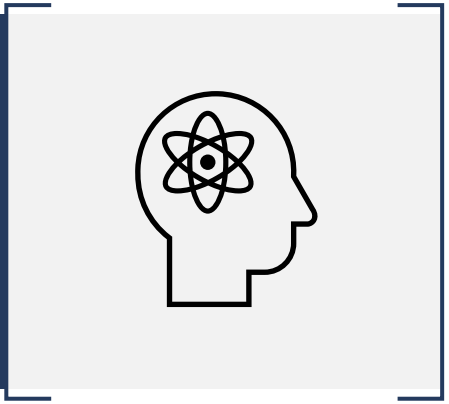
© Copyright Microsoft Corporation. All rights reserved.

FOR USE ONLY AS PART OF VIRTUAL TRAINING DAYS PROGRAM. THESE MATERIALS ARE NOT AUTHORIZED FOR DISTRIBUTION, REPRODUCTION OR OTHER USE BY NON-MICROSOFT PARTIES.

Microsoft

MOD 4: Azure Security and Network Security

Module outline



Module 04 – Outline

You will learn the following concepts:

- **Azure Security features**
  - Security Center and resource hygiene
  - Key Vault, Sentinel, and Dedicated Hosts
- **Azure network security**
  - Defense in depth
  - Network Security Groups and Firewalls
  - DDoS protection

Security tools and features

Security tools and features - Objective Domain

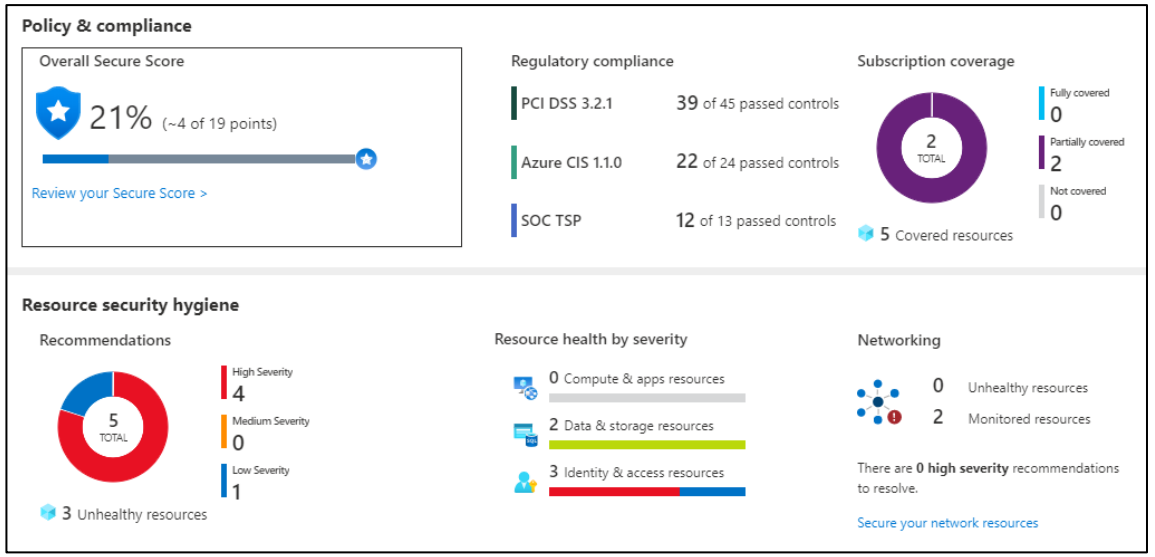
Describe the features and the functionality of:

- Azure Security Center, including policy compliance, security alerts, secure score, and resource hygiene
- Azure Sentinel
- Key Vault
- Azure Dedicated Hosts

Azure Security Center

Azure Security Center is a monitoring service that provides threat protection across both Azure and on-premises datacenters.

- Provides security recommendations
- Detect and block malware
- Analyze and identify potential attacks
- Just-in-time access control for ports



Walkthrough-Azure Security Center

Open Azure Security Center and view some of the common features and configuration options.

1. Launch Azure Security Center.
2. View Policy compliance options.
3. Review your Secure Score.
4. Set a Security Alert.
5. Explore Resource Hygiene.

Azure Security Center - capabilities

Policy Compliance

Run policies across management groups, subscriptions, or tenants.

Continuous Assessments

Assess new and deployed resources to ensure that they are configure properly.

Tailored Recommendations

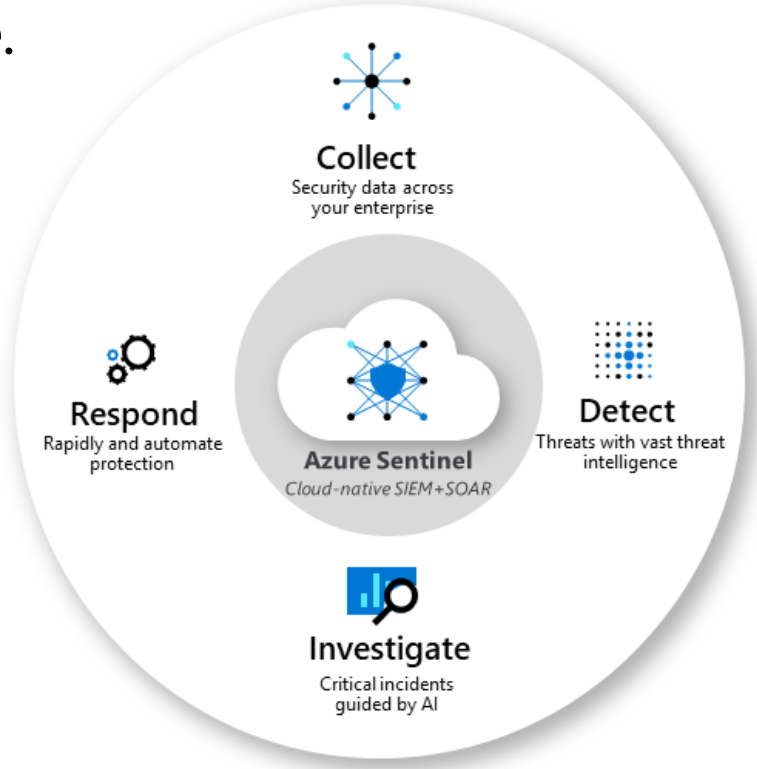
Recommendations based on existing workload with instructions on how to implement them.

Threat Protection

Analyze attempted threats through alerts and impacted resource reports.

Azure Sentinel

Azure Sentinel is a security information management (SIEM) and security automated response (SOAR) solution that provides security analytics and threat intelligence across an enterprise.



Connector and Integrations:

- Office 365
- Azure Active Director
- Azure Advanced Threat Protection
- Microsoft Cloud App Security

Azure Key Vault

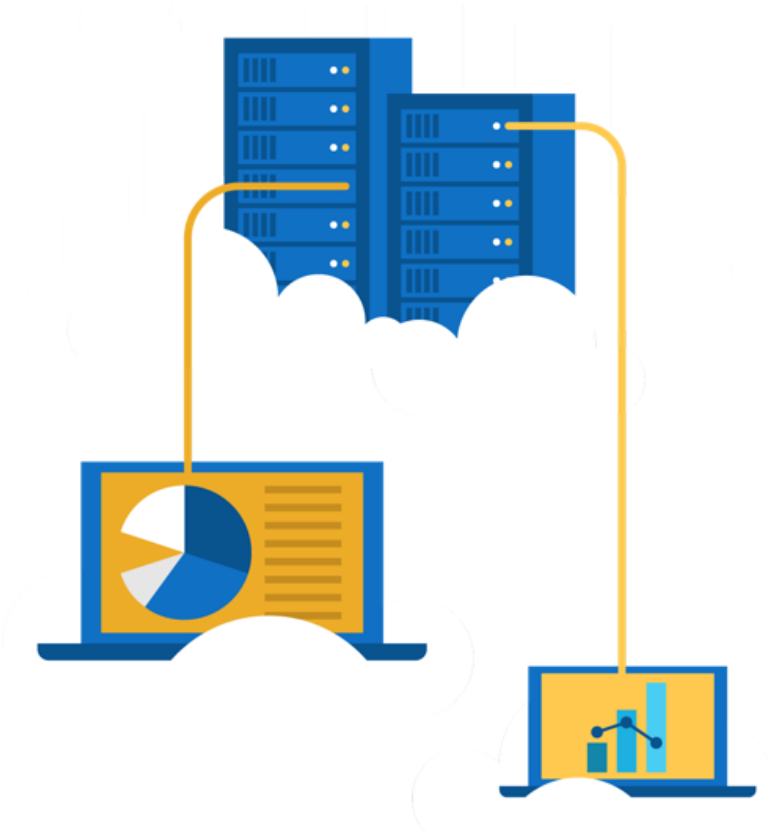
Azure Key Vault stores application secrets in a centralized cloud location in order to securely control access permissions and access logging.

- Secrets management.
- Key management.
- Certificate management.
- Storing secrets backed by hardware security modules (HSMs).

Walkthrough-Implement Azure Key Vault

Create an Azure Key vault and then create a password secret within the key vault.

1. Create an Azure key vault.
2. Add a secret to the Azure key vault.



Azure Dedicated Host

Azure Dedicated Host provides physical servers that host one or more Azure virtual machines that is dedicated to a single organization's workload.

Benefits

- Hardware isolation at the server level
- Control over maintenance event timing
- Aligned with Azure Hybrid Use Benefits

Secure network connectivity

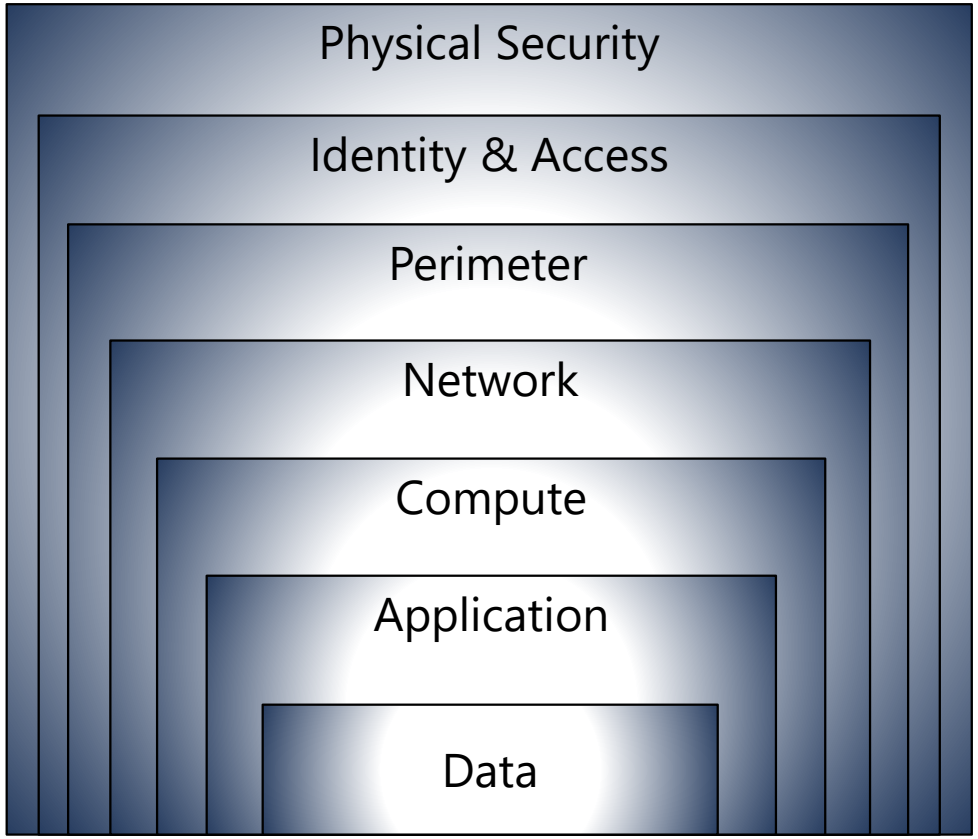
Secure Network Connectivity - Objective Domain

Describe the concept and functionality of:

- Defense in depth
- Network Security Groups (NSG)
- Azure Firewall
- Azure DDoS protection

Defense in depth

- A layered approach to securing computer systems.
- Provides multiple levels of protection.
- Attacks against one layer are isolated from subsequent layers.



Shared Security

- Migrating from customer-controlled to cloud-based datacenters shifts the responsibility for security.
- Security becomes a shared concern between cloud providers and customers.

Responsibility	On-Premises	IaaS	PaaS	SaaS
Data governance and Rights Management	Customer	Customer	Customer	Customer
Client endpoints	Customer	Customer	Customer	Customer
Account and access management	Customer	Customer	Customer	Customer
Identity and directory infrastructure	Customer	Customer	Microsoft/ Customer	Microsoft/ Customer
Application	Customer	Customer	Microsoft/ Customer	Microsoft
Network controls	Customer	Customer	Microsoft/ Customer	Microsoft
Operating system	Customer	Customer	Microsoft	Microsoft
Physical hosts	Customer	Microsoft	Microsoft	Microsoft
Physical network	Customer	Microsoft	Microsoft	Microsoft
Physical datacenter	Customer	Microsoft	Microsoft	Microsoft

Network Security Groups (NSGs)

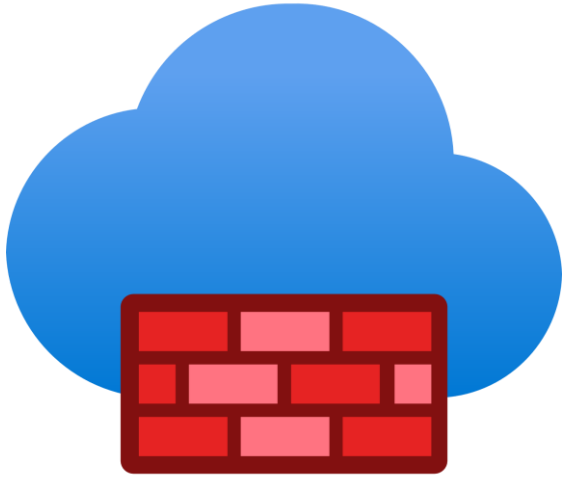
Network Security Groups (NSGs) filter network traffic to and from Azure resources on Azure Virtual Networks.

- Set inbound and outbound rules to filter by source and destination IP address, port, and protocol.
- Add multiple rules, as needed, within subscription limits.
- Azure applies default, baseline security rules to new NSGs.
- Override default rules with new, higher priority rules.

Azure Firewall

A stateful, managed Firewall as a Service (FaaS) that grants/denies server access based on originating IP address, in order to protect network resources.

- Applies inbound and outbound traffic filtering rules
- Built-in high availability
- Unrestricted cloud scalability
- Uses Azure Monitor logging



Azure Application Gateway also provides a firewall, Web Application Firewall (WAF). WAF provides centralized, inbound protection for your web applications.

Azure Distributed Denial of Service (DDoS) protection

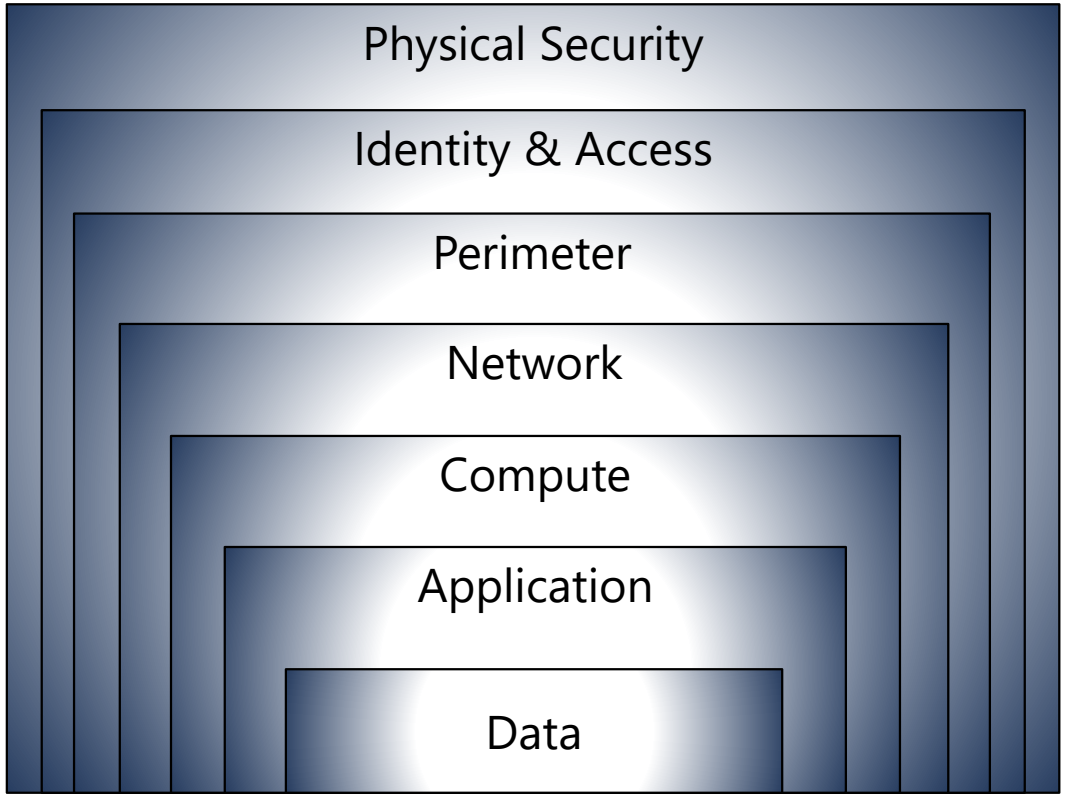
DDoS attacks overwhelm and exhaust network resources, making apps slow or unresponsive.

- Sanitizes unwanted network traffic before it impacts service availability.
- Basic service tier is automatically enabled in Azure.
- Standard service tier adds mitigation capabilities that are tuned to protect Azure Virtual Network resources.

Defense in Depth Reviewed

Combining network security solutions

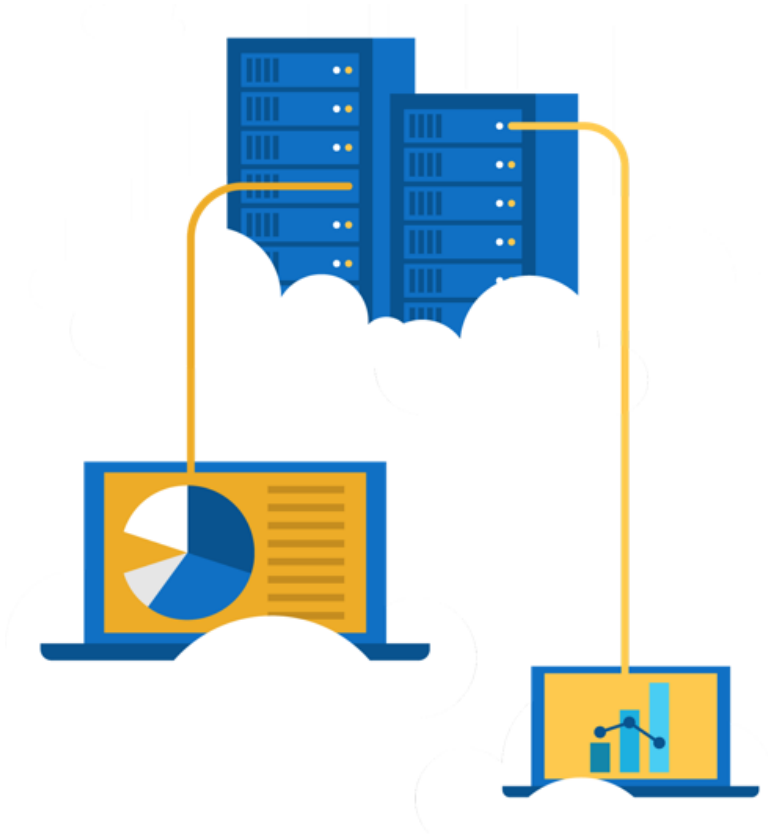
- **NSGs** with **Azure Firewall** to achieve defense in depth.
- **Perimeter layer** protects your network boundaries with Azure DDoS Protection and Azure Firewall.
- **Networking layer** only permits traffic to pass between networked resources with Network Security Group (NSG) inbound and outbound rules.



Walkthrough - Secure network traffic

Create and configure inbound & outbound security port rules.

1. Deploy a custom template to create a virtual machine.
2. Create a network security group.
3. Create an inbound security port rule to allow RDP.
4. Configure an outbound security port rule to deny Internet access.



Module 4 Review

Microsoft Learn Modules
(docs.microsoft.com/Learn)

- Azure Security Center and resource hygiene
- Key Vault, Sentinel, and Dedicated Hosts
- Defense in depth
- DDoS protection

© Copyright Microsoft Corporation. All rights reserved.

FOR USE ONLY AS PART OF VIRTUAL TRAINING DAYS PROGRAM. THESE MATERIALS ARE NOT AUTHORIZED FOR DISTRIBUTION, REPRODUCTION OR OTHER USE BY NON-MICROSOFT PARTIES.

Microsoft

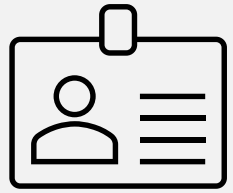
MOD 5: Identity, governance, privacy and compliance

Module 05 – Outline

You will learn the following concepts:

- **Azure identity services**
  - Authentication versus Authorization
  - Azure AD, MFA, SSO and Conditional Access
- **Azure governance features**
  - RBAC
  - Resource locks and tags
  - Policy, Blueprints, and CAF
- **Azure privacy and compliance**
  - Privacy statement and Online Services Terms
  - Trust Center and compliance documentation
  - Azure Sovereign Regions

Core Azure identity services



Azure Identity Services - Objective Domain

- Explain the difference between authentication and authorization
- Define Azure Active Directory
- Describe the functionality and usage of Azure Active Directory
- Describe the functionality and usage of Conditional Access, Multi-Factor Authentication (MFA), and Single Sign-On (SSO)

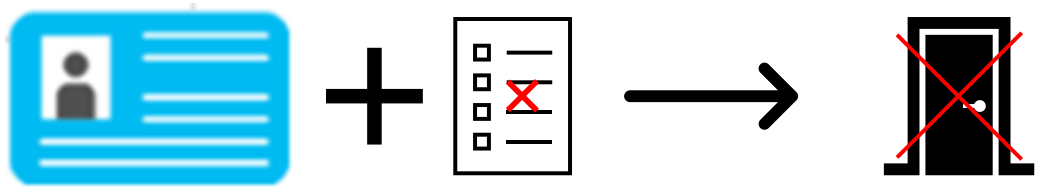
Compare Authentication and Authorization

Authentication

- Identifies the person or service seeking access to a resource.
- Requests legitimate access credentials.
- Basis for creating secure identity and access control principles.

Authorization

- Determines an authenticated person's or service's level of access.
- Defines which data they can access, and what they can do with it.



Azure Multi-Factor Authentication

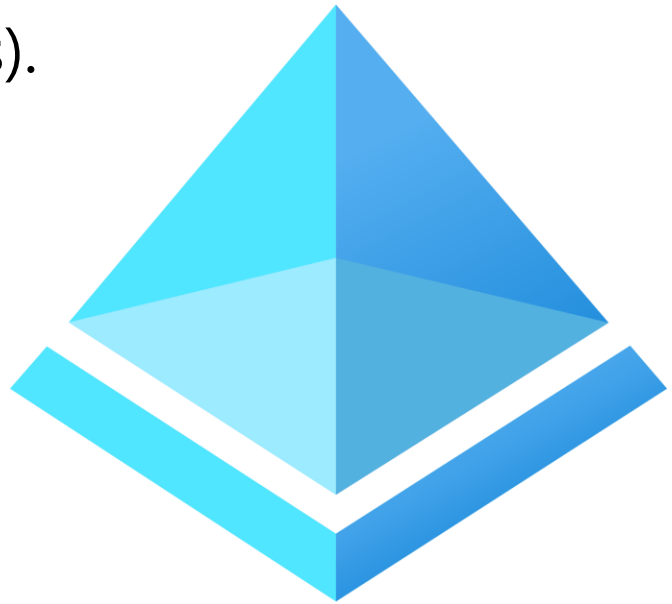
Provides additional security for your identities by requiring two or more elements for full authentication.

- Something you know.
- Something you possess.
- Something you are.

Azure Active Directory (AAD)

Azure Active Directory (AAD) is Microsoft Azure's cloud-based identity and access management service.

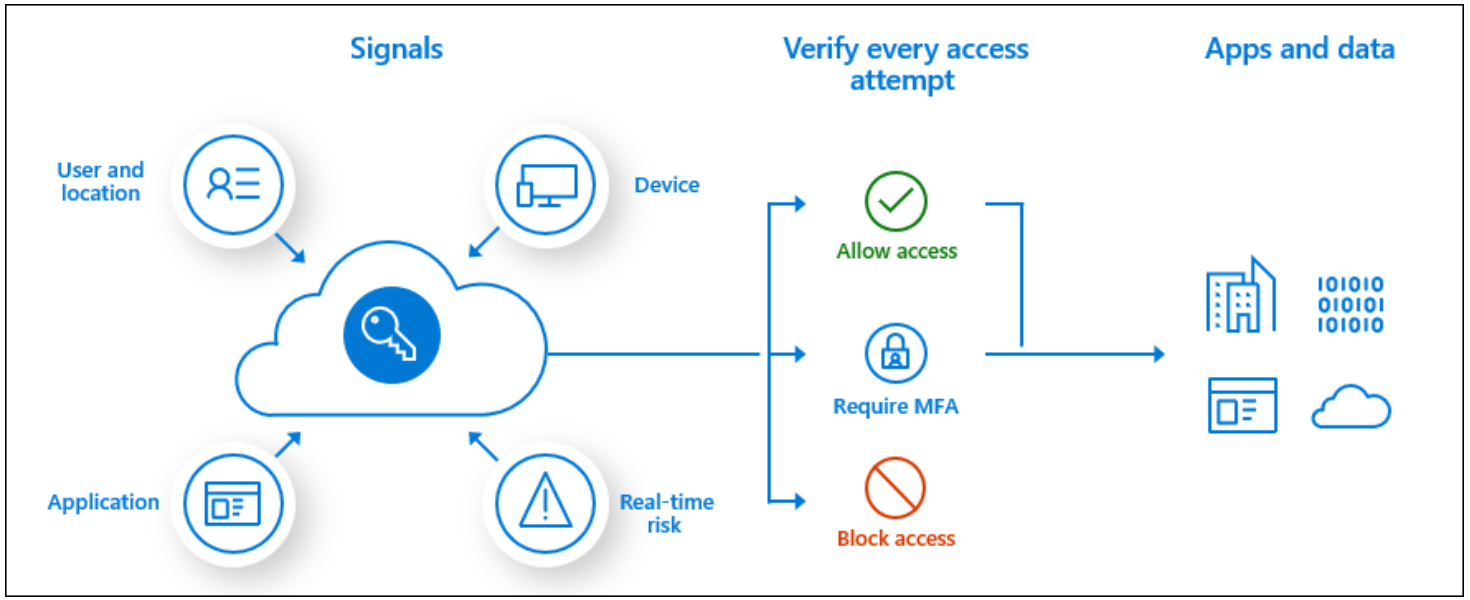
- Authentication (employees sign-in to access resources).
- Single sign-on (SSO).
- Application management.
- Business to Business (B2B).
- Business to Customer (B2C) identity services.
- Device management.



Conditional Access

Conditional Access is used by Azure Active Directory to bring signals together, to make decisions, and enforce organizational policies.

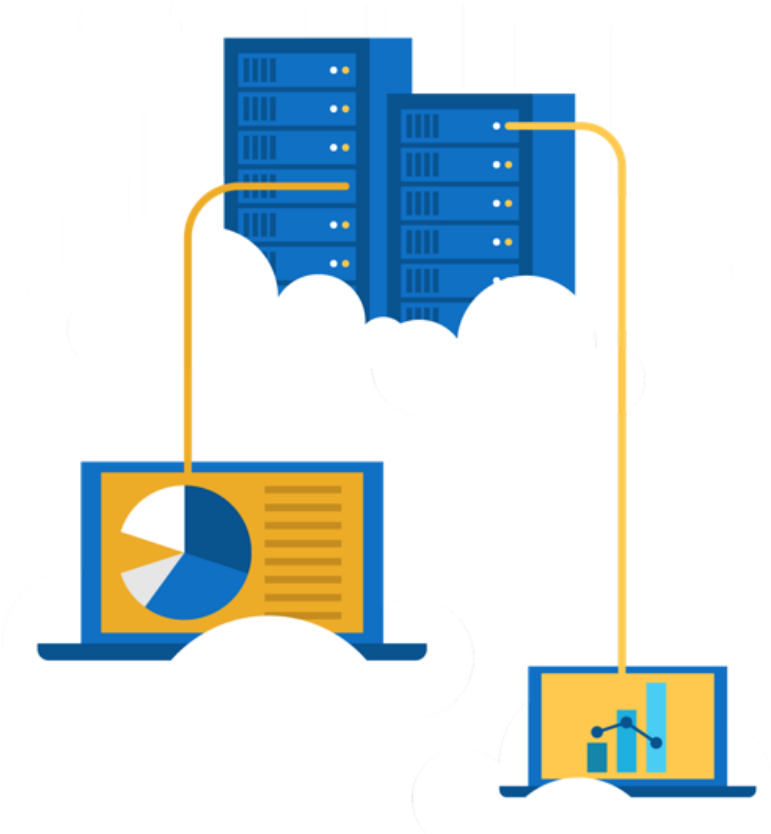
- User or Group Membership
- IP Location
- Device
- Application
- Risk Detection



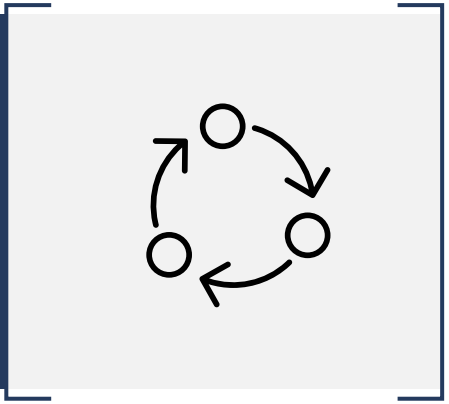
Walkthrough - Manage access with RBAC

Assign roles and view activity logs.

1. View and assign roles.
2. View the activity log and remove a role assignment.



Azure Governance Methodologies

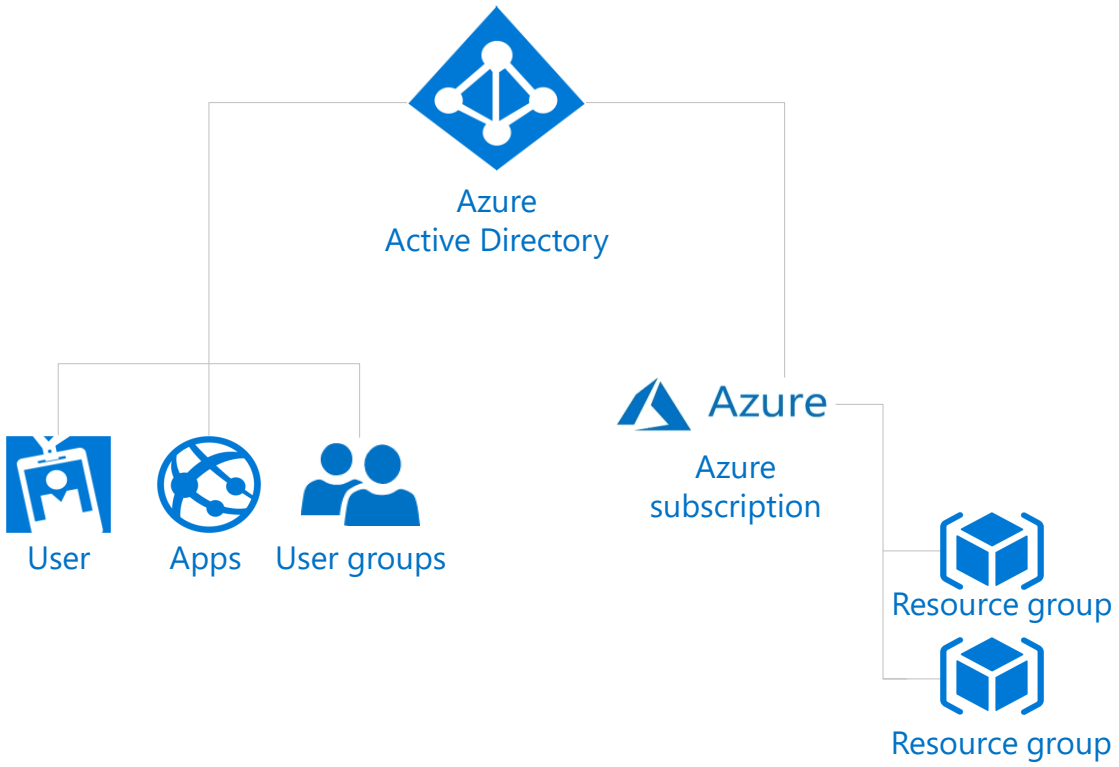


Azure Governance Methodologies - Objective Domain

Describe the functionality and the usage of:

- Role-Based Access Control (RBAC)
- Resource locks
- Tags
- Azure Policy
- Azure Blueprints
- Cloud Adoption Framework for Azure

Explore Role-based access control (RBAC)



- Fine-grained access management.
- Segregate duties within the team and grant only the amount of access to users that they need to perform their jobs.
- Enables access to the Azure portal and controlling access to resources.

Resource locks

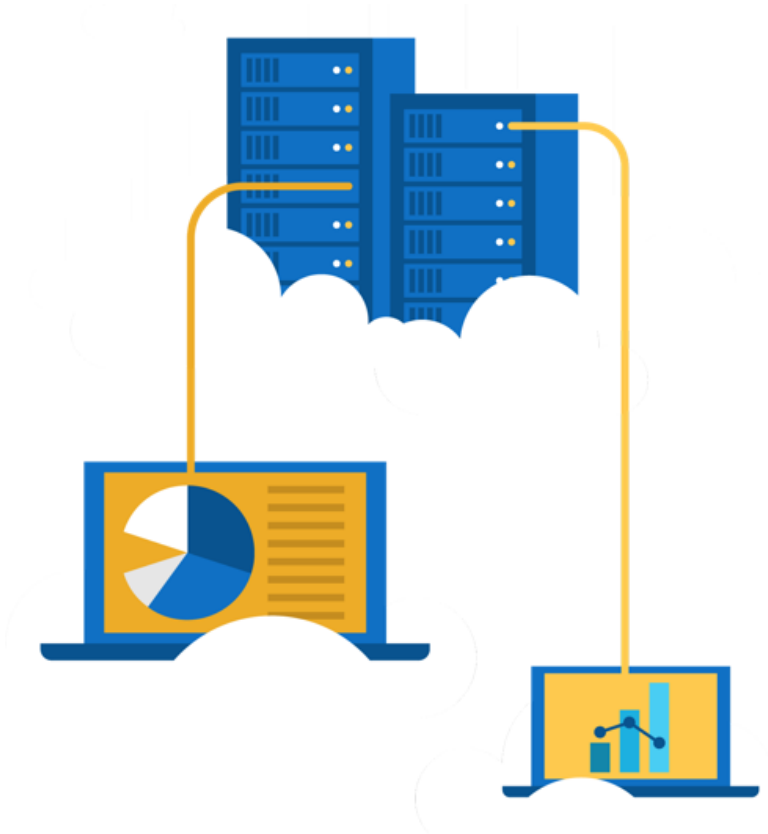
- Protect your Azure resources from accidental deletion or modification.
- Manage locks at subscription, resource group, or individual resource levels within Azure Portal.

Lock Types	Read	Update	Delete
CanNotDelete	Yes	Yes	No
ReadOnly	Yes	No	No

Walkthrough - Manage Resource Locks

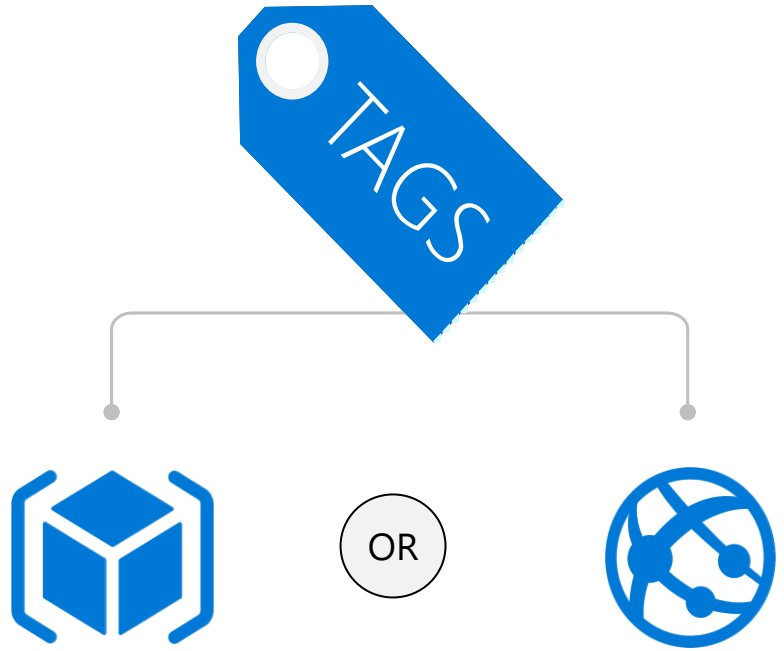
Create a resource group add a lock and test deletion, test deleting a resource in the resource group.

1. Create a resource group.
2. Add a resource lock to prevent deletion of a resource group.
3. Test deleting a member of the resource group.
4. Remove the resource lock.



Tags

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



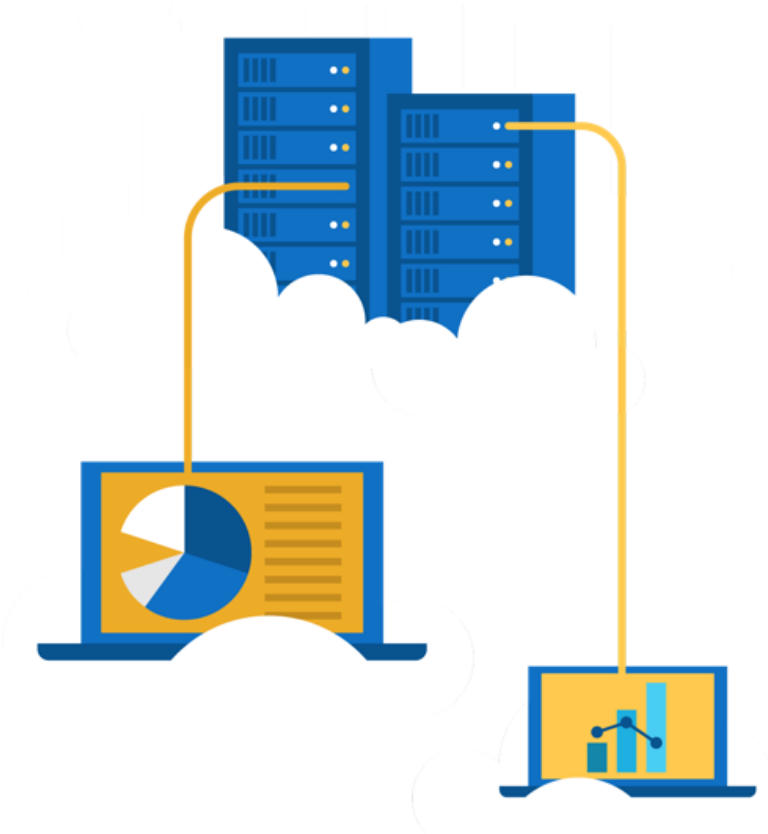
owner: joe
department: marketing
environment: production

cost-center: marketing

Walkthrough – Implement resource tagging

Create a policy assignment that requires tagging, then create a storage account and test the tagging.

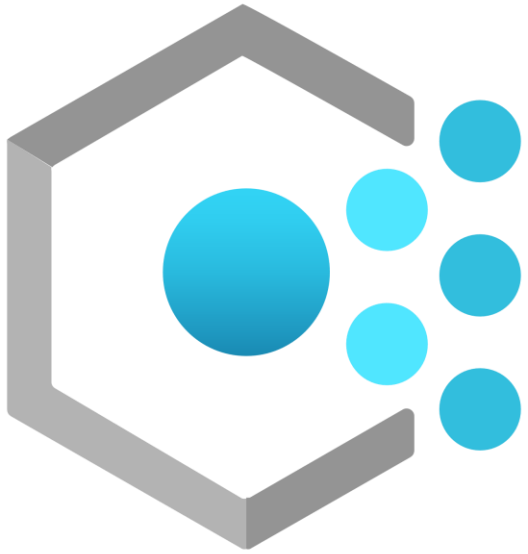
1. Create a policy assignment to require tagging.
2. Create a storage account to test required tagging.
3. View all resources with a specific tag.
4. Delete the policy assignment.



Azure Policy

Azure Policy helps to enforce organizational standards and to assess compliance at-scale. Provides governance and resource consistency with regulatory compliance, security, cost, and management.

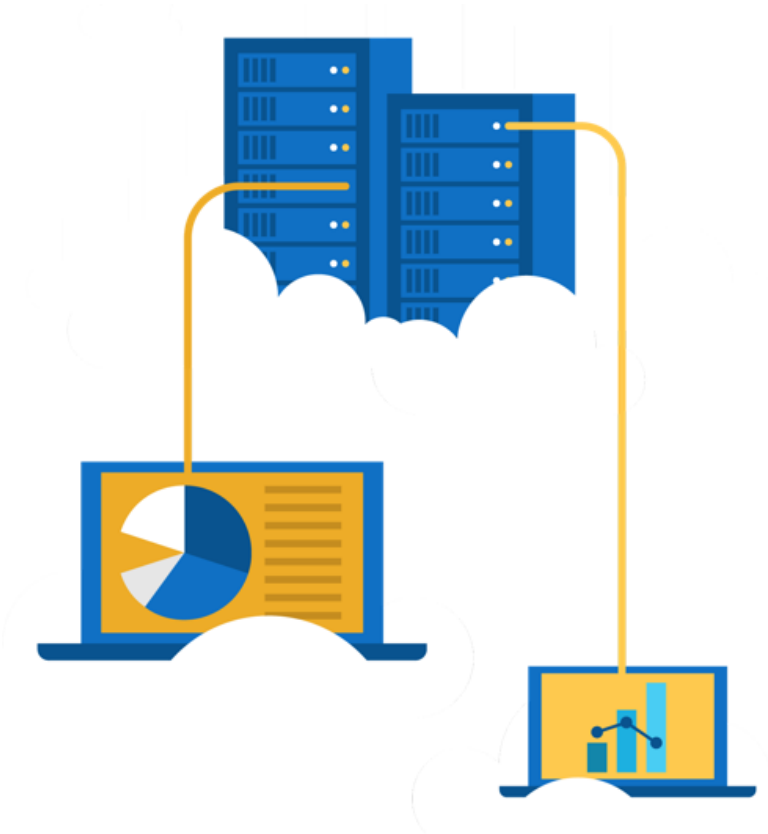
- Evaluates and identifies Azure resources that do not comply with your policies.
- Provides built-in policy and initiative definitions, under categories such as Storage, Networking, Compute, Security Center, and Monitoring.



Walkthrough - Create an Azure Policy

Create an Azure Policy to restrict deployment of Azure resources to a specific location.

1. Create a policy assignment.
2. Test the allowed location policy.
3. Delete the policy assignment.

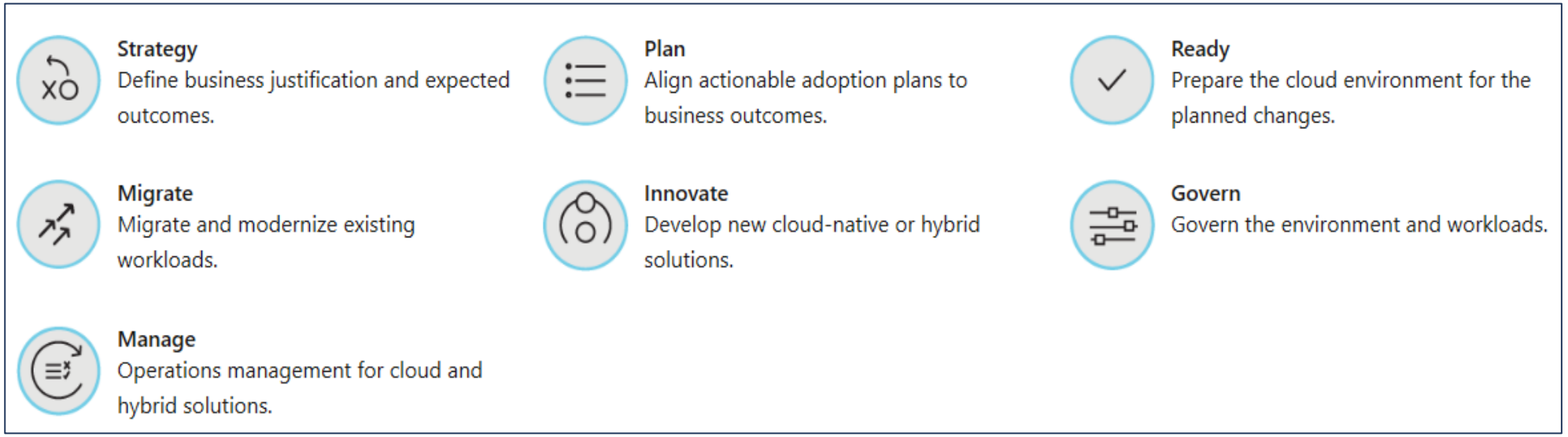


Azure Blueprints

Azure Blueprints makes it possible for development teams to rapidly build and stand up new environments. Development teams can quickly build trust through organizational compliance with a set of built-in components (such as networking) in order to speed up development and delivery.

- Role Assignments
- Policy Assignments
- Azure Resource Manager Templates
- Resource Groups

Cloud Adoption Framework



- The One Microsoft approach to cloud adoption in Azure.
- Best practices from Microsoft employees, partners, and customers.
- Tools, guidance, and narratives for strategies and outcomes.

Privacy, compliance, and data protection standards

Privacy, Compliance, and Data Protection - Objective Domain

Describe the purpose of the:

- Microsoft core tenants of Security, Privacy, and Compliance
- Microsoft Privacy Statement, Online Services Terms (OST) and Data Protection Amendment (DPA)
- Trust Center
- Azure compliance documentation
- Azure Sovereign Regions (Azure Government cloud services and Azure China cloud services)

Security, Privacy, and Compliance

Security: Secure by design. With built in intelligent security, Microsoft helps to protect against known and unknown cyberthreats, using automation and artificial intelligence.

Privacy: We are committed to ensuring the privacy of organizations through our contractual agreements, and by providing user control and transparency.

Compliance: We respect local laws and regulations and provide comprehensive coverage of compliance offerings.

Compliance Terms and Requirements

Microsoft provides the most comprehensive set of compliance offerings (including certifications and attestations) of any cloud service provider. Some compliance offerings include.

CJIS Criminal Justice Information Services	**HIPAA** Health Insurance Portability and Accountability Act
CSA STAR Certification	**ISO/IEC 27018**
EU Model Clauses	**NIST** National Institute of Standards and Technology

Microsoft privacy statement

The Microsoft privacy statement provides openness and honesty about how Microsoft handles the user data collected from its products and services.

The Microsoft privacy statement explains:

- What data Microsoft processes.
- How Microsoft processes it.
- What purposes the data is used for.

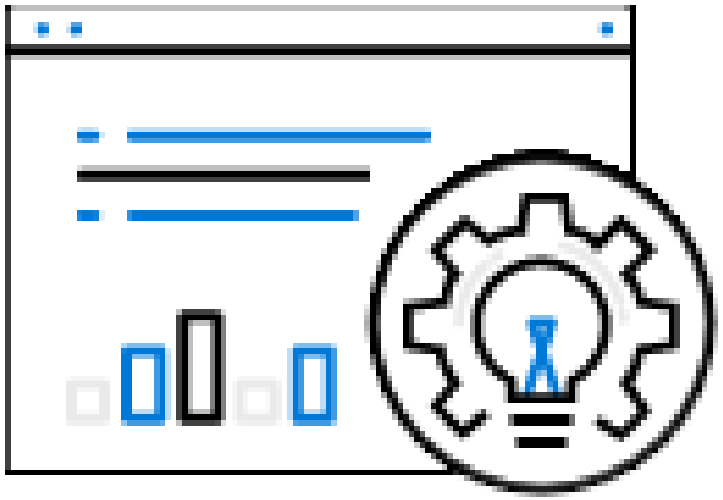
Online Services Terms and Data Protection Addendum

Online Services Terms: The licensing terms define the terms and conditions for the products and Online Services you purchase through Microsoft Volume Licensing programs.

Data Protection Addendum: The DPA sets forth the obligations, with respect to the processing and security of Customer Data and Personal Data, in connection with the Online Services.

Trust Center

Learn about security, privacy, compliance, policies, features, and practices across Microsoft's cloud products.



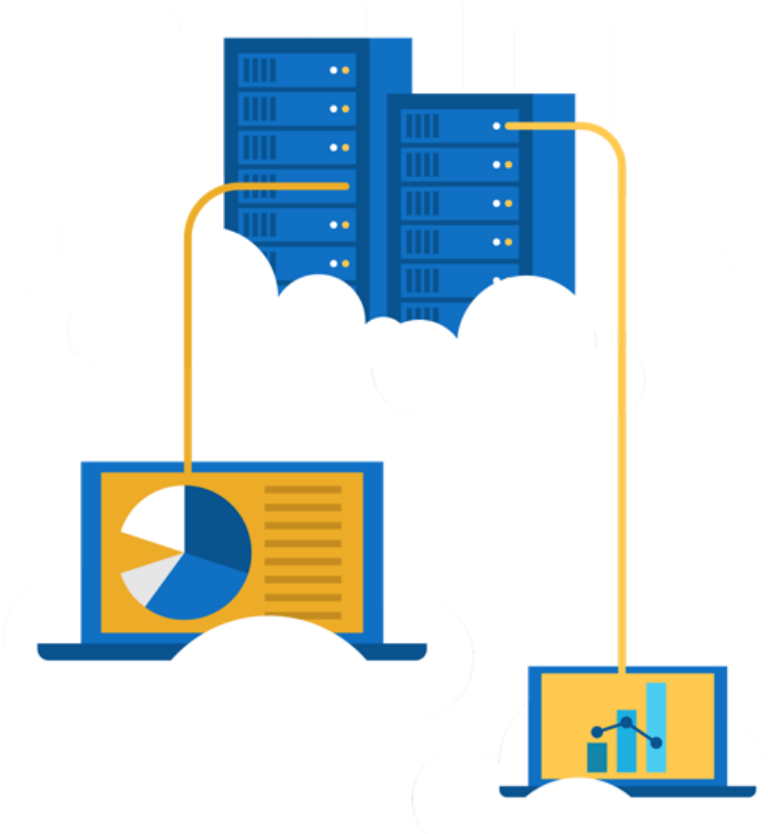
The Trust Center website provides:

- In-depth, expert information.
- Curated lists of recommended resources, arranged by topic.
- Role-specific information for business managers, administrators, engineers, risk assessors, privacy officers, and legal teams.

Walkthrough – Exploring the Trust Center

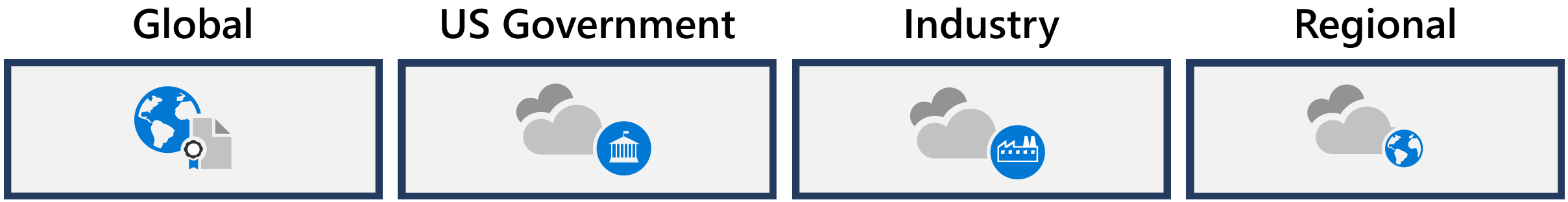
Access the Trust Center, Service Trust Portal (STP), and Compliance Manager.

1. Access the Trust Center.
2. Access the Service Trust Portal.
3. Access the Compliance Manager.



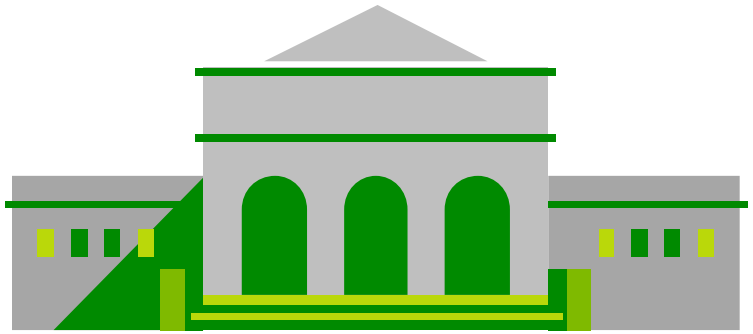
Azure Compliance Documentation

Microsoft offers a comprehensive set of compliance offerings to help your organization comply with national, regional, and industry-specific requirements that govern the collection and use of data.



Azure Sovereign Regions (US Government services)

Meets the security and compliance needs of US federal agencies, state and local governments, and their solution providers.



Azure Government:

- Separate instance of Azure.
- Physically isolated from non-US government deployments.
- Accessible only to screened, authorized personnel.

Examples of compliant standards : FedRAMP, NIST 800.171 (DIB), ITAR, IRS 1075, DoD L2, L4 & L5, and CJIS.

Azure Sovereign Regions (Azure China)

Microsoft is China's first foreign public cloud service provider, in compliance with government regulations.

Azure China features:

- Physically separated instance of Azure cloud services operated by 21Vianet
- All data stays within China to ensure compliance

Module 05 Review

Microsoft Learn Modules
(docs.microsoft.com/Learn)

- Azure identity services
- Authentication versus authorization
- Azure AD, MFA, SSO and Conditional Access
- Azure governance features
- RBAC, Resource locks and tags
- Policy, Blueprints, and CAF
- Azure privacy and compliance
- Privacy Statement, Online Services Terms, Trust Center and compliance documentation.
- Azure Sovereign Regions

© Copyright Microsoft Corporation. All rights reserved.

FOR USE ONLY AS PART OF VIRTUAL TRAINING DAYS PROGRAM. THESE MATERIALS ARE NOT AUTHORIZED FOR DISTRIBUTION, REPRODUCTION OR OTHER USE BY NON-MICROSOFT PARTIES.

Microsoft

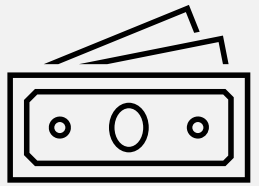
MOD 6: Azure pricing and lifecycles

Module 06 – Outline

You will learn the following concepts:

- **Methods for managing costs**
  - Factors affecting costs
  - Options to reduce and control costs
  - Azure Cost Management
- **Service Level Agreements and Lifecycles**
  - Azure Service Level Agreement (SLA)
  - Factors impacting SLAs
  - Azure product and feature lifecycle

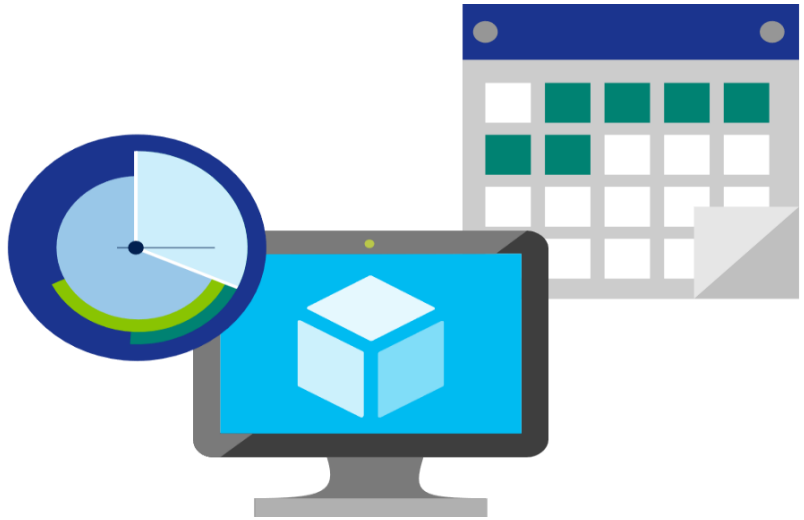
Planning and Cost Management



Planning and Cost Management - Objective Domain

- Identify factors that can affect costs (resource types, services, locations, ingress and egress traffic)
- Identify factors that can reduce costs (reserved instances, reserved capacity, hybrid use benefit, and spot pricing)
- Describe the functionality and usage of the Pricing calculator and the Total Cost of Ownership (TCO) calculator
- Describe the functionality and usage of Azure Cost Management

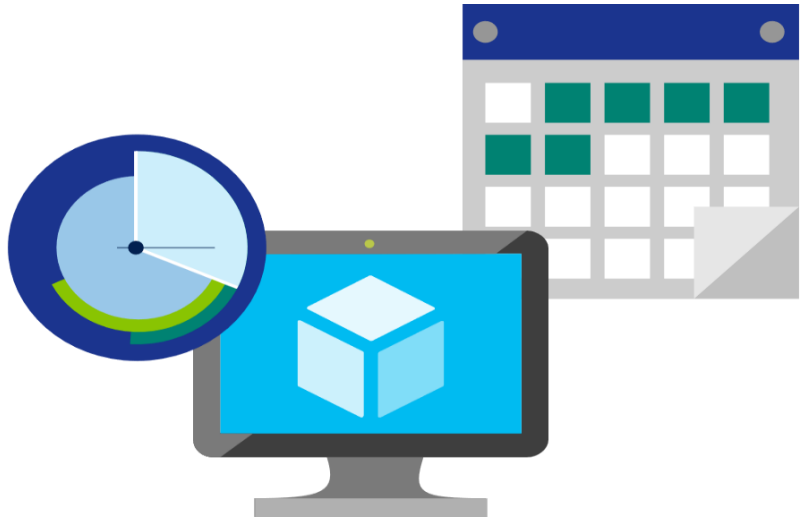
Factors affecting costs (part 1)



There are six primary factors affecting costs:

1) Resource Type	2) Services	3) Location
Costs are resource-specific, so the usage that a meter tracks and the number of meters associated with a resource, depend on the resource type.	Azure usage rates and billing periods can differ between Enterprise, Web Direct, and CSP customers.	The Azure infrastructure is globally distributed, and usage costs might vary between locations that offer Azure products, services, and resources.

Factors affecting costs (part 2)



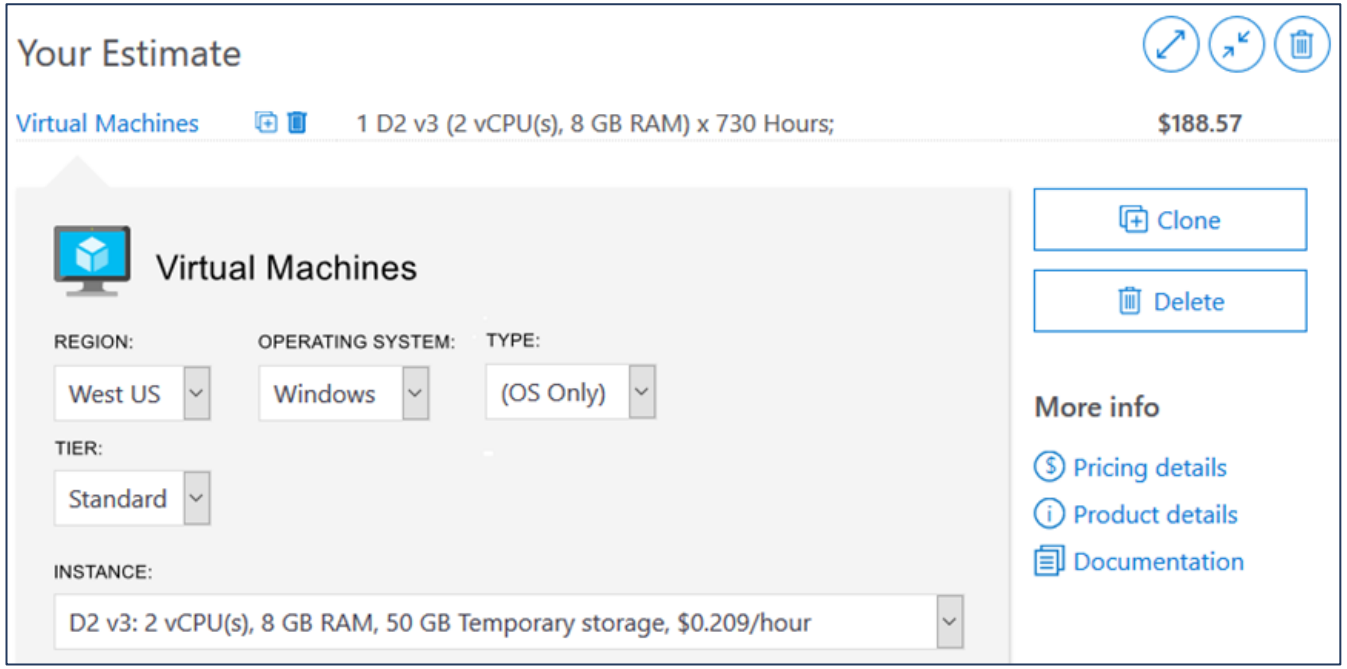
There are six primary factors affecting costs:

4) Bandwidth	5) Reserved Instances	6) Azure Hybrid Use Benefit
Some inbound data transfers are free, such as data going into Azure datacenters. For outbound data transfers, such as data going out of Azure datacenters, pricing is based on Zones.	With Azure Reservations, you commit to buying one-year or three-year plans for multiple products. Reservations can significantly reduce your resource costs up to 72% on pay-as-you-go prices.	For customers with Software Assurance, Azure Hybrid Benefit allows you to use your on-premises licenses on Azure at a reduced cost.

Pricing Calculator

The **Pricing Calculator** is a tool that helps you estimate the cost of Azure products. The options that you can configure in the Pricing Calculator vary between products, but basic configuration options include:

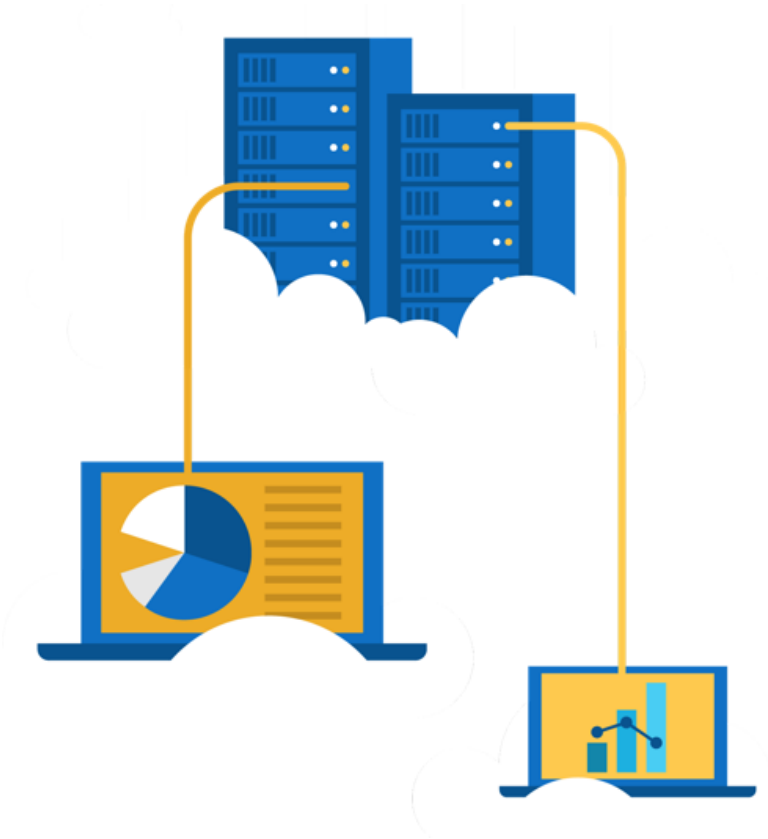
- Region
- Tier
- Billing options
- Support options
- Programs and offers
- Azure dev/test pricing



Walkthrough - Use the Azure Pricing Calculator

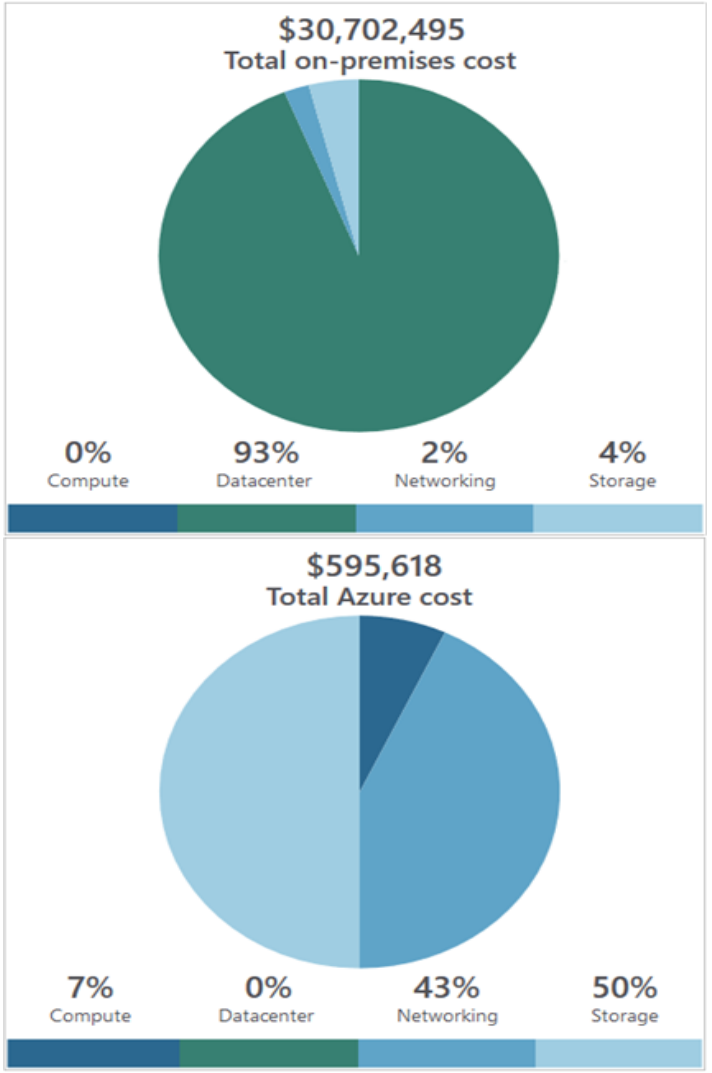
Use the Azure Pricing Calculator to generate a cost estimate for an Azure virtual machine and related network resources.

1. Configure the pricing calculator.
2. Review the pricing estimate.



Total Cost of Ownership Calculator

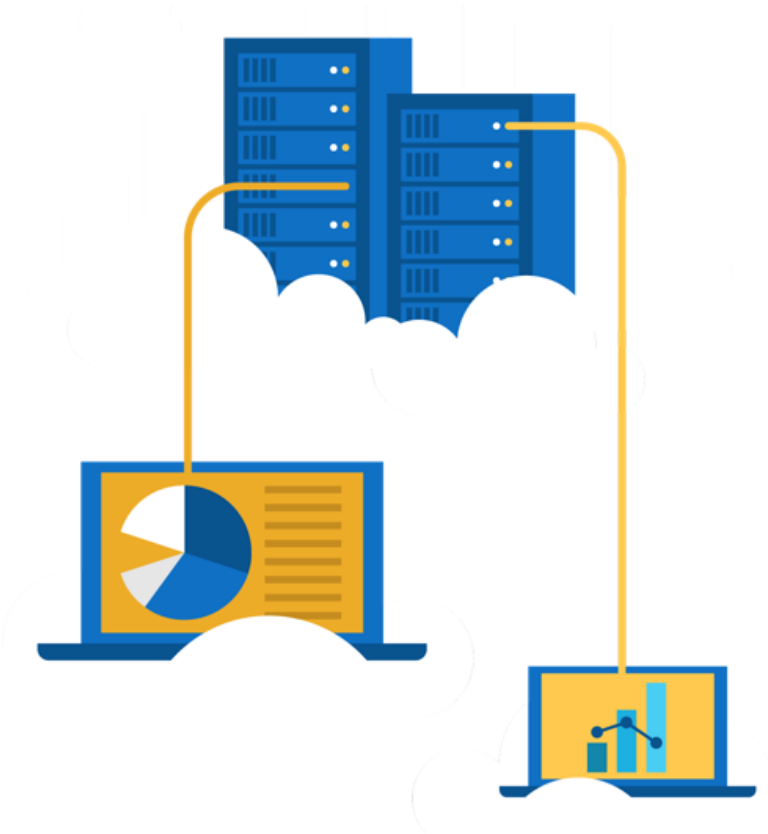
- A tool to estimate cost savings you can realize by migrating to Azure.
- A report compares the costs of on-premises infrastructures with the costs of using Azure products and services in the cloud.



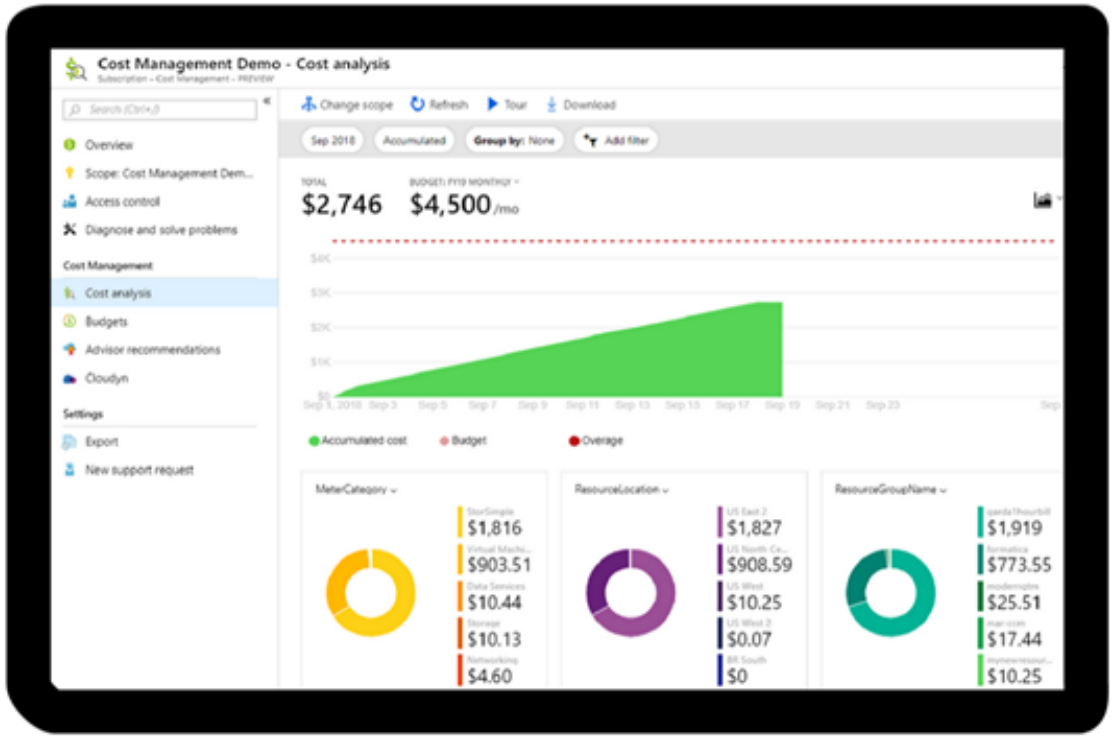
Walkthrough - Use the Azure TCO Calculator

Use the Total Cost of Ownership (TCO) Calculator to generate cost comparison report for an on-premises environment.

1. Configure the TCO calculator.
2. Review the results and save a copy.

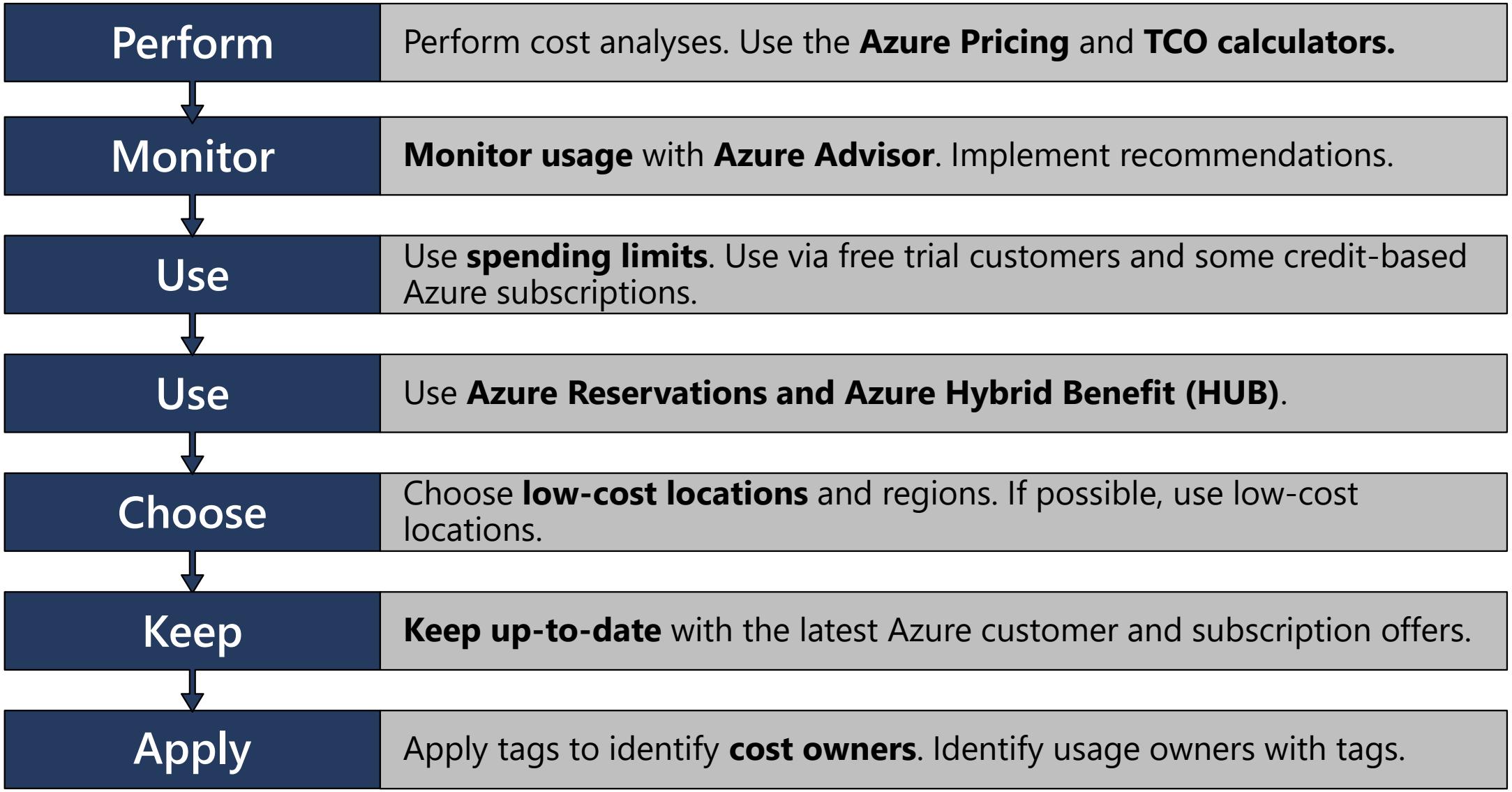


Azure Cost Management

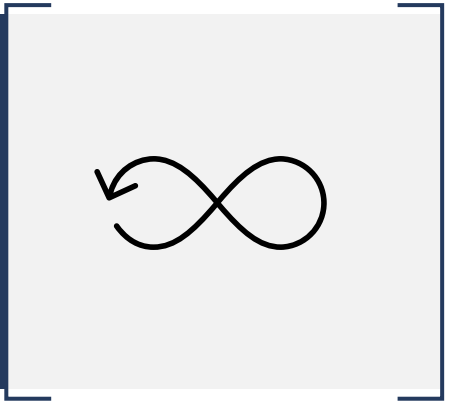


- Reporting – billing reports
- Data enrichment
- Budgets – set spend budget
- Alerting – when cost exceed limits
- Recommendation – cost recommendations

Minimizing costs



Azure SLAs and service lifecycles



Azure SLAs and service lifecycles - Objective Domain

- Describe the purpose of an Azure Service Level Agreement (SLA)
- Identify actions that can impact an SLA (i.e. Availability Zones)
- Describe the service lifecycle in Azure (Public Preview and General Availability)

Service Level Agreements (SLAs)

Service Level Agreements (SLAs) describes Microsoft's commitments for uptime and connectivity.

- SLAs are based on individual products and services.
- Detailed agreements on the service provided, and any exceptions to the SLA.
- Free and preview features/services do not offer SLAs.

SLAs for Azure products and services

- Performance targets are expressed as uptime and connectivity guarantees.
- Performance-targets range from 99% to 99.999%.
- If a service fails to meet the guarantees, a percentage of the monthly service fees can be credited.

SLA	Downtime per month
99%	7h 18m 17s
99.5%	3h 39m 8s
99.9%	43m 49s
99.95%	21m 54s
99.99%	4m 22s
99.999%	26s

Actions that affect SLAs

Lower your SLA

- Adding more services
- Choosing free or non-SLA services

Raise your SLA

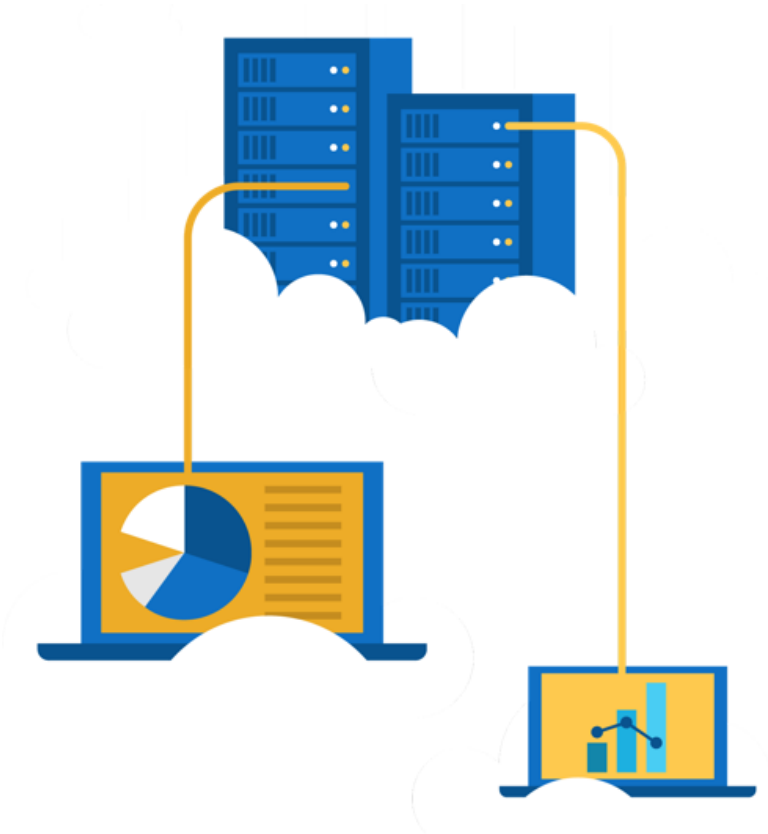
- Availability Zones
- Redundant systems

Many factors can raise or lower your SLA. Design decisions based on business goals will drive your SLA goals.

Walkthrough - Calculate a Composite SLA

Determine services SLA uptime percentages and then calculate the application composite SLA uptime percentage.

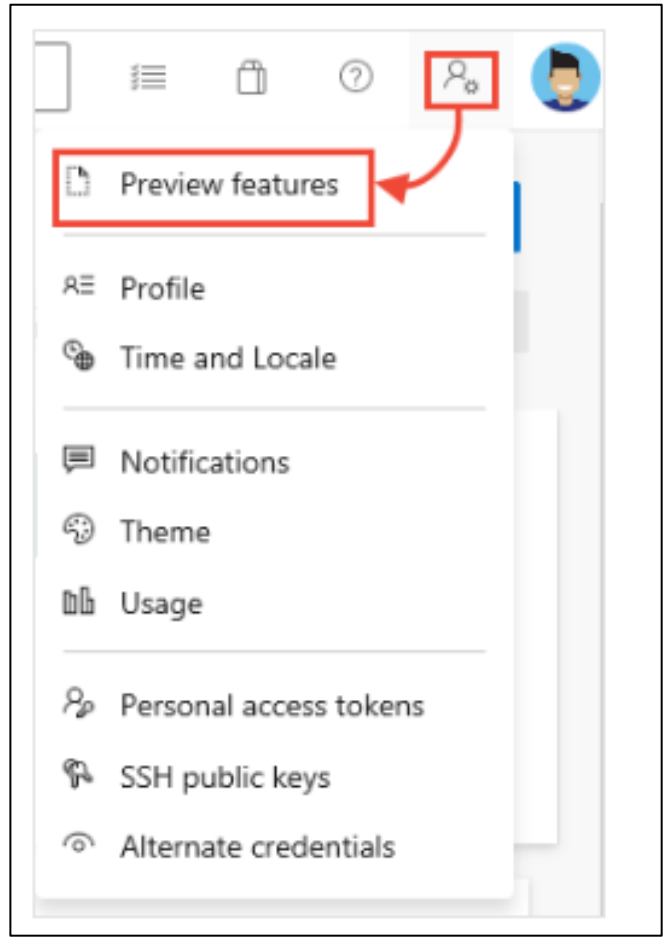
1. Determine the SLA uptime percentage values for an application.
2. Calculate the Application Composite SLA percentage uptime.



Azure Preview Program

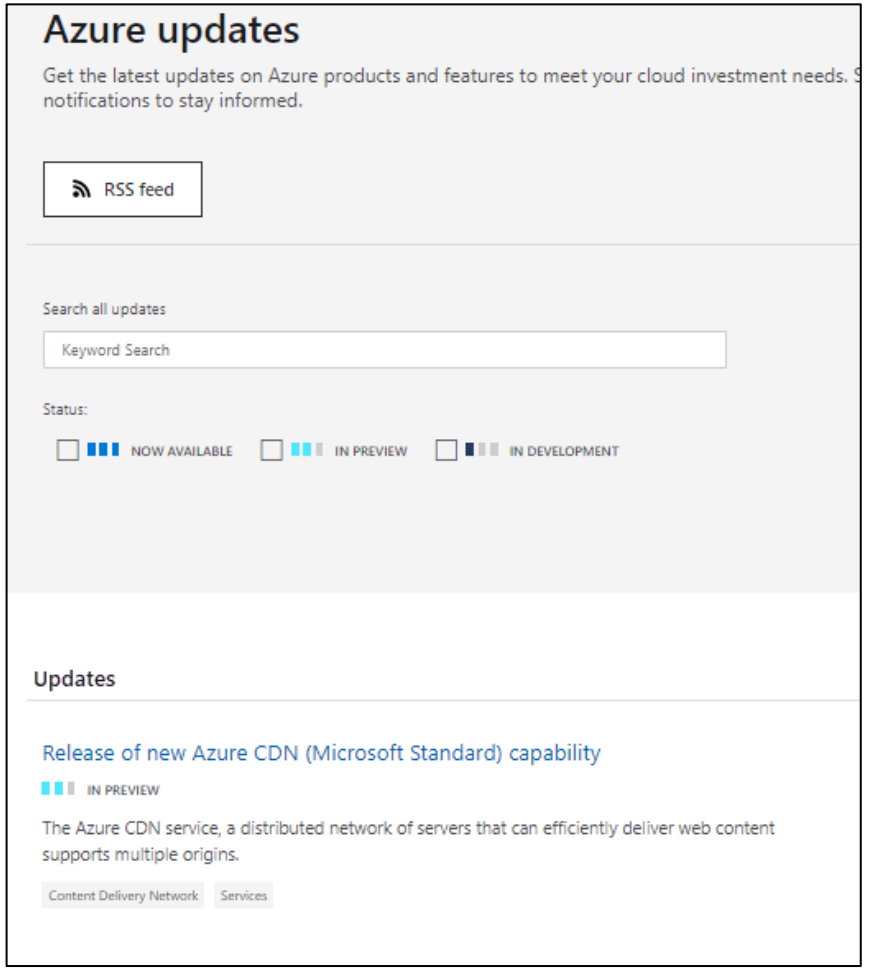
With Azure previews, users can test beta and other pre-release features, products, services, software, and regions to provide feedback.

- **Public Preview:** all Azure customers can evaluate the new features
- **Generally available (GA):** after public preview is completed, all customers can use the feature, and region availability will vary.



Monitoring service and feature updates

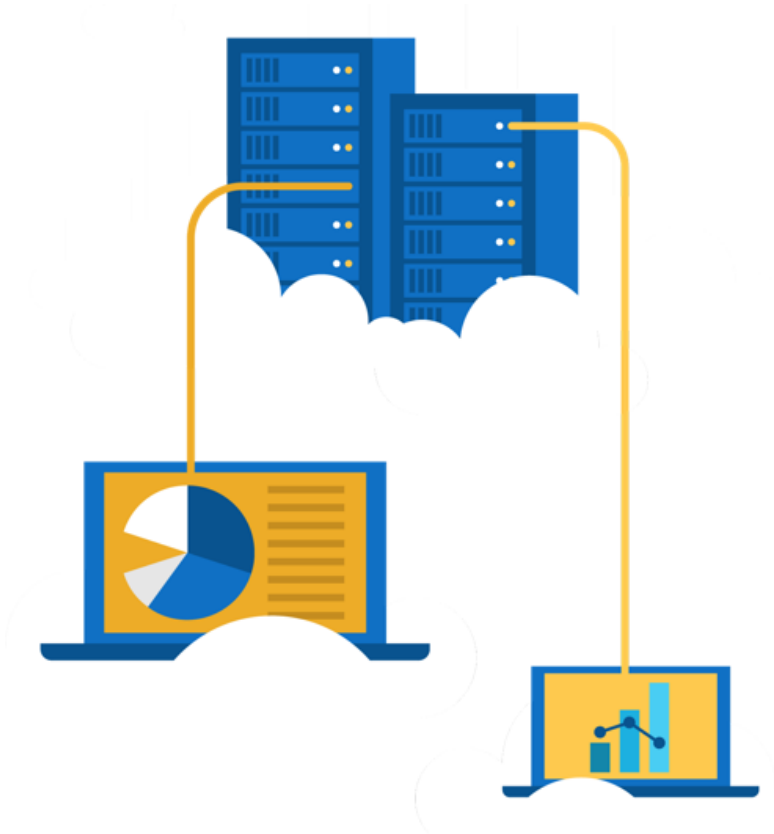
- Azure updates provides information about the Azure products, services, and features, in addition to product roadmaps and availability.
- View details about all Azure updates and their status.
- Browse and search for updates.
- Subscribe to Azure update notifications by RSS.



Walkthrough - Access Azure Preview features

Access and identify Azure preview services and features and view the latest Azure updates information.

1. Access preview services and features.
2. Review the Azure updates page.



Module 06 Review

Microsoft Learn Modules
(docs.microsoft.com/Learn)

- Factors affecting costs
- Recognize Azure Cost Management
- Azure Service Level Agreement (SLA)
- Factors impacting SLAs
- Azure product and feature lifecycle