00:00:00

Learn Azure with

00:01:04

Learn Azure with

The Tech BlackBoard

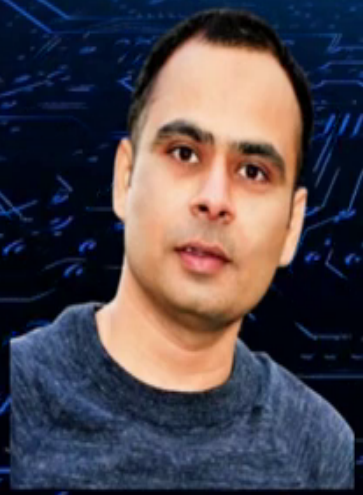
Azure Security

AZ-900

100


00:01:07
Get Certified
Build Cloud Career

00:01:10



The Tech BlackBoard

SUBSCRIBE

Share

@askthetechblackboard @thetechblackboard @Dtechblackboard

Q751: Which Azure automatic tool can Monitor all services and rapidly respond to threats?

a) Microsoft Authenticator
b) Microsoft Defender for Cloud
c) Multi Factor Authentication
d) Azure Firewall

Q7 crosoft Defender for Cloud is a cloud-native application protection platform (CNAPP) with a set of measures and practices designed to protect cloud-based applications from various cyber threats and rabilities.

Yes

No

00:02:11

https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction

Filter by title

- Microsoft Defender for Cloud documentation
- Overview
  - What is Microsoft Defender for Cloud?
  - What's new?
  - Important upcoming changes
  - Common questions
- Deploy
- Tutorials
- Samples
- Concepts
- How-to guides
- Protect your workloads
- Reference

Download PDF

What is Microsoft Defender for Cloud?

Article • 05/21/2023 • 9 contributors

Feedback

In this article

Microsoft Defender for Cloud is a cloud-native application protection platform (CNAPP) with a set of security measures and practices designed to protect cloud-based applications from various cyber threats and vulnerabilities. Defender for Cloud combines the capabilities of:

Additional resources

Training

Learning path

SC-200: Mitigate threats using Microsoft Defender for Cloud - Training

SC-200: Mitigate threats using Microsoft Defender for Cloud

Certification

Microsoft Certified: Security Operations Analyst Associate - Certifications

The Microsoft security operations analyst collaborates with organizational stakeholders to...

Documentation

Overview of Cloud Security Posture Management (CSPM)

Microsoft Defender for Cloud is a cloud-native application protection platform (CNAPP) with a set of security measures and practices designed to protect cloud-based applications from various cyber threats and vulnerabilities. Defender for Cloud combines the capabilities of:

- A development security operations (DevSecOps) solution that unifies security management at the code level across multicloud and multiple-pipeline environments
- A cloud security posture management (CSPM) solution that surfaces actions that you can take to prevent breaches
- A cloud workload protection platform (CWPP) with specific protections for servers, containers, storage, databases, and other workloads

Certification
Microsoft Certified: Security Operations Analyst Associate - Certifications
The Microsoft security operations analyst collaborates with organizational stakeholders to...

Documentation
Overview of Cloud Security Posture Management (CSPM)
Learn more about the new Defender CSPM plan and the other enhanced security features that can be enabl...
Protecting your network resources in Microsoft Defender for Cloud
This document addresses recommendations in Microsoft Defender for Cloud that help you...
The regulatory compliance dashboard in Microsoft Defender for Cloud
Learn how to add and remove regulatory standards from the

platform (CNAPP) with a set of security measures and practices designed to protect cloud-based applications from various cyber threats and vulnerabilities. Defender for Cloud combines the capabilities of:

- A development security operations (DevSecOps) solution that unifies security management at the code level across multicloud and multiple-pipeline environments
- A cloud security posture management (CSPM) solution that surfaces actions that you can take to prevent breaches
- A cloud workload protection platform (CWPP) with specific protections for servers, containers, storage, databases, and other workloads

analyst collaborates with organizational stakeholders to...

Documentation

Overview of Cloud Security Posture Management (CSPM)

Learn more about the new Defender CSPM plan and the other enhanced security features that can be enabl...

Protecting your network resources in Microsoft Defender for Cloud

This document addresses recommendations in Microsoft Defender for Cloud that help you...

The regulatory compliance dashboard in Microsoft Defender for Cloud

Learn how to add and remove regulatory standards from the regulatory compliance dashboard i...

Show 5 more

analyst collaborates with organizational stakeholders to...

Note

For pricing information, see the pricing page.

Secure cloud applications

Defender for Cloud helps you to incorporate good security practices early during the software development process, or DevSecOps. You can protect your code management environments and your code pipelines, and get insights into your development environment security posture from a single location. Defender for DevOps, a service available in Defender for Cloud, empowers security teams to manage DevOps security across multi-pipeline environments.

Today's applications require security awareness at the code,

Documentation

Overview of Cloud Security Posture Management (CSPM)

Learn more about the new Defender CSPM plan and the other enhanced security features that can be enabl...

Protecting your network resources in Microsoft Defender for Cloud

This document addresses recommendations in Microsoft Defender for Cloud that help you...

The regulatory compliance dashboard in Microsoft Defender for Cloud

Learn how to add and remove regulatory standards from the regulatory compliance dashboard i...

Show 5 more

AZ 900: Questions and Answers – Part 40

Which service enables you to achieve those goals is the secure score.

a) Azure Advisor
b) Microsoft Defender for Cloud
c) Multi Factor Authentication
d) Azure score board

Q753: Which service enables you to achieve those goals is the secure score.

a) Microsoft Authenticator
b) Microsoft Defender for Cloud
c) Multi-Factor Authentication
d) Azure score board

Secure score

Article • 06/19/2023 • 8 contributors

Feedback

In this article

Overview of secure score

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

Additional resources

Training

Module
Examine Microsoft Secure Score - Training

Examine Microsoft Secure Score

Certification
Microsoft Certified: Azure Security Engineer Associate - Certifications

The Azure security engineer implements, manages, and monitors security for resources in Azure,...

Documentation

Tracking your secure score in Microsoft Defender for Cloud

Learn about the multiple ways to access and track your secure score in Microsoft Defender for Cloud

Overview of secure score

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 Defender for Cloud that enables you to achieve those goals is the **secure score**.

All Defender for Cloud customers automatically gain access to the secure score when they enable Defender for Cloud. Microsoft Cloud Security Benchmark (MCSB), formerly known as Azure Security Benchmark, is automatically applied to your environments and will generate all the built-in recommendations that are part of this default initiative.

Certification

Microsoft Certified: Azure Security Engineer Associate - Certifications

The Azure security engineer implements, manages, and monitors security for resources in Azure,...

Documentation

Tracking your secure score in Microsoft Defender for Cloud

Learn about the multiple ways to access and track your secure score in Microsoft Defender for Cloud.

Overview

Microsoft Defender External Attack Surface Management (Defender EASM) continuously discovers and...

External attack surface management (EASM) - Defender EASM and External Attack Surface...

Learn how to gain comprehensive visibility and insights over external

Q754: Defender for Cloud continually assesses your cross-cloud resources for security issues.

Yes

No

Q755: Which Azure service is cloud-native and intelligent network firewall security service that provides threat protection for your cloud workloads running in Azure?

a) Microsoft Authenticator
b) Microsoft Defender for Cloud
c) Multi Factor Authentication
d) Azure Firewall

Article • 03/24/2023 • 25 contributors Feedback

Filter by title

Download PDF

In this article

Azure Firewall is a cloud-native and intelligent network firewall security service that provides the best of breed threat protection for your cloud workloads running in Azure. It's a fully stateful, firewall as a service with built-in high availability and unrestricted cloud scalability. It provides both east-west and north-south traffic inspection. To learn what's east-west and north-south traffic, see East-west and north-south traffic.

Azure Firewall is offered in three SKUs: Standard, Premium, and Basic.

Azure Firewall Standard

Azure Firewall Standard provides L3-L7 filtering and threat intelligence

Module
Configure Azure Firewall - Training
Learn how to configure Azure Firewall including firewall rules.

Certification
Microsoft Certified: Azure Network Engineer Associate - Certifications
Candidates for this certification should have subject matter expertise in planning, implementing, and...

Documentation

Azure Firewall Standard features
Learn about Azure Firewall features

Azure Firewall Premium features
Azure Firewall Premium is a managed, cloud-based network security service that protects your...

Azure Firewall Basic features
Learn about Azure Firewall Basic features

Q756: Which Azure service is a managed, cloud-based network security service that protects your Azure Virtual Network resources?

a) Microsoft Authenticator
b) Microsoft Defender for Cloud
c) Multi Factor Authentication
d) Azure Firewall

Q17. Azure Firewall is fully stateful.

Yes

No

Q757: Azure Firewall is fully stateful.

Yes

No

00:06:18

AZ 900: Questions and Answers – Part 40

Q758: Azure Firewall is scalable.

- Yes
- No

Q759: By default, all traffic through the firewall is blocked, a rule must be added in order to enable traffic flow.

Yes

No

When provisioned, Azure Firewall will block all traffic because the default rule is set to 'deny'.

00:04:15

AZ 900: Questions and Answers – Part 40

Q760: You have an Azure environment that contains 10 virtual networks and 100 virtual machines. You need to limit the amount of inbound traffic to all the Azure virtual networks. What should you create?

a) one application security group (ASG)
b) 10 virtual network gateways
c) 10 Azure ExpressRoute circuits
d) one Azure firewall

Q760: You have an Azure environment that contains 10 virtual networks and 100 virtual machines. You need to limit the amount of inbound traffic to all the Azure virtual networks. What should you create?

a) one application security group (ASG)
b) 10 virtual network gateways
c) 10 Azure ExpressRoute circuits
d) one Azure firewall

An Azure firewall is a feature in Azure that allows you to control inbound and outbound network traffic to and from Azure resources. You can create rules that specify the ports, protocols, and sources that can be used to access your virtual networks and virtual machines, and you can apply the firewall to all the virtual networks in your environment.
It allows you to create network filtering rules at the network level which can limit the traffic to the entire virtual network, not just to a single virtual machine.

Q761: If you need basic network level access control (based on IP address and the TCP or UDP protocols) which service should you use?

a) Microsoft Defender
b) Application security group (ASG)
c) Network security group (NSG)
d) Azure Firewall

00:09:12

Network security groups

Article • 03/16/2023 • 14 contributors

Feedback

In this article

You can use an Azure network security group to filter network traffic between Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

You can use an Azure network security group to filter network traffic between Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

This article describes the properties of a network security group rule, the default security rules that are applied, and the rule properties that you can modify to create an augmented security rule.

Q762: Which service can you use for Cloud's just-in-time (JIT) access to protect your Azure virtual machines (VMs) from unauthorized network access?

a) Application security group (ASG)
b) Network security group (NSG)
c) Azure Firewall
d) Microsoft Defender

Enable just-in-time access on VMs

Article • 06/29/2023 • 6 contributors

Feedback

In this article

You can use Microsoft Defender for Cloud's just-in-time (JIT) access to protect your Azure virtual machines (VMs) from unauthorized network access. Many times firewalls contain allow rules that leave your VMs vulnerable to attack. JIT lets you allow access to your VMs only when the access is needed, on the ports needed, and for the period of time needed.

Learn more about how JIT works and the permissions required to configure and use JIT.

In this article, you learn you how to include JIT in your security program, including how to:

Q763: Cross-Origin Resource Sharing (CORS) is a mechanism that allows domains to give each other permission for accessing each other's resources.

Yes

No

Cross-Origin Resource Sharing (CORS) support for Azure Storage

Article • 07/11/2023 • 3 contributors

Feedback

In this article

and Queue services. The File service supports CORS beginning with version 2015-02-21.

CORS is an HTTP feature that enables a web application running under one domain to access resources in another domain. Web browsers implement a security restriction known as same-origin policy that prevents a web page from calling APIs in a different domain; CORS provides a secure way to allow one domain (the origin domain) to call APIs in another domain. See the CORS specification for details on CORS.

You can set CORS rules individually for each of the Azure Storage services, by calling Set Blob Service Properties, Set File Service Properties, Set Queue Service Properties, and Set Table Service Properties. Once you set the CORS rules for the service, then a properly authorized request made against the service from a

[redacted] letApp File

[redacted] Quantum

[redacted] esource G[redacted]ph

[redacted] pring App[redacted]

[redacted] tack Admi[redacted]

[redacted] tack HCI

[redacted] ideo Inde[redacted]r

[redacted] Veb PubSu[redacted] Service

[redacted] lanageme[redacted]

[redacted] ervice

[redacted]

[redacted] Benefits

[redacted] nts

You can set CORS rules individually for each of the Azure Storage services, by calling Set Blob Service Properties, Set File Service Properties, Set Queue Service Properties, and Set Table Service Properties. Once you set the CORS rules for the service, then a properly authorized request made against the service from a different domain will be evaluated to determine whether it is allowed according to the rules you have specified.

> ⓘ **Important**
>
> CORS is not an authorization mechanism. Any request made against a storage resource when CORS is enabled must either have a valid authorization header, or must be made against a public resource.

00:14:22

AZ 900: Questions and Answers – Part 40

Q764: Which Azure service allows you to store application secrets in a centralized cloud location, to securely control access permissions, and access logging?

a) Azure Firewall
b) Azure key vault
c) Microsoft Defender

00:11:49

In this article

Azure Key Vault is one of several key management solutions in Azure, and helps solve the following problems:

- **Secrets Management** - Azure Key Vault can be used to Securely store and tightly control access to tokens, passwords, certificates, API keys, and other secrets
- **Key Management** - Azure Key Vault can be used as a Key Management solution. Azure Key Vault makes it easy to create and control the encryption keys used to encrypt your data.

Azure Key Vault is one of several key management solutions in Azure, and helps solve the following problems:

- **Secrets Management** - Azure Key Vault can be used to Securely store and tightly control access to tokens, passwords, certificates, API keys, and other secrets
- **Key Management** - Azure Key Vault can be used as a Key Management solution. Azure Key Vault makes it easy to create and control the encryption keys used to encrypt your data.
- **Certificate Management** - Azure Key Vault lets you easily provision, manage, and deploy public and private Transport Layer Security/Secure Sockets Layer (TLS/SSL) certificates for use with Azure and your internal connected resources.

Azure Key Vault has two service tiers: Standard, which encrypts

00:14:00

AZ 900: Questions and Answers – Part 40

Q765: Which service provides a user-friendly Multi-Factor Authentication experience that works with both Microsoft Azure Active Directory and Microsoft accounts and includes support for wearables and fingerprint-based approvals.

a) Azure Firewall
b) Azure key vault
c) Microsoft Defender
d) Microsoft Authenticator

Q765: Which service provides a user-friendly Multi-Factor Authentication experience that works with both Microsoft Azure Active Directory and Microsoft accounts and includes support for wearables and fingerprint-based approvals.

a) Azure Firewall
b) Azure key vault
c) Microsoft Defender
d) Microsoft Authenticator