

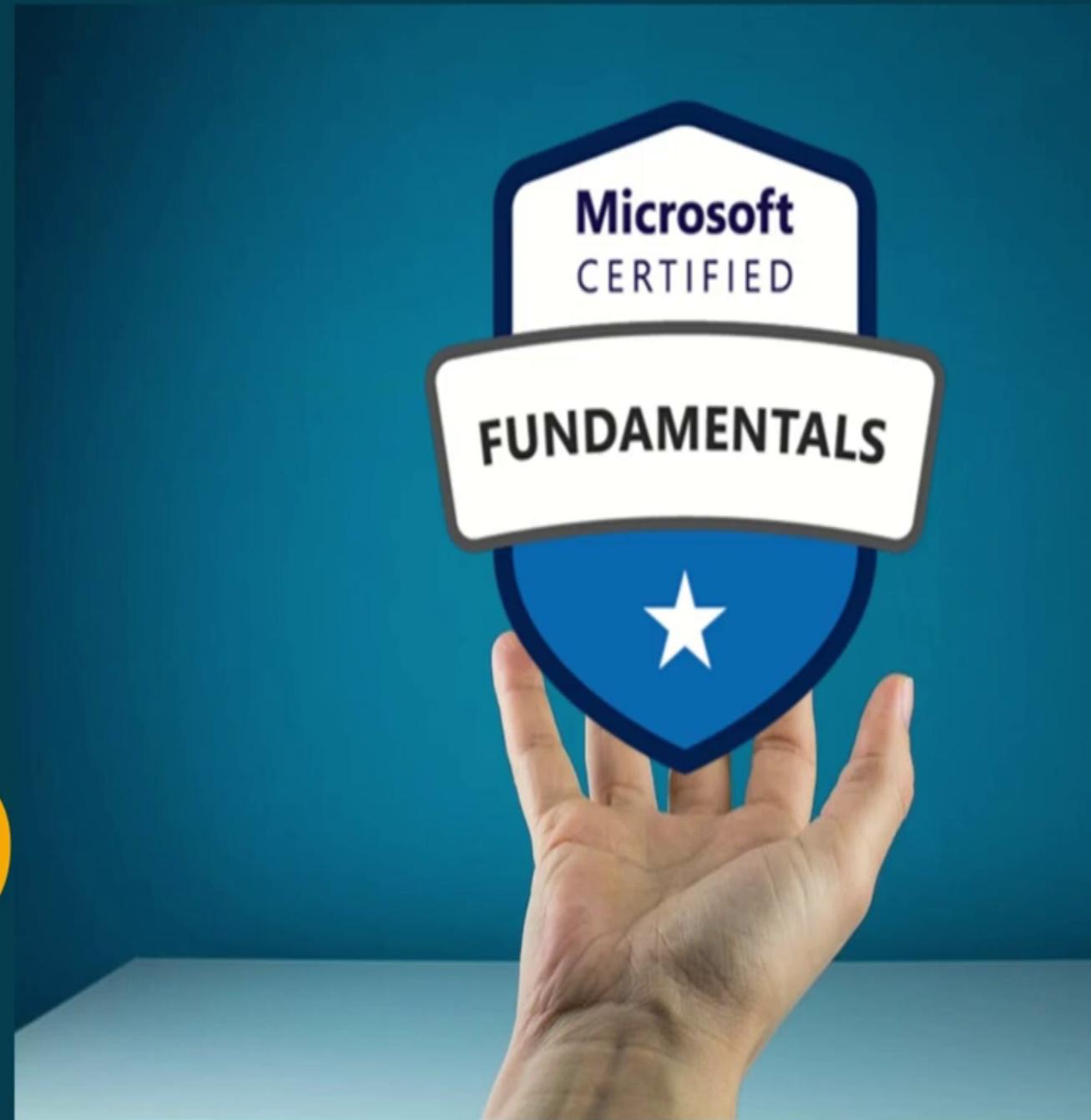


The Tech
Blackboard



Blackboard

AZ 900



20 latest & important questions



AZ 900 2023



Blackboard

Get Certified
Build Cloud Career



The Tech BlackBoard



SUBSCRIBE



Share



@askthetechblackboard



@thetechblackboard



@Dtechblackboard

Q146: What should you use to evaluate whether your company's Azure environment meets regulatory requirements?

- a) The Knowledge Center website.
- b) The Advisor blade from the Azure portal.
- c) Compliance Manager from the Security Trust Portal.
- d) The Security Center blade from the Azure portal

Q147: What should you use to evaluate whether your company's Azure environment meets regulatory requirements?

- a) Azure Service Health
- b) Azure Knowledge Center
- c) Microsoft Defender for Cloud
- d) Azure Advisor

Tutorial: Regulatory compliance x Difference between Microsoft De x | + 00:02:40 https://learn.microsoft.com/en-us/azure/defender-for-cloud/regulatory-compliance-dashboard

Join us for Cloud-native New Year: Celebrate this New Year skilling-up on Cloud-native technologies with Azure Kubernetes Service, Azure Container Apps and Azure Functions. [Learn more >](#)

 Microsoft | Learn Documentation Training Certifications Q&A Code Samples Assessments Shows Events Search Sign in

Azure Product documentation ▾ Architecture ▾ Learn Azure ▾ Develop ▾ Resources ▾ Portal Free account

Filter by title

Microsoft Defender for Cloud documentation

Overview

- What is Microsoft Defender for Cloud?
- What are the enhanced security features?
- What's new?
- Important upcoming changes

Availability

Quickstarts

Tutorials

- Planning and operations guide
- Protect your resources
- Investigate and respond to security alerts

Improve your regulatory compliance

- Manage security policies
- Investigate the health of your resources

Samples

Concepts

Download PDF

Learn / Azure / Security / Microsoft Defender for Cloud /

Tutorial: Improve your regulatory compliance

Article • 01/24/2023 • 14 minutes to read • 8 contributors Feedback

In this article

- Prerequisites
- Assess your regulatory compliance
- Investigate your regulatory compliance issues
- Remediate an automated assessment

Show 6 more

Microsoft Defender for Cloud helps streamline the process for meeting regulatory compliance requirements, using the [regulatory compliance dashboard](#). Defender for Cloud continuously assesses your hybrid cloud environment to analyze the risk factors according to the controls and best practices in the standards that you've applied to your subscriptions. The dashboard reflects the status of your compliance with these standards.

When you enable Defender for Cloud on an Azure subscription, the [Microsoft cloud security benchmark](#) is automatically assigned to that subscription. This widely respected benchmark builds on

Additional resources

Training

Learning paths and modules

[Explore compliance in Microsoft 365 - Training](#)

Explore compliance in Microsoft 365

Learning certificate

[Microsoft Certified: Security, Compliance, and Identity Fundamentals - Certifications](#)

Prove that you are familiar with Microsoft Azure and Microsoft 365 and understand how Microsoft security, compliance, and identity solutions can span across...

Documentation

[The regulatory compliance dashboard in Microsoft Defender for Cloud](#)

Learn how to add and remove regulatory standards from the regulatory compliance dashboard in Defender for Cloud

[Understanding security policies, initiatives, and recommendations in Microsoft Defender](#)

Tutorial: Regulatory compliance x Difference between Microsoft Dev x 00:03:08

https://learn.microsoft.com/en-us/azure/defender-for-cloud/regulatory-compliance-dashboard

Feedback

In this article

Prerequisites

Assess your regulatory compliance

Investigate your regulatory compliance issues

Remediate an automated assessment

Show 6 more

Microsoft Defender for Cloud helps streamline the process for meeting regulatory compliance requirements, using the [regulatory compliance dashboard](#). Defender for Cloud continuously assesses your hybrid cloud environment to analyze the risk factors according to the controls and best practices in the standards that you've applied to your subscriptions. The dashboard reflects the status of your compliance with [these standards](#).

When you enable Defender for Cloud on an Azure subscription, the [Microsoft cloud security benchmark](#) is automatically assigned to that subscription. This widely respected benchmark builds on the controls from the [Center for Internet Security \(CIS\)](#), [PCI-DSS](#) and the [National Institute of Standards and Technology \(NIST\)](#) with a focus on cloud-centric security.

The regulatory compliance dashboard shows the status of all the assessments within your environment for your chosen standards and regulations. As you act on the recommendations and reduce risk factors in your environment, your compliance posture improves.

In this tutorial you'll learn how to:

- ✓ Evaluate your regulatory compliance using the regulatory compliance dashboard
- ✓ Check Microsoft's compliance offerings for Azure, Dynamics 365 and Power Platform products
- ✓ Improve your compliance posture by taking action on recommendations
- ✓ Download PDF/CSV reports as well as certification reports of your compliance status

Explore compliance in Microsoft 365 - Training

Explore compliance in Microsoft 365

Learning certificate

[Microsoft Certified: Security, Compliance, and Identity Fundamentals - Certifications](#)

Prove that you are familiar with Microsoft Azure and Microsoft 365 and understand how Microsoft security, compliance, and identity solutions can span across...

Documentation

[The regulatory compliance dashboard in Microsoft Defender for Cloud](#)

Learn how to add and remove regulatory standards from the regulatory compliance dashboard in Defender for Cloud

[Understanding security policies, initiatives, and recommendations in Microsoft Defender for Cloud](#)

Learn about security policies, initiatives, and recommendations in Microsoft Defender for Cloud.

[Improving your security posture with recommendations in Microsoft Defender for Cloud](#)

This document walks you through how to identify security recommendations that will help you improve your security posture.

Show 5 more

Filter by title

Microsoft Defender for Cloud documentation

Overview

What is Microsoft Defender for Cloud?

What are the enhanced security features?

What's new?

Important upcoming changes

Availability

Quickstarts

Tutorials

Planning and operations guide

Protect your resources

Investigate and respond to security alerts

Improve your regulatory compliance

Manage security policies

Investigate the health of your resources

Samples

Concepts

How-to guides

Protect your workloads

Reference

Resources

Download PDF

Tutorial: Regulators compliance x Difference between Microsoft De x | + 00:03:12

https://learn.microsoft.com/en-us/azure/defender-for-cloud/regulatory-compliance-dashboard

Filter by title

Microsoft Defender for Cloud documentation

Overview

- What is Microsoft Defender for Cloud?
- What are the enhanced security features?
- What's new?
- Important upcoming changes

> Availability

> Quickstarts

✓ Tutorials

- Planning and operations guide
- Protect your resources
- Investigate and respond to security alerts
- Improve your regulatory compliance**
- Manage security policies
- Investigate the health of your resources

> Samples

> Concepts

> How-to guides

> Protect your workloads

> Reference

> Resources

Download PDF

✓ Evaluate your regulatory compliance using the regulatory compliance dashboard

✓ Check Microsoft's compliance offerings for Azure, Dynamics 365 and Power Platform products

✓ Improve your compliance posture by taking action on recommendations

✓ Download PDF/CSV reports as well as certification reports of your compliance status

✓ Setup alerts on changes to your compliance status

✓ Export your compliance data as a continuous stream and as weekly snapshots

If you don't have an Azure subscription, create a [free account](#) before you begin.

Prerequisites

To step through the features covered in this tutorial:

- [Enable enhanced security features](#). You can enable these for free for 30 days.
- You must be signed in with an account that has reader access to the policy compliance data. The [Global reader](#) for the subscription has access to the policy compliance data, but the [Security Reader](#) role doesn't. At a minimum, you'll need to have [Resource Policy Contributor](#) and [Security Admin](#) roles assigned.

Assess your regulatory compliance

The regulatory compliance dashboard shows your selected compliance standards with all their requirements, where supported requirements are mapped to applicable security assessments. The status of these assessments reflects your compliance with the standard.

Use the regulatory compliance dashboard to help focus your attention on the gaps in compliance with your chosen standards and regulations. This focused view also enables you to continuously monitor your compliance over time within dynamic cloud and hybrid environments.

1. Sign in to the Azure portal [↗](#)

Tutorial: Regulatory compliance x Difference between Microsoft Defender for Cloud and Microsoft Defender for Cloud x 00:03:15

https://learn.microsoft.com/en-us/azure/defender-for-cloud/regulatory-compliance-dashboard

To step through the features covered in this tutorial:

- Enable enhanced security features. You can enable these for free for 30 days.
- You must be signed in with an account that has reader access to the policy compliance data. The **Global reader** for the subscription has access to the policy compliance data, but the **Security Reader** role doesn't. At a minimum, you'll need to have **Resource Policy Contributor** and **Security Admin** roles assigned.

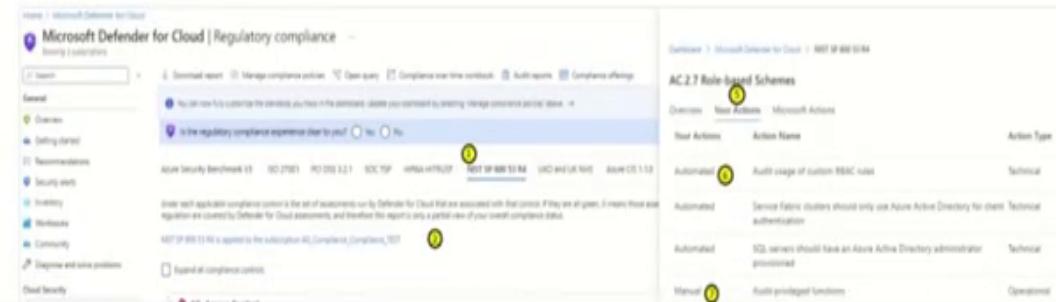
Assess your regulatory compliance

The regulatory compliance dashboard shows your selected compliance standards with all their requirements, where supported requirements are mapped to applicable security assessments. The status of these assessments reflects your compliance with the standard.

Use the regulatory compliance dashboard to help focus your attention on the gaps in compliance with your chosen standards and regulations. This focused view also enables you to continuously monitor your compliance over time within dynamic cloud and hybrid environments.

1. Sign in to the Azure portal .
2. Navigate to **Defender for Cloud > Regulatory compliance**.

The dashboard provides you with an overview of your compliance status and the set of supported compliance regulations. You'll see your overall compliance score, and the number of passing vs. failing assessments associated with each standard.



Action	Standard	Status
View details	PCI DSS 3.2.1	Passing
View details	GDPR	Passing
View details	HIPAA HITRUST CS	Passing
View details	ISO 27001	Passing
View details	NIST SP 800-53 Rev 4	Passing
View details	PCI DSS 3.2.1	Passing
View details	GDPR	Passing
View details	HIPAA HITRUST CS	Passing
View details	ISO 27001	Passing
View details	NIST SP 800-53 Rev 4	Passing

Filter by title[Microsoft Defender for Cloud documentation](#)**Overview**[What is Microsoft Defender for Cloud?](#)[What are the enhanced security features?](#)[What's new?](#)[Important upcoming changes](#)**> Availability****> Quickstarts****✓ Tutorials**[Planning and operations guide](#)[Protect your resources](#)[Investigate and respond to security alerts](#)**Improve your regulatory compliance**[Manage security policies](#)[Investigate the health of your resources](#)**> Samples****> Concepts****> How-to guides****> Protect your workloads****> Reference****> Resources**[Download PDF](#)

actions to remediate compliance concerns. (3)

- Select Control details to view Overview, Your Actions and Microsoft Actions tabs. (4)
- In the Your Actions tab, you can see the automated and manual assessments associated to the control. (5)
- Automated assessments show the number of failed resources and resource types, and link you directly to the remediation experience to address those recommendations. (6)
- The manual assessments can be manually attested, and evidence can be linked to demonstrate compliance. (7)

Investigate your regulatory compliance issues

You can use the information in the regulatory compliance dashboard to investigate any issues that may be affecting your compliance posture.

To investigate your compliance issues:

1. Sign in to the Azure portal .
2. Navigate to **Defender for Cloud > Regulatory compliance**.
3. Select a regulatory compliance standard.
4. Select a compliance control to expand it.
5. Select **Control details**.

Azure Security Benchmark V3 ISO 27001 PCI DSS 3.2.1 SOC TSP HIPAA HITRUST **NIST SP 800 53 R4**

Under each applicable compliance control is the set of assessments run by Defender for Cloud that are associated with that regulation. These assessments are covered by Defender for Cloud assessments, and therefore this report is only a partial view of your overall compliance posture.

NIST SP 800 53 R4 is applied to the subscription AG_Compliance_Compliance_TEST

Expand all compliance controls

Tutorial: Regulatory compliance x Difference between Microsoft De x | + 00:03:28 https://learn.microsoft.com/en-us/azure/defender-for-cloud/regulatory-compliance-dashboard

Join us for Cloud-native New Year: Celebrate this New Year skilling-up on Cloud-native technologies with Azure Kubernetes Service, Azure Container Apps and Azure Functions. [Learn more >](#)

 Microsoft | Learn Documentation Training Certifications Q&A Code Samples Assessments Shows Events Sign in

Azure Product documentation ▾ Architecture ▾ Learn Azure ▾ Develop ▾ Resources ▾ [Portal](#) [Free account](#)

 Filter by title

Microsoft Defender for Cloud documentation

Overview

- What is Microsoft Defender for Cloud?
- What are the enhanced security features?
- What's new?
- Important upcoming changes

Availability

Quickstarts

Tutorials

- Planning and operations guide
- Protect your resources
- Investigate and respond to security alerts

Improve your regulatory compliance

- Manage security policies
- Investigate the health of your resources

Samples

Concepts

[Download PDF](#)

Learn / Azure / Security / Microsoft Defender for Cloud /

Tutorial: Improve your regulatory compliance

Article • 01/24/2023 • 14 minutes to read • 8 contributors 

In this article

- Prerequisites
- Assess your regulatory compliance
- Investigate your regulatory compliance issues
- Remediate an automated assessment

Show 6 more

Microsoft Defender for Cloud helps streamline the process for meeting regulatory compliance requirements, using the [regulatory compliance dashboard](#). Defender for Cloud continuously assesses your hybrid cloud environment to analyze the risk factors according to the controls and best practices in the standards that you've applied to your subscriptions. The dashboard reflects the status of your compliance with these standards.

When you enable Defender for Cloud on an Azure subscription, the [Microsoft cloud security benchmark](#) is automatically assigned to that subscription. This widely respected benchmark builds on

Additional resources

Training

Learning paths and modules

[Explore compliance in Microsoft 365 - Training](#)

Explore compliance in Microsoft 365

Learning certificate

[Microsoft Certified: Security, Compliance, and Identity Fundamentals - Certifications](#)

Prove that you are familiar with Microsoft Azure and Microsoft 365 and understand how Microsoft security, compliance, and identity solutions can span across...

Documentation

The [regulatory compliance dashboard in Microsoft Defender for Cloud](#)

Learn how to add and remove regulatory standards from the regulatory compliance dashboard in Defender for Cloud

Understanding security policies, initiatives, and recommendations in Microsoft Defender

Q148: What should you use to evaluate whether your company's Azure environment meets regulatory requirements?

- a) Azure Service Health
- b) Azure Knowledge Center
- c) Azure Security Center
- d) Azure Advisor

1. First look for Compliance Manager Azure.
2. Else go for Azure security center.

Tutorial: Regulatory compliance x Difference between Microsoft D x 00:04:15

https://learn.microsoft.com/en-us/answers/questions/956836/difference-between-microsoft-defender-for-cloud-an

Microsoft | Learn Documentation Training Certifications Q&A Code Samples Assessments Shows Events

Search Sign in

Q&A Questions Tags FAQ & Help Ask a question

Activity

Difference between Microsoft Defender for Cloud and Microsoft Defender Endpoint ?

Sign in to follow questions and users

MyAzQuery 126 Aug 5, 2022, 3:33 PM

What is the difference between Microsoft Defender for Cloud and Microsoft Defender Endpoint ?

Microsoft Defender for Cloud

1 0 I have the same question 0

JamesTran-MSFT 26,616 • Microsoft Employee Aug 8, 2022, 10:55 PM

@MyAzQuery

I just wanted to check in and see if you had any other questions or if you were able to resolve this issue?

If you have any other questions, please let me know.

Thank you for your time and patience throughout this issue.

Please remember to "Accept Answer" if any answer/reply helped, so that others in the community facing

[Sign in to comment](#)

1 additional answer

[Sort by: Most helpful](#)

Ed Harrison-MSFT
196 • Microsoft Employee

Aug 5, 2022, 5:18 PM

Hi @MyAzQuery ,

Microsoft Defender is the overall "brand" for Microsoft security products, and while these do have similar names as you've spotted they are different products.

In summary:

- Microsoft Defender for Endpoint, is an enterprise endpoint security platform - it incorporates things like next generation antivirus, but also include behavioral sensors, leverages cloud based security analytics and threat intelligence in order to provide security for Windows, macOS, Linux, Android and iOS endpoints. [This link](#) provides a good overview and starting point for more information.
- Microsoft Defender for Cloud provides "Cloud Security Posture Management" (CSPM), providing a security analysis of all the resources in your cloud estates, and Cloud Workload Protection (CWP) which gives specific protection for your resources such as VMs, cloud storage, databases, security keys, containers, etc. [This link](#) provides a starting point on this service.

One of the workload protections in Defender for Cloud is "Defender for Servers" - one of the ways this provides protection of your servers is by including a license to run Defender for Endpoint on the VM, hence giving you the antivirus and other endpoint protection on that system. However, Defender for Servers also provides other protections such as Just in Time access control and adaptive network hardening.



Ed Harrison-MSFT
196 • Microsoft Employee

Aug 5, 2022, 5:18 PM

Hi @MyAzQuery ,

Microsoft Defender is the overall "brand" for Microsoft security products, and while these do have similar names as you've spotted they are different products.

In summary:

- Microsoft Defender for Endpoint, is an enterprise endpoint security platform - it incorporates things like next generation antivirus, but also include behavioral sensors, leverages cloud based security analytics and threat intelligence in order to provide security for Windows, macOS, Linux, Android and iOS endpoints. [This link](#) provides a good overview and starting point for more information.
- Microsoft Defender for Cloud provides "Cloud Security Posture Management" (CSPM), providing a security analysis of all the resources in your cloud estates, and Cloud Workload Protection (CWP) which gives specific protection for your resources such as VMs, [cloud storage, databases, security keys, containers, etc](#). [This link](#) provides a starting point on this service.

One of the workload protections in Defender for Cloud is "Defender for Servers" - one of the ways this provides protection of your servers is by including a license to run Defender for Endpoint on the VM, hence giving you the antivirus and other endpoint protection on that system. However, Defender for Servers also provides other protections such as Just in Time access control and adaptive network hardening.

In short, if you're looking to provide antivirus and other protections for something like your windows endpoints (i.e. the PCs your employees use on a daily basis) then Defender for Endpoint is the product you're after. If you are looking to protect all your resources in the cloud (Azure, AWS, GCP) then Defender for Cloud is what you're after.

I hope this helps - if so, please upvote and "mark as answer" so that others will find this in the

Q148: What should you use to evaluate whether your company's Azure environment meets regulatory requirements?

- a) Azure Service Health
- b) Azure Knowledge Center
- c) Azure Security Center
- d) Azure Advisor

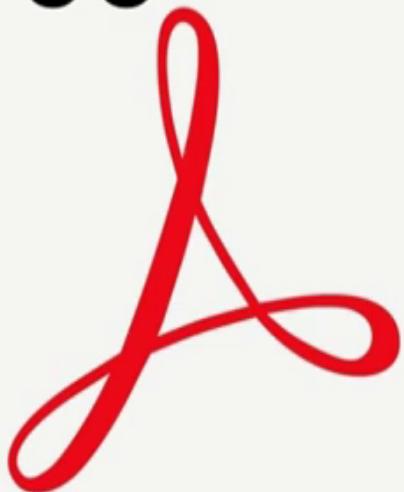
1. First look for Compliance Manager Azure.
2. Else go for Azure security center.

Please appreciate my efforts by pressing



Like

Free



PDF

147

153

164

connectus@thetechblackboard.com

00:06:32

Azure Fundamentals AZ-900



A Azure Web Apps | Hosting



16

Live
Demo



Virtual
Machines

VS



Containers

17



AZ 900 FULL COURSE



Cloud Computing Models

Cloud Deployment Models

Part 3



AZ 900 FULL COURSE



: Part 1 :

Q149: You plan to provision Platform as a Service (PaaS) resources in Azure. Which resources are an example of PaaS?

- a) an Azure web app
- b) an Azure virtual machine
- c) an Azure logic app
- d) an Azure SQL database

Azure key vault can analyze security log files from Azure virtual machines.

True

False

Q150: Azure key vault can analyze security log files from Azure virtual machines.

True

False

 Azure Key Vault is a cloud service that provides a secure store for secrets.

Blackboard

Q151: This question requires that you evaluate the underlined text to determine if it is correct.

Azure Key Vault is used to store app secrets.

Instructions: Review the underlined text. If it makes the statement correct, select “No change is needed”. If the statement is incorrect, select the answer choice that makes the statement correct.

- a) No change is needed
- b) Azure security center
- c) Azure Blob Storage
- d) Azure Repos

Q152: This question requires that you evaluate the underlined text to determine if it is correct.

Azure Key Vault is used to store secrets for Azure Active Directory (Azure AD) user accounts.

Instructions: Review the underlined text. If it makes the statement correct, select “No change is needed”. If the statement is incorrect, select the answer choice that makes the statement correct.

- a) No change is needed
- b) Azure Active Directory (Azure AD) administrative accounts
- c) Personally Identifiable Information (PII)
- d) Server applications

Q153: Your company plans to automate the deployment of servers to Azure. Your manager is concerned that you may expose administrative credentials during the deployment. You need to recommend an Azure solution that encrypts the administrative credentials during the deployment.

What should you include in the recommendation?

- a) Azure Key Vault
- b) Azure Information Protection
- c) Azure Security Center
- d) Azure Multi-Factor Authentication (MFA)

Filter by title

Learn / Azure / Security / Key Vault / General /

About Azure Key Vault

Article • 12/18/2022 • 4 minutes to read • 8 contributors

Feedback

In this article

Why use Azure Key Vault?
Next steps

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 with a software key, and a Premium tier, which includes hardware security module(HSM)-protected keys. To see a comparison between the

Additional resources

Training

Learning paths and modules
[Manage secrets in your server apps with Azure Key Vault - Training](#)

Learn how to create an Azure Key Vault to store secret values and how to enable secure access to the vault.

Learning certificate

[Microsoft Certified: Azure Developer Associate - Certifications](#)

Azure developers design, build, test, and maintain cloud applications and services.

Documentation

[Azure Key Vault Keys, Secrets, and Certificates Overview](#)

Overview of Azure Key Vault REST interface and developer details for keys, secrets and certificates.

About keys - Azure Key Vault

Overview of Azure Key Vault REST interface and developer details for keys.

Q154: Azure Key Vault automatically generates a new secret after every use.

<input checked="" type="radio"/> True	<input type="radio"/> False
---------------------------------------	-----------------------------

Q155: Which Azure service should you use to store certificates?

- a) Azure Security Center
- b) an Azure Storage account
- c) Azure Key Vault
- d) Azure Information Protection

If you are not using virtual machines and all its resources, what should you do to save cost?

- a) Stop Virtual Machine
- b) Shutdown Virtual Machine
- c) Switch off Virtual Machine

Q156: If you are not using virtual machines and all its resources, what should you do to save cost?

- a) Stop Virtual Machine
- b) Shutdown Virtual Machine
- c) Switch off Virtual Machine

Q156: If you are not using virtual machines and all its resources, what should you do to save cost?.

- a) Stop Virtual Machine
- b) Shutdown Virtual Machine
- c) Switch off Virtual Machine



Q156: If you are not using virtual machines and all its resources, what should you do to save cost?

- a) Stop Virtual Machine
- b) Shutdown Virtual Machine 
- c) Switch off Virtual Machine

OFF



Q157: You have an Azure environment that contains multiple Azure virtual machines. You plan to implement a solution that enables the client computers on your on-premises network to communicate to the Azure virtual machines. You need to recommend which Azure resources must be created for the planned solution.

Which two Azure resources should you include in the recommendation?

- a) a virtual network gateway
- b) a load balancer 
- c) an application gateway 
- d) a virtual network 
- e) a gateway subnet 



Elimination Technique

Q158: Azure web app, Azure logic app and Azure SQL database are all examples of Platform as a Service (PaaS).

True

False

Q159: DNS server runs on a virtual machine is PaaS.

True

False

Q159: DNS server runs on a virtual machine is PaaS.

True

False

In general, PaaS (Platform-as-a-Service) is about a platform where a developer can design and deploy an application. So, a regular DNS server runs on a virtual machine is not PaaS. An Azure virtual machine is considered IaaS as it offers computing resources.



Q160: SQL Server installed on a virtual machine is SaaS.

True

False

Q160: SQL Server installed on a virtual machine is SaaS.

True

False

If you install SQL Server on a virtual machine manually or by using out of the box image, it is still a virtual machine. This means customers you still need to manage all of the platform aspects.



Question has Virtual Machine?

Yes Go for IaaS



Q161: Azure SQL database is an example of PaaS.

True

False

Q161: Azure SQL database is an example of PaaS.

True

False

Customers who purchase Azure SQL Database don't need to maintain anything related to SQL platform because Microsoft manages that.



Blackboard

Q162: Azure files is an example of SaaS.

True

False

Q162: Azure files is an example of SaaS.

True

False

Azure Files is a PaaS (platform-as-a-service) offering provided by Microsoft Azure that is built on top of Azure Storage. It provides fully managed file shares over a protocol called SMB (Server Message Block).



Q163: Cloud Computing leverages virtualization to provide services to multiple customers simultaneously

True

False

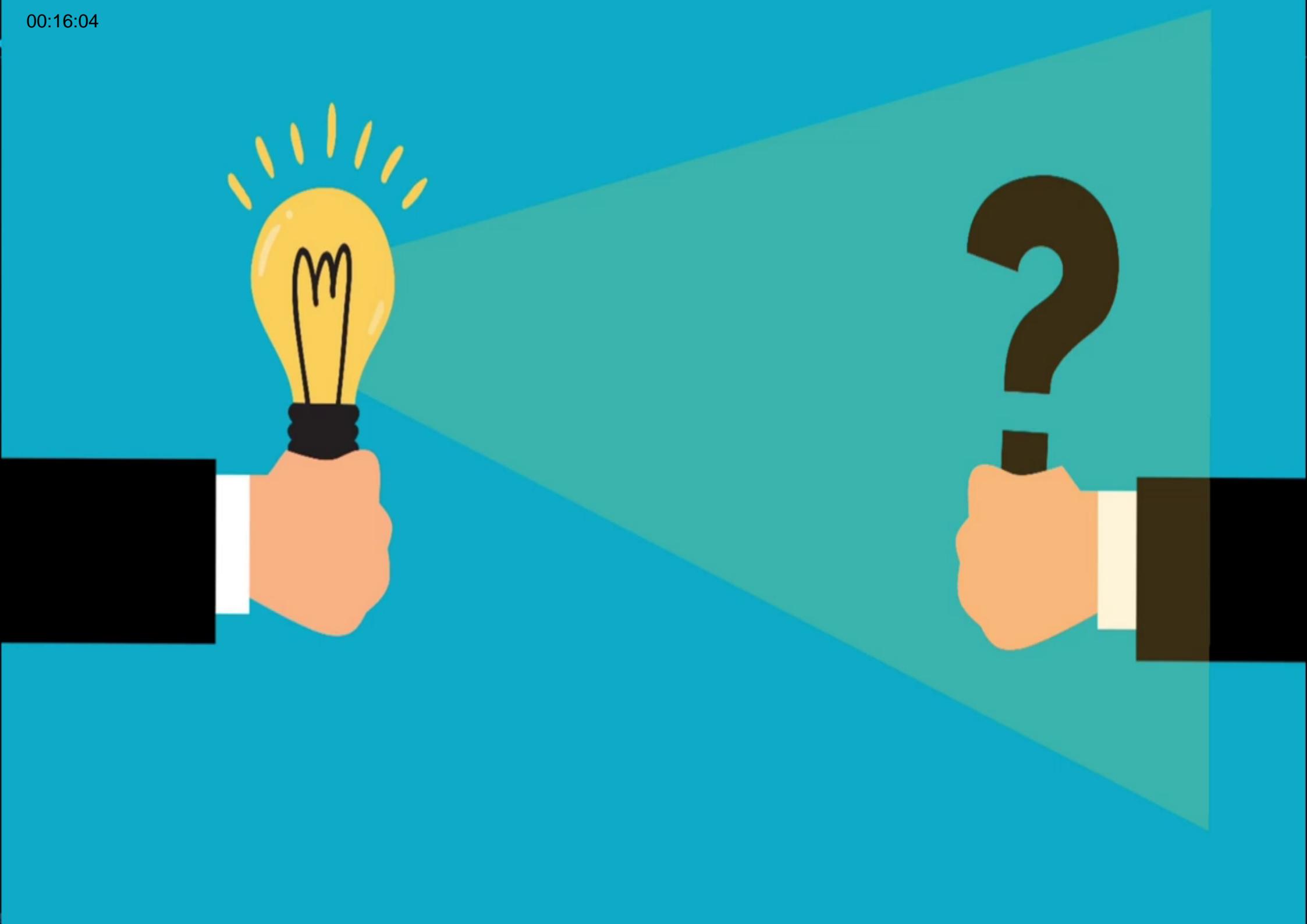
Q164: Which service provides serverless computing in Azure?

- a) Azure Virtual Machines
- b) Azure Functions
- c) Azure storage account
- d) Azure dedicated hosts

Q165: Releasing a feature to all Azure customers is called?

- a) General Availability
- b) General Preview
- c) Public Preview

00:16:04





Connect with us



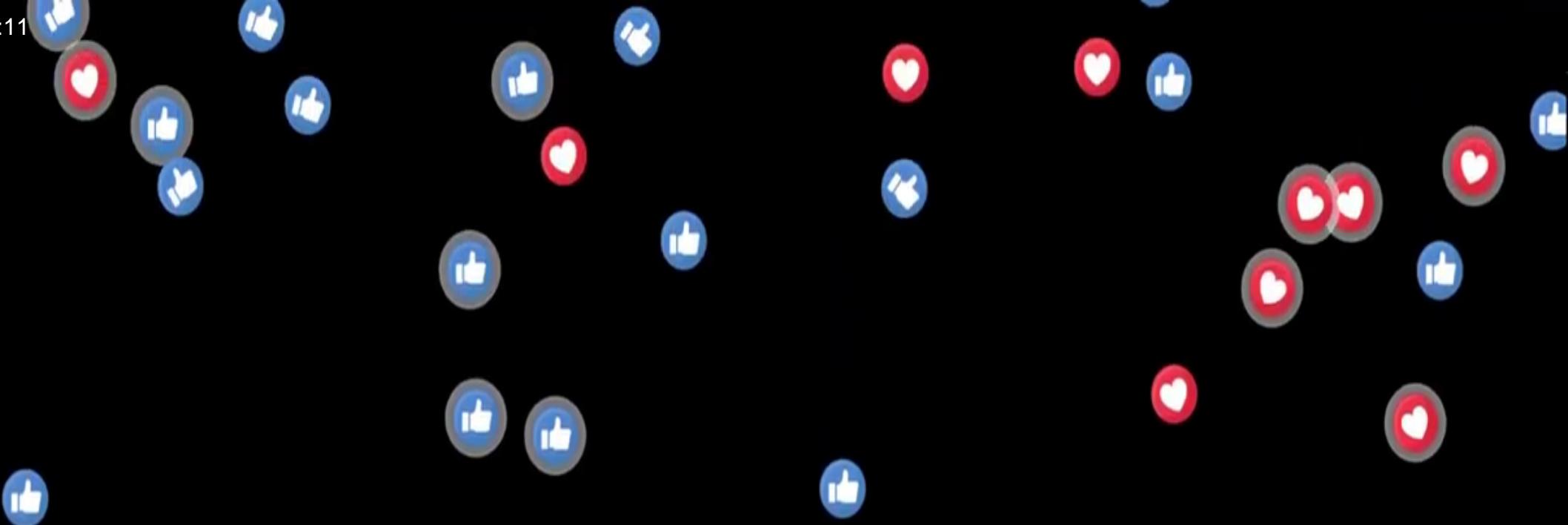
@askthetechblackboard



@thetechblackboard



@Dtechblackboard



Connect with us



@askthetechblackboard



@thetechblackboard



@Dtechblackboard

00:16:32

