EXAMTOPICS

-Expert Verified, Online, **Free**.



CERTIFICATION TEST

-CertificationTest.net - Cheap & Quality Resources With Best Support

Question #1 *Topic 1*

HOTSPOT -
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

Statements	Yes	No
All Azure Active Directory (Azure AD) license editions include the same features.	○	○
You can manage an Azure Active Directory (Azure AD) tenant by using the Azure portal.	○	○
You must deploy Azure virtual machines to host an Azure Active Directory (Azure AD) tenant.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
All Azure Active Directory (Azure AD) license editions include the same features.	○	○
You can manage an Azure Active Directory (Azure AD) tenant by using the Azure portal.	○	○
You must deploy Azure virtual machines to host an Azure Active Directory (Azure AD) tenant.	○	○

Answer Area

Statements	Yes	No
All Azure Active Directory (Azure AD) license editions include the same features.	○	○
You can manage an Azure Active Directory (Azure AD) tenant by using the Azure portal.	○	○
You must deploy Azure virtual machines to host an Azure Active Directory (Azure AD) tenant.	○	○

kset Highly Voted 1 year, 11 months ago
1) No - https://azure.microsoft.com/en-us/pricing/details/active-directory/: Azure Active Directory comes in four editions—Free, Office 365 apps, Premium P1, and Premium P2. 2) Yes - https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-access-create-new-tenant You can do all of your administrative tasks using the Azure Active Directory (Azure AD) portal, including creating a new tenant for your organization. 3) No - https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service
upvoted 52 times

Power123 Most Recent 8 months, 3 weeks ago
NYN is the answer
upvoted 1 times

megan_poirier 1 year ago
On exam today.
upvoted 1 times

LegendaryZA 1 year, 10 months ago
NYN is the answer.
upvoted 2 times

aquarian_ngc 2 years, 1 month ago
Correct Answer: No, Yes, No
upvoted 1 times

JCChien 2 years, 6 months ago

Correct Answers.

upvoted 1 times

incywincy 2 years, 8 months ago

I think that the right answers are NNN. The second question asks if you can access and manage Azure AD through Azure Portal and not through Azure Admin Center. Azure Portal is used to manage Azure Resource and not Azure AD resources. Any comment on that?

upvoted 2 times

tdasuni001 3 years, 4 months ago

NO , Yes, No

upvoted 2 times

Wandz 3 years, 4 months ago

1)No 2)Yes 3)No

upvoted 2 times

Pady1234 3 years, 5 months ago

N, Y, N

upvoted 2 times

MeisAdriano 3 years, 5 months ago

Correct

upvoted 2 times

Ken28132 3 years, 6 months ago

No Yes No

upvoted 3 times

Emmuyah 3 years, 10 months ago

correct answer

upvoted 1 times

Hajimd1984 4 years, 2 months ago

Correct

upvoted 1 times

Sanku265 4 years, 4 months ago

Correct

upvoted 1 times

BlackdaRipper 4 years, 5 months ago

No Yes No is correct.

upvoted 2 times

AZ_Student 4 years, 6 months ago

No Yes No

upvoted 1 times

Question #2 *Topic 1*

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

Azure Blueprints Azure Policy The Microsoft Cloud Adoption Framework for Azure A resource lock	provides best practices from Microsoft employees, partners, and customers, including tools and guidance to assist in an Azure deployment.

Suggested Answer:

Answer Area

Azure Blueprints Azure Policy **The Microsoft Cloud Adoption Framework for Azure** A resource lock	provides best practices from Microsoft employees, partners, and customers, including tools and guidance to assist in an Azure deployment.

Answer Area

Azure Blueprints Azure Policy **The Microsoft Cloud Adoption Framework for Azure** A resource lock	provides best practices from Microsoft employees, partners, and customers, including tools and guidance to assist in an Azure deployment.

Reference: https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/get-started/

AKYK Highly Voted 4 years, 11 months ago

Correct

upvoted 25 times

kset Highly Voted 4 years, 6 months ago

https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/ "The Cloud Adoption Framework is a collection of documentation, implementation guidance, best practices, and tools that are proven guidance from Microsoft designed to accelerate your cloud adoption journey."

upvoted 18 times

Power123 Most Recent 8 months, 3 weeks ago

The Cloud Adoption Framework is correct

upvoted 1 times

yogi0886 1 year, 8 months ago

Correct

upvoted 1 times

aquarian_ngc 2 years, 1 month ago

Correct Answer: Microsoft CAF for Azure

upvoted 1 times

RahulX 3 years ago

The Cloud Adoption Framework is correct ans.

upvoted 1 times

Mehe323 3 years ago

Tip: without much knowledge, some questions can be answered by common sense (and a bit of luck). Go over the names of the other features and think about how they relate to the question. Even if you don't know exactly what CAF is, the other answers don't seem to be really relevant to the question.

upvoted 3 times

tdasuni001 3 years, 4 months ago

The Cloud Adoption Framework brings together cloud adoption best practices from Microsoft employees, partners, and customers. The framework provides tools, guidance, and narratives.

upvoted 1 times

Ken28132 3 years, 6 months ago

CAF is the right answer

upvoted 2 times

Mcelona 3 years, 8 months ago

Correct

upvoted 1 times

Tommo 4 years, 4 months ago

Correct answer

upvoted 2 times

BlackdaRipper 4 years, 5 months ago

Correct answer

upvoted 1 times

AZ_Student 4 years, 6 months ago

CAF is the right one.

upvoted 1 times

TJ001 4 years, 7 months ago

CAF is the right answer (as given)

upvoted 1 times

Chris_Chen 4 years, 7 months ago

Correct.

upvoted 2 times

mcsank 4 years, 8 months ago

correct

upvoted 1 times

Melwin86 5 years, 1 month ago

correct https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/

upvoted 5 times

Question #3 *Topic 1*

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

Customer Lockbox Data loss prevention (DLP) eDiscovery A resource lock	is used to identify, hold, and export electronic information that might be used in an investigation.

Suggested Answer:

Answer Area

Customer Lockbox Data loss prevention (DLP) eDiscovery A resource lock	is used to identify, hold, and export electronic information that might be used in an investigation.

Answer Area

Customer Lockbox Data loss prevention (DLP) eDiscovery A resource lock	is used to identify, hold, and export electronic information that might be used in an investigation.

Reference: https://docs.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview

Rada89 Highly Voted 1 year, 11 months ago

I feel like the correct answer is eDiscovery

https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery?view=o365-worldwide

upvoted 187 times

Rada89 Highly Voted 1 year, 11 months ago

I feel like the correct answer is eDiscovery https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery?view=o365-worldwideeDiscovery 100%Customer Lockbox is used by MS engineers when they need to have access to your data. They use this for requesting permissions to access the data and there is an approval process for it.

upvoted 187 times

iamchoy 1 year, 8 months ago

eDiscovery 100%

upvoted 5 times

Hot_156 4 years, 6 months ago

Customer Lockbox is used by MS engineers when they need to have access to your data. They use this for requesting permissions to access the data and there is an approval process for it.

upvoted 18 times

PrajnaRao 5 years, 1 month ago

Answer is eDiscovery

upvoted 57 times

Power123 Most Recent 8 months, 3 weeks ago

eDiscovery → Search, identify, and export content for legal or compliance investigations

upvoted 1 times

Sweety_Certified7 1 year ago

eDiscovery is correct. https://learn.microsoft.com/en-us/purview/ediscovery "eDiscovery provides an end-to-end workflow to identify, preserve, collect, review, analyze, and export content that's responsive to your organization's internal and external investigations."

upvoted 1 times

nicolase 1 year, 5 months ago

eDiscovery (Electronic Discovery) is a feature in Microsoft Purview that allows organizations to identify, hold, and export electronic information for legal or compliance investigations. It is commonly used in scenarios such as litigation, regulatory requests, and internal audits.

upvoted 1 times

n____or 1 year, 9 months ago

This question has appeared in my exam

upvoted 1 times

LegendaryZA 1 year, 10 months ago

Answer is eDiscovery: "Electronic discovery, or eDiscovery, is the process of identifying and delivering electronic information that can be used as evidence in legal cases". https://learn.microsoft.com/en-us/purview/ediscovery

upvoted 1 times

Darkfire 1 year, 10 months ago

Answer should be eDiscovery https://learn.microsoft.com/en-us/purview/ediscovery?view=o365-worldwide You can search mailboxes and sites in the same eDiscovery search, and then export the search results. You can use Microsoft Purview eDiscovery (Standard) cases to identify, hold, and export content found in mailboxes and sites. https://learn.microsoft.com/en-us/purview/customer-lockbox-requests However, some cases require a Microsoft engineer to access your content to determine the root cause and fix the issue. Customer Lockbox requires the engineer to request access from you as a final step in the approval workflow.

upvoted 2 times

lukecage5 1 year, 10 months ago

The correct answer is eDiscovery. To use Microsoft Purview eDiscovery to identify, hold, and export electronic information, users can follow these steps: Create an eDiscovery case. Place eDiscovery holds on the relevant content locations. Search for the relevant content. Export the relevant content for further review. Microsoft Purview eDiscovery is a powerful tool that can help organizations to comply with legal and regulatory requirements, and to manage their data risks. It is also a valuable tool for organizations that are conducting investigations.

upvoted 1 times

BogdanLu 2 years ago

Answer is eDiscovery

upvoted 1 times

Sm3lly_Cat 2 years, 2 months ago

The correct answer is "eDiscovery." eDiscovery is used to identify, hold, and export electronic information that might be used in an investigation. It stands for electronic discovery and is a crucial part of legal processes, helping organizations comply with data requests for litigation or investigations.

upvoted 1 times

Levock1 2 years, 5 months ago

eDiscovery is the correct option

upvoted 1 times

excelchips11 2 years, 5 months ago

eDiscovery is the answer

upvoted 1 times

MoiLearning 2 years, 5 months ago

the answer is ediscovery

upvoted 1 times

tc_praveen 2 years, 7 months ago

eDiscovery

upvoted 1 times

frych 2 years, 8 months ago

why not eDiscovery ?

upvoted 1 times

MGJG 2 years, 9 months ago

IA:eDiscovery refers to the process of discovering, collecting, and producing electronic information (such as emails, documents, databases, and other digital files) for legal purposes, particularly in the context of litigation or investigations. It involves identifying and preserving relevant electronic records in a manner that ensures their authenticity and integrity.

upvoted 2 times

MGJG 2 years, 9 months ago

IA:eDiscovery refers to the process of discovering, collecting, and producing electronic information (such as emails, documents, databases, and other digital files) for legal purposes, particularly in the context of litigation or investigations. It involves identifying and preserving relevant electronic records in a manner that ensures their authenticity and integrity.The other options you mentioned—customer lockbox, data loss prevention, and resource lock—do not specifically pertain to the process of identifying, holding, and exporting electronic information for investigative purposes. They have different purposes: Customer Lockbox: This is a feature in cloud services that allows customers to have explicit control over when and how a cloud service provider can access their data. It's primarily a security and privacy feature. Data Loss Prevention (DLP): DLP refers to a set of tools and processes used to prevent sensitive information from being accessed, shared, or distributed in an unauthorized manner. Resource Lock: This is a term that might refer to a feature in cloud computing environments that allows users to prevent resources (such as virtual machines or storage) from being modified or deleted. It's a form of access control.

upvoted 2 times

MGJG 2 years, 9 months ago

The other options you mentioned—customer lockbox, data loss prevention, and resource lock—do not specifically pertain to the process of identifying, holding, and exporting electronic information for investigative purposes. They have different purposes: Customer Lockbox: This is a feature in cloud services that allows customers to have explicit control over when and how a cloud service provider can access their data. It's primarily a security and privacy feature. Data Loss Prevention (DLP): DLP refers to a set of tools and processes used to prevent sensitive information from being accessed, shared, or distributed in an unauthorized manner. Resource Lock: This is a term that might refer to a feature in cloud computing environments that allows users to prevent resources (such as virtual machines or storage) from being modified or deleted. It's a form of access control.

upvoted 2 times

Question #4 *Topic 1*

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

You can manage Microsoft Intune by using the

- Azure Active Directory admin center.
- Microsoft 365 compliance center.
- Microsoft 365 Defender portal.
- Microsoft Endpoint Manager admin center.

Suggested Answer:

Answer Area

You can manage Microsoft Intune by using the

- Azure Active Directory admin center.
- Microsoft 365 compliance center.
- Microsoft 365 Defender portal.
- Microsoft Endpoint Manager admin center.

Answer Area

You can manage Microsoft Intune by using the

- Azure Active Directory admin center.
- Microsoft 365 compliance center.
- Microsoft 365 Defender portal.
- Microsoft Endpoint Manager admin center.

gustavomelquiades Highly Voted 4 years, 1 month ago

The answer is: Microsoft Endpoint Manager "Endpoint Manager combines services you may know and already be using, including Microsoft Intune, Configuration Manager, Desktop Analytics, co-management, and Windows Autopilot. These services are part of the Microsoft 365 stack to help secure access, protect data, respond to risk, and manage risk." Source - https://docs.microsoft.com/en-us/mem/endpoint-manager-overview

upvoted 19 times

AyoR32 Highly Voted 1 year, 6 months ago

D, but this term is obsolete. Now this is "Microsoft Intune Admin Center" :)

upvoted 6 times

Power123 Most Recent 8 months, 3 weeks ago

Endpoint Manager Admin Center → Manage devices, apps, security baselines, and Intune policies

upvoted 1 times

LegendaryZA 1 year, 10 months ago

The answer is: Microsoft Endpoint Manager Admin Center "Endpoint Manager combines services you may know and already be using, including Microsoft Intune, Configuration Manager, Desktop Analytics, co-management, and Windows Autopilot. These services are part of the Microsoft 365 stack to help secure access, protect data, respond to risk, and manage risk." https://docs.microsoft.com/en-us/mem/endpoint-manager-overview

upvoted 1 times

XtraWest 3 years, 4 months ago

Microsoft Endpoint Manager Admin Center [Correct]

upvoted 2 times

cleristonm 3 years, 6 months ago

Why do we have this question, if the learning path for SC-900, does not talk about Microsoft Endpoint Manager and Intune ?

upvoted 3 times

Asabs 3 years, 7 months ago

The Microsoft Endpoint Manager admin center is where you can find the Microsoft Intune service, as well as other device management related settings. Understanding the features available in Intune will help you accomplish various Mobile Device Management (MDM) and Mobile Application Management (MAM) tasks.

upvoted 2 times

Lizzylizzy 3 years, 8 months ago

Microsoft intune is part of Microsoft endpoint manager

upvoted 1 times

OrangeSG 3 years, 8 months ago

Answer: Microsoft Endpoint Manager admin center Microsoft Intune, which is a part of Microsoft Endpoint Manager, provides the cloud infrastructure, the cloud-based mobile device management (MDM), cloud-based mobile application management (MAM), and cloud-based PC management for your organization. Tutorial: Walkthrough Intune in Microsoft Endpoint Manager https://learn.microsoft.com/en-us/mem/intune/fundamentals/tutorial-walkthrough-endpoint-manager

upvoted 2 times

Shubham_80884 3 years, 9 months ago

Answer: Microsoft Endpoint Manager. "Microsoft Intune is a cloud-based endpoint management solution. It manages user access and simplifies app and device management across your many devices, including mobile devices, desktop computers, and virtual endpoints."

upvoted 3 times

Lone__Wolf 3 years, 10 months ago

Correct Answer!

upvoted 1 times

jimmysplash 4 years, 2 months ago

keyword-endpoint

upvoted 2 times

egriaguo 4 years, 2 months ago

Microsoft Endpoint Manager admin center

upvoted 2 times

jdemeter 4 years, 3 months ago

Correct answer: Microsoft Endpoint Manager admin center https://docs.microsoft.com/en-us/mem/intune/remote-actions/device-management

upvoted 3 times

jdemeter 4 years, 3 months ago

Correct answer: Microsoft Endpoint Manager admin center https://docs.microsoft.com/en-us/mem/intune/remote-actions/device-managementhttps://docs.microsoft.com/en-us/learn/modules/set-up-microsoft-intune/

upvoted 3 times

jdemeter 4 years, 3 months ago

https://docs.microsoft.com/en-us/learn/modules/set-up-microsoft-intune/

upvoted 1 times

edvaldonardi 4 years, 3 months ago

KK KK KK KK

upvoted 1 times

Question #5 *Topic 1*

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

Federation is used to establish [ ] between organizations.

- multi-factor authentication (MFA)
- a trust relationship
- user account synchronization
- a VPN connection

Suggested Answer:

Answer Area

Federation is used to establish [a trust relationship] between organizations.

- multi-factor authentication (MFA)
- a trust relationship
- user account synchronization
- a VPN connection

Answer Area

Federation is used to establish [a trust relationship] between organizations.

- multi-factor authentication (MFA)
- a trust relationship
- user account synchronization
- a VPN connection

Federation is a collection of domains that have established trust. Reference: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed

Melwin86 Highly Voted 5 years, 1 month ago

correct https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed

upvoted 25 times

Power123 Most Recent 8 months, 3 weeks ago

trust relationship

upvoted 1 times

LegendaryZA 1 year, 10 months ago

The answer is Trust Relationship "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." https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/whatis-fed

upvoted 1 times

aquarian_ngc 2 years, 1 month ago

trust relationship

upvoted 1 times

RahulX 3 years ago

Trust Relationship is correct ans.

upvoted 1 times

Darkfire 3 years ago

Correct

upvoted 1 times

kxa57482 3 years, 5 months ago

Correct

upvoted 3 times

MS10 3 years, 7 months ago

Trust Relationship

upvoted 3 times

orionduo 3 years, 7 months ago

correct "Federation enables the access of services across organizational or domain boundaries by establishing trust relationships between the respective domain's identity provider. " https://learn.microsoft.com/en-us/training/modules/describe-identity-principles-concepts/6-describe-concept-federation

upvoted 4 times

Lizzylizzy 3 years, 8 months ago

Answer is trust relationship

upvoted 1 times

gustavomelquiades 4 years, 1 month ago

Answer is - federation "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." Source - https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fedFederation is the question..the answer is trust between orgs

upvoted 4 times

gustavomelquiades 4 years, 1 month ago

Answer is - federation

"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."

Source - https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed

upvoted 4 times

PaulB_NZ 3 years, 10 months ago

Federation is the question..the answer is trust between orgs

upvoted 2 times

egriaguo 4 years, 2 months ago

Correct answer

upvoted 1 times

Tommo 4 years, 4 months ago

Correct answer

upvoted 1 times

BlackdaRipper 4 years, 5 months ago

Correct answer

upvoted 1 times

TJ001 4 years, 7 months ago

right answer

upvoted 3 times

RamazanInce 4 years, 10 months ago

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.

upvoted 3 times

Question #6 *Topic 1*

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Applying system updates increases an organization's secure score in Microsoft Defender for Cloud	○	○
The secure score in Microsoft Defender for Cloud can evaluate resources across multiple Azure subscriptions	○	○
Enabling multi-factor authentication (MFA) increases an organization's secure score in Microsoft Defender for Cloud	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
Applying system updates increases an organization's secure score in Microsoft Defender for Cloud	○	○
The secure score in Microsoft Defender for Cloud can evaluate resources across multiple Azure subscriptions	○	○
Enabling multi-factor authentication (MFA) increases an organization's secure score in Microsoft Defender for Cloud	○	○

Answer Area

Statements	Yes	No
Applying system updates increases an organization's secure score in Microsoft Defender for Cloud	○	○
The secure score in Microsoft Defender for Cloud can evaluate resources across multiple Azure subscriptions	○	○
Enabling multi-factor authentication (MFA) increases an organization's secure score in Microsoft Defender for Cloud	○	○

Box 1: Yes - System updates reduces security vulnerabilities, and provide a more stable environment for end users. Not applying updates leaves unpatched vulnerabilities and results in environments that are susceptible to attacks.

Box 2: Yes -

Box 3: Yes - If you only use a password to authenticate a user, it leaves an attack vector open. With MFA enabled, your accounts are more secure. Reference: https://docs.microsoft.com/en-us/azure/security-center/secure-score-security-controls

Rayo80 Highly Voted 3 years, 11 months ago

Correct

upvoted 11 times

Power123 Most Recent 8 months, 3 weeks ago

All are correct Yes

upvoted 1 times

JoseRu 12 months ago

yes, yes, yes

upvoted 1 times

adam1598 1 year, 10 months ago

testing this for research purposes

upvoted 1 times

LegendaryZA 1 year, 10 months ago

The answer is Yes, Yes, Yes.

upvoted 2 times

Sm3lly_Cat 2 years, 2 months ago

Yes. Regularly applying system updates improves security posture and thus increases the secure score. Yes. Microsoft Defender for Cloud can evaluate resources across multiple Azure subscriptions, contributing to an overall secure score. Yes. Implementing MFA enhances security, thereby positively impacting the secure score.

upvoted 1 times

RahulX 3 years ago

Box 1: Yes - Box 2: Yes - Box 3: Yes -

upvoted 1 times

kxa57482 3 years, 5 months ago

yes yes yes

upvoted 3 times

Cololand 3 years, 6 months ago

3 times YES

upvoted 2 times

xeni66 3 years, 9 months ago

https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

upvoted 1 times

Lone__Wolf 3 years, 10 months ago

Correct Answer!

upvoted 4 times

LukeFever 3 years, 10 months ago

Correct

upvoted 4 times

Question #7 *Topic 1*

Which score measures an organization's progress in completing actions that help reduce risks associated to data protection and regulatory standards?

A. Microsoft Secure Score

B. Productivity Score

C. Secure score in Azure Security Center

D. Compliance score

Suggested Answer: *D*

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager?view=o365-worldwide
https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score-calculation?view=o365-worldwide

Community vote distribution



eddie_network_jedi Highly Voted 1 year, 11 months ago

Correct. "regulatory" is the keyword here. regulatory:compliance

upvoted 52 times

eddie_network_jedi Highly Voted 1 year, 11 months ago

Correct. "regulatory" is the keyword here. regulatory:complianceto be honest, I barely paid attention to this specific word. Looking here why the answer is 'D'.... I'm surprised that I was surprised by the specific word. Good looking out and great advice for us all (will not forget, thank you)

upvoted 52 times

KoosDuppen 4 years, 3 months ago

to be honest, I barely paid attention to this specific word. Looking here why the answer is 'D'.... I'm surprised that I was surprised by the specific word. Good looking out and great advice for us all (will not forget, thank you)

upvoted 12 times

qdam 4 years, 7 months ago

D is correct

upvoted 21 times

Power123 Most Recent 8 months, 3 weeks ago

compliance score measures your progress in completing recommended actions that help reduce risks around data protection and regulatory standards.

upvoted 1 times

User124657 11 months ago

D is correct

upvoted 1 times

JoseRu 12 months ago

D. Compliance score

upvoted 1 times

W7madridi 1 year, 7 months ago

D is the right answer

upvoted 1 times

iamchoy 1 year, 8 months ago

Yes, D is the correct one.

upvoted 1 times

LegendaryZA 1 year, 10 months ago

The answer is D. Compliance Score "Your compliance score measures your progress in completing recommended actions that help reduce risks around data protection and regulatory standards." https://learn.microsoft.com/en-us/purview/compliance-manager-faq

upvoted 1 times

RahulX 3 years ago

Compliance score

upvoted 2 times

lalalakis 3 years, 5 months ago

Am I the only one who has serious trouble identifying the differences between Microsoft 365 Defender, Defender for Cloud, Defender for Endpoint and the remaining 300 similar named Microsoft Defenders? What;s wrong with these Microsoft people, they are masochists or sth?

upvoted 20 times

kaheri 3 years, 6 months ago

D correct answer

upvoted 2 times

walkaway 3 years, 7 months ago

D - Compliance Score is the correct answer. The question doesn't ask you whether the tool is part of Azure cloud service or not. Don't be trapped on Secure score in Azure Security Center (and note that ASC is no longer the name now. It is Microsoft Defender for Cloud).

upvoted 2 times

Lizzylizzy 3 years, 8 months ago

Compliance score

upvoted 1 times

Mouratov 3 years, 9 months ago

Correct

upvoted 1 times

cantbeme 3 years, 12 months ago

on the exam today

upvoted 2 times

AdityaGupta 4 years ago

D is correct

upvoted 1 times

cormorant 4 years, 1 month ago

regulatory is related to compliance. so compliance center ftw

upvoted 1 times

Question #8 *Topic 1*

What do you use to provide real-time integration between Azure Sentinel and another security source?

A. Azure AD Connect

B. a Log Analytics workspace

C. Azure Information Protection

D. a connector

Suggested Answer: *D*

To on-board Azure Sentinel, you first need to connect to your security sources. Azure Sentinel comes with a number of connectors for Microsoft solutions, including Microsoft 365 Defender solutions, and Microsoft 365 sources, including Office 365, Azure AD, Microsoft Defender for Identity, and Microsoft Cloud App Security, etc. Reference: https://docs.microsoft.com/en-us/azure/sentinel/overview

Community vote distribution

D (100%)

Melwin86 Highly Voted 5 years, 1 month ago

correct https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources

upvoted 25 times

Power123 Most Recent 8 months, 3 weeks ago

Connectors are used to provide real-time integration between Azure Sentinel and other security sources by ingesting their logs and events. Azure Sentinel includes many built-in connectors for Microsoft services like Microsoft 365 Defender and Microsoft 365 sources, as well as connectors for third-party products.

upvoted 1 times

LegendaryZA 1 year, 10 months ago

The answer is D. A connector "Built-in connectors enable connection to the broader security ecosystem for non-Microsoft products. For example, use Syslog, Common Event Format (CEF), or REST APIs to connect your data sources with Microsoft Sentinel." https://learn.microsoft.com/en-us/azure/sentinel/connect-data-sources?tabs=azure-portal

upvoted 3 times

oiuyioyuo 3 years, 4 months ago

correct

upvoted 2 times

OrangeSG 3 years, 8 months ago

After you onboard Microsoft Sentinel into your workspace, you can use data connectors to start ingesting your data into Microsoft Sentinel. Microsoft Sentinel comes with many out of the box connectors for Microsoft services, which you can integrate in real time. Microsoft Sentinel data connectors https://learn.microsoft.com/en-us/azure/sentinel/connect-data-sources

upvoted 4 times

Lone__Wolf 3 years, 10 months ago

Correct Answer: D!

upvoted 4 times

pborlas 3 years, 10 months ago

Correct Answer : D

upvoted 3 times

Armanas 3 years, 11 months ago

Correct Answer : D https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources

upvoted 1 times

AdityaGupta 4 years ago

D is correct

upvoted 1 times

gustavomelquiades 4 years, 1 month ago

Answer is: D "Microsoft 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, and Microsoft 365 sources, including Office 365,

Azure AD, Microsoft Defender for Identity (formerly Azure ATP), and Microsoft Defender for Cloud Apps, and more. " https://docs.microsoft.com/en-us/azure/sentinel/overview

upvoted 3 times

Pedre 4 years, 2 months ago

correct

upvoted 3 times

egriaguo 4 years, 2 months ago

correct

upvoted 1 times

jdemeter 4 years, 3 months ago

D is the answer - connector

upvoted 1 times

Tommo 4 years, 4 months ago

Correct answer

upvoted 2 times

Argsailor 4 years, 5 months ago

Correct, A connector.

upvoted 1 times

imironman 4 years, 5 months ago

What do you use to provide real-time integration between Azure Sentinel and another security source? The Questions asks what do you use and connect to another security source (SIEM) , The answer is D " Connector " Because connector is used for real-time integration. After onboarding Microsoft Sentinel into your workspace, connect data sources to start ingesting your data into Microsoft Sentinel. Microsoft Sentinel comes with many connectors for Microsoft products, available out of the box and providing real-time integration. You can also enable out-of-the-box connectors to the broader security ecosystem for non-Microsoft products. For example, you can use Syslog, Common Event Format (CEF), or REST APIs to connect your data sources with Microsoft Sentinel. https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources

upvoted 4 times

BlackdaRipper 4 years, 5 months ago

Correct answer here

upvoted 1 times

Question #9 *Topic 1*

Which Microsoft portal provides information about how Microsoft cloud services comply with regulatory standard, such as International Organization for
Standardization (ISO)?

A. the Microsoft Endpoint Manager admin center

B. Azure Cost Management + Billing

C. Microsoft Service Trust Portal

D. the Azure Active Directory admin center

Suggested Answer: *C*
The Microsoft Service Trust Portal contains details about Microsoft's implementation of controls and processes that protect our cloud services and the customer data therein. Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-service-trust-portal?view=o365-worldwide

Community vote distribution
C (100%)

Melwin86 Highly Voted 5 years, 1 month ago
correct https://servicetrust.microsoft.com/
upvoted 26 times

qdam Highly Voted 4 years, 7 months ago
C is correct
upvoted 14 times

Power123 Most Recent 8 months, 3 weeks ago
The Microsoft Service Trust Portal provides a variety of content, tools, and other resources about how Microsoft cloud services protect your data, and how you can manage cloud data security and compliance for your organization
upvoted 1 times

JoseRu 12 months ago
C. Microsoft Service Trust Portal
upvoted 1 times

Sentrian 1 year, 3 months ago
C is correct
upvoted 1 times

yogi0886 1 year, 8 months ago
Correct
upvoted 1 times

LegendaryZA 1 year, 10 months ago
The answer is Microsoft Service Trust Portal "The Microsoft Service Trust Portal provides a variety of content, tools, and other resources about how Microsoft cloud services protect your data, and how you can manage cloud data security and compliance for your organization."
https://learn.microsoft.com/en-us/purview/get-started-with-service-trust-portal
upvoted 3 times

aquarian_ngc 2 years, 1 month ago
Correct option: C
upvoted 1 times

Darkfire 3 years ago
C is correct
upvoted 1 times

franky_sagan 3 years, 2 months ago
C is Correct
upvoted 1 times

lbbxtreme 3 years, 5 months ago

C is the way to go

upvoted 2 times

OrangeSG 3 years, 8 months ago

The Service Trust Portal is Microsoft's public site for publishing audit reports and other compliance-related information associated with Microsoft's cloud services. Get started with Microsoft Service Trust Portal https://learn.microsoft.com/en-us/microsoft-365/compliance/get-started-with-service-trust-portal

upvoted 3 times

CataM22 3 years, 11 months ago

A variant of this question appeared in the exam today, September 5th 2022

upvoted 1 times

AdityaGupta 4 years ago

C is correct

upvoted 1 times

gustavomelquiades 4 years, 1 month ago

Answer is: C "The Service Trust Portal contains details about Microsoft's implementation of controls and processes that protect our cloud services and the customer data therein." https://docs.microsoft.com/en-us/microsoft-365/compliance/get-started-with-service-trust-portal?view=o365-worldwide

upvoted 1 times

Tommo 4 years, 4 months ago

C is correct

upvoted 1 times

gabel 4 years, 5 months ago

Correct

upvoted 2 times

Question #10 *Topic 1*

In the shared responsibility model for an Azure deployment, what is Microsoft solely responsible for managing?

A. the management of mobile devices

B. the permissions for the user data stored in Azure

C. the creation and management of user accounts

D. the management of the physical hardware

Suggested Answer: *D*

Official Answer: D

Community vote distribution

D (100%)

Melwin86 Highly Voted 5 years, 1 month ago

correct https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

upvoted 30 times

KoosDuppen Highly Voted 4 years, 3 months ago

if in doubt, try to eliminate the obvious. If you do this here, you will probably end up at D anyways...

upvoted 6 times

Power123 Most Recent 8 months, 3 weeks ago

the management of the physical hardware

upvoted 1 times

JoseRu 12 months ago

D. the management of the physical hardware Most

upvoted 1 times

megan_poirier 1 year ago

On exam today.

upvoted 1 times

LegendaryZA 1 year, 10 months ago

Answer is: the management of the physical hardware https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

upvoted 1 times

aquarian_ngc 2 years, 1 month ago

correct answer: D - only management of Physical Cloud Infrastructure

upvoted 1 times

stewbiee 2 years, 10 months ago

Correct

upvoted 2 times

Darkfire 3 years ago

D is correct https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

upvoted 1 times

Mouratov 3 years, 9 months ago

Correct

upvoted 4 times

exampro99 3 years, 10 months ago

correct

upvoted 2 times

pborlas 3 years, 10 months ago

Answare is D:

upvoted 1 times

AdityaGupta 4 years ago

IaaS services used by any customer is always MS responsibility.

upvoted 3 times

gustavomelquiades 4 years, 1 month ago

Answare is D: "Diagram showing responsibility zones." https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

upvoted 4 times

Endi99 4 years, 4 months ago

correct answer

upvoted 2 times

Tommo 4 years, 4 months ago

correct

upvoted 2 times

yamanktish 4 years, 5 months ago

D is correct

upvoted 2 times

Question #11 *Topic 1*

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Verify explicitly is one of the guiding principles of Zero Trust.	○	○
Assume breach is one of the guiding principles of Zero Trust.	○	○
The Zero Trust security model assumes that a firewall secures the internal network from external threats.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
Verify explicitly is one of the guiding principles of Zero Trust.	○	○
Assume breach is one of the guiding principles of Zero Trust.	○	○
The Zero Trust security model assumes that a firewall secures the internal network from external threats.	○	○

Answer Area

Statements	Yes	No
Verify explicitly is one of the guiding principles of Zero Trust.	○	○
Assume breach is one of the guiding principles of Zero Trust.	○	○
The Zero Trust security model assumes that a firewall secures the internal network from external threats.	○	○

Box 1: Yes -

Box 2: Yes -

Box 3: No - The Zero Trust model does not assume that everything behind the corporate firewall is safe, the Zero Trust model assumes breach and verifies each request as though it originated from an uncontrolled network. Reference: https://docs.microsoft.com/en-us/security/zero-trust/

yulexam Highly Voted 1 year, 11 months ago

Correct... principles of zero trust: Verify explicitly, Least privileged access, Assume breach

upvoted 35 times

Matic_Prime Highly Voted 5 years ago

correct

upvoted 17 times

Power123 Most Recent 8 months, 3 weeks ago

YYN - Verify explicitly: Authenticates and authorizes every access request based on all available data points, such as user identity, location, device health, and anomalies. Use least-privilege access: Limits access to what is required through “just-in-time” and “just-enough-access” (JIT/JEA), risk-

based adaptive policies, and data protection measures. Assume breach: Segments access to minimize the potential damage of a breach, verifies end-to-end encryption, and uses analytics for threat detection and response.

upvoted 1 times

JoseRu 12 months ago

correct

upvoted 1 times

NasX 1 year, 6 months ago

Yes, Yes, No is Correct. Way I remembered it: Verify explicitly - Authenticate & authorize based on all data points/signals. Use least privilege access - Limit user access with Just in time/Just enough access Assume breach - segment access to minimize blast radius

upvoted 1 times

LegendaryZA 1 year, 10 months ago

Answer is: Yes, Yes, No https://www.microsoft.com/en-za/security/business/zero-trust

upvoted 1 times

RahulX 3 years ago

Microsoft Zero Trust is a security strategy based on the principle of Verify explicitly, Use least privilege access, Assume breach.

upvoted 2 times

Kelsi999 3 years, 3 months ago

The answers are correct. I had this question on the exam today

upvoted 3 times

kxa57482 3 years, 5 months ago

YES YES NO

upvoted 3 times

Whyiest 3 years, 6 months ago

Correct

upvoted 3 times

gustavomelquiades 4 years, 1 month ago

Answare is - Y Y N "This is the core of Zero Trust. Instead of believing everything behind the corporate firewall is safe, the Zero Trust model assumes breach and verifies each request as though it originated from an uncontrolled network." https://docs.microsoft.com/en-us/security/zero-trust/zero-trust-overview

upvoted 3 times

GMardones 4 years, 4 months ago

Correct

upvoted 1 times

itelessons 4 years, 4 months ago

Instead of believing everything behind the corporate firewall is safe, the Zero Trust model assumes breach and verifies each request as though it originated from an uncontrolled network.

upvoted 5 times

BlackdaRipper 4 years, 5 months ago

Correct answer

upvoted 1 times

Gringusss 4 years, 5 months ago

YYN is correct

upvoted 1 times

Sukhi4fornet 5 years, 1 month ago

correct

upvoted 8 times

Question #12 *Topic 1*

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Control is a key privacy principle of Microsoft.	○	○
Transparency is a key privacy principle of Microsoft.	○	○
Shared responsibility is a key privacy principle of Microsoft.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
Control is a key privacy principle of Microsoft.	○	○
Transparency is a key privacy principle of Microsoft.	○	○
Shared responsibility is a key privacy principle of Microsoft.	○	○

Answer Area

Statements	Yes	No
Control is a key privacy principle of Microsoft.	○	○
Transparency is a key privacy principle of Microsoft.	○	○
Shared responsibility is a key privacy principle of Microsoft.	○	○

Reference: https://privacy.microsoft.com/en-US/

An_is_here Highly Voted 5 years, 1 month ago

The answer is CORRECT. The Six privacy principles are: Control: We will put you in control of your privacy with easy-to-use tools and clear choices. Transparency: We will be transparent about data collection and use so you can make informed decisions. Security: We will protect the data you entrust to us through strong security and encryption. Strong legal protections: We will respect your local privacy laws and fight for legal protection of your privacy as a fundamental human right. No content-based targeting: We will not use your email, chat, files or other personal content to target ads to you. Benefits to you: When we do collect data, we will use it to benefit you and to make your experiences better.

upvoted 128 times

yulexam Highly Voted 4 years, 9 months ago

correct... 6 key privacy principle: control, transparancy, security, strong legal protection, no content based targeting, benefits to you

upvoted 21 times

Power123 Most Recent 8 months, 3 weeks ago

YYN Customer benefits: Data collection aims to provide meaningful benefits, such as improving products and personalizing experiences. No content-based targeting: Personal content like emails and files is not used for targeted advertising. Legal defense: Microsoft defends user privacy rights

against government requests for data. Legal compliance: The company complies with relevant privacy laws like GDPR and respects local data laws.

upvoted 1 times

megan_poirier 1 year ago

On exam today, August 2025

upvoted 1 times

TechyStacy 1 year, 6 months ago

Shared responsibility is a Cloud deployment model not privacy principle . ans: YES, YES, NO

upvoted 1 times

LegendaryZA 1 year, 10 months ago

The Answer is Yes, Yes, No https://www.microsoft.com/en-za/trust-center#section3

upvoted 2 times

RahulX 3 years ago

Ans by Chat GPT: Customer control, transparency, and strong legal protections for privacy Security and encryption of data No content-based targeting of advertising Inclusive, fair, and easy-to-use tools and choices Supervisable and environmentally responsible digital identity

upvoted 2 times

Vinci123 3 years, 10 months ago

Six privacy principles Firstly, Control. Putting you, the customer, in control of your privacy with easy-to-use tools and clear choices. Secondly, Transparency. Being transparent about data collection and use so that everyone can make informed decisions. Thirdly, Security. Protecting the data that's entrusted to Microsoft by using strong security and encryption. Then, Strong legal protections. Respecting local privacy laws and fighting for legal protection of privacy as a fundamental human right. After that, No content-based targeting. Not using email, chat files, or other personal content to target advertising. Lastly, Benefits. When Microsoft does collect data, it's used to benefit you, the customer, and to make your experiences better.

upvoted 2 times

Vinci123 3 years, 10 months ago

https://learn.microsoft.com/en-us/training/modules/responsible-ai-principles/ 1. fairness 2. Reliability and safety 3. Privacy and security 4. Inclusiveness 5. Transparency 6. Accountability.

upvoted 1 times

cantbeme 3 years, 12 months ago

in exam today

upvoted 2 times

cormorant 4 years, 1 month ago

SHARED RESPONSIBILITY IS NOT A PRINCIPLE

upvoted 9 times

Yelad 4 years, 1 month ago

On the exam 10/07/2022

upvoted 3 times

Twitchy_A2 4 years, 3 months ago

This link is a better to review the principles, https://www.microsoft.com/en-us/trustcenter/privacy/%E2%80%AF#section3

upvoted 5 times

BlackdaRipper 4 years, 5 months ago

YES YES NO is correct

upvoted 4 times

Randy8 4 years, 6 months ago

correct

upvoted 2 times

mrTambourine_man 4 years, 9 months ago

Correct https://www.microsoft.com/en-us/corporate-responsibility/privacy

upvoted 4 times

Matic_Prime 5 years ago

correct

upvoted 2 times

Question #13 *Topic 1*

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

[ ] a file makes the data in the file readable and usable to viewers that have the appropriate key.

- Archiving
- Compressing
- Deduplicating
- Encrypting

Suggested Answer:

Answer Area

[Encrypting] a file makes the data in the file readable and usable to viewers that have the appropriate key.

- Archiving
- Compressing
- Deduplicating
- Encrypting

Answer Area

[Encrypting] a file makes the data in the file readable and usable to viewers that have the appropriate key.

- Archiving
- Compressing
- Deduplicating
- Encrypting

P_2311 Highly Voted 5 years ago

absolutely right

upvoted 30 times

odbjegli Highly Voted 4 years, 7 months ago

Is this typo mistake? Should be decryption, right? Encryption is a process of converting normal data into an unreadable form. Decryption is a method of converting the unreadable/coded data into its original form.spot onI have the same doubtThe KEYword there is "KEY"... so anyone with appropriate key will be able to read it when it's encrypted.I thought the same. But in the guestion it says “to viewers that have the appropriate key”. So keyword is the word “KEY”. Encryption is a means of securing digital data using one or more mathematical techniques, along with a password or "key" used to decrypt the information. Decryption is a process that transforms encrypted information into its original format. To do this, parties to a private conversation use an encryption scheme, called an algorithm, and the keys to encrypt and decrypt messages.

upvoted 19 times

odbjegli 4 years, 7 months ago

Is this typo mistake? Should be decryption, right? Encryption is a process of converting normal data into an unreadable form. Decryption is a method of converting the unreadable/coded data into its original form.

upvoted 19 times

AnaruX 1 year, 2 months ago

spot on

upvoted 1 times

AshutoshSingh 4 years, 6 months ago

I have the same doubt

upvoted 3 times

BanttyLee 3 years ago

The KEYword there is "KEY"... so anyone with appropriate key will be able to read it when it's encrypted.

upvoted 3 times

Clouddog 4 years, 4 months ago

I thought the same. But in the question it says “to viewers that have the appropriate key”. So keyword is the word “KEY”. Encryption is a means of securing digital data using one or more mathematical techniques, along with a password or "key" used to decrypt the information. Decryption is a process that transforms encrypted information into its original format. To do this, parties to a private conversation use an encryption scheme, called an algorithm, and the keys to encrypt and decrypt messages.

upvoted 11 times

Power123 Most Recent 8 months, 3 weeks ago

Encrypting

upvoted 1 times

JoseRu 12 months ago

Encrypting

upvoted 1 times

LegendaryZA 1 year, 10 months ago

The answer is Encrypting https://learn.microsoft.com/en-us/purview/encryption

upvoted 1 times

ChaseT 2 years, 2 months ago

Was on exam 5/31/2024

upvoted 1 times

adv1adv22 2 years, 3 months ago

Encrypting

upvoted 1 times

Kopter 3 years, 1 month ago

I will exam next month. I think the correct answer is Encryption

upvoted 1 times

jaaake 3 years, 1 month ago

Yes, the question is tricky. But indeed it's encryption (the other 3 answers don't make sense).

upvoted 2 times

latoupi 3 years, 3 months ago

La réponse est correct, car l'encryption permet à celui qui a la clé de déchiffrement de pouvoir lire le message.et le texte dit "a file makes the data in the file readable an usable to viewers that have the appropriate key"

upvoted 1 times

Distinctive 3 years, 3 months ago

Encryption is the right answer

upvoted 3 times

Nicochet 3 years, 6 months ago

Correct. D is the option.

upvoted 1 times

ErosTargaryen 3 years, 7 months ago

on exam 12/27/22

upvoted 1 times

walkaway 3 years, 7 months ago

I don't understand why Decryption is an answer. Decryption can't happen without encryption. You all should read and repeat the sentence several times. Encryption is the method to make the file readable to people that have an appropriate key. I don't see any reason why Decryption is an answer. It must be ENCRYPTION. Archiving, Compressing, Dedulicating are all irrelevant.

upvoted 3 times

Lizzylizzy 3 years, 8 months ago

Question is kinda tricky I will go with encryption

upvoted 1 times

sibirnayek 3 years, 8 months ago

YES CORRECT ANSWER

upvoted 1 times

SamNas 3 years, 8 months ago

Correct

upvoted 1 times

Question #14 *Topic 1*

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Digitally signing a document requires a private key.	○	○
Verifying the authenticity of a digitally signed document requires the public key of the signer.	○	○
Verifying the authenticity of a digitally signed document requires the private key of the signer.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
Digitally signing a document requires a private key.	○	○
Verifying the authenticity of a digitally signed document requires the public key of the signer.	○	○
Verifying the authenticity of a digitally signed document requires the private key of the signer.	○	○

Answer Area

Statements	Yes	No
Digitally signing a document requires a private key.	○	○
Verifying the authenticity of a digitally signed document requires the public key of the signer.	○	○
Verifying the authenticity of a digitally signed document requires the private key of the signer.	○	○

Box 1: Yes - A certificate is required that provides a private and a public key.

Box 2: Yes - The public key is used to validate the private key that is associated with a digital signature.

Box 3: Yes - The private key, or rather the password to the private key, validates the identity of the signer. Reference:
https://support.microsoft.com/en-us/office/obtain-a-digital-certificate-and-create-a-digital-signature-e3d9d813-3305-4164-a820-2e063d86e512
https://docs.microsoft.com/en-us/dynamics365/fin-ops-core/fin-ops/organization-administration/electronic-signature-overview

ThomasDehottay Highly Voted 4 years, 9 months ago

Shouldn't it be Y,Y,N ? As the private key is only used (and owned) by the signer to sign the document, and the associated public key is used to verify the authenticity.

upvoted 214 times

ThomasDehottay Highly Voted 4 years, 9 months ago

Shouldn't it be Y,Y,N ? As the private key is only used (and owned) by the signer to sign the document, and the associated public key is used to verify the authenticity.Yes Correct. It's YYN. Private key can not be used to verify the authenticity.Y,Y,N - AgreeYYN, fully agreeAgree,it's yyn

upvoted 214 times

Ravikant84 4 years, 1 month ago

Yes Correct. It's YYN. Private key can not be used to verify the authenticity.

upvoted 8 times

TJ001 4 years, 7 months ago

Y,Y,N - Agree

upvoted 12 times

Alexado 4 years, 6 months ago

YYN, fully agree

upvoted 10 times

Tokiki 4 years, 4 months ago

Agree,it's yyn

upvoted 6 times

simonverma Most Recent 3 months, 3 weeks ago

It should be Y, Y and N. Verification never requires the private key. The private key is only used for signing, not for verification. Using a private key for verification would be a security risk.

upvoted 1 times

Power123 8 months, 3 weeks ago

YYN. Private key Purpose: To create the digital signature. Storage: Kept private and secured on the owner's computer. Security: Must never be shared, as compromising it would allow an imposter to create valid signatures. Public key Purpose: To verify the digital signature and confirm the document's origin and integrity. Storage: Available publicly, often embedded within a digital certificate. Security: Cannot be used to create a signature; it can only verify a signature made with its corresponding private key

upvoted 1 times

SergeTechIt 10 months, 3 weeks ago

True. Digitally signing a document is a process that uses the signer's private key to create a unique digital signature. This signature is a cryptographic hash of the document that's encrypted with the private key. True. To verify the authenticity and integrity of a digitally signed document, you need the signer's public key. The public key, which is mathematically linked to the private key, is used to decrypt the digital signature. If the decrypted hash matches a new hash generated from the document, the signature is valid, confirming the document hasn't been tampered with and was indeed signed by the private key's owner. False. Verifying a digital signature requires the public key of the signer, not their private key. The private key is meant to be kept secret and is only used for signing. If the private key were needed for verification, the entire system would be insecure, as it would have to be shared.

upvoted 3 times

megan_poirier 1 year ago

On exam today, I selected YYN and did pass.

upvoted 2 times

Rour 1 year, 4 months ago

Y,Y,N: The private key is used only for signing, not verification. It must be kept secret. Verification uses the public key.

upvoted 2 times

LegendaryZA 1 year, 10 months ago

The answer is Yes, Yes, No

https://learn.microsoft.com/en-us/previous-versions/windows/desktop/ms757036(v=vs.85)

upvoted 1 times

LegendaryZA 1 year, 10 months ago

The answer is Yes, Yes, No https://learn.microsoft.com/en-us/previous-versions/windows/desktop/ms757036(v=vs.85)Question, I agree Y Y N - but where does exam topics pull the answers from, PearsonVUE? Does Pearson VUE have the correct answers? I am just curious. I take the exam in 4 hours.

upvoted 1 times

karisumar 1 year, 4 months ago

Question, I agree Y Y N - but where does exam topics pull the answers from, PearsonVUE? Does Pearson VUE have the correct answers? I am just curious. I take the exam in 4 hours.

upvoted 1 times

Sm3lly_Cat 2 years, 2 months ago

Yes. Digitally signing a document involves using the signer's private key to create the digital signature. Yes. The public key of the signer is used to verify the digital signature and ensure the document's authenticity. No. The private key is used for signing, not for verifying the signature. Verification uses the public key.

upvoted 2 times

19PetLew 2 years, 3 months ago

Y, Y and N. You are the only one who should have your private key.

upvoted 1 times

SR1991 2 years, 8 months ago

For signature you use assymetric encryption.(https://learn.microsoft.com/en-us/training/modules/describe-security-concepts-methodologies/5-describe-encryption-hashing) The sender's private key encrypts the data -- this is the digital signature -- and the receiver uses the public key to decrypt it and verify it matches the attachment. The public key and private key in digital signatures are mathematically related but cannot be generated from each other. (https://www.techtarget.com/searchsecurity/answer/Which-private-keys-and-public-keys-can-create-a-digital-signature#:~:text=The%20sender's%20private%20key%20encrypts,be%20generated%20from%20each%20other.) So with this information the anwsers will be: Q1 Yes, private key is used for digital signature. Q2 Yes, authenticity for the signature requires a public key Q3 No, this is for encypting the data.

upvoted 2 times

jg_85 2 years, 8 months ago

YYN for Sure

upvoted 1 times

xRiot007 2 years, 11 months ago

Yes, Yes, No The private key of the signer is known only by the signer.

upvoted 1 times

RahulX 3 years ago

Yes Yes NO

upvoted 1 times

Kopter 3 years, 1 month ago

I agree YYN.

upvoted 1 times

jaaake 3 years, 1 month ago

YYN. If you have access to another party's private key, something is amiss!

upvoted 1 times

AKATTHULA 3 years, 3 months ago

YYN. Private key is only used for signing and not for authenticating.

upvoted 2 times

NitinRajNigam 3 years, 3 months ago

Y,Y,N should be the right answer.

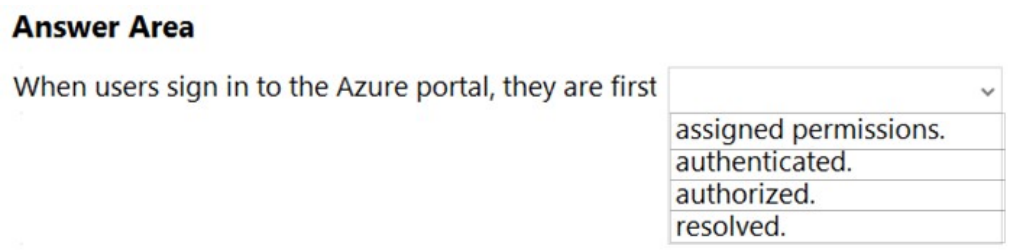
upvoted 1 times

Question #15 *Topic 1*

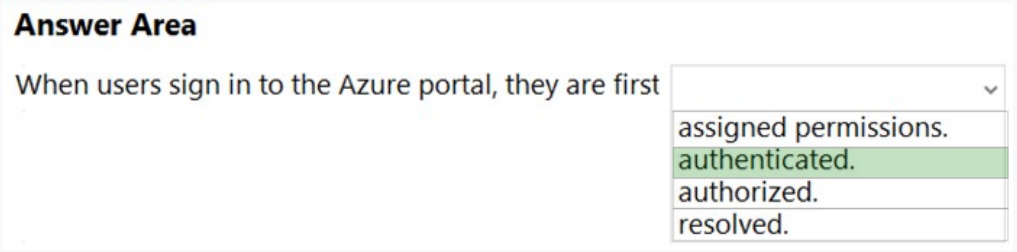
HOTSPOT -

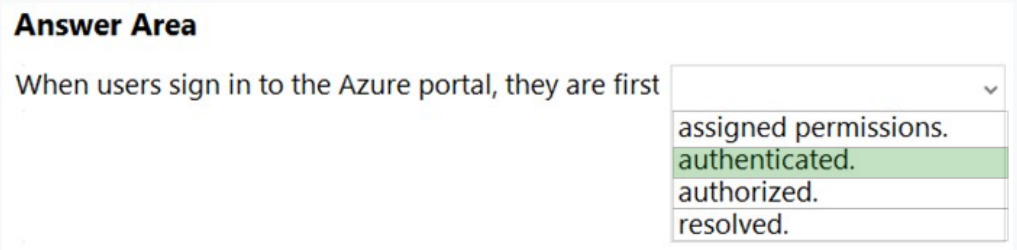
Select the answer that correctly completes the sentence.

Hot Area:



Suggested Answer:





AZ_Student Highly Voted 4 years, 6 months ago

HIGHLY correct. Authentication is who you say you are. Authorization is what permission to do you have.

upvoted 31 times

gustangelo Highly Voted 4 years, 9 months ago

Correct

upvoted 13 times

Power123 Most Recent 8 months, 3 weeks ago

Authentication is the first step in the process. After authentication, Azure uses authorization to determine what resources and actions you are permitted to access within the portal based on your assigned roles and permissions.

upvoted 1 times

LegendaryZA 1 year, 10 months ago

The answer is Authenticated "Authentication is the process of proving that you're who you say you are. This is achieved by verification of the identity of a person or device. It's sometimes shortened to AuthN. The Microsoft identity platform uses the OpenID Connect protocol for handling authentication." https://learn.microsoft.com/en-us/entra/identity-platform/authentication-vs-authorization

upvoted 1 times

Whyiest 3 years, 6 months ago

When you want to connect, here is the pattern : Authentification → Roles attributed → Authorization in function of the permission of the roles

upvoted 6 times

Lizzylizzy 3 years, 8 months ago

Authenticated

upvoted 1 times

Juliandres5845 3 years, 10 months ago

Correct

upvoted 2 times

AdityaGupta 4 years ago

legitimacy of user is checked first (Authentication) later the permissions/ roles are checked to give him Authorization to work on resources.

upvoted 4 times

AhmedEn 4 years, 3 months ago

correct

upvoted 2 times

idhashi 4 years, 3 months ago

Correct

upvoted 1 times

Tommo 4 years, 4 months ago

Correct

upvoted 1 times

Justin0020 4 years, 4 months ago

Had this question on exam. Right answer.

upvoted 4 times

Tokiki 4 years, 4 months ago

Correct

upvoted 3 times

BlackdaRipper 4 years, 5 months ago

Absolutely correct

upvoted 4 times

gamerongam 4 years, 6 months ago

Correct from Brazil, RJ https://docs.microsoft.com/en-us/azure/active-directory/develop/authentication-vs-authorization

upvoted 1 times

Question #16 *Topic 1*

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

[ ] is the process of identifying whether a signed-in user can access a specific resource.

- Authentication
- Authorization
- Federation
- Single sign-on (SSO)

Suggested Answer:

Answer Area

[Authorization] is the process of identifying whether a signed-in user can access a specific resource.

- Authentication
- **Authorization**
- Federation
- Single sign-on (SSO)

Answer Area

[Authorization] is the process of identifying whether a signed-in user can access a specific resource.

- Authentication
- **Authorization**
- Federation
- Single sign-on (SSO)

Reference: https://docs.microsoft.com/en-us/azure/app-service/overview-authentication-authorization

gustangelo Highly Voted 4 years, 9 months ago

correct, next.

upvoted 12 times

TJ001 Highly Voted 4 years, 7 months ago

authN - you are the same person you are saying you are as defined in the identity provider of the system authZ - what you are allowed to do inside the system

upvoted 6 times

megan_poirier Most Recent 1 year ago

On exam August 2025

upvoted 1 times

LegendaryZA 1 year, 10 months ago

The answer is Authorization https://learn.microsoft.com/en-us/entra/identity-platform/authentication-vs-authorization

upvoted 1 times

xRiot007 2 years, 11 months ago

Authentication - done first, will verify user credentials. Authorization - done second, will verify if the user action is permissible based on his roles/permissions

upvoted 1 times

Whyiest 3 years, 6 months ago

It's correct. Pattern of connection : Authentification → Roles attributed → Authorization in function of the permission of the roles

upvoted 1 times

FBrabble 3 years, 9 months ago

yes correct answer!

upvoted 1 times

Juliandres5845 3 years, 10 months ago

Correct

upvoted 2 times

AdityaGupta 4 years ago

legitimacy of user is checked first (Authentication) later the permissions/ roles are checked to give him Authorization to work on resources.

upvoted 3 times

cormorant 4 years, 1 month ago

authorisation to check a user's eligibility to use a resource

upvoted 4 times

idhashi 4 years, 3 months ago

Correct

upvoted 2 times

Tommo 4 years, 4 months ago

Correct

upvoted 1 times

Tokiki 4 years, 4 months ago

Correct

upvoted 1 times

bikewun 4 years, 5 months ago

CORRECT

upvoted 2 times

BlackdaRipper 4 years, 5 months ago

Correct answer. Easy!!

upvoted 2 times

gamerongam 4 years, 6 months ago

Correct https://docs.microsoft.com/en-us/azure/active-directory/develop/authentication-vs-authorization

upvoted 2 times

Ngomoney 4 years, 7 months ago

Correct

upvoted 2 times

Question #17 *Topic 1*

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

Active Directory Domain Services (AD DS) Active Directory forest trusts Azure Active Directory (Azure AD) business-to-business (B2B) Azure Active Directory business-to-consumer B2C (Azure AD B2C)	enables collaboration with business partners from external organizations such as suppliers, partners, and vendors. External users appear as guest users in the directory.

Suggested Answer:

Answer Area

Active Directory Domain Services (AD DS) Active Directory forest trusts Azure Active Directory (Azure AD) business-to-business (B2B) Azure Active Directory business-to-consumer B2C (Azure AD B2C)	enables collaboration with business partners from external organizations such as suppliers, partners, and vendors. External users appear as guest users in the directory.

Answer Area

Active Directory Domain Services (AD DS) Active Directory forest trusts Azure Active Directory (Azure AD) business-to-business (B2B) Azure Active Directory business-to-consumer B2C (Azure AD B2C)	enables collaboration with business partners from external organizations such as suppliers, partners, and vendors. External users appear as guest users in the directory.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/external-identities/what-is-b2b

TheSwedishGuy Highly Voted 4 years, 9 months ago

Correct. "Azure Active Directory (Azure AD) business-to-business (B2B) collaboration is a feature within External Identities that lets you invite guest users to collaborate with your organization. With B2B collaboration, you can securely share your company's applications and services with guest users from any other organization, while maintaining control over your own corporate data."

upvoted 49 times

Yelad Highly Voted 4 years, 1 month ago

On the exam 10/07/2022

upvoted 6 times

megan_poirier Most Recent 1 year ago

On exam today

upvoted 1 times

LegendaryZA 1 year, 10 months ago

The answer is: Azure Active Directory (Azure AD) business-to-business (B2B) "Microsoft Entra External ID includes collaboration capabilities that allow your workforce to work securely with business partners and guests. In your workforce tenant, you can use B2B collaboration to share your company's applications and services with guests, while maintaining control over your own corporate data. Work securely with external partners, even if they don't have Microsoft Entra ID or an IT department." https://learn.microsoft.com/en-us/entra/external-id/what-is-b2b

upvoted 2 times

ChaseT 2 years, 2 months ago

Was on exam 5/31/2024

upvoted 1 times

Awesome_rangan_0001 2 years, 3 months ago

CORRECT

upvoted 1 times

Awesome_rangan_0001 2 years, 3 months ago

CORRECTwe know it's correct. Would be moreover interesting if you had passed the exam and recognized the question. Next time right ;)

upvoted 1 times

lesphinx_1956 2 years, 3 months ago

we know it's correct. Would be moreover interesting if you had passed the exam and recognized the question. Next time right ;)

upvoted 1 times

DriftKing 2 years, 4 months ago

Since the names have changed now, so answer will be "Microsoft Entra B2B collaboration"

upvoted 4 times

furq2904 3 years, 1 month ago

appeared on July 1st 2023

upvoted 2 times

gggggggggggggg 3 years, 3 months ago

business-to-business (B2B) is the correct answer

upvoted 1 times

pifpaff 3 years, 5 months ago

correct !

upvoted 3 times

Nicochet 3 years, 6 months ago

Correct

upvoted 2 times

AdityaGupta 4 years ago

Azure Active Directory (Azure AD) business-to-business (B2B)

upvoted 4 times

kazan 4 years, 1 month ago

Correct

upvoted 1 times

Tommo 4 years, 4 months ago

Correct

upvoted 1 times

Justin0020 4 years, 4 months ago

Had this question on exam. Right answer.

upvoted 3 times

bikewun 4 years, 5 months ago

CORRECT

upvoted 2 times

BlackdaRipper 4 years, 5 months ago

CORRECT ANSWER

upvoted 2 times

Question #18 *Topic 1*

In the Microsoft Cloud Adoption Framework for Azure, which two phases are addressed before the Ready phase? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Plan

B. Manage

C. Adopt

D. Govern

E. Define Strategy

Suggested Answer: *A, E*
Reference: https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/overview

Community vote distribution
AE (100%)

yulexam Highly Voted 4 years, 9 months ago
A, E Correct... cloud adoption framework: strategy, plan, ready, adopt, govern, manage (SPRAGM) :)
upvoted 105 times

yulexam Highly Voted 4 years, 9 months ago
A, E Correct... cloud adoption framework: strategy, plan, ready, adopt, govern, manage (SPRAGM) :)Hi, I think you had missed out the "Migrate" stage. Just my 2 cents' worth.Adoption includes Migrate and InnovateAdopt include migratenice acronym , correct answeror S P R A S M G Strategy Plan Ready Adopt Secure Manage Govern
upvoted 105 times

JA2018 4 years, 7 months ago
Hi, I think you had missed out the "Migrate" stage. Just my 2 cents' worth.Adoption includes Migrate and InnovateAdopt include migrate
upvoted 3 times

JA2018 4 years, 7 months ago
Hi, I think you had missed out the "Migrate" stage. Just my 2 cents' worth.
upvoted 3 times

Swapdevs 4 years, 6 months ago
Adoption includes Migrate and Innovate
upvoted 5 times

lime568 4 years, 6 months ago
Adopt include migrate
upvoted 1 times

TJ001 4 years, 7 months ago
nice acronym , correct answer
upvoted 8 times

NoursBear 2 years, 2 months ago
or S P R A S M G Strategy Plan Ready Adopt Secure Manage Govern
upvoted 6 times

LegendaryZA Most Recent 1 year, 10 months ago
The answer is Plan and Define Strategy https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/
upvoted 1 times

theptr 2 years, 11 months ago
AE ==> correct
upvoted 3 times

Molota 3 years, 2 months ago
AE - Plan and define your strategy
upvoted 1 times

emmye 3 years, 7 months ago

The 2022 article outlined the 6 methodologies including Migrate Innovate secure and organise

upvoted 1 times

yonie 3 years, 7 months ago

AE correct

upvoted 2 times

Lizzylizzy 3 years, 8 months ago

Plan and define your strategy

upvoted 1 times

ricardo_27_04_1978 3 years, 8 months ago

Like in some other cases it is self intuitive. Actions like adopt, govern or manage, require something to be built first. Strategy and plan, do not.

upvoted 1 times

yogur83 3 years, 8 months ago

Plan and Define Strategy

upvoted 2 times

Rayo80 3 years, 11 months ago

A and E

upvoted 2 times

AdityaGupta 4 years ago

Plan and Define Strategy

upvoted 3 times

cormorant 4 years, 1 month ago

adopt strategy and plan makes more sense to be the beginning anyway

upvoted 1 times

daveyk00 4 years, 1 month ago

Correct https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/overview

upvoted 2 times

jmartingnlz 4 years, 1 month ago

A,E Correct

upvoted 1 times

kazan 4 years, 1 month ago

Looks correct

upvoted 1 times

Sussi04 4 years, 1 month ago

A,E are correct aswers

upvoted 1 times

DorelAdr 4 years, 2 months ago

Correct

upvoted 1 times

Question #19 *Topic 1*

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
In software as a service (SaaS), applying service packs to applications is the responsibility of the organization.	○	○
In infrastructure as a service (IaaS), managing the physical network is the responsibility of the cloud provider.	○	○
In all Azure cloud deployment types, managing the security of information and data is the responsibility of the organization.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
In software as a service (SaaS), applying service packs to applications is the responsibility of the organization.	○	○
In infrastructure as a service (IaaS), managing the physical network is the responsibility of the cloud provider.	○	○
In all Azure cloud deployment types, managing the security of information and data is the responsibility of the organization.	○	○

Answer Area

Statements	Yes	No
In software as a service (SaaS), applying service packs to applications is the responsibility of the organization.	○	○
In infrastructure as a service (IaaS), managing the physical network is the responsibility of the cloud provider.	○	○
In all Azure cloud deployment types, managing the security of information and data is the responsibility of the organization.	○	○

sas000 Highly Voted 1 year, 11 months ago

NYY is correct

upvoted 72 times

AbdullahSalam Highly Voted 4 years, 7 months ago

Not correct. It should be N N YQuestion says physical network not virtual network. That's microsoft's babyIn IAAS it's managing physical network is the responsibility of cloud provider not the organization, so answer is NYY.NYY is the correct answer. Physical security of Network Infra is the responsibility of Cloud service provider.That's cloud-101. The physical network is always the cloud provider's responsibility.

upvoted 24 times

AbdullahSalam 4 years, 7 months ago

Not correct. It should be N N Y

upvoted 24 times

ZenLeow 4 years, 2 months ago

Question says physical network not virtual network. That's microsoft's baby

upvoted 21 times

Eagrob_11 3 years, 2 months ago

In IAAS it's managing physical network is the responsibility of cloud provider not the organization, so answer is NYY.

upvoted 5 times

Ravikant84 4 years, 1 month ago

NYY is the correct answer. Physical security of Network Infra is the responsibility of Cloud service provider.

upvoted 9 times

ConfusedPM 3 years, 1 month ago

That's cloud-101. The physical network is always the cloud provider's responsibility.

upvoted 3 times

megan_poirier Most Recent 1 year ago

On exam today.

upvoted 1 times

kd333200 1 year ago

Answer - NYY

upvoted 1 times

LegendaryZA 1 year, 10 months ago

The answer is No, Yes, Yes

In software as a service (SaaS), applying service packs to applications is the responsibility of the organization.

No, this is Microsoft's responsibility

In infrastructure as a service (IaaS), managing the physical network is the responsibility of the cloud provider

Yes, this is Microsoft's responsibility

In all Azure cloud deployment types, managing the security of information and data is the responsibility of the organization

Yes, it is the organization's responsibility to ensure the security of their information and data.

https://learn.microsoft.com/en-us/training/modules/describe-security-concepts-methodologies/2-describe-shared-responsibility-model

https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility#division-of-responsibility

upvoted 3 times

LegendaryZA 1 year, 10 months ago

The answer is No, Yes, Yes In software as a service (SaaS), applying service packs to applications is the responsibility of the organization. No, this is Microsoft's responsibility In infrastructure as a service (IaaS), managing the physical network is the responsibility of the cloud provider Yes, this is Microsoft's responsibility In all Azure cloud deployment types, managing the security of information and data is the responsibility of the organization Yes, it is the organization's responsibility to ensure the security of their information and data. https://learn.microsoft.com/en-us/training/modules/describe-security-concepts-methodologies/2-describe-shared-responsibility-model https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility#division-of-responsibilitySo, it's No Yes Yes. 1) No, this is Microsoft's responsibility 2) NO (why the sudden yes?), this is Microsoft's responsibility 3) Yes, it is the organization's responsibilityNo No Yes, there I go myself :)I read the question wrong mods (the second statement is about the cloud provider, while the other two aks for the organisation), so please delete these comments while I can't :) this person is correct

upvoted 3 times

semauni 1 year, 7 months ago

So, it's No Yes Yes. 1) No, this is Microsoft's responsibility 2) NO (why the sudden yes?), this is Microsoft's responsibility 3) Yes, it is the organization's responsibility

upvoted 1 times

semauni 1 year, 7 months ago

So, it's No Yes Yes. 1) No, this is Microsoft's responsibility 2) NO (why the sudden yes?), this is Microsoft's responsibility 3) Yes, it is the organization's responsibilityNo No Yes, there I go myself :)I read the question wrong mods (the second statement is about the cloud provider, while the other two aks for the organisation), so please delete these comments while I can't :) this person is correct

upvoted 1 times

semauni 1 year, 7 months ago

No No Yes, there I go myself :)I read the question wrong mods (the second statement is about the cloud provider, while the other two aks for the organisation), so please delete these comments while I can't :) this person is correct

upvoted 1 times

semauni 1 year, 7 months ago

No No Yes, there I go myself :)

upvoted 1 times

semauni 1 year, 7 months ago

I read the question wrong mods (the second statement is about the cloud provider, while the other two aks for the organisation), so please delete these comments while I can't :) this person is correct

upvoted 1 times

BMRai 2 years, 4 months ago

It should be NYN. In third question, data security is shared responsibility of customer and cloud service provider.

upvoted 5 times

BMRai 2 years, 4 months ago

It should be NYN. In third question, data security is shared responsibility of customer and cloud service provider.So, it's ALSO the responsibility of the organization. The statement is just about that. Don't overcomplicate it ;)

upvoted 5 times

semauni 1 year, 7 months ago

So, it's ALSO the responsibility of the organization. The statement is just about that. Don't overcomplicate it ;)

upvoted 1 times

SR1991 2 years, 8 months ago

Correct answer is NYY. See the link below for the responsibilities: https://learn.microsoft.com/en-us/training/modules/describe-security-concepts-methodologies/2-describe-shared-responsibility-model

upvoted 1 times

RahulX 3 years ago

NO Yes NO

upvoted 6 times

Darkfire 3 years ago

NYY is correct IaaS Responsibility transfers to cloud provider are: - Physical Hosts - Physical Network - Phisicla datacenter https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

upvoted 1 times

Kelsi999 3 years, 3 months ago

NYY is correct. I had this question on the exam today

upvoted 8 times

walkaway 3 years, 7 months ago

N Y Y. For those who still think 3rd is a YES, read the following statement from Microsoft Docs For all cloud deployment types, you own your data and identities. You are responsible for protecting the security of your data and identities, on-premises resources, and the cloud components you control (which varies by service type). Regardless of the type of deployment, the following responsibilities are always retained by you: - Data - Endpoints - Account - Access management Ref: https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility#division-of-responsibility

upvoted 11 times

yogur83 3 years, 8 months ago

NYY is correct

upvoted 2 times

Mooooosa 3 years, 10 months ago

Please understand and review question Assume we take this services SAAS , Iaas or 1 : In Saas - system updates - Cloud Provider 2 : We take Iaas : Physical Network - Cloud Provider 3. We take cloud services which provides IAAS, Saas Paas from provider , We give data and information - organization

upvoted 3 times

Mrpython 3 years, 11 months ago

N Y Y is correct

upvoted 2 times

be9z 4 years ago

The third question is No: Answer is NYN: See reference: https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility. Confirm and upvote

upvoted 6 times

AdityaGupta 4 years ago

NYY is correct answer. Physical security of Network Infra is always a responsibility of Cloud service provider.

upvoted 1 times

SRINWANTU 4 years, 1 month ago

NYY for 3rd: For all cloud deployment types, you own your data and identities. You are responsible for protecting the security of your data and identities, on-premises resources, and the cloud components you control.

upvoted 2 times

Question #20 *Topic 1*

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Azure AD Connect can be used to implement hybrid identity.	○	○
Hybrid identity requires the implementation of two Microsoft 365 tenants.	○	○
Authentication of hybrid identifies requires the synchronization of Active Directory Domain Services (AD DS) and Azure Active Directory (Azure AD).	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
Azure AD Connect can be used to implement hybrid identity.	○	○
Hybrid identity requires the implementation of two Microsoft 365 tenants.	○	○
Authentication of hybrid identifies requires the synchronization of Active Directory Domain Services (AD DS) and Azure Active Directory (Azure AD).	○	○

Answer Area

Statements	Yes	No
Azure AD Connect can be used to implement hybrid identity.	○	○
Hybrid identity requires the implementation of two Microsoft 365 tenants.	○	○
Authentication of hybrid identifies requires the synchronization of Active Directory Domain Services (AD DS) and Azure Active Directory (Azure AD).	○	○

User_Mowgli Highly Voted 3 years, 11 months ago

Correct

upvoted 14 times

fko8 Highly Voted 2 years, 9 months ago

AD Connect is now called Entra Connect

upvoted 12 times

LegendaryZA Most Recent 1 year, 10 months ago

The answer is Yes, No, Yes

upvoted 1 times

19PetLew 2 years, 3 months ago

AD Connect renamed to Entra Connect. Azure AD renamed to Entra.

upvoted 2 times

pifpaff 3 years, 5 months ago

the answer is correct

upvoted 3 times

me2023 3 years, 7 months ago

Answer is YNY

upvoted 3 times

cris_exam 3 years, 7 months ago

YNY is correct

upvoted 3 times

jsl101669 3 years, 9 months ago

ADDS is a cloud service. On-Prem is what is required for AADConnect. I think the answer is YNN.Actually Active Directory Domain Services is a service within the AD and is not a clod service https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overviewAzure ADDS is different from ADDS. The name says it all.

upvoted 1 times

jsl101669 3 years, 9 months ago

ADDS is a cloud service. On-Prem is what is required for AADConnect. I think the answer is YNN.

upvoted 1 times

luckyiki 3 years, 8 months ago

Actually Active Directory Domain Services is a service within the AD and is not a clod service https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

upvoted 3 times

walkaway 3 years, 7 months ago

Azure ADDS is different from ADDS. The name says it all.

upvoted 5 times

FBrabble 3 years, 9 months ago

Y N Y = correct

upvoted 3 times

abilioneto 3 years, 10 months ago

YNY are the correct ones

upvoted 4 times

Mrpython 3 years, 11 months ago

Correct Answer

upvoted 4 times

Question #21 *Topic 1*

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

Azure Application Insights Azure Network Watcher Log Analytics workspaces Security baselines for Azure	provides benchmark recommendations and guidance for protecting Azure services.

Suggested Answer:

Answer Area

Azure Application Insights Azure Network Watcher Log Analytics workspaces **Security baselines for Azure**	provides benchmark recommendations and guidance for protecting Azure services.

Answer Area

Azure Application Insights Azure Network Watcher Log Analytics workspaces **Security baselines for Azure**	provides benchmark recommendations and guidance for protecting Azure services.

Reference: https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/cloud-services-security-baseline

eddie_network_jedi Highly Voted 4 years, 9 months ago

Correct, "guidance" here is the keyword. guidance:baselines

upvoted 41 times

TheSwedishGuy Highly Voted 4 years, 9 months ago

Correct. "Security baselines for Azure help you strengthen security through improved tooling, tracking, and security features. They also provide you a consistent experience when securing your environment."

upvoted 17 times

megan_poirier Most Recent 1 year ago

On exam today

upvoted 1 times

Adebowale 1 year, 6 months ago

Correct Security baselines for Azure help you strengthen security through improved tooling, tracking, and security features.

upvoted 1 times

LegendaryZA 1 year, 10 months ago

The answer is Security baselines for Azure "The Azure Security Benchmark contains recommendations that help you improve the security of your applications and data on Azure." https://learn.microsoft.com/en-us/security/benchmark/azure/overview-v1

upvoted 2 times

DK21Dilip 2 years ago

this question came in july 2024

upvoted 1 times

rodrigoisalino 2 years, 2 months ago

The question appeared in my exam today, 06/2024.

upvoted 1 times

VivanT 2 years, 3 months ago

Given Answer is correct.

upvoted 1 times

Maqsoof 2 years, 4 months ago

Security baseline for azure helps strengthen security

upvoted 1 times

user_666 2 years, 6 months ago

had this question on my exam today (01 feb 2024)

upvoted 3 times

furq2904 3 years, 1 month ago

appeared on July 1st 2023

upvoted 2 times

Nicochet 3 years, 6 months ago

Security baselines for Azure

upvoted 2 times

Lizzylizzy 3 years, 8 months ago

Security baseline for azure helps strengthen security

upvoted 1 times

AdityaGupta 4 years ago

D is correct answer

upvoted 2 times

cormorant 4 years, 1 month ago

baselines provide benchmarks

upvoted 1 times

Yelad 4 years, 1 month ago

On the exam 10/07/2022

upvoted 2 times

Ravikant84 4 years, 1 month ago

Benchmark = Baseline

upvoted 4 times

Question #22 *Topic 1*

What is an example of encryption at rest?

A. encrypting communications by using a site-to-site VPN

B. encrypting a virtual machine disk

C. accessing a website by using an encrypted HTTPS connection

D. sending an encrypted email

Suggested Answer: *B*

Reference: https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-atrest

Community vote distribution

B (100%)

walkaway Highly Voted 3 years, 7 months ago

A is Encryption in Transit B is Encryption at Rest C is Encryption in Transit D is Encryption in Transit (it's still in transit because both senders and recipients need a key to read the content. This helps protect the content during mail sending transit)

upvoted 25 times

Yelad Highly Voted 4 years, 1 month ago

On the exam 10/07/2022

upvoted 5 times

megan_poirier Most Recent 1 year ago

On exam today.

upvoted 1 times

iamchoy 1 year, 8 months ago

Seems right!

upvoted 1 times

LegendaryZA 1 year, 10 months ago

The answer is: encrypting a virtual machine disk https://learn.microsoft.com/en-us/azure/security/fundamentals/encryption-atrest

upvoted 1 times

Maqsoof 2 years, 4 months ago

Encryption at Rest

upvoted 1 times

Crucius 2 years, 12 months ago

Correct.

upvoted 1 times

furq2904 3 years, 1 month ago

appeared on July 1st 2023

upvoted 1 times

Molota 3 years, 2 months ago

B - is Encryption at Rest

upvoted 1 times

Nicochet 3 years, 6 months ago

Option B

upvoted 1 times

ricardo_27_04_1978 3 years, 8 months ago

at rest - not a communication. So, it must be VM Disk.

upvoted 1 times

Indy429 3 years, 10 months ago

Key-word is "at-rest" - the only thing considered at-rest in the line-up is the VM disk

upvoted 3 times

AdityaGupta 4 years ago

encrypting a virtual machine disk

upvoted 2 times

Oeffnen 4 years ago

Correct

upvoted 2 times

jmartingnlz 4 years, 1 month ago

Correct

upvoted 4 times

atanuforu 4 years, 2 months ago

B. encrypting a virtual machine disk

upvoted 2 times

Abrar_Ajmal 4 years, 2 months ago

B is the correct answer here, quick question are all the other questions on SC-900 on the real exam as well please?

upvoted 2 times

Question #23 *Topic 1*

Which three statements accurately describe the guiding principles of Zero Trust? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Define the perimeter by physical locations.

B. Use identity as the primary security boundary.

C. Always verify the permissions of a user explicitly.

D. Always assume that the user system can be breached.

E. Use the network as the primary security boundary.

Suggested Answer: *B, C, D*
Reference: https://docs.microsoft.com/en-us/security/zero-trust/

Community vote distribution
BCD (100%)

indecisivez Highly Voted 4 years, 3 months ago
BCD is correct
upvoted 24 times

Clouddog Highly Voted 4 years, 3 months ago
Correct, Zero Trust is a security a strategy. It is not a product or a service, but an approach in designing and implementing the following set of security principles: Verify explicitly Use least privilege access Assume breach
upvoted 16 times

Clouddog 4 years, 3 months ago
Correct, Zero Trust is a security a strategy. It is not a product or a service, but an approach in designing and implementing the following set of security principles: Verify explicitly Use least privilege access Assume breachFor more information: https://docs.microsoft.com/en-us/security/zero-trust/zero-trust-overview
upvoted 16 times

Clouddog 4 years, 3 months ago
For more information: https://docs.microsoft.com/en-us/security/zero-trust/zero-trust-overview
upvoted 4 times

TechyStacy Most Recent 1 year, 6 months ago
Least privilege, Verify explicitly, Assume breach
upvoted 1 times

LegendaryZA 1 year, 10 months ago
The answers are: B. Use identity as the primary security boundary. C. Always verify the permissions of a user explicitly. D. Always assume that the user system can be breached. https://www.microsoft.com/en-za/security/business/zero-trust
upvoted 2 times

DK21Dilip 2 years ago
this question came in july 2024
upvoted 2 times

Maqsoof 2 years, 4 months ago
BCD is correct
upvoted 1 times

Francielle 2 years, 7 months ago
C and D are Zero Trust principles, while B can also be explained by having the least possible privileges for an user (identity), thus being the primary security boundary.
upvoted 4 times

Crucius 2 years, 12 months ago
Correct.
upvoted 1 times

Molota 3 years, 2 months ago

B. Use identity as the primary security boundary. Most Voted C. Always verify the permissions of a user explicitly. Most Voted D. Always assume that the user system can be breached.

upvoted 1 times

ismalo 3 years, 6 months ago

BCD is my answer

upvoted 1 times

walkaway 3 years, 7 months ago

Just use the exclusion method to answer this question. A and E violate Zero Trust principles. BCD = Correct answer

upvoted 2 times

mikcs 3 years, 8 months ago

on exam 12/12/22

upvoted 2 times

yogur83 3 years, 8 months ago

https://docs.microsoft.com/en-us/security/zero-trust/zero-trust-overview

upvoted 2 times

Zeus009 3 years, 11 months ago

Correct

upvoted 3 times

cantbeme 3 years, 12 months ago

on exam today

upvoted 4 times

simonseztech 4 years ago

BCD is correct

upvoted 2 times

AdityaGupta 4 years ago

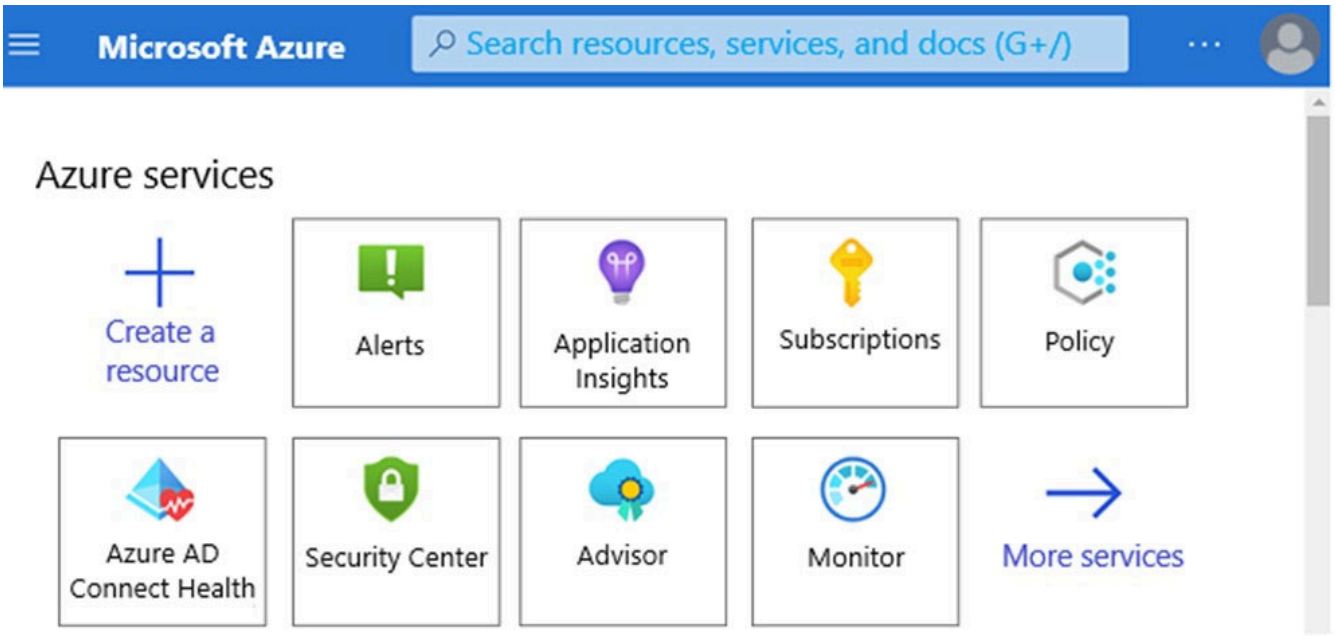
B. Use identity as the primary security boundary. Most Voted C. Always verify the permissions of a user explicitly. Most Voted D. Always assume that the user system can be breached.

upvoted 1 times

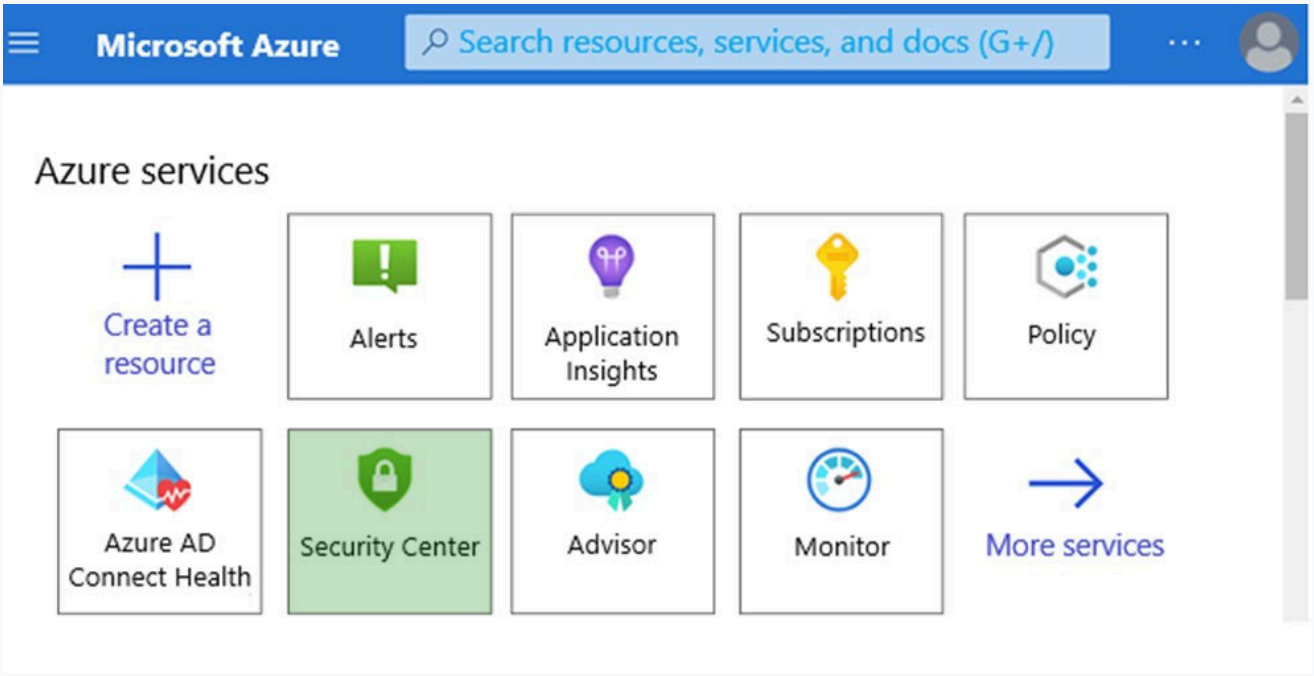
HOTSPOT -

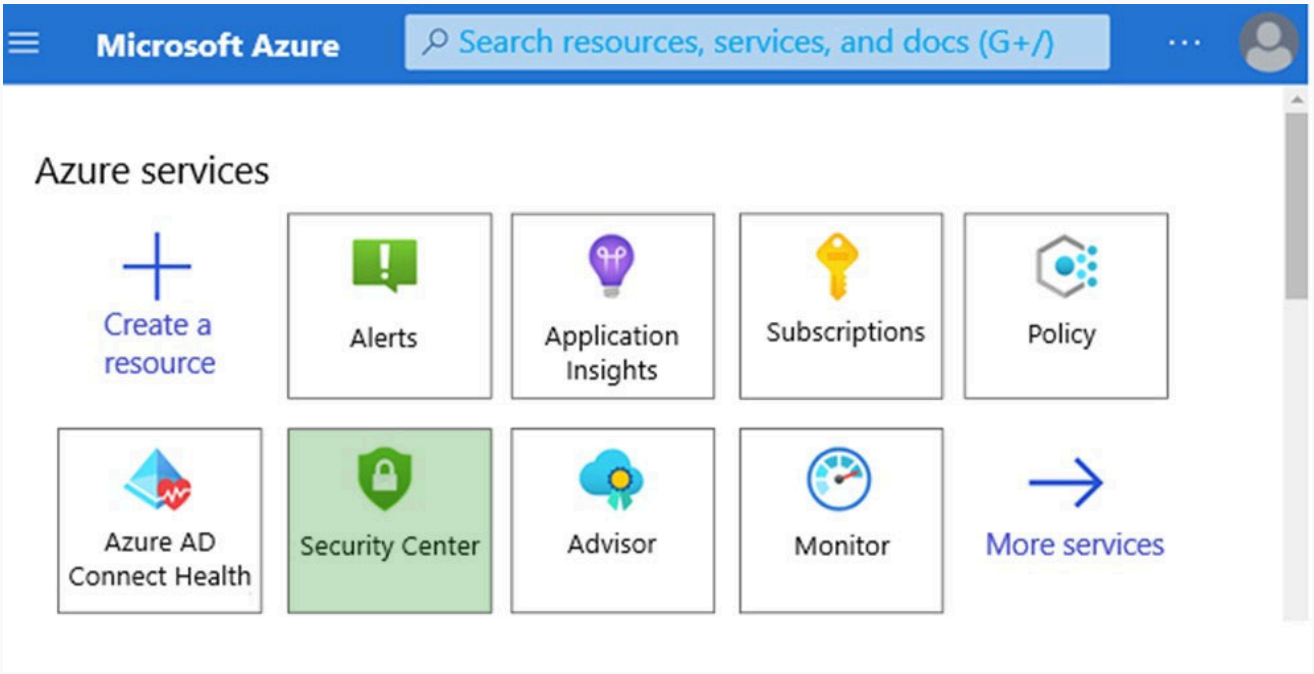
Which service should you use to view your Azure secure score? To answer, select the appropriate service in the answer area.

Hot Area:



Suggested Answer:





Reference: https://docs.microsoft.com/en-us/azure/security-center/secure-score-access-and-track

advillella Highly Voted 4 years, 3 months ago

Azure Security Center and Azure Defender are now called Microsoft Defender for Cloud

upvoted 49 times

cormorant Highly Voted 4 years, 1 month ago

Which service should you use to view your Azure sssssssecure score? sssssssecurity centre

upvoted 33 times

LegendaryZA Most Recent 1 year, 10 months ago

The answer is Security Center which is now Microsoft Defender for Cloud. https://learn.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls

upvoted 3 times

Crucius 2 years, 12 months ago

Security Center

upvoted 1 times

Darkfire 3 years ago

It's Security Center in this example. But it is now called Microsoft Defender for Cloud. https://learn.microsoft.com/nl-nl/microsoft-365/security/defender/microsoft-secure-score?view=o365-worldwide

upvoted 4 times

Dhamus 3 years, 3 months ago

It is now called Microsoft Defender for Cloud.

upvoted 2 times

Nicochet 3 years, 6 months ago

Microsoft Defender for Cloud

upvoted 4 times

yonie 3 years, 7 months ago

=Microsoft Defender for Cloud

upvoted 3 times

Lizzylizzy 3 years, 8 months ago

Security center

upvoted 1 times

abilioneto 3 years, 10 months ago

correct

upvoted 2 times

AdityaGupta 4 years ago

Azure Security Center

upvoted 2 times

cormorant 4 years, 1 month ago

security center for viewing your security score

upvoted 3 times

clem24 4 years, 2 months ago

correct

upvoted 2 times

Question #25 *Topic 1*

DRAG DROP -

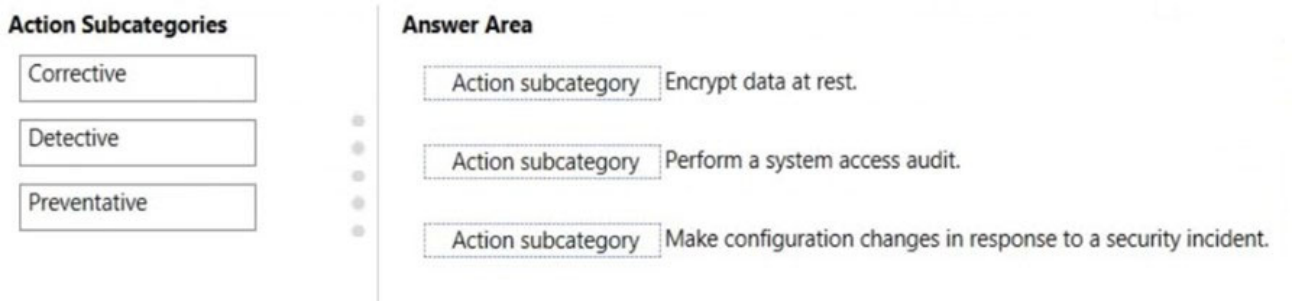
You are evaluating the compliance score in Compliance Manager.

Match the compliance score action subcategories to the appropriate actions.

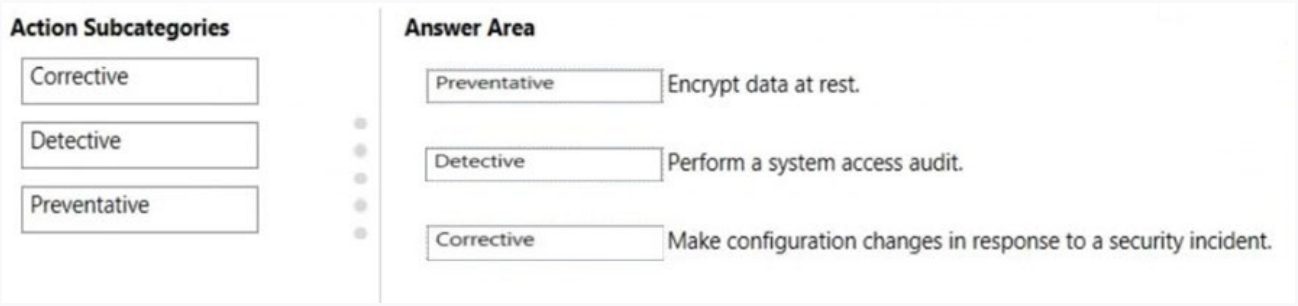
To answer, drag the appropriate action subcategory from the column on the left to its action on the right. Each action subcategory may be used once, more than once, or not at all.

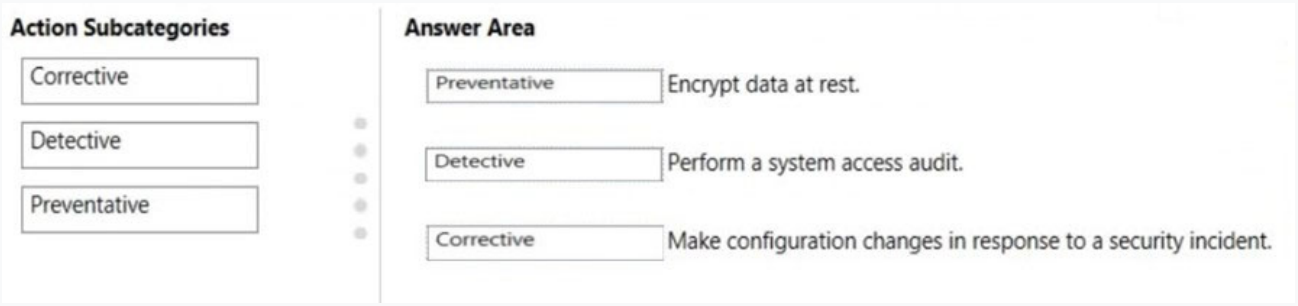
NOTE: Each correct match is worth one point.

Select and Place:



Suggested Answer:





Box 1: Preventative - Preventative actions address specific risks. For example, protecting information at rest using encryption is a preventative action against attacks and breaches. Separation of duties is a preventative action to manage conflict of interest and guard against fraud.

Box 2: Detective - Detective actions actively monitor systems to identify irregular conditions or behaviors that represent risk, or that can be used to detect intrusions or breaches. Examples include system access auditing and privileged administrative actions. Regulatory compliance audits are a type of detective action used to find process issues.

Box 3: Corrective - Corrective actions try to keep the adverse effects of a security incident to a minimum, take corrective action to reduce the immediate effect, and reverse the damage if possible. Privacy incident response is a corrective action to limit damage and restore systems to an operational state after a breach. Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score-calculation

Luanee Highly Voted 3 years, 11 months ago

It's correct

upvoted 9 times

Zeus009 Highly Voted 3 years, 11 months ago

Aligned

upvoted 9 times

LegendaryZA Most Recent 1 year, 10 months ago

The answer is: Preventative Detective Corrective https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score-calculation

upvoted 1 times

DK21Dilip 2 years ago

this question came in july 2024

upvoted 1 times

rodrigoisalino 2 years, 2 months ago

The question appeared in my exam today, 06/2024.

upvoted 1 times

user_666 2 years, 6 months ago

had this question on my exam today (01 feb 2024)

upvoted 3 times

furq2904 3 years, 1 month ago

appeared on July 1st 2023, but had only 2 boxes

upvoted 2 times

Kelsi999 3 years, 3 months ago

On the exam today. The answer is correct

upvoted 2 times

Nicochet 3 years, 6 months ago

Correct

upvoted 2 times

mikcs 3 years, 8 months ago

on exam 12/12/22

upvoted 3 times

rama161 3 years, 9 months ago

All correct

upvoted 4 times

Question #26 *Topic 1*

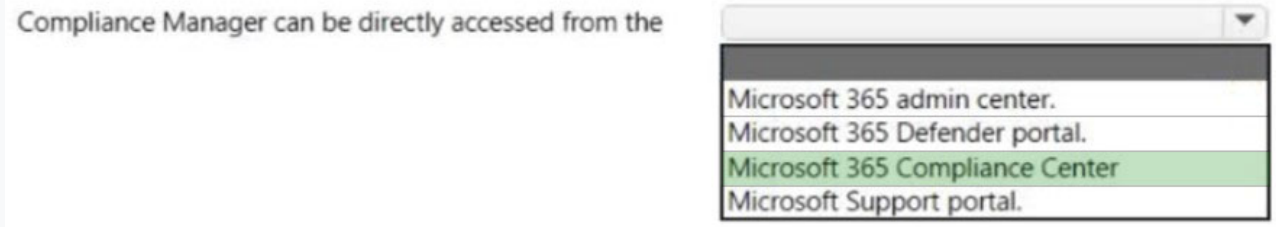
HOTSPOT -

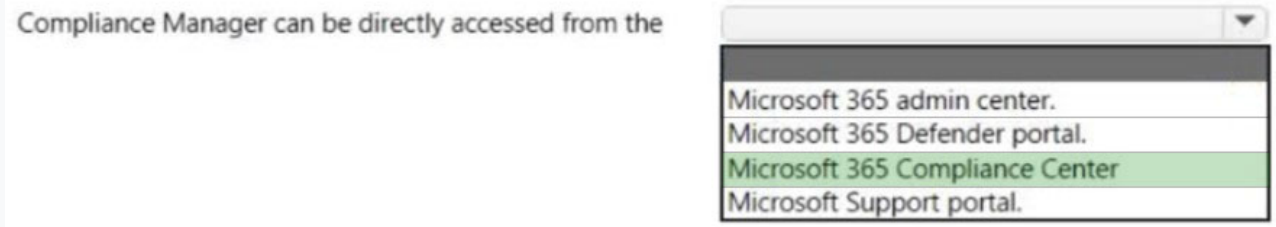
Select the answer that correctly completes the sentence.

Hot Area:



Suggested Answer:





Sign in to Compliance Manager - 1. Go to the Microsoft Purview compliance portal and sign in with your Microsoft 365 global administrator account. 2. Select Compliance Manager on the left navigation pane. You'll arrive at your Compliance Manager dashboard. The direct link to access Compliance Manager is https://compliance.microsoft.com/compliancemanager Note: Microsoft 365 compliance is now called Microsoft Purview and the solutions within the compliance area have been rebranded. Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-setup

Jeff_84 Highly Voted 3 years, 11 months ago

Compliance Centre is now known as Microsoft Purview

upvoted 34 times

Ola189 Highly Voted 3 years, 9 months ago

Correct but it's now called Microsoft Purview, not Microdoft 365 Compliance Centre.

upvoted 13 times

LegendaryZA Most Recent 1 year, 10 months ago

The answer is: Microsoft 365 Compliance Center which is now called Microsoft Purview https://learn.microsoft.com/en-us/purview/compliance-manager

upvoted 3 times

rodrigoisalino 2 years, 2 months ago

The question appeared in my exam today, 06/2024.

upvoted 2 times

Molota 3 years, 2 months ago

Microdoft 365 Compliance Centre IS Microsoft Purview

upvoted 2 times

XtraWest 3 years, 4 months ago

Microsoft Purview is correct

upvoted 2 times

yonie 3 years, 7 months ago

it's now called Microsoft Purview

upvoted 2 times

Lizzylizzy 3 years, 8 months ago

Compliance center now called purview

upvoted 2 times

yogur83 3 years, 8 months ago

In this case compliance center but MS has changed it to Microsoft Purview

upvoted 4 times

User_Mowgli 3 years, 11 months ago

Correct

upvoted 3 times

Question #27 *Topic 1*

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Statements	Yes	No
Enabling multi-factor authentication (MFA) increases the Microsoft Secure Score.	○	○
A higher Microsoft Secure Score means a lower identified risk level in the Microsoft 365 tenant.	○	○
Microsoft Secure Score measures progress in completing actions based on controls that include key regulations and standards for data protection and governance.	○	○

Suggested Answer:

Statements	Yes	No
Enabling multi-factor authentication (MFA) increases the Microsoft Secure Score.	○	○
A higher Microsoft Secure Score means a lower identified risk level in the Microsoft 365 tenant.	○	○
Microsoft Secure Score measures progress in completing actions based on controls that include key regulations and standards for data protection and governance.	○	○

Statements	Yes	No
Enabling multi-factor authentication (MFA) increases the Microsoft Secure Score.	○	○
A higher Microsoft Secure Score means a lower identified risk level in the Microsoft 365 tenant.	○	○
Microsoft Secure Score measures progress in completing actions based on controls that include key regulations and standards for data protection and governance.	○	○

Box 1: Yes - Microsoft Secure Score has updated improvement actions to support security defaults in Azure Active Directory, which make it easier to help protect your organization with pre-configured security settings for common attacks. If you turn on security defaults, you'll be awarded full points for the following improvement actions: Ensure all users can complete multi-factor authentication for secure access (9 points) Require MFA for administrative roles (10 points) Enable policy to block legacy authentication (7 points)

Box 2: Yes - Each improvement action is worth 10 points or less, and most are scored in a binary fashion. If you implement the improvement action, like create a new policy or turn on a specific setting, you get 100% of the points. For other improvement actions, points are given as a percentage of the total configuration. Note: Following the Secure Score recommendations can protect your organization from threats. From a centralized dashboard in the Microsoft 365 Defender portal, organizations can monitor and work on the security of their Microsoft 365 identities, apps, and devices.

Box 3: Yes - Microsoft Secure Score is a measurement of an organization's security posture, with a higher number indicating more improvement actions taken. Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score

vorter Highly Voted 3 years, 11 months ago

Wouldn't #3 be no, because that's the compliance score, not Secure Score?

upvoted 60 times

darkpangel Highly Voted 3 years, 11 months ago

YYN. ompliance Manager gives you an initial score based on the Microsoft 365 data protection baseline. This baseline is a set of controls that includes key regulations and standards for data protection and general data governance. https://learn.microsoft.com/en-us/microsoft-365/compliance/compliance-score-calculation?view=o365-worldwide

upvoted 24 times

megan_poirier Most Recent 1 year ago

On exam today.

upvoted 1 times

AstroGreg 1 year, 4 months ago

A high secure score is not causal to a bad identified risk level. So I think answer two is NO actually.

upvoted 1 times

KoenJas 1 year, 5 months ago

I will never be back to check these answers, but you do have DLP policies recommended in the 'Secure Score' within Microsoft Defender. I know this because, at the MSP where I worked, I was responsible for upgrading the Secure Score for all our tenants to a minimum of 70%. I always had to create at least one DLP policy for the EU to improve the Secure Score. So, it's not just the Compliance Score that focuses on data.

upvoted 1 times

LegendaryZA 1 year, 10 months ago

The answer is Yes, Yes, No https://learn.microsoft.com/en-us/defender-xdr/microsoft-secure-score

upvoted 2 times

jg_85 2 years, 8 months ago

YYN 3 Should be No, because that's the compliance score, not the Secure Score

upvoted 3 times

RahulX 2 years, 11 months ago

Yes Yes NO

upvoted 2 times

Curious76 2 years, 11 months ago

YYN For #3 be No, because that's the compliance score, not the Secure Score

upvoted 4 times

jaaake 3 years, 1 month ago

YYN is correct. This is done by the Compliance Score

upvoted 3 times

manofsteel9 3 years, 2 months ago

#3 should be "N". Compliance Score, which is a separate feature in Microsoft 365, specifically focuses on assessing an organization's adherence to key regulations and standards for data protection and governance. Compliance Score evaluates actions and configurations related to compliance requirements, industry regulations, and data protection standards. It provides a score based on the completion of recommended actions related to compliance. You can access the Microsoft 365 Security documentation at: https://docs.microsoft.com/en-us/microsoft-365/security/ You can access the Microsoft 365 Compliance documentation at: https://docs.microsoft.com/en-us/microsoft-365/compliance/ These resources should provide you with comprehensive information about Microsoft Secure Score, Compliance Score, and their respective functionalities within the Microsoft 365 environment.

upvoted 5 times

Micha338el 3 years, 2 months ago

Security Center assessments have been mapped to compliance regulations, such that each applicable regulation control has some assessments associated with it. You can view your compliance relative to the supported controls of a regulation based on the passing vs. failing assessments that align with that regulation. As you remediate more assessments, your compliance posture improves.

upvoted 1 times

FiScorp_81 3 years, 6 months ago

Correct answer YYN 3# is the Compliance Score

upvoted 5 times

PinkUnicorns 3 years, 7 months ago

YYN - Please correct

upvoted 7 times

Charly0710 3 years, 7 months ago

queda entonces YYN

upvoted 3 times

walkaway 3 years, 7 months ago

3 is a NO. The hint is the regulation and standards in the statement. Compliance Manager gives you an initial score based on the Microsoft 365 data protection baseline. This baseline is a set of controls that includes key regulations and standards for data protection and general data governance.

upvoted 4 times

Ajkom 3 years, 9 months ago

YYN , https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/microsoft-secure-score-across-the-microsoft-security-stack/ba-p/1938977

upvoted 4 times

Question #28 *Topic 1*

What can you use to provide a user with a two-hour window to complete an administrative task in Azure?

A. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

B. Azure Multi-Factor Authentication (MFA)

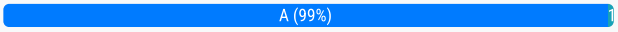
C. Azure Active Directory (Azure AD) Identity Protection

D. conditional access policies

Suggested Answer: *D*

Reference: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-policy-common

Community vote distribution



extrankie Highly Voted 5 years, 1 month ago

PIM is the correct answer A

upvoted 202 times

gills Highly Voted 5 years, 1 month ago

Provided answer is wrong. Should be A. https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure 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 Prevents removal of the last active Global Administrator role assignment

upvoted 99 times

eduardodiniz2020 Most Recent 11 months ago

PIM - Privileged Identity Management Eduardo.

upvoted 1 times

megan_poirier 1 year ago

On exam today

upvoted 1 times

LegendaryZA 1 year, 10 months ago

The answer is: Azure Active Directory (Azure AD) Privileged Identity Management (PIM) https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure

upvoted 2 times

tnttech 2 years ago

Azure PIM is correct

upvoted 1 times

Maqsoof 2 years, 4 months ago

D (Azure AD) Privileged Identity Management (PIM)

upvoted 1 times

cifofs 2 years, 4 months ago

The correct answer is D because to use PIM you must have Premium P2.

upvoted 1 times

AaronMedrano 2 years, 6 months ago

Should be A. https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure 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.

upvoted 1 times

mohamed.ali.elmasry 2 years, 7 months ago

PIM is the correct answer A

upvoted 1 times

frych 2 years, 8 months ago

PIM is correct for short time access

upvoted 1 times

Jeroenexams 2 years, 8 months ago

Answer A, PIM relates to the Azure tasks C seemsINcorrect becasue it saids POLICY, not control https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-session Conditional Access App Control enables user app access and sessions to be monitored and controlled in real time based on access and session policies. Access and session policies are used within the Defender for Cloud Apps portal to refine filters and set actions to take.

upvoted 1 times

chanc2023 2 years, 9 months ago

Most people vote for A and the answer provided by this site is D. So which one is the correct?

upvoted 1 times

geggio 2 years, 9 months ago

A right

upvoted 1 times

BrkyUlukn 2 years, 9 months ago

Correct answer is A: https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure 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 Prevents removal of the last active Global Administrator role assignment

upvoted 1 times

stewbiee 2 years, 10 months ago

PIM is the correct answer A

upvoted 2 times

xRiot007 2 years, 11 months ago

A - PIM because you give timed access

upvoted 3 times

Question #29 *Topic 1*

In a hybrid identity model, what can you use to sync identities between Active Directory Domain Services (AD DS) and Azure Active Directory (Azure AD)?

A. Active Directory Federation Services (AD FS)

B. Microsoft Sentinel

C. Azure AD Connect

D. Azure AD Privileged Identity Management (PIM)

Suggested Answer: *C*

Reference: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-azure-ad-connect

Community vote distribution

C (100%)

LegendaryZA Most Recent 1 year, 10 months ago

The answer is Azure AD Connect which is now called Microsoft Entra Connect https://learn.microsoft.com/en-us/entra/identity/hybrid/whatis-hybrid-identity

upvoted 2 times

frych 2 years, 8 months ago

AD Connect is called Entra Connect now

upvoted 3 times

fko8 2 years, 9 months ago

AD Connect now is called Entra Connect

upvoted 1 times

Tahamaffia 2 years, 11 months ago

Got this question on my exam 05/09/2023

upvoted 2 times

RahulX 2 years, 11 months ago

C. Azure AD Connect

upvoted 1 times

Crucius 2 years, 12 months ago

Correct.

upvoted 1 times

manofsteel9 3 years, 2 months ago

Correct answer

upvoted 2 times

RahulX 3 years, 5 months ago

Yes Correct Ans is Azure AD connect.

upvoted 2 times

Skillplayer 3 years, 6 months ago

Correct connect

upvoted 1 times

Lizzylizzy 3 years, 8 months ago

Azure AD connect

upvoted 2 times

Mcelona 3 years, 8 months ago

C is Correct

upvoted 4 times

FBrabble 3 years, 9 months ago

C correct

upvoted 3 times

ruank 3 years, 10 months ago

Correct

upvoted 4 times

Derag 3 years, 11 months ago

Azure AD Connect Sync Server, therefore, the answer is correct.

upvoted 3 times

Zeus009 3 years, 11 months ago

Correct

upvoted 3 times

Question #30 *Topic 1*

HOTSPOT -
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

Statements	Yes	No
You can create custom roles in Azure Active Directory (Azure AD).	○	○
Global administrator is a role in Azure Active Directory (Azure AD).	○	○
An Azure Active Directory (Azure AD) user can be assigned only one role.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
You can create custom roles in Azure Active Directory (Azure AD).	○	○
Global administrator is a role in Azure Active Directory (Azure AD).	○	○
An Azure Active Directory (Azure AD) user can be assigned only one role.	○	○

Answer Area

Statements	Yes	No
You can create custom roles in Azure Active Directory (Azure AD).	○	○
Global administrator is a role in Azure Active Directory (Azure AD).	○	○
An Azure Active Directory (Azure AD) user can be assigned only one role.	○	○

Box 1: Yes - Azure AD supports custom roles.

Box 2: Yes - Global Administrator has access to all administrative features in Azure Active Directory.

Box 3: No - Reference: https://docs.microsoft.com/en-us/azure/active-directory/roles/concept-understand-roles
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

Melwin86 Highly Voted 5 years, 1 month ago
correct 1. https://docs.microsoft.com/en-us/azure/active-directory/roles/custom-create 2,3 https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference
upvoted 36 times

cantbeme Highly Voted 3 years, 12 months ago
on exam today
upvoted 11 times

Aashish1279 Most Recent 1 year, 4 months ago

The answer is Yes, Yes, No

upvoted 1 times

LegendaryZA 1 year, 10 months ago

The answer is: Yes, Yes, No https://docs.microsoft.com/en-us/azure/active-directory/roles/custom-create https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

upvoted 1 times

geggio 2 years, 9 months ago

y-y-n right

upvoted 1 times

bigelmo_elmo 3 years, 1 month ago

This is a question from AZ-900 exam as well

upvoted 1 times

RahulX 3 years, 5 months ago

Yes Yes No

upvoted 4 times

Nicochet 3 years, 6 months ago

Y,Y,N is the correct answer

upvoted 2 times

Mcelona 3 years, 8 months ago

Y,Y,N is the answer

upvoted 3 times

FBrabble 3 years, 9 months ago

Y, Y, N is correct for sure

upvoted 4 times

IXone 3 years, 10 months ago

Correct

upvoted 3 times

Zeus009 3 years, 11 months ago

Aligned

upvoted 3 times

AdityaGupta 4 years ago

YYN is correct, multiple roles can be assigned to any user, including custom roles.

upvoted 3 times

l3ul3u 4 years, 1 month ago

Correct

upvoted 2 times

idhashi 4 years, 3 months ago

Correct

upvoted 2 times

Tommo 4 years, 4 months ago

Correct

upvoted 2 times

Question #31 *Topic 1*

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Azure Active Directory (Azure AD) is deployed to an on-premises environment.	○	○
Azure Active Directory (Azure AD) is provided as part of a Microsoft 365 subscription.	○	○
Azure Active Directory (Azure AD) is an identity and access management service.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
Azure Active Directory (Azure AD) is deployed to an on-premises environment.	○	○
Azure Active Directory (Azure AD) is provided as part of a Microsoft 365 subscription.	○	○
Azure Active Directory (Azure AD) is an identity and access management service.	○	○

Answer Area

Statements	Yes	No
Azure Active Directory (Azure AD) is deployed to an on-premises environment.	○	○
Azure Active Directory (Azure AD) is provided as part of a Microsoft 365 subscription.	○	○
Azure Active Directory (Azure AD) is an identity and access management service.	○	○

Box 1: No - Azure Active Directory (Azure AD) is a cloud-based user identity and authentication service.

Box 2: Yes - Microsoft 365 uses Azure Active Directory (Azure AD). Azure Active Directory (Azure AD) is included with your Microsoft 365 subscription.

Box 3: Yes - Azure Active Directory (Azure AD) is a cloud-based user identity and authentication service. Reference: https://docs.microsoft.com/en-us/microsoft-365/enterprise/about-microsoft-365-identity?view=o365-worldwide

gchauhanebay Highly Voted 4 years, 12 months ago

Correct is False True True

upvoted 38 times

dynamicJames Highly Voted 4 years, 12 months ago

Guys, of course you need/get an Azure AD when you license/buy a M365 tenant. Whenever you create Users via the admin.microsoft.com page, the users are created in the AAD "above".

So I go with: False True True

upvoted 19 times

dynamicJames 4 years, 12 months ago

Guys, of course you need/get an Azure AD when you license/buy a M365 tenant. Whenever you create Users via the admin.microsoft.com page, the users are created in the AAD "above". So I go with: False True Trueagreed

upvoted 19 times

faricity 4 years, 9 months ago

agreed

upvoted 2 times

LegendaryZA Most Recent 1 year, 10 months ago

The answer is No, Yes, Yes https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/cloud-governed-management-for-on-premises

upvoted 2 times

Girlgonecyber 2 years, 1 month ago

Azure AD is now Entra ID. T

upvoted 1 times

RahulX 2 years, 11 months ago

NO YES YES

upvoted 1 times

manofsteel9 3 years, 2 months ago

The answer is F,T,T Azure AD serves as the cloud-based identity and access management solution for Microsoft 365. It enables organizations to manage user identities, control access to resources, and secure applications and data in the Microsoft 365 environment. Azure AD is tightly integrated with Microsoft 365 services and provides the foundation for authentication and authorization across the suite of Microsoft cloud services. You can access the Microsoft 365 documentation at: URL: https://docs.microsoft.com/en-us/microsoft-365/

upvoted 1 times

abilioneto 3 years, 10 months ago

My guess is NYY

upvoted 7 times

smartin2010 3 years, 10 months ago

NYY, is correct.

upvoted 4 times

cantbeme 3 years, 12 months ago

on exam today

upvoted 4 times

AdityaGupta 4 years ago

NYY, is correct.

upvoted 2 times

cormorant 4 years, 1 month ago

azure AD is deployed to a cloud environment

upvoted 3 times

bharatpatoliya 4 years, 3 months ago

No, YES, YES..

upvoted 3 times

Tommo 4 years, 4 months ago

Correct

upvoted 1 times

BlackdaRipper 4 years, 5 months ago

NO YES YES is the answer

upvoted 3 times

G_unit_19 4 years, 6 months ago

N,Y,Y is correct

upvoted 2 times

Ronald88 4 years, 8 months ago

Correct false true true

upvoted 2 times

Adil251 4 years, 8 months ago

CORRECT

upvoted 2 times

Question #32 *Topic 1*

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

With Windows Hello for Business, a user's biometric data used for authentication [ ]

- is stored on an external device.
- is stored on a local device only.
- is stored in Azure Active Directory (Azure AD).
- is replaced to all the devices designated by the user.

Suggested Answer:

Answer Area

With Windows Hello for Business, a user's biometric data used for authentication [ ]

- is stored on an external device.
- **is stored on a local device only.**
- is stored in Azure Active Directory (Azure AD).
- is replicated to all the devices designated by the user.

Answer Area

With Windows Hello for Business, a user's biometric data used for authentication [ ]

- is stored on an external device.
- **is stored on a local device only.**
- is stored in Azure Active Directory (Azure AD).
- is replicated to all the devices designated by the user.

Biometrics templates are stored locally on a device. Reference: https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview

Jebli071 Highly Voted 4 years, 8 months ago

Correct !

upvoted 25 times

draadloos1973 Highly Voted 4 years, 5 months ago

Correct, data is stored in the tpm chip

upvoted 14 times

draadloos1973 4 years, 5 months ago

Correct, data is stored in the tpm chipI can't find where it says the biometric data is stored on the tpm chip. Are you sure?The thing that is saved on the TPM chip (if present) is the secure key. If a TPM chip is not available, software-based techniques are used to secure the key. (see https://learn.microsoft.com/en-us/windows/security/information-protection/tpm/how-windows-uses-the-tpm#windows-hello-for-business) I also couldn't find a source that explains where specifically the biometric data is stored. Microsoft just says, "on the device": https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-faq#where-is-windows-hello-biometrics-data-stored

upvoted 14 times

Lipseal 4 years, 2 months ago

I can't find where it says the biometric data is stored on the tpm chip. Are you sure?The thing that is saved on the TPM chip (if present) is the secure key. If a TPM chip is not available, software-based techniques are used to secure the key. (see https://learn.microsoft.com/en-us/windows/security/information-protection/tpm/how-windows-uses-the-tpm#windows-hello-for-business) I also couldn't find a source that explains where specifically the biometric data is stored. Microsoft just says, "on the device": https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-faq#where-is-windows-hello-biometrics-data-stored

upvoted 1 times

Lipseal 4 years, 2 months ago

I can't find where it says the biometric data is stored on the tpm chip. Are you sure?

upvoted 1 times

OG_Diablo 3 years, 8 months ago

The thing that is saved on the TPM chip (if present) is the secure key. If a TPM chip is not available, software-based techniques are used to secure the key. (see https://learn.microsoft.com/en-us/windows/security/information-protection/tpm/how-windows-uses-the-tpm#windows-hello-for-business) I

also couldn't find a source that explains where specifically the biometric data is stored. Microsoft just says, "on the device": https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-faq#where-is-windows-hello-biometrics-data-stored

upvoted 4 times

LegendaryZA Most Recent 1 year, 10 months ago

The answer is: is stored on a local device only https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/how-it-works

upvoted 1 times

DK21Dilip 2 years ago

this question came in july 2024

upvoted 2 times

Tahamaffia 2 years, 11 months ago

Got this question on my exam 05/09/2023

upvoted 4 times

RahulX 2 years, 11 months ago

With Windows Hello for Business, as user's biometric data used for authentication is stored on a local device only.

upvoted 1 times

furq2904 3 years, 1 month ago

appeared on July 1st 2023

upvoted 1 times

RahulX 3 years, 5 months ago

Is Stored in local Device Only.

upvoted 2 times

Nicochet 3 years, 6 months ago

Only in local device

upvoted 1 times

Lizzylizzy 3 years, 8 months ago

Stored on a local device

upvoted 1 times

abilioneto 3 years, 10 months ago

Correct

upvoted 3 times

Zeus009 3 years, 11 months ago

Aligned

upvoted 2 times

AdityaGupta 4 years ago

Correct, data is stored locally.

upvoted 3 times

johnegil 4 years, 1 month ago

Appeared on exam 12/07/2022

upvoted 5 times

Yelad 4 years, 1 month ago

On the exam 10/07/2022

upvoted 4 times

Olakunle24 4 years, 3 months ago

The Windows Hello authenticator works to authenticate and allow employees onto your enterprise network. Authentication doesn't roam among devices, isn't shared with a server, and can't easily be extracted from a device. If multiple employees share a device, each employee will use his or her own biometric data on the device. https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-biometrics-in-enterpriseHere is the statement from your link: The biometric data used to support Windows Hello is stored on the local device only. It doesn't roam and is never sent to external devices or servers.

upvoted 4 times

Olakunle24 4 years, 3 months ago

The Windows Hello authenticator works to authenticate and allow employees onto your enterprise network. Authentication doesn't roam among devices, isn't shared with a server, and can't easily be extracted from a device. If multiple employees share a device, each employee will use his or her own biometric data on the device.

https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-biometrics-in-enterprise

upvoted 4 times

imjoe 4 years, 2 months ago

Here is the statement from your link: The biometric data used to support Windows Hello is stored on the local device only. It doesn't roam and is never sent to external devices or servers.

upvoted 2 times

BlackdaRipper 4 years, 5 months ago

CORRECT ANSWER

upvoted 3 times

Question #33 *Topic 1*

What is the purpose of Azure Active Directory (Azure AD) Password Protection?

A. to control how often users must change their passwords

B. to identify devices to which users can sign in without using multi-factor authentication (MFA)

C. to encrypt a password by using globally recognized encryption standards

D. to prevent users from using specific words in their passwords

Suggested Answer: *D*

Azure AD Password Protection detects and blocks known weak passwords and their variants, and can also block additional weak terms that are specific to your organization. With Azure AD Password Protection, default global banned password lists are automatically applied to all users in an Azure AD tenant. To support your own business and security needs, you can define entries in a custom banned password list. Reference: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad-on-premises

Community vote distribution



Melwin86 Highly Voted 5 years, 1 month ago

correct https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad

upvoted 32 times

jjrodriguezbriz Highly Voted 4 years, 5 months ago

Correct

upvoted 13 times

megan_poirier Most Recent 1 year ago

On exam today.

upvoted 1 times

LegendaryZA 1 year, 10 months ago

The answer is: to prevent users from using specific words in their passwords. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-password-ban-bad

upvoted 1 times

JasekoCL 2 years, 2 months ago

Microsoft Entra Password Protection detects and blocks known weak passwords and their variants, and can also block additional weak terms that are specific to your organization. Article 02/12/2024 https://learn.microsoft.com/en-us/entra/identity/authentication/concept-password-ban-bad-on-premises

upvoted 1 times

Peace4ever 2 years, 9 months ago

I just passed my exam today, and this was one of the questions. To prevent users from using specific words in their passwords

upvoted 2 times

RahulX 2 years, 11 months ago

D. to prevent users from using specific words in their passwords

upvoted 1 times

Nemish71 2 years, 11 months ago

correct

upvoted 1 times

furq2904 3 years, 1 month ago

appeared on July 1st 2023, options were shuffled

upvoted 1 times

XtraWest 3 years, 4 months ago

The purpose of Azure Active Directory (Azure AD) Password Protection is to help prevent common passwords and weak passwords from being used in Azure AD.

upvoted 2 times

MeisAdriano 3 years, 4 months ago

why not A too?

upvoted 1 times

RahulX 3 years, 5 months ago

D is correct ans.

upvoted 1 times

Nicochet 3 years, 6 months ago

Correct

upvoted 1 times

mitchduck 3 years, 8 months ago

Correct

upvoted 2 times

Juliandres5845 3 years, 10 months ago

Correct

upvoted 2 times

abilioneto 3 years, 10 months ago

correct

upvoted 2 times

Emmuyah 3 years, 10 months ago

Correct

upvoted 1 times

Question #34 *Topic 1*

Which Azure Active Directory (Azure AD) feature can you use to evaluate group membership and automatically remove users that no longer require membership in a group?

A. access reviews

B. managed identities

C. conditional access policies

D. Azure AD Identity Protection

Suggested Answer: *A*
Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. Reference: https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

Community vote distribution
A (100%)

Melwin86 Highly Voted 5 years, 1 month ago
correct https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview
upvoted 37 times

Whyiest Highly Voted 3 years, 6 months ago
Why there is no "dynamics groups" in the option ? I think it's an error :

Dynamic groups are used to automate the management of Azure Active Directory (AAD) group membership. They allow you to define rules to automatically add or remove users from a group based on certain criteria such as their job title or department.

Access reviews, on the other hand, are used to periodically review the access permissions of users to Azure resources. They allow you to identify and revoke unnecessary access, ensuring that only the right people have the right level of access to your resources. Access reviews can be done on role assignments, group memberships, and application assignments.

In summary, Dynamic groups are used to automatically manage group membership in AAD, while access reviews are used to periodically review and revoke unnecessary access to Azure resources, so here it must be Dynamic Groups or maybe I'm wrong ?
upvoted 5 times

Whyiest 3 years, 6 months ago
Why there is no "dynamics groups" in the option ? I think it's an error : Dynamic groups are used to automate the management of Azure Active Directory (AAD) group membership. They allow you to define rules to automatically add or remove users from a group based on certain criteria such as their job title or department. Access reviews, on the other hand, are used to periodically review the access permissions of users to Azure resources. They allow you to identify and revoke unnecessary access, ensuring that only the right people have the right level of access to your resources. Access reviews can be done on role assignments, group memberships, and application assignments. In summary, Dynamic groups are used to automatically manage group membership in AAD, while access reviews are used to periodically review and revoke unnecessary access to Azure resources, so here it must be Dynamic Groups or maybe I'm wrong ?You're overthinking it. The key word in this question is "evaluate". You are given the option to set up recurring reviews and apply the decisions "automatically". Check out this video and look at the slide around the 1:30 mark. https://youtu.be/kDRjQQ22Wkk
upvoted 5 times

Barbados 3 years, 6 months ago
You're overthinking it. The key word in this question is "evaluate". You are given the option to set up recurring reviews and apply the decisions "automatically". Check out this video and look at the slide around the 1:30 mark. https://youtu.be/kDRjQQ22Wkk
upvoted 5 times

LegendaryZA Most Recent 1 year, 10 months ago
The answer is: access reviews https://learn.microsoft.com/en-us/entra/id-governance/access-reviews-overview
upvoted 2 times

PC75 2 years, 10 months ago
Correct.

upvoted 1 times

RahulX 2 years, 11 months ago

A. access reviews

upvoted 1 times

manofsteel9 3 years, 2 months ago

A-Correct answer

upvoted 1 times

nobrainatall 3 years, 6 months ago

as suggested by Barbados https://youtu.be/kDRjQQ22Wkk

upvoted 1 times

Lizzylizzy 3 years, 8 months ago

Access review is the correct answer

upvoted 1 times

dd9396 3 years, 8 months ago

A is correct, When the review is complete, access reviews can be set to manually or automatically remove access from the group membership or application assignment except for a dynamic group or originates from on-premises AD.

upvoted 2 times

InformacionFalsa 3 years, 8 months ago

That would be wrong. Dynamic groups are the ones that do it AUTOMATICALLY. If that word wouldn't appear, then the right answer would be "A"

upvoted 1 times

mitchduck 3 years, 8 months ago

A is correct

upvoted 2 times

Lone__Wolf 3 years, 10 months ago

KEYWORD evaluate:review Answer is A

upvoted 3 times

abilioneto 3 years, 10 months ago

correct

upvoted 1 times

Zeus009 3 years, 11 months ago

correct

upvoted 2 times

cantbeme 3 years, 12 months ago

on exam today

upvoted 2 times

cormorant 4 years, 1 month ago

ACCESS reviews - remove ACCESS rights

upvoted 1 times

Ravikant84 4 years, 1 month ago

Correct

upvoted 2 times

Question #35 *Topic 1*

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

Multi-factor authentication (MFA)	requires additional verification, such as a verification code sent to a mobile phone.
Pass-through authentication	
Password writeback	
Single sign-on (SSO)	

Suggested Answer:

Answer Area

Multi-factor authentication (MFA)	requires additional verification, such as a verification code sent to a mobile phone.
Pass-through authentication	
Password writeback	
Single sign-on (SSO)	

Answer Area

Multi-factor authentication (MFA)	requires additional verification, such as a verification code sent to a mobile phone.
Pass-through authentication	
Password writeback	
Single sign-on (SSO)	

Multi-factor authentication is a process where a user is prompted during the sign-in process for an additional form of identification, such as to enter a code on their cellphone or to provide a fingerprint scan. Reference: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks

Emmanski08 Highly Voted 4 years ago

if you don't know this you shouldn't be taking the exam

upvoted 38 times

Melwin86 Highly Voted 5 years, 1 month ago

correct https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa

upvoted 21 times

megan_poirier Most Recent 1 year ago

Correct answer, on exam today.

upvoted 1 times

LegendaryZA 1 year, 10 months ago

The answer is: Multi-factor authentication https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mfa-howitworks

upvoted 1 times

Peace4ever 2 years, 9 months ago

I just passed my exam today, and this was one of the questions: MFA.

upvoted 2 times

RahulX 2 years, 11 months ago

Multi-factor authentication (MFA)

upvoted 1 times

manofsteel9 3 years, 2 months ago

Correct

upvoted 1 times

RahulX 3 years, 5 months ago

MFA is correct ans.

upvoted 2 times

Zeus009 3 years, 11 months ago

Correct

upvoted 1 times

Tommo 4 years, 4 months ago

CORRECT

upvoted 1 times

bikewun 4 years, 5 months ago

CORRECT

upvoted 1 times

BlackdaRipper 4 years, 5 months ago

MFA IS CORRECT

upvoted 1 times

Moddybaba 4 years, 5 months ago

Correct answer selected (MFA)

upvoted 1 times

qdam 4 years, 7 months ago

correct answer

upvoted 3 times

Ronald88 4 years, 8 months ago

Correct MFA

upvoted 2 times

Jitusrit 4 years, 9 months ago

Correct ...mda response can be done via call, sms code, and auth app

upvoted 2 times

DALGMCI 4 years, 9 months ago

correct!

upvoted 2 times

Question #36 *Topic 1*

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Conditional access policies can use the device state as a signal.	○	○
Conditional access policies apply before first-factor authentication is complete.	○	○
Conditional access policies can trigger multi-factor authentication (MFA) if a user attempts to access a specific application.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
Conditional access policies can use the device state as a signal.	○	○
Conditional access policies apply before first-factor authentication is complete.	○	○
Conditional access policies can trigger multi-factor authentication (MFA) if a user attempts to access a specific application.	○	○

Answer Area

Statements	Yes	No
Conditional access policies can use the device state as a signal.	○	○
Conditional access policies apply before first-factor authentication is complete.	○	○
Conditional access policies can trigger multi-factor authentication (MFA) if a user attempts to access a specific application.	○	○

Box 1: Yes -

Box 2: No - Conditional Access policies are enforced after first-factor authentication is completed.

Box 3: Yes - Reference: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

Melwin86 Highly Voted 5 years, 1 month ago

correct https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-policies

upvoted 37 times

yonie Highly Voted 3 years, 8 months ago

Question needs to be updated: Device state (deprecated) This preview feature has been deprecated. Customers should use the Filter for devices condition in the Conditional Access policy, to satisfy scenarios previously achieved using device state (preview) condition.

https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions#device-state-deprecated
upvoted 7 times

LegendaryZA Most Recent 1 year, 10 months ago
The answer is Yes, No, Yes https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-policies
upvoted 1 times

rodrigoisalino 2 years, 2 months ago
The question appeared in my exam today, 06/2024.
upvoted 2 times

user_666 2 years, 6 months ago
had this question on my exam today (01 feb 2024)
upvoted 2 times

RahulX 2 years, 11 months ago
YES NO YES
upvoted 2 times

Kelsi999 3 years, 3 months ago
The answer is correct. I had this question on the exam today
upvoted 5 times

Whyiest 3 years, 6 months ago
YNY Correct
upvoted 5 times

cris_exam 3 years, 7 months ago
YNY is correct.
upvoted 4 times

OG_Diablo 3 years, 8 months ago
The answers are sort of correct. 'Device state' has since been deprecated. You can use 'Filter for devices' to achieve the same results (and much more). https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions#device-state-deprecated
upvoted 4 times

mikcs 3 years, 8 months ago
on exam 12/12/22
upvoted 3 times

Mcelona 3 years, 8 months ago
Correct
upvoted 1 times

IXone 3 years, 10 months ago
Correct
upvoted 3 times

abilioneto 3 years, 10 months ago
My guess is YNY
upvoted 2 times

AdityaGupta 4 years ago
Answer is correct: YNY
upvoted 1 times

GetulioJr 4 years ago
Answer is correct: YNY
upvoted 2 times

Yelad 4 years, 1 month ago
On the exam 10/07/2022
upvoted 4 times

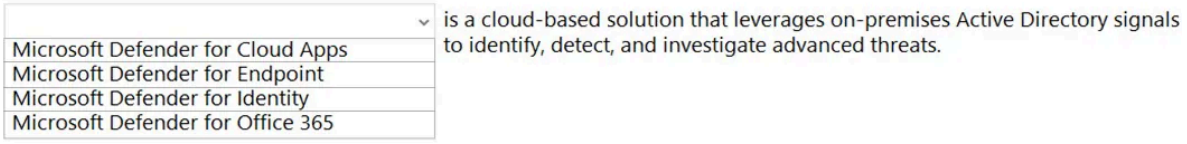
Question #37 *Topic 1*

HOTSPOT -

Select the answer that correctly completes the sentence.

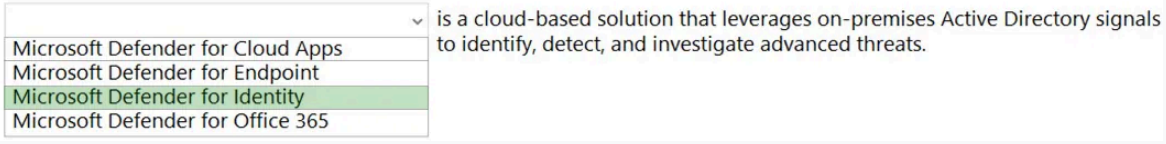
Hot Area:

Answer Area

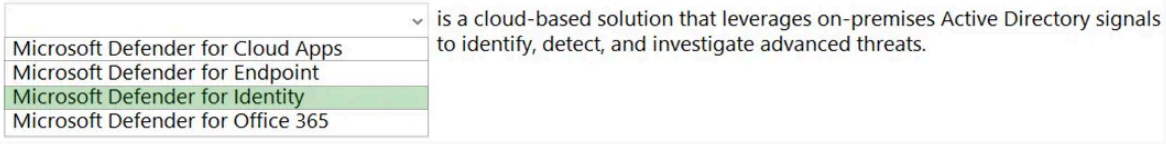


Suggested Answer:

Answer Area



Answer Area



Reference: https://docs.microsoft.com/en-us/defender-for-identity/what-is

RamazanInce Highly Voted 4 years, 10 months ago

Microsoft Defender for Identity is a cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

upvoted 45 times

Melwin86 Highly Voted 5 years, 1 month ago

correct https://docs.microsoft.com/en-us/defender-for-identity/what-is

upvoted 32 times

LegendaryZA Most Recent 1 year, 10 months ago

The answer is: Microsoft Defender for Identity https://learn.microsoft.com/en-us/defender-for-identity/what-is

upvoted 2 times

DK21Dilip 2 years ago

this question came in july 2024

upvoted 3 times

rodrigoisalino 2 years, 2 months ago

The question appeared in my exam today, 06/2024.

upvoted 2 times

Ramye 2 years, 8 months ago

Given answer is correct. Defender for Identity is fully integrated with Microsoft Defender XDR, and leverages signals from both on-premises Active Directory and cloud identities to help you better identify, detect, and investigate advanced threats directed at your organization. Source: https://learn.microsoft.com/en-us/defender-for-identity/what-is

upvoted 1 times

RahulX 2 years, 11 months ago

Microsoft Defender for Identity

upvoted 1 times

Drinn 3 years, 4 months ago

Keyword is Identity
upvoted 3 times

IXone 3 years, 10 months ago
Correct
upvoted 5 times

cormorant 4 years, 1 month ago
Microsoft Defender for IDENTITY (formerly Azure Advanced Threat Protection, also known as Azure ATP) is a cloud-based security solution that leverages your on-premises Active Directory signals to IDENTIFY, detect, and investigate advanced threats, compromised IDENTITIES, and malicious insider actions directed at your organization. https://docs.microsoft.com/en-us/defender-for-identity/what-is
upvoted 10 times

johnegil 4 years, 1 month ago
Appeared on exam 12/07/2022
upvoted 6 times

Yelad 4 years, 1 month ago
On the exam 10/07/2022
upvoted 4 times

jimmysplash 4 years, 2 months ago
correct actice directory-identity
upvoted 2 times

tnagy 4 years, 3 months ago
Wrong Answer. The answer is Microsoft Defender for End Point.

"Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats."

The question is not asking about "Compromised Identities" or threats related to Identities in specific. So the answer is NOT MD for Identity.
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide
upvoted 5 times

tnagy 4 years, 3 months ago
Wrong Answer. The answer is Microsoft Defender for End Point. "Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats." The question is not asking about "Compromised Identities" or threats related to Identities in specific. So the answer is NOT MD for Identity. https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwideHow does MDE leverage onpremise active directory signals??? Furthermore it says identify, detect and investiagte. MDE would als be able to respond. So MDI is the correct answerwrong. It should be MDI. MDI topic is also on sc200.
upvoted 5 times

yaza85 4 years, 3 months ago
How does MDE leverage onpremise active directory signals??? Furthermore it says identify, detect and investiagte. MDE would als be able to respond. So MDI is the correct answer
upvoted 4 times

sasasach 3 years, 10 months ago
wrong. It should be MDI. MDI topic is also on sc200.
upvoted 1 times

Clouddog 4 years, 4 months ago
Provided answer is correct: Microsoft Defender for Identity (formerly Azure Advanced Threat Protection, also known as Azure ATP) is a cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization
upvoted 6 times

Jebli071 4 years, 8 months ago
Correct answer and refference !
upvoted 3 times

Jitusrit 4 years, 9 months ago
Absolutely correct..
upvoted 2 times

Question #38 *Topic 1*

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

Microsoft Defender for Identity can identify advanced threats from [ ] signals.

- Azure Active Directory (Azure AD)
- Azure AD Connect
- on-premises Active Directory Domain Services (AD DS)

Suggested Answer:

Answer Area

Microsoft Defender for Identity can identify advanced threats from [on-premises Active Directory Domain Services (AD DS)] signals.

Answer Area

Microsoft Defender for Identity can identify advanced threats from [on-premises Active Directory Domain Services (AD DS)] signals.

Microsoft Defender for Identity is a cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization. Reference: https://docs.microsoft.com/en-us/defender-for-identity/what-is

Melwin86 Highly Voted 5 years, 1 month ago

correct https://docs.microsoft.com/en-us/defender-for-identity/what-is

upvoted 24 times

johnegil Highly Voted 4 years, 1 month ago

Appeared on exam 12/07/2022

upvoted 11 times

LegendaryZA Most Recent 1 year, 10 months ago

The answer is: on-premises Active Directory Domain Services (AD DS) https://learn.microsoft.com/en-us/defender-for-identity/what-is

upvoted 1 times

f0xy 1 year, 11 months ago

Nowadays it's for both on-prem and cloud: "Defender for Identity is fully integrated with Microsoft Defender XDR, and leverages signals from both on-premises Active Directory and cloud identities "

upvoted 3 times

clementious 2 years ago

ADVANCED THREATS IS THHE KEY WORD

upvoted 1 times

rodrigoisalino 2 years, 2 months ago

The question appeared in my exam today, 06/2024.

upvoted 2 times

user_666 2 years, 6 months ago

had this question on my exam today (01 feb 2024)

upvoted 3 times

RahulX 2 years, 11 months ago

Microsoft Defender for Identity can identify advanced threats from on-premises active directory domain services.

upvoted 1 times

Kelsi999 3 years, 3 months ago

Correct On the exam today

upvoted 2 times

Nicochet 3 years, 6 months ago

Correct

upvoted 4 times

mikcs 3 years, 8 months ago

on exam 12/12/22

upvoted 2 times

abilioneto 3 years, 10 months ago

correct

upvoted 2 times

smartin2010 3 years, 10 months ago

correct

upvoted 1 times

Tommo 4 years, 4 months ago

correct

upvoted 1 times

Clouddog 4 years, 4 months ago

Provided answer is correct: Defender for Identity protects the AD FS in your environment by detecting on-premises attacks on the AD FS and providing visibility into authentication events generated by the AD FS.

upvoted 5 times

Alessandro_L 4 years, 6 months ago

Correct

upvoted 3 times

Adil251 4 years, 8 months ago

CORRECT

upvoted 5 times

Question #39 *Topic 1*

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

Azure Active Directory (Azure AD) is [ ] used for authentication and authorization.

- an extended detection and response (XDR) system
- an identity provider
- a management group
- a security information and event management (SIEM) system

Suggested Answer:

Answer Area

Azure Active Directory (Azure AD) is [an identity provider] used for authentication and authorization.

- an extended detection and response (XDR) system
- an identity provider
- a management group
- a security information and event management (SIEM) system

Answer Area

Azure Active Directory (Azure AD) is [an identity provider] used for authentication and authorization.

- an extended detection and response (XDR) system
- an identity provider
- a management group
- a security information and event management (SIEM) system

Azure Active Directory (Azure AD) is a cloud-based user identity and authentication service. Reference: https://docs.microsoft.com/en-us/microsoft-365/enterprise/about-microsoft-365-identity?view=o365-worldwide

Mk1331 Highly Voted 5 years ago

Correct answer

upvoted 30 times

Melwin86 Highly Voted 5 years, 1 month ago

correct https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis

upvoted 21 times

LegendaryZA Most Recent 1 year, 10 months ago

The answer is: an identity provider https://learn.microsoft.com/en-us/entra/fundamentals/whatis

upvoted 1 times

RahulX 2 years, 11 months ago

Azure AD is an identity provider used for authentication and authorization.

upvoted 1 times

Whyiest 3 years, 7 months ago

It's the right answer

upvoted 3 times

abilioneto 3 years, 10 months ago

correct

upvoted 4 times

Emmuyah 3 years, 10 months ago

Correct Answer

upvoted 2 times

cantbeme 3 years, 12 months ago

on exam today

upvoted 2 times

andion 4 years ago

An identity provider

upvoted 2 times

cormorant 4 years, 1 month ago

Active directory is an identity provider to grant users the access rights according to their assigned roles

upvoted 1 times

Tommo 4 years, 4 months ago

correct

upvoted 2 times

Alessandro_L 4 years, 6 months ago

Correct!

upvoted 2 times

Jitusrit 4 years, 9 months ago

AAD IS cloud based identity provider..

upvoted 1 times

GuruPandian 5 years ago

Correct

upvoted 2 times

P_2311 5 years ago

correct

upvoted 2 times

Question #40 *Topic 1*

Which Azure Active Directory (Azure AD) feature can you use to provide just-in-time (JIT) access to manage Azure resources?

A. conditional access policies

B. Azure AD Identity Protection

C. Azure AD Privileged Identity Management (PIM)

D. authentication method policies

Suggested Answer: *C*

Azure AD Privileged Identity Management (PIM) provides just-in-time privileged access to Azure AD and Azure resources Reference: https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

Community vote distribution

C (100%)

Matic_Prime Highly Voted 5 years ago

correct

upvoted 22 times

OlaCharles Highly Voted 4 years, 11 months ago

I agree. PIM is used for Just In Time and Just Enough Access

upvoted 12 times

LegendaryZA Most Recent 1 year, 10 months ago

The answer is: Azure AD Privileged Identity Management (PIM) https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure

upvoted 2 times

shahmitu 2 years, 11 months ago

Correct!

upvoted 1 times

RahulX 2 years, 11 months ago

C. Azure AD Privileged Identity Management (PIM)

upvoted 1 times

furq2904 3 years, 1 month ago

appeared on July 1st 2023

upvoted 1 times

manofsteel9 3 years, 2 months ago

Correct Answer.

upvoted 1 times

obaali1990 3 years, 5 months ago

I wrote today Feb 24, 2023. I had 976/1000. This site is great

upvoted 9 times

RahulX 3 years, 5 months ago

PIM is correct ans.

upvoted 1 times

nobrainatall 3 years, 6 months ago

that's exactly is what PIM does

upvoted 1 times

Nicochet 3 years, 6 months ago

PIM correct

upvoted 1 times

Whyiest 3 years, 7 months ago

It's the correct answer. See : https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

upvoted 2 times

Rahul9802 3 years, 7 months ago

Correct Answer is PIM .....

upvoted 2 times

jcabello7 3 years, 8 months ago

PIM is the correct answer

upvoted 1 times

abilioneto 3 years, 10 months ago

correct

upvoted 2 times

andion 4 years ago

Hi, please how to make difference between PIM and PAM?

upvoted 2 times

AdityaGupta 4 years ago

C. Azure AD Privileged Identity Management (PIM)

upvoted 2 times

Question #41 *Topic 1*

Which three authentication methods can be used by Azure Multi-Factor Authentication (MFA)? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. text message (SMS)

B. Microsoft Authenticator app

C. email verification

D. phone call

E. security question

Suggested Answer: *A, B, D*
Reference: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods

Community vote distribution
ABD (94%)

Jillis Highly Voted 4 years, 12 months ago
Correct
upvoted 30 times

HK010 Highly Voted 4 years, 4 months ago
Available verification methods When users sign in to an application or service and receive an MFA prompt, they can choose from one of their registered forms of additional verification. Users can access My Profile to edit or add verification methods. The following additional forms of verification can be used with Azure AD Multi-Factor Authentication: Microsoft Authenticator app Windows Hello for Business FIDO2 security key OATH hardware token (preview) OATH software token SMS Voice call https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks
upvoted 23 times

LegendaryZA Most Recent 1 year, 10 months ago
The answers are: text message (SMS) Microsoft Authenticator App phone call https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-methods
upvoted 1 times

rodrigoisalino 2 years, 2 months ago
The question appeared in my exam today, 06/2024.
upvoted 4 times

lllaadsf 2 years, 11 months ago
correct
upvoted 1 times

Tahamaffia 2 years, 11 months ago
Got this question on my exam 05/09/2023
upvoted 1 times

RahulX 2 years, 11 months ago
A. text message (SMS) B. Microsoft Authenticator app D. phone call
upvoted 1 times

Crucius 2 years, 12 months ago
Correct.
upvoted 1 times

User1208 3 years, 2 months ago
I agree the answer can be verified with the Learning materials, but in reality, I do set up my personal email as a component of the MFA for my working email. Is that empowered by other tech?
upvoted 3 times

studytonight 3 years, 2 months ago
This was on the May 2023 exam.
upvoted 1 times

Nicochet 3 years, 6 months ago

Correct

upvoted 1 times

ehallak 3 years, 6 months ago

Correct. For more details: https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks

upvoted 2 times

Whyiest 3 years, 6 months ago

Azure AD Multi-Factor Authentication supports : - Microsoft Authenticator app - Windows Hello for Business - FIDO2 security key - OATH hardware token (preview) - OATH software token - SMS - Voice call

upvoted 2 times

2cent2 3 years, 7 months ago

verfied via the given links.

upvoted 2 times

Lizzylizzy 3 years, 8 months ago

Mfa does not include email and security questions

upvoted 2 times

Mcelona 3 years, 8 months ago

A,B,D is the answer

upvoted 3 times

IXone 3 years, 10 months ago

Correct

upvoted 1 times

Question #42 *Topic 1*

Which Microsoft 365 feature can you use to restrict communication and the sharing of information between members of two departments at your organization?

A. sensitivity label policies

B. Customer Lockbox

C. information barriers

D. Privileged Access Management (PAM)

Suggested Answer: *C*

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/information-barriers

Community vote distribution

C (100%)

Vinny2019 Highly Voted 4 years, 9 months ago

Information Barrier is the correct choice, ignore the typo :-)

upvoted 64 times

ThomasDehottay Highly Voted 4 years, 9 months ago

Correct but better with "Barriers" rather than "Batteries" :D

upvoted 41 times

The_warrior Most Recent 1 year, 5 months ago

Informatin barries is the correct answer https://learn.microsoft.com/en-us/purview/information-barriers "Microsoft Purview Information Barriers (IB) is a compliance solution that allows you to restrict two-way communication and collaboration between groups and users in Microsoft Teams, SharePoint, and OneDrive. Often used in highly regulated industries, IB can help to avoid conflicts of interest and safeguard internal information between users and organizational areas."

upvoted 1 times

LegendaryZA 1 year, 10 months ago

The answer is: information barriers https://learn.microsoft.com/en-us/purview/information-barriers

upvoted 2 times

ossk 2 years ago

correct

upvoted 1 times

Tahamaffia 2 years, 11 months ago

Got this question on my exam 05/09/2023

upvoted 3 times

RahulX 2 years, 11 months ago

Correct ans is A. You can use sensitivity label policies to restrict communication and the sharing of information between members of two departments at your organization.

upvoted 1 times

Crucius 2 years, 12 months ago

Correct.

upvoted 1 times

ltp1120 3 years, 2 months ago

Microsoft Purview Information Barriers (IB) is a compliance solution that allows you to restrict two-way communication and collaboration between groups and users in Microsoft Teams, SharePoint, and OneDrive.

upvoted 4 times

Nicochet 3 years, 6 months ago

Information Barrier

upvoted 3 times

Mcelona 3 years, 8 months ago

C is the answer

upvoted 3 times

IXone 3 years, 10 months ago

Correct : Information Barrier

upvoted 1 times

abilioneto 3 years, 10 months ago

correct

upvoted 1 times

Zeus009 3 years, 11 months ago

Information Barrier is the correct answer

upvoted 1 times

88xan 3 years, 12 months ago

Answer: C Information Barrier keyword restrict = barrier

upvoted 3 times

AdityaGupta 4 years ago

https://docs.microsoft.com/en-us/microsoft-365/compliance/information-barriers C Information Barriers

upvoted 1 times

Userer6945 4 years, 1 month ago

Why is it not PAM?

upvoted 1 times

Userer6945 4 years, 1 month ago

Why is it not PAM?I think the answer is not PAMS; reason being PAMS is not a Microsoft 365 feature. Information Barrier is a feature of Microsoft 365.I have the same doubt, but if i had to gess, maybe i would say that PAM(access) is related to permissions that users might have accessing apps or resources, not other users. Information barriers, on the other hand, is espicifically about who knows and a way to keep it secure.

upvoted 1 times

PatYeo 3 years, 7 months ago

I think the answer is not PAMS; reason being PAMS is not a Microsoft 365 feature. Information Barrier is a feature of Microsoft 365.

upvoted 1 times

ricardo_27_04_1978 3 years, 8 months ago

I have the same doubt, but if i had to gess, maybe i would say that PAM(access) is related to permissions that users might have accessing apps or resources, not other users. Information barriers, on the other hand, is espicifically about who knows and a way to keep it secure.

upvoted 1 times

Question #43 *Topic 1*

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Conditional access policies always enforce the use of multi-factor authentication (MFA).	○	○
Conditional access policies can be used to block access to an application based on the location of the user.	○	○
Conditional access policies only affect users who have Azure Active Directory (Azure AD)-joined devices.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
Conditional access policies always enforce the use of multi-factor authentication (MFA).	○	○
Conditional access policies can be used to block access to an application based on the location of the user.	○	○
Conditional access policies only affect users who have Azure Active Directory (Azure AD)-joined devices.	○	○

Answer Area

Statements	Yes	No
Conditional access policies always enforce the use of multi-factor authentication (MFA).	○	○
Conditional access policies can be used to block access to an application based on the location of the user.	○	○
Conditional access policies only affect users who have Azure Active Directory (Azure AD)-joined devices.	○	○

Reference: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

Jitusrit Highly Voted 4 years, 9 months ago

Correct..

upvoted 29 times

X98M 3 years, 2 months ago

It would be nice to have an explanation as to why an answer is correct/incorrect.

upvoted 5 times

megan_poirier Most Recent 1 year ago

Correct, NYN, on exam today August 2025.

upvoted 1 times

Pooltime123 1 year, 5 months ago

Appeared on the test today 02/27/2025.

upvoted 1 times

LegendaryZA 1 year, 10 months ago

The answer is: No, Yes, No https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-policies

upvoted 2 times

chiliman 2 years, 3 months ago

NYN is correct Third question: Cond. Access policies can apply to a variety of scenarios: Azure AD Joined Devices, Hybrid Joined Devices, Compliance Requirements > so conditional access policies are not limited to Azure AD joined devices

upvoted 1 times

RahulX 2 years, 11 months ago

NO YES NO

upvoted 2 times

RahulX 3 years, 5 months ago

1. No. 2. Yes. 3. Yes (because we can use CA Policy base location, device, IP Add, Azure Registered, Join devices) not only join devices.Read again, Note the word: 'ONLY'

upvoted 1 times

RahulX 3 years, 5 months ago

1. No. 2. Yes. 3. Yes (because we can use CA Policy base location, device, IP Add, Azure Registered, Join devices) not only join devices.

upvoted 1 times

obaali1990 Highly Voted 3 years, 5 months ago

Read again, Note the word: 'ONLY'

upvoted 11 times

Nicochet 3 years, 6 months ago

Absolutely correct!!

upvoted 2 times

JJGsy 3 years, 6 months ago

The answer to the last question must be "Yes" since it's Azure AD that offers the Conditional Access service in the first place!Read again, Note the word: 'ONLY'

upvoted 1 times

JJGsy 3 years, 6 months ago

The answer to the last question must be "Yes" since it's Azure AD that offers the Conditional Access service in the first place!

upvoted 1 times

Whyiest 3 years, 6 months ago

NYN Correct

upvoted 1 times

Whyiest 3 years, 7 months ago

Correct

upvoted 2 times

IXone 3 years, 10 months ago

Correct

upvoted 3 times

AdityaGupta 4 years ago

NYN is correct

upvoted 3 times

MugoKE 4 years, 1 month ago

Correct

upvoted 1 times

Yelad 4 years, 1 month ago

On the exam 10/07/2022

upvoted 5 times

Question #44 *Topic 1*

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Conditional access policies can be applied to global administrators.	○	○
Conditional access policies are evaluated before a user is authenticated.	○	○
Conditional access policies can use a device platform, such as Android or iOS, as a signal.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
Conditional access policies can be applied to global administrators.	○	○
Conditional access policies are evaluated before a user is authenticated.	○	○
Conditional access policies can use a device platform, such as Android or iOS, as a signal.	○	○

Answer Area

Statements	Yes	No
Conditional access policies can be applied to global administrators.	○	○
Conditional access policies are evaluated before a user is authenticated.	○	○
Conditional access policies can use a device platform, such as Android or iOS, as a signal.	○	○

Box 1: Yes - Conditional access policies can be applied to all users

Box 2: No - Conditional access policies are applied after first-factor authentication is completed.

Box 3: Yes - Users with devices of specific platforms or marked with a specific state can be used when enforcing Conditional Access policies.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

Fuji_56 Highly Voted 4 years, 4 months ago

2nd def no, first you are authenticated - then any policies are applied

upvoted 33 times

Fuji_56 Highly Voted 4 years, 4 months ago

2nd def no, first you are authenticated - then any policies are appliedYou're right, the user must first authenticate for conditional access to be applied to them.

upvoted 33 times

Dhamus 3 years, 3 months ago

You're right, the user must first authenticate for conditional access to be applied to them.

upvoted 2 times

M36570 4 years, 2 months ago

2nd is no, from official exam test preparation

upvoted 12 times

megan_poirier Most Recent 1 year ago

Correct answers, on exam today August 2025

upvoted 1 times

m0gu3 1 year, 7 months ago

Isn't this evaluated before a user is authenticated if conditional access enforces MFA?

upvoted 1 times

LegendaryZA 1 year, 10 months ago

The answer is Yes, No, Yes https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-policies https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-conditions

upvoted 2 times

rodrigoisalino 2 years, 2 months ago

The question appeared in my exam today, 06/2024.

upvoted 3 times

rodrigoisalino 2 years, 2 months ago

The question appeared in my exam today, 06/2024.i am writing on Friday - any other questions you can add? thank you

upvoted 3 times

loeloe5 2 years, 2 months ago

i am writing on Friday - any other questions you can add? thank you

upvoted 1 times

user_666 2 years, 6 months ago

had this question on my exam today (01 feb 2024)

upvoted 2 times

Ramye 2 years, 8 months ago

Given answers are correct. Conditional Access policies are enforced after first-factor authentication is completed. Conditional Access isn't intended to be an organization's first line of defense for scenarios like denial-of-service (DoS) attacks, but it can use signals from these events to determine access. Source: https://learn.microsoft.com/en-us/entra/identity/conditional-access/location-condition

upvoted 3 times

RahulX 2 years, 11 months ago

YES NO YES

upvoted 1 times

furq2904 3 years, 1 month ago

appeared on July 1st 2023

upvoted 2 times

CertAddict69 3 years, 2 months ago

I would say YYY. For the second one, Yes Conditional Access takes place after first factor authentication, but, a user is not authenticated after first factor authentication. First factor authentication is only part of the authentication process. A user is not fully authenticated until they have completed Conditional Access as well, so Conditional Access takes place BEFORE a user is authenticated as it is part of the authentication process.

upvoted 4 times

manofsteel9 3 years, 2 months ago

Correct answer is: YYY for the 2nd one, Conditional access policies in Azure Active Directory (Azure AD) are evaluated before a user is authenticated. Conditional access allows organizations to enforce additional security requirements and controls based on specific conditions, such as user location, device state, or risk level.

upvoted 4 times

Nicochet 3 years, 6 months ago

YNY is correct

upvoted 4 times

Whyiest 3 years, 6 months ago

YNY Correct

upvoted 3 times

Whyiest 3 years, 7 months ago

It's no for the 2nd one because Conditional Access start only after 1th authentification

upvoted 1 times

ricardo_27_04_1978 3 years, 8 months ago

How is it, that a global administrator could be included in complience policies? Shouldn´t he be in the top of the hierarchy? isn´t the one who makes the rules?Those are actually the accounts with more stringent compliance policies because of their admin privileges.Global admin accounts are the ones that you need to secure the most. If anything, more conditional access policies should apply to them, not less. However, it is recommended to set up a break-glass account in case of emergency. Or in case you mess up configuring a conditional access policy and block yourself (and other admins) from reverting it. The emergency account should be excluded from all conditional access policies. But it should therefore be VERY closely monitored and not used for anything else. https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/plan-conditional-access#set-up-emergency-access-accounts

upvoted 3 times

ricardo_27_04_1978 3 years, 8 months ago

How is it, that a global administrator could be included in complience policies? Shouldn´t he be in the top of the hierarchy? isn´t the one who makes the rules?

upvoted 3 times

John316 3 years, 8 months ago

Those are actually the accounts with more stringent compliance policies because of their admin privileges.

upvoted 3 times

OG_Diablo 3 years, 8 months ago

Global admin accounts are the ones that you need to secure the most. If anything, more conditional access policies should apply to them, not less. However, it is recommended to set up a break-glass account in case of emergency. Or in case you mess up configuring a conditional access policy and block yourself (and other admins) from reverting it. The emergency account should be excluded from all conditional access policies. But it should therefore be VERY closely monitored and not used for anything else. https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/plan-conditional-access#set-up-emergency-access-accounts

upvoted 5 times

IXone 3 years, 10 months ago

Correct

upvoted 5 times

Question #45 *Topic 1*

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

Applications registered in Azure Active Directory (Azure AD) are associated automatically to a

- guest account.
- managed identity.
- service principal.
- user account.

Suggested Answer:

Answer Area

Applications registered in Azure Active Directory (Azure AD) are associated automatically to a

- guest account.
- managed identity.
- service principal.
- user account.

Answer Area

Applications registered in Azure Active Directory (Azure AD) are associated automatically to a

- guest account.
- managed identity.
- service principal.
- user account.

When you register an application through the Azure portal, an application object and service principal are automatically created in your home directory or tenant. Reference: https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

thiaybovo Highly Voted 4 years, 8 months ago

CORRECT

upvoted 23 times

Clouddog Highly Voted 4 years, 4 months ago

Provided answer is correct: A service principal is created in each tenant where the application is used and references the globally unique app object. The service principal object defines what the app can actually do in the specific tenant, who can access the app, and what resources the app can access.

upvoted 22 times

LegendaryZA Most Recent 1 year, 10 months ago

The answer is: service principal https://learn.microsoft.com/en-us/entra/identity-platform/app-objects-and-service-principals?tabs=browser

upvoted 1 times

DK21Dilip 2 years ago

this question came in july 2024

upvoted 1 times

rodrigoisalino 2 years, 2 months ago

The question appeared in my exam today, 06/2024.

upvoted 2 times

lukecage5 2 years, 11 months ago

Correct answer is Service Principal. A service principal is created in each tenant where the application is used and references the globally unique app object. The service principal object defines what the app can actually do in the specific tenant, who can access the app, and what resources the app can access.

upvoted 1 times

RahulX 2 years, 11 months ago

Correct Ans. Service Principal

upvoted 1 times

Kelsi999 3 years, 3 months ago

Correct I had this question on the exam

upvoted 2 times

Whyiest 3 years, 7 months ago

The answer is correct. Here is more informations if you need : When you register an application through the Azure portal, an application object and service principal are automatically created in your home directory or tenant. A service principal is a security identity used to represent an application in Azure Active Directory (AAD). It is used to authenticate the application to access resources, and also to assign permissions to those resources. A service principal is like a user identity (login and password or certificate) for an application. An application object, on the other hand, is a representation of an application in Azure Active Directory. It contains information about the application, such as its name and URL, as well as its associated service principal. In summary, a service principal is a security identity used to authenticate an application, while an application object is a representation of the application in Azure Active Directory that contains information about the application and its associated service principal.

upvoted 12 times

abilioneto 3 years, 10 months ago

correct

upvoted 3 times

Zeus009 3 years, 11 months ago

Agreed

upvoted 1 times

cormorant 4 years, 1 month ago

key words for service principle - applications registered

upvoted 3 times

Cactuus88 4 years, 2 months ago

Correct

upvoted 1 times

rapunzellin 4 years, 4 months ago

Correct

upvoted 1 times

DemekeA 4 years, 5 months ago

Service Principal

upvoted 4 times

Ummar26 4 years, 6 months ago

correct

upvoted 6 times

Question #46 *Topic 1*

Which three authentication methods does Windows Hello for Business support? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. fingerprint

B. facial recognition

C. PIN

D. email verification

E. security question

Suggested Answer: *A, B, C*
Reference: https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-how-it-works-authentication

Community vote distribution
ABC (100%)

JayHall Highly Voted 4 years, 9 months ago
correct Windows Hello in Windows 10 enables users to sign in to their device using a PIN. https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-why-pin-is-better-than-password Windows Hello lets your employees use fingerprint or facial recognition as an alternative method to unlocking a device. With Windows Hello, authentication happens when the employee provides his or her unique biometric identifier while accessing the device-specific Windows Hello credentials. https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-biometrics-in-enterprise
upvoted 36 times

Yelad Highly Voted 4 years, 1 month ago
On the exam 10/07/2022
upvoted 6 times

megan_poirier Most Recent 1 year ago
Correct, ABC, on exam today August 2025.
upvoted 1 times

kdajflkajf 1 year, 9 months ago
correct andwer
upvoted 1 times

LegendaryZA 1 year, 10 months ago
The answer is: Fingerprint (Biometric) Facial recognition (Biometric) PIN
upvoted 1 times

rodrigoisalino 2 years, 2 months ago
The question appeared in my exam today, 06/2024.
upvoted 2 times

RahulX 2 years, 11 months ago
A. fingerprint B. facial recognition C. PIN
upvoted 1 times

joshsz 3 years ago
Correct
upvoted 1 times

Molota 3 years, 2 months ago
like when logging on the computer ... ABC
upvoted 1 times

Nicochet 3 years, 6 months ago
ABC. Correct.
upvoted 3 times

Whyiest 3 years, 6 months ago
Windows Hello for Business MFA: - Fingerprint - Facial recognition - PIN

upvoted 3 times

Whyiest 3 years, 7 months ago

Correct

upvoted 1 times

Andreew883 3 years, 7 months ago

Valid answer is A,b,c

upvoted 2 times

smartin2010 3 years, 10 months ago

Correct

upvoted 1 times

Zeus009 3 years, 11 months ago

Aligned

upvoted 1 times

johnegil 4 years, 1 month ago

Appeared on exam 12/07/2022

upvoted 3 times

taky 4 years, 1 month ago

Correct, biometric and number password are supported. Email requires internet connection on the device and security questions are used to recover access account.

upvoted 3 times

Question #47 *Topic 1*

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

When you enable security defaults in Azure Active Directory (Azure AD),

Azure AD Identity Protection
Azure AD Privileged Identity Management (PIM)
multi-factor authentication (MFA)

will be enabled for all Azure AD users.

Suggested Answer:

Answer Area

When you enable security defaults in Azure Active Directory (Azure AD),

Azure AD Identity Protection
Azure AD Privileged Identity Management (PIM)
multi-factor authentication (MFA)

will be enabled for all Azure AD users.

Answer Area

When you enable security defaults in Azure Active Directory (Azure AD),

Azure AD Identity Protection
Azure AD Privileged Identity Management (PIM)
multi-factor authentication (MFA)

will be enabled for all Azure AD users.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults

Cereb7 Highly Voted 4 years, 7 months ago

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults Security defaults make it easier to help protect your organization from these attacks with preconfigured security settings: - Requiring all users to register for Azure AD Multi-Factor Authentication. - Requiring administrators to do multi-factor authentication. - Blocking legacy authentication protocols. - Requiring users to do multi-factor authentication when necessary. - Protecting privileged activities like access to the Azure portal.

upvoted 38 times

Lazylinux Highly Voted 4 years, 1 month ago

MFA for sure https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults

upvoted 5 times

LegendaryZA Most Recent 1 year, 10 months ago

The answer is: multi-factor authentication (MFA) https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults

upvoted 1 times

RahulX 2 years, 11 months ago

Correct Ans. When Security Default is enabled in Azure AD Portal MFA is automatically enabled tenant wide but user can avoid the MFA for 14 grace period.

upvoted 2 times

cantbeme 3 years, 12 months ago

on exam today

upvoted 3 times

Lawiwi 4 years, 1 month ago

correct

upvoted 1 times

jacqs101 4 years, 4 months ago

Technically the answers on this question are all wrong.

upvoted 3 times

bikewun 4 years, 5 months ago

CORRECT

upvoted 1 times

DemekeA 4 years, 5 months ago

MFA is answer

upvoted 2 times

yulexam 4 years, 9 months ago

correct... to change the "security default" : AAD>properties>manage security defaults

upvoted 4 times

Question #48 *Topic 1*

You have an Azure subscription.
You need to implement approval-based, time-bound role activation.
What should you use?

A. Windows Hello for Business

B. Azure Active Directory (Azure AD) Identity Protection

C. access reviews in Azure Active Directory (Azure AD)

D. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

Suggested Answer: *D*
Reference: https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

Community vote distribution
D (100%)

Whyiest Highly Voted 3 years, 6 months ago
Note for your exam : When you see the key word "time" linked to an access or an authentification, assume that there is high chance that it's PIM.
upvoted 51 times

k_jay Highly Voted 4 years, 3 months ago
Correct answer!
upvoted 11 times

megan_poirier Most Recent 1 year ago
On exam today, August 2025
upvoted 1 times

LegendaryZA 1 year, 10 months ago
The answer is: Azure Active Directory (Azure AD) Privileged Identity Management (PIM) which is now called Microsoft Entra Privileged Identity Management (PIM). https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-how-to-activate-role
upvoted 1 times

RahulX 2 years, 11 months ago
Correct. D. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
upvoted 2 times

Molota 3 years, 2 months ago
Answer is PIM
upvoted 1 times

Nicochet 3 years, 6 months ago
PIM is the option.
upvoted 3 times

Whyiest 3 years, 7 months ago
D. Azure Active Directory (Azure AD) Privileged Identity Management (PIM) Azure Active Directory (Azure AD) Privileged Identity Management (PIM) is designed specifically for implementing approval-based, time-bound role activation in an Azure subscription. PIM allows you to manage and control access to privileged roles in Azure AD, Azure resources, and Azure AD-integrated SaaS apps. It enables you to elevate access on a just-in-time basis and provides an approval workflow for role activation, which can be restricted to specific time periods. This makes it an ideal choice for implementing the requirements specified in the question.
upvoted 3 times

2cent2 3 years, 7 months ago
d is correct
upvoted 2 times

PikaDeUrso 3 years, 7 months ago
Correct!
upvoted 3 times

FBrabble 3 years, 9 months ago

PIM for sure D

upvoted 1 times

IXone 3 years, 10 months ago

Correct

upvoted 1 times

abilioneto 3 years, 10 months ago

correct

upvoted 1 times

smartin2010 3 years, 10 months ago

D correct

upvoted 1 times

Benjam 3 years, 11 months ago

Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

upvoted 3 times

Zeus009 3 years, 11 months ago

Agreed

upvoted 1 times

dino23 3 years, 11 months ago

Correct answer!

upvoted 1 times

Question #49 *Topic 1*

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Global administrators are exempt from conditional access policies	○	○
A conditional access policy can add users to Azure Active Directory (Azure AD) roles	○	○
Conditional access policies can force the use of multi-factor authentication (MFA) to access cloud apps	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
Global administrators are exempt from conditional access policies	○	◉
A conditional access policy can add users to Azure Active Directory (Azure AD) roles	○	◉
Conditional access policies can force the use of multi-factor authentication (MFA) to access cloud apps	◉	○

Answer Area

Statements	Yes	No
Global administrators are exempt from conditional access policies	○	◉
A conditional access policy can add users to Azure Active Directory (Azure AD) roles	○	◉
Conditional access policies can force the use of multi-factor authentication (MFA) to access cloud apps	◉	○

Reference: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-admin-mfa

FBrabble Highly Voted 3 years, 9 months ago

N N Y correct

upvoted 14 times

IXone Highly Voted 3 years, 10 months ago

Correct

upvoted 5 times

LegendaryZA Most Recent 1 year, 10 months ago

The answer is: No, No, Yes https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview

upvoted 1 times

johnjhk 2 years, 1 month ago

Correct

upvoted 1 times

rodrigoisalino 2 years, 2 months ago

The question appeared in my exam today, 06/2024.

upvoted 2 times

RahulX 2 years, 11 months ago

NO NO YES

upvoted 1 times

RahulX 2 years, 11 months ago

NO NO YESYou can create a conditional access policy targeted to all users including Global Admin.

upvoted 1 times

RahulX 2 years, 11 months ago

You can create a conditional access policy targeted to all users including Global Admin.

upvoted 1 times

Kelsi999 3 years, 3 months ago

On the exam today. Answers are correct

upvoted 5 times

Daniel_Angelo 3 years, 4 months ago

NNY: 2º:Use Conditional Access policies to apply the right access controls when needed to keep your organization secure. can not add users to azure ad roles.

upvoted 1 times

Nicochet 3 years, 6 months ago

NNI Totally correct

upvoted 1 times

Whyiest 3 years, 6 months ago

NNY I agree with others it's correct

upvoted 4 times

abilioneto 3 years, 10 months ago

correct

upvoted 4 times

Zeus009 3 years, 11 months ago

Aligned

upvoted 4 times

Yelad 4 years, 1 month ago

On the exam 10/07/2022

upvoted 5 times

misterperson 4 years, 3 months ago

correct

upvoted 2 times

GPerez73 4 years, 3 months ago

Correct

upvoted 3 times

Question #50 *Topic 1*

When security defaults are enabled for an Azure Active Directory (Azure AD) tenant, which two requirements are enforced? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. All users must authenticate from a registered device.

B. Administrators must always use Azure Multi-Factor Authentication (MFA).

C. Azure Multi-Factor Authentication (MFA) registration is required for all users.

D. All users must authenticate by using passwordless sign-in.

E. All users must authenticate by using Windows Hello.

Suggested Answer: *B, C*
Security defaults make it easy to protect your organization with the following preconfigured security settings: ➪ Requiring all users to register for Azure AD Multi-Factor Authentication. ➪ Requiring administrators to do multi-factor authentication. ➪ Blocking legacy authentication protocols. ➪ Requiring users to do multi-factor authentication when necessary. ➪ Protecting privileged activities like access to the Azure portal. Reference: https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults

Community vote distribution
BC (100%)

JJGsy Highly Voted 3 years, 6 months ago
Misleading question, as if all users require MFA, there's no separate requirement to also require this for admins!This is wrong. The Users are Required to REGISTER to MFA not use it contineously. The difference is that Admin will be forced to use MFA ALL THE TIME. Hence the discrimination.The Answer Is Correct.
upvoted 11 times

JJGsy Highly Voted 3 years, 6 months ago
Misleading question, as if all users require MFA, there's no separate requirement to also require this for admins!
upvoted 11 times

dawnbringer69 3 years, 2 months ago
This is wrong. The Users are Required to REGISTER to MFA not use it contineously. The difference is that Admin will be forced to use MFA ALL THE TIME.

Hence the discrimination.
upvoted 5 times

dawnbringer69 3 years, 2 months ago
This is wrong. The Users are Required to REGISTER to MFA not use it contineously. The difference is that Admin will be forced to use MFA ALL THE TIME. Hence the discrimination.The Answer Is Correct.
upvoted 5 times

dawnbringer69 3 years, 2 months ago
The Answer Is Correct.
upvoted 1 times

LegendaryZA Most Recent 1 year, 10 months ago
The answer is: Administrators must always use Azure Multi-Factor Authentication (MFA). Azure Multi-Factor Authentication (MFA) registration is required for all users. https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults
upvoted 2 times

RahulX 2 years, 11 months ago
Correct B. Administrators must always use Azure Multi-Factor Authentication (MFA) C. Azure Multi-Factor Authentication (MFA) registration is required for all users
upvoted 2 times

studytonight 3 years, 2 months ago
A question that was very similar to this was on the May 2023 exam.
upvoted 1 times

Whyiest 3 years, 7 months ago

Correct

upvoted 2 times

IXone 3 years, 10 months ago

Correct

upvoted 4 times

abilioneto 3 years, 10 months ago

correct

upvoted 3 times

Zeus009 3 years, 11 months ago

B and C are joined at the hip

upvoted 4 times

cantbeme 3 years, 12 months ago

on exam today

upvoted 3 times

Mahaendhiran 4 years, 2 months ago

Correct

upvoted 1 times

misterperson 4 years, 3 months ago

correct

upvoted 1 times

Siphe 4 years, 3 months ago

Correct

upvoted 1 times

Question #51 *Topic 1*

Which type of identity is created when you register an application with Active Directory (Azure AD)?

A. a user account

B. a user-assigned managed identity

C. a system-assigned managed identity

D. a service principal

Suggested Answer: *D*

When you register an application through the Azure portal, an application object and service principal are automatically created in your home directory or tenant. Reference: https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

Community vote distribution

D (100%)

LegendaryZA Most Recent 1 year, 10 months ago

The answer is: a service principal https://learn.microsoft.com/en-us/azure/active-directory/develop/app-objects-and-service-principals#service-principal-object

upvoted 2 times

RahulX 2 years, 11 months ago

D. a service principal

upvoted 1 times

Kelsi999 3 years, 3 months ago

On the exam today. Correct answer

upvoted 1 times

Nicochet 3 years, 6 months ago

a Service Principal

upvoted 3 times

o_seun 3 years, 7 months ago

Correct service Principal is correct

upvoted 2 times

ITOPS 3 years, 7 months ago

Correct

upvoted 2 times

FBrabble 3 years, 9 months ago

Yes the answer is D service principal

upvoted 2 times

Ola189 3 years, 9 months ago

CORRECT

upvoted 3 times

IXone 3 years, 10 months ago

Correct

upvoted 2 times

abilioneto 3 years, 10 months ago

correct

upvoted 1 times

Mahaendhiran 4 years, 2 months ago

Correct

upvoted 2 times

misterperson 4 years, 3 months ago

correct

upvoted 2 times

Siphe 4 years, 3 months ago

D - correct answer.

upvoted 1 times

GPerez73 4 years, 3 months ago

Correct

upvoted 3 times

Question #52 *Topic 1*

Which three tasks can be performed by using Azure Active Directory (Azure AD) Identity Protection? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Configure external access for partner organizations.

B. Export risk detection to third-party utilities.

C. Automate the detection and remediation of identity based-risks.

D. Investigate risks that relate to user authentication.

E. Create and automatically assign sensitivity labels to data.

Suggested Answer: *C, D, E*
Official Answer: CDE

Community vote distribution
BCD (100%)

KoosDuppen Highly Voted 4 years, 3 months ago
Directly from the SC-900 Fundamentals training slides: Azure Identity Protection Enables organizations to accomplish three key tasks: • Automate the detection and remediation of identity based risks. • Investigate risks using data in the portal. • Export risk detection data to third party utilities for further analysis.
upvoted 87 times

KoosDuppen Highly Voted 4 years, 3 months ago
Directly from the SC-900 Fundamentals training slides: Azure Identity Protection Enables organizations to accomplish three key tasks: • Automate the detection and remediation of identity based risks. • Investigate risks using data in the portal. • Export risk detection data to third party utilities for further analysis.please share the slideshttps://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protectionEXPORT RDD TO OTHER TOOLS NOT ORGANIZATIONS ...."other TOOLS" = "3rd party ULTILITIES", same thing, different words mate.
upvoted 87 times

Roux 4 years, 3 months ago
please share the slideshttps://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protectionEXPORT RDD TO OTHER TOOLS NOT ORGANIZATIONS ...."other TOOLS" = "3rd party ULTILITIES", same thing, different words mate.
upvoted 3 times

Roux 4 years, 3 months ago
please share the slides
upvoted 3 times

Suresh13 4 years, 2 months ago
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protectionEXPORT RDD TO OTHER TOOLS NOT ORGANIZATIONS ...."other TOOLS" = "3rd party ULTILITIES", same thing, different words mate.
upvoted 6 times

Suresh13 4 years, 2 months ago
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection
upvoted 6 times

vskordas 3 years, 11 months ago
EXPORT RDD TO OTHER TOOLS NOT ORGANIZATIONS ...."other TOOLS" = "3rd party ULTILITIES", same thing, different words mate.
upvoted 1 times

vskordas 3 years, 11 months ago
EXPORT RDD TO OTHER TOOLS NOT ORGANIZATIONS ....
upvoted 1 times

Kuliet 3 years, 10 months ago
"other TOOLS" = "3rd party ULTILITIES", same thing, different words mate.
upvoted 7 times

JMROFLLOL 4 years, 3 months ago

As other have said, sensitivity labels have nothing to do with it.Exactly

upvoted 32 times

JMROFLLOL 4 years, 3 months ago

Selected Answer: BCD

As other have said, sensitivity labels have nothing to do with it.

upvoted 32 times

obaali1990 3 years, 5 months ago

Exactly

upvoted 2 times

LegendaryZA Most Recent 1 year, 10 months ago

The answer is: B. Export risk detection to third-party utilities. C. Automate the detection and remediation of identity based-risks. D. Investigate risks that relate to user authentication.

upvoted 1 times

Ozziie 2 years, 7 months ago

It is CDE: Microsoft Entra ID Protection helps organizations detect, investigate, and remediate identity-based risks. These identity-based risks can be further fed into tools like Conditional Access to make access decisions or fed back to a security information and event management (SIEM) tool for further investigation and correlation. The tools that are written down here are available from Microsoft, so not third parties.
Ref:https://learn.microsoft.com/en-us/entra/id-protection/overview-identity-protection

upvoted 1 times

Akacokie 2 years, 9 months ago

B. Export risk detection to third-party utilities. Most Voted C. Automate the detection and remediation of identity based-risks. Most Voted D. Investigate risks that relate to user authentication. Most Voted

upvoted 2 times

Tomix 2 years, 11 months ago

Selected Answer: BCD

upvoted 2 times

RahulX 2 years, 11 months ago

Correct Ans are B. Export risk detection to third-party utilities. C. Automate the detection and remediation of identity based-risks. D. Investigate risks that relate to user authentication.

upvoted 2 times

Darkfire 3 years ago

Answer should be BCD

upvoted 2 times

manofsteel9 3 years, 2 months ago

correct answer is BCD. I verified with the provided link from the guys here.

upvoted 1 times

bjobare 3 years, 2 months ago

Automate the detection and remediation of identity-based risks. Investigate risks using data in the portal. Export risk detection data to other tools.

upvoted 1 times

MarcioTB 3 years, 3 months ago

correct

upvoted 1 times

Distinctive 3 years, 3 months ago

THE answers are here https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection

upvoted 1 times

bahik999 3 years, 4 months ago

its CDE: C. Automate the detection and remediation of identity-based risks. D. Investigate risks that relate to user authentication. E. Create and automatically assign sensitivity labels to data. A. Azure AD Identity Protection is not used to configure external access for partner organizations. This task is typically performed using Azure AD B2B collaboration.

B. Azure AD Identity Protection does not export risk detection to third-party utilities. It provides built-in reports and notifications for risk detections.

C. Azure AD Identity Protection can automate the detection and remediation of identity-based risks by using its machine learning algorithms to detect risky sign-ins and user behavior. It can also take remedial actions such as blocking access or requiring additional authentication.

D. Azure AD Identity Protection allows investigating risks that relate to user authentication. It provides detailed reports and recommendations for remediation.

E. Azure AD Identity Protection does not create and automatically assign sensitivity labels to data. This task is typically performed using Azure Information Protection.

upvoted 1 times

bahik999 3 years, 4 months ago

its CDE: C. Automate the detection and remediation of identity-based risks. D. Investigate risks that relate to user authentication. E. Create and automatically assign sensitivity labels to data. A. Azure AD Identity Protection is not used to configure external access for partner organizations. This task is typically performed using Azure AD B2B collaboration. B. Azure AD Identity Protection does not export risk detection to third-party utilities. It provides built-in reports and notifications for risk detections. C. Azure AD Identity Protection can automate the detection and remediation of identity-based risks by using its machine learning algorithms to detect risky sign-ins and user behavior. It can also take remedial actions such as blocking access or requiring additional authentication. D. Azure AD Identity Protection allows investigating risks that relate to user authentication. It provides detailed reports and recommendations for remediation. E. Azure AD Identity Protection does not create and automatically assign sensitivity labels to data. This task is typically performed using Azure Information Protection.So it is NOT E (note the NOT in below sentence)it s. It should be BCD, that is also confirmed in the Security, Compliance and Identity fundamentals Learning path. E. Azure AD Identity Protection does not create and automatically assign sensitivity labels to data. This task is typically performed using Azure Information Protection

upvoted 1 times

Mehe323 3 years ago

So it is NOT E (note the NOT in below sentence)it s. It should be BCD, that is also confirmed in the Security, Compliance and Identity fundamentals Learning path. E. Azure AD Identity Protection does not create and automatically assign sensitivity labels to data. This task is typically performed using Azure Information Protection

upvoted 2 times

nobrainatall 3 years, 6 months ago

E is compliance and has nothing to do with Azure Identity Protection

upvoted 2 times

Nicochet 3 years, 6 months ago

Is BCD. E is incorrect.

upvoted 2 times

Whyiest 3 years, 6 months ago

100% sure that is BCD

upvoted 2 times

ok22 3 years, 6 months ago

BCD is definitely correct.

upvoted 1 times

Question #53 *Topic 1*

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

When using multi-factor authentication (MFA), a password is considered something you [ ] .

are
have
know
share

Suggested Answer:

Answer Area

When using multi-factor authentication (MFA), a password is considered something you [know] .

are
have
know
share

Answer Area

When using multi-factor authentication (MFA), a password is considered something you [know] .

are
have
know
share

Box 1: know - Multifactor authentication combines two or more independent credentials: what the user knows, such as a password; what the user has, such as a security token; and what the user is, by using biometric verification methods. Reference: https://www.techtarget.com/searchsecurity/definition/multifactor-authentication-MFA

Whyiest Highly Voted 3 years, 7 months ago

Password = know Device / code / key = have Biometric = you are

upvoted 39 times

LegendaryZA Most Recent 1 year, 10 months ago

The answer is: know https://support.microsoft.com/en-gb/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661

upvoted 1 times

Tahamaffia 2 years, 11 months ago

Got this question on my exam 05/09/2023

upvoted 2 times

RahulX 2 years, 11 months ago

Password = something you know Code = something you have Biometric = something you are.

upvoted 2 times

bigelmo_elmo 3 years, 1 month ago

If you don't know this... you shouldn't be taking the exam

upvoted 3 times

walkaway 3 years, 7 months ago

Have is for device. Know is for password.

upvoted 4 times

PoopyPants 3 years, 8 months ago

Perhaps an MFA token could be considered something you have. However MFA tokens dont contain words. Question states a PassWORD. Lousy question.

upvoted 2 times

Cegep 3 years, 10 months ago

The question states a password. That's something you know.

upvoted 3 times

vskordas 3 years, 11 months ago

The doc you provide is Know (password), hav (token- mobile), are (fingerprint) so, all of these must considered as correct, not only A

upvoted 3 times

RodrigoAB 3 years, 11 months ago

Something You Know, Have, or Are Something you ---->know<----- (eg. a password). This is the most common kind of authentication used for humans.

upvoted 4 times

Question #54 *Topic 1*

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Windows Hello for Business can use the Microsoft Authenticator app as an authentication method.	○	○
Windows Hello for Business can use a PIN code as an authentication method.	○	○
Windows Hello for Business authentication information syncs across all the devices registered by a user.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
Windows Hello for Business can use the Microsoft Authenticator app as an authentication method.	○	○
Windows Hello for Business can use a PIN code as an authentication method.	○	○
Windows Hello for Business authentication information syncs across all the devices registered by a user.	○	○

Answer Area

Statements	Yes	No
Windows Hello for Business can use the Microsoft Authenticator app as an authentication method.	○	○
Windows Hello for Business can use a PIN code as an authentication method.	○	○
Windows Hello for Business authentication information syncs across all the devices registered by a user.	○	○

Box 1: No - The Microsoft Authenticator app helps you sign in to your accounts when you're using two-factor verification. Two-factor verification helps you to use your accounts more securely because passwords can be forgotten, stolen, or compromised. Two-factor verification uses a second factor like your phone to make it harder for other people to break in to your account.

Box 2: Yes - In Windows 10, Windows Hello for Business replaces passwords with strong two-factor authentication on devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN.

Box 3: No - Windows Hello credentials are based on certificate or asymmetrical key pair. Windows Hello credentials can be bound to the device, and the token that is obtained using the credential is also bound to the device. Reference: https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview

Anand_Parappurath Highly Voted 3 years, 10 months ago

I think Windows hello is single factor authentication and MS Authenticator is used a MFA agent or device or tool. for me the ans is N,Y,N

upvoted 7 times

Anand_Parappurath 3 years, 10 months ago

I think Windows hello is single factor authentication and MS Authenticator is used a MFA agent or device or tool. for me the ans is N,Y,NWindows Hello for Business actually counts as multi-factor authentication. Because it is something you have (the physical computer) and either something you know (PIN) or something you are (biometrics). You cannot use the MS Authenticator for Windows Hello for Business, as that is something you have on a different device. WHfB is strictly local on the Windows computer. That doesn't change the correct answers, though. They remain N, Y, N.

upvoted 7 times

OG_Diablo Highly Voted 3 years, 8 months ago

Windows Hello for Business actually counts as multi-factor authentication. Because it is something you have (the physical computer) and either something you know (PIN) or something you are (biometrics). You cannot use the MS Authenticator for Windows Hello for Business, as that is something you have on a different device. WHfB is strictly local on the Windows computer. That doesn't change the correct answers, though. They remain N, Y, N.

upvoted 8 times

Ola189 3 years, 9 months ago

From https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview: 'In Windows 10, Windows Hello for Business replaces passwords with strong two-factor authentication on devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN.' Answer is correct. (NYN)

upvoted 5 times

LegendaryZA 1 year, 10 months ago

The answer is No, Yes, No https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/

upvoted 1 times

user_666 2 years, 6 months ago

had this question on my exam today (01 feb 2024)

upvoted 1 times

Tomix 2 years, 11 months ago

Yes Yes No

upvoted 2 times

RahulX 2 years, 11 months ago

No Yes No

upvoted 1 times

Mehe323 3 years ago

The explanation of the first statement is not very clear. You use the app for accounts that have their credentials stored in the cloud. Windows Hello is tied to the device, the account details to login are stored on the device. You can't use the MA app for such a device.I agree. A better explanation is "Windows Hello for Business uses a two-factor authentication method that combines a device-specific credential with a biometric or PIN gesture", not Microsoft Authenticator app. https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/#windows-hello-and-two-factor-authentication

upvoted 3 times

Mehe323 3 years ago

The explanation of the first statement is not very clear. You use the app for accounts that have their credentials stored in the cloud. Windows Hello is tied to the device, the account details to login are stored on the device. You can't use the MA app for such a device.

upvoted 3 times

KindFlame Most Recent 1 year, 4 months ago

I agree. A better explanation is "Windows Hello for Business uses a two-factor authentication method that combines a device-specific credential with a biometric or PIN gesture", not Microsoft Authenticator app. https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/#windows-hello-and-two-factor-authentication

upvoted 1 times

Molota 3 years, 2 months ago

agreed with the given answer

upvoted 1 times

StressFree 3 years, 4 months ago

e o pior q é verdade....

upvoted 1 times

smurferinoatexcel 3 years, 5 months ago

Correct. 1) MS authenticator app is not a part of Windows Hello 2) PIN is considered "something you know" 3) Windows Hello stores authentication information only on the local device

upvoted 2 times

Neeraj1978 3 years, 5 months ago

N,Y,N Windows Hello is a more personal, more secure way to get instant access to your Windows 10 devices using a PIN, facial recognition, or fingerprint. You'll need to set up a PIN as part of setting up fingerprint or facial recognition sign-in, but you can also sign in with just your PIN.

upvoted 1 times

Nicochet 3 years, 6 months ago

No Yes No

upvoted 1 times

Whyiest 3 years, 6 months ago

Windows Hello for Business MFA: - Fingerprint - Facial recognition - PIN

upvoted 2 times

FBrabble 3 years, 9 months ago

tricky question but N Y N looks correct as WH4B is a different topic than MFA in this case

upvoted 2 times

SiDoCiOuS 3 years, 10 months ago

On the exam 10/18/2022.

upvoted 3 times

656823 3 years, 10 months ago

This should be YYN, right?

upvoted 2 times

vskordas 3 years, 11 months ago

..Then why when I have to login to my bank I use MS Authenticatpr app at my mobile? ..I think MS Authenticator is MFA option.

upvoted 2 times

vskordas 3 years, 11 months ago

..Then why when I have to login to my bank I use MS Authenticatpr app at my mobile? ..I think MS Authenticator is MFA option.The bank is not a Microsoft service, they are referring to login into Microsoft accounts and devices that are included in Windows Hello for Business. Windows HfB has two main authentication options for device and Microsoft account login: something you have (the device) and something you are (biometric) OR something you know (PIN). https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/

upvoted 2 times

Mehe323 3 years ago

The bank is not a Microsoft service, they are referring to login into Microsoft accounts and devices that are included in Windows Hello for Business. Windows HfB has two main authentication options for device and Microsoft account login: something you have (the device) and something you are (biometric) OR something you know (PIN). https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/

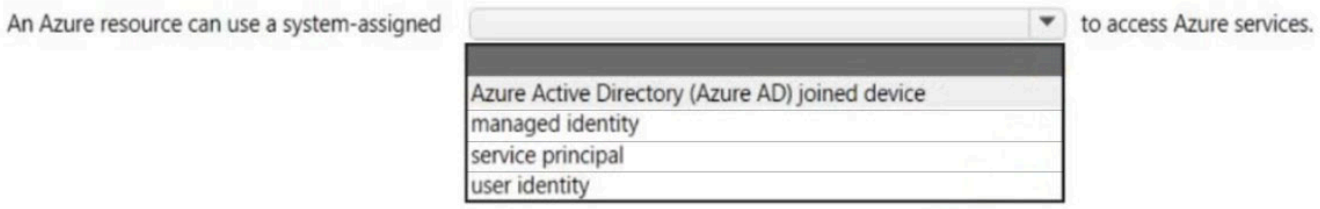
upvoted 1 times

Question #55 *Topic 1*

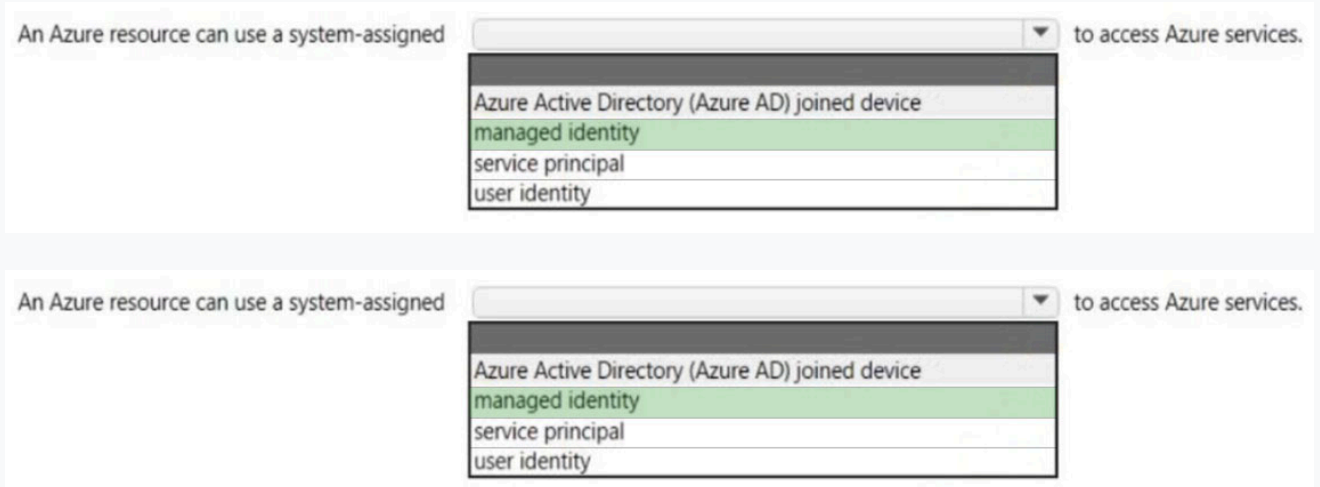
HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:



Suggested Answer:



Managed identities provide an identity for applications to use when connecting to resources that support Azure Active Directory (Azure AD) authentication. Here are some of the benefits of using managed identities: You don't need to manage credentials. Credentials aren't even accessible to you. You can use managed identities to authenticate to any resource that supports Azure AD authentication, including your own applications. Reference: https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

IXone Highly Voted 3 years, 10 months ago

Correct

upvoted 9 times

User_Mowgli Highly Voted 3 years, 11 months ago

Managed Identity

upvoted 5 times

LegendaryZA Most Recent 1 year, 10 months ago

The answer is: managed identity https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/overview#managed-identity-types

upvoted 1 times

RahulX 2 years, 11 months ago

"managed identity" is the correct answer.

upvoted 2 times

TATTIF 3 years, 4 months ago

managed identity is correct

upvoted 3 times

FBrabble 3 years, 9 months ago

managed identity = correct answer

upvoted 5 times

abilioneto 3 years, 10 months ago

correct

upvoted 3 times

Emmuyah 3 years, 10 months ago

Correct Answer

upvoted 4 times

Question #56 *Topic 1*

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

You can use [ ] in the Microsoft 365 Defender portal to identify devices that are affected by an alert.

- classifications
- incidents
- policies
- Secure score

Suggested Answer:

Answer Area

You can use [incidents] in the Microsoft 365 Defender portal to identify devices that are affected by an alert.

- classifications
- incidents
- policies
- Secure score

Answer Area

You can use [incidents] in the Microsoft 365 Defender portal to identify devices that are affected by an alert.

- classifications
- incidents
- policies
- Secure score

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender/incidents-overview?view=o365-worldwide

pallmall Highly Voted 3 years, 11 months ago

Incident:alert

upvoted 7 times

Yindave Highly Voted 3 years, 9 months ago

its a bit of a strange sentence, but yeah, Incident's the correct awnser

upvoted 6 times

LegendaryZA Most Recent 1 year, 10 months ago

The answer is incidents https://learn.microsoft.com/en-us/defender-office-365/mdo-sec-ops-manage-incidents-and-alerts

upvoted 1 times

Daniel_Angelo 3 years, 4 months ago

Yes, Incident - Alert: Microsoft 365 Defender automatically aggregates the alerts and their associated information into an incident.

upvoted 3 times

Nicochet 3 years, 6 months ago

Incidents

upvoted 3 times

FBrabble 3 years, 9 months ago

yes Incident since it is a thing that happened triggering an alert

upvoted 4 times

IXone 3 years, 10 months ago

Correct

upvoted 3 times

Zeus009 3 years, 11 months ago

Correct

upvoted 3 times

Question #57 *Topic 1*

What are two capabilities of Microsoft Defender for Endpoint? Each correct selection presents a complete solution.
NOTE: Each correct selection is worth one point.

A. automated investigation and remediation

B. transport encryption

C. shadow IT detection

D. attack surface reduction

Suggested Answer: *A, D*
Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide

Community vote distribution
AD (100%)

An_is_here Highly Voted 5 years, 1 month ago
Answers are CORRECT Microsoft Defender for Endpoint offers automatic investigation and remediation capabilities that help reduce the volume of alerts in minutes at scale. While The attack surface reduction set of capabilities provides the first line of defence in the stack.
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide#microsoft-defender-for-endpoint
upvoted 35 times

Baba65Baba Highly Voted 4 years, 6 months ago
AD is correct
upvoted 7 times

2daedf0 Most Recent 1 year, 4 months ago
correct
upvoted 1 times

LegendaryZA 1 year, 10 months ago
The answer is: automated investigation and remediation attack surface reduction https://learn.microsoft.com/en-us/defender-endpoint/microsoft-defender-endpoint
upvoted 3 times

RahulX 2 years, 11 months ago
A. automated investigation and remediation D. attack surface reduction
upvoted 1 times

Darkfire 3 years ago
Answers are correct https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide
upvoted 1 times

manofsteel9 3 years, 2 months ago
Correct! By excluding non-related statements.
upvoted 1 times

Charly0710 3 years, 7 months ago
AD https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint?view=o365-worldwide
upvoted 2 times

yonie 3 years, 7 months ago
Voted AD
upvoted 3 times

IXone 3 years, 10 months ago
A D CORRECT
upvoted 2 times

abilioneto 3 years, 10 months ago
correct

upvoted 2 times

Siphe 4 years, 3 months ago

Voted A,D

upvoted 3 times

Eric02 4 years, 4 months ago

Voted AD

upvoted 3 times

Chief 4 years, 5 months ago

https://docs.microsoft.com/en-us/learn/modules/describe-threat-protection-with-microsoft-365-defender/5-describe-defender-endpoint

upvoted 2 times

sounakroy 4 years, 6 months ago

CORRECT

upvoted 2 times

Question #58 *Topic 1*

DRAG DROP -

Match the Azure networking service to the appropriate description.

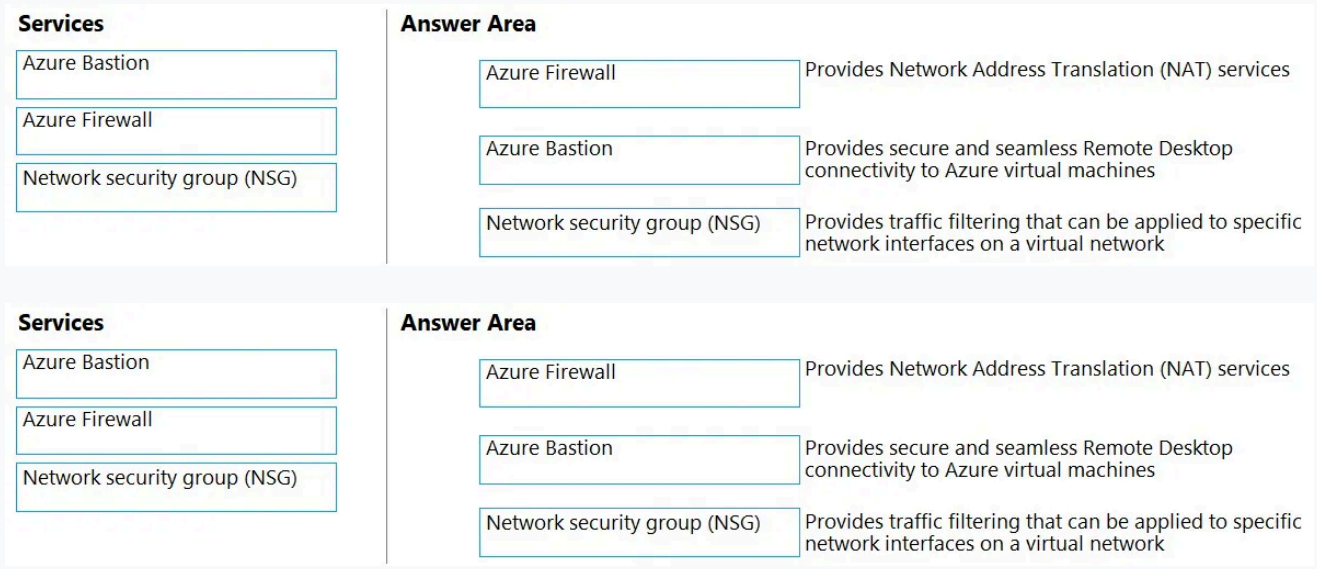
To answer, drag the appropriate service from the column on the left to its description on the right. Each service may be used once, more than once, or not at all.

NOTE: Each correct match is worth one point.

Select and Place:



Suggested Answer:



Box 1: Azure Firewall - Azure Firewall provide Source Network Address Translation and Destination Network Address Translation.

Box 2: Azure Bastion - Azure Bastion provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS. Box 3: Network security group (NSG) You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network. Reference: https://docs.microsoft.com/en-us/azure/networking/fundamentals/networking-overview https://docs.microsoft.com/en-us/azure/bastion/bastion-overview https://docs.microsoft.com/en-us/azure/firewall/features https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

Chris2pher Highly Voted 3 years, 8 months ago

That is correct. Only azure firewall can translate SNAT/DNAT while NSG cannot. But it can filter traffic. Firewall Bastion NSG

upvoted 11 times

megan_poirier Most Recent 1 year ago

Correct: Firewall Bastion NSG On exam today August 2025

upvoted 1 times

LegendaryZA 1 year, 10 months ago

The answer is: Azure Firewall Azure Bastion Network security group (NSG)

upvoted 1 times

NoursBear 2 years, 2 months ago

https://learn.microsoft.com/en-gb/training/modules/describe-basic-security-capabilities-azure/3-describe-what-azure-firewall

upvoted 1 times

RahulX 2 years, 11 months ago

Correct Azure Firewall Bastion NSG

upvoted 1 times

furq2904 3 years, 1 month ago

appeared on July 1st 2023

upvoted 1 times

bigelmo_elmo 3 years, 1 month ago

Guys its a trick question don't get confused , the given answers are correct

upvoted 2 times

manofsteel9 3 years, 2 months ago

answer is correct: Firewall, Bastion, NSG

upvoted 1 times

churkin6 3 years, 5 months ago

Firewall Bastion NSG

upvoted 1 times

dinodinobr 3 years, 9 months ago

NSG Bastion FirewallNSG doesn't provide NAT capabilities bro. This is what Azure Firewall does. NSG can be applied to NIC or subnet. The answer is Azure Firewall, Azure Bastion and NSG.But the answer says Firewall Bastion NSG Which is correct?1st option is very unclear to me 2. Bastion 3. NSG

upvoted 2 times

dinodinobr 3 years, 9 months ago

NSG Bastion Firewall

upvoted 2 times

walkaway 3 years, 7 months ago

NSG doesn't provide NAT capabilities bro. This is what Azure Firewall does. NSG can be applied to NIC or subnet. The answer is Azure Firewall, Azure Bastion and NSG.

upvoted 2 times

SUBRRA01 3 years, 9 months ago

But the answer says Firewall Bastion NSG

Which is correct?

upvoted 1 times

SUBRRA01 3 years, 9 months ago

But the answer says Firewall Bastion NSG Which is correct?1st option is very unclear to me 2. Bastion 3. NSG

upvoted 1 times

allwn 3 years, 9 months ago

1st option is very unclear to me 2. Bastion 3. NSG

upvoted 1 times

IXone 3 years, 10 months ago

CORRECT

upvoted 3 times

SiDoCiOuS 3 years, 10 months ago

On the exam 10/18/2022.

upvoted 2 times

Yelad 4 years, 1 month ago

On the exam 10/07/2022

upvoted 3 times

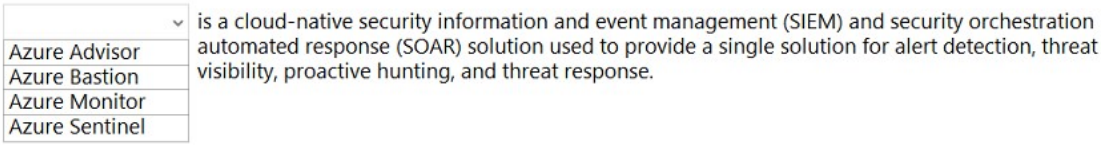
Question #59 *Topic 1*

HOTSPOT -

Select the answer that correctly completes the sentence.

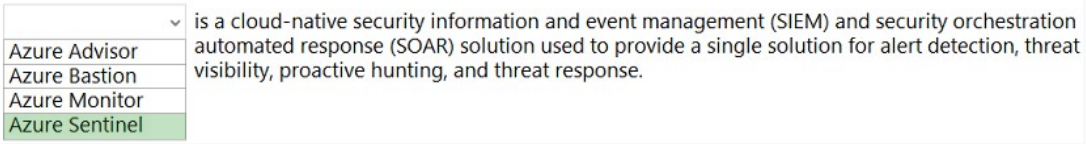
Hot Area:

Answer Area

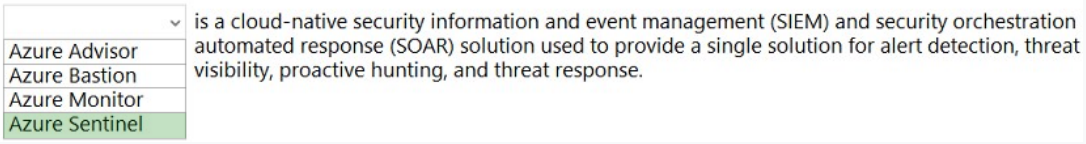


Suggested Answer:

Answer Area



Answer Area



Microsoft Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution. Reference: https://docs.microsoft.com/en-us/azure/sentinel/overview

An_is_here Highly Voted 5 years, 1 month ago

Answer is CORRECT Microsoft Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution. https://docs.microsoft.com/en-us/azure/sentinel/overview

upvoted 31 times

sokolsulejmani Highly Voted 4 years, 5 months ago

Answer is correct, keep in mind that name has changed to "Microsoft Sentinel"

upvoted 7 times

LegendaryZA Most Recent 1 year, 10 months ago

The answer is: Azure Sentinel https://learn.microsoft.com/en-us/azure/sentinel/overview?tabs=azure-portal

upvoted 1 times

RahulX 2 years, 11 months ago

Microsoft Azure Sentinel is Correct Ans.

upvoted 1 times

Darkfire 3 years ago

Answer is correct Keywords are SIEM / SOAR = Sentinal

upvoted 1 times

studytonight 3 years, 2 months ago

This was on the May 2023 exam.

upvoted 1 times

MoneyStacking 3 years, 6 months ago

Microsoft Siemtinel !!

upvoted 1 times

Lizzylizzy 3 years, 8 months ago

Azure sentinel

upvoted 4 times

IXone 3 years, 10 months ago

Microsoft Azure Sentine CORRECT

upvoted 2 times

abilioneto 3 years, 10 months ago

correct

upvoted 2 times

Zeus009 3 years, 11 months ago

Correct

upvoted 1 times

cantbeme 3 years, 12 months ago

on exam today

upvoted 3 times

jimmysplash 4 years, 2 months ago

keyword- siem

upvoted 2 times

itelessons 4 years, 2 months ago

SIEMtinel...

upvoted 4 times

misterperson 4 years, 3 months ago

correct

upvoted 1 times

Okeythaone 4 years, 3 months ago

yeah that's the correct answer

upvoted 1 times

Raze 4 years, 3 months ago

ans is correct

upvoted 1 times

Question #60 *Topic 1*

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Azure Defender can detect vulnerabilities and threats for Azure Storage.	○	○
Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	○	○
Azure Security Center can evaluate the security of workloads deployed to Azure or on-premises.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
Azure Defender can detect vulnerabilities and threats for Azure Storage.	○	○
Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	○	○
Azure Security Center can evaluate the security of workloads deployed to Azure or on-premises.	○	○

Answer Area

Statements	Yes	No
Azure Defender can detect vulnerabilities and threats for Azure Storage.	○	○
Cloud Security Posture Management (CSPM) is available for all Azure subscriptions.	○	○
Azure Security Center can evaluate the security of workloads deployed to Azure or on-premises.	○	○

Box 1: Yes - Microsoft Defender for Cloud provides security alerts and advanced threat protection for virtual machines, SQL databases, containers, web applications, your network, your storage, and more

Box 2: Yes - Cloud security posture management (CSPM) is available for free to all Azure users.

Box 3: Yes - Azure Security Center is a unified infrastructure security management system that strengthens the security posture of your data centers, and provides advanced threat protection across your hybrid workloads in the cloud - whether they're in Azure or not - as well as on premises. Reference: https://docs.microsoft.com/en-us/azure/security-center/azure-defender https://docs.microsoft.com/en-us/azure/security-center/defender-for-storage-introduction https://docs.microsoft.com/en-us/azure/security-center/security-center-introduction

sokolsulejmani Highly Voted 4 years, 5 months ago

keep in mind that Azure Security Center and Azure Defender are now called "Microsoft Defender for Cloud"

upvoted 50 times

danialonso Highly Voted 4 years, 11 months ago

All is correct!

upvoted 25 times

megan_poirier Most Recent 1 year ago

On exam today August 2025

upvoted 1 times

LegendaryZA 1 year, 10 months ago

The answer is: Yes, Yes, Yes https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction
https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-storage-introduction

upvoted 1 times

NoursBear 2 years, 2 months ago

second one is N foundational cspm is free Cloud Security cspm is not

upvoted 1 times

RahulX 2 years, 11 months ago

YES YES YES

upvoted 1 times

Curious76 2 years, 11 months ago

YYY Azure Security Center, which helps you protect workloads running in Azure against cyber threats, can now also be used to secure workloads running on-premises and in other clouds. Managing security across increasingly distributed infrastructure is complex and can create gaps that are exploited by attackers.

upvoted 2 times

furq2904 3 years, 1 month ago

appeared on July 1st 2023

upvoted 1 times

StressFree 3 years, 4 months ago

Microsoft Defender for Cloud its the new name for them

upvoted 2 times

Sorcia25 3 years, 5 months ago

Currently, the plan that is enabled by default is "Foundational CSMP", the new "Defender CSPM" isn't enabled... 'cause it will cost after the preview ends. Next week I present the exam, and if the Question was updated I'll pass my report here...

upvoted 2 times

Lille_89 3 years, 8 months ago

Correct

upvoted 4 times

RJJz 3 years, 8 months ago

cORRECT

upvoted 3 times

Yindave 3 years, 9 months ago

i hate those 'what kind of subscription support this feature' questions, but lucky i've got this one correct, all of them are YesI am happy for you.

upvoted 8 times

Yindave 3 years, 9 months ago

i hate those 'what kind of subscription support this feature' questions, but lucky i've got this one correct, all of them are Yes

upvoted 8 times

obaali1990 3 years, 5 months ago

I am happy for you.

upvoted 1 times

IXone 3 years, 10 months ago

CORRECT

upvoted 3 times

SiDoCiOuS 3 years, 10 months ago

On the exam 10/18/2022.

upvoted 4 times

hihiha 3 years, 10 months ago

I need all exam

upvoted 1 times

smartin2010 3 years, 10 months ago

Correct

upvoted 1 times

Question #61 *Topic 1*

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

You can use [ ] in the Microsoft 365 security center to view an aggregation of alerts that relate to the same attack.

- Reports
- Hunting
- Attack simulator
- Incidents

Suggested Answer:

Answer Area

You can use [Incidents] in the Microsoft 365 security center to view an aggregation of alerts that relate to the same attack.

- Reports
- Hunting
- Attack simulator
- Incidents

Answer Area

You can use [Incidents] in the Microsoft 365 security center to view an aggregation of alerts that relate to the same attack.

- Reports
- Hunting
- Attack simulator
- Incidents

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender/threat-analytics?view=o365-worldwide

Breino Highly Voted 5 years ago

Incidents: https://docs.microsoft.com/en-us/microsoft-365/security/defender/incidents-overview?view=o365-worldwide

upvoted 24 times

Alessandro_L Highly Voted 4 years, 6 months ago

Incidents - CORRECT

upvoted 5 times

LegendaryZA Most Recent 1 year, 10 months ago

The answer is: Incidents https://learn.microsoft.com/en-us/defender-xdr/incidents-overview

upvoted 1 times

MoneyStacking 3 years, 6 months ago

Indicents > alerts

upvoted 4 times

johnegil 4 years, 1 month ago

Appeared on exam 12/07/2022

upvoted 2 times

Raze 4 years, 3 months ago

ans is correct

upvoted 2 times

cyber_rip 4 years, 4 months ago

correct

upvoted 2 times

Cereb7 4 years, 4 months ago

Same link: " A view of threat-related incidents which aggregate alerts into end-to-end attack stories across Microsoft Defender for Endpoint and Microsoft Defender for Office 365 to reduce the work queue, as well as simplify and speed up your investigation."

upvoted 2 times

Surjit24 4 years, 5 months ago

Reports can allow Aggregation

upvoted 3 times

Chris_Chen 4 years, 7 months ago

Correct

upvoted 1 times

Melwin86 5 years, 1 month ago

correct

upvoted 2 times

Question #62 *Topic 1*

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Network security groups (NSGs) can deny inbound traffic from the internet.	○	○
Network security groups (NSGs) can deny outbound traffic to the internet.	○	○
Network security groups (NSGs) can filter traffic based on IP address, protocol, and port.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
Network security groups (NSGs) can deny inbound traffic from the internet.	○	○
Network security groups (NSGs) can deny outbound traffic to the internet.	○	○
Network security groups (NSGs) can filter traffic based on IP address, protocol, and port.	○	○

Answer Area

Statements	Yes	No
Network security groups (NSGs) can deny inbound traffic from the internet.	○	○
Network security groups (NSGs) can deny outbound traffic to the internet.	○	○
Network security groups (NSGs) can filter traffic based on IP address, protocol, and port.	○	○

You can use an Azure network security group to filter network traffic to and from 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. Reference: https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

Art3 Highly Voted 4 years, 11 months ago

correct!

upvoted 29 times

Jitusrit Highly Voted 4 years, 9 months ago

Correct

upvoted 9 times

megan_poirier Most Recent 1 year ago

On exam today August 2025

upvoted 1 times

LegendaryZA 1 year, 10 months ago

The answer is: Yes, Yes, Yes https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

upvoted 1 times

Melvinpisa 2 years, 6 months ago

So basically NSG can do everything that an Azure Firewall can do with the exception of NAT.

upvoted 1 times

RahulX 2 years, 11 months ago

YES YES YES

upvoted 1 times

johnegil 4 years, 1 month ago

Appeared on exam 12/07/2022

upvoted 5 times

BN7 4 years, 2 months ago

correct!

upvoted 2 times

KikaJ 4 years, 2 months ago

correct

upvoted 2 times

misterperson 4 years, 3 months ago

correct

upvoted 2 times

krnjtSingh 4 years, 3 months ago

correct

upvoted 1 times

maheshwaghmare 4 years, 3 months ago

Correct!

upvoted 2 times

Raze 4 years, 3 months ago

ans is correct

upvoted 1 times

jingling 4 years, 4 months ago

correct

upvoted 1 times

Chris_Chen 4 years, 7 months ago

Correct

upvoted 2 times

Adriamcam 4 years, 9 months ago

correct

upvoted 3 times

Question #63 *Topic 1*

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Microsoft Intune can be used to manage Android devices.	○	○
Microsoft Intune can be used to provision Azure subscriptions.	○	○
Microsoft Intune can be used to manage organization-owned devices and personal devices.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
Microsoft Intune can be used to manage Android devices.	○	○
Microsoft Intune can be used to provision Azure subscriptions.	○	○
Microsoft Intune can be used to manage organization-owned devices and personal devices.	○	○

Answer Area

Statements	Yes	No
Microsoft Intune can be used to manage Android devices.	○	○
Microsoft Intune can be used to provision Azure subscriptions.	○	○
Microsoft Intune can be used to manage organization-owned devices and personal devices.	○	○

Reference: https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune https://docs.microsoft.com/en-us/mem/intune/fundamentals/what-is-device-management

lgab Highly Voted 4 years, 12 months ago

Correct

upvoted 19 times

Whyiest Highly Voted 3 years, 7 months ago

Correct. Note that Intune does not have something to deal with provisioning ressources. Intune mainly allow you to manage endpoints.

upvoted 6 times

LegendaryZA Most Recent 1 year, 10 months ago

The answer is: Yes, No, Yes https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-device-management

upvoted 1 times

NoursBear 2 years, 2 months ago

Am sure the third one is correct but it's a bit anbiguous. You can only manage personal devices to a certain point

upvoted 1 times

jientifelmalti 2 years, 9 months ago

Correct!

upvoted 1 times

RahulX 2 years, 11 months ago

YES NO YES

upvoted 1 times

Molota 3 years, 2 months ago

Y N Y So correct answers

upvoted 1 times

obaali1990 3 years, 5 months ago

The third answer: what type of organizational devices is the question asking?

upvoted 1 times

Nicochet 3 years, 6 months ago

YNY correct

upvoted 1 times

CAPME22 3 years, 7 months ago

You can have azure subscription without intune This is correct - YNY

upvoted 2 times

clem24 4 years, 2 months ago

Correct

upvoted 1 times

misterperson 4 years, 3 months ago

correct

upvoted 1 times

fasttony77 4 years, 7 months ago

Correct

upvoted 1 times

Adil251 4 years, 8 months ago

CORRECT

upvoted 2 times

Question #64 *Topic 1*

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
You can create one Azure Bastion per virtual network.	○	○
Azure Bastion provides secure user connections by using RDP.	○	○
Azure Bastion provides a secure connection to an Azure virtual machine by using the Azure portal.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
You can create one Azure Bastion per virtual network.	○	○
Azure Bastion provides secure user connections by using RDP.	○	○
Azure Bastion provides a secure connection to an Azure virtual machine by using the Azure portal.	○	○

Answer Area

Statements	Yes	No
You can create one Azure Bastion per virtual network.	○	○
Azure Bastion provides secure user connections by using RDP.	○	○
Azure Bastion provides a secure connection to an Azure virtual machine by using the Azure portal.	○	○

Reference: https://docs.microsoft.com/en-us/azure/bastion/bastion-overview https://docs.microsoft.com/en-us/azure/bastion/tutorial-create-host-portal

mavexamtops Highly Voted 4 years, 11 months ago

Correct. https://docs.microsoft.com/en-us/azure/bastion/bastion-overview

upvoted 18 times

lgab Highly Voted 4 years, 12 months ago

Correct

upvoted 10 times

LegendaryZA Most Recent 1 year, 10 months ago

The answer is: Yes, Yes, Yes https://learn.microsoft.com/en-us/azure/bastion/bastion-overview

upvoted 1 times

RahulX 2 years, 11 months ago

YES YES YES

upvoted 1 times

Rispid 3 years, 5 months ago

Tricky question

upvoted 3 times

DikSoft 3 years, 8 months ago

Asure Bastion act as client using RDP/SSH connection to servers/VMs. End-User do not use RDP when it connect TO Bastion. YNY

upvoted 8 times

DikSoft 3 years, 8 months ago

Asure Bastion act as client using RDP/SSH connection to servers/VMs. End-User do not use RDP when it connect TO Bastion. YNYI believe it still uses rdp however only via the admin portal, not direct.

upvoted 8 times

ezapper2 3 years, 6 months ago

I believe it still uses rdp however only via the admin portal, not direct.

upvoted 2 times

cantbeme 3 years, 12 months ago

on exam today

upvoted 2 times

clem24 4 years, 2 months ago

YYY is correct

upvoted 1 times

Cereb7 4 years, 4 months ago

“Bastion provides secure RDP and SSH connectivity to all of the VMs in the virtual network in which it is provisioned.” So answer is correct needed to know with exam in 2 days.

upvoted 1 times

fred2305 4 years, 4 months ago

I should say YNY, SSH brings security, not RDPRDP session secured because is over TLSRDP is by default encrypted and mutualy authenticated so yes it is secure and there is no diffrence between RDP and SSH form a threat modeling persprective.

upvoted 2 times

fred2305 4 years, 4 months ago

I should say YNY, SSH brings security, not RDP

upvoted 2 times

Bulldozzer 4 years, 3 months ago

RDP session secured because is over TLS

upvoted 3 times

Bulldozzer 4 years, 3 months ago

RDP session secured because is over TLSRDP is by default encrypted and mutualy authenticated so yes it is secure and there is no diffrence between RDP and SSH form a threat modeling persprective.

upvoted 3 times

yaza85 4 years, 3 months ago

RDP is by default encrypted and mutualy authenticated so yes it is secure and there is no diffrence between RDP and SSH form a threat modeling persprective.

upvoted 1 times

Question #65 *Topic 1*

What feature in Microsoft Defender for Endpoint provides the first line of defense against cyberthreats by reducing the attack surface?

A. automated remediation

B. automated investigation

C. advanced hunting

D. network protection

Suggested Answer: *D*

Network protection helps protect devices from Internet-based events. Network protection is an attack surface reduction capability. Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/network-protection?view=o365-worldwide

Community vote distribution



Beng_ali Highly Voted 4 years, 7 months ago

Answer is D

upvoted 5 times

Yelad Highly Voted 4 years, 1 month ago

On the exam 10/07/2022

upvoted 5 times

LegendaryZA Most Recent 1 year, 10 months ago

The answer is: network protection https://learn.microsoft.com/en-us/defender-endpoint/network-protection#overview-of-network-protection

upvoted 1 times

czaaa 2 years, 10 months ago

It's technically ASR, but I guess D is also correct since it is network protection.

upvoted 1 times

RahulX 2 years, 11 months ago

D is correct ans.

upvoted 1 times

furq2904 3 years, 1 month ago

appeared on July 1st 2023

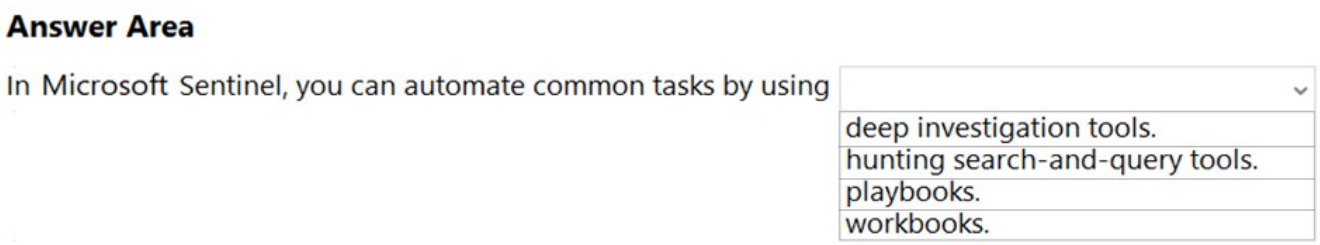
upvoted 1 times

Question #66 *Topic 1*

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:



Suggested Answer:



Reference: https://docs.microsoft.com/en-us/azure/sentinel/overview

Whyiest Highly Voted 3 years, 7 months ago

Correct answer. Workbooks in Azure Sentinel are interactive dashboards that allow users to explore and analyze security data. They provide a visual representation of security data, allowing users to quickly identify patterns and trends. Workbooks can be customized to display specific data and can be shared with other users. Playbooks in Azure Sentinel are automated response capabilities that allow users to take action on security incidents. They provide a set of predefined playbooks and actions to help users respond to security incidents quickly and effectively. Playbooks can be triggered by specific events or conditions, and can be customized to fit the needs of the organization. They also have the capability to integrate with other Azure services and third-party tools, and can be used to automate incident triage, investigations, and remediation tasks. In summary, Workbooks are for analysis and visualization of security data, whereas Playbooks are for automated incident response.

upvoted 23 times

Geolem Highly Voted 3 years, 11 months ago

https://learn.microsoft.com/en-us/azure/sentinel/overview#automate-and-orchestrate-common-tasks-by-using-playbooks

upvoted 12 times

LegendaryZA Most Recent 1 year, 10 months ago

The answer is: playbooks https://learn.microsoft.com/en-us/azure/sentinel/automation/automation#playbooks

upvoted 1 times

RahulX 2 years, 11 months ago

Playbooks is the correct ans.

upvoted 1 times

Darkfire 3 years ago

Answer is correct Keyword = Workbooks = Microsoft SentinalExcuse my language Playbooks

upvoted 1 times

Darkfire 3 years ago

Answer is correct

Keyword = Workbooks = Microsoft Sentinal

upvoted 1 times

Darkfire 3 years ago

Excuse my language Playbooks

upvoted 1 times

StressFree 3 years, 4 months ago

the word here is AUTOMATE, to automate must be Playbooks

upvoted 2 times

Nicochet 3 years, 6 months ago

Playbooks

upvoted 2 times

TheB 3 years, 7 months ago

Answer is correct Playbook

upvoted 3 times

Question #67 *Topic 1*

Which two types of resources can be protected by using Azure Firewall? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Azure virtual machines

B. Azure Active Directory (Azure AD) users

C. Microsoft Exchange Online inboxes

D. Azure virtual networks

E. Microsoft SharePoint Online sites

Suggested Answer: *D, E*
Official Answer: DE

Community vote distribution
AD (95%) (5%

Hellboy Highly Voted 4 years, 9 months ago
A and D
upvoted 60 times

Cepul Highly Voted 4 years, 8 months ago
A and D are correct
upvoted 23 times

nicky_nyasha Most Recent 1 year, 5 months ago
A & D are correct
upvoted 1 times

LegendaryZA 1 year, 10 months ago
The answer is: Azure virtual machines Azure virtual networks https://learn.microsoft.com/en-us/azure/firewall/overview
upvoted 1 times

Faceless_Void 1 year, 11 months ago
Azure Firewall = Network Address Translation, not the Firewall appliance that you think it is.
upvoted 1 times

Genichiro 2 years, 3 months ago
A and D are correct.
upvoted 1 times

zeek_9 2 years, 6 months ago
D. Azure virtual networks E. Microsoft SharePoint Online sites Azure Firewall is specifically designed to secure and control traffic between Azure virtual networks and the internet (option D). While it can provide protection for certain types of Microsoft 365 services, such as SharePoint Online sites (option E), it is not primarily focused on protecting individual Azure virtual machines (option A). Therefore, the correct selections are D and E.
upvoted 4 times

gwbr 2 years, 7 months ago
Selected Answer: DE
it is confusing and not exactly intuitive but I had to agree that D&E are the correct answers since Virtual Machine is not exactly a network resource per se, while Sharepoint is a network application. "You can use the Azure Firewall built-in Service Tags and FQDN tags to allow outbound communication to Office 365 endpoints and IP addresses." -- https://learn.microsoft.com/en-us/azure/firewall/protect-office-365
upvoted 1 times

gwbr 2 years, 7 months ago
it is confusing and not exactly intuitive but I had to agree that D&E are the correct answers since Virtual Machine is not exactly a network resource per se, while Sharepoint is a network application. "You can use the Azure Firewall built-in Service Tags and FQDN tags to allow outbound communication to Office 365 endpoints and IP addresses." -- https://learn.microsoft.com/en-us/azure/firewall/protect-office-365yeah I've been like half an hour on this and I think I may go with the minority on this onel may have changed my mind now
upvoted 1 times

NoursBear 2 years, 2 months ago

yeah I've been like half an hour on this and I think I may go with the minority on this one

upvoted 1 times

NoursBear 2 years, 2 months ago

yeah I've been like half an hour on this and I think I may go with the minority on this oneI may have changed my mind now

upvoted 1 times

NoursBear 2 years, 2 months ago

I may have changed my mind now

upvoted 1 times

Paddy71 2 years, 8 months ago

Protecting SharePoint Online with an Azure Firewall can provide several benefits. Azure Firewall is a cloud-native stateful firewall as a service that can be deployed in your virtual networks or in Azure Virtual WAN hub deployments for filtering traffic flowing between cloud resources, the Internet, and on-premises. You can create rules or policies specifying allow/deny traffic using layer 3 to layer 7 controls. You can also filter traffic going to the internet using both Azure Firewall and third parties by directing some or all traffic through third-party security providers for advanced filtering and user protection. This can help to improve the security of your SharePoint Online deployment by providing an additional layer of protection against web attacks and simplifying security management without requiring any application changes.

upvoted 2 times

schepkev 2 years, 8 months ago

A and D

upvoted 1 times

Wilderness 2 years, 9 months ago

A and D is correct

upvoted 1 times

uikty 2 years, 9 months ago

"E" is an absurd incorrect answer that I don't know where it comes from A and D

upvoted 2 times

Grimz 2 years, 10 months ago

A and D

upvoted 1 times

RahulX 2 years, 11 months ago

A and D is correct ans. Azure VM Azure Vnet

upvoted 1 times

theptr 2 years, 11 months ago

Q And D

upvoted 1 times

Darkfire 3 years ago

Should be A & D

upvoted 1 times

rsb7 3 years, 1 month ago

Correct answer AD

upvoted 1 times

Question #68 *Topic 1*

You plan to implement a security strategy and place multiple layers of defense throughout a network infrastructure.
Which security methodology does this represent?

A. threat modeling

B. identity as the security perimeter

C. defense in depth

D. the shared responsibility model

Suggested Answer: *C*
Reference: https://docs.microsoft.com/en-us/learn/modules/secure-network-connectivity-azure/2-what-is-defense-in-depth

Community vote distribution
C (100%)

eddie_network_jedi Highly Voted 4 years, 9 months ago
right, "defense" is the keyword here.
upvoted 11 times

Random_Mane_111 Highly Voted 4 years, 6 months ago
C is correct
upvoted 5 times

LegendaryZA Most Recent 1 year, 10 months ago
The answer is: defense in depth https://learn.microsoft.com/en-us/training/modules/describe-security-concepts-methodologies/3-describe-defense-depth
upvoted 1 times

Fabulous_7 2 years, 8 months ago
If someone missed this question; obviously you're not qualified for the exam..... 'DEFENSE INDEPTH'
upvoted 1 times

RahulX 2 years, 11 months ago
C. defense in depth
upvoted 1 times

LegendZA 3 years, 5 months ago
Correct
upvoted 1 times

churkin6 3 years, 5 months ago
C is Correct
upvoted 2 times

TheB 3 years, 7 months ago
keyword "multiple layers of defense" = defense In-depth
upvoted 2 times

amsioso 4 years ago
layers=depth
upvoted 2 times

TJ001 4 years, 7 months ago
right answers Defence in depth spanning Data, Application, Compute, Network , Perimeter , Identity and Access and Physical. Of this physical is more of cloud provider responsibility
upvoted 3 times

Question #69 *Topic 1*

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Microsoft Defender for Endpoint can protect Android devices.	○	○
Microsoft Defender for Endpoint can protect Azure virtual machines that run Windows 10.	○	○
Microsoft Defender for Endpoint can protect Microsoft SharePoint Online sites and content from viruses.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
Microsoft Defender for Endpoint can protect Android devices.	○	○
Microsoft Defender for Endpoint can protect Azure virtual machines that run Windows 10.	○	○
Microsoft Defender for Endpoint can protect Microsoft SharePoint Online sites and content from viruses.	○	○

Answer Area

Statements	Yes	No
Microsoft Defender for Endpoint can protect Android devices.	○	○
Microsoft Defender for Endpoint can protect Azure virtual machines that run Windows 10.	○	○
Microsoft Defender for Endpoint can protect Microsoft SharePoint Online sites and content from viruses.	○	○

2cent2 Highly Voted 3 years, 7 months ago

YYN, because "MS Defender for O365" is taking care of Sharepoint Online

upvoted 7 times

phatboi 4 years, 8 months ago

Y,Y,N https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/android-intune?view=o365-worldwide#:~:text=Defender%20for%20Endpoint%20supports%20Device,up%20VPN%20service%20while%20onboarding.

upvoted 6 times

LegendaryZA Most Recent 1 year, 10 months ago

The answer is: Yes, Yes, No https://learn.microsoft.com/en-us/defender-endpoint/non-windows?view=o365-worldwide#microsoft-defender-for-endpoint-on-android https://learn.microsoft.com/en-us/defender-endpoint/supported-capabilities-by-platform?view=o365-worldwide

upvoted 1 times

azhrhsn 2 years, 7 months ago

Yes, Yes, No

upvoted 1 times

Tahamaffia 2 years, 11 months ago

Got this question on my exam 05/09/2023

upvoted 2 times

RahulX 2 years, 11 months ago

YES YES NO

upvoted 1 times

LegendZA 3 years, 5 months ago

Correct - Y, Y, N

upvoted 2 times

Nicochet 3 years, 6 months ago

YYN is correct.

upvoted 2 times

SleepyBear 3 years, 7 months ago

shouldn't be all YYY. The Sharepoint is part of Office 365.

upvoted 2 times

SleepyBear 3 years, 7 months ago

shouldn't be all YYY. The Sharepoint is part of Office 365.Endpoint is for resources, Sharepoint Online Sites is PaaS

upvoted 2 times

Eduardo_S 3 years, 6 months ago

Endpoint is for resources, Sharepoint Online Sites is PaaS

upvoted 3 times

cantbeme 3 years, 12 months ago

on exam today

upvoted 1 times

johnegil 4 years, 1 month ago

Appeared on exam 12/07/2022

upvoted 2 times

mmNYC 4 years, 6 months ago

WHO PROTECTS SHARE POINT?Azure WAFBack-upsMicrosoft Defender for Office 365I thought same

upvoted 5 times

mmNYC 4 years, 6 months ago

WHO PROTECTS SHARE POINT?

upvoted 5 times

amgfishin 3 years, 7 months ago

Azure WAF

upvoted 2 times

skycrap 3 years, 7 months ago

Back-ups

upvoted 2 times

Hot_156 Highly Voted 4 years, 6 months ago

Microsoft Defender for Office 365

upvoted 22 times

Marisasa58 3 years, 10 months ago

I thought same

upvoted 1 times

TJ001 4 years, 7 months ago

Y, Y, N

upvoted 1 times

Question #70 *Topic 1*

What can you use to scan email attachments and forward the attachments to recipients only if the attachments are free from malware?

A. Microsoft Defender for Office 365

B. Microsoft Defender Antivirus

C. Microsoft Defender for Identity

D. Microsoft Defender for Endpoint

Suggested Answer: *A*

Reference: https://docs.microsoft.com/en-us/office365/servicedescriptions/office-365-advanced-threat-protection-service-description

Community vote distribution

A (100%)

LegendaryZA Most Recent 1 year, 10 months ago

The answer is Microsoft Defender for Office 365. https://learn.microsoft.com/en-us/defender-office-365/safe-attachments-about

upvoted 1 times

RahulX 2 years, 11 months ago

A. Microsoft Defender for Office 365

upvoted 1 times

LegendZA 3 years, 5 months ago

Correct

upvoted 1 times

Nicochet 3 years, 6 months ago

A Defender for O365 is the correct answer.

upvoted 2 times

TheB 3 years, 7 months ago

Defender for O365 is the correct answer

upvoted 3 times

Mcelona 3 years, 7 months ago

Correct

upvoted 2 times

yonie 3 years, 7 months ago

Easy A

upvoted 1 times

Mcelona 3 years, 8 months ago

A is the right answer

upvoted 1 times

pinda 3 years, 9 months ago

Correct

upvoted 1 times

cantbeme 3 years, 12 months ago

on exam today

upvoted 1 times

johnegil 4 years, 1 month ago

Appeared on exam 12/07/2022

upvoted 2 times

Kamoshika 4 years, 2 months ago

Answer is A

upvoted 1 times

Beng_ali 4 years, 7 months ago

Answer is A

upvoted 1 times

Question #71 *Topic 1*

Which feature provides the extended detection and response (XDR) capability of Azure Sentinel?

A. integration with the Microsoft 365 compliance center

B. support for threat hunting

C. integration with Microsoft 365 Defender

D. support for Azure Monitor Workbooks

Suggested Answer: *C*

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender/eval-overview?view=o365-worldwide

Community vote distribution

C (100%)

JayHall Highly Voted 4 years, 9 months ago

Correct The Microsoft 365 Defender connector for Azure Sentinel (preview) sends all Microsoft 365 Defender incidents and alerts information to Azure Sentinel and keeps the incidents synchronized. Once you add the connector, Microsoft 365 Defender incidents—which include all associated alerts, entities, and relevant information received from Microsoft Defender for Endpoint, Microsoft Defender for Identity, Microsoft Defender for Office 365, and Microsoft Cloud App Security—are streamed to Azure Sentinel as security information and event management (SIEM) data, providing you with context to perform triage and incident response with Azure Sentinel. Once in Azure Sentinel, incidents remain bi-directionally synchronized with Microsoft 365 Defender, allowing you to take advantage of the benefits of both the Microsoft 365 Defender portal and Azure Sentinel in the Azure portal for incident investigation and response. https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender-integration-with-azure-sentinel?view=o365-worldwide

upvoted 39 times

2cent2 Highly Voted 3 years, 7 months ago

Microsoft Sentinel is a cloud-native SIEM tool; Microsoft 365 Defender provides XDR capabilities for end-user environments (email, documents, identity, apps, and endpoint); and Microsoft Defender for Cloud provides XDR capabilities for infrastructure and multi-cloud platforms including virtual machines, databases, containers, and IoT.

upvoted 7 times

LegendaryZA Most Recent 1 year, 10 months ago

The answer is: integration with Microsoft 365 Defender. https://learn.microsoft.com/en-us/defender-xdr/microsoft-365-defender-integration-with-azure-sentinel

upvoted 1 times

RahulX 2 years, 11 months ago

C. integration with Microsoft 365 Defender.

upvoted 1 times

Question #72 *Topic 1*

What can you use to provide threat detection for Azure SQL Managed Instance?

A. Microsoft Secure Score

B. application security groups

C. Microsoft Defender for Cloud

D. Azure Bastion

Suggested Answer: *C*
Official Answer: C

Community vote distribution
C (100%)

OrangeSG Highly Voted 3 years, 8 months ago
Microsoft Defender for SQL is a Defender plan in Microsoft Defender for Cloud. Microsoft Defender for SQL includes functionality for surfacing and mitigating potential database vulnerabilities, and detecting anomalous activities that could indicate a threat to your database. It provides a single go-to location for enabling and managing these capabilities. Microsoft Defender for SQL https://learn.microsoft.com/en-us/azure/azure-sql/database/azure-defender-for-sql
upvoted 12 times

KingChuang Highly Voted 3 years, 11 months ago
Correct. https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction
upvoted 6 times

OCGFSC Most Recent 1 year, 4 months ago
threat detection = Microsoft Defender for Cloud
upvoted 1 times

LegendaryZA 1 year, 10 months ago
The answer is: Microsoft Defender for Cloud. https://learn.microsoft.com/en-us/azure/azure-sql/database/azure-defender-for-sql?view=azuresql
upvoted 1 times

RahulX 2 years, 11 months ago
C. Microsoft Defender for Cloud
upvoted 1 times

beaikes 2 years, 11 months ago
threat detection = Defender
upvoted 1 times

LegendZA 3 years, 5 months ago
Correct
upvoted 1 times

Nicochet 3 years, 6 months ago
Correct. Defender for cloud
upvoted 2 times

Whyiest 3 years, 6 months ago
Correct
upvoted 2 times

Qongo 3 years, 7 months ago
Correct
upvoted 1 times

pinda 3 years, 9 months ago
Correct
upvoted 3 times

Burnie 3 years, 9 months ago
Correct.

upvoted 1 times

Question #73 *Topic 1*

HOTSPOT -

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Microsoft Secure Score in the Microsoft 365 security center can provide recommendations for Microsoft Cloud App Security.	○	○
From the Microsoft 365 Defender portal, you can view how your Microsoft Secure Score compares to the score of organizations like yours.	○	○
Microsoft Secure Score in the Microsoft 365 Defender portal gives you points if you address the improvement action by using a third-party application or software.	○	○

Suggested Answer:

Answer Area

Statements	Yes	No
Microsoft Secure Score in the Microsoft 365 security center can provide recommendations for Microsoft Cloud App Security.	○	○
From the Microsoft 365 Defender portal, you can view how your Microsoft Secure Score compares to the score of organizations like yours.	○	○
Microsoft Secure Score in the Microsoft 365 Defender portal gives you points if you address the improvement action by using a third-party application or software.	○	○

Answer Area

Statements	Yes	No
Microsoft Secure Score in the Microsoft 365 security center can provide recommendations for Microsoft Cloud App Security.	○	○
From the Microsoft 365 Defender portal, you can view how your Microsoft Secure Score compares to the score of organizations like yours.	○	○
Microsoft Secure Score in the Microsoft 365 Defender portal gives you points if you address the improvement action by using a third-party application or software.	○	○

delight_1 Highly Voted 4 years, 1 month ago

I was confused with the second answer at first... Now, i verified that Microsoft Secure Score is on Microsoft 365 Defender Portal - Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score?view=o365-worldwide

upvoted 8 times

delight_1 Highly Voted 4 years, 1 month ago

I was confused with the second answer at first... Now, i verified that Microsoft Secure Score is on Microsoft 365 Defender Portal - Reference: https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score?view=o365-worldwideYYY is correct. I was confused as well. https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score-history-metrics-trends?view=o365-worldwide#compare-your-score-to-organizations-like-yours

upvoted 8 times

Darkfire 3 years ago

YYY is correct. I was confused as well. https://learn.microsoft.com/en-us/microsoft-365/security/defender/microsoft-secure-score-history-metrics-trends?view=o365-worldwide#compare-your-score-to-organizations-like-yours

upvoted 3 times

Tumi21 4 years, 1 month ago

YYY is correct

upvoted 5 times

Lorello2023 Most Recent 1 year, 6 months ago

the last one for me is no

upvoted 2 times

LegendaryZA 1 year, 10 months ago

The answer is Yes, Yes, Yes https://learn.microsoft.com/en-us/defender-xdr/microsoft-secure-score

upvoted 1 times

RahulX 2 years, 11 months ago

YES YES YES

upvoted 1 times

obaali1990 3 years, 5 months ago

Y Y Y is correct

upvoted 3 times

Dj6668 3 years, 9 months ago

Organizations gain access to robust visualizations of metrics and trends, integration with other Microsoft products, score comparison with similar organizations, and much more. The score can also reflect when third-party solutions have addressed recommended actions.

upvoted 3 times

cantbeme 3 years, 12 months ago

on exam today

upvoted 3 times

amsioso 4 years ago

https://docs.microsoft.com/en-us/microsoft-365/security/defender/portals?view=o365-worldwide

upvoted 1 times

Yelad 4 years, 1 month ago

On the exam 10/07/2022

upvoted 3 times

xprience 4 years, 3 months ago

Correct

upvoted 4 times

Question #74 *Topic 1*

Which Azure Active Directory (Azure AD) feature can you use to restrict Microsoft Intune-managed devices from accessing corporate resources?

A. network security groups (NSGs)

B. Azure AD Privileged Identity Management (PIM)

C. conditional access policies

D. resource locks

Suggested Answer: *C*
Official Answer: C

Community vote distribution
C (100%)

Adriamcam Highly Voted 4 years, 9 months ago
correct
upvoted 18 times

LegendaryZA Most Recent 1 year, 10 months ago
The answer is: https://learn.microsoft.com/en-us/mem/intune/protect/conditional-access-intune-common-ways-use#device-based-conditional-access
upvoted 1 times

Anshul10 2 years, 5 months ago
Conditional Access Policy
upvoted 1 times

RahulX 2 years, 11 months ago
C. Conditional Access Policy.
upvoted 1 times

LegendZA 3 years, 5 months ago
Correct
upvoted 1 times

obaali1990 3 years, 5 months ago
Answer is correct
upvoted 2 times

TheB 3 years, 7 months ago
C is the answer
upvoted 3 times

Tanzy360 3 years, 11 months ago
C is the correct answer
upvoted 3 times

jim85 4 years, 6 months ago
This should be Compliance Policy, not conditional access policy, see https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-startedCompliance Policy are also NO Azure Active Directory (Azure AD) featureCompliance policies have nothing to do with "Access". Conditional access policies is the right answerThat's Rightthis is incorrect. compliance policy isn't one of the available answers and if it were available, it still has nothing to do with accessThis is the correct link but if you read it further it states: When you use Conditional Access, you can configure your Conditional Access policies to use the results of your device compliance policies to determine which devices can access your organizational resources. This access control is in addition to and separate from the actions for noncompliance that you include in your device compliance policies So answer C is correct in this case
upvoted 2 times

jim85 4 years, 6 months ago
This should be Compliance Policy, not conditional access policy, see https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started
upvoted 2 times

yaza85 4 years, 3 months ago

Compliance Policy are also NO Azure Active Directory (Azure AD) feature

upvoted 3 times

sokolsulejmani Highly Voted 4 years, 5 months ago

Compliance policies have nothing to do with "Access". Conditional access policies is the right answerThat's Right

upvoted 8 times

sokolsulejmani 4 years, 5 months ago

Compliance policies have nothing to do with "Access". Conditional access policies is the right answer

upvoted 8 times

j0rgevasquez 4 years, 5 months ago

That's Right

upvoted 3 times

CatoFong 4 years, 5 months ago

this is incorrect. compliance policy isn't one of the available answers and if it were available, it still has nothing to do with access

upvoted 5 times

luckyiki 3 years, 7 months ago

This is the correct link but if you read it further it states: When you use Conditional Access, you can configure your Conditional Access policies to use the results of your device compliance policies to determine which devices can access your organizational resources. This access control is in addition to and separate from the actions for noncompliance that you include in your device compliance policies So answer C is correct in this case

upvoted 3 times

Question #75 *Topic 1*

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

Azure Active Directory (Azure AD) Privileged Identity Management (PIM) Azure Defender Azure Sentinel Microsoft Cloud App Security	can use conditional access policies to control sessions in real time.

Suggested Answer:

Answer Area

Azure Active Directory (Azure AD) Privileged Identity Management (PIM) Azure Defender Azure Sentinel **Microsoft Cloud App Security**	can use conditional access policies to control sessions in real time.

Answer Area

Azure Active Directory (Azure AD) Privileged Identity Management (PIM) Azure Defender Azure Sentinel **Microsoft Cloud App Security**	can use conditional access policies to control sessions in real time.

Reference: https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security

An_is_here Highly Voted 5 years, 1 month ago

The answer is CORRECT. Using Conditional Access App Control protection to get real-time visibility and control over access and activities within your cloud apps. https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security#architecture

upvoted 45 times

Randy8 Highly Voted 4 years, 6 months ago

Microsoft Cloud App Security has been renamed to Microsoft Defender for Cloud Apps: https://techcommunity.microsoft.com/t5/itops-talk-blog/azure-security-product-name-changes-microsoft-ignite-november/ba-p/3004418?WT.mc_id=modinfra-48365-socuff

upvoted 25 times

LegendaryZA Most Recent 1 year, 10 months ago

The answer is: Microsoft Cloud App Security which is now called Microsoft Defender for Cloud Apps https://learn.microsoft.com/en-us/defender-cloud-apps/proxy-intro-aad#how-it-works

upvoted 2 times

LegendZA 3 years, 5 months ago

Correct - Microsoft Cloud App Security which is now Microsoft Defender for Cloud Apps

upvoted 2 times

cantbeme 3 years, 12 months ago

on exam today

upvoted 3 times

Yelad 4 years, 1 month ago

On the exam 10/07/2022

upvoted 3 times

domranmanhu 4 years, 4 months ago

Correct

upvoted 2 times

DemekeA 4 years, 5 months ago

Answer is correct

upvoted 3 times

abhmala1 4 years, 6 months ago

THIS CAME ON 15.2.22 EXAM

upvoted 7 times

Alessandro_L 4 years, 6 months ago

CORRECT

upvoted 1 times

Jitusrit 4 years, 9 months ago

Absolutely right.

upvoted 1 times

mileytores 4 years, 10 months ago

Es un CASB basicamente

upvoted 1 times

Nic1234 4 years, 11 months ago

correct

upvoted 1 times

P_2311 5 years ago

correct

upvoted 3 times

Melwin86 5 years, 1 month ago

corrct https://docs.microsoft.com/en-us/cloud-app-security/proxy-intro-aad

upvoted 5 times

Question #76 *Topic 1*

HOTSPOT -

Select the answer that correctly completes the sentence.

Hot Area:

Answer Area

Azure DDoS Protection Standard can be used to protect

- Azure Active Directory (Azure AD) applications.
- Azure Active Directory (Azure AD) users.
- resource groups.
- virtual networks.

Suggested Answer:

Answer Area

Azure DDoS Protection Standard can be used to protect

- Azure Active Directory (Azure AD) applications.
- Azure Active Directory (Azure AD) users.
- resource groups.
- virtual networks.

Answer Area

Azure DDoS Protection Standard can be used to protect

- Azure Active Directory (Azure AD) applications.
- Azure Active Directory (Azure AD) users.
- resource groups.
- virtual networks.

Reference: https://docs.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview

An_is_here Highly Voted 5 years, 1 month ago

Azure DDoS Protection Standard, combined with application design best practices, provides enhanced DDoS mitigation features to defend against DDoS attacks. It is automatically tuned to help protect your specific Azure resources in a virtual network. Protection is simple to enable on any new or existing virtual network, and it requires no application or resource changes. Since Azure Resources is not listed as part of the option, VIRTUAL NETWORK is the correct answer https://docs.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview

upvoted 43 times

Nepean Highly Voted 4 years, 7 months ago

Got 1000. Answer is correct.

upvoted 31 times

LegendaryZA Most Recent 1 year, 10 months ago

The answer is: virtual networks https://learn.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview

upvoted 2 times

NoursBear 2 years, 2 months ago

I think here is the key: Azure DDoS Protection protects at layer 3 and layer 4 network layers. For web applications protection at layer 7, you need to add protection at the application layer using a WAF offering. For more information, see Application DDoS protection.

upvoted 1 times

RahulX 2 years, 11 months ago

VIRTUAL NETWORK

upvoted 1 times

bigelmo_elmo 3 years, 1 month ago

Correct answer because DDos protection is a type of protection that happens in the networking layer.

upvoted 2 times

LegendZA 3 years, 5 months ago

Correct - Virtual network.

upvoted 2 times

ra1paul 3 years, 6 months ago

Correct Answer.

upvoted 2 times

Norasit 4 years, 4 months ago

I found this question in exam today but it is AZ-900!!!

upvoted 5 times

Alessandro_L 4 years, 6 months ago

CORRECT.

upvoted 3 times

thiaybovo 4 years, 8 months ago

CORRECT

upvoted 1 times

vakkil 4 years, 8 months ago

Technically answer should be all resources in a virtual network. as per the details mentioned in one of the feature i.e. Multi-Layered protection mentioned in the below link, directs the answer to be network layer protection (i.e. virtual network). https://docs.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview

upvoted 4 times

Jitusrit 4 years, 9 months ago

DDOS HAPPENs on IP based identity, so virtual network is correct. But what is the purpose then we can say to secure the application or resources.

upvoted 3 times

LoremanReturns 4 years, 10 months ago

"Azure DDoS Protection is enabled at the Virtual Network level" https://azure.microsoft.com/en-gb/pricing/details/ddos-protection/

upvoted 6 times

Ender3 4 years, 10 months ago

IMHO, both A and D are correct. But since only one answer can be given, I am in a quandary on how to answers in a real test. I guess I would take a 50/50 chance with D.

upvoted 1 times

alopezme 4 years, 10 months ago

Azure DDoS Protection is enabled at the Virtual Network level. All protected resource types within the Virtual Network will be automatically protected when Azure DDoS Protection is enabled on the Virtual Network. https://azure.microsoft.com/en-gb/pricing/details/ddos-protection/

upvoted 2 times