Exam SC-100: Exam SC-100 Microsoft Cybersecurity Architect STUDY GUIDE

https://docs.microsoft.com/en-us/learn/certifications/exams/sc-100

To earn the **Microsoft Certified: Cybersecurity Architect Expert** certification you need to complete the following requirements as outlined below.

Complete (pass) any (1) one of the following prerequisite certifications:

MS-500 - Microsoft 365 Certified: Security Administrator Associate
Exam MS-500: Microsoft 365 Security Administration
OR
AZ-500 - Microsoft Certified: Azure Security Engineer Associate
Exam AZ-500: Microsoft Azure Security Technologies
OR
SC-200 - Microsoft Certified: Security Operations Analyst Associate
Exam SC-200: Microsoft Security Operations Analyst
OR
SC-300 - Microsoft Certified: Identity and Access Administrator Associate
Exam SC-300: Microsoft Identity and Access Administrator

AND

Pass the **SC-100: Microsoft Cybersecurity Architect** exam.

Passing one of the prerequisite certifications **AND** the SC-100 will grant you the **Microsoft Certified: Cybersecurity Architect Expert** certification.

Find out how you can stay current with in-demand skills through free certification renewals and understand how you can renew your Microsoft Certification

Prepare for the exam structure

SC-100 is scored out of 1000 possible points with a passing score of 700. You will have two to three hours seat time to complete the exam. (For more specific information please see **Exam duration and question types | Microsoft Docs**)

Many test takers report that they have more than enough time to complete it, but be cautious of the clock. The exam has a lot of reading involved, sometimes several paragraphs for a single question.

Passing score: 700

Learn more about exam scores

Exam scoring and score reports | Microsoft Docs

Exam Style and Format

All Microsoft exams have some level of division and segmentation to them. Most will have some or all of four different segment types - Case Studies, General Questions, Scenarios, and in some situations, simulations.

You may have some elements and not others, or you may end up with an exam will all of the elements.

Case Studies
In the case studies you will have several areas of information provided to you so you can learn about a particular business situation. Sometimes you're presented with an exam where you have one case study first and then regular exam questions after. I've had situations where I had all my general questions first and then I was delivered with the case study scenarios. I have even had exams where I've had two scenarios - one case study at the start of the exam, then general questions, and then another case study at the end. Honestly, you won't know what you have until you're in the actual exam what you're going to be delivered in the exam itself.

With direct respect to the cases studies themselves and the navigation, once you click next you will advance through a series of questions about the business' Azure solutions. One suggested best practice for this section is to resist the urge to read the case information first. Instead, *read the questions first*. This will help you zero in on the areas that you really need to pay special attention to as you're going through the case information. Once you answer all the questions for a case study, you will not be allowed to return to it.

If you are taking the exam at a testing center, you will be able to take notes on erasable laminate boards to document the case study's questions and key information if you wish. This can be *extremely* helpful if you like that kind of organization and referencing of notes. However, if you're taking the exam from home with an online proctor you will not be allowed to have paper of any kind. For this reason, it may be worth it to schedule the exam at a test center if you can and / or based on your needs to use the temporary note space.

General Questions
After any case study sections, the exam will move to general questions of various types.

- **Multiple choice in different forms:**
  - One correct response and three (or more) incorrect responses
  - Two or more correct responses out of five or more options
- **Drag and drop:**
  - Move the response to the correct description
- **Sort and order**
  - Move some or all elements from one side of the screen to the opposite side and place them in the correct order of execution, operation, etc.
- **Hot area:**
  - Screenshot, picture, or diagram is given; you need to select an area (target) to what you would need to solve the question asked.

For any of these types, some considerations are:

- Take the questions at face value. Don't make any assumptions or consider unstated business factors.
- Look for superlative phrases that define the business need. Phrases such as "lowest cost", "simplest solution", "highest availability", "least amount of administrative effort" and so on are key elements and drivers differentiate between two potentially correct answers. One will be better than the other based on the requirements set by the question. Sometimes it comes down to "choose the best answer" of two possible answers based on the criteria.
- Approach each question by knocking out the impossible options. Almost all answers will be something legitimately related to Azure solutions, which means they will likely be familiar to you. However, some answer options are related to different services or would be impossible to implement.

Scenarios / problem-solution question sets
Another question type you may encounter (as of the writing), was a short section with scenarios called “problem-solution question sets”. In each scenario or question set, you are given a situation and then taken through a series of possible solutions, (solution objects), for which you will have to decide if it could or couldn't be used to solve the proposed business need. Be aware that for each of these questions, once you answer and click next to move to the next question, you cannot return and change your answer. They don't want this to be treated as a multiple choice, so you have to give a final answer of "yes" or "no" for each solution before moving to the next possible solution for the scenario.

To get a better understanding of the look and feel of the exam, please see the Exam Sandbox (link below).

EXAM SANDBOX - New to Microsoft Certification exams? We have something you need to try

See what the Microsoft exam environment is like by running the Microsoft exam simulator.

Exam SC-100: Microsoft Cybersecurity Architect

https://docs.microsoft.com/en-us/learn/certifications/exams/sc-100

"Candidates for this exam should have advanced experience and knowledge in a wide range of security engineering areas, including identity and access, platform protection, security operations, securing data, and securing applications. They should also have experience with hybrid and cloud implementations."

Skills measured – SC-100

- **Design a Zero Trust strategy and architecture (30–35%)**
- **Evaluate Governance Risk Compliance (GRC) technical strategies and security operations strategies (20–25%)**
- **Design security for infrastructure (20–25%)**
- **Design a strategy for data and applications (20–25%)**

Design a Zero Trust strategy and architecture (30–35%)

Build an overall security strategy and architecture

- Identify the integration points in an architecture by using Microsoft Cybersecurity Reference Architecture (MCRA)
- Translate business goals into security requirements
- Translate security requirements into technical capabilities, including security services, security products, and security processes
- Design security for a resiliency strategy
- Integrate a hybrid or multi-tenant environment into a security strategy
- Develop a technical and governance strategy for traffic filtering and segmentation

Design a security operations strategy

- Design a logging and auditing strategy to support security operations
- Develop security operations to support a hybrid or multi-cloud environment
- Design a strategy for SIEM and SOAR
- Evaluate security workflows
- Evaluate a security operations strategy for incident management lifecycle
- Evaluate a security operations strategy for sharing technical threat intelligence

Design an identity security strategy

Note: includes hybrid and multi-cloud

- Design a strategy for access to cloud resources
- Recommend an identity store (tenants, B2B, B2C, hybrid)
- Recommend an authentication strategy
- Recommend an authorization strategy
- Design a strategy for conditional access
- Design a strategy for role assignment and delegation
- Design security strategy for privileged role access to infrastructure including identity-based firewall rules, Azure PIM
- Design security strategy for privileged activities including PAM, entitlement management, cloud tenant administration

Evaluate Governance Risk Compliance (GRC) technical strategies and security operations strategies (20–25%)

Design a regulatory compliance strategy

- Interpret compliance requirements and translate into specific technical capabilities (new or existing)
- Evaluate infrastructure compliance by using Microsoft Defender for Cloud
- Interpret compliance scores and recommend actions to resolve issues or improve security
- Design implementation of Azure Policy
- Design for data residency requirements
- Translate privacy requirements into requirements for security solutions

Evaluate security posture and recommend technical strategies to manage risk

- Evaluate security posture by using benchmarks (including Azure security benchmarks, ISO 2701, etc.)
- Evaluate security posture by using Microsoft Defender for Cloud
- Evaluate security posture by using Secure Scores
- Evaluate security posture of cloud workloads
- Design security for an Azure Landing Zone
- Interpret technical threat intelligence and recommend risk mitigations
- Recommend security capabilities or controls to mitigate identified risks

Design security for infrastructure (20–25%)

Design a strategy for securing server and client endpoints

NOTE: includes hybrid and multi-cloud

- Specify security baselines for server and client endpoints
- Specify security requirements for servers, including multiple platforms and operating systems
- Specify security requirements for mobile devices and clients, including endpoint protection, hardening, and configuration
- Specify requirements to secure Active Directory Domain Services
- Design a strategy to manage secrets, keys, and certificates
- Design a strategy for secure remote access

Design a strategy for securing SaaS, PaaS, and IaaS services

- Specify security baselines for SaaS, PaaS, and IaaS services
- Specify security requirements for IoT workloads
- Specify security requirements for data workloads, including SQL, Azure SQL Database, Azure Synapse, and Azure Cosmos DB
- Specify security requirements for web workloads, including Azure App Service
- Specify security requirements for storage workloads, including Azure Storage
- Specify security requirements for containers
- Specify security requirements for container orchestration

Design a strategy for data and applications (20–25%)

Specify security requirements for applications

- Specify priorities for mitigating threats to applications
- Specify a security standard for onboarding a new application
- Specify a security strategy for applications and APIs

Design a strategy for securing data

- Specify priorities for mitigating threats to data
- Design a strategy to identify and protect sensitive data
- Specify an encryption standard for data at rest and in motion

MS Learn – SC-100 – Design a Zero Trust strategy and architecture

- Build an overall security strategy and architecture
- Design a security operations strategy
- Design an identity security strategy

MS Learn – SC-100 – Evaluate Governance Risk Compliance (GRC) technical strategies and security operations strategies

- Evaluate a regulatory compliance strategy
- Evaluate security posture and recommend technical strategies to manage risk

MS Learn – SC-100 – Design security for infrastructure

- Understand architecture best practices and how they are changing with the Cloud
- Design a strategy for securing server and client endpoints
- Design a strategy for securing PaaS, IaaS, and SaaS services

MS Learn – SC-100 – Design a strategy for data and applications

- Specify security requirements for applications
- Design a strategy for securing data

GITHUB LABS – SC-100: Microsoft Cybersecurity Expert

This repository contains case studies for the SC-100: Microsoft Cybersecurity Architect certification:

- Case study introduction
- Build overall security strategy
- Design security operations strategy
- Design identity security strategy
- Evaluate a regulatory compliance strategy
- Evaluate security posture and recommend technical strategies
- Understand architecture best practices
- Design a strategy for securing server and client endpoints
- Design a strategy for security PaaS, IaaS and SaaS services
- Specify security requirements for applications
- Design a strategy for securing data

REFERENCE

Design a Zero Trust strategy and architecture (30–35%)

Build an overall security strategy and architecture

- Identify the integration points in an architecture by using Microsoft Cybersecurity Reference Architecture (MCRA)
- Translate business goals into security requirements
- Translate security requirements into technical capabilities, including security services, security products, and security processes
- Design security for a resiliency strategy
- Integrate a hybrid or multi-tenant environment into a security strategy
- Develop a technical and governance strategy for traffic filtering and segmentation

Design a security operations strategy

- Design a logging and auditing strategy to support security operations
- Develop security operations to support a hybrid or multi-cloud environment
- Design a strategy for SIEM and SOAR
- Evaluate security workflows
- Evaluate a security operations strategy for incident management lifecycle
- Evaluate a security operations strategy for sharing technical threat intelligence

Design an identity security strategy

Note: includes hybrid and multi-cloud

- Design a strategy for access to cloud resources
- Recommend an identity store (tenants, B2B, B2C, hybrid)
- Recommend an authentication strategy
- Recommend an authorization strategy
- Design a strategy for conditional access
- Design a strategy for role assignment and delegation
- Design security strategy for privileged role access to infrastructure including identity-based firewall rules, Azure PIM
- Design security strategy for privileged activities including PAM, entitlement management, cloud tenant administration

Microsoft Cybersecurity Reference Architectures
https://docs.microsoft.com/en-us/security/cybersecurity-reference-architecture/mcra

Azure Security Benchmark introduction
https://docs.microsoft.com/en-us/security/benchmark/azure/introduction

Overview of the Azure Security Benchmark
https://docs.microsoft.com/en-us/security/benchmark/azure/overview

What's inside Microsoft Security Best Practices
https://docs.microsoft.com/en-us/security/compass/microsoft-security-compass-introduction

Microsoft Security Best Practices module: Governance, risk, and compliance
https://docs.microsoft.com/en-us/security/compass/governance

Governance, risk, and compliance
https://docs.microsoft.com/en-us/security/compass/governance

Governance, risk, and compliance capabilities
https://docs.microsoft.com/en-us/security/compass/governance-risk-compliance-capabilities

Regulatory Compliance in Azure Policy
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/regulatory-compliance

Recommended policies for Azure services
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/recommended-policies

Azure Policy built-in policy definitions
https://docs.microsoft.com/en-us/azure/governance/policy/samples/built-in-policies

What are security policies, initiatives, and recommendations
https://docs.microsoft.com/en-us/azure/defender-for-cloud/security-policy-concept

Security posture for Microsoft Defender for Cloud
https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

What are security policies, initiatives, and recommendations?
https://docs.microsoft.com/en-us/azure/defender-for-cloud/security-policy-concept

Security recommendations - a reference guide
https://docs.microsoft.com/en-us/azure/defender-for-cloud/recommendations-reference

Security recommendations for AWS resources - a reference guide
https://docs.microsoft.com/en-us/azure/defender-for-cloud/recommendations-reference-aws

Define a security strategy
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/strategy/define-security-strategy

Cloud security functions
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/organize/cloud-security

Get started: Implement security across the enterprise environment
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/get-started/security

Security integration
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/secure/security-integration

Risk management insights
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/secure/risk-insights

Learn about Priva Privacy Risk Management
https://docs.microsoft.com/en-us/privacy/priva/risk-management

Azure security best practices
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/secure/security-top-10

Business resilience
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/secure/business-resilience

Access control
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/secure/access-control

Security operations
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/secure/security-operations

Asset protection
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/secure/asset-protection

Security governance
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/secure/security-governance

Innovation security
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/secure/innovation-security

DevSecOps controls
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/secure/devsecops-controls

Introduction to hybrid and multicloud
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/scenarios/hybrid/

What is Azure AD Privileged Identity Management?
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

Securing privileged access for hybrid and cloud deployments in Azure AD
https://docs.microsoft.com/en-us/azure/active-directory/roles/security-planning

Manage emergency access accounts in Azure AD
https://docs.microsoft.com/en-us/azure/active-directory/roles/security-emergency-access

Cloud monitoring guide: Formulate a monitoring strategy
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/strategy/monitoring-strategy

Resiliency and continuity overview
https://docs.microsoft.com/en-us/compliance/assurance/assurance-resiliency-and-continuity

Resiliency in Azure
https://docs.microsoft.com/en-us/azure/availability-zones/overview

Security development and operations overview
https://docs.microsoft.com/en-us/compliance/assurance/assurance-security-development-and-operation

Implement network segmentation patterns on Azure
https://docs.microsoft.com/en-us/azure/architecture/framework/security/design-network-segmentation

Microsoft Sentinel SOAR content catalog
https://docs.microsoft.com/en-us/azure/sentinel/sentinel-soar-content

Automate threat response with playbooks in Microsoft Sentinel
https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks

Tutorial: Use playbooks with automation rules in Microsoft Sentinel
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

Tutorial: Get started with Jupyter notebooks and MSTICPy in Microsoft Sentinel
https://docs.microsoft.com/en-us/azure/sentinel/notebook-get-started

Tutorial: Create a Power BI report from Microsoft Sentinel data
https://docs.microsoft.com/en-us/azure/sentinel/powerbi

Deploy and monitor Azure Key Vault honeytokens with Microsoft Sentinel
https://docs.microsoft.com/en-us/azure/sentinel/monitor-key-vault-honeytokens

Microsoft Sentinel workspace architecture best practices
https://docs.microsoft.com/en-us/azure/sentinel/best-practices-workspace-architecture

What is Azure Key Vault Managed HSM?
https://docs.microsoft.com/en-us/azure/key-vault/managed-hsm/overview

Configure key auto-rotation in Azure Key Vault
https://docs.microsoft.com/en-us/azure/key-vault/keys/how-to-configure-key-rotation

Visualize collected data
https://docs.microsoft.com/en-us/azure/sentinel/get-visibility

Azure Workbooks
https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-overview

Use Azure Monitor workbooks to visualize and monitor your data
https://docs.microsoft.com/en-us/azure/sentinel/monitor-your-data

Defender for Identity entity tags in Microsoft 365 Defender
https://docs.microsoft.com/en-us/microsoft-365/security/defender-identity/entity-tags?view=o365-worldwide

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

Create or update Azure custom roles using the Azure portal
https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal

Add Conditional Access to user flows in Azure Active Directory B2C
https://docs.microsoft.com/en-us/azure/active-directory-b2c/conditional-access-user-flow?pivots=b2c-user-flow

Microsoft 365 integration with on-premises environments
https://docs.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-integration

Mitigate credential attacks in Azure AD B2C with smart lockout
https://docs.microsoft.com/en-us/azure/active-directory-b2c/threat-management

Set up sign-up and sign-in with a Facebook account using Azure Active Directory B2C
https://docs.microsoft.com/en-us/azure/active-directory-b2c/identity-provider-facebook

Authenticate runbooks with Amazon Web Services
https://docs.microsoft.com/en-us/azure/automation/automation-config-aws-account

Use Azure AD to authenticate to Azure
https://docs.microsoft.com/en-us/azure/automation/automation-use-azure-ad

DNS records for Azure regions used by Azure Automation
https://docs.microsoft.com/en-us/azure/automation/how-to/automation-region-dns-records

Use Azure Private Link to securely connect networks to Azure Automation
https://docs.microsoft.com/en-us/azure/automation/how-to/private-link-security

Manage role permissions and security in Azure Automation
https://docs.microsoft.com/en-us/azure/automation/automation-role-based-access-control

Manage your Azure Automation account
https://docs.microsoft.com/en-us/azure/automation/delete-account?tabs=azure-portal

What is Azure Lighthouse?
https://docs.microsoft.com/en-us/azure/lighthouse/overview

Azure Lighthouse architecture
https://docs.microsoft.com/en-us/azure/lighthouse/concepts/architecture

Cross-tenant management experiences
https://docs.microsoft.com/en-us/azure/lighthouse/concepts/cross-tenant-management-experience

Onboard a customer to Azure Lighthouse
https://docs.microsoft.com/en-us/azure/lighthouse/how-to/onboard-customer

Azure Arc overview
https://docs.microsoft.com/en-us/azure/azure-arc/overview

Implement Conditional Access policies including Multi-Factor Authentication

Plan a Conditional Access deployment
What is Conditional Access?

Conditional Access: Require MFA for all users

Common Conditional Access policies

Typical policies deployed by organizations

- **Block legacy authentication***
- **Require MFA for administrators***
- **Require MFA for Azure management***
- **Require MFA for all users***

* These four policies when configured together, mimic functionality enabled by **security defaults**.

Additional policies

- **Sign-in risk-based Conditional Access (Requires Azure AD Premium P2)**
- **User risk-based Conditional Access (Requires Azure AD Premium P2)**
- **Require trusted location for MFA registration**
- **Block access by location**
- **Require compliant device**
- **Block access except specific apps**

Tutorial: Secure user sign-in events with Azure AD Multi-Factor Authentication

Implement privileged access management
https://docs.microsoft.com/en-us/learn/modules/m365-compliance-insider-implement-privileged-access-management/

What is Azure AD Privileged Identity Management?
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

Start using Privileged Identity Management
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started

License requirements to use Privileged Identity Management
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/subscription-requirements

Assign Azure AD roles in Privileged Identity Management
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-add-role-to-user

Incident management overview
https://docs.microsoft.com/en-us/compliance/assurance/assurance-incident-management

- Video: Microsoft Online Services incident management
- Online Services Terms (OST)
- Data Protection Addendum (DPA)
- Microsoft Cloud Incident Management Implementation Guidance for Azure and Office 365
- Office 365 - Third-Party Vulnerability Assessment of Office 365 - 2019

Microsoft security incident management: Detection and analysis
https://docs.microsoft.com/en-us/compliance/assurance/assurance-sim-detection-analysis

Security Control v3: Incident response
https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-incident-response

Protect your identities with Azure AD Identity Protection
34 minute modular reference guide

In this module, you will:
- Describe the features of Azure Active Directory Identity Protection.
- Describe the investigation and remediation features of Azure Active Directory Identity Protection.

Prerequisites
- Basic familiarity with Azure Active Directory

Enable identity protection in Azure Active Directory
31 minute modular reference guide

In this module, you will:
- How to define Azure Active Directory Identity Protection.
- About Azure Active Directory Identity Protection support for development tools.
- How users can remediate risky behavior.

Prerequisites
- Intermediate understanding of Microsoft 365 and Azure Active Directory.

How To: Configure the Azure AD Multi-Factor Authentication registration policy
Azure AD Identity Protection helps you manage the roll-out of Azure AD Multi-Factor Authentication (MFA) registration by configuring a Conditional Access policy to require MFA registration no matter what modern authentication app you are signing in to.

Plan an Azure Active Directory self-service password reset deployment
This deployment plan offers guidance and best practices for deploying Azure AD self-service password reset (SSPR).

Plan an Azure AD Multi-Factor Authentication deployment
Azure AD Multi-Factor Authentication (MFA) helps safeguard access to data and applications. It provides an additional layer of security using a second form of authentication. Organizations can use **Conditional Access** to make the solution fit their specific needs.

User experiences with Azure AD Identity Protection

With Azure Active Directory Identity Protection, you can:
- Require users to register for Azure AD Multi-Factor Authentication (MFA)
- Automate remediation of risky sign-ins and compromised users

Configure Access Reviews

Create an access review of Azure AD roles in Privileged Identity Management

This article describes how to create one or more access reviews for privileged Azure AD roles.

Create an access review of groups and applications in Azure AD access reviews

Access to groups and applications for employees and guests changes over time. To reduce the risk associated with stale access assignments, administrators can use Azure Active Directory (Azure AD) to create access reviews for group members or application access. If you need to routinely review access, you can also create recurring access reviews. For more information about these scenarios, see **Manage user access** and **Manage guest access**.

You can also create access reviews using APIs. For more information, see the **Azure AD access reviews API reference**. For a code sample, see **Example of retrieving Azure AD access reviews via Microsoft Graph**.

Additional reference and review:

- **Review access to groups or applications**
- **Review access for yourself to groups or applications**
- **Complete an access review of groups or applications**

Activate and configure PIM

Privileged Identity Management "How-to" Guides

Deploy Azure AD Privileged Identity Management (PIM)
This article is a step-by-step guide describing how to plan the deployment of Privileged Identity Management (PIM) in your Azure Active Directory (Azure AD) organization. You'll reassign users in high-privileged roles to less powerful built-in or custom roles where possible, and plan for just-in-time role assignments for your most privileged roles. In this article, we make recommendations for both deployment planning and implementation.

Start using Privileged Identity Management
This article describes how to enable Privileged Identity Management (PIM) and get started using it.

Prepare PIM for Azure AD roles

1. **Configure Azure AD role settings**.
2. **Give eligible assignments**.
3. **Allow eligible users to activate their Azure AD role just-in-time**.

Prepare PIM for Azure roles
Here are the tasks we recommend for you to prepare Privileged Identity Management to manage

Azure roles for a subscription:

1. **Discover Azure resources**
2. **Configure Azure role settings**.
3. **Give eligible assignments**.
4. **Allow eligible users to activate their Azure roles just-in-time**.

Evaluate Governance Risk Compliance (GRC) technical strategies and security operations strategies (20–25%)

Design a regulatory compliance strategy

- Interpret compliance requirements and translate into specific technical capabilities (new or existing)
- Evaluate infrastructure compliance by using Microsoft Defender for Cloud
- Interpret compliance scores and recommend actions to resolve issues or improve security
- Design implementation of Azure Policy
- Design for data residency requirements
- Translate privacy requirements into requirements for security solutions

Evaluate security posture and recommend technical strategies to manage risk

- Evaluate security posture by using benchmarks (including Azure security benchmarks, ISO 2701, etc.)
- Evaluate security posture by using Microsoft Defender for Cloud
- Evaluate security posture by using Secure Scores
- Evaluate security posture of cloud workloads
- Design security for an Azure Landing Zone
- Interpret technical threat intelligence and recommend risk mitigations
- Recommend security capabilities or controls to mitigate identified risks

Planning and operations guide
https://docs.microsoft.com/en-us/azure/defender-for-cloud/security-center-planning-and-operations-guide

Protect your Kubernetes data plane hardening
https://docs.microsoft.com/en-us/azure/defender-for-cloud/kubernetes-workload-protections

Tutorial: Protect your resources with Microsoft Defender for Cloud
https://docs.microsoft.com/en-us/azure/defender-for-cloud/tutorial-protect-resources

Automate responses to Microsoft Defender for Cloud triggers
https://docs.microsoft.com/en-us/azure/defender-for-cloud/workflow-automation

Connect your AWS accounts to Microsoft Defender for Cloud
https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws

Azure security solutions for AWS
https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/aws/aws-azure-security-solutions

Security recommendations for AWS resources - a reference guide
https://docs.microsoft.com/en-us/azure/defender-for-cloud/recommendations-reference-aws

Connect Microsoft Sentinel to Amazon Web Services to ingest AWS service log data
https://docs.microsoft.com/en-us/azure/sentinel/connect-aws

Tutorial: Triage, investigate, and respond to security alerts
https://docs.microsoft.com/en-us/azure/defender-for-cloud/tutorial-security-incident

Tutorial: Improve your regulatory compliance
https://docs.microsoft.com/en-us/azure/defender-for-cloud/regulatory-compliance-dashboard

Manage security policies
https://docs.microsoft.com/en-us/azure/defender-for-cloud/tutorial-security-policy

Investigate users in Microsoft 365 Defender
https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-users

What is an Azure landing zone?
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/

Azure landing zone - design principles
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/design-principles

Expand your landing zone
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/considerations/

Refactor landing zones
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/refactor

Transition existing Azure environments to the Azure landing zone conceptual architecture
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/transition

Scenario: Transition existing Azure environments to the Azure landing zone conceptual architecture
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/align-scenarios

Scenario-specific enterprise-scale landing zones in Azure
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/enterprise-scale/scenario-specific-enterprise-scale-landing-zones

Improve landing zone security
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ready/considerations/landing-zone-security

Details of the ISO 27001:2013 Regulatory Compliance built-in initiative
https://docs.microsoft.com/en-us/azure/governance/policy/samples/iso-27001

Azure Policy built-in initiative definitions
https://docs.microsoft.com/en-us/azure/governance/policy/samples/built-in-initiatives

Understand Azure Policy effects
https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects

What's available in the Microsoft Purview governance portal?
https://docs.microsoft.com/en-us/azure/purview/overview

Quickstart: Create a collection and assign permissions in the Microsoft Purview Data Map
https://docs.microsoft.com/en-us/azure/purview/quickstart-create-collection

Use the Microsoft Purview governance portal
https://docs.microsoft.com/en-us/azure/purview/use-azure-purview-studio

Classification best practices in the Microsoft Purview governance portal
https://docs.microsoft.com/en-us/azure/purview/concept-best-practices-classification

Integrate Microsoft Purview with Azure security products
https://docs.microsoft.com/en-us/azure/purview/how-to-integrate-with-azure-security-products

What is Microsoft Defender for Cloud?
https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction

- **Defender for Cloud secure score continually assesses** your security posture so you can track new security opportunities and precisely report on the progress of your security efforts.
- **Defender for Cloud recommendations secures** your workloads with step-by-step actions that protect your workloads from known security risks.
- **Defender for Cloud alerts defends** your workloads in real-time so you can react immediately and prevent security events from developing.

Microsoft Defender for Cloud's enhanced security features
https://docs.microsoft.com/en-us/azure/defender-for-cloud/enhanced-security-features-overview

Archive for what's new in Defender for Cloud?
https://docs.microsoft.com/en-us/azure/defender-for-cloud/release-notes-archive

Microsoft Defender for Cloud threat intelligence report
https://docs.microsoft.com/en-us/azure/defender-for-cloud/threat-intelligence-reports

Details of the NIST SP 800-53 Rev. 5 (Azure Government) Regulatory Compliance built-in initiative
https://docs.microsoft.com/en-us/azure/governance/policy/samples/gov-nist-sp-800-53-r5

Details of the DoD Impact Level 5 (Azure Government) Regulatory Compliance built-in initiative
https://docs.microsoft.com/en-us/azure/governance/policy/samples/gov-dod-impact-level-5

Design security for infrastructure (20–25%)

Design a strategy for securing server and client endpoints

NOTE: includes hybrid and multi-cloud

- Specify security baselines for server and client endpoints
- Specify security requirements for servers, including multiple platforms and operating systems
- Specify security requirements for mobile devices and clients, including endpoint protection, hardening, and configuration
- Specify requirements to secure Active Directory Domain Services
- Design a strategy to manage secrets, keys, and certificates
- Design a strategy for secure remote access

Design a strategy for securing SaaS, PaaS, and IaaS services

- Specify security baselines for SaaS, PaaS, and IaaS services
- Specify security requirements for IoT workloads
- Specify security requirements for data workloads, including SQL, Azure SQL Database, Azure Synapse, and Azure Cosmos DB
- Specify security requirements for web workloads, including Azure App Service
- Specify security requirements for storage workloads, including Azure Storage
- Specify security requirements for containers
- Specify security requirements for container orchestration

Security baselines for Azure
https://docs.microsoft.com/en-us/security/benchmark/azure/security-baselines-overview

Security Control v3: Network security
https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security

Security Control v3: Identity management
https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management

Security Control v3: Privileged access
https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access

Security Control v3: Data protection
https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection

Security Control v3: Posture and vulnerability management
https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management

Data Discovery & Classification
https://docs.microsoft.com/en-us/azure/azure-sql/database/data-discovery-and-classification-overview?view=azuresql

What is data classification
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/policy-compliance/data-classification

Platform integrity and security overview

- Firmware security
- Platform code integrity
- UEFI Secure Boot
- Measured boot and host attestation
- Project Cerberus
- Encryption at rest
- Hypervisor security

Get started with content explorer
https://docs.microsoft.com/en-us/microsoft-365/compliance/data-classification-content-explorer

Azure services for securing network connectivity
https://docs.microsoft.com/en-us/azure/architecture/framework/security/design-network-connectivity

Best practices for endpoint security on Azure
https://docs.microsoft.com/en-us/azure/architecture/framework/security/design-network-endpoints

Welcome to Microsoft Defender for IoT for organizations
https://docs.microsoft.com/en-us/azure/defender-for-iot/organizations/overview

System architecture for OT system monitoring
https://docs.microsoft.com/en-us/azure/defender-for-iot/organizations/architecture

Tutorial: Integrate Microsoft Sentinel and Microsoft Defender for IoT
https://docs.microsoft.com/en-us/azure/sentinel/iot-solution

Quickstart: Get started with Defender for IoT
https://docs.microsoft.com/en-us/azure/defender-for-iot/organizations/getting-started

Best practices for planning your OT network monitoring
https://docs.microsoft.com/en-us/azure/defender-for-iot/organizations/plan-network-monitoring

Microsoft Defender for IoT Edge azureiotsecurity
https://docs.microsoft.com/en-us/azure/defender-for-iot/device-builders/security-edge-architecture

OT threat monitoring in enterprise SOCs
https://docs.microsoft.com/en-us/azure/defender-for-iot/organizations/concept-sentinel-integration

Monitor hybrid security using Microsoft Defender for Cloud and Microsoft Sentinel
https://docs.microsoft.com/en-us/azure/architecture/hybrid/hybrid-security-monitoring

Migrate or deploy Azure Virtual Desktop instances to Azure
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/scenarios/wvd/

- Strategy for Azure Virtual Desktop
- Plan for Azure Virtual Desktop
- Migrate to Azure Virtual Desktop
- Manage an Azure Virtual Desktop environment
- Govern an Azure Virtual Desktop environment

Azure Virtual Desktop proof of concept
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/scenarios/wvd/proof-of-concept

Use Azure Firewall to protect Azure Virtual Desktop deployments
https://docs.microsoft.com/en-us/azure/firewall/protect-azure-virtual-desktop

Configure key auto-rotation in Azure Key Vault
https://docs.microsoft.com/en-us/azure/key-vault/keys/how-to-configure-key-rotation

- Azure Encryption at Rest
- Azure services data encryption support table
- Use an Azure RBAC to control access to keys, certificates and secrets
- Monitoring Key Vault with Azure Event Grid
- Azure Data Encryption At Rest
- Azure Storage Encryption
- Azure Disk Encryption

Azure security baseline for Azure Cosmos DB
https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/cosmos-db-security-baseline

Linux security baseline
https://docs.microsoft.com/en-us/azure/governance/policy/samples/guest-configuration-baseline-linux

Windows security baseline
https://docs.microsoft.com/en-us/azure/governance/policy/samples/guest-configuration-baseline-windows

Docker security baseline
https://docs.microsoft.com/en-us/azure/governance/policy/samples/guest-configuration-baseline-docker

Security Control v3: Endpoint security
https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-endpoint-security

Protecting Your SQL Server Intellectual Property
https://docs.microsoft.com/en-us/sql/relational-databases/security/protecting-your-sql-server-intellectual-property

SQL Injection
https://docs.microsoft.com/en-us/sql/relational-databases/security/sql-injection

Row-Level Security
https://docs.microsoft.com/en-us/sql/relational-databases/security/row-level-security

Dynamic Data Masking
https://docs.microsoft.com/en-us/sql/relational-databases/security/dynamic-data-masking?view=sql-server-ver16

What is Azure SQL Managed Instance?
https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/sql-managed-instance-paas-overview

Onboard devices and configure Microsoft Defender for Endpoint capabilities
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/onboard-configure

Defender for Endpoint onboarding Windows Client
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/onboard-windows-client

Learn about data loss prevention
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp

Learn about Endpoint data loss prevention
https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-learn-about

How to develop secure applications using Azure Cosmos DB
https://azure.microsoft.com/en-us/blog/how-to-develop-secure-applications-using-azure-cosmos-db/

Azure Automation in a hybrid environment
https://docs.microsoft.com/en-us/azure/architecture/hybrid/azure-automation-hybrid

Azure Automation update management
https://docs.microsoft.com/en-us/azure/architecture/hybrid/azure-update-mgmt

Azure Virtual Desktop for the enterprise
https://docs.microsoft.com/en-us/azure/architecture/example-scenario/wvd/windows-virtual-desktop

Computer forensics chain of custody in Azure
https://docs.microsoft.com/en-us/azure/architecture/example-scenario/forensics/

Overview of Microsoft Defender for Containers
https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-introduction

Defender for Containers architecture
https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-architecture

Enable Microsoft Defender for Containers
https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-enable

Configure Azure Bastion

Connect to virtual machines through the Azure portal by using Azure Bastion
40 minute modular reference guide

Deploy Azure Bastion to securely connect to Azure virtual machines directly within the Azure portal, to effectively replace an existing jumpbox solution. Monitor remote sessions by using diagnostic logs. Manage remote sessions by disconnecting a user session.

After completing this module, you'll be able to:

- Evaluate Azure Bastion as a replacement for a VM jumpbox solution
- Configure Bastion to securely connect to VMs
- Manage remote sessions by enabling diagnostic logs and monitoring remote sessions

Prerequisites

- Experience managing remote connections to virtual machines
- Familiarity with networking concepts like virtual networks, public and private IPs, and network protocols SSH, RDP, and TLS
- (Optional) Access to an Azure subscription where you have permissions to create resources like VMs

What is Azure Bastion?

Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal. The Azure Bastion service is a fully platform-managed PaaS service that you provision inside your virtual network. It provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS. When you connect via Azure Bastion, your virtual machines do not need a public IP address, agent, or special client software.

Bastion provides secure RDP and SSH connectivity to all of the VMs in the virtual network in which it is provisioned. Using Azure Bastion protects your virtual machines from exposing RDP/SSH ports to the outside world, while still providing secure access using RDP/SSH.

Tutorial: Configure Bastion and connect to a Windows VM through a browser

This tutorial shows you how to connect to a virtual machine through your browser using Azure Bastion and the Azure portal. In the Azure portal, you deploy Bastion to your virtual network. After deploying Bastion, you connect to a VM via its private IP address using the Azure portal. Your VM does not need a public IP address or special software. Once the service is provisioned, the RDP/SSH experience is available to all of the virtual machines in the same virtual network. For more information about Azure Bastion, see **What is Azure Bastion?.**

In this tutorial, you'll learn how to:

- Create a bastion host for your VNet
- Connect to a Windows virtual machine

Working with NSG access and Azure Bastion

When working with Azure Bastion, you can use network security groups (NSGs). For more information, see **Security Groups.**

Azure Bastion FAQ

Design a strategy for data and applications (20–25%)

Specify security requirements for applications

- Specify priorities for mitigating threats to applications
- Specify a security standard for onboarding a new application
- Specify a security strategy for applications and APIs

Design a strategy for securing data

- Specify priorities for mitigating threats to data
- Design a strategy to identify and protect sensitive data
- Specify an encryption standard for data at rest and in motion

Platform code integrity
https://docs.microsoft.com/en-us/azure/security/fundamentals/code-integrity

About GitHub Advanced Security
https://docs.github.com/en/enterprise-cloud@latest/get-started/learning-about-github/about-github-advanced-security

Develop secure applications on Azure
https://docs.microsoft.com/en-us/azure/security/develop/secure-develop

OAuth app policies
https://docs.microsoft.com/en-us/defender-cloud-apps/app-permission-policy

Azure security baseline for Azure Front Door
https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/front-door-security-baseline

End-to-end TLS with Azure Front Door
https://docs.microsoft.com/en-us/azure/frontdoor/end-to-end-tls

Web Application Firewall (WAF) on Azure Front Door
https://docs.microsoft.com/en-us/azure/frontdoor/web-application-firewall

Geo-filtering on a domain for Azure Front Door
https://docs.microsoft.com/en-us/azure/frontdoor/front-door-geo-filtering

Azure security baseline for API Management
https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/api-management-security-baseline

Azure security baseline for App Service
https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/app-service-security-baseline

Getting started with the Threat Modeling Tool
https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-getting-started

Threat Modeling Tool feature overview
https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-feature-overview

Microsoft Threat Modeling Tool threats
https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats

Using Microsoft Sentinel with Azure Web Application Firewall
https://docs.microsoft.com/en-us/azure/web-application-firewall/waf-sentinel

Configure WAF policies using Azure Firewall Manager
https://docs.microsoft.com/en-us/azure/web-application-firewall/shared/manage-policies

Configure Azure Storage firewalls and virtual networks
https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security

Backup and restore plan to protect against ransomware
https://docs.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware

Understanding just-in-time (JIT) VM access
https://docs.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-overview

Configure Just in Time VM access via Microsoft Defender for Cloud

Protect your servers and VMs from brute-force and malware attacks with Microsoft Defender for Cloud
44 minute modular reference guide

In this module, you'll discover how to protect VMs and servers with Microsoft Defender for Cloud

After completing this module, you'll be able to:
- Learn how to protect VM-based resources and networks with Microsoft Defender for Cloud
- Install and use malware protection to stop virus attacks on your exposed endpoints
- Enable JIT VM Access

Prerequisites
- Basic familiarity with Azure services, particularly Microsoft Defender for Cloud.
- Familiarity with Azure virtual machines and virtual networking.

Understanding just-in-time (JIT) VM access

This page explains the principles behind Microsoft Defender for Cloud's just-in-time (JIT) VM access feature and the logic behind the recommendation.

To learn how to apply JIT to your VMs using the Azure portal (either Security Center or Azure Virtual Machines) or programatically, see How to secure your management ports with JIT.

JIT requires Azure Defender for servers to be enabled on the subscription.

Secure your management ports with just-in-time access

Lock down inbound traffic to your Azure Virtual Machines with Microsoft Defender for Cloud's just-in-time (JIT) virtual machine (VM) access feature. This reduces exposure to attacks while providing easy access when you need to connect to a VM.

For a full explanation about how JIT works and the underlying logic, see Just-in-time explained.

This page teaches you how to include JIT in your security program. You'll learn how to:

- Enable JIT on your VMs - You can enable JIT with your own custom options for one or more VMs using Security Center, PowerShell, or the REST API. Alternatively, you can enable JIT with default, hard-coded parameters, from Azure virtual machines. When enabled, JIT locks down inbound traffic to your Azure VMs by creating a rule in your network security group.
- Request access to a VM that has JIT enabled - The goal of JIT is to ensure that even though your inbound traffic is locked down, Security Center still provides easy access to connect to VMs when needed. You can request access to a JIT-enabled VM from Security Center, Azure virtual machines, PowerShell, or the REST API.
- Audit the activity - To ensure your VMs are secured appropriately, review the accesses to your JIT-enabled VMs as part of your regular security checks.

Secure your management ports with just-in-time access
https://docs.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-usage

Web app private connectivity to Azure SQL Database
https://docs.microsoft.com/en-us/azure/architecture/example-scenario/private-web-app/private-web-app

App Service overview
https://docs.microsoft.com/en-us/azure/app-service/overview

App Service Environment overview
https://docs.microsoft.com/en-us/azure/app-service/environment/overview

Web content filtering
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/web-content-filtering

SAML single sign-on for on-premises applications with Application Proxy
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-single-sign-on-on-premises-apps

Configure custom domains with Azure AD Application Proxy
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-custom-domain

Tutorial: Add app authentication to your web app running on Azure App Service
https://docs.microsoft.com/en-us/azure/app-service/scenario-secure-app-authentication-app-service

Storage

Configure access control for storage accounts

Authorizing access to data in Azure Storage

Each time you access data in your storage account, your client makes a request over HTTP/HTTPS to Azure Storage. Every request to a secure resource must be authorized, so that the service ensures that the client has the permissions required to access the data.

Delegate access with a shared access signature

A shared access signature (SAS) is a URI that grants restricted access rights to Azure Storage resources. You can provide a shared access signature to clients who should not be trusted with your storage account key but to whom you wish to delegate access to certain storage account resources. By distributing a shared access signature URI to these clients, you can grant them access to a resource for a specified period of time, with a specified set of permissions.

The URI query parameters comprising the SAS token incorporate all of the information necessary to grant controlled access to a storage resource. A client who is in possession of the SAS can make a request against Azure Storage with just the SAS URI, and the information contained in the SAS token is used to authorize the request.

Configure key management for storage accounts

Authorize with Shared Key

Every request made against a storage service must be authorized, unless the request is for a blob or container resource that has been made available for public or signed access. One option for authorizing a request is by using Shared Key, described in this article.

- Blob Service REST API
- Queue Service REST API
- Table Service REST API
- Storage Services REST

Configure Azure AD authentication for Azure Storage

Authorize access to blobs and queues using Azure Active Directory

Azure Storage supports using Azure Active Directory (Azure AD) to authorize requests to Blob and Queue storage. With Azure AD, you can use Azure role-based access control (Azure RBAC) to grant permissions to a security principal, which may be a user, group, or application service principal. The security principal is authenticated by Azure AD to return an OAuth 2.0 token. The token can then be used to authorize a request against Blob or Queue storage.

Authorizing requests against Azure Storage with Azure AD provides superior security and ease of use over Shared Key authorization. Microsoft recommends using Azure AD authorization with your blob and queue applications when possible to minimize potential security vulnerabilities inherent in Shared Key.

Authorization with Azure AD is available for all general-purpose and Blob storage accounts in all public regions and national clouds. Only storage accounts created with the Azure Resource Manager deployment model support Azure AD authorization.

Blob storage additionally supports creating shared access signatures (SAS) that are signed with Azure AD credentials. For more information, see Grant limited access to data with shared access signatures.

Azure Files supports authorization with AD (preview) or Azure AD DS (GA) over SMB for domain-joined VMs only. To learn about using AD (preview) or Azure AD DS (GA) over SMB for Azure Files, see Overview of Azure Files identity-based authentication support for SMB access.

Authorization with Azure AD is not supported for Azure Table storage. Use Shared Key to authorize requests to Table storage.

Secure your Azure Storage account
45 minute modular reference guide

Learn how Azure Storage provides multilayered security to protect your data. Find out how to use access keys, to secure networks, and to use Advanced Threat Protection to proactively monitor your system.

After completing this module, you'll be able to:
- Understand storage account keys.
- Understand shared access signatures.
- Understand transport-level encryption with HTTPS.
- Understand Advanced Threat Protection.
- Control network access.

Prerequisites
- None

Authorize access to blobs using Azure Active Directory
https://docs.microsoft.com/en-us/azure/storage/blobs/authorize-access-azure-active-directory

Access Azure Data Lake Storage Gen2 using OAuth 2.0 with an Azure service principal
https://docs.microsoft.com/en-us/azure/databricks/data/data-sources/azure/adls-gen2/azure-datalake-gen2-sp-access

Remote access to on-premises applications through Azure AD Application Proxy
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy

---

After spending time reviewing the training available on the Microsoft Learn pages, you can add onto your skilling by reviewing corresponding articles from DOCS.MICROSOFT.COM

Below are targeted resources, most closely aligned with the “Skills Measured” outline from the exam requirements. There are also some subtopics to those six main domain areas of study, and where applicable, I have added additional reference information below.

Additional Reading

- Azure Active Directory integrations with authentication and synchronization protocols
  - Header-based authentication
  - LDAP authentication
  - OAuth 2.0 authentication
  - OIDC authentication
  - Password based SSO authentication
  - RADIUS authentication
  - Remote Desktop Gateway services
  - Secure Shell (SSH)
  - SAML authentication
  - Windows Authentication - Kerberos Constrained Delegation
  - Directory synchronization
  - LDAP Synchronization
  - SCIM synchronization
- **Manage Information Protection – Sensitivity Labels**
  - Learn about sensitivity labels
  - Why choose built-in labeling over the AIP add-in for Office apps
  - Get started with sensitivity labels
  - Restrict access to content by using sensitivity labels to apply encryption
  - Apply a sensitivity label to content automatically
  - How to configure auto-labeling for Office apps
  - How to configure auto-labeling policies for SharePoint, OneDrive, and Exchange
  - Rights Management issuer and Rights Management owner
  - Use sensitivity labels to protect content in Microsoft Teams, Microsoft 365 groups, and SharePoint sites
  - Enable sensitivity labels for Office files in SharePoint and OneDrive
  - Assign sensitivity labels to Microsoft 365 groups in Azure Active Directory
- **Manage Information Protection – Sensitive Information Types**
  - Learn about sensitive information types
  - Microsoft Purview Data Loss Prevention policies
  - Sensitivity labels
  - Retention labels
  - Insider risk management
  - Communication compliance
  - Auto-labelling policies
  - Microsoft Priva
  - Sensitive information type entity definitions
  - Create a custom sensitive information type
  - Create a custom sensitive information type in PowerShell
- What is Azure Information Protection
- Microsoft 365 guidance for security & compliance
- What is Azure AD Identity Governance
- Manage sensitivity labels in Office apps
- Understand threat intelligence in Microsoft Sentinel
- Use Jupyter notebooks to hunt for security threats

This STUDY GUIDE was developed by
Jason Zandri - Microsoft Technical Trainer.

ABOUT THE AUTHOR

Jason Zandri has been working in the information technology field since the late 1990s. He has worked for several multi-national corporations as well as smaller technology firms and startups.

He has been training students, formally in the classroom as a Microsoft Certified Trainer, and informally in online articles and tutorials, for nearly 25 years - back to the days of DOS, Windows 3.1x, and NT4.

He is always interested in expanding his knowledge through ongoing review and self-study and is always ready to meet new people and make new contacts via LinkedIn.

You can connect with him there via https://www.linkedin.com/in/jasonzandri/

Jason Zandri

AZURE TECHNICAL TRAINER / MICROSOFT TECHNICAL TRAINER

Jason.Zandri@microsoft.com

Microsoft

Microsoft Azure

https://www.linkedin.com/company/microsoft

https://www.linkedin.com/in/jasonzandri/

BONUS - Material relative to the AZ-500 Microsoft Azure Security Technologies exam and the Microsoft Azure Security Engineer Associate certification

This bonus section of this study guide serves as a thorough repository for resources, tutorials, and insights towards passing the AZ-500 certification. The structure follows the **AZ-500 exam outline**, which consists of 4 core areas of content, as shown below. Within each section you will find information dedicated to each subcategory of content contained in the exam outline.

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

In each subsection, you will find links to additional topics. In some cases, there is summary and introductory information regarding the linked article / learn tutorial - it is suggested that you review the summary information and then follow the links to the additional, more detailed information.

Prerequisites to AZ-500

To be successful in the AZ-500 ramp process, it's important for you to have some base knowledge on architecting technologies. Candidates for this exam will need to be familiar with scripting and automation and should have a deep understanding of networking and virtualization. A candidate should also have a strong familiarity with cloud capabilities, administering and operating Azure products and services, and have some exposure to other Microsoft products and services.

To acquire these skills during your AZ-500 skilling plan, it will be important that you have the following areas of knowledge before coming into this coursework:

- Understand security best practices and industry security requirements such as defense in depth, least privileged access, role-based access control, multi-factor authentication, shared responsibility, and zero trust model
- Be familiar with security protocols such as Virtual Private Networks (VPN), Internet Security Protocol (IPSec), Secure Socket Layer (SSL), disk and data encryption methods.
- Have experience with Windows and Linux operating systems and scripting languages.
- Have some experience deploying Azure workloads. This course does not cover the basics of Azure administration, instead the course content builds on that knowledge by adding security specific information.
    - AZ-900 Azure Fundamentals covers introductory basics and the foundation for Azure and Cloud environments
    - AZ-104 Azure Administrator covers all the basics and the foundation for Cloud Administrators covering the core elements for operating systems, virtualization, cloud infrastructure, storage structures, and networking.

For the AZ-500 certification - the content and material and the exam itself - there is a wide berth of information assumed from the domain areas of study for AZ-900 Azure Fundamentals. Those domain areas cover introductory basics and the foundational information for Azure and Cloud environments

The domain areas of study for the **AZ-104 Azure Administrator exam** for the **Microsoft Azure Administrator Associate** certification covers all the basics and the foundation for Cloud Administrators covering the core elements for operating systems, virtualization, cloud infrastructure, storage structures, and networking.

All of this information is needed as core knowledge before moving on to this material. The **BONUS section** following this one includes reference and review information relative to the **AZ-104 Microsoft Azure Administrator certification**

Manage identity and access (30-35%)

Manage Azure Active Directory Identities

Configure security for service principals

How to: Use the portal to create an Azure AD application and service principal that can access resources

This article shows you how to create a new Azure Active Directory (Azure AD) application and service principal that can be used with the role-based access control. When you have applications, hosted services, or automated tools that needs to access or modify resources, you can create an identity for the app. This identity is known as a service principal. Access to resources is restricted by the roles assigned to the service principal, giving you control over which resources can be accessed and at which level. For security reasons, it's always recommended to use service principals with automated tools rather than allowing them to log in with a user identity.

This article shows you how to use the portal to create the service principal in the Azure portal. It focuses on a single-tenant application where the application is intended to run within only one organization. You typically use single-tenant applications for line-of-business applications that run within your organization. You can also **use Azure PowerShell to create a service principal.**

Application and service principal objects in Azure Active Directory

This article describes application registration, application objects, and service principals in Azure Active Directory: what they are, how they're used, and how they are related to each other. A multi-tenant example scenario is also presented to illustrate the relationship between an application's application object and corresponding service principal objects.

Manage Azure AD directory groups

Access with Azure Active Directory groups

Azure DevOps Services
Do you want an easier way to control who can access your team's critical resources and key business assets in Azure DevOps Services? If you already use Microsoft services like Microsoft 365 or **Azure Active Directory (Azure AD)**, you can use the same identities with your organization. **Azure AD works with your organization** to control access and authenticate users.

When you organize directory members with **Azure AD groups**, you can reuse those groups to manage permissions in bulk for your organization. Just add those groups to the group that you want. For example, add them to built-in groups like Project Collection Administrators or Contributors, or manually created groups like your project management team. Azure AD group members inherit permissions from the Azure DevOps group, so

you don't have to manage group members one at a time.

Not familiar with Azure AD, but want to check it out? Learn more about **Azure AD benefits** and differences in how you **control organization access with Microsoft accounts or with Azure AD**.

Prerequisites

- Your organization must be connected to Azure Active Directory. **My organization uses Microsoft accounts only. Can I switch to Azure AD?**. Learn how to **connect your organization to Azure AD**.
- You must be a Project Administrator, Project Collection Administrator, or organization Owner. You must also have at least Basic access, not Stakeholder.
- To create and manage Azure AD groups, you need Azure AD administrator permissions or have the directory administrator delegate those permissions to you in the **Azure portal**.
- Azure AD changes might take up to 1 hour to be visible in Azure DevOps.

Set up self-service group management in Azure Active Directory

You can enable users to create and manage their own security groups or Microsoft 365 groups in Azure Active Directory (Azure AD). The owner of the group can approve or deny membership requests and can delegate control of group membership. Self-service group management features are not available for mail-enabled security groups or distribution lists.

Create a basic group and add members using Azure Active Directory

You can create a basic group using the Azure Active Directory (Azure AD) portal. For the purposes of this article, a basic group is added to a single resource by the resource owner (administrator) and includes specific members (employees) that need to access that resource. For more complex scenarios, including dynamic memberships and rule creation, see the **Azure Active Directory user management documentation**.

Create Azure users and groups in Azure Active Directory

41 minute modular reference guide

In this module, you will:

- Add users to Azure Active Directory.
- Manage app and resource access by using Azure Active Directory groups.
- Give guest users access in Azure Active Directory business to business (B2B).

Prerequisites

- None

Manage Azure AD users

Manage users and groups in Azure Active Directory

50 minute modular reference guide

In this module, you will:

- Learn the difference between Azure AD and Windows Server Active Directory
- Understand tenants, subscriptions, and users
- Create a new Azure Active Directory
- Add users and groups to an Azure AD
- Manage roles in an Azure AD
- Learn how to create a hybrid identity solution with Azure AD Connect

Prerequisites

- Basic understanding of identity and role-based access control
- Understand how to use the Azure portal

Create an Azure account
39 minute modular reference guide

In this module, you will:

- Learn about Azure sign-up options including Azure free account.
- Create an Azure free account.
- Understand how billing works in Azure.
- Learn about different support options.

Prerequisites

- Knowledge of basic cloud computing terms and concepts
- A valid credit card to register for an Azure free account (optional)

Configure password writeback

Allow users to reset their password with Azure Active Directory self-service password reset
31 minute modular reference guide

In this module, you will:

- Decide whether to implement self-service password reset.
- Implement self-service password reset to meet your requirements.
- Configure self-service password reset to customize the experience.

Prerequisites

- Basic understanding of Azure Active Directory

Configure authentication methods including password hash and Pass Through

User sign-in with Azure Active Directory Pass-through Authentication

Implement password hash synchronization with Azure AD Connect sync

This article provides information that you need to synchronize your user passwords from an on-premises Active Directory instance to a cloud-based Azure Active Directory (Azure AD) instance.

What is federation with Azure AD?

Federation is a collection of domains that have established trust. The level of trust may vary, but typically includes authentication and almost always includes authorization. A typical federation might include a number of organizations that have established trust for shared access to a set of resources.

You can federate your on-premises environment with Azure AD and use this federation for authentication and authorization. This sign-in method ensures that all user authentication occurs on-premises. This method allows administrators to implement more rigorous levels of access control. Federation with AD FS and PingFederate is available.

Azure Active Directory Seamless Single Sign-On

Azure Active Directory Seamless Single Sign-On (Azure AD Seamless SSO) automatically signs users in when they are on their corporate devices connected to your corporate network. When enabled, users don't need to type in their passwords to sign in to Azure AD, and usually, even type in their usernames. This feature provides your users easy access to your cloud-based applications without needing any additional on-premises components.

Key benefits

- *Great user experience*
- Users are automatically signed into both on-premises and cloud-based applications.
- Users don't have to enter their passwords repeatedly.
- *Easy to deploy & administer*
- No additional components needed on-premises to make this work.
- Works with any method of cloud authentication - **Password Hash Synchronization** or **Pass-through Authentication**.
- Can be rolled out to some or all your users using Group Policy.
- Register non-Windows 10 devices with Azure AD without the need for any AD FS infrastructure. This capability needs you to use version 2.1 or later of the **workplace-join client**.

Feature highlights

- Sign-in username can be either the on-premises default username (userPrincipalName) or another attribute configured in Azure AD Connect (Alternate ID). Both use cases work because Seamless SSO uses the securityIdentifier claim in the Kerberos ticket to look up the corresponding user object in Azure AD.
- Seamless SSO is an opportunistic feature. If it fails for any reason, the user sign-in experience goes back to its regular behavior - i.e, the user needs to enter their password on the sign-in page.

- If an application (for example, **https://myapps.microsoft.com/contoso.com**) forwards a domain_hint (OpenID Connect) or whr (SAML) parameter - identifying your tenant, or login_hint parameter - identifying the user, in its Azure AD sign-in request, users are automatically signed in without them entering usernames or passwords.
- Users also get a silent sign-on experience if an application (for example, **https://contoso.sharepoint.com**) sends sign-in requests to Azure AD's endpoints set up as tenants - that is, **https://login.microsoftonline.com/contoso.com/<..>** or **https://login.microsoftonline.com/<tenant_ID>/<..>** - instead of Azure AD's common endpoint - that is, **https://login.microsoftonline.com/common/<...>**.
- Sign out is supported. This allows users to choose another Azure AD account to sign in with, instead of being automatically signed in using Seamless SSO automatically.
- Microsoft 365 Win32 clients (Outlook, Word, Excel, and others) with versions 16.0.8730.xxxx and above are supported using a non-interactive flow. For OneDrive, you will have to activate the **OneDrive silent config feature** for a silent sign-on experience.
- It can be enabled via Azure AD Connect.
- It is a free feature, and you don't need any paid editions of Azure AD to use it.
- It is supported on web browser-based clients and Office clients that support **modern authentication** on platforms and browsers capable of Kerberos authentication

Azure AD Connect sync: Understand and customize synchronization

The Azure Active Directory Connect synchronization services (Azure AD Connect sync) is a main component of Azure AD Connect. It takes care of all the operations that are related to synchronize identity data between your on-premises environment and Azure AD. Azure AD Connect sync is the successor of DirSync, Azure AD Sync, and Forefront Identity Manager with the Azure Active Directory Connector configured.

This topic is the home for Azure AD Connect sync (also called sync engine) and lists links to all other topics related to it. For links to Azure AD Connect, see **Integrating your on-premises identities with Azure Active Directory**.

The sync service consists of two components, the on-premises Azure AD Connect sync component and the service side in Azure AD called Azure AD Connect sync service.

Authentication (PTA), OAuth, and passwordless

Permissions and Consent Framework
66 minute modular reference guide

In this module, you will:
- Compare and contrast different permission types supported by the Microsoft identity platform

- Compare and contrast the difference between static and dynamic consent in user permissions
- Create an app that implements dynamic consent for incrementally obtaining permissions as needed from users

Prerequisites

- Basic knowledge of OAuth authentication flows and terminologies
- Ability to develop with ASP.NET Core at the intermediate level
- Ability to develop with JavaScript or TypeScript at the intermediate level
- Experience using Visual Studio Code at the beginner level
- Access to a Microsoft 365 tenant

How does Azure Active Directory Pass-through Authentication work?

This article is an overview of how Azure Active directory (Azure AD) Pass-through Authentication works. For deep technical and security information, see the Security deep dive article.

Azure Active Directory Pass-through Authentication: Current limitations

Supported scenarios
The following scenarios are supported:

- User sign-ins to web browser-based applications.
- User sign-ins to Outlook clients using legacy protocols such as Exchange ActiveSync, EAS, SMTP, POP and IMAP.
- User sign-ins to legacy Office client applications and Office applications that support **modern authentication**: Office 2013 and 2016 versions.
- User sign-ins to legacy protocol applications such as PowerShell version 1.0 and others.
- Azure AD joins for Windows 10 devices.
- App passwords for Multi-Factor Authentication.

Unsupported scenarios
The following scenarios are *not* supported:

- Detection of users with **leaked credentials**.
- Azure AD Domain Services needs Password Hash Synchronization to be enabled on the tenant. Therefore tenants that use Pass-through Authentication *only* don't work for scenarios that need Azure AD Domain Services.
- Pass-through Authentication is not integrated with **Azure AD Connect Health**.

Azure Active Directory Pass-through Authentication security deep dive

This article provides a more detailed description of how Azure Active Directory (Azure AD) Pass-through Authentication works. It focuses on the security aspects of the feature. This article is for security and IT administrators, chief compliance and security officers, and other IT professionals who are responsible for IT security and compliance at small-to-medium sized organizations or large enterprises.

The topics addressed include:

- Detailed technical information about how to install and register the Authentication Agents.
- Detailed technical information about the encryption of passwords during user sign-in.
- The security of the channels between on-premises Authentication Agents and Azure AD.
- Detailed technical information about how to keep the Authentication Agents operationally secure.
- Other security-related topics.

User Privacy and Azure Active Directory Pass-through Authentication

Azure AD Pass-through Authentication creates the following log type, which can contain Personal Data:

- Azure AD Connect trace log files.
- Authentication Agent trace log files.
- Windows Event log files.

Improve user privacy for Pass-through Authentication in two ways:

1. Upon request, extract data for a person and remove data from that person from the installations.
2. Ensure no data is retained beyond 48 hours.

Transfer Azure subscription between Azure AD tenants

Transfer an Azure subscription to a different Azure AD directory

Organizations might have several Azure subscriptions. Each subscription is associated with a particular Azure Active Directory (Azure AD) directory. To make management easier, you might want to transfer a subscription to a different Azure AD directory. When you transfer a subscription to a different Azure AD directory, some resources are not transferred to the target directory. For example, all role assignments and custom roles in Azure role-based access control (Azure RBAC) are permanently deleted from the source directory and are not be transferred to the target directory.

This article describes the basic steps you can follow to transfer a subscription to a different Azure AD directory and re-create some of the resources after the transfer.

Transfer billing ownership of an Azure subscription to another account

This article shows the steps needed to transfer billing ownership of an Azure subscription to another account. Before you transfer billing ownership for a subscription, read **About transferring billing ownership for an Azure subscription**.

If you want to keep your billing ownership but change subscription type, see **Switch your Azure subscription to another offer**. To control who can access resources in the

subscription, see **Azure built-in roles**.

If you're an Enterprise Agreement (EA) customer, your enterprise administrator can transfer billing ownership of your subscriptions between accounts. For more information, **Change Azure subscription or account ownership**.

Only the billing administrator of an account can transfer ownership of a subscription.

Configure secure access by using Azure AD

Monitor privileged access for Azure AD Privileged Identity Management (PIM)

Implement privileged access management
39 minute modular reference guide

In this module, you will:
- Explain the difference between privileged access management and privileged identity management.
- Describe the privileged access management process flow.
- Describe how to configure and enable privileged access management.

Prerequisites
- Cloud computing concepts
- Microsoft 365 product and services

What is Azure AD Privileged Identity Management?

Privileged Identity Management (PIM) is a service in Azure Active Directory (Azure AD) that enables you to manage, control, and monitor access to important resources in your organization. These resources include resources in Azure AD, Azure, and other Microsoft Online Services such as Microsoft 365 or Microsoft Intune. The following video introduces you to important PIM concepts and features.

Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about.

Here are some of the key features of Privileged Identity Management:
- Provide just-in-time privileged access to Azure AD and Azure resources
- Assign time-bound access to resources using start and end dates
- Require approval to activate privileged roles
- Enforce multi-factor authentication to activate any role
- Use justification to understand why users activate
- Get notifications when privileged roles are activated
- Conduct access reviews to ensure users still need roles
- Download audit history for internal or external audit

Privileged Identity Management supports the following scenarios:

Privileged Role administrator permissions

- Enable approval for specific roles
- Specify approver users or groups to approve requests
- View request and approval history for all privileged roles

Approver permissions

- View pending approvals (requests)
- Approve or reject requests for role elevation (single and bulk)
- Provide justification for my approval or rejection

Eligible role user permissions

- Request activation of a role that requires approval
- View the status of your request to activate
- Complete your task in Azure AD if activation was approved

Configure Access Reviews

Create an access review of Azure AD roles in Privileged Identity Management

This article describes how to create one or more access reviews for privileged Azure AD roles.

Create an access review of groups and applications in Azure AD access reviews

Access to groups and applications for employees and guests changes over time. To reduce the risk associated with stale access assignments, administrators can use Azure Active Directory (Azure AD) to create access reviews for group members or application access. If you need to routinely review access, you can also create recurring access reviews. For more information about these scenarios, see **Manage user access** **and** **Manage guest access**.

You can also create access reviews using APIs. What you do to manage access reviews of groups and application users in the Azure portal can also be done using Microsoft Graph APIs. For more information, see the **Azure AD access reviews API reference**. For a code sample, see **Example of retrieving Azure AD access reviews via Microsoft Graph**.

Additional reference and review:

- **Review access to groups or applications**
- **Review access for yourself to groups or applications**
- **Complete an access review of groups or applications**

Activate and configure PIM

Privileged Identity Management "How-to" Guides

Deploy Azure AD Privileged Identity Management (PIM)
This article is a step-by-step guide describing how to plan the deployment of Privileged Identity Management (PIM) in your Azure Active Directory (Azure AD) organization. You'll reassign users in high-privileged roles to less powerful built-in or custom roles where

possible, and plan for just-in-time role assignments for your most privileged roles. In this article, we make recommendations for both deployment planning and implementation.

Start using Privileged Identity Management
This article describes how to enable Privileged Identity Management (PIM) and get started using it.

Use Privileged Identity Management (PIM) to manage, control, and monitor access within your Azure Active Directory (Azure AD) organization. With PIM you can provide as-needed and just-in-time access to Azure resources, Azure AD resources, and other Microsoft online services like Microsoft 365 or Microsoft Intune.

Prepare PIM for Azure AD roles
Here are the tasks we recommend for you to prepare Privileged Identity Management to manage

Azure AD roles:

4. **Configure Azure AD role settings**.
5. **Give eligible assignments**.
6. **Allow eligible users to activate their Azure AD role just-in-time**.

Prepare PIM for Azure roles
Here are the tasks we recommend for you to prepare Privileged Identity Management to manage

Azure roles for a subscription:

5. **Discover Azure resources**
6. **Configure Azure role settings**.
7. **Give eligible assignments**.
8. **Allow eligible users to activate their Azure roles just-in-time**.

Implement Conditional Access policies including Multi-Factor Authentication

Plan a Conditional Access deployment
What is Conditional Access?

Conditional Access: Require MFA for all users

Common Conditional Access policies

Typical policies deployed by organizations

- **Block legacy authentication***
- **Require MFA for administrators***
- **Require MFA for Azure management***
- **Require MFA for all users***

* These four policies when configured together, mimic functionality enabled by **security defaults**.

Additional policies

- **Sign-in risk-based Conditional Access (Requires Azure AD Premium P2)**

- **User risk-based Conditional Access (Requires Azure AD Premium P2)**
- **Require trusted location for MFA registration**
- **Block access by location**
- **Require compliant device**
- **Block access except specific apps**

Tutorial: Secure user sign-in events with Azure AD Multi-Factor Authentication

This tutorial shows an administrator how to enable Azure AD Multi-Factor Authentication.

In this tutorial you learn how to:

- Create a Conditional Access policy to enable Azure AD Multi-Factor Authentication for a group of users
- Configure the policy conditions that prompt for MFA
- Test the MFA process as a user

Prerequisites

To complete this tutorial, you need the following resources and privileges:

- A working Azure AD tenant with at least an Azure AD Premium P1 or trial license enabled.
- If needed, **create one for free**.
- An account with *global administrator* privileges.
- A non-administrator user with a password you know, such as *testuser*. You test the end-user Azure AD Multi-Factor Authentication experience using this account in this tutorial.
- If you need to create a user, see **Quickstart: Add new users to Azure Active Directory**.
- A group that the non-administrator user is a member of, such as *MFA-Test-Group*. You enable Azure AD Multi-Factor Authentication for this group in this tutorial.
- If you need to create a group, see how to **Create a group and add members in Azure Active Directory**.

Secure Azure Active Directory users with Multi-Factor Authentication

38 minute modular reference guide

In this module, you will:

- Learn about Azure AD Multi-Factor Authentication (Azure AD MFA)
- Create a plan to deploy Azure AD MFA
- Turn on Azure AD MFA for users and specific apps

Prerequisites

- Basic knowledge of the Azure portal
- Basic knowledge of Azure Active Directory

Strengthen authentication (conditional access) with Azure Active Directory

24 minute modular reference guide

In this module, you will:

- Define modern authentication.
- Understand how to enable multi-factor authentication.
- Explain how passwordless authentication improves security.

Prerequisites

- Intermediate understanding of Microsoft 365 and Azure Active Directory.

Configure Azure AD identity protection

Protect your identities with Azure AD Identity Protection
34 minute modular reference guide

In this module, you will:
- Describe the features of Azure Active Directory Identity Protection.
- Describe the investigation and remediation features of Azure Active Directory Identity Protection.

Prerequisites
- Basic familiarity with Azure Active Directory

Enable identity protection in Azure Active Directory
31 minute modular reference guide

In this module, you will:
- How to define Azure Active Directory Identity Protection.
- About Azure Active Directory Identity Protection support for development tools.
- How users can remediate risky behavior.

Prerequisites
- Intermediate understanding of Microsoft 365 and Azure Active Directory.

How To: Configure the Azure AD Multi-Factor Authentication registration policy
Azure AD Identity Protection helps you manage the roll-out of Azure AD Multi-Factor Authentication (MFA) registration by configuring a Conditional Access policy to require MFA registration no matter what modern authentication app you are signing in to.

Plan an Azure Active Directory self-service password reset deployment
This deployment plan offers guidance and best practices for deploying Azure AD self-service password reset (SSPR).

Plan an Azure AD Multi-Factor Authentication deployment
Azure AD Multi-Factor Authentication (MFA) helps safeguard access to data and applications. It provides an additional layer of security using a second form of authentication. Organizations can use **Conditional Access** to make the solution fit their specific needs.

This deployment guide shows you how to plan and then test an Azure AD Multi-Factor Authentication roll-out.

User experiences with Azure AD Identity Protection

With Azure Active Directory Identity Protection, you can:
- Require users to register for Azure AD Multi-Factor Authentication (MFA)
- Automate remediation of risky sign-ins and compromised users

All of the Identity Protection policies have an impact on the sign in experience for users. Allowing users to register for and use tools like Azure AD MFA and self-service password reset can lessen the impact. These tools along with the appropriate policy choices give users a self-remediation option when they need it.

Manage Application Access

Create App Registration

Quickstart: Register an application with the Microsoft identity platform
In this quickstart, you register an app in the Azure portal so the Microsoft identity platform can provide authentication and authorization services for your application and its users.

Each application you want the Microsoft identity platform to perform identity and access management (IAM) for needs to be registered. Whether it's a client application like a web or mobile app, or it's a web API that backs a client app, registering it establishes a trust relationship between your application and the identity provider, the Microsoft identity platform.

Prerequisites
- An Azure account with an active subscription - **create an account for free**
- Completion of **Quickstart: Set up a tenant**

Configure App Registration permission scopes

Quickstart: Configure an application to expose a web API

In this quickstart, you register a web API with the Microsoft identity platform and expose it to client apps by adding an example scope. By registering your web API and exposing it through scopes, you can provide permissions-based access to its resources to authorized users and client apps that access your API.

The code in a client application requests permission to perform operations defined by your web API by passing an access token along with its requests to the protected resource (the web API). Your web API then performs the requested operation only if the access token it receives contains the scopes required for the operation.

Prerequisites
- An Azure account with an active subscription - **create an account for free**
- Completion of **Quickstart: Set up a tenant**

Manage App Registration permission consent

Quickstart: Configure a client application to access a web API

In this quickstart, you provide a client app registered with the Microsoft identity platform with scoped, permissions-based access to your own web API. You also provide the client app access to Microsoft Graph.

By specifying a web API's scopes in your client app's registration, the client app can obtain an access token containing those scopes from the Microsoft identity platform. Within its code, the web API can then provide permission-based access to its resources based on the scopes found in the access token.

Prerequisites

- An Azure account with an active subscription - **create an account for free**
- Completion of **Quickstart: Register an application**
- Completion of **Quickstart: Configure an application to expose a web API**

Control authentication for your APIs with Azure API Management

55 minute modular reference guide

In this module, you will:

- Use API keys to secure your APIs
- Use client certificate authentication to secure your APIs

Prerequisites

- Basic understanding of certificates
- Basic understanding of API Management

Manage API access to Azure subscriptions and resources

Publish and manage your APIs with Azure API Management
38 minute modular reference guide

In this module, you will:

- Create an Azure API gateway
- Import an API to the API gateway
- Publish an API ready for developer access
- Call an API with a subscription key

Prerequisites

- Familiarity with basic concepts of web APIs, such as operations and endpoints

Subscriptions in Azure API Management

Subscriptions are an important concept in Azure API Management. They're the most common way for API consumers to get access to APIs published through an API Management instance. This article provides an overview of the concept.

How to use Role-Based Access Control in Azure API Management

Azure API Management relies on Azure role-based access control (Azure RBAC) to enable fine-grained access management for API Management services and entities (for example, APIs and policies). This article gives you an overview of the built-in and custom roles in API Management. For more information on access management in the Azure portal, see **Get started with access management in the Azure portal.**

Manage Access Control

Configure subscription and resource permissions

Add or remove Azure role assignments using the Azure portal

Azure role-based access control (Azure RBAC) is the authorization system you use to manage access to Azure resources. To grant access, you assign roles to users, groups, service principals, or managed identities at a particular scope. This article describes how to assign roles using the Azure portal.

If you need to assign administrator roles in Azure Active Directory, see **View and assign administrator roles in Azure Active Directory.**

Secure your Azure resources with role-based access control (RBAC)
37 minute modular reference guide

In this module, you will:
- Verify access to resources for yourself and others
- Grant access to resources
- View activity logs of RBAC changes

Prerequisites
- Knowledge of basic Azure concepts, such as the Azure portal and resource groups

Configure resource group permissions

Control and organize Azure resources with Azure Resource Manager
46 minute modular reference guide

In this module, you will:
- Use resource groups to organize Azure resources
- Use tags to organize resources
- Apply policies to enforce standards in your Azure environments
- Use resource locks to protect critical Azure resources from accidental deletion

Prerequisites
- Access to an Azure subscription to complete the exercises

Build a cloud governance strategy on Azure
48 minute modular reference guide

In this module, you will:

- Make organizational decisions about your cloud environment by using the Cloud Adoption Framework for Azure.
- Define who can access cloud resources by using Azure role-based access control.
- Apply a resource lock to prevent accidental deletion of your Azure resources.
- Apply tags to your Azure resources to help describe their purpose.
- Control and audit how your resources are created by using Azure Policy.
- Enable governance at scale across multiple Azure subscriptions by using Azure Blueprints.

Prerequisites

- You should be familiar with basic computing concepts and terminology.
- An understanding of cloud computing is helpful, but isn't necessary.

Manage Azure Resource Manager resource groups by using the Azure portal

Learn how to use the **Azure portal** with **Azure Resource Manager** to manage your Azure resource groups. For managing Azure resources, see **Manage Azure resources by using the Azure portal.**

Other articles about managing resource groups:

- **Manage Azure resource groups by using Azure CLI**
- **Manage Azure resource groups by using Azure PowerShell**

Configure custom RBAC roles

What is Azure role-based access control (Azure RBAC)?

Access management for cloud resources is a critical function for any organization that is using the cloud. Azure role-based access control (Azure RBAC) helps you manage who has access to Azure resources, what they can do with those resources, and what areas they have access to.

Azure RBAC is an authorization system built on **Azure Resource Manager** that provides fine-grained access management of Azure resources.

Classic subscription administrator roles, Azure roles, and Azure AD roles

This article helps explain the following roles and when you would use each:

- Classic subscription administrator roles
- Azure roles
- Azure Active Directory (Azure AD) roles

Understand Azure role definitions

If you are trying to understand how an Azure role works or if you are creating your own **Azure custom role**, it's helpful to understand how roles are defined. This article describes the details of role definitions and provides some examples.

Azure custom roles

If the **Azure built-in roles** don't meet the specific needs of your organization, you can create your own custom roles. Just like built-in roles, you can assign custom roles to users, groups, and service principals at management group, subscription, and resource group scopes.

Custom roles can be shared between subscriptions that trust the same Azure AD directory. There is a limit of 5,000 custom roles per directory. (For Azure Germany and Azure China 21Vianet, the limit is 2,000 custom roles.) Custom roles can be created using the Azure portal, Azure PowerShell, Azure CLI, or the REST API.

Create custom roles for Azure resources with role-based access control (RBAC)
30 minute modular reference guide

In this module, you will:

- Identify role definition structure and properties
- Create and manage an Azure custom role for resource access management

Prerequisites

- Basic knowledge of access management concepts in Azure like Azure role-based access control (RBAC).
- (Optional) Access to an Azure subscription where you have the User Access Administrator or Owner role for your account

Identify the appropriate role

Manage access to an Azure subscription by using Azure role-based access control (RBAC)
21 minute modular reference guide

In this module, you will:

- Identify the appropriate role to assign to an employee.
- Identify scenarios where the Global Administrator for Azure Active Directory might need to temporarily elevate their access in Azure.
- Grant the employee management access to a subscription.

Prerequisites

- A basic understanding of how Azure role-based access control (RBAC) works
- (Optional) Access to an Azure subscription where you have the Global Administrator role for your account

Steps to add a role assignment

Azure role-based access control (Azure RBAC) is the authorization system you use to manage access to Azure resources. To grant access, you assign roles to users, groups, service principals, or managed identities at a particular scope. This article describes the high-level steps to add a role assignment using the **Azure portal**, **Azure PowerShell**, **Azure CLI**, or the **REST API**.

The following articles offer detailed steps for how to add role assignments.

- **Add or remove Azure role assignments using the Azure portal**
- **Add or remove Azure role assignments using Azure PowerShell**
- **Add or remove Azure role assignments using Azure CLI**
- **Add or remove Azure role assignments using the REST API**

Apply principle of least privilege

Zero Trust Deployment Guide for Microsoft Azure Active Directory

Microsoft is providing a series of deployment guides for customers who have engaged in a **Zero Trust security strategy**. In this guide, we cover how to deploy and configure Azure Active Directory (Azure AD) capabilities to support your Zero Trust security strategy.

For simplicity, this document will focus on ideal deployments and configuration. We will call out the integrations that need Microsoft products other than Azure AD and we will note the licensing needed within Azure AD (Premium P1 vs P2), but we will not describe multiple solutions (one with a lower license and one with a higher license).

Administrator roles by admin task in Azure Active Directory

In this article, you can find the information needed to restrict a user's administrator permissions by assigning least privileged roles in Azure Active Directory (Azure AD). You will find administrator tasks organized by feature area and the least privileged role required to perform each task, along with additional non-Global Administrator roles that can perform the task.

Interpret permissions

Permissions and consent in the Microsoft identity platform endpoint

Applications that integrate with Microsoft identity platform follow an authorization model that gives users and administrators control over how data can be accessed. The implementation of the authorization model has been updated on the Microsoft identity platform endpoint, and it changes how an app must interact with the Microsoft identity platform. This article covers the basic concepts of this authorization model, including scopes, permissions, and consent.

Azure Active Directory consent framework

The Azure Active Directory (Azure AD) consent framework makes it easy to develop multi-tenant web and native client applications. These applications allow sign-in by user accounts from an Azure AD tenant that's different from the one where the application is registered. They may also need to access web APIs such as the Microsoft Graph API (to access Azure AD, Intune, and services in Microsoft 365) and other Microsoft services' APIs, in addition to your own web APIs.

Admin consent on the Microsoft identity platform

Some permissions require consent from an administrator before they can be granted within a tenant. You can also use the admin consent endpoint to grant permissions to an entire tenant.

Understanding Azure AD application consent experiences

Learn more about the Azure Active Directory (Azure AD) application consent user experience. So you can intelligently manage applications for your organization and/or develop applications with a more seamless consent experience.

Check access

Define identity and access management in Azure Active Directory
15 minute modular reference guide

In this module, you will:
- Define the latest identity technologies.
- Understand the value of securing your identity.
- Explain how identity is core to security.

Prerequisites
- Intermediate understanding of Microsoft 365 and Azure Active Directory.

Quickstart: View the access a user has to Azure resources

You can use the Access control (IAM) blade in **Azure role-based access control (Azure RBAC)** to view the access a user or another security principal has to Azure resources. However, sometimes you just need to quickly view the access for a single user or another security principal. The easiest way to do this is to use the Check access feature in the Azure portal.

Tutorial: Grant a user access to Azure resources using the Azure portal

Azure role-based access control (Azure RBAC) is the way that you manage access to Azure resources. In this tutorial, you grant a user access to create and manage virtual machines in a resource group.

In this tutorial, you learn how to:
- Grant access for a user at a resource group scope
- Remove access

Implement platform protection (15-20%)

Implement Advanced Network Security

Configure and manage virtual networks for Azure administrators
13 Hour 14 minute modular reference guide

Learn how to configure and manage Azure network capabilities like connectivity services, application protection, application delivery, and network monitoring services.

Prerequisites

- **Azure Fundamentals Part 1: Describe core Azure concepts**
- **Azure Fundamentals Part 2: Describe core Azure services**
- **Azure Fundamentals Part 3: Describe core solutions and management tools on Azure**
- **Azure Fundamentals Part 4: Describe general security and network security features**
- **Azure Fundamentals Part 5: Describe identity, governance, privacy, and compliance features**
- **Azure Fundamentals Part 6: Describe Azure cost management and service level agreements**
- **Prerequisites for Azure administrators**

Secure the connectivity of virtual networks (VPN authentication, Express Route encryption)

Secure network connectivity on Azure
32 minute modular reference guide

Learn about the Azure services you can use to help ensure that your network is safe, secure, and trusted.

After completing this module, you'll be able to:

- Identify the layers that make up a *defense in depth* strategy.
- Explain how Azure Firewall enables you to control what traffic is allowed on the network.
- Configure network security groups to filter network traffic to and from Azure resources within a Microsoft Azure virtual network.
- Explain how Azure DDoS Protection helps protect your Azure resources from DDoS attacks.

Prerequisites

- You should be familiar with basic computing concepts and terminology.
- An understanding of cloud computing is helpful, but isn't necessary.

Connect your on-premises network to Azure with VPN Gateway
39 minute modular reference guide

VPN Gateway in Azure provides secure connectivity between your on-premises networks and clients.

After completing this module, you'll be able to:

- Learn the features and use cases of VPN gateways
- Learn the requirements for provisioning VPN gateways
- Provision site-to-site VPN gateways

Prerequisites

- Familiarity with Azure virtual networking

Connect your on-premises network to the Microsoft global network by using ExpressRoute
40 minute modular reference guide

Connect your on-premises systems and users to Azure and Office 365 by using ExpressRoute for private, dedicated, and guaranteed throughput connectivity.

After completing this module, you'll be able to:
- Describe the features and capabilities of ExpressRoute
- Describe the use cases for using ExpressRoute to integrate traditional networks with Azure

Prerequisites
- Basic knowledge of network concepts

Configure Network Security Groups (NSGs) and Application Security Groups (ASGs)

Secure and isolate access to Azure resources by using network security groups and service endpoints
43 minute modular reference guide

Network security groups and service endpoints help you secure your virtual machines and Azure services from unauthorized network access.

After completing this module, you'll be able to:
- Identify the capabilities and features of network security groups.
- Identify the capabilities and features of virtual network service endpoints.
- Use network security groups to restrict network connectivity.
- Use virtual network service endpoints to control network traffic to and from Azure services.

Prerequisites
- Knowledge of basic networking concepts, including subnets and IP addressing
- Basic familiarity with Azure services, specifically Azure SQL Database and Azure Storage
- Familiarity with Azure virtual machines and virtual networking

Tutorial: Filter network traffic with a network security group using the Azure portal

You can filter network traffic inbound to and outbound from a virtual network subnet with a network security group. Network security groups contain security rules that filter network traffic by IP address, port, and protocol. Security rules are applied to resources deployed in a subnet.

In this tutorial, you learn how to:
- Create a network security group and security rules
- Create a virtual network and associate a network security group to a subnet
- Deploy virtual machines (VM) into a subnet
- Test traffic filters

If you prefer, you can complete this tutorial using the **Azure CLI** **or** **PowerShell**.

Create and configure Azure Firewall

Implement Windows Server IaaS VM network security
69 minute modular reference guide

In this module, you will focus on how to improve the network security for Windows Server infrastructure as a service (IaaS) virtual machines (VMs) and how to diagnose network security issues with those VMs.

After completing this module, you'll be able to:

- Implement Network Security Groups (NSGs) with Windows Server IaaS VMs.
- Implement adaptive network hardening.
- Implement Azure Firewall.
- Implement Windows Defender Firewall in Windows Server IaaS VMs.
- Choose an appropriate filtering solution.
- Capture network traffic with Network Watcher.

Prerequisites
To get the best learning experience from this module, it's important that you have knowledge and experience in the following areas:

- Managing Windows Server operating systems (OSs) and Windows Server workloads in on-premises scenarios, including AD DS, Domain Name System (DNS), the Distributed File System (DFS), Microsoft Hyper-V, and file and storage services
- Common Windows Server management tools
- Core Microsoft compute, storage, networking, and virtualization technologies
- On-premises resiliency Windows Server–based compute and storage technologies
- Implementing and managing IaaS services in Azure
- Azure Active Directory (Azure AD)
- Security-related technologies (firewalls, encryption, multi-factor authentication)
- Windows PowerShell scripting
- Automation and monitoring

What is Azure Firewall?

Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources. It's a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability.

Features
To learn about Azure Firewall features, see **Azure Firewall features**.

Pricing and SLA
For Azure Firewall pricing information, see **Azure Firewall pricing**.
For Azure Firewall SLA information, see **Azure Firewall SLA**.

What's new
To learn what's new with Azure Firewall, see **Azure updates**.

Next steps

- **Tutorial: Deploy and configure Azure Firewall using the Azure portal**

- **Deploy Azure Firewall using a template**
- **Create an Azure Firewall test environment**

Configure Azure Front Door service as an Application Gateway

What is Azure Front Door?

Azure Front Door is a global, scalable entry-point that uses the Microsoft global edge network to create fast, secure, and widely scalable web applications. With Front Door, you can transform your global consumer and enterprise applications into robust, high-performing personalized modern applications with contents that reach a global audience through Azure.

Frequently asked questions for Azure Front Door

This article answers common questions about Azure Front Door features and functionality.

Quickstart: Create a Front Door for a highly available global web application

Get started with Azure Front Door by using the Azure portal to set up high availability for a web application.

In this quickstart, Azure Front Door pools two instances of a web application that run in different Azure regions. You create a Front Door configuration based on equal weighted and same priority backends. This configuration directs traffic to the nearest site that runs the application. Azure Front Door continuously monitors the web application. The service provides automatic failover to the next available site when the nearest site is unavailable.

Routing architecture overview (Azure Front Door)

When Azure Front Door receives your client requests, it will do one of two things. Either answers them if you enable caching or forwards them to the appropriate application backend as a reverse proxy.

Next steps

- Learn about **Web Application Firewall on Azure Front Door**

Configure a Web Application Firewall (WAF) on Azure Application Gateway

Load balance your web service traffic with Application Gateway

92 minute modular reference guide

Improve application resilience by distributing load across multiple servers and use path-based routing to direct web traffic.

After completing this module, you'll be able to:

- Identify the load balancing capabilities of Application Gateway

- Create an Application Gateway and configure load balancing
- Configure an Application Gateway to use URL path-based routing

Prerequisites
- Knowledge of basic networking concepts
- Familiarity with Azure virtual machines and Azure App Service
- Familiarity with Azure virtual networking

What is Azure Web Application Firewall on Azure Application Gateway?

Azure Web Application Firewall (WAF) on Azure Application Gateway provides centralized protection of your web applications from common exploits and vulnerabilities. Web applications are increasingly targeted by malicious attacks that exploit commonly known vulnerabilities. SQL injection and cross-site scripting are among the most common attacks.

What's new
To learn what's new with Azure Web Application Firewall, see **Azure updates**.

Next steps
- Learn more about **WAF managed rules**
- Learn more about **Custom Rules**

Configure Azure Bastion

Connect to virtual machines through the Azure portal by using Azure Bastion
40 minute modular reference guide

Deploy Azure Bastion to securely connect to Azure virtual machines directly within the Azure portal, to effectively replace an existing jumpbox solution. Monitor remote sessions by using diagnostic logs. Manage remote sessions by disconnecting a user session.

After completing this module, you'll be able to:
- Evaluate Azure Bastion as a replacement for a VM jumpbox solution
- Configure Bastion to securely connect to VMs
- Manage remote sessions by enabling diagnostic logs and monitoring remote sessions

Prerequisites
- Experience managing remote connections to virtual machines
- Familiarity with networking concepts like virtual networks, public and private IPs, and network protocols SSH, RDP, and TLS
- (Optional) Access to an Azure subscription where you have permissions to create resources like VMs

What is Azure Bastion?

Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal. The Azure Bastion service is a fully platform-managed PaaS service that you provision inside your virtual network. It provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal

over TLS. When you connect via Azure Bastion, your virtual machines do not need a public IP address, agent, or special client software.

Bastion provides secure RDP and SSH connectivity to all of the VMs in the virtual network in which it is provisioned. Using Azure Bastion protects your virtual machines from exposing RDP/SSH ports to the outside world, while still providing secure access using RDP/SSH.

Tutorial: Configure Bastion and connect to a Windows VM through a browser

This tutorial shows you how to connect to a virtual machine through your browser using Azure Bastion and the Azure portal. In the Azure portal, you deploy Bastion to your virtual network. After deploying Bastion, you connect to a VM via its private IP address using the Azure portal. Your VM does not need a public IP address or special software. Once the service is provisioned, the RDP/SSH experience is available to all of the virtual machines in the same virtual network. For more information about Azure Bastion, see **What is Azure Bastion?**.

In this tutorial, you'll learn how to:

- Create a bastion host for your VNet
- Connect to a Windows virtual machine

Working with NSG access and Azure Bastion

When working with Azure Bastion, you can use network security groups (NSGs). For more information, see **Security Groups**.

Azure Bastion FAQ

Configure a firewall on a storage account, Azure SQL, KeyVault, or App Service

Protect data in-transit and at rest

43 minute modular reference guide

Explore encryption options available within Azure SQL, on-premises SQL Server and Open Source data platforms and Secure Enclaves. Implement database and instance firewalls.

After completing this module, you'll be able to:

- Understand the data encryption options available in the various platforms
- Configure encryption for data at rest and in transit
- Implement object level encryption
- Configure SQL Server to use Azure Key Vault
- Understand the difference between database and instance firewalls in Azure SQL Database
- Explore Secure Enclaves

Prerequisites

- Ability to use tools for running queries against a Microsoft SQL database, either on-premises on cloud-based.
- Understanding of why security is a crucial part of database system planning.
- Experience creating and configuring resources using the Azure portal.

Configure Azure Storage firewalls and virtual networks

Azure Storage provides a layered security model. This model enables you to secure and control the level of access to your storage accounts that your applications and enterprise environments demand, based on the type and subset of networks used. When network rules are configured, only applications requesting data over the specified set of networks can access a storage account. You can limit access to your storage account to requests originating from specified IP addresses, IP ranges or from a list of subnets in an Azure Virtual Network (VNet).

Storage accounts have a public endpoint that is accessible through the internet. You can also create **Private Endpoints for your storage account,** which assigns a private IP address from your VNet to the storage account, and secures all traffic between your VNet and the storage account over a private link. The Azure storage firewall provides access control access for the public endpoint of your storage account. You can also use the firewall to block all access through the public endpoint when using private endpoints. Your storage firewall configuration also enables select trusted Azure platform services to access the storage account securely.

Dig deeper into Azure Storage security in **Azure Storage security guide.**

Implement Service Endpoints

Create a service endpoint

Service endpoints are a way for Azure DevOps to connect to external systems or services. They're a bundle of properties securely stored by Azure DevOps, which includes but isn't limited to the following properties:

- Service name
- Description
- Server URL
- Certificates or tokens
- User names and passwords

Extensions are then able to use the service endpoint to acquire the stored details to do the necessary operations on that service. Follow this guide to create a new Service Point contribution and use it in your extension.

Virtual Network service endpoints

Virtual Network (VNet) service endpoint provides secure and direct connectivity to Azure services over an optimized route over the Azure backbone network. Endpoints allow you

to secure your critical Azure service resources to only your virtual networks. Service Endpoints enables private IP addresses in the VNet to reach the endpoint of an Azure service without needing a public IP address on the VNet.

Implement DDoS protection

Secure network connectivity on Azure
32 minute modular reference guide

Learn about the Azure services you can use to help ensure that your network is safe, secure, and trusted.

After completing this module, you'll be able to:

- Identify the layers that make up a defense in depth strategy.
- Explain how Azure Firewall enables you to control what traffic is allowed on the network.
- Configure network security groups to filter network traffic to and from Azure resources within a Microsoft Azure virtual network.
- Explain how Azure DDoS Protection helps protect your Azure resources from DDoS attacks.

Prerequisites

- You should be familiar with basic computing concepts and terminology.
- An understanding of cloud computing is helpful, but isn't necessary.

Azure DDoS Protection Standard overview

Distributed denial of service (DDoS) attacks are some of the largest availability and security concerns facing customers that are moving their applications to the cloud. A DDoS attack attempts to exhaust an application's resources, making the application unavailable to legitimate users. DDoS attacks can be targeted at any endpoint that is publicly reachable through the internet.

To learn about Azure DDoS Protection Standard pricing, see **Azure DDoS Protection Standard pricing**.

Quickstart: Create and configure Azure DDoS Protection Standard

Get started with Azure DDoS Protection Standard by using the Azure portal.

A DDoS protection plan defines a set of virtual networks that have DDoS protection standard enabled, across subscriptions. You can configure one DDoS protection plan for your organization and link virtual networks from multiple subscriptions to the same plan.

In this quickstart, you'll create a DDoS protection plan and link it to a virtual network.

Prerequisites

- If you don't have an Azure subscription, create a **free account** before you begin.
- Sign in to the Azure portal at **https://portal.azure.com**. Ensure that your account is assigned to the **network contributor** role or to a **custom role** that is assigned the appropriate actions listed in the how-to guide on **Permissions**.

View and configure DDoS protection telemetry

Azure DDoS Protection standard provides detailed attack insights and visualization with DDoS Attack Analytics. Customers protecting their virtual networks against DDoS attacks have detailed visibility into attack traffic and actions taken to mitigate the attack via attack mitigation reports & mitigation flow logs. Rich telemetry is exposed via Azure Monitor including detailed metrics during the duration of a DDoS attack. Alerting can be configured for any of the Azure Monitor metrics exposed by DDoS Protection. Logging can be further integrated with **Azure Sentinel**, Splunk (Azure Event Hubs), OMS Log Analytics, and Azure Storage for advanced analysis via the Azure Monitor Diagnostics interface.

In this tutorial, you'll learn how to:

- Configure alerts for DDoS protection metrics
- Use DDoS protection telemetry
- View DDoS mitigation policies
- View DDoS protection alerts in Microsoft Defender for Cloud

Configure advanced security for compute

Configure endpoint protection

Endpoint protection assessment and recommendations in Microsoft Defender for Cloud

Microsoft Defender for Cloud provides health assessments of supported versions of Endpoint protection solutions. This article explains the scenarios that lead Security Center to generate the following two recommendations:

- Install endpoint protection solutions on your virtual machine
- Resolve endpoint protection health issues on your machines

Microsoft Endpoint Protection for Azure

Microsoft Endpoint Protection for Azure - how to install, update, and configure it to constantly scan for viruses and malware within our Azure instances.

Protect against threats with Microsoft Defender Advanced Threat Protection
1 Hour 12 minute modular reference guide

Learn how Microsoft Defender Advanced Threat Protection can help your organization stay secure.

After completing this module, you'll be able to:

- Define the capabilities of Microsoft Defender Advanced Threat Protection.
- Understand how to hunt threats within your network.
- Explain how Microsoft Defender Advanced Threat Protection can remediate risks in your environment.

Prerequisites
In order to get the best learning experience from this module, it's important that you have knowledge and experience of:

- Windows Server operating system and workloads in on-premises scenarios.
- Common Windows Server management tools.
- Core Microsoft compute, storage, networking, and virtualization technologies.
- On-premises resiliency Windows Server-based compute and storage technologies.
- Implementing and managing IaaS services in Microsoft Azure.
- Azure AD.
- Security-related technologies (firewalls, encryption, multi-factor authentication).
- Windows PowerShell scripting.
- Automation and monitoring.

Configure and monitor system updates for VMs

Azure Automation Update Management

Update Management is a configuration component of Automation. Windows and Linux computers, both in Azure and on-premises, send assessment information about missing updates to the Log Analytics workspace. Azure Automation then uses that information to create a schedule for automatic deployment of the missing updates.

The following steps highlight the actual implementation:

1. Create a Log Analytics workspace.
2. Create an Automation account.
3. Link the Automation account with the Log Analytics workspace.
4. Enable Update Management for Azure VMs.
5. Enable Update Management for non-Azure VMs.

Manage updates and patches for your VMs

Software updates in Azure Automation Update Management provides a set of tools and resources that can help manage the complex task of tracking and applying software updates to machines in Azure and hybrid cloud. An effective software update management process is necessary to maintain operational efficiency, overcome security issues, and reduce the risks of increased cyber security threats. However, because of the changing nature of technology and the continual appearance of new security threats, effective software update management requires consistent and continual attention.

Update Management supports the deployment of first-party updates and the pre-downloading of them. This support requires changes on the systems being updated. See Configure Windows Update settings for Azure Automation Update Management to learn how to configure these settings on your systems.

Before attempting to manage updates for your VMs, ensure that you've enabled Update Management on them using one of these methods:

- Enable Update Management from an Automation account
- Enable Update Management by browsing the Azure portal

- Enable Update Management from a runbook
- Enable Update Management from an Azure VM

To learn how to create alerts to notify you about update deployment results, see create alerts for Update Management.

You can query Azure Monitor logs to analyze update assessments, deployments, and other related management tasks. It includes pre-defined queries to help you get started.

Configure authentication for Azure Container Registry

Authenticate with an Azure container registry

There are several ways to authenticate with an Azure container registry, each of which is applicable to one or more registry usage scenarios.

Recommended ways include authenticating to a registry directly via individual login, or your applications and container orchestrators can perform unattended, or "headless," authentication by using an Azure Active Directory (Azure AD) service principal.

Azure Container Registry authentication with service principals

You can use an Azure Active Directory (Azure AD) service principal to provide container image ***docker push*** and ***pull*** access to your container registry. By using a service principal, you can provide access to "headless" services and applications.

Use an Azure managed identity to authenticate to an Azure container registry

Use a managed identity for Azure resources to authenticate to an Azure container registry from another Azure resource, without needing to provide or manage registry credentials. For example, set up a user-assigned or system-assigned managed identity on a Linux VM to access container images from your container registry, as easily as you use a public registry.

For this article, you learn more about managed identities and how to:

- Enable a user-assigned or system-assigned identity on an Azure VM
- Grant the identity access to an Azure container registry
- Use the managed identity to access the registry and pull a container image

Configure security for different types of containers

Container security in Security Center

This article describes how you can use Security Center, together with the optional Azure Defender plans for container registries, severs, and Kubernetes, to improve, monitor, and maintain the security of your containers and their apps.
You'll learn how Security Center helps with these core aspects of container security:

- Vulnerability management - scanning container images
- Environment hardening

- Run-time protection for AKS nodes and clusters

Azure Kubernetes Service (AKS) clusters - Protections offered by Security Center

- Continuous assessment of your AKS clusters' configurations to provide visibility into misconfigurations, and guidelines to help you resolve any discovered issues.
Learn more about environment hardening through security recommendations.

- Threat protection for AKS clusters and Linux nodes. Alerts for suspicious activities are provided by the optional Azure Defender for Kubernetes.
Learn more about run-time protection for AKS nodes and clusters.

Container hosts (VMs running Docker) - Protections offered by Security Center

- Continuous assessment of your Docker configurations to provide visibility into misconfigurations, and guidelines to help you resolve any discovered issues with the optional Azure Defender for servers.
Learn more about environment hardening through security recommendations.

Implement vulnerability management

Security Control: Vulnerability Management

Vulnerability management recommendations focus on addressing issues related to continuously acquiring, assessing, and acting on new information in order to identify and remediate vulnerabilities as well as minimizing the window of opportunity for attackers.

Azure Defender's integrated vulnerability assessment solution for Azure and hybrid machines

A core component of every cyber risk and security program is the identification and analysis of vulnerabilities.

Security Center regularly checks your connected machines to ensure they're running vulnerability assessment tools.

When a machine is found that doesn't have vulnerability assessment solution deployed, Security Center generates the following security recommendation:

A vulnerability assessment solution should be enabled on your virtual machines

Use this recommendation to deploy the vulnerability assessment solution to your Azure virtual machines and your Azure Arc enabled hybrid machines.

Configure isolation for AKS

Network concepts for applications in Azure Kubernetes Service (AKS)

In a container-based microservices approach to application development, application components must work together to process their tasks. Kubernetes provides various resources that enable this application communication. You can connect to and expose applications internally or externally. To build highly available applications, you can load balance your applications. More complex applications may require configuration of ingress traffic for SSL/TLS termination or routing of multiple components. For security reasons, you may also need to restrict the flow of network traffic into or between pods and nodes.

This article introduces the core concepts that provide networking to your applications in AKS:

- Services
- Azure virtual networks
- Ingress controllers
- Network policies

Access and identity options for Azure Kubernetes Service (AKS)

There are different ways to authenticate, control access/authorize and secure Kubernetes clusters. Using Kubernetes role-based access control (Kubernetes RBAC), you can grant users, groups, and service accounts access to only the resources they need. With Azure Kubernetes Service (AKS), you can further enhance the security and permissions structure by using Azure Active Directory and Azure RBAC. These approaches help you secure your cluster access and provide only the minimum required permissions to developers and operators.

This article introduces the core concepts that help you authenticate and assign permissions in AKS:

- Kubernetes role-based access control (Kubernetes RBAC)
- Roles and ClusterRoles
- RoleBindings and ClusterRoleBindings
- Kubernetes service accounts
- Azure Active Directory integration
- Azure RBAC
- Azure RBAC to authorize access to the AKS resource
- Azure RBAC for Kubernetes Authorization (Preview)

Storage options for applications in Azure Kubernetes Service (AKS)

Applications that run in Azure Kubernetes Service (AKS) may need to store and retrieve data. For some application workloads, this data storage can use local, fast storage on the node that is no longer needed when the pods are deleted. Other application workloads may require storage that persists on more regular data volumes within the Azure platform. Multiple pods may need to share the same data volumes, or reattach data volumes if the pod is rescheduled on a different node. Finally, you may need to inject sensitive data or application configuration information into pods.

This article introduces the core concepts that provide storage to your applications in AKS:

- Volumes
- Persistent volumes
- Storage classes
- Persistent volume claims

Security hardening for AKS agent node host OS

Azure Kubernetes Service (AKS) is a secure service compliant with SOC, ISO, PCI DSS, and HIPAA standards. This article covers the security hardening applied to AKS virtual machine hosts. For more information about AKS security, see Security concepts for applications and clusters in Azure Kubernetes Service (AKS).

This document is scoped to Linux agents in AKS only.

Azure Kubernetes Service Workshop
2 Hours 25 minutes modular reference guide

In this workshop, you'll go through tasks to deploy a multicontainer application to Kubernetes on Azure Kubernetes Service (AKS).

After completing this module, you'll be able to:
- Create an Azure Kubernetes Service cluster
- Choose the best deployment options for your Pods
- Expose Pods to internal and external network users
- Configure SSL/TLS for Azure Kubernetes Service ingress
- Monitor the health of an Azure Kubernetes Service cluster
- Scale your application in an Azure Kubernetes Service cluster

Prerequisites
- Knowledge of Kubernetes and its concepts
- Access to an Azure subscription

Configure security for container registry

Azure Container Registry (ACR) registries - Protections offered by Security Center

- Vulnerability assessment and management tools for the images in your Azure Resource Manager-based ACR registries with the optional Azure Defender for container registries. Learn more about scanning your container images for vulnerabilities.

Build and store container images with Azure Container Registry
49 minute modular reference guide

Azure Container Registry is a managed Docker registry service based on the open-source Docker Registry 2.0. Container Registry is private, hosted in Azure, and allows you to build, store, and manage images for all types of container deployments. Learn how to build and store container images with Azure Container Registry.

After completing this module, you'll be able to:

- Deploy an Azure container registry
- Build a container image using Azure Container Registry Tasks
- Deploy the container to an Azure container instance
- Replicate the container image to multiple Azure regions

Prerequisites

- None

Use Azure Defender for container registries to scan your images for vulnerabilities

This page explains how to use the built-in vulnerability scanner to scan the container images stored in your Azure Resource Manager-based Azure Container Registry.

When Azure Defender for container registries is enabled, any image you push to your registry will be scanned immediately. In addition, any image pulled within the last 30 days is also scanned.

When the scanner reports vulnerabilities to Security Center, Security Center presents the findings and related information as recommendations. In addition, the findings include related information such as remediation steps, relevant CVEs, CVSS scores, and more. You can view the identified vulnerabilities for one or more subscriptions, or for a specific registry.

Azure Container Registry roles and permissions

The Azure Container Registry service supports a set of built-in Azure roles that provide different levels of permissions to an Azure container registry. Use Azure role-based access control (Azure RBAC) to assign specific permissions to users, service principals, or other identities that need to interact with a registry, for example to pull or push container images. You can also define custom roles with fine-grained permissions to a registry for different operations.

Implement Azure Disk Encryption

Azure Disk Encryption for Windows VMs

Azure Disk Encryption helps protect and safeguard your data to meet your organizational security and compliance commitments. It uses the Bitlocker feature of Windows to provide volume encryption for the OS and data disks of Azure virtual machines (VMs), and is integrated with Azure Key Vault to help you control and manage the disk encryption keys and secrets.

If you use Microsoft Defender for Cloud, you're alerted if you have VMs that aren't encrypted. The alerts show as High Severity and the recommendation is to encrypt these VMs.

You can learn the fundamentals of Azure Disk Encryption for Windows in just a few minutes with the Create and encrypt a Windows VM with Azure CLI quickstart or the Create and encrypt a Windows VM with Azure Powershell quickstart.

Next steps

- Quickstart - Create and encrypt a Windows VM with Azure CLI
- Quickstart - Create and encrypt a Windows VM with Azure Powershell
- Azure Disk Encryption scenarios on Windows VMs
- Azure Disk Encryption prerequisites CLI script
- Azure Disk Encryption prerequisites PowerShell script
- Creating and configuring a key vault for Azure Disk Encryption

Azure Disk Encryption for virtual machines and virtual machine scale sets

Linux virtual machines

The following articles provide guidance for encrypting Linux virtual machines.

Current version of Azure Disk Encryption

- Overview of Azure Disk Encryption for Linux virtual machines
- Azure Disk Encryption scenarios on Linux VMs
- Create and encrypt a Linux VM with Azure CLI
- Create and encrypt a Linux VM with Azure PowerShell
- Create and encrypt a Linux VM with the Azure portal
- Azure Disk Encryption Extension Schema for Linux
- Creating and configuring a key vault for Azure Disk Encryption
- Azure Disk Encryption sample scripts
- Azure Disk Encryption troubleshooting
- Azure Disk Encryption frequently asked questions

Azure disk encryption with Azure AD (previous version)

- Overview of Azure Disk Encryption with Azure AD for Linux virtual machines
- Azure Disk Encryption with Azure AD scenarios on Linux VMs
- Creating and configuring a key vault for Azure Disk Encryption with Azure AD (previous release)

Windows virtual machines

The following articles provide guidance for encrypting Windows virtual machines.

Current version of Azure Disk Encryption

- Overview of Azure Disk Encryption for Windows virtual machines
- Azure Disk Encryption scenarios on Windows VMs
- Create and encrypt a Windows VM with Azure CLI
- Create and encrypt a Windows VM with Azure PowerShell
- Create and encrypt a Windows VM with the Azure portal
- Azure Disk Encryption Extension Schema for Windows
- Creating and configuring a key vault for Azure Disk Encryption
- Azure Disk Encryption sample scripts
- Azure Disk Encryption troubleshooting

- Azure Disk Encryption frequently asked questions

Azure disk encryption with Azure AD (previous version)

- Overview of Azure Disk Encryption with Azure AD for Windows virtual machines
- Azure Disk Encryption with Azure AD scenarios on Windows VMs
- Creating and configuring a key vault for Azure Disk Encryption with Azure AD (previous release)

Virtual machine scale sets

The following articles provide guidance for encrypting virtual machine scale sets.

- Overview of Azure Disk Encryption for virtual machine scale sets
- Encrypt a virtual machine scale sets using the Azure CLI
- Encrypt a virtual machine scale sets using Azure Powershell.
- Encrypt a virtual machine scale sets using the Azure Resource Manager
- Create and configure a key vault for Azure Disk Encryption
- Use Azure Disk Encryption with virtual machine scale set extension sequencing

Azure data security and encryption best practices

This article describes best practices for data security and encryption.

The best practices are based on a consensus of opinion, and they work with current Azure platform capabilities and feature sets. Opinions and technologies change over time and this article is updated on a regular basis to reflect those changes.

Azure data encryption at rest

Microsoft Azure includes tools to safeguard data according to your company's security and compliance needs.

This paper focuses on:

- How data is protected at rest across Microsoft Azure
- Discusses the various components taking part in the data protection implementation,
- Reviews pros and cons of the different key management protection approaches.

Encryption at Rest is a common security requirement. In Azure, organizations can encrypt data at rest without the risk or cost of a custom key management solution. Organizations have the option of letting Azure completely manage Encryption at Rest. Additionally, organizations have various options to closely manage encryption or encryption keys.

Data encryption models

An understanding of the various encryption models and their pros and cons is essential for understanding how the various resource providers in Azure implement encryption at Rest. These definitions are shared across all resource providers in Azure to ensure common language and taxonomy.

There are three scenarios for server-side encryption:

- Server-side encryption using Service-Managed keys
  - Azure Resource Providers perform the encryption and decryption operations
  - Microsoft manages the keys
  - Full cloud functionality

- Server-side encryption using customer-managed keys in Azure Key Vault
  - Azure Resource Providers perform the encryption and decryption operations
  - Customer controls keys via Azure Key Vault
  - Full cloud functionality

- Server-side encryption using customer-managed keys on customer-controlled hardware
  - Azure Resource Providers perform the encryption and decryption operations
  - Customer controls keys on customer-controlled hardware
  - Full cloud functionality

Configure authentication and security for Azure App Service

Security recommendations for App Service

This article contains security recommendations for Azure App Service. Implementing these recommendations will help you fulfill your security obligations as described in our shared responsibility model and will improve the overall security for your Web App solutions. For more information on what Microsoft does to fulfill service provider responsibilities, read Azure infrastructure security.

Authentication and authorization in Azure App Service and Azure Functions

Azure App Service provides built-in authentication and authorization support, so you can sign in users and access data by writing minimal or no code in your web app, RESTful API, and mobile back end, and also Azure Functions. This article describes how App Service helps simplify authentication and authorization for your app.

Secure authentication and authorization require deep understanding of security, including federation, encryption, JSON web tokens (JWT) management, grant types, and so on. App Service provides these utilities so that you can spend more time and energy on providing business value to your customer.

For information specific to native mobile apps, see User authentication and authorization for mobile apps with Azure App Service.

OS and runtime patching in Azure App Service

This article shows you how to get certain version information regarding the OS or software in App Service.
App Service is a Platform-as-a-Service, which means that the OS and application stack are managed for you by Azure; you only manage your application and its data. More control over the OS and application stack is available you in Azure Virtual Machines.

With that in mind, it is nevertheless helpful for you as an App Service user to know more information, such as:

- How and when are OS updates applied?
- How is App Service patched against significant vulnerabilities (such as zero-day)?
- Which OS and runtime versions are running your apps?

For security reasons, certain specifics of security information are not published. However, the article aims to alleviate concerns by maximizing transparency on the process, and how you can stay up-to-date on security-related announcements or runtime updates.

Configure SSL/TLS certs

Top 5 security items to consider before pushing to production
45 minute modular reference guide

Secure your web applications on Azure and protect your apps against the most common and dangerous web application attacks.

After completing this module, you'll be able to:

- Use Microsoft Defender for Cloud
- Verify your application's inputs and outputs
- Store your secrets into Key Vault
- Ensure you are using the latest version of your framework, and its security features
- Validate that your program dependencies and libraries are safe to use

Prerequisites

- None

Configuring TLS for an application in Azure

Transport Layer Security (TLS), previously known as Secure Socket Layer (SSL) encryption, is the most commonly used method of securing data sent across the internet. This common task discusses how to specify an HTTPS endpoint for a web role and how to upload a TLS/SSL certificate to secure your application.

Add a TLS/SSL certificate in Azure App Service

Azure App Service provides a highly scalable, self-patching web hosting service. This article shows you how to create, upload, or import a private certificate or a public certificate into App Service.

Once the certificate is added to your App Service app or function app, you can secure a custom DNS name with it or use it in your application code.

Configure authentication for Azure Kubernetes Service

Best practices for authentication and authorization in Azure Kubernetes Service (AKS)

As you deploy and maintain clusters in Azure Kubernetes Service (AKS), you need to implement ways to manage access to resources and services. Without these controls, accounts may have access to resources and services they don't need. It can also be hard to track which set of credentials were used to make changes.

This best practices article focuses on how a cluster operator can manage access and identity for AKS clusters. In this article, you learn how to:

- Authenticate AKS cluster users with Azure Active Directory
- Control access to resources with Kubernetes role-based access control (Kubernetes RBAC)
- Use Azure RBAC to granularly control access to the AKS resource and the Kubernetes API at scale, as well as to the kubeconfig.
- Use a managed identity to authenticate pods themselves with other services

Next steps

- Integrate Azure Active Directory with AKS
- Use managed identities for Azure resources with AKS

For more information about cluster operations in AKS, see the following best practices:

- Multi-tenancy and cluster isolation
- Basic Kubernetes scheduler features
- Advanced Kubernetes scheduler features

Azure security baseline for Azure Kubernetes Service

The Azure Security Baseline for Azure Kubernetes Service contains recommendations that will help you improve the security posture of your deployment.

The baseline for this service is drawn from the Azure Security Benchmark version 1.0, which provides recommendations on how you can secure your cloud solutions on Azure with our best practices guidance.

For more information, see Azure Security Baselines overview.

Security concepts for applications and clusters in Azure Kubernetes Service (AKS)

To protect your customer data as you run application workloads in Azure Kubernetes Service (AKS), the security of your cluster is a key consideration. Kubernetes includes security components such as network policies and Secrets. Azure then adds in components such as network security groups and orchestrated cluster upgrades. These security components are combined to keep your AKS cluster running the latest OS security updates and Kubernetes releases, and with secure pod traffic and access to sensitive credentials.

This article introduces the core concepts that secure your applications in AKS

To get started with securing your AKS clusters, see Upgrade an AKS cluster.

For associated best practices, see Best practices for cluster security and upgrades in AKS and Best practices for pod security in AKS.

For additional information on core Kubernetes and AKS concepts, see the following articles:

- Kubernetes / AKS clusters and workloads
- Kubernetes / AKS identity
- Kubernetes / AKS virtual networks
- Kubernetes / AKS storage
- Kubernetes / AKS scale

Configure automatic updates

Manage Azure updates
40 minute modular reference guide

You'll be able to enable Azure Update Management, deploy updates, review an update assessment, and manage updates for your Azure VMs.

After completing this module, you'll be able to:

- Describe Azure updates.
- Enable Update Management.
- Deploy updates.
- Review an update assessment.
- Manage updates for your Azure VMs.

Prerequisites

- Intermediate understanding of Microsoft 365

Configure Windows Update settings for Azure Automation Update Management

Azure Automation Update Management relies on the Windows Update client to download and install Windows updates. There are specific settings that are used by the Windows Update client when connecting to Windows Server Update Services (WSUS) or Windows Update. Many of these settings can be managed with:

- Local Group Policy Editor
- Group Policy
- PowerShell
- Directly editing the Registry

Update Management respects many of the settings specified to control the Windows Update client. If you use settings to enable non-Windows updates, Update Management will also manage those updates. If you want to enable downloading of updates before an update deployment occurs, update deployment can be faster, more efficient, and less likely to exceed the maintenance window.

For additional recommendations on setting up WSUS in your Azure subscription and securely keep your Windows virtual machines up to date, review Plan your deployment for updating Windows virtual machines in Azure using WSUS.

Manage security operations (25-30%)

Azure Monitor

Azure security benchmark introduction

New services and features are released daily in Azure, developers are rapidly publishing new cloud applications built on these services, and attackers are always seeking new ways to exploit misconfigured resources. The cloud moves fast, developers move fast, and attackers are always on the move. How do you keep up and make sure that your cloud deployments are secure? How are security practices for cloud systems different from on-premises systems? How do you monitor for consistency across many independent development teams?

Microsoft has found that using *security benchmarks* can help you quickly secure cloud deployments. Benchmark recommendations from your cloud service provider give you a starting point for selecting specific security configuration settings in your environment and allow you to quickly reduce risk to your organization.

The Azure Security Benchmark includes a collection of high-impact security recommendations you can use to help secure the services you use in Azure:

- Security controls: These recommendations are generally applicable across your Azure tenant and Azure services. Each recommendation identifies a list of stakeholders that are typically involved in planning, approval, or implementation of the benchmark.
- Service baselines: These apply the controls to individual Azure services to provide recommendations on that service's security configuration.

Create and customize alerts

Improve incident response with alerting on Azure
44 minute modular reference guide

In this module, you'll learn how to respond to incidents and activities in your infrastructure through alerting capabilities in Azure Monitor.

After completing this module, you'll be able to:

- Configure alerts on events in your Azure resources based on metrics, log events, and Activity log events
- Learn how to use smart groups to identify and group related alerts to reduce alert noise
- Understand the different alert types that Azure Monitor supports

Prerequisites

- Basic knowledge of Azure Monitor

Create, view, and manage activity log alerts by using Azure Monitor

Activity log alerts are the alerts that get activated when a new activity log event occurs that matches the conditions specified in the alert.

These alerts are for Azure resources and can be created by using an Azure Resource Manager template. They also can be created, updated, or deleted in the Azure portal. Typically, you create activity log alerts to receive notifications when specific changes occur to resources in your Azure subscription. Alerts are often scoped to particular resource groups or resources.

When you create alert rules, ensure the following:

- The subscription in the scope isn't different from the subscription where the alert is created.
- The criteria must be the level, status, caller, resource group, resource ID, or resource type event category on which the alert is configured.
- There's no "anyOf" condition or nested conditions in the alert configuration JSON. Basically, only one "allOf" condition is allowed with no further "allOf" or "anyOf" conditions.
- When the category is "administrative," you must specify at least one of the preceding criteria in your alert. You may not create an alert that activates every time an event is created in the activity logs.
- Alerts cannot be created for events in Alert category of activity log.

Additional articles:

- Learn about webhook schema for activity logs.
- Read an overview of activity logs.
- Learn more about action groups.
- Learn about service health notifications.

Monitor security logs by using Azure Monitor

Azure Monitor Logs overview

Azure Monitor Logs is a feature of Azure Monitor that collects and organizes log and performance data from monitored resources. Data from different sources such as platform logs from Azure services, log and performance data from virtual machines agents, and usage and performance data from applications can be consolidated into a single workspace so they can be analyzed together using a sophisticated query language that's capable of quickly analyzing millions of records. You may perform a simple query that just retrieves a specific set of records or perform sophisticated data analysis to identify critical patterns in your monitoring data. Work with log queries and their results interactively using Log Analytics, use them in an alert rules to br proactively notified of issues, or visualize their results in a workbook or dashboard.

Azure Monitor Logs is one half of the data platform supporting Azure Monitor. The other is Azure Monitor Metrics which stores numeric data in a time-series database. This makes this data more lightweight than data in Azure Monitor Logs and capable of supporting near real-time scenarios making them particularly useful for alerting and fast detection of issues. Metrics though can only store numeric data in a particular structure, while Logs can store a variety of different data types each with their own structure. You can also perform complex analysis on Logs data using log queries which cannot be used for analysis of Metrics data.

Azure Monitor Metrics overview

Azure Monitor Metrics is a feature of Azure Monitor that collects numeric data from monitored resources into a time series database. Metrics are numerical values that are collected at regular intervals and describe some aspect of a system at a particular time. Metrics in Azure Monitor are lightweight and capable of supporting near real-time scenarios making them particularly useful for alerting and fast detection of issues. You can analyze them interactively with metrics explorer, be proactively notified with an alert when a value crosses a threshold, or visualize them in a workbook or dashboard.

Design a holistic monitoring strategy on Azure
57 minute modular reference guide

In this module, you'll learn how to use monitoring services on Azure to bring operational excellence to your applications and infrastructure.

After completing this module, you'll be able to:

- Select the appropriate monitoring solution based on use case
- Integrate monitoring solutions to create a unified monitoring strategy
- Analyze infrastructure security by using Microsoft Defender for Cloud
- Analyze enterprise security by using Azure Sentinel

Prerequisites

- Basic knowledge of Azure services
- Basic knowledge of operational concepts, such as monitoring, logging, and alerting

Overview of the Azure Security Benchmark (v1)

The Azure Security Benchmark contains recommendations that help you improve the security of your applications and data on Azure.

This benchmark focuses on cloud-centric control areas. These controls are consistent with well-known security benchmarks, such as those described by the Center for Internet Security (CIS) Controls Version 7.1.

The following controls are used in the Azure Security Benchmark:

- Network security
- Logging and monitoring
- Identity and access control
- Data protection
- Vulnerability management
- Inventory and asset management
- Secure configuration
- Malware defense
- Data recovery
- Incident response
- Penetration tests and red team exercises

You can also download the Azure Security Benchmark v1 excel spreadsheet.

Configure diagnostic logging and log retention

Analyze your Azure infrastructure by using Azure Monitor logs
36 minute modular reference guide

In this module, you'll learn how to use Azure Monitor logs to extract valuable information about your infrastructure from log data.

After completing this module, you'll be able to:
- Identify the features and capabilities of Azure Monitor logs
- Create basic Azure Monitor log queries to extract information from log data

Prerequisites
- None

Create, view, and manage log alerts using Azure Monitor

Log alerts allow users to use a Log Analytics query to evaluate resources logs every set frequency, and fire an alert based on the results. Rules can trigger one or more actions using Action Groups. Learn more about functionality and terminology of log alerts.

This article shows you how to create and manage log alerts using Azure Monitor. Alert rules are defined by three components:

- Target: A specific Azure resource to monitor.
- Criteria: Logic to evaluate. If met, the alert fires.
- Action: Notifications or automation - email, SMS, webhook, and so on.

You can also create log alert rules using Azure Resource Manager templates, which are described in a separate article.

Additional articles:
- Learn about log alerts.
- Create log alerts using Azure Resource Manager Templates.
- Understand webhook actions for log alerts.
- Learn more about log queries.

Create, view, and manage metric alerts using Azure Monitor

Metric alerts in Azure Monitor provide a way to get notified when one of your metrics crosses a threshold. Metric alerts work on a range of multi-dimensional platform metrics, custom metrics, Application Insights standard and custom metrics. In this article, we will describe how to create, view, and manage metric alert rules through Azure portal and Azure CLI. You can also create metric alert rules using Azure Resource Manager templates, which are described in a separate article.

You can learn more about how metric alerts work from metric alerts overview.

Additional articles:
- Create metric alerts using Azure Resource Manager Templates

- Understand how metric alerts work
- Understand how metric alerts with Dynamic Thresholds condition work
- Understand the web hook schema for metric alerts
- Troubleshooting problems in metric alerts

Microsoft Defender for Cloud

Evaluate vulnerability scans from Microsoft Defender for Cloud

Secure score in Microsoft Defender for Cloud

Microsoft Defender for Cloud has two main goals:
- to help you understand your current security situation
- to help you efficiently and effectively improve your security

The central feature in Security Center that enables you to achieve those goals is secure score.
Security Center continually assesses your resources, subscriptions, and organization for security issues. It then aggregates all the findings into a single score so that you can tell, at a glance, your current security situation: the higher the score, the lower the identified risk level.

For more information, see How your secure score is calculated

You can find your overall secure score, as well as your score per subscription, through the Azure portal or programatically as described in the following sections:
- Get your secure score from the portal
- Get your secure score from the REST API
- Get your secure score from Azure Resource Graph (ARG)

Resolve security threats with Microsoft Defender for Cloud
44 minute modular reference guide

In this module, you'll use the alert capabilities of Microsoft Defender for Cloud to watch for and respond to threats.

After completing this module, you'll be able to:
- View security alerts in Microsoft Defender for Cloud
- Define an incident response plan
- Use a Workflow automation to automate a security response

Prerequisites
- Basic familiarity with Microsoft Defender for Cloud

Configure Just in Time VM access by using Microsoft Defender for Cloud

Protect your servers and VMs from brute-force and malware attacks with Microsoft Defender for Cloud

44 minute modular reference guide

In this module, you'll discover how to protect VMs and servers with Microsoft Defender for Cloud

After completing this module, you'll be able to:

- Learn how to protect VM-based resources and networks with Microsoft Defender for Cloud
- Install and use malware protection to stop virus attacks on your exposed endpoints
- Enable JIT VM Access

Prerequisites

- Basic familiarity with Azure services, particularly Microsoft Defender for Cloud.
- Familiarity with Azure virtual machines and virtual networking.

Understanding just-in-time (JIT) VM access

This page explains the principles behind Microsoft Defender for Cloud's just-in-time (JIT) VM access feature and the logic behind the recommendation.

To learn how to apply JIT to your VMs using the Azure portal (either Security Center or Azure Virtual Machines) or programatically, see How to secure your management ports with JIT.

JIT requires Azure Defender for servers to be enabled on the subscription.

Secure your management ports with just-in-time access

Lock down inbound traffic to your Azure Virtual Machines with Microsoft Defender for Cloud's just-in-time (JIT) virtual machine (VM) access feature. This reduces exposure to attacks while providing easy access when you need to connect to a VM.

For a full explanation about how JIT works and the underlying logic, see Just-in-time explained.

This page teaches you how to include JIT in your security program. You'll learn how to:

- Enable JIT on your VMs - You can enable JIT with your own custom options for one or more VMs using Security Center, PowerShell, or the REST API. Alternatively, you can enable JIT with default, hard-coded parameters, from Azure virtual machines. When enabled, JIT locks down inbound traffic to your Azure VMs by creating a rule in your network security group.
- Request access to a VM that has JIT enabled - The goal of JIT is to ensure that even though your inbound traffic is locked down, Security Center still provides easy access to connect to VMs when needed. You can request access to a JIT-enabled VM from Security Center, Azure virtual machines, PowerShell, or the REST API.
- Audit the activity - To ensure your VMs are secured appropriately, review the accesses to your JIT-enabled VMs as part of your regular security checks.

Configure centralized policy management by using Microsoft Defender for Cloud

Working with security policies

A security policy defines the desired configuration of your workloads and helps ensure you're complying with the security requirements of your company or regulators.

Microsoft Defender for Cloud makes its security recommendations based on your chosen policies. Security Center policies are based on policy initiatives created in Azure Policy. You can use Azure Policy to manage your policies and to set policies across Management groups and across multiple subscriptions.

Security Center offers the following options for working with security policies:

- View and edit the built-in default policy - When you enable Security Center, a built-in initiative named 'ASC default' is automatically assigned to all Security Center registered subscriptions. To customize this initiative, you can enable or disable individual policies within it. See the list of built-in security policies to understand the options available out-of-the-box.
- Add your own custom policies - If you want to customize the security initiatives applied to your subscription, you can do so within Security Center. You'll then receive recommendations if your machines don't follow the policies you create. For instructions on building and assigning custom policies, see Using custom security policies.
- Add regulatory compliance policies - Security Center's regulatory compliance dashboard shows the status of all the assessments within your environment in the context of a particular standard or regulation (such as Azure CIS, NIST SP 800-53 R4, SWIFT CSP CSCF-v2020). For more information, see Improve your regulatory compliance.

Related information:

- Learn how to set policies using PowerShell
- Learn how to edit a security policy in Azure Policy
- Learn how to set a policy across subscriptions or on Management groups using Azure Policy.
- Learn how to enable Security Center on all subscriptions in a management group

Configure compliance policies and evaluate for compliance by using Microsoft Defender for Cloud

Security recommendations in Microsoft Defender for Cloud

This topic explains how to view and understand the recommendations in Microsoft Defender for Cloud to help you protect your Azure resources.

What are security recommendations? - Recommendations are actions for you to take in order to secure your resources.

Security Center periodically analyzes the security state of your Azure resources to identify potential security vulnerabilities. It then provides you with recommendations on how to remediate those vulnerabilities.

Each recommendation provides you with:

- A short description of the issue
- The remediation steps to carry out in order to implement the recommendation

- The affected resources

Related information:
- Remediate recommendations
- Prevent misconfigurations with Enforce/Deny recommendations.
- Automate responses to Security Center triggers
- Exempt a resource from a recommendation
- Security recommendations - a reference guide

Remediate recommendations in Microsoft Defender for Cloud

Recommendations give you suggestions on how to better secure your resources. You implement a recommendation by following the remediation steps provided in the recommendation.

After reviewing all the recommendations, decide which one to remediate first. We recommend that you use the Secure Score impact to help prioritize what to do first.

To learn more about Security Center, see the following topics:
- Setting security policies in Microsoft Defender for Cloud - Learn how to configure security policies for your Azure subscriptions and resource groups.
- Security health monitoring in Microsoft Defender for Cloud - Learn how to monitor the health of your Azure resources.

Azure Sentinel

Create and customize alerts

Audit the security of Windows Server IaaS Virtual Machines
45 minute modular reference guide

You'll learn about Microsoft Defender for Cloud and how to onboard Windows Server computers to Security Center. You'll also learn about Azure Sentinel, security information and event management (SIEM), and security orchestration, automation and response (SOAR).

After completing this module, you'll be able to:
- Describe Microsoft Defender for Cloud.
- Enable Microsoft Defender for Cloud in hybrid environments.
- Onboard Windows Server computers to Microsoft Defender for Cloud.
- Implement and assess security policies.
- Describe Azure Sentinel.
- Implement SIEM and SOAR.
- Protect your resources with Microsoft Defender for Cloud.

Prerequisites
In order to get the best learning experience from this module, it's important that you have knowledge and experience of the following:

- Managing Windows Server operating system and Windows Server workloads in on-premises scenarios, including Active Directory Domain Services (AD DS), Domain Name System (DNS), the Distributed File System (DFS), Microsoft Hyper-V, and file and storage services
- Common Windows Server management tools
- Core Microsoft compute, storage, networking, and virtualization technologies
- On-premises resiliency Windows Server–based compute and storage technologies
- Implementing and managing infrastructure as a service (IaaS) services in Azure
- Azure Active Directory (Azure AD)
- Security-related technologies (firewalls, encryption, multi-factor authentication)
- Windows PowerShell scripting
- Automation and monitoring

Tutorial: Create custom analytics rules to detect threats

Once you have connected your data sources to Azure Sentinel, you can create custom rules that can search for specific criteria across your environment and generate incidents when the criteria are matched so that you can investigate them. This tutorial helps you create custom rules to detect threats with Azure Sentinel.

This tutorial helps you detect threats with Azure Sentinel.
- Create analytics rules
- Automate threat responses

Tutorial: Detect threats out-of-the-box

Once you have connected your data sources to Azure Sentinel, you'll want to be notified when something suspicious occurs. That's why Azure Sentinel provides out-of-the-box, built-in templates to help you create threat detection rules. These templates were designed by Microsoft's team of security experts and analysts based on known threats, common attack vectors, and suspicious activity escalation chains. Rules created from these templates will automatically search across your environment for any activity that looks suspicious. Many of the templates can be customized to search for activities, or filter them out, according to your needs. The alerts generated by these rules will create incidents that you can assign and investigate in your environment.

This tutorial helps you detect threats with Azure Sentinel:
- Use out-of-the-box threat detections
- Automate threat responses

Configure data sources to Azure Sentinel

Quickstart: On-board Azure Sentinel

In this quickstart, learn how to on-board Azure Sentinel.

To on-board Azure Sentinel, you first need to enable Azure Sentinel, and then connect your data sources. Azure Sentinel comes with a number of connectors for Microsoft solutions, available out of the box and providing real-time integration, including Microsoft

365 Defender (formerly Microsoft Threat Protection) solutions, Microsoft 365 sources (including Office 365), Azure AD, Microsoft Defender for Identity (formerly Azure ATP), Microsoft Cloud App Security, Azure Defender alerts from Microsoft Defender for Cloud, and more. In addition, there are built-in connectors to the broader security ecosystem for non-Microsoft solutions. You can also use Common Event Format (CEF), Syslog or REST-API to connect your data sources with Azure Sentinel.

After you connect your data sources, choose from a gallery of expertly created workbooks that surface insights based on your data. These workbooks can be easily customized to your needs.

Connect data sources

Once you have enabled Azure Sentinel, the first thing you need to do is connect your data sources. Azure Sentinel comes with a number of connectors for Microsoft solutions, available out of the box and providing real-time integration, including Microsoft 365 Defender (formerly Microsoft Threat Protection) solutions, Microsoft 365 sources (including Office 365), Azure AD, Microsoft Defender for Identity (formerly Azure ATP), Microsoft Cloud App Security, and more. In addition, there are built-in connectors to the broader security ecosystem for non-Microsoft solutions. You can also use Common Event Format (CEF), Syslog or REST-API to connect your data sources with Azure Sentinel.

Evaluate results from Azure Sentinel

Quickstart: Get started with Azure Sentinel

In this quickstart, you will learn how to quickly be able to view and monitor what's happening across your environment using Azure Sentinel. After you connected your data sources to Azure Sentinel, you get instant visualization and analysis of data so that you can know what's happening across all your connected data sources. Azure Sentinel gives you workbooks that provide you with the full power of tools already available in Azure as well as tables and charts that are built in to provide you with analytics for your logs and queries. You can either use built-in workbooks or create a new workbook easily, from scratch or based on an existing workbook.

Tutorial: Create custom analytics rules to detect threats

Once you have connected your data sources to Azure Sentinel, you can create custom rules that can search for specific criteria across your environment and generate incidents when the criteria are matched so that you can investigate them. This tutorial helps you create custom rules to detect threats with Azure Sentinel.

This tutorial helps you detect threats with Azure Sentinel.

- Create analytics rules
- Automate threat responses

Configure workflow automation by using Azure Sentinel

Tutorial: Set up automated threat responses in Azure Sentinel

This tutorial helps you to use security playbooks in Azure Sentinel to set automated threat responses to security-related issues detected by Azure Sentinel.

- Understand playbooks
- Create a playbook
- Run a playbook
- Automate threat responses

Hunt for threats with Azure Sentinel

If you're an investigator who wants to be proactive about looking for security threats, Azure Sentinel powerful hunting search and query tools to hunt for security threats across your organization's data sources. But your systems and security appliances generate mountains of data that can be difficult to parse and filter into meaningful events. To help security analysts look proactively for new anomalies that weren't detected by your security apps, Azure Sentinel' built-in hunting queries guide you into asking the right questions to find issues in the data you already have on your network.

For example, one built-in query provides data about the most uncommon processes running on your infrastructure - you wouldn't want an alert about each time they are run, they could be entirely innocent, but you might want to take a look at the query on occasion to see if there's anything unusual.

Use hunting livestream in Azure Sentinel to detect threats

Use hunting livestream to create interactive sessions that let you test newly created queries as events occur, get notifications from the sessions when a match is found, and launch investigations if necessary. You can quickly create a livestream session using any Log Analytics query.

- **Test newly created queries as events occur**
  You can test and adjust queries without any conflicts to current rules that are being actively applied to events. After you confirm these new queries work as expected, it's easy to promote them to custom alert rules by selecting an option that elevates the session to an alert.

- **Get notified when threats occur**
  You can compare threat data feeds to aggregated log data and be notified when a match occurs. Threat data feeds are ongoing streams of data that are related to potential or current threats, so the notification might indicate a potential threat to your organization. Create a livestream session instead of a custom alert rule when you want to be notified of a potential issue without the overheads of maintaining a custom alert rule.

- **Launch investigations**
  If there is an active investigation that involves an asset such as a host or user, you can

view specific (or any) activity in the log data as it occurs on that asset. You can be notified when that activity occurs.

Connect data from threat intelligence providers

Azure Sentinel lets you import the threat indicators your organization is using, which can enhance your security analysts' ability to detect and prioritize known threats. Several features from Azure Sentinel then become available or are enhanced:

- Analytics includes a set of scheduled rule templates you can enable to generate alerts and incidents based on matches of log events from your threat indicators.
- Workbooks provide summarized information about the threat indicators imported into Azure Sentinel and any alerts generated from analytics rules that match your threat indicators.
- Hunting queries allow security investigators to use threat indicators within the context of common hunting scenarios.
- Notebooks can use threat indicators when you investigate anomalies and hunt for malicious behaviors.

Configure Security Policies

Configure security settings by using Azure Policy

Identify security threats with Microsoft Defender for Cloud
43 minute modular reference guide

In this module, you'll discover how to detect and respond to threats with Microsoft Defender for Cloud.

After completing this module, you'll be able to:
- Configure Microsoft Defender for Cloud to monitor your Azure resources
- Use the Microsoft Defender for Cloud dashboard to identify potential security issues
- Analyze the recommendations made by Security Center

Prerequisites
- Basic familiarity with Azure services

Using custom security policies

To help secure your systems and environment, Microsoft Defender for Cloud generates security recommendations. These recommendations are based on industry best practices, which are incorporated into the generic, default security policy supplied to all customers. They can also come from Security Center's knowledge of industry and regulatory standards.

With this feature, you can add your own *custom* initiatives. You'll then receive recommendations if your environment doesn't follow the policies you create. Any custom initiatives you create will appear alongside the built-in initiatives in the regulatory compliance dashboard, as described in the tutorial Improve your regulatory compliance.

As discussed in the Azure Policy documentation, when you specify a location for your custom initiative, it must be a management group or a subscription.

Azure Policy definition structure

Azure Policy establishes conventions for resources. Policy definitions describe resource compliance conditions and the effect to take if a condition is met. A condition compares a resource property field or a value to a required value. Resource property fields are accessed by using aliases. When a resource property field is an array, a special array alias can be used to select values from all array members and apply a condition to each one. Learn more about conditions.

By defining conventions, you can control costs and more easily manage your resources. For example, you can specify that only certain types of virtual machines are allowed. Or, you can require that resources have a particular tag. Policy assignments are inherited by child resources. If a policy assignment is applied to a resource group, it's applicable to all the resources in that resource group.

The policy definition *policyRule* schema is found here: https://schema.management.azure.com/schemas/2019-09-01/policyDefinition.json

Additional review:

- See the initiative definition structure
- Review examples at Azure Policy samples.
- Review Understanding policy effects.
- Understand how to programmatically create policies.
- Learn how to get compliance data.
- Learn how to remediate non-compliant resources.
- Review what a management group is with Organize your resources with Azure management groups.

Azure Policy built-in definitions for Microsoft Defender for Cloud

This page is an index of Azure Policy built-in policy definitions related to the Microsoft Defender for Cloud. The following groupings of policy definitions are available:

- The initiatives group lists the Azure Policy initiative definitions in the 'Security Center' category.
- The default initiative group lists all the Azure Policy definitions that are part of the Microsoft Defender for Cloud default initiative.
- The category group lists all the Azure Policy definitions in the 'Security Center' category.

For more information about security policies, see Working with security policies. For additional Azure Policy built-ins for other services, see Azure Policy built-in definitions.

The name of each built-in policy definition links to the policy definition in the Azure portal. Use the link in the Version column to view the source on the Azure Policy GitHub repo.

To learn more, see the following articles.

- See the built-ins on the Azure Policy GitHub repo.

- Review Understanding policy effects.
- Microsoft Defender for Cloud planning and operations guide: Learn how to plan and understand design considerations in Microsoft Defender for Cloud.
- Security health monitoring in Microsoft Defender for Cloud: Learn how to monitor the health of your Azure resources.
- Manage and respond to security alerts in Microsoft Defender for Cloud: Learn how to manage and respond to security alerts.
- Monitor partner solutions with Microsoft Defender for Cloud: Learn how to monitor the health status of your partner solutions.
- Azure Policy: Learn to audit and govern your Azure resources.

Configure security settings by using Azure Blueprint

What is Azure Blueprints?

Just as a blueprint allows an engineer or an architect to sketch a project's design parameters, Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements. Azure Blueprints makes it possible for development teams to rapidly build and stand up new environments with trust they're building within organizational compliance with a set of built-in components, such as networking, to speed up development and delivery.

Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:

- Role Assignments
- Policy Assignments
- Azure Resource Manager templates (ARM templates)
- Resource Groups

- Create a blueprint - Portal.
- Create a blueprint - PowerShell.
- Create a blueprint - REST API.

Choose the best Azure landing zone to support your cloud operations requirements
1 Hour 29 minute modular reference guide

Azure landing zones can accelerate configuration of your cloud environment. This module will help you choose and get started with the best landing zone option for your needs.

After completing this module, you'll be able to:

- Compare your operations management, governance, and security requirements to common operating models.
- Evaluate Azure landing zone implementation options against your short-term and long-term requirements.
- Choose the best Azure landing zones and support Learn modules to support your cloud adoption needs.

Prerequisites

- An understanding of your organization’s cloud adoption strategy.

- Familiarity with Azure cloud environment including network configuration, network connectivity, and Azure Active Directory.
- Familiarity with Azure governance tools including Azure Policy, Azure Blueprints, and Azure Resource Manager templates.
- A general understanding of the environmental requirements needed to proceed with your cloud adoption plan.

Configure a playbook by using Azure Sentinel

Tutorial: Set up automated threat responses in Azure Sentinel

This tutorial helps you to use security playbooks in Azure Sentinel to set automated threat responses to security-related issues detected by Azure Sentinel.

- Understand playbooks
- Create a playbook
- Run a playbook
- Automate threat responses

Hunt for threats with Azure Sentinel

The foundation of Azure Sentinel is the data store; it combines high-performance querying, dynamic schema, and scales to massive data volumes. The Azure portal and all Azure Sentinel tools use a common API to access this data store. The same API is also available for external tools such as Jupyter notebooks and Python. While many common tasks can be carried out in the portal, Jupyter extends the scope of what you can do with this data. It combines full programmability with a huge collection of libraries for machine learning, visualization, and data analysis. These attributes make Jupyter a compelling tool for security investigation and hunting.

Keep track of data during hunting with Azure Sentinel

Threat hunting typically requires reviewing mountains of log data looking for evidence of malicious behavior. During this process, investigators find events that they want to remember, revisit, and analyze as part of validating potential hypotheses and understanding the full story of a compromise.

Hunting bookmarks in Azure Sentinel help you do this, by preserving the queries you ran in **Azure Sentinel - Logs**, along with the query results that you deem relevant. You can also record your contextual observations and reference your findings by adding notes and tags. Bookmarked data is visible to you and your teammates for easy collaboration.

You can revisit your bookmarked data at any time on the **Bookmarks** tab of the **Hunting** pane. You can use filtering and search options to quickly find specific data for your current investigation. Alternatively, you can view your bookmarked data directly in the **HuntingBookmark** table in your Log Analytics workspace.

Secure Data and Applications (25-30%)

Storage

Configure access control for storage accounts

Authorizing access to data in Azure Storage

Each time you access data in your storage account, your client makes a request over HTTP/HTTPS to Azure Storage. Every request to a secure resource must be authorized, so that the service ensures that the client has the permissions required to access the data.

Delegate access with a shared access signature

A shared access signature (SAS) is a URI that grants restricted access rights to Azure Storage resources. You can provide a shared access signature to clients who should not be trusted with your storage account key but to whom you wish to delegate access to certain storage account resources. By distributing a shared access signature URI to these clients, you can grant them access to a resource for a specified period of time, with a specified set of permissions.

The URI query parameters comprising the SAS token incorporate all of the information necessary to grant controlled access to a storage resource. A client who is in possession of the SAS can make a request against Azure Storage with just the SAS URI, and the information contained in the SAS token is used to authorize the request.

Configure key management for storage accounts

Authorize with Shared Key

Every request made against a storage service must be authorized, unless the request is for a blob or container resource that has been made available for public or signed access. One option for authorizing a request is by using Shared Key, described in this article.

- Blob Service REST API
- Queue Service REST API
- Table Service REST API
- Storage Services REST

Configure Azure AD authentication for Azure Storage

Authorize access to blobs and queues using Azure Active Directory

Azure Storage supports using Azure Active Directory (Azure AD) to authorize requests to Blob and Queue storage. With Azure AD, you can use Azure role-based access control (Azure RBAC) to grant permissions to a security principal, which may be a user, group, or

application service principal. The security principal is authenticated by Azure AD to return an OAuth 2.0 token. The token can then be used to authorize a request against Blob or Queue storage.

Authorizing requests against Azure Storage with Azure AD provides superior security and ease of use over Shared Key authorization. Microsoft recommends using Azure AD authorization with your blob and queue applications when possible to minimize potential security vulnerabilities inherent in Shared Key.

Authorization with Azure AD is available for all general-purpose and Blob storage accounts in all public regions and national clouds. Only storage accounts created with the Azure Resource Manager deployment model support Azure AD authorization.

Blob storage additionally supports creating shared access signatures (SAS) that are signed with Azure AD credentials. For more information, see Grant limited access to data with shared access signatures.

Azure Files supports authorization with AD (preview) or Azure AD DS (GA) over SMB for domain-joined VMs only. To learn about using AD (preview) or Azure AD DS (GA) over SMB for Azure Files, see Overview of Azure Files identity-based authentication support for SMB access.

Authorization with Azure AD is not supported for Azure Table storage. Use Shared Key to authorize requests to Table storage.

Secure your Azure Storage account
45 minute modular reference guide

Learn how Azure Storage provides multilayered security to protect your data. Find out how to use access keys, to secure networks, and to use Advanced Threat Protection to proactively monitor your system.

After completing this module, you'll be able to:

- Understand storage account keys.
- Understand shared access signatures.
- Understand transport-level encryption with HTTPS.
- Understand Advanced Threat Protection.
- Control network access.

Prerequisites

- None

Configure Azure AD Domain Services authentication for Azure Files

Overview of Azure Files identity-based authentication options for SMB access

Azure Files supports identity-based authentication over Server Message Block (SMB) through on-premises Active Directory Domain Services (AD DS) and Azure Active Directory Domain Services (Azure AD DS). This article focuses on how Azure file shares

can use domain services, either on-premises or in Azure, to support identity-based access to Azure file shares over SMB. Enabling identity-based access for your Azure file shares allows you to replace existing file servers with Azure file shares without replacing your existing directory service, maintaining seamless user access to shares.

Azure Files enforces authorization on user access to both the share and the directory/file levels. Share-level permission assignment can be performed on Azure Active Directory (Azure AD) users or groups managed through the Azure role-based access control (Azure RBAC) model. With RBAC, the credentials you use for file access should be available or synced to Azure AD. You can assign Azure built-in roles like Storage File Data SMB Share Reader to users or groups in Azure AD to grant read access to an Azure file share.

At the directory/file level, Azure Files supports preserving, inheriting, and enforcing Windows DACLs just like any Windows file servers. You can choose to keep Windows DACLs when copying data over SMB between your existing file share and your Azure file shares. Whether you plan to enforce authorization or not, you can use Azure file shares to back up ACLs along with your data.

To learn how to enable on-premises Active Directory Domain Services authentication for Azure file shares, see Enable on-premises Active Directory Domain Services authentication over SMB for Azure file shares.

To learn how to enable Azure AD DS authentication for Azure file shares, see Enable Azure Active Directory Domain Services authentication on Azure Files.

For more information about Azure Files and identity-based authentication over SMB, see these resources:

- Planning for an Azure Files deployment
- Enable on-premises Active Directory Domain Services authentication over SMB for Azure file shares
- Enable Azure Active Directory Domain Services authentication on Azure Files
- FAQ

Create and manage Shared Access Signatures (SAS)

Grant limited access to Azure Storage resources using shared access signatures (SAS)

A shared access signature (SAS) provides secure delegated access to resources in your storage account without compromising the security of your data. With a SAS, you have granular control over how a client can access your data. You can control what resources the client may access, what permissions they have on those resources, and how long the SAS is valid, among other parameters.

To get started with shared access signatures, see the following articles for each SAS type.

User delegation SAS

- Create a user delegation SAS for a container or blob with PowerShell
- Create a user delegation SAS for a container or blob with the Azure CLI
- Create a user delegation SAS for a container or blob with .NET

S**ervice SAS**

- Create a service SAS for a container or blob with .NET

Account SAS
- Create an account SAS with .NET

Next steps
- Delegate access with a shared access signature (REST API)
- Create a user delegation SAS (REST API)
- Create a service SAS (REST API)
- Create an account SAS (REST API)

Create a shared access policy for a blob or blob container

Create a service SAS for a container or blob

A shared access signature (SAS) enables you to grant limited access to containers and blobs in your storage account. When you create a SAS, you specify its constraints, including which Azure Storage resources a client is allowed to access, what permissions they have on those resources, and how long the SAS is valid.

Every SAS is signed with a key. You can sign a SAS in one of two ways:
- With a key created using Azure Active Directory (Azure AD) credentials. A SAS that is signed with Azure AD credentials is a *user delegation* SAS.
- With the storage account key. Both a *service SAS* and an *account SAS* are signed with the storage account key.

A user delegation SAS offers superior security to a SAS that is signed with the storage account key. Microsoft recommends using a user delegation SAS when possible. For more information, see Grant limited access to data with shared access signatures (SAS).

This article shows how to use the storage account key to create a service SAS for a container or blob with the Azure Storage client library for Blob Storage.

For additional information you can review:
- Grant limited access to Azure Storage resources using shared access signatures (SAS)
- Create a service SAS

Define a stored access policy

A stored access policy provides an additional level of control over service-level shared access signatures (SAS) on the server side. Establishing a stored access policy serves to group shared access signatures and to provide additional restrictions for signatures that are bound by the policy. You can use a stored access policy to change the start time, expiry time, or permissions for a signature, or to revoke it after it has been issued.

The following storage resources support stored access policies:
- Blob containers
- File shares
- Queues
- Tables

Configure Storage Service Encryption

Azure Storage encryption for data at rest

Azure Storage automatically encrypts your data when it is persisted to the cloud. Azure Storage encryption protects your data and to help you to meet your organizational security and compliance commitments.

Customer-managed keys for Azure Storage encryption

You can use your own encryption key to protect the data in your storage account. When you specify a customer-managed key, that key is used to protect and control access to the key that encrypts your data. Customer-managed keys offer greater flexibility to manage access controls.

You must use either Azure Key Vault or Azure Key Vault Managed Hardware Security Model (HSM) (preview) to store your customer-managed keys. You can either create your own keys and store them in the key vault or managed HSM, or you can use the Azure Key Vault APIs to generate keys. The storage account and the key vault or managed HSM must be in the same region and in the same Azure Active Directory (Azure AD) tenant, but they can be in different subscriptions.

For more information about Azure Key Vault, see What is Azure Key Vault?.

Check the encryption status of a blob

Every block blob, append blob, or page blob that was written to Azure Storage after October 20, 2017 is encrypted with Azure Storage encryption. Blobs created prior to this date continue to be encrypted by a background process.

This article shows how to determine whether a given blob has been encrypted.

Server-side encryption of Azure Disk Storage

Server-side encryption (SSE) protects your data and helps you meet your organizational security and compliance commitments. SSE automatically encrypts your data stored on Azure managed disks (OS and data disks) at rest by default when persisting it to the cloud.

Data in Azure managed disks is encrypted transparently using 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant. For more information about the cryptographic modules underlying Azure managed disks, see Cryptography API: Next Generation

Server-side encryption does not impact the performance of managed disks and there is no additional cost.

For more information please see:

- Enable end-to-end encryption using encryption at host with either the Azure PowerShell module, the Azure CLI, or the Azure portal.
- Enable double encryption at rest for managed disks with either the Azure PowerShell module, the Azure CLI or the Azure portal.
- Enable customer-managed keys for managed disks with either the Azure PowerShell module, the Azure CLI or the Azure portal.
- Explore the Azure Resource Manager templates for creating encrypted disks with customer-managed keys

Configure encryption with customer-managed keys stored in Azure Key Vault

Azure Storage encrypts all data in a storage account at rest. By default, data is encrypted with Microsoft-managed keys. For additional control over encryption keys, you can manage your own keys. Customer-managed keys must be stored in Azure Key Vault or Key Vault Managed Hardware Security Model (HSM) (preview).

This article shows how to configure encryption with customer-managed keys stored in a key vault by using the Azure portal, PowerShell, or Azure CLI. To learn how to configure encryption with customer-managed keys stored in a managed HSM, see Configure encryption with customer-managed keys stored in Azure Key Vault Managed HSM (preview).

Databases

Enable database authentication

Secure your Azure SQL Database
67 minute modular reference guide

Secure your Azure SQL Database to keep your data secure and diagnose potential security concerns as they happen.

After completing this module, you'll be able to:
- Control network access to your Azure SQL Database using firewall rules
- Control user access to your Azure SQL Database using authentication and authorization
- Protect your data in transit and at rest
- Audit and monitor your Azure SQL Database for access violations

Prerequisites
- None

Configure database authentication and authorization
64 minute modular reference guide

Contrast authentication using Azure Active Directory vs Windows Active Directory vs SQL Server authentication. Implement various security principals and configure permissions.

After completing this module, you'll be able to:

- Learn about authentication options for Azure SQL Database
- Create various security principals
- Configure permissions within a SQL database

Prerequisites

- Basic understanding of Active Directory.
- Understanding of why security is a crucial part of database system planning.
- Ability to write code in the SQL language, particular the Microsoft T-SQL dialect, at a basic level.
- Experience creating and configuring resources using the Azure portal.

Enable database auditing

Secure your data with Azure SQL
1 Hour 24 minute modular reference guide

Ensuring the security and compliance of data is always a top priority. In this module, you'll learn how to use Azure SQL to secure your data, configure logins and users, use tools and techniques for monitoring security, ensure that your data meets industry and regulatory compliance standards, and take advantage of the extra benefits and intelligence that Azure provides. We'll also cover some of the networking considerations for securing SQL.

After completing this module, you'll be able to:

- Make an informed decision about securing your network.
- Manage and deliver access management and authorization.
- Protect, encrypt, and mask data.
- Manage and monitor security for your Azure SQL Database instance and Azure SQL managed instance.

Prerequisites

- Experience working with, maintaining, and developing with SQL Server
- Experience with Azure, such as deploying and managing resources

Configure Azure SQL Database Advanced Threat Protection

Implement compliance controls for sensitive data
20 minute modular reference guide

Explore data classification capabilities and degrees of confidentiality. Explore and configure advanced threat protection options, including SQL injection.

After completing this module, you'll be able to:

- Plan and implement data classification in Azure SQL Database
- Understand and configure Azure threat protection

Prerequisites

- Ability to write code in the SQL language, particular the Microsoft T-SQL dialect, at a basic level.

- Experience creating and configuring resources using the Azure portal.

Advanced Threat Protection for Azure SQL Database, SQL Managed Instance, and Azure Synapse Analytics

Advanced Threat Protection for Azure SQL Database, Azure SQL Managed Instance and Azure Synapse Analytics detects anomalous activities indicating unusual and potentially harmful attempts to access or exploit databases.

Advanced Threat Protection is part of the Azure Defender for SQL offering, which is a unified package for advanced SQL security capabilities. Advanced Threat Protection can be accessed and managed via the central Azure Defender for SQL portal.

Advanced Threat Protection provides a new layer of security, which enables customers to detect and respond to potential threats as they occur by providing security alerts on anomalous activities. Users receive an alert upon suspicious database activities, potential vulnerabilities, and SQL injection attacks, as well as anomalous database access and queries patterns. Advanced Threat Protection integrates alerts with Microsoft Defender for Cloud, which include details of suspicious activity and recommend action on how to investigate and mitigate the threat. Advanced Threat Protection makes it simple to address potential threats to the database without the need to be a security expert or manage advanced security monitoring systems.

For a full investigation experience, it is recommended to enable auditing, which writes database events to an audit log in your Azure storage account. To enable auditing, see Auditing for Azure SQL Database and Azure Synapse or Auditing for Azure SQL Managed Instance.

Configure security policies to manage data
39 minute modular reference guide

Learn how to set up policies to classify, retain, and protect your cloud-based data.

After completing this module, you'll be able to:
- Learn how to classify your data
- Configure your data retention requirements
- Explore data ownership and sovereignty

Prerequisites
- None

Implement database encryption

Introduction to securing data at rest on Azure
30 minute modular reference guide

Identify the data in your organization and store it on Azure. Store secrets securely, and use client-side encryption and Storage Service Encryption to help protect your data.

After completing this module, you'll be able to:

- Identify the types of data that your organization is using and the security requirements for that data
- Identify the encryption capabilities for services on Azure

Prerequisites

- Basic understanding of SSL/TLS encryption
- Basic knowledge of Azure PaaS services

Protect data in-transit and at rest
43 minute modular reference guide

Explore encryption options available within Azure SQL, on-premises SQL Server and Open Source data platforms and Secure Enclaves. Implement database and instance firewalls.

After completing this module, you'll be able to:

- Understand the data encryption options available in the various platforms
- Configure encryption for data at rest and in transit
- Implement object level encryption
- Configure SQL Server to use Azure Key Vault
- Understand the difference between database and instance firewalls in Azure SQL Database
- Explore Secure Enclaves

Prerequisites

- Ability to use tools for running queries against a Microsoft SQL database, either on-premises on cloud-based.
- Understanding of why security is a crucial part of database system planning.
- Experience creating and configuring resources using the Azure portal.

Transparent Data Encryption (TDE)

Transparent Data Encryption (TDE) encrypts SQL Server, Azure SQL Database, and Azure Synapse Analytics (SQL Data Warehouse) data files. This encryption is known as encrypting data at rest.

To help secure a database, you can take precautions like:

- Designing a secure system.
- Encrypting confidential assets.
- Building a firewall around the database servers.

But a malicious party who steals physical media like drives or backup tapes can restore or attach the database and browse its data.

One solution is to encrypt sensitive data in a database and use a certificate to protect the keys that encrypt the data. This solution prevents anyone without the keys from using the data. But you must plan this kind of protection in advance.

Related tasks

- Move a TDE Protected Database to Another SQL Server
- Enable TDE on SQL Server Using EKM
- Extensible Key Management Using Azure Key Vault (SQL Server)

Related content

- Transparent Data Encryption with Azure SQL Database
- Get started with Transparent Data Encryption (TDE) in Azure Synapse Analytics
- SQL Server Encryption
- SQL Server and Database Encryption Keys (Database Engine)

See also

- Security Center for SQL Server Database Engine and Azure SQL Database
- FILESTREAM (SQL Server)

Implement Azure SQL Database Always Encrypted

Transparent data encryption or always encrypted?

Transparent Data Encryption (TDE) and Always Encrypted are two different encryption technologies offered by SQL Server and Azure SQL Database. Generally, encryption protects data from unauthorized access in different scenarios. They are complementary features, and this blog post will show a side-by-side comparison to help decide which technology to choose and how to combine them to provide a layered security approach.

Always Encrypted

Always Encrypted is a feature designed to protect sensitive data, such as credit card numbers or national identification numbers (for example, U.S. social security numbers), stored in Azure SQL Database or SQL Server databases. Always Encrypted allows clients to encrypt sensitive data inside client applications and never reveal the encryption keys to the Database Engine (SQL Database or SQL Server). As a result, Always Encrypted provides a separation between those who own the data and can view it, and those who manage the data but should have no access. By ensuring on-premises database administrators, cloud database operators, or other high-privileged unauthorized users, can't access the encrypted data, Always Encrypted enables customers to confidently store sensitive data outside of their direct control. This allows organizations to store their data in Azure, and enable delegation of on-premises database administration to third parties, or to reduce security clearance requirements for their own DBA staff.

See Also

- Configure Always Encrypted using SSMS
- Configure Always Encrypted using PowerShell
- Develop applications using Always Encrypted
- Configure column encryption using Always Encrypted Wizard
- Always Encrypted cryptography
- CREATE COLUMN MASTER KEY (Transact-SQL)
- CREATE COLUMN ENCRYPTION KEY (Transact-SQL)
- CREATE TABLE (Transact-SQL)
- column_definition (Transact-SQL)
- sys.column_encryption_keys (Transact-SQL)
- sys.column_encryption_key_values (Transact-SQL)

- sys.column_master_keys (Transact-SQL)
- sys.columns (Transact-SQL)
- sp_refresh_parameter_encryption (Transact-SQL)

Key Vault

Manage access to Key Vault

Protect against security threats on Azure
23 minute modular reference guide

Learn how Azure can help you protect the workloads that you run both in the cloud and in your on-premises datacenter.

After completing this module, you'll be able to:
- Strengthen your security posture and protect against threats by using Microsoft Defender for Cloud.
- Collect and act on security data from many different sources by using Azure Sentinel.
- Store and access sensitive information such as passwords and encryption keys securely in Azure Key Vault.
- Manage dedicated physical servers to host your Azure VMs for Windows and Linux by using Azure Dedicated Host.

Prerequisites
- You should be familiar with basic computing concepts and terminology.
- An understanding of cloud computing is helpful, but isn't necessary.

Key Vault Authentication Fundamentals

Azure Key Vault allows you to securely store and manage application credentials such as secrets, keys, and certificates in a central and secure cloud repository. Key Vault eliminates the need to store credentials in your applications. Your applications can authenticate to Key Vault at run time to retrieve credentials.

As an administrator, you can tightly control which users and applications can access your key vault and you can limit and audit the operations they perform. This document explains the fundamental concepts of the key vault access model. It will and provide you with an introductory level of knowledge and show you how you can authenticate a user or application to key vault from start to finish.

Required Knowledge
This document assumes you are familiar with the following concepts. If you are not familiar with any of these concepts, follow the help links before proceeding.
- Azure Active Directory link
- Security Principals link

Virtual network service endpoints for Azure Key Vault

The virtual network service endpoints for Azure Key Vault allow you to restrict access to a specified virtual network. The endpoints also allow you to restrict access to a list of IPv4 (internet protocol version 4) address ranges. Any user connecting to your key vault from outside those sources is denied access.

Configure Azure Key Vault firewalls and virtual networks

This article will provide you with guidance on how to configure the Azure Key Vault firewall. This document will cover the different configurations for the Key Vault firewall in detail, and provide step-by-step instructions on how to configure Azure Key Vault to work with other applications and Azure services.

Secure access to a key vault

Azure Key Vault is a cloud service that safeguards encryption keys and secrets like certificates, connection strings, and passwords. Because this data is sensitive and business critical, you need to secure access to your key vaults by allowing only authorized applications and users. This article provides an overview of the Key Vault access model. It explains authentication and authorization, and describes how to secure access to your key vaults.

For more information on Key Vault, see About Azure Key Vault; for more information on what can be stored in a key vault, see About keys, secrets, and certificates.

Additional Reference Resources

- About Azure Key Vault
- Azure Active Directory
- Privileged Identity Management
- Azure RBAC
- Private Link

Next steps

- Authenticate to Azure Key Vault
- Assign a Key Vault access policy
- Assign Azure role to access to keys, secrets, and certificates
- Configure Key Vault firewalls and virtual networks
- Establish a private link connection to Key Vault

Manage permissions to secrets, certificates, and keys

How to create an Azure key vault and vault access policy by using a Resource Manager template

Azure Key Vault is a cloud service that provides a secure store for secrets like keys, passwords, and certificates. This article describes the process for deploying an Azure Resource Manager template (ARM template) to create a key vault.

An ARM template is a JavaScript Object Notation (JSON) file that defines the infrastructure and configuration for your project. The template uses declarative syntax. In

declarative syntax, you describe your intended deployment without writing the sequence of programming commands to create the deployment.

Assign a Key Vault access policy using the Azure portal

A Key Vault access policy determines whether a given service principal, namely an application or user group, can perform different operations on Key Vault secrets, keys, and certificates. You can assign access policies using the Azure portal (this article), the Azure CLI, or Azure PowerShell.

Key vault supports up to 1024 access policy entries, with each entry granting a distinct set of permissions to a particular security principal. Because of this limitation, we recommend assigning access policies to groups of users, where possible, rather than individual users. Using groups makes it much easier to manage permissions for multiple people in your organization. For more information, see Manage app and resource access using Azure Active Directory groups

For full details on Key Vault access control, see Azure Key Vault security: Identity and access management.

For more information on creating groups in Azure Active Directory through the Azure portal, see Create a basic group and add members

About Azure Key Vault secrets

Key Vault provides secure storage of secrets, such as passwords and database connection strings.

From a developer's perspective, Key Vault APIs accept and return secret values as strings. Internally, Key Vault stores and manages secrets as sequences of octets (8-bit bytes), with a maximum size of 25k bytes each. The Key Vault service doesn't provide semantics for secrets. It merely accepts the data, encrypts it, stores it, and returns a secret identifier ("id"). The identifier can be used to retrieve the secret at a later time.

For highly sensitive data, clients should consider additional layers of protection for data. Encrypting data using a separate protection key prior to storage in Key Vault is one example.

Key Vault also supports a contentType field for secrets. Clients may specify the content type of a secret to assist in interpreting the secret data when it's retrieved. The maximum length of this field is 255 characters. There are no pre-defined values. The suggested usage is as a hint for interpreting the secret data. For instance, an implementation may store both passwords and certificates as secrets, then use this field to differentiate. There are no predefined values.

Configure RBAC usage in Azure Key Vault

Azure Key Vault security

You use Azure Key Vault to protect encryption keys and secrets like certificates, connection strings, and passwords in the cloud. When storing sensitive and business critical data, you need to take steps to maximize the security of your vaults and the data stored in them.

Identity and access management

When you create a key vault in an Azure subscription, it's automatically associated with the Azure AD tenant of the subscription. Anyone trying to manage or retrieve content from a vault must be authenticated by Azure AD.

- Authentication establishes the identity of the caller.
- Authorization determines which operations the caller can perform. Authorization in Key Vault uses a combination of Azure role-based access control (Azure RBAC) and Azure Key Vault access policies.

Access model overview

Access to vaults takes place through two interfaces or planes. These planes are the management plane and the data plane.

- The *management plane* is where you manage Key Vault itself and it is the interface used to create and delete vaults. You can also read key vault properties and manage access policies.
- The *data plane* allows you to work with the data stored in a key vault. You can add, delete, and modify keys, secrets, and certificates.

To access a key vault in either plane, all callers (users or applications) must be authenticated and authorized. Both planes use Azure Active Directory (Azure AD) for authentication. For authorization, the management plane uses Azure role-based access control (Azure RBAC) and the data plane uses a Key Vault access policy.

The model of a single mechanism for authentication to both planes has several benefits:

- Organizations can control access centrally to all key vaults in their organization.
- If a user leaves, they instantly lose access to all key vaults in the organization.
- Organizations can customize authentication by using the options in Azure AD, such as to enable multi-factor authentication for added security.

Manage certificates

Azure Key Vault keys, secrets and certificates overview

Azure Key Vault enables Microsoft Azure applications and users to store and use several types of secret/key data. Key Vault resource provider supports two resource types: vaults and managed HSMs.

About Azure Key Vault certificates

Key Vault certificates support provides for management of your x509 certificates and the following behaviors:

- Allows a certificate owner to create a certificate through a Key Vault creation process or through the import of an existing certificate. Includes both self-signed and Certificate Authority generated certificates.
- Allows a Key Vault certificate owner to implement secure storage and management of X509 certificates without interaction with private key material.
- Allows a certificate owner to create a policy that directs Key Vault to manage the life-cycle of a certificate.
- Allows certificate owners to provide contact information for notification about life-cycle events of expiration and renewal of certificate.
- Supports automatic renewal with selected issuers - Key Vault partner X509 certificate providers / certificate authorities.

Get started with Key Vault certificates

The following scenarios outline several of the primary usages of Key Vault's certificate management service including the additional steps required for creating your first certificate in your key vault.

The following are outlined:

- Creating your first Key Vault certificate
- Creating a certificate with a Certificate Authority that is partnered with Key Vault
- Creating a certificate with a Certificate Authority that is not partnered with Key Vault
- Import a certificate

Manage secrets

Configure and manage secrets in Azure Key Vault
29 minute modular reference guide

Storing and handling secrets, encryption keys, and certificates directly is risky, and every usage introduces the possibility of unintentional data exposure. Azure Key Vault provides a secure storage area for managing all your app secrets so you can properly encrypt your data in transit or while it's being stored.

After completing this module, you'll be able to:

- Explore proper usage of Azure Key Vault
- Manage access to an Azure Key Vault
- Explore certificate management with Azure Key Vault
- Configure a Hardware Security Module Key-generation solution

Manage secrets in your server apps with Azure Key Vault
46 minute modular reference guide

Your application requires service passwords, connection strings, and other secret configuration values to do its job. Storing and handling secret values is risky, and every usage introduces the possibility of leakage. Azure Key Vault, in combination with

managed identities for Azure resources, enables your Azure web app to access secret configuration values easily and securely without needing to store any secrets in your source control or configuration.

After completing this module, you'll be able to:

- Explore what types of information can be stored in Azure Key Vault
- Create an Azure Key Vault and use it to store secret configuration values
- Enable secure access to the vault from an Azure App Service web app with managed identities for Azure resources
- Implement a web application that retrieves secrets from the vault

Configure key rotation

About keys

Azure Key Vault provides two types of resources to store and manage cryptographic keys:

- **Vaults** - Software-protected and HSM-protected (with Premium SKU) keys
- **Managed HSM pools** - HSM-protected keys

- Vaults - Vaults provide a low-cost, easy to deploy, multi-tenant, zone-resilient (where available), highly available key management solution suitable for most common cloud application scenarios.
- Managed HSMs - Managed HSM provides single-tenant, zone-resilient (where available), highly available HSMs to store and manage your cryptographic keys. Most suitable for applications and usage scenarios that handle high value keys. Also helps to meet most stringent security, compliance, and regulatory requirements.

Backup and restore of Key Vault items

Azure Key Vault backup

This document shows you how to back up secrets, keys, and certificates stored in your key vault. A backup is intended to provide you with an offline copy of all your secrets in the unlikely event that you lose access to your key vault.
Azure Key Vault automatically provides features to help you maintain availability and prevent data loss. Back up secrets only if you have a critical business justification. Backing up secrets in your key vault may introduce operational challenges such as maintaining multiple sets of logs, permissions, and backups when secrets expire or rotate.

Key Vault maintains availability in disaster scenarios and will automatically fail over requests to a paired region without any intervention from a user. For more information, see Azure Key Vault availability and redundancy.

If you want protection against accidental or malicious deletion of your secrets, configure soft-delete and purge protection features on your key vault. For more information, see Azure Key Vault soft-delete overview.

Restore Key Vault key and secret for encrypted VMs using Azure Backup

This article talks about using Azure VM Backup to perform restore of encrypted Azure VMs, if your key and secret don't exist in the key vault. These steps can also be used if you want to maintain a separate copy of the key (Key Encryption Key) and secret (BitLocker Encryption Key) for the restored VM.

This article has been updated to use the new Azure PowerShell Az module. You can still use the AzureRM module, which will continue to receive bug fixes until at least December 2020. To learn more about the new Az module and AzureRM compatibility, see Introducing the new Azure PowerShell Az module. For Az module installation instructions, see Install Azure PowerShell.

- Backup encrypted VMs - Encrypted Azure VMs have been backed up using Azure Backup. Refer to the article Manage backup and restore of Azure VMs using PowerShell for details about how to back up encrypted Azure VMs.
- Configure Azure Key Vault – Ensure that key vault to which keys and secrets need to be restored is already present. Refer to the article Get Started with Azure Key Vault for details about key vault management.
- Restore disk - Ensure that you've triggered the restore job for restoring disks for encrypted VM using PowerShell steps. This is because this job generates a JSON file in your storage account containing keys and secrets for the encrypted VM to be restored.

After restoring key and secret back to key vault, refer to the article Manage backup and restore of Azure VMs using PowerShell to create encrypted VMs from restored disk, key, and secret.

BONUS - Material relative to the AZ-104 Microsoft Azure Administrator certification

Microsoft Certified: Azure Administrator Associate certification (Exam AZ-104: Microsoft Azure Administrator)

There are five main domains for the exam:

Manage Azure Identities and Governance (15-20%)
Implement and manage storage (15-20%)
Deploy and manage Azure Compute Resources (15-20%)
Configure and manage virtual networking (30-35%)
Monitor and back up Azure resources (15-20%)

Below is a listing of all the subtopic information as it corresponds back to these five main domains. Where I have been able to, I have provided links to additional study details and resources for additional review

Some of these exam topics overlap with AZ-104, AZ-305, and AZ-500; it is important to understand these within the parameters of each certification track and exam:

AZ-104: Microsoft Azure Administrator – administration and operations
AZ-305: Designing Microsoft Azure Infrastructure Solutions – technologies, architecture, and design
AZ-500: Microsoft Azure Security Technologies – security

Manage Azure Identities and Governance (15-20%)

— Manage Azure AD objects (users, groups, and devices)
— What is Azure Active Directory?
— Create users and groups
— Add or delete users using Azure Active Directory
— New-AzureADUser
— Manage user and group properties
— Add or update a user's profile information using Azure Active Directory

— Edit your group information using Azure Active Directory
— Manage device settings
— Manage device identities using the Azure portal
— How To: Manage stale devices in Azure AD
— Perform bulk user updates
— Manage guest accounts
— What is guest user access in Azure Active Directory B2B?
— Manage guest access with Azure AD access reviews
— Quickstart: Add guest users to your directory in the Azure portal
— Configure Azure AD Join
— How to: Plan your Azure AD join implementation
— How To: Plan your hybrid Azure Active Directory join implementation
— Tutorial: Configure hybrid Azure Active Directory join for federated domains
— Tutorial: Configure hybrid Azure Active Directory join for managed domains
— Configure self-service password reset
— Plan an Azure Active Directory self-service password reset
— How it works: Azure AD self-service password reset
— Licensing requirements for Azure AD self-service password reset
— Manage role-based access control (RBAC)
— What is role-based access control (RBAC) for Azure resources?
— Create a custom role
— Tutorial: Create a custom role for Azure resources using Azure PowerShell
— Tutorial: Create a custom role for Azure resources using Azure CLI
— Add or remove role assignments using Azure RBAC and the Azure portal
— List role assignments using Azure RBAC and the Azure portal
— Understand deny assignments for Azure resources
— Understand how multiple Azure Active Directory tenants interact
— Manage subscriptions and governance
— Overview of Management services in Azure
— Configure Azure policies
— What is Azure Policy?
— Quickstart: Create a policy assignment to identify non-compliant resources
— Tutorial: Create and manage policies to enforce compliance
— Configure resource locks
— Configure resource policies
— Identify auditing requirements
— Lock resources to prevent unexpected changes
— Understand best practices for minimizing Azure costs such as performing cost analysis, creating spending limits and quotas, and using tags to identify cost owners; use Azure reservations; use Azure Advisor recommendations
— Manage resource groups
— Use Azure policies for resource groups
— Implement and set tagging on resource groups
— Move resources across resource groups
— Remove resource groups
— Manage Azure Resource Manager resource groups by using the Azure portal

— Manage Azure resource groups by using Azure PowerShell
— Understand Azure subscriptions
— Create an additional Azure subscription
— Change your Azure subscription to a different offer
— Configure cost center quotas and tagging
— Understand planning and management of costs
— Azure Advisor – Cost recommendations
— What is Azure Cost Management and Billing?
— Quickstart: Explore and analyze costs with cost analysis
— Create management groups for resource organization and management
— Organize your resources with Azure management groups
— Manage your resources with management groups

Implement and manage storage (15-20%)

— Manage storage accounts
— Introduction to Azure Storage
— Locally redundant storage (LRS)
— Zone-redundant storage (ZRS)
— Geo-redundant storage (GRS)
— Read-access geo-redundant storage (RA-GRS)
— Geo-zone-redundant storage (GZRS)
— Zone-redundant storage (ZRS): Highly available Azure Storage applications
— Azure Storage redundancy
— Azure Blobs: A massively scalable object store for text and binary data.
— Azure Files: Managed file shares for cloud or on-premises deployments.
— Azure Queues: A messaging store for reliable messaging between application components.
— Azure Tables: A NoSQL store for schemaless storage of structured data.
— Azure Files – highly available network file shares
— Introduction to Azure Files
— Create Azure file share
— Deploy Azure File Sync
— Configure Azure Storage firewalls and virtual networks
— Storage account overview
— Create an Azure Storage account
— Upgrade to a general-purpose v2 storage account
— Create and configure storage accounts
— Configure network access to the storage account
— Understand Virtual Network Service Endpoints
— Configure Azure Storage firewalls and virtual networks
— Create and configure storage account
— Azure storage account overview
— Generate shared access signature
— Install and use Azure Storage Explorer
— Get started with Storage Explorer

— Manage access keys (PowerShell) and manage via the Portal
— Delegate access with a shared access signature
— Using Shared Access Signatures (SAS)
— Grant limited access to Azure Storage resources using shared access signatures (SAS)
— Manage storage account access keys
— Azure Storage redundancy
— Authorize access to blobs and queues using Azure Active Directory
— Manage data in Azure Storage
— Use the Azure Import/Export service to export data from Azure Blob storage
— Use the Azure Import/Export service to import data to Azure Blob Storage
— Delete an import/export job
— Import data to Azure Blobs
— Export data from Azure Blobs
— Import data to Azure Files
— **Disks:** Use Azure Backup to back up the VM disks used by your Azure virtual machines. Also consider using Azure Site Recovery to protect your VMs in the event of a regional disaster.
— **Block blobs:** Turn on soft delete to protect against object-level deletions and overwrites, or copy block blobs to another storage account in a different region using AzCopy, Azure PowerShell, or the Azure Data Movement library.
— **Files:** Use AzCopy or Azure PowerShell to copy your files to another storage account in a different region.
— **Tables:** use AzCopy to export table data to another storage account
— What is Azure CLI
— Get started with Azure CLI
— Install the Azure CLI
— Quickstart: Create and manage Azure file shares with the Azure portal
— Create an Azure file share
— Planning for an Azure File Sync deployment
— Tutorial: Extend Windows file servers with Azure File Sync
— Quickstart: Upload, download, and list blobs with the Azure portal
— Azure Blob storage: hot, cool, and archive access tiers
— Tutorial: Build a highly available application with Blob storage
— Create an Azure Storage account
— Implement Azure storage replication
— Azure AD Connect Sync: Customizing Synchronization options
— Integrating your on-premises identities with Azure Active Directory
— Create Azure sync group
— Troubleshoot Azure File Sync
— Introduction to Storage Queues
— Azure Table Storage Overview
— Overview of Azure Table storage
— Introduction to Azure managed disks
— Azure Storage Service Encryption for Data at Rest
— Service-Level Agreement (SLA) for Storage

Deploy and manage Azure Compute Resources (15-20%)

— Azure Advisor – Get started with Advisor
— Azure Advisor – High Availability recommendations
— Azure Advisor – Security recommendations
— Azure Advisor – Performance recommendations
— Azure Advisor – Cost recommendations
— Availability options for virtual machines in Azure
— Create and configure a VM for Windows in the portal
— Create and configure a VM for Windows with PowerShell
— Create a Windows virtual machine with the Azure CLI
— Create and Manage Windows VMs with Azure PowerShell
— Manage Azure disks with Azure PowerShell
— Deploy applications to a Windows virtual machine in Azure with the Custom Script Extension
— Create a custom image of an Azure VM with Azure PowerShell
— Configure high availability
— Deploy and configure scale sets
— Quickstart: Create a virtual machine scale set in the Azure portal
— Quickstart: Create a virtual machine scale set with Azure CLI
— Quickstart: Create a virtual machine scale set with Azure PowerShell
— Quickstart: Create a Windows virtual machine scale set with an Azure template
— Quickstart: Create a Linux virtual machine scale set with an Azure template
— Tutorial: Create and manage a virtual machine scale set with the Azure CLI
— Tutorial: Create and manage a virtual machine scale set with Azure PowerShell
— Tutorial: Create and use disks with virtual machine scale set with the Azure CLI
— Tutorial: Create and use disks with virtual machine scale set with Azure PowerShell
— Automate deployment of VMs
— Tutorial: Automatically scale a virtual machine scale set with the Azure CLI
— Tutorial: Automatically scale a virtual machine scale set with Azure PowerShell
— Manage the availability of Windows virtual machines in Azure
— Configure multiple virtual machines in an availability set for redundancy
— Use managed disks for VMs in an availability set
— Use scheduled events to proactively response to VM impacting events
— Configure each application tier into separate availability sets
— Combine a Load Balancer with availability sets
— Use availability zones to protect from datacenter level failures
— Modify Azure Resource Manager (ARM) template
— Save a deployment as an ARM template
— Extend Azure Resource Manager template functionality
— Update a resource in an Azure Resource Manager template
— Understand the structure and syntax of Azure Resource Manager templates
— Azure Resource Manager templates overview
— Tutorial: Create and deploy your first ARM template.
— Understand the structure and syntax of ARM templates.
— Quickstart: Create and deploy ARM templates by using the Azure portal
— Start/Stop VMs during off-hours solution in Azure Automation

— Prepare a Windows VHD or VHDX to upload to Azure
— Deploy an Azure VM from a user VHD
— Prepare and customize a master VHD image
— Upload a Windows VM image to Azure for Resource Manager deployments
— Quickstart: Create and deploy Azure Resource Manager templates by using the Azure portal
— Download the template for a VM
— Use the Azure Custom Script Extension Version 2 with Linux virtual machines
— Custom Script Extension for Windows
— Deploy applications to a Windows virtual machine in Azure with the Custom Script Extension
— Tutorial: Create and use a custom image for virtual machine scale sets with the Azure CLI
— Tutorial: Create and use a custom image for virtual machine scale sets with Azure PowerShell
— Tutorial: Automatically scale a virtual machine scale set with an Azure template
— Azure Disk Encryption for Linux VMs
— Azure Disk Encryption for Windows VMs
— Move a Windows VM to another Azure subscription or resource group
— Windows VM sizes
— Move resources to a new resource group or subscription
— Attach a managed data disk to a Windows VM by using the Azure portal
— Attach a data disk to a Windows VM with PowerShell
— Using Managed Disks in Azure Resource Manager Templates
— Quickstart template for deploying multiple data disks
— Manage Azure disks with Azure PowerShell
— How to open ports to a virtual machine with the Azure portal
— Create and manage a Windows virtual machine that has multiple NICs
— Redeploy Windows virtual machine to new Azure node
— Azure Kubernetes Service (AKS)
— Quickstart: Deploy an Azure Kubernetes Service (AKS) cluster using the Azure portal
— Kubernetes core concepts for AKS
— Intro Azure Kubernetes Service (AKS)
— AKS quickstart in the Azure portal or with the Azure CLI
— Kubernetes role-based access control (RBAC)
— Access and identity options for AKS
— Integrate Azure Active Directory with AKS
— Kubernetes master logs
— Monitor Azure Kubernetes Service container health
— What is Azure Container Instances?
— Quickstart: Deploy a container instance in Azure using the Azure portal
— Quickstart: Deploy a container instance in Azure using the Azure CLI
— App Service overview
— Azure App Service plan overview
— Create an ASP.NET Core web app in Azure
— Azure App Service plan overview
— Manage an App Service plan in Azure
— Azure VM replication between regions

Configure and manage virtual networking (30-35%)

— Virtual network peering overview
— Create and manage Azure virtual networks for Windows virtual machines with Azure PowerShell
— Create connectivity between virtual networks
— Create and configure VNET peering
— Create and configure VNET to VNET
— Verify virtual network connectivity
— Create virtual network gateway
— Implement and manage virtual networking
— Virtual network traffic routing
— Configure a Point-to-Site connection to a VNet using native Azure certificate authentication
— Troubleshoot Azure point-to-site connection problems
— Configure a VNet-to-VNet VPN gateway connection by using the Azure portal
— Configure a VPN gateway for transit in a virtual network peering
— Point-to-site VPN
— Site-to-site VPN
— Azure VPN Gateway
— Configure a VPN gateway for transit in a virtual network peering
— Common PowerShell commands for Azure Virtual Networks
— Virtual network peering permissions
— User-defined routes overview
— Hub-spoke network topology in Azure
— Configure virtual network-to-virtual network connections
— Diagnose a virtual machine routing problem
— Troubleshoot connections with Azure Network Watcher using the Azure portal
— Troubleshoot virtual network peering issues
— What are the constraints related to Global VNet Peering and Load Balancers?
— Create a Hub-spoke network topology in Azure.
— Create, change, or delete a virtual network peering.
— Azure Virtual Network frequently asked questions (FAQ) VNet Peering
— Tutorial: Connect virtual networks with virtual network peering using the Azure portal
— Create a virtual network peering – different deployment models, same subscription
— Virtual network peering constraints and behaviors
— Learn about all virtual network peering settings
— Learn how to create a hub and spoke network topology
— What is Azure Virtual Network?
— Outbound connections in Azure – Outbound connections
— Outbound connections in Azure – Public IP addresses
— Outbound connections in Azure – Load Balancer
— Virtual network service integration
— Virtual network service endpoints overview
— Network security groups
— Application security groups

— Route tables
— Quickstart: Create a virtual network using the Azure portal
— Virtual network traffic routing
— Networking limits
— Create, change, or delete a virtual network
— Create, change, or delete a public IP address
— Add, change, or remove IP addresses for an Azure network interface
— Associate a public IP address to a virtual machine
— Subnet extension
— Virtual network traffic routing
— Add network interfaces to or remove network interfaces from virtual machines
— What is Azure DNS?
— What is Azure Private DNS?
— Quickstart: Create an Azure DNS zone and record using the Azure portal
— Azure DNS FAQ
— Name resolution for resources in Azure virtual networks
— Name resolution using your own DNS server
— Use Azure DNS to provide custom domain settings for an Azure service
— Tutorial: Host your domain in Azure DNS
— Quickstart: Create an Azure private DNS zone using the Azure portal
— Tutorial: Map an existing custom DNS name to Azure App Service
— Create, change, or delete a network security group
— Create, change, or delete a network interface
— Tutorial: Deploy and configure Azure Firewall using the Azure portal
— Create an Azure Bastion host
— Application Gateway configuration overview
— Tutorial: Balance internal traffic load with a Basic load balancer in the Azure portal
— Create an internal load balancer by using the Azure PowerShell module
— Quickstart: Create a Load Balancer to load balance VMs using the Azure portal
— Troubleshoot Azure Load Balancer
— Diagnose on-premises connectivity via VPN gateways
— Network Performance Monitor solution: Performance monitoring
— What is Azure Network Watcher?
— Troubleshoot Virtual Network Gateway and Connections using Azure Network Watcher Azure CLI
— Troubleshoot connections with Azure Network Watcher using the Azure portal
— Create a route-based VPN gateway using the Azure portal
— Create a Site-to-Site connection in the Azure portal
— ExpressRoute overview
— Virtual Network Gateways for ExpressRoute
— Configure Express Route
— Create and modify an ExpressRoute circuit
— Link a virtual network to an ExpressRoute circuit
— Tutorial: Create an ExpressRoute association using Azure Virtual WAN
— About Azure Virtual WAN
— Tutorial: Create a Site-to-Site connection using Azure Virtual WAN

Monitor and back up Azure resources (15-20%)

— Metrics in Azure Monitor
— Analyze log data in Azure Monitor
— Learn more about the Azure Monitor data platform.
— Learn about log data in Azure Monitor.
— Learn about the monitoring data available for different resources in Azure.
— Quickstart: Monitor an Azure resource with Azure Monitor
— Tutorial: Collect and analyze resource logs from an Azure resource
— Monitoring Azure resources with Azure Monitor
— Get started with Log Analytics in Azure Monitor
— Get started with log queries in Azure Monitor
— Overview of log queries in Azure Monitor
— Create, view, and manage metric alerts using Azure Monitor
— Use Azure Monitor to send emails for Health Service Faults
— Create Metric Alerts for Logs in Azure Monitor
— Metric alerts overview
— Platform metrics
— Custom metrics
— Popular logs from Azure Monitor converted to metrics
— Set-AzDiagnosticSetting
— Learn how to create, view, and manage metric alerts in Azure
— Learn how to deploy metric alerts using Azure Resource Manager templates
— Learn more about action groups
— Learn more about Dynamic Thresholds condition type
— Metrics are available for large list of Azure services
— Performance counters for Windows & Linux machines
— Heartbeat records for Agent Health
— Update management records
— Event data logs
— Learn about log alerts in Azure.
— Learn about alerts in Azure.
— Manage Application Insights resources using PowerShell
— Restore a disk and create a recovered VM
— Restore files to a Virtual Machine in Azure
— Back up a Windows Server to Azure
— Recover files from Azure to a Windows Server
— Back up an Azure VM
— Back up Windows Server or Windows workstation
— Back up Windows Server to Azure
— Back up DPM workloads to Azure
— Prepare to back up workloads using Azure Backup Server
— Manage Azure VM backups
— Managing files and folders
— Recover individual files from an Azure VM
— Restore an Azure VM
— Securing cloud backup data in Recovery Services vaults

— Install the Azure Backup MARS agent
— Back up an IaaS VM
— Back up an Azure Backup Server
— Back up a Windows Server
— Backup multiple Azure VMs
— Azure Backup – Frequently asked questions – Recovery Services Vault
— Azure Backup – Frequently asked questions – Azure VM Backup
— Azure Backup – Frequently asked questions – Backup Azure Files
— Azure Backup – FAQ – SQL Server databases that are running on an Azure VM backup
— Recover files from Azure virtual machine backup
— Back up and restore encrypted Azure VM
— Restore Key Vault key and secret for encrypted VMs using Azure Backup
— Create Recovery Services Vault
— Configure and review backup reports
— Perform backup operation
— Create and configure backup policy
— Restore a disk and create a recovered VM in Azure
— Back up and restore Azure VMs with PowerShell
— Back up a virtual machine in Azure with the CLI
— Manage Azure VM backups with Azure Backup service
— Restore files to a virtual machine in Azure
— About Site Recovery
— Azure Site Recovery
— What is Site Recovery?
— Replicate VMware virtual machines and Windows/Linux physical servers to Azure
— Set up disaster recovery to a secondary Azure region for an Azure VM
— Disaster recovery of on-premises VMware virtual machines or physical servers to a secondary site

The linked information provided below is presented in general reference to the domain topics for the former AZ-103 exam with some updates for the AZ-104 exam.

It is offered as additional reference and for the benefit of extended knowledge and review.

-- Sign up for Azure Active Directory Premium editions
-- Add your custom domain name using the Azure Active Directory portal
-- Add branding to your organization's Azure Active Directory sign-in page
-- Associate or add an Azure subscription to your Azure Active Directory tenant
-- What are virtual machine scale sets
-- Overview of autoscale with Azure virtual machine scale sets
-- Overview of autoscale in Microsoft Azure Virtual Machines, Cloud Services, and Web Apps
-- Automatically scale a virtual machine scale set in the Azure portal
-- Advanced autoscale configuration using Resource Manager templates for VM Scale Sets
-- How to configure auto scaling for a Cloud Service in the portal
-- Configure multiple virtual machines in an availability set for redundancy
-- Use managed disks for VMs in an availability set
-- Use scheduled events to proactively response to VM impacting events
-- Configure each application tier into separate availability sets
-- Combine a Load Balancer with availability sets
-- Use availability zones to protect from datacenter level failures
-- Create a virtual machine
-- Create a Windows virtual machine in the Azure portal
-- Create a Windows virtual machine in Azure with PowerShell
-- Create a Windows virtual machine with the Azure CLI
-- Create a custom image of an Azure VM with Azure PowerShell
-- Create and deploy highly available virtual machines with Azure PowerShell
-- Create a virtual machine scale set and deploy a highly available app on Windows with Azure PowerShell
-- Load balance Windows virtual machines in Azure to create a highly available application with Azure PowerShell
-- Create and Manage Windows VMs with Azure PowerShell
-- Manage Azure disks with Azure PowerShell
-- Deploy applications to a Windows virtual machine in Azure with the Custom Script Extension
-- Create and manage Azure virtual networks for Windows virtual machines with Azure PowerShell
-- Back up and restore files for Windows virtual machines in Azure
-- Monitor and update a Windows virtual machine in Azure
-- Use Microsoft Defender for Cloud to monitor Windows virtual machines
-- Maintenance for virtual machines in Azure
-- Add a Managed Disk using PowerShell

-- Create a zone redundant virtual machine scale set
-- Load balance VMs across zones using a Standard Load Balancer with a zone-redundant frontend
-- Load balance VMs within a zone using a Standard Load Balancer with a zonal frontend
-- Zone-redundant storage
-- SQL Database
-- Event Hubs geo-disaster recovery
-- Service Bus geo-disaster recovery
-- Create a zone-redundant virtual network gateway
-- VMware to Azure disaster recovery architecture
-- SLA for Virtual Machines
-- Load balance internet traffic to VMs
-- Load balance internal traffic to VMs
-- Load balance VMs across availability zones
-- Load balance VMs within a specific availability zone
-- Configure port forwarding in Load Balancer
-- Manage web traffic with an application gateway.
-- Restrict web traffic with a web application firewall on an application gateway.
-- Enable SSL termination on an application gateway.
-- Host multiple web sites using an application gateway.
-- Route traffic based on the URL in an application gateway.
-- Redirect traffic to specific servers in an application gateway pool.
-- Create an application using .NET with Azure SQL DB or Node.js with MongoDB
-- Map an existing custom domain to your application
-- Bind an existing SSL certificate to your application
-- Add a CDN to your application
-- Create and manage a scale set with the Azure CLI or Azure Powershell
-- Use data disks with the Azure CLI or Azure Powershell
-- Use a custom VM image with the Azure CLI or Azure Powershell
-- Deploy apps to a scale set with the Azure CLI or Azure Powershell
-- Autoscale a scale set with the Azure CLI or Azure Powershell
-- Azure Application Architecture Guide
-- Create a function that integrates with Azure Logic Apps
-- Create a serverless API using Azure Functions
-- Create an OpenAPI definition for a function
-- Automate resizing uploaded images using Event Grid
-- Create a serverless web app to store pictures with metadata
-- Filter network traffic
-- Route network traffic
-- Restrict network access to resources
-- Connect virtual networks
-- Deploy your site to Azure
-- Scale with Azure Load Balancer
-- Reduce latency with Azure Traffic Manager
-- Azure Service Health Dashboard

-- Designing resilient applications for Azure: An overview of the key concepts for architecting highly available applications in Azure.
-- Availability checklist: A checklist for verifying that your application implements the best design practices for high availability.
-- Designing highly available applications using RA-GRS: Design guidance for building applications to take advantage of RA-GRS.
-- Tutorial: Build a highly available application with Blob storage:A tutorial that shows how to build a highly available application that automatically switches between endpoints as failures and recoveries are simulated.
-- Disks: Use Azure Backup to back up the VM disks used by your Azure virtual machines. Also consider using Azure Site Recovery to protect your VMs in the event of a regional disaster.
-- Block blobs: Turn on soft delete to protect against object-level deletions and overwrites, or copy block blobs to another storage account in a different region using AzCopy, Azure PowerShell, or the Azure Data Movement library.
-- Files: Use AzCopy or Azure PowerShell to copy your files to another storage account in a different region.
-- Tables: use AzCopy to export table data to another storage account in a different region.
-- What is VPN Gateway
-- About VPN Gateway configuration settings
-- VPN Gateway FAQ
-- Virtual Network Gateways for ExpressRoute.
-- About zone-redundant gateways.
-- About Virtual WAN
-- Azure Content Delivery Network - Dynamic site acceleration
-- Azure Content Delivery Network - CDN caching rules
-- Azure Content Delivery Network - HTTPS custom domain support
-- Azure Content Delivery Network - Azure diagnostics logs
-- Azure Content Delivery Network - File compression
-- Azure Content Delivery Network - Geo-filtering
-- Compare Azure CDN product features
-- Azure Event Grid to enable your business to react quickly to critical events in a reliable, scalable, and secure manner.
-- Azure Logic Apps to automate business processes.
-- Azure Machine Learning to add machine learning and AI models to your solution.
-- Azure Stream Analytics to run real-time analytic computations on the data streaming from your devices.
-- Azure Functions Premium plan for enterprise serverless workloads
-- Azure Functions - Create a function that integrates with Azure Logic Apps
-- Azure Functions - Create a serverless API using Azure Functions
-- Azure Functions - Create an OpenAPI definition for a function
-- Azure Functions - Automate resizing uploaded images using Event Grid
-- Azure Functions - Create a serverless web app to store pictures with metadata
-- Optimize the performance and reliability of Azure Functions
-- Check traffic with a schedule-based logic app

-- Manage mailing list requests with a logic app
-- Process emails and attachments with a logic app
-- Monitor changes to VMs with logic apps
-- Resize uploaded images
-- Integrating Azure Automation with Event Grid
-- Azure Advisor - Get started with Advisor
-- Azure Advisor - High Availability recommendations
-- Azure Advisor - Security recommendations
-- Azure Advisor - Performance recommendations
-- Azure Advisor - Cost recommendations
-- Tutorial: Deploy and configure Azure Firewall using the Azure portal
-- Deploy Azure Firewall using a template
-- Create an Azure Firewall test environment
-- Azure boundary security best practices
-- Azure database security best practices
-- Azure data security and encryption best practices
-- Azure network security best practices
-- Azure operational security best practices
-- Azure PaaS Best Practices
-- Azure Service Fabric security best practices
-- Best practices for Azure VM security
-- Implementing a secure hybrid network architecture in Azure
-- Internet of Things security best practices
-- Securing PaaS databases in Azure
-- Securing PaaS web and mobile applications using Azure App Service
-- Securing PaaS web and mobile applications using Azure Storage
-- Security best practices for IaaS workloads in Azure
-- Security groups
-- Azure network security overview
-- Azure identity management security overview
-- Azure Active Directory Premium
-- Security principals
-- Overview of single sign-on
-- What is application access and single sign-on with Azure Active Directory?
-- Integrate Azure Active Directory single sign-on with SaaS apps
-- Single sign-on with Application Proxy
-- Azure Active Directory Seamless Single Sign-On: Quickstart
-- Enabling Azure AD Application Proxy
-- Publish applications using Azure AD Application Proxy
-- Tutorial: Add an on-premises application for remote access through Application Proxy in Azure Active Directory
-- Working with conditional access
-- Multi-Factor Authentication
-- What is Azure Multi-Factor Authentication?
-- Built-in roles for Azure resources
-- View your access and usage reports

-- Get started with Azure Active Directory reporting
-- Azure Active Directory reporting guide
-- What is Azure Active Directory B2C?
-- Azure Active Directory B2C preview: Sign up and sign in consumers in your applications
-- Azure Active Directory B2C Preview: Types of applications
-- Get started with Azure AD device registration
-- Automatic device registration with Azure AD for Windows domain-joined devices
-- Set up automatic registration of Windows domain-joined devices with Azure AD
-- What is Azure AD Privileged Identity Management?
-- Assign Azure AD directory roles in PIM
-- Azure AD Identity Protection
-- Channel 9: Azure AD and Identity Show: Identity Protection Preview
-- Hybrid identity white paper
-- Azure AD team blog
-- Azure AD access reviews
-- Manage user access with Azure AD access reviews
-- Tutorial: Authenticate and authorize users end-to-end in Azure App Service (Windows)
-- Tutorial: Authenticate and authorize users end-to-end in Azure App Service for Linux
-- How to configure your app to use Azure Active Directory login
-- How to configure your app to use Facebook login
-- How to configure your app to use Google login
-- How to configure your app to use Microsoft Account login
-- How to configure your app to use Twitter login
-- What is Azure Active Directory
-- Edit the Azure Information Protection policy and create a new label
-- Configure Azure Information Protection policy settings that work together
-- Azure ATP frequently asked questions
-- Working with security alerts
-- Azure ATP Architecture
-- Azure ATP prerequisites
-- Azure ATP sizing tool
-- Azure ATP capacity planning
-- Configure event forwarding
-- Configuring Windows event forwarding
-- Install Azure ATP
-- Azure ATP Prerequisites
-- What's new in Azure ATP
-- Plan capacity for Azure ATP
-- Azure ATP Reconnaissance alerts
-- What are Azure Reservations
-- Locally redundant storage (LRS): Low-cost data redundancy for Azure Storage
-- Zone-redundant storage (ZRS): Highly available Azure Storage applications
-- Geo-redundant storage (GRS): Cross-regional replication for Azure Storage
-- Azure Storage scalability and performance targets

-- Designing highly available applications using RA-GRS Storage
-- Microsoft Azure Storage redundancy options and read access geo redundant storage
-- SOSP Paper - Azure Storage: A highly available cloud storage service with strong consistency
-- Authenticate access to Azure blobs and queues using Azure Active Directory
-- Overview of Azure Active Directory authorization over SMB for Azure Files (preview)
-- Authorize Storage access with Shared Key
-- Restore a disk and create a recovered VM
-- Restore files to a Virtual Machine in Azure
-- Back up a Windows Server to Azure
-- Recover files from Azure to a Windows Server
-- Back up an Azure VM
-- Back up Windows Server or Windows workstation
-- Back up DPM workloads to Azure
-- Prepare to back up workloads using Azure Backup Server
-- Manage Azure VM backups
-- Managing files and folders
-- Recover individual files from an Azure VM
-- Restore an Azure VM
-- Securing cloud backup data in Recovery Services vaults
-- Back up an IaaS VM
-- Back up an Azure Backup Server
-- Back up a Windows Server
-- Backup multiple Azure VMs
-- Azure Backup - Frequently asked questions – Recovery Services Vault
-- Azure Backup - Frequently asked questions – Azure VM Backup
-- Azure Backup - Frequently asked questions – Backup Azure Files
-- Azure Backup - FAQ – SQL Server databases that are running on an Azure VM backup
-- Recover files from Azure virtual machine backup
-- Back up and restore encrypted Azure VM
-- Restore Key Vault key and secret for encrypted VMs using Azure Backup
-- Configure a DSC pull server
-- Configure an alias record to refer to an Azure Public IP address
-- Configure an alias record to support apex domain names with Traffic Manager
-- Configure an alias record for zone records
-- Azure Network Security Groups (NSG) – Best Practices and Lessons Learned
-- Tutorial: Balance internal traffic load with a Basic load balancer in the Azure portal
-- Azure Standard Load Balancer overview
-- Azure Policy
-- Azure Role Based Access Controls