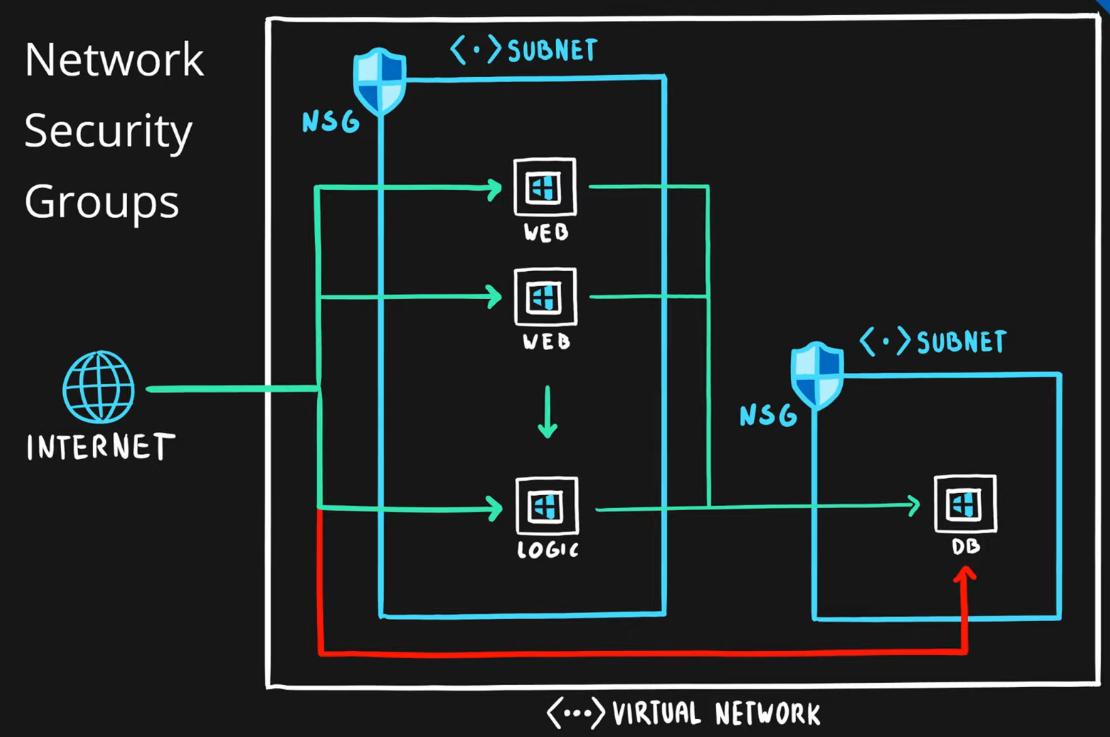
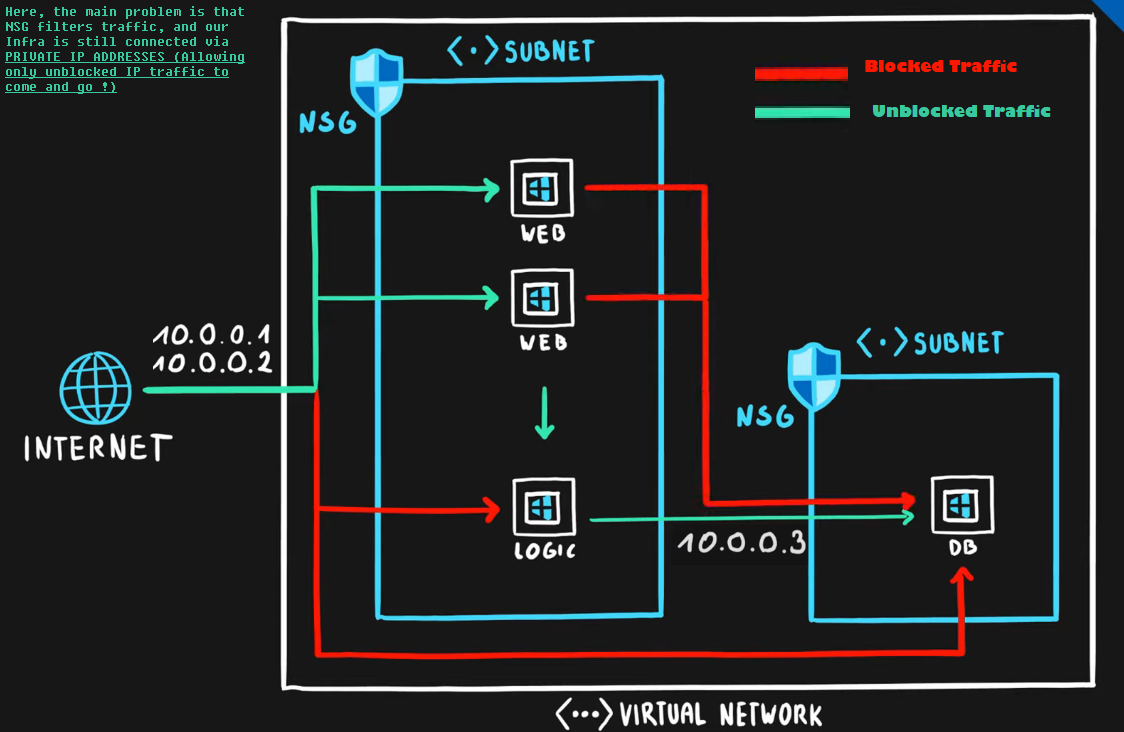
1. [Episode 21: Security Groups | NSG and ASG | Network Security Groups and Application Security groups](https://marczak.io/az-900/" \l "ep21)
2. **Network Security Groups**

* Designed to **filter traffic** to (inbound) and from (outbound) Azure resources located in - Azure Virtual Network
* Filtering controlled by **rules**
* Ability to have **multiple** inbound and outbound **rules**
* Rules are created by specifying
  + **Source**/**Destination** (IP addresses, service tags, application security groups)
  + **Protocol** (TCP, UDP, any)
  + **Port** (or Port Ranges, ex. 3389 – RDP, 22 – SSH, 80 HTTP, 443 HTTPS)
  + **Direction** (inbound or outbound)
  + **Priority** (order of evaluation)



1. **Application Security Groups**

* Feature that allows **grouping of virtual machines** located in Azure virtual network
* Designed to **reduce** the **maintenance effort** (assign ASG instead of the explicit IP address)

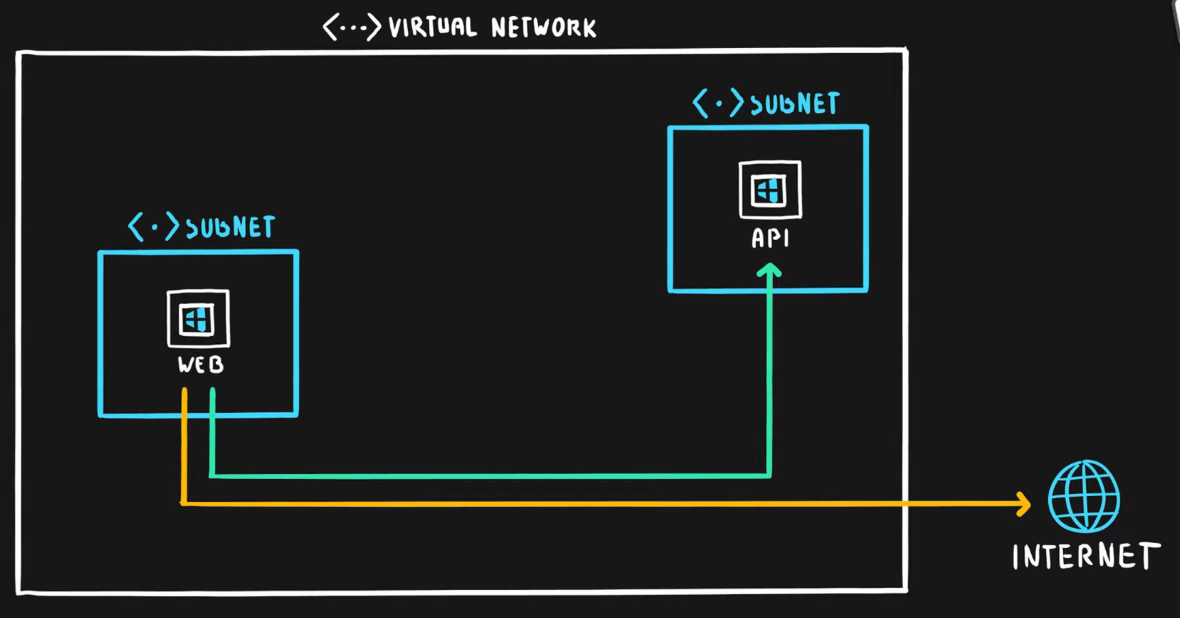


Graphical user interface, diagram

Description automatically generated

1. [Episode 22: User-defined Routes (UDR)](https://marczak.io/az-900/#ep22)
2. **Routing**

Process of finding/selecting a path for traffic in one or across multiple networks.



1. **User-defined Routes**

* Custom (user-defined, static) routes (UDRs)
* Designed to **override Azure’s default routing** or **add new routes**
* Managed via Azure Route Table resource
* Associated with a **zero or more Virtual Network subnets**

Diagram

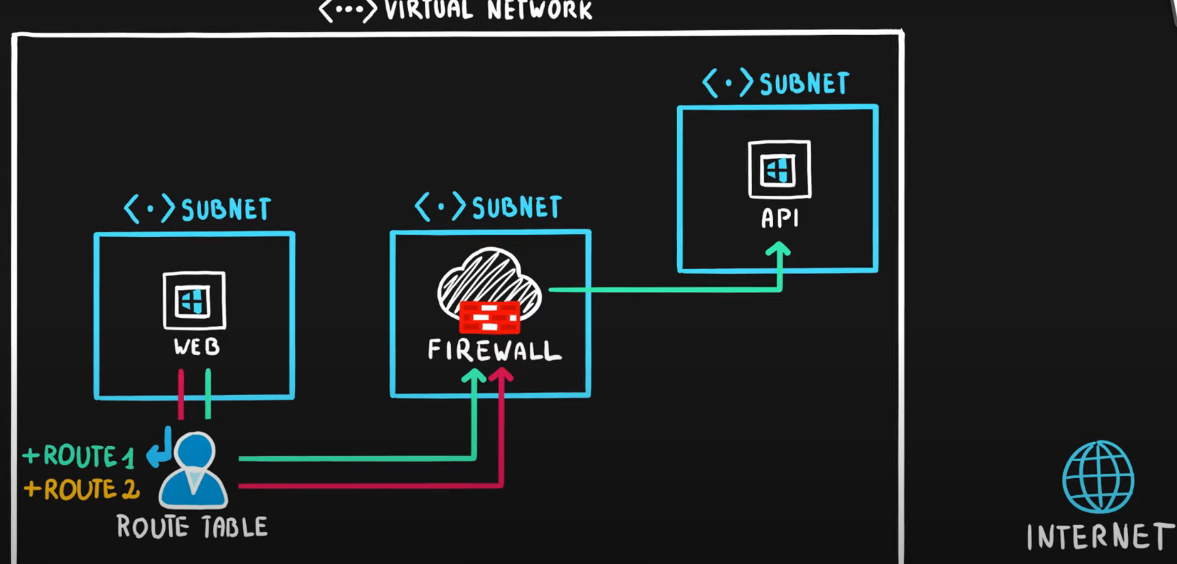
Description automatically generated

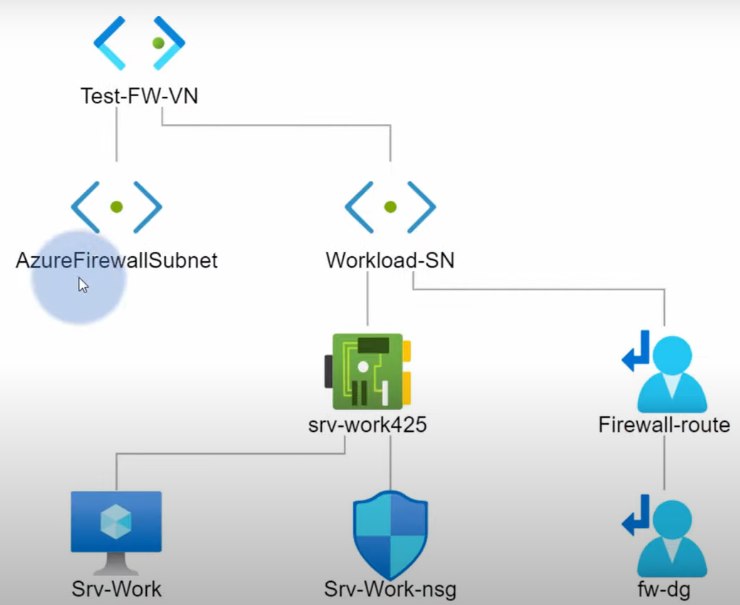
1. [Episode 23: Azure Firewall](https://marczak.io/az-900/#ep23)

* **Firewall**

A firewall is a network security service that monitors and controls **incoming** and **outgoing** traffic.

* **Azure Firewall**
* Managed, cloud-based **firewall service** (PaaS, Firewall as a Service)
* Built-in **high availability**
* Highly **Scalable**
* **Inbound** & **outbound** traffic filtering rules
* Support for **FQDN** (Fully Qualified Domain Name), ex. microsoft.com
* Fully integrated with Azure Monitor for logging and analytics





1. [Episode 24: Azure DDoS Protection](https://marczak.io/az-900/#ep24)

### **DoS - Denial of Service**

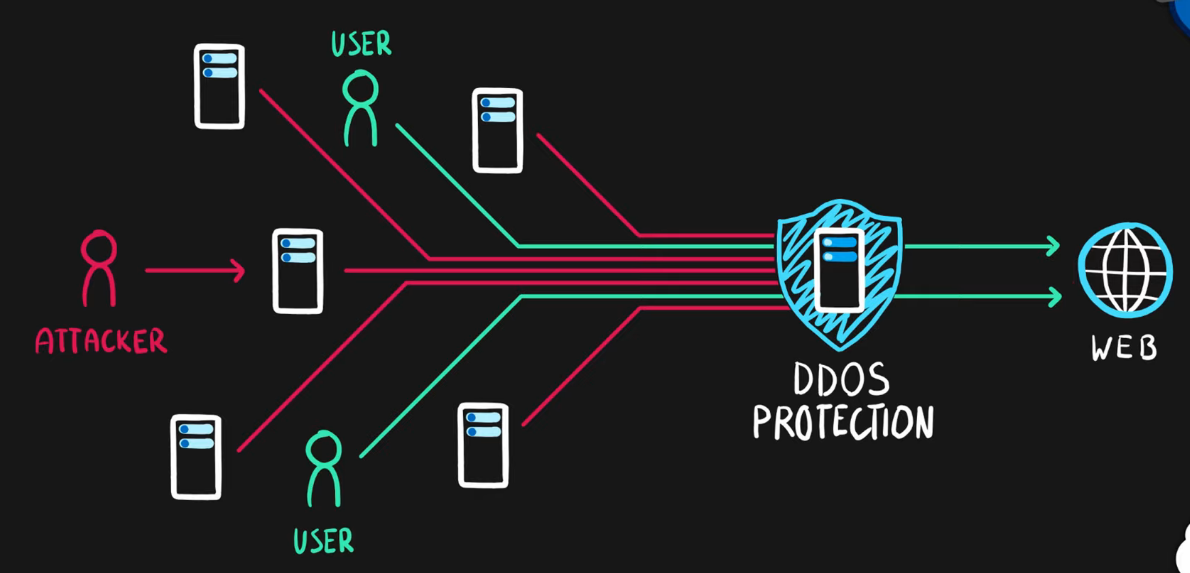
Cyber-attack with intent to cause temporary or indefinite **disruption of service**

### **DDoS - Distributed Denial of Service**

**DoS** attacks that is originating **from multiple servers**

## Azure DDoS Protection

* **DDoS protection service** in Azure
* Designed to
  + **Detect malicious traffic** **and block it** while allowing legitimate users to connect
  + **Prevent additional costs** for auto-scaling environments
* Two tiers
  + **Basic** – automatically enabled for the Azure platform
  + **Standard** – additional mitigation & monitoring capabilities for Azure Virtual Network resources
* Standard tier uses machine learning to **analyze traffic patterns** for better accuracy



1. [Episode 25: Azure Identity Services | Identity, Authentication, Authorization & Azure AD](https://marczak.io/az-900/#ep25)

## Identity

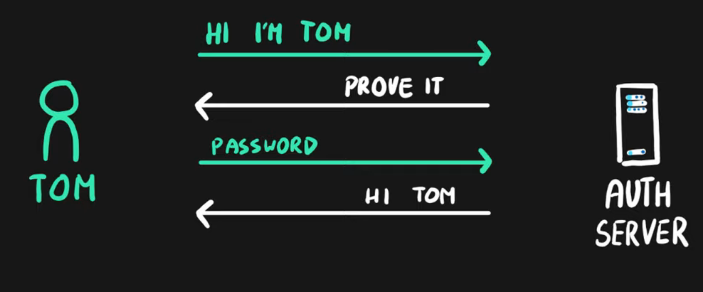
* A user with a username and password.
* Also applications or other servers with secret keys or certificates.
* The fact of being something or someone.

Icon

Description automatically generated

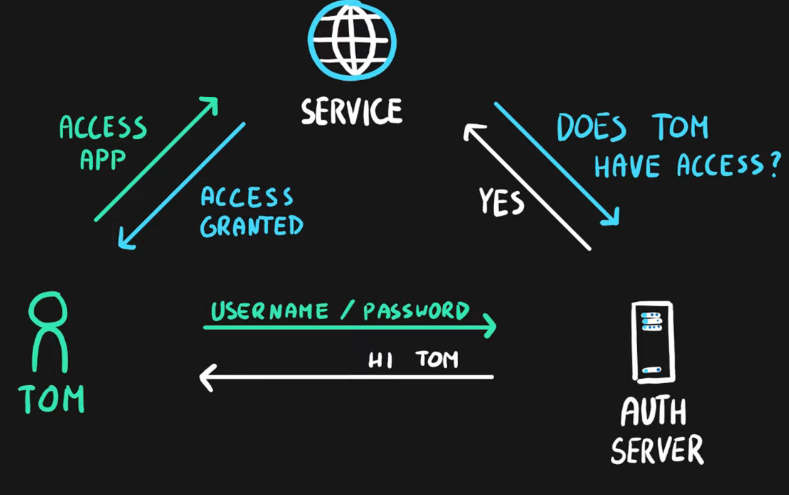
### **Authentication**

The process of **verification/assertion of identity**

****

### **Authorization**

The process of **ensuring** that only **authenticated identities** get **access to the resources** for which they have been granted access.



### **Access Management**

The process of **controlling**, **verifying**, **tracking** and **managing access** to authorized users and applications.

## Azure Active Directory

* Identity and Access Management service in Azure
* Identities management – users, groups, applications
* Access management – subscriptions, resource groups, roles, role assignments, authentication & authorization settings, etc.
* Used by multiple Microsoft cloud platforms
  + Azure
  + Microsoft 365
  + Office 365
  + Live.com services (Skype, OneDrive, etc.)

Graphical user interface, diagram, application

Description automatically generated

### **Multi-factor Authentication (MFA)**

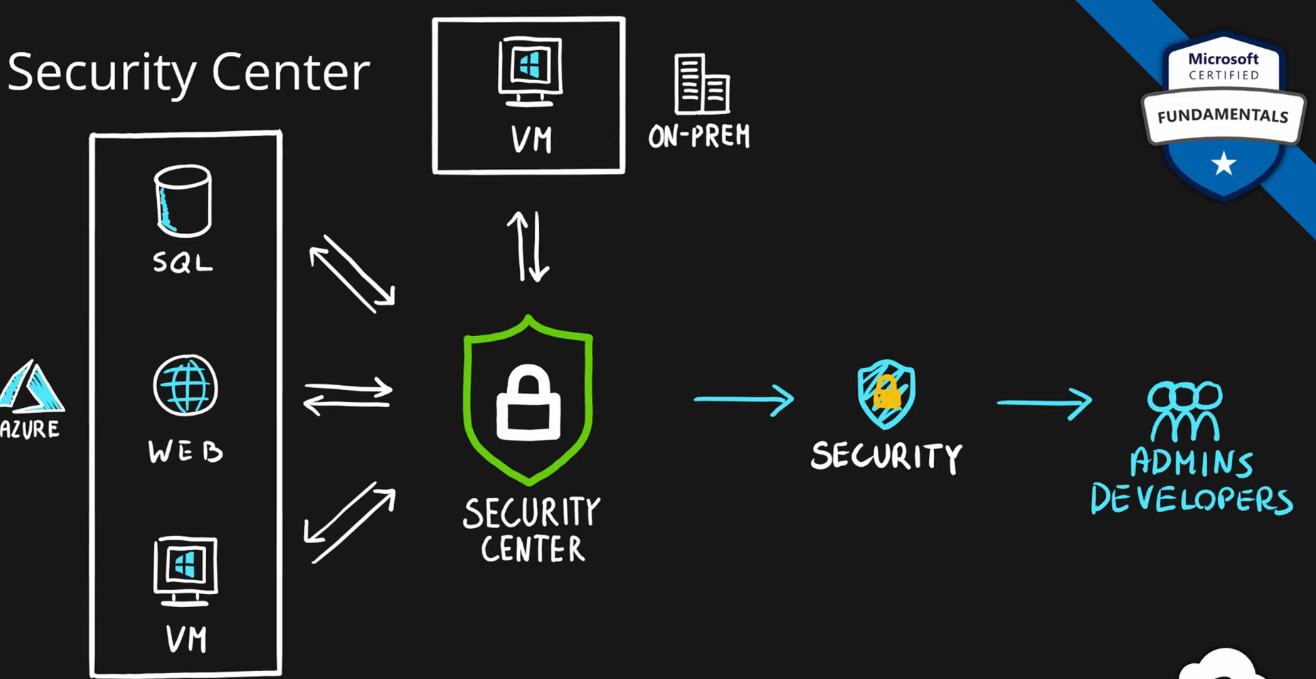
* Process of authentication using more than one factor (evidence) to prove identity
* Factor types
  + Knowledge Factor – “Something you know”, ex. password, pin
  + Possession Factor – “Something you have”, ex. phone, token, card, key
  + Physical Characteristic Factor – “Something you are”, ex. fingerprint, voice, face, eye iris
  + Location Factor – “Somewhere you are”, ex. GPS location
* Supported by Azure AD by default (simple on-off switch)



1. [Episode 26: Azure Security Center and usage scenarios](https://marczak.io/az-900/#ep26)

**Identity**

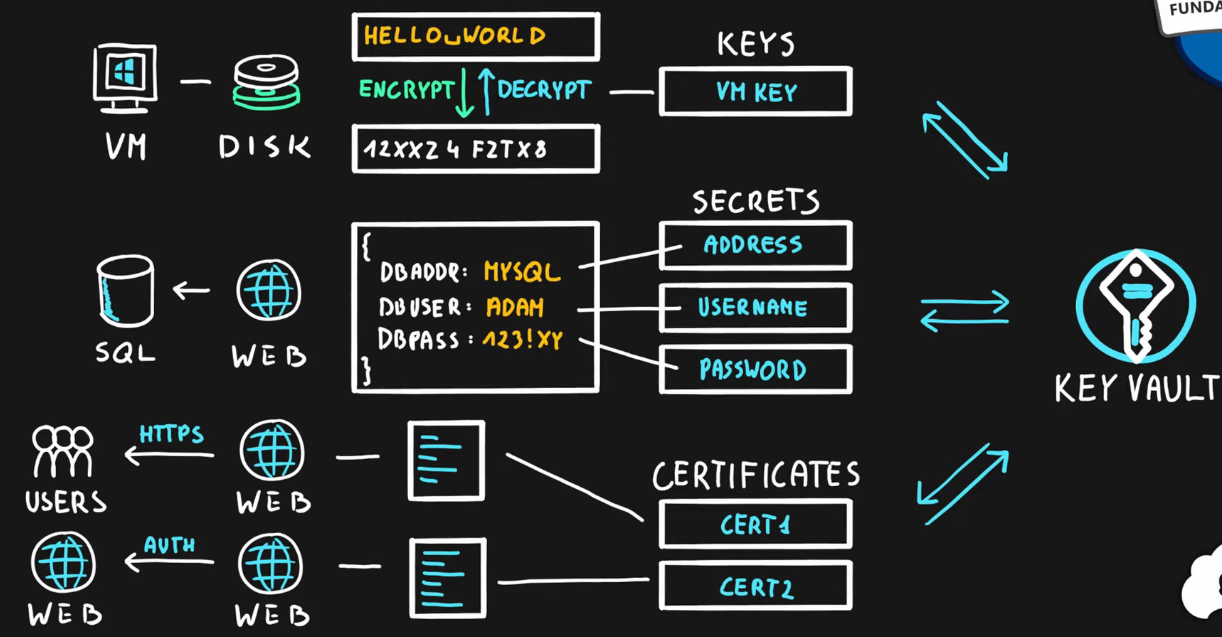
* **Centralized**/**unified** infrastructure and platform **security management service**
* **Natively embedded** in Azure services
* **Integrated** with **Azure Advisor**
* Two tiers
  + **Free** (Azure Defender OFF) – included in all Azure services, provides continuous assessments, security scores, and actionable security recommendations
  + **Paid** (Azure Defender ON) – hybrid security, threat protection alerts, vulnerability scanning, just-in-time (JIT) VM access, etc.



1. [Episode 27: Key Vault](https://marczak.io/az-900/#ep27)

**Azure Key Vault**

* **Managed service** for **securing sensitive information** (application/platform) (PaaS)
* **Secure storage service** for
  + **Keys**,
  + **Secrets** and
  + **Certificates**
* **Highly integrated** with other Azure services (VMs, Logic Apps, Data Factory, Web Apps, etc.)
* **Centralization**
* Access **monitoring** and **logging**

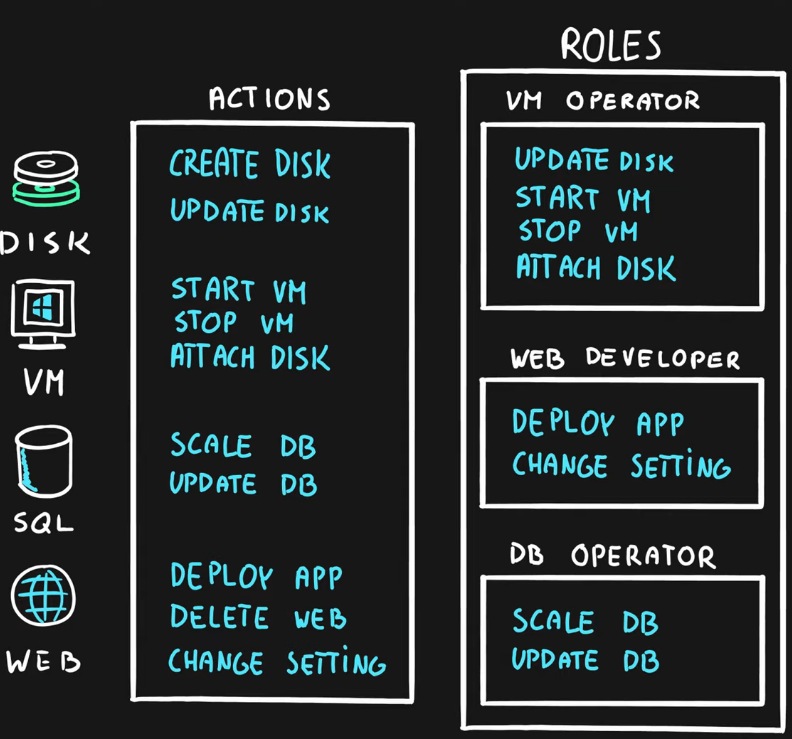


1. [Episode 28: Role-Based Access Control (RBAC)](https://marczak.io/az-900/#ep28)

## What is a Role?

**Role** (role definition) is a **collection of actions** that **the assigned identity** will be able to perform.

Role definition is an answer to the question “**What** can be done?”



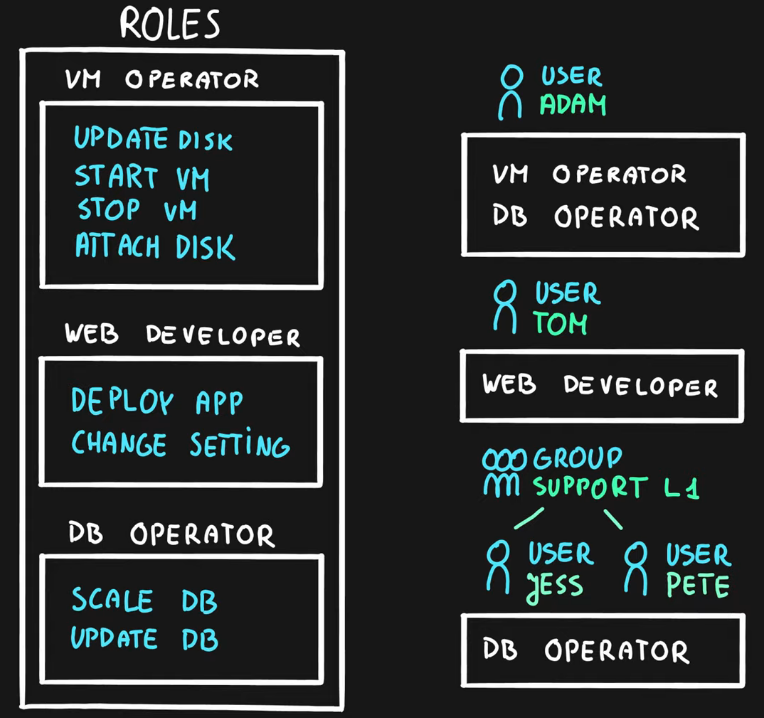
## What is a Security Principal?

**Security Principal** is an Azure object (identity) that   
can be assigned to a role (ex. users, groups or applications).

**Security Principal assignment** is an answer to the question “**Who** can do it?”

Diagram

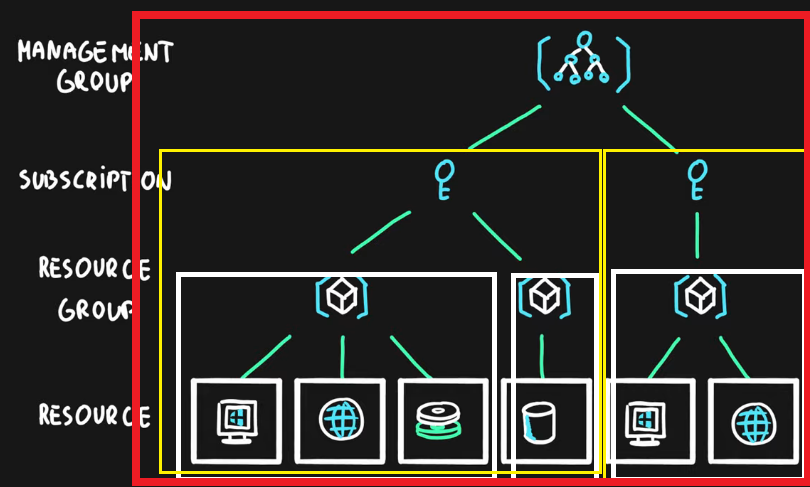
Description automatically generated



## What is a Scope?

**Scope** is one or more Azure resources that the access applies to.

**Scope assignment** is an answer to a question “**Where** can it be done?”



### **What is a Role Assignment?**

**Role assignment** is a combination of the **role definition**, **security principal** and **scope**.

Graphical user interface, text, application

Description automatically generated

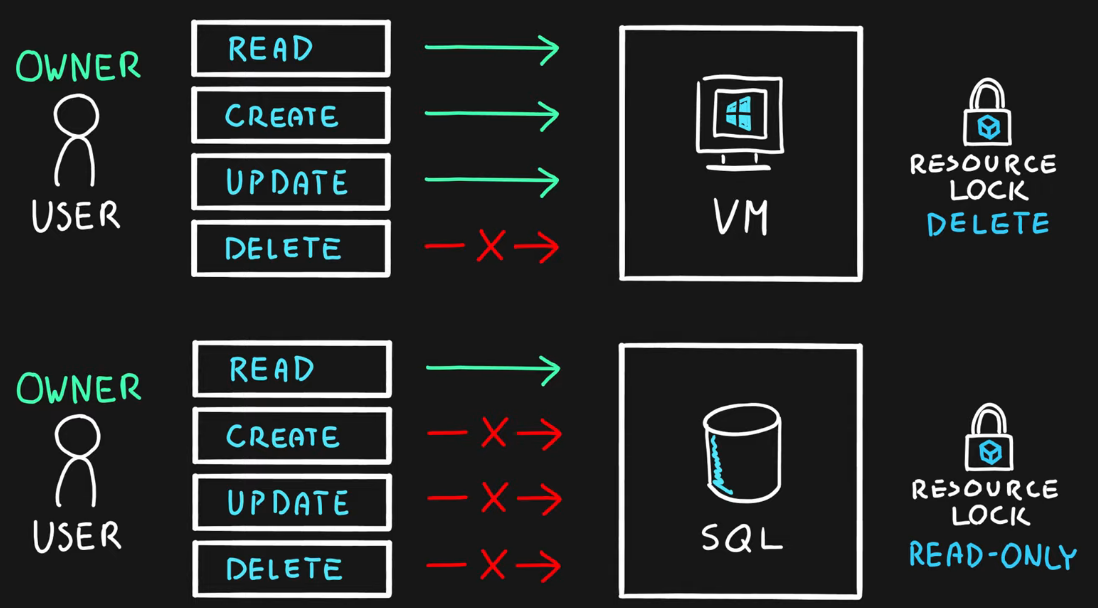
## Azure Role-based Access Control (RBAC)

* Authorization system built on Azure Resource Manager (ARM)
* Designed **for fine-grained access management** of Azure Resources
* Role assignment is combination of
  + **Role definition** – list of permissions like create VM, delete SQL, assign permissions, etc.
  + **Security Principal** – user, group, service principal and managed identity and
  + **Scope** – resource, resource groups, subscription, management group
* Hierarchical
  + Management Groups > Subscriptions > Resource Groups > Resources
* Built-in and Custom roles are supported

1. [Episode 29: Resource Locks](https://marczak.io/az-900/#ep29)

**What is an Azure Resource Lock?**

* Designed to **prevent accidental deletion** and/or **modification**
* Used in conjunction with RBAC
* Two types of locks
  + **Read-only** (**ReadOnly**) – only read actions are allowed
  + **Delete** (**CanNotDelete**) – all actions except delete are allowed



* Scopes are **hierarchical** (**inherited**)
  + Subscriptions > Resource Groups > Resources

Diagram

Description automatically generated

* **Management Groups** can’t be locked
* Only **Owner** and **User Access Administrator** roles can manage locks (**built-in** roles)

Graphical user interface

Description automatically generated

1. [Episode 30: Tags](https://marczak.io/az-900/#ep30)

**Azure Resource Tags**

* Tags are simple **Name** (key) - **Value** **pairs**
* Designed to help with **organization of Azure resources**
* Used for resource **governance**, **security**, **operations management**, **cost management**, **automation**, etc.
* Typical **tagging strategies**
  + **Functional** – mark by **function** ( ex: environment = production )
  + **Classification** – mark by **policies used** ( ex: classification = restricted )
  + **Finance**/**Accounting** – mark for **billing purposes** ( ex: department = finance )
  + **Partnership** – mark by **association of users/groups** ( ex: owner = adam )
* Applicable for **resources**, **resource groups** and **subscriptions**
* **NOT inherited** by default

Graphical user interface, application

Description automatically generated

1. [Episode 31: Azure Policy](https://marczak.io/az-900/#ep31)

**Azure Policy**

* Designed to help with resource **governance**, **security**, **compliance**, **cost management**, etc.
* **Policies** focus on **resource properties** (**RBAC** focused on **user actions**)
* Policy **definition** – Defines what should happen
  + Define the **condition** (if/else) and the **effect** (deny, audit, append, modify, etc.)
  + Examples include allowed *resource types*, *allowed locations*, *allowed SKUs*, *inherit resource tags*
* **Built-in** and **custom** policies are supported
* Policy **initiative** – a **group** of policy definitions
* Policy **assignment** – assignment of a policy definition/initiative to a scope
  + Scopes can be assigned to
    - management groups,
    - subscriptions,
    - resource groups, and
    - resources
* Policies allow for **exclusions of scopes**
* Checked during **resource creation** or **updates** and **existing ones with remediation tasks**

Diagram

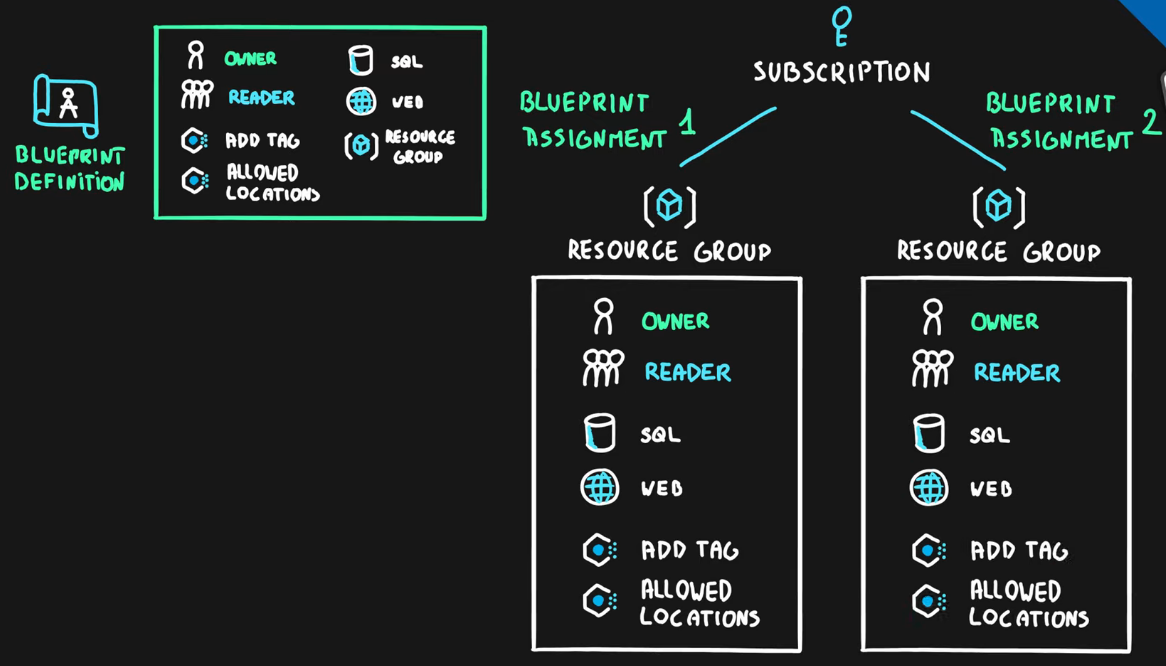
Description automatically generated

1. [Episode 32: Azure Blueprints](https://marczak.io/az-900/#ep32)

**Azure Blueprints**

* **Package** of various Azure components (**artifacts**)
  + **Resource Groups**
  + **ARM Templates**
  + **Policy Assignments**
  + **Role Assignments**
* **Centralized storage** for organizationally **approved design patterns**
* Blueprint **definition** – describing what should happen (reusable package)
* Blueprint **assignment** – describing where it should happen (package deployment)

A screenshot of a computer

Description automatically generated with low confidence

1. [Episode 33: Cloud Adoption Framework](https://marczak.io/az-900/#ep33)

## Cloud adoption

**Cloud adoption** is a strategic move by an organization to leverage cloud in their business

## Cloud Adoption Framework

Cloud Adoption Framework for Azure is a set of

* **tools**,
* **best practices**,
* **guidelines** and
* **documentation**

prepared by Microsoft to help companies with their cloud adoption journey.

## Strategy

**1.** Understand your motivation

* Answer the question **WHY MOVE?**
* Common Motivation Triggers include
  + **Migration**
    - Cost Savings on infrastructure
    - Reduction in complexity
    - Operation optimization
    - Increased business agility
  + **Innovation**
    - Reaching a global scale
    - Customer experience improvements
    - Transformation of products or services
    - Market disruption

**2.** BusinessOutcome

* Answer the question **WHAT TO MEASURE?**
* Defined, concise and observable outcome captured by a specific measure, for example
  + Increase in revenue
  + Increase in profit
  + Cost reduction
  + Global access to customers
  + Reaching new markets

**3.** Business Justification

* Answer the question **WHAT’S MY RETURN ON INVESTMENT?**
* Develop a business case to validate the financial model that supports your motivations and outcomes
* Tools that support this process are
  + Azure TCO (Total Cost of Ownership) calculator - estimate current on-prem costs
  + Azure Pricing Calculator - estimate future Azure costs
  + Azure Cost Management - see current Azure costs

**4.** First Project

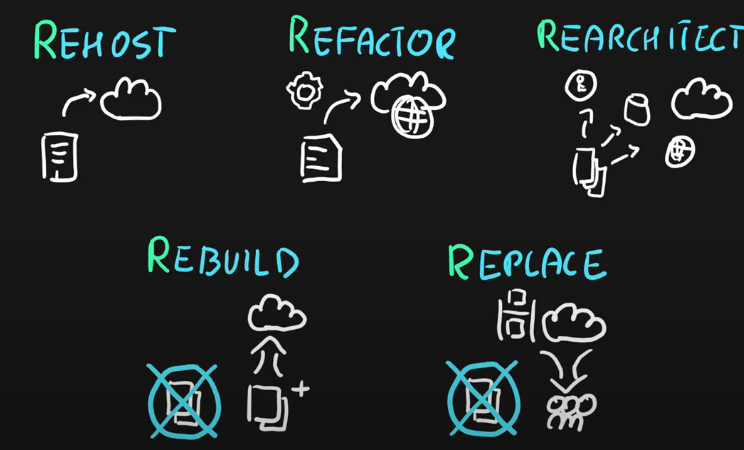
* Choose first project to validate your strategy (Proof of concept - POC) based on
  + Business Criteria
    - Currently operating
    - Dedicated owner
    - Strong motivation to move
  + Technical Criteria
    - Minimum dependencies and assets

Text

Description automatically generated

## Plan

1. Digital Estate (INVENTORY OF ASSETS)
   * Review current landscape and list all projects/solutions (digital assets)
   * Choose one of the five (5) R’s of rationalization
     + Rehost - move as is; typically into containers or IaaS (virtual machines)
     + Refactor - make small code changes and move to PaaS (ex. Azure SQL, Azure App Service, etc.)
     + Rearchitect - make complex code changes to introduce new features or fix incompatible apps
     + Rebuild - create a new application using cloud first design
     + Replace - review available SaaS solutions and replace legacy or unneeded applications
2. Initial Organization Alignment
   * Align people so they will support your adoption plan
   * Map people to capabilities
3. Skills Readiness Plan
   * Review current skills and address the gaps
4. Cloud Adoption Plan - combine everything from steps 1 to 3 into a single cloud adoption plan



## Ready

1. Azure Setup Guide - Review the Azure setup guide to become familiar with the tools and approaches you need to use to create a landing zone.
2. Azure Landing Zone - Choose an appropriate Azure Subscription type that best suits your needs and establish an initial Azure environment.
3. Extend Landing Zone - Expand the initial landing zone to fit your business needs.
4. Best Practices - Review everything and ensure best practices are followed.

Graphical user interface, application

Description automatically generated

## Adopt

## 

### **Migrate**

1. First Migration - migrate your first application to familiarize yourself with the cloud, guidelines and tools
2. Migration Scenarios - review and prepare migration scenarios/guidelines for your company
   * Virtual Machines - Linux, Windows, etc.
   * Apps - Java, .NET, NodeJS web apps, etc.
   * Data - SQL Server, PostreSQL, File Servers, etc.
   * Other - VMware, Azure Stack, etc.

A picture containing diagram

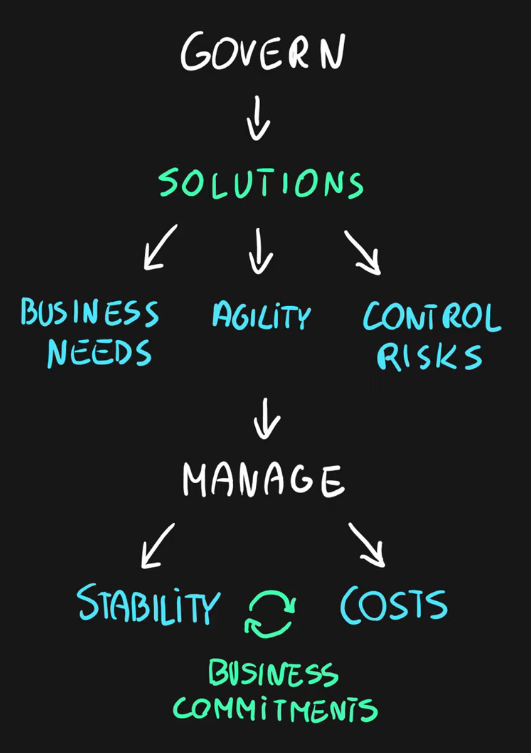
Description automatically generated

1. Best Practices - address common migration needs through the application of consistent best practices.
2. Process Improvements - important part of this porcess heavy activity is to identify bottlenecks and improve with every migration

### **Innovate**

1. Business Value Consensus (VALUE TO STRATEGY)
   1. Create hypothetical customer need
   2. Decide on solution that solves it
   3. Map this to your strategy
2. Innovation Guide (TOOLS) - choose available Azure tools that will help your build this application
3. Best Practices - verify that best practices are followed for all tools in the toolchain
4. Process Improvements - gather feedback from the users and the customers to improve architectural decisions and future products

## Govern & Manage

1. Define governance solutions - Choose solutions to maintain compliance, security and ensure total control of the environment.
   * Those solutions should focus to

Address Business Needs

Provide Agility

Control Risks

1. Manage cloud environment (CLOUD OPERATIONS) - Hand over solutions and environment to cloud operations team for maintenance. Team should ensure that stability and costs are always in perfect balance to meet business commitments. Team should allow environment to grow, evolve and adapt to changing business needs.

## Organize

Ensure that everyone knows what to do and when to do it for every stage in this process. One of the ways to achieve this is via RACI (Responsible, Accountable, Consulted, and Informed) matrix.

1. [Episode 34: Core tenets of Security, Privacy, and Compliance](https://marczak.io/az-900/#ep34)

|  |  |  |  |
| --- | --- | --- | --- |
| Document/Website | Info | Offers | Audience |
| Microsoft Privacy Statement | Collection, Purpose and Usage of Personal Data | All Microsoft offers including services, applications, websites, software, servers, devices | Everyone - end  customers or  companies |
| Online Services Terms (OST) | Licensing Terms (legal agreement) - usage rights about Azure services. What can be done and what is forbidden. | Microsoft Online Services like Azure, Microsoft 365 services, Bing Maps, etc. | Organizations –  legal teams |
| Data Protection Addendum | Appending to OST describing obligations by both parties (Microsoft and you) with regards to the processing of customer and personal data | Microsoft Online Services like Azure, Microsoft 365 services, Bing Maps, etc. | Organizations –  legal teams,  security teams |
| Trust Center | One-stop shop web portal for everything related to security, compliance, privacy, policies, best practices, etc. | Microsoft Online Services like Azure, Microsoft 365 services, Bing Maps,SharePoint etc. | Organizations –  legal teams,  security teams,  business managers,  administrators |
| Azure Compliance Documentation | Web portal focusing on compliance offerings in Azure, simmilar to the trust center but narrowed down | Azure | Organizations –  legal teams,  security teams,  business managers,  Azure administrators |

**Azure Sovereign Regions**

Azure Sovereign Regions provide Azure services in markets with very strict regulatory requirements

* Azure Government designed for the US government
  + Separate instance of Azure (lifecycle, services, portal, etc.)
  + Physically isolated from other Azure regions
  + Only autorized scanned personel can get access
* Azure China designed for the Chinese market
  + Separate instance of Azure (lifecycle, services, portal, etc.)
  + Physically isolated from other Azure regions
  + Operated by a Chinese telecom company called 21Vianet

