



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



## **CERTIFICATION TEST**

- [CertificationTest.net](https://CertificationTest.net) - Cheap & Quality Resources With Best Support

You need to recommend a solution to generate a monthly report of all the new Azure Resource Manager resource deployments in your subscription.

What should you include in the recommendation?

- A. the Change Tracking management solution
- B. Application Insights
- C. Azure Monitor action groups
- D. Azure Activity Log

**Suggested Answer: D**

Activity logs are kept for 90 days. You can query for any range of dates, as long as the starting date isn't more than 90 days in the past.

Through activity logs, you can determine:

- ⇒ what operations were taken on the resources in your subscription
- ⇒ who started the operation
- ⇒ when the operation occurred
- ⇒ the status of the operation
- ⇒ the values of other properties that might help you research the operation

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/view-activity-logs>

Community vote distribution

D (100%)

🗳️ 👤 **DatBroNZ** Highly Voted 4 years, 5 months ago  
Option "D"

- A. the Change Tracking management solution - used on Automation
  - B. Application Insights - monitor live APPs
  - C. Azure Monitor action groups - notification preferences
  - D. Azure Activity Log - subscription-level events
- upvoted 63 times

🗳️ 👤 **rdemontis** 3 years, 7 months ago  
thanks for explanation  
upvoted 2 times

🗳️ 👤 **czarul79** Highly Voted 4 years, 2 months ago  
On the exam , this question has been changed & swapped. Now the answer is "Azure Log Analytics"  
upvoted 44 times

🗳️ 👤 **rdemontis** 3 years, 7 months ago  
thanks  
upvoted 1 times

🗳️ 👤 **Odidepse** Most Recent 3 years, 2 months ago  
Presented answer is correct. In AZ-305  
upvoted 3 times

🗳️ 👤 **Linie\_Klar** 3 years, 3 months ago  
Its D. But now its has been change to azure log analytics  
upvoted 1 times

🗳️ 👤 **plmmsg** 3 years, 3 months ago  
D. Azure Activity Log (Azure Log Analytics)  
upvoted 1 times

🗳️ 👤 **LordBuks** 3 years, 4 months ago

**Selected Answer: D**

Definitely D

upvoted 1 times

  **scottishstvaeo** 3 years, 4 months ago

**Selected Answer: D**

I agree with those how say that the answer is D.

Over the activity log you can track who, when and what =D

upvoted 1 times

  **RavindraDevkhile** 3 years, 4 months ago

**Selected Answer: D**



Option "D"

upvoted 1 times

  **Azure\_daemon** 3 years, 4 months ago



D is the correct answer

upvoted 2 times

  **ITrob523** 3 years, 4 months ago

On exam 02/2022. Answer is correct


upvoted 2 times

  **nicold2** 3 years, 5 months ago

**Selected Answer: D**

activity log!

upvoted 1 times

  **Dpejic** 3 years, 6 months ago


Appear in exam 23-dec-2021

upvoted 3 times

  **hardy007** 3 years, 6 months ago

I passed with 800, I would say 10% of my exams were new questions. 90% are from the questions here and lastly, some answers in which people voted high are not always correct. Wish you all the best.

upvoted 3 times

  **BorgesQC** 3 years, 8 months ago

EXAM AZ-303 AND EXAM AZ-304 WILL RETIRE ON MARCH 31, 2022. A new exam, Exam AZ-305, will be available in November 2021.

upvoted 2 times

  **anthonyphuc** 3 years, 6 months ago

the comment without meaning. Instead, give your answer.

upvoted 3 times

  **kvsvasvasvf** 3 years, 8 months ago

Through activity logs, you can determine:

- what operations were taken on the resources in your subscription
- who started the operation
- when the operation occurred
- the status of the operation
- the values of other properties that might help you research the operation

upvoted 1 times

  **kvsvasvasvf** 3 years, 8 months ago

this answer is correct

upvoted 1 times

  **syu31svc** 3 years, 9 months ago

<https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log>

Answer is D

upvoted 2 times

You have an Azure subscription that contains an Azure SQL database named DB1.  
 Several queries that query the data in DB1 take a long time to execute.  
 You need to recommend a solution to identify the queries that take the longest to execute.  
 What should you include in the recommendation?

- A. SQL Database Advisor
- B. Azure Monitor
- C. Performance Recommendations
- D. Query Performance Insight

**Suggested Answer: D**

Query Performance Insight provides intelligent query analysis for single and pooled databases. It helps identify the top resource consuming and long-running queries in your workload. This helps you find the queries to optimize to improve overall workload performance and efficiently use the resource that you are paying for.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/query-performance-insight-use>

Community vote distribution

D (100%)

 **speedminer** Highly Voted 4 years, 9 months ago

Per the provided link:

"Query Performance Insight provides intelligent query analysis for single and pooled databases. It helps identify the top resource consuming and long-running queries in your workload. This helps you find the queries to optimize to improve overall workload performance and efficiently use the resource that you are paying for."

upvoted 34 times

 **sanketshah** 4 years, 5 months ago

D is correct

upvoted 8 times

 **David\_986969** Highly Voted 4 years, 7 months ago

In the exam 11/11/2020

upvoted 10 times

 **Aquib\_Chiniwala** Most Recent 2 years, 8 months ago

**Selected Answer: D**

D is correct

upvoted 1 times

 **Aquib\_Chiniwala** 2 years, 8 months ago

D is correct

upvoted 1 times

 **cz65rv** 2 years, 11 months ago

**Selected Answer: D**


Given answer is correct

upvoted 1 times

 **Hary001** 3 years, 1 month ago

looks like correct ANS

upvoted 1 times

 **hertino** 3 years, 2 months ago

In AZ-305 exam, 9 april 22

upvoted 6 times

 **Odidepse** 3 years, 2 months ago

D is correct



upvoted 2 times

🗨️ 👤 **plmmmsg** 3 years, 3 months ago

D. Query Performance Insight

upvoted 1 times

🗨️ 👤 **Azure\_daemon** 3 years, 4 months ago

Query Performance Insight is the correct answer

upvoted 2 times

🗨️ 👤 **awalao** 3 years, 6 months ago

**Selected Answer: D**

D is correct.

upvoted 2 times

🗨️ 👤 **sharepoint\_Azure\_pp** 3 years, 8 months ago

Option D is correct or can say i choose the same.

was there in 17th October 2021 cleared with 900

upvoted 3 times

🗨️ 👤 **syu31svc** 3 years, 9 months ago

<https://docs.microsoft.com/en-us/azure/azure-sql/database/query-performance-insight-use>

Query Performance Insight provides intelligent query analysis for single and pooled databases. It helps identify the top resource consuming and long-running queries in your workload. This helps you find the queries to optimize to improve overall workload performance and efficiently use the resource that you are paying for. Query Performance Insight helps you spend less time troubleshooting database performance by providing:

Deeper insight into your databases resource (DTU) consumption

Details on top database queries by CPU, duration, and execution count (potential tuning candidates for performance improvements)

Answer is D 100%

upvoted 3 times

🗨️ 👤 **heamgu** 4 years ago

D. Query Performance Insight

upvoted 1 times

🗨️ 👤 **yeanningmedal71** 4 years, 1 month ago

D is correct

upvoted 3 times

🗨️ 👤 **betamode** 4 years, 4 months ago

Correct answer

upvoted 1 times

🗨️ 👤 **suryareddy** 4 years, 5 months ago

D is correct

upvoted 3 times

**HOTSPOT -**

You have an Azure App Service Web App that includes Azure Blob storage and an Azure SQL Database instance. The application is instrumented by using the

Application Insights SDK.

You need to design a monitoring solution for the web app.

Which Azure monitoring services should you use? To answer, select the appropriate Azure monitoring services in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Scenario	Azure monitoring service
Correlate Azure resource usage and performance data with application configuration and performance data.	<div><div></div><div>Azure Application Insights</div><div>Azure Service Map</div><div>Azure Monitor Logs</div><div>Azure Activity Log</div></div>
Visualize the relationships between application components.	<div><div></div><div>Azure Application Insights</div><div>Azure Service Map</div><div>Azure Monitor Logs</div><div>Azure Activity Log</div></div>
Track requests and exceptions to a specific line of code within the application.	<div><div></div><div>Azure Application Insights</div><div>Azure Service Map</div><div>Azure Monitor Logs</div><div>Azure Activity Log</div></div>
Analyze how many users return to the application and how often they select a particular dropdown value.	<div><div></div><div>Azure Application Insights</div><div>Azure Service Map</div><div>Azure Monitor Logs</div><div>Azure Activity Log</div></div>

## Answer Area

### Scenario

Correlate Azure resource usage and performance data with application configuration and performance data.

Visualize the relationships between application components.

Track requests and exceptions to a specific line of code within the application.

Analyze how many users return to the application and how often they select a particular dropdown value.

### Azure monitoring service

Azure Application Insights  
Azure Service Map  
Azure Monitor Logs  
Azure Activity Log

Azure Application Insights  
Azure Service Map  
Azure Monitor Logs  
Azure Activity Log

Azure Application Insights  
Azure Service Map  
Azure Monitor Logs  
Azure Activity Log

Azure Application Insights  
Azure Service Map  
Azure Monitor Logs  
Azure Activity Log

Suggested Answer:

Note: You can select Logs from either the Azure Monitor menu or the Log Analytics workspaces menu.

Reference:


<https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/log-query-overview>

 **airairo**  4 years, 6 months ago

I searched again:

- 1) Azure Log Analytics
- 2) Azure Service Map
- 3) Azure Application Insights
- 4) Azure Application Insights

upvoted 79 times

 **Lexa** 4 years, 6 months ago


Unfortunately, there is no option "Azure Log Analytics"

upvoted 1 times

 **Azure\_Chief** 4 years, 6 months ago

You had it right the first time, box 2 is App insights the application map. Service Map is for VMs.

upvoted 12 times

 **AWS56** 4 years, 5 months ago

"1- Azure Log Analytics:" --> Where is this ? Not there in the list of answers to pick

upvoted 3 times

 **nightfearz** 4 years, 2 months ago

Azure monitor logs = Azure log analytics

<https://docs.microsoft.com/en-us/azure/azure-monitor/logs/data-platform-logs>

upvoted 9 times

 **AubinBakana** 2 years, 10 months ago

No, it's not the same thing. Azure monitor produces Logs & Metrix, different Log Analytics.

upvoted 2 times

🗨️ 👤 **kaunhe** 4 years, 1 month ago

Just google the description for #2 and you will see it's clearly App Insights. First link shows description for App insights.  
upvoted 2 times

🗨️ 👤 **aak0308** 3 years, 11 months ago

This is wrong, answer should be Azure Service Map not application insight for 2. Here is my explanation

1. Azure Log Analytics / Azure Activity log
2. Azure Service Map

Azure Service Map : To discover and identify all the components and map the communication between different components and services.

Application Map in Application Insight : Application Map helps you spot performance bottlenecks or failure hotspots across all components of your distributed application.

3. Azure Application Insight
4. Azure Application Insight

upvoted 10 times

🗨️ 👤 **Angarali** 3 years ago

Azure Monitor Logs, not Azure Activity Log  
upvoted 1 times

🗨️ 👤 **Kanmaj10** 3 years, 3 months ago

The key differentiation is "relationships between App components" which means its Application Map , instead of Service Map which is about "relationship between services at an OS level" not so much within the Application.

upvoted 1 times

🗨️ 👤 **kilowd** 3 years ago

Azure Service Maps is correct

Service maps are visual, customizable representations of your architecture. Maps automatically show your app's connections and dependencies, including applications, databases, hosts, servers, and out-of-process services.

Application Map helps you spot performance bottlenecks or failure hotspots across all components of your distributed application. Each node on the map represents an application component or its dependencies; and has health KPI and alerts status

upvoted 1 times

🗨️ 👤 **azurecert2021** Highly Voted 👍 4 years, 4 months ago

answer is

Azure Monitor Logs\Azure Log Analytics

Azure Application Insights

Azure Application Insights

Azure Application Insights

following is the justification :-

Azure Monitor Logs\Azure Log Analytics (whatever option is available in exam for sure both wont come in choice ,if both are present in choice then preferred answer is Azure Monitor Logs.

Azure Log Analytics :-You can send data about the application and resource usage to Azure Log Analytics. You can then build queries on the stored data.

Azure Monitor Logs:- it is a feature of Azure Monitor that collects and organizes log and performance data from monitored resources. Data from different sources such as platform logs from Azure services, log and performance data from virtual machines agents, and usage and performance data from applications can be consolidated into a single workspace so they can be analyzed together using a sophisticated query language that's capable of quickly analyzing millions of records.

upvoted 72 times

🗨️ 👤 **jjyang** Most Recent 🔒 2 years, 10 months ago

Service Map automatically discovers application components on Windows and Linux systems and maps the communication between services

<https://docs.microsoft.com/en-us/azure/azure-monitor/vm/service-map>

Mapping overview...

upvoted 3 times

🗨️ 👤 **AubinBakana** 2 years, 10 months ago

The answer is correct (Update):

Azure Application insight: The service you use to monitor application using log, metrix, maps, etc...

Service Map: A feature in Azure Monitor & App Insights

Azure Monitor Logs: They are simply referring to the logs, as opposed to metrix, not log analytics workspace. Just the logs.

Azure Activity Log: A log of activities in your subscription

1 - Azure Monitor Logs

2 - Service Map

(Keywor - visualise)

3 - Application Insight

4 - Activity Log.

upvoted 2 times

🗳️ 👤 **AubinBakana** 2 years, 10 months ago

The answer is correct:

Azure Application insight: The service you use to monitor application using log, metrix, maps, etc...

Service Map: A feature in Azure Monitor & App Insights

Azure Monitor Logs: They are simply referring to the logs, as opposed to metrix, not log analytics workspace. Just the logs.

Azure Activity Log: A log of activities in your subscription

upvoted 1 times

🗳️ 👤 **g6singh** 3 years, 1 month ago

Azure Monitor Logs\Azure Log Analytics

Azure Application Insights

Azure Application Insights

Azure Application Insights

upvoted 2 times

🗳️ 👤 **VijayRaja2000** 3 years, 1 month ago

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-insights-overview> justifies the choice of Azure Application Insights for 3 and 4th options..First and Second are obvious..

upvoted 1 times

🗳️ 👤 **Kanmaj10** 3 years, 3 months ago

For 2 , its not Service Map. Service Map is about OS level communication mapping. Answer is App Insights.

upvoted 2 times

🗳️ 👤 **plmmsg** 3 years, 3 months ago

Azure Monitor Logs\Azure Log Analytics

Azure Application Insights

Azure Application Insights

Azure Application Insights

upvoted 3 times

🗳️ 👤 **plmmsg** 3 years, 5 months ago

Azure Monitor Logs\Azure Log Analytics

Azure Application Insights

Azure Application Insights

Azure Application Insights

upvoted 5 times

🗳️ 👤 **azure\_novice** 3 years, 6 months ago

the answer is correct

just read the documentation regarding azure service map.

upvoted 2 times

🗳️ 👤 **AberdeenAngus** 3 years, 1 month ago

Where I work we're using Service Map for our VMs. I don't think it can work with web apps or other PaaS resources. And App Insights provides a diagram of connected resource.

upvoted 1 times

🗳️ 👤 **walkwolf3** 3 years, 7 months ago

---Azure Monitor Logs\Azure Log Analytics

Log Analytics helps correlate the usage and performance data collected by Application Insights with configuration and performance data across the

Azure resources that support the app.

<https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/app-service-web-app/app-monitoring#components>

<https://docs.microsoft.com/en-us/azure/azure-monitor/logs/data-platform-logs>

---Azure Application Insights(Application Map)

Application Map helps you spot performance bottlenecks or failure hotspots across all components of your distributed application.

One of the key objectives with this experience is to be able to visualize complex topologies with hundreds of components.

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-map?tabs=net>

upvoted 3 times

  **walkwolf3** 3 years, 7 months ago

---Azure Application Insights

You can investigate specific dependency calls, and correlate them to requests and exceptions.

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/asp-net-dependencies>

---Azure Application Insights



Usage analysis with Application Insights

Retention - how many users come back?

Retention helps you understand how often your users return to use their app

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/usage-overview#retention---how-many-users-come-back>

upvoted 1 times

  **tallurhi** 3 years, 7 months ago

It should be applicaiton insights for all

By viewing an Application Insights resource in the Azure portal, you can visualize the telemetry captured from your app in a variety of ways.

Live metrics streams: Charts that display performance values as they vary in near-real time.

Metrics explorer: Tool that shows how metrics vary over time.

Alerts: Messages automatically sent to app admins when target metrics exceed specified thresholds. You can use alerts to ensure your team is aware of critical issues immediately.

Profiler: Shows how a set of requests, like those for a single web page, were delivered. You can use these profiles, for example, to see which page elements load slowly.

Application Map: Displays the components of an application and how they link to each other. You can use the data shown with each component to diagnose performance bottlenecks and failure hotspots.

Usage analysis: Information about your app's users. For example, you can see numbers of unique users and sessions and information about user retention.

upvoted 3 times

  **student22** 3 years, 8 months ago



1) Azure Monitor Logs (Azure Log Analytics)

2) Azure Application Insights

3) Azure Application Insights

4) Azure Application Insights

upvoted 3 times

  **tteesstt** 3 years, 8 months ago

1) Monitor Logs

2) Application Insights

3) Application Insights

4) Application Insights



Azure Service Map is VM related but we are using Azure App Service.

<https://docs.microsoft.com/en-us/azure/azure-monitor/vm/service-map>

You can view relationship between components using Application Map in application insights:



<https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-map?tabs=net>

upvoted 3 times

  **waqas** 3 years, 8 months ago

2nd option must be Azure Service Map.....Service Map automatically discovers application components on Windows and Linux systems and maps the communication between services. With Service Map, you can view your servers in the way that you think of them: as interconnected systems that deliver critical services. Service Map shows connections between servers, processes, inbound and outbound connection latency, and ports across any TCP-connected architecture, with no configuration required other than the installation of an agent.

upvoted 1 times

  **waqas** 3 years, 8 months ago

My bad...Please discard my above comments.It must be Application Map...not Service Map...

upvoted 2 times

  **syu31svc** 3 years, 9 months ago

<https://docs.microsoft.com/en-us/azure/azure-monitor/logs/data-platform-logs>

1st one is Monitor Logs

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-map?tabs=net>

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-insights-overview>

The rest are Application Insights

upvoted 4 times

You have an on-premises Hyper-V cluster. The cluster contains Hyper-V hosts that run Windows Server 2016 Datacenter. The hosts are licensed under a

Microsoft Enterprise Agreement that has Software Assurance.

The Hyper-V cluster contains 30 virtual machines that run Windows Server 2012 R2. Each virtual machine runs a different workload. The workloads have predictable consumption patterns.

You plan to replace the virtual machines with Azure virtual machines that run Windows Server 2016. The virtual machines will be sized according to the consumption pattern of each workload.

You need to recommend a solution to minimize the compute costs of the Azure virtual machines.

Which two recommendations should you include in the solution? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Configure a spending limit in the Azure account center.
- B. Create a virtual machine scale set that uses autoscaling.
- C. Activate Azure Hybrid Benefit for the Azure virtual machines.
- D. Purchase Azure Reserved Virtual Machine Instances for the Azure virtual machines.
- E. Create a lab in Azure DevTest Labs and place the Azure virtual machines in the lab.

**Suggested Answer:** CD

C: For customers with Software Assurance, Azure Hybrid Benefit for Windows Server allows you to use your on-premises Windows Server licenses and run

Windows virtual machines on Azure at a reduced cost. You can use Azure Hybrid Benefit for Windows Server to deploy new virtual machines with Windows OS.



D: With Azure Reserved VM Instances (RIs) you reserve virtual machines in advance and save up to 80 percent.

Reference:

<https://azure.microsoft.com/en-us/pricing/reserved-vm-instances/> <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/hybrid-use-benefit-licensing>

Community vote distribution

CD (100%)

 **speedminer**  4 years, 9 months ago



Seems correct, both would reduce cost if used.

upvoted 50 times

 **sanketshah** 4 years, 5 months ago

both answers are correct.

upvoted 9 times

 **syu31svc**  3 years, 9 months ago

<https://azure.microsoft.com/en-us/pricing/hybrid-benefit/>

Azure Hybrid Benefit is a licensing benefit that helps you to significantly reduce the costs of running your workloads in the cloud. It works by letting you use your on-premises Software Assurance-enabled Windows Server and SQL Server licenses on Azure. And now, this benefit applies to RedHat and SUSE Linux subscriptions, too.

<https://azure.microsoft.com/en-us/pricing/reserved-vm-instances/>

Significantly reduce costs—up to 72 percent<sup>1</sup> compared to pay-as-you-go prices—with one-year or three-year terms on Windows and Linux virtual machines (VMs). When you combine the cost savings gained from Azure RIs with the added value of the Azure Hybrid Benefit, you can save up to 80 percent<sup>2</sup>.

Lower your total cost of ownership by combining Azure Reserved Instances with pay-as-you-go prices to manage costs across predictable and variable workloads. In many cases, you can further reduce your costs with reserved instance size flexibility.

C and D are the answers





upvoted 19 times

  **BigSoda** 3 years, 8 months ago

syu31svc - your answers tend to be the most informative and relevant ones on this site! Thanks mate.

upvoted 2 times

  **Teringzooi** Most Recent 3 years, 1 month ago

**Selected Answer: CD**

Correct answers are: C & D

<https://azure.microsoft.com/en-us/pricing/hybrid-benefit/>



Azure Hybrid Benefit is a licensing benefit that helps you to significantly reduce the costs of running your workloads in the cloud. It works by letting you use your on-premises Software Assurance-enabled Windows Server and SQL Server licenses on Azure. And now, this benefit applies to RedHat and SUSE Linux subscriptions, too.

<https://azure.microsoft.com/en-us/pricing/reserved-vm-instances/>

Significantly reduce costs—up to 72 percent<sup>1</sup> compared to pay-as-you-go prices—with one-year or three-year terms on Windows and Linux virtual machines (VMs). When you combine the cost savings gained from Azure RIs with the added value of the Azure Hybrid Benefit, you can save up to 80 percent<sup>2</sup>.

Lower your total cost of ownership by combining Azure Reserved Instances with pay-as-you-go prices to manage costs across predictable and variable workloads. In many cases, you can further reduce your costs with reserved instance size flexibility.

upvoted 1 times

  **Dawn7** 3 years, 3 months ago

**Selected Answer: CD**

I would choose C&D

upvoted 2 times

  **plmmmsg** 3 years, 3 months ago

C & D are correct answers

upvoted 1 times

  **Azure\_daemon** 3 years, 4 months ago

C & D are correct answers, both help to reduce the cost

upvoted 1 times

  **moon2351** 3 years, 5 months ago

**Selected Answer: CD**

Correct

upvoted 1 times

  **DonBoat** 3 years, 5 months ago

**Selected Answer: CD**

correct

upvoted 1 times

  **sureshdy** 3 years, 7 months ago

correct

upvoted 3 times

  **tteesstt** 3 years, 8 months ago

Correct.

upvoted 2 times

  **dkltruong88** 3 years, 9 months ago

Was in exam today 1-10-2021. I passed with score 896. I chose C, D

upvoted 2 times

  **souvik123** 3 years, 9 months ago

C. Activate Azure Hybrid Benefit for the Azure virtual machines.

D. Purchase Azure Reserved Virtual Machine Instances for the Azure virtual machines.

upvoted 1 times

🗨️ 👤 **tita\_tovenaar** 3 years, 11 months ago

Confirmed correct as per ref:

<https://azure.microsoft.com/en-us/pricing/hybrid-benefit/#calculator>

"Achieve the lowest cost of ownership by combining the Azure Hybrid Benefit, reservation pricing, and extended security updates".

upvoted 2 times

🗨️ 👤 **aak0308** 3 years, 11 months ago

C, D is correct answer. VM will be sized per the individual workload gives away that the VM's are not identical which is why it is not B. Else B is a better answer if VM's can be identical.

upvoted 4 times

🗨️ 👤 **heamgu** 4 years ago

C. Activate Azure Hybrid Benefit for the Azure virtual machines.

D. Purchase Azure Reserved Virtual Machine Instances for the Azure virtual machines.

upvoted 1 times

🗨️ 👤 **bbc** 4 years, 2 months ago

on exam today

upvoted 5 times

🗨️ 👤 **kuroro** 4 years, 2 months ago

In exam 19-04-2021

upvoted 2 times

## HOTSPOT -

You have an Azure subscription that contains the SQL servers on Azure shown in the following table.

Name	Resource group	Location
SQLsvr1	RG1	East US
SQLsvr2	RG2	West US

The subscription contains the storage accounts shown in the following table.

Name	Resource group	Location	Account kind
storage1	RG1	East US	StorageV2 (general purpose v2)
storage2	RG2	Central US	BlobStorage

You create the Azure SQL databases shown in the following table.

Name	Resource group	Server	Pricing tier
SQLdb1	RG1	SQLsvr1	Standard
SQLdb2	RG1	SQLsvr1	Standard
SQLdb3	RG2	SQLsvr2	Premium

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
When you enable auditing for SQLdb1, you can store the audit information to storage1.	<input type="radio"/>	<input type="radio"/>
When you enable auditing for SQLdb2, you can store the audit information to storage2.	<input type="radio"/>	<input type="radio"/>
When you enable auditing for SQLdb3, you can store the audit information to storage2.	<input type="radio"/>	<input type="radio"/>

### Answer Area

	Statements	Yes	No
Suggested Answer:	When you enable auditing for SQLdb1, you can store the audit information to storage1.	<input checked="" type="radio"/>	<input type="radio"/>
	When you enable auditing for SQLdb2, you can store the audit information to storage2.	<input type="radio"/>	<input checked="" type="radio"/>
	When you enable auditing for SQLdb3, you can store the audit information to storage2.	<input type="radio"/>	<input checked="" type="radio"/>

Box 1: Yes -

Be sure that the destination is in the same region as your database and server.

Box 2: No -

Box 3: No -

Reference:

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-auditing>



 **Hooters**  4 years, 1 month ago

YNN is the answer by looking at the storage location and its tier  
upvoted 43 times

 **danielcr** 4 years ago

YNN, can't use storage2 because it's in other region (checked in portal)

upvoted 13 times

  **examineezer** 3 years, 6 months ago

Seems like the documentation doesn't say that it has to be in the same region, but if you try it in a lab you'll see that it does.

upvoted 1 times

  **LuiZ146**  4 years, 2 months ago

The last one is no, because the Azure SQL Server and the storage account are in different locations.

upvoted 15 times

  **kumarofrcet** 4 years, 1 month ago

Plus - Premium storage is not supported currently

upvoted 8 times

  **demonite** 4 years, 1 month ago



Sql Premium sku not premium storage

upvoted 7 times

  **dennnnnnnnnn** 3 years, 11 months ago

blobstorage imply premium storage account

upvoted 3 times

  **joefdez** 3 years, 3 months ago

BlobStorage is Standard, BlockBlobStorage and FileStorage are Premium.

YNN, because the auditing needs to be on same region.

upvoted 3 times

  **FrancisFerreira** 3 years, 3 months ago

Dont think so...

BlobStorage = Premium Page Blob

BlockBlobStorage = Premium Block/Append Blob



FileStorage = Premium File Share

upvoted 2 times

  **gauravit43**  2 years, 2 months ago

I have passed AZ-305 on 15th April,2023 and this question was there in the exam

upvoted 1 times

  **GarryK** 2 years, 9 months ago

YNN.

BlobStorage is legacy storage.

Premium storage with BlockBlobStorage is supported. Standard storage is supported. However, for audit to write to a storage account behind a VNet or firewall, you must have a general-purpose v2 storage account. If you have a general-purpose v1 or blob storage account, upgrade to a general-purpose v2 storage account. For specific instructions see, Write audit to a storage account behind VNet and firewall. For more information, see Types of storage accounts.

<https://learn.microsoft.com/en-us/azure/azure-sql/database/auditing-overview?view=azuresql>

upvoted 1 times

  **dpakrawat** 3 years ago

was in the exam on 6/17

upvoted 2 times

  **Azure\_daemon** 3 years, 2 months ago

The SQL and storage (event hub or log analytic workspace) has to be in the same region, also one of the auditing limitation is that, Premium storage is currently not supported.

upvoted 2 times

  **Odidepse** 3 years, 2 months ago

Presented answer if correct, Y, N, N

upvoted 1 times

  **plmmsg** 3 years, 3 months ago

yes. no, no

upvoted 1 times

🗨️ 👤 **Azure\_daemon** 3 years, 4 months ago

Auditing limitations

Premium storage is currently not supported.

Hierarchical namespace for Azure Data Lake Storage Gen2 storage account is currently not supported.

Enabling auditing on a paused Azure Synapse is not supported. To enable auditing, resume Azure Synapse.

Auditing for Azure Synapse SQL pools supports default audit action groups only.

upvoted 1 times

🗨️ 👤 **BhupalS** 3 years, 4 months ago

YNN

Auditing limitations

Premium storage is currently not supported.

Hierarchical namespace for Azure Data Lake Storage Gen2 storage account is currently not supported.

Enabling auditing on a paused Azure Synapse is not supported. To enable auditing, resume Azure Synapse.

Auditing for Azure Synapse SQL pools supports default audit action groups only.

upvoted 2 times

🗨️ 👤 **Dpejic** 3 years, 6 months ago

On exam 24.12.2021

upvoted 3 times

🗨️ 👤 **Dpejic** 3 years, 6 months ago

On exam 22-dec-2021

upvoted 4 times

🗨️ 👤 **sharepoint\_Azure\_pp** 3 years, 8 months ago

YNN is the answer or can say i choose the same.

was there in 17th October 2021 cleared with 900

upvoted 5 times

🗨️ 👤 **tteesstt** 3 years, 8 months ago

Correct.

upvoted 1 times

🗨️ 👤 **syu31svc** 3 years, 9 months ago

You can store the audit information in Blob storage as long as the storage account is in the same location as the Azure SQL Server

<https://docs.microsoft.com/en-us/azure/azure-sql/database/auditing-overview>

Premium storage is currently not supported.

Yes No No is correct

upvoted 3 times

🗨️ 👤 **SpicyMonkey** 3 years, 9 months ago

Auditing limitations

Premium storage is currently not supported.

<https://docs.microsoft.com/en-us/azure/azure-sql/database/auditing-overview#auditing-limitations>

upvoted 2 times

🗨️ 👤 **souvik123** 3 years, 9 months ago

Y --> audit is possible on same location

N--> different location to sql server

N- -> blob is not a valid option on Storage V1 & Storage V2 & Storage in a different location

upvoted 1 times

A company has a hybrid ASP.NET Web API application that is based on a software as a service (SaaS) offering. Users report general issues with the data. You advise the company to implement live monitoring and use ad hoc queries on stored JSON data. You also advise the company to set up smart alerting to detect anomalies in the data. You need to recommend a solution to set up smart alerting. What should you recommend?

- A. Azure Site Recovery and Azure Monitor Logs
- B. Azure Data Lake Analytics and Azure Monitor Logs
- C. Azure Application Insights and Azure Monitor Logs
- D. Azure Security Center and Azure Data Lake Store

**Suggested Answer: C**

Application Insights, a feature of Azure Monitor, is an extensible Application Performance Management (APM) service for developers and DevOps professionals.

Use it to monitor your live applications. It will automatically detect performance anomalies, and includes powerful analytics tools to help you diagnose issues and to understand what users actually do with your app.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-insights-overview>

Community vote distribution

C (100%)

  **AnilV**  4 years, 7 months ago

Finally Answer C "Azure Application Insights and Azure Log Analytics". Unable to delete my earlier comments. Sorry for the confusion.

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/proactive-diagnostics>

upvoted 100 times

  **malyaban** 4 years, 3 months ago

Yes Answer is C as many here are confusing JSON data with Big Data, Data Lake Analytics is strictly Big Data, JSON data can be any NoSQL DB

upvoted 16 times

  **arseyam**  4 years, 7 months ago

Answer is C


Collect custom JSON data in Azure Monitor

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-sources-json>

Application Insights smart detection

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/proactive-diagnostics>

upvoted 36 times

  **5am** 3 years, 11 months ago

your first link is limited for Linux.

upvoted 2 times

  **azurecert2021** 4 years, 4 months ago

this looks correct.

upvoted 2 times

  **Teringzooi**  3 years, 1 month ago

**Selected Answer: C**

Answer is: C

Collect custom JSON data in Azure Monitor

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-sources-json>

Application Insights smart detection

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/proactive-diagnostics>

upvoted 1 times

🗨️ **Dawn7** 3 years, 3 months ago

**Selected Answer: C**

Correct

upvoted 1 times

🗨️ **plmmmsg** 3 years, 3 months ago

C. Azure Application Insights and Azure Monitor Logs

upvoted 1 times

🗨️ **Azure\_daemon** 3 years, 4 months ago

C is the correct answer

upvoted 1 times

🗨️ **Eitant** 3 years, 6 months ago

**Selected Answer: C**

Answer is C

upvoted 2 times

🗨️ **examineezer** 3 years, 6 months ago

Azure Application Insights - specifically the Smart detection feature.

upvoted 1 times

🗨️ **syu31svc** 3 years, 9 months ago

"ASP.NET Web API application"

Answer is C 100%

upvoted 2 times

🗨️ **NewGuyAmazon** 3 years, 9 months ago

correct ans

upvoted 1 times

🗨️ **souvik123** 3 years, 10 months ago

C. Azure Application Insights and Azure Monitor Logs

upvoted 1 times

🗨️ **StarkStrange** 3 years, 10 months ago

ans C "Azure Application Insights and Azure Log Analytics"

upvoted 3 times

🗨️ **heamgu** 4 years ago

C. Azure Application Insights and Azure Monitor Logs

upvoted 7 times

🗨️ **MaheshS** 4 years ago

C is the right answer

upvoted 2 times

🗨️ **ashishg2105** 4 years, 1 month ago

Answer is 'C'.

The smart alerting feature is available in Application Insights

upvoted 3 times

🗨️ **Hooters** 4 years, 1 month ago

C - Azure Application Insights and Azure Log Analytics can detect anomalies in the data

upvoted 2 times

🗨️ **aspirin** 4 years, 2 months ago

Whats wrong with the questions here? Answer C is correct but no one can correct this in the front end answers? The learn effect lacks if you see the wrong answer the second, the third time and so on!

upvoted 5 times

You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant. The subscription contains 10 resource groups, one for each department at your company.

Each department has a specific spending limit for its Azure resources.

You need to ensure that when a department reaches its spending limit, the compute resources of the department shut down automatically.

Which two features should you include in the solution? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Azure Logic Apps
- B. Azure Monitor alerts
- C. the spending limit of an Azure account
- D. Cost Management budgets
- E. Azure Log Analytics alerts

**Suggested Answer:** CD

C: The spending limit in Azure prevents spending over your credit amount. All new customers who sign up for an Azure free account or subscription types that include credits over multiple months have the spending limit turned on by default. The spending limit is equal to the amount of credit and it can't be changed.

D: Turn on the spending limit after removing

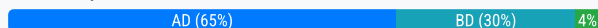
This feature is available only when the spending limit has been removed indefinitely for subscription types that include credits over multiple months. You can use this feature to turn on your spending limit automatically at the start of the next billing period.

1. Sign in to the Azure portal as the Account Administrator.
2. Search for Cost Management + Billing.
3. Etc.

Reference:

<https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/spending-limit>

Community vote distribution



**arseyam** 4 years, 7 months ago

Answer should be B and D

Spending limit on Azure account affects all the subscription not just a specific resource group and it is a feature provided for specific subscription types like the free one.

The way to achieve the requirements is by doing the following:

1. Azure Monitor > Alerts > Manage Actions > create action groups with action type "Automation Runbook" > stop VM
2. Create budgets scoped by the resource groups > in the alert section choose the previously created action groups.

upvoted 140 times

**agimenez** 3 years, 11 months ago

Some resource is needed to shut down the VMS. The spending limit of an Azure account does not have this behavior. I am not sure whether a Logic App or Automation Runbook.

upvoted 2 times

**GetulioJr** 3 years, 11 months ago

answer is correct and can be checked in this link:

REF: <https://abundantcode.com/azure-qa-6-spending-limit-and-resources-shutdown/>

upvoted 2 times

**cfsxtuv33** 3 years, 8 months ago

You are correct, at least the link gives the correct information. Thank you for this link, I agree, the provided answer is correct!

upvoted 2 times



**itenginerd** 3 years, 3 months ago



The problem with spending limits is they don't exist on "real" subscription types. Nobody with production running in Azure should have spending limits available to them. PayGo, EA, CSP, Azure Plan--none of these subscription types support spending limits.



<https://azure.microsoft.com/en-us/support/legal/offer-details/>

upvoted 1 times

  **cards** 3 years, 6 months ago

When the budget thresholds you've created are exceeded, only notifications are triggered. None of your resources are affected and your consumption isn't stopped.

upvoted 3 times

  **NickGR** 4 years, 6 months ago



Thats correct arseyam. You need to create a budget for the resource group scope and set an alert with an action group to shutdown the VM.

upvoted 4 times

  **sanketshah** 4 years, 5 months ago

B and D are correct answer.

upvoted 2 times

  **Elecktrus** Highly Voted 4 years, 6 months ago

Answer is B & D



According to the MS-Article: <https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/cost-management-budget-scenario>

You need to have:

- 1) Azure Budget
- 2) Azure Monitor to create an alert and actions for this alert (Action Groups)
- 3) the action group run the App Logic Workflow

The answer can include only 2 actions, so step 1) -> D and step 2) -> B



upvoted 39 times

  **jallaix** 4 years, 3 months ago

Wrong because the provided MS article associates an action group directly to a budget => No Azure Monitor alert is involved.

But the document talks about Logic App => answer is: A + D.



upvoted 24 times

  **sjai** 3 years, 9 months ago

A & D. Here is the snippet from the docs

You're done with all the supporting components needed to effectively orchestrate your budget. Now all you need to do is create the budget and configure it to use the action group you created.

upvoted 1 times

  **FinMessner** 3 years, 5 months ago



Wrong. <https://andreas-wilm.github.io/2020-06-01-enforce-budgets/>

upvoted 1 times

  **soi** 4 years, 6 months ago

true & final answer

upvoted 5 times

  **Lexa** 4 years, 5 months ago

Totally agree

upvoted 1 times

  **walexkino** Most Recent 2 years, 6 months ago

Selected Answer: AD

Thats the right answer B and D

upvoted 1 times

  **Mozammelhosain** 2 years, 6 months ago

ms word is very important software, because its a soft with any foundation exm: [www.gefaridf.com](http://www.gefaridf.com)

upvoted 1 times

  **A\_GEE** 2 years, 6 months ago

Selected Answer: BD

Agree with arseyam

upvoted 2 times

🗨️ 👤 **AubinBakana** 2 years, 10 months ago

Selected Answer: AD

Create an Azure Automation Runbook to stop VMs by using webhooks.

Create an Azure Logic App to be triggered based on the budget threshold value and call the runbook with the right parameters.

Create an Azure Monitor Action Group that will be configured to trigger the Azure Logic App when the budget threshold is met.

Create the Azure budget with the wanted thresholds and wire it to the action group.

upvoted 2 times

🗨️ 👤 **AubinBakana** 2 years, 10 months ago

Update:

Here the budget would have to be set against the resource group. While my choice is still A & D, I have the wrong explanation here. Please ignore it.

I wish there were a delete, undo or update option.

upvoted 1 times

🗨️ 👤 **VijayRaja2000** 3 years ago

What I don't understand is that everyone here talks about the VM which is not at all part of the question. What happens if a particular department uses some other resources?

upvoted 2 times

🗨️ 👤 **VijayRaja2000** 3 years, 1 month ago

As explained in the following link, once you set the "Spending limit", on reaching this limit of consumption, the resources that you are using are automatically shut down. So you don't need any monitoring or action group.

This configuration of spending limit is part of Azure Cost management. So, for me the given answers of C and D look fine.

I don't understand why everyone is talking about the VM as nothing about VM is mentioned in the given question.

<https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/spending-limit>

upvoted 1 times

🗨️ 👤 **AubinBakana** 2 years, 10 months ago

They are talking about Azure Spending limit here, which is the limit for the subscription, not just a particular resource

upvoted 1 times

🗨️ 👤 **Alezz** 3 years, 2 months ago

Refer to this link

<https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/cost-management-budget-scenario#create-an-azure-logic-app-for-orchestration>

upvoted 1 times

🗨️ 👤 **kanweng** 3 years, 3 months ago

the example <https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/cost-management-budget-scenario>

Budget alert --> (Monitor alerts --Action group, Actions) --> logic app (end email and http) --> http request runbook by webhook url

you don't need to have the logic app anyway.

Budget alert --> (Monitor alerts --Action group, Actions) --> Azure automation runbook

upvoted 1 times

🗨️ 👤 **kanweng** 3 years, 3 months ago

i will only select A (Logic app) if you need send Email, then shutdown (call azure monitor alert, then action group (runbook)).

we don't need send email, therefore, the answer is B & D

upvoted 1 times

🗨️ 👤 **itenginerd** 3 years, 3 months ago

This one's not straightforward. The real catch here is that the best doc I've seen in this discussion describes using 3 of the 4 technologies--A, B, and D.

<https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/cost-management-budget-scenario>

upvoted 1 times

🗨️ 👤 **LukaG** 3 years, 3 months ago

Selected Answer: AD

The answer is A & D.

Microsoft wrote a nice piece about it: <https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/cost-management-budget-scenario>  
upvoted 2 times

🗨️ 👤 **Jcbrow27** 3 years, 3 months ago

**Selected Answer: AD**

AD

you need a logic app.

upvoted 2 times

🗨️ 👤 **arun** 3 years, 3 months ago

**Selected Answer: AD**

A, D

please refer <https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/cost-management-budget-scenario#create-an-azure-logic-app-for-orchestration....> it explains exact same scenario..

Budgets can be set up to trigger a notification when a specified threshold is met. You can provide multiple thresholds to be notified at and the Logic App..

The logic app will be used to shut down all VMs in the resource group when threshold met.

upvoted 2 times

🗨️ 👤 **Dawn7** 3 years, 3 months ago

**Selected Answer: BD**

I think B&D are correct.

upvoted 2 times

🗨️ 👤 **plmmsg** 3 years, 3 months ago

A. Azure Logic App - to shut down the server

D. Cost Management budgets - check against the budget

upvoted 2 times

## HOTSPOT -

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Kind	Location
storage1	Azure Storage account	Storage	East US
storage2	Azure Storage account	StorageV2	East US
Workspace1	Azure Log Analytics workspace	<i>Not applicable</i>	East US
Workspace2	Azure Log Analytics workspace	<i>Not applicable</i>	East US
Hub1	Azure event hub	<i>Not applicable</i>	East US

You create an Azure SQL database named DB1 that is hosted in the East US region.

To DB1, you add a diagnostic setting named Settings1. Settings1 archives SQLInsights to storage1 and sends SQLInsights to Workspace1.

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

Hot Area:

### Answer Area

Statements	Yes	No
You can add a new diagnostic setting that archives SQLInsights logs to storage2.	<input type="radio"/>	<input type="radio"/>
You can add a new diagnostic setting that sends SQLInsights logs to Workspace2.	<input type="radio"/>	<input type="radio"/>
You can add a new diagnostic setting that sends SQLInsights logs to Hub1.	<input type="radio"/>	<input type="radio"/>

### Answer Area

Statements	Yes	No
<b>Suggested Answer:</b> You can add a new diagnostic setting that archives SQLInsights logs to storage2.	<input type="radio"/>	<input checked="" type="radio"/>
You can add a new diagnostic setting that sends SQLInsights logs to Workspace2.	<input checked="" type="radio"/>	<input type="radio"/>
You can add a new diagnostic setting that sends SQLInsights logs to Hub1.	<input checked="" type="radio"/>	<input type="radio"/>

Box 1: No -

You archive logs only to Azure Storage accounts.

Box 2: Yes -

Box 3: Yes -

Sending logs to Event Hubs allows you to stream data to external systems such as third-party SIEMs and other log analytics solutions.

Note: A single diagnostic setting can define no more than one of each of the destinations. If you want to send data to more than one of a particular destination type

(for example, two different Log Analytics workspaces), then create multiple settings. Each resource can have up to 5 diagnostic settings.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/diagnostic-settings>

  **cookiesiecooks** 3 years, 3 months ago

the context is Storage1 is already added in the diagnostic section which you couldn't add it unless replace it so its N-Y-Y  
upvoted 2 times


  **techweck** 2 years, 10 months ago

then work space is also added, so as per you it should be N, N , Y.

but we can add upto 5 diag rules. its just that a single diag can have 1 same type of desktnation.

answer is Yes, Yes , Yes

upvoted 2 times

  **sanketshah** 4 years, 5 months ago

Answer should be

Yes

Yes



Yes

upvoted 15 times

  **sreejayan** 4 years, 4 months ago

Agreed - Y-Y-Y

upvoted 11 times

  **gssd4scoder** 3 years, 8 months ago

100% agre with you

upvoted 3 times

  **FK2974**  4 years, 4 months ago

I've put this question in during my recent training and MS trainer told this should be all Yes/Yes/Yes

upvoted 39 times

  **Jayeshp877**  2 years, 4 months ago

1.N

2.N

3.Y

100% correct, Tested

upvoted 2 times

  **[Removed]** 3 years ago

The question states add a NEW diagnostic setting, and I just tried it for all 3. The answer is Y.Y.Y

upvoted 2 times

  **Alezz** 3 years, 2 months ago

There is no indication that there was any new diagnostic settings created thus working on the assumption it's a brand new setup.

Just tested in lab and it works. Y-Y-Y

upvoted 2 times

  **Teringzooi** 3 years, 2 months ago

In which exam? AZ-305?

upvoted 2 times

  **necroknigh** 2 years, 11 months ago

Yes, this question is on the AZ-305 exam.

upvoted 1 times

  **kanweng** 3 years, 3 months ago

Yes, Yes, Yes,

You can have up to 5 diagnostic setting

Please, Notes

The storage account needs to be in the same region as the resource being monitored if the resource is regional.

The event hub namespace needs to be in the same region as the resource being monitored if the resource is regional.

only Kind(Storage, Storagev2), BlockBlobStorage is not supported.

upvoted 2 times

🗨️ 👤 **JBS** 3 years, 3 months ago

Answer is YYY. Options are clearly stating "you can add 'new' diagnostic settings". It is not saying modifying an existing settings.

A single diagnostic setting can define no more than one of each of the destinations. If you want to send data to more than one of a particular destination type (for example, two different Log Analytics workspaces), then create multiple settings. Each resource can have up to 5 diagnostic settings. Ref: <https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/diagnostic-settings?tabs=CMD>

upvoted 1 times

🗨️ 👤 **plmmsg** 3 years, 3 months ago

YES, YES, YES

upvoted 1 times

🗨️ 👤 **OlivierPaudex** 3 years, 4 months ago

The only difference I saw is that storage2 is a V2, compared to storage1.

If storage2 is a normal blob V2 storage, the answer is YES-YES-YES.

If storage2 is another type of storage (shared files, datalake), the answer is NO-YES-YES

But where did you see that storage2 is not a normal V2 blob storage ?

upvoted 1 times

🗨️ 👤 **vipin0114** 3 years, 6 months ago

Tested in LAB, answer is Yes, Yes, Yes

upvoted 5 times

🗨️ 👤 **Dpejic** 3 years, 6 months ago

Appere on exam 23-dec-2021

upvoted 3 times

🗨️ 👤 **dmitritr** 3 years, 7 months ago

NY: Only Storage V2 is shown as an option

Destination details:

- Send to Log Analytics workspace

-Archive to a storage account

Showing only general-purpose v2 storage account

-Stream to an event hub

-Send to partner solution

upvoted 1 times

🗨️ 👤 **JayBee65** 3 years ago

Your first N refers to V2 storage, so it should be a Y

upvoted 1 times

🗨️ 👤 **Metwally** 3 years, 8 months ago

Tested on lab it should be Y,Y,Y

upvoted 2 times

🗨️ 👤 **shafqat** 3 years, 8 months ago

Azure Data Lake Storage Gen2 accounts are not currently supported as a destination for diagnostic settings even though they may be listed as a valid option in the Azure portal.

No

Yes

Yes

upvoted 3 times

🗨️ 👤 **tteesstt** 3 years, 8 months ago

Yes/Yes/Yes - there is no limit on how many diagnostic settings you can create.

upvoted 1 times

🗨️ 👤 **dkltruong88** 3 years, 9 months ago

Was in exam today 1-10-2021. I passed with score 896. I chose Y, Y, Y

upvoted 6 times

  **syu31svc** 3 years, 9 months ago

<https://docs.microsoft.com/en-us/azure/azure-sql/database/metrics-diagnostic-telemetry-logging-streaming-export-configure?tabs=azure-portal>

You will also learn about the destinations to which you can stream this diagnostic telemetry and how to choose among these choices. Your destination options include:

Log Analytics and SQL Analytics

Event Hubs

Azure Storage

All Yes

upvoted 1 times

## HOTSPOT -

You deploy several Azure SQL Database instances.

You plan to configure the Diagnostics settings on the databases as shown in the following exhibit.

**Diagnostics settings**

Save Discard Delete Provide feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic settings name Diagnostic1

## Category details

log	Retention (days)
<input checked="" type="checkbox"/> SQLInsights	90 ✓
<input checked="" type="checkbox"/> AutomaticTuning	90 ✓
<input type="checkbox"/> QueryStoreRuntimeStatistics	0
<input type="checkbox"/> QueryStoreWaitStatistics	0
<input type="checkbox"/> Errors	0
<input type="checkbox"/> DatabaseWaitStatistics	0
<input type="checkbox"/> Timeouts	0
<input type="checkbox"/> Blocks	0
<input type="checkbox"/> Deadlocks	0

metric	Retention (days)
<input type="checkbox"/> Basic	0

## Destination details

☒ Send to Log Analytics

Subscription  
Azure Pass - Sponsorship

Log Analytics workspace  
sk200814 ( eastus )

☒ Archive to a storage account

Showing all storage accounts including classic storage accounts

Location  
East US

Subscription  
Azure Pass - Sponsorship

Storage account \*  
contoso20

☐ Stream to an event hub

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

The amount of time that SQLInsights data will be stored in blob storage is **[answer choice]**.

30 days  
90 days  
730 days  
indefinite

The maximum amount of time that SQLInsights data can be stored in Azure Log Analytics is **[answer choice]**.

30 days  
90 days  
730 days  
indefinite



Suggested Answer:

### Answer Area

The amount of time that SQLInsights data will be stored in blob storage is [answer choice].

30 days
90 days
730 days
indefinite

The maximum amount of time that SQLInsights data can be stored in Azure Log Analytics is [answer choice].

30 days
90 days
730 days
indefinite

In the exhibit, the SQLInsights data is configured to be stored in Azure Log Analytics for 90 days. However, the question is asking for the maximum amount of time that the data can be stored which is 730 days.

**sallymaher** Highly Voted 4 years, 3 months ago

wrong answer should be 90 and 730 if you choose 0 it will be correct  
upvoted 81 times

**STH** 3 years, 5 months ago

now 0 means indefinite (maybe this was not possible 9 months ago)  
upvoted 2 times

**AlexD332** 4 years ago

it seems 90 is correct for the first one

"First, if you are using storage for archiving, you generally want your data around for more than 365 days. Second, if you choose a retention policy that is greater than 0, the expiration date is attached to the logs at the time of storage. You can't change the date for those logs once stored."

<https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/diagnostic-settings?tabs=CMD#create-in-azure-portal>

upvoted 3 times

**AWS56** 4 years, 2 months ago

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/data-retention-privacy>

90, 730 are correct

upvoted 7 times

**abhishek\_arya02** 4 years, 1 month ago

you are correct. rest of team can check the MS documentation <https://docs.microsoft.com/en-us/azure/azure-sql/database/metrics-diagnostic-telemetry-logging-streaming-export-configure?tabs=azure-portal#data-retention-policy-and-pricing>

upvoted 1 times

**lupuscon** Highly Voted 4 years, 2 months ago

According to this:

<https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/diagnostic-settings>

Because a retention policy is set

It should be 90 days and 730 days

upvoted 12 times

**saexams** 4 years, 2 months ago

Answers are correct, first is indefinite due to checkbox selected for Archive to a storage account.

upvoted 8 times

**lupuscon** 4 years, 2 months ago

@saexams this setting only allows for longer storage if you keep the retention policy at 0

>>For example, if you set the retention policy for WorkflowRuntime to 180 days and then 24 hours later set it to 365 days, the logs stored during those first 24 hours will be automatically deleted after 180 days, while all subsequent logs of that type will be automatically deleted after 365 days. Changing the retention policy later doesn't make the first 24 hours of logs stay around for 365 days.<<

So it is 90 days and 730 days (maximum Storage duration possible)

upvoted 4 times

🗨️ **victorlie** Most Recent 2 years, 10 months ago

Tricky question

upvoted 1 times

🗨️ **AubinBakana** 2 years, 10 months ago

It's a trick question. The back up in the storage account blob will be stored indefinitely and for 90 days in the LAWS. However,, the question is asking what is the maximum amount time that that data can be stored. This does not even have anything to do with this particular question - unfair, I know.

Answer is:

- Indefinite for blob &

- 730 for in the log analytics workspace.

upvoted 1 times

🗨️ **AubinBakana** 2 years, 10 months ago

It's a trick question. The back up in the storage account blob will be stored indefinitely and for 90 days in the LAWS. However,, the question is asking what is the maximum amount time that that data can be stored. This does not even have anything to do with this particular question - unfair, I know.

Answer is:

- Indefinite for blob &

- 730 for in the log analytics workspace.

upvoted 1 times

🗨️ **VijayRaja2000** 3 years ago

Given Answers are correct.

Indefinite : Archiving logs and metrics to an Azure storage account is useful for audit, static analysis, or backup. Compared to Azure Monitor Logs and a Log Analytics workspace, Azure storage is less expensive and logs can be kept there indefinitely.

<https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/diagnostic-settings?tabs=portal#destinations>

730 days : By default Application Insights and Log Analytics has a data retention of 90 days. You can opt to extend the retention up to 730 days.

<https://support.tygraph.com/support/solutions/articles/67000572648-changing-azure-log-analytics-retention>

upvoted 1 times

🗨️ **OCHT** 3 years, 1 month ago

90 and 730. It's verified.

upvoted 1 times

🗨️ **achechen** 3 years, 1 month ago

This question seems to be outdated. Tested in Azure Portal. When you select "Archive to a storage account" option, the following info is displayed:

"Retention only applies to storage account. Retention policy ranges from 1 to 365 days. If you do not want to apply any retention policy and retain data forever, set retention (days) to 0."

upvoted 1 times

🗨️ **VijayRaja2000** 3 years, 1 month ago

For storage account, it is indefinite for sure as you can see from this link <https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/diagnostic-settings?tabs=CMD>. For log analytics workspace, it seems to be depending upon the pricing tier.

upvoted 1 times

🗨️ **hertino** 3 years, 2 months ago

In AZ-305 exam, 9 april 22

upvoted 7 times

🗨️ **kanweng** 3 years, 3 months ago

90 and 730,

the picture Retention Day is for Storage account, ( you don't set the Retention day for Log analytics in Diagnostic setting (picture).

upvoted 1 times

🗨️ **plmmsg** 3 years, 3 months ago

answer is 90, 730

upvoted 1 times

🗨️ 👤 **arun** 3 years, 3 months ago

Have tried it... when we enable 'Archive to Storage Account' option then only the retention period section is shown... so the retention period is applicable only to Storage account so 90 & 730 are right answers.

upvoted 1 times

🗨️ 👤 **plmmmsg** 3 years, 4 months ago

90 and 730

upvoted 1 times

🗨️ 👤 **vipin0114** 3 years, 6 months ago

If selected value is 90 then it will consider 90 days and if selected value is 0 then it will consider indefinite. so correct answer is 90 and 730 days

upvoted 2 times

🗨️ 👤 **Dpejic** 3 years, 6 months ago

On exam 24.12.2021

upvoted 4 times

🗨️ 👤 **aromanrod** 3 years, 6 months ago

that's correct, 90 is the amount of retention time in LogAnalytics, but the logs will be stored indefinitely, if you need to clean up the logs is necessary to apply life cycle management for Storage Accounts. Second question: is asking for the maximum amount of time that Log Analytics could store the log on it, so the maximum amount is 730 days. both answers are correct.

upvoted 2 times

Your company uses Microsoft System Center Service Manager on its on-premises network. You plan to deploy several services to Azure. You need to recommend a solution to push Azure service health alerts to Service Manager. What should you include in the recommendation?

- A. IT Service Management Connector (ITSM)
- B. Azure Event Hubs
- C. Azure Notification Hubs
- D. Application Insights Connector

**Suggested Answer: A**

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/itsmc-overview>

Community vote distribution

A (100%)

  **pk1977** Highly Voted 4 years, 3 months ago

Seems correct.

<https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/itsmc-overview>

ITSMC supports connections with the following ITSM tools:

ServiceNow

System Center Service Manager

Provance

Cherwell

With ITSMC, you can:

Create work items in your ITSM tool, based on your Azure alerts (Metric Alerts, Activity Log Alerts, and Log Analytics alerts).

Optionally, you can sync your incident and change request data from your ITSM tool to an Azure Log Analytics workspace.

Also:

<https://azure.microsoft.com/en-us/blog/how-to-develop-your-service-health-alerting-strategy/>

"plug the alerts into your existing problem management system using a webhook/ITSM connection so you can follow your normal workflow."

And:

<https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/itsmc-connections-scsrm>

upvoted 31 times

  **syu31svc** 3 years, 9 months ago

You said it all


A is the answer indeed

upvoted 2 times

  **heamgu** Highly Voted 4 years ago

A. IT Service Management Connector (ITSM)

upvoted 7 times

  **Snownoodles** Most Recent 3 years, 2 months ago

Is this question obsoleted?

<https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/itsmc-overview>

"As of March 1, 2022, System Center ITSM integrations with Azure alerts is no longer enabled for new customers. New System Center ITSM Connections are not supported. Existing ITSM connections are supported"

upvoted 3 times

  **kanweng** 3 years, 3 months ago

**Selected Answer: A**

Create Azure Service Health Alert with Action Group (Azure monitor alert), ---> ITSM

upvoted 1 times

🗨️ 👤 **Uglydotcom** 3 years, 4 months ago

A should be correct

upvoted 1 times

🗨️ 👤 **VT1100** 3 years, 5 months ago

**Selected Answer: A**

ITSM is for connectivity between ticketing systems like SNOW or Service Manager.

upvoted 2 times

🗨️ 👤 **us3r** 3 years, 5 months ago

**Selected Answer: A**

ITSM

.

upvoted 1 times

🗨️ 👤 **Dpejic** 3 years, 6 months ago

On exam 24.12.2021

upvoted 2 times

🗨️ 👤 **Dpejic** 3 years, 6 months ago

Appere on exam 23-dec-2021

upvoted 1 times

🗨️ 👤 **wooyourdaddy** 3 years, 6 months ago

**Selected Answer: A**

Ref link: <https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/itsmc-overview#configuration-steps>

upvoted 2 times

🗨️ 👤 **NewGuyAmazon** 3 years, 9 months ago

seems correct

upvoted 2 times

🗨️ 👤 **lowczy** 3 years, 11 months ago

This question appeared in real exam.

upvoted 6 times

## HOTSPOT -

You have an Azure subscription that contains 300 Azure virtual machines that run Windows Server 2019. You need to centrally monitor all warning events in the System logs of the virtual machines.

What should you include in the solution? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Resource to create in Azure:

An event hub
A Log Analytics workspace
A search service
A storage account

Configuration to perform on the virtual machines:

Create event subscriptions
Configure Continuous delivery
Install the Microsoft Monitoring Agent
Modify the membership of the Event Log Readers group

**Answer Area**

Resource to create in Azure:

An event hub
A Log Analytics workspace
A search service
A storage account


Suggested Answer:

Configuration to perform on the virtual machines:

Create event subscriptions
Configure Continuous delivery
Install the Microsoft Monitoring Agent
Modify the membership of the Event Log Readers group


Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-sources-windows-events> <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/agent-windows>

 **happypig13** Highly Voted 4 years, 3 months ago

answer correct

upvoted 32 times

 **Rume** Highly Voted 4 years ago

Came in todays exam 6 Jun 2021!

upvoted 13 times

🗨️ 👤 **gauravit43** Most Recent 2 years, 2 months ago

I have passed AZ-305 on 15th April,2023 and this question was there in the exam  
upvoted 1 times

🗨️ 👤 **GreenMood** 2 years, 10 months ago

in AZ-305 exam, 12th August.  
upvoted 3 times

🗨️ 👤 **hertino** 3 years, 2 months ago

In AZ-305 exam, 9 april 22  
upvoted 7 times

🗨️ 👤 **plmmsg** 3 years, 3 months ago

A Log Analytics Workspace &  
Microsoft Monitoring Agent  
upvoted 1 times

🗨️ 👤 **syu31svc** 3 years, 9 months ago

"monitor all warning events" so use log analytics workspace

Install the agent on the VM is the logical answer from the second drop down  
upvoted 2 times

🗨️ 👤 **nkx** 3 years, 9 months ago

Came in exam on 20-sep-21, i passed, answers are correct  
upvoted 4 times

🗨️ 👤 **komoyek** 3 years, 11 months ago

Good luck to all 🍀🍀🍀  
upvoted 11 times

🗨️ 👤 **heamgu** 4 years ago

A Log Analytics Workspace  
Install the Microsoft Monitoring Agent  
upvoted 3 times

🗨️ 👤 **angevil** 4 years ago

why not event Hub?  
upvoted 1 times

🗨️ 👤 **DragonsGav** 4 years ago

Event Hub you can not analyse or correlate logs. Log Analytics workspace is one central place, where you can collect all logs from different  
resources and query/action  
upvoted 1 times

🗨️ 👤 **pentium75** 3 years, 10 months ago

Azure Event Hub has NOTHING to do with Windows events.  
upvoted 1 times

🗨️ 👤 **derin68** 4 years, 1 month ago

Seems correct. Discussed in the <https://www.examttopics.com/exams/microsoft/az-303/view/12/> #57  
upvoted 3 times

🗨️ 👤 **AkashS** 4 years, 1 month ago

Correct  
upvoted 1 times

🗨️ 👤 **LT** 4 years, 1 month ago

Passed the exam (8th May 2021). This question was in exam. Dump covered 50-60%  
upvoted 5 times

🗨️ 👤 **AustinY** 4 years, 3 months ago

Correct answers! Similar questions exist in AZ-303  
upvoted 6 times

You have an Azure SQL database named DB1 that contains multiple tables.  
 You need to improve the performance of DB1. The solution must minimize administrative effort.  
 What should you use?

- A. automatic tuning
- B. Azure Advisor
- C. Azure Monitor
- D. Query Performance Insight

**Suggested Answer: A**

Azure SQL Database and Azure SQL Managed Instance automatic tuning provides peak performance and stable workloads through continuous performance tuning based on AI and machine learning.

Automatic tuning is a fully managed intelligent performance service that uses built-in intelligence to continuously monitor queries executed on a database, and it automatically improves their performance.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/automatic-tuning-overview>


Community vote distribution

A (100%)

 **AustinY** Highly Voted 4 years, 2 months ago

Correct!


upvoted 31 times

 **Meedeh** Highly Voted 4 years, 1 month ago

Automatic tuning is a fully managed intelligent performance service that uses built-in intelligence to continuously monitor queries executed on a database, and it automatically improves their performance.

<https://docs.microsoft.com/en-us/azure/azure-sql/database/automatic-tuning-overview>

upvoted 20 times


 **Teringzooi** Most Recent 3 years, 1 month ago

**Selected Answer: A**

Correct answer: A

<https://docs.microsoft.com/en-us/sql/relational-databases/automatic-tuning/automatic-tuning?view=sql-server-ver15>

upvoted 1 times

 **Dawn7** 3 years, 3 months ago

**Selected Answer: A**

Correct

upvoted 2 times

 **Jcbrow27** 3 years, 3 months ago

**Selected Answer: A**

<https://docs.microsoft.com/en-us/sql/relational-databases/automatic-tuning/automatic-tuning?view=sql-server-ver15>

notifies you whenever a potential performance issue is detected and lets you apply corrective actions, or lets the Database Engine automatically fix performance problems.

upvoted 1 times

 **plmmsg** 3 years, 3 months ago

Automatic tuning

upvoted 1 times

 **Azure\_daemon** 3 years, 4 months ago

A is correct

upvoted 1 times



🗨️ 👤 **Dawn7** 3 years, 5 months ago

**Selected Answer: A**

I think A is correct

upvoted 1 times

🗨️ 👤 **moon2351** 3 years, 8 months ago

Correct!

upvoted 2 times

🗨️ 👤 **syu31svc** 3 years, 9 months ago

"improve the performance" so answer is A

upvoted 2 times

🗨️ 👤 **Andres\_P** 3 years, 9 months ago

Why not D? Query Performance Insigh

upvoted 2 times

🗨️ 👤 **ImNotReallyHere** 3 years, 7 months ago

Because the question also states that it must minimize administrative effort. Query Performance Insights requires an admin to interpret the results and take action while Automatic Tuning is.... Automatic.

upvoted 8 times

🗨️ 👤 **Manish03Nov** 3 years, 10 months ago

Correct!

upvoted 1 times

🗨️ 👤 **Dinya\_jui** 3 years, 11 months ago

Correct!

Automatic tuning is a fully managed intelligent performance service that uses built-in intelligence to continuously monitor queries executed on a database, and it automatically improves their performance.

upvoted 3 times

🗨️ 👤 **heamgu** 4 years ago

A. automatic tuning

upvoted 5 times

You need to recommend a solution to generate a monthly report of all the new Azure Resource Manager resource deployments in your subscription.

What should you include in the recommendation?

- A. Azure Advisor
- B. Azure Analysis Services
- C. Azure Monitor action groups
- D. Azure Log Analytics

**Suggested Answer: D**



Log Analytics is a tool in the Azure portal used to edit and run log queries with data in Azure Monitor Logs. You may write a simple query that returns a set of records and then use features of Log Analytics to sort, filter, and analyze them. Or you may write a more advanced query to perform statistical analysis and visualize the results in a chart to identify a particular trend.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-overview>



Community vote distribution

D (100%)

  **RickMorais** Highly Voted 3 years, 10 months ago

This question could have different options. Consulting other fonts I found the D option was Azure Activity Logs.

Explanation: Activity logs are kept for 90 days. You can query for any range of dates, as long as the starting date isn't more than 90 days in the past.  
upvoted 10 times

  **anthonyphuc** Highly Voted 3 years, 6 months ago

Repeated question #1 on this topic

#1: Activity Log

#13: Log Analytics

upvoted 6 times

  **plmmsg** Most Recent 3 years, 3 months ago

D. Azure Log Analytics

upvoted 1 times

  **ixl2pass** 3 years, 5 months ago

I will go with Azure Monitor. Centralized logs, auto analysis, integration with 3rd party . It meets all the requirements.

<https://docs.microsoft.com/en-us/azure/azure-monitor/logs/service-providers>

<https://docs.microsoft.com/en-us/azure/azure-monitor/best-practices-analysis>



<https://docs.microsoft.com/en-us/azure/azure-monitor/partners>

upvoted 1 times

  **Dpejic** 3 years, 6 months ago

On exam 24.12.2021

upvoted 4 times

  **wooyourdaddy** 3 years, 6 months ago

Selected Answer: D

Ref Link: <https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log>

upvoted 6 times

  **Eitant** 3 years, 6 months ago

Selected Answer: D

Correct Answer

upvoted 4 times

  **Ahmadtooo** 3 years, 7 months ago

Correct Answer: D

You need to recommend a solution to generate a monthly report of all the new Azure Resource Manager resource deployments in your subscription.

What should you include in the recommendation?

upvoted 2 times

  **Ahmadtooo** 3 years, 7 months ago


The Azure Activity Log provides insight into subscription-level events that have occurred in Azure. This includes a range of data, from Azure Resource Manager operational data to updates on Service Health events.

upvoted 3 times

  **syu31svc** 3 years, 9 months ago



Best answer here is D

upvoted 3 times

  **GuxMAN** 3 years, 9 months ago



Repeated question. Follow the answers from Q1

upvoted 5 times

  **Viji30** 3 years, 10 months ago

what is the answer? no discussion

upvoted 1 times

  **seedati** 3 years, 10 months ago

correct

upvoted 3 times

Your company provides customer support for multiple Azure subscriptions and third-party hosting providers.

You are designing a centralized monitoring solution. The solution must provide the following services:

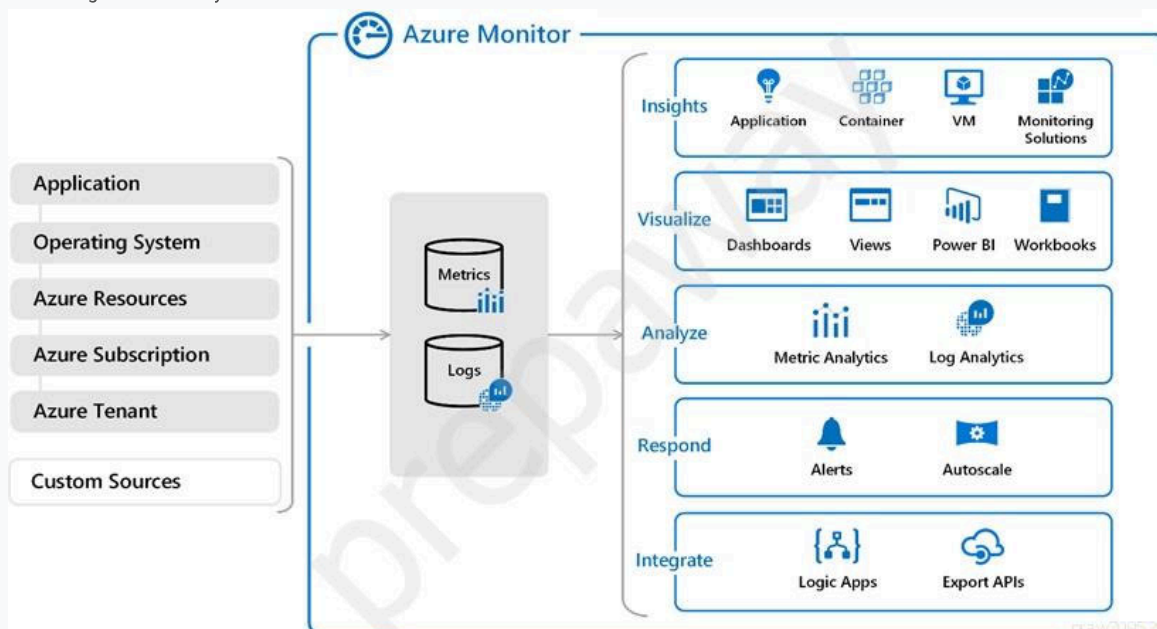
- ⇒ Collect log and diagnostic data from all the third-party hosting providers into a centralized repository.
- ⇒ Collect log and diagnostic data from all the subscriptions into a centralized repository.
- ⇒ Automatically analyze log data and detect threats.
- ⇒ Provide automatic responses to known events.

Which Azure service should you include in the solution?

- A. Azure Sentinel
- B. Azure Log Analytics
- C. Azure Monitor
- D. Azure Application Insights

**Suggested Answer: C**

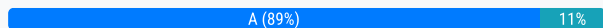
The following diagram gives a high-level view of Azure Monitor. At the center of the diagram are the data stores for metrics and logs, which are the two fundamental types of data used by Azure Monitor. On the left are the sources of monitoring data that populate these data stores. On the right are the different functions that Azure Monitor performs with this collected data. This includes such actions as analysis, alerting, and streaming to external systems.



Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/overview>

Community vote distribution



asahel Highly Voted 3 years, 9 months ago

Sentinel: Detect previously undetected threats and Respond to incidents rapidly  
upvoted 46 times

Ario 3 years, 9 months ago

You are Absolutely correct  
upvoted 4 times

simonevenezia Highly Voted 3 years, 9 months ago

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

Microsoft Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution. Azure Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Azure Sentinel is your birds-eye view across the enterprise alleviating the stress of increasingly sophisticated attacks, increasing volumes of alerts, and long resolution time frames.

Collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.

Detect previously undetected threats, and minimize false positives using Microsoft's analytics and unparalleled threat intelligence.

Investigate threats with artificial intelligence, and hunt for suspicious activities at scale, tapping into years of cyber security work at Microsoft.

Respond to incidents rapidly with built-in orchestration and automation of common tasks.

upvoted 18 times

🗲️ 👤 **Marciojsilva** Most Recent 2 years, 9 months ago

**Selected Answer: C**

Azure Sentinel can be integrated into Azure Monitor which already automatically responds to known events. Check out the video in the description of the given answer.

C is correc

upvoted 1 times

🗲️ 👤 **jellybiscuit** 2 years, 9 months ago

**Selected Answer: C**

Monitor - it's going to exist whether or not you choose to use Sentinel.

upvoted 1 times

🗲️ 👤 **viveksen1** 2 years, 10 months ago

Sentinel should be the correct answer ....option A

upvoted 3 times

🗲️ 👤 **DChilds** 2 years, 10 months ago

**Selected Answer: C**

Azure Sentinel can be integrated into Azure Monitor which already automatically responds to known events. Check out the video in the description of the given answer.

C is correct.

upvoted 1 times

🗲️ 👤 **AubinBakana** 2 years, 10 months ago

**Selected Answer: C**

Sentinel pulls data from Log Analytics workspace, with in turn pulls data from Monitor. Data collected from Azure monitor can be sent to 3rd party SIEMS, such as Azure Sentinel which can then be used for threat intelligence, ITSM tool, APM providers, etc.

The answer here is not that simple but with Azure Monitor, you can achieve everything that is required here.

The need to clarify this question as obviously, it is umbiguous with all the opinion devise here.

Both Monitor & Sentinel are required here but if I have to pick, it has to be Azure Monitor

Contrary to the majority, the answer has to be C.

upvoted 1 times

🗲️ 👤 **NunoVarelaa** 2 years, 11 months ago

**Selected Answer: A**

Correct Answer: A

upvoted 2 times

🗲️ 👤 **LillyLiver** 3 years ago

**Selected Answer: C**

I was completely on-board with others that it was Sentinal. But something was pulling at me and telling me that wasn't right. Go to the provided URL. There is a 5 minute video on this and now I believe that the given answer is correct.

Sentinel won't meet all the requirements by itself. But it can pull the data from AZ Monitor and do what it needs to. So yes, the answer is C.

upvoted 1 times

🗲️ 👤 **Teringzooi** 3 years, 1 month ago

**Selected Answer: A**

Correct Answer: A

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

Microsoft Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution. Azure Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response.

upvoted 2 times

🗲️ 👤 **Kanmaj10** 3 years, 3 months ago

Answer should be Sentinel. Monitor is just one of the tools Sentinel uses . Whenever , we hear the words intelligence , threat analysis etc. the answer should be sentinel. Offcourse it would require Monitor collect the logs and create alerting etc.

upvoted 1 times

🗲️ 👤 **plmmsg** 3 years, 3 months ago

A. Azure Sentinel

upvoted 2 times

🗲️ 👤 **arun** 3 years, 3 months ago

**Selected Answer: A**

Sentinel can collect log from any sources and detect threats

upvoted 2 times

🗲️ 👤 **LuBarba** 3 years, 4 months ago

**Selected Answer: A**

Azure Sentinel

upvoted 3 times

🗲️ 👤 **Hudhaifa** 3 years, 4 months ago

On Exam 19th Feb 2022

upvoted 2 times

🗲️ 👤 **jeetnix2121** 3 years, 4 months ago

what you have selected ?

upvoted 1 times

🗲️ 👤 **VT1100** 3 years, 5 months ago

**Selected Answer: A**

Now re-branded to Microsoft Sentinel, it is used for SIEM and 3rd party connectivity.

upvoted 5 times

🗲️ 👤 **pruntelnetworks** 3 years, 5 months ago

**Selected Answer: A**

A sentinel

upvoted 4 times

You are designing an Azure resource deployment that will use Azure Resource Manager templates. The deployment will use Azure Key Vault to store secrets.

You need to recommend a solution to meet the following requirements:

- ⇒ Prevent the IT staff that will perform the deployment from retrieving the secrets directly from Key Vault.
- ⇒ Use the principle of least privilege.

Which two actions should you recommend? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Create a Key Vault access policy that allows all get key permissions, get secret permissions, and get certificate permissions.
- B. From Access policies in Key Vault, enable access to the Azure Resource Manager for template deployment.
- C. Create a Key Vault access policy that allows all list key permissions, list secret permissions, and list certificate permissions.
- D. Assign the IT staff a custom role that includes the Microsoft.KeyVault/Vaults/Deploy/Action permission.
- E. Assign the Key Vault Contributor role to the IT staff.

**Suggested Answer: BD**

B: To access a key vault during template deployment, set `enabledForTemplateDeployment` on the key vault to true.

D: The user who deploys the template must have the `Microsoft.KeyVault/vaults/deploy/action` permission for the scope of the resource group and key vault.

Incorrect Answers:

E: To grant access to a user to manage key vaults, you assign a predefined key vault Contributor role to the user at a specific scope.


If a user has Contributor permissions to a key vault management plane, the user can grant themselves access to the data plane by setting a Key Vault access policy. You should tightly control who has Contributor role access to your key vaults. Ensure that only authorized persons can access and manage your key vaults, keys, secrets, and certificates.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/key-vault-parameter> <https://docs.microsoft.com/en-us/azure/key-vault/general/overview-security>

Community vote distribution

BD (100%)

 **certmonster** Highly Voted 4 years, 8 months ago


The answers are correct.

upvoted 57 times

 **sanketshah** 4 years, 5 months ago

given answer is correct.

upvoted 5 times

 **Virendrak** Highly Voted 4 years, 8 months ago

The answers are correct:

1. On access policy page of azure key vault check the option "Azure Resource Manager for template deployment"

Enable Access to:

Azure Virtual Machines for deployment

Azure Resource Manager for template deployment

Azure Disk Encryption for volume encryption

2. Add a custom role for IT staff

upvoted 14 times

 **OCHT** Most Recent 3 years, 1 month ago

Ofcos BD .

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/key-vault-parameter?tabs=azure-cli>

upvoted 1 times

 **kanweng** 3 years, 3 months ago

**Selected Answer: BD**

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/key-vault-parameter?tabs=azure-cli>

upvoted 3 times

  **plmmsg** 3 years, 3 months ago

B & D is correct answers

upvoted 1 times

  **ERROR505** 3 years, 4 months ago

**Selected Answer: BD**

Correct

upvoted 1 times

  **Hudhaifa** 3 years, 4 months ago

On Exam 19th Feb 2022

upvoted 1 times

  **Azure\_daemon** 3 years, 4 months ago


B & D are the correct answers

upvoted 1 times

  **examineezer** 3 years, 6 months ago

I guess D is preferable to E because of the "principle of least privilege" requirement.



upvoted 1 times

  **dorian\_grecu** 3 years, 6 months ago

**Selected Answer: BD**

The answers are correct.

upvoted 5 times

  **Bob888** 3 years, 8 months ago

BD are correct

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/key-vault-parameter?tabs=azure-powershell>

upvoted 2 times

  **syu31svc** 3 years, 9 months ago

"least privilege"

Only B and D fit the bill

upvoted 2 times

  **nkx** 3 years, 9 months ago

Came in exam on 20-sep-21, i passed, answers are correct, but i choose E by mistake, but passed

upvoted 4 times

  **murongqing** 3 years, 11 months ago

B&D correct answer

upvoted 1 times

  **DragonsGav** 4 years ago

Correct BD

Option D [Refer to <https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/template-tutorial-use-key-vault>]

upvoted 2 times

  **heamgu** 4 years ago

B. From Access policies in Key Vault, enable access to the Azure Resource Manager for template deployment.

D. Assign the IT staff a custom role that includes the Microsoft.KeyVault/Vaults/Deploy/Action permission.

upvoted 1 times

  **LT** 4 years, 1 month ago

Passed the exam (8th May 2021). This question was in exam. Dump covered 50-60%

upvoted 4 times

  **17Master** 3 years, 4 months ago

moderador "delete LT"



upvoted 1 times

  **Amit3** 4 years ago

So how did you cover rest of exam material (50-40%) ?

upvoted 1 times

  **cfsxtuv33** 4 years ago

What other material did you use for the exam?

upvoted 1 times

You have an Azure subscription that contains web apps in three Azure regions.

You need to implement Azure Key Vault to meet the following requirements:

- ⇒ In the event of a regional outage, all keys must be readable.
- ⇒ All the web apps in the subscription must be able to access Key Vault.
- ⇒ The number of Key Vault resources to be deployed and managed must be minimized.

How many instances of Key Vault should you implement?

- A. 1
- B. 2
- C. 3
- D. 6

#### Suggested Answer: A

The contents of your key vault are replicated within the region and to a secondary region at least 150 miles away but within the same geography. This maintains high durability of your keys and secrets. See the Azure paired regions document for details on specific region pairs. Example: Secrets that must be shared by your application in both Europe West and Europe North. Minimize these as much as you can. Put these in a key vault in either of the two regions. Use the same URI from both regions. Microsoft will fail over the Key Vault service internally.

Reference:

<https://docs.microsoft.com/en-us/azure/key-vault/general/disaster-recovery-guidance>

Community vote distribution

C (50%)

A (50%)

🗳️ 👤 **Smiles99** Highly Voted 4 years, 3 months ago

The correct answer is A. The question asks "How many instances of Key Vault should you implement?". You need just one. Azure already makes the Key highly available and automatically failover on case of an outage to a paired region except for the Brazil South Region.

upvoted 78 times

🗳️ 👤 **sallymaher** Highly Voted 4 years, 3 months ago

Correct answer is C, in the event of a regional outage, all keys must be readable. I believe the trick here is "keys" key vault can store certificate, keys and secrets during the failover "get" Get (properties of) keys that means "Key" will not be readable

ref: <https://docs.microsoft.com/en-us/azure/key-vault/general/disaster-recovery-guidance>

ref: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault>

Warning section

upvoted 24 times

🗳️ 👤 **[Removed]** 4 years, 3 months ago

however the question only talks about web app accessing key vault. As the VM encryption is not mentioned I believe answer should be 1. During regional outage 1 key vault will allow retrieving key and secrets from VM and web app from other regions

upvoted 2 times

🗳️ 👤 **sallymaher** 4 years, 3 months ago

at the same you are assuming the apps in 3 paired regions, what if they are not? , so to be in safe side you should consider this factor and create 3 key vaults, still my answer is 3

upvoted 9 times

🗳️ 👤 **zsedo** 3 years, 8 months ago

During a regional outage you cannot put new / update the existing secrets, keys, certificates.

That is basically the limitation. "During failover, your key vault is in read-only mode."

<https://docs.microsoft.com/en-us/azure/key-vault/general/disaster-recovery-guidance>

I would go with "A".

upvoted 3 times

🗳️ 👤 **Terinzooi** 3 years, 1 month ago

Wrong. 1 keyvault.

<https://docs.microsoft.com/en-us/azure/key-vault/general/disaster-recovery-guidance>

Correct answer: A

upvoted 1 times

🗳️ 👤 **AWS56** 4 years, 2 months ago

C is incorrect, As per "<https://docs.microsoft.com/en-us/azure/key-vault/general/disaster-recovery-guidance>" check below

----

In the rare event that an entire Azure region is unavailable, the requests that you make of Azure Key Vault in that region are automatically routed (failed over) to a secondary region except in the case of the Brazil South region. When the primary region is available again, requests are routed back (failed back) to the primary region. Again, you don't need to take any action because this happens automatically.

-----

The correct answer is A

upvoted 13 times

🗳️ 👤 **ShivaUdari** Most Recent 1 year, 9 months ago

Selected Answer: C

Apps are in 3 different regions, so need 3 KV's and KV pairing doesn't happen to 3 regions.

upvoted 1 times

🗳️ 👤 **calotta1** 1 year, 10 months ago

Answer must be A based on the article provided - "In the rare event that an entire Azure region is unavailable, the requests that you make of Azure Key Vault in that region are automatically routed (failed over) to a secondary region . When the primary region is available again, requests are routed back (failed back) to the primary region. Again, you don't need to take any action because this happens automatically."

upvoted 1 times

🗳️ 👤 **wwwmmm** 2 years, 6 months ago

Anyone passed the exam can share what they choose and whether they passed please?

upvoted 1 times

🗳️ 👤 **PPP164** 2 years, 8 months ago

Correct answer is A only, key vault automatically replicated to paired region. Even though web apps are deployed to 3 different regions, in order to get key vault access one can registered all 3 web apps under Azure AD App Registration so actually there is no linkage between regions of web app deployment and regions of key vault. It is trick only.

upvoted 1 times

🗳️ 👤 **ROLLINGROCKS** 2 years, 9 months ago

Selected Answer: C

3 REGIONS = 3 KEY VAULTS

upvoted 1 times

🗳️ 👤 **ROLLINGROCKS** 2 years, 9 months ago

Selected Answer: A

3 REGIONS = 3 KEY VAULTS

upvoted 1 times

🗳️ 👤 **ROLLINGROCKS** 2 years, 9 months ago

I meant C :(

upvoted 1 times

🗳️ 👤 **sapien45** 3 years ago

In the rare event that an entire Azure region is unavailable, the requests that you make of Azure Key Vault in that region are automatically routed (failed over) to a secondary region except in the case of the Brazil South and Qatar Central region. When the primary region is available again, requests are routed back (failed back) to the primary region. Again, you don't need to take any action because this happens automatically.

A

upvoted 1 times

🗳️ 👤 **VijayRaja2000** 3 years, 1 month ago

Might be useful . In the rare event that an entire Azure region is unavailable, the requests that you make of Azure Key Vault in that region are automatically routed (failed over) to a secondary region except in the case of the Brazil South and Qatar Central region. When the primary region is available again, requests are routed back (failed back) to the primary region. Again, you don't need to take any action because this happens automatically.

<https://docs.microsoft.com/en-us/azure/key-vault/general/disaster-recovery-guidance>

upvoted 1 times

🗳️ 👤 **itengineerd** 3 years, 3 months ago

Selected Answer: C

Per Microsoft: <https://docs.microsoft.com/en-us/azure/key-vault/general/best-practices>

"Our recommendation is to use a vault per application per environment (development, pre-production, and production), per region. This helps you not share secrets across environments and regions. It will also reduce the threat in case of a breach"

With apps in 3 regions, C would appear to be the correct best-practices answer.

upvoted 6 times

🗳️ 👤 **ROLLINGROCKS** 2 years, 9 months ago

This is the correct answer. Forget about the availability, if you are working in three regions, you need a Key Vault per region.

upvoted 1 times

🗳️ 👤 **Fal9911** 2 years, 9 months ago

Make more sense in general

upvoted 1 times

🗳️ 👤 **kanchanar05** 3 years, 3 months ago

As Azure Vault is region-specific, 3 vaults would be required.

upvoted 1 times

🗳️ 👤 **soucine** 3 years, 3 months ago

**Selected Answer: A**

This is really confusing. Microsoft's recommendation is :

"Our recommendation is to use a vault per application per environment (development, pre-production, and production), per region. This helps you not share secrets across environments and regions. It will also reduce the threat in case of a breach."

But we don't know how many webs app we have. We only know that we have these apps in three regions. So it seems like the question is about the automatic intergrated replication/fail-over mechanism, and thus the answer would be 1 (A).

Source : <https://docs.microsoft.com/en-us/azure/key-vault/general/best-practices#:~:text=Our%20recommendation%20is%20to%20use,in%20case%20of%20a%20breach.>

upvoted 1 times

🗳️ 👤 **FlyingMachine** 3 years, 3 months ago

**Selected Answer: C**

3 KVs in 3 Regions

upvoted 1 times

🗳️ 👤 **thebarber87** 3 years, 3 months ago

**Selected Answer: A**

Answer is 1

upvoted 1 times

🗳️ 👤 **plmmsg** 3 years, 3 months ago

**Selected Answer: A**

1 key is enough

upvoted 2 times

🗳️ 👤 **d3an** 3 years, 4 months ago

**Selected Answer: A**

Available in regional outage

upvoted 2 times

You have an Azure Active Directory (Azure AD) tenant.

You plan to provide users with access to shared files by using Azure Storage. The users will be provided with different levels of access to various Azure file shares based on their user account or their group membership.

You need to recommend which additional Azure services must be used to support the planned deployment.

What should you include in the recommendation?

- A. an Azure AD enterprise application
- B. Azure Information Protection
- C. an Azure AD Domain Services (Azure AD DS) instance
- D. an Azure Front Door instance

**Suggested Answer: C**

Azure Files supports identity-based authentication over Server Message Block (SMB) through two types of Domain Services: on-premises Active Directory Domain Services (AD DS) and Azure Active Directory Domain Services (Azure AD DS).

Reference:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-active-directory-domain-service-enable>

Community vote distribution



**nlr** Highly Voted 4 years, 9 months ago

Given answer is correct

upvoted 49 times

**sanketshah** 4 years, 5 months ago

given answer is correct.

upvoted 3 times

**leo\_az300** Highly Voted 3 years, 8 months ago

Answer is correct,

There are 2 levels of permissions to assign to users, one is on file-share level, and another is on directory level

Configure share-level permissions for Azure Files

Once either Azure AD DS or on-premises AD DS authentication is enabled, you can use Azure built-in roles or configure custom roles for Azure AD identities and assign access rights to any file shares in your storage accounts. The assigned permission allows the granted identity to get access to the share only, nothing else, not even the root directory. You still need to separately configure directory or file-level permissions for Azure file shares.

Configure directory or file-level permissions for Azure Files

Azure file shares enforce standard Windows file permissions at both the directory and file level, including the root directory. Configuration of directory or file-level permissions is supported over both SMB and REST. Mount the target file share from your VM and configure permissions using Windows File Explorer, Windows icacfs, or the Set-ACL command.

upvoted 19 times

**rdemontis** 3 years, 7 months ago

thanks for explanation

upvoted 2 times

**hertino** Most Recent 3 years, 2 months ago

In AZ-305 exam, 9 april 22

upvoted 10 times

**plmmg** 3 years, 3 months ago

Selected Answer: C

C. an Azure AD Domain Services (Azure AD DS) instance

upvoted 1 times

🗨️ 👤 **17Master** 3 years, 4 months ago

correct answer is C. Azure AD DS over SMB  
upvoted 2 times

🗨️ 👤 **Dawn7** 3 years, 5 months ago

**Selected Answer: C**

I will go with C  
upvoted 1 times

🗨️ 👤 **Dpejic** 3 years, 6 months ago

On exam 24.12.2021  
upvoted 3 times

🗨️ 👤 **sharepoint\_Azure\_pp** 3 years, 8 months ago

Answer is correct or can say i choose the same.  
was there in 17th October 2021 cleared with 900  
upvoted 4 times

🗨️ 👤 **syu31svc** 3 years, 9 months ago

Key word is "files"

<https://docs.microsoft.com/en-us/azure/storage/files/storage-files-active-directory-overview#how-it-works>

Azure file shares leverages Kerberos protocol for authenticating with either on-premises AD DS or Azure AD DS

Answer is C

upvoted 3 times

🗨️ 👤 **souvik123** 3 years, 9 months ago

C. an Azure AD Domain Services (Azure AD DS) instance  
upvoted 1 times

🗨️ 👤 **RagazzoAlex** 3 years, 12 months ago

Other options do not make sense  
upvoted 4 times

🗨️ 👤 **heamgu** 4 years ago

C. an Azure AD Domain Services (Azure AD DS) instance  
upvoted 3 times

🗨️ 👤 **demonite** 4 years, 1 month ago

Correct answer  
<https://docs.microsoft.com/en-us/azure/storage/files/storage-files-active-directory-overview#how-it-works>  
upvoted 2 times

🗨️ 👤 **Vipsao** 4 years, 3 months ago

The answer is correct  
upvoted 2 times

🗨️ 👤 **Manishsaini** 4 years, 3 months ago

given answer is correct  
upvoted 3 times

🗨️ 👤 **glam** 4 years, 5 months ago

C. an Azure AD Domain Services (Azure AD DS) instance  
upvoted 4 times

🗨️ 👤 **Jinder** 4 years, 5 months ago

Can someone please explain where you get a clue to use Azure AD DS. Question statement never talked about hybrid/on-prem users and groups.  
Thanks  
upvoted 3 times

🗨️ 👤 **fred00r** 4 years, 5 months ago



I think the key here is:

"Azure Files supports identity-based authentication over Server Message Block (SMB) through two types of Domain Services: on-premises Active Directory Domain Services (AD DS) and Azure Active Directory Domain Services (Azure AD DS)"

- <https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-active-directory-domain-service-enable?tabs=azure-portal>

So AZ DS is set.

upvoted 9 times

  **Jinder** 4 years, 4 months ago

Thanks. That makes sense.

upvoted 5 times

## DRAG DROP -

Your company has users who work remotely from laptops.

You plan to move some of the applications accessed by the remote users to Azure virtual machines. The users will access the applications in Azure by using a point-to-site VPN connection. You will use certificates generated from an on-premises-based Certification authority (CA).

You need to recommend which certificates are required for the deployment.

What should you include in the recommendation? To answer, drag the appropriate certificates to the correct targets. Each certificate may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

**Certificates**

A root CA certificate that has the private key

A root CA certificate that has the public key only

A user certificate that has the private key

A user certificate that has the public key only

**Answer Area**

Trusted Root Certification Authorities certificate store on each laptop:

Certificate

The users' Personal store on each laptop:

Certificate

The Azure VPN gateway:

Certificate

**Suggested Answer:****Certificates**

A root CA certificate that has the private key

A root CA certificate that has the public key only

A user certificate that has the private key

A user certificate that has the public key only

**Answer Area**

Trusted Root Certification Authorities certificate store on each laptop:


A root CA certificate that has the public key only

The users' Personal store on each laptop:

A user certificate that has the private key

The Azure VPN gateway:

A user certificate that has the public key only

 **MaxBlanche** Highly Voted 4 years, 7 months ago


The last answer is wrong, the VPN Gateway should have the Root certificate with the public key installed (<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-point-to-site-rm-ps#upload>).

upvoted 135 times

 **Ario** 3 years, 9 months ago

agree last one should be same as first one

upvoted 5 times

 **Rayrichi** 4 years, 6 months ago

agree. Last answer is Root certificate with the public key

upvoted 11 times

 **Mj11Az** 4 years ago

But each cert can be used once so it cant be ROOT public 2 times?



upvoted 2 times

 **Amit3** 4 years ago

The ques say you can use each certificate more than once.

upvoted 1 times



  **FinMessner** 3 years, 5 months ago

READ THE QUESTION! I'm so sick of people commenting that just add confusion by not reading the question. If you can't read then you don't need to be testing for Azure Architect.

upvoted 18 times

  **kilowd** 3 years ago

As much as he is wrong there is no need for you to be so harsh on him..everyone makes mistakes, u can also be wrong sometimes so chill and be polite plz

upvoted 5 times


  **gp777**  4 years, 5 months ago

Root public

User Private

Root Public

upvoted 71 times

  **AD3** 3 years, 4 months ago

For point-to-site connection using VPN. The user's public key is provided to the remote which is the gateway. User keeps it's private key with him/her on his/her laptop.

upvoted 1 times

  **heero**  2 years, 9 months ago


The last answer is wrong, the VPN Gateway should have the Root certificate with the public key

upvoted 2 times

  **senseibrutal** 2 years, 11 months ago

correcto

upvoted 1 times

  **Snownoodles** 3 years, 2 months ago

The third answer should be root certificate(public key), this is why:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about>

"The validation of the client certificate is performed by the VPN gateway and happens during establishment of the P2S VPN connection"

When establish P2S VPN, only client certificate verification is required, client certificate is signed by root private key, so root public key is required on VPN gateway to validate client certificate.

upvoted 3 times

  **teyol51117** 3 years, 3 months ago

This was in an exam today.

upvoted 2 times

  **itenginerd** 3 years, 3 months ago

I've deployed this in production:

Root cert (public key only) goes to the user systems in Trusted Root.

User cert (must have private key) goes to the user systems in Personal.

Root cert (public key only) goes to Azure as described in the how-to docs.

upvoted 3 times



  **plmmmsg** 3 years, 3 months ago

- Root CA with public key

- User Certificate with private key

- Root CA with public key

upvoted 1 times

  **anto64** 3 years, 5 months ago

BOX1: root CA private

BOX2: user private

BOX3: root CA public

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-certificates-point-to-site#clientcert>

<https://www.youtube.com/watch?v=Ur0WNjnXJrU>

upvoted 1 times

  **AD3** 3 years, 4 months ago

BOX3 is User's public key. If you don't give your public key to the remote which is VPN gateway, your private key encryption when reaches the gateway can't be unencrypted. Understand it's key-pair which gives you ability to communicate securely with the other party. As a user you keep

your private key and give your public key to others with whom you want to communicate.

upvoted 2 times

🗨️ 👤 **AD3** 3 years, 4 months ago

Basically the answer given by the moderator is correct.

upvoted 1 times

🗨️ 👤 **AD3** 3 years, 4 months ago

Why would root CA give up their private key to others? Assume you are the CA authority and have your private key. Would you give your private key or your public key to others?

upvoted 2 times

🗨️ 👤 **itenginerd** 3 years, 3 months ago

From your doc link: After creating a self-signed root certificate, export the root certificate public key .cer file (not the private key). You will later upload this file to Azure.

Box 2 and 3 are correct. Box 1 is root public, tho.

The root CA private key is the most private/important piece of the certificate identity chain. You would never ever upload it for any purpose like this--that's like pasting your password into chat.

upvoted 1 times

🗨️ 👤 **tinchohd** 3 years, 6 months ago

in the Q#3 VPN Gateway - when you configure the azure VPN gateway certificate asked you to upload the root Certificate... end of discussion, and of course is public. Q1 and Q2 are correct

upvoted 1 times

🗨️ 👤 **ivanmung** 3 years, 6 months ago

Root public

User Private

User Public cert to decrypt user's ssl vpn that encrypted by user's private cert

upvoted 5 times

🗨️ 👤 **pruntelnetworks** 3 years, 5 months ago

public cert is used to encrypt, private is used to decrypt. Not other way around.

upvoted 2 times

🗨️ 👤 **Gtese** 3 years, 8 months ago

answer is corrcet.

third box, vpn gateway get and store a certificate(public key)(web host) from trust CA.

never share private key with the others ,keep it security!

upvoted 2 times

🗨️ 👤 **syu31svc** 3 years, 9 months ago

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal#uploadfile>

upload public root certificate data to Azure

1st and 3rd drop downs are the same; root certificate with public key

2nd drop down is user with private key based on the term "Personal" (just my own reasoning for this one)

upvoted 3 times

🗨️ 👤 **poplovic** 3 years, 9 months ago

This is a typical two-way auth process.

On the client laptop

1. To verify the Gateway (server), you need a public Root cert (cert chain to gateway's leaf cert) in the trust cert store.

2. To prove your own identity, you need a user cert with private key in MY cert store.

The gateway needs to verify client's public cert, therefore a Root cert (cert chain to client's leaf cert) is needed.

The correct answer

Root public (chain to gateway's leaf cert)

User private

Root public (chain to client's leaf cert)

upvoted 5 times

🗉 👤 **souvik123** 3 years, 9 months ago

- Root CA with public key
- User Certificate with private key
- Root CA with public key

upvoted 5 times

🗉 👤 **Gautam1985** 3 years, 10 months ago

VPN --> Root Certificate with public key. Rest two question answer is correct

upvoted 2 times

🗉 👤 **souvik123** 3 years, 10 months ago

- Root CA with public key
- User Certificate with private key
- Root CA with public key

upvoted 1 times

## HOTSPOT -

You are building an application that will run in a virtual machine (VM). The application will use Azure Managed Identity. The application uses Azure Key Vault, Azure SQL Database, and Azure Cosmos DB.

You need to ensure the application can use secure credentials to access these services.

Which authorization method should you recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Functionality	Authorization method
Azure Key Vault	<div> <div></div> <div> Hash-based message authentication code (HMAC)  Azure Managed Identity  Role-Based Access Controls (RBAC)  HTTPS encryption </div> </div>
Azure SQL	<div> <div></div> <div> Hash-based message authentication code (HMAC)  Azure Managed Identity  Role-Based Access Controls (RBAC)  HTTPS encryption </div> </div>
Cosmos DB	<div> <div></div> <div> Hash-based message authentication code (HMAC)  Azure Managed Identity  Role-Based Access Controls (RBAC)  HTTPS encryption </div> </div>


### Answer Area

Functionality	Authorization method
Azure Key Vault	<div> <div></div> <div> Hash-based message authentication code (HMAC)  <b>Azure Managed Identity</b>  Role-Based Access Controls (RBAC)  HTTPS encryption </div> </div>
Azure SQL	<div> <div></div> <div> Hash-based message authentication code (HMAC)  <b>Azure Managed Identity</b>  Role-Based Access Controls (RBAC)  HTTPS encryption </div> </div>
Cosmos DB	<div> <div></div> <div> Hash-based message authentication code (HMAC)  <b>Azure Managed Identity</b>  Role-Based Access Controls (RBAC)  HTTPS encryption </div> </div>

Note: Managed identities for Azure resources is the new name for the service formerly known as Managed Service Identity (MSI).

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>

 **EgorAivazov** Highly Voted 4 years, 5 months ago

I don't get it. In the question's body, it's written: "Which AUTHENTICATION method should you recommend?". However, in the image of the answer area, it's clearly mentioned that the AUTHORIZATION method should be selected...

In case if you need to select the AUTHENTICATION types, then the answer should be

1. AMI

2. AMI

3. AMI

In case if you need to select the AUTHORIZATION type, then the answer should be



1. RBAC

2. RBAC

3. HMAC

So, which one is correct? Your comments are welcome!

upvoted 95 times

  **Aghora** 4 years, 4 months ago



In case if you need to select the AUTHORIZATION type, then the answer should be

1. RBAC

2. RBAC



3. HMAC ----- Also RBAC works

upvoted 7 times

  **soren** 4 years, 1 month ago

The mods changed the question text from authentication to authorization to match the graphic. RBAC, RBAC, HMAC seems right in this case.

upvoted 3 times

  **dmlists** 3 years, 8 months ago

now that data plane RBAC is available for Cosmos DB, I believe 3 should be also RBAC: <https://docs.microsoft.com/en-us/azure/cosmos-db/managed-identity-based-authentication>

upvoted 5 times

  **megapokerbum** 3 years, 4 months ago

I think the bottom one per, <https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>

What Azure services support the feature?

Managed identities for Azure resources can be used to authenticate to services that support Azure AD authentication. For a list of supported Azure services, see [services that support managed identities for Azure resources](#).

Which operations can I perform using managed identities?

Resources that support system assigned managed identities allow you to:

Enable or disable managed identities at the resource level.

Use role-based access control (RBAC) to grant permissions.

View the create, read, update, and delete (CRUD) operations in Azure Activity logs.

View sign in activity in Azure AD sign in logs.

MI for authentication

RBAC for authorization (grant permissions)

upvoted 2 times

  **Reza666**  4 years, 6 months ago

This is a tricky question. It asks the authentication methods which is AMI for all three boxes but there is a similar question in az-301 which asked about authorisation methods which in that case RBAC, RBAC, HMAC are the correct answers.

upvoted 41 times

  **KhabibcandefeatGSP** 4 years, 1 month ago

For those wondering why use HMAC and not RBAC for CosmosDB even though RBAC is available for CosmosDB - Azure RBAC support in Azure Cosmos DB applies to control plane operations only. Data plane operations are secured using primary keys or resource tokens which uses HMAC.

So the right answers are:-

1. RBAC

2. RBAC

3. HMAC

upvoted 7 times

  **gssd4scoder** 4 years, 1 month ago

Not agree, RBAC is supported also for data plane operations: <https://docs.microsoft.com/en-us/azure/cosmos-db/how-to-setup-rbac>  
upvoted 6 times

  **norbitek** 4 years ago

That's why for me for AUTHORIZATION it should be 3 x RBAC  
upvoted 4 times

  **alexshang** Most Recent 2 years, 12 months ago

CosmosDB support RBAC on Data Plane as well.

Azure Cosmos DB exposes a built-in role-based access control (RBAC) system that lets you:

Authenticate your data requests with an Azure Active Directory (Azure AD) identity.

Authorize your data requests with a fine-grained, role-based permission model.

RBAC for all

upvoted 2 times

  **Chamfdoo** 3 years ago

Question is asking "Which authorization method should you recommend?"

So Authentication Method is : AMI

So as per the question answer should be : RBAC, RBAC and HMAC

upvoted 2 times

  **FireOzzie** 3 years, 3 months ago

Agree with the answers

upvoted 1 times

  **plmmsg** 3 years, 3 months ago

RBAC, RBAC, HMAC are the correct answers.

upvoted 1 times

  **plmmsg** 3 years, 3 months ago

1. AMI

2. AMI

3. AMI

upvoted 1 times

  **AD3** 3 years, 3 months ago

Basics of Authorization: <https://docs.microsoft.com/en-us/azure/architecture/framework/security/design-identity-authorization>

Authorization is a process that grants or denies access to a system by verifying whether the accessor has the permissions to perform the requested action. The accessor in this context is the workload (cloud application) or the user of the workload. The action might be operational or related to resource management. There are two main approaches to authorization: role-based and resource-based. Both can be configured with Azure AD.

So Azure clearly says Authorization is RBAC.

Step 1: Authentication probably using MI

Step 2: Ok you are authenticated who you are but I still want to see if you are authorized to use it for the requested operation. RBAC.

upvoted 1 times

  **FinMessner** 3 years, 5 months ago

<https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal?tabs=current>

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

upvoted 1 times

  **ixl2pass** 3 years, 5 months ago

AMI for all.

Cosmos DB (Refer "Access Data" section in <https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-vm-managed-identities-cosmos?tabs=azure-portal>)

SQL (Refer "Enable Managed Identity on App" in <https://docs.microsoft.com/en-us/azure/app-service/tutorial-connect-msi-sql-database?tabs=windowsclient%2Cdotnet>)

upvoted 1 times

🗨️ 👤 **Xia\_Li** 3 years, 5 months ago

I think answer given is correct  
upvoted 2 times

🗨️ 👤 **ParthiBas** 3 years, 6 months ago

The answer given is correct AMI for all  
upvoted 1 times

🗨️ 👤 **aromanrod** 3 years, 6 months ago

You need to ensure the application can use secure credentials to access these services.

Answer given is correct AMI for all  
upvoted 2 times

🗨️ 👤 **chichi0307** 3 years, 8 months ago

i think AMI\*3  
reason "secure credentials to access these services"  
upvoted 3 times

🗨️ 👤 **syu31svc** 3 years, 9 months ago

<https://docs.microsoft.com/en-us/azure/cosmos-db/database-security?tabs=sql-api#how-does-azure-cosmos-db-secure-my-database>

Azure Cosmos DB uses hash-based message authentication code (HMAC) for authorization.

Third Drop down is HMAC

Key Vault and Azure SQL would be RBAC for sure  
upvoted 3 times

🗨️ 👤 **poplovic** 3 years, 9 months ago

The fact "The application will use Azure Managed Identity"  
The question "which AuthZ method should you recommend"  
The answers are all "RBAC"

for Key vault: both management plane and data plane support RBAC now.

<https://docs.microsoft.com/en-us/azure/key-vault/general/rbac-guide?tabs=azure-cli>

for Azure SQL: you can set RBAC at the SQL server

for Cosmos DB: <https://docs.microsoft.com/en-us/azure/cosmos-db/secure-access-to-data?tabs=using-primary-key#rbac>

upvoted 1 times

🗨️ 👤 **Dhelaila** 3 years, 9 months ago

Answer is correct.

As the application will already use Azure Managed Identity, you don't need other methodes.

upvoted 5 times

🗨️ 👤 **aabdous** 3 years, 8 months ago

Don't confuse authorization and authentication.

Authorisation is RBAC or HMAC

Authentication is managed identity or AD account

upvoted 1 times

You have an Azure subscription that contains a custom application named Application1. Application1 was developed by an external company named Fabrikam, Ltd. Developers at Fabrikam were assigned role-based access control (RBAC) permissions to the Application1 components. All users are licensed for the Microsoft 365 E5 plan.

You need to recommend a solution to verify whether the Fabrikam developers still require permissions to Application1. The solution must meet the following requirements:

- ⇒ To the manager of the developers, send a monthly email message that lists the access permissions to Application1.
- ⇒ If the manager does not verify an access permission, automatically revoke that permission.
- ⇒ Minimize development effort.

What should you recommend?

- A. Create an Azure Automation runbook that runs the Get-AzureADUserAppRoleAssignment cmdlet.
- B. Create an Azure Automation runbook that runs the Get-AzRoleAssignment cmdlet.
- C. In Azure Active Directory (Azure AD), create an access review of Application1.
- D. In Azure Active Directory (AD) Privileged Identity Management, create a custom role assignment for the Application1 resources.

**Suggested Answer: C**

Community vote distribution

C (100%)

🗳️ 👤 **Tombarc** Highly Voted 4 years, 10 months ago

The correct answer is C. The answer D leads you to believe it's correct as the access view and assignment are created using Privileged Access Management (PIM), but in the last part, it mentions role assignment, which doesn't make any sense.  
upvoted 44 times

🗳️ 👤 **Alexevansigg** Highly Voted 4 years, 8 months ago

Correct. Heres the Documentation on Access reviews:  
<https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-user-access-with-access-reviews>  
upvoted 16 times

🗳️ 👤 **ReginaldoBarreto** 4 years, 2 months ago

This link have a excellent documentation. tks  
upvoted 4 times

🗳️ 👤 **plmmsg** Most Recent 3 years, 3 months ago

**Selected Answer: C**

C. In Azure Active Directory (Azure AD), create an access review of Application1.  
upvoted 1 times

🗳️ 👤 **us3r** 3 years, 5 months ago

**Selected Answer: C**

access review  
upvoted 1 times

🗳️ 👤 **NebulousNeo** 3 years, 6 months ago

**Selected Answer: C**

Correct Answer  
upvoted 2 times

🗳️ 👤 **leo\_az300** 3 years, 8 months ago

Office 365 E5 in question gave hint that users have Azure AD premium P2 license. Office 365 subscriptions include the Free edition, but Office 365 E1, E3, E5, F1 and F3 subscriptions also include the features listed under the Office 365 apps column.

With P2 license, you can set up Access Review, C is correct  
upvoted 3 times



🗳️ 👤 **syu31svc** 3 years, 9 months ago

<https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview>

Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. User's access can be reviewed on a regular basis to make sure only the right people have continued access.

Have reviews recur periodically: You can set up recurring access reviews of users at set frequencies such as weekly, monthly, quarterly or annually, and the reviewers will be notified at the start of each review. Reviewers can approve or deny access with a friendly interface and with the help of smart recommendations.

Answer is C

upvoted 2 times

🗳️ 👤 **tvS2021** 3 years, 11 months ago

this question is appeared in my exam today. i cleared 304 exam.

upvoted 6 times

🗳️ 👤 **Rume** 4 years ago

came in exam today 6 June... selected "C - Access Review"

upvoted 7 times

🗳️ 👤 **demonite** 4 years, 1 month ago

For anyone wondering how the changes are auto applied <https://docs.microsoft.com/en-us/azure/active-directory/governance/complete-access-review#apply-the-changes>

upvoted 2 times

🗳️ 👤 **neil1985\_jy** 4 years, 3 months ago

Clarification - "With Azure Active Directory (Azure AD), you can easily ensure that users have appropriate access. You can ask the users themselves or a decision maker to participate in an access review and recertify (or attest) to users' access. The reviewers can give their input on each user's need for continued access based on suggestions from Azure AD. When an access review is finished, you can then make changes and remove access from users who no longer need it"

upvoted 1 times

🗳️ 👤 **Jinder** 4 years, 4 months ago

In today's exam.

upvoted 2 times

🗳️ 👤 **suryareddy** 4 years, 4 months ago

Jinder, what did you answer :-). Pl share

upvoted 2 times

🗳️ 👤 **PravinDhote** 4 years, 3 months ago

Whatever he answered, no one can cross validate whether its correct or wrong

;D

upvoted 5 times

🗳️ 👤 **timurlan** 4 years, 1 month ago

He wants to know which answer is incorrect )

upvoted 1 times

🗳️ 👤 **FK2974** 4 years, 4 months ago

Yes C is correct!!

upvoted 3 times

🗳️ 👤 **glam** 4 years, 5 months ago

C. In Azure Active Directory (Azure AD), create an access review of Application1.

upvoted 3 times

🗳️ 👤 **milind8451** 4 years, 5 months ago



Right ans

upvoted 2 times

🗳️ 👤 **Blaaa** 4 years, 5 months ago

Correct answers

upvoted 3 times

  **bbartek** 4 years, 5 months ago

At first I was thinking it's a tricky one, because of the specified license, but according to MS Identity Governance is supported in this scenario:

Enterprise Mobility + Security E5/A5, Microsoft 365 E5/A5, Microsoft 365 E5/A5 Security, and Azure Active Directory Premium Plan 2 provide the rights for a user to benefit from Azure Active Directory Identity Governance.

So answer C is correct.

upvoted 2 times

## DRAG DROP -

A company named Contoso, Ltd. has an Azure Active Directory (Azure AD) tenant that uses the Basic license.

You plan to deploy two applications to Azure. The applications have the requirements shown in the following table.

Application name	Requirement
Customer	Users must authenticate by using a personal Microsoft account and multi-factor authentication
Reporting	Users must authenticate by using either Contoso credentials or a personal Microsoft account. You must be able to manage the accounts from Azure AD.

Which authentication strategy should you recommend for each application? To answer, drag the appropriate authentication strategies to the correct applications.

Each authentication strategy may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

## Authentication Strategies

An Azure AD B2C tenant

An Azure AD v1.0 endpoint

An Azure AD v2.0 endpoint

## Answer Area

Customer: Authentication strategy

Reporting: Authentication strategy

## Suggested Answer:

## Authentication Strategies

An Azure AD B2C tenant

An Azure AD v1.0 endpoint

An Azure AD v2.0 endpoint

## Answer Area

Customer: An Azure AD v2.0 endpoint

Reporting: An Azure AD B2C tenant

## Box 1: Azure AD V2.0 endpoint -

Microsoft identity platform is an evolution of the Azure Active Directory (Azure AD) developer platform. It allows developers to build applications that sign in all

Microsoft identities and get tokens to call Microsoft APIs, such as Microsoft Graph, or APIs that developers have built. The Microsoft identity platform consists of:

OAuth 2.0 and OpenID Connect standard-compliant authentication service that enables developers to authenticate any Microsoft identity, including:

Work or school accounts (provisioned through Azure AD)

Personal Microsoft accounts (such as Skype, Xbox, and Outlook.com)

Social or local accounts (via Azure AD B2C)

## Box 2: Azure AD B2C tenant -

Azure Active Directory B2C provides business-to-customer identity as a service. Your customers use their preferred social, enterprise, or local account identities to get single sign-on access to your applications and APIs.

Azure Active Directory B2C (Azure AD B2C) integrates directly with Azure Multi-Factor Authentication so that you can add a second layer of security to sign-up and sign-in experiences in your applications.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory-b2c/active-directory-b2c-reference-mfa> <https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-overview>

I believe the answers are the other way around:

Box 1: B2C

Box 2: V2 endpoint

upvoted 163 times

  **Pinkee888** 3 years, 2 months ago

Agree Customers - Business to Customers \ Reporting contoso credential and Microsoft account so should be v2.0

upvoted 2 times

  **sanketshah** 4 years, 5 months ago

B2C

V2 Endpoint

upvoted 4 times

  **Wis10** 4 years ago

Correct. B2C intended to customer-facing apps, V2 you can manage the accounts from Azure AD

upvoted 4 times

  **KhabibcandefeatGSP** 4 years, 1 month ago

Both should be Azure AD v2.0 which is actually MS Identity platform v2.0. Azure AD 1.0 didn't support personal account logins but V2.0 does.

Question says "Each authentication strategy may be more than once". So in my view "Azure AD v2.0" can be used for both.

Evidence - Check out the diagram in this link - <https://docs.microsoft.com/en-us/azure/active-directory/azuread-dev/about-microsoft-identity-platform#microsoft-identity-platform-experience>

upvoted 3 times

  **pentium75** 3 years, 10 months ago

They have Azure AD Basic (!) tenant. Basic doesn't support MFA (except for O365 apps). Customers are supposed to use MFA, thus they need B2C tenant for that.

Azure AD 2.0 endpoint would work if they had P1 license.

upvoted 5 times

  **aspirin**  4 years, 1 month ago

1/3 answers on examtopics.com have a false answer - this is one of the false. The learn effect sucks if people can only pay to correct the answers but no one change it in the frontend. When you don't know anything, why must people pay for that?

upvoted 70 times

  **AubinBakana**  2 years, 10 months ago

The confusion here stems from the fact that first App is called Customer & the Other Reporting. If you read carefully you will understand that both apps are customer facing app.

Customer App: AAD v2

Reporting App: B2C Tenant

Answer is correct.

upvoted 3 times

  **vijeet** 3 years ago

Azure AD B2C is a separate service from Azure Active Directory (Azure AD). It is built on the same technology as Azure AD but for a different purpose. It allows businesses to build customer facing applications, and then allow anyone to sign up into those applications with no restrictions on user account.

Reporting: "Must be able to manage account from Azure AD" thus V2 is correct

Customer: B2C supports MFA from personal account

V1 is not recommended

upvoted 1 times

  **Kent\_020** 3 years, 2 months ago

The answer is correct.

#1 Azure AD – identity as a service provider for organization users, providing and controlling access to cloud resources

#2 Azure AD B2B – a feature in Azure AD which allows cross-organization collaboration through authentication

#3 Azure AD B2C – an independent service for building consumer application identity repository

upvoted 1 times

  **cloudera** 3 years, 3 months ago

B2C (for Customer access) and ADV2 for Reporting access.

upvoted 2 times

🗨️ 👤 **plmmmsg** 3 years, 3 months ago

Box 1: B2C

Box 2: V2 endpoint

upvoted 1 times

🗨️ 👤 **arun** 3 years, 3 months ago

<https://docs.microsoft.com/en-us/azure/active-directory-b2c/multi-factor-authentication?pivots=b2c-user-flow> - for customer to access using personal account with MFA, so B2C

<https://joonasw.net/view/azure-ad-v2-and-msal-from-dev-pov> - for Report users to access using either organization or personal account with MFA, so AAD V2 endpoint.

upvoted 1 times

🗨️ 👤 **zeeek** 3 years, 3 months ago

box 1 B2C because the personal account only and no AD credentials

Box 2 V2 endpoint, recommended for new projects

upvoted 2 times

🗨️ 👤 **smonkey** 3 years, 5 months ago

MFA-b2c

<https://docs.microsoft.com/en-us/azure/active-directory-b2c/multi-factor-authentication?pivots=b2c-user-flow>

upvoted 1 times

🗨️ 👤 **17Master** 3 years, 4 months ago

in your link it says:

Azure Active Directory B2C (Azure AD B2C) integrates directly with Azure AD Multi-Factor Authentication.

then you need a P1 license. does not apply with the Azure request. Both must be Azure AD v2.0

upvoted 1 times

🗨️ 👤 **BayleafSoftware** 1 year, 8 months ago

No you dont, with Basic you can still have MFA if you enable system defaults, which will apply MFA to ALL.

you only need the P1 to be able to pick and chose who has MFA

upvoted 1 times

🗨️ 👤 **leo\_az300** 3 years, 8 months ago

Azure AD B2C and Azure AD 2.0

Azure AD B2C is a separate service from Azure Active Directory (Azure AD). It is built on the same technology as Azure AD but for a different purpose. So it can NOT be used to Reporting Application which required for managing azzount from Azure AD.

As ther Azure AD is using basic license which does NOT support MFA, only Azure AD B2C meets Customer application requirement.

upvoted 3 times

🗨️ 👤 **syu31svc** 3 years, 9 months ago

Answers are reversed

<https://docs.microsoft.com/en-us/azure/active-directory-b2c/overview>

Your customers use their preferred social, enterprise, or local account identities to get single sign-on access to your applications and APIs

<https://docs.microsoft.com/en-us/azure/active-directory-b2c/multi-factor-authentication?pivots=b2c-user-flow>

Azure Active Directory B2C (Azure AD B2C) integrates directly with Azure AD Multi-Factor Authentication so that you can add a second layer of security to sign-up and sign-in experiences in your applications

<https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-overview>

OAuth 2.0 and OpenID Connect standard-compliant authentication service enabling developers to authenticate several identity types, including: Work or school accounts, provisioned through Azure AD

Personal Microsoft account, like Skype, Xbox, and Outlook.com

Social or local accounts, by using Azure AD B2C

upvoted 4 times

🗨️ 👤 **Dhelaila** 3 years, 9 months ago

Given answer is correct.

Customer = V2 endpoint (Only need a personal MS account)

Reporting = B2C (Contoso or personal MS account)

See also: <https://docs.microsoft.com/en-us/azure/active-directory-b2c/overview>

upvoted 5 times

🗨️ 👤 **Venkatmr** 3 years, 9 months ago

The answer provided here is correct

<https://docs.microsoft.com/en-us/azure/active-directory-b2c/overview>

upvoted 1 times

🗨️ 👤 **Kowser** 3 years, 10 months ago

answer would be box 1 B2C AND Box 2 :- v2 endpoint

<https://docs.microsoft.com/en-us/azure/active-directory-b2c/multi-factor-authentication?pivots=b2c-user-flow>

upvoted 2 times

🗨️ 👤 **souvik123** 3 years, 10 months ago

Box 1: B2C

Box 2: V2 endpoint

upvoted 2 times

🗨️ 👤 **PerfumoPeru** 3 years, 10 months ago

This is the right one...: Reporting App has azure AD Tenant, so it should be managed by an Azure AD V2 endpoint, because Azure AD B2C is flawed on Authorization, it doesn't have RBAC but it has policy claims which is not enough for Contoso.

Customer, definitely is a Azure B2C management for sure.

upvoted 1 times

## HOTSPOT -

You manage a network that includes an on-premises Active Directory domain and an Azure Active Directory (Azure AD).

Employees are required to use different accounts when using on-premises or cloud resources. You must recommend a solution that lets employees sign in to all company resources by using a single account. The solution must implement an identity provider.

You need to provide guidance on the different identity providers.

How should you describe each identity provider? To answer, select the appropriate description from each list in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

## Answer Area

Identity Provider	Description
synchronized identity	<div> <div></div> <div> User management occurs on-premises. Azure AD authenticates employees by using on-premises passwords. User management occurs on-premises. The on-premises domain controller authenticates employee credentials. Both user management and authentication occur in Azure AD. </div> </div>
federated identity	<div> <div></div> <div> User management occurs on-premises. Azure AD authenticates employees by using on-premises passwords. User management occurs on-premises. The on-premises domain controller authenticates employee credentials. Both user management and authentication occur in Azure AD. </div> </div>

## Suggested Answer:

## Answer Area

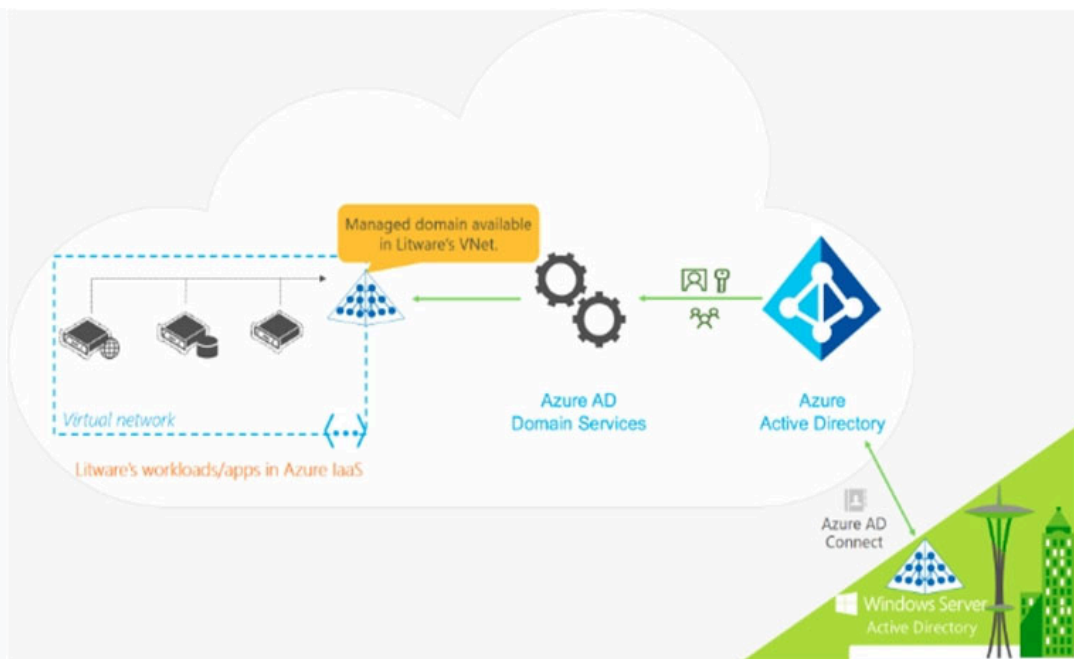
Identity Provider	Description
synchronized identity	<div> <div></div> <div> User management occurs on-premises. Azure AD authenticates employees by using on-premises passwords. User management occurs on-premises. The on-premises domain controller authenticates employee credentials. Both user management and authentication occur in Azure AD. </div> </div>
federated identity	<div> <div></div> <div> User management occurs on-premises. Azure AD authenticates employees by using on-premises passwords. User management occurs on-premises. The on-premises domain controller authenticates employee credentials. Both user management and authentication occur in Azure AD. </div> </div>

Box1: User management occurs on-premises. Azure AD authenticates employees by using on-premises passwords.

Azure AD Domain Services for hybrid organizations

Organizations with a hybrid IT infrastructure consume a mix of cloud resources and on-premises resources. Such organizations synchronize identity information from their on-premises directory to their Azure AD tenant. As hybrid organizations look to migrate more of their on-premises applications to the cloud, especially legacy directory-aware applications, Azure AD Domain Services can be useful to them.

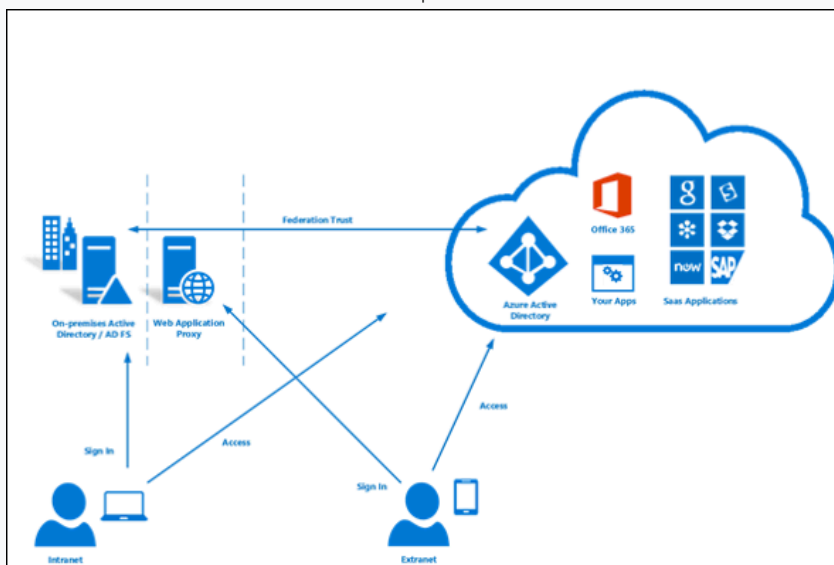
Example: Litware Corporation has deployed Azure AD Connect, to synchronize identity information from their on-premises directory to their Azure AD tenant. The identity information that is synchronized includes user accounts, their credential hashes for authentication (password hash sync) and group memberships.



User accounts, group memberships, and credentials from Litware's on-premises directory are synchronized to Azure AD via Azure AD Connect. These user accounts, group memberships, and credentials are automatically available within the managed domain.

Box 2: User management occurs on-premises. The on-premises domain controller authenticates employee credentials.

You can federate your on-premises environment with Azure AD and use this federation for authentication and authorization. This sign-in method ensures that all user authentication occurs on-premises.



Reference:

<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-overview> <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed>

**mmmore** Highly Voted 4 years, 6 months ago  
Correct  
upvoted 49 times

**milind8451** Highly Voted 4 years, 5 months ago  
Right ans.

Sync identity denotes Pass thru authentication or Pass hash sync. Federated identity denotes ADFS and in ADFS, authentication happens at on-prem DCs.  
upvoted 14 times

**pingpongset** Most Recent 2 years, 10 months ago  
Does anyone understand this part? It said "Employees are required to use different accounts. ", But "you must recommend a solution that lets employees sign in to all company resources by using a single account." This is confusing.



"Employees are required to use different accounts when using on-premises or cloud resources. You must recommend a solution that lets employees sign in to all company resources by using a single account. "

upvoted 1 times

🗳️ 👤 **OCHT** 3 years, 1 month ago

We can figure out given that following 4 points are hiccups of AZ AD domain service :-

- 1.This is a stand-alone managed domain. It is not an extension of Litware's on-premises domain.
- 2.Litware's IT administrator does not need to manage, patch or monitor this domain or any domain controllers for this managed domain.
- 3.There is no need to manage AD replication to this domain. User accounts, group memberships and credentials from Litware's on-premises directory are synchronized to Azure AD via Azure AD Connect. These are automatically available within this managed domain.
4. Since the domain is managed by Azure AD Domain Services, Litware's IT administrator does not have Domain Administrator or Enterprise Administrator privileges on this domain.

Aware what kind of on-premise tasks there. Thence , answers are correct.

upvoted 1 times

🗳️ 👤 **plmmsg** 3 years, 3 months ago

answer is correct

upvoted 1 times

🗳️ 👤 **syu31svc** 3 years, 9 months ago

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-hybrid-identity-design-considerations-identity-adoption-strategy#:~:text=Synchronized%3A%20these%20are%20identities%20that,is%20called%20a%20password%20hash.>

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/media/plan-hybrid-identity-design-considerations/integration-scenarios.png>

Synchronized: these are identities that exist on-premises and in the cloud. Using Azure AD Connect, these users are either created or joined with existing Azure AD accounts. The user's password hash is synchronized from the on-premises environment to the cloud in what is called a password hash. When using synchronized the one caveat is that if a user is disabled in the on-premises environment, it can take up to three hours for that account status to show up in Azure AD. This is due to the synchronization time interval.

Federated: these identities exist both on-premises and in the cloud. Using Azure AD Connect, these users are either created or joined with existing Azure AD accounts.

Answer is correct

upvoted 4 times

🗳️ 👤 **Gautam1985** 3 years, 10 months ago

correct as provided

upvoted 1 times

🗳️ 👤 **glam** 4 years, 5 months ago

Box1: User management occurs on-premises. Azure AD authenticates employees by using on-premises passwords.

Box 2: User management occurs on-premises. The on-premises domain controller authenticates employee credentials.

upvoted 4 times

🗳️ 👤 **[Removed]** 4 years, 5 months ago

for Sych , Pass through authentication as well the authentication will be done in on premises AD...hence the authentication is done via on premises domain controller? bit confised about the answer here

upvoted 1 times

🗳️ 👤 **teehex** 3 years, 10 months ago

The solution is to use Password hash Auth.

upvoted 1 times

🗳️ 👤 **sanketshah** 4 years, 5 months ago

given answer is correct.

upvoted 2 times

## HOTSPOT -

You configure the Diagnostics settings for an Azure SQL database as shown in the following exhibit.

## Diagnostics setting

Save Discard Delete Provide feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic setting name

Diagnostic1

Category details

log

- ☒ SQLInsights
- ☒ AutomaticTuning
- ☒ QueryStoreRuntimeStatistics
- ☒ QueryStoreWaitStatistics
- ☒ Errors
- ☒ DatabaseWaitStatistics
- ☒ Timeouts
- ☒ Blocks
- ☒ Deadlocks

Destination details

☒ Send to Log Analytics

Subscription

Azure Pass - Sponsorship

Log Analytics workspace

sk200814 ( eastus )

☐ Archive to a storage account

☐ Stream to an event hub

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

To perform real-time reporting by using Microsoft Power BI, you must first **[answer choice]**.

- clear Send to Log Analytics
- clear SQLInsights
- select Archive to a storage account
- select Stream to an event hub

Diagnostics data can be reviewed in **[answer choice]**.

- Azure Analysis Services
- Azure Application Insights
- Azure SQL Analytics
- Microsoft SQL Server Analysis Services (SSAS)
- SQL Health Check

**Suggested Answer:**

**Answer Area**

To perform real-time reporting by using Microsoft Power BI, you must first **[answer choice]**.

clear Send to Log Analytics
clear SQL Insights
select Archive to a storage account
select Stream to an event hub

Diagnostics data can be reviewed in **[answer choice]**.

Azure Analysis Services
Azure Application Insights
Azure SQL Analytics
Microsoft SQL Server Analysis Services (SSAS)
SQL Health Check

  **dkltruong88** Highly Voted 3 years, 9 months ago

Was in exam today 1-10-2021. I passed with score 896. I chose the same provided answer  
upvoted 15 times

  **arslanshah86** 3 years, 8 months ago



Hello Dear, What would you say about the percentage of questions that came from these dump?  
upvoted 2 times

  **pruntelnetworks** 3 years, 5 months ago



in az-303 my pct was about 20-40%  
upvoted 1 times

  **pruntelnetworks** 3 years, 5 months ago

of course I did not see all 200+ questions on this dump. I saw about 80 questions.  
upvoted 1 times

  **xyz213** 3 years, 5 months ago

in my az303 2 weeks ago 85% of the dump  
upvoted 3 times

  **laili** 3 years, 5 months ago

This is not az304  
upvoted 3 times

  **hoangton** Highly Voted 3 years, 11 months ago

Answer is correct

Because: Diagnostics settings for an Azure SQL database so box 2 should be Azure SQL Analytics.

upvoted 6 times

  **f2002642** Most Recent 2 years, 10 months ago

Diagnostic logs sent to the Log Analytics workspace can be consumed by SQL Analytics and logs sent to Event hubs can be consumed by Power BI, third-party logging, and telemetry streams.

Hence answer provided is correct.

upvoted 2 times

  **plmmg** 3 years, 3 months ago

Data streamed to a Event hub and consumed by SQL Analytics.

upvoted 1 times

  **syu31svc** 3 years, 9 months ago

<https://docs.microsoft.com/en-us/azure/azure-sql/database/metrics-diagnostic-telemetry-logging-streaming-export-configure?tabs=azure-portal#stream-into-sql-analytics>

View service health by streaming hot-path data to Power BI

By using Event Hubs, Stream Analytics, and Power BI, you can easily transform your metrics and diagnostics data into near real-time insights on your Azure services.

1st drop down is stream to event hub

2nd drop down is SQL Health Check to me because it's diagnostics data we are talking about (just my own reasoning)  
upvoted 4 times

🗨️ **syu31svc** 3 years, 8 months ago

Ignore what I mentioned about the 2nd drop down

SQL Analytics is the answer for the 2nd drop down

Data streamed to a Log Analytics workspace can be consumed by SQL Analytics

<https://docs.microsoft.com/en-us/azure/azure-sql/database/metrics-diagnostic-telemetry-logging-streaming-export-configure?tabs=azure-portal>  
upvoted 7 times

🗨️ **Gautam1985** 3 years, 10 months ago

correct

upvoted 4 times

🗨️ **BenWat** 3 years, 11 months ago

From: <https://docs.microsoft.com/en-us/azure/azure-sql/database/metrics-diagnostic-telemetry-logging-streaming-export-configure>

\*Data streamed to a Log Analytics workspace can be consumed by SQL Analytics.

\*Use Event Hubs, Stream Analytics, and Power BI to transform your diagnostics data into near real-time insights on your Azure services

upvoted 5 times

🗨️ **somenick** 3 years, 12 months ago

Provided answer is correct

upvoted 2 times

🗨️ **BrettusMaximus** 3 years, 11 months ago

Since Azure SQL Analytics is in Preview, second answer needs to be  
- Azure Application Insights.

Azure SQL Analytics (Preview function) is a cloud-based solution that gathers the performance metrics of several Azure database service components such as Azure SQL databases, Azure elastic pooled, and managed instances. You can manage the data collection across multiple subscriptions. It provides a platform to collect, analyze, and visualize the database performance metrics that are helpful for performance troubleshooting and reporting purposes.

upvoted 4 times

🗨️ **examineezer** 3 years, 6 months ago

<https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4pCWz>

"The exam may contain questions on Preview features if those features are commonly used."

upvoted 1 times

🗨️ **bird1982** 3 years, 12 months ago

I think the answer is correct. Anymore suggestion?

upvoted 1 times

🗨️ **Moyuihftg** 3 years, 12 months ago

I guess its:

- select Archive to a storage account

- Azure Application Insights

upvoted 2 times


🗨️ **GetulioJr** 3 years, 11 months ago

If you have no idea. Do not guess.



upvoted 15 times

🗨️ **FinMessner** 3 years, 5 months ago

Exactly, I wish some of you would just keep your opinions to yourself. All you're doing is clogging up the portal and wasting time.  
upvoted 3 times

  **tita\_tovenaar** 3 years, 11 months ago

Requirement is real-time reporting. You're guessing wrong with anything starting with "Archive"  
upvoted 1 times

  **FinMessner** 3 years, 5 months ago

Grr...

upvoted 2 times

You plan to deploy an application named App1 that will run on five Azure virtual machines. Additional virtual machines will be deployed later to run App1.

You need to recommend a solution to meet the following requirements for the virtual machines that will run App1:

- ⇒ Ensure that the virtual machines can authenticate to Azure Active Directory (Azure AD) to gain access to an Azure key vault, Azure Logic Apps instances, and an Azure SQL database.
- ⇒ Avoid assigning new roles and permissions for Azure services when you deploy additional virtual machines.
- ⇒ Avoid storing secrets and certificates on the virtual machines.
- ⇒ Minimize administrative effort for managing identities.

Which type of identity should you include in the recommendation?

- A. a service principal that is configured to use a certificate
- B. a system-assigned managed identity
- C. a service principal that is configured to use a client secret
- D. a user-assigned managed identity

#### Suggested Answer: D

Managed identities for Azure resources is a feature of Azure Active Directory.

User-assigned managed identity can be shared. The same user-assigned managed identity can be associated with more than one Azure resource.

Incorrect Answers:

B: System-assigned managed identity cannot be shared. It can only be associated with a single Azure resource.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>

Community vote distribution

D (100%)

mmore Highly Voted 4 years, 6 months ago

Correct

upvoted 59 times

SnakePlissken Highly Voted 4 years ago

I'm a little confused. All the requirements point to a user-assigned managed identity, but that is not supported by Azure Key Vault. "Key Vault references currently only support system-assigned managed identities. User-assigned identities cannot be used." Everybody is so convinced that the answer is correct, but I think it should be system-assigned, although the question is almost shouting user-assigned.

<https://docs.microsoft.com/en-us/azure/app-service/app-service-key-vault-references#granting-your-app-access-to-key-vault>

<https://www.examtactics.com/discussions/microsoft/view/45744-exam-az-204-topic-3-question-11-discussion/>

<https://docs.microsoft.com/en-us/azure/app-service/app-service-key-vault-references#granting-your-app-access-to-key-vault>

<https://www.examtactics.com/discussions/microsoft/view/45744-exam-az-204-topic-3-question-11-discussion/>

upvoted 8 times

Anilpanda10 4 years ago

good point. Has anyone found an answer to this?

upvoted 2 times

SnakePlissken 4 years ago

Sorry for the double references, I can't edit my comment anymore.

upvoted 1 times

Charles99 4 years ago

maybe there's a mistake in the doco? I've just verified in the portal that i can ref a user assigned managed identity to an access policy

upvoted 3 times

SnakePlissken 4 years ago

Nice work, Charles99! I tried to test it in the sandbox and could create all the resources I needed, except a user-assigned managed identity :\

After your confirmation, I will go for a user-assigned managed identity.

upvoted 1 times

🗨️ **SnakePlissken** 4 years ago

Now I'm really confused! According to this article it's possible to access the Key Vault with a user-assigned managed identity.

<https://thecodeblogger.com/2020/06/13/user-assigned-managed-identity-with-azure-key-vault/>

But on this page, Key Vault is not in the list of managed identities.

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/services-support-managed-identities>

Maybe the support is already built in, but the Microsoft documentation is not updated?

upvoted 2 times

🗨️ **BenWat** 3 years, 11 months ago

Key vault is lower down the page under the AAD section:

The following services support Azure AD authentication, and have been tested with client services that use managed identities for Azure resources.

upvoted 1 times

🗨️ **scottishstvao** 3 years, 9 months ago

Hey bud, you got it on the wrong way.

The answer is User-Assigned, you can do a Lab before comment wrong suppositions. People can follow what you say and put it wrong at the test time.

upvoted 8 times

🗨️ **VijayRaja2000** Most Recent 3 years, 1 month ago

Correct, we need to use user assigned managed identity for Virtual machines to share the same identity for the future virtual machines and use this identity (AAD based authentication) to access all the other resources

upvoted 2 times

🗨️ **hertino** 3 years, 2 months ago

In AZ-305 exam, 9 april 22

upvoted 4 times

🗨️ **cloudera** 3 years, 3 months ago

Selected Answer: D

Seems D is the correct answer based on the following info:

System-assigned managed identities allow you to:

- Enable or disable managed identities at the resource level.
- Use role-based access control (RBAC) to grant permissions.
- View the create, read, update, and delete (CRUD) operations in Azure Activity logs.
- View sign-in activity in Azure AD sign-in logs.

User-assigned managed identities allow you to:

- You can create, read, update, and delete the identities.
- You can use RBAC role assignments to grant permissions.
- User assigned managed identities can be used ON MORE THAN ONE RESOURCE.
- CRUD operations are available for review in Azure Activity logs.
- View sign-in activity in Azure AD sign-in logs.

upvoted 3 times

🗨️ **Dawn7** 3 years, 3 months ago

Selected Answer: D

I would choose D

upvoted 1 times

🗨️ **plmmsg** 3 years, 3 months ago

Selected Answer: D

User-assigned managed identity

upvoted 1 times

🗨️ **arun** 3 years, 3 months ago

Selected Answer: D

refer <https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/how-manage-user-assigned-managed-identities?pivots=identity-mi-methods-azp>

upvoted 1 times

🗨️ 👤 **S\_AB** 3 years, 4 months ago

**Selected Answer: D**

User managed identity, will be for more than 1 VM.

upvoted 1 times

🗨️ 👤 **anupam77** 3 years, 4 months ago

Correct Answer Given [User-assigned managed identity]

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>

User-assigned managed identity:-

"For example, a workload where multiple virtual machines need to access the same resource."

System-assigned managed identity:-

"For example, an application that runs on a single virtual machine"

upvoted 2 times

🗨️ 👤 **chintupawan** 3 years, 4 months ago

Given answer is correct. We can definitely assign user identity to key vault.

Keys points to consider why Managed User Identity is the correct answer.

1. New VM will be added in future

2. Minimize administrative efforts.

Managed User Identity is not tied to a resource life time. It can be assigned to multiple resources.

upvoted 2 times

🗨️ 👤 **Nokaído** 3 years, 5 months ago

Both User assigne and System Assigned Identity will do the job but the System assigned identity is the one without the aministrative hassle. You just click on Systemassigned idenity on the VM side and than go to the KeyVault -> Access Policies and add the VM by searching for its name. For me B should be the right answer.

upvoted 1 times

🗨️ 👤 **Eitant** 3 years, 6 months ago

**Selected Answer: D**

Correct Answer

upvoted 1 times

🗨️ 👤 **oug** 3 years, 7 months ago

Correct!

upvoted 2 times

🗨️ 👤 **strohcj** 3 years, 8 months ago

Just a note...To create a user assigned managed identity, you need MI Contributor role and create the MI in the portal, then you can assign RBAC permissions. The MI will need to be deleted separately when no longer in use. System assigned MI is enabled with the resource is created or after creation under VM - Identity. It is automatically deleted when the VM is deleted. User assigned MI is more secure but in this case, system assigned would save work. My vote is for system assigned.

upvoted 1 times

🗨️ 👤 **syu31svc** 3 years, 9 months ago

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>

Managed identities provide an identity for applications to use when connecting to resources that support Azure Active Directory (Azure AD) authentication

User-assigned You may also create a managed identity as a standalone Azure resource. You can create a user-assigned managed identity and assign it to one or more instances of an Azure service

D is the answer

upvoted 3 times

🗨️ 👤 **cfsxtuv33** 3 years, 8 months ago

Answer is correct. <https://thecodeblogger.com/2020/06/13/user-assigned-managed-identity-with-azure-key-vault/>

upvoted 1 times

🗨️ 👤 **nkV** 3 years, 9 months ago



Came in exam on 20-sep-21, i passed, answer are correct  
upvoted 3 times

You are designing a large Azure environment that will contain many subscriptions.

You plan to use Azure Policy as part of a governance solution.

To which three scopes can you assign Azure Policy definitions? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. management groups
- B. subscriptions
- C. Azure Active Directory (Azure AD) tenants
- D. resource groups
- E. Azure Active Directory (Azure AD) administrative units
- F. compute resources

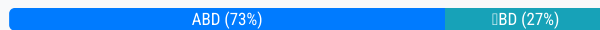
**Suggested Answer:** ABD

Azure Policy evaluates resources in Azure by comparing the properties of those resources to business rules. Once your business rules have been formed, the policy definition or initiative is assigned to any scope of resources that Azure supports, such as management groups, subscriptions, resource groups, or individual resources.

Reference:

<https://docs.microsoft.com/en-us/azure/governance/policy/overview>

Community vote distribution



**David\_986969** Highly Voted 4 years, 9 months ago

Correct answer

upvoted 38 times

**milind8451** Highly Voted 4 years, 5 months ago

A, B, D are correct as these 3 are the top 3 selections for Azure policies but if we could choose 4 then individual resources can also be selected.

upvoted 16 times

**JDA** 4 years, 4 months ago

This is correct. It is rarely advisable to apply policies to an individual resource, but I believe it can be done.

upvoted 4 times

**santafe** Most Recent 2 years, 11 months ago

Selected Answer: ABD

yes correct

yes correct

yes correct

upvoted 3 times

**VijayRaja2000** 3 years ago

Correct

An assignment is a policy definition or initiative that has been assigned to a specific scope. This scope could range from a management group to an individual resource. The term scope refers to all the resources, resource groups, subscriptions, or management groups that the definition is assigned to.

<https://docs.microsoft.com/en-us/azure/governance/policy/overview>

upvoted 1 times

**Teringzooi** 3 years, 2 months ago

Correct answers: A B D

In AZ-305 exam

upvoted 1 times

**hertino** 3 years, 2 months ago

In AZ-305 exam, 9 april 22

upvoted 1 times

🗨️ 👤 **plmmmsg** 3 years, 3 months ago

A, B, D are correct answer

upvoted 1 times

🗨️ 👤 **durel** 3 years, 3 months ago

**Selected Answer: ABD**

is the correct answer

upvoted 1 times

🗨️ 👤 **S\_AB** 3 years, 4 months ago

**Selected Answer: ABD**

Correct.

upvoted 2 times

🗨️ 👤 **moon2351** 3 years, 5 months ago

Answer is ABD ABD

upvoted 3 times

🗨️ 👤 **Xia\_Li** 3 years, 5 months ago

Correct

upvoted 1 times

🗨️ 👤 **MightyG** 3 years, 5 months ago

**Selected Answer: ABD**

It is obvious

upvoted 2 times

🗨️ 👤 **syu31svc** 3 years, 9 months ago

ABD for sure

upvoted 3 times

🗨️ 👤 **Gautam1985** 3 years, 10 months ago

correct

upvoted 2 times

🗨️ 👤 **MaheshS** 4 years ago

Correct answer

upvoted 4 times

🗨️ 👤 **bbcz** 4 years, 2 months ago

On Exam 05/01/2021

upvoted 7 times

🗨️ 👤 **glam** 4 years, 5 months ago

A. management groups

B. subscriptions

D. resource groups

upvoted 5 times

You are designing a microservices architecture that will be hosted in an Azure Kubernetes Service (AKS) cluster. Apps that will consume the microservices will be hosted on Azure virtual machines. The virtual machines and the AKS cluster will reside on the same virtual network.

You need to design a solution to expose the microservices to the consumer apps. The solution must meet the following requirements:

- ⇒ Ingress access to the microservices must be restricted to a single private IP address and protected by using mutual TLS authentication.
- ⇒ The number of incoming microservice calls must be rate-limited.
- ⇒ Costs must be minimized.

What should you include in the solution?

- A. Azure App Gateway with Azure Web Application Firewall (WAF)
- B. Azure API Management Premium tier with virtual network connection
- C. Azure API Management Standard tier with a service endpoint
- D. Azure Front Door with Azure Web Application Firewall (WAF)

#### Suggested Answer: B

One option is to deploy APIM (API Management) inside the cluster VNet.

The AKS cluster and the applications that consume the microservices might reside within the same VNet, hence there is no reason to expose the cluster publicly as all API traffic will remain within the VNet. For these scenarios, you can deploy API Management into the cluster VNet. API Management Premium tier supports VNet deployment.

Reference:

<https://docs.microsoft.com/en-us/azure/api-management/api-management-kubernetes>

Community vote distribution

B (100%)

🗳️ **xAlx** Highly Voted 4 years, 6 months ago

Answer is correct:

<https://docs.microsoft.com/en-us/azure/api-management/api-management-kubernetes#option-2-install-an-ingress-controller>

taking into account TLS support and traffic control

upvoted 40 times

🗳️ **BrettusMaximus** 3 years, 11 months ago

It cannot be either A: or D: as the need for a PRIVATE IP address.

upvoted 5 times

🗳️ **arseyam** Highly Voted 4 years, 6 months ago

Deploying Azure API Management in a virtual network is only available in the Premium and Developer tiers of API Management.

<https://docs.microsoft.com/en-us/azure/api-management/api-management-using-with-vnet>

upvoted 16 times

🗳️ **adolover** 4 years, 4 months ago

Isolated as well.

upvoted 3 times

🗳️ **Teringzooi** Most Recent 3 years, 2 months ago

Selected Answer: B

Correct answer: B

In AZ-305

upvoted 2 times

🗳️ **hertino** 3 years, 2 months ago

In AZ-305 exam, 9 april 22

upvoted 3 times

🗳️ **k14us** 3 years, 3 months ago

A is meeting all the pre-reqs and is cheaper than the APIM premium

upvoted 1 times

🗳️ 👤 **plmmsg** 3 years, 3 months ago

B. Azure API Management Premium tier  
upvoted 1 times

🗳️ 👤 **arun** 3 years, 3 months ago

**Selected Answer: B**

Vnet support is only on Premium version.. refer the comparison mentioned at <https://docs.microsoft.com/en-us/azure/api-management/api-management-features>  
upvoted 1 times

🗳️ 👤 **S\_AB** 3 years, 4 months ago

**Selected Answer: B**

Only premium and developer for API management vnet deployment  
upvoted 1 times

🗳️ 👤 **examineezer** 3 years, 6 months ago

I don't understand why the premium feature of VNET deployment is required here. As far as I can tell the premium tier is only required if APIM is used to manage APIs which are consumed by consumers OUTSIDE of the VNET. But here, everything is inside the same VNET!  
upvoted 1 times

🗳️ 👤 **examineezer** 3 years, 6 months ago

Apologies - in both internal mode and external mode it looks like Premium is required:

<https://docs.microsoft.com/en-us/azure/api-management/api-management-kubernetes#option-2-install-an-ingress-controller>  
upvoted 3 times

🗳️ 👤 **examineezer** 3 years, 6 months ago

Nice table comparing APIM premium to standard here:

<https://docs.microsoft.com/en-us/azure/api-management/api-management-features>  
upvoted 2 times

🗳️ 👤 **Azurefox79** 3 years, 6 months ago

**Selected Answer: B**

VNet connection supported only in Premium and Developer Tiers, not standard  
upvoted 2 times

🗳️ 👤 **cfsxtuv33** 3 years, 8 months ago

The thing I've noticed when reviewing these questions is that whenever one of the answers has "premium" in it, then that's the answer.  
upvoted 7 times

🗳️ 👤 **leo\_az300** 3 years, 8 months ago

It should be API Management with AKS in the same Virtual Network with the Add servers. To control rate limit, you can use access restriction policies in API Management.

The only thing I didn't get is why it's premium not standard?  
upvoted 1 times

🗳️ 👤 **syu31svc** 3 years, 9 months ago

<https://docs.microsoft.com/en-us/azure/api-management/api-management-kubernetes#option-2-install-an-ingress-controller>

Mutual TLS authentication is natively supported by API Management and can be enabled in Kubernetes by installing an Ingress Controller.

<https://docs.microsoft.com/en-us/azure/api-management/media/api-management-aks/ingress-controller.png>

Answer is B  
upvoted 1 times

🗳️ 👤 **Manish03Nov** 3 years, 9 months ago



Answer is correct.

Ref : <https://docs.microsoft.com/en-us/azure/api-management/api-management-using-with-vnet?tabs=stv2>  
upvoted 1 times

🗳️ 👤 **Gautam1985** 3 years, 10 months ago

correct

upvoted 1 times

  **modiallo** 3 years, 11 months ago

Correct Answer

... the AKS cluster and the applications that consume the microservices might reside within the same VNet, hence there is no reason to expose the cluster publicly as all API traffic will remain within the VNet. For these scenarios, you can deploy API Management into the cluster VNet. API Management Developer and Premium tiers support VNet deployment.

upvoted 1 times

## HOTSPOT -

A company plans to implement an HTTP-based API to support a web app. The web app allows customers to check the status of their orders. The API must meet the following requirements:

- ⇒ Implement Azure Functions.
- ⇒ Provide public read-only operations.
- ⇒ Do not allow write operations.

You need to recommend configuration options.

What should you recommend? To answer, configure the appropriate options in the dialog box in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Topic	Value
HTTP methods	<div>▼</div> <div>API methods</div> <div>GET only</div> <div>GET and POST only</div> <div>GET, POST, and OPTIONS only</div>
Authorization level	<div>▼</div> <div>Function</div> <div>Anonymous</div> <div>Admin</div>

Suggested Answer:

**Answer Area**

Topic	Value
HTTP methods	<div>▼</div> <div>API methods</div> <div>GET only</div> <div>GET and POST only</div> <div>GET, POST, and OPTIONS only</div>
Authorization level	<div>▼</div> <div>Function</div> <div>Anonymous</div> <div>Admin</div>

HTTP methods: GET only -

Authorization level: Anonymous -

The option is Allow Anonymous requests. This option turns on authentication and authorization in App Service, but defers authorization decisions to your application code. For authenticated requests, App Service also passes along authentication information in the HTTP headers. This option provides more flexibility in handling anonymous requests.

Reference:

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

LT Highly Voted 4 years, 1 month ago

Correct answer..!!!!

upvoted 25 times

wai107 Highly Voted 4 years ago

anonymous: No API key is required.

function: A function-specific API key is required. This is the default value if none is provided.

admin: The master key is required.

<https://docs.microsoft.com/en-us/java/api/com.microsoft.azure.functions.annotation.httptrigger.authlevel?view=azure-java-stable>

upvoted 11 times

  **LillyLiver** 3 years ago

This is good information as to the "why" of option 2.

upvoted 1 times

  **gauravit43**  2 years, 2 months ago

I have passed AZ-305 on 15th April,2023 and this question was there in the exam

upvoted 1 times

  **dasEnder** 3 years, 1 month ago

I say is wrong! The question says Customers need to access the data. If you make it anonymous then everyone can access the data!

upvoted 1 times

  **AberdeenAngus** 2 years, 11 months ago

Anonymous only means that no key is required. You can still set up authentication, for example with Azure AD, which is probably a better option most of the time. I thought this page explained it clearly <https://docs.microsoft.com/en-us/azure/azure-functions/security-concepts?tabs=v4>



upvoted 2 times

  **plmmsg** 3 years, 3 months ago

GET Method

Anonymous

upvoted 1 times

  **Dpejic** 3 years, 6 months ago

Appere on exam 23-dec-2021

upvoted 3 times

  **syu31svc** 3 years, 9 months ago

"public read-only"

GET Method and Anonymous level are correct

upvoted 4 times

  **dkltruong88** 3 years, 9 months ago



Was in exam today 1-10-2021. I passed with score 896. I chose the provided answer

upvoted 5 times

  **Gautam1985** 3 years, 10 months ago

correct

upvoted 2 times

  **gssd4scoder** 4 years, 1 month ago

Very trivial

upvoted 2 times

  **examineezer** 3 years, 6 months ago

Maybe for you but not necessarily for others. I dont see how your comment is any benefit to anyone.

upvoted 14 times

  **onlyonetime** 4 years, 1 month ago

Correct

upvoted 1 times

  **Meedeh** 4 years, 1 month ago

Correct answer

upvoted 1 times



A company named Contoso Ltd., has a single-domain Active Directory forest named contoso.com.

Contoso is preparing to migrate all workloads to Azure. Contoso wants users to use single sign-on (SSO) when they access cloud-based services that integrate with Azure Active Directory (Azure AD).

You need to identify any objects in Active Directory that will fail to synchronize to Azure AD due to formatting issues. The solution must minimize costs.

What should you include in the solution?

- A. Azure AD Connect Health
- B. Microsoft Office 365 IdFix
- C. Azure Advisor
- D. Password Export Server version 3.1 (PES v3.1) in Active Directory Migration Tool (ADMT)

**Suggested Answer: B**

Community vote distribution

B (100%)

  **sogey** Highly Voted 4 years, 6 months ago

"IdFix is used to perform discovery and remediation of identity objects and their attributes in an on-premises Active Directory environment in preparation for migration to Azure Active Directory. "

<https://github.com/Microsoft/idxfix>

upvoted 51 times

  **shashu07** Highly Voted 4 years, 6 months ago

IdFix identifies errors such as duplicates and formatting problems in your Active Directory Domain Services (AD DS) domain before you synchronize to Office 365.

upvoted 11 times

  **S\_AB** Most Recent 3 years, 4 months ago

**Selected Answer: B**

idxfix.

<https://github.com/Microsoft/idxfix>

upvoted 2 times

  **anupam77** 3 years, 4 months ago

**Selected Answer: B**

Correct Answer

upvoted 1 times

  **Hudhaifa** 3 years, 4 months ago

On Exam 19th Feb 2022

upvoted 3 times

  **nicknamedude** 3 years, 7 months ago

**Selected Answer: B**

Based on experience

upvoted 7 times

  **syu31svc** 3 years, 9 months ago

<https://docs.microsoft.com/en-us/troubleshoot/azure/active-directory/objects-dont-sync-ad-sync-tool>

Use the IdFix DirSync Error Remediation Tool to find objects and errors that prevent synchronization to Azure AD.

Answer is B

upvoted 4 times

  **rdemontis** 3 years, 7 months ago

Correct. Thanks for the documentation attached.

upvoted 1 times

🗨️ 👤 **nkx** 3 years, 9 months ago

Came in exam on 20-sep-21, i passed, answer is correct

upvoted 5 times

🗨️ 👤 **Gautam1985** 3 years, 10 months ago

correct

upvoted 2 times

🗨️ 👤 **jdev** 3 years, 10 months ago

Is IdFix still available from MSFT?

upvoted 1 times

🗨️ 👤 **cfsxtuv33** 3 years, 11 months ago

Answer is correct: Microsoft Office 365 IdFix tool provides the customer with the ability to identify and remediate object errors in their Active Directory in preparation for deployment to Azure Active Directory or Office 365.

upvoted 1 times

🗨️ 👤 **modiallo** 3 years, 11 months ago

The Microsoft Office 365 IdFix tool provides the customer with the ability to identify and remediate object errors in their Active Directory in preparation for deployment to Azure Active Directory or Office 365

upvoted 1 times

🗨️ 👤 **modiallo** 3 years, 11 months ago

Correct.

<https://docs.microsoft.com/en-us/troubleshoot/azure/active-directory/objects-dont-sync-ad-sync-tool#run-idfix-to-check-for-duplicates-missing-attributes-and-rule-violations>

upvoted 1 times

🗨️ 👤 **ReginaldoBarreto** 4 years, 2 months ago

<https://docs.microsoft.com/pt-br/troubleshoot/azure/active-directory/objects-dont-sync-ad-sync-tool#symptoms>

upvoted 1 times

🗨️ 👤 **VlijmenFileer** 4 years, 3 months ago

Relevant URLs:

<https://docs.microsoft.com/en-us/troubleshoot/azure/active-directory/troubleshoot-pwd-sync>

<https://github.com/microsoft/ifix>

<https://docs.microsoft.com/en-US/troubleshoot/azure/active-directory/objects-dont-sync-ad-sync-tool>

upvoted 1 times

🗨️ 👤 **azurecert2021** 4 years, 4 months ago

Cause:-

This issue occurs for one of the following reasons:

The domain value that's used by AD DS attributes hasn't been verified.

One or more object attributes that require a unique value have a duplicate attribute value (such as the proxyAddresses attribute or the UserPrincipalName attribute) in an existing user account.

One or more object attributes violate formatting requirements that restrict the characters and the character length of attribute values.

One or more object attributes match exclusion rules for directory synchronization.

<https://docs.microsoft.com/en-us/troubleshoot/azure/active-directory/objects-dont-sync-ad-sync-tool>

upvoted 2 times

🗨️ 👤 **azurecert2021** 4 years, 4 months ago

Some examples of the error message that you may receive:

A synchronized object with the same proxy address already exists in your Microsoft Online Services directory.

Unable to update this object because the user ID is not found.

Unable to update this object in Microsoft Online Services because the following attributes associated with this object have values that may already be associated with another object in your local directory.

upvoted 1 times

## DRAG DROP -

A company has an existing web application that runs on virtual machines (VMs) in Azure.

You need to ensure that the application is protected from SQL injection attempts and uses a layer-7 load balancer. The solution must minimize disruption to the code for the existing web application.

What should you recommend? To answer, drag the appropriate values to the correct items. Each value may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

**Values**






**Answer Area****Item****Value**

Azure Service

Features

**Suggested Answer:**

**Values**






**Answer Area****Item****Value**

Azure Service

Features

Box 1: Azure Application Gateway

Azure Application Gateway provides an application delivery controller (ADC) as a service. It offers various layer 7 load-balancing capabilities for your applications.

Box 2: Web Application Firewall (WAF)

Application Gateway web application firewall (WAF) protects web applications from common vulnerabilities and exploits.

This is done through rules that are defined based on the OWASP core rule sets 3.0 or 2.2.9.

There are rules that detects SQL injection attacks.

Reference:

<https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-faq> <https://docs.microsoft.com/en-us/azure/application-gateway/waf-overview>

 **Elecktrus**  4 years, 6 months ago

Answer is correct. Because:

1-Azure Application Gateway, Azure Load Balancer y Azure Traffic Manager are all of them Load Balancers. But they are different: Application Gateway works in OSI layer 7 , Load Balancer works in OSI Layer 4 and Traffic Manager works with DNS. So, the only that verify the requirement (load-balance at level 7) is Azure Application Gateway



2) Features are Web Application Firewall, SSL-Offloading and url-content routing. Obviously, the only to protect against SQLInjections is Firewall (ssl-offloading is to manage https request) so the answer is Web Applicaton Firewall.

By the way, there is another one Load Balancer, named Azure Front Door, that works in OSI level 7, too.

<https://docs.microsoft.com/en-us/azure/architecture/guide/technology-choices/load-balancing-overview>



<https://docs.microsoft.com/es-es/azure/web-application-firewall/ag/ag-overview>

upvoted 88 times

  **andyR** 4 years, 6 months ago

Good to also remember which LB are regional V inter - regional

upvoted 2 times

  **bing** 3 years, 2 months ago

Azure Front Door Global HTTP(S)

Traffic Manager Global non-HTTP(S)

Application Gateway Regional HTTP(S)

Azure Load Balancer Regional non-HTTP(S)

upvoted 3 times

  **georgemich1** 3 years, 4 months ago

thanks!

upvoted 1 times

  **airairo**  4 years, 6 months ago



came in exam last month.

upvoted 9 times

  **gauravit43**  2 years, 2 months ago

I have passed AZ-305 on 15th April,2023 and this question was there in the exam

upvoted 2 times

  **OCHT** 3 years, 1 month ago

Agree . Az service=> AGW , AZ feature => WAF .


Correct answer.

upvoted 1 times

  **teyol51117** 3 years, 3 months ago



On exam 31.03.2022

upvoted 1 times

  **plmmsg** 3 years, 3 months ago

Answer is correct

upvoted 1 times

  **Dpejic** 3 years, 6 months ago

On exam 24.12.2021

upvoted 4 times

  **Dpejic** 3 years, 6 months ago

Appere on exam 23-dec-2021


upvoted 3 times

  **sharepoint\_Azure\_pp** 3 years, 8 months ago

Answer is correct or can say i choose the same.

was there in 17th October 2021 cleared with 900

upvoted 2 times

  **dkltruong88** 3 years, 9 months ago

Was in exam today 1-10-2021. I passed with score 896. I chose provided answer

upvoted 3 times

  **syu31svc** 3 years, 9 months ago

Layer 7 so Service is Application Gateway

<https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/ag-overview>

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

Feature is WAF

upvoted 1 times

🗨️ 👤 **ExStudent** 3 years, 9 months ago

I looked up MS documentation and WAF is referenced as a service & not as a Feature

upvoted 1 times

🗨️ 👤 **examineezer** 3 years, 6 months ago

You are right, but the only combined answer that makes sense here is AG for service and WAF for feature.

upvoted 1 times

🗨️ 👤 **tvS2021** 3 years, 11 months ago

passed 304 today, this question appeared in my exam.

upvoted 2 times

🗨️ 👤 **glam** 4 years, 5 months ago

Box 1: Azure Application Gateway

Box 2: Web Application Firewall (WAF)

upvoted 2 times

🗨️ 👤 **milind8451** 4 years, 5 months ago

Correct. Application GW will work as Layer 7 LB and WAF which is part of it, will protect from SQL Injection attack.

upvoted 1 times

🗨️ 👤 **Blaaa** 4 years, 5 months ago

Correct

upvoted 2 times

🗨️ 👤 **uzairahm007** 4 years, 6 months ago

discussion under

<https://www.examttopics.com/discussions/microsoft/view/11672-exam-az-301-topic-2-question-25-discussion/>

upvoted 1 times

You have an Azure subscription. The subscription has a blob container that contains multiple blobs. Ten users in the finance department of your company plan to access the blobs during the month of April. You need to recommend a solution to enable access to the blobs during the month of April only. Which security solution should you include in the recommendation?

- A. access keys
- B. conditional access policies
- C. certificates
- D. shared access signatures (SAS)

**Suggested Answer: D**

Reference:



<https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview>

Community vote distribution

D (100%)

  **KumarPV** Highly Voted 4 years, 6 months ago

SAS is the best option  
upvoted 31 times

  **JohnWick2020** Highly Voted 4 years, 4 months ago

Answer is D. Shared Access Signatures.  
This allows for limited-time fine grained access control to resources. So you can generate URL, specify duration (for month of April) and disseminate URL to 10 team members. On May 1, the SAS token is automatically invalidated, denying team members continued access.  
upvoted 22 times

  **alexshang** Most Recent 2 years, 12 months ago

D. Ad hoc SAS  
<https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview>  
upvoted 1 times

  **exnaniantwort** 3 years, 3 months ago

FYI what is conditional access and when to use it:  
Conditional Access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action.  
Example: A payroll manager wants to access the payroll application and is required to do multi-factor authentication to access it.

Common decisions:

Block access

Most restrictive decision

Grant access

Least restrictive decision, can still require one or more of the following options:

Require multi-factor authentication

Require device to be marked as compliant

Require Hybrid Azure AD joined device

Require approved client app

Require app protection policy (preview)

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

upvoted 1 times

  **Dawn7** 3 years, 3 months ago

**Selected Answer: D**

SAS is correct  
upvoted 1 times

🗨️ 👤 **plmmsg** 3 years, 3 months ago

Answer is SAS

upvoted 1 times

🗨️ 👤 **arun** 3 years, 3 months ago

**Selected Answer: D**

Implemented and Tested

upvoted 1 times

🗨️ 👤 **S\_AB** 3 years, 4 months ago

**Selected Answer: D**

Shared Access Signatures.

upvoted 1 times

🗨️ 👤 **us3r** 3 years, 5 months ago

**Selected Answer: D**

SAS the answ

upvoted 1 times

🗨️ 👤 **Dpejic** 3 years, 6 months ago

Appere on exam 23-dec-2021

upvoted 3 times

🗨️ 👤 **rdemontis** 3 years, 7 months ago

**Selected Answer: D**

Answer is D. Shared Access Signatures.

This allows for limited-time fine grained access control to resources. So you can generate URL, specify duration (for month of April) and disseminate URL to 10 team members. On May 1, the SAS token is automatically invalidated, denying team members continued access

upvoted 2 times

🗨️ 👤 **sharepoint\_Azure\_pp** 3 years, 8 months ago

SAS correct and i choose the same.

was there in 17th October 2021 cleared with 900

upvoted 3 times

🗨️ 👤 **syu31svc** 3 years, 9 months ago

This is D for sure

upvoted 2 times

🗨️ 👤 **lowczy** 3 years, 11 months ago

This question appeared in real exam.

upvoted 3 times

🗨️ 👤 **sujeetkb2021** 4 years ago

SAS is the correct answer

upvoted 2 times

🗨️ 👤 **Vipsao** 4 years, 3 months ago

SAS is right answer

upvoted 4 times

🗨️ 👤 **ElsaBBP** 4 years, 4 months ago

SAS is the only option for time-based access

upvoted 3 times

## HOTSPOT -

You plan to deploy an Azure web app named App1 that will use Azure Active Directory (Azure AD) authentication.

App1 will be accessed from the internet by the users at your company. All the users have computers that run Windows 10 and are joined to Azure AD.

You need to recommend a solution to ensure that the users can connect to App1 without being prompted for authentication and can access App1 only from company-owned computers.

What should you recommend for each requirement? To answer, select the appropriate options in the answer area.

Hot Area:

**Answer Area**

The users can connect to App1 without being prompted for authentication:

An Azure AD app registration
An Azure AD managed identity
Azure AD Application Proxy

The users can access App1 only from company-owned computers:

A conditional access policy
An Azure AD administrative unit
Azure Application Gateway
Azure Blueprints
Azure Policy

**Answer Area**

The users can connect to App1 without being prompted for authentication:

An Azure AD app registration
An Azure AD managed identity
Azure AD Application Proxy

**Suggested Answer:** The users can access App1 only from company-owned computers:

A conditional access policy
An Azure AD administrative unit
Azure Application Gateway
Azure Blueprints
Azure Policy

Box 1: An Azure AD app registration

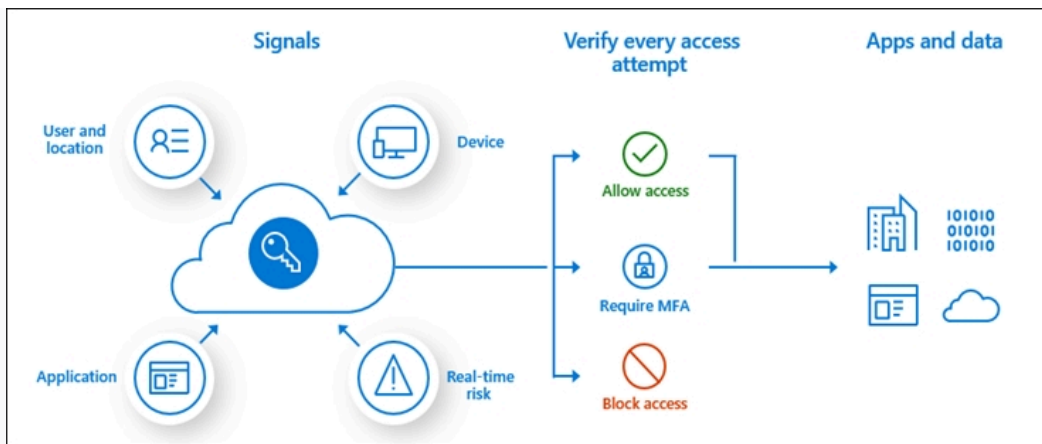
Azure active directory (AD) provides cloud based directory and identity management services. You can use azure AD to manage users of your application and authenticate access to your applications using azure active directory.

You register your application with Azure active directory tenant.

Box 2: A conditional access policy

Conditional Access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action. By using Conditional Access policies, you can apply the right access controls when needed to keep your organization secure and stay out of your user's way when not needed.





Reference:

<https://codingcanvas.com/using-azure-active-directory-authentication-in-your-web-application/> <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview>

**mmore** Highly Voted 4 years, 6 months ago

Seems correct.

upvoted 38 times

**glam** Highly Voted 4 years, 5 months ago

Box 1: An Azure AD app registration

Box 2: A conditional access policy

upvoted 24 times

**Snownoodles** Most Recent 2 years, 8 months ago

Azure joined devices can "SSO to both cloud and on-premises resources"

<https://learn.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join>

upvoted 1 times

**Pinkee888** 3 years, 2 months ago

Presented answer is correct. Register the app uses key vault for authentication, no longer prompts for authentication and restrict access exclusive to company supplied computers through conditional access policy.

upvoted 1 times

**AberdeenAngus** 2 years, 11 months ago

"Register the app uses key vault for authentication, no longer prompts for authentication"?? Anyone know a doc which supports this?

upvoted 1 times

**hertino** 3 years, 2 months ago

In AZ-305 exam, 9 april 22

upvoted 7 times

**teyol51117** 3 years, 3 months ago

On exam 31.03.2022

upvoted 2 times

**plmsg** 3 years, 3 months ago

App registration

Conditional access policy

upvoted 1 times

**syu31svc** 3 years, 9 months ago

<https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy>

Application Proxy is a feature of Azure AD that enables users to access on-premises web applications from a remote client

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>

Managed identities provide an identity for applications to use when connecting to resources that support Azure Active Directory (Azure AD) authentication

1st drop down is app registration

"access App1 only from company-owned computers" -> this would be conditional access  
upvoted 4 times

🗨️ 👤 **examineezer** 3 years, 6 months ago  
It isnt an on-premises web application.  
upvoted 1 times

🗨️ 👤 **red\_vix** 3 years, 11 months ago  
very good  
upvoted 1 times

🗨️ 👤 **lowczy** 3 years, 11 months ago  
This question appeared in real exam.  
upvoted 5 times

🗨️ 👤 **ruckii** 4 years ago  
only from company own computers.  
if we go with app registration, will this be full filed?  
upvoted 1 times

🗨️ 👤 **DragonsGav** 4 years ago  
App Registration  
- Register the Application  
- Configure SSO

Conditional Access will make sure only Domain joined computers are allowed.  
upvoted 2 times

🗨️ 👤 **pentium75** 3 years, 10 months ago  
The app "will use Azure Active Directory (Azure AD) authentication" - and it will do that because you register it as an app in AAD and configure SSO.

Once its registered in AAD, you can use Conditional Access policies to configure options for this specific app - and here you can specify that computers must be domain-joined.  
upvoted 4 times

🗨️ 👤 **ReginaldoBarreto** 4 years, 2 months ago  
<https://docs.microsoft.com/en-us/powerapps/developer/data-platform/walkthrough-register-app-azure-active-directory#:~:text=Create%20an%20application%20registration%201%20Create%20an%20application,the%20options%20and%20click%20on%20Add%20permi>

"After consenting to use their Dataverse account with the ISV's application, end users can connect to Dataverse environment from external application. The c form is not displayed again to other users after the first user who has already consented to use the ISV's app. Apps registered in Azure Active Directory are m which implies that other Dataverse users from other tenant can connect to their environment using the ISV's app."  
upvoted 1 times

🗨️ 👤 **Ganesh\_k** 4 years, 3 months ago  
Ans should be Managed identity and Conditional access  
<https://docs.microsoft.com/en-us/azure/app-service/overview-managed-identity?tabs=dotnet>  
upvoted 2 times

🗨️ 👤 **j888** 4 years, 3 months ago  
I believed managed Identity is to give permission to the application itself to access other resources. Meanwhile, the Azure AD app registration is to allow the authenticated user on Azure AD to sign in to the registered application. So the answer itself is correct.  
upvoted 8 times

🗨️ 👤 **Tidopuddy** 4 years, 3 months ago  
Box 1. App Proxy  
Box 2. Conditional access policy  
upvoted 6 times

🗨️ 👤 **zipstore** 4 years, 2 months ago  
No on-premise AD involved, only Azure AD.  
upvoted 1 times

🗨️ 👤 **DragonsGav** 4 years ago

Application proxy is only for apps which are on-prem and you want to publish them so users do not require VPN. Question is for a Web App configured in Azure, not an application hosted in a company DC.

upvoted 3 times

🗨️ 👤 **youlital003** 4 years, 2 months ago

"Azure Active Directory's Application Proxy provides secure remote access to on-premises web applications." <https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy>

App1 is an Az Web APP.

upvoted 2 times

🗨️ 👤 **[Removed]** 4 years, 4 months ago

How app registration with ad will ensure user can connect without being prompted for authentication?

upvoted 4 times

🗨️ 👤 **mshad** 4 years ago

I also had the same question

upvoted 1 times

🗨️ 👤 **Said\_kram** 4 years, 1 month ago

we can set up authentication (SSO) in app registration

upvoted 1 times

🗨️ 👤 **pentium75** 3 years, 10 months ago

The users are using Windows 10 on domain-joined computers, thus the users are already authenticated to Azure AD. When you configure the App for SSO with Azure AD, users are logged in automatically "without being prompted for authentication [another time]".

upvoted 3 times

🗨️ 👤 **milind8451** 4 years, 5 months ago

Right ans.

upvoted 4 times

## HOTSPOT -

You plan to create an Azure environment that will contain a root management group and 10 child management groups. Each child management group will contain five Azure subscriptions. You plan to have between 10 and 30 resource groups in each subscription.

You need to design an Azure governance solution. The solution must meet the following requirements:

- ⇒ Use Azure Blueprints to control governance across all the subscriptions and resource groups.
- ⇒ Ensure that Blueprints-based configurations are consistent across all the subscriptions and resource groups.
- ⇒ Minimize the number of blueprint definitions and assignments.

What should you include in the solution? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Level at which to define the blueprints:

The child management groups

The root management group

The subscriptions

Level at which to create the blueprint assignments:

The child management groups

The root management group

The subscriptions

**Answer Area**

Level at which to define the blueprints:

The child management groups

The root management group

The subscriptions

Suggested Answer:

Level at which to create the blueprint assignments:

The child management groups

The root management group

The subscriptions

Box 1: The root management group

When creating a blueprint definition, you'll define where the blueprint is saved. Blueprints can be saved to a management group or subscription that you have

Contributor access to. If the location is a management group, the blueprint is available to assign to any child subscription of that management group.

Box 2: The root management group

Each directory is given a single top-level management group called the "Root" management group. This root management group is built into the hierarchy to have all management groups and subscriptions fold up to it. This root management group allows for global policies and Azure role assignments to be applied at the directory level.

Each Published Version of a blueprint can be assigned to an existing management group or subscription.

Reference:

<https://docs.microsoft.com/en-us/azure/governance/blueprints/overview> <https://docs.microsoft.com/en-us/azure/governance/management-groups/overview>

Disagree with answer #2.

Answer 1: The root management group (correct)

Answer 2: The subscriptions

Explanation: When creating a blueprint definition, you'll define where the blueprint is saved. Blueprints can be saved to a management group or subscription that you have Contributor access to. If the location is a management group, the blueprint is available to assign to any child subscription of that management group.

Since question #2 clearly mentions the scope of assignments, it should be on the subscription level.

upvoted 84 times

  **subbu3071988** 3 years, 9 months ago

I can't understand why is everyone getting confused on this especially Box2. I have a simple question- how do you control governance across all subscriptions and RGs by creating Blueprint assignments at Subscription level? If you do it at the subscription level, then subscription owners will have permission to change/delete the Blueprint assignment. This means by creating Blueprint assignment at subscription level, you will not be able to "control governance across all subscriptions and RGs".

Note- Blueprint assignments can be done both at the MG level (Rest API) and at subscription level. So these would be my answers-

Box 1: The root management group

Box 2: The root management group

Ref- <https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/governance/blueprints/concepts/resource-locking.md>

upvoted 49 times

  **rdemontis** 3 years, 7 months ago

Correct! Thanks for explanation

upvoted 2 times

  **therealss** 3 years, 4 months ago

Well I'm confused now. The process of an assignment includes the creation of resources, and you have to have a subscription to hold actual resources (i.e. - a mgmt group, unto itself, cannot hold resources). Also, the idea that "subscription owners will have permission to change/delete the Blueprint assignment"....that's only true if you use DON'T LOCK as the resource locking mode (which is the default, but that is under the control the assignee). Plus if you use the portal, subscription is the only option to do an assignment. I'm reading on this thread that the REST API allows it, so I do have some doubts, but overall, I think it's subscription. <https://adamtheautomator.com/azure-blueprints/>

upvoted 2 times

  **cloudprospect** 3 years ago

Also:

Ensure that Blueprints-based configurations are consistent across all the subscriptions and resource groups.

Minimize the blueprints and assignments.

If every subscription is subject to the same policies and we want to minimize the number of assignments, root assignment is correct.

upvoted 1 times

  **Oracleist** 4 years, 1 month ago

you can assign a blueprint to a management group using REST API...

upvoted 3 times

  **Kamekung** 4 years, 1 month ago

After a blueprint has been published, \*\*it can be assigned to a subscription.\*\* Assign the blueprint that you created to one of the subscriptions under your management group hierarchy. If the blueprint is saved to a subscription, it can only be assigned to that subscription.

<https://docs.microsoft.com/en-us/azure/governance/blueprints/create-blueprint-portal>

upvoted 3 times

  **teehex** 3 years, 10 months ago

Why did the answer get many votes? It is the wrong answer. To minimize the administrative effort you must assign to a higher scope. Blueprint can be assigned to MG technically. Read this one <https://docs.microsoft.com/en-us/rest/api/blueprints/assignments/create-or-update> (properties.scope).

upvoted 12 times

  **Aghora**  4 years, 4 months ago

tested . no need to confuse things .

I created a blueprint . when creating your asked for the location - I selected the tenant group .

I then saved as a draft . then published it with version1.0.

the blueprint was in definitions blade and now where else.

I then clicked on assign(no another place to "CREATE" assignments ) the first thing I was asked for is SUBSCRIPTION !. so the answer is

1- Root management group

2- Subscriptions

upvoted 60 times

🗨️ 👤 **sallymaher** 4 years, 4 months ago

Me also tested in the lab you can't assign the blueprint to a management group only to subscription

upvoted 6 times

🗨️ 👤 **VincentZhang** 3 years, 9 months ago

The question is not asking you where to assign but which level to create the assignment.

upvoted 5 times

🗨️ 👤 **Deepbond** 4 years, 3 months ago

Blueprint can be assigned to management group using REST API but not from Portal.

<https://docs.microsoft.com/en-us/azure/governance/blueprints/overview#blueprint-assignment>

upvoted 19 times

🗨️ 👤 **skywalker** Most Recent 4 months, 2 weeks ago

Assigning a blueprint definition to a management group means the assignment object exists at the management group. The deployment of artifacts still targets a subscription. To perform a management group assignment, the Create Or Update REST API must be used and the request body must include a value for properties.scope to define the target subscription.

<https://learn.microsoft.com/en-us/azure/governance/blueprints/overview>

Answer 1: The root management group

Answer 2: The root management group

upvoted 1 times

🗨️ 👤 **calotta1** 1 year, 10 months ago

Creation can be done at Management Group, but assignment has to be sub level - <https://learn.microsoft.com/en-us/azure/governance/blueprints/create-blueprint-portal#assign-a-blueprint>

upvoted 1 times

🗨️ 👤 **gauravit43** 2 years, 3 months ago

root management group and subscription

upvoted 1 times

🗨️ 👤 **Blzs** 3 years ago

I am testing this at the Azure portal now. I have a few test management groups. When I create a new Blueprint definition and select "definition location" the root management group is greyed out to me. I can only select a child management group. No matter if they have a subscription or not. Later when I try to assign the blueprint, I can only select a Subscription.

So based on this experience, the correct answer seems to be:

1) Child level

2) Subscriptions

upvoted 2 times

🗨️ 👤 **Blzs** 3 years ago

correction... I didn't have access to the root management group.

So:

1) root

2) subscriptions

upvoted 1 times

🗨️ 👤 **teyol51117** 3 years, 3 months ago

On exam 31.03.2022

upvoted 2 times

🗨️ 👤 **kanweng** 3 years, 3 months ago

<https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/deployment-stages#:~:text=The%20blueprint%20assignment%20object%20is%20created,-A%20user%2C%20group&text=The%20assignment%20object%20exists%20at,of%20managed%20identity%20is%20selected.>

The blueprint assignment object is created

A user, group, or service principal assigns a blueprint to a subscription. The assignment object exists at the subscription level where the blueprint was assigned. Resources created by the deployment aren't done in context of the deploying entity.

upvoted 1 times

🗨️ 👤 **MaroofAli** 3 years, 3 months ago

Blueprint assignment

Each Published Version of a blueprint can be assigned (with a max name length of 90 characters) to an existing management group or subscription. In the portal, the blueprint defaults the Version to the one Published most recently. If there are artifact parameters or blueprint parameters, then the parameters are defined during the assignment process.

Note

Assigning a blueprint definition to a management group means the assignment object exists at the management group. The deployment of artifacts still targets a subscription. To perform a management group assignment, the Create Or Update REST API must be used and the request body must include a value for properties.scope to define the target subscription.

Reference: <https://docs.microsoft.com/en-us/azure/governance/blueprints/overview#blueprint-assignment>

upvoted 3 times

🗨️ 👤 **arun** 3 years, 3 months ago

<https://docs.microsoft.com/en-us/azure/governance/blueprints/overview#blueprint-assignment>

Assigning a blueprint definition to a management group means the assignment object exists at the management group. The deployment of artifacts still targets a subscription

so Root Management is correct for both boxes.

upvoted 3 times

🗨️ 👤 **plmmmsg** 3 years, 3 months ago

Root management group for both

upvoted 1 times

🗨️ 👤 **us3r** 3 years, 5 months ago

- 1) root management group
- 2) root management group

The only option to prevent subscription owners from removing a blueprint assignment is to assign the blueprint to a management group. In this scenario, only Owners of the management group have the permissions needed to remove the blueprint assignment.

<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/governance/blueprints/concepts/resource-locking.md#assign-at-management-group>

upvoted 2 times

🗨️ 👤 **chichi0307** 3 years, 8 months ago

Root Management Group is highest level. If assign to mgmt group, it will be available for assigning subscripuion in that management group. so answer is corect.Refer microsoft video.

<https://docs.microsoft.com/en-us/azure/governance/blueprints/overview#blueprint-definition-locations>

upvoted 1 times

🗨️ 👤 **rafpullo** 3 years, 8 months ago

Answer is correct. You assign blueprint to subscription not to management group. A blueprint crates resources and resources are in a subscription not in a mgmt groups which is a concept for governance not for hosting resources and bill their consumption

upvoted 1 times

🗨️ 👤 **syu31svc** 3 years, 9 months ago

If you can define at the root level surely you can create at the root level for consistency and minimizing definitions

upvoted 1 times

🗨️ 👤 **subbu3071988** 3 years, 9 months ago



Box 1: Root management group (most agree with it)

So the confusion is on Box 2 whether its MG or Subscription.

You can create Blueprint Assignment at both MG level (using Rest API) and subscription level. If you create the Assignment at Subscription level, then subscription owners can change/remove the Blueprint assignments thereby the purpose of "to control governance across all subscriptions and RGs" will be defeated. The only option to prevent subscription owners from removing a blueprint assignment is to assign the blueprint to a management group.

<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/governance/blueprints/concepts/resource-locking.md>

upvoted 3 times

  **Ario** 3 years, 9 months ago

Answer is correct

upvoted 1 times



You have an Azure subscription.

You need to recommend a solution to provide developers with the ability to provision Azure virtual machines. The solution must meet the following requirements:

- ⇒ Only allow the creation of the virtual machines in specific regions.
- ⇒ Only allow the creation of specific sizes of virtual machines.

What should you include in the recommendation?

- A. Azure Resource Manager templates
- B. Azure Policy
- C. conditional access policies
- D. role-based access control (RBAC)

**Suggested Answer: B**

Community vote distribution

B (100%)

🗳️ 👤 **idrisfi** Highly Voted 4 years, 6 months ago

Correct

<https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/manage/azure-server-management/common-policies#restrict-vm-size>  
upvoted 37 times

🗳️ 👤 **ahorva** 3 years, 5 months ago

Answer is correct

VM Size - Allowed virtual machine size SKU - <https://docs.microsoft.com/en-us/azure/governance/policy/samples/built-in-policies#compute>

Location - Allowed locations - <https://docs.microsoft.com/en-us/azure/governance/policy/samples/built-in-policies#general>  
upvoted 1 times

🗳️ 👤 **xAlx** Highly Voted 4 years, 6 months ago

Correct

upvoted 12 times

🗳️ 👤 **gauravit43** Most Recent 2 years, 2 months ago

I have passed AZ-305 on 15th April,2023 and this question was there in the exam  
upvoted 1 times

🗳️ 👤 **sapien45** 3 years ago

Sounds like an AWS question

upvoted 1 times

🗳️ 👤 **Teringzooi** 3 years, 2 months ago

Selected Answer: B

Correct answer: B

<https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/manage/azure-server-management/common-policies#restrict-vm-size>  
upvoted 1 times

🗳️ 👤 **plmmg** 3 years, 3 months ago

answer is Policy

upvoted 1 times

🗳️ 👤 **moon2351** 3 years, 5 months ago

Selected Answer: B

Correct

upvoted 1 times

🗳️ 👤 **pruntelnetworks** 3 years, 5 months ago

Selected Answer: B

b is correct

upvoted 1 times

🗉 👤 **sakshi250291** 3 years, 6 months ago

**Selected Answer: B**

Correct

upvoted 1 times

🗉 👤 **ScubaDiver123456** 3 years, 6 months ago

**Selected Answer: B**

What I believe to be correct

upvoted 1 times

🗉 👤 **jadepe** 3 years, 6 months ago

**Selected Answer: B**

Correct

upvoted 1 times

🗉 👤 **m4mayur** 3 years, 6 months ago

**Selected Answer: B**

Correct answer

upvoted 3 times

🗉 👤 **cfsxtuv33** 3 years, 7 months ago

**Selected Answer: B**

Answer seems to be correct

upvoted 3 times

🗉 👤 **rdemontis** 3 years, 7 months ago

**Selected Answer: B**

Azure Policy is the way you can govern resources creation in Azure: <https://docs.microsoft.com/en-us/azure/governance/policy/overview>

upvoted 6 times

🗉 👤 **sharepoint\_Azure\_pp** 3 years, 8 months ago

Azure policy is what i choose and seems to be correct as well

was there in 17th October 2021 cleared with 900

upvoted 2 times

🗉 👤 **syu31svc** 3 years, 9 months ago

This is B 101%

upvoted 3 times

🗉 👤 **nkV** 3 years, 9 months ago

Came in exam on 20-sep-21, i passed, answer is correct

upvoted 2 times

Your company has the offices shown in the following table.

Location	IP address space	Public NAT segment
Montreal	10.10.0.0/16	190.15.1.0/24
Seattle	172.16.0.0/16	194.25.2.0/24

The network contains an Active Directory domain named contoso.com that is synced to Azure Active Directory (Azure AD).

All users connect to an Exchange Online.

You need to recommend a solution to ensure that all the users use Azure Multi-Factor Authentication (MFA) to connect to Exchange Online from one of the offices.

What should you include in the recommendation?

- A. a virtual network and two Microsoft Cloud App Security policies
- B. a named location and two Microsoft Cloud App Security policies
- C. a conditional access policy and two virtual networks
- D. a conditional access policy and two named locations

**Suggested Answer: D**

Conditional Access policies are at their most basic an if-then statement combining signals, to make decisions, and enforce organization policies. One of those signals that can be incorporated into the decision-making process is network location.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition#named-locations>

Community vote distribution

D (100%)

 **quyennv** Highly Voted 4 years, 7 months ago

Correct answer

upvoted 36 times

 **glam** Highly Voted 4 years, 5 months ago

D. a conditional access policy and two named locations

upvoted 13 times

 **AlfL** Most Recent 3 years, 3 months ago

**Selected Answer: D**

answer is correct

upvoted 2 times

 **exnaniantwort** 3 years, 3 months ago

Named locations

Locations are named in the Azure portal under Azure Active Directory > Security > Conditional Access > Named locations. These named network locations may include locations like an organization's headquarters network ranges, VPN network ranges, or ranges that you wish to block. Named locations can be defined by IPv4/IPv6 address ranges or by countries.

To define a named location by IPv4/IPv6 address ranges, you'll need to provide:


A Name for the location

One or more IP ranges

Optionally Mark as trusted location

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>

upvoted 6 times

 **Dawn7** 3 years, 3 months ago

**Selected Answer: D**

I think D is correct

upvoted 1 times

 **moon2351** 3 years, 5 months ago

Answer is D

upvoted 1 times

🗨️ 👤 **Dpejic** 3 years, 6 months ago

Appere on exam 23-dec-2021

upvoted 5 times

🗨️ 👤 **examineezer** 3 years, 6 months ago

[https://docs.microsoft.com/en-us/graph/api/resources/namedlocation?view=graph-rest-](https://docs.microsoft.com/en-us/graph/api/resources/namedlocation?view=graph-rest-1.0#~:text=Named%20locations%20are%20custom%20rules,in%20a%20Conditional%20Access%20policy.)

[1.0#~:text=Named%20locations%20are%20custom%20rules,in%20a%20Conditional%20Access%20policy.](https://docs.microsoft.com/en-us/graph/api/resources/namedlocation?view=graph-rest-1.0#~:text=Named%20locations%20are%20custom%20rules,in%20a%20Conditional%20Access%20policy.)

upvoted 2 times

🗨️ 👤 **Eitant** 3 years, 6 months ago

**Selected Answer: D**

Correct answer

upvoted 2 times

🗨️ 👤 **Eitant** 3 years, 6 months ago

**Selected Answer: D**

Correct answer

upvoted 1 times

🗨️ 👤 **syu31svc** 3 years, 9 months ago

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>

These named network locations may include locations like an organization's headquarters network ranges, VPN network ranges, or ranges that you wish to block

Answer is D

upvoted 3 times

🗨️ 👤 **dkltruong88** 3 years, 9 months ago

Was in exam today 1-10-2021. I passed with score 896. I chose D

upvoted 6 times

🗨️ 👤 **medi01** 3 years, 10 months ago

Single named location can contain multiple IP ranges. Why would we need two named locations???

upvoted 4 times

🗨️ 👤 **Gautam1985** 3 years, 10 months ago

correct

upvoted 1 times

🗨️ 👤 **[Removed]** 3 years, 10 months ago

"All the users use Azure Multi-Factor Authentication (MFA) to connect to Exchange Online from ONE of the offices."

So really only one named location is necessary.

upvoted 6 times

🗨️ 👤 **jjdevine** 3 years, 10 months ago

Yes I found this confusing.

upvoted 2 times

🗨️ 👤 **red\_vix** 3 years, 11 months ago

that's correct

upvoted 1 times

🗨️ 👤 **alphamode** 4 years, 5 months ago

Correct answer

upvoted 5 times

## HOTSPOT -

Your organization has developed and deployed several Azure App Service Web and API applications. The applications use Azure Key Vault to store several authentication, storage account, and data encryption keys. Several departments have the following requests to support the applications:

Department	Request
Security	<ul style="list-style-type: none"><li>Review membership of administrative roles and require users to provide a justification for continued membership.</li><li>Get alerts about changes in administrator assignments.</li><li>See a history of administrator activation, including which changes administrators made to Azure resources.</li></ul>
Development	<ul style="list-style-type: none"><li>Enable the applications to access Azure Key Vault and retrieve keys for use in code.</li></ul>
Quality Assurance	<ul style="list-style-type: none"><li>Receive temporary administrator access to create and configure additional Web and API applications in the test environment.</li></ul>

You need to recommend the appropriate Azure service for each department request.

What should you recommend? To answer, configure the appropriate options in the dialog box in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Department	Azure Service
Security	<div><div></div><div>Azure AD Privileged Identity Management</div><div>Azure Managed Identity</div><div>Azure AD Connect</div><div>Azure AD Identity Protection</div></div>
Development	<div><div></div><div>Azure AD Privileged Identity Management</div><div>Azure Managed Identity</div><div>Azure AD Connect</div><div>Azure AD Identity Protection</div></div>
Quality Assurance	<div><div></div><div>Azure AD Privileged Identity Management</div><div>Azure Managed Identity</div><div>Azure AD Connect</div><div>Azure AD Identity Protection</div></div>

## Answer Area

### Department Azure Service

Security

Azure AD Privileged Identity Management
Azure Managed Identity
Azure AD Connect
Azure AD Identity Protection

Development

Azure AD Privileged Identity Management
Azure Managed Identity
Azure AD Connect
Azure AD Identity Protection

Quality Assurance

Azure AD Privileged Identity Management
Azure Managed Identity
Azure AD Connect
Azure AD Identity Protection

Suggested Answer:

  **mmmore** Highly Voted 4 years, 6 months ago

Correct

upvoted 66 times

  **QiangQiang** 4 years, 1 month ago

The first one should be Azure AD Identity Protection to create an access review

upvoted 8 times

  **QiangQiang** 4 years, 1 month ago

never mind, it's Azure AD Identity Governance that covers access review, Not ID Protection. my bad

upvoted 16 times

  **Lexa** Highly Voted 4 years, 5 months ago

QA section confused a little, but it's correct: "Provide just-in-time privileged access to Azure AD and Azure resources"

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure#what-does-it-do>

upvoted 18 times

  **dandirindan** 4 years, 4 months ago

great comment on jit access,

upvoted 4 times

  **Azure\_daemon** Most Recent 3 years, 1 month ago



The first box is wrong, Security team needs access review and that only comes with the Azure AD P2 tier which is the identity protection

upvoted 3 times

  **cwilson91** 3 years, 1 month ago

Was on the AZ-305 exam - 5.7.22

upvoted 5 times

  **plmmsg** 3 years, 3 months ago

Security: PIM

Development: Mange identity

Quality Assurance: PIM

upvoted 3 times

  **moon2351** 3 years, 5 months ago

Answer is correct

upvoted 2 times



  **syu31svc** 3 years, 9 months ago

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure#what-does-it-do>

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

1st and 3rd drop downs are PIM



"access Key Vault" -> This would be Managed Identity for 2nd drop down  
upvoted 7 times

  **nk** 3 years, 9 months ago

Came in exam on 20-sep-21, i passed, answers are correct  
upvoted 4 times

  **cfsxtuv33** 3 years, 7 months ago

The answers are correct. The only issue I have is that you comment on quite a few questions as if you remember each and every one that was on your test. I'm not buying it for a second.  
upvoted 8 times

  **catfood** 2 years, 10 months ago

ikr - you don't get a list of questions you got right when you complete the exam, we aren't that stupid  
upvoted 1 times

  **Gautam1985** 3 years, 10 months ago

correct  
upvoted 1 times

  **cfsxtuv33** 3 years, 11 months ago

Yes! We all finally agree on this one!  
Security: PIM  
Development: Mange identity  
Quality Assurance: PIM  
upvoted 6 times

  **ashishg2105** 4 years, 1 month ago

Answer is Correct!!  
upvoted 3 times

  **dadageer** 4 years, 2 months ago

Correct answers!  
upvoted 3 times

  **Prasanna3215** 4 years, 3 months ago

Correct  
upvoted 2 times

  **glam** 4 years, 5 months ago



Azure AD Privileged Identity Management  
Azure Managed Service identities  
Azure AD Privileged Identity Management  
upvoted 6 times

  **alphamode** 4 years, 5 months ago

100% correct answer  
upvoted 4 times

  **milind8451** 4 years, 5 months ago

Right ans.  
upvoted 3 times

  **Blaaa** 4 years, 5 months ago

Correct

upvoted 2 times



Your network contains an on-premises Active Directory forest.

You discover that when users change jobs within your company, the membership of the user groups are not being updated. As a result, the users can access resources that are no longer relevant to their job.

You plan to integrate Active Directory and Azure Active Directory (Azure AD) by using Azure AD Connect.

You need to recommend a solution to ensure that group owners are emailed monthly about the group memberships they manage.

What should you include in the recommendation?

- A. Azure AD Identity Protection
- B. Azure AD access reviews
- C. Tenant Restrictions
- D. conditional access policies

**Suggested Answer: B**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview>



Community vote distribution

B (100%)

  **gcpjay** Highly Voted 4 years, 6 months ago

Answer is correct.

upvoted 41 times

  **JustDiscussing** Highly Voted 4 years, 6 months ago


in exam this week

upvoted 11 times

  **menhazuddin** Most Recent 2 years, 7 months ago

correct



upvoted 1 times

  **itenginerd** 3 years, 3 months ago

Selected Answer: B

On my exam today.

upvoted 1 times

  **Dawn7** 3 years, 3 months ago

Selected Answer: B

Correct

upvoted 1 times

  **pruntelnetworks** 3 years, 5 months ago

Selected Answer: B

correct

upvoted 1 times

  **sujitwarrier11** 3 years, 5 months ago

Im a little confused, Privileged Identity Management also has access reviews. So what should I choose?

upvoted 1 times

  **godjackal** 2 years, 10 months ago



read the question

upvoted 1 times

  **Dpejic** 3 years, 6 months ago

Appere on exam 23-dec-2021

upvoted 3 times

  **jadepe** 3 years, 6 months ago

Selected Answer: B

Correct

upvoted 3 times

🗲️ 👤 **sharepoint\_Azure\_pp** 3 years, 8 months ago

AD access review is correct or can say i choose the same.

was there in 17th October 2021 cleared with 900

upvoted 3 times

🗲️ 👤 **syu31svc** 3 years, 9 months ago

<https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview>

Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. User's access can be reviewed on a regular basis to make sure only the right people have continued access.

Answer is B

upvoted 2 times

🗲️ 👤 **OCHT** 3 years, 1 month ago

Agree with this.

upvoted 1 times

🗲️ 👤 **nkx** 3 years, 9 months ago

Came in exam on 20-sep-21, i passed, answer is correct

upvoted 3 times

🗲️ 👤 **Gautam1985** 3 years, 10 months ago

correct

upvoted 1 times

🗲️ 👤 **tvS2021** 3 years, 11 months ago

This question in my exam today. passed 304 exam

upvoted 2 times

🗲️ 👤 **Linus0** 3 years, 11 months ago

Access Reviews under Azure AD Identity Governance

upvoted 2 times

🗲️ 👤 **bbcZ** 4 years, 2 months ago

On Exam 05/01/2021

upvoted 4 times

🗲️ 👤 **stieltjes** 4 years, 2 months ago

in exam yesterday

upvoted 3 times

## HOTSPOT -

You have five .NET Core applications that run on 10 Azure virtual machines in the same subscription.

You need to recommend a solution to ensure that the applications can authenticate by using the same Azure Active Directory (Azure AD) identity.

The solution must meet the following requirements:

- ⇒ Ensure that the applications can authenticate only when running on the 10 virtual machines.
- ⇒ Minimize administrative effort.

What should you include in the recommendation? To answer, select the appropriate options in the answer area.

Hot Area:

**Answer Area**

To provision the Azure AD identity:

<input type="text"/>
Create a system-assigned Managed Identities for Azure resources
Create a user-assigned Managed Identities for Azure resources
Register each application in Azure AD

To authenticate, request a token by using:

<input type="text"/>
An Azure AD v1.0 endpoint
An Azure AD v2.0 endpoint
An Azure Instance Metadata Service identity OAuth2 endpoint

**Answer Area**

To provision the Azure AD identity:

<input type="text"/>
Create a system-assigned Managed Identities for Azure resources
Create a user-assigned Managed Identities for Azure resources
Register each application in Azure AD

To authenticate, request a token by using:

<input type="text"/>
An Azure AD v1.0 endpoint
An Azure AD v2.0 endpoint
An Azure Instance Metadata Service identity OAuth2 endpoint

Suggested Answer:

Box 1: Create a system-assigned Managed Identities for Azure resource

The managed identities for Azure resources feature in Azure Active Directory (Azure AD) feature provides Azure services with an automatically managed identity in Azure AD. You can use the identity to authenticate to any service that supports Azure AD authentication, including Key Vault, without any credentials in your code.

A system-assigned managed identity is enabled directly on an Azure service instance. When the identity is enabled, Azure creates an identity for the instance in the Azure AD tenant that's trusted by the subscription of the instance. After the identity is created, the credentials are provisioned onto the instance.

Box 2: An Azure Instance Metadata Service Identity

See step 3 and 5 below.

How a system-assigned managed identity works with an Azure VM

1. Azure Resource Manager receives a request to enable the system-assigned managed identity on a VM.
2. Azure Resource Manager creates a service principal in Azure AD for the identity of the VM. The service principal is created in the Azure AD tenant that's trusted by the subscription.
3. Azure Resource Manager configures the identity on the VM by updating the Azure Instance Metadata Service identity endpoint with the service principal client ID and certificate.
4. After the VM has an identity, use the service principal information to grant the VM access to Azure resources. To call Azure Resource Manager, use role-based access control (RBAC) in Azure AD to assign the appropriate role to the VM service principal. To call Key Vault, grant your code access to the specific secret or key in Key Vault.
5. Your code that's running on the VM can request a token from the Azure Instance Metadata service endpoint, accessible only from within the VM

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>

  **andyR**  4 years, 7 months ago


should be user assigned MI

upvoted 133 times

  **MaxBlanche** 4 years, 7 months ago

I agree

upvoted 3 times

  **idrisfi** 4 years, 7 months ago

I agree, as the same identity needs to be shared across resources

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview#managed-identity-types>

upvoted 6 times

  **dandirindan** 4 years, 4 months ago

another question is that user managed identities can be shared among virtual machines, but system managed identities cant

upvoted 4 times

  **ElsaBBP** 4 years, 4 months ago

exactly, user-assigned managed identities are shared and the same not per instance.

upvoted 4 times

  **nandacharya3**  4 years, 2 months ago

Somestmes, discussions, lead to more confusion

upvoted 62 times

  **JayBee65** 3 years ago

I couldn't agree less. It's all good for learning

upvoted 2 times

  **china5000** 3 years, 5 months ago

Rather, these kinds of decussions widen our understanding of the topic, encourage us to do our own research, try it ourselves if possible.

upvoted 12 times

  **Mr\_wippy** 3 years, 3 months ago

Agree. While my primary use of discussion is to find the right answer, I don't mind seeing a discussion with different opinions. It forces me to collate all the data the find the answer makes more sense to me

upvoted 7 times

  **Cg007**  1 year, 2 months ago

1. To provision the Azure AD identity:

Create a system-assigned Managed Service Identity: This is a type of identity that is tied to the lifecycle of a specific resource, such as an Azure virtual machine. Using system-assigned identities, the identity is automatically managed by Azure and does not require any manual effort once set up.

2. To authenticate, request a token by using:

An Azure AD v2.0 endpoint: The Azure AD v2.0 endpoint supports the latest protocol and allows applications to use the Microsoft identity platform to

authenticate users and access secured resources in Azure.

By choosing these options, you'll ensure that each of the 10 virtual machines has its own identity that can be used by the applications running on them. Since the identity is tied to the machine, the application will only be able to authenticate when running on the virtual machine. The use of system-assigned Managed Service Identity reduces administrative overhead because it doesn't require manual management of the identity lifecycle.

upvoted 1 times

🗳️ 👤 **One111** 2 years, 10 months ago

User assigned managed identity = 5 apps on 10 VMs.

Endpoint v2 = only one that remains supported and provide authentication. V1 depreciated. IMDS provided info about vm for all processes inside vm, anonymously.

upvoted 1 times

🗳️ 👤 **One111** 2 years, 10 months ago

Azure Instance Metadata Service doesn't provide authentication channel. This is wrong answer.

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/instance-metadata-service?tabs=windows>

Azure Instance Metadata Service (IMDS) provides information about currently running virtual machine instances. Instance Metadata Service is only accessible from within a running virtual machine instance on a non-routable IP address. VMs are limited to interacting with metadata/functionality that pertains to themselves.

IMDS is not a channel for sensitive data. The API is unauthenticated and open to all processes on the VM. Information exposed through this service should be considered as shared information to all applications running inside the VM.

upvoted 1 times

🗳️ 👤 **AberdeenAngus** 3 years, 1 month ago

Good link explaining how an app running on a VM can get an access token using Azure Instance Metadata Service:

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/how-to-use-vm-token#get-a-token-using-http>

upvoted 2 times

🗳️ 👤 **pillow2274** 3 years, 2 months ago

I found this regarding the 2nd part of the question which I agree is correct and thought i'd post it.

'Your code that's running on the server can request a token from the Azure Instance Metadata service endpoint, accessible only from within the server.'

<https://docs.microsoft.com/en-us/azure/azure-arc/servers/managed-identity-authentication>

upvoted 2 times

🗳️ 👤 **exnaniantwort** 3 years, 3 months ago

can anyone explain Azure AD V1, V2 endpoint and Azure Instance Metadata service endpoint?

upvoted 3 times

🗳️ 👤 **AD3** 3 years, 3 months ago

Why system assigned

1. No admin as they are created automatically and deleted automatically with the resource which is the VM. One requirement is no or less admin effort.

2. The other point is the app is authenticated only when running on these VMs. So if the VM dies and new VM is created the app will not be authenticated. This fits perfectly as the life cycle requirement. The user managed identities are created by user and hence have more admin effort & they still exists when the VM is deleted. So if new VM is created the user managed identity will get assigned and the app will still be authenticated.

upvoted 3 times

🗳️ 👤 **plmmsg** 3 years, 3 months ago

1. User Assigned Managed Identity

2. Metadata Service identity endpoint

upvoted 2 times

🗳️ 👤 **us3r** 3 years, 5 months ago

User-assigned managed IDENTITY (type I believe)

AZ instance metadata service OAuth2 endpoint

1) minimize admin effort

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/managed-identity-best-practice-recommendations#using-user-assigned-identities-to-reduce-administration>

2) you CANNOT create system-assigned MI, they are auto created.

System assigned Managed Identities are automatically created along with the Azure resource and the life cycle of the managed identity depends on the Azure resource.

3) ensure app can auth only with 10 VMs

the user-assigned MI will be associated only with the AZ resources (10 VMs).

Yes, you can associate with more resources, but you can also create a new VM and associate its automatically created system-assigned MI with AAD.

Case closed

upvoted 8 times



  **MARKMKENYA** 2 years, 4 months ago

You didnt explain the second part of the question - why Instance metadata service OAuth2 end point? Does it even exist?

The Azure Instance Metadata Service (IMDS) provides information about currently running virtual machine instances - and its not used to authenticcate.

<https://learn.microsoft.com/en-us/azure/virtual-machines/instance-metadata-service?tabs=windows>

upvoted 1 times

  **DonBoat** 3 years, 5 months ago

Box1: User-assigned: User assigned is sharable whilst system assigned is not. Thus will defeat the requirement that all VMs must run with same identity

Box2: Metadata service

upvoted 1 times

  **student22** 3 years, 8 months ago

1. User Assigned Managed Identity

2. Metadata Service identity endpoint (given answer)

upvoted 6 times

  **syu31svc** 3 years, 9 months ago

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/how-managed-identities-work-vm#user-assigned-managed-identity>

Your code that's running on the VM can request a token from the Azure Instance Metadata Service identity endpoint, accessible only from within the VM: <http://169.254.169.254/metadata/identity/oauth2/token>

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>

User-assigned You may also create a managed identity as a standalone Azure resource. You can create a user-assigned managed identity and assign it to one or more instances of an Azure service

User-assigned managed identities and OAuth2 are the answers

upvoted 2 times

  **nkx** 3 years, 9 months ago



Came in exam on 20-sep-21, i passed, answers are correct

upvoted 3 times

  **examineezer** 3 years, 6 months ago

Rubbish

upvoted 11 times

  **Gautam1985** 3 years, 10 months ago

Its should be user Assigned Managed Identity. Second question answer is correct.

upvoted 4 times

  **tehex** 3 years, 10 months ago

Guys, the hint is this the word "Only" >>> "...authenticate only when running on the 10 virtual machines.". With system-assigned managed identity it is tied to the VM you assign only. But with user-assigned managed identity you can add it to anywhere else.

upvoted 1 times

  **pentium75** 3 years, 10 months ago

"With system-assigned managed identity it is tied to the (!) VM you assign only" - exactly, there is a dedicated identity for EACH VM. But the requirement here is that all VMs must use "the same identity", thus system-assigned MI can't work.

upvoted 6 times

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains two administrative user accounts named Admin1 and Admin2.

You create two Azure virtual machines named VM1 and VM2.

You need to ensure that Admin1 and Admin2 are notified when more than five events are added to the security log of VM1 or VM2 during a period of 120 seconds.

The solution must minimize administrative tasks.

What should you create?

- A. two action groups and two alert rules
- B. one action group and one alert rule
- C. five action groups and one alert rule
- D. two action groups and one alert rule

**Suggested Answer: B**


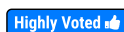
Community vote distribution

B (100%)

 **mmmore**  4 years, 6 months ago

Seems correct.

upvoted 34 times

 **alphamode**  4 years, 5 months ago

Option B is correct. An alert rule can have multiple VMs as target. Also mentioned here at Azure documentation:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-overview>

The following are key attributes of an alert rule:

Target Resource - Defines the scope and signals available for alerting. A target can be any Azure resource. Example targets:

Virtual machines.

Storage accounts.

Log Analytics workspace.

Application Insights.



For certain resources (like virtual machines), you can specify multiple resources as the target of the alert rule.

Also, as per another Azure documentation - Various alerts may use the same action group or different action groups depending on the user's requirements.

In Summary, you just need one 1 alert rule and 1 action group and thus option B seems to be correct.

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/action-groups>

upvoted 32 times

 **Testing6132**  2 years, 12 months ago

The answer is correct.

upvoted 1 times

 **Pinkee888** 3 years, 2 months ago

Presented answer is correct. One action group and one alert rule delivers the required solution with minimal administrative effort.

upvoted 1 times

 **moon2351** 3 years, 5 months ago

**Selected Answer: B**

Answer is B

upvoted 1 times

 **Eitant** 3 years, 6 months ago



Selected Answer: B

Correct answer  
upvoted 2 times

🗨️ **cfsxtuv33** 3 years, 7 months ago

Selected Answer: B

ehh, B sounds good  
upvoted 2 times

🗨️ **syu31svc** 3 years, 9 months ago

just one action group for the 2 administrators will do

B is correct  
upvoted 2 times

🗨️ **Gautam1985** 3 years, 10 months ago

correct  
upvoted 2 times

🗨️ **Oracleist** 4 years, 1 month ago

one action group can send email to multiple recipient.  
upvoted 4 times

🗨️ **AlokM** 4 years, 2 months ago

it'll just need 1 action group (can support multiple notifications for sending emails, per notification single email id) and 1 alert rule (can include multiple VMs in the resources section).. Thank you !  
upvoted 4 times

🗨️ **Blimpy** 4 years, 3 months ago

Im a bit confused as the question does not state that the two admins are part of an ARM role or that they belong to an email distribution group. An action group can only take one email address. In previous exams this would mean that one action group per email notification. In this case we have two admins , which means two action groups.. anyone else have any thoughts?  
upvoted 2 times

🗨️ **malyaban** 4 years, 3 months ago

I think D because one Alert Rule for VM1 or 2 but to send emails to Admin1 & 2 you need 2 action groups  
upvoted 1 times

🗨️ **malyaban** 4 years, 3 months ago

I stand corrected Answer is B :-) This is a cheeky one - remember you can always email one and send SMS the other at the same time for the same action group. Also now you can send multiple notifications for one action group.  
upvoted 1 times

🗨️ **examineezer** 3 years, 6 months ago

One action group can send emails to multiple people.  
upvoted 1 times

🗨️ **abhishek\_arya02** 4 years, 2 months ago

It also says "The solution must minimize administrative tasks." so that's why one action group  
upvoted 1 times

🗨️ **glam** 4 years, 5 months ago

B. one action group and one alert rule  
upvoted 4 times

🗨️ **milind8451** 4 years, 5 months ago

Seems right, you can choose 2 Vms in Scope of 1 Alert rule and then can put condition of security logs and then create an alert group to notify both admins.  
upvoted 2 times

🗨️ **MadEgg** 4 years, 5 months ago

I think we need two alert rules for each VM.  
Of course we can have one alert rule which triggers if there are more than five accumulated security events from VM1 and VM2. If doing so it would trigger if there are two alerts from VM1 and three from VM2 for example - I don't think that this is the requested solution.

We need two alert rules to trigger if there are five security events at VM1 or five security events at VM2 - in my opinion, that's the solution requested in the question.

upvoted 1 times

  **examineezer** 3 years, 6 months ago

Even if you were right - the only option with two alert rules says two action groups. You definitely do not need two action groups here.

upvoted 1 times

  **kopper2019** 4 years, 6 months ago

correct answer

upvoted 3 times

  **uzairahm007** 4 years, 6 months ago

would we not need a action rule for each VM?

upvoted 2 times

  **Elecktrus** 4 years, 6 months ago

Not, in the action rule you can define a filter that apply to both VM, for example a regexp with the machine name

upvoted 7 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains a group named Group1. Group1 contains all the administrative user accounts.

You discover several login attempts to the Azure portal from countries where administrative users do NOT work.

You need to ensure that all login attempts to the Azure portal from those countries require Azure Multi-Factor Authentication (MFA).

Solution: Create an Access Review for Group1.

Does this solution meet the goal?

A. Yes

B. No

**Suggested Answer: B**

Instead implement Azure AD Privileged Identity Management.

Note: Azure Active Directory (Azure AD) Privileged Identity Management (PIM) is a service that enables you to manage, control, and monitor access to important resources in your organization.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

Community vote distribution

B (100%)

  **shashu07**  4 years, 6 months ago

Enable Conditional Access Policy

upvoted 34 times

  **j888** 4 years, 3 months ago

I believed PIM is correct, as PIM main purpose is to restrict the admin access and it can as well forcing the requirement of MFA for Admin access. However, I do agree that if there is such a condition require for the unknown location to use MFA then this can be either conditional access (require p2 licence) or MFA service setting (you can place range of known IP addresses to not requiring IP add).

upvoted 2 times

  **yaiba** 4 years, 3 months ago

P1 can do Multi-Factor Authentication with Conditional Access too..

<https://azure.microsoft.com/en-us/pricing/details/active-directory/>

upvoted 4 times

  **KumarPV**  4 years, 6 months ago

Agreed

upvoted 8 times

  **bootless**  2 years, 10 months ago

Identity Protection with Conditional Access should work



upvoted 1 times

  **itengineerd** 3 years, 3 months ago

**Selected Answer: B**

No, access reviews don't get it done. There are several ways to enable MFA without needing PIM, tho!

upvoted 1 times

  **Dawn7** 3 years, 3 months ago

**Selected Answer: B**

Correct

upvoted 1 times

  **plmmsg** 3 years, 3 months ago

Answer is NO

upvoted 1 times

🗨️ 👤 **Dawn7** 3 years, 4 months ago

**Selected Answer: B**

I will go with NO.

upvoted 1 times

🗨️ 👤 **chichi0307** 3 years, 8 months ago

correct

a malicious actor getting access

an authorized user inadvertently impacting a sensitive resour

upvoted 1 times

🗨️ 👤 **syu31svc** 3 years, 9 months ago

Access reviews are used to access the memberships of users and groups defined in Azure AD

Answer is clearly No

upvoted 3 times

🗨️ 👤 **rajvelm** 4 years ago

Seems Y is correct answer

upvoted 1 times

🗨️ 👤 **mingled** 3 years, 10 months ago

lol... N (or B)

upvoted 2 times

🗨️ 👤 **erickim007** 4 years ago

The answer is 'Yes' as we need to use Azure AD Conditional Access. PIM is great tool that work against Azure AD Permission, Azure Subscription Role, RBAC Permission. PIM wouldn't be used for Azure AD resources (e.g. security group or Application).

Azure Management Configuration (i.e. allowed or not) can be completed in Azure AD User setting and MFA should be completed by Azure AD Conditional Access, and shouldn't be using PIM.

upvoted 1 times

🗨️ 👤 **pentium75** 3 years, 10 months ago

Yes, "we need to use Azure AD Conditional Access", but the suggestion solution here is "an Access Review", which does NOT meet the goal, thus the Answer is NO.

upvoted 5 times

🗨️ 👤 **glam** 4 years, 5 months ago

B. No .....

upvoted 3 times

🗨️ 👤 **airairo** 4 years, 5 months ago

came in the exam last month.

upvoted 3 times

🗨️ 👤 **kopper2019** 4 years, 6 months ago

Enable Conditional Access Policy as well

upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains a group named Group1. Group1 contains all the administrative user accounts.

You discover several login attempts to the Azure portal from countries where administrative users do NOT work.

You need to ensure that all login attempts to the Azure portal from those countries require Azure Multi-Factor Authentication (MFA).

Solution: Implement Azure AD Identity Protection for Group1.

Does this solution meet the goal?

A. Yes

B. No

#### Suggested Answer: B

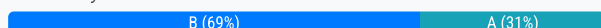
Implement Azure AD Privileged Identity Management for everyone.

Note: Azure Active Directory (Azure AD) Privileged Identity Management (PIM) is a service that enables you to manage, control, and monitor access to important resources in your organization.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

Community vote distribution



**Othermike** Highly Voted 4 years, 6 months ago

The answer is no , cause you can't make any rules in Identity protection to require MFA For Azure portal and you can't add the location either . I think we should use conditional access policy to solve this problem .. I am 100% sure that the answer is no  
upvoted 66 times

**Biden** 4 years ago

Answer is NO...MS recommends using Conditional Access policies for MFA: <https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa>  
upvoted 2 times

**esatu** 4 years, 5 months ago

MFA Registration Policy in Identity Protection can be used to require MFA. Risky sign-ins allows entering trusted IPs/Locations. You can check it in the portal. I think the answer is yes.  
upvoted 8 times

**cherry23** 3 years, 11 months ago

answer is Yes <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies>  
upvoted 5 times

**sjai** 3 years, 9 months ago

YES

"Configured trusted network locations are used by Identity Protection in some risk detections to reduce false positives."

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies>

upvoted 1 times

**nExoR** 4 years ago

the answer is YES <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies>  
upvoted 3 times

**idrisfl** Highly Voted 4 years, 7 months ago

I would have said Yes.

PIM is for access rights elevation, whereas Identity Protection is closely hooked to Conditional access for forcing MFA

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection#risk-detection-and-remediation>

upvoted 35 times

🗨️ 👤 **mmmore** 4 years, 6 months ago

Agreed

upvoted 1 times

🗨️ 👤 **heany** 4 years, 3 months ago

Agreed. Under identity protection -> report -> risky sign-in -> configure trusted IP, you can configure countries

upvoted 4 times

🗨️ 👤 **tteesstt** 3 years, 8 months ago

Report is just that, for reporting. It doesn't proactively do anything other than reporting.

upvoted 2 times

🗨️ 👤 **BoxGhost** 3 years, 10 months ago

But the suggestion here is to implement Identity Protection. If they have not configured identity protection yet then something else must be blocking the logins such as a CA policy blocking certain countries.

upvoted 1 times

🗨️ 👤 **mindtrax** 4 years, 4 months ago

Agreed the question is about identity protection and in their answer they refer to PIM, which is something different.

upvoted 3 times

🗨️ 👤 **silwal** Most Recent 2 years, 10 months ago

Answer is A

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies>

We can configure custom Conditional Access Policy under Identity Protection Policy

upvoted 2 times

🗨️ 👤 **Raj99** 2 years, 11 months ago

answer is Y, MFA can be enabled under Identity protection blade.

upvoted 1 times

🗨️ 👤 **sapien45** 3 years ago

Implement Azure AD Privileged Identity Management for everyone. = Identity Protection

Implement Azure AD Privileged Identity Management for Group1 = Conditional Access

No

upvoted 1 times

🗨️ 👤 **itenginerd** 3 years, 3 months ago

Selected Answer: B

You need to ensure that all login attempts to the Azure portal from those countries require Azure Multi-Factor Authentication (MFA).

Identity Protection does not enable MFA, it processes signals and identifies risk.

upvoted 2 times

🗨️ 👤 **exnaniantwort** 3 years, 3 months ago

Answer is NO

Identity Protection is a tool that allows 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 your SIEM.

The signals generated by and fed to Identity Protection, 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 based on your organization's enforced policies.

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection>

Conditional access is not included in Identity Protection

upvoted 1 times

🗨️ 👤 **JBS** 3 years, 3 months ago

Selected Answer: B

Alone IP doesn't work. It required conditional access policies to enable MFA

upvoted 1 times

🗨️ **Dawn7** 3 years, 3 months ago

**Selected Answer: B**

Correct

upvoted 1 times

🗨️ **PG4141** 3 years, 3 months ago

**Selected Answer: A**

Refer : <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection>

Identity Protection identifies risks of many types, including:

Anonymous IP address use

Atypical travel

Malware linked IP address

Unfamiliar sign-in properties

Leaked credentials

Password spray

and more...

The risk signals can trigger remediation efforts such as requiring users to: perform Azure AD Multi-Factor Authentication, reset their password using self-service password reset, or blocking until an administrator takes action.

upvoted 1 times

🗨️ **itengineerd** 3 years, 3 months ago

AIP generates and processes signals. It does not in and of itself enable MFA.

upvoted 1 times

🗨️ **catfood** 2 years, 10 months ago

Identity Protection | Sign-in risk policy - can set to a specific group of users, can require MFA but you can't specific a list of countries that the admins don't work from. It might learn that eventually, or realise that its impossible travel, but a conditional access policy would be a better option here

upvoted 1 times

🗨️ **plmmsg** 3 years, 3 months ago

**Selected Answer: B**

No. use conditional access policy

upvoted 1 times

🗨️ **Naqsh27** 3 years, 3 months ago

**Selected Answer: B**

The Answer is no.

the reference is <https://techcommunity.microsoft.com/t5/itops-talk-blog/what-s-the-difference-between-azure-active-directory-identity/ba-p/1320887>

But I have also implemented both AAD Identity protection and Conditional Access Policies.

AAD IP is an automated response to predefined signals that allows seamless mitigation and/or remediation of possible issues that cause them Conditional Access Policies allow you to target a Specific Group (Group 1 with all the admins) and set "rules" based on various options (some of which may include AAD IP risk levels). These conditional rules may allow or block access or be more refined by allowing access only if you meet certain criteria (MFA)

In AAD IP - the only thing you can set is the MFA registration policy which is a global setting but does not correlate to controlled access to any specific part of Azure Portal or App.

upvoted 2 times

🗨️ **depaul** 3 years, 3 months ago

**Selected Answer: B**

Not sure How people are confussed in this, this is a clear "NO".. you need to have conditional access for enforcing MFA

upvoted 1 times



🗨️ **arun** 3 years, 3 months ago

**Selected Answer: A**

I think 'Yes' is right answer. pls refer <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies#azure-ad-mfa-registration-policy>

Identity Protection can help organizations roll out Azure AD Multi-Factor Authentication (MFA) using a Conditional Access policy requiring registration at sign-in. Enabling this policy is a great way to ensure new users in your organization have registered for MFA on their first day

upvoted 2 times

  **S\_AB** 3 years, 4 months ago

**Selected Answer: B**

I think is Yes. Because you can config a policy to force MFA with Identity protection and you can define mfa and login from diferent country is a risk.

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies>



upvoted 1 times

  **Sistemas\_ASMWS** 3 years, 4 months ago

**Selected Answer: B**

I think Azure AD Identity Protection isn't the feature that gives you MFA.

upvoted 1 times

  **us3r** 3 years, 5 months ago

**Selected Answer: A**

read the question!

Several attempts have already be discovered!

So, Azure AD identity Protection is the answer.

YES

upvoted 2 times



Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains a group named Group1. Group1 contains all the administrative user accounts.

You discover several login attempts to the Azure portal from countries where administrative users do NOT work.

You need to ensure that all login attempts to the Azure portal from those countries require Azure Multi-Factor Authentication (MFA).

Solution: You implement an access package.

Does this meet the goal?

A. Yes

B. No

#### Suggested Answer: B

Instead implement Azure AD Privileged Identity Management.


Note: Azure Active Directory (Azure AD) Privileged Identity Management (PIM) is a service that enables you to manage, control, and monitor access to important resources in your organization.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

Community vote distribution

B (100%)

 **KumarPV** Highly Voted 4 years, 6 months ago

Agreed

upvoted 13 times

 **glam** Highly Voted 4 years, 5 months ago

B. No .....


upvoted 8 times

 **Dawn7** Most Recent 3 years, 3 months ago

Selected Answer: B

Clear NO

upvoted 1 times

 **Dawn7** 3 years, 3 months ago

Clear NO

upvoted 1 times

 **moon2351** 3 years, 5 months ago

Selected Answer: B

Answer is B

upvoted 2 times

 **syu31svc** 3 years, 9 months ago

<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-create>

An access package enables you to do a one-time setup of resources and policies that automatically administers access for the life of the access package

Answer is definitely No

upvoted 2 times

 **Viji30** 3 years, 10 months ago

what is the correct one?

upvoted 1 times

 **scottishstvao** 3 years, 9 months ago

As per discussion on the other questions.

The best approach to archive it is using the Conditional Acces.

But, some people said that using the Azure AD Identity Protection should help as well.



As per documentation, I think that it will help as well.

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection#risk-detection-and-remediation>  
upvoted 5 times

  **AB20101** 3 years, 4 months ago

Azure AD Identity Protection doesn't allow you select specific countries

upvoted 1 times

  **red\_vix** 3 years, 11 months ago

Correct

upvoted 1 times

## HOTSPOT -

Your company has the divisions shown in the following table.

Division	Azure subscription	Azure Active Directory (Azure AD) tenant
East	Sub1, Sub2	East.contoso.com
West	Sub3, Sub4	West.contoso.com

You plan to deploy a custom application to each subscription. The application will contain the following:

- ⇒ A resource group
- ⇒ An Azure web app

Custom role assignments -

- 
- ⇒ An Azure Cosmos DB account

You need to use Azure Blueprints to deploy the application to each subscription.

What is the minimum number of objects required to deploy the application? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Management groups:

1
2
3
4

Blueprint definitions:

1
2
3
4

Blueprint assignments:

1
2
3
4

### Answer Area

Management groups:

1
2
3
4

Blueprint definitions:

1
2
3
4

Blueprint assignments:

1
2
3
4

Suggested Answer:

Box 1: 2 -

One management group for East, and one for West.

When creating a blueprint definition, you'll define where the blueprint is saved. Blueprints can be saved to a management group or subscription that you have

Contributor access to. If the location is a management group, the blueprint is available to assign to any child subscription of that management group.

Box 2: 1 -

One definition as the you plan to deploy a custom application to each subscription.



With Azure Blueprints, the relationship between the blueprint definition (what should be deployed) and the blueprint assignment (what was deployed) is preserved.

Box 3: 4 -

One assignment for each subscription.

Reference:

<https://docs.microsoft.com/en-us/azure/governance/blueprints/overview>

 **devianter81**  4 years, 9 months ago

2,2,4

Management groups can't span AAD tenant, so you need 2 management groups. Blueprints definition can be saved within management group which, in turn, means you need 2 blueprint definitions.

Blueprint assignments are at subscription level, therefore you need 4.

upvoted 131 times

 **Arulkumar\_Subramaniam** 4 years, 8 months ago

When creating a blueprint definition, you'll define where the blueprint is saved. Blueprints can be saved to a management group or subscription that you have Contributor access to. So we will need at least 2 blueprint definitions

<https://docs.microsoft.com/en-us/azure/governance/blueprints/overview>

upvoted 5 times

 **temporal111** 4 years, 8 months ago

I think blueprint should be 1 due to the fact that you can create one for the first division, export it and finally you could import it into the second division

<https://docs.microsoft.com/en-us/azure/governance/blueprints/how-to/import-export-ps>

upvoted 5 times

 **KhabibcandefeatGSP** 4 years, 1 month ago

Correct answer is 2 2 2.

upvoted 18 times

🗨️ 👤 **Ajdifasudfo0** 3 years, 8 months ago

you also have to define the subscription in that process

"Assigning a blueprint definition to a management group means the assignment object exists at the management group. The deployment of artifacts still targets a subscription. To perform a management group assignment, the Create Or Update REST API must be used and the request body must include a value for properties.scope to define the target subscription."

upvoted 1 times

🗨️ 👤 **tita\_tovenaar** 3 years, 11 months ago

NO, answer is 2-2-4. See quote:

"Blueprints can be saved to a management group or subscription that you have Contributor access to. If the location is a management group, the blueprint is available to assign to any child subscription of that management group."

<https://docs.microsoft.com/en-us/azure/governance/blueprints/overview#blueprint-definition-locations>

upvoted 8 times

🗨️ 👤 **Azurefox79** 3 years, 6 months ago

Nope, read the full article bud. Each Published Version of a blueprint can be assigned (with a max name length of 90 characters) to an existing management group or subscription.

<https://docs.microsoft.com/en-us/azure/governance/blueprints/overview>

upvoted 3 times

🗨️ 👤 **RemonB** 3 years, 7 months ago

I agree with the text part, 2 mgmt groups, 1 blueprint stored 2 times on both management groups, and assigned 4 times to the subscription.

Only open question, is it 2-1-4 or 2-2-4. I'm not clear to what to choose.

upvoted 2 times

🗨️ 👤 **Nokaido** 3 years, 5 months ago

Since the blueprint is the same on both management groups I think 2-1-4 is correct.

upvoted 1 times

🗨️ 👤 **gssd4scoder** 4 years, 1 month ago

Why can't span AAD tenant? I can create tenants in my Visual Studio Subscription under the Root Management group that includes subscription of my org. Please explain

upvoted 1 times

🗨️ 👤 **tita\_tovenaar** 3 years, 11 months ago

Not sure what you did in VS (you might have created subdomains), but documentation is clear:

"Each directory is given a single top-level management group called the "Root" management group. This root management group is built into the hierarchy to have all management groups and subscriptions fold up to it."

<https://docs.microsoft.com/en-us/azure/governance/management-groups/overview#root-management-group-for-each-directory>

upvoted 1 times

🗨️ 👤 **Wis10** 4 years ago

Because there are two different tenants: east.contoso.com and west.contoso.com, each one with an Azure AD

upvoted 2 times

🗨️ 👤 **[Removed]** 3 years, 10 months ago

because tenant is top most object this hierarchy. Even root mgmt group comes under tenant. Each tenant has its own resources. BP is also one resource. and point here is, there are two tenant.

upvoted 1 times

🗨️ 👤 **GetulioJr** Highly Voted 👍 4 years ago

After giving a lot of though, I will go with the answer, you will need 2, 2 and 2.

You need 2 Management Groups as there is to AAD involved.

You need 2 Blueprint as you will need one definition in each root management group.

You need 2 Assignments as you can assign the blueprints to the root management group though the REST API.

Ref on root management group:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-management-groups>

"Each Azure AD tenant is given a single top-level management group called the root management group. This root management group is built into the hierarchy to have all management groups and subscriptions fold up to it. This group allows global policies and Azure role assignments to be applied at the directory level."

upvoted 32 times

  **yyuryyucicuryyforme** 3 years, 5 months ago

Each Blueprint assignment to (or perhaps via?) a management group must use the API, and must specify the one (sole) Subscription ID that the assignment applies to, using the 'properties.scope' string in the request body.

So Blueprint assignment is one per subscription, even assigned via management group.

See <https://docs.microsoft.com/en-us/rest/api/blueprints/assignments/create-or-update>

And search for properties.scope

Thus the answer is 2 2 4 regardless of assignment via management group level or assignment at subscription level.

upvoted 3 times

  **pabloartgal** Most Recent 2 years, 7 months ago

Assigning a blueprint definition to a management group means the assignment object exists at the management group. The deployment of artifacts still targets a subscription. To perform a management group assignment, the Create Or Update REST API must be used and the request body must include a value for properties.scope to define the target subscription.

Then the answer is correct.

box 1 = 2

box 2 = 1

box 3 = 4.

upvoted 1 times

  **Snownoodles** 2 years, 8 months ago



2-2-2

2 AAD, so 2 root MG

BP defs # = Root MG#, so it's BP defs # is 2

You can assign BP to Root MGs, so BP assignments # = 2

upvoted 1 times

  **AubinBakana** 2 years, 10 months ago

- 2 Management groups to separate regions

- 1 Blueprint Definition

- Assign that blueprint definition to each of the subscriptions. That's 4.

Answer is correct.

upvoted 2 times

  **AubinBakana** 2 years, 10 months ago

People should just be quiet if they are not sure about what they are doing instead of clogging the thread. The answer is correct.

upvoted 2 times

  **AubinBakana** 2 years, 10 months ago

People should just be quiet if they are not sure about what they are doing instead of clogging the thread. The answer is correct.

upvoted 1 times

  **manojchavan** 3 years, 1 month ago

Question is about "minimum number of objects required to deploy the application".

2 management groups one for tenant (can't have same across tenant)

2 Blueprint Objects (one definition but need two objects one for each tenant stored at management group level)

2 Blueprint assignments (since it can be assigned at Management group level, minimum 2 are required)

upvoted 1 times

  **Azure\_daemon** 3 years, 1 month ago

The correct answer is 2,1,2, the first two box is obvious the tricky one is the third box, which the given answer is wrong, it says the minimum number of object plus the published blueprint can be assigned either to a management group or a subscription, so in this case the number of assignments will be 2 (East and West management groups):

Blueprint assignment:

Each Published Version of a blueprint can be assigned (with a max name length of 90 characters) to an existing management group or subscription. In the portal, the blueprint defaults the Version to the one Published most recently. If there are artifact parameters or blueprint parameters, then the parameters are defined during the assignment process.

upvoted 1 times

🗨️ 👤 **AberdeenAngus** 3 years, 1 month ago

Must be 4 assignments, because the web app name is one of the parameters specified in the assignment, and web app names must be globally unique (unless we're deploying web apps into ASEs, and the question doesn't say this). We are deploying 4 web apps, 1 into each subscription, so 4 assignments.

A web site must have a globally unique URL. When you create a web site that uses a hosting plan, the URL is `http://<app-name>.azurewebsites.net`. The app name must be globally unique. <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/resource-name-rules#microsoftweb>  
upvoted 2 times

🗨️ 👤 **cwilson91** 3 years, 1 month ago

On AZ-305 exam - 5.7.22  
upvoted 3 times

🗨️ 👤 **cloudera** 3 years, 3 months ago

In my opinion, it should be:

2 Management groups,  
2 Blueprint Definitions - one definition for each management group which makes it 2) and  
2 blueprints assignment - blueprint assignments can be done at the Management or at the Subscription level. I will prefer to assign them at the management level rather than the subscription level so fewer admin tasks, also a minimum number of objects is what the question specifically asking.  
upvoted 1 times

🗨️ 👤 **itenginerd** 3 years, 3 months ago

On my exam today.  
upvoted 1 times

🗨️ 👤 **itenginerd** 3 years, 3 months ago

It's 2-2-4 for me. Blueprint definitions can be assigned to different mgmt groups or subs. But Azure has very few concepts for those assignments to cross tenant boundaries. Two tenants means two mgmt groups, two blueprint definitions (even if one's a copy of the other, they're still two separate definitions) and 4 assignments (one per sub).  
upvoted 1 times

🗨️ 👤 **HarryZ** 3 years, 3 months ago

should be 2,1,2  
design like this: one root subscription, under one root there are 2 management group (East and West), under each group there are two subscription. With this design, you have 2 mgr group, 1 blueprint stored at the root, then assign the blueprint to 2 mgr group. So, 2,1,2.  
upvoted 1 times

🗨️ 👤 **plmmsg** 3 years, 3 months ago

Answer is 2,2,2  
upvoted 1 times

🗨️ 👤 **BD1193** 3 years, 3 months ago

2 - because of diff tenant  
1- create BP for one MG, export/import to other MG  
2 - question mentions "assignment object", not assignment during deployment. BP assignment objects can exists at MG level (with REST API)  
upvoted 1 times

You have an Azure Active Directory (Azure AD) tenant.

You plan to deploy Azure Cosmos DB databases that will use the SQL API.

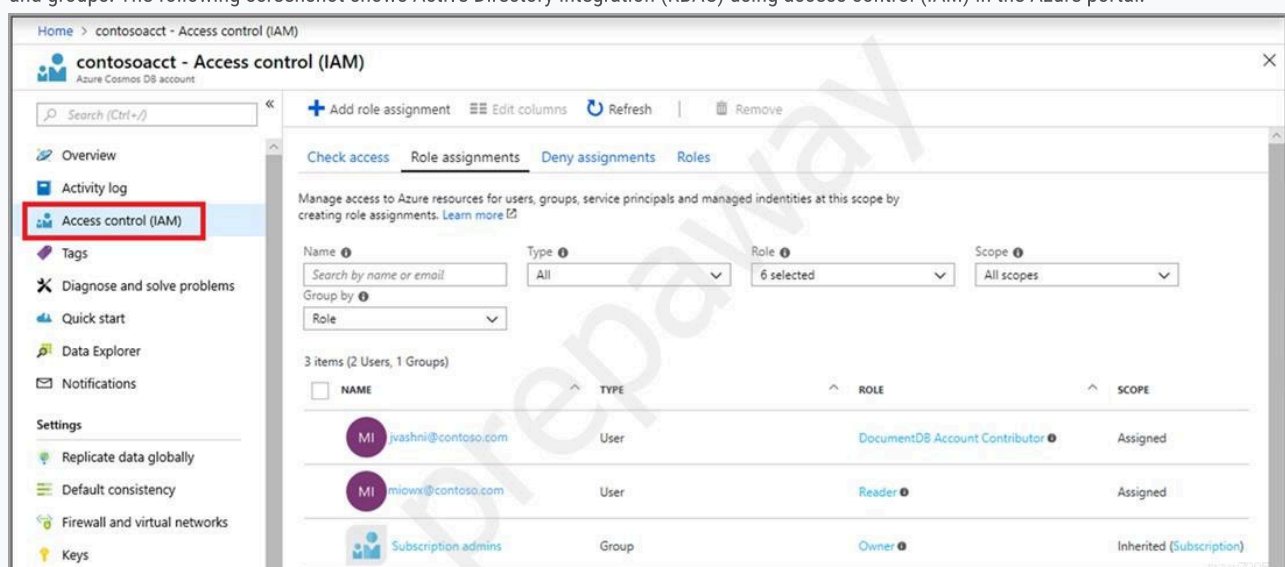
You need to recommend a solution to provide specific Azure AD user accounts with read access to the Cosmos DB databases.

What should you include in the recommendation?

- A. shared access signatures (SAS) and conditional access policies
- B. certificates and Azure Key Vault
- C. a resource token and an Access control (IAM) role assignment
- D. master keys and Azure Information Protection policies

#### Suggested Answer: C

The Access control (IAM) pane in the Azure portal is used to configure role-based access control on Azure Cosmos resources. The roles are applied to users, groups, service principals, and managed identities in Active Directory. You can use built-in roles or custom roles for individuals and groups. The following screenshot shows Active Directory integration (RBAC) using access control (IAM) in the Azure portal:



Reference:

<https://docs.microsoft.com/en-us/azure/cosmos-db/role-based-access-control>

Community vote distribution

C (100%)

**pattasana** Highly Voted 4 years, 6 months ago

Given answer is correct

upvoted 36 times

**sanketshah** 4 years, 5 months ago

given answer is correct.

upvoted 6 times

**Examerr** 3 years, 9 months ago

given answer is correct.

upvoted 3 times

**azurecert2021** Highly Voted 4 years, 4 months ago

given answer is correct.

You can use resource tokens to get access to the data in Azure Cosmos DB. And you can provide role-based access control to the users defined in Azure AD.

Azure Cosmos DB uses two types of keys to authenticate users and provide access to its data and resources.

Primary keys Used for administrative resources: database accounts, databases, users, and permissions

Resource tokens Used for application resources: containers, documents, attachments, stored procedures, triggers, and UDFs.

as here we read access to the Cosmos DB databases so we need use a hash resource token specifically constructed for the user, resource(database),



and permission(read).

assign Cosmos DB Account Reader Role to user through Access control (IAM) RBAC

<https://docs.microsoft.com/en-us/azure/cosmos-db/secure-access-to->



data#:~:text=Open%20the%20Azure%20portal%2C%20and,user%2C%20group%2C%20or%20application

upvoted 30 times

  **rdemontis** 3 years, 7 months ago

Thanks, very good explanation!

upvoted 1 times

  **leo\_az300** 3 years, 8 months ago


thanks for explanation, much better than simply saying "answer is correct"

upvoted 7 times

  **Jeanphi72** 3 years, 2 months ago

FYI: Outdated explanation see the link for more information

upvoted 1 times

  **OCHT**  3 years, 1 month ago

**Selected Answer: C**



Verified. Even , some URL explanations are outdated.

upvoted 1 times

  **cwilson91** 3 years, 1 month ago

On AZ-305 exam - 5.7.22



upvoted 3 times

  **Dawn7** 3 years, 3 months ago

**Selected Answer: C**

C seems correct

upvoted 1 times

  **Eitant** 3 years, 6 months ago

**Selected Answer: C**

Correct answer

upvoted 1 times

  **syu31svc** 3 years, 9 months ago

A shared access signature (SAS) is a URI that grants restricted access rights to Azure Storage resources -> This makes A wrong

B is completely irrelevant so it's wrong as well

Azure Information Protection (AIP) is a cloud-based solution that enables organizations to classify and protect documents and emails by applying labels. -> D is wrong as well

It can only be C as the answer

upvoted 4 times

  **Gautam1985** 3 years, 10 months ago

correct

upvoted 1 times

  **bbcZ** 4 years, 2 months ago



On Exam 05/01/2021

upvoted 6 times

  **cfsxtuv33** 3 years, 11 months ago


On exam...good to know...what answer did you pick?????

upvoted 1 times

  **Vipsao** 4 years, 3 months ago



The answer is correct

upvoted 2 times

  **glam** 4 years, 5 months ago

C. a resource token and an Access control (IAM) role assignment

upvoted 1 times

  **Blaaa** 4 years, 5 months ago

C is correct

upvoted 1 times

  **peacegrace** 4 years, 6 months ago

Answer should be correct based on this :

[https://docs.microsoft.com/en-us/azure/cosmos-db/secure-access-to-](https://docs.microsoft.com/en-us/azure/cosmos-db/secure-access-to-data#:~:text=Open%20the%20Azure%20portal%2C%20and,user%2C%20group%2C%20or%20application.)

[data#:~:text=Open%20the%20Azure%20portal%2C%20and,user%2C%20group%2C%20or%20application.](https://docs.microsoft.com/en-us/azure/cosmos-db/secure-access-to-data#:~:text=Open%20the%20Azure%20portal%2C%20and,user%2C%20group%2C%20or%20application.)

upvoted 1 times

  **anandpsg101** 4 years, 6 months ago

Correct answer

upvoted 3 times

You deploy an Azure virtual machine that runs an ASP.NET application. The application will be accessed from the internet by the users at your company.

You need to recommend a solution to ensure that the users are pre-authenticated by using their Azure Active Directory (Azure AD) account before they can connect to the ASP.NET application.

What should you include in the recommendation?

- A. a public Azure Load Balancer
- B. Azure Application Gateway
- C. Azure Traffic Manager
- D. an Azure AD enterprise application

**Suggested Answer: D**



You can manage service principals in the Azure portal through the Enterprise Applications experience. Service principals are what govern an application connecting to Azure AD and can be considered the instance of the application in your directory.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added>

Community vote distribution

D (100%)

  **dadageer** Highly Voted 4 years, 2 months ago

none of the other three answers made sense so I was left with D.

upvoted 30 times

  **LT** Highly Voted 4 years, 1 month ago

D is the answer.. No brainer. Other options are completely irrelevant.

upvoted 14 times

  **dasEnder** Most Recent 3 years, 1 month ago



But how this is enforced? The application should then add the enforcement?!

upvoted 1 times

  **Azure\_daemon** 3 years, 1 month ago

The first 3 answers are totally irrelevant to the question, and D is the correct answer, I wish all the AZ exam questions was that easy

upvoted 2 times

  **Teringzooi** 3 years, 1 month ago

Selected Answer: D

Correct answer: D

leo\_az300 6 months, 4 weeks ago

The solution is to pre-authenticate user with AZURE AD account, then they can connect web app in azure. This makes sense to use service principal.

You can manage service principals in the Azure portal through the Enterprise Applications experience.

upvoted 1 times

  **[Removed]** 3 years, 5 months ago

Selected Answer: D


Only D can do authentication. Others are Load Balancers.

upvoted 2 times

  **examineezer** 3 years, 6 months ago

From what I can gather, Enterprise applications are essentially Service Principals, which are instances of Application Objects, and can include definitions of role assignments.

upvoted 2 times

  **parkranger** 3 years, 8 months ago

Main reason for Enterprise application usage -

Applications have been able to leverage Windows Server Active Directory for user authentication for many years without requiring the application to be registered or recorded in the directory. Now the organization will have improved visibility to exactly how many applications are using the directory and for what purpose.

upvoted 3 times

🗨️ 👤 **leo\_az300** 3 years, 8 months ago

The solution is to pre-authenticate user with AZURE AD account, then they can connect web app in azure. This makes sense to use service principal.

You can manage service principals in the Azure portal through the Enterprise Applications experience. So D is correct

upvoted 3 times

🗨️ 👤 **syu31svc** 3 years, 9 months ago

Key here is "pre-authenticated" so answer is D

upvoted 1 times

🗨️ 👤 **Gautam1985** 3 years, 10 months ago

correct

upvoted 1 times

🗨️ 👤 **AdityaGupta** 3 years, 10 months ago

Can I not manage authentication with Application Gateway by using certificates?

upvoted 1 times

🗨️ 👤 **pentium75** 3 years, 10 months ago

I don't think so. APPGW can proxy authentication requests between client and backend. But I'm not aware of a function that you authenticate to APPGW and THEN you can access the application behind it.

upvoted 1 times

🗨️ 👤 **Vipsao** 4 years, 3 months ago

The answer is correct

upvoted 5 times

🗨️ 👤 **securitynija** 4 years, 3 months ago

correct

upvoted 4 times

## HOTSPOT -



You have an Azure blueprint named BP1.

The properties of BP1 are shown in the Properties exhibit. (Click the Properties tab.)

[All services](#) > [Blueprints](#) | [Blueprint definitions](#) >

**BP1**

Blueprints

 Publish Blueprint  Edit Blueprint  Delete Blueprint

Name : BP1  State : Draft  
Definition location : All PAYG Subscriptions Description: Assigns policies to address specific recommendations from the Azure Security Benchmark.  
Definition location ID : 

Version : Draft

The basic configuration of the blueprint is shown in the Basics exhibit. (Click the Basics tab.)


## Edit blueprint

**Basics** [Artifacts](#)

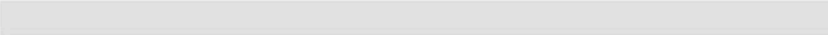

Blueprint name 

BP1

Blueprint description

Assigns policies to address specific recommendations from the Azure Security Benchmark. 

Definition location  




 

The management group or subscription where the blueprint is saved. The definition location determines the scope that the blueprint may be assigned to. Learn more at [aka.ms/BlueLocation](https://aka.ms/BlueLocation).

The artifacts attached to BP1 are shown in the Artifacts exhibit. (Click the Artifacts tab.)

[Basics](#) **Artifacts**

Add artifacts to the blueprint. Add resource groups to organize where the artifacts should be deployed and assigned.

NAME	ARTIFACT TYPE	PARAMETERS
 Subscription		
 Audit Azure Security Benchmark recommendations and deploy specific supporting VM Extensions	Policy assignment	0 out of 12 parameters populated
 Add artifact...		
 Database Resource Group		
	Resource group	0 out of 2 parameters populated
 Add artifact...		

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 assign BP1 in its current state.	<input type="radio"/>	<input type="radio"/>
BP1 has a role assignment defined.	<input type="radio"/>	<input type="radio"/>
When BP1 is assigned, you will need to provide a resource group name.	<input type="radio"/>	<input type="radio"/>

Suggested Answer:

## Answer Area

Statements	Yes	No
You can assign BP1 in its current state.	<input type="radio"/>	<input checked="" type="radio"/>
BP1 has a role assignment defined.	<input type="radio"/>	<input checked="" type="radio"/>
When BP1 is assigned, you will need to provide a resource group name.	<input checked="" type="radio"/>	<input type="radio"/>

Box 1: No -

BP1 is in draft mode.

When a blueprint is first created, it's considered to be in Draft mode. When it's ready to be assigned, it needs to be Published.

Box 2: No -

The BP1 artifacts include one Policy assignment and a Resource group, but no Role assignments.

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

Role Assignments -

Policy Assignments -

Azure Resource Manager templates (ARM templates)

Resource Groups -

Box 3: Yes -

Yes, the BP1 artifacts include a Resource group.


Reference:

<https://docs.microsoft.com/en-us/azure/governance/blueprints/overview>

 **Krsto** Highly Voted 4 years, 1 month ago

Answer is correct

upvoted 27 times

 **syu31svc** Highly Voted 3 years, 9 months ago

<https://docs.microsoft.com/en-us/azure/governance/blueprints/overview>

When a blueprint is first created, it's considered to be in Draft mode. When it's ready to be assigned, it needs to be Published

Assign BP1 is No

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

Role Assignments  
Policy Assignments  
Azure Resource Manager templates (ARM templates)  
Resource Groups

No role assignment seen so BP1 role assignment defined is No

0 parameters defined for resource group so need to provide RG name is Yes

N N Y

upvoted 22 times

🗨️ 👤 **Dpejic** Most Recent 3 years, 6 months ago

On exam 24.12.2021

upvoted 4 times

🗨️ 👤 **Dpejic** 3 years, 6 months ago

Appere on exam 23-dec-2021

upvoted 4 times

🗨️ 👤 **dkltruong88** 3 years, 9 months ago

Was in exam today 1-10-2021. I passed with score 896. I chose provided answer

upvoted 6 times

🗨️ 👤 **kumarts** 3 years, 11 months ago

Blue print needs a resource group name but the question in 3 is BP1 which cannot be assigned in its current state

upvoted 1 times

🗨️ 👤 **kumarts** 3 years, 11 months ago

When you say BP cannot be assigned in its current state in 1, 3 should be definitely No

upvoted 2 times

🗨️ 👤 **pentium75** 3 years, 10 months ago

But contrary to question 1, question 3 does not mention the "current state". IF you assign this BP (later when it's not a draft anymore), THEN it asks for RG name because it contains an RG that does not have any parameters (thus also no name) specified.

upvoted 3 times

🗨️ 👤 **examineezer** 3 years, 6 months ago

My thoughts exactly.

upvoted 2 times

🗨️ 👤 **Hank\_Qin** 4 years ago

3 should No:

Each Published Version of a blueprint can be assigned (with a max name length of 90 characters) to an existing management group or subscription.

upvoted 1 times

🗨️ 👤 **keilah123** 4 years ago

You need to read the question again. It's asking about the Resource Group artifact. Since 0 out of 2 parameter are populated, the resource group name is missing, hence you need to provide it during the assignment. You better try it so you can understand better.

upvoted 2 times

🗨️ 👤 **Hank\_Qin** 4 years ago

Should be Y Y N. According to <https://docs.microsoft.com/en-us/azure/governance/blueprints/overview>. For item 2, blueprint definition can have role assignment. For item 3, Each Published Version of a blueprint can be assigned (with a max name length of 90 characters) to an existing management group or subscription. Not resource group.

upvoted 1 times

🗨️ 👤 **Amit3** 4 years ago

Blueprint BP1 is in Draft state, so how can it be assigned ?. Answer should be N.



upvoted 2 times

🗨️ 👤 **jr\_luciano** 3 years, 4 months ago

The question is asking WHEN it will be assigned, that is, at some point it will be assigned, which obviously will be after the BP is published.



Should be NNY

upvoted 1 times

  **teehex** 3 years, 10 months ago



Lol where is role assignment in the BP? Please show me. I can only see Azure Policy assignment + Resource Group

upvoted 2 times

  **OCHT** 3 years, 1 month ago

It's NNY . At least , BP1 is in draft.

upvoted 1 times

  **bbc** 4 years, 2 months ago

On Exam 05/01/2021

upvoted 12 times



Your company wants to use an Azure Active Directory (Azure AD) hybrid identity solution.

You need to ensure that users can authenticate if the internet connection to the on-premises Active Directory is unavailable. The solution must minimize authentication prompts for the users.

What should you include in the solution?

- A. password hash synchronization and Azure AD Seamless Single Sign-On (Azure AD Seamless SSO)
- B. pass-through authentication and Azure AD Seamless Single Sign-On (Azure AD Seamless SSO)
- C. an Active Directory Federation Services (AD FS) server

**Suggested Answer: A**

With Password hash synchronization + Seamless SSO the authentication is in the cloud.

Incorrect Answers:

Pass-through Authentication and federation rely on on-premises infrastructure.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn>

Community vote distribution

A (100%)

 **Debleenac** Highly Voted 4 years, 3 months ago

Correct answer

upvoted 34 times

 **Santosh43** Highly Voted 4 years, 3 months ago

With password hash sync and seamless single sign on it will first try to use kerberos against your on prem infrastructure. If that is offline or you are outside the office, you will be able to enter your password to access the services. With adfs or pass through auth, you are offline if the on prem service is offline.

upvoted 31 times

 **One111** Most Recent 2 years, 10 months ago

PHS will allow to authenticate to cloud resources with or without onprem internet connectivity. PtA always require onprem (AADG server or other member server with PtA agent to be up, running and communicating with Azure).

Correct answer is PtA.

upvoted 1 times

 **teyo151117** 3 years, 3 months ago

On exam 31.03.2022

upvoted 3 times

 **iwuehfkj3** 3 years, 6 months ago

Selected Answer: A

correct

upvoted 2 times

 **bluewaves** 3 years, 6 months ago

Selected Answer: A

Answer is correct

upvoted 3 times

 **syu31svc** 3 years, 9 months ago

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn#comparing-methods>

What are the requirements for on-premises Internet and networking beyond the provisioning system? -> shows "None" for Password hash synchronization + Seamless SSO

Answer is correct

upvoted 3 times

🗨️ 👤 **tita\_tovenaar** 3 years, 11 months ago

It's A or B depending on how you read the question. If you read it as "users must still be able to authenticate IN AZURE if internet ..." then it's A. If you rather read it as "on-prem users must be able to authenticate if internet ..." then it's B.

This question is like the picture of the old woman/young girl, if you see one version it's difficult to see the other. Since the company doesn't have AAD yet, I assume we're in scenario B: users are still mainly on-prem, and a connection between AAD and on-prem AD must not complicate authentication if internet is down.

upvoted 2 times

🗨️ 👤 **pentium75** 3 years, 10 months ago

The whole exam is about Azure. So if it says "users must be able to authenticate", then this is about authenticating to Azure.

upvoted 5 times

🗨️ 👤 **tvs2021** 3 years, 11 months ago

on Exam (7-19-2021). passed 304 exam

upvoted 3 times

🗨️ 👤 **BenWat** 3 years, 11 months ago

This shows the importance of reading the question "if the internet connection to the on-premises Active Directory is unavailable". I originally read it as if users were on prem with the AD and the risk was the internet connection to AAD might be lost. Doh.

upvoted 4 times

🗨️ 👤 **examineezer** 3 years, 8 months ago

Me too

upvoted 2 times

🗨️ 👤 **GetulioJr** 4 years ago

Answer is correct.:

You need to ensure that users can authenticate if the internet connection TO THE on-premises Active Directory is unavailable

If there is no internet in On-Premises the other two methods will not work, but he can still sign-in through Azure with first method.

upvoted 4 times

🗨️ 👤 **AMMANANA** 4 years, 1 month ago

Ans: B

Pass through

Explanation

Since here users should still be able to authenticate even if the internet connection is not available, you must use Pass-through authentication. This would ensure users are authenticated via the on-premises Active Directory setup.

upvoted 1 times

🗨️ 👤 **modiallo** 3 years, 11 months ago

Ans is A:

Azure AD Pass-through Authentication. Provides a simple password validation for Azure AD authentication services by using a software agent that \*\*runs on one or more on-premises servers\*\*. The servers validate the users directly with your on-premises Active Directory, which ensures that the password validation doesn't happen in the cloud.

upvoted 1 times

🗨️ 👤 **Rume** 4 years, 1 month ago

Correct Answer is Password Hash Sync...

Refer: <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn>

scroll down to "Comparing Methods"

upvoted 1 times

🗨️ 👤 **ashishg2105** 4 years, 1 month ago

Incorrect Answer. Answer is B.

Since here users should still be able to authenticate even if the internet connection is not available, you must use Pass-through authentication. This would ensure users are authenticated via the on-premises Active Directory setup.

upvoted 2 times


🗨️ 👤 **modiallo** 3 years, 11 months ago

Ans is A:

Azure AD Pass-through Authentication. Provides a simple password validation for Azure AD authentication services by using a software agent that



**\*\*runs on one or more on-premises servers\*\***. The servers validate the users directly with your on-premises Active Directory, which ensures that the password validation doesn't happen in the cloud.

upvoted 1 times

  **bbc** 4 years, 2 months ago

On Exam 05/01/2021

upvoted 3 times

  **Stan007** 4 years, 3 months ago

it should be

B. pass-through authentication and Azure AD Seamless Single Sign-On (Azure AD Seamless SSO)

Explanation



Since here users should still be able to authenticate even if the internet connection is not available, you must use Pass-through authentication. This would ensure users are authenticated via the on-premises Active Directory setup.

upvoted 6 times

  **Montrealcupid** 4 years, 3 months ago



disagree, if the internet connection to the on-premises Active Directory is unavailable, user still need to be able to authenticate with AAD, they have no means to connect to on-prem, pass-through won't work

upvoted 20 times

  **AustinY** 4 years, 3 months ago

PT uses on-premises components.

upvoted 3 times

  **modiallo** 3 years, 11 months ago

Ans is A:

Azure AD Pass-through Authentication. Provides a simple password validation for Azure AD authentication services by using a software agent that **\*\*runs on one or more on-premises servers\*\***. The servers validate the users directly with your on-premises Active Directory, which ensures that the password validation doesn't happen in the cloud.

upvoted 1 times

## HOTSPOT -

You need to design an Azure policy that will implement the following functionality:

- ⇒ For new resources, assign tags and values that match the tags and values of the resource group to which the resources are deployed.
- ⇒ For existing resources, identify whether the tags and values match the tags and values of the resource group that contains the resources.
- ⇒ For any non-compliant resources, trigger auto-generated remediation tasks to create missing tags and values.

The solution must use the principle of least privilege.

What should you include in the design? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Azure Policy effect to use:

Append
EnforceOPAConstraint
EnforceRegoPolicy
Modify

Azure Active Directory (Azure AD) object and RBAC role to use for the remediation tasks:

A managed identity with the Contributor role
A managed identity with the User Access Administrator role
A service principal with the Contributor role
A service principal with the User Access Administrator role

### Suggested Answer:

#### Answer Area

Azure Policy effect to use:

Append
EnforceOPAConstraint
EnforceRegoPolicy
Modify

Azure Active Directory (Azure AD) object and RBAC role to use for the remediation tasks:

A managed identity with the Contributor role
A managed identity with the User Access Administrator role
A service principal with the Contributor role
A service principal with the User Access Administrator role

#### Box 1: Modify -

Modify is used to add, update, or remove properties or tags on a resource during creation or update. A common example is updating tags on resources such as costCenter. Existing non-compliant resources can be remediated with a remediation task. A single Modify rule can have any number of operations.

Incorrect Answers:

- ⇒ The following effects are deprecated: EnforceOPAConstraint, EnforceRegoPolicy
- ⇒ Append is used to add additional fields to the requested resource during creation or update. A common example is specifying allowed IPs for a storage resource.

#### Box 2: A managed identity with the Contributor role

- ⇒ Managed identity

How remediation security works: When Azure Policy runs the template in the deployIfNotExists policy definition, it does so using a managed identity. Azure

Policy creates a managed identity for each assignment, but must have details about what roles to grant the managed identity.

- ⇒ Contributor role

The Contributor role grants the required access to apply tags to any entity.

Reference:

<https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects> <https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects>

🗲️ 👤 **hkmikemak** Highly Voted 👍 4 years, 2 months ago  
Correct: Modify

<https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects#modify>  
remediation task is only mention in MODIFY section, not in APPEND section  
upvoted 30 times

🗲️ 👤 **TOM1000** Highly Voted 👍 4 years, 2 months ago  
Append is intended for use with non-tag properties. While Append can add tags to a resource during a create or update request, it's recommended to use the Modify effect for tags instead. so answers provided are correct.  
upvoted 7 times

🗲️ 👤 **tim\_27\_us** Most Recent 🕒 2 years, 8 months ago  
Box1: Modify  
Box 2: Contributor role  
upvoted 1 times

🗲️ 👤 **Teringzooi** 3 years, 1 month ago  
Today in AZ-305 exam. I picked these.  
Passed.  
upvoted 4 times

🗲️ 👤 **IndrasenR** 3 years, 3 months ago  
This came in 305 on 25-Mar-2022  
upvoted 6 times

🗲️ 👤 **plmmsg** 3 years, 3 months ago  
answer is correct  
upvoted 2 times

🗲️ 👤 **Dpejic** 3 years, 6 months ago  
Appere on exam 23-dec-2021  
upvoted 3 times

🗲️ 👤 **syu31svc** 3 years, 9 months ago  
<https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects#modify>

Modify is used to add, update, or remove properties or tags on a subscription or resource during creation or update. A common example is updating tags on resources such as costCenter. Existing non-compliant resources can be remediated with a remediation task. A single Modify rule can have any number of operations.

1st Drop down is Modify

least privilege so 2nd drop down is managed identity with contributor role  
upvoted 3 times

🗲️ 👤 **OCHT** 3 years, 1 month ago  
I have seen this on AZ-104 . Correct answer.  
upvoted 1 times



🗲️ 👤 **dkltruong88** 3 years, 9 months ago  
Was in exam today 1-10-2021. I passed with score 896. I chose provided answer  
upvoted 3 times

🗲️ 👤 **JavaTechi** 3 years, 10 months ago  
provided answer is correct. Why Modify? Existing non-compliant resources can be remediated. As per the question, remediation is expected for existing resources.

As per the the documentation here: <https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects>



EnforceOPAConstraint & EnforceRegoPolicy is deprecated

upvoted 2 times

  **gssd4scoder** 4 years, 1 month ago


Given answers are correct

upvoted 2 times

  **fromage** 4 years, 2 months ago

Append looks enough for me.

upvoted 3 times



  **examineezer** 3 years, 6 months ago

"Append is intended for use with non-tag properties. While Append can add tags to a resource during a create or update request, it's recommended to use the Modify effect for tags instead."

<https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects>

What "should" you include.... you should follow Microsoft's advice and choose Modify.

upvoted 1 times

  **securitynija** 4 years, 3 months ago

correct

upvoted 3 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. Your company has an on-premises Active Directory Domain Services (AD DS) domain and an established Azure Active Directory (Azure AD) environment.

Your company would like users to be automatically signed in to cloud apps when they are on their corporate desktops that are connected to the corporate network.

You need to enable single sign-on (SSO) for company users.

Solution: Install and configure an Azure AD Connect server to use password hash synchronization and select the `Enable single sign-on` option.

Does the solution meet the goal?

A. Yes

B. No

#### Suggested Answer: A

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

Seamless SSO can be combined with either the Password Hash Synchronization or Pass-through Authentication sign-in methods.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-ss0>

Community vote distribution

A (100%)

🗳️ **Enforcer** Highly Voted 4 years, 3 months ago

Correct!

upvoted 19 times

🗳️ **sharepoint\_Azure\_pp** Highly Voted 3 years, 8 months ago

this was there is 1st set of 3 Y/N question

if asked from cloud side then: Password hash synchronization is correct

If asked from on premise side: Pass-through Authentication is correct

Clear with 900 on 17th october 2021

upvoted 18 times

🗳️ **wooyourdaddy** 3 years, 6 months ago

Aces, don't hear or see this much, simple explanation and correct !! We need more of you on these sites!!

upvoted 3 times

🗳️ **Eitant** Most Recent 3 years, 6 months ago

Selected Answer: A

Correct answer

upvoted 2 times

🗳️ **syu31svc** 3 years, 9 months ago

Provided link supports answer as Yes

upvoted 2 times

🗳️ **dkltruong88** 3 years, 9 months ago

Was in exam today 1-10-2021. I passed with score 896. I chose Yes

upvoted 5 times

🗳️ **nkV** 3 years, 9 months ago



Came in exam on 20-sep-21, i passed, answers are correct

upvoted 3 times

🗳️ **ts2021** 3 years, 11 months ago

on exam (7-19-2021). passed 304

upvoted 5 times

  **DannyGupta** 4 years, 1 month ago

Yee eeee

upvoted 4 times



Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. Your company has an on-premises Active Directory Domain Services (AD DS) domain and an established Azure Active Directory (Azure AD) environment.

Your company would like users to be automatically signed in to cloud apps when they are on their corporate desktops that are connected to the corporate network.

You need to enable single sign-on (SSO) for company users.

Solution: Install and configure an Azure AD Connect server to use pass-through authentication and select the `Enable single sign-on` option.

Does the solution meet the goal?

A. Yes

B. No


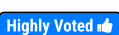
**Suggested Answer: A**

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

Seamless SSO can be combined with either the Password Hash Synchronization or Pass-through Authentication sign-in methods.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso>

 **Enforcer**  4 years, 3 months ago

Correct!

upvoted 15 times

 **temprao123**  4 years ago

Given answer is correct. Seamless SSO can be combined with either the Password Hash Synchronization or Pass-through Authentication sign-in methods



<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso>

upvoted 11 times

 **17Master** 3 years, 4 months ago

correcto.

upvoted 1 times

 **Kent\_020**  3 years, 1 month ago

This question is the same as this one:

<https://www.examttopics.com/exams/microsoft/az-304/view/48/>

upvoted 1 times

 **Kent\_020** 3 years, 1 month ago

This question is the same as this one:

<https://www.examttopics.com/exams/microsoft/az-304/view/49/>

upvoted 1 times

 **plmmsg** 3 years, 3 months ago

Pass-through

upvoted 1 times

 **sharepoint\_Azure\_pp** 3 years, 8 months ago

this was there is 1st set of 3 Y/N question

if asked from cloud side then: Password hash synchronization is correct

If asked from on premise side:Pass-through Authentication is correct

Clear with 900 on 17th october 2021

upvoted 8 times

🗨️ 👤 **dkltruong88** 3 years, 9 months ago

Was in exam today 1-10-2021. I passed with score 896. I chose Yes  
upvoted 5 times

🗨️ 👤 **syu31svc** 3 years, 9 months ago

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta>

You can combine Pass-through Authentication with the Seamless Single Sign-On feature

Answer is Yes

upvoted 2 times

🗨️ 👤 **nkx** 3 years, 9 months ago

Came in exam on 20-sep-21, i passed, answers are correct  
upvoted 2 times

🗨️ 👤 **tvS2021** 3 years, 11 months ago

passed 304. on exam (7-19-2021)  
upvoted 2 times

🗨️ 👤 **cfsxtuv33** 3 years, 11 months ago

Congrats...so what's the answer?????????  
upvoted 2 times

🗨️ 👤 **sreejit4u2003** 4 years ago

Should be no..It should be pwd hash sync and sso  
upvoted 1 times

🗨️ 👤 **Amit3** 4 years ago

That's what Azure AD Connect Server facilitates. So Answer is YES.  
upvoted 3 times

🗨️ 👤 **securitynija** 4 years, 3 months ago

correct  
upvoted 4 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. Your company has an on-premises Active Directory Domain Services (AD DS) domain and an established Azure Active Directory (Azure AD) environment.

Your company would like users to be automatically signed in to cloud apps when they are on their corporate desktops that are connected to the corporate network.

You need to enable single sign-on (SSO) for company users.

Solution: Configure an AD DS server in an Azure virtual machine (VM). Configure bidirectional replication.

Does the solution meet the goal?

A. Yes

B. No

**Suggested Answer: B**

Instead install and configure an Azure AD Connect server.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso>

  **Vipsao**  4 years, 3 months ago




Yes, The answers is correct, it is No

upvoted 11 times

  **msidy2020** 3 years, 11 months ago

Appreciate if you can just give "YES" or "No". it further makes discussion confusing

upvoted 18 times

  **dkltruong88**  3 years, 9 months ago

Was in exam today 1-10-2021. I passed with score 896. I chose No

upvoted 7 times

  **Kamo\_**  3 years, 3 months ago

insult

upvoted 1 times

  **sharepoint\_Azure\_pp** 3 years, 8 months ago

this was there is 1st set of 3 Y/N question

if asked from cloud side then: Password hash synchronization is correct

If asked from on premise side:Pass-through Authentication is correct

Clear with 900 on 17th october 2021

upvoted 3 times

  **syu31svc** 3 years, 9 months ago

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso>

Answer is No

upvoted 4 times

  **DragonsGav** 4 years ago

No should be the answer.

upvoted 4 times

  **Cluster007** 4 years, 3 months ago

Correct

upvoted 4 times

You are designing an Azure web app that will use Azure Active Directory (Azure AD) for authentication.

You need to recommend a solution to provide users from multiple Azure AD tenants with access to App1. The solution must ensure that the users use Azure Multi-

Factor Authentication (MFA) when they connect to App1.

Which two types of objects should you include in the recommendation? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Azure AD conditional access policies
- B. Azure AD managed identities
- C. an Identity Experience Framework policy
- D. an Azure application security group
- E. an Endpoint Manager app protection policy
- F. Azure AD guest accounts

**Suggested Answer: AF**

A: The Conditional Access feature in Azure Active Directory (Azure AD) offers one of several ways that you can use to secure your app and protect a service.

Conditional Access enables developers and enterprise customers to protect services in a multitude of ways including:

- ⇒ Multi-factor authentication
- ⇒ Allowing only Intune enrolled devices to access specific services
- ⇒ Restricting user locations and IP ranges

Conditional Access policies are powerful tools, we recommend excluding the following accounts from your policy:

- ⇒ Service accounts and service principals.

If your organization has these accounts in use in scripts or code, consider replacing them with managed identities.

Incorrect Answers:

B: Managed Identity does not support cross-directory scenarios.

E: Application security groups enable you to configure network security as a natural extension of an application's structure, allowing you to group virtual machines and define network security policies based on those groups.


Note: The correct options should be application registration with Azure, this will allow the authentication of users on the AD to access the application. A default application registration validates that the user has valid login credentials. This can be your Active Directory or in case of a multi-tenant application the directory where the user is originated from.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-conditional-access-dev-guide> <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-azure-management> <https://www.re-markable.net/understanding-azure-active-directory-application-registrations/>

Community vote distribution

AF (100%)

 **sallymaher** Highly Voted 4 years, 3 months ago

Correct answer is A and F, Managed identity for resources, you need to allow other users from other tenant to use your resources and apply conditional access, so you will use guest account ( B2b ) and conditional access

upvoted 87 times

 **stephw** 4 years, 1 month ago

Indeed. In Conditional Access the App will be represented as a service principal ... not as a managed identity ;)

=> agreed: A/F

upvoted 6 times

 **glam** Highly Voted 4 years, 3 months ago

A. Azure AD conditional access policies

F. Azure AD guest accounts

upvoted 28 times

 **totalz** Most Recent 2 years, 3 months ago

Even though F is correct, but have u seen what have to be done to make this a valid answer?

upvoted 1 times

🗳️ 👤 **Jackdisuin** 2 years, 5 months ago

correct

upvoted 1 times

🗳️ 👤 **Snownoodles** 2 years, 8 months ago

**Selected Answer: AF**

The answers given are correct.

This question didn't mention "multi-tenant application", only mentioned users from "multi-tenant".

IF the application is "multi-tenant", you won't need guest users. But the application in this question is single-tenant.

upvoted 1 times

🗳️ 👤 **learner06** 3 years ago

**Selected Answer: AF**

A and F are correct

upvoted 1 times

🗳️ 👤 **AlfL** 3 years, 3 months ago

**Selected Answer: AF**

i choose A F

upvoted 1 times

🗳️ 👤 **certhawk** 3 years, 3 months ago

Correct answer is A & B. The key to the question is "Multiple Azure AD tenants", if all tenants are azure ad, then there's no need to create guest accounts. If tenants were not Azure AD, then guest account would have been possible. Details on how to configure for multiple azure tenants here: <https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-convert-app-to-be-multi-tenant>

upvoted 1 times

🗳️ 👤 **exnaniantwort** 3 years, 3 months ago

WRONG

With Azure AD B2B, the partner uses their own identity management solution, so there is no external administrative overhead for your organization. Guest users sign in to your apps and services with their own work, school, or social identities.

\*\*\*\*\*The partner uses their own identities and credentials, whether or not they have an Azure AD account.\*\*\*\*\*

You don't need to manage external accounts or passwords.

You don't need to sync accounts or manage account lifecycles.

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

F is correct.

B is definitely wrong by the way.

upvoted 1 times

🗳️ 👤 **itenginerd** 3 years, 3 months ago

These statements are wholly incorrect: "if all tenants are azure ad, then there's no need to create guest accounts. If tenants were not Azure AD, then guest account would have been possible. "

The definition of a guest user is someone who has an account in another Azure AD tenant. There is no concept of a guest user who ISN'T part of another Azure AD tenant. I have access to about 75 customer Azure tenants at the moment, I live and die on guest user access every day.

upvoted 1 times

🗳️ 👤 **AberdeenAngus** 3 years, 1 month ago

Don't think so... where I work there are hundreds of guest user accounts including my own gmail account, I very much doubt if the rest are all in other Azure AD tenants. I also don't see this as a requirement in <https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal>

upvoted 2 times

🗳️ 👤 **JayBee65** 3 years ago

With B2B collaboration, you can securely share your company's applications and services with external users, while maintaining control over your own corporate data. Work safely and securely with external partners, large or small, even if they don't have Azure AD or an IT department. So guests can be either users from other AAD or other identities

upvoted 1 times

🗳️ 👤 **us3r** 3 years, 5 months ago

**Selected Answer: AF**

agree AF

upvoted 1 times

🗳️ 👤 **Estudiante\_BH** 3 years, 5 months ago

ill go with A + F it is correct

upvoted 1 times

🗳️ 👤 **Eitant** 3 years, 6 months ago

**Selected Answer: AF**

Correct answer

upvoted 3 times

🗳️ 👤 **waqas** 3 years, 8 months ago

A & B is the answer

upvoted 3 times

🗳️ 👤 **TheAzureArchitect** 3 years, 7 months ago

No.

By a process of elimination we can say only A&F are correct.

We must have guest accounts (or B2C etc) for a multi-tenant app, and must have MFA. These facts rule out the other choices.

upvoted 2 times

🗳️ 👤 **syu31svc** 3 years, 9 months ago

"ensure that the users use Azure Multi-Factor Authentication (MFA)" -> This supports A as one of the answers for sure

"multiple Azure AD tenants" -> This would support F as the answer

Managed identities are for resources and services, not for users hence B is wrong

CDE are definitely wrong

A and F it is

upvoted 3 times

🗳️ 👤 **nkx** 3 years, 9 months ago

Came in exam on 20-sep-21, i passed, answers are correct

upvoted 3 times

🗳️ 👤 **teehex** 3 years, 10 months ago

A + F are needed. Everything is here <https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-tutorial-require-mfa>

upvoted 3 times

🗳️ 👤 **DragonsGav** 4 years ago

Answers should be A and C

<https://docs.microsoft.com/en-us/azure/active-directory-b2c/solution-articles>

upvoted 2 times

🗳️ 👤 **tita\_tovenaar** 3 years, 11 months ago

I can't see anything at all in your ref. that would support alternative C.

upvoted 3 times

🗳️ 👤 **QiangQiang** 4 years, 1 month ago

AB,

register the app allowing multi-tenant access

enable conditional access

upvoted 8 times

🗳️ 👤 **tita\_tovenaar** 3 years, 11 months ago

B - managed identities ... that's for services and resources mainly and won't make any bridge between your Ad and the other tenants.

upvoted 4 times

You need to create an Azure Storage account that uses a custom encryption key.

What do you need to implement the encryption?

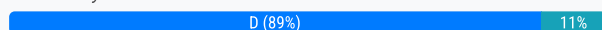
- A. a certificate issued by an integrated certification authority (CA) and stored in Azure Key Vault
- B. a managed identity that is configured to access the storage account
- C. an Azure Active Directory Premium subscription
- D. an Azure key vault in the same Azure region as the storage account

**Suggested Answer: A**

You can use your own encryption key to protect the data in your storage account. When you specify a customer-managed key, that key is used to protect and control access to the key that encrypts your data.

You must use either Azure Key Vault or Azure Key Vault Managed Hardware Security Model (HSM) (preview) to store your customer-managed keys.

Community vote distribution



**ab\_cd** Highly Voted 4 years, 3 months ago

D

The storage account and the key vault or managed HSM must be in the same region and in the same Azure Active Directory (Azure AD) tenant, but they can be in different subscriptions.

upvoted 96 times

**Montrealcupid** 4 years, 3 months ago

Agreed.

You must use either Azure Key Vault or Azure Key Vault Managed Hardware Security Module (HSM) (preview) to store your customer-managed keys. You can either create your own keys and store them in the key vault or managed HSM, or you can use the Azure Key Vault APIs to generate keys. The storage account and the key vault or managed HSM must be in the same region and in the same Azure Active Directory (Azure AD) tenant, but they can be in different subscriptions.

upvoted 13 times

**glam** Highly Voted 4 years, 3 months ago

D. an Azure key vault in the same Azure region as the storage account

upvoted 16 times

**MARKMKENYA** Most Recent 2 years, 4 months ago

Answer is B and i have noticed many errors in discussions answers.

Is the a mlantois for this exam?

<https://learn.microsoft.com/en-us/azure/storage/common/customer-managed-keys-configure-existing-account?tabs=azure-portal>

upvoted 2 times

**GarryK** 2 years, 8 months ago

Selected Answer: B

<https://learn.microsoft.com/en-us/azure/storage/common/customer-managed-keys-configure-existing-account?tabs=azure-portal>

When you enable customer-managed keys for an existing storage account, you must specify a managed identity that will be used to authorize access to the key vault that contains the key. The managed identity must have permissions to access the key in the key vault.

You can use a new or existing key vault to store customer-managed keys. The storage account and key vault may be in different regions or subscriptions in the same tenant. To learn more about Azure Key Vault, see [Azure Key Vault Overview](#) and [What is Azure Key Vault?](#).

So B

upvoted 1 times

**kmeena** 2 years, 10 months ago

The documentation in Microsoft says - They can be in different region.  
<https://docs.microsoft.com/en-us/azure/storage/common/customer-managed-keys-overview>

"You can either create your own keys and store them in the key vault or managed HSM, or you can use the Azure Key Vault APIs to generate keys. The storage account and the key vault or managed HSM must be in the same Azure Active Directory (Azure AD) tenant, but they can be in different regions and subscriptions."

upvoted 2 times

🗳️ 👤 **AubinBakana** 2 years, 10 months ago

**Selected Answer: D**

I wonder what they'd mark us. I am pretty adamant the answer is D.

upvoted 1 times

🗳️ 👤 **silwal** 2 years, 10 months ago

**Selected Answer: B**

When you enable customer-managed keys for a storage account, you must specify a managed identity that will be used to authorize access to the key vault that contains the key. The managed identity must have permissions to access the key in the key vault.

[https://docs.microsoft.com/en-us/azure/storage/common/customer-managed-keys-configure-key-vault?  
toc=%2Fazure%2Fstorage%2Fblobs%2Ftoc.json&tabs=portal](https://docs.microsoft.com/en-us/azure/storage/common/customer-managed-keys-configure-key-vault?toc=%2Fazure%2Fstorage%2Fblobs%2Ftoc.json&tabs=portal)

D is wrong - Do not need to be in the same region

Nothing to do with A.

upvoted 2 times

🗳️ 👤 **silwal** 2 years, 10 months ago

B

When you enable customer-managed keys for a storage account, you must specify a managed identity that will be used to authorize access to the key vault that contains the key. The managed identity must have permissions to access the key in the key vault.

[https://docs.microsoft.com/en-us/azure/storage/common/customer-managed-keys-configure-key-vault?  
toc=%2Fazure%2Fstorage%2Fblobs%2Ftoc.json&tabs=portal](https://docs.microsoft.com/en-us/azure/storage/common/customer-managed-keys-configure-key-vault?toc=%2Fazure%2Fstorage%2Fblobs%2Ftoc.json&tabs=portal)

upvoted 1 times

🗳️ 👤 **Testing6132** 2 years, 12 months ago

**Selected Answer: D**

Nothing to do with the Cert.

upvoted 2 times

🗳️ 👤 **OCHT** 3 years, 1 month ago

Had seen this kind of question on AZ-500 . Answer is D.

upvoted 2 times

🗳️ 👤 **Lyibai** 3 years, 1 month ago

D. an Azure key vault in the same Azure region as the storage account

upvoted 2 times

🗳️ 👤 **AiFL** 3 years, 3 months ago

**Selected Answer: D**

i think it's D because is it not about cert?

upvoted 2 times

🗳️ 👤 **[Removed]** 3 years, 3 months ago

**Selected Answer: D**

D is correct

upvoted 1 times

🗳️ 👤 **plmmsg** 3 years, 3 months ago

**Selected Answer: D**

Answer should be D. same region

upvoted 1 times



🗳️ 👤 **anthonyphuc** 3 years, 3 months ago

**Selected Answer: D**



must be same region

upvoted 1 times


  **arun** 3 years, 3 months ago

**Selected Answer: D**

<https://docs.microsoft.com/en-us/azure/storage/common/customer-managed-keys-overview>

"You can either create your own keys and store them in the key vault or managed HSM, or you can use the Azure Key Vault APIs to generate keys. The storage account and the key vault or managed HSM must be in the same region and in the same Azure Active Directory (Azure AD) tenant, but they can be in different subscriptions."

upvoted 1 times

  **Choquito** 3 years, 3 months ago

A is the answer, the key word is custom. keyvault do not need to be in the same region as the storage account

upvoted 1 times

## HOTSPOT -

You plan to create an Azure environment that will have a root management group and five child management groups. Each child management group will contain five Azure subscriptions. You plan to have between 10 and 30 resource groups in each subscription.

You need to design a solution for the planned environment. The solution must meet the following requirements:

Prevent users who are assigned the Owner role for the subscriptions from deleting the resource groups from their respective subscription.

- 
- ⇒ Ensure that you can update RBAC role assignments across all the subscriptions and resource groups.
- ⇒ Minimize administrative effort.

What should you include in the solution? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Update the RBAC role assignments:

Azure Blueprints
Azure Policy
Azure Security Center

Prevent the deletion of the resource groups:

Azure Blueprints assignments that set locking mode at the subscription level
Resource locks at the resource group level
Resource locks at the subscription level

### Answer Area

Update the RBAC role assignments:

Azure Blueprints
Azure Policy
Azure Security Center

Prevent the deletion of the resource groups:

Azure Blueprints assignments that set locking mode at the subscription level
Resource locks at the resource group level
Resource locks at the subscription level

Suggested Answer:

Box 1: Azure Blueprints -

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

Role Assignments -

Policy Assignments -

Azure Resource Manager templates (ARM templates)

Resource Groups -

Incorrect:

A policy is a default allow and explicit deny system focused on resource properties during deployment and for already existing resources.

Box 2: Resource locks at the subscription level

To minimize administrative effort lock at the subscription level.

Note: As an administrator, you can lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources.

Reference:

<https://docs.microsoft.com/en-us/azure/governance/blueprints/overview> <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources>

🗨️ 👤 **Jasper666** Highly Voted 4 years, 1 month ago

Answer should be Azure blueprints in both areas.  
upvoted 69 times

🗨️ 👤 **d0bermannn** 3 years, 11 months ago

agreed, and explanation provided said exactly this (2xbp)  
upvoted 4 times

🗨️ 👤 **Kevmeister** 4 years ago

I agree with Jasper666, as per the source:

<https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking#locking-modes-and-states>

It's typically possible for someone with appropriate Azure role-based access control (Azure RBAC) on the subscription, such as the 'Owner' role, to be allowed to alter or delete any resource. This access isn't the case when Azure Blueprints applies locking as part of a deployed assignment. If the assignment was set with the Read Only or Do Not Delete option, not even the subscription owner can perform the blocked action on the protected resource.

Trying to use resource locks at subscription level can be removed by owners.

upvoted 18 times

🗨️ 👤 **demonite** 4 years ago

I agree

upvoted 2 times

🗨️ 👤 **Suharsh** 4 years ago

Agree. The right answer is Azure blueprint.

upvoted 2 times

🗨️ 👤 **rdemontis** 3 years, 7 months ago

Thanks for explanation

upvoted 2 times

🗨️ 👤 **RubberenRobbie** Highly Voted 4 years ago

Blueprints for both. An owner CAN remove a resource lock. Only a blueprint can deny owners  
upvoted 13 times

🗨️ 👤 **cwilson91** Most Recent 3 years, 1 month ago

On AZ-305 exam - 5.7.22

upvoted 5 times

🗨️ 👤 **Pupu86** 3 years, 2 months ago

Not sure if handling 5 x 5 subscriptions resource locks is considered minimal effort - so that is considered not a right answer to me  
upvoted 1 times

🗨️ 👤 **plmsg** 3 years, 3 months ago

Azure blueprints for both box

upvoted 1 times

🗨️ 👤 **Ali526** 3 years, 4 months ago

After owners of ExamTopics (this web site) have found that an overwhelming majority (sometimes 100%) of contributors have agreed upon a different answer than theirs, it may be a good idea to correct their own answer.

upvoted 5 times

🗨️ 👤 **itenginerd** 3 years, 3 months ago

TBQH, wrestling with the discussion teaches you as much or more than just cycling the questions. At least in my experience.

upvoted 5 times

🗨️ 👤 **BhupalS** 3 years, 5 months ago

It's typically possible for someone with appropriate Azure role-based access control (Azure RBAC) on the subscription, such as the 'Owner' role, to be allowed to alter or delete any resource. This access isn't the case when Azure Blueprints applies locking as part of a deployed assignment. If the assignment was set with the Read Only or Do Not Delete option, not even the subscription owner can perform the blocked action on the protected resource.

This security measure protects the consistency of the defined blueprint and the environment it was designed to create from accidental or programmatic deletion or alteration.

As per requirements, both answer should be Blueprints

upvoted 1 times

🗨️ 👤 **Inland** 3 years, 7 months ago

[www.docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking](https://www.docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking) (refer to notes) and the following option is correct.

Box 1: Azure Blueprints

Box 2: Resource locks at the subscription level

upvoted 3 times

🗨️ 👤 **itengineerd** 3 years, 3 months ago

From your cited document: It's typically possible for someone with appropriate Azure role-based access control (Azure RBAC) on the subscription, such as the 'Owner' role, to be allowed to alter or delete any resource. This access isn't the case when Azure Blueprints applies locking as part of a deployed assignment. If the assignment was set with the Read Only or Do Not Delete option, not even the subscription owner can perform the blocked action on the protected resource.

The only way to fully prevent someone with Owner rights from later lifting the lock would be to lock it in the Blueprint.

upvoted 1 times

🗨️ 👤 **syu31svc** 3 years, 9 months ago

Update RBAC role is Blueprint; no argument on this one

<https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking>

If the assignment was set with the Read Only or Do Not Delete option, not even the subscription owner can perform the blocked action on the protected resource.

Prevent deletion is at Blueprint level

upvoted 1 times

🗨️ 👤 **syu31svc** 3 years, 9 months ago

I meant Blueprint assignment locking for prevent deletion

upvoted 2 times

🗨️ 👤 **nkV** 3 years, 9 months ago

Came in exam on 20-sep-21, i passed, answers are correct, Answer should be Azure blueprints in both areas.

upvoted 5 times

🗨️ 👤 **souvik123** 3 years, 9 months ago

Azure Blueprint for both options.

upvoted 2 times

🗨️ 👤 **teehex** 3 years, 10 months ago

To minimize administrative effort the answer must be Azure Blueprint with setting lock mode.<https://docs.microsoft.com/en-us/azure/governance/blueprints/tutorials/protect-new-resources>

upvoted 2 times

🗨️ 👤 **MaheshS** 4 years ago

Yes it should be Azure blueprints for both

upvoted 1 times

🗨️ 👤 **DragonsGav** 4 years ago

Azure Blueprints should be the answer for both questions.

upvoted 1 times

🗨️ 👤 **mahwish** 4 years ago


Blueprints for both

upvoted 1 times

🗨️ 👤 **Rajyahoo** 4 years ago

Question is "from deleting the resource groups". If you use BluePrint to lock, all artifacts in BP is locked.

upvoted 2 times

  **jr\_luciano** 3 years, 4 months ago

Each artifact can have its individual lock.

"Resources created by artifacts in a blueprint assignment have four states: Not Locked, Read Only, Cannot Edit / Delete, or Cannot Delete. Each artifact type can be in the Not Locked state."

<https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking#locking-modes-and-states>

upvoted 1 times

  **pentium75** 3 years, 10 months ago

Can't you specify the lock specifically for "Resource Group" objects in BP?

upvoted 2 times

  **ChocolateNagaViper** 3 years, 4 months ago

Rajyadoo is correct. Setting the Do Not Delete mode through Blueprints will prevent all artifacts and resource groups from being deleted:

<https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking>. Since this is more restrictive than required in the question, we can't consider that the correct answer. The shown answer is correct.

upvoted 1 times

  **jr\_luciano** 3 years, 4 months ago

Each artifact can have its individual lock.

"Resources created by artifacts in a blueprint assignment have four states: Not Locked, Read Only, Cannot Edit / Delete, or Cannot Delete. Each artifact type can be in the Not Locked state."

<https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking#locking-modes-and-states>

upvoted 1 times

Your company has the divisions shown in the following table.

Division	Azure subscription	Azure Active Directory (Azure AD) tenant
East	Sub1	East.contoso.com
West	Sub2	West.contoso.com

Sub1 contains an Azure web app that runs an ASP.NET application named App1. App1 uses the Microsoft identity platform (v2.0) to handle user authentication.

Users from east.contoso.com can authenticate to App1.

You need to recommend a solution to allow users from west.contoso.com to authenticate to App1.

What should you recommend for the west.contoso.com Azure AD tenant?

- A. a conditional access policy
- B. pass-through authentication
- C. guest accounts
- D. an app registration

**Suggested Answer: D**

There are several components that make up the Microsoft identity platform:

⇒ OAuth 2.0 and OpenID Connect standard-compliant authentication service

Application management portal: A registration and configuration experience in the Azure portal, along with the other Azure management capabilities.

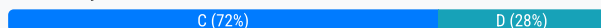
▪

You register an application using the App registrations experience in the Azure portal so that your app can be integrated with the Microsoft identity platform and call Microsoft Graph.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-overview> <https://docs.microsoft.com/en-us/graph/auth-register-app-v2>

Community vote distribution



🗳️ **jallaix** Highly Voted 4 years, 2 months ago

Login through app registration with multi-tenant enabled:

AADSTS50020: User account 'xxx@tenant2.com' from identity provider 'tenant2.com' does not exist in tenant 'tenant1' and cannot access the application 'xxx' in that tenant. The account needs to be added as an external user in the tenant first. Sign out and sign in again with a different Azure Active Directory user account.

It works after inviting the user as a guest, thus answer is C.

upvoted 59 times

🗳️ **gssd4scoder** 4 years, 1 month ago

agree with u

upvoted 1 times

🗳️ **subbu3071988** 3 years, 8 months ago

Ok let's consider it should be a combination of both guest user account(s) and then app registered for the tenant user(s). However, just by allowing access as a guest account user(s), will not solve the authentication concern. App registration for that tenant is a must and outweighs the basic guest account access. With Option C, you can complete the solution with option D. But most importantly, Option C alone cannot be a recommended independent solution. So I would go for Option D.

upvoted 7 times

🗳️ **rdemontis** 3 years, 7 months ago

You don't need to register the app on the tenant2 using guest accounts. Guest users should be defined in tenant1 so you can access to the tenant1 resources using your tenant2 account credentials.

upvoted 2 times

🗳️ **yyuryyucicuryyforme** 3 years, 5 months ago

My thoughts are we have two possible solution recommendations are 1) use guest accounts 2) convert single tenant app to multi tenant. However option 2) is not the simplest and may ideally require application changes to handle admin consent process - and also there is no need for creating an app registration in the added tenant so would seem to rule out D). Option1) is simplest and we are talking about a single organization albeit two divisions - there may never be more than one extra tenant and multitenant conversion would be overkill, so my answer would be C). A) or B) do not contribute to solving the main requirement.

upvoted 1 times

🗄️ 👤 **Lb83** Highly Voted 4 years, 2 months ago

An account with the right privileges to the west tenant has to register the app so that the app can be associated with their directory. This implies that the app is configured for multi tenancy. If the question asked "what could be done in East?" Guest accounts would be viable.

upvoted 23 times

🗄️ 👤 **soucine** 3 years, 3 months ago

I don't think registering the app would be enough, since the ASP.NET code need to validate the issued AD token using the tenant id and the client id (information you get when you register the app). => Answer : C

upvoted 1 times

🗄️ 👤 **GarryK** Most Recent 2 years, 8 months ago

Selected Answer: C

<https://learn.microsoft.com/en-us/azure/active-directory/develop/howto-convert-app-to-be-multi-tenant>

App registration is already done in the home tenant East. You dont need another app registration in the tenant West even if you picked multi-tenant.

<https://learn.microsoft.com/en-us/azure/active-directory/develop/single-and-multi-tenant-apps>

Even its recommended here to use guest accounts:

Accounts in this directory only Single tenant All user and guest accounts in your directory can use your application or API.

Use this option if your target audience is internal to your organization.

upvoted 1 times

🗄️ 👤 **MARKMKENYA** 2 years, 4 months ago

Its the same organization and the app access is not temporary. I think the correct answer is app registration and selecting multi tenant. Guest users are users in another organization - not for users in your organization but in a different office using a different child domain.

upvoted 1 times

🗄️ 👤 **AubinBakana** 2 years, 10 months ago

Selected Answer: D

Both Apps are of the same company. Those who are thinking of Guess account are not thinking hard enough. When setting App Registration you get to specify if this app will be available to other apps in the account.

upvoted 2 times

🗄️ 👤 **AberdeenAngus** 3 years ago

I'm going A, Conditional Access Policy. I really don't think guest accounts are needed. The new tenant does need a conditional access policy to control logins to the app.

<https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-convert-app-to-be-multi-tenant>

upvoted 1 times

🗄️ 👤 **Teringzooi** 3 years, 1 month ago

Today in AZ-305 exam. None of these answers came in the exam.

I chose Governance Identity.

upvoted 5 times

🗄️ 👤 **Zsolt72** 3 years, 2 months ago

Selected Answer: C

It says:

App1 uses the Microsoft identity platform (v2.0) to handle user authentication.

This means that you already had az app registration!

For the other tenant users the the guest account setup is needed.

upvoted 5 times

🗄️ 👤 **cloudera** 3 years, 3 months ago

Selected Answer: C

Which comes first chicken or eggs? LOL Very debatable question.

Apps need to be registered first on AAD and then invite guest users from west.tenant.name, then the users accept the terms and conditions etc and vola... (you know the rest :))

I would pick C. Guest Account as the answer.

upvoted 2 times

🗳️ 👤 **itengineerD** 3 years, 3 months ago

On my exam today.

upvoted 1 times

🗳️ 👤 **Dawn7** 3 years, 3 months ago

**Selected Answer: C**

I would go with C

upvoted 1 times

🗳️ 👤 **jaydee7** 3 years, 3 months ago

keep going, as of today C leads with 3 votes while D has 2 votes.

upvoted 1 times

🗳️ 👤 **Jcbrow27** 3 years, 3 months ago

**Selected Answer: C**

Guest is correct

upvoted 1 times

🗳️ 👤 **Devangkumar** 3 years, 3 months ago

**Selected Answer: D**

D seems correct answer!

Single-tenant apps are only available in the tenant they were registered in, also known as their home tenant.

Multi-tenant apps are available to users in both their home tenant and other tenants.

Source: <https://docs.microsoft.com/en-us/azure/active-directory/develop/single-and-multi-tenant-apps>

upvoted 3 times

🗳️ 👤 **plmmsg** 3 years, 3 months ago

**Selected Answer: C**

Guest account

upvoted 1 times

🗳️ 👤 **us3r** 3 years, 5 months ago

**Selected Answer: C**

question is for west AAD tenant, answer is GUEST ACCOUNTS

upvoted 1 times

🗳️ 👤 **sprabhuraj** 3 years, 5 months ago

**Selected Answer: C**

Check the discussion

upvoted 1 times

🗳️ 👤 **Dpejic** 3 years, 6 months ago

On exam 24.12.2021

upvoted 3 times



You have an Azure Active Directory (Azure AD) tenant named contoso.com that has a security group named Group1. Group1 is configured for assigned membership. Group1 has 50 members, including 20 guest users.

You need to recommend a solution for evaluating the membership of Group1. The solution must meet the following requirements:

- ⇒ The evaluation must be repeated automatically every three months.
- ⇒ Every member must be able to report whether they need to be in Group1.
- ⇒ Users who report that they do not need to be in Group1 must be removed from Group1 automatically.
- ⇒ Users who do not report whether they need to be in Group1 must be removed from Group1 automatically.

What should you include in the recommendation?

- A. Change the Membership type of Group1 to Dynamic User.
- B. Implement Azure AD Privileged Identity Management.
- C. Implement Azure AD Identity Protection.
- D. Create an access review.

#### Suggested Answer: A

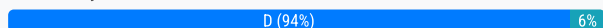
In Azure Active Directory (Azure AD), you can create complex attribute-based rules to enable dynamic memberships for groups. Dynamic group membership reduces the administrative overhead of adding and removing users.

When any attributes of a user or device change, the system evaluates all dynamic group rules in a directory to see if the change would trigger any group adds or removes. If a user or device satisfies a rule on a group, they are added as a member of that group. If they no longer satisfy the rule, they are removed.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership>

Community vote distribution



🗳️ **rithvik** Highly Voted 4 years, 3 months ago

Create access review should be the option  
upvoted 126 times

🗳️ **glam** Highly Voted 4 years, 3 months ago

D. Create an access review.  
upvoted 26 times

🗳️ **tim\_27\_us** Most Recent 2 years, 8 months ago

Yes D.  
upvoted 1 times

🗳️ **One111** 2 years, 10 months ago

**Selected Answer: D**

Only Access Review allows to automate process every 3 month and automatically managed group members.  
upvoted 1 times

🗳️ **AubinBakana** 2 years, 10 months ago

**Selected Answer: A**

Keyword here is automatically & periodically. In the case of Access Review, a manager or an admin has to do the review after a request or the conditions have been met.  
upvoted 1 times

🗳️ **NunoVarelaa** 2 years, 11 months ago

**Selected Answer: D**

D for sure  
upvoted 1 times

🗳️ **Sudhaker** 2 years, 11 months ago

**Selected Answer: D**

Access Reviews

upvoted 1 times

🗨️ 👤 **Ashin** 3 years, 3 months ago

The answer should be Dynamic User .

Reasons : The question is specifically asking to automate the adding and removing of the user .

In the official documentation of Access Review it is explicitly mentioned that the Access reviews should only be used if automation is not possible.

We can also create rules for Dynamic Group also. The users will be added/removed based on the rules that are satisfied.

<https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview>

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership>

upvoted 2 times

🗨️ 👤 **JayBee65** 3 years ago

And " Every member must be able to report whether they need to be in Group1." so a property cannot be used to auto add or remove users. They must decide themselves.

upvoted 1 times

🗨️ 👤 **VijayRaja2000** 3 years ago

I think that here the key is "The evaluation must be repeated automatically every three months". Dynamic users removes the members of the group when there is any change in the attributes of that users that we configure in the rule. This cannot be scheduled to be executed every three months.

upvoted 2 times

🗨️ 👤 **plmmmsg** 3 years, 3 months ago

**Selected Answer: D**

Create an access review.

upvoted 1 times

🗨️ 👤 **Dawn7** 3 years, 3 months ago

**Selected Answer: D**

D is correct.

upvoted 2 times

🗨️ 👤 **Billabongs** 3 years, 4 months ago

Access Review is the answer

upvoted 2 times

🗨️ 👤 **Xia\_Li** 3 years, 5 months ago

**Selected Answer: D**

Create Access Review

upvoted 1 times

🗨️ 👤 **Nokaido** 3 years, 5 months ago

**Selected Answer: D**

Create access review

upvoted 1 times

🗨️ 👤 **Suhasrs** 3 years, 5 months ago

**Selected Answer: D**

Only in Access Review can you automate the checks

upvoted 1 times

🗨️ 👤 **china5000** 3 years, 6 months ago

D. Create an access review

upvoted 1 times

🗨️ 👤 **china5000** 3 years, 6 months ago

One more thing: How users report back if they need to be in Group1 or not? This option is only available in Access Review.

upvoted 3 times

🗨️ 👤 **Carroyo826** 3 years, 6 months ago

Create Access Review correct answer

upvoted 1 times

🗨️ 👤 **sakshi250291** 3 years, 6 months ago

**Selected Answer: D**

D -Access Reviews

upvoted 1 times

Your company purchases an app named App1.

You need to recommend a solution to ensure that App1 can read and modify access reviews.

What should you recommend?

- A. From API Management services, publish the API of App1, and then delegate permissions to the Microsoft Graph API.
- B. From the Azure Active Directory admin center, register App1. From the Access control (IAM) blade, delegate permissions.
- C. From the Azure Active Directory admin center, register App1, and then delegate permissions to the Microsoft Graph API.
- D. From API Management services, publish the API of App1. From the Access control (IAM) blade, delegate permissions.

**Suggested Answer: B**

The app must be registered. You can register the application in the Azure Active Directory admin center.

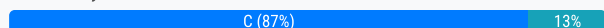
The Azure AD access reviews feature has an API in the Microsoft Graph endpoint.

You can register an Azure AD application and set it up for permissions to call the access reviews API in Graph.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app>

Community vote distribution



**rithvik** Highly Voted 4 years, 3 months ago

correct answer is C

upvoted 63 times

**nicksb19** 4 years ago

C seems correct verified with the settings in Azure portal.

<https://docs.microsoft.com/en-us/graph/use-the-api>

upvoted 6 times

**d0bermannn** 3 years, 11 months ago

and explanation said exactly that

upvoted 5 times

**glam** Highly Voted 4 years, 3 months ago

C. From the Azure Active Directory admin center, register App1, and then delegate permissions to the Microsoft Graph API.

upvoted 23 times

**One111** Most Recent 2 years, 10 months ago

**Selected Answer: C**

IAM options on resource allows to assign entity's permissions on that resource. In this questions we are ask to delegate permissions to read write access reviews from that app. It will need GraphAPI to query these settings.

upvoted 1 times

**plmmsg** 3 years, 3 months ago

**Selected Answer: C**

answer is C

upvoted 1 times

**arun** 3 years, 3 months ago

**Selected Answer: C**

<https://docs.microsoft.com/en-us/graph/accessreviews-overview>

upvoted 1 times

**AD3** 3 years, 3 months ago

'C' for sure. From Microsoft doc <https://devblogs.microsoft.com/microsoft365dev/retrieving-azure-ad-access-reviews/#:~:text=Click%20on%20%E2%80%9CSelect%20an%20API%E2%80%9D%2C%20click%20on%20%E2%80%9CMicrosoft,and%20Manage%20all%20prog>

"Register an Azure AD application which has permissions to call the access reviews API in Graph".

upvoted 1 times

**zeek** 3 years, 3 months ago

Correct answer is C. you need to access the GraphAPIs

upvoted 1 times

🗨️ **reachmymind** 3 years, 4 months ago

**Selected Answer: C**

After Registering AppX from Azure AD Admin Center

Portal -> AD -> AppX -> API Permissions -> Microsoft Graph

--> Application Permissions

---> Access Review

-----> AccessReview.Read.All

-----> AccessReview.ReadWrite.All

-----> AccessReview.ReadWrite.Membership

upvoted 2 times

🗨️ **petey212** 3 years, 4 months ago

**Selected Answer: B**

Although C would work, Microsoft graph is not specific enough to delegating permissions for this one application.

upvoted 2 times

🗨️ **itenginerd** 3 years, 3 months ago

I don't disagree with you, but the explanation circling one and then talking about Graph makes B a suspect answer. Besides, you can't assign rights to Graph (or anything relevant to access reviews) thru IAM as far as I know.

upvoted 1 times

🗨️ **us3r** 3 years, 5 months ago

**Selected Answer: C**

graph API

upvoted 1 times

🗨️ **moon2351** 3 years, 5 months ago

**Selected Answer: C**

C is correct

upvoted 1 times

🗨️ **wardy1983** 3 years, 5 months ago

Selected Answer: C

upvoted 1 times

🗨️ **ryuhei** 3 years, 6 months ago

**Selected Answer: C**

answer C

upvoted 1 times

🗨️ **Eitant** 3 years, 6 months ago

**Selected Answer: C**

Correct answer

upvoted 1 times

🗨️ **ritgllfjljaeargil** 3 years, 6 months ago

**Selected Answer: C**

Answer is C

upvoted 4 times

🗨️ **harkamal** 3 years, 8 months ago

answer should be B because when you register an application in AD then authorization in this case should also be thru AD. C can not be the answer because it says 1st register app in AD , then for auth. how can it ship it over to Graph. its my understanding

upvoted 1 times

🗨️ **rsharma007** 3 years, 8 months ago

MS Graph exposes granular permissions to app to access other resources including MS and non-microsoft service. Think of Graph as a broker that sits between the various resource providers. You as a user can give apps (delegate) access to resources bounded by your own privileges. An admin can also give app permissions when user sign in is not supported in which application runs with the permissions assigned by the admin.

Graph enables your app access to all the MS security providers to programmatically access and build custom logic based on the MS provided solution.

upvoted 1 times

You have 200 resource groups across 20 Azure subscriptions.

Your company's security policy states that the security administrator must verify all assignments of the Owner role for the subscriptions and resource groups once a month. All assignments that are not approved by the security administrator must be removed automatically. The security administrator must be prompted every month to perform the verification.

What should you use to implement the security policy?

- A. Identity Secure Score in Azure Security Center
- B. Access reviews in Identity Governance
- C. the user risk policy in Azure Active Directory (Azure AD) Identity Protection
- D. role assignments in Azure Active Directory (Azure AD) Privileged Identity Management (PIM)

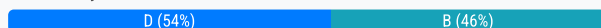
**Suggested Answer: B**

Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. User's access can be reviewed on a regular basis to make sure only the right people have continued access.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview>

Community vote distribution



🗳️ 👤 **AKumar** Highly Voted 4 years, 3 months ago

Given Answer is correct- here is the explanation -

<https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview#when-should-you-use-access-reviews>  
upvoted 27 times

🗳️ 👤 **somenick** 3 years, 12 months ago

Guys, NONE of the given answers are not working. You can try it in portal for free. I'm wondering if anyone got this question on the exam? We should mark and report it to Microsoft on the exam.

upvoted 3 times

🗳️ 👤 **dasEnder** 3 years, 1 month ago

PIM is AAD P2 licensed. Did you changed the license?

upvoted 1 times

🗳️ 👤 **sallymaher** 4 years, 3 months ago

in the same link you have provided check" Where do you create reviews? " u need to review owner role so through the PIM , but also not role assignment but PIM-Manage

upvoted 2 times

🗳️ 👤 **tita\_tovenaar** 3 years, 11 months ago

see my earlier comment, this is not suitable here since Azure triggers a review on every group and application, see purple note in ref.

<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review#create-one-or-more-access-reviews>  
upvoted 1 times

🗳️ 👤 **nsvijay04b1** 3 years, 10 months ago

correct.

PIM is again going to use 'identity governance's access reviews'

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-start-security-review>  
upvoted 4 times

🗳️ 👤 **yasinetm** Highly Voted 4 years, 3 months ago

I think it's D.

Privileged Identity Management allows to create access reviews in order to check role assignments.

Access reviews in Identity Governance allows to review groups and application assignments.

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-start-access-review>  
upvoted 14 times

🗨️ **PaulM1122** 4 years, 3 months ago

No, PIM wil only create an access review when a user is requesting the rolél.

upvoted 6 times

🗨️ **Kode** 4 years ago

Yes but no. It does require PIM, but D states role assignment within PIM... that does not meet the objective. You will need to create an access review in PIM, which is part of Identity Governance.

So create access review in Identity Governance is correct

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-start-security-review#open-access-reviews>

upvoted 4 times

🗨️ **4tune** 3 years, 9 months ago

there is access review within PIM which is different from the access review in the first blade of identity governance

upvoted 1 times

🗨️ **sapien45** 3 years ago

A play on words ... yiu aree right.

Acces Review are the key words, not role assignement

B

upvoted 1 times

🗨️ **Snownoodles** Most Recent 2 years, 8 months ago

"access review" is for group members, access package review. This is for common user review not privileged users review..

"PIM Azure AD roles" is for privileged administrator role's review

"PIM Azure resource" is for Azure RBAC roles review.

The correct answer should be "PIM Azure resource" review. Since there is no such answer,, the given answer is the closest one.

upvoted 1 times

🗨️ **ezfix** 2 years, 9 months ago

D. The question is poorly written or the interface has changed. Subscription & Resource Group access reviews are under PIM, and there are two ways to get to them. These are different than the normal access reviews listed in answer B, which are "Team + Group" access reviews. Option 1 - AD Privileged Identity Management, Azure Resources, select the subscription or management group, then Access Reviews. Option 2 - Azure Active Directory, Identity Governance, Privileged Identity Management - Azure Resources, select the subscription or management group, then Access Reviews. If you simply went to Azure Active Directory, Identity Governance, Access Reviews, you would only be able to use "Team + Group" or "Applications", and not the subscription or resource groups which this question is describing. Hope this helps.

upvoted 1 times

🗨️ **ezfix** 2 years, 9 months ago

D. Access reviews for "Groups", use AD Identity Governance. Access review for "roles", use Azure AD Privileged Identity Management (PIM). Reviewed in the portal and this is correct.

<https://learn.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview>

upvoted 1 times

🗨️ **One111** 2 years, 10 months ago

Selected Answer: D

PIM for Azure resources (based on RBAC) is best option here.

upvoted 2 times

🗨️ **LillyLiver** 3 years ago

Selected Answer: D

Guys (Gals), it's PIM. Proven in my tenant.

If you go into "AAD > Identity Governance > Privileged Identity Governance > Azure Resources > Discover Resources", you can select the subscription to manage access reviews on.

I'm thinking that this question has some older content, but it's still valid.

upvoted 2 times

🗨️ **Jag74** 3 years ago

Selected Answer: B

<https://docs.microsoft.com/en-us/azure/active-directory/governance/identity-governance-overview>

upvoted 1 times

🗨️ **Azure\_daemon** 3 years, 1 month ago

For Azure AD roles or ARM roles we use PIM for the App/Group we use access review so D is the correct answer



upvoted 1 times

🗨️ **AD3** 3 years, 3 months ago

'C'. See the question & answer for Examtopics 303 Question #4Topic 2

HOTSPOT -

You plan to implement an access review to meet the following requirements:

shows the section for time and access revoke rule.

upvoted 1 times

🗨️ **petey212** 3 years, 4 months ago

**Selected Answer: B**

Access reviews is the simplest method for recurring review of access permissions and it allows the person to approve/deny.

upvoted 1 times

🗨️ **[Removed]** 3 years, 4 months ago

**Selected Answer: B**

B is the right answer

upvoted 1 times

🗨️ **bacug** 3 years, 4 months ago

**Selected Answer: D**

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

upvoted 1 times

🗨️ **Gluckos** 3 years, 5 months ago

**Selected Answer: D**

In PIM can select more subscriptions

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-create-azure-ad-roles-and-resource-roles-review#create-access-reviews>

" 4)For Azure AD roles, select Azure AD roles again under Manage. For Azure resources, select the subscription you want to manage."

Identity Governance doesn't.. but works with a subscription scope

upvoted 1 times

🗨️ **kanweng** 3 years, 3 months ago

The next piece of Azure AD Identity Governance is Privileged Identity Management (PIM)

upvoted 1 times

🗨️ **us3r** 3 years, 5 months ago

**Selected Answer: B**

Have reviews recur periodically: You can set up recurring access reviews of users at set frequencies such as weekly, monthly, quarterly or annually, and the reviewers will be notified at the start of each review. Reviewers can approve or deny access with a friendly interface and with the help of smart recommendations

source <https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview#when-should-you-use-access-reviews>

upvoted 1 times

🗨️ **ScubaDiver123456** 3 years, 6 months ago

**Selected Answer: D**

I believe it is D (Access review through PIM) since it can do Azure resource role checks and provide an automatic way to repeat them every month. It can also automatically remove access

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-create-azure-ad-roles-and-resource-roles-review>

upvoted 1 times

🗨️ **Eitant** 3 years, 6 months ago

**Selected Answer: B**

Correct Answer

upvoted 1 times

## HOTSPOT -

Your company has 20 web APIs that were developed in-house.

The company is developing 10 web apps that will use the web APIs. The web apps and the APIs are registered in the company's Azure Active Directory (Azure

AD) tenant. The web APIs are published by using Azure API Management.

You need to recommend a solution to block unauthorized requests originating from the web apps from reaching the web APIs. The solution must meet the following requirements:

- ⇒ Use Azure AD-generated claims.
- ⇒ Minimize configuration and management effort.

What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Grant permissions to allow the web apps to access the web APIs by using:

Azure AD
Azure API Management
The web APIs

Configure a JSON Web Token (JWT) validation policy by using:

Azure AD
Azure API Management
The web APIs

**Answer Area**

**Suggested Answer:**

Grant permissions to allow the web apps to access the web APIs by using:

Azure AD
Azure API Management
The web APIs

Configure a JSON Web Token (JWT) validation policy by using:

Azure AD
Azure API Management
The web APIs

Unofficial **Highly Voted** 4 years, 3 months ago

Permissions are granted by AD. First answer should be Azure AD  
upvoted 84 times

glam **Highly Voted** 4 years, 3 months ago

Box1: Azure AD  
Box2: API Management  
upvoted 57 times

ShivaUdari **Most Recent** 1 year, 9 months ago

In 305 it's  
AD  
APIM  
upvoted 1 times

cwilson91 3 years, 1 month ago

On AZ-305 exam - 5.7.22

upvoted 9 times

🗄️ 👤 **plmmmsg** 3 years, 3 months ago

Box1-Azure AD

Box2-API Management

upvoted 2 times

🗄️ 👤 **us3r** 3 years, 5 months ago

1) AAD

2) APIM

upvoted 2 times

🗄️ 👤 **Ataimo007** 3 years, 8 months ago

Azure AD

APIM

I have implemented this architecture countless of times.

upvoted 12 times

🗄️ 👤 **syu31svc** 3 years, 9 months ago

"Use Azure AD-generated claims" -> grant permissions using Azure AD

<https://docs.microsoft.com/en-us/azure/api-management/api-management-access-restriction-policies>

The validate-jwt policy enforces existence and validity of a JSON web token (JWT) extracted from either a specified HTTP Header or a specified query parameter.

JWT is from API Management

upvoted 2 times

🗄️ 👤 **nkx** 3 years, 9 months ago

I passed on 20-sep-21, I choose below one, Box1: Azure AD

Box2: API Management

upvoted 7 times

🗄️ 👤 **souvik123** 3 years, 9 months ago

Box1-Azure AD

Box2-API Management

upvoted 2 times

🗄️ 👤 **DragonsGav** 4 years ago

Azure AD [<https://docs.microsoft.com/en-us/azure/api-management/api-management-howto-protect-backend-with-aad>]

API Management

upvoted 3 times

🗄️ 👤 **SnakePlissken** 4 years ago

Steps to take:

1 - In Azure AD, register an application (backend-app) to represent the API.

2 - In Azure AD, register another application (client-app) to represent a client application that needs to call the API.

3 - In Azure AD, grant permissions to allow the client-app to call the backend-app.

4 - In APIM, configure the Developer Console to call the API using OAuth 2.0 user authorization.

5 - In APIM, add the validate-jwt policy to validate the OAuth token for every incoming request.

A. Grant permissions by using: Azure AD (Step 3)

B. Configure JWT validation policy by using: Azure APIM (Step 5)

<https://docs.microsoft.com/en-us/azure/api-management/api-management-howto-protect-backend-with-aad>

upvoted 26 times

🗄️ 👤 **Prince2690** 4 years, 1 month ago

For permissions, it should be done by Azure AD. <https://docs.microsoft.com/en-us/azure/api-management/api-management-howto-protect-backend-with-aad>.

1. Azure AD
  2. API Management
- upvoted 2 times

🗲️ 👤 **Prince2690** 4 years, 1 month ago

Box1-Azure AD

Box2-API Management

upvoted 2 times

🗲️ 👤 **ashishg2105** 4 years, 1 month ago

First Box incorrect. Answer is Azure AD

upvoted 3 times

🗲️ 👤 **claudio82** 4 years, 1 month ago

I recently work with JWT and and active directory,

The answer definitively is:

AD

API Managment

upvoted 5 times

🗲️ 👤 **aspirin** 4 years, 2 months ago

Azure AD

Azure Api Management

upvoted 4 times

## HOTSPOT -

You need to design a resource governance solution for an Azure subscription. The solution must meet the following requirements:

- ⇒ Ensure that all ExpressRoute resources are created in a resource group named RG1.
- ⇒ Delegate the creation of the ExpressRoute resources to an Azure Active Directory (Azure AD) group named Networking.
- ⇒ Use the principle of least privilege.

What should you include in the solution? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Ensure that all ExpressRoute resources are created in RG1:

- A custom RBAC role assignment at the level of RG1
- A custom RBAC role assignment at the subscription level
- An Azure Blueprints assignment that sets locking mode for the level of RG1
- An Azure Policy assignment at the subscription level that has an exclusion
- Multiple Azure Policy assignments at the resource group level except for RG1

Delegate the creation of the ExpressRoute resources to Networking:

- A custom RBAC role assignment at the level of RG1
- A custom RBAC role assignment at the subscription level
- An Azure Blueprints assignment that sets locking mode for the level of RG1
- An Azure Policy assignment at the subscription level that has an exclusion
- Multiple Azure Policy assignments at the resource group level except for RG1

**Suggested Answer:****Answer Area**

Ensure that all ExpressRoute resources are created in RG1:

- A custom RBAC role assignment at the level of RG1
- A custom RBAC role assignment at the subscription level
- An Azure Blueprints assignment that sets locking mode for the level of RG1
- An Azure Policy assignment at the subscription level that has an exclusion
- Multiple Azure Policy assignments at the resource group level except for RG1

Delegate the creation of the ExpressRoute resources to Networking:

- A custom RBAC role assignment at the level of RG1
- A custom RBAC role assignment at the subscription level
- An Azure Blueprints assignment that sets locking mode for the level of RG1
- An Azure Policy assignment at the subscription level that has an exclusion
- Multiple Azure Policy assignments at the resource group level except for RG1

Box 1: An Azure policy assignment at the subscription level that has an exclusion

Box 2: A custom RBAC role assignment at the level of RG1

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


Reference:

<https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage>

- 🗨️ 👤 **sharepoint\_Azure\_pp** Highly Voted 3 years, 8 months ago  
mentioned answer are correct  
Chooosed the same cleared with 900 on 17th October 2021  
upvoted 12 times
- 🗨️ 👤 **OCHT** Most Recent 3 years, 1 month ago  
Answers are correct.  
upvoted 1 times
- 🗨️ 👤 **itengineerd** 3 years, 3 months ago  
On my exam today.  
upvoted 2 times
- 🗨️ 👤 **plmmmsg** 3 years, 3 months ago  
Answer is correct  
upvoted 1 times
- 🗨️ 👤 **Dpejic** 3 years, 6 months ago  
On exam 24.12.2021  
upvoted 5 times
- 🗨️ 👤 **syu31svc** 3 years, 9 months ago  
"Ensure that all ExpressRoute resources are created " -> this would imply use of policy  
  
"principle of least privilege" -> custom RBAC role at RG level  
  
Answer is correct  
upvoted 8 times
- 🗨️ 👤 **Gautam1985** 3 years, 10 months ago  
correct  
upvoted 2 times
- 🗨️ 👤 **JDA** 4 years, 4 months ago  
The answers are correct.  
upvoted 4 times
- 🗨️ 👤 **TheMo** 4 years, 4 months ago  
Correct Answer  
upvoted 3 times
- 🗨️ 👤 **azurecert2021** 4 years, 4 months ago  
given answer is correct.  
upvoted 3 times
- 🗨️ 👤 **glam** 4 years, 5 months ago  
Box 1: An Azure policy assignment at the subscription level that has an exclusion  
Box 2: A custom RBAC role assignment at the level of RG1  
upvoted 3 times
- 🗨️ 👤 **Blaaa** 4 years, 5 months ago  
Correct answers  
upvoted 4 times
- 🗨️ 👤 **zeeshankaizer** 4 years, 5 months ago  
Shouldn't it be RBAC role assignment at subscription level?  
upvoted 2 times
- 🗨️ 👤 **meonyahoo** 4 years, 5 months ago  
Not required as only RG1 is allowed for creating resource  
upvoted 3 times
- 🗨️ 👤 **MikeHugeNerd** 4 years, 5 months ago  
No. At the resource group level ensures the principle of least privilege.  
upvoted 11 times
- 🗨️ 👤 **oshoparsi** 4 years, 3 months ago

but we don't know where is the Networking group who should be able to build the express rout in RG1. so I think the RBAC should be at the subscription level...

upvoted 1 times

  **pentium75** 3 years, 10 months ago

The networking group is an AAD group. This AAD group needs permission to create resources in RG1, thus it needs permission in RG1, thus you assign permission at RG1 level.

upvoted 4 times

  **jellybiscuit** 2 years, 9 months ago

The end result is really the same.

If you grant at the subscription level, technically, you have given them more rights than you needed.

But... the policy blocks them anyway.

Like I said, functionally, they're the same, but applying at the RG would more closely follow least privilege.

upvoted 1 times

  **milind8451** 4 years, 5 months ago



Why do you need an exclusion? Simply create a policy to allow to create expressRoute in a particular RG and assign to subscription, what exclusion is needed here?

upvoted 5 times

  **openidshanks1** 4 years, 5 months ago

create policy to deny creation of express route and exclude rg1 from the policy, assign this to the subscription

upvoted 11 times

  **bbartek** 4 years, 5 months ago

Policies have allow by default, deny explicitly model. Hence, if you want to accomplish this scenario, you need to explicitly deny creating ExpressRoute for an entire subscription, with the exclusion for RG1

upvoted 48 times

  **Suhasrs** 3 years, 5 months ago

thanks for the explanation

upvoted 1 times

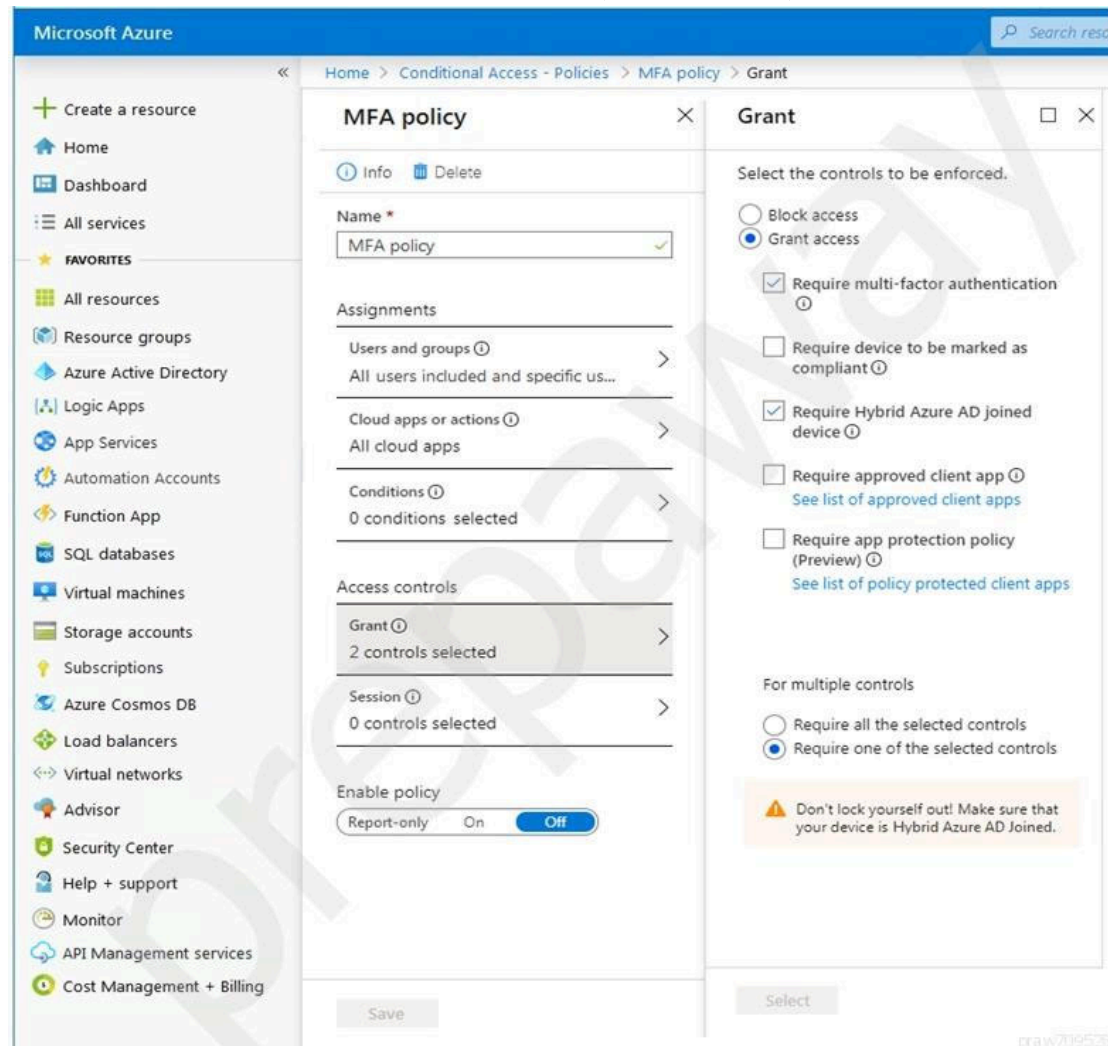
  **rdemontis** 3 years, 7 months ago

Thank you very much for explanation

upvoted 1 times

You have an Azure Active Directory (Azure AD) tenant and Windows 10 devices.

You configure a conditional access policy as shown in the exhibit. (Click the Exhibit tab.)



What is the result of the policy?

- A. All users will always be prompted for multi-factor authentication (MFA).
- B. Users will be prompted for multi-factor authentication (MFA) only when they sign in from devices that are NOT joined to Azure AD.
- C. All users will be able to sign in without using multi-factor authentication (MFA).
- D. Users will be prompted for multi-factor authentication (MFA) only when they sign in from devices that are joined to Azure AD.

**Suggested Answer: B**

Either the device should be joined to Azure AD or MFA must be used.

Community vote distribution

C (100%)

**ruckii** Highly Voted 4 years, 7 months ago

The policy is not enabled. It's in off state as I see  
upvoted 116 times

**TEMPKAKAM** 4 years, 6 months ago

Correct Answer:C

Explanation:

In this scenario, the enable policy is set to Off in the image. So, this policy will have no impact.

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

upvoted 11 times

**andyR** 4 years, 7 months ago





correct - answer is C

upvoted 15 times

  **sanketshah** 4 years, 5 months ago



Correct answer C

upvoted 5 times

  **quyennv** 4 years, 7 months ago



yes :)) the result is C

upvoted 25 times

  **3nteng** 4 years, 3 months ago

the off is the 'report only'. if that is on, it will only report and not enforce

upvoted 7 times

  **Krsto** 4 years, 3 months ago

Not correct, policy has three states, on, off and report only. This policy is off.

upvoted 12 times

  **Chris\_MG** 3 years, 5 months ago

look her



<https://www.youtube.com/watch?v=7t0oWyjWJN4>

upvoted 1 times

  **Table2022** 4 years ago

Please use brain before comment

upvoted 23 times

  **jugha** 4 years, 2 months ago

The policy is set to off, so the policy is effective.

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa>

...

9. Confirm your settings and set Enable policy to On

...

The 'Report only' is just one of the three options by enable policy.

<https://youtu.be/NZbPYfhh5Kc>

upvoted 10 times

  **zuzu\_toggler** 3 years, 9 months ago

Doc Link shows the step #9.

upvoted 1 times

  **Richard\_M** 3 years, 3 months ago

The Enable Policy has 3 states:

1) Report-Only

2) On

3) Off

In this case, it is OFF, so correct answer is C

Look under the "Configure a Conditional Access policy in report-only mode" header in the Tips box. Can't be clearer than that

Also, you can test yourself, and click on one of the 3 states mentioned yourself

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-insights-reporting#configure-a-conditional-access-policy-in-report-only-mode>

upvoted 2 times

  **Richard\_M** 3 years, 3 months ago

I think I need to clarify my answer. This seems to be an existing Policy. Why? The Save button is not enabled. This means, that the current info on the screen is current status of the Policy. If the Enable Policy button had been "On", then the Answer B would be correct, because you would get a MFA Prompt OR validated if you are on a Hybrid Azure AD joined device since the "Require one of the selected controls" is selected. Note the questions state "Users WILL be".

upvoted 2 times

  **eloylb**  4 years, 6 months ago

The right answer is C because the policy is Off

upvoted 15 times

- 🗳️ 👤 **3nteng** 4 years, 3 months ago  
the off is the 'report only'. if that is on, it will only report and not enforce  
upvoted 3 times
- 🗳️ 👤 **ITStudies** 4 years, 3 months ago  
Dont misguide  
upvoted 4 times
- 🗳️ 👤 **jellybiscuit** Most Recent 🔍 2 years, 9 months ago  
Selected Answer: C  
The policy is definitely disabled (Off)  
It won't apply to anyone.  
upvoted 1 times
- 🗳️ 👤 **pingpongset** 2 years, 10 months ago  
what is the answer if it is ON?  
upvoted 3 times
- 🗳️ 👤 **kanchanar05** 3 years, 3 months ago  
B. Because Policy has not configured. Asking you to configure.  
upvoted 1 times
- 🗳️ 👤 **mabwwdb** 3 years, 3 months ago  
I agree with C being the correct answer if the policy is SAVED with the Enable Policy is kept OFF..., BUT depending on how the question is interpreted, correct answer could still be B. Because if the question is just meant to ask: What is the result of the policy WHEN APPLIED (meaning enabled), then the answer is B.  
upvoted 3 times
- 🗳️ 👤 **410ns0** 2 years, 11 months ago  
I agree with you  
upvoted 1 times
- 🗳️ 👤 **Tote** 3 years, 4 months ago  
Selected Answer: C  
C, the policy is off  
upvoted 1 times
- 🗳️ 👤 **AJ1313** 3 years, 5 months ago  
MS sometimes does really stupid confusing things & that's why I like AWS. The policy has three states, on, off and report only..  
upvoted 2 times
- 🗳️ 👤 **ixl2pass** 3 years, 5 months ago  
You need to know that MFA is enable by default since Oct 2019. So its not just dependent on this policy <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>  
So even if the policy is not enabled MFA is still active by virtue of security defaults and its enforced. So the given answer is correct.  
upvoted 1 times
- 🗳️ 👤 **SanjSL** 3 years, 5 months ago  
The 'Report only' option is selected by default.  
<https://youtu.be/NZbPYfhb5Kc>  
The policy is set to off, so the answer is C.  
upvoted 2 times
- 🗳️ 👤 **Sst121** 3 years, 6 months ago  
Selected Answer: C  
policy is not enabled  
upvoted 3 times
- 🗳️ 👤 **mtk93** 3 years, 6 months ago  
Selected Answer: C  
Since policy is set to OFF. Answer is C  
upvoted 3 times
- 🗳️ 👤 **Eitant** 3 years, 6 months ago  
Selected Answer: C  
Policy status is off

upvoted 4 times

🗨️ 👤 **examineezer** 3 years, 6 months ago

I don't think they are trying to catch you out. Its just a confusing question.

upvoted 1 times

🗨️ 👤 **raud** 3 years, 7 months ago

Section "Enable policy" is a subdivision to "MFA policy", parallel to "Assignments" and "Access control". Hence only Grant plays the role to this question.

upvoted 1 times

🗨️ 👤 **Mikhail1989** 3 years, 7 months ago

C is the correct answer.

upvoted 2 times

🗨️ 👤 **saninjesse** 3 years, 7 months ago

Answer should be C:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa>

After confirming your settings using report-only mode, an administrator can move the Enable policy toggle from Report-only to On.

upvoted 2 times

## HOTSPOT -

You have an Azure Active Directory (Azure AD) tenant.

You plan to use Azure Monitor to monitor user sign-ins and generate alerts based on specific user sign-in events.

You need to recommend a solution to trigger the alerts based on the events.

What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Send Azure AD logs to:

An Azure event hub
An Azure Log Analytics workspace
An Azure Storage account

Signal type to use for triggering the alerts:

Activity log
Log
Metric

**Suggested Answer:****Answer Area**

Send Azure AD logs to:

An Azure event hub
An Azure Log Analytics workspace
An Azure Storage account

Signal type to use for triggering the alerts:

Activity log
Log
Metric

Box 1: An Azure Log Analytics workspace

To be able to create an alert we send the Azure AD logs to An Azure Log Analytics workspace.

Note: You can forward your AAD logs and events to either an Azure Storage Account, an Azure Event Hub, Log Analytics, or a combination of all of these.

Box 2: Log -

Ensure Resource Type is an analytics source like Log Analytics or Application Insights and signal type as Log.

Reference:


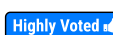
<https://4sysops.com/archives/how-to-create-an-azure-ad-admin-login-alert/> <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-log>

 **JasonYin**  4 years, 1 month ago

Answer is correct, we should query against Logs not 'Activity Log'.


'Activity Log' is for recording changes of Azure Resources such as create or modify Azure resource. We are asked to generate alert based on Sign in event, which should be 'Logs'.

upvoted 48 times

 **QiangQiang**  4 years, 1 month ago

the second should be "Activity Log"

upvoted 19 times

 **gssd4scoder** 4 years, 1 month ago



no, activity log records other kind of activities: <https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log>

upvoted 4 times

 **Kevmeister** 4 years ago

Agreed, As per <https://4sysops.com/archives/how-to-create-an-azure-ad-admin-login-alert/> it specifically states: "In the Log Analytics workspaces > platform - Logs tab, you gain access to the online Kusto Query Language (KQL) query editor. In my environment, the administrator I want to alert has a User Principal Name (UPN) of auobrien.david@outlook.com. We can run the following query to find all the login events for this user:"

upvoted 2 times

  **examineezer** 3 years, 6 months ago

There's another type of activity log

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-activity-logs-azure-monitor>

upvoted 1 times

  **examineezer** 3 years, 6 months ago

Having said that... when we create an "activity log" alert, this is linked to Resource Activity Logs, and not AAD Activity Logs. So QiangQiang is wrong.

upvoted 2 times

  **JayBee65** 3 years ago

No, The Azure Activity log provides insight into any subscription-level events that have occurred in Azure, e.g. all create, update, delete, and action operations performed through Resource Manager. All log types can be found here <https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log-schema>

upvoted 2 times

  **Snownoodles** Most Recent 2 years, 8 months ago

answer is correct:

<https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-create-new-alert-rule?tabs=metric>

upvoted 1 times

  **Snownoodles** 2 years, 8 months ago

Sorry, the 2nd should be "Activity log"



"Activity log alerts are triggered when a new activity log event occurs that matches the defined conditions"

<https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-overview#types-of-alerts>

Log is for "statistics" based on Log analytics.

"Activity Log" is for event

upvoted 1 times

  **One111** 2 years, 10 months ago

Log Analytics workspace to keep data longer than month and be able to use queries and alerts.

Sign-in logs to look for events related to authentication.

upvoted 1 times



  **AberdeenAngus** 3 years ago

Log alert: an alert created from a query in Log Analytics

Activity log alert: an alert created using the activity log as the source, nothing to do with log analytics

<https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-types>

upvoted 1 times

  **HananS** 3 years, 3 months ago

The first one is Azure Event, you can check the link

[https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/activity-](https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log#:~:text=CategoryValue%20%3D%20%22Administrative%22,Send%20to%20Azure%20Event%20Hubs,the%20records%20in%20each%20payload.)

[log#:~:text=CategoryValue%20%3D%20%22Administrative%22,Send%20to%20Azure%20Event%20Hubs,the%20records%20in%20each%20payload.](https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log#:~:text=CategoryValue%20%3D%20%22Administrative%22,Send%20to%20Azure%20Event%20Hubs,the%20records%20in%20each%20payload.)

upvoted 1 times

  **sharepoint\_Azure\_pp** 3 years, 8 months ago

Answer is correct

Choose the same cleared with 900 on 17th October 2021

upvoted 7 times

  **sandyman** 3 years, 8 months ago

Answer is correct -

Monitor sign-in and audit logs

Organizations should monitor sign-in and audit log activity from the emergency accounts and trigger notifications to other administrators. When you monitor the activity on break glass accounts, you can verify these accounts are only used for testing or actual emergencies. You can use Azure Log

Analytics to monitor the sign-in logs and trigger email and SMS alerts to your admins whenever break glass accounts sign in.

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

upvoted 2 times

🗨️ **syu31svc** 3 years, 9 months ago

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-integrate-activity-logs-with-log-analytics>

In the Diagnostic settings menu, select the Send to Log Analytics workspace check box, and then select Configure.

<https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-log>

Given answer is correct; Log Analytics Workspace and Log

upvoted 2 times

🗨️ **Gautam1985** 3 years, 10 months ago

correct

upvoted 2 times

🗨️ **kumarts** 3 years, 10 months ago

Given answer is correct. Kindly refer <https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-log>

upvoted 2 times

🗨️ **tvS2021** 3 years, 11 months ago

on exam (7-19-2021). passed 304

upvoted 4 times

🗨️ **RickMorais** 3 years, 10 months ago

Nice... but the relevant information was your choice in the test.

upvoted 3 times

🗨️ **JayBee65** 3 years ago

Not unless they scored 100%

upvoted 2 times

🗨️ **nsvijay04b1** 3 years, 10 months ago

congratulations.

Would be great if you confirm the right answer.

upvoted 3 times

🗨️ **norbiteK** 4 years ago

I believe answer is correct.

This scenario is described here:

<https://docs.microsoft.com/en-us/azure/active-directory/roles/security-emergency-access#create-an-alert-rule>

We have to use Custom log search that is assigned to Log signal type

upvoted 7 times

🗨️ **nicksb19** 4 years ago

Signal type Log and using "Custom log Search" is correct. Activity Log has only 9 options none of which satisfy to get sign-on details. Also the below is most likely the search query you need to include:

// All SigninLogs events

// All Azure signin events.

SigninLogs

| project UserDisplayName, Identity, UserPrincipalName, AppDisplayName, AppId, ResourceDisplayName

upvoted 3 times

🗨️ **GetulioJr** 4 years ago

The answer is correct:

I noticed that are some question on the second box if it is Activity Log or Log and even though you would find sign-in information in both, you can only do query based on KUSTO with LOG, and as the admin wants to me notified "based on specific user sign-in events.", so LOG here is the right one, as he will be able to create a query to define this specific event. That is the reason LOG is chosen here.

So answer is correct.

upvoted 3 times

  **neokrieg** 4 years ago

Answers are correct for second box you can use log for alerting <https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-unified-log>

upvoted 1 times

  **erickim007** 4 years, 1 month ago

User Sign-in is 'Activity Log' and 'Activity Log' is available signal.

Therefore the second should be 'Activity Log'.

upvoted 3 times

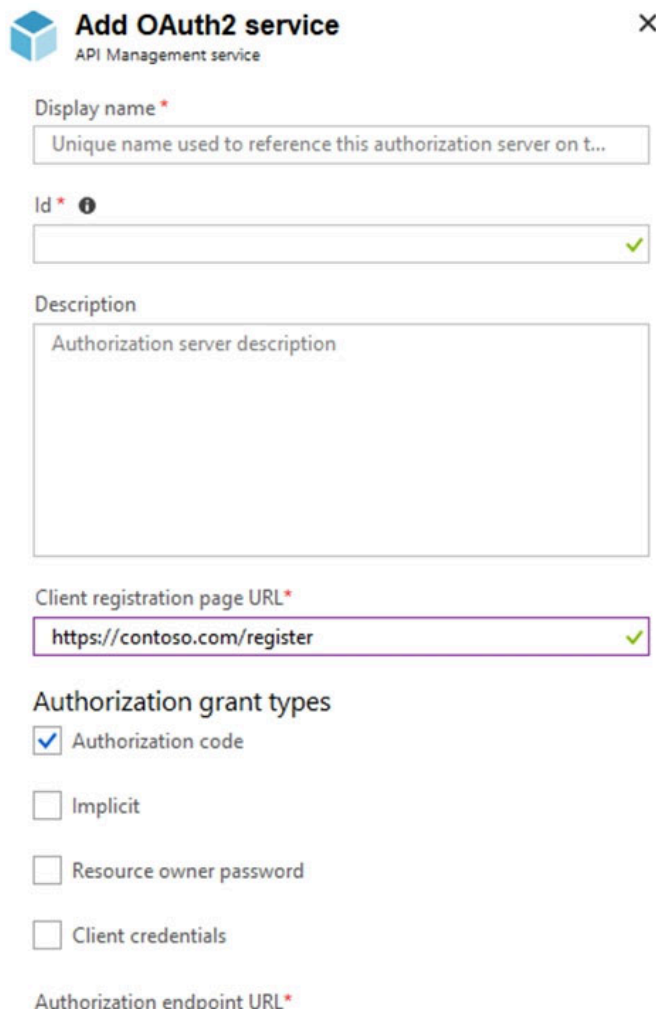
  **Oracleist** 4 years, 1 month ago

Monitor generate alerts on Metric and ACTIVITY LOG only!!

upvoted 3 times

## HOTSPOT -

You configure OAuth2 authorization in API Management as shown in the following exhibit.



**Add OAuth2 service**  
API Management service

Display name \*  
Unique name used to reference this authorization server on t...

Id \* ⓘ  
[ ] ✓

Description  
Authorization server description

Client registration page URL \*  
https://contoso.com/register ✓

**Authorization grant types**

☒ Authorization code

☐ Implicit

☐ Resource owner password

☐ Client credentials

Authorization endpoint URL \*

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

The selected authorization grant type is for [answer choice].

- Background services
- Headless device authentication
- Web applications

To enable custom data in the grant flow, select [answer choice].

- Client credentials
- Resource owner password
- Support state parameter

Suggested Answer:

**Answer Area**

The selected authorization grant type is for [answer choice].

- Background services
- Headless device authentication
- Web applications

To enable custom data in the grant flow, select [answer choice].

- Client credentials
- Resource owner password
- Support state parameter

Box 1: Web applications -



The Authorization Code Grant Type is used by both web apps and native apps to get an access token after a user authorizes an app.

Note: The Authorization Code grant type is used by confidential and public clients to exchange an authorization code for an access token.

After the user returns to the client via the redirect URL, the application will get the authorization code from the URL and use it to request an access token.

Incorrect Answers:

Not Headless device authentication:

A headless system is a computer that operates without a monitor, graphical user interface (GUI) or peripheral devices, such as keyboard and mouse.

Headless computers are usually embedded systems in various devices or servers in multi-server data center environments. Industrial machines, automobiles, medical equipment, cameras, household appliances, airplanes, vending machines and toys are among the myriad possible hosts of embedded systems.

Box 2: Client Credentials -

How to include additional client data

In case you need to store additional details about a client that don't fit into the standard parameter set the custom data parameter comes to help:

POST /c2id/clients HTTP/1.1 -

Host: demo.c2id.com -

Content-Type: application/json -

Authorization: Bearer ztucZS1ZyFKgh0tUEruUtiSTXhnexmd6

```
{
  "redirect_uris": [ "https://myapp.example.com/callback" ],
  "data": { "reg_type": "3rd-party",
    "approved": true,
    "author_id": 792440 }
}
```


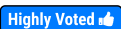
The data parameter permits arbitrary content packaged in a JSON object. To set it you will need the master registration token or a one-time access token with a client-reg:data scope.

Incorrect Answers:

Authorization protocols provide a state parameter that allows you to restore the previous state of your application. The state parameter preserves some state object set by the client in the Authorization request and makes it available to the client in the response.

Reference:

<https://developer.okta.com/blog/2018/04/10/oauth-authorization-code-grant-type> <https://connect2id.com/products/server/docs/guides/client-registration>

 **dadageer**  4 years, 2 months ago

Correct!

<https://docs.microsoft.com/en-us/azure/api-management/api-management-howto-oauth2>

upvoted 23 times

 **express**  3 years, 11 months ago

Should be D - support state parameters

upvoted 20 times

 **us3r** 3 years, 4 months ago

support state parameter is not related with the custom data.

Use of the state parameter:

If a state parameter is included in the request, the same value should appear in the response. The app should verify that the state values in the request and response are identical.

Link <https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-auth-code-flow>

Correct answer: Client credentials

reason: read the explanation in the answer field

upvoted 2 times

🗨️ **Bijith** 3 years, 10 months ago

Right. it should be support state parameters

upvoted 4 times

🗨️ **JaQua** Most Recent 3 years ago

support state param:

[https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-auth-code-](https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-auth-code-flow#:~:text=The%20value%20can%20also%20encode%20information%20about%20the%20user%27s%20state%20in%20the%20app%20before%20the%20autl)

[flow#:~:text=The%20value%20can%20also%20encode%20information%20about%20the%20user%27s%20state%20in%20the%20app%20before%20the%20autl](https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-auth-code-flow#:~:text=The%20value%20can%20also%20encode%20information%20about%20the%20user%27s%20state%20in%20the%20app%20before%20the%20autl)

upvoted 1 times

🗨️ **OCHT** 3 years, 1 month ago

I selected Web Application and State Parameter

upvoted 1 times

🗨️ **itenginerd** 3 years, 3 months ago

On my exam today.

upvoted 2 times

🗨️ **examineezer** 3 years, 6 months ago

After reading this link I believe that the "Client Credentials" GRANT TYPE is not what most people think. Therefore I believe the answer is support state parameter.

<https://docs.microsoft.com/en-us/azure/api-management/api-management-howto-oauth2>

upvoted 1 times

🗨️ **Dpejic** 3 years, 6 months ago

On exam 24.12.2021

upvoted 2 times

🗨️ **Dpejic** 3 years, 6 months ago

Appere on exam 23-dec-2021

upvoted 2 times

🗨️ **sharepoint\_Azure\_pp** 3 years, 8 months ago

Mentioned answers are correct.

Choose the same cleared with 900 on 17th October 2021

upvoted 5 times

🗨️ **waqas** 3 years, 8 months ago

Mentioned Answers are correct.

upvoted 1 times

🗨️ **syu31svc** 3 years, 9 months ago

<https://docs.microsoft.com/en-us/azure/api-management/api-management-howto-oauth2>

I would go with the answers provided

upvoted 4 times

🗨️ **niravkanakhara** 3 years, 9 months ago

Its API managment, so web appliation is acutally API and authorization code is also selected. Answer should be Web Application and Client Credential to authorize api using Azure AD JWT token.

upvoted 1 times

🗨️ **nkV** 3 years, 9 months ago

I passed on 20-sep-21, I choose second as support state parameters, first web application

upvoted 2 times

🗨️ **dennnnnnnnnn** 3 years, 10 months ago

Agreed should be D - support state parameters

custom data means "state" in oauth2 grant flow

upvoted 4 times

🗨️ **BoxGhost** 3 years, 10 months ago

I'm also leaning towards support state based on this:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-client-creds-grant-flow>

A value that's included in the request that's also returned in the token response. It can be a string of any content that you want. The state is used to encode information about the user's state in the app before the authentication request occurred, such as the page or view they were on.

upvoted 2 times

🗨️ 👤 **Preppy** 3 years, 10 months ago

Answer to the second part should be to enable the Support State Parameters checkbox. See the AAD Developer Support team blog article that details this: <https://blogs.aaddevsup.xyz/2019/11/state-parameter-in-mvc-application/>

By enabling that box, you enable the use of the State parameter in the request, to which you can add additional state data via a dictionary. When the token is returned back, you are then returned this custom data as shown in the article.

This is the preferred way to support custom data, per the RFC for oauth 2.0, section 3.1.2.2: <https://datatracker.ietf.org/doc/html/rfc6749#section-3.1.2.2>: "the client MAY use the "state" request parameter to achieve per-request customization."

upvoted 8 times

🗨️ 👤 **tv2021** 3 years, 11 months ago

on exam (7-19-2021). passed 304.

upvoted 2 times

🗨️ 👤 **RickMorais** 3 years, 10 months ago

Given answer, pleeeeeease.

upvoted 3 times

🗨️ 👤 **nsvijay04b1** 3 years, 10 months ago

Congratulations and thanks.

It would be great if you confirm what is correct answer.

upvoted 3 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. Your company has deployed several virtual machines (VMs) on-premises and to Azure. Azure ExpressRoute has been deployed and configured for on-premises to Azure connectivity.

Several VMs are exhibiting network connectivity issues.

You need to analyze the network traffic to determine whether packets are being allowed or denied to the VMs.

Solution: Use Azure Network Watcher to run IP flow verify to analyze the network traffic.

Does the solution meet the goal?

A. Yes

B. No

#### Suggested Answer: A

The Network Watcher Network performance monitor is a cloud-based hybrid network monitoring solution that helps you monitor network performance between various points in your network infrastructure. It also helps you monitor network connectivity to service and application endpoints and monitor the performance of

Azure ExpressRoute.

Note:

IP flow verify checks if a packet is allowed or denied to or from a virtual machine. The information consists of direction, protocol, local IP, remote IP, local port, and remote port. If the packet is denied by a security group, the name of the rule that denied the packet is returned. While any source or destination IP can be chosen,

IP flow verify helps administrators quickly diagnose connectivity issues from or to the internet and from or to the on-premises environment.

IP flow verify looks at the rules for all Network Security Groups (NSGs) applied to the network interface, such as a subnet or virtual machine NIC. Traffic flow is then verified based on the configured settings to or from that network interface. IP flow verify is useful in confirming if a rule in a Network Security Group is blocking ingress or egress traffic to or from a virtual machine.

Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview> <https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview>

Community vote distribution

A (100%)

 **sharepoint\_Azure\_pp** Highly Voted 3 years, 8 months ago

This was there as 2nd set of 3 Y/N question.

Azure network watcher is correct

Choose the same cleared with 900 on 17th October 2021

upvoted 16 times

 **pentium75** Highly Voted 3 years, 10 months ago

I think it's clearly "Yes" what they are after. But still, a thought: The company has several VMs in cloud and several VMs on premises. We are not told which VMs experience network issues, thus in theory it could be that the issue is between two on-premise VMs. Wouldn't Network Watcher be unable to support this investigation?

upvoted 6 times

 **examineezer** 3 years, 6 months ago

Valid observation.

upvoted 1 times

 **jr\_luciano** Most Recent 3 years, 4 months ago

Selected Answer: A

Answer is Yes

upvoted 2 times

 **syu31svc** 3 years, 9 months ago

This is the correct solution



Answer is Yes

upvoted 3 times

  **El\_Hechizo** 3 years, 11 months ago

Correct see: <https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview#:~:text=IP%20flow%20verify%20checks%20if,denied%20the%20packet%20is%20returned>.

upvoted 3 times

  **tvS2021** 3 years, 11 months ago

on exam (7-19-2021). cleared 304.

upvoted 3 times

  **gssd4scoder** 4 years ago

Correct <https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview>. It was something similar in AZ-303 and I passed the exam.

upvoted 4 times

  **Puspendu** 4 years ago

Seems to be correct

upvoted 4 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. Your company has deployed several virtual machines (VMs) on-premises and to Azure. Azure ExpressRoute has been deployed and configured for on-premises to Azure connectivity.

Several VMs are exhibiting network connectivity issues.

You need to analyze the network traffic to determine whether packets are being allowed or denied to the VMs.

Solution: Use the Azure Advisor to analyze the network traffic.

Does the solution meet the goal?

A. Yes

B. No

#### Suggested Answer: B

Instead use Azure Network Watcher to run IP flow verify to analyze the network traffic.

Note: Advisor is a personalized cloud consultant that helps you follow best practices to optimize your Azure deployments. It analyzes your resource configuration and usage telemetry and then recommends solutions that can help you improve the cost effectiveness, performance, high availability, and security of your Azure resources.

With Advisor, you can:

Get proactive, actionable, and personalized best practices recommendations.

Improve the performance, security, and high availability of your resources, as you identify opportunities to reduce your overall Azure spend.

Get recommendations with proposed actions inline.

Reference:

<https://docs.microsoft.com/en-us/azure/advisor/advisor-overview>

Community vote distribution

B (100%)

 **gssd4scoder** Highly Voted 4 years ago

Correct: no. It's Azure Network Watcher what you need.

upvoted 9 times

 **jr\_luciano** Most Recent 3 years, 4 months ago

Selected Answer: B

Answer is No

upvoted 1 times

 **sharepoint\_Azure\_pp** 3 years, 8 months ago

This was there as 2nd set of 3 Y/N question.

Azure network watcher is correct

Choose the same cleared with 900 on 17th October 2021

upvoted 4 times

 **syu31svc** 3 years, 9 months ago

Advisor does not perform such a requirement

Answer is No for sure

upvoted 1 times

 **Gautam1985** 3 years, 10 months ago

Correct

upvoted 1 times

 **tvS2021** 3 years, 11 months ago



on exam (7-19-2021). passed 304

upvoted 2 times

 **RickMorais** 3 years, 10 months ago



administrator. Could you please delete this user?

upvoted 3 times

  **Viji30** 3 years, 9 months ago

why? why? why?

upvoted 1 times

  **Viji30** 3 years, 9 months ago

Only users who has the role of moderator who can perform this action.

incorrect answer: administrator

upvoted 4 times

You have 500 Azure web apps in the same Azure region. The apps use a premium Azure key vault for authentication. A developer reports that some authentication requests are being throttled. You need to recommend a solution to increase the available throughput of the key vault. The solution must minimize costs. What should you recommend?

- A. Change the pricing tier.
- B. Configure geo-replication.
- C. Configure load balancing for the apps.
- D. Increase the number of key vaults in the subscription.

**Suggested Answer: D**

To maximize your Key Vault throughput rates, here are some recommended guidelines/best practices for maximizing your throughput:

1. Ensure you have throttling in place. Client must honor exponential back-off policies for 429's and ensure you are doing retries as per the guidance below.
2. Divide your Key Vault traffic amongst multiple vaults and different regions. Use a separate vault for each security/availability domain. If you have five apps, each in two regions, then we recommend 10 vaults each containing the secrets unique to app and region.

Reference:

<https://docs.microsoft.com/en-us/azure/key-vault/general/overview-throttling>

Community vote distribution

D (100%)

🗳️ 👤 **Raj1703** Highly Voted 3 years, 12 months ago

This is correct and logical. Expansion of Geography will not reduce throttle. Moreover, pricing tier does not make sense when the ask is to optimize cost. Increase vault instance is the right choice under given circumstance.

upvoted 14 times

🗳️ 👤 **cfsxtuv33** 3 years, 11 months ago

Agreed, increasing vault instance is correct.

upvoted 2 times

🗳️ 👤 **simonevenezia** 3 years, 9 months ago

D is the correct answer. Read better <https://docs.microsoft.com/en-us/azure/key-vault/general/overview-throttling#how-does-key-vault-handle-its-limits>, link in explanation too.

upvoted 3 times

🗳️ 👤 **pentium75** 3 years, 10 months ago

Would there even be a higher pricing tier than Premium (the current one)?

upvoted 4 times

🗳️ 👤 **sharepoint\_Azure\_pp** Highly Voted 3 years, 8 months ago

Option D is correct

Choose the same cleared with 900 on 17th October 2021

upvoted 8 times

🗳️ 👤 **itenginerd** Most Recent 3 years, 3 months ago

**Selected Answer: D**

On my exam today.

upvoted 3 times

🗳️ 👤 **us3r** 3 years, 4 months ago

**Selected Answer: D**

increase the number of key vaults

upvoted 1 times

🗳️ 👤 **Eitant** 3 years, 6 months ago

**Selected Answer: D**

Correct answer





upvoted 1 times

  **syu31svc** 3 years, 9 months ago

Provided link supports the answer given

D is correct

upvoted 1 times

  **Entarch** 3 years, 12 months ago

Correct answer

upvoted 7 times

## DRAG DROP -

Your on-premises network contains a server named Server1 that runs an ASP.NET application named App1.

You have a hybrid deployment of Azure Active Directory (Azure AD).

You need to recommend a solution to ensure that users sign in by using their Azure AD account and Azure Multi-Factor Authentication (MFA) when they connect to App1 from the internet.

Which three Azure services should you recommend be deployed and configured in sequence? To answer, move the appropriate services from the list of services to the answer area and arrange them in the correct order.

Select and Place:

**Services****Answer Area**

an internal Azure Load Balancer

an Azure AD conditional access policy

Azure AD Application Proxy

an Azure AD managed identity

a public Azure Load Balancer

an Azure AD enterprise application

an App Service plan

**Suggested Answer:****Services****Answer Area**

an internal Azure Load Balancer

an Azure AD conditional access policy

Azure AD Application Proxy

an Azure AD managed identity

a public Azure Load Balancer

an Azure AD enterprise application

an App Service plan

Azure AD Application Proxy

an Azure AD managed identity

an Azure AD enterprise application

**Step 1: Azure AD Application proxy**

Azure AD Application Proxy is a prerequisite for a scenario with an on-premises legacy applications published for cloud access,

Note: Application Proxy is a feature of Azure AD that enables users to access on-premises web applications from a remote client. Application Proxy includes both the Application Proxy service which runs in the cloud, and the Application Proxy connector which runs on an on-premises server.

**Step 2: an Azure AD managed identity**

Microsoft's identity solutions span on-premises and cloud-based capabilities. These solutions create a common user identity for authentication and authorization to all resources, regardless of location. We call this hybrid identity.

**Step 3: an Azure AD conditional access policy**

Conditional Access is the tool used by Azure Active Directory to bring signals together, to make decisions, and enforce organizational policies. Conditional Access is at the heart of the new identity driven control plane.

With hybrid identity to Azure AD and hybrid identity management these scenarios become possible.

**Reference:**

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted> <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview>

🗄️ 👤 **norbitek** Highly Voted 4 years ago

For me it should be:

AD Application Proxy

AD Enterprise Application

AD Conditional access policy

upvoted 117 times

🗄️ 👤 **norbitek** 3 years, 12 months ago

Following blog describes how to do that:

<https://thesleepyadmins.com/2019/02/>

upvoted 10 times

🗄️ 👤 **vitol** Highly Voted 3 years, 12 months ago

First AD Enterprise APPLICATION to register APP

Second APP Proxy (only IWA,SAML,WSFED authentication methods are available)

Third Conditional Access

upvoted 19 times

🗄️ 👤 **pentium75** 3 years, 10 months ago

Question is in which order to DEPLOY the services. And before you can configure application proxy for your registered enterprise app, you must first deploy application proxy connector. MS document lists it in this order:

1. Deploy Application Proxy connector
2. Create Enterprise App
3. Configure Application Proxy in Enterprise App

upvoted 10 times

🗄️ 👤 **DChilds** Most Recent 2 years, 10 months ago

AD Application Proxy

AD Enterprise Application

<https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-add-on-premises-application>.

AD Conditional access policy

upvoted 4 times

🗄️ 👤 **AubinBakana** 2 years, 10 months ago

How could they get this wrong?

The App does get a Managed ID once added to Enterprise App, so no need for that.

The answer should be:

- Enterprise App
- Application Proxy
- Conditional Access

upvoted 3 times

🗄️ 👤 **cloudera** 3 years, 3 months ago

Based on this article, the correct answer should be:

<https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-add-on-premises-application>

1. Application Proxy
2. Enterprise Application Registration
3. Conditional Access - the article doesn't cover but it is obvious to enable MFA which is one of the requirements in the question.

upvoted 5 times

🗄️ 👤 **itengineerd** 3 years, 3 months ago

On my exam today.

upvoted 1 times

🗄️ 👤 **plmmsg** 3 years, 3 months ago

1. AD Application Proxy
2. AD Enterprise App
3. AD Conditional Access Policy

upvoted 3 times

🗳️ 👤 **Preeto18** 3 years, 3 months ago

Answer is :

AD Application Proxy

AD Enterprise Application

AD Conditional access policy

upvoted 2 times

🗳️ 👤 **[Removed]** 3 years, 5 months ago

AD proxy

AD enterprise app

Conditional policy

upvoted 4 times

🗳️ 👤 **ScubaDiver123456** 3 years, 6 months ago

I believe it should be

AD App Proxy

Enterprise App registration

Conditional Access

<https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-add-on-premises-application>

upvoted 2 times

🗳️ 👤 **Dpejic** 3 years, 6 months ago

On exam 24.12.2021

upvoted 2 times

🗳️ 👤 **Dpejic** 3 years, 6 months ago

In exam today 22-dec-2021

upvoted 2 times

🗳️ 👤 **Foxywolf** 3 years, 6 months ago

[https://youtu.be/\\_2kWq5H4NhY](https://youtu.be/_2kWq5H4NhY)

upvoted 3 times

🗳️ 👤 **sharepoint\_Azure\_pp** 3 years, 8 months ago

It should be:

AD Application Proxy

AD Enterprise Application

AD Conditional access policy

is correct choose the same

cleared with 900 on 17th October 2021

upvoted 13 times

🗳️ 👤 **sharepoint\_Azure\_pp** 3 years, 8 months ago

it should be:

AD Application Proxy

AD Enterprise Application

AD Conditional access policy

Choose the same cleared with 900 on 17th October 2021

upvoted 3 times

🗳️ 👤 **syu31svc** 3 years, 9 months ago

<https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-add-on-premises-application>

Install and register a connector


Under Manage, select Application proxy (Step1)

Add an on-premises app to Azure AD

Select Enterprise applications, and then select New application (Step 2)

Need MFA so last step is Conditional Access

upvoted 3 times

  **souvik123** 3 years, 9 months ago

AD Application Proxy

AD Enterprise Application

AD Conditional access policy

upvoted 5 times

A company named Contoso, Ltd. has an Azure Active Directory (Azure AD) tenant that is integrated with Microsoft 365 and an Azure subscription. Contoso has an on-premises identity infrastructure. The infrastructure includes servers that run Active Directory Domain Services (AD DS), Active Directory

Federation Services (AD FS), Azure AD Connect, and Microsoft Identity Manager (MIM).

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Active Directory forest and a Microsoft 365 tenant. Fabrikam has the same on-premises identity infrastructure components as Contoso.

A team of 10 developers from Fabrikam will work on an Azure solution that will be hosted in the Azure subscription of Contoso. The developers must be added to the Contributor role for a resource group in the Contoso subscription.

You need to recommend a solution to ensure that Contoso can assign the role to the 10 Fabrikam developers. The solution must ensure that the Fabrikam developers use their existing credentials to access resources.

What should you recommend?

- A. Configure an AD FS relying party trust between the Fabrikam and Contoso AD FS infrastructure.
- B. In the Azure AD tenant of Contoso, create cloud-only user accounts for the Fabrikam developers.
- C. Configure an organization relationship between the Microsoft 365 tenants of Fabrikam and Contoso.
- D. In the Azure AD tenant of Contoso, use MIM to create guest accounts for the Fabrikam developers.

**Suggested Answer: D**


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.

Reference:

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

Community vote distribution

D (100%)

 **syu31svc** Highly Voted 3 years, 9 months ago

"Contoso has a partnership with a company named Fabrikam" so this would mean Azure AD B2B

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

Answer is D

upvoted 13 times

 **jr\_luciano** Most Recent 3 years, 4 months ago

But if you create guest accounts, you are not meeting this requirement: "The solution must ensure that the Fabrikam developers use their existing credentials to access resources."

upvoted 1 times

 **jr\_luciano** 3 years, 4 months ago

Sorry, the given answer is correct!

upvoted 1 times

 **Uglydotcom** 3 years, 4 months ago

Selected Answer: D

Only D is providing Guest access to Contoso. Guest access will allow them to use their creds.

upvoted 2 times

 **agente232** 3 years, 5 months ago

answer D does not fulfill the requirements as it is creating guest accounts

D. In the Azure AD tenant of Contoso, use MIM to create guest accounts for the Fabrikam developers.

upvoted 1 times

 **yyuryyucicuryyforme** 3 years, 5 months ago

Actually answer D does certainly work for granting Fabrikam Azure AD tenant existing identities access to Contoso Azure subscription resources

upvoted 1 times

🗨️ 👤 **yyuryyucicuryyforme** 3 years, 5 months ago

<https://docs.microsoft.com/en-us/microsoft-identity-manager/microsoft-identity-manager-2016-connector-graph>  
upvoted 1 times

🗨️ 👤 **ksml** 3 years, 8 months ago

Why not B? I don't see any MIM reference on linked page: <https://docs.microsoft.com/en-us/azure/active-directory/external-identities/what-is-b2b>  
upvoted 1 times

🗨️ 👤 **examineezer** 3 years, 6 months ago

Reference to MIM here

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/hybrid-cloud-to-on-premises>  
upvoted 2 times

🗨️ 👤 **examineezer** 3 years, 6 months ago

Apologies - the link above seems to be specifically for accessing on-premise applications. You may be right, maybe it is B.  
upvoted 1 times

🗨️ 👤 **examineezer** 3 years, 6 months ago

Nope - B is wrong because:

"A cloud-only user account is an account that was created in your Azure AD directory using either the Azure portal or Azure AD PowerShell cmdlets. These user accounts aren't synchronized from an on-premises directory."

...and...

"The solution must ensure that the Fabrikam developers use their existing credentials to access resources."

upvoted 2 times

🗨️ 👤 **examineezer** 3 years, 6 months ago

<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/tutorial-create-instance#enable-user-accounts-for-azure-ad-ds>  
upvoted 1 times

🗨️ 👤 **VincentZhang** 3 years, 9 months ago

Answer is correct  
upvoted 4 times

You are designing an Azure governance solution.

All Azure resources must be easily identifiable based on the following operational information: environment, owner, department, and cost center.

You need to ensure that you can use the operational information when you generate reports for the Azure resources.

What should you include in the solution?

- A. an Azure data catalog that uses the Azure REST API as a data source
- B. Azure Active Directory (Azure AD) administrative units
- C. an Azure management group that uses parent groups to create a hierarchy
- D. an Azure policy that enforces tagging rules

**Suggested Answer: D**

You use Azure Policy to enforce tagging rules and conventions. By creating a policy, you avoid the scenario of resources being deployed to your subscription that don't have the expected tags for your organization. Instead of manually applying tags or searching for resources that aren't compliant, you create a policy that automatically applies the needed tags during deployment.

Note: Organizing cloud-based resources is a crucial task for IT, unless you only have simple deployments. Use naming and tagging standards to organize your resources for these reasons:

Resource management: Your IT teams will need to quickly locate resources associated with specific workloads, environments, ownership groups, or other important information. Organizing resources is critical to assigning organizational roles and access permissions for resource management.

Reference:

<https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/decision-guides/resource-tagging> <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-policies>

Community vote distribution

D (100%)

AlanJP **Highly Voted** 3 years, 12 months ago

I agree - answer seems correct

upvoted 20 times

OCHT **Most Recent** 3 years, 1 month ago

**Selected Answer: D**

D is correct.

upvoted 2 times

hertino 3 years, 2 months ago

In AZ-305 exam, 9 april 22

upvoted 3 times

jr\_luciano 3 years, 4 months ago

**Selected Answer: D**

Correct Answer: D

upvoted 1 times

jamlearn 3 years, 5 months ago

**Selected Answer: D**

correct answer

upvoted 1 times

Eitant 3 years, 6 months ago

**Selected Answer: D**

Correct answer

upvoted 1 times

gssd4scoder 3 years, 8 months ago

Hundred percent is D

upvoted 3 times



🗨️ 👤 **syu31svc** 3 years, 9 months ago  
"easily identifiable"

Answer is tagging for sure; D  
upvoted 3 times

🗨️ 👤 **murongqing** 3 years, 10 months ago  
correct  
upvoted 2 times

🗨️ 👤 **Ykh** 3 years, 10 months ago  
Given answer is correct.  
upvoted 1 times

🗨️ 👤 **gssd4scoder** 3 years, 12 months ago  
Reply is D  
upvoted 4 times

## HOTSPOT -

You are designing an access policy for your company.

Occasionally, the developers at the company must stop, start, and restart Azure virtual machines. The development team changes often.

You need to recommend a solution to provide the developers with the required access to the virtual machines. The solution must meet the following requirements:

- ⇒ Provide permissions only when needed.
- ⇒ Use the principle of least privilege.
- ⇒ Minimize costs.

What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Azure Active Directory (Azure AD) license:

Free
Premium P1
Premium P2

Security feature:

Just in time VM access
A conditional access policy
Azure AD Privileged Identity Management

### Answer Area

Azure Active Directory (Azure AD) license:

Free
Premium P1
Premium P2

Suggested Answer:

Security feature:

Just in time VM access
A conditional access policy
Azure AD Privileged Identity Management

AlanJP Highly Voted 3 years, 12 months ago

I think answer is correct. JIT is for access to the VM, not access to the resource in the portal which is required to start/stop the VM  
upvoted 54 times

somenick 3 years, 12 months ago

Agree. See: <https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-configure-role-settings>  
upvoted 6 times

rdemontis 3 years, 7 months ago

exactly, you are right!  
upvoted 2 times

Nand0111 Highly Voted 4 years ago

Second option should be Just in time vm access  
upvoted 15 times

rjwolf82 3 years, 3 months ago

Not true, JIT is an option to enable RDP access for someone up to 24 hours, after that the access will be automatically disabled. Someone with JIT access can't start, stop VM's.  
upvoted 1 times

norbitek 3 years, 12 months ago


For me answer is correct.

just-in-time VM access do not implement user-based assignment.

Better option is to use PIM and just-in-time role assignments

See: <https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-configure-role-settings>

upvoted 20 times

 **BrettusMaximus** 3 years, 11 months ago

Agreed Answer is correct- In addition JIT needs the Defender licence.


upvoted 3 times

 **BoxGhost** 3 years, 10 months ago

Please stop up voting this. The question clearly states they need to stop and start the VM. JIT is only for RDP access, thus it does not meet the requirements.

<https://azure.microsoft.com/en-gb/blog/just-in-time-vm-access-is-generally-available/>

upvoted 71 times

 **us3r** 3 years, 4 months ago


highly voted they said... upvote they said...

upvoted 1 times

 **Sathya22** 3 years, 9 months ago

Yes JIT is only for access

upvoted 4 times

 **icedog** Most Recent 3 years, 5 months ago

You can't Start a VM with Just-In-Time access so it's an invalid answer

P2 and PIM are the correct answers

upvoted 7 times

 **FinMessner** 3 years, 5 months ago

For everyone saying JIT VM Access -- if JITVMA only allows RDP and SSH access then how will you start the VM once you've stopped it if you can't access the VM control panel?

upvoted 2 times

 **tomatosis** 3 years, 6 months ago


I think should be JIT instead. The question clearly says that "You need to recommend a solution to provide the developers with the required access to the virtual machines", so the key is to "access" only. Once we have JIT in place, then developers can start/stop VM as necessary. Dont forget we have to minimize the cost as well.

upvoted 1 times

 **tomatosis** 3 years, 6 months ago

To add, P2 is required for Just in Time <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing#available-versions-of-azure-ad-multi-factor-authentication>

upvoted 1 times

 **waqas** 3 years, 8 months ago

Mentioned Answers are correct.


upvoted 2 times

 **syu31svc** 3 years, 8 months ago

To achieve the requirement, you need to implement Azure AD Privileged Identity Management (PIM). Privileged Identity Management (PIM) is a service in Azure Active Directory (Azure AD) that enables you to manage, control, and monitor access to important resources in your organization. Using PIM feature requires an Azure AD Premium P2 license.


Answer is correct

upvoted 2 times

 **nkV** 3 years, 9 months ago

came in exam on 20-sep-21, I passed, i choose second one as just in time access

upvoted 2 times

 **jamess** 3 years, 10 months ago

PIM gives greater control including the ability to grant JIT. <https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

Fulfills requirements. Requires P2 lic.

upvoted 2 times

🗨️ 👤 **tita\_tovenaar** 3 years, 11 months ago

Since developers change often, I guess PIM becomes a true hassle. Not just are their accounts temporary, but temp access to VMs have to be dealt with separately. And who is going to approve? another config headache.

It's definitely cheaper, and probably easier, to just enable JIT access to the VMs.

If developers had been stable, maybe PIM could work.

upvoted 1 times

🗨️ 👤 **tita\_tovenaar** 3 years, 11 months ago

... and just to add, if JIT access is sufficient, then you don't need P2 either.

upvoted 1 times

🗨️ 👤 **examineezer** 3 years, 6 months ago

But JIT isn't sufficient.

upvoted 1 times

🗨️ 👤 **sandeepreddytalla** 3 years, 11 months ago

p2

PIM

JIT Need Azure defender, need to pay 15USD for every VM.

upvoted 5 times

🗨️ 👤 **vitol** 3 years, 12 months ago

100% answer is correct. (JIT is just a RDP rule in NSG nothing much)

upvoted 3 times

## HOTSPOT -

You have the Free edition of a hybrid Azure Active Directory (Azure AD) tenant. The tenant uses password hash synchronization.

You need to recommend a solution to meet the following requirements:

- ⇒ Prevent Active Directory domain user accounts from being locked out as the result of brute force attacks targeting Azure AD user accounts.
- ⇒ Block legacy authentication attempts to Azure AD integrated apps.
- ⇒ Minimize costs.

What should you recommend for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

To protect against brute force attacks:

	▼
Azure AD Password Protection	
Conditional access policies	
Pass-through authentication	
Smart lockout	

To block legacy authentication attempts:

	▼
Azure AD Application Proxy	
Azure AD Password Protection	
Conditional access policies	
Enable Security defaults	

**Suggested Answer:****Answer Area**

To protect against brute force attacks:

	▼
Azure AD Password Protection	
Conditional access policies	
Pass-through authentication	
Smart lockout	

To block legacy authentication attempts:

	▼
Azure AD Application Proxy	
Azure AD Password Protection	
Conditional access policies	
Enable Security defaults	

**Box 1: Smart lockout -**

Smart lockout helps lock out bad actors that try to guess your users' passwords or use brute-force methods to get in. Smart lockout can recognize sign-ins that come from valid users and treat them differently than ones of attackers and other unknown sources. Attackers get locked out, while your users continue to access their accounts and be productive.

**Box 2: Conditional access policies**

If your environment is ready to block legacy authentication to improve your tenant's protection, you can accomplish this goal with Conditional Access.

How can you prevent apps using legacy authentication from accessing your tenant's resources? The recommendation is to just block them with a Conditional

Access policy. If necessary, you allow only certain users and specific network locations to use apps that are based on legacy authentication.

Reference:

🗨️ 👤 **MrRandom** Highly Voted 3 years, 10 months ago

Glven answers are not correct, as they are using Azure AD Free.

-Smart Lockout requires Azure AD P1 or higher (Source: <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>)

-Conditional Access Policies requires Azure AD P1 or higher (Source: <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>)

Correct answers are Pass-Through Authentication (PTA) and Security Defaults

PTA Rationale: Authentication and password policy is handled by OnPrem DCs. We can configure security policies OnPrem to disable and account for X amount of minutes for password spray attacks.

Security Defaults: Blocking legacy authentication protocols (Source: <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>)

This also minimizes cost.

upvoted 51 times

🗨️ 👤 **kilowd** 2 years, 11 months ago

Smart lockout

Security defaults

Smart lockout is always on, for all Azure AD customers, with these default settings that offer the right mix of security and usability.

CUSTOMIZATION of the smart lockout settings, with values specific to your organization, requires Azure AD Premium P1 or higher licenses for your users.

upvoted 3 times

🗨️ 👤 **sapien45** 3 years ago

Thank you for the smart explanations

upvoted 1 times

🗨️ 👤 **[Removed]** 3 years, 10 months ago

Smart lockout is always on, for all Azure AD customers, with these default settings that offer the right mix of security and usability. Customization of the smart lockout settings, with values specific to your organization, requires Azure AD Premium P1 or higher licenses for your users.

Pass through auth wont stop on prem accounts being locked out, quite the opposite.

Smart lockout and Security Defaults make the most sense for Azure AD Free customers

upvoted 44 times

🗨️ 👤 **kktamang** 3 years, 3 months ago

No. Read question carefully. It says infra runs with Azure free license. Smart lock and conditional access need AAD premium P1 license.

upvoted 1 times

🗨️ 👤 **ninjaTT** 3 years, 2 months ago

you can use Smart Lock with Azure AD for no extra cost

upvoted 4 times

🗨️ 👤 **SanjSL** 3 years, 5 months ago

Smart lockout is always on, for all Azure AD customers, with these default settings that offer the right mix of security and usability. Customization of the smart lockout settings, with values specific to your organization, requires Azure AD Premium P1 or higher licenses for your users.

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout#how-smart-lockout-works>

Microsoft is making security defaults available to everyone.

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults#availability>

## Smart lockout and Security Defaults

upvoted 18 times

  **kktamang** 3 years, 3 months ago

No. Read question carefully. It says infra runs with Azure free license. Smart lock and conditional access need AAD premium P1 license.

upvoted 2 times

  **JayBee65** 3 years ago

Please review this link <https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout> which clearly states that statement to be wrong. "Smart lockout is always on, for \*\*\*ALL\*\*\* Azure AD customers,". P1 is required to customise the settings, again as stated on the link.

upvoted 2 times

  **dkltruong88**  3 years, 9 months ago

Was in exam today 1-10-2021. I passed with score 896. I chose smart lockout for 1 and Enable Security Defaults for 2

upvoted 36 times

  **Cg007**  1 year, 2 months ago

1. To protect against brute force attacks:



Smart lockout should be recommended. Azure AD has a smart lockout feature that can recognize sign-ins coming from valid users and treat them differently than ones that are likely from attackers. Smart lockout can lock out attackers while letting valid users continue to access their accounts.

2. To block legacy authentication attempts:

Enable Security defaults should be recommended. Security defaults in Azure AD make it easier to help protect your organization with preconfigured security settings for common attacks. This includes blocking legacy authentication protocols that can be used with guessing simple passwords or are not capable of doing multi-factor authentication.

Both options are available in the free edition of Azure AD and do not incur additional costs, which satisfies the requirement to minimise costs.

upvoted 1 times

  **Cg007** 1 year, 2 months ago

For the Free edition of Azure AD, full Conditional Access policy functionality is not available. Conditional Access requires Azure AD Premium P1 or P2, which are paid versions.



upvoted 1 times

  **rana9371** 2 years, 7 months ago

Smart Lockout is always enable for all versions of Azure AD. In this question Azure AD free version is used so smart lockout is enabled by default but can't make any changes to setting of smart lockout. So, if there is a need to make changes in the setting of Smart Lockout then it requires AAD P1 or higher license.

So, Smart Lockout is correct answer.

upvoted 1 times

  **kmeena** 2 years, 12 months ago

Smart lockout

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout#how-smart-lockout-works>

Enable security defaults

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

upvoted 1 times

  **g6singh** 3 years, 1 month ago

1. Smart Lockout

Smart lockout is always on, for all Azure AD customers, with these default settings that offer the right mix of security and usability. Customization of the smart lockout settings, with values specific to your organization, requires Azure AD Premium P1 or higher licenses for your users.

2. Security Default

Security defaults:

Available versions of Azure AD Multi-Factor Authentication

Azure AD Multi-Factor Authentication can be used, and licensed, in a few different ways depending on your organization's needs. All tenants are entitled to basic multifactor authentication features via Security Defaults.

upvoted 1 times

🗨️ 👤 **cloudera** 3 years, 3 months ago

With an AAD Free license, I would say:

1. SMART LOCKOUT with default setting (Customization require AAD Premium P1 as explained here: <https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout#:~:text=Customization%20of%20the%20smart%20lockout,user%20is%20never%20locked%20out>).

Azure AD > Security > Authentication Methods

2. DEFAULT SECURITY SETTING (also available to AAD free version)

Azure AD > Properties > Manage Security Defaults > Toggle to YES > Save

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>  
upvoted 3 times

🗨️ 👤 **kktamang** 3 years, 3 months ago

Question is very confusing. Smart Lock protects from Brute Force attack but requires AAD P1 or higher license but Question says company has free AAD license.

upvoted 1 times

🗨️ 👤 **JayBee65** 3 years ago

No, you are wrong, read the information above and stop saying everyone is wrong when you are wrong :)

upvoted 1 times

🗨️ 👤 **exnaniantwort** 3 years, 3 months ago

Conditional access and Security defaults both can do  
see

Conditional access

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication>

Security defaults:

Available versions of Azure AD Multi-Factor Authentication

Azure AD Multi-Factor Authentication can be used, and licensed, in a few different ways depending on your organization's needs. All tenants are entitled to basic multifactor authentication features via Security Defaults.

But conditional access is rejected because the question states it's free subscription.

Security default is available for free version (stated above)

upvoted 1 times

🗨️ 👤 **AdamHarrison** 3 years, 3 months ago

Can confirm Smart Lockout and Security Defaults based on the course I just finished, which had this question in the practice tests.

upvoted 1 times

🗨️ 👤 **plmmsg** 3 years, 3 months ago

1. Smart Lockout
  2. Security Default
- upvoted 1 times

🗨️ 👤 **ixl2pass** 3 years, 5 months ago

Smart Lock and Security defaults

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>  
upvoted 2 times

🗨️ 👤 **qerem** 3 years, 5 months ago

Smart Lockout & Security Defaults :

Smart lockout helps lock out bad actors that try to guess your users' passwords or use brute-force methods to get in. Smart lockout can recognize sign-ins that come from valid users and treat them differently than ones of attackers and other unknown sources. Attackers get locked out, while your users continue to access their accounts and be productive.

upvoted 2 times

🗨️ 👤 **student22** 3 years, 8 months ago



1. Smart lockout
  2. Security defaults
- upvoted 11 times

🗒️ 👤 **syu31svc** 3 years, 8 months ago

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout>

Smart lockout helps lock out bad actors that try to guess your users' passwords or use brute-force methods to get in

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults#blocking-legacy-authentication>

Protect brute force using smart lockout and block legacy using security defaults

upvoted 1 times

🗒️ 👤 **nkx** 3 years, 9 months ago

came in exam on 20-sep-21, I passed, i choose pass through and enable default

upvoted 2 times

🗒️ 👤 **souvik123** 3 years, 9 months ago

1. Smart Lockout
2. Security Default

upvoted 4 times

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains several administrative user accounts. You need to recommend a solution to identify which administrative user accounts have NOT signed in during the previous 30 days. Which service should you include in the recommendation?

- A. Azure AD Privileged Identity Management (PIM)
- B. Azure AD Identity Protection
- C. Azure Advisor
- D. Azure Activity Log

**Suggested Answer: A**

Community vote distribution

A (100%)

AlanJP **Highly Voted** 3 years, 12 months ago

Correct - PIM access review  
upvoted 32 times

YWDB 3 years, 8 months ago

Tested correct.  
upvoted 2 times

GetulioJr **Highly Voted** 3 years, 11 months ago

That is not a hard question, the answer is D, Azure Activity Log. You just create a query. That's it.  
upvoted 12 times

sapien45 3 years ago

There is only one thing never hard in you  
upvoted 3 times

Farid77 3 years, 11 months ago

the question is about accounts that have NOT signed in so there will be no records in the log file. The provided answer PIM is then correct.  
upvoted 5 times

tita\_tovenaar 3 years, 11 months ago

Incorrect, @Getulio is right. The answer is a PowerShell script that runs on activity logs. PIM will tell you role creation dates etc. but it doesn't tell you who hasn't logged on for the last 30 days.  
upvoted 2 times

cfsxtuv33 3 years, 11 months ago

Correct, or use a free-ware called CJWDEV and run it against AD and find out last log on or if the user has EVER logged on.  
upvoted 1 times

Ario 3 years, 9 months ago

Your answer isn't correct :

The Activity log is a platform log in Azure while Privileged Identity Management (PIM) is a service - question clearly ask about what service you recommend here ! so PIM is correct answer for this specific question.  
upvoted 4 times

Richard\_M 3 years, 3 months ago

Incorrect.. You're suggesting to run a query to find what? And then, with no results, match to what? The request is for a Service that allows you to find accounts that haven't logged in in 30 days. Access Review in PIM allows for that, without having to go through extra steps to match against yet another list you need to query.  
upvoted 1 times

One111 2 years, 10 months ago

Access Review is part of PAM, not PIM.  
upvoted 1 times

🗨️ **hertino** Most Recent 3 years, 2 months ago

In AZ-305 exam, 9 april 22

upvoted 4 times

🗨️ **kanweng** 3 years, 3 months ago

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-perform-azure-ad-roles-and-resource-roles-review>

after step 5 see the picture (Last sign in is more than 30 days ago).

upvoted 4 times

🗨️ **bacug** 3 years, 5 months ago

Selected Answer: A

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-use-audit-log?tabs=new>

upvoted 2 times

🗨️ **Carroyo826** 3 years, 6 months ago

PIM --> Privileged Identity Management

upvoted 1 times

🗨️ **examineezer** 3 years, 6 months ago

Its PIM, but not access review. Its audit history.

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/azure-pim-resource-rbac>

upvoted 1 times

🗨️ **examineezer** 3 years, 6 months ago

Sorry I've changed my mind (again). I can't see last sign-in in audit history either.

upvoted 1 times

🗨️ **examineezer** 3 years, 6 months ago

Ok final answer - PIM access reviews.

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-create-azure-ad-roles-and-resource-roles-review>

"The need for access to privileged Azure resource and Azure AD roles by employees changes over time. To reduce the risk associated with stale role assignments, you should regularly review access. You can use Azure Active Directory (Azure AD) Privileged Identity Management (PIM) to create access reviews for privileged access to Azure resource and Azure AD roles."

<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review>

"In the Enable review decision helpers section, choose whether you want your reviewer to receive recommendations during the review process. When enabled, users who have signed in during the previous 30-day period are recommended for approval. Users who haven't signed in during the past 30 days are recommended for denial."

upvoted 5 times

🗨️ **Dpejic** 3 years, 6 months ago

In exam today 22-dec-2021

upvoted 3 times

🗨️ **Dpejic** 3 years, 6 months ago

In exam today 22-dec-2021

upvoted 2 times

🗨️ **ivanmung** 3 years, 6 months ago

To identify the admin user is not sign-in past 30 days:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-perform-azure-ad-roles-and-resource-roles-review>

upvoted 3 times

🗨️ **leo\_az300** 3 years, 8 months ago

I would vote for D. As question specified this is for administrative account, and PIM doesn't manage some classic administrator roles as below,

You cannot manage the following classic subscription administrator roles in Privileged Identity Management:

Account Administrator

Service Administrator

Co-Administrator

upvoted 1 times

  **itenginerd** 3 years, 3 months ago

Those are roles associated with Azure Classic infrastructure. If you're still having to manage those, you have more problems than which admins haven't signed on in the last 90 days...

upvoted 1 times

  **syu31svc** 3 years, 8 months ago

Answer is A

PIM for access review

upvoted 1 times

  **poplovic** 3 years, 9 months ago

again, this is a question regarding "you need to recommend", not "meet the goal"

For the recommendation question, it is asking for the best practice. There might be multiple possible approaches. We need to choose the best one.

PIM access review is designed for this purpose. it is better than writing some code by querying the activity log. That is why it requires P2 license.


<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-create-azure-ad-roles-and-resource-roles-review>

upvoted 4 times

  **Gautam1985** 3 years, 10 months ago

correct



upvoted 1 times

  **Tripp\_F** 3 years, 11 months ago

PIM is correct. From 301 discussion:



"You can use the Privileged Identity Management (PIM) audit history to see all role assignments and activations within the past 30 days for all privileged roles. If you want to see the full audit history of activity in your Azure Active Directory (Azure AD) organization, including administrator, end user, and synchronization activity, you can use the Azure Active Directory security and activity reports."

upvoted 6 times

  **BrettusMaximus** 3 years, 11 months ago

Yes- but it wont give you a list of users who have not signed in.

upvoted 3 times

  **dennnnnnnnnn** 3 years, 11 months ago

You are right, it won't generate a list of "not signed in for past 30days"

However ,the question is "recommend a solution to identify"

So, you can use PIM can identify the admin XXX is not on the list of past 30 days sign-in history.

All in all, the question did highlight 30days, which matched with the PIM audit history duration.

upvoted 2 times

  **examineezer** 3 years, 6 months ago

"to see all role assignments and activations".... this is NOT sign-ins!

upvoted 1 times

  **vitol** 3 years, 11 months ago

Access Review provides only details about those accounts have access to a specific role with some sort of criteria the correct answer to me is "Activity logs" even though the best answer could be "sign-in logs"

upvoted 5 times

A company deploys Azure Active Directory (Azure AD) Connect to synchronize identity information from their on-premises Active Directory Domain Services (AD DS) directory to their Azure AD tenant. The identity information that is synchronized includes user accounts, credential hashes for authentication (password sync), and group memberships. The company plans to deploy several Windows and Linux virtual machines (VMs) to support their applications.

The VMs have the following requirements:

- ⇒ Support domain join, LDAP read, LDAP bind, NTLM and Kerberos authentication, and Group Policy.
- ⇒ Allow users to sign in to the domain using their corporate credentials and connect remotely to the VM by using Remote Desktop.

You need to support the VM deployment.

Which service should you use?

- A. Active Directory Federation Services (AD FS)
- B. Azure AD Privileged Identity Management
- C. Azure Managed Identity
- D. Azure AD Domain Services

**Suggested Answer: D**

Azure AD Domain Services provides managed domain services such as domain join, group policy, LDAP, Kerberos/NTLM authentication that are fully compatible with Windows Server Active Directory.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-overview>

Community vote distribution

D (100%)

AlanJP **Highly Voted** 3 years, 12 months ago

Answer seems correct

upvoted 16 times

d0bermannn 3 years, 11 months ago

and trivial:)

upvoted 2 times

vhmarsh16 **Highly Voted** 3 years, 11 months ago

correct.

Azure Active Directory Domain Services (AD DS) provides managed domain services such as domain join, group policy, lightweight directory access protocol (LDAP), and Kerberos/NTLM authentication. You use these domain services without the need to deploy, manage, and patch domain controllers (DCs) in the cloud.

upvoted 8 times

itenginerd **Most Recent** 3 years, 3 months ago

On my exam today.

upvoted 1 times

itenginerd 3 years, 3 months ago

**Selected Answer: D**

On the exam today.

upvoted 2 times

jr\_luciano 3 years, 4 months ago

**Selected Answer: D**

Answer is correct

upvoted 1 times

Carroyo826 3 years, 6 months ago

Letter D : Azure AD Domain Services

Thanks you !!

upvoted 1 times

🗨️ 👤 **rhinyx** 3 years, 7 months ago

**Selected Answer: D**

correct

upvoted 4 times

🗨️ 👤 **sharepoint\_Azure\_pp** 3 years, 8 months ago

Azure AD Domain Services is correct choose the same  
cleared with 900 on 17th October 2021

upvoted 7 times

🗨️ 👤 **syu31svc** 3 years, 8 months ago

<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/overview>

Answer is correct

upvoted 2 times

🗨️ 👤 **teehex** 3 years, 10 months ago

D is correct answer and it is the only feasible option among all  
upvoted 3 times

🗨️ 👤 **akaz** 3 years, 10 months ago

ADFS does not allow other authentication protocols, such as LDAP.  
upvoted 2 times

🗨️ 👤 **tvS2021** 3 years, 11 months ago

on exam (7-19-2021). passed 304  
upvoted 3 times

## HOTSPOT -

You are designing a software as a service (SaaS) application that will enable Azure Active Directory (Azure AD) users to create and publish online surveys. The

SaaS application will have a front-end web app and a back-end web API. The web app will rely on the web API to handle updates to customer surveys.

You need to design an authorization flow for the SaaS application. The solution must meet the following requirements:

- ⇒ To access the back-end web API, the web app must authenticate by using OAuth 2 bearer tokens.
- ⇒ The web app must authenticate by using the identities of individual users.

What should you include in the solution? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

The access tokens will be generated by:

	▼
Azure AD	
A web app	
A web API	

Authorization decisions will be performed by:

	▼
Azure AD	
A web app	
A web API	

**Answer Area**

The access tokens will be generated by:

	▼
Azure AD	
A web app	
A web API	


Suggested Answer:

Authorization decisions will be performed by:

	▼
Azure AD	
A web app	
A web API	

Reference:

<https://docs.microsoft.com/lb-lu/azure/architecture/multitenant-identity/web-api> <https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-v1-dotnet-webapi>

 **crazyaboutazure** Highly Voted 3 years, 11 months ago

answer is correct, web app does the authentication based on token and web API makes authorization decisions based on the user identity.

<https://docs.microsoft.com/en-us/azure/architecture/multitenant-identity/web-api>

upvoted 29 times

 **JayBee65** 3 years ago

The URL suggests

There are two main approaches you can take:



Delegated user identity. The web application authenticates with the user's identity.

Application identity. The web application authenticates with its client ID, using OAuth 2 client credential flow.

Since the question mentions OAuth 2 bearer tokens, this suggests Application not Delegated user identity, in which case "The web API cannot

perform any authorization based on the user identity. All authorization decisions are made by the web application." so the second answer is the Web App

upvoted 2 times

  **AberdeenAngus** 2 years, 11 months ago

Got to be Delegated, because Application breaks the requirement "The web app must authenticate by using the identities of individual users" so Web API is correct

upvoted 3 times

  **kooll**  3 years, 11 months ago

Seems to be:



1 Azure AD

2 Web app

Based of link below if I'm understanding it correctly.

<https://docs.microsoft.com/en-us/azure/architecture/multitenant-identity/web-api#:~:text=All%20authorization%20decisions%20are%20made,logic%20in%20the%20Web%20API.>

upvoted 13 times

  **binq** 3 years, 2 months ago

No. Given answer is correct. You gave good link, but wrong section. It's not application identity. You use delegated identity of users, so read one section above. It clearly states to use WEB API then.

upvoted 1 times

  **tita\_tovenaar** 3 years, 11 months ago

thanks, the link actually covers this particular use case. Azure AD and web app.

upvoted 3 times

  **BoxGhost** 3 years, 10 months ago

Surely that article confirms API is actually the correct one?

<https://docs.microsoft.com/en-us/azure/architecture/multitenant-identity/web-api#authenticating-in-the-web-api>

Authenticating in the web API



The web API has to authenticate the bearer token.

upvoted 3 times

  **J4U** 3 years, 9 months ago

No. The web API makes authorization decisions based on the user identity. Only in case of application identity, web app does the authorization.

upvoted 7 times

  **davidfernandezperrino**  3 years, 5 months ago

It's

1 Azure AD

2 Web API

"a front-end web app and a back-end web API". Frontend web app will make petitions via bearer token, and it should be the back-end web api who should give or not answer based on roles. The API should never trust frontend requests, cause they are easily hackable :)

upvoted 5 times

  **Xia\_Li** 3 years, 5 months ago

The answer is correct.

There are two main approaches you can take:

Delegated user identity: The web application authenticates with the user's identity.

Application identity: The web application authenticates with its client ID, using OAuth 2 client credential flow.



With user's identity, we need to take Delegated user identity:

->The bearer token sent to the web API contains the user identity.

->The web API makes authorization decisions based on the user identity.

<https://docs.microsoft.com/ib-lu/azure/architecture/multitenant-identity/web-api>

upvoted 3 times

  **Dpejic** 3 years, 6 months ago

Appere on exam 23-dec-2021

upvoted 4 times



🗨️ 👤 **syu31svc** 3 years, 8 months ago

<https://docs.microsoft.com/en-us/azure/architecture/multitenant-identity/images/access-token.png>

Answer is correct

upvoted 2 times

🗨️ 👤 **jppdks** 3 years, 9 months ago

Answer is correct <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/auth-oauth2>

upvoted 2 times

🗨️ 👤 **Spooky7** 3 years, 9 months ago

It is like the most common scenario in web application design. Azure AD provides token, web apps includes token in each request to web api, web api authorize requests based on claims in the token. So answer is correct.

upvoted 7 times

🗨️ 👤 **leo\_az300** 3 years, 9 months ago

why it's web app not web API??? it's 2021, how can people still mix up [authorization] and [authentication]?

You need to enable user [authorization] in web app which is choose who can request

Web API will [authenticate] the token which allow request.

upvoted 2 times

🗨️ 👤 **Gautam1985** 3 years, 10 months ago

correct answer

upvoted 1 times

🗨️ 👤 **JimGrayham** 3 years, 10 months ago

Answer is correct.

"If you authenticate with Azure AD, it's strongly recommended to get the access token from Azure AD, even with client credential flow."

"The web API makes authorization decisions based on the user identity."

<https://docs.microsoft.com/lb-lu/azure/architecture/multitenant-identity/web-api>

upvoted 3 times

🗨️ 👤 **murongqing** 3 years, 10 months ago

Azure AD

Web App

<https://docs.microsoft.com/en-us/azure/architecture/multitenant-identity/web-api>

upvoted 2 times

🗨️ 👤 **Pinto** 3 years, 10 months ago

is this similar to <https://www.examtopycs.com/discussions/microsoft/view/46673-exam-az-304-topic-2-question-44-discussion/> ?

upvoted 1 times

🗨️ 👤 **ulcers** 3 years, 10 months ago

Check the link, the question states it must use the signed in user to auth, so we are using delegated perms, so it's azure ad and web api

upvoted 1 times

🗨️ 👤 **tankard777** 3 years, 11 months ago

1 azure ad

2 web app

upvoted 3 times

🗨️ 👤 **gssd4scoder** 3 years, 11 months ago

why web api and not web app?

upvoted 1 times

🗨️ 👤 **dennnnnnnnnn** 3 years, 11 months ago

web app is front end client, the world never use front end app to perform authorization decisions. So, it must be backend web api

upvoted 2 times

🗨️ 👤 **jmay** 3 years, 5 months ago

front-end does not mean client-side. It does not say the front-end is an SPA.

The web app needs to determine what the authenticated user can see / access and present the frontend accordingly. As a result, the authorisation level must be evaluated by the web app.

upvoted 1 times

  **alryazvrn** 3 years, 12 months ago

I guess the second answer should be - web app, but I am not sure. As authentication between web app and api is done via bearer token

upvoted 2 times

You have a hybrid deployment of Azure Active Directory (Azure AD).

You need to recommend a solution to ensure that the Azure AD tenant can be managed only from the computers on your on-premises network. What should you include in the recommendation?

- A. a conditional access policy
- B. Azure AD roles and administrators
- C. Azure AD Application Proxy
- D. Azure AD Privileged Identity Management

**Suggested Answer: A**

*Community vote distribution*

A (100%)

  **HDZ78**  3 years, 12 months ago

Appears to be correct.  
upvoted 21 times

  **syu31svc**  3 years, 8 months ago

Incorrect Answers:

B. Azure AD roles and administrators

This used to configure various roles for users. Configuring the Azure AD roles does not limit the access for an application from specific Device / IP location.

C. Azure AD Application Proxy

Azure Active Directory's Application Proxy provides secure remote access to on-premises web applications.

D. Azure AD Privileged Identity Management

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.

Answer is A

upvoted 20 times

  **sapien45** 3 years ago



Most useful answer  
upvoted 1 times

  **jr\_luciano**  3 years, 4 months ago

**Selected Answer: A**

Answer is A

upvoted 1 times

  **sakshi250291** 3 years, 6 months ago

**Selected Answer: A**

Correct

upvoted 1 times

  **Eitant** 3 years, 6 months ago

**Selected Answer: A**



Correct answer

upvoted 1 times

  **Azurefox79** 3 years, 6 months ago


you can use CA to restrict certain actions, such as admin actions. You can require X,Y,Z controls for admin actions such as IP address range of corporate network, device state for hybrid joined devices and MFA among others

upvoted 3 times

  **jppdks** 3 years, 9 months ago



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

upvoted 3 times

  **aleksey\_o** 3 years, 10 months ago

Sure answer a conditional access policy

upvoted 2 times

  **Ykh** 3 years, 10 months ago

Yes, seems correct as this is the only option which seems relevant.

upvoted 1 times

You plan to automate the deployment of resources to Azure subscriptions.

What is a difference between using Azure Blueprints and Azure Resource Manager templates?

- A. Azure Resource Manager templates remain connected to the deployed resources.
- B. Only Azure Resource Manager templates can contain policy definitions.
- C. Azure Blueprints remain connected to the deployed resources.
- D. Only Azure Blueprints can contain policy definitions.

**Suggested Answer: C**

With Azure Blueprints, the relationship between the blueprint definition (what should be deployed) and the blueprint assignment (what was deployed) is preserved.

This connection supports improved tracking and auditing of deployments. Azure Blueprints can also upgrade several subscriptions at once that are governed by the same blueprint.

Incorrect:

Not A: Nearly everything that you want to include for deployment in Azure Blueprints can be accomplished with a Resource Manager template. However, a

Resource Manager template is a document that doesn't exist natively in Azure - each is stored either locally or in source control. The template gets used for deployments of one or more Azure resources, but once those resources deploy there's no active connection or relationship to the template.

Reference:

<https://docs.microsoft.com/en-us/answers/questions/26851/how-is-azure-blue-prints-different-from-resource-m.html>

Community vote distribution

C (100%)

 **jppdks** Highly Voted 3 years, 9 months ago

C is correct

Nearly everything that you want to include for deployment in Azure Blueprints can be accomplished with an ARM template. However, an ARM template is a document that doesn't exist natively in Azure - each is stored either locally or in source control. The template gets used for deployments of one or more Azure resources, but once those resources deploy there's no active connection or relationship to the template.

With Azure Blueprints, the relationship between the blueprint definition (what should be deployed) and the blueprint assignment (what was deployed) is preserved. This connection supports improved tracking and auditing of deployments. Azure Blueprints can also upgrade several subscriptions at once that are governed by the same blueprint.

<https://docs.microsoft.com/en-us/azure/governance/blueprints/overview>

upvoted 16 times

 **SpamLover** Highly Voted 3 years, 10 months ago

It seems correct

upvoted 15 times

 **OCHT** Most Recent 3 years, 1 month ago

**Selected Answer: C**

I selected D during the exam. After verification, should be C.

It preserves both definition and assignment.

upvoted 1 times

 **hertino** 3 years, 2 months ago

In AZ-305 exam, 9 april 22

upvoted 3 times

 **favela** 3 years, 3 months ago



what about D ?

upvoted 2 times

 **AberdeenAngus** 3 years, 1 month ago

A template can contain and deploy a policy definition, example link <https://docs.microsoft.com/en-us/azure/governance/policy/assign-policy-template>

upvoted 1 times

  **favela** 3 years, 3 months ago

due to blueprint is about template from your environment with the policies include ARM they don't bring you policies

upvoted 1 times

  **exnaniantwort** 3 years, 3 months ago

why D is wrong?

upvoted 2 times

  **jr\_luciano** 3 years, 4 months ago

**Selected Answer: C**

C is the answer

upvoted 1 times

  **syu31svc** 3 years, 8 months ago

<https://docs.microsoft.com/en-us/answers/questions/26851/how-is-azure-blue-prints-different-from-resource-m.html>

With Azure Blueprints, the relationship between the blueprint definition (what should be deployed) and the blueprint assignment (what was deployed) is preserved

C is the answer

upvoted 6 times

  **maymaythar** 3 years, 10 months ago

Given answer is right?

upvoted 2 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains a group named Group1. Group1 contains all the administrative user accounts.

You discover several login attempts to the Azure portal from countries where administrative users do NOT work.

You need to ensure that all login attempts to the Azure portal from those countries require Azure Multi-Factor Authentication (MFA).

Solution: Implement Azure AD Privileged Identity Management.

Does this solution meet the goal?

A. Yes

B. No

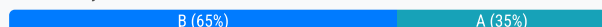
**Suggested Answer: A**

Azure Active Directory (Azure AD) Privileged Identity Management (PIM) is a service that enables you to manage, control, and monitor access to important resources in your organization.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

*Community vote distribution*



**VincentZhang** 3 years, 9 months ago

answer is wrong. The right answer is Conditional Access  
upvoted 28 times

**zeek** 3 years, 3 months ago

there is no conditional access option for this question, so i think all of them is no, there is no correct answer  
upvoted 1 times

**rdemontis** 3 years, 7 months ago

exactly. MFA authentication for PIM is used when the user (already authenticated to the azure portal) wants to activate a new elevated role. But this is not the case:

"You can require that users complete a multifactor authentication challenge when they sign in. You can also require that users complete a multifactor authentication challenge when they activate a role in Azure Active Directory (Azure AD) Privileged Identity Management (PIM). This way, even if the user didn't complete multifactor authentication when they signed in, they'll be asked to do it by Privileged Identity Management"

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

upvoted 6 times

**17Master** 3 years, 4 months ago

there are three of the same questions here, none of the three have the Conditional Access option. so what is the answer?  
for me it must be PIM because it fits more.  
upvoted 1 times

**kilowd** 3 years ago

Azure MFA can be leveraged as an additional verification mechanism through:

Conditional Access policies

Azure AD Identity Protection to mitigate risky sign-ins

Step-up authentication mechanisms, like the OneDrive Personal Vault feature

The Azure MFA NPS Extension

Azure MFA registration can be combined with the registration for Azure AD Self-service Password Reset, to make the registration for the one complete the registration for the other.

upvoted 1 times

  **AubinBakana** 2 years, 10 months ago

There does not have to be a right answer. Read the description above.  
upvoted 2 times

  **AubinBakana** 2 years, 10 months ago

There does not have to be a right answer. Read the description above.  
upvoted 1 times

  **17Master** 3 years, 3 months ago



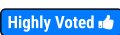
yes is correct. check this link:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-require-mfa>

We recommend that you require multifactor authentication (MFA or 2FA) for all your administrators. Multifactor authentication reduces the risk of an attack using a compromised password.

You can require that users complete a multifactor authentication challenge when they sign in. You can also require that users complete a multifactor authentication challenge when they activate a role in Azure Active Directory (Azure AD) Privileged Identity Management (PIM). This way, even if the user didn't complete multifactor authentication when they signed in, they'll be asked to do it by Privileged Identity Management.

upvoted 3 times

  **syu31svc**  3 years, 9 months ago

Answer is No

Conditional access is the solution

upvoted 7 times

  **gssd4scoder** 3 years, 8 months ago


Few doubts you're right man

upvoted 1 times

  **rxlicon**  1 year, 10 months ago



The correct answer is Identity Protection as a Signal source for Conditinal Access"

upvoted 1 times

  **PPP164** 2 years, 8 months ago

Correct answer is ADPIM, Yes

upvoted 1 times

  **Snownoodles** 2 years, 8 months ago



Conditional Access

upvoted 1 times



  **jellybiscuit** 2 years, 9 months ago



No. -- the answer is a conditional access policy

PIM can require MFA, but only for elevated (administrative) roles -- meaning it can't apply to all users. It also cannot consider location.

upvoted 2 times

  **One111** 2 years, 10 months ago



Conditional Access policy with country based on IP addresses is needed. If admins have Authenticator on mobiles with GPS, this could be hardened by using GPS coordinates from their devices.

upvoted 1 times

  **AubinBakana** 2 years, 10 months ago



I am adamant this is false. Conditional Access.

upvoted 1 times

  **kilowd** 3 years ago

Azure MFA can be leveraged as an additional verification mechanism through:

Conditional Access policies

Azure AD Identity Protection to mitigate risky sign-ins



Step-up authentication mechanisms, like the OneDrive Personal Vault feature

The Azure MFA NPS Extension

Azure MFA registration can be combined with the registration for Azure AD Self-service Password Reset, to make the registration for the one complete the registration for the other.

upvoted 1 times

🗳️ 👤 **bhuren** 3 years, 2 months ago

Right Solution would be AZ Identity Protection - Sign-in Risk Policy

upvoted 1 times

🗳️ 👤 **Zsolt72** 3 years, 2 months ago

**Selected Answer: A**

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure#what-does-it-do>

What does it do?

- Enforce multi-factor authentication to activate any role

upvoted 2 times

🗳️ 👤 **azlan69** 3 years, 3 months ago

it's a Yes answer :

Unlike Conditional Access, Azure PIM only applies to administrative roles within Azure and Azure AD. This is an important consideration, both as it relates to 'administrative' functions as well as, more importantly, the idea of Azure and Azure AD 'roles'. Also, unlike Conditional Access, Azure PIM requires Microsoft's highest license tiers (E5 or Premium 2) for any users that are subject to the tool.

upvoted 2 times

🗳️ 👤 **itenginerd** 3 years, 3 months ago

On my exam today was another question with the correct answer "Use Privileged Identity Manager to enable MFA", so I'd think Microsoft would say this is a functional answer. Yes, I'd do it with Conditional Access in production, but this answer plays if you have AD Premium P2 in place.

upvoted 1 times

🗳️ 👤 **kanweng** 3 years, 3 months ago

**Selected Answer: B**

No,

the correct answer should be Azure AD Identity Protection

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks>

upvoted 1 times

🗳️ 👤 **Plesking** 3 years, 3 months ago

I encountered a similar situation at work and Azure AD identity protection is the answer here.

upvoted 1 times

🗳️ 👤 **hobozero** 3 years, 3 months ago

As many others have point out, Conditional Access is the correct answer, but PIM is only relevant during role activation. The correct answer is Identity Protection as a Signal source for Conditional Access"

"Administrators can specify entire countries/regions IP ranges to block or allow traffic from."

"Signals integration with Azure AD Identity Protection allows Conditional Access policies to identify risky sign-in behavior. Policies can then force users to change their password, do multi-factor authentication to reduce their risk level, or block access until an administrator takes manual action."

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

upvoted 1 times

🗳️ 👤 **petey212** 3 years, 3 months ago

**Selected Answer: A**

a - this is technically correct because you can enable mfa through PIM. conditional access is more appropriate (because you can specify the regions it is enabled) but pim is still an acceptable answer as you can enforce mfa.

upvoted 3 times

🗳️ 👤 **azlan69** 3 years, 3 months ago

correct : Unlike Conditional Access, Azure PIM only applies to administrative roles within Azure and Azure AD. This is an important consideration, both as it relates to 'administrative' functions as well as, more importantly, the idea of Azure and Azure AD 'roles'. The question mentioned on the administrator role

upvoted 1 times

You manage an Azure environment for a company. The environment has over 25,000 licensed users and 100 mission-critical applications. You need to recommend a solution that provides advanced user threat detection and remediation strategies. What should you recommend?

- A. Azure Active Directory (Azure AD) authentication
- B. Microsoft Identity Manager
- C. Azure Active Directory (Azure AD) Identity Protection
- D. Azure Active Directory Federation Services (AD FS)
- E. Azure Active Directory (Azure AD) Connect

**Suggested Answer:** C

Reference:

<https://docs.microsoft.com/en-us/azure/security/fundamentals/threat-detection>

Community vote distribution

C (100%)

 **syu31svc**  3 years, 9 months ago

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection>


Identity Protection uses the learnings Microsoft has acquired from their position in organizations with Azure AD, the consumer space with Microsoft Accounts, and in gaming with Xbox to protect your users. Microsoft analyses 6.5 trillion signals per day to identify and protect customers from threats.

This is C for sure  
upvoted 19 times

 **Testing6132**  2 years, 12 months ago

**Selected Answer: C**

Obvious answer  
upvoted 1 times

 **Eitant** 3 years, 6 months ago

**Selected Answer: C**


Correct Answer  
upvoted 3 times

 **cfsxtuv33** 3 years, 8 months ago

"C" is definitely the answer, no doubt about it.  
upvoted 4 times

 **gssd4scoder** 3 years, 8 months ago

Agree with the answer, it's C  
upvoted 3 times

 **waqas** 3 years, 8 months ago

C is the answer.  
upvoted 4 times

You store web access logs data in Azure Blob storage.

You plan to generate monthly reports from the access logs.

You need to recommend an automated process to upload the data to Azure SQL Database every month.

What should you include in the recommendation?

- A. Data Migration Assistant
- B. Microsoft SQL Server Migration Assistant (SSMA)
- C. Azure Data Factory
- D. AzCopy

**Suggested Answer: C**

Azure Data Factory is the platform that solves such data scenarios. It is the cloud-based ETL and data integration service that allows you to create data-driven workflows for orchestrating data movement and transforming data at scale. Using Azure Data Factory, you can create and schedule data-driven workflows (called pipelines) that can ingest data from disparate data stores. You can build complex ETL processes that transform data visually with data flows or by using compute services such as Azure HDInsight Hadoop, Azure Databricks, and Azure SQL Database.

Reference:

<https://docs.microsoft.com/en-gb/azure/data-factory/introduction>

Community vote distribution

C (100%)

  **syu31svc** Highly Voted 3 years, 9 months ago

"automated process"

Data Factory is the obvious choice here

upvoted 26 times

  **gssd4scoder** 3 years, 8 months ago

obvious and only, agree. azcopy can't directly access logs

upvoted 3 times

  **hertino** Highly Voted 3 years, 2 months ago

In AZ-305 exam, 9 april 22

upvoted 5 times

  **MSlave** Most Recent 3 years, 6 months ago

Selected Answer: C

correct

upvoted 1 times

  **InformationOverload** 3 years, 7 months ago

@syu31svc knows his stuff!

upvoted 2 times

## HOTSPOT -

You have a resource group named RG1 that contains the objects shown in the following table.

Name	Type	Location
ASP-RG1	App Service plan	East US
KV1	Azure Key Vault	East US
KV2	Azure Key Vault	West Europe
App1	Azure Logic Apps	West US

You need to configure permissions so that App1 can copy all the secrets from KV1 to KV2. App1 currently has the Get permission for the secrets in KV1.

Which additional permissions should you assign to App1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Permission to assign so that App1 can copy the secrets from KV1:

▼

Add  
Backup  
Create  
List  
Unwrap Key

Permission to assign so that App1 can copy the secrets to KV2:

▼

Create  
Import  
List  
Wrap Key

### Answer Area

Permission to assign so that App1 can copy the secrets from KV1:

▼

Add  
Backup  
Create  
List  
Unwrap Key

Suggested Answer:

Permission to assign so that App1 can copy the secrets to KV2:

▼

Create  
Import  
List  
Wrap Key

Box 1: List -

Get: Gets the specified Azure key vault.

List: The List operation gets information about the vaults associated with the subscription.

Box 2: Create -

Create Or Update: Create or update a key vault in the specified subscription.

Reference:

<https://docs.microsoft.com/en-us/rest/api/keyvault/>

🗳️ 👤 **Ario** Highly Voted 3 years, 9 months ago

Given answer is correct

upvoted 21 times

🗳️ 👤 **STH** 3 years, 5 months ago

Yes : as "App1 currently has the Get permission for the secrets in KV1", only List permission is needed to access all secrets and values in KV1

Then, having all informations, we only need Create permission to populate KV2

upvoted 3 times

🗳️ 👤 **dirgiklis** Highly Voted 3 years, 7 months ago

There is no "Create" or "Import" permission for Secrets, only "Set".

upvoted 12 times

🗳️ 👤 **telepeti** 3 years, 4 months ago

I had this question yesterday, still with the 4 wrong options for KV2 restore.

upvoted 1 times

🗳️ 👤 **MasterArmSwitch** 3 years, 7 months ago

You are right: <https://docs.microsoft.com/en-us/azure/key-vault/secrets/about-secrets#secret-access-control>

Then what is the answer ?

upvoted 1 times

🗳️ 👤 **walkwolf3** 3 years, 7 months ago

Azure key vault does have "Create" and "Import". Given answer is correct.

<https://docs.microsoft.com/en-us/azure/key-vault/general/security-features#privileged-access>

upvoted 2 times

🗳️ 👤 **AB20101** 3 years, 4 months ago

The questions is asking to copy secrets, not to create key vaults

upvoted 3 times

🗳️ 👤 **magichappens** 2 years, 10 months ago

I just checked it and indeed there is a "Create" and "Import" permission. However, "List" and "Create" is the right answer.

upvoted 1 times

🗳️ 👤 **plmmsg** Most Recent 3 years, 3 months ago

list

Import

upvoted 1 times

🗳️ 👤 **joehoesofat** 3 years, 4 months ago

I say backup and import are the only 2 ways- or... use a read only copy in the other region-

MS says you can't move a Secret to another region- or if you do- backup and import is it!

<https://docs.microsoft.com/en-us/azure/key-vault/general/move-region#prerequisites>

<https://docs.microsoft.com/en-us/answers/questions/199024/how-to-copy-azure-keyvault-secrets-to-other-subscr.html>

upvoted 1 times

🗳️ 👤 **joehoesofat** 3 years, 4 months ago

Ok i was wrong the restore wont work either- !!! dang- ok this is too devops for me- i am just going with the answer list and create

<https://docs.microsoft.com/en-us/azure/key-vault/general/move-region#prerequisites>

upvoted 1 times

🗳️ 👤 **joehoesofat** 3 years, 4 months ago

MS says you can't move a Secret to another region- or if you do- backup and import is it!

<https://docs.microsoft.com/en-us/azure/key-vault/general/move-region#prerequisites>

<https://docs.microsoft.com/en-us/answers/questions/199024/how-to-copy-azure-keyvault-secrets-to-other-subscr.html>

Below is all a rabbit hole for cross region- use read only copy instead for cross region!

This <https://docs.microsoft.com/en-us/azure/key-vault/general/assign-access-policy?tabs=azure-portal>

Leads to this-Authenticate to key vault in code-

<https://docs.microsoft.com/en-us/azure/key-vault/general/authentication>

Leads to this Azure Key Vault developer's guide | Microsoft Docs



upvoted 1 times

  **joeoesofat** 3 years, 4 months ago

Ok i was wrong the restore wont work either- !!! dang- ok this is too devops for me- i am just going with the answer list and create

<https://docs.microsoft.com/en-us/azure/key-vault/general/move-region#prerequisites>

upvoted 1 times

  **jmay** 3 years, 5 months ago

The question / answers are flawed. The question specifically asked "copy all the SECRETS" - not keys, not certificates. And for secrets, there is no "create" or "import" operations but only "set". Some may argue it is about the Key Vault it self, so "Create" is applicable. But KV2 has already been created.

The only argument to make "Import" applausible is the text label used in Azure Portal. However, the label reads "Generate/Import".

I guess I just need to roll the dice for this question.

upvoted 2 times

  **micofucho** 3 years, 5 months ago

I think it would be 'Import' for the second box:

Import Key: 'Imports an externally created key, stores it, and returns key parameters and attributes to the client.'

<https://docs.microsoft.com/en-us/rest/api/keyvault/import-key/import-key>

Create key: 'Creates a new key, stores it, then returns key parameters and attributes to the client.'

<https://docs.microsoft.com/en-us/rest/api/keyvault/create-key/create-key>

Technically, both solutions are valid, but may be Import is more appropriate, because the key already exists. The Import key help page says '..Imports an externally created key,...', so, in this case, the key has already been created, in the first vault.

upvoted 1 times

  **yyuryyuciryyforme** 3 years, 5 months ago

Create - a new secret will be generated by Azure

Import - the pre-existing secret will be imported

For example in Powershell the same cmdlet is used for both - Add-AzKeyVaultKey - and the difference between create and import is in the different switches - e.g. during create you may specify the key type (RSA or elliptic) and size, and during import you must specify the key file and password.

upvoted 1 times

  **examineezer** 3 years, 6 months ago

1. List all keys
2. For each key, "Get Key"
3. For each response, "Import"

Why is it Import and not Create?

"Get Key" response is of type "KeyBundle"

<https://docs.microsoft.com/en-us/rest/api/keyvault/get-key/get-key#keybundle>

KeyBundle includes key of type "JsonWebKey".

"Create Key" request body does not include JsonWebKey (it is not for pre-existing keys).

<https://docs.microsoft.com/en-us/rest/api/keyvault/create-key/create-key#request-body>

Import Key request body DOES include JsonWebKey.



<https://docs.microsoft.com/en-us/rest/api/keyvault/import-key/import-key#request-body>

upvoted 1 times

  **cfsxtuv33** 3 years, 8 months ago

Working in PowerShell you would need to "import" the secrets into KV2. The first box is correct but perhaps the second box should be "import." Any rebuttal is welcome.

upvoted 5 times

  **waqas** 3 years, 8 months ago

Given answers are correct.

upvoted 4 times

  **leo\_az300** 3 years, 8 months ago

I would go with List & Import

If you check API response body for Get Key and Import Key, they match each other. But Create Key API request body needs more fields.

upvoted 3 times

  **Ajdlfasudfo0** 3 years, 8 months ago

isn't import for restoring the backup? Which we cannot use because they are in different geo regions

upvoted 4 times

  **syu31svc** 3 years, 8 months ago

I would say

List to copy from KV1

Import to copy to KV2

upvoted 4 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. Your company has deployed several virtual machines (VMs) on-premises and to Azure. Azure ExpressRoute has been deployed and configured for on-premises to Azure connectivity.

Several VMs are exhibiting network connectivity issues.

You need to analyze the network traffic to determine whether packets are being allowed or denied to the VMs.

Solution: Install and configure the Microsoft Monitoring Agent and the Dependency Agent on all VMs. Use the Wire Data solution in Azure Monitor to analyze the network traffic.

Does the solution meet the goal?

A. Yes

B. No

#### Suggested Answer: B

Instead use Azure Network Watcher to run IP flow verify to analyze the network traffic.

Note: Wire Data looks at network data at the application level, not down at the TCP transport layer. The solution doesn't look at individual ACKs and SYN's.

Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview> <https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview>

Community vote distribution

B (100%)


 **syu31svc** Highly Voted 3 years, 9 months ago

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-packet-capture-overview>

Network Watcher variable packet capture allows you to create packet capture sessions to track traffic to and from a virtual machine. Packet capture helps to diagnose network anomalies both reactively and proactively. Other uses include gathering network statistics, gaining information on network intrusions, to debug client-server communications and much more.

Answer is No


upvoted 7 times

 **Snownoodles** Most Recent 2 years, 8 months ago

**Selected Answer: B**

IP flow verify

upvoted 1 times

 **OCHT** 3 years, 1 month ago

**Selected Answer: B**

Wire Data was EOL . Thence, we must opt out the answer not good.

upvoted 1 times

 **Kctaz** 3 years, 4 months ago

Given answer is correct.

upvoted 1 times

 **Ajdlfasudfo0** 3 years, 8 months ago

also, Wire Data solution has reached end of life

upvoted 2 times

 **gssd4scoder** 3 years, 8 months ago

Agree with answer and explanation, Network Watcher

upvoted 3 times



Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. Your company has deployed several virtual machines (VMs) on-premises and to Azure. Azure ExpressRoute has been deployed and configured for on-premises to Azure connectivity.

Several VMs are exhibiting network connectivity issues.

You need to analyze the network traffic to determine whether packets are being allowed or denied to the VMs.

Solution: Use the Azure Traffic Analytics solution in Azure Log Analytics to analyze the network traffic.

Does the solution meet the goal?

A. Yes

B. No

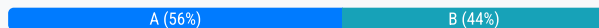
**Suggested Answer: B**

Instead use Azure Network Watcher to run IP flow verify to analyze the network traffic.

Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview> <https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview>

Community vote distribution



**scottishstvaeo** Highly Voted 3 years, 8 months ago

Hey Guys,

Let's discuss this one!

I think the answer should be yes.

Traffic Analytics is a cloud-based solution that provides visibility into user and application activity in cloud networks. Traffic analytics analyzes Network Watcher network security group (NSG) flow logs to provide insights into traffic flow in your Azure cloud. With traffic analytics, you can:

Visualize network activity across your Azure subscriptions and identify hot spots.

Identify security threats to, and secure your network, with information such as open-ports, applications attempting internet access, and virtual machines (VM) connecting to rogue networks.

Understand traffic flow patterns across Azure regions and the internet to optimize your network deployment for performance and capacity.

Pinpoint network misconfigurations leading to failed connections in your network.

<https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics>

upvoted 15 times

**rdemontis** 3 years, 7 months ago

Exactly. Traffic Analytics has a superset of services of which one is a network watcher. So the answer is yes, in fact you can use this solution as well. This solution can provide much more in terms of analysis of network traffic, but if you just want a simple solution to understand blocked traffic, you can use the IP flow verify tool

upvoted 4 times

**Gluckos** 3 years, 4 months ago

Azure traffic Analytics is only for cloud resources... It's possible to have others vm's on-premise.

upvoted 7 times

**catfood** 2 years, 10 months ago

typical microsoft question that has ambiguity - is it the on prem or the azure VMs that are having the problem. Does anyone actually sanity check these questions at MS ?

upvoted 1 times

**sharepoint\_Azure\_pp** Highly Voted 3 years, 8 months ago

It was a part of 2nd set of 3 Y/N question

Azure network watcher is correct

choose the same

cleared with 900 on 17th October 2021

upvoted 11 times

🗄️ 👤 **DevilsLife** Most Recent 2 years, 10 months ago

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview>

"IP flow verify checks if a packet is allowed or denied to or from a virtual machine."

upvoted 2 times

🗄️ 👤 **AubinBakana** 2 years, 10 months ago

Selected Answer: A

Traffic analytics do use NSG Flow Logs from Azure Traffic Manager. The answer should Yes.

Here's a direct quote from Msft:

"Traffic analytics is a cloud-based solution that provides visibility into user and application activity in your cloud networks. Specifically, traffic analytics analyzes Azure Network Watcher network security group (NSG) flow logs to provide insights into traffic flow in your Azure cloud."

<https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics>

upvoted 1 times

🗄️ 👤 **AubinBakana** 2 years, 10 months ago

Selected Answer: B

Analyse pack, sound like packet capture, doesn't it? you can't do packet capture with Traffic Analytics.

upvoted 2 times

🗄️ 👤 **AubinBakana** 2 years, 10 months ago

Please ignore this answer. Traffic Analytics should at least help answer some question, it dose analyse NSG Flow Logs from Network Watcher.

upvoted 2 times

🗄️ 👤 **Indigoprofrader** 3 years ago

FAQ for Traffic Analytics says it can check which ports are reachable between 2 IPs. So it can check if traffic gets through on the TCP layer 4 level. I would say it's "yes"

<https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics-faq#how-do-i-check-which-ports-are-reachable--or-blocked--between-ip-pairs-with-nsg-rules->

upvoted 1 times

🗄️ 👤 **OCHT** 3 years, 1 month ago

Selected Answer: A

Should be A. AZ Net Watcher undertakes the analysis of IP flow.

upvoted 1 times

🗄️ 👤 **mr\_sandy** 3 years, 3 months ago

Selected Answer: B

No.

Traffic Analytics now supports collecting NSG Flow Logs data at a higher frequency of 10 mins.

Traffic analytics uses point in time snapshots, it does not allow you to determine the success / failure of individual packets. For individual packet level analysis Network Watcher IP flow is required.

upvoted 2 times

🗄️ 👤 **jmay** 3 years, 5 months ago

Selected Answer: A

"With traffic analytics, you can:

...

- Understand traffic flow patterns across Azure regions and the internet to optimize your network deployment for performance and capacity.
- Pinpoint network misconfigurations leading to failed connections in your network.

"

<https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics>

upvoted 1 times

🗄️ 👤 **[Removed]** 3 years, 5 months ago

Selected Answer: A

Answer should be Yes.

Network Analytics can be useful here to inspect the data traffic

upvoted 2 times

🗨️ **tomatosis** 3 years, 6 months ago

For series of questions as such, my trainer told me that there is only 1 correct answer for it. Let's say we confirm network watcher is the correct one, the rest must be wrong. I know my explanation is not from technical point of view, but our goal is to pass the exam.

upvoted 7 times

🗨️ **sapien45** 3 years ago

Wrong. I have no interest in passing the exam. I am only interested in getting proficient on Azure Security

upvoted 1 times

🗨️ **AubinBakana** 2 years, 10 months ago

You trainer told you wrong. There may be no good answer or multiple good answers.

upvoted 2 times

🗨️ **examineezer** 3 years, 6 months ago

These questions are completely independent of other questions. Read it like this - can you use the Azure Traffic Analytics solution in Azure Log Analytics to analyze the network traffic, including the determination of whether packets are being allowed or denied to the VMs? I think the answer is Yes.

<https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics>

upvoted 3 times

🗨️ **examineezer** 3 years, 7 months ago

So many of these types have questions have people commenting "no its not this answer - because its XXXX".

Read carefully the question:

"Some question sets might have more than one correct solution, while others might not have a correct solution."

upvoted 7 times

🗨️ **student22** 3 years, 8 months ago

No

---

upvoted 1 times

🗨️ **tteesstt** 3 years, 8 months ago

Not 100% on this one but I'd go for a Yes.

upvoted 2 times

🗨️ **syu31svc** 3 years, 8 months ago

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview>

IP flow verify checks if a packet is allowed or denied to or from a virtual machine.

Answer is No

upvoted 2 times

🗨️ **scottishstvao** 3 years, 8 months ago

The question only mentions Traffic Analytics. Not the network watcher IP flow, so we should check what it can do.

This kind of question can have more than one answer.

upvoted 4 times

🗨️ **mike933** 3 years, 8 months ago

Phrasing is so specific that it rather refers to network watcher, even though Traffic Analytics would be also fine, for example to verify if access isn't blocked by rules set in network security groups.

upvoted 1 times

**HOTSPOT -**

You manage a database environment for a Microsoft Volume Licensing customer named Contoso, Ltd. Contoso uses License Mobility through Software Assurance.

You need to deploy 50 databases. The solution must meet the following requirements:

- ⇒ Support automatic scaling.
- ⇒ Minimize Microsoft SQL Server licensing costs.

What should you include in the solution? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Purchase model:

DTU
vCore
Azure reserved virtual machine instances

Deployment option:

An Azure SQL managed instance
An Azure SQL Database elastic pool
A SQL Server Always On availability group

**Answer Area**

Suggested Answer:

Purchase model:

DTU
vCore
Azure reserved virtual machine instances

Deployment option:

An Azure SQL managed instance
An Azure SQL Database elastic pool
A SQL Server Always On availability group

Box 1: vCore -

Virtual core (vCore)-based purchasing model (recommended). This purchasing model provides a choice between a provisioned compute tier and a serverless compute tier. With the provisioned compute tier, you choose the exact amount of compute resources that are always provisioned for your workload. With the serverless compute tier, you specify the autoscaling of the compute resources over a configurable compute range

Box 2: An Azure SQL Database Elastic pool

Azure SQL Database provides the following deployment options for a database:

- ⇒ Single database represents a fully managed, isolated database.
- ⇒ Elastic pool is a collection of single databases with a shared set of resources, such as CPU or memory. Single databases can be moved into and out of an elastic pool.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/purchasing-models>

R2: Minimize Microsoft SQL Server licensing costs

But question mentioned License with software assurance. Therefore you can use Azure Hybrid Benefit for your Azure SQL database. In the provisioned compute tier of the vCore-based purchasing model, you can exchange your existing licenses for discounted rates on Azure SQL Database and Azure SQL Managed Instance by using Azure Hybrid Benefit. So purchase mode should be vCore.

vCore & Elastic pool

upvoted 38 times

  **rdemontis** 3 years, 7 months ago

thanks for explanation

upvoted 3 times

  **rdemontis** 3 years, 7 months ago

And can confirm with microsoft documentation:

<https://docs.microsoft.com/en-us/azure/azure-sql/azure-hybrid-benefit?tabs=azure-powershell>

upvoted 3 times

  **anupam77** 3 years, 3 months ago

Correct.

Enable Azure Hybrid Benefit

Azure SQL Database

You can choose or change your licensing model for Azure SQL Database using the Azure portal or the API of your choice.

You can only apply the Azure Hybrid licensing model when you choose a vCore-based purchasing model and the provisioned compute tier for your Azure SQL Database. Azure Hybrid Benefit isn't available for service tiers under the DTU-based purchasing model or for the serverless compute tier.

<https://docs.microsoft.com/en-us/azure/azure-sql/azure-hybrid-benefit?tabs=azure-powershell>

upvoted 4 times

  **tteesstt**  3 years, 9 months ago

DTU is cheaper but you need vCore model to apply hybrid benefits.

What is Azure Hybrid Benefit for SQL Server, and am I eligible for it?

<https://azure.microsoft.com/en-us/pricing/details/azure-sql-database/elastic/>

upvoted 9 times

  **haazybanj**  2 years, 7 months ago

Answer is correct

upvoted 1 times

  **AubinBakana** 2 years, 10 months ago

This option "Minimize Microsoft SQL Server licensing costs." pretty much threw me off thinking as I thought this alone forced the choice to be a full SQL Server on a VM. I guess I didn't understand. I think they should have said SQL License to avoid confusion but I will not make the mistake again.

Thank you for the explanation.

upvoted 1 times

  **kanweng** 3 years, 3 months ago

For Azure SQL Database, Azure Hybrid Benefit is only available when using the provisioned compute tier of the vCore-based purchasing model. Azure Hybrid Benefit doesn't apply to DTU-based purchasing models or the serverless compute tier.

upvoted 1 times

  **waqas** 3 years, 8 months ago

Given answers are correct.

upvoted 1 times

  **syu31svc** 3 years, 8 months ago

<https://docs.microsoft.com/en-us/azure/azure-sql/database/purchasing-models>

Virtual core (vCore)-based purchasing model (recommended). This purchasing model provides a choice between a provisioned compute tier and a serverless compute tier. With the provisioned compute tier, you choose the exact amount of compute resources that are always provisioned for your workload. With the serverless compute tier, you specify the autoscaling of the compute resources over a configurable compute range

vCore as purchasing model

"deploy 50 databases"

elastic pool for deployment

upvoted 2 times

🗳️ 👤 **roky** 3 years, 9 months ago

I think the answer might be DTU or vCore and sql elastic pool

refer these

<https://docs.microsoft.com/ko-kr/azure/azure-sql/database/elastic-pool-overview#how-do-i-choose-the-correct-pool-size>

upvoted 2 times

🗳️ 👤 **sjai** 3 years, 9 months ago

In the provisioned compute tier of the vCore-based purchasing model, you can exchange your existing licenses for discounted rates on Azure SQL Database and Azure SQL Managed Instance by using Azure Hybrid Benefit

<https://docs.microsoft.com/en-us/azure/azure-sql/azure-hybrid-benefit?tabs=azure-powershell>

upvoted 1 times

🗳️ 👤 **monkalways** 3 years, 9 months ago

Answer is correct.

upvoted 1 times

🗳️ 👤 **Ario** 3 years, 9 months ago

Deployment option should be : SQL Managed Instance :

SQL Managed Instance uses vCores mode and enables you to define maximum CPU cores and maximum of storage allocated to your instance. All databases within the managed instance will share the resources allocated to the instance.

<https://docs.microsoft.com/en-us/azure/azure-sql/database/scale-resources>

upvoted 2 times

🗳️ 👤 **Sathya22** 3 years, 9 months ago

In this question , it is not mentioned whether migration is happening . So Definitely SQL managed instance is not the answer

upvoted 1 times

🗳️ 👤 **monkalways** 3 years, 9 months ago

Disagree. Deployment option should be elastic pool, which supports vCore-based purchasing model too.

[https://docs.microsoft.com/en-us/azure/azure-sql/database/elastic-pool-](https://docs.microsoft.com/en-us/azure/azure-sql/database/elastic-pool-overview#:~:text=%20Creating%20a%20new%20SQL%20Database%20elastic%20pool,pool%20to%20create%20a%20pool%20directly...%20More%20)

[overview#:~:text=%20Creating%20a%20new%20SQL%20Database%20elastic%20pool,pool%20to%20create%20a%20pool%20directly...%20More%20](https://docs.microsoft.com/en-us/azure/azure-sql/database/elastic-pool-overview#:~:text=%20Creating%20a%20new%20SQL%20Database%20elastic%20pool,pool%20to%20create%20a%20pool%20directly...%20More%20)

upvoted 2 times

🗳️ 👤 **Ario** 3 years, 9 months ago

You are right with elastic pool we save some money which required in this question

upvoted 2 times

🗳️ 👤 **TheAzureArchitect** 3 years, 7 months ago

Managed instance is the answer when you need near 100% compatibility with an existing on-prem deployment of SQL.

The question does not mention migration of a solution so managed instance is not the solution.

upvoted 1 times

DRAG DROP -

You plan to import data from your on-premises environment into Azure. The data is shown in the following table.

On-premises source	Azure target
A Microsoft SQL Server 2012 database	An Azure SQL database
A table in a Microsoft SQL Server 2014 database	An Azure Cosmos DB account that uses the SQL API

What should you recommend using to migrate the data? To answer, drag the appropriate tools to the correct data sources. Each tool may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

### Tools

AzCopy

Azure Cosmos DB Data Migration Tool

Data Management Gateway

Data Migration Assistant

### Answer Area

From the SQL Server 2012 database:

Tool

From the table in the SQL Server 2014 database:

Tool

### Suggested Answer:

### Tools

AzCopy

Azure Cosmos DB Data Migration Tool

Data Management Gateway

Data Migration Assistant

### Answer Area

From the SQL Server 2012 database:

Data Migration Assistant

From the table in the SQL Server 2014 database:

Azure Cosmos DB Data Migration Tool

Reference:

<https://docs.microsoft.com/en-us/azure/dms/tutorial-sql-server-to-azure-sql> <https://docs.microsoft.com/en-us/azure/cosmos-db/import-data>

 **sharepoint\_Azure\_pp** Highly Voted 3 years, 8 months ago

Given answers are correct

choose the same


cleared with 900 on 17th October 2021

upvoted 17 times

 **plmmsg** Most Recent 3 years, 3 months ago

correct answer

upvoted 2 times

 **Dpejic** 3 years, 6 months ago

On exam 24.12.2021

upvoted 4 times

 **walkwolf3** 3 years, 7 months ago

Given answers are correct

The Data Migration Assistant (DMA) migrates SQL sources to SQL destinations.

<https://docs.microsoft.com/en-us/sql/dma/dma-overview?view=sql-server-ver15#supported-source-and-target-versions>

Azure Cosmos DB Data Migration tool is to migrate different sources including SQL to Azure Cosmo DB

You can import from JSON files, CSV files, SQL, MongoDB, Azure Table storage, Amazon DynamoDB, and even Azure Cosmos DB SQL API collections.

You migrate that data to collections and tables for use with Azure Cosmos DB.

<https://docs.microsoft.com/en-us/azure/cosmos-db/import-data>

upvoted 4 times

🗲️ 👤 **waqas** 3 years, 8 months ago

Given answers are correct.

upvoted 2 times

🗲️ 👤 **syu31svc** 3 years, 8 months ago

provided links support answer given

upvoted 2 times

🗲️ 👤 **gssd4scoder** 3 years, 8 months ago

It's correct without any further doubt

upvoted 2 times

🗲️ 👤 **cfsxtuv33** 3 years, 8 months ago

Answers are correct for both boxes.

upvoted 2 times

🗲️ 👤 **roky** 3 years, 9 months ago

i think it might be correct

refer these

1 : <https://docs.microsoft.com/ko-kr/sql/dma/dma-overview?view=sql-server-ver15#supported-source-and-target-versions>

2 : <https://docs.microsoft.com/ko-kr/azure/cosmos-db/import-data#import-from-sql-server>

upvoted 2 times



You have an Azure virtual machine named VM1 that runs Windows Server 2019 and contains 500 GB of data files. You are designing a solution that will use Azure Data Factory to transform the data files, and then load the files to Azure Data Lake Storage. What should you deploy on VM1 to support the design?

- A. the Azure Pipelines agent
- B. the Azure File Sync agent
- C. the On-premises data gateway
- D. the self-hosted integration runtime

**Suggested Answer: D**

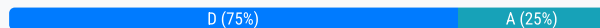
The integration runtime (IR) is the compute infrastructure that Azure Data Factory uses to provide data-integration capabilities across different network environments. For details about IR, see Integration runtime overview.

A self-hosted integration runtime can run copy activities between a cloud data store and a data store in a private network. It also can dispatch transform activities against compute resources in an on-premises network or an Azure virtual network. The installation of a self-hosted integration runtime needs an on-premises machine or a virtual machine inside a private network.

Reference:

<https://docs.microsoft.com/en-us/azure/data-factory/create-self-hosted-integration-runtime>

Community vote distribution



🗳️ 👤 **ForYEO** Highly Voted 4 years, 7 months ago

answer is correct:

<https://docs.microsoft.com/en-us/azure/data-factory/connector-file-system>

"

If your data store is located inside an on-premises network, an Azure virtual network, or Amazon Virtual Private Cloud, you need to configure a self-hosted integration runtime to connect to it.

"

upvoted 37 times

🗳️ 👤 **shaktiprasad88** 3 years, 3 months ago

Use the self-hosted integration runtime even if the data store is in the cloud on an Azure Infrastructure as a Service (IaaS) virtual machine.

upvoted 1 times

🗳️ 👤 **speedminer** Highly Voted 4 years, 9 months ago

The integration runtime (IR) is the compute infrastructure that Azure Data Factory uses to provide data-integration capabilities across different network environments. For details about IR, see Integration runtime overview.

A self-hosted integration runtime can run copy activities between a cloud data store and a data store in a private network. It also can dispatch transform activities against compute resources in an on-premises network or an Azure virtual network. The installation of a self-hosted integration runtime needs an on-premises machine or a virtual machine inside a private network.

This article describes how you can create and configure a self-hosted IR.

upvoted 17 times

🗳️ 👤 **Lengthmad** 4 years, 2 months ago

Great example of cut and paste from the original answer

upvoted 19 times

🗳️ 👤 **Viji30** 3 years, 9 months ago

so what, summarize here

upvoted 1 times

🗳️ 👤 **crv2011** 4 years, 1 month ago



upvoted 4 times

🗨️ **AubinBakana** Most Recent 2 years, 10 months ago

Of all the 4 options that has to be the answer. Although it is not the only option  
upvoted 1 times

🗨️ **VijayRaja2000** 3 years ago

When you use the Azure Data Factory to move the data, the solution that you will need to install on the VM would be Self Hosted Integrated Runtime only. I have never seen anyone using any other solution on the VM with ADF  
upvoted 1 times

🗨️ **hertino** 3 years, 2 months ago

In AZ-305 exam, 9 april 22  
upvoted 2 times

🗨️ **Simon\_G** 3 years, 3 months ago

D. the self-hosted integration runtime

Similar question in Az-303 Module 8 Review Questions:

Your organization has an Azure VM named OEM\_VM3 that runs on Windows Server 2019 and contains 1 TB of data files.

You are asked to design a solution using Azure Data Factory to transform the data files and then load them into Azure Data Lake Storage.

What should you deploy on OEM\_VM3 to support your design?

Correct answer (provided by MS): A self-hosted integration runtime. A self-hosted integration runtime can run copy activities between a cloud data store and a data store in a private network.

upvoted 1 times

🗨️ **LuBarba** 3 years, 4 months ago

**Selected Answer: D**

SHIR is needed for connecting the on-prem data store

upvoted 1 times

🗨️ **jr\_luciano** 3 years, 4 months ago

**Selected Answer: D**

Answer: D

upvoted 2 times

🗨️ **us3r** 3 years, 4 months ago

**Selected Answer: A**

test wrong vote.

Answer: D

upvoted 1 times

🗨️ **Dpejic** 3 years, 6 months ago

Appere on exam 23-dec-2021

upvoted 3 times

🗨️ **dkltruong88** 3 years, 9 months ago

Was in exam today 1-10-2021. I passed with score 896. I chose D

upvoted 9 times

🗨️ **syu31svc** 3 years, 9 months ago

"solution that will use Azure Data Factory to transform the data files"

This is D for sure; self-hosted integration runtime

upvoted 1 times

🗨️ **am110** 3 years, 11 months ago

To me answer seems D. Self hosted IR because it is mentioned in below link that "Use the self-hosted integration runtime even if the data store is in the cloud on an Azure Infrastructure as a Service (IaaS) virtual machine." <https://docs.microsoft.com/en-us/azure/data-factory/create-self-hosted-integration-runtime>



upvoted 3 times

🗨️ **cfsxtuv33** 4 years ago

After careful review of the question I have to agree with some comments regarding where this all takes place. In the question, there is absolutely no mention of on-prem. This seems to take place in Azure. If that is the case then "the self-hosted integration runtime" is not necessarily the answer.

According to Microsoft "A self-hosted integration runtime can run copy activities between a cloud data store and a data store in a private network. It also can dispatch transform activities against compute resources in an on-premises network or an Azure virtual network."

upvoted 3 times

  **cfsxtuv33** 3 years, 11 months ago

You're absolutely correct, there is no mention of on-prem. Regardless, the other answers really don't fit at all.

upvoted 2 times

  **BoxGhost** 3 years, 10 months ago

They can also be deployed onto Azure VMs:

<https://azure.microsoft.com/en-gb/resources/templates/vms-with-selfhost-integration-runtime/>

upvoted 3 times

  **gssd4scoder** 4 years ago



Anyway I think that Azure File Sync should do the work. Since Azure Data Lake Storage is in the end a Storage account.

upvoted 2 times

  **Amit3** 4 years ago

I have worked with Azure Data Factory for a long time and given answer is correct.

upvoted 4 times

  **KNG** 4 years, 3 months ago

Correct.

Use the self-hosted integration runtime even if the data store is in the cloud on an Azure Infrastructure as a Service (IaaS) virtual machine.

<https://docs.microsoft.com/en-us/azure/data-factory/create-self-hosted-integration-runtime>

upvoted 1 times

  **ElsaBBP** 4 years, 4 months ago



read the question again. it says both data and Data Lake are in Azure, so Azure pipeline is the answer not the self hosted IR.

upvoted 3 times

  **HNatalie** 4 years, 3 months ago



self host IR is for private network

upvoted 2 times

  **MRabi** 4 years, 1 month ago

The installation of a self-hosted integration runtime needs an on-premises machine or a virtual machine inside a private network.

upvoted 1 times

  **4tune** 4 years, 1 month ago

It is a virtual machine sitting in azure. A private network.

A self-hosted integration runtime can run copy activities between a cloud data store and a data store in a private network. It also can dispatch transform activities against compute resources in an on-premises network or an Azure virtual network.

upvoted 2 times

**HOTSPOT -**

Your company is designing a multi-tenant application that will use elastic pools and Azure SQL databases. The application will be used by 30 customers.

You need to design a storage solution for the application. The solution must meet the following requirements:

- ⇒ Operational costs must be minimized.
- ⇒ All customers must have their own database.
- ⇒ The customer databases will be in one of the following three Azure regions: East US, North Europe, or South Africa North.

What is the minimum number of elastic pools and Azure SQL Database servers required? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Elastic pools:

▼
1
3
6
10
30

Azure SQL Database servers:

▼
1
3
6
10
30

**Answer Area**

Elastic pools:

▼
1
3
6
10
30

Suggested Answer:

Azure SQL Database servers:

▼
1
3
6
10
30

Box 1: 3 -

The server, its pools & databases must be in the same Azure region under the same subscription.

Box 2: 3 -

A server can have up to 5000 databases associated to it.

Reference:

<https://vincentlauzon.com/2016/12/18/azure-sql-elastic-pool-overview/>

If they mentioned,

The customer databases will be in the following three Azure regions; Then, that means it is ok to have the databases in all three regions.

BUT,

They mentioned,

The customer databases will be in ONE OF THE following three Azure regions, which means all the databases must be in ONLY ONE region, and it can be East US, North Europe, or South Africa North.

A server can have up to 5000 databases associated to it.

So the answer should be 1 Azure SQL database server and 1 Elastic pool.

upvoted 37 times

  **wwwmmm** 2 years, 6 months ago

This is not a logic test, what if several customer dbs fall into different regions, then will 1 server and 1 pool still fit the purpose? I think it should be 3 servers, 3 pools.

upvoted 1 times

  **rsharma007** 3 years, 8 months ago

Customer DB will be in one of the 3 regions. So they should have that option which can only be achieved by having an elastic pool in each region. It is ok to have to have it all in one region, but that wouldn't meet the requirement .

upvoted 6 times

  **ShivaUdari** 1 year, 9 months ago

It's not DB, it's DB's. So all three will be in any one region.

upvoted 1 times

  **examineezer** 3 years, 7 months ago

I think what the question meant was "the customer databases will be across three regions". They're not testing grammar or logic.

upvoted 19 times

  **Warriors** 3 years, 3 months ago

And how do you know what the question meant? Did you set it? If you interpret the question as is, then @RasiR is correct

upvoted 3 times

  **mchint01**  4 years, 8 months ago



Correct

upvoted 28 times

  **Chris\_Munnik**  3 years ago

The customers only need their on DB, not their own server. And the fact that the customer databases will be in ONE OF THE following three Azure regions, means it will be 1 & 1.

upvoted 3 times

  **Zsolt72** 3 years, 2 months ago

I mean the key here is the multi tenant application that is a cross region architecture for possible customers from different regions. So I suppose the mentioned 3 regions should contains the infrastructure.

3/3

upvoted 2 times



  **cloudera** 3 years, 2 months ago

All the customer databases will be in one of the three regions or the database can spread across 3 regions?

The question is not clear.

If the database can spread across 3 regions then the answer is correct. If not, 1 DB server and 1 Elastic pool.

upvoted 2 times

  **ranjitklive** 3 years, 3 months ago

Answer --> 3, 3

Customer can belong to any of the 3 regions given. So, we need 3 DB servers at the very least. One elastic pool per DB server, therefore 3 Elastic Pool.

upvoted 1 times

  **therealss** 3 years, 4 months ago

It's pretty obvious to me that "a multi-tenant app with 30 customers" might need 3 regions BECUASE those disparate customers could have varying legal requirements that require them store corporate data in a specific geography. This scenario is much more likely than "hey, let's spin a wheel and decide where our 1 central DB is...one of these 3 is good!". So back to the answer, I'd go with 3 and 3.

upvoted 3 times

🗳️ 👤 **Uglydotcom** 3 years, 4 months ago

One SQL server to hold one elastic pool in each of the 3 regions mentioned, so answer is 3 pools, 3 servers.

upvoted 1 times

🗳️ 👤 **Dpejic** 3 years, 6 months ago

On exam 24.12.2021

upvoted 4 times

🗳️ 👤 **donathon** 3 years, 6 months ago

Elastic Pool can only stretch across a single region so it should be 3 3.

upvoted 5 times

🗳️ 👤 **sharepoint\_Azure\_pp** 3 years, 8 months ago

i choose 3 & 3

cleared with 900 on 17th October 2021

upvoted 14 times

🗳️ 👤 **waqas** 3 years, 8 months ago

Given answers are correct.

upvoted 1 times

🗳️ 👤 **syu31svc** 3 years, 8 months ago

If the customers can be in one of the three Azure Regions, this means that it will probably have customers in all regions, these are the regions where the customers will be, so you will need 3 elastic pools, one for each region and one sql server for each region.

upvoted 3 times

🗳️ 👤 **davidfernandezperrino** 3 years, 5 months ago

yeah, that's the key. Customers can be in one of the three azure regions, but you have 30 customers, and they are not saying that "all customers are in the same region", so you have to cover the three regions => 3 elastic pools with 3 servers

upvoted 1 times

🗳️ 👤 **dkltruong88** 3 years, 9 months ago

Was in exam today 1-10-2021. I passed with score 896. I chose 3 and 3

upvoted 5 times

🗳️ 👤 **bingomutant** 4 years, 7 months ago

The customer databases will be in one of the following three Azure regions - this is ambiguous. Does it mean ALL databases must be in one region - or each customer database can be in one of 3 regions? I think it must be the latter so 3/3. But there is doubt.

upvoted 3 times

🗳️ 👤 **Oliz** 4 years, 7 months ago

how did we arrive at 3 for the number of DB servers? why not 1 since 5000 DBs can be hosted on a server? Moreover, the question said the databases would be hosted in ONE of the 3 regions mentioned.

upvoted 2 times

🗳️ 👤 **mmmore** 4 years, 7 months ago

This is a bit of a trick question. My first thought was 3 databases and 3 elastic pools. Given that you will use 3 separate regions. But it could be that they actually mean that the databases should be in ONE of the three regions. I that case you need 1 db and elastic pool.

upvoted 4 times

🗳️ 👤 **MaxBlanche** 4 years, 7 months ago

⇒ All customers must have their own database.

⇒ The customer databases will be in one of the following three Azure regions: East US, North Europe, or South Africa North.

This means that we'll have many dbs, part on region 1, part on region 2 and part on region 3. So we'll need 3 servers and 3 pools.

upvoted 3 times

🗳️ 👤 **TheAzureArchitect** 3 years, 7 months ago

Microsoft don't do trick questions. You were correct with 3 and 3.

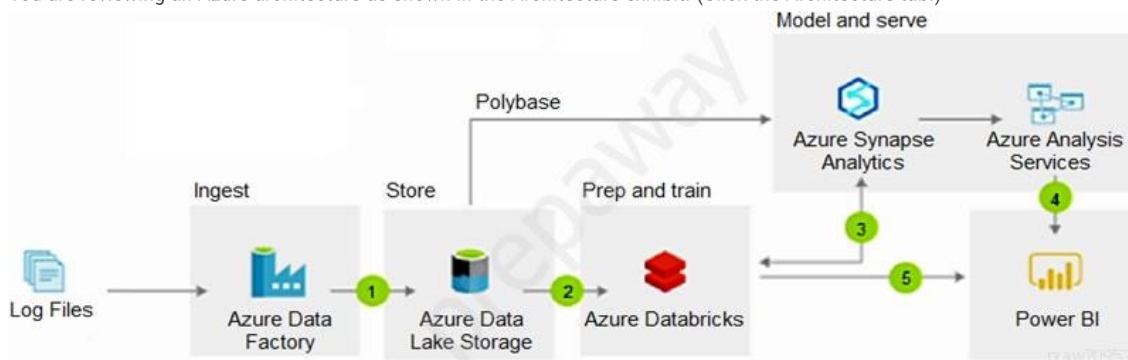
upvoted 2 times

🗳️ 👤 **saditya1** 4 years, 7 months ago

correct

upvoted 2 times

You are reviewing an Azure architecture as shown in the Architecture exhibit. (Click the Architecture tab.)



The estimated monthly costs for the architecture are shown in the Costs exhibit. (Click the Costs tab.)

Estimate total: US\$7,739.99		
Azure Synapse Analytics	Tier: Compute-optimised Gen2, Compute: DWU 100 x 1 ...	US\$998.88
Data Factory	Azure Data Factory V2 Type, Data Pipeline Service type, ...	US\$4,993.14
Azure Analysis Services	Developer (hours), 5 Instance(s), 720 Hours	US\$475.20
Power BI Embedded	1 node(s) x 1 Months, Node type: A1, 1 Virtual Core(s), 3...	US\$735.91
Storage Accounts	Block Blob Storage, General Purpose V2, LRS Redundan...	US\$21.84
Azure Databricks	Data Analytics Workload, Premium Tier, 1 D3V2 (4 vCPU...	US\$515.02

The log files are generated by user activity to Apache web servers. The log files are in a consistent format. Approximately 1 GB of logs are generated per day.

Microsoft Power BI is used to display weekly reports of the user activity.

You need to recommend a solution to minimize costs while maintaining the functionality of the architecture.

What should you recommend?

- A. Replace Azure Synapse Analytics and Azure Analysis Services with SQL Server on an Azure virtual machine.
- B. Replace Azure Synapse Analytics with Azure SQL Database Hyperscale.
- C. Replace Azure Data Factory with CRON jobs that use AzCopy.
- D. Replace Azure Databricks with Azure Machine Learning.

#### Suggested Answer: C

AzCopy is a command-line utility that you can use to copy blobs or files to or from a storage account.

Cron is one of the most useful utility that you can find in any Unix-like operating system. It is used to schedule commands at a specific time. These scheduled commands or tasks are known as "Cron Jobs".

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-configure>

Community vote distribution

C (100%)

**gcpjay** Highly Voted 4 years, 6 months ago

The question states that "The log files are in a consistent format." So, no ETL is required. The files can be copied directly using the AzCopy command.  
upvoted 71 times

**JDA** Highly Voted 4 years, 4 months ago

The answer is C. In the real world, I'd be asking some hard questions about why ADF was costing so much with that traffic volume ...  
upvoted 22 times

**tteesst** 3 years, 8 months ago

I made a mistake once and kept ADF running for 2 days. The pipeline was pretty basic - to copy logs to SQL Database. The bill for those 2 days was over 100\$.  
upvoted 2 times

**ShivaUdari** 1 year, 9 months ago

I left Dedicated SQL Pool running for 2 days and it costed 500\$



upvoted 1 times

🗨️ 👤 **GaneshPP** Most Recent 2 years, 8 months ago

Even though C is the right answer, its like recommending - don't use cloud.

upvoted 1 times

🗨️ 👤 **pingpongset** 2 years, 10 months ago

"Replace Azure Data Factory with CRON jobs that use AzCopy." but where are the Cron jobs using AzCopy running?

upvoted 1 times

🗨️ 👤 **ShivaUdari** 1 year, 9 months ago

Majority Apache Servers on Linux, so CRON can be used.

upvoted 1 times

🗨️ 👤 **AubinBakana** 2 years, 10 months ago

Selected Answer: C

The fact that they are using ADF & Synapse Analysis is a huge alert. They both pretty much do the same in most case. A good place to start to look. And if you are just copying log files to ADL, of course Azure Data Factory with CRON jobs has to be the answer

upvoted 2 times

🗨️ 👤 **Dawn7** 3 years, 3 months ago

Selected Answer: C

Answer is c

upvoted 1 times

🗨️ 👤 **plmmsg** 3 years, 3 months ago

Selected Answer: C

AZCopy

upvoted 1 times

🗨️ 👤 **ShivaNatarajan** 3 years, 6 months ago

If not ADF which service is going to be used to orchestrate this data pipeline ?

upvoted 1 times

🗨️ 👤 **Dpejic** 3 years, 6 months ago

Appere on exam 23-dec-2021

upvoted 3 times

🗨️ 👤 **syu31svc** 3 years, 8 months ago

I'd take C for 2 reasons

1) Data Factory is the most expensive service used so it should be replaced

2) Log files in consistent format so just use AzCopy will do

upvoted 4 times

🗨️ 👤 **dkltruong88** 3 years, 9 months ago

Was in exam today 1-10-2021. I passed with score 896. I chose C

upvoted 3 times

🗨️ 👤 **Tachinsky** 3 years, 9 months ago

Correct. Also appears in the practice questions for AZ304

upvoted 2 times

🗨️ 👤 **Gautam1985** 3 years, 10 months ago

Correct

upvoted 1 times

🗨️ 👤 **StarkStrange** 3 years, 10 months ago

Have used a similar arch in one of our use case. ADF doesn't cost this much, anyways, with this bill probably the given ans is correct.

upvoted 1 times

🗨️ 👤 **az\_architect** 3 years, 10 months ago



Since, ADF is being used for trivial task of just copying the log files already in consistent format. Hence, it need to go to save the cost.

upvoted 3 times

🗨️ 👤 **AravindITGuy** 3 years, 12 months ago

if we notice in the diagram Azure Data Factory is where the most money is spent, and the solution is to minimize costs hence we need to look for a solution that deals with data factory and makes sense so I would say C is the right answer.

upvoted 4 times

  **atwind** 4 years, 4 months ago

<https://medium.com/@nimishrao/moving-a-file-in-seconds-to-your-azure-data-lake-generation-2-using-azcopy-6dde114258>

upvoted 2 times

You deploy Azure App Service Web Apps that connect to on-premises Microsoft SQL Server instances by using Azure ExpressRoute. You plan to migrate the SQL Server instances to Azure.

Migration of the SQL Server instances to Azure must:

- ⇒ Support automatic patching and version updates to SQL Server.
- ⇒ Provide automatic backup services.
- ⇒ Allow for high-availability of the instances.
- ⇒ Provide a native VNET with private IP addressing.
- ⇒ Encrypt all data in transit.
- ⇒ Be in a single-tenant environment with dedicated underlying infrastructure (compute, storage).

You need to migrate the SQL Server instances to Azure.

Which Azure service should you use?

- A. SQL Server in a Docker container running on Azure Container Instances (ACI)
- B. SQL Server in Docker containers running on Azure Kubernetes Service (AKS)
- C. SQL Server Infrastructure-as-a-Service (IaaS) virtual machine (VM)
- D. Azure SQL Database Managed Instance
- E. Azure SQL Database with elastic pools

**Suggested Answer: D**

Azure SQL Database Managed Instance configured for Hybrid workloads. Use this topology if your Azure SQL Database Managed Instance is connected to your on-premises network. This approach provides the most simplified network routing and yields maximum data throughput during the migration.

Reference:

<https://docs.microsoft.com/en-us/azure/dms/resource-network-topologies>

*Community vote distribution*

D (100%)

 **H** Highly Voted 4 years, 6 months ago


Correct answer

upvoted 46 times

 **QiangQiang** 4 years, 1 month ago

No, it should be E. SQLMI doesn't support private IP address

upvoted 1 times

 **tita\_tovenaar** 3 years, 11 months ago

wrong: "SQL Managed Instance has private IP addresses in its own virtual network", ref

<https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/connect-application-instance#connect-inside-a-different-vnet>

upvoted 9 times

 **sjai** 3 years, 9 months ago

At a high level, SQL Managed Instance is a set of service components. These components are hosted on a dedicated set of isolated virtual machines that run inside the customer's virtual network subnet. These machines form a virtual cluster.


<https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/connectivity-architecture-overview>

upvoted 9 times

 **erickim007** Highly Voted 4 years ago

the given answer is correct. Cannot have Azure SQL because it does not support VNET integration. SQL MI supports it.

upvoted 14 times

 **bruncili** 3 years, 4 months ago

Azure SQL Database can leverage private endpoint to support VNET integration

<https://docs.microsoft.com/en-us/azure/virtual-network/vnet-integration-for-azure-services#private-link-and-private-endpoints>

upvoted 1 times

🗳️ 👤 **jr\_luciano** Most Recent 3 years, 4 months ago

**Selected Answer: D**

Correct answer

upvoted 1 times

🗳️ 👤 **Akakentavr** 3 years, 4 months ago

The correct answer is D as one of the features related to Azure SQL Managed Instance is native Vnet integration - a native virtual network (VNet) implementation that addresses common security concerns

<https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/sql-managed-instance-paas-overview>

upvoted 1 times

🗳️ 👤 **c\_groleau** 3 years, 5 months ago

E - Azure SQL Database with elastic pools would be correct as well since it can have a private endpoint in the VNET

upvoted 1 times

🗳️ 👤 **TheBank** 3 years, 1 month ago

But its not native VNET Integration as with Azure SQL Managed Instance

upvoted 1 times

🗳️ 👤 **Eitant** 3 years, 6 months ago

**Selected Answer: D**

Correct answer

upvoted 2 times

🗳️ 👤 **syu31svc** 3 years, 9 months ago

"Support automatic patching and version updates"

Answer is D for sure

upvoted 5 times

🗳️ 👤 **GuxMAN** 3 years, 9 months ago

I think it's a trick question. I have been studying for the exam and I don't remember reading from Azure SQL Database MI, but I have read from Azure SQL MI, and only the above three options (A, B and C) indicate SQL Server, and the question is about the options for migrate SQL Server instances. The most reasonable option (following the observation if it is DB or Server) is C (IaaS), but this does not support automatic updates and patches. I'll see if this question will be in my close exam.

upvoted 1 times

🗳️ 👤 **SRJ11** 3 years, 10 months ago

C. SQL Server Infrastructure-as-a-Service (IaaS) virtual machine (VM)

Requirement - Provide a native VNET with private IP addressing.

This cannot be achieved on Azure SQL. With VNET integration you can restrict only the services within that VNET can reach DB, but still they have to reach the public endpoint of the DB (xx.database.windows.net) and not to a private IP.

upvoted 1 times

🗳️ 👤 **examineezer** 3 years, 6 months ago

This doesnt support automatic patching and version updates to SQL Server though does it?

upvoted 1 times

🗳️ 👤 **yyuryyuciryyforme** 3 years, 5 months ago

Azure supports automated backup and automated patching for an Azure VM with SQL Server installed. It must be either SQL Server 2014 or 2016+, and with the SQL IaaS Agent extension in full management mode. A pair of VMs with AGs can support the multiple SQL instances required. Not strictly mentioned in the question, but reasonable implication is existing on-premises SQL licensing. With Software Assurance in a migration scenario both on-premises and cloud VMs are covered for 180 days. An Azure VM as the SQL AG failover server would not require a license if used purely for business continuity. Using SQL on an Azure VM with multiple instances could be the best solution.

<https://docs.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/automated-backup>

<https://docs.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/automated-patching>

<https://docs.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/sql-server-iaas-agent-extension-automate-management>

I think my answer will be C.

upvoted 2 times

🗳️ 👤 **tehex** 3 years, 10 months ago

D is the correct answer.

Everything is in this section <https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/sql-managed-instance-paas-overview#key-features-and-capabilities>

upvoted 2 times

🗳️ 👤 **Shashprasad** 3 years, 11 months ago

Answer is D, refer the link and check in that 'Key features and capabilities', all the requirements are met.

<https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/sql-managed-instance-paas-overview>

upvoted 2 times

🗳️ 👤 **Oracleist** 4 years, 1 month ago

Managed Instance(Be in a single-tenant environment with dedicated underlying infrastructure (compute, storage))

read

<https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/sql-managed-instance-paas-overview>

upvoted 4 times

🗳️ 👤 **parkranger** 3 years, 6 months ago

1. Single-tenant with dedicated underlying infrastructure (compute, storage). 2. Automatic patch

upvoted 1 times

🗳️ 👤 **reubems** 4 years, 1 month ago

Exactly, on that link you mention it appears as capabilities this:

Isolated environment (VNet integration, single tenant service, dedicated compute and storage)

So the right answer is Managed Instance.

upvoted 2 times

🗳️ 👤 **QiangQiang** 4 years, 1 month ago

it should be E.

upvoted 1 times

🗳️ 👤 **nooranikhan** 4 years, 2 months ago

You guys seem to have missed the most important part of the question "Be in a single-tenant environment with dedicated underlying infrastructure (compute, storage)" Managed instances runs on shared infrastructure. Only IAAS can allow you to choose reserved instances

upvoted 4 times

🗳️ 👤 **Oracleist** 4 years, 2 months ago

read better

<https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/sql-managed-instance-paas-overview>

Key features and capabilities

upvoted 7 times

🗳️ 👤 **4tune** 4 years, 1 month ago

reserved instances doesn't equate to dedicated or isolated

upvoted 2 times

🗳️ 👤 **dcprice** 4 years, 4 months ago

why isn't "E. Azure SQL Database with elastic pools" a valid option then?

upvoted 3 times

🗳️ 👤 **yaiba** 4 years, 3 months ago

because of "native Vnet with private addressing".

SQL Managed Instance can be injected in customer's VNet.


<https://docs.microsoft.com/en-us/azure/azure-sql/database/features-comparison>

upvoted 2 times

🗳️ 👤 **glam** 4 years, 5 months ago

D. Azure SQL Database Managed Instance

upvoted 3 times

  **milind8451** 4 years, 5 months ago

Right ans.

upvoted 3 times

You plan to store data in Azure Blob storage for many years. The stored data will be accessed rarely.

You need to ensure that the data in Blob storage is always available for immediate access. The solution must minimize storage costs.

Which storage tier should you use?

- A. Cool
- B. Archive
- C. Hot

**Suggested Answer: A**

Data in the cool access tier can tolerate slightly lower availability, but still requires high durability, retrieval latency, and throughput characteristics similar to hot data. For cool data, a slightly lower availability service-level agreement (SLA) and higher access costs compared to hot data are acceptable trade-offs for lower storage costs.

Incorrect Answers:

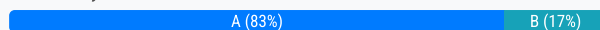
B: Archive storage stores data offline and offers the lowest storage costs but also the highest data rehydrate and access costs.

Archive - Optimized for storing data that is rarely accessed and stored for at least 180 days with flexible latency requirements (on the order of hours).

Reference:

<https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers>

Community vote distribution



**nasascientist** Highly Voted 4 years, 6 months ago

Cool tier is correct answer.. hot tier will be costlier and accessing data from archive tier takes time.

upvoted 42 times

**crraburn** Highly Voted 4 years, 4 months ago

Coolio

upvoted 21 times

**Sam12** 4 years, 4 months ago

I'll see you when you get there...

upvoted 10 times

**us3r** 3 years, 4 months ago

As I walk through the valley of the shadow of death

I take a look at my life, and realize there's nothin' left

upvoted 6 times

**examrobot** Most Recent 3 years, 3 months ago

Selected Answer: A

archive is not immediately accessible, so it's cool

upvoted 1 times

**Netspud** 3 years, 3 months ago

Selected Answer: A

A is correct

upvoted 1 times

**azahran** 3 years, 3 months ago

Both Cool and Hot are online so for sure Cool.

upvoted 1 times

**Dawn7** 3 years, 3 months ago

Selected Answer: A

Sorry, I will go with A. Cool.



upvoted 2 times

**Dawn7** 3 years, 3 months ago

**Selected Answer: B**



I will go with B

upvoted 1 times

  **Dawn7** 3 years, 3 months ago

Forget this. My mistake.



upvoted 2 times

  **Dawn7** 3 years, 4 months ago

**Selected Answer: A**

A is correct.

upvoted 1 times

  **Carroyo826** 3 years, 6 months ago

Cool ----> correct answer



upvoted 1 times

  **syu31svc** 3 years, 8 months ago

"always available for immediate access" yet "minimize storage costs"



Answer is A

upvoted 4 times

  **nkV** 3 years, 9 months ago

came in exam on 20-sep-21, I passed, i choose given answer

upvoted 3 times

  **asahel** 3 years, 9 months ago

Hot because the data in Blob storage is always available for immediate access

upvoted 1 times

  **Spooky7** 3 years, 9 months ago

In cool tier you also have immediate access, just little bit slower than in hot tier. In archive tier you don't have an access and you need request it first.

upvoted 1 times

  **Sathya22** 3 years, 9 months ago

Read the question carefully . It was mentioned that files will be accessed RARELY . So COOL is the correct answer

upvoted 1 times

  **BlackZeros** 3 years, 11 months ago


was in exam today, answer is correct

upvoted 3 times

  **SnakePlissken** 4 years ago

Wow, a fundamentals question!

upvoted 4 times

  **glam** 4 years, 5 months ago

A. Cool

upvoted 3 times



## DRAG DROP -

You are designing a virtual machine that will run Microsoft SQL Server and will contain two data disks. The first data disk will store log files, and the second data disk will store data. Both disks are P40 managed disks.

You need to recommend a caching policy for each disk. The policy must provide the best overall performance for the virtual machine while preserving integrity of the SQL data and logs.

Which caching policy should you recommend for each disk? To answer, drag the appropriate policies to the correct disks. Each policy may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

Select and Place:

## Policies

None

ReadOnly

ReadWrite

## Answer Area

Log: Policy

Data: Policy

## Suggested Answer:

## Policies

ReadWrite

## Answer Area

Log: None

Data: ReadOnly

## Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sql/virtual-machines-windows-sql-performance>

 **M4gnet1k** Highly Voted 4 years, 7 months ago

The answers provided are correct, here is the explanation and supporting websites:

Log: None—Log files have primarily write-heavy operations. Therefore, they do not benefit from the ReadOnly cache.

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/premium-storage-performance#disk-caching>

Data: readonly—If you have separate storage pools for the log and data files, enable read caching only on the storage pool for the data files.

<https://docs.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices>

upvoted 97 times

 **syu31svc** 3 years, 9 months ago

Good find there!

upvoted 4 times

 **AubinBakana** 2 years, 10 months ago

Thank you


upvoted 1 times

 **glam** Highly Voted 4 years, 5 months ago

Log: None—

Data: readonly—

upvoted 7 times

 **ranjitklive** Most Recent 3 years, 3 months ago

Set host caching to read-only for data file disks.

Set host caching to none for log file disks.

upvoted 2 times

🗨️ 👤 **Droz36** 3 years, 6 months ago

<https://docs.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices-storage>

Correct

upvoted 1 times

🗨️ 👤 **azurecert2021** 4 years, 4 months ago

correct.

upvoted 4 times

🗨️ 👤 **kopper2019** 4 years, 6 months ago

correct

- Use premium SSDs for the best price/performance advantages. Configure Read only cache for data files and no cache for the log file.

upvoted 4 times

🗨️ 👤 **JustDiscussing** 4 years, 6 months ago

Following are the recommended disk cache settings for data disks,

TABLE 9

Disk caching setting recommendation on when to use this setting

None Configure host-cache as None for write-only and write-heavy disks.

ReadOnly Configure host-cache as ReadOnly for read-only and read-write disks.

ReadWrite Configure host-cache as ReadWrite only if your application properly handles writing cached data to persistent disks when needed.

<https://docs.microsoft.com/en-us/azure/virtual-machines/premium-storage-performance#disk-caching>

upvoted 3 times

🗨️ 👤 **xAlx** 4 years, 6 months ago

Correct

<https://docs.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices#disks-guidance>

If you are using separate disks for data and log files, enable read caching on the data disks hosting your data files and TempDB data files. This can result in a significant performance benefit. Do not enable caching on the disk holding the log file as this causes a minor decrease in performance.

upvoted 3 times

🗨️ 👤 **yyuryyucicuryyforme** 3 years, 5 months ago

Indeed

<https://docs.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/performance-guidelines-best-practices-storage#data-file-caching-policies>

ata disk Enable Read-only caching for the disks hosting SQL Server data files.

Reads from cache will be faster than the uncached reads from the data disk.

Uncached IOPS and throughput plus Cached IOPS and throughput will yield the total possible performance available from the virtual machine within the VMs limits, but actual performance will vary based on the workload's ability to use the cache (cache hit ratio).

Transaction log disk Set the caching policy to None for disks hosting the transaction log. There is no performance benefit to enabling caching for the Transaction log disk, and in fact having either Read-only or Read/Write caching enabled on the log drive can degrade performance of the writes against the drive and decrease the amount of cache available for reads on the data drive.

upvoted 2 times

You are designing a SQL database solution. The solution will include 20 databases that will be 20 GB each and have varying usage patterns. You need to recommend a database platform to host the databases. The solution must meet the following requirements:

- ⇒ The compute resources allocated to the databases must scale dynamically.
- ⇒ The solution must meet an SLA of 99.99% uptime.
- ⇒ The solution must have reserved capacity.
- ⇒ Compute charges must be minimized.

What should you include in the recommendation?

- A. 20 databases on a Microsoft SQL server that runs on an Azure virtual machine in an availability set
- B. 20 instances of Azure SQL Database serverless
- C. 20 databases on a Microsoft SQL server that runs on an Azure virtual machine
- D. an elastic pool that contains 20 Azure SQL databases

**Suggested Answer: D**

Azure SQL Database elastic pools are a simple, cost-effective solution for managing and scaling multiple databases that have varying and unpredictable usage demands. The databases in an elastic pool are on a single server and share a set number of resources at a set price.

Elastic pools in Azure SQL Database enable

SaaS developers to optimize the price performance for a group of databases within a prescribed budget while delivering performance elasticity for each database.

Guaranteed 99.995 percent uptime for SQL Database

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/elastic-pool-overview> <https://azure.microsoft.com/en-us/pricing/details/sql-database/elastic/>

Community vote distribution

D (100%)

🗳️ **xAlx** Highly Voted 4 years, 6 months ago

Correct

upvoted 35 times

🗳️ **syu31svc** Highly Voted 3 years, 8 months ago

Answer is D

<https://docs.microsoft.com/en-us/azure/azure-sql/database/elastic-pool-overview>

Azure SQL Database elastic pools are a simple, cost-effective solution for managing and scaling multiple databases that have varying and unpredictable usage demands. The databases in an elastic pool are on a single server and share a set number of resources at a set price. Elastic pools in Azure SQL Database enable SaaS developers to optimize the price performance for a group of databases within a prescribed budget while delivering performance elasticity for each database.

upvoted 7 times

🗳️ **OCHT** Most Recent 3 years, 1 month ago

**Selected Answer: D**

Correct answer is D

upvoted 1 times

🗳️ **Dawn7** 3 years, 3 months ago

**Selected Answer: D**

D is correct

upvoted 1 times

🗳️ **us3r** 3 years, 4 months ago

**Selected Answer: D**

D for the win

upvoted 1 times

🗨️ 👤 **AhmedHassan16** 3 years, 5 months ago

D. is the correct answer.

upvoted 1 times

🗨️ 👤 **Eitant** 3 years, 6 months ago

**Selected Answer: D**

Correct answer

upvoted 4 times

🗨️ 👤 **MasterArmSwitch** 3 years, 7 months ago

For me, due:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/serverless-tier-overview#scenarios-well-suited-for-serverless-compute>  
and

<https://docs.microsoft.com/en-us/azure/azure-sql/database/serverless-tier-overview#scenarios-well-suited-for-provisioned-compute>  
answer is D

upvoted 2 times

🗨️ 👤 **student22** 3 years, 8 months ago

D

---

I think Elastic Pools with reserved capacity will be cheaper than server less.

upvoted 2 times

🗨️ 👤 **nkx** 3 years, 9 months ago

came in exam on 20-sep-21, I passed, i choose A

upvoted 2 times

🗨️ 👤 **arslanshah86** 3 years, 9 months ago

"A" cant be correct. AVSets dont have 99.99% SLA

upvoted 7 times

🗨️ 👤 **VincentZhang** 3 years, 8 months ago

That's correct. AVSet is 99.95% while AVZone is 99.99%.

<https://www.azure.cn/en-us/support/sla/virtual-machines/>

upvoted 3 times

🗨️ 👤 **mootaa** 4 years, 1 month ago

Azure SQL databases can also do Reserved Capacity <https://docs.microsoft.com/en-us/azure/azure-sql/database/reserved-capacity-overview>

upvoted 2 times

🗨️ 👤 **Carlous** 4 years, 2 months ago

Curious, why not B?

upvoted 2 times

🗨️ 👤 **pekay** 4 years, 2 months ago

key is: databases that will be 20 GB each and have varying usage patterns. hence elastic pools

upvoted 8 times

🗨️ 👤 **Charles99** 4 years ago

so what? why won't serverless fulfill these two requirements?

upvoted 1 times

🗨️ 👤 **BoxGhost** 3 years, 10 months ago

It says 99.99% uptime required. Surely serverless is not suitable because of the warmup time as HDZ78 already mentioned?

<https://docs.microsoft.com/en-us/azure/azure-sql/database/serverless-tier-overview#scenarios>

Serverless is price-performance optimized for single databases with intermittent, unpredictable usage patterns that can afford some delay in compute warm-up after idle usage periods. In contrast, the provisioned compute tier is price-performance optimized for single databases or multiple databases in elastic pools with higher average usage that cannot afford any delay in compute warm-up

upvoted 1 times

🗨️ 👤 **Charles99** 4 years ago

rather, the reason can't be serverless is due to reserved capacity which is not supported in server tier

upvoted 7 times

🗨️ 👤 **GetulioJr** 4 years ago

That is right, B is out of question because it does not allow reserved capacity.

"Azure Hybrid Benefit (AHB) and reserved capacity discounts do not apply to the serverless compute tier."

REF: <https://docs.microsoft.com/en-us/azure/azure-sql/database/serverless-tier-overview#billing>

upvoted 3 times

🗨️ 👤 **ddb116** 4 years ago

This think people are not understanding reserved capacity. This is about pre-committing database servers. Essentially paying ahead.

Azure SQL Services for Managed instances and Azure SQL Database can both be have it. I agree with Mootu. With elastic pools you are sharing resources.

<https://docs.microsoft.com/en-us/azure/azure-sql/database/reserved-capacity-overview>

I think the answer is B.

upvoted 2 times

🗨️ 👤 **HDZ78** 3 years, 12 months ago

It depends on how you interpret reserved capacity. The GA blogpost way back clearly states that warm-up times after a period of inactivity are the trade off for serverless: <https://techcommunity.microsoft.com/t5/azure-sql/optimize-price-performance-with-compute-auto-scaling-in-azure/ba-p/966149>

To me that would make it D.

upvoted 1 times

🗨️ 👤 **Vipsao** 4 years, 3 months ago

D is Correct

upvoted 2 times

🗨️ 👤 **gdawg** 4 years, 4 months ago

HMMMM i read " The compute resources allocated to the databases must scale dynamically." to mean that it must autoscale and therefore went for B as that is the only option that autoscales, question is do they mean autoscale when they say "scale dynamically"?

upvoted 3 times

🗨️ 👤 **Leon3020** 4 years, 2 months ago

I would understand scale dynamically is equivalent to autoscale, otherwise we can Azure VM without autoscale included is also scale dynamically.

upvoted 1 times

🗨️ 👤 **Leon3020** 4 years, 2 months ago

Sorry, above is incorrect after I found below statement in MS website.

Dynamic scalability is different from autoscale. Autoscale is when a service scales automatically based on criteria, whereas dynamic scalability allows for manual scaling with a minimal downtime.

So the correct answer is B

upvoted 2 times

🗨️ 👤 **AmitDeorukhkar** 4 years, 2 months ago

Hello Leon, Was the article from where you fetched this Dynamic vs Auto scale in context to Azure SQL?

Both B and D sounds correct but in terms of terminologies, it cold be a different service

upvoted 1 times

🗨️ 👤 **glam** 4 years, 5 months ago

D. an elastic pool that contains 20 Azure SQL databases

upvoted 3 times

🗨️ 👤 **KirubakaraSen** 4 years, 6 months ago

99.95%?? Requirement is to have 99.99%.. Is this a typo..

upvoted 2 times

🗨️ 👤 **joshyz73** 4 years, 5 months ago

Not a typo. The article linked and the explanation say 99.995%, which is even greater than 99.99% (which is 99.990%), so it's all correct.

upvoted 2 times

🗨️ 👤 **arseyam** 4 years, 5 months ago

- Azure SQL Database Business Critical or Premium tiers configured as Zone Redundant Deployments have an availability guarantee of at least 99.995%.

- Azure SQL Database Business Critical or Premium tiers not configured for Zone Redundant Deployments, General Purpose, Standard, or Basic tiers, or Hyperscale tier with two or more replicas have an availability guarantee of at least 99.99%.

[https://azure.microsoft.com/en-us/support/legal/sla/sql-database/v1\\_5/](https://azure.microsoft.com/en-us/support/legal/sla/sql-database/v1_5/)

upvoted 4 times

You have an app named App1 that uses two on-premises Microsoft SQL Server databases named DB1 and DB2.

You plan to migrate DB1 and DB2 to Azure.

You need to recommend an Azure solution to host DB1 and DB2. The solution must meet the following requirements:

- ⇒ Support server-side transactions across DB1 and DB2.
- ⇒ Minimize administrative effort to update the solution.

What should you recommend?

- A. two Azure SQL databases in an elastic pool
- B. two Azure SQL databases on different Azure SQL Database servers
- C. two Azure SQL databases on the same Azure SQL Database managed instance
- D. two SQL Server databases on an Azure virtual machine

**Suggested Answer: C**

SQL Managed Instance enables system administrators to spend less time on administrative tasks because the service either performs them for you or greatly simplifies those tasks.

Note: Azure SQL Managed Instance is designed for customers looking to migrate a large number of apps from an on-premises or IaaS, self-built, or ISV provided environment to a fully managed PaaS cloud environment, with as low a migration effort as possible. Using the fully automated Azure Data Migration Service, customers can lift and shift their existing SQL Server instance to SQL Managed Instance, which offers compatibility with SQL Server and complete isolation of customer instances with native VNet support. With Software Assurance, you can exchange your existing licenses for discounted rates on SQL Managed Instance using the Azure Hybrid Benefit for SQL Server. SQL Managed Instance is the best migration destination in the cloud for SQL Server instances that require high security and a rich programmability surface.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/sql-managed-instance-paas-overview>

Community vote distribution

C (100%)

🗳️ **xAlx** Highly Voted 🍎 4 years, 6 months ago

Correct

<https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/sql-managed-instance-paas-overview#azure-active-directory-integration>  
upvoted 43 times

🗳️ **ruangel** Highly Voted 🍎 4 years, 1 month ago

<https://www.examttopics.com/exams/microsoft/az-303/view/2/>

You need to implement Azure services to host DB1 and DB2. The solution must support server-side transactions across DB1 and DB2.

Solution: You deploy DB1 and DB2 to SQL Server on an Azure virtual machine.

Reference: <https://docs.particular.net/nservicebus/azure/understanding-transactionality-in-azure>

upvoted 25 times

🗳️ **MrClumsy** 3 years, 5 months ago

<https://docs.microsoft.com/en-us/azure/azure-sql/database/elastic-transactions-overview>

In Important block:

Distributed transactions for Azure SQL Managed Instance are now generally available.

I believe correct answer is: C

upvoted 2 times

🗳️ **examineezer** 3 years, 6 months ago

Wrong, this doesnt minimize administrative effort compared with Managed Instance

upvoted 7 times

🗳️ **sapien45** 3 years ago

Nonsense.

<https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/sql-managed-instance-paas-overview?view=azuresql#azure-active-directory-integration>



. Azure AD server principals (logins) enable you to specify users and groups from your Azure AD tenant as true instance-scoped principals, capable of performing any instance-level operation, including cross-database queries within the same managed instance.

upvoted 1 times

  **hertino** Most Recent 3 years, 2 months ago

In AZ-305 exam, 9 april 22

upvoted 1 times

  **Dawn7** 3 years, 3 months ago

**Selected Answer: C**

I think C is correct


upvoted 1 times

  **massnonn** 3 years, 5 months ago

**Selected Answer: C**

Distributed transactions for Azure SQL Managed Instance are now generally available. Elastic Database Transactions for Azure SQL Database are in preview. <https://docs.microsoft.com/en-us/azure/azure-sql/database/elastic-transactions-overview>

upvoted 2 times

  **exammaster1000** 3 years, 6 months ago

This is C

Distributed transactions for Azure SQL Managed Instance are now generally available. Dec 2021

<https://docs.microsoft.com/en-us/azure/azure-sql/database/elastic-transactions-overview#transact-sql-development-experience>

upvoted 3 times

  **MasterArmSwitch** 3 years, 7 months ago

According to this: <https://docs.microsoft.com/en-us/azure/azure-sql/database/elastic-transactions-overview#transactions-for-sql-managed-instance> for me Answer is C



upvoted 2 times

  **syu31svc** 3 years, 8 months ago

"Minimize administrative effort to update "

This is C; Managed Instance

upvoted 6 times

  **tteesstt** 3 years, 9 months ago


Depends. If we assume Preview answers are allowed, then C, if not then D.

upvoted 2 times

  **nkx** 3 years, 9 months ago

came in exam on 20-sep-21, I passed, i choose C

upvoted 3 times

  **waqas** 3 years, 9 months ago

Answer is D....as other options are still under Preview.

upvoted 1 times

  **teehex** 3 years, 10 months ago

Managed instance already supported server-side transactions <https://docs.microsoft.com/en-us/azure/azure-sql/database/elastic-transactions-overview#transact-sql-development-experience>

upvoted 5 times

  **El\_Hechizo** 3 years, 11 months ago

Both C and D support server-side transactions but C has a less administrative effort

upvoted 8 times

  **stephw** 4 years, 1 month ago

Actually this should be a series of questions ... multiple answers are correct.

See <https://docs.microsoft.com/en-us/azure/azure-sql/database/elastic-transactions-overview>

upvoted 1 times

  **GeoTan** 4 years, 1 month ago

Answer is D

upvoted 4 times

  **Andrea25** 4 years, 1 month ago





Why you confuse others?

Minimize administrative effort to update the solution. --> You use an Azure virtual machine for minimize administrative effort??

The right ans is C

upvoted 12 times

  **kaunhe** 4 years, 1 month ago

Answer is C: Managed Instances

<https://docs.microsoft.com/en-us/azure/azure-sql/database/elastic-transactions-overview>

Transact-SQL development experience

"A server-side distributed transactions using Transact-SQL are available only for Azure SQL Managed Instance. Distributed transaction can be executed only between Managed Instances that belong to the same Server trust group. In this scenario, Managed Instances need to use linked server to reference each other."

Don't confuse this with the AZ-303 questions like I did. The correct answer is managed instances.

upvoted 14 times

  **claudio82** 4 years, 2 months ago

303 question, an the answer is D. "instead use virtual machine instance"

upvoted 9 times

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Location
VNET1	Virtual network	West US
Workspace1	Azure Log Analytics workspace	West US
storage1	Storage account	West US
storage2	Storage account	East US

You need to archive the diagnostic data for VNET1 for 365 days. The solution must minimize costs.

Where should you archive the data?

- A. Workspace1
- B. storage1
- C. storage2

**Suggested Answer: B**

Incorrect Answers:

A: When you create a new workspace, it automatically creates several Azure resources that are used by the workspace:

⇒ Azure Storage account: Is used as the default datastore for the workspace.

Note: The workspace is the top-level resource for Azure Machine Learning, providing a centralized place to work with all the artifacts you create when you use

Azure Machine Learning.

Reference:

<https://docs.microsoft.com/en-us/azure/machine-learning/concept-workspace>

Community vote distribution

B (100%)

GetulioJr Highly Voted 4 years ago

Answer is correct. Here is microsoft recommendation:

"Archiving logs and metrics to an Azure storage account is useful for audit, static analysis, or backup. Compared to Azure Monitor Logs and a Log Analytics workspace, Azure storage is less expensive and logs can be kept there indefinitely."

"The storage account needs to be in the same region as the resource being monitored if the resource is regional."

REF: <https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/diagnostic-settings?tabs=CMD>

upvoted 47 times

rdemontis 3 years, 7 months ago

thanks for explanation and for the documentation attached

upvoted 3 times

kwaazaar Highly Voted 4 years, 3 months ago

Probably storage1, since it's in the same region. Otherwise you pay for data transfer.

Has nothing to do with machine learning.

upvoted 15 times

icedog 3 years, 4 months ago

It's a bit more than that.

You can't Diagnostic settings to Archive to a storage account that is not in the same region as the resource itself.

upvoted 1 times

Dawn7 Most Recent 3 years, 3 months ago

Selected Answer: B

B is correct

upvoted 1 times

us3r 3 years, 4 months ago

Selected Answer: B

vote b

upvoted 1 times

🗨️ 👤 **AhmedHassan16** 3 years, 5 months ago

B. is the correct answer

Storage1 is the same region and cheaper than the log analytics workspace

upvoted 1 times

🗨️ 👤 **syu31svc** 3 years, 8 months ago

The storage account needs to be in the same region as the resource being monitored. it will incur additional egress charges to transfer data so answer is B

upvoted 5 times

🗨️ 👤 **jayantthegreat2** 4 years ago

B (storage 1) is correct as it is cost effective and can store data for longer periods whereas in Azure Log Analytics workspace, every GB of data ingested into your Azure Monitor Log Analytics workspace can be retained at no charge for up to first 31 days. Data retained beyond first 31 days will be charged per the data retention prices listed below.

upvoted 6 times

🗨️ 👤 **Oracleist** 4 years, 2 months ago

if I pay for Log analytics why not send to workspace?

upvoted 2 times

🗨️ 👤 **us3r** 3 years, 4 months ago

it is what it is

upvoted 1 times

🗨️ 👤 **shooty** 4 years, 2 months ago

Clever remark ! It there a trick here finally ?

No sure anyway, we don't use analytics for archive retention usually.

I'll pick Storage 1 anyway!

upvoted 2 times

🗨️ 👤 **sunmonkey** 4 years, 2 months ago

The question is asking to archive the data, so a storage account would be more cost effective.

upvoted 4 times

🗨️ 👤 **Kctaz** 3 years, 4 months ago

A bit late to answer you but here is why you choose Azure Storage here instead of Log analytics workspace : the question is asking to retain the data for 365 days while log analytics workspace only keep them 90 days (thought you can expand to 730 days in some situations). So, normally, if you want to keep your logs more than 90 days, you send them to a storage.

A ref among others :

<https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log#send-to-azure-storage>

upvoted 2 times

🗨️ 👤 **Snownoodles** 2 years, 8 months ago

"while log analytics workspace only keep them 90 days" - this is not correct.

Log analytics workspace can keep logs up to 730 days.

"90" is free days that you can keep logs with.

LAW is not for archiving, is for interactive query.

So the correct answer is storage1.

upvoted 1 times

🗨️ 👤 **Vipsao** 4 years, 3 months ago

The answer is correct. This is Storage 1

upvoted 6 times

You plan to create an Azure Cosmos DB account that uses the SQL API. The account will contain data added by a web application. The web application will send data daily.

You need to recommend a notification solution that meets the following requirements:

- ⇒ Sends email notifications when data is received from the web application
- ⇒ Minimizes compute cost

What should you include in the recommendation?

- A. Deploy an Azure logic app that has a SendGrid connector configured to use an Azure Cosmos DB action.
- B. Deploy a function app that is configured to use the Consumption plan and an Azure Event Hubs binding.
- C. Deploy a function app that is configured to use the Consumption plan and a SendGrid binding.
- D. Deploy an Azure logic app that has a webhook configured to use a SendGrid action.

#### Suggested Answer: C

You can send email by using SendGrid bindings in Azure Functions. Azure Functions supports an output binding for SendGrid.

Note: When you're using the Consumption plan, instances of the Azure Functions host are dynamically added and removed based on the number of incoming events.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-functions/functions-bindings-sendgrid> <https://docs.microsoft.com/en-us/azure/azure-functions/functions-scale#consumption-plan>

Community vote distribution

C (100%)

🗳️ 👤 **kwaazaar** Highly Voted 4 years, 3 months ago

Function apps support triggers for CosmosDB, logic apps do not.

<https://docs.microsoft.com/nl-nl/azure/azure-functions/functions-bindings-cosmosdb-v2-trigger?tabs=csharp>

CosmosDB actions makes no sense: we don't want to modify the CosmosDB data.

upvoted 31 times

🗳️ 👤 **BrettusMaximus** 3 years, 11 months ago

Correct answer

Azure functions can be directly tied to the change feed of Cosmos DB.

<https://docs.microsoft.com/en-us/azure/cosmos-db/change-feed-functions>

upvoted 7 times

🗳️ 👤 **BrettusMaximus** 3 years, 11 months ago

Note: Send Grid ==> send Email

upvoted 9 times

🗳️ 👤 **nkv** Highly Voted 3 years, 9 months ago

came in exam on 20-sep-21, I passed, i choose C

upvoted 9 times

🗳️ 👤 **rxlicon** Most Recent 1 year, 10 months ago

You can send email by using SendGrid bindings in Azure Functions

Azure functions can be directly tied to the change feed of Cosmos DB

upvoted 1 times

🗳️ 👤 **Dawn7** 3 years, 3 months ago

Selected Answer: C

I would choose C here

upvoted 1 times

🗳️ 👤 **FinMessner** 3 years, 5 months ago

Azure Functions consumption plan is billed based on per-second resource consumption and executions. Consumption plan pricing includes a monthly free grant of 1 million requests and 400,000 GB-s of resource consumption per month per subscription in pay-as-you-go pricing across all

function apps in that subscription. Azure Functions Premium plan provides enhanced performance and is billed on a per second basis based on the number of vCPU-s and GB-s your Premium Functions consume. Customers can also run Functions within their App Service plan at regular App Service plan rates.

upvoted 1 times

🗳️ 👤 **Eitant** 3 years, 6 months ago

**Selected Answer: C**

Correct answer

upvoted 2 times

🗳️ 👤 **Dpejic** 3 years, 6 months ago

Appere on exam 23-dec-2021

upvoted 3 times

🗳️ 👤 **syu31svc** 3 years, 8 months ago

A and D are out since "minimize compute cost"

<https://docs.microsoft.com/en-us/azure/azure-functions/functions-bindings-cosmosdb-v2-trigger?tabs=csharp>

<https://docs.microsoft.com/en-us/azure/azure-functions/functions-bindings-sendgrid?tabs=csharp>

<https://docs.sendgrid.com/ui/sending-email/how-to-send-email-with-marketing-campaigns>

C is the answer

upvoted 4 times

🗳️ 👤 **dkltruong88** 3 years, 9 months ago

Was in exam today 1-10-2021. I passed with score 896. I chose C

upvoted 6 times

🗳️ 👤 **pentium75** 3 years, 10 months ago

This seems to be the only question in both AZ-303 and AZ-304 that includes a 3rd party solution (SendGrid) in the suggestion solution.

upvoted 4 times

🗳️ 👤 **murongqing** 3 years, 10 months ago

correct:

consumption plan: (min computer cost) Scale automatically and only pay for compute resources when your functions are running

upvoted 1 times

🗳️ 👤 **Bijith** 3 years, 10 months ago

D is correct.

To save cost LogicApp and work on top of webhook trigger

upvoted 1 times

🗳️ 👤 **ashish0711** 3 years, 11 months ago

Answer seems D.

We have to save compute costs, Use Azure Logic Apps instead of Azure Functions. As the web application will send a notification via a web trigger to the Azure Logic App, then use an Azure Logic App that has a webhook trigger and the SendGrid action can be used to send a notification.

upvoted 3 times

🗳️ 👤 **dennnnnnnnnn** 3 years, 11 months ago

Both C & D can satisfy the requirement. However, C did mentioned "Consumption plan" but not Logic App. So C would be more precise in low costing aspect

upvoted 4 times

🗳️ 👤 **GetulioJr** 4 years ago

Answer seems right. Function supports trigger with CosmosDB with SQL API is used and the text mentions it. There is also a text explaining how to do it below. That with sendgrid to send the email is all that is needed. So I will go with answer C

<https://docs.microsoft.com/en-us/azure/azure-functions/functions-create-cosmos-db-triggered-function>

upvoted 5 times

🗳️ 👤 **jaiarya** 4 years ago

Correct Answer is D.

Here since we need to save the compute cost so Logic App needs to be used instead of Function App.

2. Since the application are sending via webtrigger so SendGrid Action would be required.

upvoted 1 times

🗨️ 👤 **VincentZhang** 3 years, 9 months ago

pls explain on how a logic app to trigger a function of SendGrid?

upvoted 1 times

🗨️ 👤 **jmay** 3 years, 5 months ago

<https://docs.microsoft.com/en-us/azure/connectors/connectors-create-api-sendgrid>

upvoted 1 times

🗨️ 👤 **LT** 4 years, 1 month ago

Correct Answer - C. Deploy a function app that is configured to use the Consumption plan and a SendGrid binding.

<https://docs.microsoft.com/en-us/azure/azure-functions/functions-bindings-sendgrid?tabs=csharp#example>

upvoted 3 times

🗨️ 👤 **VivekSood** 4 years, 1 month ago

So what is the right answer?

upvoted 2 times

**HOTSPOT -**

You on-premises network contains a file server named Server1 that stores 500 GB of data.

You need to use Azure Data Factory to copy the data from Server1 to Azure Storage.

You add a new data factory.

What should you do next? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

From Server1:

- ☐ Install an Azure File Sync agent.
- ☐ Install a self-hosted integration runtime.
- ☐ Install the File Server Resource Manager role service.

From the data factory:

- ☐ Create a pipeline.
- ☐ Create an import/export job.
- ☐ Provision an Azure-SQL Server Integration Services (SSIS) integration runtime.

**Answer Area**

From Server1:

- ☐ Install an Azure File Sync agent.
- ☒ Install a self-hosted integration runtime.
- ☐ Install the File Server Resource Manager role service.

Suggested Answer:

From the data factory:

- ☒ Create a pipeline.
- ☐ Create an import/export job.
- ☐ Provision an Azure-SQL Server Integration Services (SSIS) integration runtime.

Box 1: Install a self-hosted integration runtime

The Integration Runtime is a customer-managed data integration infrastructure used by Azure Data Factory to provide data integration capabilities across different network environments.

Box 2: Create a pipeline -

With ADF, existing data processing services can be composed into data pipelines that are highly available and managed in the cloud. These data pipelines can be scheduled to ingest, prepare, transform, analyze, and publish data, and ADF manages and orchestrates the complex data and processing dependencies

Reference:

<https://docs.microsoft.com/en-us/azure/machine-learning/team-data-science-process/move-sql-azure-adf>

🗨️ **verbatim86** Highly Voted 4 years, 3 months ago

correct / <https://docs.microsoft.com/pl-pl/azure/data-factory/tutorial-hybrid-copy-data-tool>  
upvoted 30 times

🗨️ **BenBen** Highly Voted 4 years, 3 months ago

I still don't get why we should use ADF to move files to Azure haha  
upvoted 14 times

🗨️ **sunmonkey** 4 years, 2 months ago

Most likely to transform the data somehow during the process.  
upvoted 4 times

🗨️ **demonite** 4 years, 1 month ago

Yep ETL  
upvoted 1 times

🗨️ **pentium75** 3 years, 10 months ago

So that you can later save 4993.14 USD per month by replacing ADF with AZCOPY, see topic 3 question 3 ;)

<https://www.examttopics.com/discussions/microsoft/view/38657-exam-az-304-topic-3-question-3-discussion/>  
upvoted 80 times

🗨️ **anthonyphuc** 3 years, 6 months ago

the question just comes for getting the knowledge :)))  
upvoted 1 times

🗨️ **tteesstt** 3 years, 9 months ago

Lmao, good one!  
upvoted 3 times

🗨️ **wwwwmm** 2 years, 6 months ago

Right on, and it's a huge strategic cost-saving item in your department in future!  
upvoted 1 times

🗨️ **Harald105** Most Recent 3 years, 6 months ago

Nicely played, pentium75 :)  
upvoted 5 times

🗨️ **syu31svc** 3 years, 9 months ago

<https://docs.microsoft.com/en-us/azure/data-factory/create-self-hosted-integration-runtime?tabs=data-factory>

"A self-hosted integration runtime can run copy activities between a cloud data store and a data store in a private network"

<https://docs.microsoft.com/en-us/azure/data-factory/introduction>

"With Data Factory, you can use the Copy Activity in a data pipeline to move data from both on-premises and cloud source data stores to a centralization data store in the cloud for further analysis"

Answer is correct  
upvoted 4 times

🗨️ **pentium75** 3 years, 10 months ago

In second box, there is an option "Provision Azure-SQL Server SSIS runtime," which is obviously wrong as we need a self-hosted (not an Azure-SQL) runtime. But still, don't we have to provision the self-hosted SSIS runtime in Azure Data Factory before we deploy it to the on-premise server?  
upvoted 2 times

🗨️ **mahwish** 4 years ago

2nd is create an import export job  
upvoted 2 times

🗨️ **arytech** 4 years ago

It seems to be correct for me, as there is no "copy data tool" option in the data factory bombo box, the most approximated one is "create a pipeline" as described in the following references (the last one hits the nail for me).

References:



<https://docs.microsoft.com/en-us/azure/data-factory/copy-activity-overview>

<https://docs.microsoft.com/en-us/azure/data-factory/quickstart-create-data-factory-copy-data-tool>

upvoted 3 times

  **SnakePlissken** 4 years ago

1. StorageV2

Only storage type with storage tiers. The Central Europe region is no Azure region. In that geographic region, only Germany West Central has storage accounts with storage tiers. By the way, France Central is not situated in Central Europe geographically.



2. ZRS

Protection against single datacenter failure.

[https://en.wikipedia.org/wiki/Central\\_Europe](https://en.wikipedia.org/wiki/Central_Europe)

<https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy#redundancy-in-the-primary-region>

upvoted 1 times

  **awalao** 3 years, 6 months ago



Hey watch where your comment. your comment should be in the next question. lmao

upvoted 3 times

  **nabylon** 4 years, 3 months ago

It should mention :data to be migrated is from a SQL Server database...

upvoted 2 times

  **lawry** 3 years, 9 months ago

nope, because it is not a SQL Server DB, then box2 select the first one;

if it is a SQL Server DB, the better way is to use the 3rd one for box2;

upvoted 1 times

  **prashantjoge** 4 years, 3 months ago

the link provided has no relation to the question asked... Not sure if this question makes sense?

upvoted 3 times

  **Mikie889** 4 years, 3 months ago

Correct...

upvoted 2 times

**HOTSPOT -**

You have an on-premises file server that stores 2 TB of data files.

You plan to move the data files to Azure Blob storage in the Central Europe region.

You need to recommend a storage account type to store the data files and a replication solution for the storage account. The solution must meet the following requirements:

- ⇒ Be available if a single Azure datacenter fails.
- ⇒ Support storage tiers.
- ⇒ Minimize cost.

What should you recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Account type:

	▼
Blob storage	
Storage (general purpose v1)	
StorageV2 (general purpose v2)	

Replication solution:

	▼
Geo-redundant storage (GRS)	
Zone-redundant storage (ZRS)	
Locally-redundant storage (LRS)	
Read-access geo-redundant storage (RA-GRS)	

**Answer Area**

Suggested Answer:

Account type:

	▼
Blob storage	
Storage (general purpose v1)	
StorageV2 (general purpose v2)	

Replication solution:

	▼
Geo-redundant storage (GRS)	
Zone-redundant storage (ZRS)	
Locally-redundant storage (LRS)	
Read-access geo-redundant storage (RA-GRS)	

Box 1: Blob storage -

Blob storage supports storage tiers

Note: Azure offers three storage tiers to store data in blob storage: Hot Access tier, Cool Access tier, and Archive tier. These tiers target data at different stages of its lifecycle and offer cost-effective storage options for different use cases.

Box 2: Zone-redundant storage (ZRS)

Data in an Azure Storage account is always replicated three times in the primary region. Azure Storage offers two options for how your data is replicated in the primary region:

- ⇒ Zone-redundant storage (ZRS) copies your data synchronously across three Azure availability zones in the primary region.
- ⇒ Locally redundant storage (LRS) copies your data synchronously three times within a single physical location in the primary region. LRS is the least expensive replication option, but is not recommended for applications requiring high availability.

Reference:

pmukund7 Highly Voted 4 years, 3 months ago

Answer is

Account Type: StorageV2

Replication solution: Zone-redundant storage (ZRS)

The blobstorage and StorageV1 doesn't support ZRS replication.

upvoted 141 times

Unofficial 4 years, 3 months ago

That is correct

upvoted 1 times

sallymaher 4 years, 3 months ago

Yes Correct blobstorage doesn't support ZRS

upvoted 4 times

prashantjoge 4 years, 3 months ago

also only v2 supports access tier (hot and cold)

upvoted 5 times

claudio82 4 years, 2 months ago

excelent argument, thank you for your contribution

upvoted 5 times

glam Highly Voted 4 years, 3 months ago

Account Type: StorageV2

Replication solution: Zone-redundant storage (ZRS)

upvoted 14 times

MantuKumarDeka Most Recent 2 years ago

AZ 305 3 June 2023

upvoted 1 times

crayonsin 2 years, 10 months ago

i am fine with V2, but second one should be GRS because of single data center fails. one region could have 2 or more DC, if only one fails, your data is still safe if it is GRS. considering min cost....

upvoted 2 times

AubinBakana 2 years, 10 months ago

I was pretty sure it's hate when they get something so simple wrong. Answer is StorageV2(GP V2) & ZRS

upvoted 1 times

JayBee65 3 years ago

To minimise cost use standard not premium.

GPv2 is recommended as a default by MS

ZRS is cheapest option that supports a data centre failure

upvoted 1 times

hertino 3 years, 2 months ago

In AZ-305 exam, 9 april 22

upvoted 5 times

plmsg 3 years, 3 months ago

answer is V2 & ZRS

upvoted 1 times

Kctaz 3 years, 4 months ago

Answer :

Storage V2 and ZRS.

ZRS is pretty obvious.

But why you should choose Storage V2 rather than Blob storage ? Because if you deploy a storage account and want only Blob, then you need to

select a premium storage. Premium Blobs are more expansive than the Blobs you have in your Storage V2. Question says : minimize the cost. So you can't choose Blob Storage (premium) or worse (legacy blob storage.....). You can't choose Storage V1 since they don't support access tiers.

upvoted 2 times

🗨️ 👤 **Bhupals** 3 years, 4 months ago

Supported storage account types

The following table shows which redundancy options are supported by each type of storage account. For information for storage account types, see Storage account overview.

#### SUPPORTED STORAGE ACCOUNT TYPES

LRS ZRS GRS/RA-GRS GZRS/RA-GZRS

General-purpose v21

General-purpose v1

Premium block blob1

Legacy blob

Premium file shares General-purpose v21

Premium block blobs1

Premium file shares General-purpose v21

General-purpose v1

Legacy blob General-purpose v21

upvoted 1 times

🗨️ 👤 **sujitwarrier11** 3 years, 5 months ago

I think storage V2 is the correct answer as I think that is what Microsoft is pushing us to use in the future. I heard the other storage types will be phased out eventually.

upvoted 1 times

🗨️ 👤 **massnonn** 3 years, 5 months ago

the blob storage support ZRS <https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy#supported-azure-storage-services>  
the General-purpose v1 not support ZRS

upvoted 1 times

🗨️ 👤 **[Removed]** 3 years, 6 months ago

Its should be

Box1: Storage V2 and

Bpx2: ZRS

upvoted 1 times

🗨️ 👤 **examineezer** 3 years, 6 months ago

"What should you recommend?"

I assume by "Blob" the option is actually Standard Blob storage (legacy), which should never be recommended. In any case, it doesnt support LRS.

Described as "legacy blob" in the table here:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy>

upvoted 1 times

🗨️ 👤 **Dpejic** 3 years, 6 months ago

Appere on exam 23-dec-2021

upvoted 2 times

🗨️ 👤 **VincentZhang** 3 years, 8 months ago

Hi Guys, look at the question itself: "You plan to move the data files to Azure Blob storage in the Central Europe region", it has highlighted that data will move to BLOB Storage, so the question here is narrowed to that is the Storage V2 under BLOB Storage?

upvoted 1 times

🗨️ 👤 **azuremaddy** 3 years, 8 months ago

This question was in AZ-303, and the Correct Answer is - StorageV2 & ZRS

upvoted 6 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You are designing an Azure solution for a company that has four departments. Each department will deploy several Azure app services and Azure SQL databases.

You need to recommend a solution to report the costs for each department to deploy the app services and the databases. The solution must provide a consolidated view for cost reporting that displays cost broken down by department.

Solution: Create a resource group for each resource type. Assign tags to each resource group.

Does this meet the goal?

A. Yes

B. No

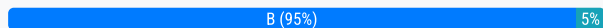
#### Suggested Answer: A

Tags enable you to retrieve related resources from different resource groups. This approach is helpful when you need to organize resources for billing or management.

Reference:

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

Community vote distribution



**sunmonkey** Highly Voted 4 years, 2 months ago

No since each department will deploy several app services and DBs. If we group like resources in resource groups we will not be able to get a break down by department.

upvoted 53 times

**gssd4scoder** 4 years ago

Agree hundred percent with you

upvoted 2 times

**kubinho** 4 years ago

why not ? You are not able to filter by tags? If you have 4 dept a 1 resources group for lets say storage account and you tag every SA with name of department, then you can filter tags and see departments resources and see price.. I would say answer is YES in here

upvoted 3 times

**Amit3** 4 years ago

The questions say tag resource group and not resources, so how can you get which resource belongs to which department?.

upvoted 13 times

**VincentZhang** 3 years, 8 months ago

Answer is almost correct, just tag on the resources instead of resource group as what said in explanation.

upvoted 2 times

**AlexD332** 4 years ago

there are no words they will use resources from other department so we can assume they will use only their own resources - the answer is YES

upvoted 3 times

**BoxGhost** 3 years, 10 months ago

Look at the wording. It says create a resource group for each resource type. It should be create a resource group for each department.

"Create a resource group for each resource type. Assign tags to each resource group."

It also states each department will deploy web apps and SQL. Therefore the solution doesn't work.

upvoted 14 times

**ZetaZeti** Highly Voted 4 years ago

No.

You have to assign a tag like Department1 or Department2 or Department3 or Department4 on each resource so you can filter for instance all

resources relative to the first department by selecting the tag Department1.

The option is wrong because if we put let me say all the storage accounts in RG1 and we assign a tag to it as the option says for instance StAcs we don't have any possibility to filter the storage accounts belonging to the first department.

upvoted 13 times

  **ZetaZeti** 4 years ago

Of course another option would be to create 4 RGs one for each department and to assign a tag to each one like Department1 or Department2 or Department3 or Department4. Then we put inside the RG tagged Department1 all the resources belonging to the first department and so on. In this case though we do not have the RGs divided by resource type as the option requires.

upvoted 1 times

  **GaneshPP** Most Recent 2 years, 8 months ago

Ans is NO. RG will have resources from all depts, so no use of its tag.

upvoted 1 times

  **AubinBakana** 2 years, 10 months ago

Selected Answer: A

this is so unfair. By assigning tags to the RG, you can still get to your resource after you assign a policy to inherit the tags from the RG. So technically, at this stage, how it is presented, this answer is not entirely false.



I would have to go with Yes on this one.

upvoted 1 times

  **jellybiscuit** 2 years, 9 months ago

They key point here is that they created the RGs for each resource type... not for each department.

upvoted 1 times

  **OCHT** 3 years, 1 month ago

Link is correct. However , it's false to the question statements.

upvoted 2 times

  **AubinBakana** 2 years, 10 months ago

Yes, the question is badly stated.

upvoted 1 times

  **g6singh** 3 years, 1 month ago

Given Ans: Create a resource group for each resource type. Assign tags to each resource group.

Correct Ans : NO

It should be 1 or 4 resource groups and each resource will have tag as per department, i.e. Department#1, Department2 3... 4..

Also there is no mention that different department will use each others resources, even if they use, Cost would still be on resource owner.

upvoted 1 times

  **johnny19873** 3 years, 3 months ago

Selected Answer: B

It's B

upvoted 1 times

  **ERROR505** 3 years, 3 months ago

Selected Answer: B

It is definitely NO as tagging the resources is not available for the costs:

Most Azure resources support tagging. However, some tags aren't available in Cost Management and billing. Additionally, resource group tags aren't supported.

<https://docs.microsoft.com/en-us/azure/cost-management-billing/costs/quick-acm-cost-analysis#group-costs>

upvoted 2 times

  **plmmsg** 3 years, 3 months ago

Selected Answer: B

ANSWER is NO

upvoted 2 times

  **Rambo3** 3 years, 4 months ago

You can create 4 RGs one for each department and to assign a tag to each one like Department1 or Department2 or Department3 or Department4.

Then we put inside the RG tagged Department1 all the resources belonging to the first department and so on. Tags are inheritable, but you can use a policy to make sure a tag is copied from a RG to its resources.

upvoted 1 times

🗲️ 👤 **Tote** 3 years, 4 months ago

**Selected Answer: B**

No, tags are not inhereted from Resource Groups to resources

upvoted 3 times

🗲️ 👤 **Tote** 3 years, 4 months ago

**Selected Answer: B**

No, tags are not inhereted from Resource Group to the resources.

upvoted 1 times

🗲️ 👤 **[Removed]** 3 years, 4 months ago

**Selected Answer: B**

This is certainly no as once you club all the resources of different department in one RG tagging the RG won't be of any help while getting cost for each dept

upvoted 1 times

🗲️ 👤 **siddjay** 3 years, 5 months ago

It Says "Create a resource group for each resource type" hence we can tag individual RGs i.e. each SQL DB will be in its own RG. Hence Answer is CORRECT.

upvoted 1 times

🗲️ 👤 **ScubaDiver123456** 3 years, 6 months ago

**Selected Answer: B**

either tag individual resources or place resources owned by a department into their own tagged resource groups

upvoted 3 times

🗲️ 👤 **jc0611** 3 years, 6 months ago

**Selected Answer: B**

should tag individual resources rather than rg

upvoted 4 times

🗲️ 👤 **jadepe** 3 years, 6 months ago

**Selected Answer: B**

Answer: no. With the proposed solution, the tags will allow you to distinguish by resource type, not by department, which is what is needed

upvoted 3 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You are designing an Azure solution for a company that has four departments. Each department will deploy several Azure app services and Azure SQL databases.

You need to recommend a solution to report the costs for each department to deploy the app services and the databases. The solution must provide a consolidated view for cost reporting that displays cost broken down by department.

Solution: Create a new subscription for each department.

Does this meet the goal?

A. Yes

B. No

**Suggested Answer: B**

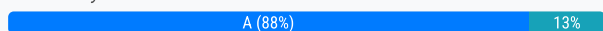
Instead, create a resources group for each resource type. Assign tags to each resource

Note: Tags enable you to retrieve related resources from different resource groups. This approach is helpful when you need to organize resources for billing or management.

Reference:

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

Community vote distribution



**timHAG** Highly Voted 4 years, 2 months ago

it should be yes, with sub. for each dept. we can get the spending for each spending. RG for resource group will not fix it, RG for each dept. will.  
upvoted 39 times

**J4U** 3 years, 9 months ago

Yes. We can create a consolidated report for all subscriptions under MG scope. Filters allows to see breakdown of resources under each subscription.  
upvoted 2 times

**J4U** 3 years, 9 months ago

<https://docs.microsoft.com/en-us/azure/cost-management-billing/costs/group-filter>  
upvoted 1 times

**claudio82** Highly Voted 4 years, 1 month ago

Answer is correct. You need a CONSOLIDATED report, of all departments

Dep 1 50

Dep 2 35

Dep 3 80

Dep 4 55

By subscription yo only get

Subcription 1 50

upvoted 18 times

**johnnsmith** 4 years, 1 month ago

You can use management group as the scope and use "grouped by subscription". So the answer is yes.  
upvoted 16 times

**demonite** 4 years, 1 month ago

agreed should be yes. It's under the same tenant.  
upvoted 4 times

**bertybert15** 3 years, 3 months ago

You have a subscription for each department...therefor the subscription report will show the costs for that department only and a report from the MG level will consolidate all 4 Subs into 1 report



upvoted 1 times

🗨️ 👤 **RJ06** Most Recent 10 months, 1 week ago

I think it should be NO because having cost management at subscription level would include cost of other resources/resource groups created in that subscription. The aim is to report on the costs for each department to deploy the "app services and the databases".

upvoted 1 times

🗨️ 👤 **rxlicon** 1 year, 10 months ago

You have a subscription for each department...therefor the subscription report will show the costs for that department only and a report from the MG level will consolidate all 4 Subs into 1 report

upvoted 1 times

🗨️ 👤 **GaneshPP** 2 years, 8 months ago

The question says - "The solution must provide a consolidated view for cost reporting that displays cost broken down by department.", so ans is No

upvoted 1 times

🗨️ 👤 **f2002642** 2 years, 10 months ago

The correct answer as per the MS practice test is "NO".

upvoted 3 times

🗨️ 👤 **DChilds** 2 years, 10 months ago

Selected Answer: B

The goal is to break down cost in the entire subscription by department so separate subscriptions is not the answer. Correct answer is B.

upvoted 1 times

🗨️ 👤 **nidhogg** 2 years, 10 months ago

to break down cost in the entire SOLUTION by department. Subscriptions are not mentioned in the text.

'A' works well here.

upvoted 1 times

🗨️ 👤 **AubinBakana** 2 years, 10 months ago

This question could better formulated. Here also you can get your answer. You just have to consider admin effort.

Click each of the option can still lead you to the solution. I guess they want to emphasis on tag here?

upvoted 1 times

🗨️ 👤 **ajjihad1** 2 years, 10 months ago

Each subscripoin is one department. So generating a report based on the subscription will give us the spending of each department.

upvoted 1 times

🗨️ 👤 **cloudera** 3 years, 2 months ago

Selected Answer: A

Yes but not a good solution but should answer the question/

upvoted 1 times

🗨️ 👤 **cloudera** 3 years, 2 months ago

meant to say not a very bad solution. Another option is one subscription, RG for each department and tagging enforced for each resource.

upvoted 2 times

🗨️ 👤 **Eitant** 3 years, 6 months ago

Selected Answer: A

Should be YES

upvoted 6 times

🗨️ 👤 **DerekKey** 3 years, 7 months ago

Should be YES:

Cost managment / Cost analysis / Scope: Account / Group by: Subscription

upvoted 3 times

🗨️ 👤 **syu31svc** 3 years, 8 months ago

I would take No as the answer

"consolidated view for cost reporting" would mean it falls under a single subscription

upvoted 2 times

🗨️ 👤 **poplovic** 3 years, 9 months ago

Azure portal -> subscription -> cost management - > cost analysis.

So "yes"

upvoted 2 times

  **souvik123** 3 years, 9 months ago

YES : Subscription has a view of costs of resources used by department and convenient way.


upvoted 1 times

  **SnakePlissken** 4 years ago

Answer is Yes.

This solution is the most convenient, costs are split per department without any effort.

upvoted 3 times

  **kbnk** 4 years, 1 month ago

should be A-yes. That gives us consolidated and even detailed view on resources per dept without any effort

upvoted 3 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You are designing an Azure solution for a company that has four departments. Each department will deploy several Azure app services and Azure SQL databases.

You need to recommend a solution to report the costs for each department to deploy the app services and the databases. The solution must provide a consolidated view for cost reporting that displays cost broken down by department.

Solution: Place all resources in the same resource group. Assign tags to each resource.

Does the solution meet the goal?

A. Yes

B. No

**Suggested Answer: B**

Instead, create a resources group for each resource type. Assign tags to each resource



Note: Tags enable you to retrieve related resources from different resource groups. This approach is helpful when you need to organize resources for billing or management.

Reference:

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

Community vote distribution

A (100%)

  **sallymaher** Highly Voted 4 years, 3 months ago

Answer is yes , tag will be the department and value the department name  
upvoted 78 times

  **claudio82** 4 years, 2 months ago

Works, but is not recommended has single resource group for all resources, its necessary organize resource according a clasification.  
upvoted 6 times

  **mehdimed** 4 years ago


<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources?tabs=json#tags-and-billing> the documentation says it's fine  
upvoted 5 times

  **kwaazaar** 4 years, 3 months ago

Consolidated view is required, so costs per departments in one view I assume. Changing filter all the time is not suffice.  
upvoted 1 times

  **kwaazaar** 4 years, 3 months ago

Correction: you can set the 'Group By' to a specific tag, so would work indeed.  
upvoted 4 times

  **malyaban** Highly Voted 4 years, 3 months ago

Again please see the explanation - same question was in AZ-303, here it is actually correct in saying it is not recommended to put all resources in the same RG, but it is a YES as it will still work. The perfect answer is in the explanation - Instead, create a resources group for each resource type. Assign tags to each \*\*\*resource\*\*\*  
upvoted 17 times

  **tin1624** Most Recent 2 years, 5 months ago

nothing is mentioned about tags on question.. quite tricky one to choose  
upvoted 1 times

  **AubinBakana** 2 years, 10 months ago

This would work. But considering the state of the question, we don't have enough information to tell if this is bad practice. This question was poorly formulated.  
upvoted 1 times

🗳️ 👤 **cloudera** 3 years, 2 months ago

**Selected Answer: A**

Yes this should solve the problem.

upvoted 1 times

🗳️ 👤 **jr\_luciano** 3 years, 4 months ago

**Selected Answer: A**

Answer is Yes.

upvoted 2 times

🗳️ 👤 **massnonn** 3 years, 5 months ago

this is answer for the MOC:

Create an individual resource group for each department and place the separate resources for each department in their individual groups.

Cost Management can track by Resource Group. Allows you to report by resource group.

upvoted 2 times

🗳️ 👤 **Eitant** 3 years, 6 months ago

**Selected Answer: A**

Answer is Yes.

upvoted 3 times

🗳️ 👤 **[Removed]** 3 years, 6 months ago

**Selected Answer: A**

Answer is Yes. Indeed not a good solution but works

upvoted 3 times

🗳️ 👤 **syu31svc** 3 years, 8 months ago

This will work so Yes

upvoted 1 times

🗳️ 👤 **Elmessery** 3 years, 9 months ago

"recommend a solution to report the costs for each department to deploy the app services and the databases" it will work but your recommendation should be accurate. I think "No" is the right

upvoted 1 times

🗳️ 👤 **souvik123** 3 years, 9 months ago

YES : Resource Tags are used for the reason to classify resources in common RG

upvoted 1 times

🗳️ 👤 **Matrics** 4 years ago

The answer should be yes because you can create tags for each department for the resources. However, not a good practice to put everything under one resource group.

upvoted 3 times

🗳️ 👤 **MaheshS** 4 years ago

Answer should be Yes. Though this is not best the practice but it will work since you easily differentiate the cost of each department in the bill by segregating the tags.

upvoted 1 times

🗳️ 👤 **GetulioJr** 4 years ago

Answer should be YES.

It will definitely works as expected !

upvoted 2 times

🗳️ 👤 **erickim007** 4 years ago

not a best practice but it would work.

upvoted 3 times

🗳️ 👤 **sujeetkb2021** 4 years ago

answer is Yes. The question provides only 2 resource types web app and SQL database. And the cost of each department can be calculated based on the tags applied on each resource

upvoted 1 times

## HOTSPOT -

You have an Azure SQL database named DB1.

You need to recommend a data security solution for DB1. The solution must meet the following requirements:

- ⇒ When helpdesk supervisors query DB1, they must see the full number of each credit card.
- ⇒ When helpdesk operators query DB1, they must see only the last four digits of each credit card number.
- ⇒ A column named Credit Rating must never appear in plain text within the database system, and only client applications must be able to decrypt the Credit Rating column.

What should you include in the recommendation? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Helpdesk requirements:

Always Encrypted
Azure Advanced Threat Protection (ATP)
Dynamic data masking
Transparent Data Encryption (TDE)

Credit Rating requirement:

Always Encrypted
Azure Advanced Threat Protection (ATP)
Dynamic data masking
Transparent Data Encryption (TDE)

**Answer Area**

Helpdesk requirements:

Always Encrypted
Azure Advanced Threat Protection (ATP)
Dynamic data masking
Transparent Data Encryption (TDE)

Suggested Answer:

Credit Rating requirement:

Always Encrypted
Azure Advanced Threat Protection (ATP)
Dynamic data masking
Transparent Data Encryption (TDE)

Box 1: Dynamic data masking -

Dynamic data masking helps prevent unauthorized access to sensitive data by enabling customers to designate how much of the sensitive data to reveal with minimal impact on the application layer. It's a policy-based security feature that hides the sensitive data in the result set of a query over designated database fields, while the data in the database is not changed.

Box 2: Always encrypted -

Data stored in the database is protected even if the entire machine is compromised, for example by malware. Always Encrypted leverages client-side encryption: a database driver inside an application transparently encrypts data, before sending the data to the database. Similarly, the driver decrypts encrypted data retrieved in query results.

Reference:

<https://azure.microsoft.com/en-us/blog/transparent-data-encryption-or-always-encrypted/>

🗨️ 👤 **MKAZ** Highly Voted 🏆 4 years, 3 months ago

Correct!!

upvoted 32 times

🗨️ 👤 **Amit3** Highly Voted 🏆 4 years ago

For Second Answer 'Always Encrypt' explanations is here

<https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine?view=sql-server-ver15>

upvoted 8 times

🗨️ 👤 **Dpejic** Most Recent 🔒 3 years, 6 months ago

Appere on exam 23-dec-2021

upvoted 3 times

🗨️ 👤 **syu31svc** 3 years, 9 months ago

"see only the last four digits" -> This implies data masking

"must never appear in plain text" and "only client applications must be able to decrypt" -> Always Encrypted

Answer is correct

upvoted 6 times

🗨️ 👤 **AlexD332** 4 years ago

Correct

upvoted 2 times

🗨️ 👤 **PandaTuga** 4 years, 1 month ago

Correct. dynamic data masking explained here:

<https://docs.microsoft.com/en-us/sql/relational-databases/security/dynamic-data-masking?view=sql-server-ver15>

upvoted 2 times

🗨️ 👤 **dadageer** 4 years, 2 months ago

Answers are correct!

upvoted 2 times

🗨️ 👤 **Vipsao** 4 years, 3 months ago

The answer is correct

upvoted 3 times

You are designing a data protection strategy for Azure virtual machines. All the virtual machines use managed disks.

You need to recommend a solution that meets the following requirements:

- ⇒ The use of encryption keys is audited.
- ⇒ All the data is encrypted at rest always.
- ⇒ You manage the encryption keys, not Microsoft.

What should you include in the recommendation?

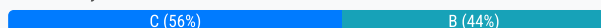
- A. client-side encryption
- B. Azure Storage Service Encryption
- C. Azure Disk Encryption
- D. Encrypting File System (EFS)

**Suggested Answer: C**

Reference:

<https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-overview>

Community vote distribution



🗨️ **SriRamOne** Highly Voted 4 years, 1 month ago

Since it says "All of the Data", the answer is C.

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-faq#how-is-azure-disk-encryption-different-from-storage-server-side-encryption-with-customer-managed-key-and-when-should-i-use-each-solution>

upvoted 20 times

🗨️ **addam23** 3 years, 10 months ago

This link says us:

"- If your requirements include encrypting all of the above and end-to-end encryption, use Azure Disk Encryption.

-If your requirements include encrypting only data at rest with customer-managed key, then use Server-side encryption with customer-managed keys. You cannot encrypt a disk with both Azure Disk Encryption and Storage server-side encryption with customer managed keys"

So the answer is B

upvoted 10 times

🗨️ **rdemontis** 3 years, 6 months ago

Absolutely agree with you.

"Azure Storage encryption automatically encrypts your data stored on Azure managed disks (OS and data disks) at rest by default when persisting it to the cloud"

"Full control of your keys

You must grant access to managed disks in your Key Vault to use your keys for encrypting and decrypting the DEK. This allows you full control of your data and keys. You can disable your keys or revoke access to managed disks at any time. You can also audit the encryption key usage with Azure Key Vault monitoring to ensure that only managed disks or other trusted Azure services are accessing your keys."

<https://docs.microsoft.com/en-us/azure/virtual-machines/disk-encryption>

<https://docs.microsoft.com/en-us/azure/virtual-machines/disk-encryption-overview>

upvoted 2 times

🗨️ **rxlicon** Most Recent 1 year, 10 months ago

Since it says "All of the Data"

Azure Disk Encryption provides end-to-end encryption for the OS disk, data disks, and the temporary disk with a customer-managed key.

If your requirements include encrypting all of the above and end-to-end encryption, use Azure Disk Encryption.

if your requirements include encrypting only data at rest with customer-managed key, then use Server-side encryption with customer-managed keys.

You can't encrypt a disk with both Azure Disk Encryption and Storage server-side encryption with customer managed keys.

upvoted 1 times

🗳️ 👤 **Jeanphi72** 3 years, 2 months ago

**Selected Answer: B**

Here: <https://docs.microsoft.com/en-us/azure/virtual-machines/disk-encryption#restrictions-1>

Supports ephemeral OS disks but only with platform-managed keys.

However I find it crazy that so many answers are unclear ... Maybe the documentation of Azure is not clear enough

upvoted 1 times

🗳️ 👤 **Jeanphi72** 3 years, 2 months ago

Sorry C, <https://docs.microsoft.com/en-us/azure/virtual-machines/disk-encryption#server-side-encryption-versus-azure-disk-encryption>

upvoted 1 times

🗳️ 👤 **arun** 3 years, 3 months ago

**Selected Answer: B**

please refer below links and explanation, it has answers for all given requirements.

<https://docs.microsoft.com/en-us/azure/virtual-machines/disk-encryption#full-control-of-your-keys>

- You can audit the encryption key usage with Azure Key Vault monitoring to ensure that only managed disks or other trusted Azure services are accessing your keys

<https://docs.microsoft.com/en-us/azure/virtual-machines/disk-encryption#customer-managed-keys>

- You can choose to manage encryption at the level of each managed disk, with your own custom keys

<https://docs.microsoft.com/en-us/azure/virtual-machines/disk-encryption>

- Most Azure managed disks are encrypted with Azure Storage encryption, which uses server-side encryption (SSE) to protect your data and to help you meet your organizational security and compliance commitments

upvoted 1 times

🗳️ 👤 **reachmymind** 3 years, 4 months ago

**Selected Answer: C**

the key here is not whether SSE or ADE can encrypt or do it using CMK, it is about "The use of encryption keys is audited", with SSE+CMK audit is "Unhealthy, not applicable if exempt" and with ADE it is "Healthy" ...

upvoted 2 times

🗳️ 👤 **jr\_luciano** 3 years, 4 months ago

**Selected Answer: C**

Answer is C.

upvoted 1 times

🗳️ 👤 **Whitesec** 3 years, 5 months ago

Azure storage Server-Side Encryption can be answer but the options say 'Azure Storage Services Encryption' and that is different.

Azure Storage Service Encryption

Data at rest in Azure Blob storage and Azure file shares can be encrypted in both server-side and client-side scenarios.

Azure Storage Service Encryption (SSE) can automatically encrypt data before it is stored, and it automatically decrypts the data when you retrieve it.

The process is completely transparent to users. Storage Service Encryption uses 256-bit Advanced Encryption Standard (AES) encryption, which is one of the strongest block ciphers available. AES handles encryption, decryption, and key management transparently. Please see the link below

<https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-overview>

upvoted 4 times

🗳️ 👤 **sprabhuraj** 3 years, 5 months ago

**Selected Answer: C**

The link is self-explanatory

upvoted 1 times

🗳️ 👤 **bacug** 3 years, 5 months ago

**Selected Answer: B**

<https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption?toc=/azure/storage/blobs/toc.json>

upvoted 1 times

🗳️ 👤 **STH** 3 years, 5 months ago

**Selected Answer: C**



if you follow the link and look "Encryption at Rest" section you will see the following :

"Any customer using Azure Infrastructure as a Service (IaaS) features can achieve encryption at rest for their IaaS VMs and disks through Azure Disk Encryption"

<https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-atrest#azure-disk-encryption>

upvoted 1 times

  **examineezer** 3 years, 6 months ago

I'd go for C

<https://docs.microsoft.com/en-us/azure/virtual-machines/disk-encryption-overview#comparison>

upvoted 2 times

  **yyuryyucicuryyforme** 3 years, 5 months ago

I agree, Azure Disk Encryption with VolumeType = All to encrypt the temporary disk - as Defender for Cloud can audit encryption state health for Azure Disk Encryption

The other way to encrypt the temporary disk is using server-side encryption with encryption at host but Defender for Cloud cannot audit disk encryption health state for encryption at host, according to the comparison table linked to.

upvoted 1 times

  **agente232** 3 years, 6 months ago

**Selected Answer: B**

read the link it is self explanatory

upvoted 1 times

  **student22** 3 years, 8 months ago

C. Azure Disk Encryption

---

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-faq#how-is-azure-disk-encryption-different-from-storage-server-side-encryption-with-customer-managed-key-and-when-should-i-use-each-solution->

upvoted 3 times

  **ShehuUsman** 3 years, 8 months ago

I will go for B, because question says "encryption at rest"

Note: ASSE is majorly for encryption at rest.

upvoted 1 times

  **syu31svc** 3 years, 8 months ago

<https://docs.microsoft.com/en-us/azure/virtual-machines/disk-encryption#full-control-of-your-keys>

C is correct

upvoted 2 times

  **sjai** 3 years, 9 months ago

I think B

Storage server-side encryption encrypts Azure managed disks in Azure Storage. Managed disks are encrypted by default with Server-side encryption with a platform-managed key (as of June 10, 2017). You can manage encryption of managed disks with your own keys by specifying a customer-managed key.

upvoted 1 times

  **leo\_az300** 3 years, 9 months ago

Answer is correct

Both Azure Disk Encrypt and Azure Server Side Encryption(Customer Managed Key) can meet all 3 requirements. For given answers, C is correct

upvoted 2 times

You have an on-premises application named App1 that uses an Oracle database.

You plan to use Azure Databricks to transform and load data from App1 to an Azure Synapse Analytics instance.

You need to ensure that the App1 data is available to Databricks.

Which two Azure services should you include in the solution? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Azure Data Box Gateway
- B. Azure Data Lake Storage
- C. Azure Import/Export service
- D. Azure Data Factory
- E. Azure Data Box Edge

**Suggested Answer:** BD

Automate data movement using Azure Data Factory, then load data into Azure Data Lake Storage, transform and clean it using Azure Databricks, and make it available for analytics using Azure Synapse Analytics. Modernize your data warehouse in the cloud for unmatched levels of

Note: Integrate data silos with Azure Data Factory, a service built for all data integration needs and skill levels. Easily construct ETL and ELT processes code-free within the intuitive visual environment, or write your own code. Visually integrate data sources using more than 90+ natively built and maintenance-free connectors at no added cost. Focus on your data and the serverless integration service does the rest.

Reference:

<https://azure.microsoft.com/en-us/services/databricks/#capabilities> <https://azure.microsoft.com/en-us/services/data-factory/>

Community vote distribution

BD (100%)

 **howdee** Highly Voted 4 years, 1 month ago

Correct answer. Azure Data factory with Self Hosted Integration Runtime (installed on premise) can move the data to data lake storage  
upvoted 18 times

 **gssd4scoder** 3 years, 11 months ago

why to ADLS? why not directly to Synapse?  
upvoted 1 times

 **STH** 3 years, 5 months ago

Yes, we could even ask "why ADF ?" :

OK Data Factory is made for ETL and Data Lake for storage, but...

What is the link with Databricks and Synapse as mentioned in the question ??


It is said that we want to perform the ETL job with Databricks and to store data into Synapse, so why would we use two more resources when Databrick can directly connect to Oracle and to Synapse ?

It is just a matter of what script we use

It works, but ADLS is useless, and if we use ADF we should not use Databricks, and vice versa


Answer is correct but stupid

upvoted 2 times

 **[Removed]** Highly Voted 3 years, 6 months ago

Selected Answer: BD

Correct. App1 data -> ADF -> A Storage Lake -> Azure Databricks , Synapse Analytics  
upvoted 7 times

 **pabloartgal** Most Recent 2 years, 8 months ago

<https://learn.microsoft.com/en-us/azure/synapse-analytics/sql-data-warehouse/sql-data-warehouse-overview-what-is>

<https://azure.microsoft.com/en-in/solutions/architecture/modern-data-warehouse/>

<https://learn.microsoft.com/en-us/azure/architecture/solution-ideas/media/enterprise-data-warehouse.png>

Azure Databricks is placed after 2, as this grants the ability to provide on-click streamlined workflows to prepare and train data.



Azure Data Factory is used for data integration that allows you to create, schedule and orchestrate extract, transform and load (ELT) workloads.

For storing the data, you can use Azure Data Lake as this is a highly scalable and cost-effective data lake (storage) solution for big data analytics.  
upvoted 1 times

  **AubinBakana** 2 years, 10 months ago

Why this can be confusing. To create Azure Synapse analytics, you first must create an ADLS. So at this point, I am assuming that because we have already got an ADLS, there's got to be another option.

I guess the key here is to know that the other options are absolutely a no.  
upvoted 1 times

  **Dawn7** 3 years, 3 months ago



**Selected Answer: BD**

Correct  
upvoted 1 times

  **[Removed]** 3 years, 3 months ago



**Selected Answer: BD**

Correct answer  
upvoted 1 times

  **NDubey** 3 years, 4 months ago

Data Box Edge also provides a computing platform via IoT Edge, which lets you deploy Azure services and custom code and applications to the edge. This means that you can analyze, filter, or transform your data right at the edge as part of your workflow. Data Box Edge acts as a storage gateway, creating a link between your site and Azure storage. This makes moving data into and out of Azure storage as easy as working with a local network share.

Can this be Azure Data Box Edge & ADLS?  
upvoted 1 times

  **siddjay** 3 years, 5 months ago

Answer is CORRECT  
upvoted 1 times

  **Dpejic** 3 years, 6 months ago

Appere on exam 23-dec-2021  
upvoted 3 times



  **syu31svc** 3 years, 8 months ago

This is correct


Data Lake to store the data and Data Factory for the ETL process  
upvoted 4 times

  **Gautam1985** 3 years, 10 months ago



Correct  
upvoted 2 times

  **Anu2020** 3 years, 11 months ago

Azure Synapse uses Azure Data Lake Storage Gen2 as a data warehouse and a consistent data model that incorporates administration, monitoring and metadata management sections.  
upvoted 1 times

  **demonite** 4 years, 1 month ago

Correct answer  
upvoted 3 times

  **Krsto** 4 years, 1 month ago

Answer is correct  
upvoted 3 times

You have 100 devices that write performance data to Azure Blob storage.  
You plan to store and analyze the performance data in an Azure SQL database.  
You need to recommend a solution to move the performance data to the SQL database.  
What should you include in the recommendation?

- A. Azure Database Migration Service
- B. Azure Data Factory
- C. Azure Data Box
- D. Data Migration Assistant

**Suggested Answer: B**




















You can copy data from Azure Blob to Azure SQL Database using Azure Data Factory.



Reference:

<https://docs.microsoft.com/en-us/azure/data-factory/tutorial-copy-data-dot-net>

Community vote distribution

B (100%)

-   **ruslan\_bespalov\_netconomy** Highly Voted 4 years, 2 months ago
  - A. Azure Database Migration Service - migrates the database from on-prem to Azure
  - B. Azure Data Factory - the remaining correct answer
  - C. Azure Data Box - physically move the data, has no business here
  - D. Data Migration Assistant -- migrates the database from on-prem to Azure (helper)upvoted 90 times
-   **rdemontis** 3 years, 7 months ago  
thanks for the explanation  
upvoted 2 times
-   **Vipsao** Highly Voted 4 years, 3 months ago  
The answer is correct  
upvoted 6 times
-   **hertino** Most Recent 3 years, 2 months ago  
In AZ-305 exam, 9 april 22  
upvoted 2 times
-   **Dawn7** 3 years, 3 months ago  
Selected Answer: B  
Always Data Factory   
upvoted 5 times
-   **[Removed]** 3 years, 3 months ago  
Selected Answer: B  
Correct answer  
upvoted 1 times
-   **Dpejic** 3 years, 6 months ago  
On exam 24.12.2021  
upvoted 3 times
-   **Eitant** 3 years, 6 months ago  
Selected Answer: B  
Correct answer  
upvoted 1 times
-   **syu31svc** 3 years, 8 months ago  
This is B for sure  
upvoted 2 times

  **Gautam1985** 3 years, 10 months ago



correct

upvoted 2 times

  **gssd4scoder** 4 years ago

Seems correct

upvoted 4 times

  **us3r** 3 years, 4 months ago

seems legit

upvoted 1 times

## HOTSPOT -

You have a web application that uses a MongoDB database. You plan to migrate the web application to Azure. You must migrate to Cosmos DB while minimizing code and configuration changes.

You need to design the Cosmos DB configuration.

What should you recommend? To answer, select the appropriate values in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

### Answer Area

Option	Value
MongoDB compatibility	<div>▼</div> <div>Database</div> <div>API</div> <div>Collection</div> <div>Account</div>
API	<div>▼</div> <div>Cassandra API</div> <div>DocumentDB API</div> <div>Graph API</div> <div>MongoDB API</div> <div>Table API</div>

### Answer Area

Option	Value
MongoDB compatibility	<div>▼</div> <div>Database</div> <div>API</div> <div>Collection</div> <div>Account</div>
API	<div>▼</div> <div>Cassandra API</div> <div>DocumentDB API</div> <div>Graph API</div> <div>MongoDB API</div> <div>Table API</div>

Suggested Answer:

MongoDB compatibility: API -

API: MongoDB API -

Azure Cosmos DB comes with multiple APIs:

- ⇒ SQL API, a JSON document database service that supports SQL queries. This is compatible with the former Azure DocumentDB.
- ⇒ MongoDB API, compatible with existing Mongo DB libraries, drivers, tools and applications.
- ⇒ Cassandra API, compatible with existing Apache Cassandra libraries, drivers, tools, and applications.
- ⇒ Azure Table API, a key-value database service compatible with existing Azure Table Storage.
- ⇒ Gremlin (graph) API, a graph database service supporting Apache Tinkerpop's graph traversal language, Gremlin.

Reference:

<https://docs.microsoft.com/en-us/azure/cosmos-db/create-mongodb-dotnet>

  **glam**  4 years, 3 months ago

Account

MongoDB API

upvoted 55 times

  **AmitDeorukhkar** 4 years, 1 month ago

Hello all, I think answer could be Database or API for Part 1 and MongoDB API for Part 2.

How Account could be an answer. Could you share documentation or on what basis it can be Account. Please, I would like to get documentation to refer, thanks !

upvoted 3 times

  **demonite** 4 years, 1 month ago

Account and MongoDB API.



Get started with an account <https://docs.microsoft.com/en-us/azure/cosmos-db/create-mongodb-dotnet#create-a-database-account>

upvoted 1 times

  **stephw** 4 years, 1 month ago

Agreed: I guess this is account as the MongoDB version compatibility is set when you create the CosmosDB account and attached to the account (as well as the MongoDB API btw).

upvoted 1 times

  **tita\_tovenaar** 3 years, 11 months ago

first should be API. The question is not what to do first, but to ensure compatibility. According to docs, that's done through the API. See ref:

<https://docs.microsoft.com/en-us/azure/cosmos-db/mongodb-introduction#how-the-api-works>

upvoted 12 times

  **rdemontis** 3 years, 7 months ago

Yes, I think you're right and the question is a little misleading. Trying to translate the meaning of the question we can say it states what are the step you have to do in order to CONFIGURE a Cosmos DB Account. So you have a cosmos db account and you need to do some configuration to guarantee compatibility with a Mongo DB database. So the first thing you have to choose for this configuration is the API. The second is which API specifically. Maybe a bit demented but this is only explanation i can find.

upvoted 3 times

  **praveen\_617** 4 years, 1 month ago

Account

MongoDB API

are the correct answers.

<https://docs.microsoft.com/en-us/azure/cosmos-db/create-mongodb-nodejs#create-an-azure-cosmos-db-account>

```
az cosmosdb create --name <cosmosdb-name> --resource-group myResourceGroup --kind MongoDB
```

The --kind MongoDB parameter enables MongoDB client connections.

upvoted 6 times

  **erickim007**  4 years ago

This question is bit confusing. Second option is very obvious but first one is very strange. Azure CosmosDB, in fact, does not host any database engine for MongoDB therefore 'Database' and/or 'Collection' would not be correct selection.

So it is either 'API' or 'Account'. Account because we specify MongoDB Server version we want to use for the account. But it is my understanding that CosmosDB uses wire protocol, meaning that MongoDB compatibility (i.e. Server version) is equivalent to API version. This is why we do not have create new Account to upgrade or downgrade MongoDB API. In addition, development team needs to know MongoDB Server (i.e. API) version to connect to it (or using SDK).

So if this question comes up and even if I get a wrong mark, I would go with

- API

- MongoDB API



That's because when we investigate compatibility to migrate, I would assess MongoDB server and API version we use currently, and configure 'version' field when creating CosmosDB account.

upvoted 22 times

🗲️ 👤 **LillyLiver** Most Recent 2 years, 12 months ago

Here's a handy little tutorial. Given answers are correct.

<https://docs.microsoft.com/en-us/azure/cosmos-db/mongodb/tutorial-mongotools-cosmos-db>

upvoted 2 times

🗲️ 👤 **g6singh** 3 years, 1 month ago

1- API

First thing you have to choose for this configuration is the API.

2- MongoDB API

The second is which API specifically.

upvoted 1 times

🗲️ 👤 **hikpd** 3 years, 2 months ago

Just tested. When you go to the portal and select Create Cosmos DB, the first selection is --- Which API best suits your workload? So the provided answer is correct.

upvoted 1 times

🗲️ 👤 **plmmsg** 3 years, 3 months ago

API

MongoDB AP

upvoted 1 times

🗲️ 👤 **us3r** 3 years, 4 months ago

api/mongo api

upvoted 1 times

🗲️ 👤 **jmay** 3 years, 5 months ago

It should be API / MongoDB API.

For the first one, if you create a CosmosDB via the Portal, you can see that it clearly prompts "Select API option > Which API best suits your workload?" as the first step of setting up an account.

The question specifically asks about "MongoDB COMPATIBILITY". It is the API you select that make it compatible. not the account. As the account is only a logical container.

upvoted 2 times

🗲️ 👤 **Dpejic** 3 years, 6 months ago

Appere on exam 23-dec-2021

upvoted 3 times

🗲️ 👤 **DerekKey** 3 years, 7 months ago

Account - version compatibility is selected at the account level during the creation

MongoDB API -

upvoted 1 times

🗲️ 👤 **DerekKey** 3 years, 7 months ago

I have reviewed the question again:

"MongoDB compatibility" -> it is at API level

So answer should be:

API

MongoDB API

upvoted 3 times

🗲️ 👤 **student22** 3 years, 8 months ago

API

MongoDB API

upvoted 2 times

🗲️ 👤 **waqas** 3 years, 8 months ago

API and MongoDB API.

upvoted 1 times

🗨️ 👤 **syu31svc** 3 years, 8 months ago

<https://docs.microsoft.com/en-us/azure/cosmos-db/mongodb/create-mongodb-nodejs#create-an-azure-cosmos-db-account>

Create an account for CosmosDB first so compatibility is Account

API is definitely Mongo

upvoted 3 times

🗨️ 👤 **poplovic** 3 years, 9 months ago

API and MongoDB API

for 1) Azure Cosmos DB API for MongoDB implements the wire protocol for MongoDB. This implementation allows transparent compatibility with native MongoDB client SDKs, drivers, and tools. Azure Cosmos DB does not host the MongoDB database engine. Any MongoDB client driver compatible with the API version you are using should be able to connect, with no special configuration.

<https://docs.microsoft.com/en-us/azure/cosmos-db/mongodb/mongodb-introduction#how-the-api-works>

upvoted 4 times

🗨️ 👤 **tongtong** 3 years, 9 months ago

about API, the 2nd question is about it, no idea about question 1, I would go for Collection.

upvoted 2 times

🗨️ 👤 **pentium75** 3 years, 10 months ago

Maybe question 1 is not referring to any Azure setting at all, but just 'on which level will this solution be MongoDB compatible', and that would be 'API'?

upvoted 1 times

🗨️ 👤 **GetulioJr** 3 years, 11 months ago

The answer is correct, First box you choose API then in the second box it asks, but which API, then you choose, MongoDB API. This is a straight forward question. Too many answers here.

upvoted 4 times

You have 100 servers that run Windows Server 2012 R2 and host Microsoft SQL Server 2014 instances. The instances host databases that have the following characteristics:

- ⇒ The largest database is currently 3 TB. None of the databases will ever exceed 4 TB.
- ⇒ Stored procedures are implemented by using CLR.

You plan to move all the data from SQL Server to Azure.

You need to recommend an Azure service to host the databases. The solution must meet the following requirements:

- ⇒ Whenever possible, minimize management overhead for the migrated databases.
- ⇒ Minimize the number of database changes required to facilitate the migration.
- ⇒ Ensure that users can authenticate by using their Active Directory credentials.

What should you include in the recommendation?

- A. Azure SQL Database elastic pools
- B. Azure SQL Database Managed Instance
- C. Azure SQL Database single databases
- D. SQL Server 2016 on Azure virtual machines

**Suggested Answer: B**

Reference:

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-managed-instance>

Community vote distribution

B (100%)

🗳️ 👤 **Tombarc** Highly Voted 4 years, 10 months ago

B is the correct answer. Azure SQL DB does not support CLR stored procedure:

ref: <https://docs.microsoft.com/en-gb/azure/azure-sql/database/transact-sql-differences-sql-server#transact-sql-syntax-not-supported-in-azure-sql-database>

ref: <https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/transact-sql-differences-sql-server#clr>  
upvoted 39 times

🗳️ 👤 **17Master** 3 years, 3 months ago

D. SQL Server 2016 in VM Azure vs B. Azure SQL Managed Instance

CLR Integration - Enabling for both.

<https://docs.microsoft.com/en-us/sql/relational-databases/clr-integration/clr-integration-enabling?view=sql-server-ver15>

So the issue here is: who supports Active Directory authentication?

- Directly it would be "D".
- Through Azure AD Connect it would be "B". (doesn't mention Azure AD)

Correct answer is D

upvoted 1 times

🗳️ 👤 **walkwolf3** 3 years, 7 months ago

Correct

SQL Managed Instance enables you to move your on-premises applications to Azure with minimal application or database changes.

<https://docs.microsoft.com/en-us/azure/azure-sql/migration-guides/managed-instance/sql-server-to-managed-instance-overview#overview>  
upvoted 4 times

🗳️ 👤 **pentum7** Highly Voted 4 years, 7 months ago

Correct:

SQL Managed Instance allows existing SQL Server customers to lift and shift their on-premises applications to the cloud with minimal application and database changes. At the same time, SQL Managed Instance preserves all PaaS capabilities (automatic patching and version updates, automated backups, high availability) that drastically reduce management overhead and TCO.

upvoted 21 times

🗨️ 👤 **prashantjoge** 4 years, 3 months ago

why not D?

upvoted 4 times

🗨️ 👤 **CKL** 4 years, 1 month ago

Logically, even we don't know about the answer or explanation, but we know that Microsoft will promote their native product, D is not, B is. Fundamental of guessing :)

upvoted 9 times

🗨️ 👤 **Krsto** 4 years, 3 months ago

Because of "Whenever possible, minimize management overhead for the migrated databases". Managed instance does not require for you to do VM and SQL updates, this is done by Microsoft.

upvoted 5 times

🗨️ 👤 **demonite** 4 years, 1 month ago

same applies for Azure SQL so what's your point here

upvoted 2 times

🗨️ 👤 **GetulioJr** 4 years ago

Azure SQL is PaaS, all service is maintained by Microsoft. VM with SQL is IaaS, so you need to maintain updates, OS, patches etc. So this is the reason D is not an option here.

upvoted 2 times

🗨️ 👤 **BoxGhost** 3 years, 10 months ago

No, it explicitly states they need to login using Active Directory credentials. Azure SQL and MI are both out since they only support Azure AD. It's carefully worded as "Wherever possible" rather than an explicit requirement. Therefore D is the only option that works.

upvoted 1 times

🗨️ 👤 **17Master** 3 years, 3 months ago

D. SQL Server 2016 in VM Azure vs B. Azure SQL Managed Instance

CLR Integration - Enabling for both.

<https://docs.microsoft.com/en-us/sql/relational-databases/clr-integration/clr-integration-enabling?view=sql-server-ver15>

So the issue here is: who supports Active Directory authentication?

- Directly it would be "D".

- Through Azure AD Connect it would be "B". (doesn't mention Azure AD)

Correct answer is D

upvoted 1 times

🗨️ 👤 **kenshiroo** Most Recent 1 year, 11 months ago

With the Common Language Runtime (CLR) hosted in Microsoft SQL Server (called CLR integration), you can author stored procedures, triggers, user-defined functions, user-defined types, and user-defined aggregates in managed code. CLR is also available in Azure SQL Database Managed Instance.

<https://learn.microsoft.com/en-us/shows/data-exposed/its-just-sql-clr-in-azure-sql-database-managed-instance>

upvoted 1 times

🗨️ 👤 **omerc061** 2 years, 4 months ago

Answer is correct;

Let me explain;

1

"Azure SQL Managed Instance is ideal for customers interested in instance-scoped features, such as SQL Server Agent, Common language runtime (CLR), Database Mail, Distributed transactions, and Machine Learning Services."

2

You can use SQL Managed Instance to do lift-and-shift migrations to Azure without having to redesign your applications.

Link

<https://learn.microsoft.com/en-us/training/modules/design-data-storage-solution-for-relational-data/3-design-for-azure-sql-managed-instance#:~:text=You%20can%20use,Machine%20Learning%20Services.>


upvoted 1 times

🗨️ 👤 **sapien45** 3 years ago

Though the clr enabled configuration option is enabled in Azure SQL Database, developing CLR user functions are not supported in Azure SQL Database.

B



upvoted 1 times

  **[Removed]** 3 years, 3 months ago

**Selected Answer: B**

Correct answer

upvoted 1 times

  **plmmsg** 3 years, 3 months ago

**Selected Answer: B**

Azure SQL Database Managed Instance

upvoted 1 times

  **c\_groleau** 3 years, 5 months ago

**Selected Answer: B**

- A. Azure SQL Database elastic pools - Doesn't support CLR
- B. Azure SQL Database Managed Instance - Correct answer
- C. Azure SQL Database single databases - Doesn't support CLR
- D. SQL Server 2016 on Azure virtual machines - Doesn't minimize cost.

upvoted 6 times

  **chiranjibdas** 3 years, 6 months ago


Can anyone suggest me How we are ruling out the option. A - with Elastic pool. Managed Instance and Elastic pool - both will serve the purpose, I believe, But Elastic pool is cheaper. In Microsoft ESI portal Mock Test, Similar Question is answered with Elastic Pool. So I am little confused here with Option B - Managed Instance which is bit more expensive than the elastic Pool.

upvoted 2 times

  **PapaLion** 3 years, 7 months ago

The Correct Answer is the D we are not talking about hybrid environment so to use AD for authentication the correct answer is the D

upvoted 1 times

  **FinMessner** 3 years, 5 months ago

How do you plan to use AD for authentication on an Azure VM if you don't have a hybrid domain?

upvoted 1 times

  **syu31svc** 3 years, 8 months ago

"minimize management overhead"

I would go for B

upvoted 1 times

  **17Master** 3 years, 3 months ago

if you migrate to sql server in VM you are minimizing the changes. since it is the same platform. Answer is D.

upvoted 1 times

  **Gautam1985** 3 years, 10 months ago

correct

upvoted 1 times

  **erickim007** 4 years ago

there are 3 key requirements that we need to consider.

1. CLR
2. Active Directory (and I believe this is not Azure AD).
3. Minimum Changes

With Azure SQL Server, and MI, even with Azure AD is integrated with Admin operation. And I do not believe Window Authentication is supported for both of option.

Even with CLR, there are few functions that are not support. Access to File System. We do not know what CLR does and we cannot predict changes that the limitation would cause.

In addition, client does not seem mind managing the server by themselves. It seems like there are willing to manage patching and upgrade as they are more concerns around changes/impact/risks comes with migration.

Based upon above, SQL using VM should be recommended.

upvoted 7 times

  **AlexD332** 4 years ago

plus they mention db size won't excide 4Gb

upvoted 4 times

  **UnknownSecret** 3 years, 11 months ago

You are right, it shuld be D. Azure SQL MI does to support AD on-premises logons. As we move our DM from on-premises, the:  
"by using their Active Directory credentials"

means that Windows Logon type must be supported.

upvoted 2 times

  **pentium75** 3 years, 10 months ago

Per the link below, Azure SQL MI does support AD auth with on-premise credentials if you use SSO ...

<https://docs.microsoft.com/en-us/azure/azure-sql/database/authentication-aad-configure?tabs=azure-powershell>

upvoted 2 times

  **UnknownSecret** 3 years, 10 months ago

Yes, I would agree with you if SSO is used. But is not.

More about the workaround mentioned by you is here:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/authentication-mfa-ssms-overview>

upvoted 2 times

  **pentium75** 3 years, 10 months ago

Tricky. SQL Server on VM (D) "is the only way to use Windows authentication to SQL Server." On the other hand, SQL Managed Instance supports "Active Directory integrated authentication ... Use this method if you are logged into Windows using your Azure Active Directory credentials from a federated domain, or a managed domain that is configured for seamless single sign-on for pass-through and password hash authentication."

Since they are asking what to INCLUDE in the solution (not for the COMPLETE solution), we could include SQL Managed Instance AND AD Connect with SSO in the solution. Then B would work.

upvoted 2 times

  **17Master** 3 years, 3 months ago

D. SQL Server 2016 in VM Azure vs B.Azure SQL Managed Instance

CLR Integration - Enabling for both.

<https://docs.microsoft.com/en-us/sql/relational-databases/clr-integration/clr-integration-enabling?view=sql-server-ver15>

So the issue here is: who supports Active Directory authentication?

- Directly it would be "D".

- Through Azure AD Connect it would be "B". (doesn't mention Azure AD)



Correct answer is D

upvoted 1 times

  **hendry781** 4 years, 3 months ago

Shouldnt the answer be D as it requires Windows AD authentication? Azure SQL MI doesnt support Windows Authentication

upvoted 3 times

  **rocrock** 4 years, 3 months ago

Azure Active Directory (Azure AD) authentication - Azure SQL: Yes. Azure AD users only. SQL Managed Instance: Yes. Including server-level Azure AD logins.

upvoted 1 times

  **17Master** 3 years, 3 months ago

D. SQL Server 2016 in VM Azure vs B.Azure SQL Managed Instance

CLR Integration - Enabling for both.

<https://docs.microsoft.com/en-us/sql/relational-databases/clr-integration/clr-integration-enabling?view=sql-server-ver15>

So the issue here is: who supports Active Directory authentication?

- Directly it would be "D".

- Through Azure AD Connect it would be "B". (doesn't mention Azure AD)

Correct answer is D

upvoted 1 times

🗨️ 👤 **glam** 4 years, 5 months ago

B. Azure SQL Database Managed Instance  
upvoted 3 times

🗨️ 👤 **milind8451** 4 years, 5 months ago

CLR is support by SQL Managed instance only. Ans is correct.  
upvoted 9 times

🗨️ 👤 **TheAzureArchitect** 3 years, 7 months ago

CLR also works on SQL on VM.  
I believe the answer should be D, SQL VM, as AD login not supported on MI.  
upvoted 1 times

🗨️ 👤 **17Master** 3 years, 3 months ago

correct.  
D. SQL Server 2016 in VM Azure vs B.Azure SQL Managed Instance  
CLR Integration - Enabling for both.  
<https://docs.microsoft.com/en-us/sql/relational-databases/clr-integration/clr-integration-enabling?view=sql-server-ver15>  
So the issue here is: who supports Active Directory authentication?  
- Directly it would be "D".  
- Through Azure AD Connect it would be "B". (doesn't mention Azure AD)  
Correct answer is D  
upvoted 1 times

🗨️ 👤 **JustDiscussing** 4 years, 6 months ago

in exam this week  
upvoted 2 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have an Azure Storage account that contains two 1-GB data files named File1 and File2. The data files are set to use the archive access tier. You need to ensure that File1 is accessible immediately when a retrieval request is initiated.

Solution: For File1, you set Access tier to Hot.

Does this meet the goal?

A. Yes

B. No

#### Suggested Answer: A

The hot access tier has higher storage costs than cool and archive tiers, but the lowest access costs. Example usage scenarios for the hot access tier include:

- ⇒ Data that's in active use or expected to be accessed (read from and written to) frequently.
- ⇒ Data that's staged for processing and eventual migration to the cool access tier.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers>

Community vote distribution

A (100%)

  **lupuscon**  4 years, 2 months ago

The Answer is correct and to clear up the confusion.

File != File Share

In this case the File should be called a blob

Archive Tier is only available for Blob Storage and Blob Containers

In a Blob Container you can set the Access-Tier per blob

upvoted 25 times

  **jmay** 3 years, 5 months ago




never had this confusion... but thanks anyway :)

upvoted 7 times

  **nkx**  3 years, 9 months ago



came in exam on 20-sep-21, I passed, i choose given answer

upvoted 8 times

  **AubinBakana**  2 years, 10 months ago

While the answer is correct, the question is bad. Because they start with saying that both files are set to use Archive tier. This is enough to confuse.

upvoted 1 times

  **Dawn7** 3 years, 3 months ago

 **Selected Answer: A**



I think it is correct

upvoted 1 times

  **mpellizzon** 3 years, 3 months ago

"You need to ensure that File1 is accessible immediately when \*\*\*a retrieval request is initiated\*\*\*." If it is in archive, even changing to Hot is impossible to be immediately available, isn't it?

upvoted 4 times

  **AlexD332** 4 years ago

Why Hot but not Cool?

upvoted 1 times

  **keilah123** 4 years ago

This is a series of question, each one will provide different solutions and we have to check if the solution will meet the goal or not. Both hot and cool are correct. Maybe on next question, the solution that will be provide is "Hot"



upvoted 9 times

  **ruslan\_bespalov\_netconomy** 4 years, 2 months ago

This is really confusing. YES - you set the Hot tier but NO - you can't set it for file, you set it for the whole storage.

I guess the expected answer here is still A (Yes) but the question itself is incorrect

upvoted 2 times

  **ruslan\_bespalov\_netconomy** 4 years, 2 months ago

Disregard that. It's possible to set the tier per file. The answer Yes is correct

upvoted 6 times

  **FBFTopics** 3 years, 5 months ago

You're right:

"Storage accounts have a default access tier setting that indicates the online tier in which a new blob is created. The default access tier setting can be set to either Hot or Cool. Users can override the default setting for an individual blob when uploading the blob or changing its tier".

<https://docs.microsoft.com/en-us/azure/storage/blobs/access-tiers-overview>

upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have an Azure Storage account that contains two 1-GB data files named File1 and File2. The data files are set to use the archive access tier. You need to ensure that File1 is accessible immediately when a retrieval request is initiated.

Solution: You add a new file share to the storage account.

Does this meet the goal?

A. Yes

B. No

**Suggested Answer: B**

Community vote distribution

B (100%)

🗲️ **stieltjes** Highly Voted 4 years, 2 months ago

correct

upvoted 13 times

🗲️ **Dawn7** Most Recent 3 years, 3 months ago

**Selected Answer: B**

Correct

upvoted 2 times

🗲️ **Dawn7** 3 years, 3 months ago

Correct

upvoted 1 times

🗲️ **[Removed]** 3 years, 3 months ago

**Selected Answer: B**

Correct

upvoted 1 times

🗲️ **anupam77** 3 years, 3 months ago

**Selected Answer: B**

Correct answer given

upvoted 1 times

🗲️ **syu31svc** 3 years, 8 months ago

Answer is No

It's the access tier you need to change

upvoted 3 times

🗲️ **nkx** 3 years, 9 months ago

came in exam on 20-sep-21, I passed, i choose given answer

upvoted 3 times

🗲️ **bigngster** 3 years, 10 months ago

Correct. But this is not a good question.

As other have pointed out, Azure file share does NOT have an archive tier (<https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-create-file-share?tabs=azure-portal>) . Only 3 tiers are available, Transaction optimized, Hot, Cool.

Perhaps creating an Azure file share is the first step in rehydrating the data. Moving data to Cool / hot tier is rehydrating. However, the question stops short in just stating creating a file share, which does nothing to the original data.

upvoted 1 times

🗨️ 👤 **El\_Hechizo** 3 years, 11 months ago

What a crap question, if it is intended to check the knowledge on the access tier should be NO, otherwise YES  
upvoted 1 times

🗨️ 👤 **kiwi123** 3 years, 11 months ago

archive tier, should be No?  
upvoted 2 times

🗨️ 👤 **Linus0** 3 years, 11 months ago

If files stored in File Share are not accessible immediately, then how long will take when user access the file?

Answer is A

upvoted 2 times

🗨️ 👤 **ReginaldoBarreto** 4 years ago

question without foot or head....

This question is about the TIER, not the storage type.

upvoted 2 times

🗨️ 👤 **PhyMac** 4 years ago

I think the answer is A.

File share of Azure storage account provides immediate access.

upvoted 2 times

🗨️ 👤 **pentium75** 3 years, 10 months ago

Not if it's in the archive tier: "Data in the archive tier can take several hours to retrieve depending on the specified rehydration priority."

<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/storage/blobs/storage-blob-storage-tiers.md>

upvoted 1 times

🗨️ 👤 **Rajesh123** 3 years, 2 months ago

slow and high reterival cost

upvoted 1 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You have an Azure Storage account that contains two 1-GB data files named File1 and File2. The data files are set to use the archive access tier. You need to ensure that File1 is accessible immediately when a retrieval request is initiated. Solution: You move File1 to a new storage account. For File1, you set Access tier to Archive. Does this meet the goal?

- A. Yes
- B. No

**Suggested Answer: B**

Instead use the hot access tier.

The hot access tier has higher storage costs than cool and archive tiers, but the lowest access costs. Example usage scenarios for the hot access tier include:

Data that's in active use or expected to be accessed (read from and written to) frequently.

- 
- ⇒ Data that's staged for processing and eventual migration to the cool access tier.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers>

Community vote distribution

B (100%)

maciezie **Highly Voted** 4 years, 2 months ago

Correct

upvoted 20 times

syu31svc **Highly Voted** 3 years, 9 months ago

<https://docs.microsoft.com/en-us/azure/storage/blobs/archive-rehydrate-overview?tabs=azure-portal>

While a blob is in the archive access tier, it's considered to be offline and can't be read or modified. In order to read or modify data in an archived blob, you must first rehydrate the blob to an online tier, either the hot or cool tier. There are two options for rehydrating a blob that is stored in the archive tier:

Copy an archived blob to an online tier: You can rehydrate an archived blob by copying it to a new blob in the hot or cool tier with the Copy Blob or Copy Blob from URL operation. Microsoft recommends this option for most scenarios.

Change a blob's access tier to an online tier: You can rehydrate an archived blob to hot or cool by changing its tier using the Set Blob Tier operation.

Answer is No

upvoted 5 times

Dawn7 **Most Recent** 3 years, 3 months ago

**Selected Answer: B**

Correct

upvoted 1 times

[Removed] 3 years, 3 months ago

**Selected Answer: B**

Correct

upvoted 1 times

azurelearner666 3 years, 3 months ago

It's No.

But the comment "Instead use the hot access tier" is wrong. At least partially.

As the Hot & Cool access tiers will enable "Immediate access"

upvoted 1 times

You are designing an order processing system in Azure that will contain the Azure resources shown in the following table.

Name	Type	Purpose
App1	Web app	Processes customer orders
Function1	Function	Check product availability at vendor 1
Function2	Function	Check product availability at vendor 2
storage1	Storage account	Stores order processing logs

The order processing system will have the following transaction flow:

- ⇒ A customer will place an order by using App1.
- ⇒ When the order is received, App1 will generate a message to check for product availability at vendor 1 and vendor 2.
- ⇒ An integration component will process the message, and then trigger either Function1 or Function2 depending on the type of order.
- ⇒ Once a vendor confirms the product availability, a status message for App1 will be generated by Function1 or Function2.
- ⇒ All the steps of the transaction will be logged to storage1.

Which type of resource should you recommend for the integration component?

- A. an Azure Data Factory pipeline
- B. an Azure Service Bus queue
- C. an Azure Event Grid domain
- D. an Azure Event Hubs capture

#### Suggested Answer: A

A data factory can have one or more pipelines. A pipeline is a logical grouping of activities that together perform a task.

The activities in a pipeline define actions to perform on your data.

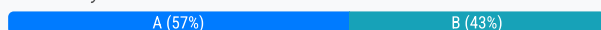
Data Factory has three groupings of activities: data movement activities, data transformation activities, and control activities.

Azure Functions is now integrated with Azure Data Factory, allowing you to run an Azure function as a step in your data factory pipelines.

Reference:

<https://docs.microsoft.com/en-us/azure/data-factory/concepts-pipelines-activities>

Community vote distribution



🗳️ 👤 **MaxBlanche** Highly Voted 4 years, 7 months ago

B would be a more appropriate answer  
upvoted 101 times

🗳️ 👤 **mmmore** 4 years, 6 months ago

Agreed, I believe this question is looking us to recognise that messages need be able sent from different application components. A service bus will do this. The actual orchestration via Data Factory doesn't make a lot of sense. Something like Durable (Azure) Functions would be more suited for that.  
upvoted 12 times

🗳️ 👤 **andyR** 4 years, 7 months ago

agreed  
upvoted 4 times

🗳️ 👤 **Moley** 4 years, 1 month ago

"An integration component will process the message, and then trigger either Function1 or Function2 depending on the type of order." to me this describes an Event Grid  
upvoted 8 times

🗳️ 👤 **soren** 4 years, 1 month ago

Agreed. There can be a generic trigger associated with the queue and within that trigger logic can determine the order type and execute the correct AZ function. The trigger can also do the logging. ADF could work but seems out of place for this task IMO.  
upvoted 4 times

🗳️ 👤 **examineezer** 3 years, 6 months ago

Question states "will process the message, and then trigger EITHER Function1 OR Function2" (not both)  
upvoted 2 times

🗳️ 👤 **uzairahm007** Highly Voted 👍 4 years, 6 months ago

Look at the question carefully it states:

An integration component will **\*\*process\*\*** the message, and then trigger either Function1 or Function2 depending on the type of order.

The keyword is process the message neither Service Bus nor Event Grid provide those functionalities.

There is not mentioned where you would be storing the message but Azure Data Factory can integrate with various platforms and pick messages and based on that could fire either Function1 or Function2 based on order type.

upvoted 74 times

🗳️ 👤 **examineezer** 3 years, 7 months ago

Event grid supports filtering. Message comes in. Filter the message based on type of order. Simple.

upvoted 2 times

🗳️ 👤 **PerfumoPeru** 3 years, 11 months ago

Plus, this "process" should be audited, sending data to Azure Storage Account. So ADF is correct.

upvoted 4 times

🗳️ 👤 **Oracleist** 4 years, 2 months ago

an ETL tool for managing a transaction... mmm smells strange.

BUS has a FIFO option that is necessary for "check availability"

upvoted 14 times

🗳️ 👤 **arseyam** 4 years, 6 months ago

Microsoft Azure Service Bus is a fully managed enterprise message broker with message queues and public-subscribe topics. Service Bus is used to decouple applications and services from each other, providing the following benefits:

Load-balancing work across competing workers

Safely routing and transferring data and control across service and application boundaries

Coordinating transactional work that requires a high-degree of reliability

In the question

When the order is received, App1 will generate a message to check for product availability at vendor 1 and vendor 2.

With Topics the Publisher sends a message to a topic and one or more subscribers receive a copy of the message, depending on filter rules set on these subscriptions.

<https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-queues-topics-subscriptions#topics-and-subscriptions>

upvoted 12 times

🗳️ 👤 **seaman33** Most Recent 🔍 6 months ago

Selected Answer: B

Thinking as an architect:

1. Order requests must be processed with ordering guarantees, otherwise you'll get a mess
2. Although technically both ADF and ASB (with filtering) have required integration/processing capabilities, ADF doesn't provide ordering guarantees.

Answer is B: ASB

upvoted 1 times

🗳️ 👤 **rxlicon** 1 year, 10 months ago

the problem is that in the answers options you haven't a topic but only the queue service. So ASB can't process to different functions.

Leaves only A, Azure Data factory

upvoted 1 times

🗳️ 👤 **manajerOfEmptiness** 2 years, 5 months ago

Selected Answer: A

The requirement can be achieved with Service Bus topics/subscriptions by sending the message based on metadata to subscribers listening to a specific topic.

But since there is no such answer Factory is second best

upvoted 1 times

🗳️ 👤 **jellybiscuit** 2 years, 9 months ago

Selected Answer: B

This is what the Service Bus does.

upvoted 1 times

🗨️ 👤 **nidhogg** 2 years, 10 months ago

**Selected Answer: A**

As @tteesstt said before, it's 1:M vs 1:1, it can't be SB.

A) ADF pipeline

upvoted 1 times

🗨️ 👤 **AubinBakana** 2 years, 10 months ago

**Selected Answer: A**

The answer is correct. I got it wrong at first but after analysis, I have come to understand the question better.

The messaging, which is probably held using Service bus Topic, is done separately. This question is about the integration component, not the messaging service. ADF will do the processing of the messages, and the trigger F1 and/or F2.

upvoted 4 times

🗨️ 👤 **sapien45** 3 years ago

Azure Service Bus

FIFO

Delivery guarantee : At-Most-Once

It stores messages in a "broker" (for example, a queue) until the consuming party is ready to receive the messages.

B

upvoted 3 times

🗨️ 👤 **AberdeenAngus** 3 years, 1 month ago

Where I work it's common to have the front end put messages in a service bus queue/topic to be processed by back end functions. This is critical to avoid the functions from being overwhelmed in busy times. So I'm going service bus.

Also, I don't know how the ADF which some people are proposing could be triggered to process the message from the web app, in my experience ADF is more for batch processes.

upvoted 1 times

🗨️ 👤 **Pupu86** 3 years, 2 months ago

For people who chose B, you obviously didn't setup and serverless environment with Azure before... without logging the data to storage you could do with Event Grid to determine the function app to call based on message type but when you need to manage the flow of data to storage account, you will ultimately need ADF or Logic App to handle the logic flow regardless whether you use ADF for ETL or not.

Answer is Azure Data Factory

upvoted 2 times

🗨️ 👤 **StevensDKLrg** 3 years, 3 months ago

**Selected Answer: A**

The question clearly asks "Which type of resource should you recommend for the integration component?". The integration component will "process the message, and then trigger either Function1 or Function2 depending on the type of order." This is not asking how to send the message; it's asking how to process the message. I believe the answer is correct, ADF.

upvoted 4 times

🗨️ 👤 **Dawn7** 3 years, 3 months ago

**Selected Answer: B**

I would go with B

upvoted 1 times

🗨️ 👤 **arun** 3 years, 3 months ago

**Selected Answer: A**

As per below link 'ADF pipeline' can consume message from Web Activity and it support transform as well so it can parse/validate the incoming message and call respective function (1 or 2)..

<https://docs.microsoft.com/en-us/azure/data-factory/concepts-pipelines-activities?tabs=data-factory#control-flow-activities>

I use ASB queue which cannot do message validation by itself to decide which function should be called further.

However, ASB Topic can do the expected behavior but it's not mentioned in the answer so i think 'ADF pipeline' is best suitable from the given option.

upvoted 3 times

🗨️ 👤 **northgaterebel** 3 years, 4 months ago





**Selected Answer: B**

Answer is Service Bus, no doubt. When to use: Order processing and financial transactions.

<https://docs.microsoft.com/en-us/azure/event-grid/compare-messaging-services#comparison-of-services>

upvoted 3 times

  **ScottyKnows** 3 years, 4 months ago

**Selected Answer: A**

Multiple sources confirm it to be Datafactory.

upvoted 4 times

  **carlos045** 3 years, 4 months ago

i think is B

upvoted 1 times

**HOTSPOT -**

You have an existing implementation of Microsoft SQL Server Integration Services (SSIS) packages stored in an SSISDB catalog on your on-premises network.

The on-premises network does not have hybrid connectivity to Azure by using Site-to-Site VPN or ExpressRoute.

You want to migrate the packages to Azure Data Factory.

You need to recommend a solution that facilitates the migration while minimizing changes to the existing packages. The solution must minimize costs.

What should you recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

**Answer Area**

Store the SSISDB catalog by using:

Azure SQL Database
Azure Synapse Analytics
SQL Server on an Azure virtual machine
SQL Server on an on-premises computer

Implement a runtime engine for package execution by using:

Self-hosted integration runtime only
Azure-SQL Server Integration Services Integration Runtime (IR) only
Azure-SQL Server Integration Services Integration Runtime and self-hosted integration runtime

**Suggested Answer:****Answer Area**

Store the SSISDB catalog by using:

Azure SQL Database
Azure Synapse Analytics
SQL Server on an Azure virtual machine
SQL Server on an on-premises computer

Implement a runtime engine for package execution by using:

Self-hosted integration runtime only
Azure-SQL Server Integration Services Integration Runtime (IR) only
Azure-SQL Server Integration Services Integration Runtime and self-hosted integration runtime

Box 1: Azure SQL database -

You can't create the SSISDB Catalog database on Azure SQL Database at this time independently of creating the Azure-SSIS Integration Runtime in Azure Data

Factory. The Azure-SSIS IR is the runtime environment that runs SSIS packages on Azure.

Box 2: Azure-SQL Server Integration Service Integration Runtime and self-hosted integration runtime

The Integration Runtime (IR) is the compute infrastructure used by Azure Data Factory to provide data integration capabilities across different network environments. Azure-SSIS Integration Runtime (IR) in Azure Data Factory (ADF) supports running SSIS packages.

Self-hosted integration runtime can be used for data movement in this scenario.

Reference:

<https://docs.microsoft.com/en-us/azure/data-factory/create-azure-integration-runtime> <https://docs.microsoft.com/en-us/sql/integration-services/lift-shift/ssis-azure-connect-to-catalog-database>

 **glam**  4 years, 5 months ago

Box 1: Azure SQL database -

Box 2: Azure-SQL Server Integration Service Integration Runtime and self-hosted integration runtime

upvoted 51 times

  **uzairahm007** Highly Voted 4 years, 6 months ago

Why Self hosted IR?



This article describes how to run SQL Server Integration Services (SSIS) packages on an Azure-SSIS Integration Runtime (Azure-SSIS IR) in Azure Data Factory with a self-hosted integration runtime (self-hosted IR) configured as a proxy.

With this feature, you can access data on-premises without having to join your Azure-SSIS IR to a virtual network. The feature is useful when your corporate network has a configuration too complex or a policy too restrictive for you to inject your Azure-SSIS IR into it.

<https://docs.microsoft.com/en-us/azure/data-factory/self-hosted-integration-runtime-proxy-ssis>


As Azure cloud does not connectivity to on Premise network you would need to implement self Hosted-IR as well

upvoted 16 times

  **jhoomtv** 4 years, 6 months ago

because data coming from on-prem, you need self hosted

upvoted 5 times

  **FinMessner** 3 years, 5 months ago

It's going to an Azure SQL DB first...

upvoted 1 times

  **sallymaher** 4 years, 3 months ago

in this case you are moving the package directly to ADF , so why you will use Azure SQL in the first box ??? As long as I'll use Azure SQL so Azure IR is enough .

upvoted 4 times

  **[Removed]** Most Recent 3 years, 3 months ago

Correct answer given

upvoted 2 times

  **FinMessner** 3 years, 5 months ago

Provision. Before you can deploy and run SSIS packages in Azure, you have to provision the SSIS Catalog (SSISDB) and the Azure-SSIS Integration Runtime.

You don't need a self-hosted integration runtime also because the catalog is now in an Azure SQL SSIS DB.

upvoted 1 times

  **syu31svc** 3 years, 8 months ago

<https://docs.microsoft.com/en-us/sql/integration-services/lift-shift/ssis-azure-lift-shift-ssis-packages-overview?view=sql-server-ver15>

You can now move your SQL Server Integration Services (SSIS) projects, packages, and workloads to the Azure cloud. Deploy, run, and manage SSIS projects and packages in the SSIS Catalog (SSISDB) on Azure SQL Database or SQL Managed Instance with familiar tools such as SQL Server Management Studio (SSMS).

<https://docs.microsoft.com/en-us/azure/data-factory/self-hosted-integration-runtime-proxy-ssis>

With this feature, you can access data and run tasks on premises without having to join your Azure-SSIS IR to a virtual network

Answer is correct

upvoted 4 times

  **sapien45** 3 years ago

Great answer

upvoted 1 times

  **Gautam1985** 3 years, 10 months ago

Correct

upvoted 2 times

  **El\_Hechizo** 3 years, 11 months ago

To run SSIS packages, you need "Azure-SQL Server Integration services Integration runtime" <https://www.youtube.com/watch?v=weiHOeje-QA> min 3:07. To connect without VPN or Express Route, you need to install a self-hosted integration runtime that acts as a proxy (as seen on video). Then the second Box is: "Azure-SQL Server Integration services Integration runtime and self-hosted integration".

For the first one, I guess Azure SQL Database.

upvoted 5 times

🗨️ 👤 **Jasper666** 4 years ago

Select the Set up Self-Hosted Integration Runtime as a proxy for your Azure-SSIS Integration Runtime check box to choose whether you want to configure a self-hosted IR as proxy for your Azure-SSIS IR. Since we migrated completely to azure this is not needed. Box 1 is azure sql database and Box 2 is azure SSIS IR only. (<https://docs.microsoft.com/en-us/azure/data-factory/self-hosted-integration-runtime-proxy-ssis>)

upvoted 1 times

🗨️ 👤 **Amit3** 4 years ago

Question says you need to facilitate migration but doesn't say you have migrated already.

upvoted 1 times

🗨️ 👤 **aspirin** 4 years, 2 months ago

Correct answer

upvoted 3 times

🗨️ 👤 **Leon3020** 4 years, 2 months ago

The installation of a self-hosted integration runtime needs an on-premises machine or a virtual machine inside a private network.

I would select 2 for Box 2.

upvoted 1 times

🗨️ 👤 **prashantjoge** 4 years, 3 months ago

is this even in the syllabus... id ont see any mention of this in MS learn

upvoted 4 times

🗨️ 👤 **ElsaBBP** 4 years, 4 months ago

the second answer would be C only if you have a stable Site to Site connectivity or ER. without this, an SSIS IR only is the correct answer. I know the question is so misleading :)

upvoted 2 times

🗨️ 👤 **rizabeer** 4 years, 5 months ago

In my opinion the answer is correct, as per your reference @uzairahm007, "This article describes how to run SQL Server Integration Services (SSIS) packages on an Azure-SSIS Integration Runtime (Azure-SSIS IR) in Azure Data Factory with a self-hosted integration runtime (self-hosted IR) configured as a proxy.

With this feature, you can access data on-premises without having to join your Azure-SSIS IR to a virtual network. The feature is useful when your corporate network has a configuration too complex or a policy too restrictive for you to inject your Azure-SSIS IR into it." So both self hosted and Azure SSIS IR are needed for this feature to work.

upvoted 6 times

🗨️ 👤 **heany** 4 years, 5 months ago

second one should be IR only. as self-hosting is running on on-prem network. but it also mentioned 'The on-premises network does not have hybrid connectivity to Azure by using Site-to-Site VPN or ExpressRoute'

upvoted 2 times

🗨️ 👤 **Sasi27** 4 years, 5 months ago

so whats the answer then ?

upvoted 1 times

You have 70 TB of files on your on-premises file server.

You need to recommend solution for importing data to Azure. The solution must minimize cost.

What Azure service should you recommend?

- A. Azure StorSimple
- B. Azure Batch
- C. Azure Data Box
- D. Azure Stack Hub

**Suggested Answer: C**

Microsoft has engineered an extremely powerful solution that helps customers get their data to the Azure public cloud in a cost-effective, secure, and efficient manner with powerful Azure and machine learning at play. The solution is called Data Box.

Data Box and is in general availability status. It is a rugged device that allows organizations to have 100 TB of capacity on which to copy their data and then send it to be transferred to Azure.

Incorrect Answers:


A: StoreSimple would not be able to handle 70 TB of data.

Reference:

<https://www.vembu.com/blog/what-is-microsoft-azure-data-box-disk-edge-heavy-gateway-overview/>


Community vote distribution

C (100%)


-  **speedminer** Highly Voted 4 years, 9 months ago

<https://docs.microsoft.com/en-us/azure/databox/data-box-overview>


80TB max for Databox

upvoted 23 times
-  **folkmusic99** 4 years ago

100-TB device has 80 TB or usable capacity after RAID 5 protection


upvoted 5 times
-  **sumedh01** Highly Voted 4 years, 7 months ago

Storage capacity 100 TB device has 80 TB usable capacity after RAID 5 protection


upvoted 9 times
-  **Dawn7** Most Recent 3 years, 3 months ago

**Selected Answer: C**

I think it is correct

upvoted 1 times
-  **Dpejic** 3 years, 6 months ago


On exam 24.12.2021

upvoted 2 times
-  **sharepoint\_Azure\_pp** 3 years, 8 months ago

Azure Data box is correct

choose the same

cleared with 900 on 17th October 2021

upvoted 5 times
-  **syu31svc** 3 years, 8 months ago

The Microsoft Azure Data Box cloud solution lets you send terabytes of data into and out of Azure in a quick, inexpensive, and reliable way. The secure data transfer is accelerated by shipping you a proprietary Data Box storage device. Each storage device has a maximum usable storage capacity of 80 TB and is transported to your datacenter through a regional carrier.

Answer is C

upvoted 2 times

🗨️ 👤 **Gautam1985** 3 years, 10 months ago

correct

upvoted 1 times

🗨️ 👤 **tvS2021** 3 years, 11 months ago

on exam (7-19-2021). cleared 304 exam.

upvoted 6 times

🗨️ 👤 **GetulioJr** 4 years ago

StorSimple would fit only 15 TB or up to 38 TB. So answer is correct.

REF: <https://docs.microsoft.com/en-us/azure/storsimple/storsimple-8000-technical-specifications-and-compliance>

upvoted 1 times

🗨️ 👤 **pentium75** 3 years, 10 months ago

Could also use more than one device, but it would surely not 'minimize cost'.

upvoted 1 times

🗨️ 👤 **ShahEM** 4 years, 2 months ago

Correct

upvoted 2 times

🗨️ 👤 **glam** 4 years, 5 months ago

C. Azure Data Box

upvoted 4 times

🗨️ 👤 **milind8451** 4 years, 5 months ago

Right ans.

upvoted 3 times

🗨️ 👤 **Blaaa** 4 years, 5 months ago

Correct

upvoted 3 times

🗨️ 👤 **Hanger\_Man** 4 years, 7 months ago

correct

upvoted 4 times

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen. You are designing an Azure solution for a company that has four departments. Each department will deploy several Azure app services and Azure SQL databases.

You need to recommend a solution to report the costs for each department to deploy the app services and the databases. The solution must provide a consolidated view for cost reporting that displays cost broken down by department.

Solution: Create a separate resource group for each department. Place the resources for each department in its respective resource group. Does this meet the goal?

- A. Yes
- B. No

**Suggested Answer: B**

Instead create a resources group for each resource type. Assign tags to each resource group.

Note: Tags enable you to retrieve related resources from different resource groups. This approach is helpful when you need to organize resources for billing or management.

Reference:

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

Community vote distribution

A (100%)

🗳️ 👤 **Shailen** Highly Voted 4 years, 1 month ago

Correct Answer is yes, below are the simple steps to fetch consolidated cost report for each Resource Group (department in this case).

1. Open Azure portal and navigate to subscription and then cost analysis (under cost management).
2. A consolidated view will appear with a nice main diagram and multiple pie charts and one of them is showing costs for each resource group.
3. You may also select "Resource Group Name" under option "Group by" on the main chart. This will bring also bring a consolidated view for each resource group!

upvoted 58 times

🗳️ 👤 **photon99** 1 year, 4 months ago

The key point is "Assign tags to each resource" , as tags are not inherited which means if you assign a tag to a RG >> it will not propagated/inherited to the underneath resources , so you MUST assign tags to each individual resource.

upvoted 1 times

🗳️ 👤 **MARKMKENYA** 2 years, 4 months ago

Ive tested this and its true

upvoted 1 times

🗳️ 👤 **sco\_murad** Highly Voted 4 years, 1 month ago

Resource Groups are used to delegate administration, not for cost allocation. Tags should be used for this purpose!

upvoted 21 times

🗳️ 👤 **jnlhj** 3 years, 10 months ago

But in this question, it says "You need to recommend a solution to ...". The solution can solve the problem, but is not the recommended solution by administrator. So "No" is right.

upvoted 3 times

🗳️ 👤 **sjai** 3 years, 9 months ago

But in the end, it says "Does it meet the goal". It does meet the goal.

upvoted 8 times

🗳️ 👤 **examineezer** 3 years, 6 months ago

Exactly. "Does this meet the goal?"

upvoted 2 times

🗳️ 👤 **DeepHouse** 4 years, 1 month ago

That's true, but it doesn't mean the given answer is correct.

Cost management can breakdown costs per RG, so the answer is A. Yes.

upvoted 16 times

🗳️ 👤 **ShivaUdari** Most Recent 1 year, 9 months ago

Selected Answer: A

It's simple, we can use separate RG's to achieve the goal.

upvoted 1 times

🗳️ 👤 **rxlicon** 1 year, 10 months ago

cost analysis

A consolidated view will appear

You may also select "Resource Group Name" under option "Group by"

upvoted 1 times

🗳️ 👤 **muni53** 2 years, 7 months ago

Even though resource group creation suffice the purpose but it is not recommended. Create tags instead

upvoted 1 times

🗳️ 👤 **AubinBakana** 2 years, 10 months ago

I guess this question was designed to raise awareness of tags. It just needs a better formulation. At the exam, yes to all that have tag on it I suppose, smiling.

upvoted 3 times

🗳️ 👤 **marco\_aimi** 3 years, 3 months ago

for sure a better solution with tag, no doubt, but mind question : " Does it meet the goal?"

Yes

upvoted 1 times

🗳️ 👤 **us3r** 3 years, 4 months ago

Selected Answer: A

VOTE A

upvoted 1 times

🗳️ 👤 **TariqKipkemei** 3 years, 4 months ago

Selected Answer: A

Answer is A

upvoted 1 times

🗳️ 👤 **massnonn** 3 years, 5 months ago

Selected Answer: A

Cost Management can track by Resource Group. Allows you to report by resource group.

upvoted 1 times

🗳️ 👤 **Eitant** 3 years, 6 months ago

Selected Answer: A

Answer is YES

upvoted 3 times

🗳️ 👤 **[Removed]** 3 years, 6 months ago

Selected Answer: A

Answer should be Yes, tags will help to find data if combined to multiple resources group. In this case ask is department based and resource group is set to department. Yes is right

upvoted 5 times

🗳️ 👤 **RamprasadPeesa** 3 years, 7 months ago

I would go for yes, eventhough this is not recommended because sometime isolation is more a requirement than cost. So the goal is met. so "Yes".

upvoted 1 times

🗳️ 👤 **syu31svc** 3 years, 8 months ago

You can filter by resource group so answer is Yes

<https://docs.microsoft.com/en-us/azure/cost-management-billing/costs/group-filter>

upvoted 7 times

🗳️ 👤 **wojack119** 3 years, 9 months ago



Same question in [www.skillpipe.com](http://www.skillpipe.com) that provided by training course, answer is Yes.

upvoted 6 times

  **pentium75** 3 years, 10 months ago

That would probably meet the goal of getting cost report per department, but would it be feasible in general? Having one RG per department is not a Best Practice and would cause other implications (like difficult permission management etc.). Would they consider a solution 'meeting the goal' in that case?

upvoted 2 times

  **lucasasterio** 3 years, 11 months ago

Answer is YES

upvoted 3 times

You have an Azure subscription that contains 100 virtual machines.

You plan to design a data protection strategy to encrypt the virtual disks.

You need to recommend a solution to encrypt the disks by using Azure Disk Encryption. The solution must provide the ability to encrypt operating system disks and data disks.

What should you include in the recommendation?

- A. a certificate
- B. a key
- C. a passphrase
- D. a secret

**Suggested Answer: B**


For enhanced virtual machine (VM) security and compliance, virtual disks in Azure can be encrypted. Disks are encrypted by using cryptographic keys that are secured in an Azure Key Vault. You control these cryptographic keys and can audit their use.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/encrypt-disks>

Community vote distribution

B (100%)

 **speedminer** Highly Voted 4 years, 9 months ago

Azure Disk Encryption requires an Azure Key Vault to control and manage disk encryption keys and secrets. Your key vault and VMs must reside in the same Azure region and subscription.

upvoted 28 times

 **saditya1** Highly Voted 4 years, 7 months ago

B is correct

upvoted 15 times

 **AberdeenAngus** Most Recent 3 years, 1 month ago

I created a VM and key vault, and encrypted the os disk following the steps in <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-cli-quickstart>

Afterwards my key vault contained no keys, 1 secret

upvoted 1 times

 **Dawn7** 3 years, 3 months ago

Selected Answer: B

A key is correct

upvoted 1 times

 **us3r** 3 years, 4 months ago

Selected Answer: B

vote b

upvoted 1 times

 **Dpejic** 3 years, 6 months ago

Appere on exam 23-dec-2021

upvoted 1 times

 **sharepoint\_Azure\_pp** 3 years, 8 months ago

Key is correct

choose the same

cleared with 900 on 17th October 2021

upvoted 7 times

 **syu31svc** 3 years, 9 months ago

B for sure

upvoted 1 times

🗨️ 👤 **Gautam1985** 3 years, 10 months ago

correct

upvoted 1 times

🗨️ 👤 **tvS2021** 3 years, 11 months ago

this on exam (7-19-2021) . passed 304

upvoted 5 times

🗨️ 👤 **Amit3** 4 years ago

B is the only answer here, keys could be customer or Azure assigned in AKV.

upvoted 2 times

🗨️ 👤 **Prince2690** 4 years, 1 month ago

It requires key to be created in AKV.

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault>

upvoted 2 times

🗨️ 👤 **glam** 4 years, 5 months ago

B. a key

upvoted 4 times

🗨️ 👤 **David\_986969** 4 years, 9 months ago

Why not a secret that configures the key as the secret?

upvoted 1 times

🗨️ 👤 **KakashiHatake** 4 years, 8 months ago

Eventually, you are configuring a key only. B is correct.

upvoted 14 times

🗨️ 👤 **biboker766** 4 years, 5 months ago

with data disk secret may not work

upvoted 1 times

🗨️ 👤 **pentium75** 3 years, 10 months ago

I too was wondering if a key isn't considered a secret, but no, KV manages "secrets and keys" per MS documentation. Thus a key is not considered a "secret."

upvoted 1 times

You have data files in Azure Blob storage.

You plan to transform the files and move them to Azure Data Lake Storage.

You need to transform the data by using mapping data flow.

Which Azure service should you use?

- A. Azure Data Box Gateway
- B. Azure Storage Sync
- C. Azure Data Factory
- D. Azure Databricks

**Suggested Answer: C**

You can use Copy Activity in Azure Data Factory to copy data from and to Azure Data Lake Storage Gen2, and use Data Flow to transform data in Azure Data Lake Storage Gen2.

Reference:

<https://docs.microsoft.com/en-us/azure/data-factory/connector-azure-data-lake-storage>

Community vote distribution

C (100%)

  **razvi**  4 years, 9 months ago

C is correct.

<https://docs.microsoft.com/en-us/azure/data-factory/concepts-data-flow-overview#:~:text=Mapping%20data%20flows%20are%20visually%20designed%20data%20transformations,Factory%20pipelines%20that%20use%20scaled-out%20Apache%20Spark%20clusters.>

upvoted 34 times

  **folkmusic99**  4 years ago

Seems like Azure Data Factory is the new favorite for a lot of answers.

upvoted 28 times

  **GregoryGerard** 3 years, 9 months ago

Perhaps it is the most costly :-)

upvoted 7 times

  **examineezer** 3 years, 6 months ago

ADF is cheap generally speaking.

upvoted 2 times

  **Dawn7**  3 years, 3 months ago

**Selected Answer: C**

Always Data Factory 🙏

upvoted 3 times

  **syu31svc** 3 years, 8 months ago


C is the answer for sure

upvoted 3 times

  **Gautam1985** 3 years, 10 months ago

Correct

upvoted 2 times

  **glam** 4 years, 5 months ago

C. Azure Data Factory

upvoted 5 times

  **kopper2019** 4 years, 6 months ago

Data flow = Azure Data Factory

upvoted 9 times