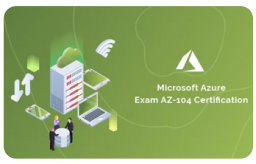


Level: Advanced

Microsoft Azure Exam AZ-104 Certification

← Back to the **Course**

Monitor and maintain Azure resources - **Practice Mode**

Completed on Sat, 04 Oct 2025

Attempt | Marks Obtained | Your Score | Result

Share this Report in Social Media Share

Download Report

Domain wise Quiz Performance Report

No.	Domain	Total Question	Correct	Incorrect	Unattempted	Marked for Review
1	Monitor and maintain Azure resources	14	9	5	0	0
Total	All Domains	14	9	5	0	0

Review the Answers

Filter By

Question 1

Correct

Domain: Monitor and maintain Azure resources

You configure an alert rule at the subscription scope that triggers on all administrative operations and uses an action group to send email notifications to admin@contoso.com. You also configure an alert processing rule that suppresses all notifications for the entire subscription from May 24, 2025, to May 27, 2025. If a new resource group is created in this subscription on May 25, 2025, will the notification email be sent? (Select Yes/No)

A. Yes

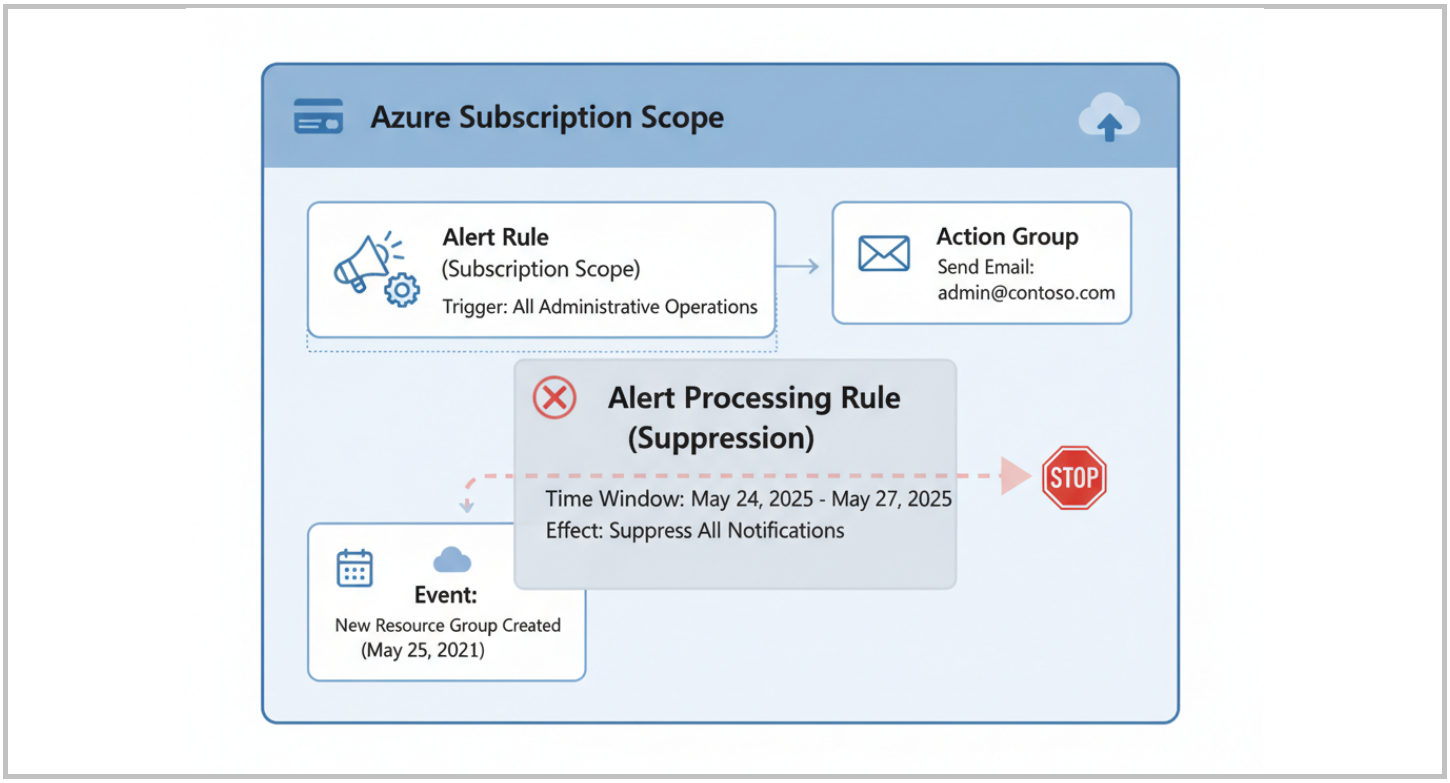
B. No right

Explanation:

Correct Answer: B

Option B: No is correct because the alert processing rule is actively in effect during the specified date range (May 24-27, 2025). Even though the underlying alert rule for administrative operations is triggered by the creation of a resource group, the alert processing rule's primary function is to suppress notifications. Therefore, the associated action group will not execute its email sending action during this window.

Option A: Yes is incorrect because the alert processing rule takes precedence over the alert rule's action within its defined scope and time period. The notification will be suppressed, preventing the email from being sent.



References:

https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-processing-rules?tabs=portal

https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-processing-rules?tabs=portal#what-should-this-rule-do

Ask our Experts

Did you like this **Question?**

Question 2

Correct

Domain: Monitor and maintain Azure resources

You have the same Azure Monitor configuration as in the previous question, including an alert rule for all administrative operations and an alert processing rule that suppresses notifications from May 24, 2025, to May 27, 2025. You add a tag to an existing resource group on May 29, 2025. Will you receive an email notification for this action? (Select Yes/No)

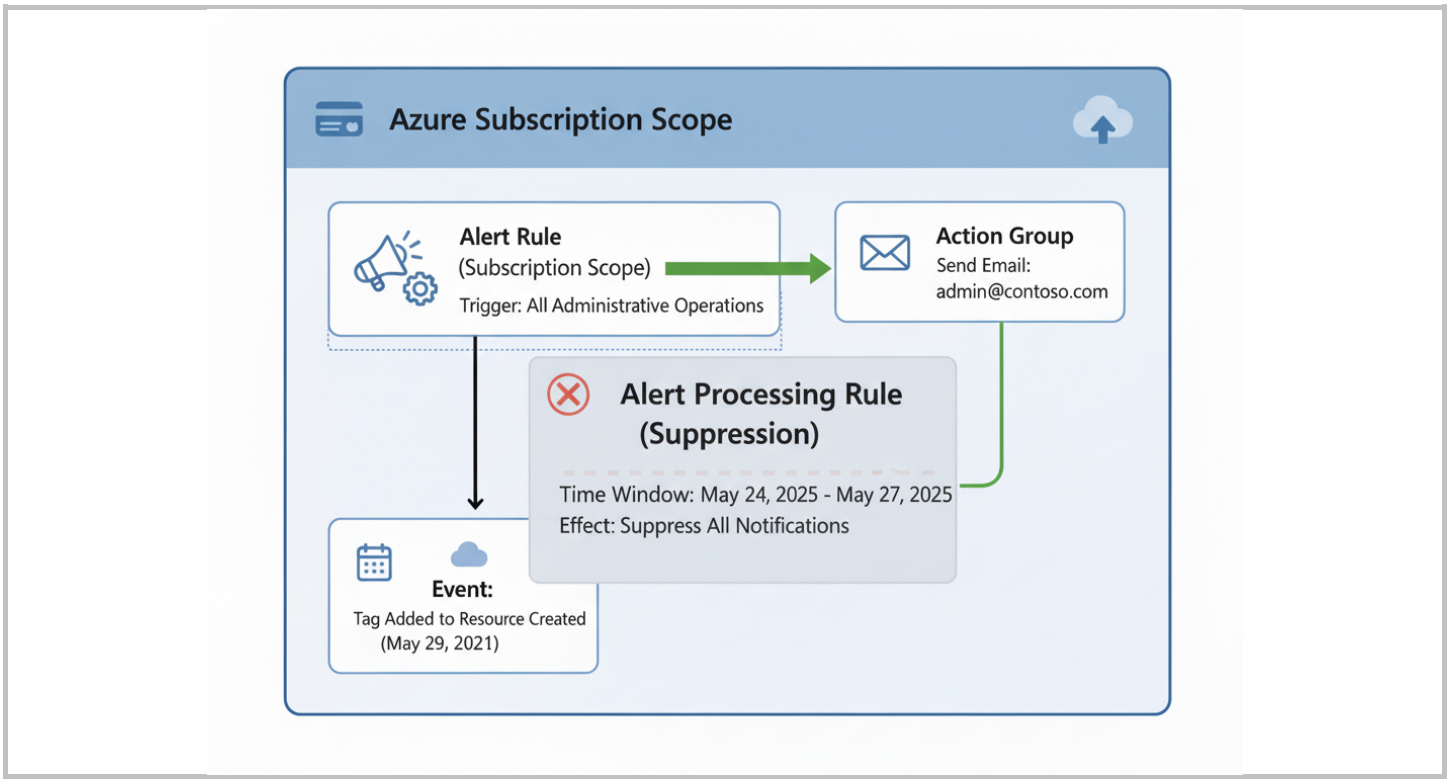
- A. Yes right
- B. No

Explanation:

Correct Answer: A

Option A: Yes is correct because the administrative action (adding a tag) is performed on May 29, 2025. This date falls outside the active period of the alert processing rule's suppression window (May 24-27, 2025). Therefore, the suppression rule no longer applies, and the alert rule for administrative operations will trigger its action group, successfully sending the email notification as expected.

Option B: No is incorrect because the alert processing rule's suppression period has ended. The alert will be processed and the notification sent.



References:

https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-processing-rules?tabs=portal

https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-processing-rules?tabs=portal#what-should-this-rule-do

Ask our Experts

Did you like this **Question?**

Question 3 Correct

Domain: Monitor and maintain Azure resources

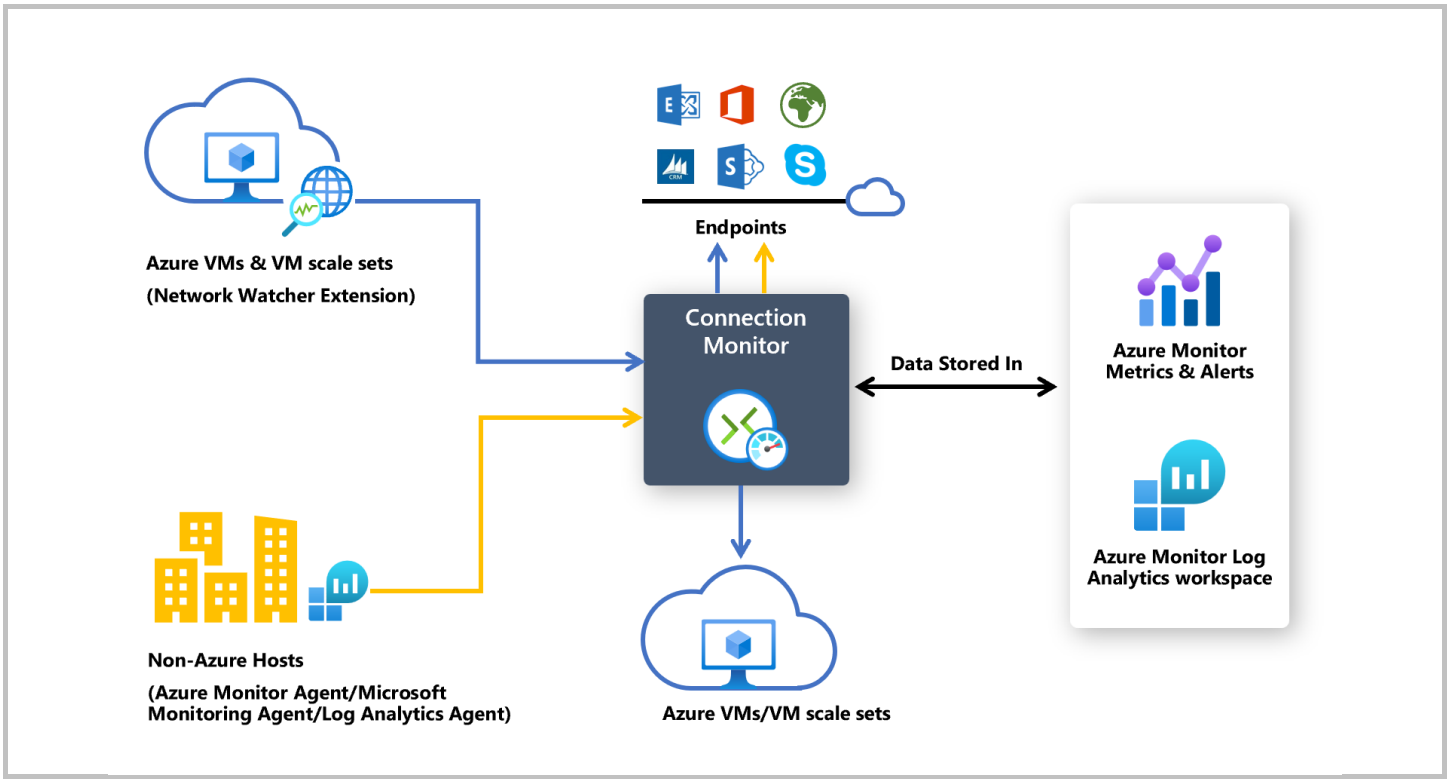
Your company's IT department needs to continuously monitor the network connectivity, latency, and availability between virtual machines belonging to different departments, which are located on separate subnets within an Azure Virtual Network. Which Azure Network Watcher feature should you recommend for this requirement?

- A. Connection Monitor right
- B. Network Security Group Flow Logs
- C. Network Topology
- D. Traffic Analytics

Explanation:

Correct Answer: A

Option A: Connection Monitor is correct because it is specifically designed for actively and continuously monitoring connectivity between endpoints, such as virtual machines, across Azure regions, subscriptions, or even on-premises. It provides rich data on network availability, latency, and packet loss, which directly addresses the need for continuous monitoring between VMs in different subnets.



Option B: Network Security Group Flow Logs are incorrect because - as they capture information about IP traffic flowing through an NSG (allowed or denied). While useful for security auditing and traffic analysis, they do not actively monitor or report on real-time connectivity status or performance between endpoints.

Option C: Network Topology is incorrect because this feature provides a graphical representation of your network resources and their relationships. It is a visualization tool for understanding network architecture but does not offer active, real-time monitoring of connectivity status or performance metrics.

Option D: Traffic Analytics is incorrect because it processes Network Watcher flow logs to provide insights into network traffic patterns. It's useful for identifying hotspots, security threats, and optimizing network performance at a macro level, but it does not offer the granular, active connectivity monitoring between specific VMs that Connection Monitor provides.

Reference:

Azure Network Watcher – Connection Monitor

Ask our Experts

Did you like this **Question?**

Question 4

Incorrect

Domain: Monitor and maintain Azure resources

You are tasked with configuring Azure Network Watcher's Connection Monitor for a new set of Azure Virtual Machines to assess their network performance and connectivity. What is the correct sequence of steps to configure Connection Monitor for a new

deployment?

Your Answer	Correct Answer
1. E. Enable Network Watcher in the relevant Azure region	1. E. Enable Network Watcher in the relevant Azure region
2. B. Create a Connection Monitor resource	2. B. Create a Connection Monitor resource
3. A. Configure the source and destination endpoints	3. D. Define the monitoring settings (e.g., test groups, protocols, frequency)
4. D. Define the monitoring settings (e.g., test groups, protocols, frequency)	4. A. Configure the source and destination endpoints
5. C. Review the monitoring results and performance metrics	5. C. Review the monitoring results and performance metrics

Explanation:

Correct Answers: E, B, D, A and C

The correct sequence for configuring Connection Monitor ensures that the foundational services are in place before defining specific monitoring tasks.

1. **Enable Network Watcher in the relevant Azure region.**
2. **Create a Connection Monitor resource.**
3. **Define the monitoring settings (e.g., test groups, protocols, frequency).**
4. **Configure the source and destination endpoints.**
5. **Review the monitoring results and performance metrics.**

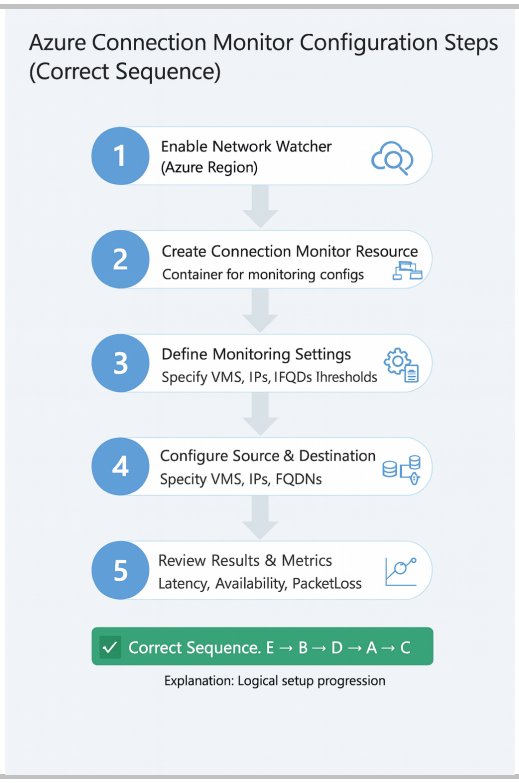
Step E: Enable Network Watcher in the relevant Azure region. This is the foundational first step. Network Watcher is a regional service, and it must be enabled in the Azure region(s) where your monitored resources reside before any of its features, including Connection Monitor, can be used.

Step B: Create a Connection Monitor resource. Once Network Watcher is enabled in the region, you create an instance of the Connection Monitor resource itself, which will house your monitoring configurations.

Step D: Define the monitoring settings (e.g., test groups, protocols, frequency). Within the Connection Monitor resource, you define how the monitoring will be performed. This includes specifying test groups, choosing protocols (TCP, ICMP), setting testing frequency, and configuring thresholds.

Step A: Configure the source and destination endpoints. Next, you identify the specific virtual machines or endpoints that will act as the sources (where the tests originate) and destinations (where the tests are directed).

Step C: Review the monitoring results and performance metrics. Once the Connection Monitor is fully set up and has begun collecting data, you can access its dashboard to review real-time and historical data on connectivity status, latency, and packet loss.



Reference:

https://learn.microsoft.com/en-us/azure/network-watcher/connection-monitor-create-using-portal

Ask our Experts

Did you like this **Question?**

Question 5

Correct

Domain: Monitor and maintain Azure resources

A company needs to gain comprehensive visibility into the operational health and performance bottlenecks of its Azure Virtual Machines and Virtual Machine Scale Sets. You are tasked with recommending a solution that provides detailed insights into resource utilization, active processes, and network dependencies. What is the primary purpose of Azure VM Insights?

A. To automate Azure virtual machine provisioning and lifecycle management

B. To monitor and analyze the performance, health, and dependencies of Azure VMs right

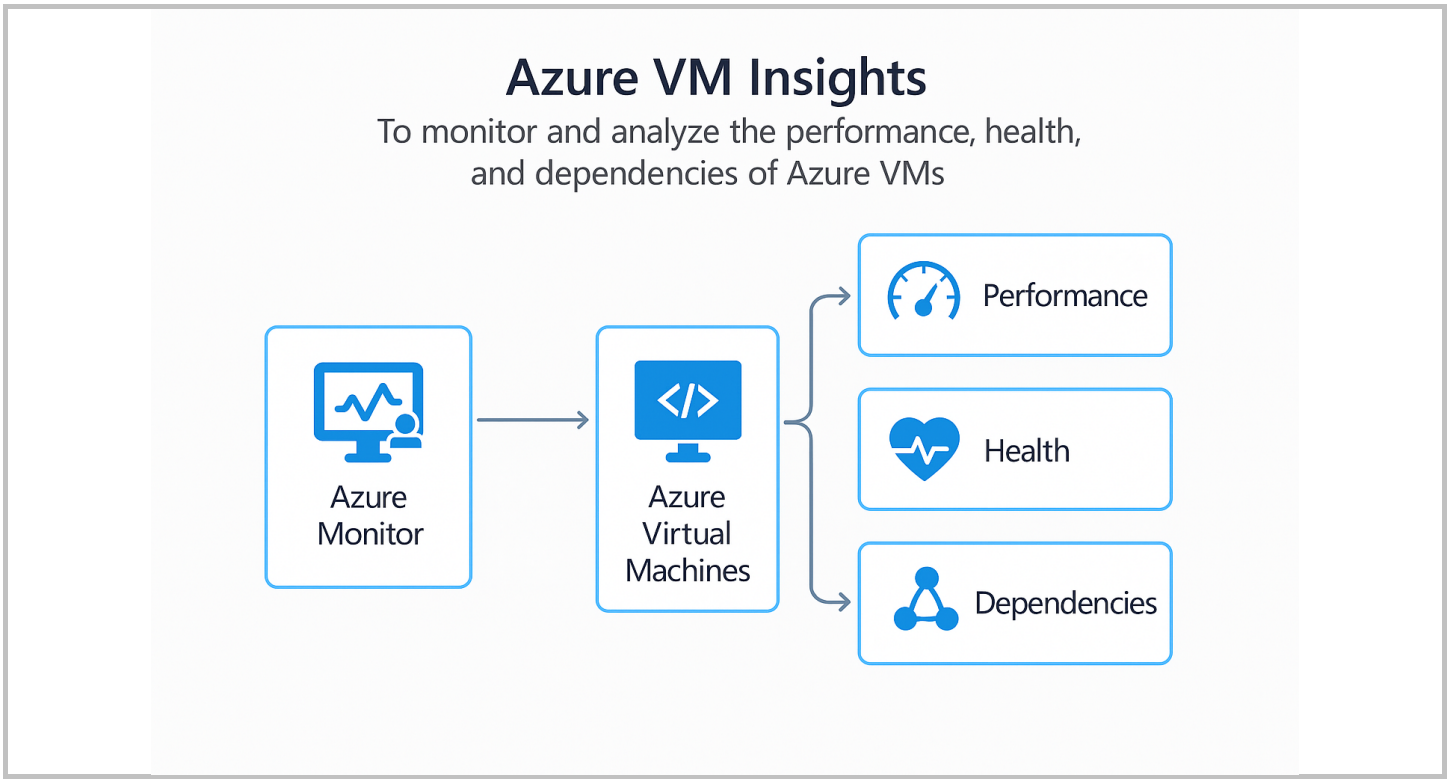
C. To configure and enforce security policies and compliance for Azure VMs

D. To create, manage, and optimize virtual networks for Azure VMs

Explanation:

Correct Answer: B

Option B: To monitor and analyze the performance, health, and dependencies of Azure VMs is correct because Azure VM Insights is a feature of Azure Monitor specifically designed to provide a comprehensive, unified solution for monitoring the performance, health, and application dependencies of Azure virtual machines and Virtual Machine Scale Sets. It collects metrics and logs, visualizes performance trends (CPU, memory, disk, network), and maps active processes and network connections to help identify and diagnose issues.



Option A: To automate Azure virtual machine provisioning and lifecycle management is incorrect because automation tasks are primarily handled by services like Azure Automation, Azure Resource Manager templates, or Azure DevOps, not Azure VM Insights. VM Insights is a monitoring tool.

Option C: To configure and enforce security policies and compliance for Azure VMs is incorrect because security policies and compliance are managed by services such as Microsoft Defender for Cloud and Azure Policy. VM Insights provides operational insights, not security posture management.

Option D: To create, manage, and optimize virtual networks for Azure VMs is incorrect because virtual network management is handled by the Azure Virtual Network service, Azure Load Balancer, and Network Watcher. VM Insights reports on network dependencies but does not manage the underlying network infrastructure.

Reference:

Azure VM Insights Overview

Ask our Experts

Did you like this **Question?**

Question 6 Correct

Domain: Monitor and maintain Azure resources

Your team needs a centralized tool within Azure Monitor to gain a consolidated view of the performance, capacity utilization, and overall availability status across all your Azure Storage accounts. This tool should offer proactive insights and facilitate quick identification of issues. Which of the following Azure Monitor features should you recommend?

A. Azure Log Analytics

B. Azure Activity Log

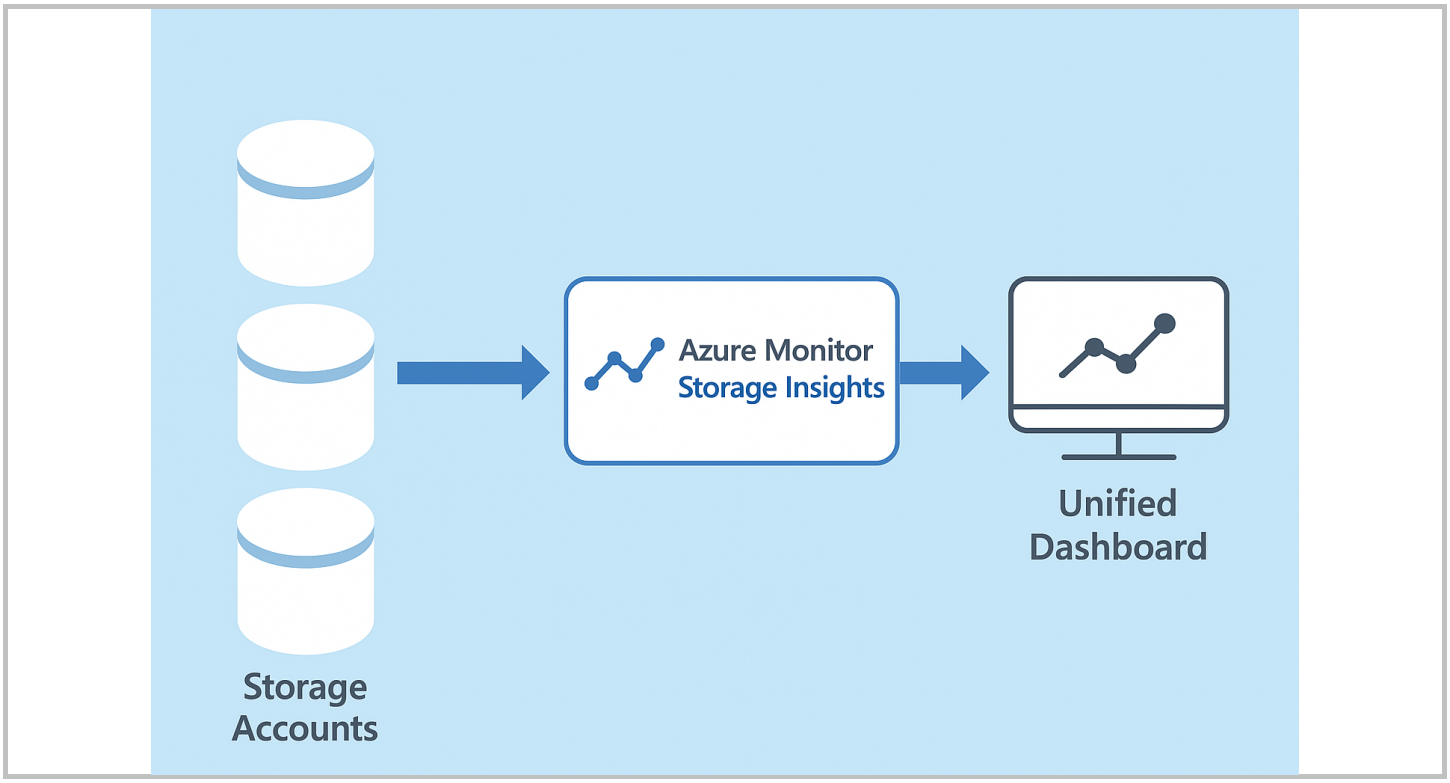
C. Azure Monitor Storage Insights right

D. Microsoft Defender for Cloud

Explanation:

Correct Answer: C

Option C: Azure Monitor Storage Insights is correct because it is a feature within Azure Monitor specifically tailored to provide a unified and centralized view of performance, capacity, and availability for all your Azure Storage accounts. It aggregates key metrics (e.g., transactions, latency, capacity usage) and presents them in pre-built dashboards, enabling quick identification of issues and proactive monitoring.



Option A: Azure Log Analytics is incorrect because while Azure Log Analytics is a powerful service for collecting and querying various types of log data (including some storage logs), it is a general-purpose logging solution. It does not natively provide the dedicated, unified dashboard for storage performance and capacity that Storage Insights offers without significant custom configuration.

Option B: Azure Activity Log is incorrect because the Azure Activity Log records resource-level control-plane operations (e.g., create, update, delete resources, role assignments). It is an audit log for "who did what, when," not a source for performance, capacity, or availability metrics of a running service like Azure Storage.

Option D: Microsoft Defender for Cloud is incorrect because Microsoft Defender for Cloud is focused on security posture management, vulnerability assessments, and threat protection across your Azure environment, including Storage accounts. While it provides security recommendations for storage, it is not designed to monitor operational metrics like performance, capacity, or availability.

Reference:

Azure Monitor Storage insights Overview

Ask our Experts

Did you like this **Question?**

Question 7 Correct

Domain: Monitor and maintain Azure resources

An IT operations team needs a tool within Azure Monitor that allows them to interactively explore and visualize numerical metric data

from various Azure resources. They require the ability to create custom charts, apply filters, and analyze performance trends over specific time ranges without writing complex queries. Which Azure Monitor tool should you suggest for this purpose?

A. Log Analytics

B. Metrics Explorer right

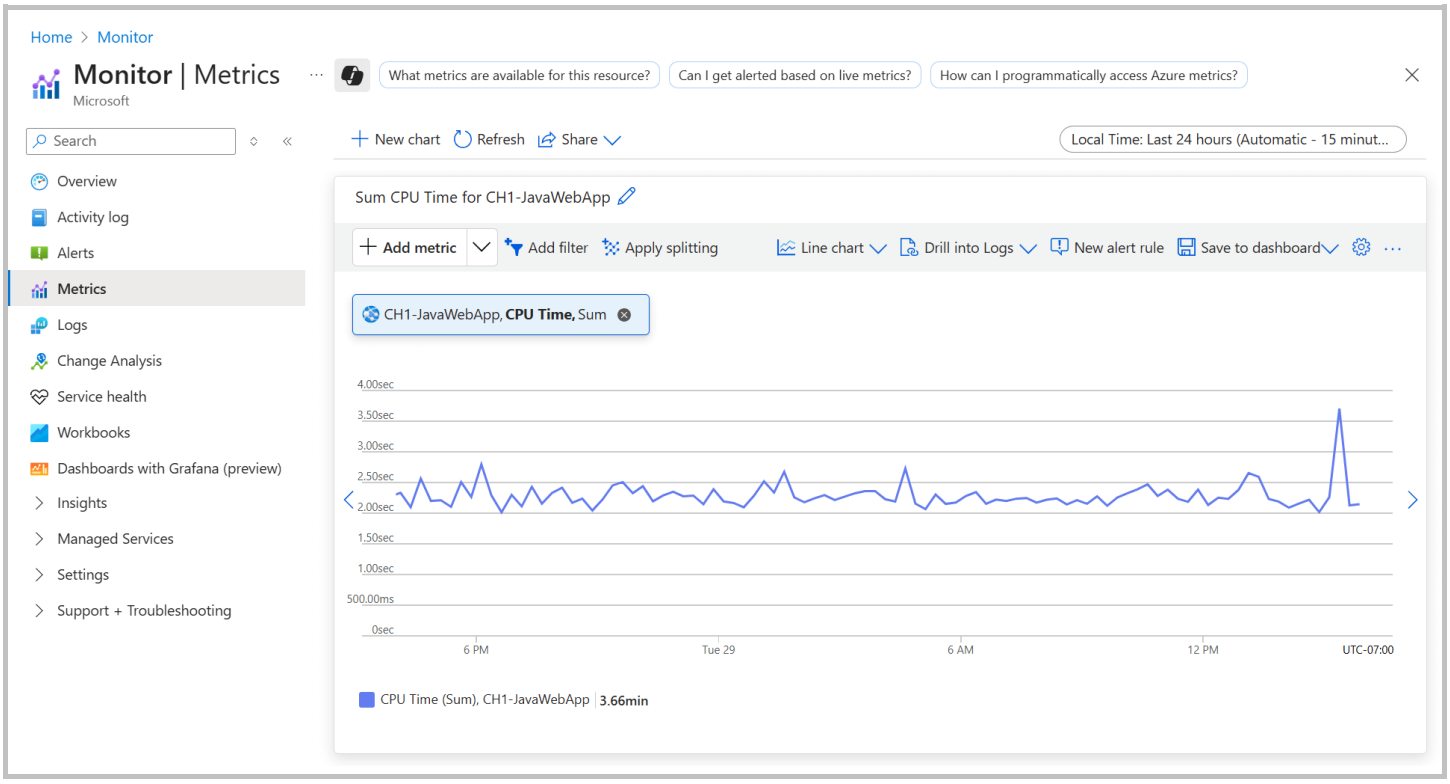
C. Application Insights

D. Azure Monitor Workbooks

Explanation:

Correct Answer: B

Option B: Metrics Explorer is correct because it is the dedicated tool within Azure Monitor for interactively analyzing and charting metric data. It provides a graphical interface to select metrics, apply aggregations, filters, and splits, and visualize the data in various chart types. This allows operations teams to easily monitor resource performance and diagnose issues by interacting directly with the metric data.



Option A: Log Analytics is incorrect because Log Analytics is primarily used for collecting, storing, and querying log data, using the Kusto Query Language (KQL). While some metrics can be ingested as logs, Metrics Explorer is the purpose-built tool for direct, interactive analysis of numerical metric data.

Option C: Application Insights is incorrect because Application Insights is an Application Performance Management (APM) service that specializes in monitoring live web applications. While it collects metrics, its focus is on application-specific performance, availability, and usage, rather than a general-purpose interactive metric exploration tool for all Azure resources.

Option D: Azure Monitor Workbooks is incorrect because Workbooks are flexible canvases for creating interactive reports and dashboards from various data sources (logs, metrics, alerts). While they can display metric charts, they are more about creating curated views rather than being the primary tool for interactive exploration and ad-hoc analysis of raw metric data.

Reference:

Get started with Azure Monitor Metrics Explorer

Ask our Experts

Did you like this **Question?**

Question 8 Correct

Domain: Monitor and maintain Azure resources

An Azure administrator receives an "Upcoming Purge" alert from Azure Backup for a SQL Server instance running on an Azure Virtual Machine. What does this alert indicate, and what is the appropriate immediate action the administrator should consider?

A. The alert indicates that backup data is nearing permanent deletion due to retention policy, and the administrator should review and potentially extend the retention policy right

B. The alert signifies that the SQL Server VM is running low on disk space, and the administrator should allocate more storage to the VM

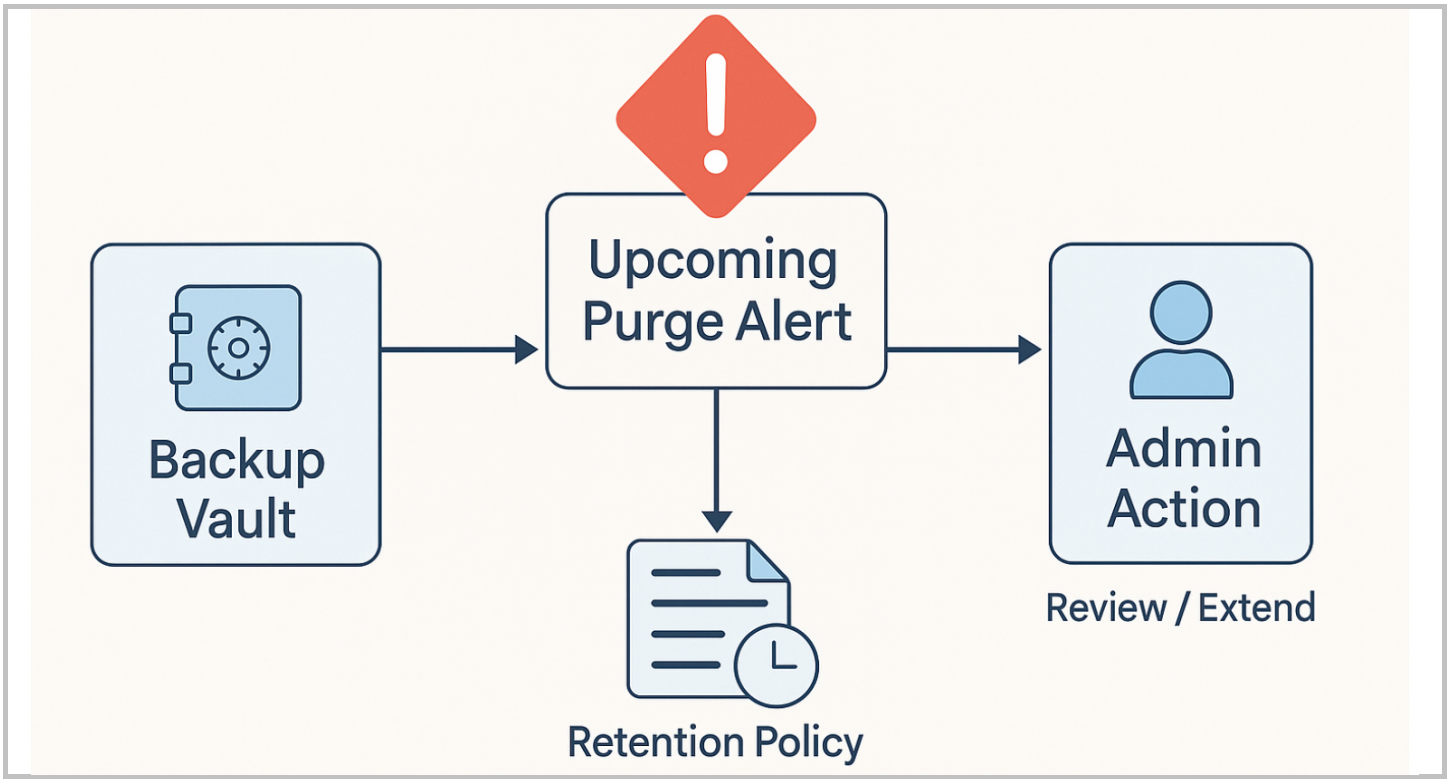
C. The alert warns of an upcoming planned Azure maintenance event for the SQL Server VM, and the administrator should schedule application downtime

D. The alert indicates a recent backup job failure for the SQL Server, and the administrator should investigate the cause of the failure

Explanation:

Correct Answer: A

Option A: The alert indicates that backup data is nearing permanent deletion due to retention policy, and the administrator should review and potentially extend the retention policy is correct because an "Upcoming Purge" alert from Azure Backup is a critical notification. It explicitly warns that one or more recovery points (backup data) for the specified protected item (the SQL Server VM in this case) are approaching the end of their defined retention period and will soon be permanently deleted. To prevent unintended data loss, the administrator's immediate and appropriate action is to review the existing backup retention policy and extend it if the data needs to be kept for a longer duration.



Option B: The alert signifies that the SQL Server VM is running low on disk space, and the administrator should allocate more storage to the VM is incorrect because this alert is generated by Azure Backup in relation to its retention policies for backup data, not in response to storage space issues on the actual virtual machine's operational disks. Disk space alerts would typically come from VM Insights or other monitoring tools.

Option C: The alert warns of an upcoming planned Azure maintenance event for the SQL Server VM, and the administrator should schedule application downtime is incorrect because this alert has no relation to Azure platform maintenance events. Azure Backup alerts are specific to backup operations and data lifecycle.

Option D: The alert indicates a recent backup job failure for the SQL Server, and the administrator should investigate the cause of the failure is incorrect because a backup job failure would trigger a distinct alert type (e.g., "Backup Job Failed"). The "Upcoming Purge" alert refers to the lifecycle management of existing backup data, not the success or failure of a new backup operation.

Reference:

Azure Backup Alerts

Ask our Experts

Did you like this **Question?**

Question 9 Incorrect

Domain: Monitor and maintain Azure resources

You are tasked with configuring Azure Backup for several existing Azure Virtual Machines within your subscription. You want to use the

Azure Backup Center for a streamlined workflow. What is the correct sequence of steps to configure these VMs for backup?

Your Answer	Correct Answer
1. C. Search and open the Backup Center in the Azure portal	1. C. Search and open the Backup Center in the Azure portal
2. A. Click on +Backup to initiate the backup configuration	2. B. Create or select an existing Recovery Services vault
3. D. Create or select an existing backup policy	3. A. Click on +Backup to initiate the backup configuration
4. B. Create or select an existing Recovery Services vault	4. D. Create or select an existing backup policy
5. E. Add the virtual machines to be protected	5. E. Add the virtual machines to be protected
6. F. Click on Enable backup to finalize	6. F. Click on Enable backup to finalize

Explanation:

Correct Answers: C, B, A, D, E and F

The correct sequence ensures that the necessary foundational resources (vault) and configurations (policy) are in place before enabling backup for the VMs.

C. Search and open the Backup Center in the Azure portal.

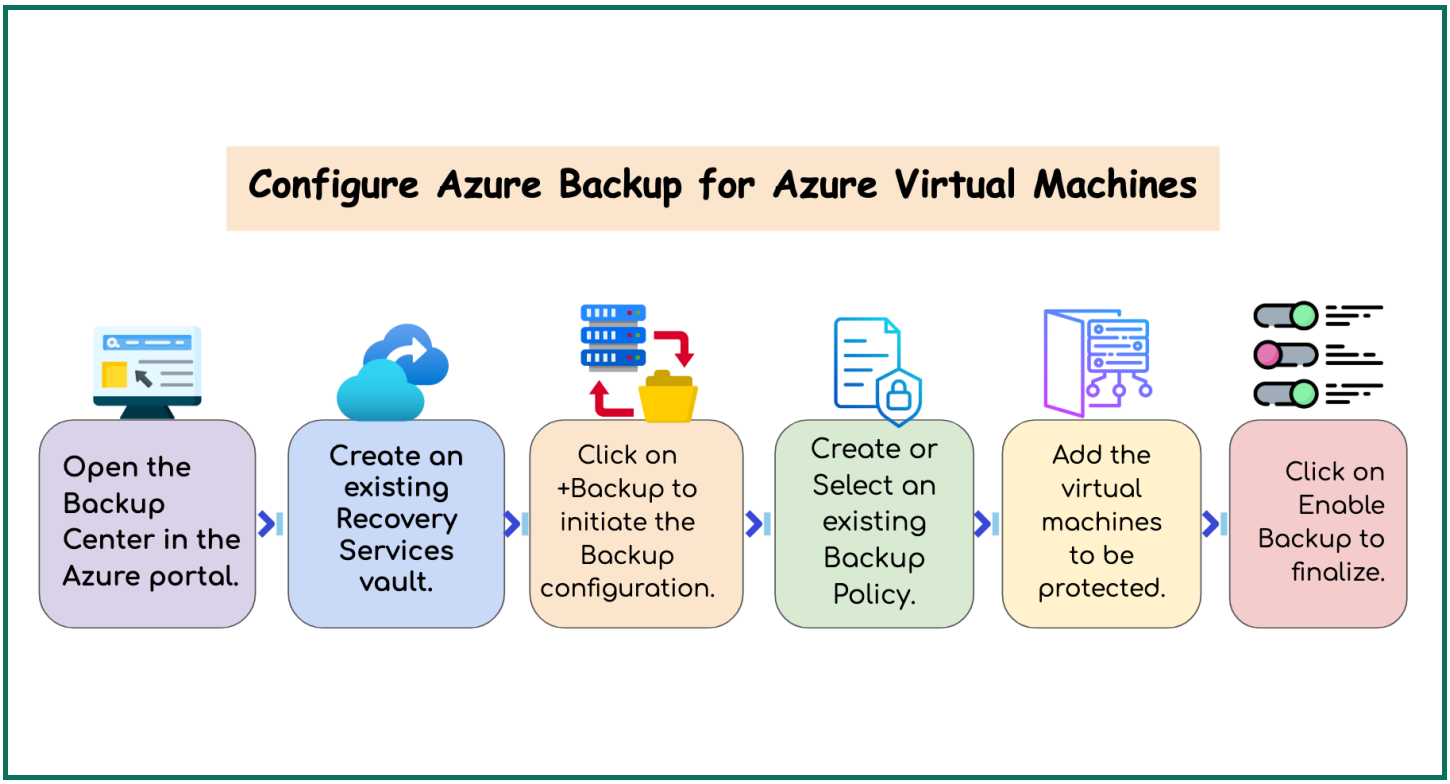
B. Create or select an existing Recovery Services vault.

A. Click on +Backup to initiate the backup configuration.

D. Create or select an existing backup policy.

E. Add the virtual machines to be protected.

F. Click on Enable backup to finalize.



Step C: Search and open the Backup Center in the Azure portal. For a streamlined experience across all backup activities, starting from the Azure Backup Center is the recommended approach as it provides a centralized management interface.

Step B: Create or select an existing Recovery Services vault. A Recovery Services vault is the fundamental storage and management entity required by Azure Backup. It must exist before you can configure any backup operations.

Step A: Click on +Backup to initiate the backup configuration. Within the Backup Center or a specific Recovery Services vault, you start the process of backing up new workloads by selecting the +Backup option.

Step D: Create or select an existing backup policy. A backup policy defines crucial settings like backup schedule (how often) and retention range (how long backups are kept). This must be defined before you can associate VMs with a backup configuration.

Step E: Add the virtual machines to be protected. After a policy is defined, you then select the specific Azure Virtual Machines that you wish to associate with this backup policy.

Step F: Click on Enable backup to finalize. This final action confirms your selections, links the chosen VMs to the policy within the Recovery Services vault, and initiates the first backup job according to the policy's schedule.

References:

https://learn.microsoft.com/en-us/azure/backup/backup-center-overview

https://learn.microsoft.com/en-us/azure/backup/backup-azure-vms-introduction

https://learn.microsoft.com/en-us/azure/backup/quick-backup-vm-portal

Ask our Experts

Did you like this **Question?**

Question 10 Incorrect

Domain: Monitor and maintain Azure resources

Your company uses various Azure services and needs to implement a robust backup strategy. You are responsible for choosing the appropriate vault type for different workloads.

For each of the following Azure services, identify whether you would choose a Recovery Services vault or a Backup vault for its backup solution:

Azure Database for PostgreSQL servers

SQL Server running in an Azure VM

Azure Files shares

A. Backup vault, Recovery Services vault, Recovery Services vault right

B. High Availability & Disaster Recovery (HADR)

C. Backup vault only wrong

D. Recovery Services vault only

Explanation:

Correct Answer: A

Correct Assignments:

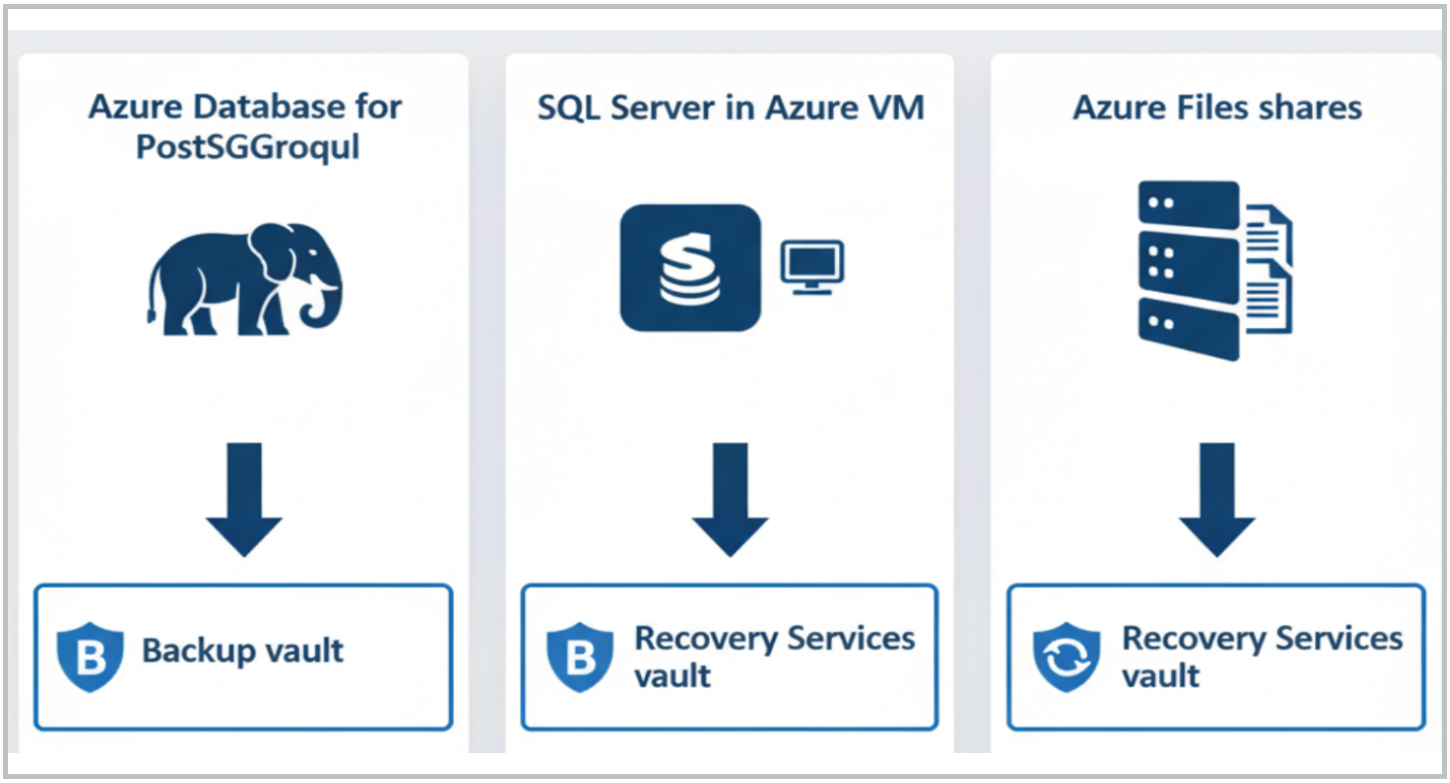
1. **Azure Database for PostgreSQL servers: Backup vault**
2. **SQL Server running in an Azure VM: Recovery Services vault**
3. **Azure Files shares: Recovery Services vault**

Azure has two primary vault types for backup: Recovery Services vaults and Backup vaults, each supporting different workloads, though some overlap exists. Backup vaults are generally newer and designed for specific modern PaaS workloads.

Azure Database for PostgreSQL servers → Backup vault: Backup vault is the correct choice because the Backup vault is the recommended and supported vault type for backing up Azure Database for PostgreSQL servers (Flexible and Single Server). It provides enhanced capabilities for these PaaS databases.

SQL Server in Azure VM → Recovery Services vault: The Recovery Services vault is the correct choice because it is the established and supported vault type for protecting SQL Server instances running inside Azure Virtual Machines (IaaS SQL).

Azure Files shares → Recovery Services vault: The Recovery Services vault is the correct choice because it is the supported vault type for backing up Azure file shares (both standard and premium).



Option B: High Availability & Disaster Recovery (HADR) is incorrect because HADR refers to a strategy or set of technologies (like Always On Availability Groups, failover clusters, or geo-replication) for ensuring continuous operation and data accessibility, not a type of backup vault. While backup is a component of a comprehensive HADR plan, HADR itself is not an Azure Backup vault type. This option is a distractor that falls into a different category of Azure services.

Option C: Backup vault only is incorrect because this option implies that all three specified services (Azure Database for PostgreSQL servers, SQL Server running in an Azure VM, and Azure Files shares) would use only a Backup vault. While Azure Database for PostgreSQL servers indeed uses a Backup vault, SQL Server running in an Azure VM and Azure Files shares both use a Recovery Services vault. Therefore, this option is incomplete and inaccurate for the entire list.

Option D: Recovery Services vault only is incorrect because this option implies that all three specified services would use only a Recovery Services vault. While SQL Server running in an Azure VM and Azure Files shares do use a Recovery Services vault, Azure Database for PostgreSQL servers uses a Backup vault. Therefore, this option is also incomplete and inaccurate for the entire list.

References:

https://learn.microsoft.com/en-us/azure/backup/backup-vault-overview

https://learn.microsoft.com/en-us/azure/backup/quick-backup-azure-files-vault-tier-portal

Ask our Experts

Did you like this **Question?**

Question 11 Correct

Domain: Monitor and maintain Azure resources

An international IT company is experiencing budget overruns on its Azure subscriptions and needs to set up proactive alerts within Azure Cost Management to gain better visibility and control over spending. Which of the following alert types is NOT a native, built-in alert capability directly configurable within Azure Cost Management?

A. Budget alert

B. Credit alert

C. Department spending quota alert right

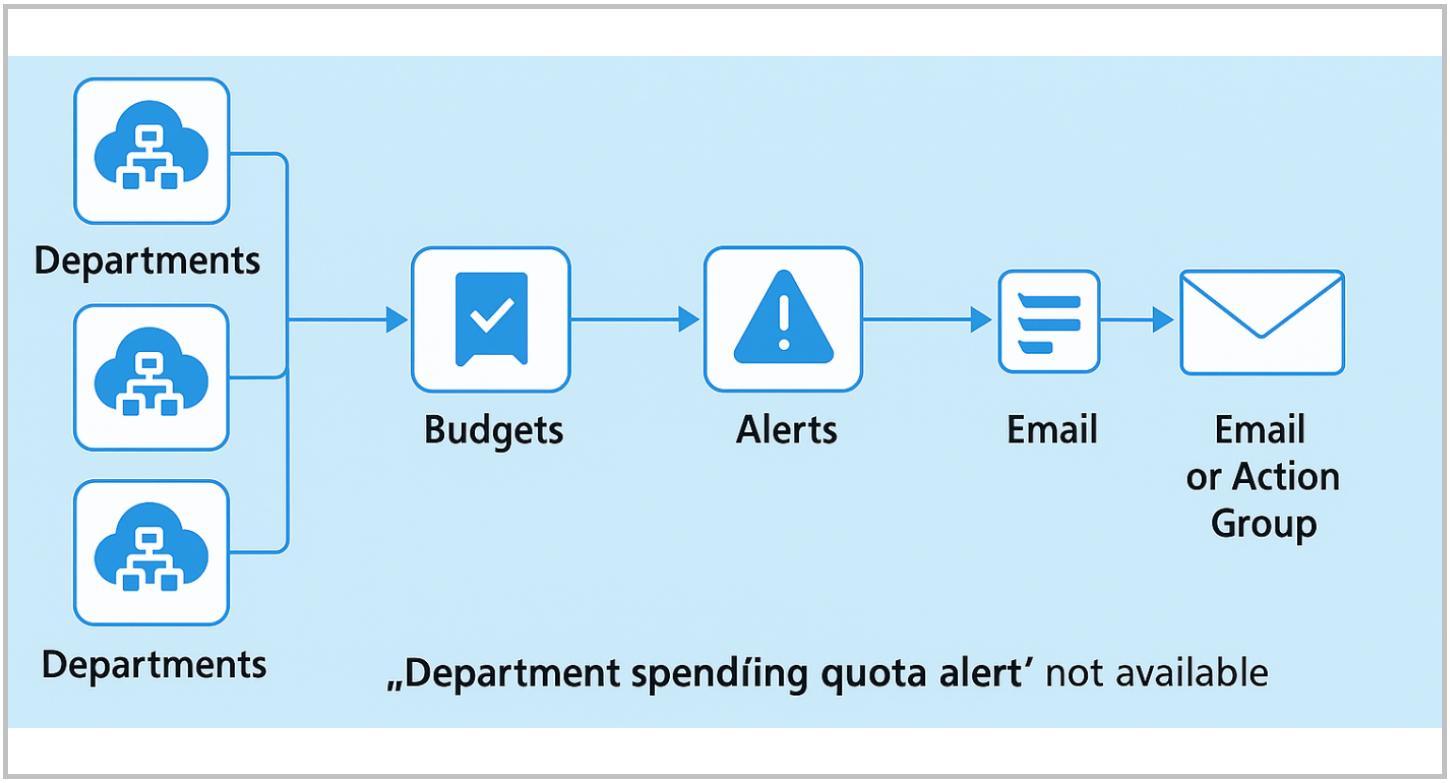
D. Forecast alert

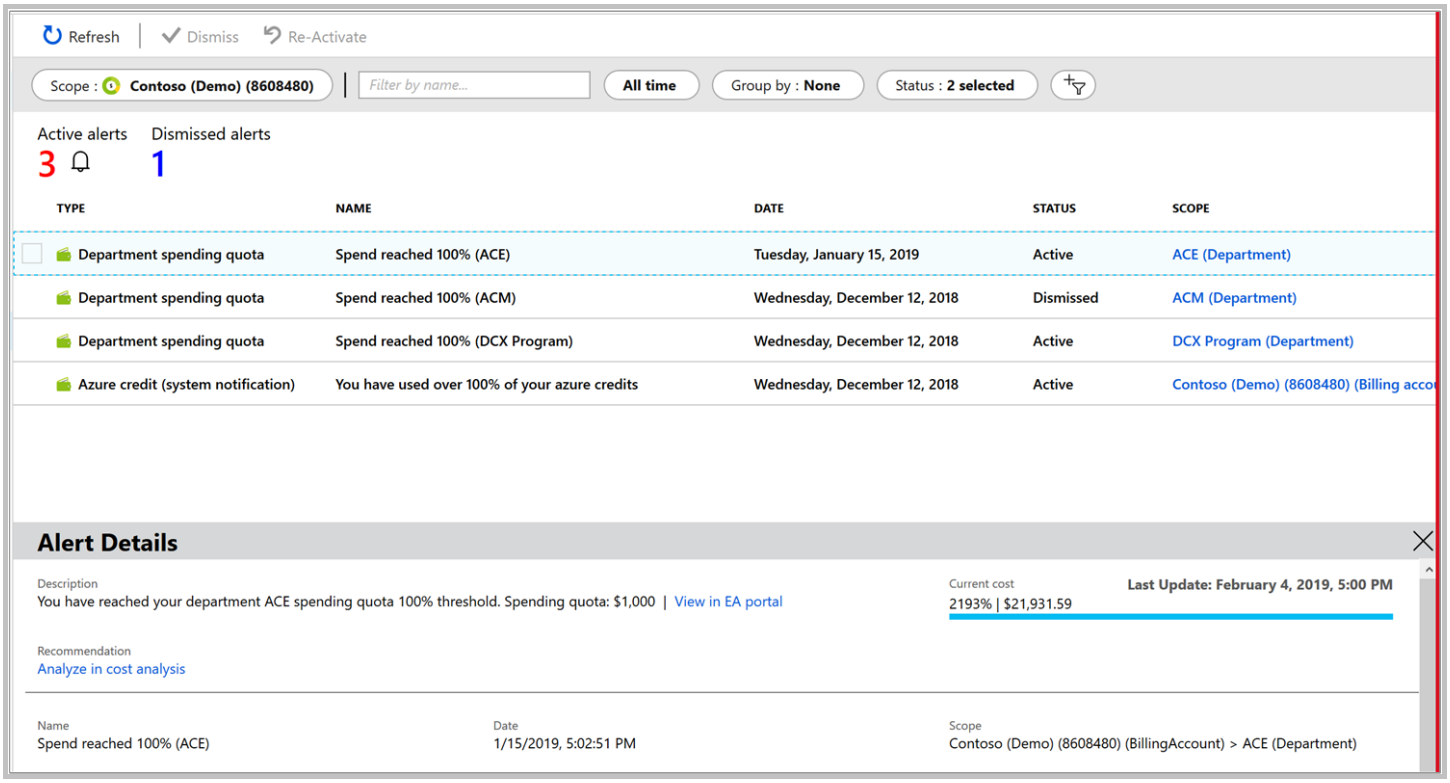
Explanation:

Correct Answer: C

Azure Cost Management provides several built-in alert types to help organizations manage and control their spending.

Option C: Department spending quota alert is correct because "department spending quota alert" is not a native, built-in alert type directly available in Azure Cost Management. While you can implement department-level cost tracking using management groups, resource groups, and tags, and then apply budgets to those scopes, there isn't a specific, predefined alert type called "department spending quota." You would typically use a standard budget alert applied to the scope representing the department.





Option A: Budget alert is incorrect because budget alerts are a core, built-in feature of Azure Cost Management. They allow you to set spending thresholds (actual or forecasted) for a subscription, resource group, or management group and receive notifications when these thresholds are met or exceeded.

Option B: Credit alert is incorrect because credit alerts are automatically generated by Azure to notify you when your Azure Prepayment (formerly monetary commitment) credit balance is being consumed or is nearing depletion. This is a crucial built-in alert for customers with enterprise agreements.

Option D: Forecast alert is incorrect because forecast alerts are a native feature within Azure Cost Management. These alerts use machine learning to analyze historical spending patterns and predict future costs, notifying you if your forecasted spending is projected to exceed a specified budget or threshold.

References:

https://learn.microsoft.com/en-us/azure/cost-management-billing/costs/cost-mgt-alerts-monitor-usage-spending

https://learn.microsoft.com/en-us/azure/cost-management-billing/costs/overview-cost-management

Ask our Experts

Did you like this **Question?**

Question 12 Incorrect

Domain: Monitor and maintain Azure resources

An international IT company has deployed 200 Windows and Linux virtual machines in Azure. They plan to roll out Azure VM Insights on all of them to centralize performance and health monitoring. Which three of the following are essential prerequisites for successfully enabling Azure VM Insights on these virtual machines? (Select 3)

Your Answer

B. An active Log Analytics workspace linked to the subscription

A. A direct connection from the virtual machine to the Azure Instance Metadata Service (IMDS) endpoint (169.254.169.254)

C. Global Administrator in Microsoft Entra ID for the user performing the setup

Correct Answer

A. A direct connection from the virtual machine to the Azure Instance Metadata Service (IMDS) endpoint (169.254.169.254)

B. An active Log Analytics workspace linked to the subscription

D. The Dependency Agent installed on the virtual machines

Explanation:

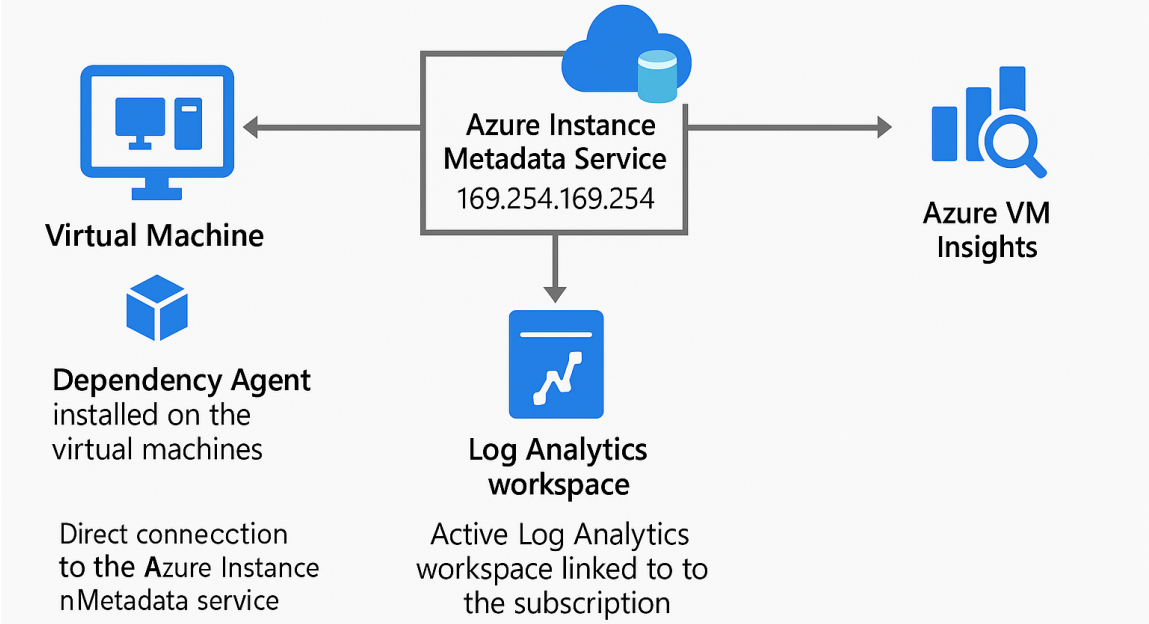
Correct Answers: A, B and D

Azure VM Insights relies on specific agents and services to collect and process performance and dependency data from your virtual machines.

Option A: A direct connection from the virtual machine to the Azure Instance Metadata Service (IMDS) endpoint (169.254.169.254) is correct because the Dependency Agent, which is crucial for VM Insights' mapping functionality, requires access to the Azure IMDS endpoint. This endpoint provides crucial metadata about the VM to the agent.

Option B: An active Log Analytics workspace linked to the subscription is correct because Azure VM Insights uses a Log Analytics workspace as its backend data store. All performance metrics, process data, and dependency information collected by the monitoring agents are sent to this workspace for storage, analysis, and visualization. You must have a configured workspace before you can onboard VMs.

Option D: The Dependency Agent installed on the virtual machines is correct because for the "Maps" feature of VM Insights (which visualizes processes and network dependencies) to function, the Dependency Agent must be installed on the virtual machines. This agent collects data about running processes and active network connections.



Option C: Global Administrator in Microsoft Entra ID rights for the user performing the setup is incorrect because Global Administrator rights are very high-level administrative permissions in Microsoft Entra and are typically not required to configure Azure VM Insights. The necessary permissions are usually at the subscription or resource group level (e.g., Log Analytics Contributor, Monitoring Contributor roles).

Option E: A separate, dedicated network subnet for VM Insights agents is incorrect because VM Insights agents (Log Analytics agent and Dependency agent) communicate over the existing virtual machine's network interface. They do not require a separate or dedicated network subnet for their operation.

References:

https://learn.microsoft.com/en-us/azure/virtual-machines/instance-metadata-service?tabs=windows

https://learn.microsoft.com/en-us/azure/azure-monitor/vm/vminsights-enable-overview

Ask our Experts

Did you like this **Question?**

Question 13 Incorrect

Domain: Monitor and maintain Azure resources

A company has 100 on-premises virtual machines protected by Azure Site Recovery for their business continuity plan. Due to a major network outage at the on-premises head office, all connectivity to the local data center is lost, requiring a disaster recovery failover. What is the correct sequence of steps an administrator would take to perform a planned failover of these systems to the Azure cloud?

Your Answer	Correct Answer
1. D. Choose the appropriate recovery point & ensure the on-premises source server is shut down	1. C. Navigate to the Recovery Services Vault and select Replicated items
2. C. Navigate to the Recovery Services Vault and select Replicated items	2. A. Select the Virtual Machine to fail over and click on Failover
3. A. Select the Virtual Machine to fail over and click on Failover	3. D. Choose the appropriate recovery point & ensure the on-premises source server is shut down
4. B. Commit the failover operation	4. B. Commit the failover operation

Explanation:

Correct Answers: C, A, D and B

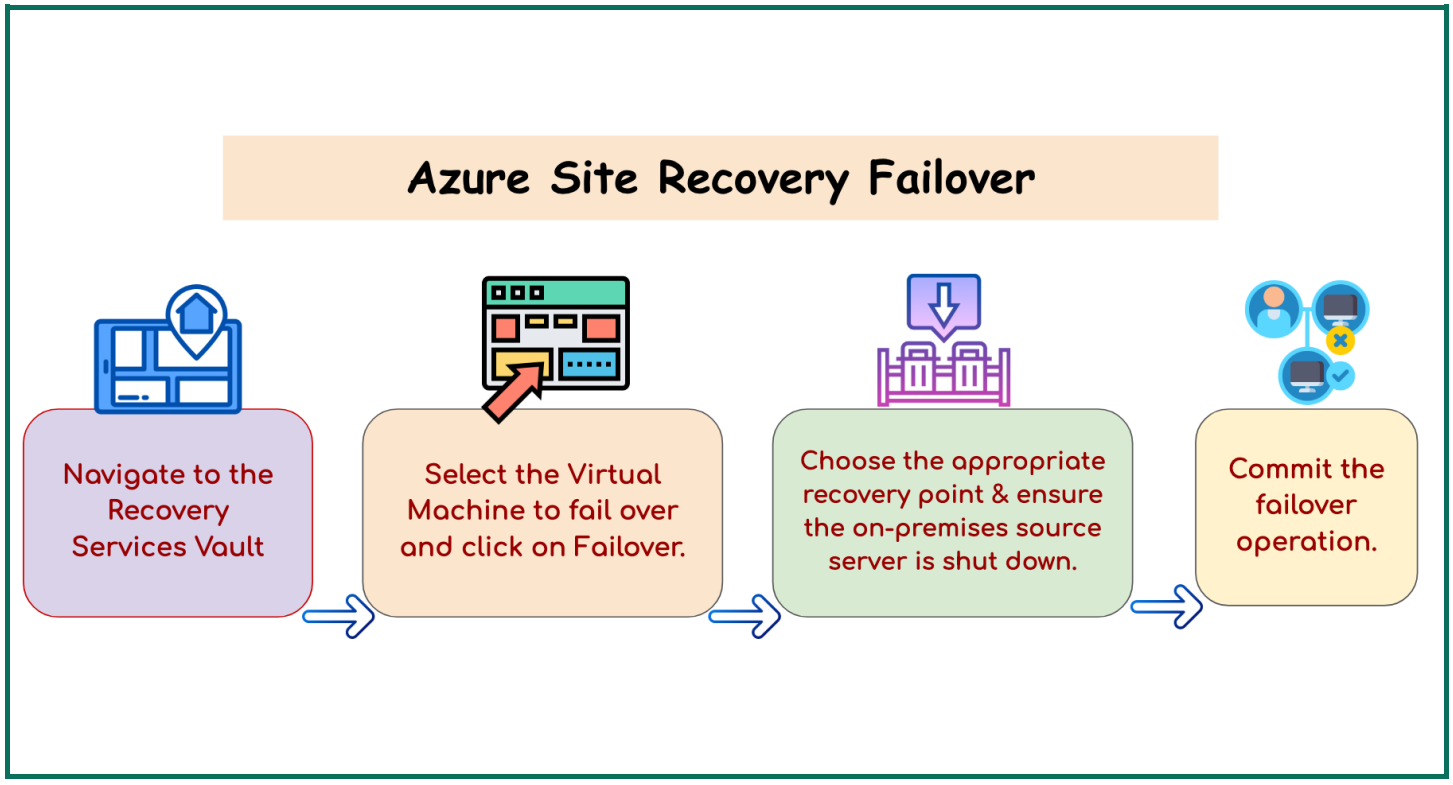
Performing a failover in Azure Site Recovery involves a specific sequence of actions to ensure data integrity and successful migration of workload operations to Azure.

C. Navigate to the Recovery Services Vault and select Replicated items.

A. Select the Virtual Machine to fail over and click on Failover.

D. Choose the appropriate recovery point & ensure the on-premises source server is shut down.

B. Commit the failover operation



Step C: Navigate to the Recovery Services Vault and select Replicated items. This is the initial step to access the management

interface for your protected on-premises machines. All replicated items are managed within the Recovery Services vault.

Step A: Select the VM(s) to fail over and click on Failover. Once you've located the replicated items, you select the specific virtual machine(s) you wish to fail over to Azure and initiate the failover process.

Step D: Choose the appropriate recovery point and ensure the on-premises source server is shut down. During the failover wizard, you will be prompted to select a specific recovery point (e.g., latest, application-consistent) to restore the VM from. Critically, to prevent data consistency issues (split-brain scenarios), it is essential to ensure that the on-premises source server corresponding to the VM being failed over is shut down before or during this step.

Step B: Commit the failover operation. After the virtual machine has successfully failed over to Azure and you have thoroughly verified that it is running and accessible as expected (e.g., applications are working), you must perform a Commit action. Committing the failover makes the recovery point permanent and deletes all older recovery points. This is the final step in solidifying the failover.

References:

https://learn.microsoft.com/en-us/azure/site-recovery/azure-to-azure-tutorial-failover-failback

https://learn.microsoft.com/en-us/azure/site-recovery/site-recovery-test-failover-to-azure

Ask our Experts

Did you like this **Question?**

Question 14

Correct

Domain: Monitor and maintain Azure resources

A company runs a public-facing website on three Azure Virtual Machines (VMs) located behind an Azure Load Balancer. The website experiences significant traffic spikes over weekends, leading to performance degradation. The company's primary goals are to reduce cloud hosting costs during off-peak hours and maintain high availability and performance during peak traffic times without manual intervention. Azure Advisor has provided recommendations related to cost optimization and operational excellence. Which two of the following solutions are the most cost-effective and scalable approaches to address this usage pattern? (Select 2)

A. Manually change the VM series to a more powerful one during peak times

B. Manually resize the existing VMs to a larger size to accommodate peak traffic

- [x] C. Deploy the website application to an Azure Virtual Machine Scale Set right
- [x] D. Migrate the website application to Azure App Service right

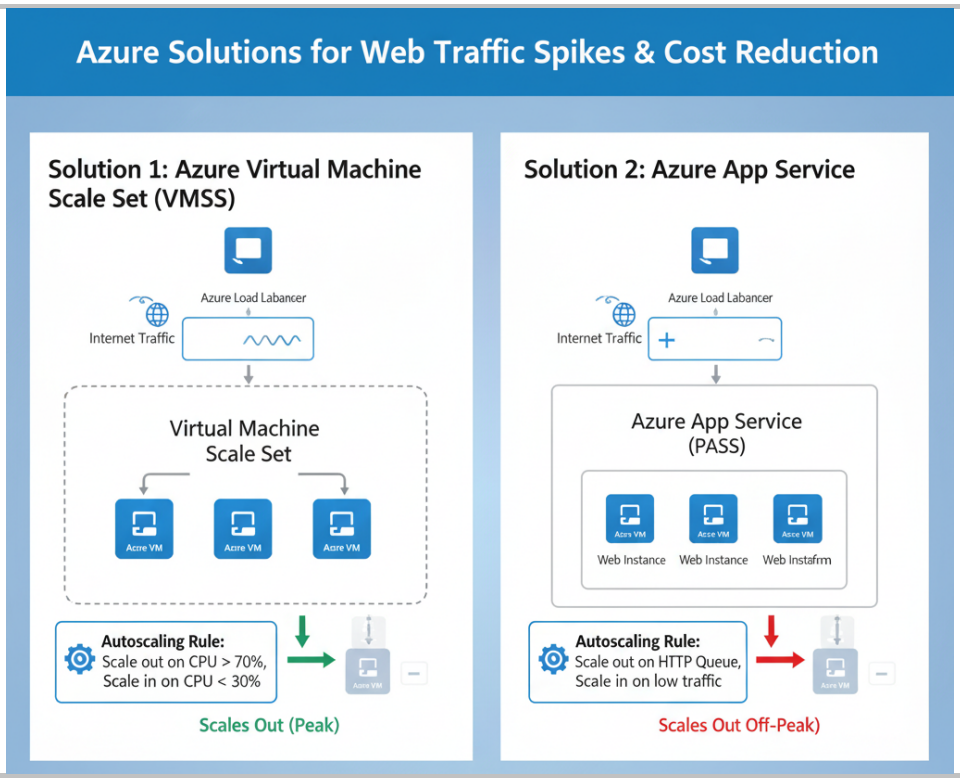
Explanation:

Correct Answers: C and D

The core requirements are cost-effectiveness (reducing costs during off-peak) and scalability (handling peak traffic without manual intervention). Solutions that offer automatic scaling are best suited for this.

Option C: Deploy the website application to an Azure Virtual Machine Scale Set is correct because Azure Virtual Machine Scale Sets are designed for deploying and managing a group of identical, load-balanced VMs. They inherently support autoscaling, meaning new VM instances can be automatically added when traffic increases (scaling out) and removed when traffic decreases (scaling in). This directly addresses both cost-effectiveness (only pay for what's needed) and automatic scalability for fluctuating demand.

Option D: Migrate the website application to Azure App Service is correct because Azure App Service is a Platform-as-a-Service (PaaS) offering that provides a fully managed environment for hosting web applications. App Service has built-in autoscaling capabilities that can automatically adjust the number of instances based on traffic or predefined schedules. This is highly cost-effective as you pay only for the compute resources consumed, and it significantly reduces operational overhead, further contributing to cost savings and increased scalability.



Option A: Manually change the VM series to a more powerful one during peak times is incorrect because this is a manual operation, which goes against the "without manual intervention" requirement. It also involves downtime to change VM sizes and would not be cost-effective if not scaled back down, leading to over-provisioning during off-peak hours.

Option B: Manually resize the existing VMs to a larger size to accommodate peak traffic is incorrect because this is also a manual operation and suffers from the same drawbacks as changing VM series. Resizing to a larger size permanently would lead to increased costs during off-peak hours, and manually resizing up and down introduces operational burden and potential downtime. It does not provide the dynamic, automatic scalability needed.

References:

https://learn.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-deploy-app

https://learn.microsoft.com/en-us/dotnet/azure/migration/app-service

Ask our Experts

Did you like this **Question?**

Finish Review