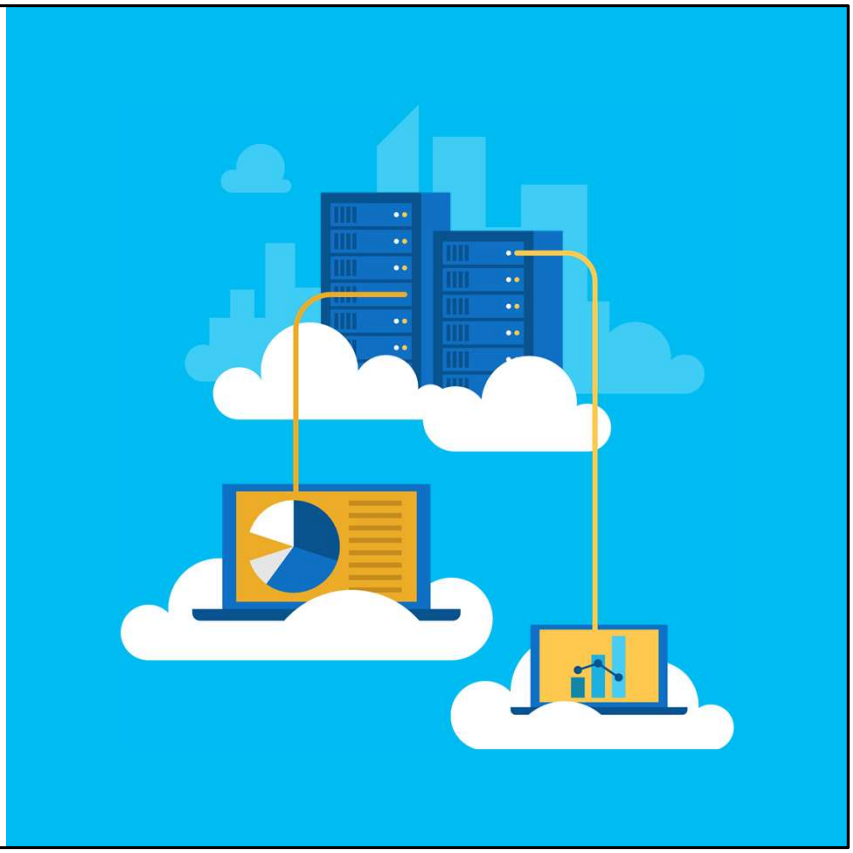
Microsoft

AZ-900T0x

Learning Path:

Examine Microsoft Azure Security, privacy, compliance, and trust



Adjust the cover for either AZ-900T00 or AZ-900T01.

Learning Objectives

You will learn the following concepts:

- Networking
  - Defense in depth
  - Firewalls, DDoS, Network Security Groups, and more
- Azure Identity
  - Authentication, Authorization, and MFA
- Security Tools
  - Azure Security Center
  - Information Protection and Advanced Threat Protection
- Azure Governance, Compliance, and Monitoring
  - Policy and Blueprints
  - Trust Center, Compliance Manager, and Government

This slide is important. We are telling the learners… This is what I am going to tell you.

We then tell them / show them.

At the end we review what we told them.

Then we give them references for further learning.

Then we say Thanks you where we will then put our closing deck for customer feedback…

Module: Securing network connectivity

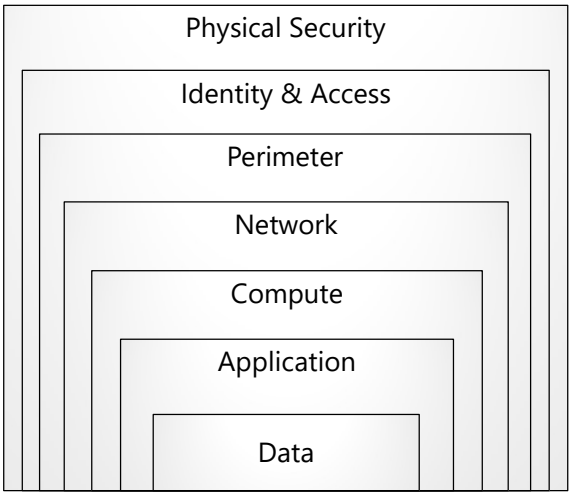
Securing Network Connectivity
Introduction

Learning objectives:

- Learn how security responsibility is shared with Azure
- Learn how identity management provides protection, even outside your network
- Learn how encryption capabilities built into Azure can protect your data

Explore Defense in depth

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



This is conceptual, to be kept high level, explaining how security options can be targeted at each layer.

Define Shared security

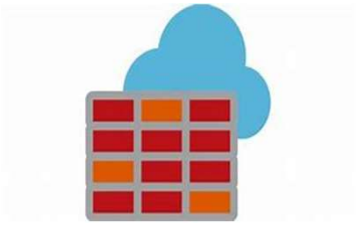
Migrating from customer-controlled to cloud-based datacenters shifts the responsibility for security. Security becomes a shared concern between cloud providers and customers.

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

This is comparable to the Shared Responsibility slide, but specific to security.

Explore Azure Firewall

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



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

✔ Azure Application Gateway also provides a firewall, called the Web Application Firewall (WAF). WAF provides centralized, inbound protection for your web applications against common exploits and vulnerabilities.

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

Azure Firewall - https://azure.microsoft.com/en-us/services/azure-firewall/

Explore Azure Distributed Denial of Service (DDoS) protection

- **What is a DDoS attack?**
- **What does DDoS Protection do?**
  - ❑ Sanitizes unwanted network traffic, before it impacts service availability.
  - ❑ Basic service tier is automatically enabled in Azure.
  - ❑ Standard service tier adds mitigation capabilities, tuned to protect Azure Virtual Network resources.

Azure DDoS Protection - https://azure.microsoft.com/en-us/services/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, tuned to protect Azure

Virtual Network resources.

Define Network Security Groups (NSGs)

Filters 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.
- Override default rules with new, higher priority, rules.

NSG -https://docs.microsoft.com/en-us/azure/virtual-network/security-overview#network-security-groups

Define Application Security Groups (ASGs)

ASGs - provide for the grouping of servers with similar port filtering requirements, and group together servers with similar functions, such as web servers.

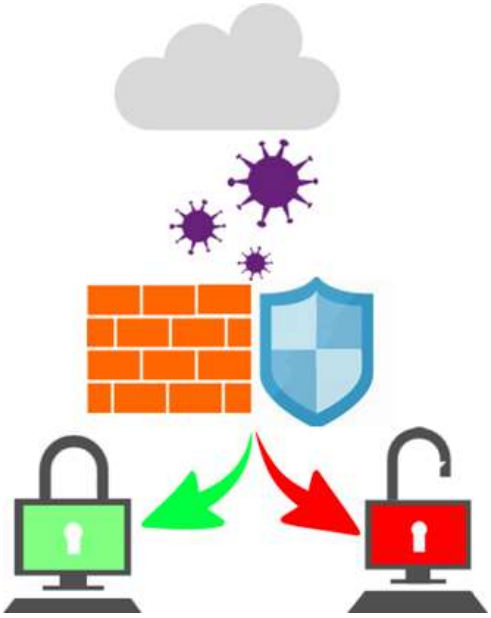
ASG - https://docs.microsoft.com/en-us/azure/virtual-network/security-overview#application-security-groups

- Allows you to reuse your security policy at scale without manual maintenance of explicit IP addresses.
- Handles the complexity of explicit IP addresses and multiple rule sets, allowing you to focus on your business logic.

Choose Azure network security solutions

Azure supports combined network security solutions:

- NSGs with Azure Firewall
- Web Application Firewall (WAF) with Azure Firewall.
- **Perimeter layer** protects your networks' 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.



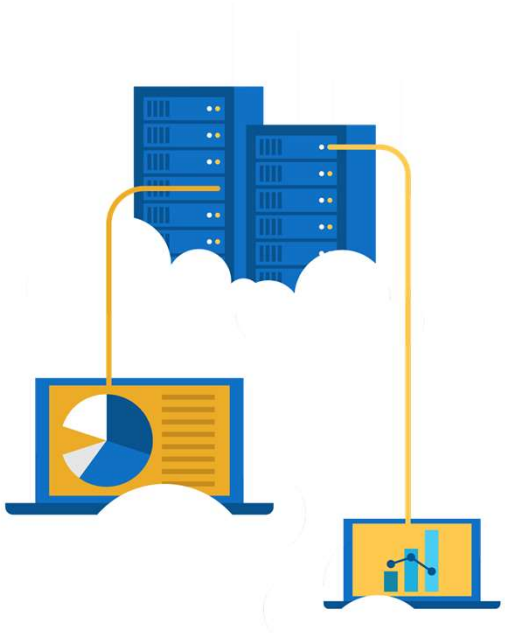
This slide uses the Defense in Depth perimeter and networking layers as examples. Discussing Azure networking security solutions at each layer is beyond the scope of this course.

Microsoft

Walkthrough – Secure network traffic

Create and configure inbound and 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.

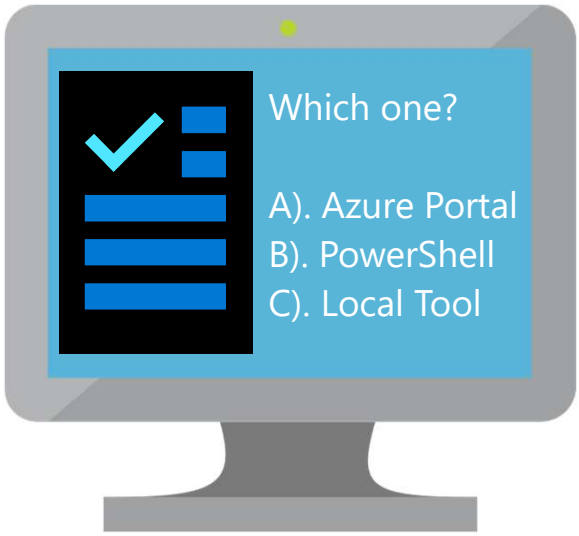


Knowledge Check

Populate with instructions to use the polling tool of your choice

Module:
Securing Network Connectivity

1. Use your Smartphones or Mobile Devices
2. Go to (*insert polling app link of your choice*)
   Enter Code: 123-45-678
3. Please participate in the quiz for this section



WWL recommends using polling to be completed for every 7 – 10 slides and preferably at the end of each section. This helps break classes up and adds more interactivity especially for remote classes.

In order to promote interactivity, WWL suggests the use of Mentimeter, Kahoot or a similar polling technology. Please feel free to adjust this slide as needed and populate with the instructions based on the polling tool of your choice.

Summary: Securing network connectivity

In this module we explored the tools and capabilities to apply network security to your solutions in the cloud. Using a concept of Defense in Depth, you add layers of security onto your systems make it more difficult for attackers to get access to your data.

Module: Core Azure identity services

Core Azure identity services
Introduction

Learning objectives:

- Review authentication versus authorization
- Explain Azure Active Directory
- Explore Azure Multi-factor authentication (MFA)

Compare Authentication and authorization

Two concepts are fundamental to understanding identity and access.

Authentication

Authorization

✔ Authentication is sometimes shortened to *AuthN*, and authorization is sometimes shortened to *AuthZ*.

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.

Explore Azure Active Directory (AD)

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.

Azure AD - https://azure.microsoft.com/en-us/services/active-directory/

Explore Azure Multi-Factor Authentication

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

Discuss what could qualify for each of the items listed

- *Something you know*: This could be a password or the answer to a security question.
- *Something you possess*: This might be a mobile app that receives a notification, or a token-generating device.
- *Something you are*: This is typically some sort of biometric property, such as a fingerprint or face scan used on many mobile devices.

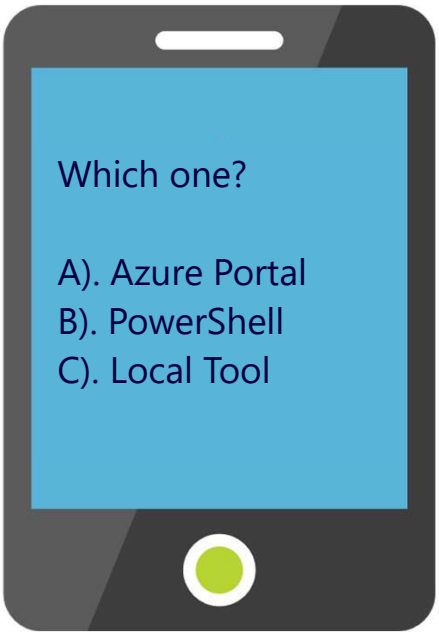
MFA - https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks

Knowledge Check

Populate with instructions to use the polling tool of your choice

Module:
Core Azure Identity Services

1. Use your Smartphones or Mobile Devices
2. Go to *(insert polling app link of your choice)*
3. Enter Code: 123-45-678
4. Please participate in the quiz for this section



WWL recommends using polling to be completed for every 7 – 10 slides and preferably at the end of each section. This helps break classes up and adds more interactivity especially for remote classes.

In order to promote interactivity, WWL suggests the use of Mentimeter, Kahoot or a similar polling technology. Please feel free to adjust this slide as needed and populate with the instructions based on the polling tool of your choice.

Summary: Core Azure Identity Services

Identity allows us to maintain a security perimeter, even outside our physical control. With single sign-on and appropriate role-based access configuration, we can always be sure who has the ability to see and manipulate our data and infrastructure.

In this module you learned about:

- Authentication versus authorization
- Azure Active Directory
- Azure Multi-factor authentication (MFA)

Module: Security tools and features

Security Tools and Features
Introduction

Learning objectives:

- Examine Azure Security Center.
- List the capabilities of Azure Key Vault.
- Explore Azure Information Protection and Azure Threat Protection.

Explore Azure Security Center

A monitoring service that provides threat protection across all your Azure, and on-premises, services.

- Security recommendations
- Monitors security settings
- Automatically applies your security policies

Azure Security https://azure.microsoft.com/en-us/services/security-center/

- Provides security recommendations based on your configurations, resources, and networks.
- Monitors security settings across your on-premises and cloud workloads.
- Automatically applies your security policies to any new services you provision.

Walkthrough: Azure Security Center usage scenarios

You can use Security Center in the *Detect*, *Assess*, and *Diagnose* stages of an incident response.

Azure Security Center planning and operations guide - https://docs.microsoft.com/en-us/azure/security-center/security-center-planning-and-operations-guide

Explore Azure Key Vault

Stores application secrets in a centralized cloud location, to securely control access permissions, and access logging.

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

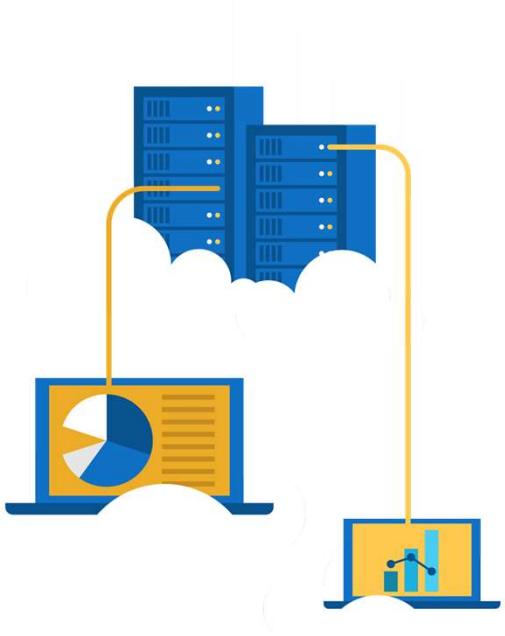
Azure Key Vault -https://azure.microsoft.com/en-us/services/key-vault/

Microsoft

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.



Define Azure Information Protection (AIP)

Classifies and protects documents, and emails, by applying labels.

- Automatically using rules and conditions defined by administrators.
- Manually, by users.
- By combining automatic and manual methods, guided by recommendations.

For purchasing details, see : https://azure.microsoft.com/en-us/pricing/details/information-protection/
AIP - https://docs.microsoft.com/en-us/azure/information-protection/what-is-information-protection

- Automatically using rules and conditions defined by administrators.
- Manually, by users.
- By combining automatic and manual methods, guided by recommendations.

Define Azure Advanced Threat Protection (Azure ATP)

Cloud-based security solution for identifying, detecting, and investigating advanced threats, compromised identities, and malicious insider actions.

- Dedicated **portal** for monitoring and responding to suspicious activity.
- **Sensors** installed directly onto your domain controllers.
- **Cloud service** runs on Azure infrastructure.

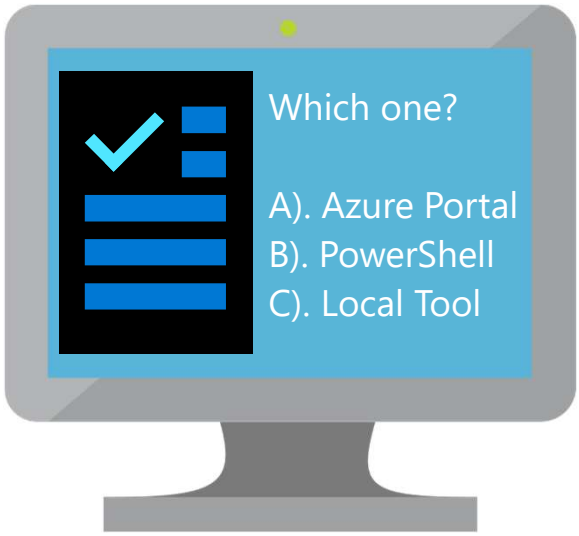
ATP - https://azure.microsoft.com/en-us/features/azure-advanced-threat-protection/

Knowledge Check

Populate with instructions to use the polling tool of your choice

Module:
Security Tools and Features

1. Use your Smartphones or Mobile Devices
2. Go to (*insert polling app link of your choice*)
   Enter Code: 123-45-678
3. Please participate in the quiz for this section



WWL recommends using polling to be completed for every 7 – 10 slides and preferably at the end of each section. This helps break classes up and adds more interactivity especially for remote classes.

In order to promote interactivity, WWL suggests the use of Mentimeter, Kahoot or a similar polling technology. Please feel free to adjust this slide as needed and populate with the instructions based on the polling tool of your choice.

Summary: Security Tools and Features

This module is only introductory. Security is a deep and complex topic, so whatever your cloud approach, an ongoing security education is necessary. But this module should get you started in the right direction.

We explored:

- Azure Security Center.
- Azure Key Vault.
- Azure Information Protection
- Azure Threat Protection.

Module: Azure Governance methodologies

Azure Governance Methodologies
Introduction

Learning objectives:

- Apply policies to control and audit resource creation.
- Learn how role-based security can fine-tune access to your resources.
- Review Microsoft's policies and privacy guarantees.
- Learn how to monitor your resources.

Define Azure Policy

Azure Policy is a service to create, assign, and, manage policies. These policies enforce different rules and effects over your resources, so those resources stay compliant with your corporate standards and service-level agreements (SLAs).

Azure Policy - https://azure.microsoft.com/en-us/services/azure-policy

Stay compliant with your corporate standards and service level agreements (SLAs) by using policy definitions to enforce rules and effects for your Azure resources.

- 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.

Implementing Azure Policy

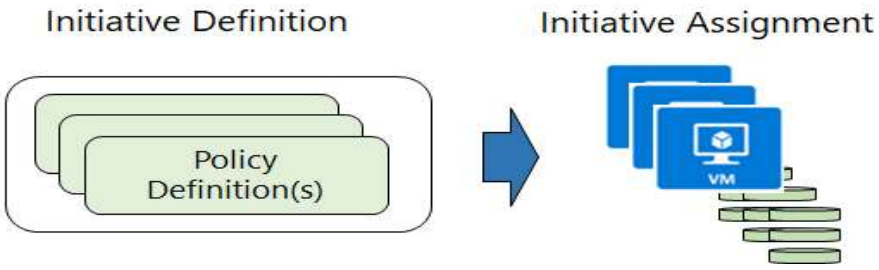
Create a policy definition → Assign the definition to resources → Review the evaluation results

A policy definition expresses what to evaluate and what action to take. Implement your policy definition by assigning it to a group of resources. Review the results. Results are either compliant or non-compliant.

✔ Policy evaluation happens about once an hour, which means that if you make changes to your policy definition and create a policy assignment then it will be re-evaluated over your resources within the hour.

Azure Policy Samples - https://docs.microsoft.com/en-us/azure/governance/policy/samples/

Define Policy Initiatives



Policy Initiatives work with Azure Policies

- **Initiative definitions g**roup multiple policy definitions into a single unit, to track compliance at a higher scope. For example, one initiative can monitor all your Azure Security Center recommendations.
- **Initiative assignments** are assigned to a specific scope and reduce the need to make an initiative definition for each scope.

Walkthrough - Create an Azure Policy

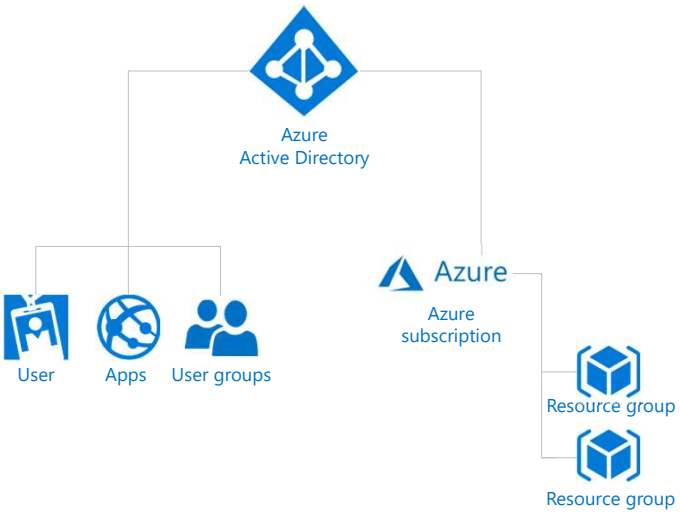
Create an Azure Policy to restrict deployment of Azure resources to a specific location.

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

You can use this as a demonstration, have the students step through the tasks together, or have the students try it themselves.

Explore Role-based access control (RBAC)

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



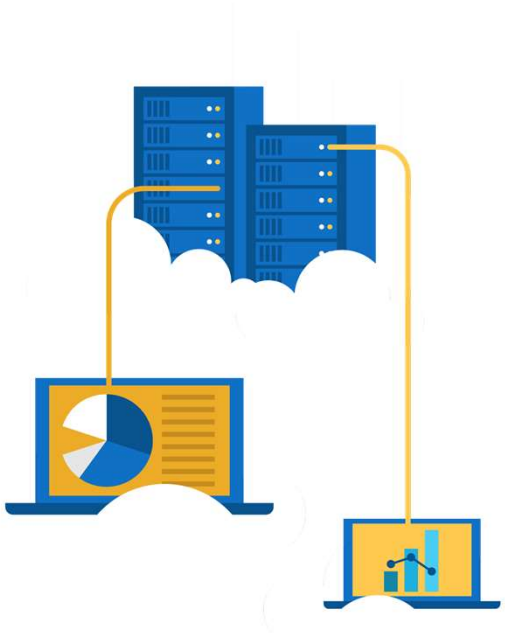
Azure RBAC - https://docs.microsoft.com/en-us/azure/role-based-access-control/overview

Microsoft

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.



Define Resource locks

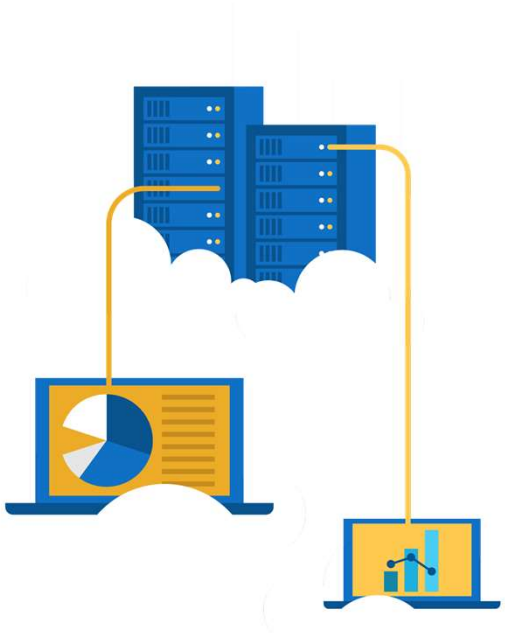
Lock Types	Read	Update	Delete
CanNotDelete	Yes	Yes	No
ReadOnly	Yes	No	No

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

Resource Locks - https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources

Microsoft

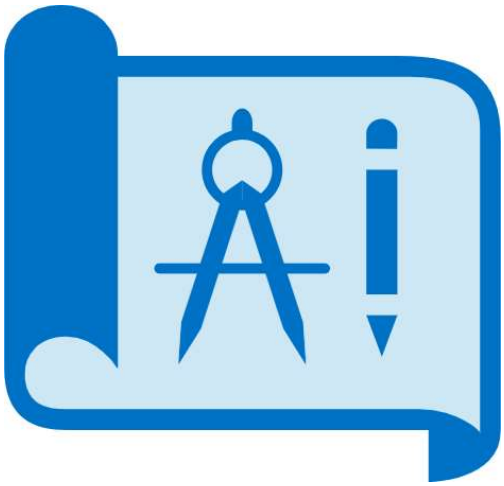
Walkthrough – Manage Resource Locks



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

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.

Explore Azure Blueprints



Create reusable environment definitions that can recreate your Azure resources, like VMs, and apply your policies instantly.

Azure Blueprints - https://azure.microsoft.com/en-us/services/blueprints/

- Help audit and trace your deployments, and maintain compliance using built-in tools and artifacts.
- Associate blueprints with specific Azure DevOps build artifacts, and release pipelines, for rigorous tracking.

Define Subscription Governance

There are mainly three aspects to consider in relation to creating and managing subscriptions.

Billing	**Reports and chargeback can be generated per subscriptions**
Access Control	A subscription is a deployment boundary for Azure resources and can set up role-based access control.
Subscription Limits	Subscriptions are also bound to some hard limitations. If there is a need to go over those limits, then additional subscriptions may be needed. If you hit a hard limit, there is no flexibility.

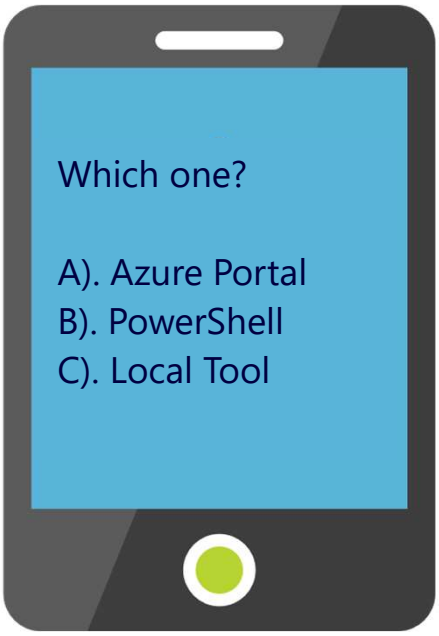
✔ There is more information about subscription limits - https://docs.microsoft.com/en-us/azure/azure-subscription-service-limits

Knowledge Check

Populate with instructions to use the polling tool of your choice

Module:
Azure Governance Methodologies

1. Use your Smartphones or Mobile Devices
2. Go to *(insert polling app link of your choice)*
3. Enter Code: 123-45-678
4. Please participate in the quiz for this section



WWL recommends using polling to be completed for every 7 – 10 slides and preferably at the end of each section. This helps break classes up and adds more interactivity especially for remote classes.

In order to promote interactivity, WWL suggests the use of Mentimeter, Kahoot or a similar polling technology. Please feel free to adjust this slide as needed and populate with the instructions based on the polling tool of your choice.

Summary: Azure Governance Methodologies

Within this module we learned how policy, blueprints, resource locks and other tools like RBAC can help you govern you content.

During this module we explored:

- Apply policies to control and audit resource creation.
- Learn how role-based security can fine-tune access to your resources.
- Review Microsoft's policies.
- Learn how to monitor your resources.

Module: Monitoring and reporting in Azure

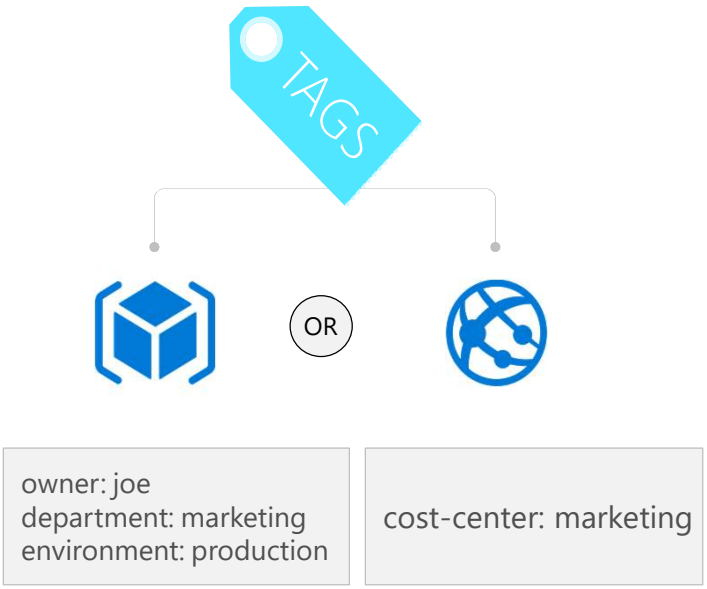
Monitoring and Reporting
Introduction

Learning Objectives:

- Review resource tags and the value of using them.
- Monitor the health of your Azure solutions and systems.
- Check on the help of Azure and its components.

Explore Tags

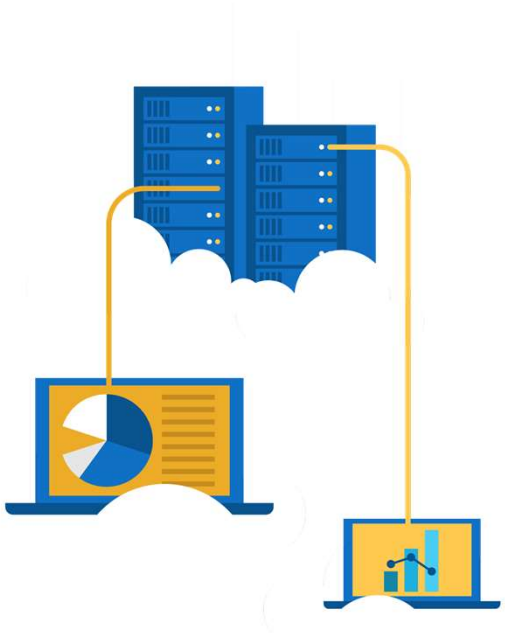
- Provides metadata for your Azure resources.
- Logically organizes resources into a taxonomy.
- Consists of a name-value pair.
- Very useful for rolling up billing information.



Tags - https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags

Microsoft

Walkthrough – Implement resource tagging



Create a policy assignment that requires tagging, create a storage account and test the tagging, view resources with a specified tag, and remove the tagging policy.

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.

Explore Azure Monitor

Collect, analyse, and act on telemetry from cloud and on-premises environments, to maximize your applications' availability and performance.

Azure Monitor - https://azure.microsoft.com/en-us/services/monitor/

- Starts collecting data as soon as you create an Azure subscription and add resources.
- Activity Logs record all resource creation and modification events.
- Metrics measure resource performance and consumption.
- Add an Azure monitor agent to collect operational data for a resource.

Explore Azure Service Health

Evaluate the impact of Azure service issues with personalized guidance and support, notifications, and issue resolution updates.

Azure Status	Service Health	Azure Resource Health

Azure Service Health - https://azure.microsoft.com/en-us/services/monitor/

Components of Azure service health :

- Azure Status provides a global overview Azure services' state of health.
- Service Health has a customizable dashboard for tracking the state of services in the regions you use.
- Azure Resource Health can diagnose and obtain support

for Azure service issues affecting your resources.

Monitor applications and services

Integrate Azure Monitor with other Azure services to improve your data monitoring capabilities and gain better insights into your operations.

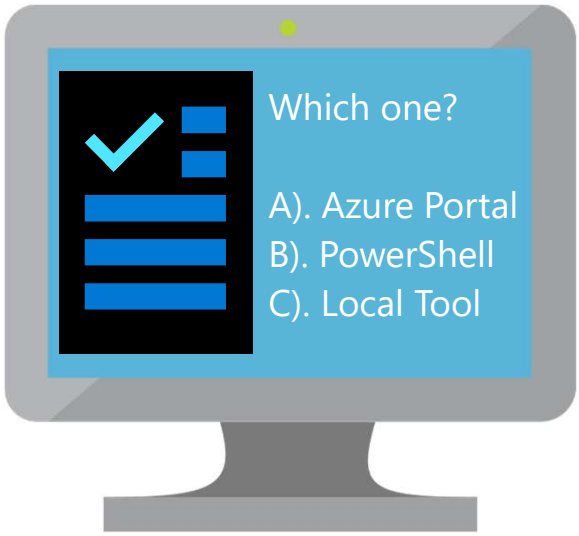
Analyze	Use variants of Azure Monitor for resources (containers, virtual machines, etc.), with Azure Application Insights for applications.
Respond	Azure Alerts can respond proactively to critical conditions identified in your monitor data and use Auto-scale with Azure Monitor Metrics.
Visualize	Use Azure Monitor data to create interactive visualizations, charts, and tables with Power BI.
Integrate	Integrate Azure Monitor with other systems to build customized solutions to suit your needs and requirements.

Knowledge Check

Populate with instructions to use the polling tool of your choice

Module:
Monitoring and Reporting

1. Use your Smartphones or Mobile Devices
2. Go to (*insert polling app link of your choice*)
   Enter Code: 123-45-678
3. Please participate in the quiz for this section



WWL recommends using polling to be completed for every 7 – 10 slides and preferably at the end of each section. This helps break classes up and adds more interactivity especially for remote classes.

In order to promote interactivity, WWL suggests the use of Mentimeter, Kahoot or a similar polling technology. Please feel free to adjust this slide as needed and populate with the instructions based on the polling tool of your choice.

Summary: Monitoring and Reporting

During this module we learned about several great tools to help us monitor the health of our solutions in Azure.

We looked at:

- The use and value of resource tagging.
- How to use Azure Monitor.
- Why Azure Service Health can keep us up to date on how Azure and our solutions are running.

Module: Privacy, compliance, and data protection standards

Privacy, Compliance, and Data Protection
Introduction

Learning objectives:

- List compliance terms and requirements
- Review the Microsoft Privacy Statement
- Explore the Trust Center, Compliance Manager, and Service Trust Portal
- Explain government specific Azure capabilities

Explore 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**
General Data Protection Regulation (GDPR)	**National Institute of Standards and Technology (NIST)**

Should discuss the questions below with students. When selecting a cloud provider to host your solutions, you should understand how that provider can help you comply with regulations and standards. Some questions to ask about a potential provider include:

- How compliant is the cloud provider when it comes to handling sensitive data?
- How compliant are the services offered by the cloud provider?
- How can I deploy my own cloud-based solutions to scenarios that have accreditation or compliance requirements?

You can view all the Microsoft compliance offerings at Microsoft Compliance Center - Compliance Offerings

Identify 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.

Microsoft's Privacy Statement at - microsoft.com/privacystatement

Explore 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.

Trust Center - https://www.microsoft.com/trustcenter

Explore Service Trust Portal (STP)

A Trust Center companion website for compliance-related publications about Microsoft cloud services. Hosts the Compliance Manager service.

Use STP to access :

- Audit reports across Microsoft cloud services.
- Guides to using Microsoft cloud services for regulatory compliance.
- Publications about trust, and how Microsoft cloud services protect your data.

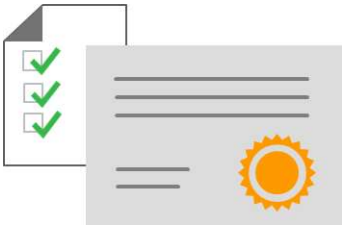
STP - https://servicetrust.microsoft.com/

Explore Compliance Manager

Workflow-based, risk assessment tool in Trust Portal that supports your organization's regulatory compliance activities.

Compliance Manager features :

- Assign, track, and verify your compliance and assessment-related activities.
- Provides a score by evaluating your compliance status.
- Stores and manages your compliance-related artifacts in a secure digital repository.



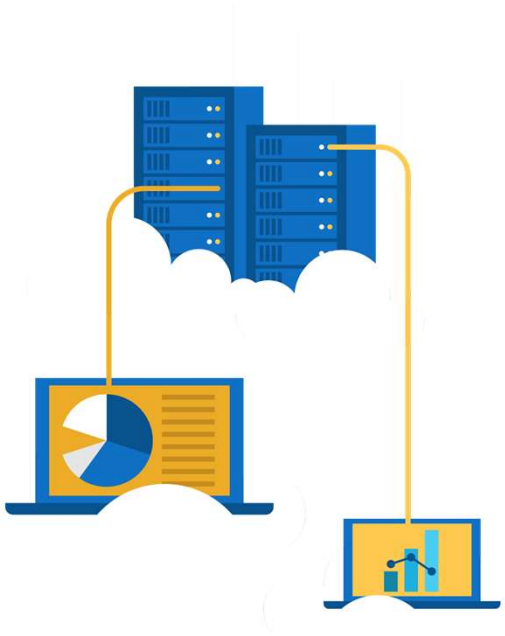
✔ Compliance Manager is a dashboard that provides a summary of your data protection and compliance status, as well as recommendations to improve your data protection and compliance status. The Customer Actions provided in Compliance Manager are recommendations only. Each organization must evaluate the effectiveness of these recommendations, in their respective regulatory environment, prior to implementation. Compliance Manager recommendations should not be interpreted as a guarantee of compliance.

Microsoft

Walkthrough – Explore 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.



Identify Azure 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 Government - https://azure.microsoft.com/en-us/global-infrastructure/government/

Acronym explanations

- FedRAMP : US Federal Risk and Authorization Management Program (FedRAMP) is a standardized approach for assessing, monitoring, and authorizing cloud computing products and services under the US Federal Information Security Management Act (FISMA).
- NIST 800.171 (DIB) : National Institute of Standards and Technology (NIST) 800.171 standardizes security requirements for handling US Federal controlled unclassified information.
- ITAR : International Traffic in Arms Regulations (ITAR) relate to managing the export and import of defense articles.
- IRS 1075 : US Internal Revenue Service Publication 1075 contains guidelines for US government agencies to protect Federal tax information.
- DoD L2, L4 & L5 : US Department of Defense (DoD) Levels 2, 4, and 5 are security authorization requirements for cloud service providers that host DoD information, systems, and applications.
- CJIS : US Criminal Justice Information Services' (CJIS) policies establish security requirements and controls to safeguard criminal justice information.

Identify Azure China 21Vianet

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

Azure China 21Vianet features:

- Physically separated instance of Azure cloud services, located in China.
- Pperated by 21Vianet (Azure China 21Vianet).

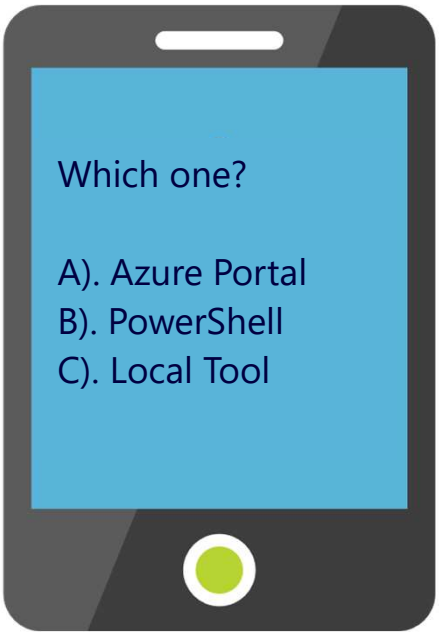
Azure China 21Vianet - https://docs.microsoft.com/en-us/azure/china/

Knowledge Check

Populate with instructions to use the polling tool of your choice

Module:
Privacy, Compliance, and Data Protection

1. Use your Smartphones or Mobile Devices
2. Go to *(insert polling app link of your choice)*
3. Enter Code: 123-45-678
4. Please participate in the quiz for this section



WWL recommends using polling to be completed for every 7 – 10 slides and preferably at the end of each section. This helps break classes up and adds more interactivity especially for remote classes.

In order to promote interactivity, WWL suggests the use of Mentimeter, Kahoot or a similar polling technology. Please feel free to adjust this slide as needed and populate with the instructions based on the polling tool of your choice.

Summary: Privacy, Compliance, and Data Protection

In this module we learned how Microsoft and Azure are designed and provide tools to help you be more compliant, trust in your solutions, and work with Azure in a government scenario if you need that capability.

We learned about:

- Compliance terms and requirements
- The Microsoft Privacy Statement
- The Trust Center, Compliance Manager, and Service Trust Portal
- Government Azure capabilities

Learning Path review

As you have time, cover the module review questions in the student materials.