/user groups. Role-based access control is an approach that's used for restricting access to users and applications on the system/network. This approach is widely used in today's market for security and access control.



## 2) Azure Policy

Azure Policy basically restricts resource creation in a specific location and it can also be used in more depth also.

Here, you need to create an Azure Policy to restrict resource creation in specific regions and test your policy, also.



### 3) Resource Manager Locks

Resource Manager Locks are used by admins to lock Azure Resources to prevent accidental changes or deletion of the resources by users while testing or doing some work.

Here, you need to create locks on specific resource groups to avoid accidental changes or deletion.

Dashboard > CreateVm-Canonical.UbuntuServer-18.04-LTS-20201231142619 >

Deom Virtual machine

Search (Ctrl+/) Connect Start Restart Stop Capture Delete Refresh Open in mobile

Size

Security

Advisor recommendations

Extensions

Continuous delivery

Availability + scaling

Configuration

Identity

Properties

**Locks**

Operations

Bastion

JSON View

Essentials

Resource group (change) k21

Status Running

Location North Europe

Subscription (change) Azure for Students

Subscription ID 5230f109-b5ca-43d9-9b4a-3979fbdef9b6

Tags (change) Click here to add tags

Operating system Linux (ubuntu 18.04)

Size Standard D2s v3 (2 vcpus, 8 GiB memory)

Public IP address 40.85.129.11

Virtual network/subnet k21-vnet/default

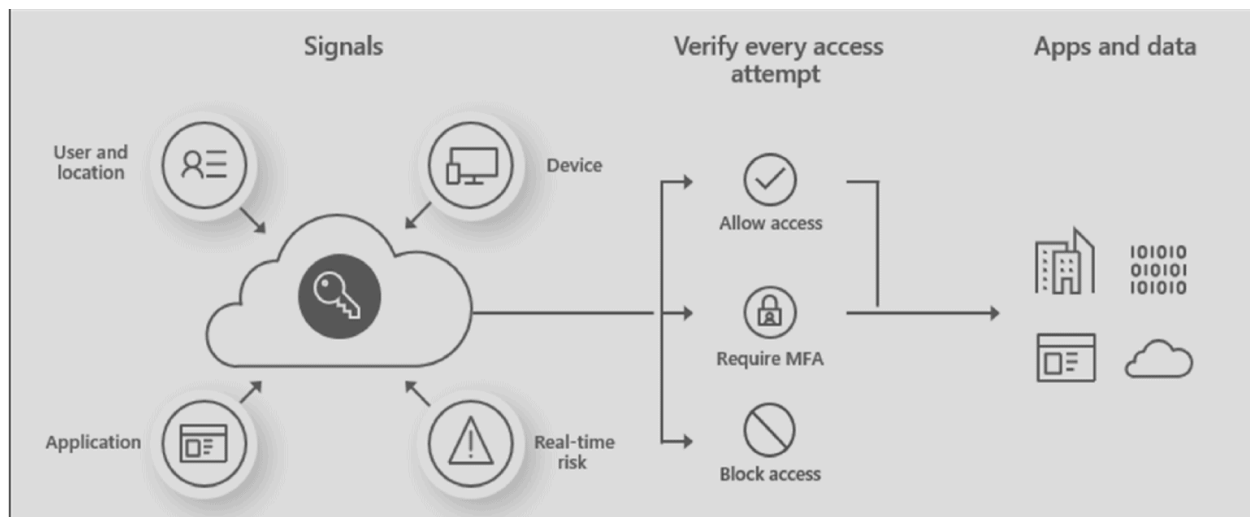
DNS name Configure

Properties Monitoring Capabilities (7) Recommendations Tutorials

#### 4) MFA, Conditional Access, and AAD Identity Protection

Multi-Factor Authentication is one of the very crucial steps for any organization that wants to implement a higher level of security. In Azure, Conditional Access and Azure Active Directory Identity Protection is used for the purpose of MFA.

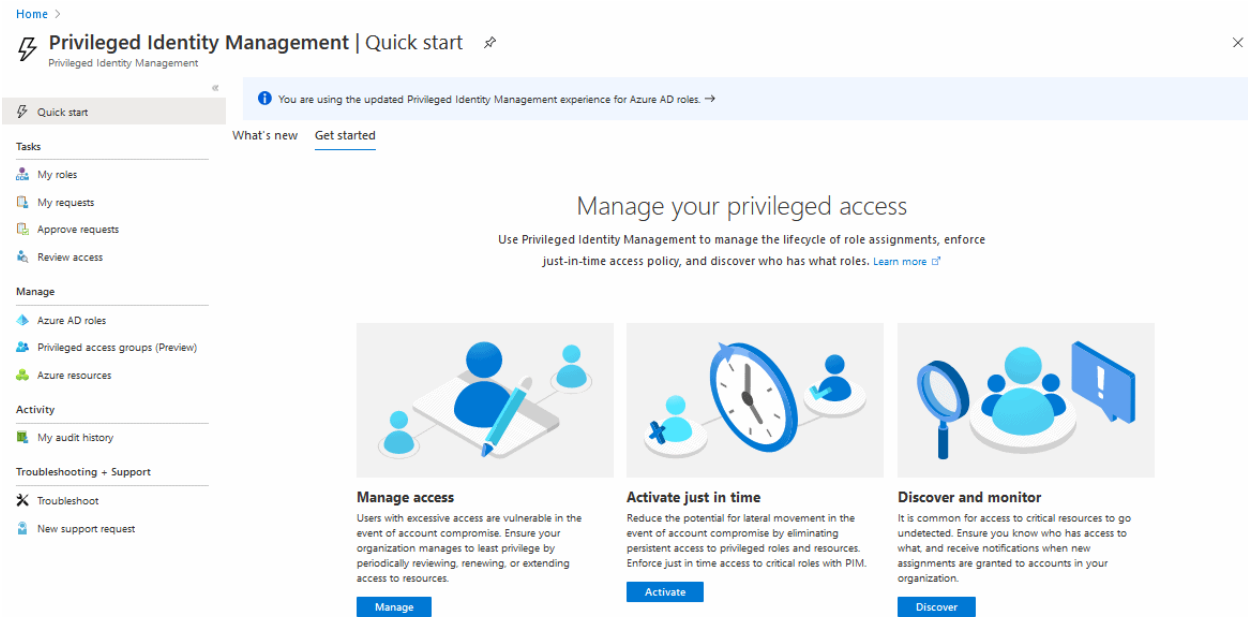
Here, you need to create a VM and then implement Multi-Factor Authentication that will use Azure Active Directory Services for Authentication.



#### 5) Azure AD Privileged Identity Management

Azure AD Privileged Identity Management service allows Admins to manage and control user access to high-level resources of the organization.

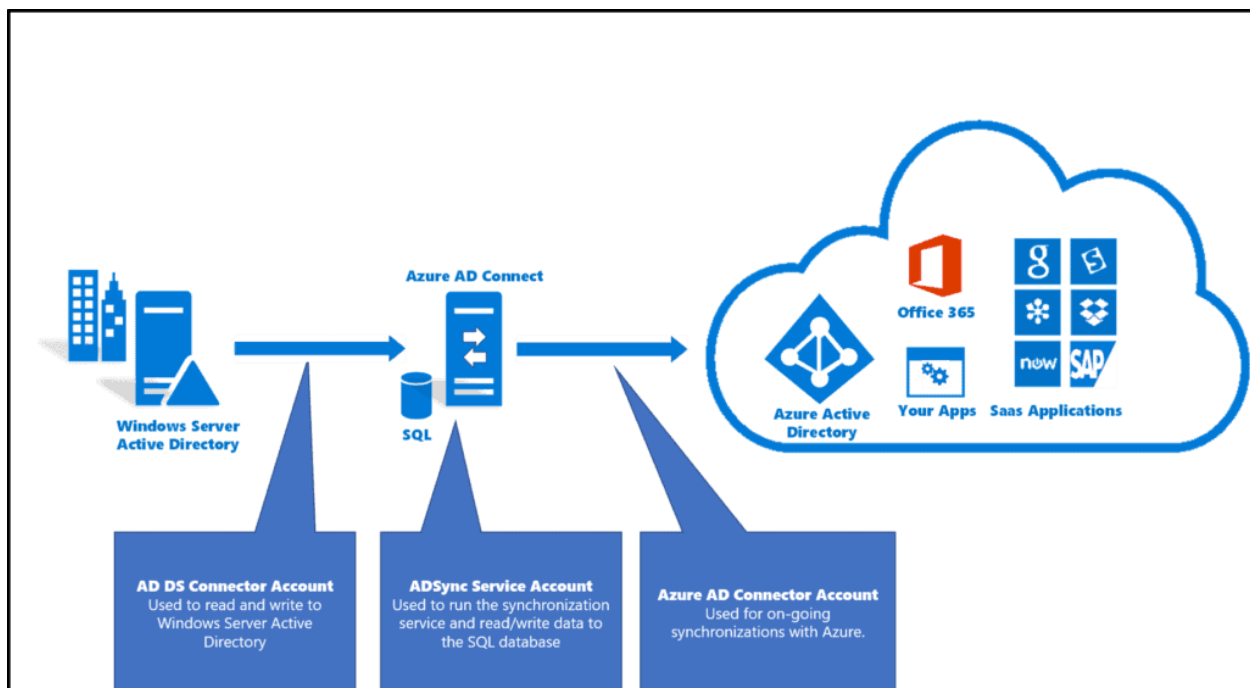
In this Activity Guide, you'll create resources in Azure and then implement access restrictions on users for accessing the resources.



## 6) Implement Directory Synchronization

Azure Directory Synchronization is a tool that allows users to Manage Identities of Azure Active Directory and also to manage all the updates of user accounts, groups, and contacts that are synced to the Azure Active Directory Tenant.

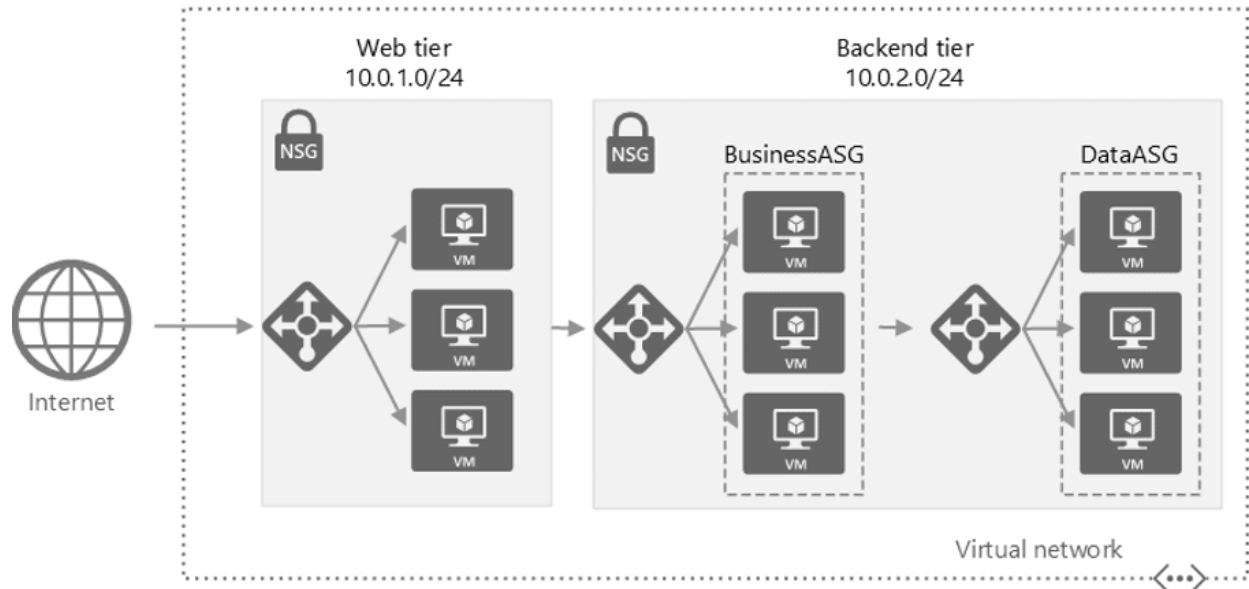
In this Activity Guide, you will work with Active Directory Domain Services where you will be creating an Azure Domain Forest and Creating an Azure Active Directory Tenant and synching them.



## 7) Network Security Groups and Application Security Groups

Network Security Groups is used in an organization to filter the network traffic flow of an Azure Virtual Network. NSG's have security rules in them that can be used to restrict inbound/outbound traffic from different kinds of Azure Services.

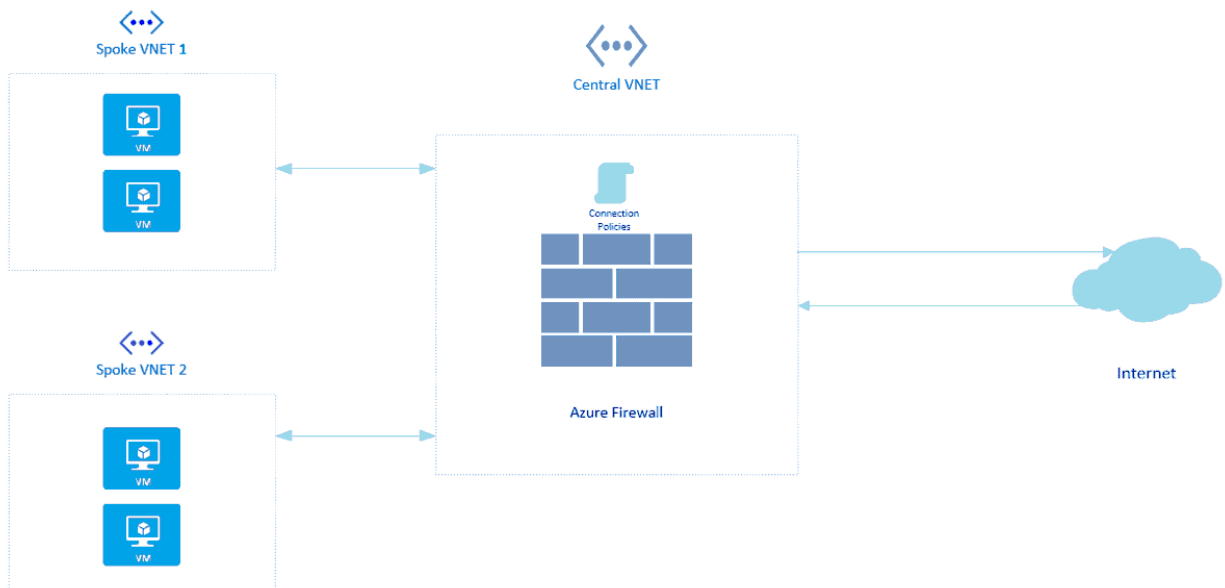
In this Activity Guide, you'll have to configure the Network Security Group rule for a group of Servers to perform to RDP.



## 8) Azure Firewall

Azure Firewall is a cloud-based network security service in Azure. Azure Firewall protects our Virtual Network Resources and this is a built-in service.

Here, you'll be Configuring Azure Firewall to control inbound and outbound network access of your organization.



## 9) Configuring and Securing ACR and AKS

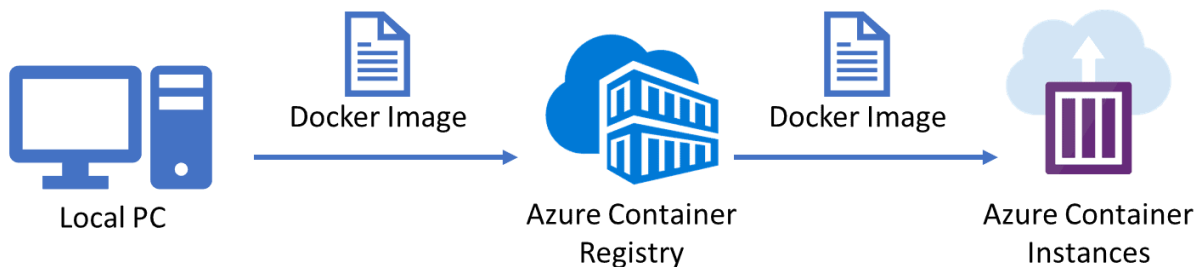
**Azure Container Registry (ACR)** is a managed, private Docker registry service based on the open-source Docker Registry 2.0. Create and maintain Azure container registries to store and manage your private Docker container images and related artifacts.

There are security benefits to working with ACR. Firstly, it provides signed container images, so your Kubernetes cluster can verify that the code it's running is the code you pushed to your registry from your build system.

You can log in to a registry using the Azure CLI or the standard docker login command. Azure Container Registry transfers container images over HTTPS, and supports TLS to secure client connections.

**Azure Kubernetes Service (AKS)** is a fully-managed service that allows you to run Kubernetes in Azure without having to manage your own Kubernetes clusters. Azure manages all the complex parts of running Kubernetes, and you can focus on your containers.

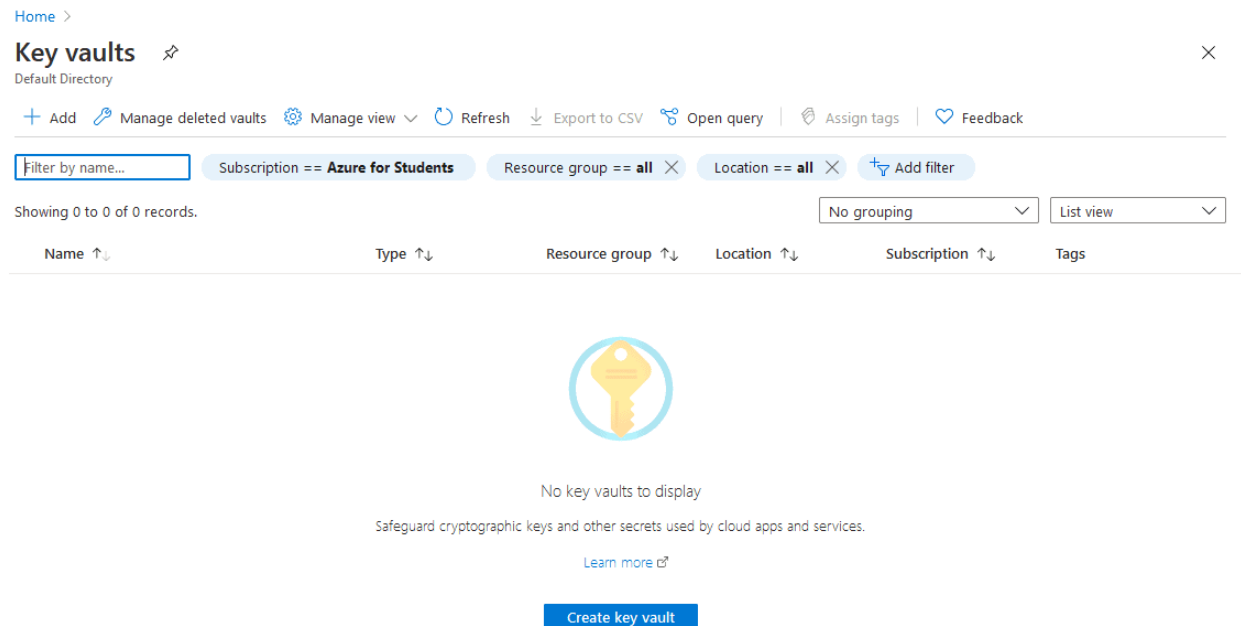
For improved security and management, AKS lets you integrate with Azure AD to use Kubernetes role-based access control (Kubernetes RBAC).



## 10) Key Vault (Implementing Secure Data by setting up Always Encrypted)

Azure Key Vault as the name suggests is a service provided by Azure Cloud to store all the keys, passwords, and certificates.

Always Encrypted is a data encryption technology that ensures that sensitive data remains always encrypted and never show as plaintext in a database, whether it's at rest, moving between client and server or it's in use.









## 11) Securing Azure SQL Database


In this Activity Guide, we will help you to Secure an Azure SQL Database by creating rules in Azure Firewall to prevent various attacks such as SQL Injection and Data Exfiltration.

Home >

## SQL databases

Default Directory


 Add
  Reservations
  Edit columns
  Refresh
  Assign tags
  Delete

 Try our new Azure SQL resource browser! This experience offers a unified view of all your SQL Server resources in Azure as well as improved sorting and filtering. Click here to go to the new experience.

**Subscriptions:** 1 of 2 selected – Don't see a subscription? [Open Directory + Subscription settings](#)

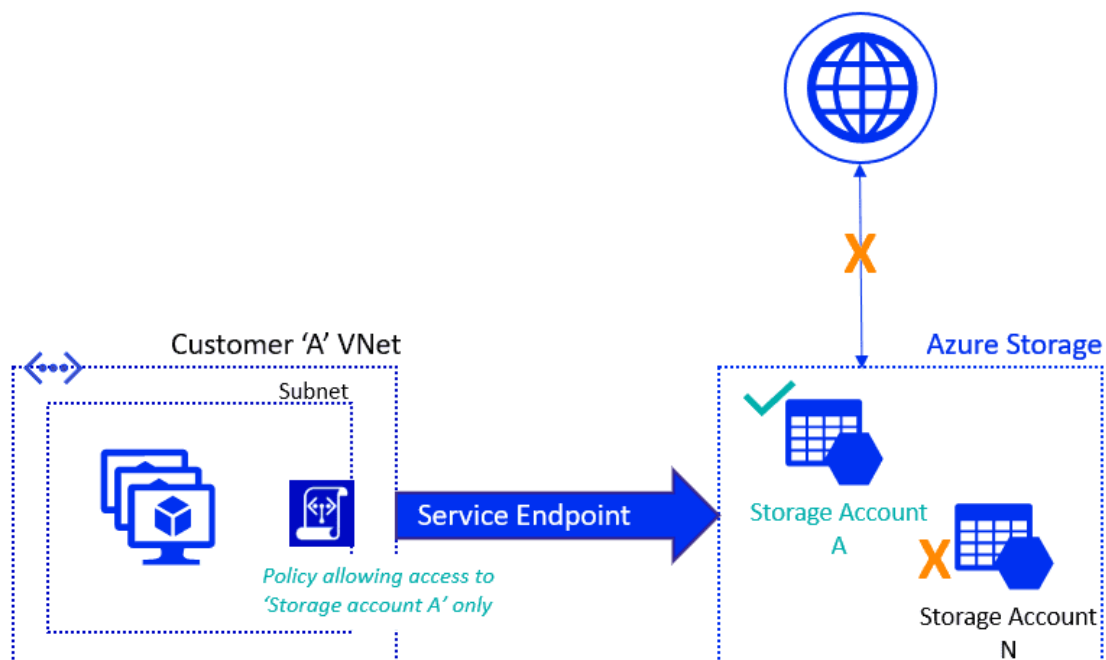
Filter by name...
 Azure for Students St...
 All resource groups
 All locations
 All tags
 No grouping

0 items

Name ↑↓	Status	Replication role	Server	Pricing tier	Location ↑↓	Subscription ↑↓
 <p>No SQL databases to display</p> <p>Try changing your filters if you don't see what you're looking for.</p> <p><a href="#">Create SQL database</a></p>						

## 12) Service Endpoints and Securing Storage

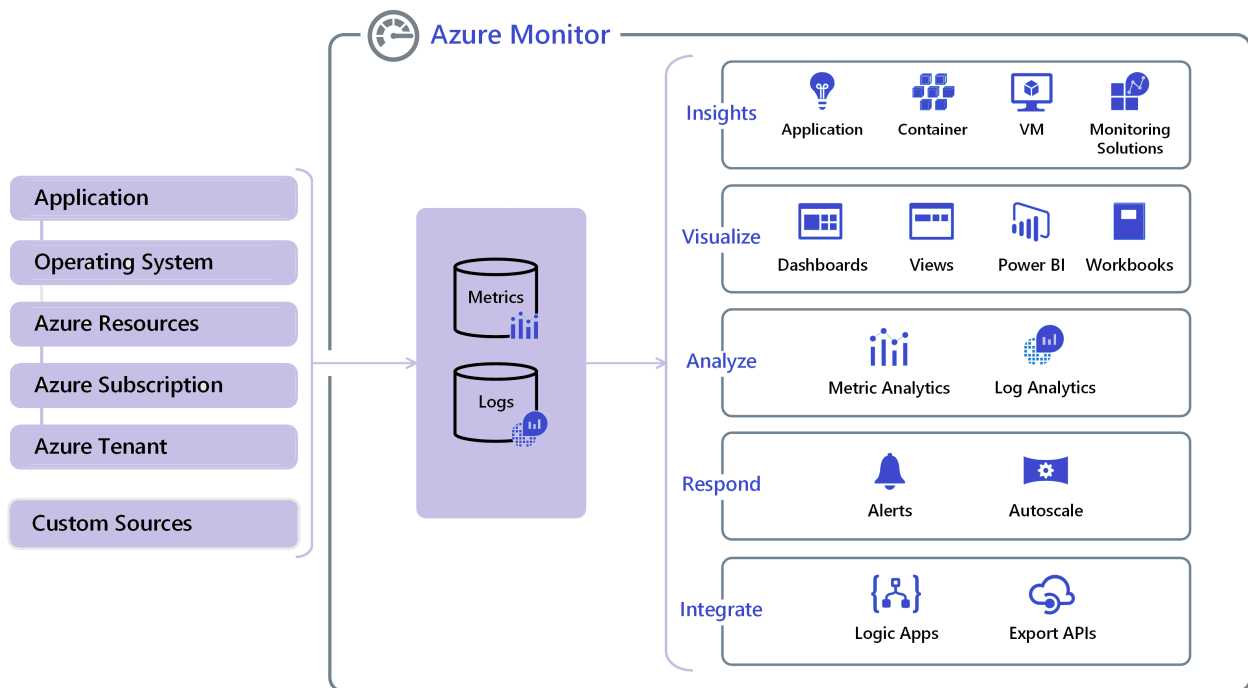
Virtual Network service endpoint provides a secure and direct connection to Azure Services. Service Endpoint removes the need for a Public IP address to access an endpoint of an Azure service and this is done by enabling a Private IP address in the Vnet by using Service Endpoint.





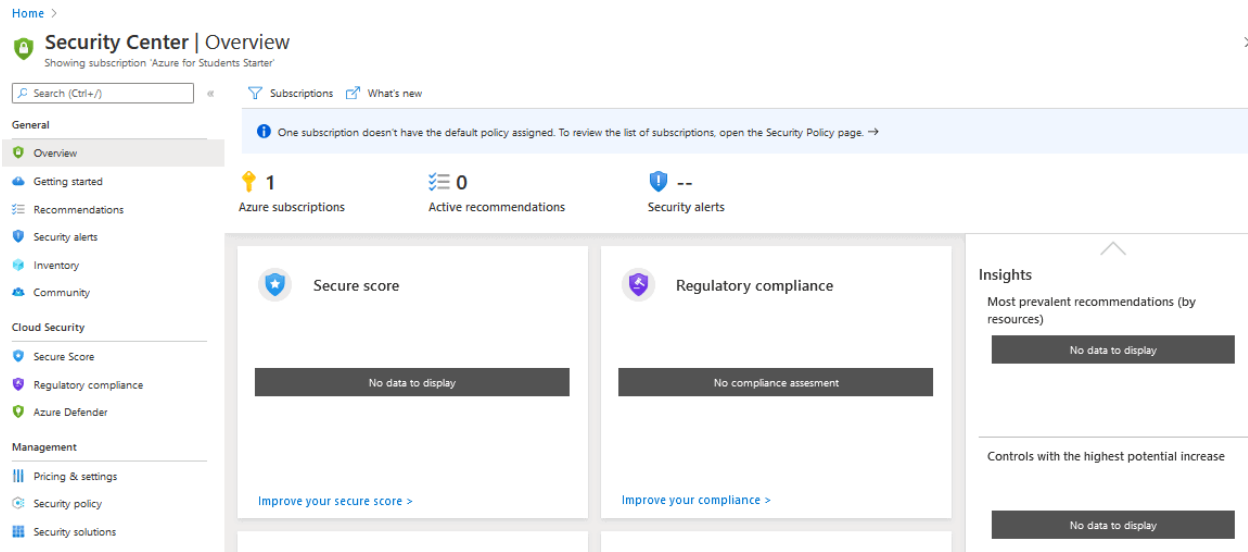
### 13) Azure Monitor

Azure Monitor is a monitoring service provided by Azure. By using Azure Monitor helps to maximize the performance and availability of businesses. The Azure Monitor acts on the telemetry of the Cloud and On-Premises Environments and provides the optimum configurations for the resources.



### 14) Azure Security Center

Azure Security Center is an infrastructure tool provide by Azure Cloud for security management and threat protection. This tool provides security to Cloud Resources and On-premises Resources as well.



## 15) Azure Sentinel

Azure Sentinel is a very advanced service of Azure. It is a scalable, cloud-native, security information event management, and security orchestration automated response solution.

In this Activity Guide, you'll have to collect data from the Azure Activity and Security Center. And also you have to add built-in and custom alerts.



## Collect

Security data across  
your enterprise



## Respond

Rapidly and automate  
protection



## Azure Sentinel

*Cloud-native SIEM+SOAR*



## Detect

Threats with vast threat  
intelligence



## Investigate

Critical incidents  
guided by AI