Level: Advanced

Microsoft Azure Exam AZ-104 Certification

← Back to the **Course**

Azure Backup and Recovery - **Practice Mode**

Completed on Sat, 18 Oct 2025

1st	1/5	20.00%	FAIL
Attempt	Marks Obtained	Your Score	Result

Download Report

Domain wise Quiz Performance Report

No.	Domain	Total Question	Correct	Incorrect	Unattempted	Marked for Review
1	Monitor and maintain Azure resources	5	1	4	0	0
Total	All Domains	5	1	4	0	0

Review the Answers

Filter By

Question 1 Incorrect

Domain: Monitor and maintain Azure resources

View Case Study

You are tasked with creating a Recovery Services vault in the East US region and configuring it to back up an existing Windows virtual machine named TestVM1. You need to ensure the vault is created under the existing resource group FabrikamRG and is named FabrikamBackupVault. Once the vault is created, validate its configuration for backup. Arrange the steps in the correct order.

Note: To achieve the above requirement drag the correct options and then drop them in the correct order into the answer area

Your Answer	Correct Answer
1. F. Navigate to the Azure portal and select "Create a resource"	1. F. Navigate to the Azure portal and select "Create a resource"
2. C. Choose the subscription and resource group FabrikamRG	2. E. Search for and select "Recovery Services vault"
3. B. Select the region as East US	3. C. Choose the subscription and resource group FabrikamRG
4. D. Specify the vault name as FabrikamBackupVault	4. D. Specify the vault name as FabrikamBackupVault
5. A. Click "Review + Create", then click "Create"	5. B. Select the region as East US
6. E. Search for and select "Recovery Services vault"	6. A. Click "Review + Create", then click "Create"

Explanation:

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

Navigate to the Azure portal and select "Create a resource": You start by logging into the Azure portal. Once logged in, click on the "Create a resource" option available on the home page or the left-hand menu. This action is the entry point for provisioning any new resource in Azure. By selecting this, you access the Azure Marketplace where various resource types can be searched and deployed.

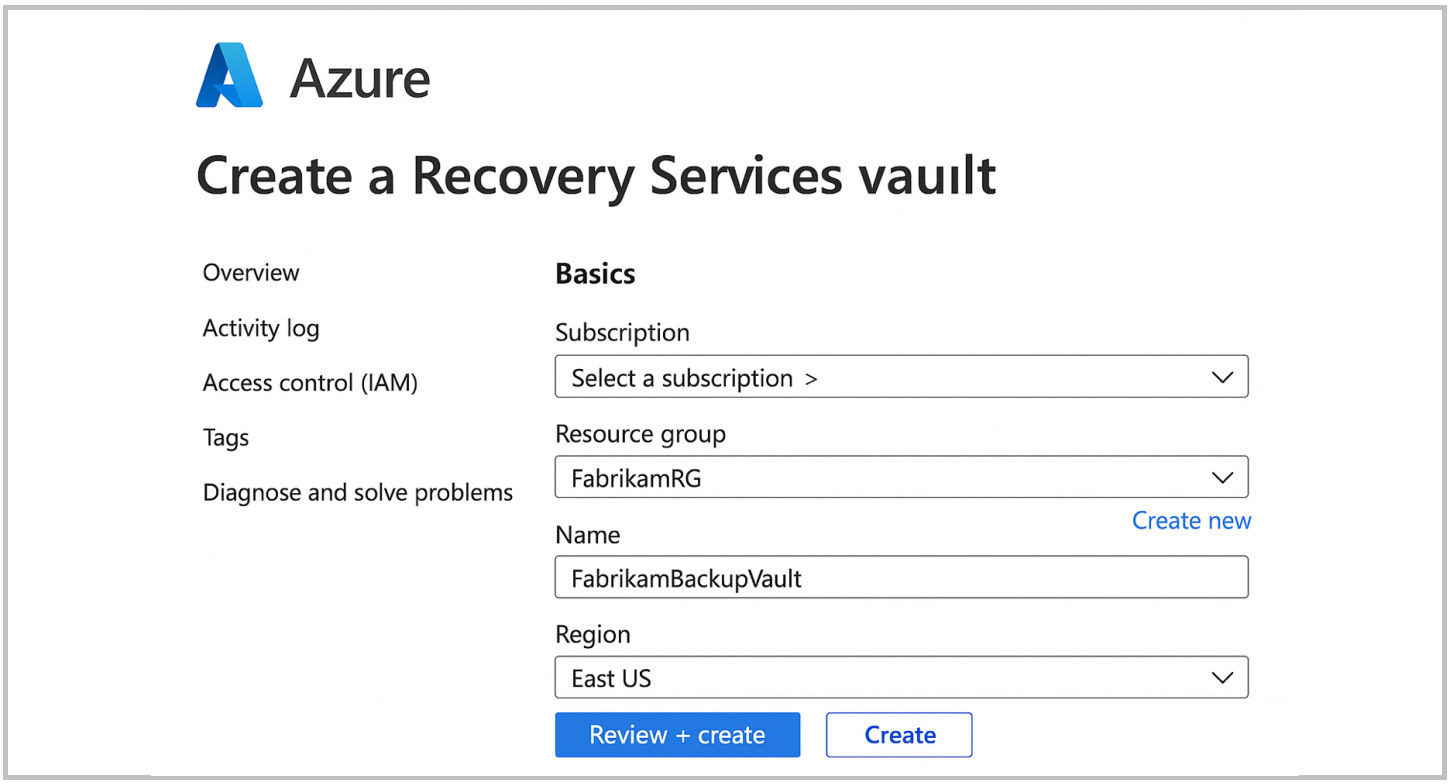
Search for and select "Recovery Services vault": In the Marketplace search bar, type "Recovery Services vault" and select it from the list of results. The Recovery Services vault is a specialized Azure resource designed to manage and store backup data for VMs, databases, and other workloads. Selecting it opens the vault creation page where you configure its details.

Choose the subscription and resource group FabrikamRG: Once the Recovery Services vault creation page opens, select the subscription under which the resource will be billed. Then, choose the resource group where the vault will be created. In this case, select the pre-existing resource group FabrikamRG. Resource groups help organize and manage related resources.

Specify the vault name as FabrikamBackupVault: Enter a unique name for the Recovery Services vault in the name field, such as FabrikamBackupVault. This name will be used to identify the vault in your Azure environment and should reflect its purpose, making it easy to distinguish from other vaults.

Select the region as East US: Choose the East US region as the location for the Recovery Services vault. This ensures the vault is geographically close to the resources it will back up (e.g., TestVM1), minimizing latency and potentially reducing costs associated with data transfers.

Click "Review + Create", then click "Create": After configuring all the required fields, click on the "Review + Create" button. This step allows you to verify all the entered details for correctness. Once confirmed, click "Create" to deploy the Recovery Services vault. Azure will validate your inputs and begin the resource deployment process.



This sequence ensures you follow the logical flow required by the Azure portal to successfully create a Recovery Services vault in the specified region and resource group. The vault will then be ready to configure backup for resources like TestVM1.

Reference:

https://learn.microsoft.com/en-us/azure/backup/backup-create-recovery-services-vault

Ask our Experts

Did you like this **Question?**

Question 2 Incorrect

Domain: Monitor and maintain Azure resources

View Case Study

What are the three necessary steps to create an Azure Backup vault for Fabrikam, Inc. as part of their backup and disaster recovery strategy? (Select three)

- [x] A. Create a Recovery Services vault in the East US region right
- [x] B. Enable backup for individual resources before creating the vault wrong
- [ ] C. Assign access policies for the vault to relevant users right
- [x] D. Configure backup jobs after creating the vault right

E. Establish alerts for backup job failures during vault creation

---

Explanation:

Correct Answers: A, C and D

The necessary steps for creating and setting up an Azure Backup vault involve creating the vault itself, assigning access policies, and configuring backup jobs. Following steps are required -

Option A: Create a Recovery Services vault in the East US region is correct.

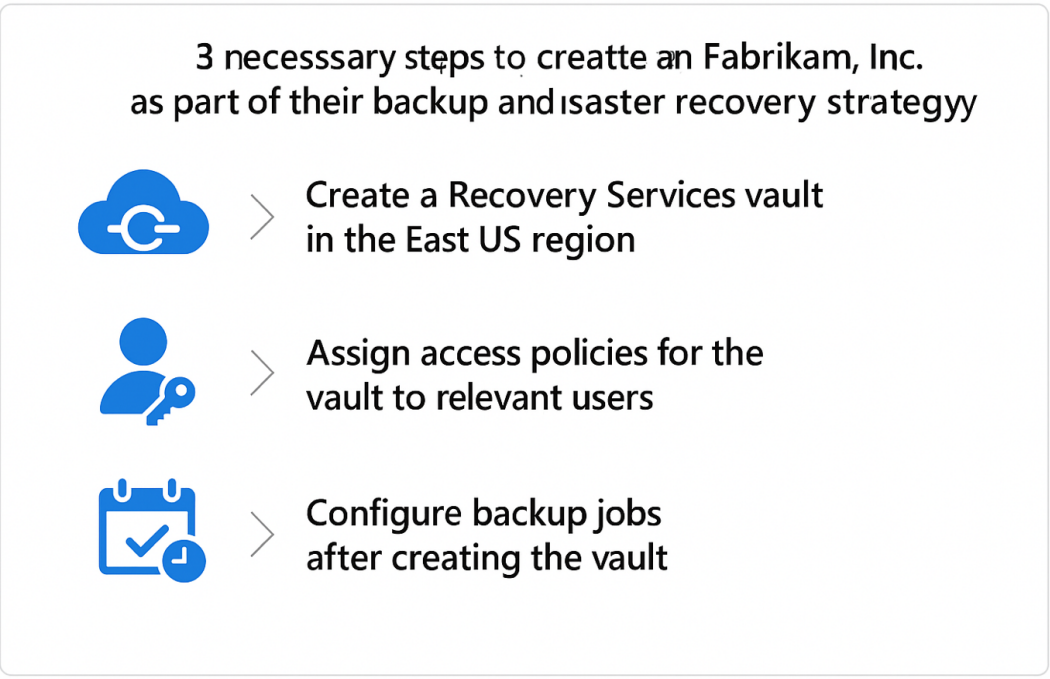
This step is necessary as the first part of setting up backup management for Fabrikam's resources. The Recovery Services vault will centralize the management of backup and restore operations, making it essential for implementing a backup strategy. It explicitly satisfies the requirement to manage backups for TestVM1, FinanceDB, and SharedDocs. The vault should be created in the same region as the primary resources for optimal performance and compliance.

Option C: Assign access policies for the vault to relevant users is correct.

This step is important because ensuring that the appropriate users have access to the Recovery Services vault is critical for managing backups securely. Access policies define who can perform backup and restore operations and help in maintaining compliance and security, particularly in environments like Fabrikam's, where they may have multiple users accessing sensitive financial data. Properly configured access ensures that only authorized personnel can change backup configurations or initiate restores.

Option D: Configure backup jobs after creating the vault is correct.

After creating the Recovery Services vault, the next logical step is to configure backup jobs for the individual resources. This involves specifying what resources to back up, setting retention periods, and determining backup frequencies. This step is crucial to ensure that the data for TestVM1, FinanceDB, and SharedDocs is backed up according to the established policies that meet Fabrikam's RTO and RPO requirements.



Option B: Enable backup for individual resources before creating the vault is incorrect because you must first create the Recovery Services vault to manage the backups of individual resources. Without the vault, there is no system in place to organize and handle the backups. After the vault is created, you can proceed to enable backup for TestVM1, FinanceDB, and SharedDocs. Therefore, this option does not follow the logical sequence required for setting up Azure Backup.

Option E: Establish alerts for backup job failures during vault creation is incorrect because while establishing alerts is an essential part of a comprehensive backup strategy, this step cannot occur during the vault's creation. Alerts need to be configured after the Recovery Services vault has been created and backup jobs have been set up. Alerts monitor the health of backup jobs and notify administrators of any failures or issues; thus, they are a post-creation task rather than part of the vault creation process itself.

Reference:

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

Ask our Experts

Did you like this **Question?**

Question 3 Incorrect

Domain: Monitor and maintain Azure resources

View Case Study

You have configured a backup policy for TestVM1 in the FabrikamBackupVault. The VM encountered a ransomware attack, and you need to restore it to the state from the last backup. Which steps should you perform?

A. Delete the compromised TestVM1 and create a new VM using the recovery point

B. Use the "Restore VM" option in the Recovery Services vault and select the latest recovery point right

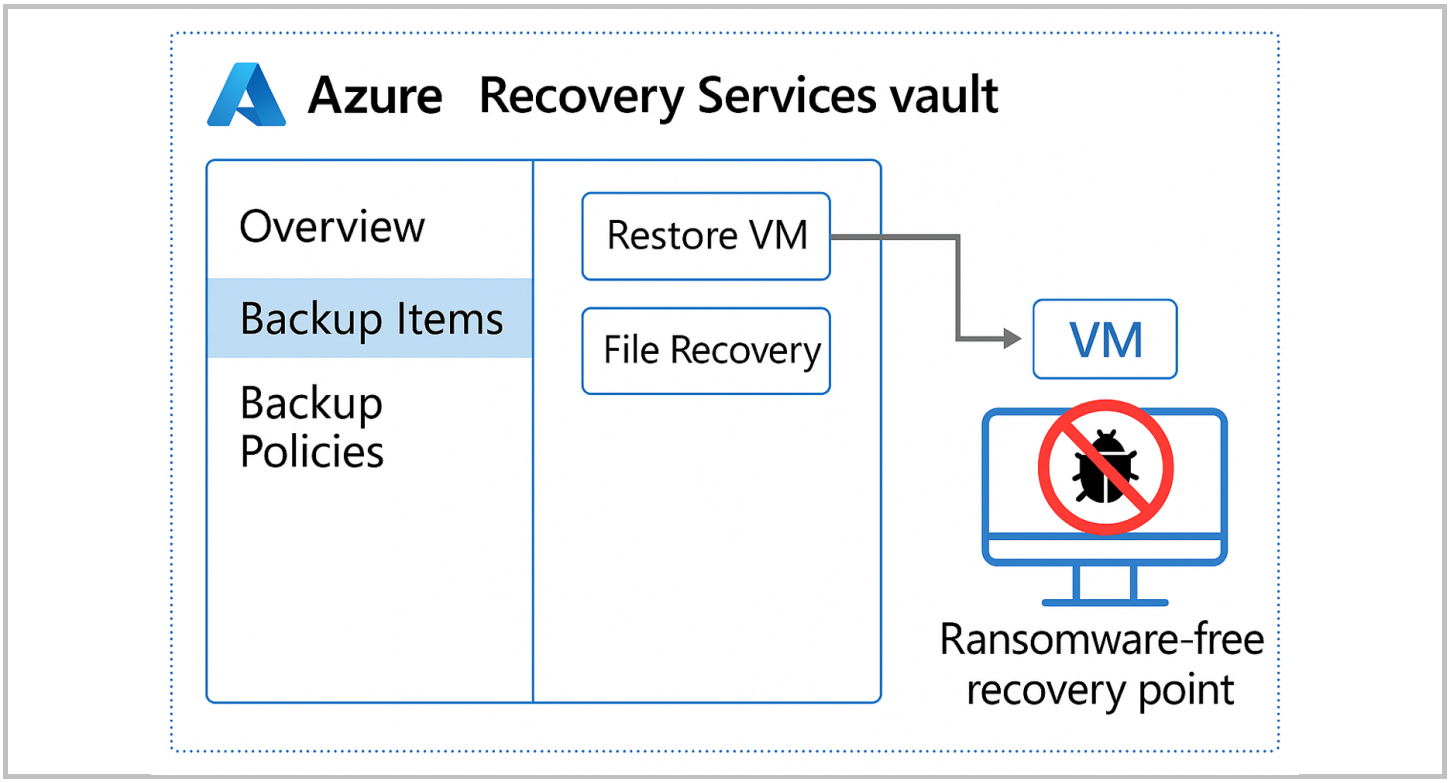
C. Use PowerShell to run the Restore-AzRecoveryServicesBackupItem cmdlet

D. Perform a file-level recovery of TestVM1 and replace the affected files wrong

---

Explanation:

Option B: Use the "Restore VM" option in the Recovery Services vault and select the latest recovery point is correct because the "Restore VM" option in the Recovery Services vault is the appropriate method for restoring a full virtual machine. It allows you to select a recovery point from the backups configured in the vault and restore the VM to its last known healthy state. This method ensures that all VM configurations, disks, and data are reverted to a ransomware-free recovery point.



Option A: Delete the compromised TestVM1 and create a new VM using the recovery point is incorrect because while creating a new VM from a recovery point is a valid approach in some scenarios, it is not necessary for this use case. The "Restore VM" option already handles the restoration without requiring manual deletion or recreation of the VM, making it the more efficient and straightforward solution.

Option C: Use PowerShell to run the Restore-AzRecoveryServicesBackupItem cmdlet is incorrect because the Restore-AzRecoveryServicesBackupItem cmdlet is not designed for restoring full virtual machines. Instead, it is used to restore individual items, such as files or application data. This cmdlet cannot perform the full VM restoration required to recover from a ransomware attack

Option D: Perform a file-level recovery of TestVM1 and replace the affected files is incorrect because File-level recovery only restores individual files or folders and does not address system-level compromises that are typical of ransomware attacks. Simply replacing

files will not guarantee the removal of the ransomware, and it does not restore the entire VM to a clean state.

Reference:

https://learn.microsoft.com/en-us/azure/backup/backup-azure-arm-restore-vms#choose-a-vm-restore-configuration

Ask our Experts

Did you like this **Question?**

Question 4 Incorrect

Domain: Monitor and maintain Azure resources

View Case Study

Fabrikam, Inc. has configured Azure Site Recovery for TestVM1. During a regional outage in the East US, you need to initiate a failover to the West US. What steps should you follow in Azure Site Recovery?

A. Run a test failover before initiating a full failover to ensure the secondary region is ready wrong

B. Perform a "Planned Failover" to avoid data loss in the target region

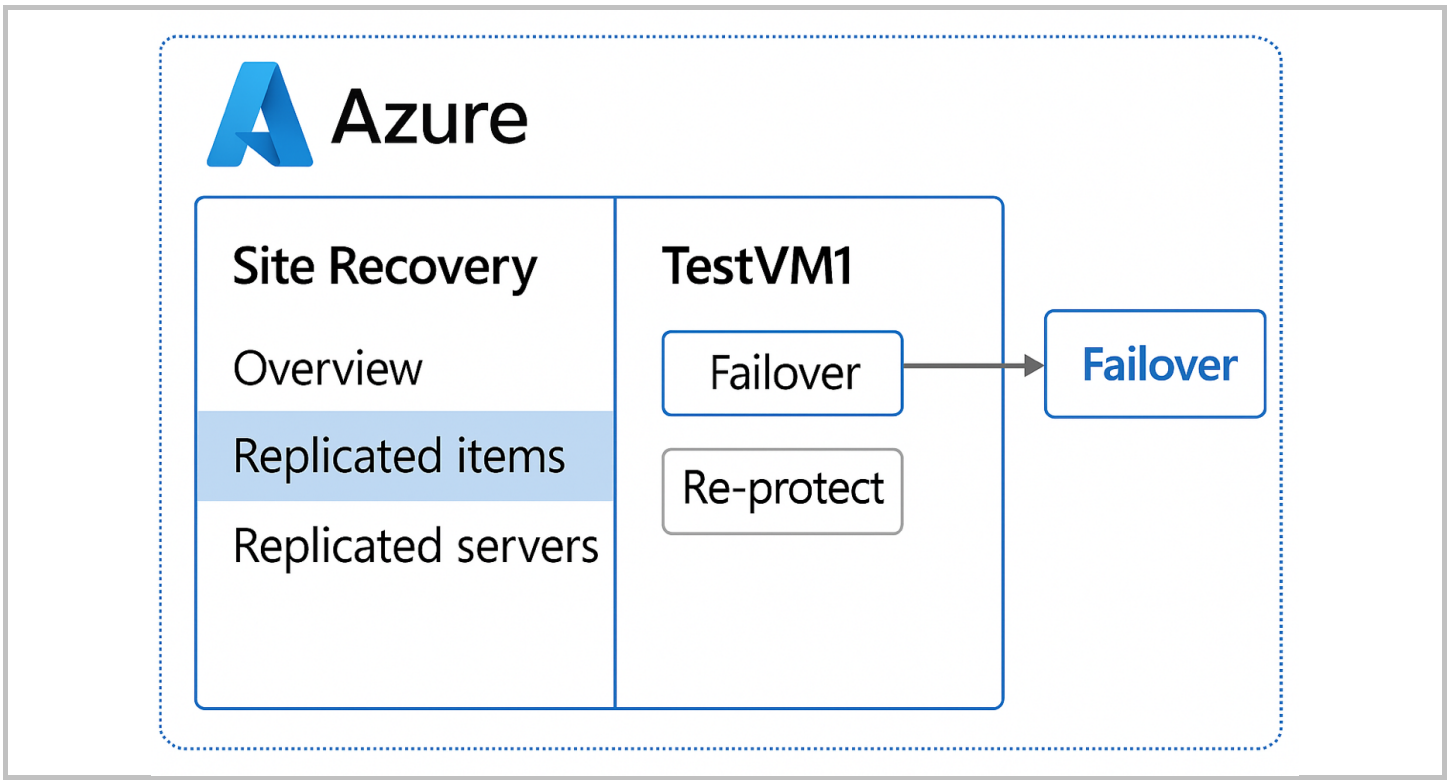
C. Stop all workloads on TestVM1 before initiating the failover

D. Navigate to the Recovery Services vault, select the replicated item TestVM1, and click "Failover" right

Explanation:

Correct Answer: D

Option D: Navigate to the Recovery Services vault, select the replicated item TestVM1, and click "Failover" is correct because initiating a failover for a replicated virtual machine (TestVM1) requires navigating to the Recovery Services vault where replication is managed. By selecting the replicated item and clicking "Failover," Azure Site Recovery initiates the process to bring the VM online in the secondary region (West US). This is the primary and necessary step to execute a failover. Failover ensures continuity of services during regional outages by switching to the target region where the replica is stored.



Option A: Run a test failover before initiating a full failover to ensure the secondary region is ready is incorrect because while a Test Failover is a best practice to verify readiness during regular operations, it is not feasible during an actual outage. In this case, the East US region is down, and performing a test failover would not ensure service continuity. The correct approach is to initiate a full failover immediately to bring TestVM1 online in the West US.

Option B: Perform a "Planned Failover" to avoid data loss in the target region is incorrect because a Planned Failover requires both source and target regions to be operational, as it replicates any pending changes before the failover. Since the East US region is experiencing a regional outage, a Planned Failover cannot be executed. Instead, an Unplanned Failover is appropriate during an outage to immediately switch to the secondary region, accepting the possibility of some data loss.

Option C: Stop all workloads on TestVM1 before initiating the failover is incorrect because during a regional outage, the source VM (TestVM1) is already inaccessible, making it impossible to stop workloads on it. The failover process in Azure Site Recovery automatically handles the switch to the replica VM in the target region. Stopping workloads is not a necessary step and cannot be performed in this scenario.

Reference:

Tutorial: Run a disaster recovery drill for Azure VMs

Ask our Experts

Did you like this **Question?**

Question 5 Correct

Domain: Monitor and maintain Azure resources

View Case Study

You want to configure backup reports and alerts for all protected resources in FabrikamBackupVault. Which of the following three actions must you take?

Note: Drag the correct options and then drop them into the answer area

Your Answer	Correct Answer
A. Enable Azure Monitor diagnostics and route logs to Log Analytics	A. Enable Azure Monitor diagnostics and route logs to Log Analytics
B. Configure an Action Group in Azure Monitor for backup alerts	B. Configure an Action Group in Azure Monitor for backup alerts
D. Enable email notifications for failed backup jobs in the Recovery Services vault settings	D. Enable email notifications for failed backup jobs in the Recovery Services vault settings

Explanation:

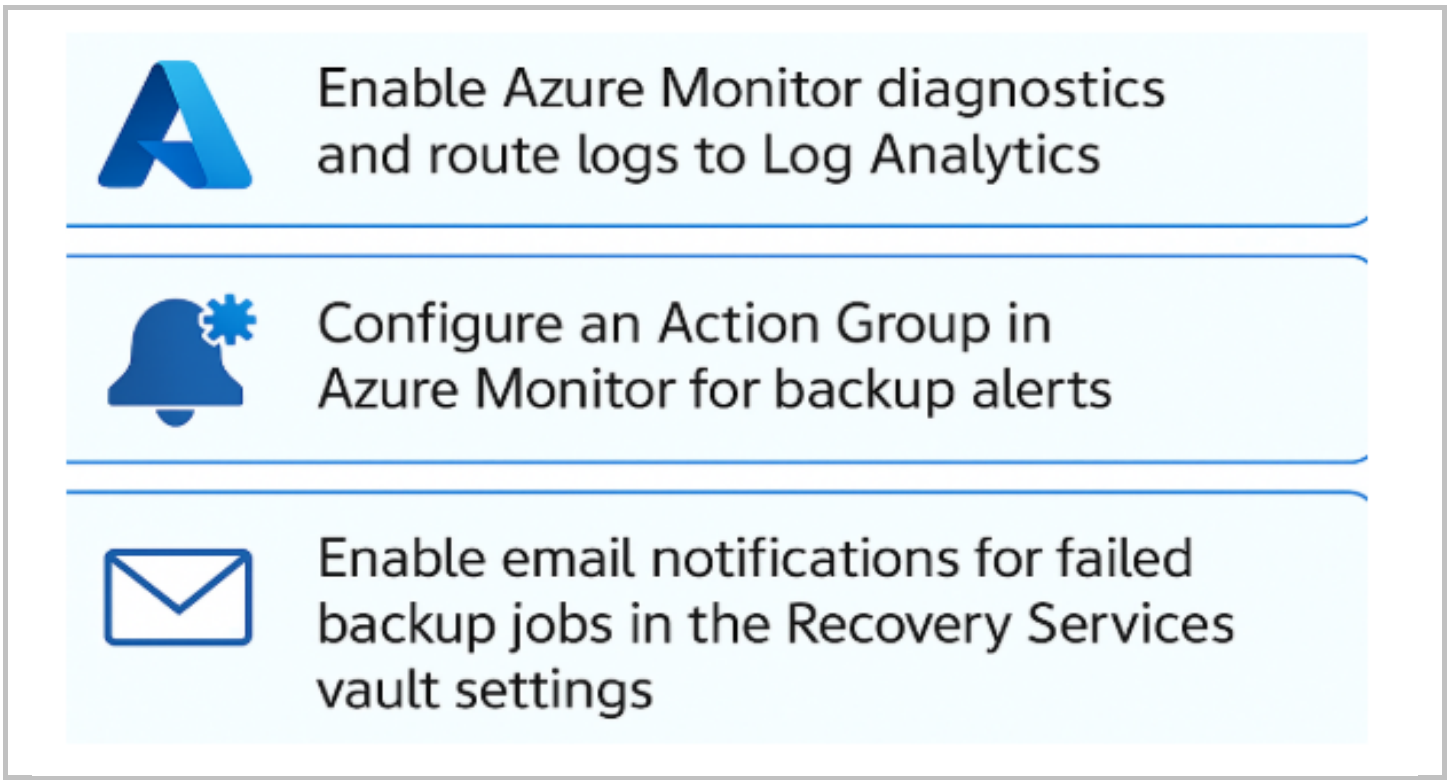
Correct Answers: A, B and D

The following actions are a must to configure backup reports and alerts for all protected resources in FabrikamBackupVault:

Option A: Enable Azure Monitor diagnostics and route logs to Log Analytics is correct because - Enabling Azure Monitor diagnostics and routing logs to Log Analytics allows you to gather detailed monitoring and alerting data for all protected resources in the Recovery Services vault. Logs from the backup operations, such as success or failure events, will be available in Log Analytics, making it easier to create customized alerts and reports using Azure Monitor.

Option B: Configure an Action Group in Azure Monitor for backup alerts is correct because - Configuring an Action Group in Azure Monitor for backup alerts is the appropriate step to receive notifications for backup job failures, successes, and other significant events. You can define specific actions, such as sending an email, text message, or invoking a webhook, to alert the appropriate users or administrators when backup jobs fail or encounter issues.

Option D: Enable email notifications for failed backup jobs in the Recovery Services vault settings is correct because - Enabling email notifications for failed backup jobs in the Recovery Services vault settings is the most straightforward method to get alerts for backup failures. This setting provides automated email notifications directly from the Recovery Services vault when a backup job fails, ensuring that the team is promptly informed of any issues with backups.



Option C: Use Power BI to visualize backup trends and failures is incorrect because while Power BI is a powerful tool for data visualization, it is not directly involved in configuring backup reports and alerts for Recovery Services vaults. Power BI can be used to visualize data from Log Analytics (after logs are routed there), but it is not a primary tool for configuring alerts or reporting within Azure Backup services.

References:

https://learn.microsoft.com/en-us/azure/backup/backup-azure-monitoring-built-in-monitor?tabs=recovery-services-vaults

https://learn.microsoft.com/en-us/azure/azure-monitor/alerts/action-groups

https://learn.microsoft.com/en-us/azure/backup/guidance-best-practices

Ask our Experts

Did you like this **Question?**

Finish Review