Exam

AZ-104

Microsoft Azure Administrator

Free demo	80 sample questions
Full exam	507 questions with answers and explanations
Contents	Questions with answers and explanations

Exam domains

Domain	Exam weight	Questions
D1 Manage Azure identities and governance	20–25%	19
D2 Implement and manage storage	15–20%	14
D3 Deploy and manage Azure compute resources	20–25%	19
D4 Implement and manage virtual networking	15–20%	17
D5 Monitor and maintain Azure resources	10–15%	11

This is a free demo from Dumpsgate: 80 of the exam's 507 questions. **Get the full AZ-104 exam** with every question, answer and explanation.

Question 1

Hotspot (dropdowns) · Domain: D1 Manage Azure identities and governance › Manage Azure subscriptions and governance

You have an Azure subscription that contains the hierarchy shown in the following exhibit.

Tenant Root Group

└── ManagementGroup1

```
└── Subscription1
    └── RG1
        └── VM1
```

Dumpsgate

Answer Area

You can assign Policy1 to:

- Subscription1 and RG1 only
- ManagementGroup1 and Subscription1 only
- Tenant Root Group, ManagementGroup1, and Subscription1 only
- Tenant Root Group, ManagementGroup1, Subscription1, and RG1 only
- Tenant Root Group, ManagementGroup1, Subscription1, RG1, and VM1

You can exclude Policy1 from:

- VM1 only
- RG1 and VM1 only
- Subscription1, RG1, and VM1 only
- ManagementGroup1, Subscription1, RG1, and VM1 only
- Tenant Root Group, ManagementGroup1, Subscription1, RG1, and VM1

You can assign Policy1 to: Subscription1 and RG1 only | ManagementGroup1 and Subscription1 only | Tenant Root Group, ManagementGroup1, and Subscription1 only | Tenant Root Group, ManagementGroup1, Subscription1, and RG1 only | Tenant Root Group, ManagementGroup1, Subscription1, RG1, and VM1

You can exclude Policy1 from: VM1 only | RG1 and VM1 only | Subscription1, RG1, and VM1 only | ManagementGroup1, Subscription1, RG1, and VM1 only | Tenant Root Group, ManagementGroup1, Subscription1, RG1, and VM1

Answer

- You can assign Policy1 to: **Tenant Root Group, ManagementGroup1, Subscription1, and RG1 only**
- You can exclude Policy1 from: **Subscription1, RG1, and VM1 only**

Explanation

Azure Policy assignments can be scoped to a management group, subscription, or resource group, but not directly to an individual VM. For this hierarchy, that means Tenant Root Group, ManagementGroup1, Subscription1, and RG1 are valid assignment scopes. Policy1 can be excluded at Subscription1, RG1, or VM1; ManagementGroup1 and Tenant Root Group are not valid exclusions in the listed choices.

https://learn.microsoft.com/en-us/azure/governance/policy/overview
https://learn.microsoft.com/azure/governance/policy/concepts/scope
https://learn.microsoft.com/en-us/azure/governance/policy/assign-policy-portal
https://learn.microsoft.com/en-gb/azure/governance/policy/concepts/assignment-structure

✗ **Box 1: Subscription1 and RG1 only** Subscription1 and RG1 only
Both are valid assignment scopes, but this choice leaves out the two management groups, which can also be assignment scopes. It is therefore incomplete for the hierarchy shown.

https://learn.microsoft.com/en-us/azure/governance/policy/overview
https://learn.microsoft.com/azure/governance/policy/concepts/scope
https://learn.microsoft.com/en-us/azure/governance/policy/assign-policy-portal

✗ **Box 1: ManagementGroup1 and Subscription1 only** ManagementGroup1 and Subscription1 only
These are valid assignment scopes, but the assignment can also be made at Tenant Root Group and RG1. This choice omits those valid scopes.

https://learn.microsoft.com/en-us/azure/governance/policy/overview
https://learn.microsoft.com/azure/governance/policy/concepts/scope
https://learn.microsoft.com/en-us/azure/governance/policy/assign-policy-portal

✗ **Box 1: Tenant Root Group, ManagementGroup1, and Subscription1 only** Tenant Root Group, ManagementGroup1, and Subscription1 only
All three listed scopes are valid, but RG1 is also a valid assignment scope. This option therefore leaves out a supported scope.

https://learn.microsoft.com/en-us/azure/governance/policy/overview
https://learn.microsoft.com/azure/governance/policy/concepts/scope
https://learn.microsoft.com/en-us/azure/governance/policy/assign-policy-portal

✓ **Box 1: Tenant Root Group, ManagementGroup1, Subscription1, and RG1 only** Tenant Root Group, ManagementGroup1, Subscription1, and RG1 only
Azure Policy can be assigned at management-group, subscription, and resource-group scopes. In the

Free demo · full exam: 507 questions

hierarchy, Tenant Root Group and ManagementGroup1 are management groups, followed by Subscription1 and RG1; VM1 is an individual resource and is not a valid assignment scope for this question.

https://learn.microsoft.com/en-us/azure/governance/policy/overview
https://learn.microsoft.com/azure/governance/policy/concepts/scope
https://learn.microsoft.com/en-us/azure/governance/policy/assign-policy-portal

✗ **Box 1: Tenant Root Group, ManagementGroup1, Subscription1, RG1, and VM1** Tenant Root Group, ManagementGroup1, Subscription1, RG1, and VM1
The management groups, subscription, and resource group are valid assignment scopes. VM1 is an individual resource, which is not a supported scope for assigning the policy in this question.

https://learn.microsoft.com/en-us/azure/governance/policy/overview
https://learn.microsoft.com/azure/governance/policy/concepts/scope
https://learn.microsoft.com/en-us/azure/governance/policy/assign-policy-portal

✗ **Box 2: VM1 only** VM1 only
VM1 can be excluded, but it is not the only valid exclusion scope listed in the hierarchy. Subscription1 and RG1 can also be excluded.

https://learn.microsoft.com/azure/governance/policy/concepts/scope
https://learn.microsoft.com/en-gb/azure/governance/policy/concepts/assignment-structure

✗ **Box 2: RG1 and VM1 only** RG1 and VM1 only
Both RG1 and VM1 can be excluded, but Subscription1 can also be excluded. This choice omits that valid scope.

https://learn.microsoft.com/azure/governance/policy/concepts/scope
https://learn.microsoft.com/en-gb/azure/governance/policy/concepts/assignment-structure

✓ **Box 2: Subscription1, RG1, and VM1 only** Subscription1, RG1, and VM1 only
The policy can be excluded from the subscription, a resource group within it, or a resource within that group. Thus Subscription1, RG1, and VM1 are the applicable exclusion scopes in the answer choices.

https://learn.microsoft.com/azure/governance/policy/concepts/scope
https://learn.microsoft.com/en-gb/azure/governance/policy/concepts/assignment-structure

✗ **Box 2: ManagementGroup1, Subscription1, RG1, and VM1 only** ManagementGroup1, Subscription1, RG1, and VM1 only
Subscription1, RG1, and VM1 are valid exclusions, but ManagementGroup1 is not included as an exclusion scope in the correct set. This option adds that management group.

https://learn.microsoft.com/azure/governance/policy/concepts/scope
https://learn.microsoft.com/en-gb/azure/governance/policy/concepts/assignment-structure

✗ **Box 2: Tenant Root Group, ManagementGroup1, Subscription1, RG1, and VM1** Tenant Root Group, ManagementGroup1, Subscription1, RG1, and VM1
Although Subscription1, RG1, and VM1 can be excluded, this option also includes Tenant Root Group and ManagementGroup1. Those management groups are not valid exclusions in the listed answer set.

https://learn.microsoft.com/azure/governance/policy/concepts/scope
https://learn.microsoft.com/en-gb/azure/governance/policy/concepts/assignment-structure

Question 2

Multiple choice · Domain: D1 Manage Azure identities and governance › Manage access to Azure resources

You are managing access to Azure resources for a growing development team. Some developers need to manage virtual machines, while others only need to read resource configurations. Rather than assigning built-in roles directly to individual users, your organization wants to use a group-based approach for easier maintenance.

Which combination of Microsoft Entra features and Azure RBAC elements should you implement?

A. Create a security group in Microsoft Entra ID for developers who manage VMs, add the appropriate users, and assign the 'Virtual Machine Contributor' built-in role to the group at the subscription scope.

B. Create individual custom roles for each developer with specific VM management permissions, then assign those roles directly to each user account.

C. Create a Microsoft 365 group in Microsoft Entra ID, add users to it, and assign the 'Owner' role at the resource group level to grant all permissions.

D. Use Microsoft Entra ID access reviews to periodically audit group membership, then assign the 'Reader' built-in role to a group of read-only developers and the 'Virtual Machine Contributor' role to another group.

Answer

- A. **Create a security group in Microsoft Entra ID for developers who manage VMs, add the appropriate users, and assign the 'Virtual Machine Contributor' built-in role to the group at the subscription scope.**
- D. **Use Microsoft Entra ID access reviews to periodically audit group membership, then assign the 'Reader' built-in role to a group of read-only developers and the 'Virtual Machine Contributor' role to another group.**

Explanation

Use Microsoft Entra groups to organize developers by the access they need, then assign Azure built-in roles to those groups rather than to each person. A assigns Virtual Machine Contributor to the VM-managers group, while D covers both VM managers and read-only developers by assigning the appropriate roles to separate groups. Access reviews can also help periodically check whether group membership remains appropriate.

https://learn.microsoft.com/en-us/entra/id-governance/deploy-access-reviews
https://learn.microsoft.com/en-us/entra/id-governance/access-reviews-overview
https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/general
https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/compute

✓ **A** Create a security group in Microsoft Entra ID for developers who manage VMs, add the appropriate users, and assign the 'Virtual Machine Contributor' built-in role to the group at the subscription scope. This uses a group as the access-management unit and grants the VM-management permission through the built-in role suited to that task. Assigning the role at subscription scope makes it apply to resources in that subscription; this choice addresses the VM-managing developers, while D also covers the read-only group.

https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/compute

✗ **B** Create individual custom roles for each developer with specific VM management permissions, then assign those roles directly to each user account.
This assigns access to individual users, contrary to the organization’s preference for group-based

Free demo · full exam: 507 questions

management. Creating a separate custom role for each developer also adds maintenance work when built-in roles and group assignments fit the stated needs.

https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/compute

✗ **C** Create a Microsoft 365 group in Microsoft Entra ID, add users to it, and assign the 'Owner' role at the resource group level to grant all permissions.
The Owner role grants broad permissions, which is excessive for developers who only need VM management or read access. It does not separate users according to the two access levels described in the scenario.

https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/general

✓ **D** Use Microsoft Entra ID access reviews to periodically audit group membership, then assign the 'Reader' built-in role to a group of read-only developers and the 'Virtual Machine Contributor' role to another group.
Separate groups with Reader and Virtual Machine Contributor roles match the read-only and VM-management needs without assigning roles directly to individuals. Access reviews provide a way to periodically review group membership and help ensure access remains appropriate.

https://learn.microsoft.com/en-us/entra/id-governance/deploy-access-reviews
https://learn.microsoft.com/en-us/entra/id-governance/access-reviews-overview
https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/general
https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/compute

Question 3

Single choice · Domain: D1 Manage Azure identities and governance › Manage access to Azure resources

Your organization uses Microsoft Entra ID with a hybrid identity scenario. You need to delegate resource access management to team leads so they can grant appropriate role assignments to their team members without full subscription owner permissions. Which two capabilities should you configure?

A. Custom RBAC role definitions with specific resource permissions and delegation of role assignment permissions to team leads
B. Microsoft Entra ID administrative units and Entra ID-only groups for team organization
C. Subscription owner role assigned to all team leads with conditional access policies
D. Azure Policy for role assignments and resource naming conventions
E. Managed Identity assignment combined with service principal creation by team leads

Answer: A. Custom RBAC role definitions with specific resource permissions and delegation of role assignment permissions to team leads

Explanation

Custom Azure RBAC roles let the organization define resource permissions appropriate to each team, while delegated role-assignment permissions let team leads grant those roles to their members. This meets the requirement to manage resource access without giving team leads full subscription owner permissions. Administrative units, Azure Policy, and managed identities do not provide this combination of scoped resource permissions and delegated role assignment.

https://learn.microsoft.com/en-us/azure/role-based-access-control/delegate-role-assignments-overview
https://learn.microsoft.com/azure/role-based-access-control/custom-roles

Free demo · full exam: 507 questions

✓ **A** Custom RBAC role definitions with specific resource permissions and delegation of role assignment permissions to team leads
Custom roles can specify the resource actions that team members need, and Azure RBAC supports delegating permission to assign roles. Together, these capabilities allow team leads to grant appropriate access without giving them the broad permissions of a subscription owner.
https://learn.microsoft.com/en-us/azure/role-based-access-control/delegate-role-assignments-overview
https://learn.microsoft.com/azure/role-based-access-control/custom-roles

✗ **B** Microsoft Entra ID administrative units and Entra ID-only groups for team organization
Administrative units help scope management of Microsoft Entra directory objects and roles; they do not by themselves delegate Azure resource role assignments. Organizing users into groups also does not give team leads permission to assign Azure RBAC roles.
https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/administrative-units
https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/admin-units-manage?tabs=admin-center

✗ **C** Subscription owner role assigned to all team leads with conditional access policies
The Owner role provides broad control over subscription resources, including access management, which exceeds the requested limited delegation. Conditional Access policies govern access conditions and do not narrow the Owner role's resource permissions.
https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/privileged

✗ **D** Azure Policy for role assignments and resource naming conventions
Azure Policy is used to audit or enforce resource configuration and governance requirements, not to delegate the ability to grant RBAC roles to team leads. Naming conventions likewise do not provide role-assignment permissions.
https://learn.microsoft.com/en-us/azure/role-based-access-control/policy-reference

✗ **E** Managed Identity assignment combined with service principal creation by team leads
Managed identities and service principals are identities used by applications or services, not a mechanism for delegating scoped Azure resource role assignments to team leads. This would not satisfy the stated requirement to let leads grant appropriate roles to team members.

Question 4

Single choice · Domain: D1 Manage Azure identities and governance › Manage Azure subscriptions and governance

Your company has multiple Azure subscriptions managed by different departments. You need to ensure consistent security and compliance policies are applied across all subscriptions while allowing departments to manage their own resources. Which two governance features should you implement?

A. Azure Policy and Azure Management Groups
B. Role-Based Access Control (RBAC) and Azure Blueprints only
C. Microsoft Entra ID conditional access and subscription locks
D. Resource locks and custom role definitions across all subscriptions
E. Azure Advisor recommendations and resource naming policies

Answer: A. Azure Policy and Azure Management Groups

Explanation
Azure Management Groups let you organize subscriptions into a hierarchy, and Azure Policy assignments

at a management-group scope can apply governance requirements across the subscriptions beneath it. This gives the company a way to enforce consistent security and compliance rules while departments retain control over their own resources through their delegated permissions. [1][9]

https://learn.microsoft.com/en-us/azure/governance/management-groups/manage
https://learn.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage

✓ **A** Azure Policy and Azure Management Groups
Management Groups provide a scope above individual subscriptions, allowing subscriptions managed by different departments to be organized together. Azure Policy can then be assigned at that scope to apply consistent requirements across those subscriptions. [1][9]

https://learn.microsoft.com/en-us/azure/governance/management-groups/manage
https://learn.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage

✗ **B** Role-Based Access Control (RBAC) and Azure Blueprints only
RBAC can control which actions departments may perform, but it does not itself enforce security and compliance requirements on resources. This option also omits the combination of Azure Policy and Management Groups that supports consistent policy assignment across subscriptions; Azure Blueprints are not needed for that approach. [1][2][7]

https://learn.microsoft.com/en-us/azure/governance/management-groups/manage
https://learn.microsoft.com/en-us/azure/governance/blueprints/blueprint-retirement
https://learn.microsoft.com/en-us/azure/governance/blueprints/overview

✗ **C** Microsoft Entra ID conditional access and subscription locks
Conditional Access governs access to identities and resources, while subscription locks help prevent certain changes or deletions. Neither provides a way to assign a consistent set of resource-compliance policies across multiple subscriptions.

✗ **D** Resource locks and custom role definitions across all subscriptions
Resource locks prevent specified operations, and custom roles define permissions. These can help protect resources and delegate management, but they do not provide the policy-based compliance enforcement requested.

✗ **E** Azure Advisor recommendations and resource naming policies
Azure Advisor provides recommendations rather than centrally enforcing requirements across subscriptions. Naming policies alone address only naming conventions, not the broader security and compliance policies in the scenario.

Question 5

Multiple choice · Domain: D1 Manage Azure identities and governance › Manage Azure subscriptions and governance

Your organization has created several resource groups for different projects within a single subscription. You want to track and optimize cloud spending across projects. You need to assign costs to each project team, prevent unexpected cost overruns, and generate detailed reports showing resource consumption by project.

Which Azure features should you implement? (Select all that apply.)

A. Apply cost allocation tags to all resources and configure cost management budgets with alerts
B. Use Azure Cost Management and Billing to analyze costs by tag and create spending reports
C. Implement Azure Policy to enforce mandatory tagging on all new resources
D. Assign different RBAC roles to each project team to control resource creation
E. Configure resource locks to prevent accidental resource deletion and cost overages

Free demo · full exam: 507 questions

Answer

- A. **Apply cost allocation tags to all resources and configure cost management budgets with alerts**
- B. **Use Azure Cost Management and Billing to analyze costs by tag and create spending reports**
- C. **Implement Azure Policy to enforce mandatory tagging on all new resources**

Explanation

Apply project-identifying tags so costs can be attributed to each team, and use Azure Cost Management to analyze those costs and produce reports by tag. Budgets with alerts help teams identify when spending is approaching a threshold so they can respond; alerts do not automatically stop resource spending. Azure Policy can enforce required tags on new resources, supporting consistent project-level reporting.

https://learn.microsoft.com/en-us/azure/cost-management-billing/costs/cost-allocation-introduction
https://learn.microsoft.com/azure/cost-management-billing/costs/overview-cost-management
https://learn.microsoft.com/en-us/azure/cost-management-billing/costs/cost-analysis-common-uses
https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/tag-policies
https://learn.microsoft.com/en-us/azure/cost-management-billing/costs/enable-tag-inheritance

✓ **A** Apply cost allocation tags to all resources and configure cost management budgets with alerts
Project tags let Azure cost data be grouped and attributed by project. Budgets with alerts help teams notice spending approaching a configured threshold, although an alert does not itself prevent or stop spending.

https://learn.microsoft.com/en-us/azure/cost-management-billing/costs/cost-allocation-introduction
https://learn.microsoft.com/azure/cost-management-billing/costs/overview-cost-management
https://learn.microsoft.com/en-us/azure/cost-management-billing/costs/enable-tag-inheritance
https://learn.microsoft.com/th-th/azure/cost-management-billing/understand/plan-manage-costs

✓ **B** Use Azure Cost Management and Billing to analyze costs by tag and create spending reports
Cost Management provides cost analysis and reporting, and filtering or grouping by project tags gives the organization detailed views of resource costs by project. This directly supports tracking and optimizing spending across teams.

https://learn.microsoft.com/azure/cost-management-billing/costs/overview-cost-management
https://learn.microsoft.com/en-us/azure/cost-management-billing/costs/cost-analysis-common-uses
https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/track-costs

✓ **C** Implement Azure Policy to enforce mandatory tagging on all new resources
A policy requiring project tags helps ensure new resources carry the information needed for consistent cost attribution. Without consistent tags, costs may be harder to report accurately by project.

https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/tag-policies
https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effect-modify

✗ **D** Assign different RBAC roles to each project team to control resource creation
RBAC controls who can access or create resources, but it does not assign their costs to project teams or generate consumption reports. It may support access governance, but it does not meet the stated cost tracking and reporting needs.

✗ **E** Configure resource locks to prevent accidental resource deletion and cost overages
Resource locks help prevent deletion or modification of protected resources; they are not spending controls and do not prevent cost overages. Cost analysis and budget alerts are the relevant tools for monitoring spending thresholds.

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

Free demo · full exam: 507 questions

Question 6

Yes / No · Domain: D1 Manage Azure identities and governance › Manage Microsoft Entra users and groups

You have a Microsoft Entra tenant named contoso.com that has the External collaboration settings shown in the following exhibit.

Guest user access restrictions

- Guest users have the same access as members (most inclusive)
- Selected: Guest users have limited access to properties and memberships of directory objects
- Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Guest invite restrictions

- Selected: Anyone in the organization can invite guest users including guests and non-admins (most inclusive)
- Member users and users assigned to specific admin roles can invite guest users including guests with member permissions
- Only users assigned to specific admin roles can invite guest users
- No one in the organization can invite guest users including admins (most restrictive)

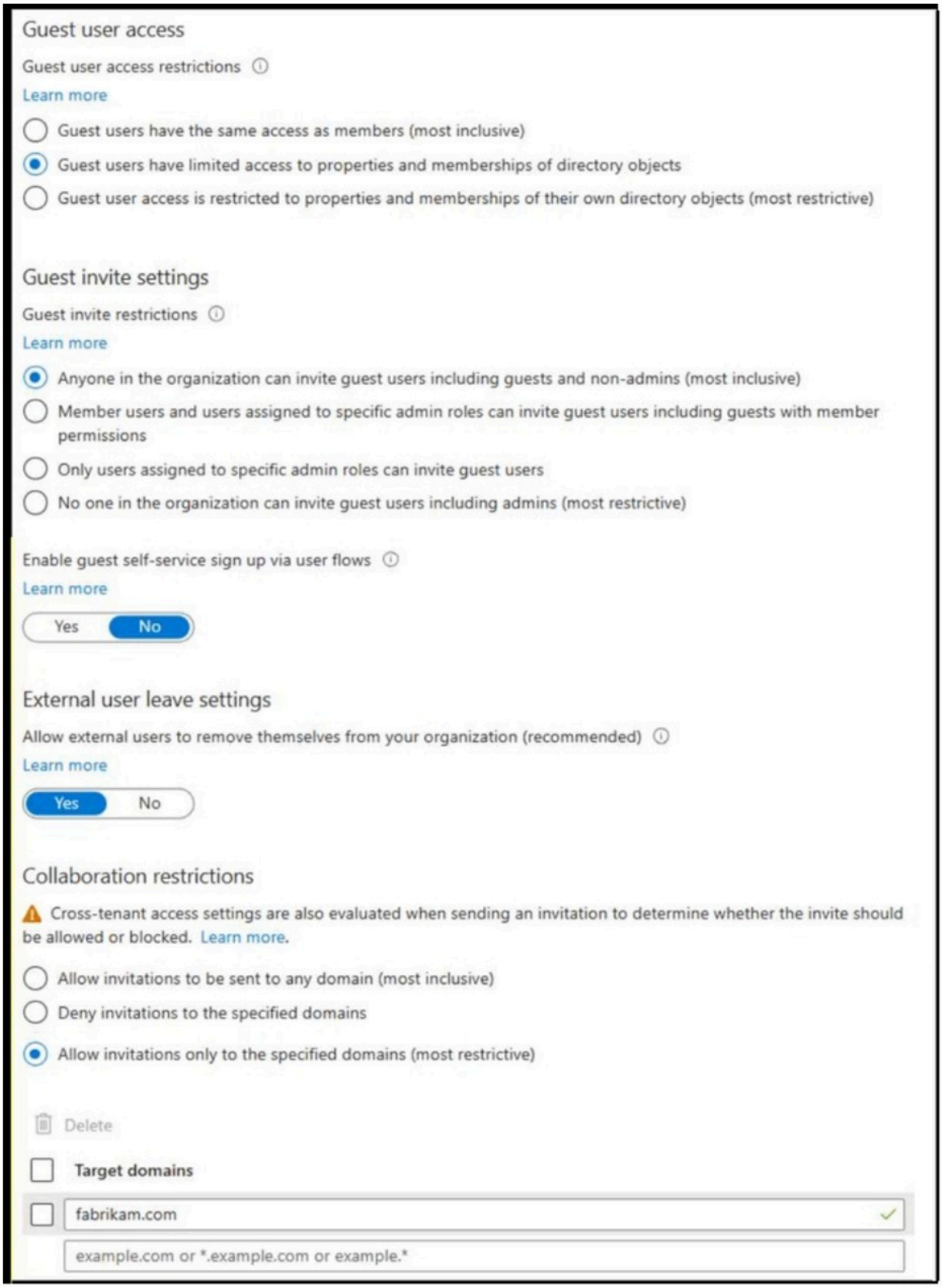
Enable guest self-service sign up via user flows: No

Allow external users to remove themselves from your organization (recommended): Yes

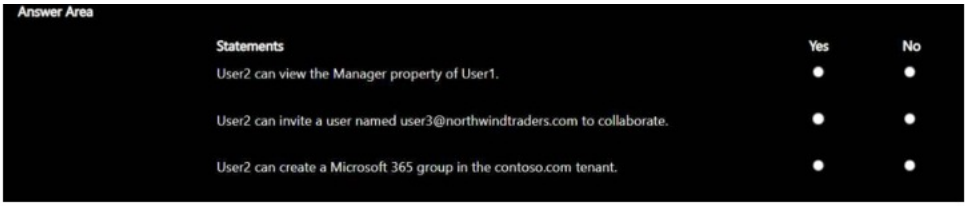
Collaboration restrictions

- Allow invitations to be sent to any domain (most inclusive)
- Deny invitations to the specified domains
- Selected: Allow invitations only to the specified domains (most restrictive)
- Target domain: fabrikam.com

Dumpsgate



Name	Type	Role	Tenant
User1	Member	Helpdesk Administrator	contoso.com
User2	Guest	*None*	fabrikam.com



The tenant contains the users shown in the following table.

Name	Type	Role	Tenant
User1	Member	Helpdesk Administrator	contoso.com
User2	Guest	None	fabrikam.com

User2 is an invited guest of User1.

For each of the following statements, select Yes if the statement is true. Otherwise, select No. Each correct selection is worth one point.

1. User2 can view the Manager property of User1.
2. User2 can invite a user named user3@northwindtraders.com to collaborate.
3. User2 can create a Microsoft 365 group in the contoso.com tenant.

Statement	Yes	No
User2 can view the Manager property of User1.	☐	☐
User2 can invite a user named user3@northwindtraders.com to collaborate.	☐	☐
User2 can create a Microsoft 365 group in the contoso.com tenant.	☐	☐

Answer

- User2 can view the Manager property of User1. **Yes**
- User2 can invite a user named user3@northwindtraders.com to collaborate. **No**
- User2 can create a Microsoft 365 group in the contoso.com tenant. **No**

Explanation

User2 is a guest, but the tenant allows guests to invite other guests. That permission does not override the domain allowlist: invitations are permitted only to fabrikam.com, so User2 cannot invite an address at northwindtraders.com. The selected guest-access restriction still allows User2 to view User1's Manager property, while guest status does not allow User2 to create a Microsoft 365 group in contoso.com.

https://learn.microsoft.com/entra/external-id/external-collaboration-settings-configure
https://learn.microsoft.com/en-us/entra/external-id/allow-deny-list
https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-guest-users
https://learn.microsoft.com/en-us/entra/identity/users/users-restrict-guest-permissions

✓ **Statement 1** User2 can view the Manager property of User1.
The selected guest-access setting limits guests' access to directory-object properties and memberships, but does not restrict them to viewing only their own objects. Under this setting, User2 can view the Manager property of User1.

https://learn.microsoft.com/en-us/entra/identity/users/users-restrict-guest-permissions

✗ **Statement 2** User2 can invite a user named user3@northwindtraders.com to collaborate.

The invitation setting allows guests to invite other guests, so User2 is not excluded just because User2 is a guest. However, invitations are allowed only to the specified domain fabrikam.com, and northwindtraders.com is not on the allowlist.

https://learn.microsoft.com/entra/external-id/external-collaboration-settings-configure
https://learn.microsoft.com/en-us/entra/external-id/allow-deny-list

✗ **Statement 3** User2 can create a Microsoft 365 group in the contoso.com tenant.
User2 is a guest with no assigned role in contoso.com. Guest users do not have permission to create Microsoft 365 groups in the tenant.

https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-guest-users
https://learn.microsoft.com/microsoft-365/solutions/manage-creation-of-groups

---

Question 7

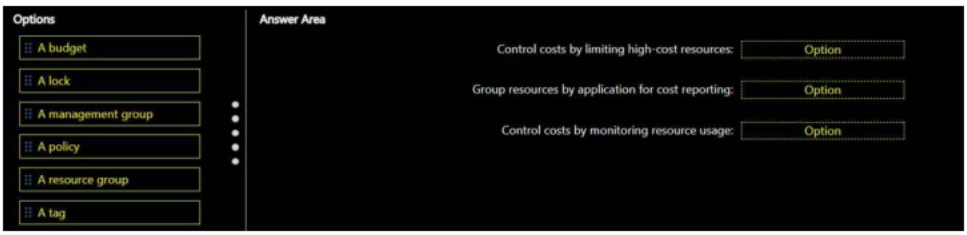
Drag and drop · Domain: D1 Manage Azure identities and governance › Manage Azure subscriptions and governance

You need to implement multiple Azure subscriptions for production and development environments. The solution must meet the following requirements:

- Control costs by limiting the number of high-cost resources that can be provisioned in the subscriptions.
- Group all the resources by application for cost reporting.
- Control costs by monitoring resource usage.

What should you configure for each requirement? To answer, drag the appropriate options to the correct requirements. Each option 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.



Items:

- A. A budget
- B. A lock
- C. A management group
- D. A policy
- E. A resource group
- F. A tag

Place them on:

1. Control costs by limiting the number of high-cost resources that can be provisioned in the subscriptions.
2. Group all the resources by application for cost reporting.
3. Control costs by monitoring resource usage.

Answer

- Control costs by limiting the number of high-cost resources that can be provisioned in the subscriptions. → **D. A policy**
- Group all the resources by application for cost reporting. → **F. A tag**
- Control costs by monitoring resource usage. → **A. A budget**

Explanation

Use a policy to restrict which high-cost resources can be provisioned in the subscriptions. Apply a tag to resources so costs can be grouped by application in cost reports. Configure a budget to monitor spending or usage and receive alerts when defined thresholds are reached.

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/group-filter
https://learn.microsoft.com/en-us/azure/governance/policy/samples/built-in-policies
https://learn.microsoft.com/en-us/azure/cost-management-billing/costs/tutorial-acm-create-budgets?tabs=psbudget&trk=article-ssr-frontend-pulse_little-text-block

✓ **A budget** A budget
A budget lets you monitor spending against a defined amount and configure alerts when thresholds are reached. That meets the requirement to control costs by monitoring resource usage.

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/tutorial-acm-create-budgets?tabs=psbudget&trk=article-ssr-frontend-pulse_little-text-block

✗ **A lock** A lock
A lock protects a resource from deletion or modification; it does not monitor usage or set spending thresholds. It also does not restrict how many high-cost resources can be provisioned.

https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources

✗ **A management group** A management group
A management group organizes subscriptions so governance can be applied across them, but it does not itself group resources by application in cost reports. Tags provide that reporting dimension.

https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/overview?source=recommendations
https://learn.microsoft.com/en-us/azure/cost-management-billing/costs/group-filter

✓ **A policy** A policy
A policy can deny deployments that do not meet defined rules, such as restricting high-cost resource types or SKUs. This helps limit the high-cost resources that can be provisioned in the subscriptions.

https://learn.microsoft.com/en-us/azure/governance/policy/samples/built-in-policies

✗ **A resource group** A resource group
A resource group is a container for resources that are managed together, but grouping resources by application for cost reporting is better done with tags. Resources for an application might also span multiple resource groups.

https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/manage-resource-groups-portal
https://learn.microsoft.com/en-us/azure/cost-management-billing/costs/group-filter

✓ **A tag** A tag
A tag can identify the application associated with each resource, allowing costs to be grouped and analyzed by that tag. This directly supports cost reporting by application.

https://learn.microsoft.com/en-us/azure/cost-management-billing/costs/group-filter
https://learn.microsoft.com/en-us/azure/cost-management-billing/costs/customize-cost-analysis-views

Free demo · full exam: 507 questions

Question 8

Single choice · Domain: D1 Manage Azure identities and governance › Manage Microsoft Entra users and groups

You have a Microsoft Entra tenant named contoso.com that contains the users shown in the following table.

Name	Department	Job title
User1	HR	Manager
User2	HR	Trainer
User3	IT	Support
User4	Finance	Manager
User5	Finance	Trainer

You create a dynamic user group named Group1 that has the following membership rule. (user.department -eq "MR") -and (user.jobTitle -eq "Manager") -or (user.jobTitle -eq "Support") Which users will be members of Group1?

A. User1 only
B. User1 and User2 only
C. User1 and User3 only
D. User1 and User4 only
E. User1, User2, and User4

Answer: C. User1 and User3 only

Explanation

The provided answer key marks C. Under the usual interpretation of the rule, User3 qualifies because their job title is Support, and User1 would qualify only if the department condition were `HR` rather than the shown `MR`. As written, the rule and table do not support C: User1 has department HR, not MR, so only User3 matches. The key appears to rely on a typo in the rule.

https://learn.microsoft.com/en-us/entra/identity/users/groups-dynamic-membership

✗ **A** User1 only
User1 has the job title Manager, but their department is HR, not MR, so they do not match the first branch as written. This option also omits User3, whose job title is Support and therefore matches the second branch.

https://learn.microsoft.com/en-us/entra/identity/users/groups-dynamic-membership

✗ **B** User1 and User2 only
User2 is an HR Trainer, so they match neither the department-and-Manager branch nor the Support branch. User1 also does not match the shown department value MR, and this option omits User3.

https://learn.microsoft.com/en-us/entra/identity/users/groups-dynamic-membership

✓ **C** User1 and User3 only
This is the answer marked correct in the provided key and would fit if the rule's department value were HR: User1 is an HR Manager, while User3 has the job title Support. However, the rule shown says MR, so User1 does not satisfy it as written; literally, only User3 matches.

https://learn.microsoft.com/en-us/entra/identity/users/groups-dynamic-membership

✗ **D** User1 and User4 only
User4 is a Finance Manager, so they do not match the department-and-Manager branch, and their title is not Support. User1 also has department HR rather than the shown MR value.
https://learn.microsoft.com/en-us/entra/identity/users/groups-dynamic-membership

✗ **E** User1, User2, and User4
User2 is a Trainer and User4 is a Finance Manager, so neither matches either branch of the rule. User1's department is HR rather than MR, so this group is not supported by the rule as written.
https://learn.microsoft.com/en-us/entra/identity/users/groups-dynamic-membership

---

Question 9

Yes / No · Domain: D1 Manage Azure identities and governance › Manage access to Azure resources

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

Name	Member of
User1	Group1
User2	Group2
User3	Group3

The groups are configured as shown in the following table.

Name	Type	Microsoft Entra roles can be assigned to the group
Group1	Security	Yes
Group2	Security	Yes
Group3	Microsoft 365	Yes

The RG1 Access control (IAM) role assignments shown include Group1 (Group), Owner, This resource, and a user (User), Owner, Subscription (Inherited).

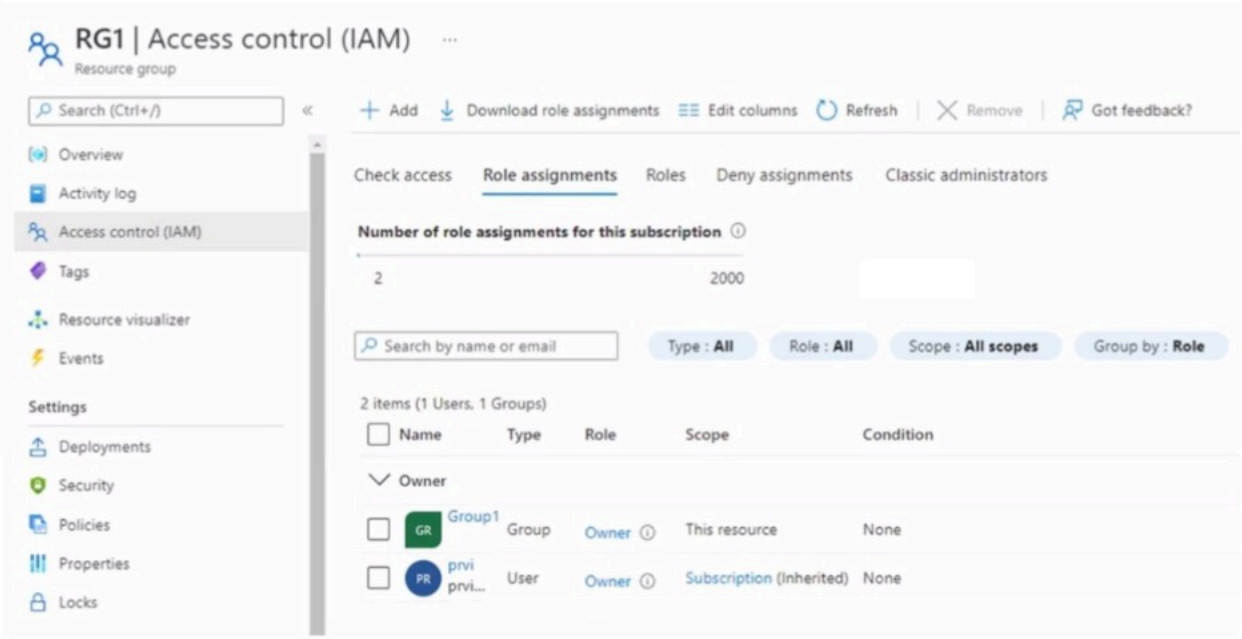
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

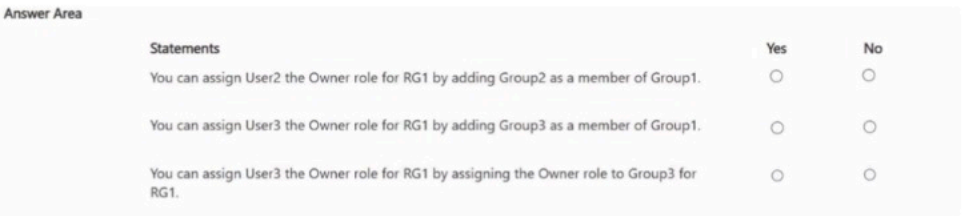
NOTE: Each correct selection is worth one point.

Dumpsgate

Name	Member of
User1	Group1
User2	Group2
User3	Group3

Name	Type	Microsoft Entra roles can be assigned to the group
Group1	Security	Yes
Group2	Security	Yes
Group3	Microsoft 365	Yes





Statement	Yes	No
You can assign User2 the Owner role for RG1 by adding Group2 as a member of Group1.	☐	☐
You can assign User3 the Owner role for RG1 by adding Group3 as a member of Group1.	☐	☐
You can assign User3 the Owner role for RG1 by assigning the Owner role to Group3 for RG1.	☐	☐

Answer

- You can assign User2 the Owner role for RG1 by adding Group2 as a member of Group1. **No**
- You can assign User3 the Owner role for RG1 by adding Group3 as a member of Group1. **No**
- You can assign User3 the Owner role for RG1 by assigning the Owner role to Group3 for RG1. **Yes**

Explanation

The Owner role is assigned to Group1 at RG1, but Azure role assignments do not flow through nested group membership. Therefore, adding Group2 or Group3 to Group1 does not grant their members the role. Assigning Owner directly to Group3 at RG1 does grant the role to User3, who is a direct member of Group3.

https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments

✗ **Statement 1** You can assign User2 the Owner role for RG1 by adding Group2 as a member of Group1.
No. This would make Group2 a nested member of Group1, and Azure role assignments do not grant access through nested group membership. User2 therefore would not receive Group1's Owner role through this change.

https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments

✗ **Statement 2** You can assign User3 the Owner role for RG1 by adding Group3 as a member of Group1.
No. Adding Group3 to Group1 is also nested group membership, which does not propagate Azure role assignments to the nested group's users. User3 would not gain the Owner role through Group1 this way.

https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments

✓ **Statement 3** You can assign User3 the Owner role for RG1 by assigning the Owner role to Group3 for RG1.
Yes. The Owner role can be assigned directly to a group at the RG1 scope. Because User3 is a direct member of Group3, User3 receives the permissions from that group assignment.

https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments

Question 10

Hotspot (dropdowns) · Domain: D1 Manage Azure identities and governance › Manage Microsoft Entra users and groups

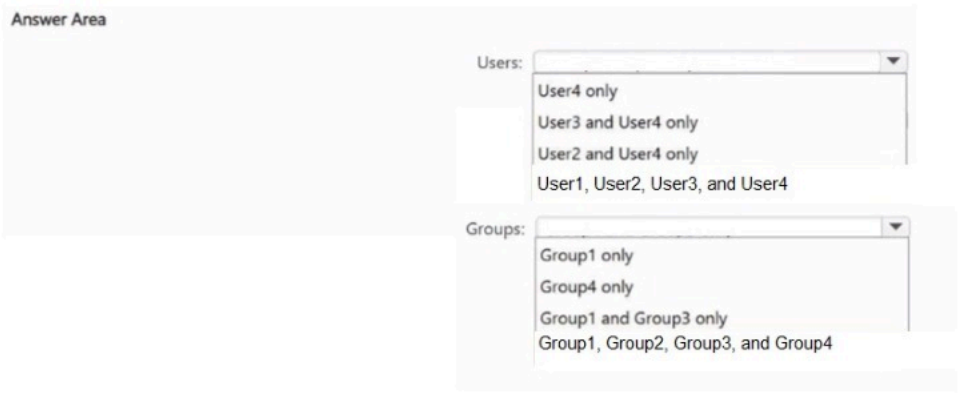
You have a Microsoft Entra tenant that contains the users shown in the following table.

Name	Member of	Assigned license
User1	Group1	Microsoft Entra ID P2
User2	Group2	None
User3	None	Microsoft Entra ID P2
User4	None	None

Free demo · full exam: 507 questions

Name	Member of	Assigned license
User1	Group1	Microsoft Entra ID P2
User2	Group2	*None*
User3	*None*	Microsoft Entra ID P2
User4	*None*	*None*

Name	Member of	Assigned license
User1	Group1	Microsoft Entra ID P2
User2	Group2	*None*
User3	*None*	Microsoft Entra ID P2
User4	*None*	*None*



The tenant contains the groups shown in the following table.

Name	Member of	Assigned license
User1	Group1	Microsoft Entra ID P2
User2	Group2	None
User3	None	Microsoft Entra ID P2
User4	None	None

Which users and groups can be deleted? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Users: User4 only | User3 and User4 only | User2 and User4 only | User1, User2, User3, and User4

Groups: Group1 only | Group4 only | Group1 and Group3 only | Group1, Group2, Group3, and Group4

Answer

- Users: **User1, User2, User3, and User4**
- Groups: **Group1 and Group3 only**

Question 11

Single choice · Domain: D1 Manage Azure identities and governance › Manage Azure subscriptions and governance

You have an Azure subscription named Sub1 that contains a resource group named RG1. You need to ensure that all current and future resources in RG1 have a tag of Department =HR applied. What should you do?

A. Create and assign an Azure policy.
B. Apply the Departments tag to Sub1.
C. Apply the Department =HR tag to each resource in RG1.
D. Apply the Departments tag directly to RG1.

Answer: A. Create and assign an Azure policy.

Explanation

Create and assign an Azure Policy at the RG1 scope that adds or modifies the Department=HR tag. Configure remediation so the policy can also apply the tag to existing resources; the policy then covers future resources in RG1 as well. Azure resource tags do not automatically inherit from a subscription or resource group.

https://learn.microsoft.com/en-us/previous-versions/azure/azure-resource-manager/management/tag-resources
https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effect-modify
https://learn.microsoft.com/azure/governance/policy/tutorials/govern-tags
https://learn.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources?WT.mc_id=AZ-MVP-5004810

✓ **A** Create and assign an Azure policy.
Assign a policy at RG1 that adds or modifies the Department=HR tag. Remediation can apply the tag to existing resources, while the policy governs resources created in the group later.

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effect-modify
https://learn.microsoft.com/azure/governance/policy/tutorials/govern-tags
https://learn.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources?WT.mc_id=AZ-MVP-5004810

✗ **B** Apply the Departments tag to Sub1.
This names the wrong tag and applies it at the subscription scope rather than ensuring that resources in

Free demo · full exam: 507 questions

RG1 have Department=HR. A tag on the subscription is not automatically inherited by its resources.

https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/tag-policies
https://learn.microsoft.com/en-us/previous-versions/azure/azure-resource-manager/management/tag-resources

✗ **C** Apply the Department =HR tag to each resource in RG1.
Tagging each resource individually could cover current resources, but it does not ensure future resources receive the tag. A policy at RG1 can govern both existing resources through remediation and future resources.

https://learn.microsoft.com/en-us/azure/governance/policy/concepts/effect-modify
https://learn.microsoft.com/azure/governance/policy/tutorials/govern-tags
https://learn.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources?WT.mc_id=AZ-MVP-5004810

✗ **D** Apply the Departments tag directly to RG1.
This uses the wrong tag name and applies a tag only to the resource group itself. Resource-group tags are not automatically inherited by resources in the group.

https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/tag-policies
https://learn.microsoft.com/en-us/previous-versions/azure/azure-resource-manager/management/tag-resources

---

Question 12

Single choice · Domain: D1 Manage Azure identities and governance › Manage access to Azure resources

You have an Azure subscription that contains a user named User1.

You need to ensure that User1 can deploy virtual machines and manage virtual networks. The solution must use the principle of least privilege.

Which role-based access control (RBAC) role should you assign to User1?

A. Owner
B. Virtual Machine Administrator Login
C. Contributor
D. Virtual Machine Contributor

Answer: C. Contributor

Explanation

Among the listed single roles, Contributor is the role that lets User1 deploy virtual machines and manage virtual networks. It can manage Azure resources but cannot grant access to others, unlike Owner; it is broader than a narrowly scoped combination of resource-specific roles, but the other listed roles do not cover both requirements. Assign it at the narrowest scope that contains the resources User1 must manage.

https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/compute
https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles?WT.mc_id=MVP_319025
https://learn.microsoft.com/azure/role-based-access-control/built-in-roles/networking
https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/privileged

✗ **A** Owner
Owner can manage resources and grant access to others, which exceeds the stated needs. Contributor covers the required resource management without Owner's permission to assign access.

https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles?WT.mc_id=MVP_319025
https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/privileged

✗ **B** Virtual Machine Administrator Login
This role grants sign-in permissions for virtual machines; it does not provide the permissions to deploy virtual machines or manage virtual networks. It therefore does not meet either resource-management requirement.

https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/identity
https://learn.microsoft.com/azure/active-directory/devices/howto-vm-sign-in-azure-ad-linux

✓ **C** Contributor
Contributor can create and manage Azure resources, including virtual machines and virtual networks, but cannot grant access to others. Of the listed single-role choices, it is the role that covers both required tasks without the additional access-management capability of Owner.

https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/compute
https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles?WT.mc_id=MVP_319025
https://learn.microsoft.com/azure/role-based-access-control/built-in-roles/networking

✗ **D** Virtual Machine Contributor
Virtual Machine Contributor can manage virtual machines, but its scope is compute resources rather than virtual network management. User1 would still lack the permissions needed to manage virtual networks.

https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/compute
https://learn.microsoft.com/azure/role-based-access-control/built-in-roles/networking

---

Question 13

Yes / No · Domain: D1 Manage Azure identities and governance › Manage access to Azure resources

You have an Azure subscription named Sub1 that contains the resources shown in the following table.

Name	Description
RG2	Resource group
VNet2	Virtual network in RG2 that contains a subnet named Subnet2

The subscription contains the users shown in the following table.

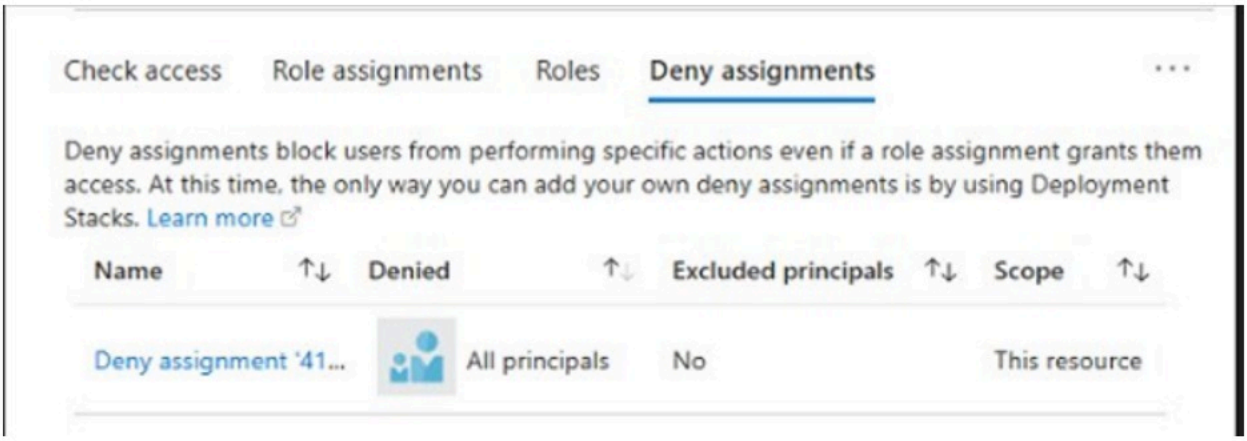
Name	Role	Role scope
Admin1	Network Contributor	Sub1
Admin2	Contributor	RG2
Admin3	Owner	VNet2

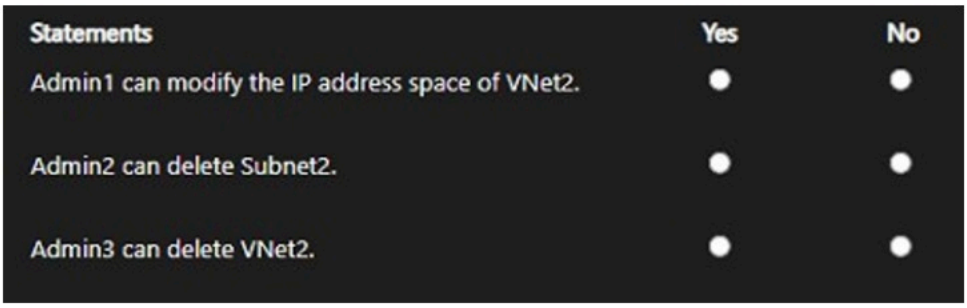
VNet2 was created by using the following cmdlet.

```
New-AzResourceGroupDeploymentStack -Name Deploy1 -ResourceGroupName RG2 -TemplateFile Deplo
```

The screenshot shows the Deny assignments tab. It states: “Deny assignments block users from performing specific actions even if a role assignment grants them access. At this time, the only way you can add your own deny assignments is by using Deployment Stacks. Learn more.” The deny assignment table shows: Name: Deny assignment '41...; Denied: All principals; Excluded principals: No; Scope: This resource.

Free demo · full exam: 507 questions





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

Statement	Yes	No
Admin1 can modify the IP address space of VNet2.	☐	☐
Admin2 can delete Subnet2.	☐	☐
Admin3 can delete VNet2.	☐	☐

Answer

- Admin1 can modify the IP address space of VNet2. **Yes**
- Admin2 can delete Subnet2. **Yes**
- Admin3 can delete VNet2. **No**

Explanation

Admin1 has Network Contributor at subscription scope, so they can modify VNet2's IP address space; the deployment-stack deny assignment is configured for deletion, not modification. Admin2's Contributor role at RG2 permits deleting Subnet2, while the deny assignment shown for VNet2 does not prevent that child-resource deletion. Admin3 has Owner on VNet2, but the DenyDelete setting blocks deletion of VNet2 for all principals, with no exclusions.

https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-subnet?tabs=azure-portal
https://learn.microsoft.com/en-us/azure/virtual-network/manage-virtual-network
https://learn.microsoft.com/en-us/azure/role-based-access-control/deny-assignments
https://learn.microsoft.com/en-us/azure/azure-resource-manager/bicep/deployment-stacks?tabs=azure-cli
https://learn.microsoft.com/en-us/azure/role-based-access-control/permissions/networking

✓ **Statement 1** Admin1 can modify the IP address space of VNet2.
Yes. Network Contributor at the subscription scope includes permissions to manage virtual networks, including modifying VNet2's address space. The DenyDelete setting blocks deletion, not this modification.

https://learn.microsoft.com/en-us/azure/virtual-network/manage-virtual-network
https://learn.microsoft.com/en-us/azure/role-based-access-control/deny-assignments
https://learn.microsoft.com/en-us/azure/azure-resource-manager/bicep/deployment-stacks?tabs=azure-cli
https://learn.microsoft.com/en-us/azure/role-based-access-control/permissions/networking

✓ **Statement 2** Admin2 can delete Subnet2.
Yes. Contributor at RG2 includes permission to delete subnet resources in that resource group. The deny assignment shown is on VNet2 and its DenyDelete setting prevents deletion of the protected resource; it does not prevent deleting Subnet2.

https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-subnet?tabs=azure-portal
https://learn.microsoft.com/en-us/azure/role-based-access-control/deny-assignments
https://learn.microsoft.com/en-us/azure/azure-resource-manager/bicep/deployment-stacks?tabs=azure-cli
https://learn.microsoft.com/en-us/azure/role-based-access-control/permissions/networking

✗ **Statement 3** Admin3 can delete VNet2.
No. Although Owner at the VNet2 scope would otherwise allow Admin3 to delete it, the deployment stack created a DenyDelete assignment that applies to all principals and has no excluded principals. That deny assignment blocks deletion of VNet2.

https://learn.microsoft.com/en-us/azure/role-based-access-control/deny-assignments
https://learn.microsoft.com/en-us/azure/azure-resource-manager/bicep/deployment-stacks?tabs=azure-cli
https://learn.microsoft.com/en-us/dotnet/api/microsoft.azure.management.resources.deploymentstacks.models.denysettings?view=az-ps-latest
https://learn.microsoft.com/en-us/javascript/api/%40azure/arm-resourcesdeploymentstacks/denysettingsmode?view=azure-node-latest

---

Question 14

Single choice · Domain: D1 Manage Azure identities and governance › Manage Azure subscriptions and governance

You have an Azure subscription.

Your company has three external partners. You plan to deploy 10 virtual machines that will be used by the partners.

You need to ensure that you can track the partners' use of the virtual machines by using Microsoft Cost Management. The solution must minimize administrative effort.

What should you do first?

A. Define a virtual machine naming strategy.
B. Enable VM insights.
C. Create three host groups.
D. Create a tag for each partner.

Answer: D. Create a tag for each partner.

Explanation

Create a tag for each partner so you can apply the appropriate partner tag to the virtual machines and use Microsoft Cost Management to group or filter costs by that tag. This provides a direct way to track each partner's VM usage without creating separate host groups or relying on naming conventions.

https://learn.microsoft.com/en-us/azure/cost-management-billing/costs/cost-allocation-introduction
https://learn.microsoft.com/en-us/azure/cost-management-billing/costs/group-filter

✗ **A** Define a virtual machine naming strategy.
A naming strategy can make the VMs easier to identify, but names are not the cost-allocation mechanism needed to track each partner's costs in Cost Management. Tags let you categorize resources and filter or group cost data by partner.

https://learn.microsoft.com/en-us/azure/cost-management-billing/costs/cost-allocation-introduction
https://learn.microsoft.com/en-us/azure/cost-management-billing/costs/group-filter
https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/resource-naming

✗ **B** Enable VM insights.
VM insights provides monitoring information about virtual machine performance and health, not partner-based cost tracking in Microsoft Cost Management. It would add configuration effort without meeting the stated cost-tracking requirement.

https://learn.microsoft.com/en-us/azure/azure-monitor/vm/vminsights-performance
https://learn.microsoft.com/en-us/azure/azure-monitor/vm/monitor-virtual-machine

✗ **C** Create three host groups.
Host groups are used to organize dedicated hosts, not to categorize VM costs by external partner. Creating them would add administrative effort and would not be the direct Cost Management approach for tracking partner usage.

https://learn.microsoft.com/en-us/azure/virtual-machines/dedicated-hosts-how-to
https://learn.microsoft.com/en-us/azure/virtual-machines/dedicated-hosts

✓ **D** Create a tag for each partner.
Tags let you identify which partner each VM is associated with, and Cost Management can group or filter cost data using tags. This directly supports partner-level tracking while avoiding the extra infrastructure organization required by host groups.

https://learn.microsoft.com/en-us/azure/cost-management-billing/costs/cost-allocation-introduction
https://learn.microsoft.com/en-us/azure/cost-management-billing/costs/group-filter

Dumpsgate

Question 15

Single choice · Domain: D1 Manage Azure identities and governance › Manage Microsoft Entra users and groups

You have an Azure AD tenant named adatum.com that contains the groups shown in the following table.

Name	Member of
Group1	*None*
Group2	Group1
Group3	Group2

Name	Member of
User1	Group1
User2	Group2
User3	Group3
User4	*None*

Adatum.com contains the users shown in the following table.

You assign the Azure AD Premium P2 license to Group l and User4.

Which users are assigned the Azure AD Premium P2 license?

A. User4 only
B. User1 and User4 only
C. User1. User2. and User4 only
D. User1, User2, User3, and User4

Answer: B. User1 and User4 only

Explanation

Group1 licensing covers its direct user member, User1; it does not extend through nested groups to User2 or User3. User4 receives the license because it is assigned directly to that user, so the licensed users are User1 and User4 only. [6]

https://learn.microsoft.com/en-us/entra/fundamentals/license-users-groups

✗ **A** User4 only
User4 receives the license through the direct user assignment. However, User1 is also a direct member of Group1, which has the license assigned, so User1 is licensed too.

https://learn.microsoft.com/en-us/entra/fundamentals/license-users-groups

✓ **B** User1 and User4 only
User1 is a direct member of the licensed Group1, and User4 is assigned the license directly. User2 and User3 belong to nested groups, and the license assigned to Group1 does not propagate through nested group membership.

https://learn.microsoft.com/en-us/entra/fundamentals/license-users-groups

✗ **C** User1, User2, and User4 only
User1 and User4 are licensed, but User2 is a member of Group2 rather than a direct member of Group1. The Group1 license does not reach User2 through the nested group.

https://learn.microsoft.com/en-us/entra/fundamentals/license-users-groups

✗ **D** User1, User2, User3, and User4
User1 and User4 are licensed, but User2 and User3 are members of nested groups, not direct members of Group1. The Group1 license does not extend to those users through Group2 or Group3.
https://learn.microsoft.com/en-us/entra/fundamentals/license-users-groups

Question 16

Single choice · Domain: D1 Manage Azure identities and governance › Manage Microsoft Entra users and groups

You have an Azure subscription that contains two users named User1 and User2.

You need to enable self-service password reset (SSPR) for User1. The solution must ensure that SSPR is disabled for User2.

What should you do first?

A. Create an authentication context.
B. Configure an Authentication methods policy.
C. Create a group.
D. Disable security defaults.

Answer: C. Create a group.

Explanation

To enable SSPR for User1 while keeping it disabled for User2, configure SSPR for a selected group containing User1 but not User2. Creating that group is the first step; you can then add User1 and select the group as the SSPR scope. [1][2]
https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr
https://learn.microsoft.com/en-us/azure/active-directory/authentication/quickstart-sspr

✗ **A** Create an authentication context.
An authentication context is not the mechanism for selecting which users are enabled for SSPR. The requirement is met by scoping SSPR to a group that contains User1 but not User2.
https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr
https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-policy

✗ **B** Configure an Authentication methods policy.
An Authentication methods policy manages which authentication methods are available; it does not establish the user scope needed to enable SSPR for User1 while excluding User2. Create the group for the SSPR scope first.
https://learn.microsoft.com/azure/active-directory/authentication/concept-authentication-methods-manage
https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-policy

✓ **C** Create a group.
SSPR can be scoped to selected users or groups. Creating a group allows you to include User1 and exclude User2, after which you can configure SSPR for that group.
https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr
https://learn.microsoft.com/en-us/azure/active-directory/authentication/quickstart-sspr

✗ **D** Disable security defaults.
Disabling security defaults does not provide the user-specific SSPR scope required here. A group is needed to target User1 without enabling SSPR for User2.

Question 17

Single choice · Domain: D1 Manage Azure identities and governance › Manage access to Azure resources

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 Adatum and an Azure Subscription named Subscription1. Adatum contains a group named Developers. Subscription1 contains a resource group named Dev.

You need to provide the Developers group with the ability to create Azure logic apps in the Dev resource group.

Solution: On Subscription1, you assign the Logic App Operator role to the Developers group.

Does this meet the goal?

A. Yes
B. No

Answer: B. No

Explanation

No. Assigning the Logic App Operator role at the subscription scope gives Developers permissions that apply within the Dev resource group, but that role does not include permission to create logic apps. The group needs a role that grants logic app creation, such as Logic App Contributor, scoped to Dev or a parent scope.[2]

https://learn.microsoft.com/azure/role-based-access-control/built-in-roles/integration

✗ **A** Yes
The subscription scope would cover the Dev resource group, but scope alone is not enough: the Logic App Operator role does not grant permission to create logic apps.[2]

https://learn.microsoft.com/azure/role-based-access-control/built-in-roles/integration

✓ **B** No
Logic App Operator permissions allow operations such as reading and enabling or disabling logic apps, but do not include creating them. Therefore, assigning this role to Developers on Subscription1 does not meet the requirement.[2]

https://learn.microsoft.com/azure/role-based-access-control/built-in-roles/integration

Question 18

Single choice · Domain: D1 Manage Azure identities and governance › Manage Microsoft Entra users and groups

You have a Microsoft Entra tenant named contoso.com.

You collaborate with an external partner named fabrikam.com.

You plan to invite users in fabrikam.com to the contoso.com tenant.

You need to ensure that invitations can be sent only to fabrikam.com users.

What should you do in the Microsoft Entra admin center?

A. From External collaboration settings, configure the Guest user access restrictions settings.
B. From Cross-tenant access settings, configure the Tenant restrictions settings.
C. From External collaboration settings, configure the Collaboration restrictions settings.
D. From Cross-tenant access settings, configure the Microsoft cloud settings.

Answer: C. From External collaboration settings, configure the Collaboration restrictions settings.

Explanation

To restrict invitations to users from fabrikam.com, configure the domain allow/deny list under External collaboration settings. The Collaboration restrictions setting lets you allow invitations only for specified domains, so you can allow fabrikam.com and block other domains. This setting controls which external users can be invited to the contoso.com tenant.

https://learn.microsoft.com/en-us/entra/external-id/allow-deny-list
https://learn.microsoft.com/entra/external-id/external-collaboration-settings-configure

✗ **A** From External collaboration settings, configure the Guest user access restrictions settings.
Guest user access restrictions control what guest users can see or do after they have access to the tenant. They do not limit invitations to users from particular domains.

https://learn.microsoft.com/en-us/entra/identity/users/users-restrict-guest-permissions
https://learn.microsoft.com/entra/external-id/external-collaboration-settings-configure

✗ **B** From Cross-tenant access settings, configure the Tenant restrictions settings.
Cross-tenant access settings govern trust and access between organizations' Microsoft Entra tenants; they are not the setting for limiting guest invitations by email domain. To restrict invitees to fabrikam.com, use the domain restrictions in External collaboration settings.

https://learn.microsoft.com/entra/external-id/external-collaboration-settings-configure
https://learn.microsoft.com/entra/external-id/cross-tenant-access-overview

✓ **C** From External collaboration settings, configure the Collaboration restrictions settings.
Collaboration restrictions let you allow or block invitations based on the external user's domain. Configure an allow list containing fabrikam.com so invitations can be sent only to users from that domain.

https://learn.microsoft.com/en-us/entra/external-id/allow-deny-list
https://learn.microsoft.com/entra/external-id/external-collaboration-settings-configure

✗ **D** From Cross-tenant access settings, configure the Microsoft cloud settings.
Microsoft cloud settings configure collaboration with organizations in other Microsoft cloud environments, such as separate national clouds. They do not restrict invitations to a particular domain such as fabrikam.com.

https://learn.microsoft.com/entra/external-id/cross-tenant-access-overview

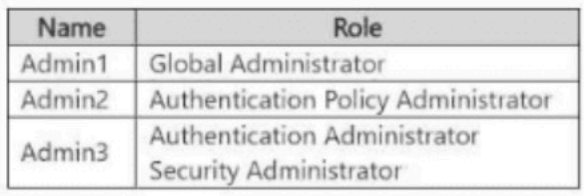
Free demo · full exam: 507 questions

Question 19

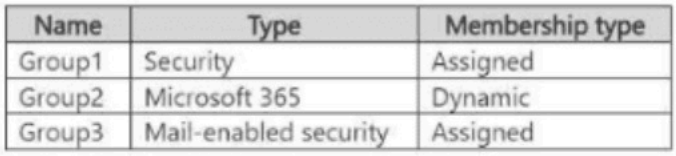
Hotspot (dropdowns) · Domain: D1 Manage Azure identities and governance › Manage Microsoft Entra users and groups

You have a Microsoft Entra tenant that contains the users shown in the following table.

Name	Role
Admin1	Global Administrator
Admin2	Authentication Policy Administrator
Admin3	Authentication Administrator; Security Administrator



Name	Role
Admin1	Global Administrator
Admin2	Authentication Policy Administrator
Admin3	Authentication Administrator Security Administrator



Name	Type	Membership type
Group1	Security	Assigned
Group2	Microsoft 365	Dynamic
Group3	Mail-enabled security	Assigned

The tenant contains the groups shown in the following table.

Name	Type	Membership type
Group1	Security	Assigned
Group2	Microsoft 365	Dynamic
Group3	Mail-enabled security	Assigned

Self-service password reset (SSPR) needs to be configured for the tenant.

Which users can configure SSPR, and for which group can SSPR be enabled? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Users: Admin1 only | Admin2 only | Admin3 only | Admin1 and Admin2 only | Admin2 and Admin3 only | Admin1, Admin2, and Admin3

Group: Group1 only | Group2 only | Group1 or Group2 only | Group1 or Group3 only | Group1, Group2, or Group3

Answer

- Users: **Admin1 and Admin2 only**
- Group: **Group1 or Group3 only**

Explanation

Admin1 can configure SSPR as a Global Administrator, and Admin2 can configure it as an Authentication Policy Administrator. Admin3's Authentication Administrator and Security Administrator roles do not grant the required SSPR configuration permission. SSPR can be enabled for Group1 and Group3 because they are security groups; Group2 is a Microsoft 365 group, so it is not eligible for this SSPR group selection.

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-policy
https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr
https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

✗ **Users: Admin1 only** Admin1 only
Admin1 can configure SSPR because Global Administrators have the required permissions. However, Admin2, as an Authentication Policy Administrator, can also configure SSPR, so Admin1 only is incomplete.

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-policy
https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

✗ **Users: Admin2 only** Admin2 only
Admin2 can configure SSPR as an Authentication Policy Administrator. Admin1 can also configure it as a Global Administrator, so Admin2 only is incomplete.

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-policy
https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

✗ **Users: Admin3 only** Admin3 only
Admin3 has the Authentication Administrator and Security Administrator roles, but neither role gives Admin3 the required SSPR configuration permission in this scenario. Admin1 and Admin2 have roles that do grant that permission.

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-policy
https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

✓ **Users: Admin1 and Admin2 only** Admin1 and Admin2 only
Global Administrators and Authentication Policy Administrators can configure SSPR, so Admin1 and Admin2 qualify. Admin3's listed roles do not provide that configuration permission.

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-policy
https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

✗ **Users: Admin2 and Admin3 only** Admin2 and Admin3 only
Admin2 can configure SSPR as an Authentication Policy Administrator. Admin3's Authentication Administrator and Security Administrator roles do not grant the required permission, and this choice also omits Admin1, a Global Administrator.

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-policy
https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

✗ **Users: Admin1, Admin2, and Admin3** Admin1, Admin2, and Admin3
Admin1 and Admin2 can configure SSPR based on their assigned roles. Admin3's roles do not grant the required SSPR configuration permission, so including Admin3 makes this choice incorrect.

Free demo · full exam: 507 questions

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-policy
https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

✗ **Group: Group1 only** Group1 only
Group1 is a security group and can be selected for SSPR. Group3 is also a mail-enabled security group and is eligible, so restricting the choice to Group1 is incomplete.

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-policy
https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr

✗ **Group: Group2 only** Group2 only
Group2 is a Microsoft 365 group, which is not eligible for enabling SSPR in this scenario. The eligible groups are Group1 and Group3.

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-policy
https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr

✗ **Group: Group1 or Group2 only** Group1 or Group2 only
Group1 is eligible because it is a security group. Group2 is a Microsoft 365 group and is not eligible, while Group3 is also eligible because it is a mail-enabled security group.

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-policy
https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr

✓ **Group: Group1 or Group3 only** Group1 or Group3 only
Group1 is a security group, and Group3 is a mail-enabled security group; both are eligible for SSPR. Group2 is a Microsoft 365 group and is not eligible.

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-policy
https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr

✗ **Group: Group1, Group2, or Group3** Group1, Group2, or Group3
Group1 and Group3 are eligible security groups. Group2 is a Microsoft 365 group and is not eligible, so this choice includes an invalid group.

https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-policy
https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr

Question 20

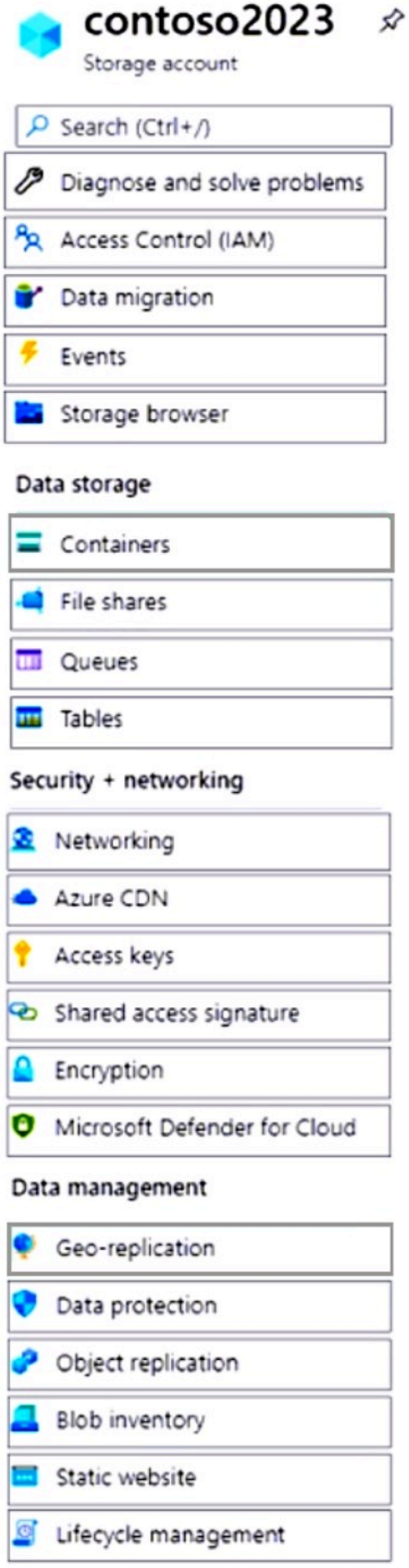
Multiple choice · Domain: D2 Implement and manage storage › Configure access to storage

You have a Microsoft Entra user named User1 and a read-access geo-redundant storage (RA-GRS) account named contoso2023. You need to meet the following requirements:

- User1 must be able to write blob data to contoso2023.
- The contoso2023 account must fail over to its secondary endpoint.

Which two settings should you configure? To answer, select the appropriate settings in the answer area. NOTE Each correct selection is worth one point.

Free demo · full exam: 507 questions


contoso2023
Storage account
Search (Ctrl+/)
Diagnose and solve problems
Access Control (IAM)
Data migration
Events
Storage browser
Data storage
Containers
File shares
Queues
Tables
Security + networking
Networking
Azure CDN
Access keys
Shared access signature
Encryption
Microsoft Defender for Cloud
Data management
Geo-replication
Data protection
Object replication
Blob inventory
Static website
Lifecycle management

Answer

- A. **Access Control (IAM)**
- C. **Geo-replication**

Explanation

Configure Access Control (IAM) to grant User1 permission to write blob data, such as through an appropriate Azure role assignment. Configure Geo-replication to initiate account failover from the primary to the secondary endpoint; the account's RA-GRS redundancy provides a readable secondary but does not itself perform failover. Therefore, the settings are A and C.

https://learn.microsoft.com/azure/storage/common/storage-initiate-account-failover
https://learn.microsoft.com/azure/storage/common/storage-auth-aad-rbac-portal
https://learn.microsoft.com/en-us/azure/storage/blobs/authorize-data-operations-portal

✓ **A** Access Control (IAM)
Use IAM role assignments to grant User1 the required blob data write permissions, for example by assigning an appropriate storage data role. This addresses the requirement for a Microsoft Entra user to write blob data.

https://learn.microsoft.com/azure/storage/common/storage-auth-aad-rbac-portal
https://learn.microsoft.com/en-us/azure/storage/blobs/authorize-data-operations-portal

✗ **B** Access keys
Account access keys provide shared-key authorization, rather than granting User1 blob data access through Microsoft Entra role-based access control. This is not the setting needed to authorize User1 as specified.

https://learn.microsoft.com/azure/storage/common/storage-auth-aad-rbac-portal
https://learn.microsoft.com/en-us/azure/storage/blobs/authorize-data-operations-portal

✓ **C** Geo-replication
Geo-replication settings are where you manage the storage account's replication and initiate failover to its secondary endpoint. This addresses the requirement that contoso2023 fail over.

https://learn.microsoft.com/azure/storage/common/storage-initiate-account-failover
https://learn.microsoft.com/en-us/azure/storage/common/storage-initiate-account-failover
https://learn.microsoft.com/en-us/azure/storage/common/storage-failover-customer-managed-unplanned?tabs=grs-ra-grs

✗ **D** Data protection
Data protection settings configure features such as blob recovery and retention; they do not grant User1 write permissions or initiate account failover. Geo-replication is the relevant setting for failing over to the secondary endpoint.

https://learn.microsoft.com/azure/storage/common/storage-initiate-account-failover
https://learn.microsoft.com/en-us/azure/storage/blobs/versioning-enable
https://learn.microsoft.com/en-us/azure/storage/blobs/soft-delete-blob-enable

Question 21

Single choice · Domain: D2 Implement and manage storage › Configure access to storage

Your organization has a storage account containing sensitive customer data in Azure Blob Storage. Currently, the storage account is accessible from any IP address on the internet. You need to restrict access so that only resources within your organization's on-premises network and specific Azure virtual networks can access the blobs.

What is the best approach to implement this requirement?

A. Configure Azure Storage firewall rules to deny all traffic by default, then add allow rules for your on- premises IP range and the subnet address spaces of your Azure virtual networks.

B. Use a shared access signature (SAS) token with a short expiration time and distribute it only to authorized users to access the storage account.

C. Create a private endpoint for the storage account within a virtual network and disable public network access, then configure a site-to-site VPN to connect your on-premises network to the virtual network.

D. Apply an Azure key vault to encrypt all data in the storage account and restrict the key vault access using network rules.

Answer: A. Configure Azure Storage firewall rules to deny all traffic by default, then add allow rules for your on- premises IP range and the subnet address spaces of your Azure virtual networks.

Explanation

Azure Storage firewall rules let you deny access by default and allow only the organization’s on-premises IP range and selected Azure virtual networks. For the virtual network rules, the relevant subnets must be configured to use the required storage service endpoint. This directly restricts which networks can reach the blobs without requiring a private-endpoint and VPN redesign.

https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security-virtual-networks

✓ **A** Configure Azure Storage firewall rules to deny all traffic by default, then add allow rules for your on-premises IP range and the subnet address spaces of your Azure virtual networks.
This restricts network access to the specified on-premises IP range and selected virtual networks, matching the requirement. Azure virtual network rules rely on configuring the appropriate storage service endpoint on the allowed subnets.

https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security-virtual-networks

✗ **B** Use a shared access signature (SAS) token with a short expiration time and distribute it only to authorized users to access the storage account.
A SAS can limit delegated access by permissions and validity period, but it does not by itself restrict the storage account to the organization’s on-premises network and selected virtual networks. The account would remain accessible over the public network to callers with a valid token.

https://learn.microsoft.com/en-us/azure/storage/common/storage-sas-overview

✗ **C** Create a private endpoint for the storage account within a virtual network and disable public network access, then configure a site-to-site VPN to connect your on-premises network to the virtual network.
A private endpoint with public network access disabled can provide private connectivity, and a VPN can extend that connectivity to on-premises. However, this is a more extensive private-connectivity design than the requested network allow-list; the storage firewall rules in A directly allow the specified on-premises IP range and virtual networks.

https://learn.microsoft.com/en-us/azure/private-link/tutorial-private-endpoint-storage-portal

Free demo · full exam: 507 questions

https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security-virtual-networks

✗ **D** Apply an Azure key vault to encrypt all data in the storage account and restrict the key vault access using network rules.
Key Vault network rules restrict access to the vault, not which networks can connect to the storage account's blob endpoint. Encryption protects data but does not meet the requirement to restrict blob access by source network.

https://learn.microsoft.com/cli/azure/keyvault/network-rule
https://learn.microsoft.com/en-us/azure/storage/common/secure-storage

Question 22

Single choice · Domain: D2 Implement and manage storage › Configure Azure Files and Azure Blob Storage

Your organization stores customer data in an Azure storage account using the hot tier. Compliance auditors have flagged a risk that data older than 90 days should be moved to cool storage to reduce costs and meet data lifecycle policies. You need to automate this transition. Which Azure storage feature should you implement?

A. Azure Blob Storage lifecycle management policy with a rule to transition blobs from hot to cool tier after 90 days
B. Azure Automation runbook scheduled daily to move blobs to cool tier if their last access time exceeds 90 days
C. Azure Data Factory pipeline with a monthly copy activity to export aged blobs to cool storage
D. Manual audit process with PowerShell scripts executed quarterly to identify and move aged blobs
E. Azure Archive tier configuration applied to all blobs upon creation

Answer: A. Azure Blob Storage lifecycle management policy with a rule to transition blobs from hot to cool tier after 90 days

Explanation

Azure Blob Storage lifecycle management policies automate actions on blobs based on age, including tier transitions. A rule can move blobs from the hot tier to the cool tier after 90 days, matching the stated cost and lifecycle requirements. The policy avoids relying on recurring custom jobs or manual audits.

https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-structure
https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-access-tiers
https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-overview?tabs=azure-powershell

✓ **A** Azure Blob Storage lifecycle management policy with a rule to transition blobs from hot to cool tier after 90 days
Lifecycle management policies can apply tier transitions based on blob age. Configuring a rule to move eligible blobs from hot to cool after 90 days directly automates the compliance requirement.

https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-structure
https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-access-tiers
https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-overview?tabs=azure-powershell

✗ **B** Azure Automation runbook scheduled daily to move blobs to cool tier if their last access time exceeds 90 days
A runbook could be built to perform tier changes, but it requires custom scripting and scheduling for an action that lifecycle management handles natively. It also bases the condition on last access time,

whereas the requirement specifies data older than 90 days.

https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-structure
https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-access-tiers
https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-overview?tabs=azure-powershell

✗ **C** Azure Data Factory pipeline with a monthly copy activity to export aged blobs to cool storage
A monthly copy pipeline is not the direct lifecycle tier-transition feature requested and may copy data rather than simply change its access tier. It adds pipeline management when a lifecycle policy can transition qualifying blobs automatically.

https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-structure
https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-access-tiers
https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-overview?tabs=azure-powershell

✗ **D** Manual audit process with PowerShell scripts executed quarterly to identify and move aged blobs
Quarterly manual execution does not provide the automated, policy-based transition the organization needs. It can also leave blobs in the hot tier beyond the 90-day threshold while waiting for the next audit.

https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-structure
https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-overview?tabs=azure-powershell

✗ **E** Azure Archive tier configuration applied to all blobs upon creation
This would place all blobs in the archive tier immediately rather than moving only data older than 90 days to cool storage. The requested destination is the cool tier, and the transition should depend on blob age.

https://learn.microsoft.com/en-us/azure/storage/blobs/access-tiers-online-manage
https://learn.microsoft.com/en-us/azure/storage/blobs/access-tiers-best-practices
https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-access-tiers

Question 23

Single choice · Domain: D2 Implement and manage storage › Configure access to storage

Your organization stores sensitive customer data in Azure Blob Storage. You currently allow storage account access via public endpoint, but security requirements now mandate that access must occur only through a private endpoint. You also need to ensure that even if someone obtains a storage account key, they cannot access the data. Which two actions should you take?

A. Disable public network access to the storage account and implement shared access signature (SAS) token-based authentication with time-limited expiration

B. Disable public network access to the storage account and configure a private endpoint connected to your virtual network

C. Enable Azure Firewall rules to block all public traffic and rotate storage account keys monthly

D. Implement IP-based firewall rules to allow only specific external IP addresses and use managed identities for authentication

E. Use Azure DDoS protection and require mutual TLS certificates for all storage account connections

Answer: B. Disable public network access to the storage account and configure a private endpoint connected to your virtual network

Explanation

B combines the two network actions needed for private-only access: disable public network access and create a private endpoint connected to the virtual network. This makes the storage account reachable

Free demo · full exam: 507 questions

through the private network path rather than its public endpoint, so possession of a key alone does not provide access from the public internet. A private endpoint is a network control, however; if the requirement is that a key must be unusable even to someone who can reach the private endpoint, shared-key authorization must also be disabled, which no option explicitly states.

https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security-set-default-access
https://learn.microsoft.com/en-us/azure/private-link/tutorial-private-endpoint-storage-portal
https://learn.microsoft.com/azure/storage/common/shared-key-authorization-prevent

✗ **A** Disable public network access to the storage account and implement shared access signature (SAS) token-based authentication with time-limited expiration
Disabling public network access is relevant, but this option does not configure a private endpoint for authorized access through the virtual network. Time-limited SAS tokens also do not establish the required private network path, and SAS authorization is not the same as disabling shared-key authorization.

https://learn.microsoft.com/azure/storage/common/shared-key-authorization-prevent
https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security-set-default-access
https://learn.microsoft.com/en-us/azure/private-link/tutorial-private-endpoint-storage-portal

✓ **B** Disable public network access to the storage account and configure a private endpoint connected to your virtual network
This disables access through the public endpoint and provides private connectivity to the storage account through the virtual network. A key by itself cannot bypass that network restriction from the public internet. The private endpoint is a network control, though; disabling shared-key authorization would be needed to make an obtained key unusable even for someone who can reach the private endpoint.

https://learn.microsoft.com/azure/storage/common/shared-key-authorization-prevent
https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security-set-default-access
https://learn.microsoft.com/en-us/azure/private-link/tutorial-private-endpoint-storage-portal

✗ **C** Enable Azure Firewall rules to block all public traffic and rotate storage account keys monthly
Rotating keys does not prevent someone from using a key they have obtained before it is rotated. This option also does not specify disabling the storage account's public network access and configuring a private endpoint, as required for private-only access.

https://learn.microsoft.com/azure/storage/common/shared-key-authorization-prevent
https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security-set-default-access
https://learn.microsoft.com/en-us/azure/private-link/tutorial-private-endpoint-storage-portal

✗ **D** Implement IP-based firewall rules to allow only specific external IP addresses and use managed identities for authentication
Allowing specific external IP addresses still permits access through the public endpoint, rather than restricting access to a private endpoint. Managed identities can avoid relying on account keys for supported clients, but this option does not meet the stated private-only networking requirement.

https://learn.microsoft.com/en-us/azure/storage/common/secure-storage
https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security-set-default-access
https://learn.microsoft.com/en-us/azure/private-link/tutorial-private-endpoint-storage-portal

✗ **E** Use Azure DDoS protection and require mutual TLS certificates for all storage account connections
DDoS protection addresses availability, and mutual TLS is not the network configuration asked for here. Neither action disables public network access or establishes a private endpoint for the storage account.

https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security-set-default-access
https://learn.microsoft.com/en-us/azure/private-link/tutorial-private-endpoint-storage-portal

Free demo · full exam: 507 questions

Question 24

Single choice · Domain: D2 Implement and manage storage › Configure and manage storage accounts

Your organization is planning to migrate a traditional on-premises relational database to Azure. The database supports critical business applications and must maintain high availability with automatic failover. You need a managed service that requires minimal administrative overhead and supports automatic backups, georedundancy, and transparent failover to a replica.

Which Azure database service should you implement?

A. Azure SQL Database with Business Critical tier and active geo-replication
B. Azure Database for PostgreSQL single server with manual backup and replication setup
C. Azure Virtual Machine with SQL Server installed and Storage Spaces Direct
D. Azure Cosmos DB with multi-region replication and eventual consistency

Answer: A. Azure SQL Database with Business Critical tier and active geo-replication

Explanation

Azure SQL Database is a managed relational database service, so it is a natural fit for migrating a traditional relational workload while reducing administrative overhead. The Business Critical tier provides high-availability capabilities, and geo-replication supports a secondary database in another region. For automatic, transparent failover, configure the geo-replicated databases with an auto-failover group. Azure SQL Database also provides managed backups.

https://learn.microsoft.com/en-us/azure/azure-sql/database/active-geo-replication-overview?view=azuresql-db
https://learn.microsoft.com/en-us/azure/reliability/reliability-sql-database
https://learn.microsoft.com/azure/azure-sql/database/auto-failover-group-overview
https://learn.microsoft.com/en-us/azure/sql-database/sql-database-service-tier-business-critical

✓ **A** Azure SQL Database with Business Critical tier and active geo-replication
This is the managed relational option, and the Business Critical tier and geo-replication address high availability and a regional replica. Configure the geo-replicated databases with an auto-failover group to provide automatic failover and a stable connection endpoint for applications. Azure SQL Database also handles backups as a managed service.

https://learn.microsoft.com/en-us/azure/azure-sql/database/active-geo-replication-overview?view=azuresql-db
https://learn.microsoft.com/en-us/azure/reliability/reliability-sql-database
https://learn.microsoft.com/azure/azure-sql/database/auto-failover-group-overview
https://learn.microsoft.com/en-us/azure/sql-database/sql-database-service-tier-business-critical

✗ **B** Azure Database for PostgreSQL single server with manual backup and replication setup
The option explicitly calls for manual backup and replication setup, which conflicts with the requirement for minimal administrative overhead and automatic backups. It also does not specify the transparent automatic failover configuration required by the scenario.

https://learn.microsoft.com/en-us/azure/backup/backup-azure-database-postgresql
https://learn.microsoft.com/en-us/azure/backup/backup-azure-database-postgresql-server-faq

✗ **C** Azure Virtual Machine with SQL Server installed and Storage Spaces Direct
Running SQL Server on a virtual machine leaves more infrastructure and database administration to the organization than a managed database service. Storage Spaces Direct alone does not provide the requested managed, georedundant database failover experience.

✗ **D** Azure Cosmos DB with multi-region replication and eventual consistency
Cosmos DB offers distributed multi-region capabilities, but it is a NoSQL database rather than a relational database service for this traditional relational workload. Its eventual consistency option also does not make it the appropriate relational migration target.

Free demo · full exam: 507 questions

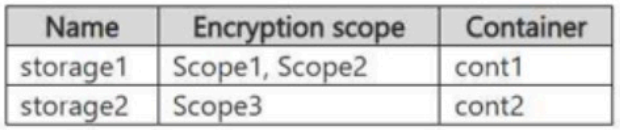
https://learn.microsoft.com/en-us/azure/cosmos-db/distributed-nosql
https://learn.microsoft.com/azure/cosmos-db/consistency-levels
https://learn.microsoft.com/en-us/azure/cosmos-db/use-cases
https://learn.microsoft.com/en-us/cosmos-db/overview

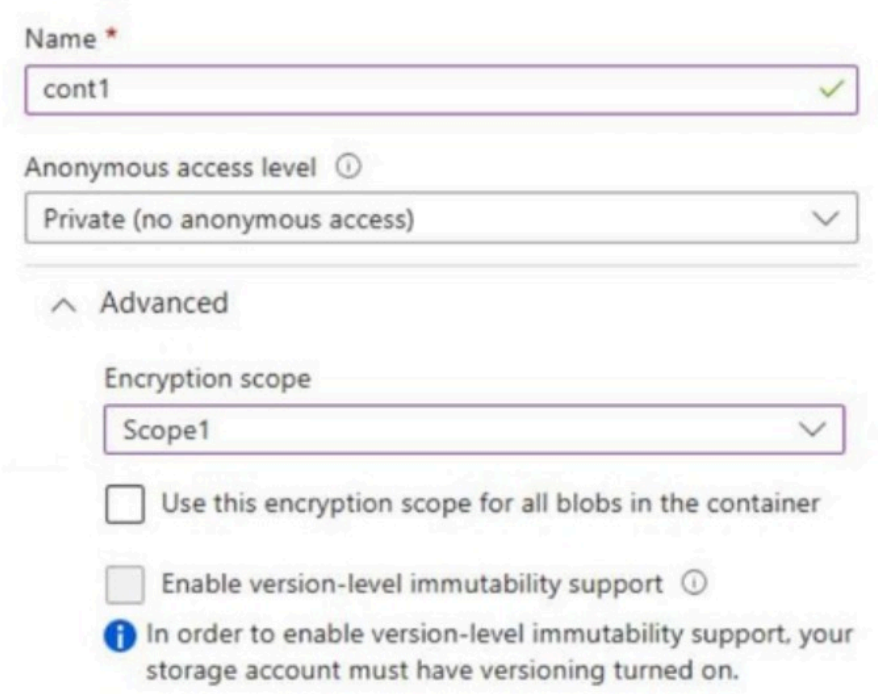
Question 25

Yes / No · Domain: D2 Implement and manage storage › Configure and manage storage accounts

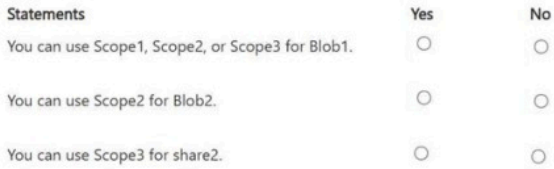
You have an Azure subscription that contains the storage accounts shown in the following table.

Name	Encryption scope	Container
storage1	Scope1, Scope2	cont1
storage2	Scope3	cont2





Answer Area



Statement	Yes	No
You can use Scope1, Scope2, or Scope3 for Blob1.	☐	☐
You can use Scope2 for Blob2.	☐	☐
You can use Scope3 for share2.	☐	☐

Answer

- You can use Scope1, Scope2, or Scope3 for Blob1. **No**
- You can use Scope2 for Blob2. **Yes**
- You can use Scope3 for share2. **No**

Explanation

Blob1 and Blob2 are uploaded to cont1 in storage1, which has Scope1 and Scope2; Scope3 belongs to storage2 and therefore is not available for blobs in cont1. Because the container's setting to use Scope1 for all blobs is unchecked, a blob can use another scope available in storage1, such as Scope2. Encryption scopes apply to blobs, not to the Azure file share share2.

https://learn.microsoft.com/en-us/azure/storage/blobs/encryption-scope-overview
https://learn.microsoft.com/en-us/azure/storage/blobs/encryption-scope-manage

✗ **Statement 1** You can use Scope1, Scope2, or Scope3 for Blob1.
No. Blob1 is uploaded to cont1 in storage1, so it can use scopes available in storage1, namely Scope1 and Scope2. Scope3 belongs to storage2 and is not available for a blob in storage1.

https://learn.microsoft.com/en-us/azure/storage/blobs/encryption-scope-overview
https://learn.microsoft.com/en-us/azure/storage/blobs/encryption-scope-manage

✓ **Statement 2** You can use Scope2 for Blob2.
Yes. Scope2 is available in storage1, the account that contains cont1. The container's option to use Scope1 for all blobs is unchecked, so the container default does not prevent Blob2 from using Scope2.

https://learn.microsoft.com/en-us/azure/storage/blobs/encryption-scope-overview
https://learn.microsoft.com/en-us/azure/storage/blobs/encryption-scope-manage

✗ **Statement 3** You can use Scope3 for share2.
No. share2 is an Azure file share, whereas encryption scopes are used for blobs; they cannot be selected for the file share. Scope3's presence in storage2 does not make it an encryption option for share2.

https://learn.microsoft.com/en-us/azure/storage/blobs/encryption-scope-overview

Question 26

Yes / No · Domain: D2 Implement and manage storage › Configure Azure Files and Azure Blob Storage

You have an Azure Storage account named storage1 that has the Blob service properties shown in the following exhibit.

Blob service property	Value
Hierarchical namespace	Disabled
Default access tier	Hot
Blob anonymous access	Disabled
Blob soft delete	Enabled (45 days)
Container soft delete	Enabled (45 days)
Versioning	Disabled
Change feed	Disabled
NFS v3	Disabled
Allow cross-tenant replication	Disabled
Storage tasks assignments	None

Dumpsgate

Blob service

Hierarchical namespace	Disabled
Default access tier	Hot
Blob anonymous access	Disabled
Blob soft delete	Enabled (45 days)
Container soft delete	Enabled (45 days)
Versioning	Disabled
Change feed	Disabled
NFS v3	Disabled
Allow cross-tenant replication	Disabled
Storage tasks assignments	None

Name	Access tier
File1	Hot
File2	Cool
File3	Archive

Date	Action
January 5	Delete File1.
January 15	Move File2 to the Archive access tier.
April 5	Rehydrate File3.

Answer Area

Statements	Yes	No
You are charged an early deletion penalty for File1.	○	○
You are charged an early deletion penalty for File2.	○	○
You are charged an early deletion penalty for File3.	○	○

On Janurary1, you add blobs to storage1 as shown in the following table.

Name	Access tier
File1	Hot
File2	Cool
File3	Archive

You perform the actions shown in the following table.

Date	Action

January 5	Delete File1.
January 15	Move File2 to the Archive access tier.
April 5	Rehydrate File3.

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

NOTE: Each correct selection is worth one point.

Statement	Yes	No
You are charged an early deletion penalty for File1.	☐	☐
You are charged an early deletion penalty for File2.	☐	☐
You are charged an early deletion penalty for File3.	☐	☐

Answer

- You are charged an early deletion penalty for File1. **No**
- You are charged an early deletion penalty for File2. **Yes**
- You are charged an early deletion penalty for File3. **Yes**

Explanation

Hot-tier blobs have no minimum storage duration, so deleting File1 on January 5 does not incur an early deletion penalty. Cool-tier blobs have a 30-day minimum, and File2 was moved to Archive after only 14 days. Archive-tier blobs have a 180-day minimum, so rehydrating File3 on April 5—about 94 days after it was added—incurs an early deletion penalty.

https://learn.microsoft.com/en-us/azure/storage/blobs/archive-blob?tabs=azure-portal
https://learn.microsoft.com/en-us/azure/storage/blobs/cost-estimate-archive-retrieval-set-tier
https://learn.microsoft.com/fi-fi/azure/storage/blobs/access-tiers-overview

✓ **Statement 1** You are charged an early deletion penalty for File1. — No
File1 was stored in the Hot tier, which has no minimum storage duration. Deleting it on January 5 therefore does not incur an early deletion penalty.

https://learn.microsoft.com/fi-fi/azure/storage/blobs/access-tiers-overview

✓ **Statement 2** You are charged an early deletion penalty for File2. — Yes
File2 was stored in the Cool tier on January 1 and moved to Archive on January 15, before the Cool tier's 30-day minimum duration had elapsed. Moving it early incurs an early deletion penalty.

https://learn.microsoft.com/en-us/azure/storage/blobs/archive-blob?tabs=azure-portal
https://learn.microsoft.com/fi-fi/azure/storage/blobs/access-tiers-overview

✓ **Statement 3** You are charged an early deletion penalty for File3. — Yes
File3 was stored in Archive on January 1 and rehydrated on April 5, about 94 days later. Because this is before the Archive tier's 180-day minimum duration, rehydrating it incurs an early deletion penalty.

https://learn.microsoft.com/en-us/azure/storage/blobs/storage-blob-rehydration
https://learn.microsoft.com/en-us/azure/storage/blobs/archive-rehydrate-to-online-tier
https://learn.microsoft.com/en-us/azure/storage/blobs/cost-estimate-archive-retrieval-set-tier
https://learn.microsoft.com/fi-fi/azure/storage/blobs/access-tiers-overview

Free demo · full exam: 507 questions

Question 27

Single choice · Domain: D2 Implement and manage storage › Configure and manage storage accounts

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

Name	Performance	Premium account type
storage1	Standard	*Not applicable*
storage2	Premium	Block blobs
storage3	Premium	File shares
storage4	Premium	Page blobs

You need to deploy an app named App1 that requires blob storage in the Hot access tier. Which storage accounts can you useforAppI?

A. storage1 only
B. storage1 and storage4 only
C. storage2 and storage4 only
D. storage1, storage2. and storage4 only
E. storage1, storage2. storage3, and storage4

Answer: A. storage1 only

Explanation

App1 requires blob storage that supports the Hot access tier. The Standard account, storage1, can meet that requirement. The listed Premium account types—block blobs, file shares, and page blobs—do not provide the Hot blob access tier, so the correct choice is storage1 only.

https://learn.microsoft.com/en-us/azure/storage/blobs/access-tiers-online-manage
https://learn.microsoft.com/en-sg/azure/storage/blobs/storage-blobs-introduction

✓ **A** storage1 only
Storage1 is the only Standard account in the table, and it can be used for blob storage in the Hot access tier. The Premium account types listed do not meet the Hot-tier requirement.

https://learn.microsoft.com/en-us/azure/storage/blobs/access-tiers-online-manage
https://learn.microsoft.com/en-sg/azure/storage/blobs/storage-blobs-introduction

✗ **B** storage1 and storage4 only
Storage1 is suitable, but storage4 is a Premium page blob account. Page blobs do not support the Hot blob access tier, so storage4 cannot be included.

https://learn.microsoft.com/en-us/azure/storage/blobs/access-tiers-online-manage
https://learn.microsoft.com/en-sg/azure/storage/blobs/storage-blobs-introduction

✗ **C** storage2 and storage4 only
Storage2 is a Premium block blob account, and storage4 is a Premium page blob account. Neither listed Premium account type supports the Hot access tier, and this choice also omits storage1.

https://learn.microsoft.com/en-us/azure/storage/blobs/access-tiers-online-manage
https://learn.microsoft.com/en-sg/azure/storage/blobs/storage-blobs-introduction

✗ **D** storage1, storage2, and storage4 only
Storage1 meets the requirement, but storage2 and storage4 are Premium block blob and Premium page blob accounts, respectively. They cannot provide blob storage in the Hot access tier.

https://learn.microsoft.com/en-us/azure/storage/blobs/access-tiers-online-manage
https://learn.microsoft.com/en-sg/azure/storage/blobs/storage-blobs-introduction

✗ **E** storage1, storage2, storage3, and storage4
Storage1 meets the requirement, but storage2 and storage4 are Premium block blob and page blob accounts, and storage3 is a Premium file shares account. Those Premium account types do not provide Hot-tier blob storage.

https://learn.microsoft.com/en-us/azure/storage/blobs/access-tiers-online-manage
https://learn.microsoft.com/en-sg/azure/storage/blobs/storage-blobs-introduction

Question 28

Multiple choice · Domain: D2 Implement and manage storage › Configure access to storage

You have an Azure subscription that contains a storage account named storage1. The storage1 account contains blob data.

You need to assign a role to a user named User1 to ensure that the user can access the blob data in storage1. The role assignment must support conditions.

Which two roles can you assign to User1? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Storage Blob Data Contributor
B. Storage Blob Data Owner
C. Storage Account Backup Contributor
D. Storage Account Contributor
E. Storage Blob Delegator
F. Owner

Dumpsgate

Answer

- A. **Storage Blob Data Contributor**
- B. **Storage Blob Data Owner**

Explanation

User1 needs a role that grants access to blob data and can be assigned with a condition. Storage Blob Data Contributor and Storage Blob Data Owner both grant blob data permissions and support Azure role-assignment conditions for blob data access. The other choices either do not grant the required blob data access or are not the appropriate data roles for this condition-based assignment.

https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/storage
https://learn.microsoft.com/en-us/azure/role-based-access-control/conditions-format
https://learn.microsoft.com/azure/storage/blobs/storage-auth-abac
https://learn.microsoft.com/en-us/azure/role-based-access-control/conditions-overview

✓ **A** Storage Blob Data Contributor
This role grants permissions to read, write, and delete blob data, so it meets the data-access requirement. It is also a supported role for applying conditions to blob data access.

https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/storage
https://learn.microsoft.com/azure/storage/blobs/storage-auth-abac
https://learn.microsoft.com/en-us/azure/role-based-access-control/conditions-overview

✓ **B** Storage Blob Data Owner
This role grants broad access to blob data, including permissions to manage containers and blobs. It supports conditions on blob data access, so it satisfies both requirements.

https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/storage
https://learn.microsoft.com/azure/storage/blobs/storage-auth-abac
https://learn.microsoft.com/en-us/azure/role-based-access-control/conditions-overview

✗ **C** Storage Account Backup Contributor
This role is intended for backup-related operations on a storage account, not for granting User1 the required blob data access. It is not one of the blob data roles suitable for the requested condition-based access.

https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/storage

✗ **D** Storage Account Contributor
This role provides management-plane access to the storage account, but does not grant access to read or modify blob data. Therefore, it does not meet the scenario's data-access requirement.

https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/storage
https://learn.microsoft.com/en-us/azure/storage/blobs/authorize-data-operations-portal

✗ **E** Storage Blob Delegator
This role grants permission to obtain a user delegation key, which can be used to create a user delegation SAS. It does not itself grant access to the blob data required by the scenario.

https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/storage
https://learn.microsoft.com/en-us/azure/storage/blobs/authorize-data-operations-portal

✗ **F** Owner
The Owner role grants broad control over Azure resources, but it does not grant the blob data permissions needed to access blob contents through Azure RBAC. A blob data role is required instead.

https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/storage
https://learn.microsoft.com/en-us/azure/storage/blobs/authorize-data-operations-portal

Question 29

Multiple choice · Domain: D2 Implement and manage storage › Configure access to storage

You have an Azure container registry in the Standard tier.

You need to enable the admin user account and retrieve the password for the account Which settings should you use?

A. Networking
B. Properties
C. Identity
D. Access keys
D. Access keys

Answer: D. Access keys

Explanation

Use **Access keys** to enable the Azure Container Registry admin user and retrieve its credentials. The Access keys page provides the admin-user setting and displays the associated username and passwords after the account is enabled. [1][2]

https://learn.microsoft.com/en-us/azure/container-registry/container-registry-faq
https://learn.microsoft.com/en-gb/azure/container-registry/container-registry-authentication

✗ **A** Networking
Networking controls connectivity and network access to the registry. It does not provide the admin-user toggle or the account password.

https://learn.microsoft.com/en-us/azure/container-registry/container-registry-access-selected-networks

✗ **B** Properties
Properties shows registry information and settings, but it is not where you enable the admin user or retrieve its credentials. Those controls are under Access keys.

https://learn.microsoft.com/en-us/azure/container-registry/container-registry-faq
https://learn.microsoft.com/en-gb/azure/container-registry/container-registry-authentication

✗ **C** Identity
Identity is for configuring a managed identity for the registry. It does not manage the registry's admin user account or its password.

https://learn.microsoft.com/en-gb/azure/container-registry/container-registry-authentication

✓ **D** Access keys
The Access keys settings include the admin-user toggle and display the username and passwords for that account. Enable the admin user there, then retrieve its password from the same page.

https://learn.microsoft.com/en-us/azure/container-registry/container-registry-faq
https://learn.microsoft.com/en-gb/azure/container-registry/container-registry-authentication

Dumpsgate

Question 30

Single choice · Domain: D2 Implement and manage storage › Configure and manage storage accounts

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

Name	Kind	Performance	Replication	Access tier
Storage1	Storage (general purpose v1)	Premium	Geo-redundant storage (GRS)	*None*
Storage2	StorageV2 (general purpose v2)	Standard	Locally-redundant storage (LRS)	Cool
Storage3	StorageV2 (general purpose v2)	Premium	Read-access geo-redundant storage (RA-GRS)	Hot
Storage4	BlobStorage	Standard	Locally-redundant storage (LRS)	Hot

You need to identify which storage account can be converted to zone-redundant storage (ZRS) replication by requesting a live migration from Azure support.

What should you identify?

A. Storage1
B. Storage2
C. Storage3
D. Storage4

Answer: B. Storage2

Explanation

Identify Storage2. It is a standard StorageV2 (general-purpose v2) account using LRS, which can be migrated to ZRS through a live migration requested from Azure support. The other accounts have an account kind or performance configuration that does not meet the requirements for this migration path.

https://learn.microsoft.com/en-us/azure/storage/common/redundancy-migration
https://learn.microsoft.com/en-us/azure/storage/common/storage-redundancy-change-faq

✗ **A** Storage1
Storage1 is a general-purpose v1 account, not a StorageV2 account. It cannot use the specified live-migration path to ZRS in its current configuration.

https://learn.microsoft.com/en-us/azure/storage/common/redundancy-migration
https://learn.microsoft.com/en-us/azure/storage/common/general-purpose-version-1-zone-redundant-storage-migration-overview

✓ **B** Storage2
Storage2 is a standard StorageV2 account currently using LRS. This account configuration is eligible for live migration to ZRS by requesting the migration from Azure support.

https://learn.microsoft.com/en-us/azure/storage/common/redundancy-migration
https://learn.microsoft.com/en-us/azure/storage/common/storage-redundancy-change-faq

Free demo · full exam: 507 questions

✗ **C** Storage3
Storage3 has premium performance and RA-GRS replication. It does not have the standard LRS configuration required for the live migration to ZRS described in the question.
https://learn.microsoft.com/en-us/azure/storage/common/redundancy-migration
https://learn.microsoft.com/en-us/azure/storage/common/storage-redundancy-change-faq

✗ **D** Storage4
Storage4 is a BlobStorage account rather than a StorageV2 account. It therefore does not meet the account-kind requirement for this live migration path in its current configuration.
https://learn.microsoft.com/en-us/azure/storage/common/redundancy-migration

Question 31

Single choice · Domain: D2 Implement and manage storage › Configure Azure Files and Azure Blob Storage

You have an Azure subscription. The subscription contains a storage account named storage1 that has the lifecycle management rules shown in the following table.

Name	If base blobs were last modified more than (days)	Then
Rule1	5 days	Move to cool storage
Rule2	5 days	Delete the blob
Rule3	5 days	Move to archive storage

On June 1, you store a blob named File1 in the Hot access tier of storage1. What is the state of File1 on June 7?

A. stored in the Archive access tier
B. stored in the Hot access tier
C. stored in the Cool access tier
D. deleted

Answer: D. deleted

Explanation

By June 7, File1 was last modified more than five days earlier, so it meets the age condition for all three lifecycle rules. When multiple lifecycle actions apply to the same blob, the delete action takes precedence over tier changes, so File1 is deleted. [1]
https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-structure

✗ **A** stored in the Archive access tier
File1 meets the condition for the archive rule, but it also meets the delete rule's condition. When both actions apply, deletion takes precedence, so the blob is not left in the Archive tier. [1]
https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-structure

✗ **B** stored in the Hot access tier

By June 7, more than five days have passed since File1 was stored, so it meets the age condition for lifecycle actions. The applicable delete action takes precedence, rather than leaving it in the Hot tier. [1]

https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-structure

✗ **C** stored in the Cool access tier
File1 meets the condition for the Cool-tier rule, but it also meets the delete rule's condition. Deletion takes precedence over the tier-change action, so File1 is not left in the Cool tier. [1]

https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-structure

✓ **D** deleted
On June 7, File1 is more than five days past its last modification, so the conditions for the rules are met. Because the delete action takes precedence over the tier-change actions, File1 is deleted. [1]

https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-structure

Question 32

Single choice · Domain: D2 Implement and manage storage › Configure and manage storage accounts

You have an on-premises server that contains a folder named D:\Folder1.

You need to copy the contents of D:\Folder1 to the public container in an Azure Storage account named contoso data.

Which command should you run?

A. https://contosodata.blob.core.windows.net/public
B. azcopy sync D:\folder1 https://contosodata.blob.core.windows.net/public --snapshot
C. azcopy copy D:\folder1 https://contosodata.blob.core.windows.net/public --recursive
D. az storage blob copy start-batch D:\Folder1 https://contosodata.blob.core.windows.net/public

Answer: C. azcopy copy D:\folder1 https://contosodata.blob.core.windows.net/public --recursive

Explanation

Use `azcopy copy` to upload the contents of the local folder to the Azure Blob Storage container. The `--recursive` option tells AzCopy to include files in subfolders, matching the requirement to copy the folder's contents to the `public` container. [1][3]

https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-blobs-upload
https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy

✗ **A** https://contosodata.blob.core.windows.net/public
This is the URL of the destination container, not a command that copies files. It does not specify the local source folder or an upload operation.

✗ **B** azcopy sync D:\folder1 https://contosodata.blob.core.windows.net/public --snapshot
`sync` is intended to synchronize source and destination contents, rather than perform the requested copy operation. Also, `--snapshot` is not the option needed to recursively upload a local folder in this scenario.

https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-blobs-synchronize

✓ **C** azcopy copy D:\folder1 https://contosodata.blob.core.windows.net/public --recursive
`azcopy copy` uploads data from the local source path to the specified Blob Storage destination. The `--recursive` flag includes files in subdirectories, so this command copies the contents of `D:\Folder1` to the public container.

https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-blobs-upload
https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy

✗ **D** az storage blob copy start-batch D:\Folder1 https://contosodata.blob.core.windows.net/public
This Azure CLI batch-copy command is not the appropriate way to upload a local folder; its arguments do not provide a valid local-folder upload operation. Use AzCopy's `copy` command with the local path and `--recursive` instead.

https://learn.microsoft.com/en-us/cli/azure/storage/blob/copy?view=azure-cli-latest

---

Question 33

Yes / No · Domain: D2 Implement and manage storage › Configure Azure Files and Azure Blob Storage

You have an Azure subscription. The subscription contains a storage account named storage1 that has the lifecycle management rules shown in the following table.

Name	Blob prefix	If base blobs were last modified more than (days ago)	Then
Rule1	container1/	3 days	Move to archive storage
Rule2	Not applicable	5 days	Move to cool storage
Rule3	container2/	10 days	Delete the blob
Rule4	container2/	15 days	Move to archive storage

Name	Blob prefix	If base blobs were last modified more than (days ago)	Then
Rule1	container1/	3 days	Move to archive storage
Rule2	*Not applicable*	5 days	Move to cool storage
Rule3	container2/	10 days	Delete the blob
Rule4	container2/	15 days	Move to archive storage

Name	Location	Access tier
File1	container1	Hot
File2	container2	Hot

Answer Area

Statements	Yes	No
On June 6, File1 will be stored in the Cool access tier.	○	○
On June 7, File2 will be stored in the Cool access tier.	○	○
On June 16, File2 will be stored in the Archive access tier.	○	○

Statement	Yes	No
On June 6, File1 will be stored in the Cool access tier.	☐	☐
On June 7, File2 will be stored in the Cool access tier.	☐	☐
On June 16, File2 will be stored in the Archive access tier.	☐	☐

Answer

- On June 6, File1 will be stored in the Cool access tier. **No**
- On June 7, File2 will be stored in the Cool access tier. **Yes**
- On June 16, File2 will be stored in the Archive access tier. **No**

Explanation

Lifecycle rules use the blob's last-modified age and apply only after the configured number of days has been exceeded. On June 6, File1 qualifies for the container1 archive rule, while the account-wide cool rule's five-day threshold has not been exceeded. File2 qualifies for the account-wide cool rule on June 7, but by June 16 it qualifies for deletion and has not exceeded the archive rule's 15-day threshold.

https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-structure
https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-access-tiers

✗ **Statement 1** On June 6, File1 will be stored in the Cool access tier.
No. File1 is in container1, so Rule1 applies and moves it to archive after its last-modified age exceeds three days. On June 6, the account-wide cool rule's requirement of more than five days has not been exceeded, so File1 is not moved to Cool.

https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-structure
https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-access-tiers

✓ **Statement 2** On June 7, File2 will be stored in the Cool access tier.
Yes. File2's last-modified age is six days on June 7, which exceeds Rule2's five-day threshold. Rule2 applies to blobs without a prefix restriction, and File2 has not yet reached Rule3's 10-day deletion threshold.

https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-structure
https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-access-tiers

✗ **Statement 3** On June 16, File2 will be stored in the Archive access tier.
No. File2's age is 15 days on June 16, which does not exceed Rule4's 15-day threshold for moving it to Archive. It has already exceeded Rule3's 10-day threshold for deletion, so it will not be moved to Archive under Rule4.

https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-structure
https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-access-tiers

Free demo · full exam: 507 questions

Question 34

Single choice · Domain: D3 Deploy and manage Azure compute resources › Provision and manage containers in the Azure portal

You are provisioning a containerized application in Azure. The application consists of multiple microservices, each deployed as a separate container, and they must communicate with each other over a virtual network.

You need a managed container orchestration platform that handles scaling, networking, and updates automatically.

Which Azure service should you use, and what is the primary networking model it uses for inter-container communication?

A. Azure Container Instances; containers communicate via Docker bridge networking within a container group, and external communication occurs through public IP addresses.

B. Azure Kubernetes Service (AKS); services use Kubernetes service objects within a virtual network, providing DNS-based discovery and load balancing for inter-pod communication.

C. Azure Container Registry; provides a managed registry for storing container images with built-in networking for pulling images during deployment.

D. Azure App Service; runs containers using a managed Kubernetes backend with automatic networking configuration and integrated load balancing.

Answer: B. Azure Kubernetes Service (AKS); services use Kubernetes service objects within a virtual network, providing DNS-based discovery and load balancing for inter-pod communication.

Explanation

AKS is a managed Kubernetes platform suited to the scenario's separately deployed microservices and need for orchestration, scaling, and updates. Its Kubernetes networking uses Services for stable service discovery and load balancing, while cluster DNS lets workloads locate services by name. AKS also supports networking through an Azure virtual network, making option B the best fit.

https://learn.microsoft.com/azure/aks/dns-concepts
https://learn.microsoft.com/en-us/azure/aks/concepts-network
https://learn.microsoft.com/azure/aks/concepts-network-services

✗ **A** Azure Container Instances; containers communicate via Docker bridge networking within a container group, and external communication occurs through public IP addresses.
Azure Container Instances can run containers in container groups, but that is not a managed orchestration platform for coordinating separately deployed microservices and handling their scaling and updates. The described Docker bridge model also does not accurately capture container-group networking, where group containers share a network context.

https://learn.microsoft.com/en-us/azure/container-instances/container-instances-virtual-network-concepts
https://learn.microsoft.com/en-us/azure/container-instances/container-instances-container-groups

✓ **B** Azure Kubernetes Service (AKS); services use Kubernetes service objects within a virtual network, providing DNS-based discovery and load balancing for inter-pod communication.
AKS is the managed Kubernetes service that fits the requirement to orchestrate containerized microservices and manage scaling and updates. Kubernetes Services provide stable service endpoints and load balancing, and cluster DNS supports name-based discovery between workloads; AKS supports cluster networking with an Azure virtual network.

https://learn.microsoft.com/azure/aks/dns-concepts
https://learn.microsoft.com/en-us/azure/aks/concepts-network
https://learn.microsoft.com/azure/aks/concepts-network-services

Free demo · full exam: 507 questions

✗ **C** Azure Container Registry; provides a managed registry for storing container images with built-in networking for pulling images during deployment.
Azure Container Registry stores and manages container images; it does not deploy or orchestrate running microservices, manage their scaling, or provide their inter-container communication model. It can supply images to a deployment, but it is not the platform requested here.

https://learn.microsoft.com/en-us/azure/container-registry/container-registry-get-started-portal
https://learn.microsoft.com/en-us/training/modules/store-manage-containers-azure-container-registry/
https://learn.microsoft.com/azure/container-registry/?WT.mc_id=javascript-0000-cxa

✗ **D** Azure App Service; runs containers using a managed Kubernetes backend with automatic networking configuration and integrated load balancing.
Azure App Service is not the managed Kubernetes orchestration service described in the question, and the option's claim that it runs containers using a managed Kubernetes backend does not make it the right choice for this requirement. AKS directly provides Kubernetes orchestration and its service-based networking model.

Question 35

Single choice · Domain: D3 Deploy and manage Azure compute resources › Automate deployment of resources by using Azure Resource Manager (ARM) templates or Bicep files

You are deploying a new web application to Azure App Service. Your infrastructure team wants to automate future deployments using an Infrastructure-as-Code approach. The solution must support parameter reuse across multiple deployments and allow conditional logic for different environments (development, staging, production).

Which of the following would be the most appropriate choice for this scenario?

A. Use a Bicep file with parameter files for each environment and conditional expressions to define environment-specific resources, then deploy using the Azure CLI.

B. Manually create the App Service in the Azure portal and export it as a JSON template for future deployments.

C. Write an Azure PowerShell script that uses hard-coded resource names and SKUs, then execute it locally for each deployment.

D. Use an Azure Resource Manager (ARM) template in JSON format with extensive nested templates and parameter overrides for each environment.

Answer: A. Use a Bicep file with parameter files for each environment and conditional expressions to define environment-specific resources, then deploy using the Azure CLI.

Explanation

A Bicep file with separate parameter files lets the team reuse the infrastructure definition while supplying values for development, staging, and production. Bicep supports conditional resource deployment, and the Azure CLI can deploy the template, meeting the scenario's automation and environment-specific requirements. [1][2][3][6]

https://learn.microsoft.com/en-us/azure/azure-resource-manager/bicep/conditional-resource-deployment
https://learn.microsoft.com/azure/azure-resource-manager/bicep/parameters
https://learn.microsoft.com/en-us/azure/azure-resource-manager/bicep/deploy-cli
https://learn.microsoft.com/en-us/azure/azure-resource-manager/bicep/parameter-files?WT.mc_id=MVP_319025&tabs=Bicep

✓ **A** Use a Bicep file with parameter files for each environment and conditional expressions to define environment-specific resources, then deploy using the Azure CLI.
This approach reuses one infrastructure definition while parameter files provide environment-specific values. Bicep supports conditional resource deployment, and it can be deployed with the Azure CLI, making this the best fit for automated deployments across environments.

https://learn.microsoft.com/en-us/azure/azure-resource-manager/bicep/conditional-resource-deployment
https://learn.microsoft.com/azure/azure-resource-manager/bicep/parameters
https://learn.microsoft.com/en-us/azure/azure-resource-manager/bicep/deploy-cli
https://learn.microsoft.com/en-us/azure/azure-resource-manager/bicep/parameter-files?WT.mc_id=MVP_319025&tabs=Bicep

✗ **B** Manually create the App Service in the Azure portal and export it as a JSON template for future deployments.
The portal can export a template from existing resources, but this option starts with manual creation rather than defining the deployment for repeatable automation. It also does not specify parameter files or conditional logic for the different environments.

https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/export-template-portal
https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/quickstart-create-templates-use-the-portal

✗ **C** Write an Azure PowerShell script that uses hard-coded resource names and SKUs, then execute it locally for each deployment.
Hard-coded names and SKUs make it difficult to reuse the deployment across development, staging, and production without editing the script. This choice does not provide the requested parameterized, declarative infrastructure definition or conditional environment-specific resources.

✗ **D** Use an Azure Resource Manager (ARM) template in JSON format with extensive nested templates and parameter overrides for each environment.
ARM templates can be parameterized, but the proposed extensive nesting and overrides add complexity that is not needed for this scenario. Bicep provides a more direct way to define reusable infrastructure with parameter files and conditional logic.

https://learn.microsoft.com/azure/azure-resource-manager/bicep/parameters
https://learn.microsoft.com/azure/azure-resource-manager/bicep/file
https://learn.microsoft.com/en-us/azure/azure-resource-manager/bicep/parameter-files?WT.mc_id=MVP_319025&tabs=Bicep

Question 36

Single choice · Domain: D3 Deploy and manage Azure compute resources › Create and configure Azure App Service

Your organization is configuring Azure App Service for a line-of-business application that must meet compliance requirements for data residency and encryption. The application requires custom domain support, SSL/TLS certificates, and the ability to scale to multiple instances. Which two App Service plan tiers meet the minimum requirements?

A. Standard and Premium tiers, which support custom domains, SSL/TLS binding, and multiple instances
B. Free and Shared tiers with a purchased SSL certificate
C. Basic tier only, which includes all enterprise features
D. Premium and Isolated tiers with Azure Firewall integration
E. Dedicated Host deployments for App Service

Free demo · full exam: 507 questions

Answer: A. Standard and Premium tiers, which support custom domains, SSL/TLS binding, and multiple instances

Explanation

Standard and Premium provide the required combination of custom-domain support, SSL/TLS certificate binding, and scaling to multiple instances, making option A the correct choice among those offered. Data residency depends on choosing an appropriate deployment region, while encryption requirements must be met through the applicable App Service configuration; the tier names alone do not establish compliance. References [1] and [2] describe plan capabilities and scaling, and [3] and [5] cover domain certificates and SSL bindings.

https://learn.microsoft.com/en-us/azure/app-service/overview-hosting-plans
https://learn.microsoft.com/en-us/azure/app-service/manage-scale-up
https://learn.microsoft.com/en-us/azure/app-service/tutorial-secure-domain-certificate
https://learn.microsoft.com/azure/app-service/configure-ssl-bindings

✓ **A** Standard and Premium tiers, which support custom domains, SSL/TLS binding, and multiple instances
Both tiers support the domain, certificate-binding, and scaling capabilities called for in the scenario. The organization must also select an appropriate region and configure encryption to address its compliance requirements.

https://learn.microsoft.com/en-us/azure/app-service/overview-hosting-plans
https://learn.microsoft.com/en-us/azure/app-service/manage-scale-up
https://learn.microsoft.com/en-us/azure/app-service/tutorial-secure-domain-certificate
https://learn.microsoft.com/azure/app-service/configure-ssl-bindings

✗ **B** Free and Shared tiers with a purchased SSL certificate
Buying a certificate does not add the plan capabilities needed to meet the combined requirements, particularly scaling to multiple instances. Free and Shared plans do not provide the same feature set as the Standard and Premium tiers.

https://learn.microsoft.com/en-us/azure/app-service/overview-hosting-plans
https://learn.microsoft.com/en-us/azure/app-service/manage-scale-up
https://learn.microsoft.com/azure/app-service/configure-ssl-bindings

✗ **C** Basic tier only, which includes all enterprise features
The claim that Basic includes all enterprise features is incorrect, and this option does not identify the Standard-and-Premium pair that satisfies the question as keyed. Basic is a lower tier with a more limited feature set than Standard and Premium.

https://learn.microsoft.com/en-us/azure/app-service/overview-hosting-plans
https://learn.microsoft.com/en-us/azure/app-service/manage-scale-up

✗ **D** Premium and Isolated tiers with Azure Firewall integration
Although Premium supports the stated App Service capabilities, Azure Firewall integration is not what establishes support for custom domains, SSL/TLS binding, or multiple instances. Isolated is not needed to meet those requirements; the answer calls for the Standard and Premium tiers.

https://learn.microsoft.com/en-us/azure/app-service/overview-hosting-plans
https://learn.microsoft.com/en-us/azure/app-service/manage-scale-up
https://learn.microsoft.com/en-us/azure/app-service/environment/creation

✗ **E** Dedicated Host deployments for App Service
A dedicated-host deployment is not the requested pair of App Service plan tiers. It is not necessary to obtain the domain, certificate-binding, and scaling capabilities described in the scenario.

https://learn.microsoft.com/en-us/azure/app-service/overview-hosting-plans
https://learn.microsoft.com/en-us/azure/app-service/environment/creation

Question 37

Single choice · Domain: D3 Deploy and manage Azure compute resources › Create and configure Azure App Service

Your organization has deployed a web application on Azure App Service and is now receiving requests to add more compute capacity during peak hours and scale down during off-peak times to optimize costs. Which approach should you implement?

A. Configure App Service autoscale rules based on CPU utilization metrics, with scale-out at 70 percent CPU and scale-in at 40 percent CPU
B. Manually add or remove App Service instances on a schedule using Azure Automation runbooks
C. Migrate the application to a higher-tier App Service plan that has more built-in capacity
D. Deploy a second App Service instance in another region and use Traffic Manager to distribute load
E. Implement Azure Kubernetes Service (AKS) with Horizontal Pod Autoscaler for scaling

Answer: A. Configure App Service autoscale rules based on CPU utilization metrics, with scale-out at 70 percent CPU and scale-in at 40 percent CPU

Explanation

App Service autoscale can adjust the number of instances as demand changes, which addresses both adding capacity during peak hours and scaling down during quieter periods. CPU-based rules use a workload metric to trigger those changes; the stated thresholds are the rule values in option A. This avoids relying on manual changes or replacing the existing hosting approach. [3][4][11]

https://learn.microsoft.com/en-us/azure/azure-monitor/autoscale/autoscale-get-started
https://learn.microsoft.com/en-us/azure/app-service/manage-automatic-scaling?WT.mc_id=AZ-MVP-4033351
https://learn.microsoft.com/en-us/azure/azure-monitor/autoscale/autoscale-understanding-settings

✓ **A** Configure App Service autoscale rules based on CPU utilization metrics, with scale-out at 70 percent CPU and scale-in at 40 percent CPU
Autoscale rules can use CPU metrics to increase instances as demand rises and decrease them when demand falls. This directly meets the need to add capacity during peak hours and reduce it during off-peak times. [3][4][11]

https://learn.microsoft.com/en-us/azure/azure-monitor/autoscale/autoscale-get-started
https://learn.microsoft.com/en-us/azure/app-service/manage-automatic-scaling?WT.mc_id=AZ-MVP-4033351
https://learn.microsoft.com/en-us/azure/azure-monitor/autoscale/autoscale-understanding-settings

✗ **B** Manually add or remove App Service instances on a schedule using Azure Automation runbooks
A schedule can run automation at predetermined times, but it does not react to actual CPU utilization as the proposed autoscale rules do. It could also change capacity at an unsuitable time if demand differs from the schedule. [8]

https://learn.microsoft.com/en-us/azure/automation/shared-resources/schedules

✗ **C** Migrate the application to a higher-tier App Service plan that has more built-in capacity
Moving to a higher tier provides more capacity, but by itself it does not scale the number of instances up during peak hours and down during off-peak times. It therefore does not address the requested demand-based capacity adjustment.

✗ **D** Deploy a second App Service instance in another region and use Traffic Manager to distribute load
Traffic Manager can route traffic among endpoints, including endpoints in different regions, but that is not the same as automatically scaling App Service instances in response to CPU demand. This adds a multi-region deployment rather than directly implementing the requested scale-out and scale-in behavior. [1][6]

https://learn.microsoft.com/en-us/azure/app-service/web-sites-traffic-manager
https://learn.microsoft.com/en-us/azure/traffic-manager/traffic-manager-how-it-works

✗ **E** Implement Azure Kubernetes Service (AKS) with Horizontal Pod Autoscaler for scaling
AKS can scale workloads using Kubernetes mechanisms, but adopting it would require moving the application from its existing App Service deployment to a different hosting platform. App Service autoscale addresses the stated capacity requirement without that migration.

Question 38

Single choice · Domain: D3 Deploy and manage Azure compute resources › Provision and manage containers in the Azure portal

You are provisioning a containerized application in the Azure portal using Azure Container Instances (ACI).

The application requires persistent storage, environment-specific configuration values, and the ability to scale horizontally in the future. Which two features should you implement now?

A. Mount Azure Files shares for persistent storage and use environment variables defined in the container group specification for configuration

B. Attach managed disks to container instances and hardcode all configuration values in the container image

C. Use local storage within the container and store configuration in Azure Blob Storage

D. Implement Azure Container Registry with image tagging and use only read-only file systems

E. Deploy containers to Azure Kubernetes Service (AKS) instead for persistent storage support

Answer: A. Mount Azure Files shares for persistent storage and use environment variables defined in the container group specification for configuration

Explanation

Option A provides both capabilities the application needs now: Azure Files can persist data beyond a container's lifecycle, and environment variables in the container group specification allow configuration to vary by environment without rebuilding the image. These choices are compatible with the stated ACI deployment. If the application later needs orchestration for horizontal scaling, it can adopt a platform such as AKS; the ACI storage and configuration choices do not themselves provide autoscaling.

https://learn.microsoft.com/en-us/azure/container-instances/container-instances-reference-yaml
https://learn.microsoft.com/azure/container-instances/container-instances-orchestrator-relationship
https://learn.microsoft.com/en-us/azure/container-instances/container-instances-volume-azure-files?trk=article-ssr-frontend-pulse_little-text-block
https://learn.microsoft.com/en-us/azure/aks/cluster-autoscaler-overview

✓ **A** Mount Azure Files shares for persistent storage and use environment variables defined in the container group specification for configuration
Azure Files provides persistent shared storage that can be mounted into an ACI container group. ACI container group specifications support environment variables, keeping configuration values separate from the container image and making them easier to vary by environment. These features meet the persistence and configuration requirements without changing the requested ACI deployment.

https://learn.microsoft.com/en-us/azure/container-instances/container-instances-reference-yaml
https://learn.microsoft.com/en-us/azure/container-instances/container-instances-volume-azure-files?trk=article-ssr-frontend-pulse_little-text-block

✗ **B** Attach managed disks to container instances and hardcode all configuration values in the container image

This is not the appropriate ACI storage approach: ACI supports mounting Azure Files shares for persistent storage, rather than attaching managed disks to container instances as proposed. Hardcoding configuration also ties environment-specific values to the image, making them less flexible to change.

https://learn.microsoft.com/en-us/azure/container-instances/container-instances-reference-yaml
https://learn.microsoft.com/en-us/azure/container-instances/container-instances-volume-azure-files?trk=article-ssr-frontend-pulse_little-text-block

✗ **C** Use local storage within the container and store configuration in Azure Blob Storage
Local container storage is not suitable for data that must persist beyond the container's lifecycle. Although Blob Storage can hold data, this option does not provide the straightforward mounted persistent file share that ACI offers with Azure Files, and it does not use the specified container-group environment-variable configuration approach.

https://learn.microsoft.com/en-us/azure/container-instances/container-instances-reference-yaml
https://learn.microsoft.com/en-us/azure/container-instances/container-instances-volume-azure-files?trk=article-ssr-frontend-pulse_little-text-block

✗ **D** Implement Azure Container Registry with image tagging and use only read-only file systems
An Azure Container Registry and image tags help manage container images, but they do not provide persistent application storage or environment-specific configuration. Read-only file systems also do not satisfy the requirement for persistent writable application data.

https://learn.microsoft.com/en-us/azure/container-instances/container-instances-volume-azure-files?trk=article-ssr-frontend-pulse_little-text-block

✗ **E** Deploy containers to Azure Kubernetes Service (AKS) instead for persistent storage support
The scenario specifies provisioning the application in ACI, and ACI can provide persistent storage through Azure Files, so switching to AKS is not required to meet that need. AKS may be considered later if the application requires orchestration and scaling capabilities, but this option does not implement the requested ACI features now.

https://learn.microsoft.com/azure/container-instances/container-instances-orchestrator-relationship
https://learn.microsoft.com/en-us/azure/container-instances/container-instances-volume-azure-files?trk=article-ssr-frontend-pulse_little-text-block
https://learn.microsoft.com/en-us/azure/aks/cluster-autoscaler-overview

Question 39

Single choice · Domain: D3 Deploy and manage Azure compute resources › Automate deployment of resources by using Azure Resource Manager (ARM) templates or Bicep files

You are automating the deployment of a complex multi-resource Azure infrastructure including virtual networks, virtual machines, and storage accounts. Your organization requires that all deployments be version-controlled, support parameterization for different environments (development, staging, production), and allow modular reuse of components. Which deployment approach best meets these requirements?

A. Azure Resource Manager (ARM) JSON templates with linked templates for modularity and parameter files for environment-specific values

B. Azure CLI scripts executed sequentially with hardcoded values for each environment

C. Bicep files transpiled to ARM templates with a single monolithic parameter file for all environments

D. Azure Portal user interface deployments with manual configuration and documented steps

E. PowerShell runbooks stored in Azure Automation with inline variable definitions

Free demo · full exam: 507 questions

Answer: A. Azure Resource Manager (ARM) JSON templates with linked templates for modularity and parameter files for environment-specific values

Explanation

Option A best meets all three requirements: ARM templates can be stored and version-controlled as deployment files, linked templates support modular reuse, and separate parameter files can supply values for development, staging, and production. This provides a repeatable way to deploy the specified resources while keeping environment-specific configuration separate from the reusable templates.

https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/linked-templates?tabs=azure-powershell

✓ **A** Azure Resource Manager (ARM) JSON templates with linked templates for modularity and parameter files for environment-specific values
This approach represents the infrastructure in deployment templates that can be version-controlled and reused. Linked templates provide modularity, while distinct parameter files let each environment supply its own values without duplicating the infrastructure definition.

https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/linked-templates?tabs=azure-powershell

✗ **B** Azure CLI scripts executed sequentially with hardcoded values for each environment
Hardcoded values make the scripts environment-specific and require maintaining separate scripts or editing values for each environment. Sequential scripts also do not provide the linked-template modular reuse requested in the scenario.

✗ **C** Bicep files transpiled to ARM templates with a single monolithic parameter file for all environments
Bicep can be used to define reusable infrastructure, but this choice specifies one parameter file for all environments rather than keeping development, staging, and production values separately parameterized. The single-file approach does not meet the scenario's environment-specific configuration requirement as well as option A.

https://learn.microsoft.com/en-us/azure/azure-resource-manager/bicep/modules
https://learn.microsoft.com/en-us/azure/azure-resource-manager/bicep/parameter-files?WT.mc_id=MVP_319025&tabs=Bicep

✗ **D** Azure Portal user interface deployments with manual configuration and documented steps
Manual portal deployments rely on people repeating configuration steps, making them less consistent and harder to reproduce than template-based deployments. Documentation alone does not provide parameterized, modular deployment artifacts for version control.

✗ **E** PowerShell runbooks stored in Azure Automation with inline variable definitions
Runbooks can automate operational tasks, but inline variable definitions couple values to the script rather than cleanly separating parameters for multiple environments. This option also does not specify modular infrastructure templates for reusing the network, virtual machine, and storage components.

https://learn.microsoft.com/en-us/azure/automation/start-runbooks
https://learn.microsoft.com/en-us/azure/automation/manage-runbooks

Question 40

Single choice · Domain: D3 Deploy and manage Azure compute resources › Create and configure Azure App Service

You have deployed an Azure App Service web application that needs to serve static content (CSS, JavaScript, images) and dynamic content (HTML generated from code). Users are distributed across multiple geographic regions, and you want to improve performance by caching static content closer to users and reducing load on the origin server.

Which Azure service should you integrate with App Service to meet this requirement?

A. Azure Traffic Manager
B. Azure Content Delivery Network (CDN)
C. Azure Load Balancer
D. Azure Application Gateway

Answer: B. Azure Content Delivery Network (CDN)

Explanation

Azure Content Delivery Network (CDN) caches static assets at edge locations closer to users in different geographic regions. This reduces the distance those assets travel and the number of requests the App Service origin must handle. CDN therefore directly meets the requirement to improve static-content performance while reducing origin load; dynamic content can continue to be generated by the application.

https://learn.microsoft.com/en-us/azure/architecture/best-practices/cdn

✗ **A** Azure Traffic Manager
Traffic Manager routes users to endpoints using DNS-based traffic-routing methods; it does not provide edge caching for static files. It therefore does not meet the requirement to cache CSS, JavaScript, and images closer to users.

https://learn.microsoft.com/en-us/azure/traffic-manager/traffic-manager-load-balancing-azure
https://learn.microsoft.com/en-us/azure/traffic-manager/traffic-manager-how-it-works

✓ **B** Azure Content Delivery Network (CDN)
Azure CDN caches static content at geographically distributed edge locations, so users can retrieve it from a location closer to them. Serving cached assets from the CDN also reduces requests and workload on the App Service origin.

https://learn.microsoft.com/en-us/azure/architecture/best-practices/cdn

✗ **C** Azure Load Balancer
Azure Load Balancer distributes network traffic among back-end resources; it does not cache static content at edge locations. It would not provide the requested reduction in origin requests by serving cached assets near users.

✗ **D** Azure Application Gateway
Application Gateway provides web-traffic routing and load-balancing capabilities, but it is not the service for globally caching static assets close to users. Azure CDN is the appropriate choice for that caching requirement.

https://learn.microsoft.com/en-us/azure/application-gateway/overview

Free demo · full exam: 507 questions

Question 41

Single choice · Domain: D3 Deploy and manage Azure compute resources › Create and configure Azure App Service

You have an Azure App Service web app named webapp1 that is accessible by default at webapp1.azurewebsites.net. You have a custom DNS domain of www.contoso.com that is registered at a third-party registrar. For www.contoso.com, you create a DNS CNAME record that points to webapp1.azurewebsites.net.

You need to configure webapp1 so that users can access webapp1 from www.contoso.com. What should you do?

A. Add www.contoso.com as an allowed origin for Cross-Origin Resource Sharing (CORS).
B. Add webapp1.azurewebsites.net as a custom domain binding for webapp1.
C. Add www.contoso.com as a redirect in webapp1.
D. Add www.contoso.com as a custom domain binding for webapp1

Answer: D. Add www.contoso.com as a custom domain binding for webapp1

Explanation

The CNAME record directs www.contoso.com to webapp1.azurewebsites.net, but App Service must also be configured to recognize www.contoso.com as a hostname for the app. Add www.contoso.com as a custom domain binding for webapp1. This lets requests using the custom domain reach the web app; a CORS setting or redirect is not a substitute for that binding.

https://learn.microsoft.com/en-us/azure/app-service/overview-custom-domains
https://learn.microsoft.com/en-us/azure/app-service/app-service-web-tutorial-custom-domain?tabs=subdomain%2Cpowershell

✗ **A** Add www.contoso.com as an allowed origin for Cross-Origin Resource Sharing (CORS).
CORS controls whether browser-based code from one origin can make cross-origin requests to the app. It does not configure App Service to accept www.contoso.com as a hostname, which is what this scenario requires.

https://learn.microsoft.com/en-us/cli/azure/webapp/cors?view=azure-cli-latest

✗ **B** Add webapp1.azurewebsites.net as a custom domain binding for webapp1.
webapp1.azurewebsites.net is already the app's default Azure hostname. The hostname that must be added as a custom domain binding is www.contoso.com, so App Service recognizes requests sent to that name.

https://learn.microsoft.com/en-us/azure/app-service/overview-custom-domains
https://learn.microsoft.com/en-us/azure/app-service/app-service-web-tutorial-custom-domain?tabs=subdomain%2Cpowershell

✗ **C** Add www.contoso.com as a redirect in webapp1.
A redirect would instruct clients to navigate to another URL; it does not bind www.contoso.com to the App Service app. The custom hostname must be configured on the app so requests using it can be served.

https://learn.microsoft.com/en-us/azure/app-service/overview-custom-domains
https://learn.microsoft.com/en-us/azure/app-service/app-service-web-tutorial-custom-domain?tabs=subdomain%2Cpowershell

✓ **D** Add www.contoso.com as a custom domain binding for webapp1.
The CNAME record points www.contoso.com to the app's default hostname, and the matching custom domain binding configures App Service to accept that hostname. This is the required app-side configuration for users to access webapp1 by www.contoso.com.

https://learn.microsoft.com/en-us/azure/app-service/overview-custom-domains

Free demo · full exam: 507 questions

https://learn.microsoft.com/en-us/azure/app-service/app-service-web-tutorial-custom-domain?tabs=subdomain%2Cpowershell

Question 42

Single choice · Domain: D3 Deploy and manage Azure compute resources › Create and configure virtual machines

You have an Azure subscription that contains an availability set named AS1. AS1 has the following settings:

- Fault domains: 3
- Update domains: 5

You deploy 16 virtual machines to AS1.

What is the minimum number of virtual machines that will be available during maintenance of the datacenter?

A. 10
B. 11
C. 12
D. 13
E. 15

Answer: C. 12

Explanation

Planned maintenance is performed one update domain at a time, so only the VMs in one update domain are unavailable at once. With 16 VMs spread across 5 update domains, the largest group has 4 VMs (⌈16 ÷ 5⌉). Therefore, at least 16 − 4 = 12 VMs remain available; the 3 fault domains do not change this update-domain calculation.

https://learn.microsoft.com/en-us/azure/virtual-machines/availability-set-overview?trk=public_post_comment-text

✗ **A** 10
This would mean 6 VMs are unavailable during maintenance. With 16 VMs across 5 update domains, no single update domain contains more than 4 VMs, so at least 12 remain available.

https://learn.microsoft.com/en-us/azure/virtual-machines/availability-set-overview?trk=public_post_comment-text

✗ **B** 11
This would mean 5 VMs are unavailable at once. Maintenance proceeds one update domain at a time, and distributing 16 VMs across 5 domains puts at most 4 in any one domain.

https://learn.microsoft.com/en-us/azure/virtual-machines/availability-set-overview?trk=public_post_comment-text

✓ **C** 12
The largest update domain can contain 4 of the 16 VMs because 16 VMs are distributed across 5 update domains. If those 4 are unavailable during maintenance, 12 VMs remain available.

https://learn.microsoft.com/en-us/azure/virtual-machines/availability-set-overview?trk=public_post_comment-text

✗ **D** 13
This assumes that no more than 3 VMs are unavailable. But 16 VMs spread across 5 update domains require one domain to hold 4 VMs, so only 12 are guaranteed to remain available when that domain is maintained.

https://learn.microsoft.com/en-us/azure/virtual-machines/availability-set-overview?trk=public_post_comment-text

✗ **E** 15
This would mean only 1 VM is unavailable during maintenance. Because 16 VMs are spread across 5 update domains, one domain contains 4 VMs, and maintenance of that domain can make those 4 unavailable.

https://learn.microsoft.com/en-us/azure/virtual-machines/availability-set-overview?trk=public_post_comment-text

Question 43

Single choice · Domain: D3 Deploy and manage Azure compute resources › Create and configure virtual machines

You have an Azure subscription that has the public IPv4 addresses shown in the following table.

Name	Location	Availability zone
IP1	East US	1
IP2	East US	Zone-redundant
IP3	East US	2

You need to create a virtual machine named VM1 that has the following settings:

- Region: East US
- Availability options: Availability zone
- Availability zone: Zone 1

Which public IPv4 addresses can you assign to VM1?

A. IPI only
B. IP1orlP2only
C. IP1 or IP3 only
D. IP1, IP2, or IP3

Answer: B. IP1orlP2only

Explanation

VM1 is in East US Zone 1, so its public IP must either be in Zone 1 or be zone-redundant. IP1 is in Zone 1, and IP2 is zone-redundant, so both are assignable. IP3 is in Zone 2 and cannot be assigned to this Zone 1 VM. [1]

https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-addresses/

✗ **A** IP1 only
IP1 is assignable because it is in Zone 1, but it is not the only compatible address. IP2 is zone-redundant and can also be assigned to the Zone 1 VM. [1]

https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-addresses/

✓ **B** IP1 or IP2 only
IP1 is in the VM's Zone 1, and IP2 is zone-redundant, so both are compatible with VM1. IP3 is in Zone 2 and is not compatible with a VM in Zone 1. [1]

Free demo · full exam: 507 questions

https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-addresses/

✗ **C** IP1 or IP3 only
IP1 is compatible because it is in Zone 1, but IP3 is in Zone 2 and therefore does not match VM1's zone. This choice also omits zone-redundant IP2, which is compatible. [1]

https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-addresses/

✗ **D** IP1, IP2, or IP3
IP1 and zone-redundant IP2 are compatible with a Zone 1 VM. IP3 is zonal in Zone 2, so it cannot be assigned to VM1 in Zone 1. [1]

https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-addresses/

Question 44

Yes / No · Domain: D3 Deploy and manage Azure compute resources › Automate deployment of resources by using Azure Resource Manager (ARM) templates or Bicep files

You have an Azure subscription that contains a resource group named RG1.

You have a file named File1.bicep as shown in the File1.bicep exhibit. (Click the File1.bicep tab.)

```
resource vnet 'Microsoft.Network/virtualNetworks@2023-11-01' = {
  name: 'VNet1'
  location: resourceGroup().location
  tags: {
    CostCenter: '12345'
  }
  properties: {
    addressSpace: {
      addressPrefixes: [
        '10.0.0.0/24'
      ]
    }
    enableVmProtection: false
    enableDdosProtection: false
    subnets: [
      {
        name: 'Subnet1'
        properties: {
          addressPrefix: '10.0.0.0/24'
        }
      }
    ]
  }
}
```

```
resource vnet 'Microsoft.Network/virtualNetworks@2023-11-01' = {
  name: 'VNet1'
  location: resourceGroup().location
  tags: {
    CostCenter: '12345'
  }
  properties: {
    addressSpace: {
      addressPrefixes: [
        '10.0.0.0/24'
      ]
    }
    enableVmProtection: false
    enableDdosProtection: false
    subnets: [
      {
        name: 'Subnet1'
        properties: {
          addressPrefix: '10.0.0.0/24'
        }
      }
    ]
  }
}
```

```
resource vnet 'Microsoft.Network/virtualNetworks@2023-11-01' = {
  name: 'VNet1'
  location: resourceGroup().location
  tags: {
    CostCenter: '67890'
  }
  properties: {
    addressSpace: {
      addressPrefixes: [
        '10.0.0.0/16'
      ]
    }
    enableVmProtection: false
    enableDdosProtection: false
    subnets: [
      {
        name: 'Subnet2'
        properties: {
          addressPrefix: '10.0.1.0/24'
        }
      }
    ]
  }
}
```

Answer Area

Statements	Yes	No
VNet1 has a `CostCenter` tag that has a value of `12345`.	○	○

You create a file named File2.bicep as shown in the File2.bicep exhibit. (Click the File2.bicep tab.)

```
resource vnet 'Microsoft.Network/virtualNetworks@2023-11-01' = {
  name: 'VNet1'
  location: resourceGroup().location
  tags: {
    CostCenter: '67890'
  }
  properties: {
    addressSpace: {
      addressPrefixes: [
        '10.0.0.0/16'
      ]
    }
    enableVmProtection: false
    enableDdosProtection: false
    subnets: [
      {
        name: 'Subnet2'
        properties: {
          addressPrefix: '10.0.1.0/24'
        }
      }
    ]
  }
}
```

You run the following PowerShell commands.

```
New-AzResourceGroupDeployment -ResourceGroupName RG1 -TemplateFile File1.bicep
New-AzResourceGroupDeployment -WhatIf -ResourceGroupName RG1 -TemplateFile File2.bicep
```

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

NOTE: Each correct selection is worth one point.

Statement	Yes	No
VNet1 has a CostCenter tag that has a value of 12345.	☐	☐
VNet1 has an IP address space of 10.0.0.0/16.	☐	☐
VNet1 has two subnets.	☐	☐

Answer

- VNet1 has a CostCenter tag that has a value of 12345. **Yes**
- VNet1 has an IP address space of 10.0.0.0/16. **No**
- VNet1 has two subnets. **No**

Dumpsgate

Question 45

Single choice · Domain: D3 Deploy and manage Azure compute resources › Automate deployment of resources by using Azure Resource Manager (ARM) templates or Bicep files

You have an Azure virtual machine named VM1 that runs Windows Server. You generate a VM1 Azure Resource Manager (ARM) template. You plan to deploy a virtual machine named VM2 from the ARM template. What can you configure during the deployment of VM2?

A. virtual machine size
B. administrator username
C. resource group
D. operating system

Answer: C. resource group

Explanation

Free demo · full exam: 507 questions

The ARM template defines the virtual machine configuration, while the deployment is started at a chosen resource-group scope. For this deployment, you can select the resource group for VM2; changing its size, administrator username, or operating system would require those settings to be parameterized or edited in the template.

https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/export-template-powershell
https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/deploy-powershell
https://learn.microsoft.com/azure/azure-resource-manager/templates/deploy-cli

✗ **A** virtual machine size
The VM size is a configuration value in the template. It is not a deployment-time choice unless the template exposes it as a parameter or is edited to allow changing it.

https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/export-template-powershell
https://learn.microsoft.com/en-us/azure/virtual-machines/windows/template-description

✗ **B** administrator username
The administrator username is part of the VM configuration represented by the template, rather than the deployment scope. It would need to be exposed as a parameter or changed in the template to be configurable for this deployment.

https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/export-template-powershell
https://learn.microsoft.com/en-us/azure/virtual-machines/windows/template-description

✓ **C** resource group
You choose the target resource group when deploying the template. The resource group is the deployment scope, so it can be selected for VM2 without changing the VM settings in the template.

https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/deploy-powershell
https://learn.microsoft.com/azure/azure-resource-manager/templates/deploy-cli

✗ **D** operating system
The template specifies the VM's OS configuration or image. To deploy VM2 with a different operating system, you would need to change or parameterize that part of the template.

https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/export-template-powershell
https://learn.microsoft.com/en-us/azure/virtual-machines/windows/template-description

Dumpsgate

Question 46

Single choice · Domain: D3 Deploy and manage Azure compute resources › Provision and manage containers in the Azure portal

You have an Azure subscription that contains a container group named Group1. Group1 contains two Azure container instances as shown in the following table.

Name	Resource request	Resource limit
container1	2 CPUs	2 CPUs
container2	3 CPUs	4 CPUs

You need to ensure that container2 can use CPU resources without negatively affecting container1.

What should you do?

A. Increase the resource limit of container1 to three CPUs.
B. Increase the resource limit of container2 to six CPUs.
C. Remove the resource limit for both containers.
D. Decrease the resource limit of container2 to two CPUs.

Answer: C. Remove the resource limit for both containers.

Explanation

Container1 requests 2 CPUs, so its request is the allocation to preserve; its current 2-CPU limit prevents it from using spare CPU. Removing the limits lets the containers use available CPU beyond their requests, so container2 can use spare capacity while container1 retains its requested resources. This meets the goal better than raising or lowering either container's limit. [1]

https://learn.microsoft.com/en-us/azure/container-instances/container-instances-resource-and-quota-limits

✗ **A** Increase the resource limit of container1 to three CPUs.
This raises container1's maximum, not container2's, and does not remove the cap that prevents container1 from using spare CPU. It therefore does not address the requirement for container2 to use available CPU while preserving container1's requested resources. [1]

https://learn.microsoft.com/en-us/azure/container-instances/container-instances-resource-and-quota-limits

✗ **B** Increase the resource limit of container2 to six CPUs.
A higher limit would let container2 use more CPU, but it would not remove the limit on container1. This does not ensure container1 can use spare CPU beyond its current limit if needed. [1]

https://learn.microsoft.com/en-us/azure/container-instances/container-instances-resource-and-quota-limits

✓ **C** Remove the resource limit for both containers.
Removing the limits lets the containers use available CPU beyond their requests, rather than imposing the current maximums of 2 CPUs for container1 and 4 CPUs for container2. Container1's 2-CPU request remains the resource allocation to preserve, while container2 can use spare CPU. [1]

https://learn.microsoft.com/en-us/azure/container-instances/container-instances-resource-and-quota-limits

✗ **D** Decrease the resource limit of container2 to two CPUs.
This would cap container2 at 2 CPUs, below its current 4-CPU limit, restricting rather than enabling its ability to use available CPU. It also leaves container1's limit unchanged. [1]

https://learn.microsoft.com/en-us/azure/container-instances/container-instances-resource-and-quota-limits

Free demo · full exam: 507 questions

Question 47

Single choice · Domain: D3 Deploy and manage Azure compute resources › Automate deployment of resources by using Azure Resource Manager (ARM) templates or Bicep files

You have an Azure subscription. You plan to deploy the resources shown in the following table.

Name	Type
IP1	Microsoft.Network/publicIPAddresses
NSG1	Microsoft.Network/networkSecurityGroups
VNET1	Microsoft.Network/virtualNetworks
NIC1	Microsoft.Network/networkInterfaces
VM1	Microsoft.Compute/virtualMachines

You need to create a single Azure Resource Manager (ARM) template that will be used to deploy the resources. Which resource should be added to the dependsOn section for VM1?

A. IP1
B. VNET1
C. NIC1
D. NSG1

Answer: C. NIC1

Explanation

VM1 must have its network interface available before Azure can create the virtual machine, so NIC1 is the direct resource dependency to include in VM1's dependsOn section. IP1, VNET1, and NSG1 may be involved in the network configuration, but they are not the interface that VM1 attaches to. Any dependencies required to create NIC1 are handled in NIC1's own deployment dependencies. [1][2]

https://learn.microsoft.com/en-us/azure/virtual-machines/windows/template-description
https://learn.microsoft.com/azure/azure-resource-manager/templates/resource-dependency

✗ **A** IP1
IP1 is a public IP address, not the resource that VM1 uses as its network interface. VM1 depends directly on NIC1; IP1 can be a dependency of the network configuration without being the direct dependency to list for VM1. [1][2]

https://learn.microsoft.com/en-us/azure/virtual-machines/windows/template-description
https://learn.microsoft.com/azure/azure-resource-manager/templates/resource-dependency

✗ **B** VNET1
VNET1 provides the virtual network that the network interface connects to, but VM1 attaches to NIC1 rather than directly to the virtual network. NIC1's deployment can depend on VNET1, so VNET1 does not replace VM1's direct dependency on NIC1. [1][2]

https://learn.microsoft.com/en-us/azure/virtual-machines/windows/template-description
https://learn.microsoft.com/azure/azure-resource-manager/templates/resource-dependency

✓ **C** NIC1
NIC1 is the network interface that VM1 uses, so it must exist before VM1 can be deployed with that

Free demo · full exam: 507 questions

interface. Adding NIC1 to VM1's dependsOn section ensures that deployment order. [1][2]

https://learn.microsoft.com/en-us/azure/virtual-machines/windows/template-description
https://learn.microsoft.com/azure/azure-resource-manager/templates/resource-dependency

✗ **D** NSG1
NSG1 controls network traffic and may be associated with a network interface or subnet, but VM1 does not attach to the network security group as its network interface. The direct dependency for VM1 in this resource list is NIC1. [1][2]

https://learn.microsoft.com/en-us/azure/virtual-machines/windows/template-description
https://learn.microsoft.com/azure/azure-resource-manager/templates/resource-dependency

Question 48

Single choice · Domain: D3 Deploy and manage Azure compute resources › Automate deployment of resources by using Azure Resource Manager (ARM) templates or Bicep files

You have two Azure Resource Manager (ARM) templates named Template1 and Template2.

Deployments of Template1 currently fail because a virtual machine extension in Template1 depends on a resource referenced in Template2.

You need to ensure that Template1 and Template2 deploy together as a single transaction, and that if either deployment fails, the overall deployment fails. Both templates must remain separate and reusable.

What should you do?

A. In Template1, configure the provisionAfterExtensions property of the virtual machine extension.
B. In Template1, set the dependsOn property of the virtual machine extension.
C. Add the resources from Template2 to Template1.
D. Create a parent template that references Template1 and Template2 as linked templates.

Answer: D. Create a parent template that references Template1 and Template2 as linked templates.

Explanation

Create a parent template that deploys Template1 and Template2 as linked templates. This lets the templates remain separate and reusable while the parent coordinates them as one deployment operation. If either linked deployment fails, the parent deployment also fails.

https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/linked-templates
https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/linked-templates?tabs=azure-powershell

✗ **A** In Template1, configure the provisionAfterExtensions property of the virtual machine extension.
This property concerns the ordering of virtual machine extensions, not orchestration between two separate ARM templates. It does not make Template1 and Template2 part of one deployment or ensure that a failure in either template fails the overall deployment.

https://learn.microsoft.com/en-us/azure/templates/microsoft.compute/2025-04-01/virtualmachines/extensions

✗ **B** In Template1, set the dependsOn property of the virtual machine extension.
The dependsOn property expresses dependencies between resources in a template; it does not combine separate templates into one orchestrated deployment. It therefore does not meet the requirement to deploy both templates together while keeping them separate and reusable.

https://learn.microsoft.com/azure/azure-resource-manager/templates/resource-dependency

✗ **C** Add the resources from Template2 to Template1.
Putting Template2's resources into Template1 would no longer keep the templates separate. It also does not satisfy the stated requirement to reuse both templates as separate units.

✓ **D** Create a parent template that references Template1 and Template2 as linked templates.
A parent template can orchestrate deployments of both linked templates while leaving their contents separate and reusable. Because the parent manages the linked deployments, a failure in either deployment causes the overall parent deployment to fail.

https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/linked-templates
https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/linked-templates?tabs=azure-powershell

---

Question 49

Single choice · Domain: D3 Deploy and manage Azure compute resources › Automate deployment of resources by using Azure Resource Manager (ARM) templates or Bicep files

You have an Azure subscription.

You create the following Azure Resource Manager (ARM) template named Templatejson.

```
{
  "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {},
  "variables": {},
  "resources": [
    {
      "type": "Microsoft.Resources/resourceGroups",
      "apiVersion": "2022-12-01",
      "location": "eastus",
      "name": "Marketing"
    }
  ],
  "outputs": {}
}
```

You need to deploy Template.json.

Which PowerShell cmdlet should you run from Azure Cloud Shell?

A. New-AzManagementGroupDeployment
B. New-AzTenantDeployment
C. New-AzResourceGroupDeployment
D. New-AzSubscriptionDeployment

Answer: D. New-AzSubscriptionDeployment

Explanation

The template defines a `Microsoft.Resources/resourceGroups` resource, which is created at subscription

scope. Because the deployment is to be run from the Azure subscription, use `New-AzSubscriptionDeployment` (also exposed as `New-AzDeployment`) rather than a management-group, tenant, or resource-group-scope deployment cmdlet. [9]

https://learn.microsoft.com/en-us/powershell/module/az.resources/new-azdeployment?view=azps-16.0.0

✗ **A** New-AzManagementGroupDeployment
This cmdlet deploys an ARM template at management-group scope. The template creates a resource group at subscription scope, so this is not the deployment scope required here.

https://learn.microsoft.com/en-us/powershell/module/az.resources/new-azmanagementgroupdeployment?view=azps-16.0.0

✗ **B** New-AzTenantDeployment
This cmdlet deploys an ARM template at tenant scope. The template's resource group resource is intended to be created at subscription scope, so tenant scope is not appropriate.

https://learn.microsoft.com/en-us/powershell/module/az.resources/new-aztenantdeployment?view=azps-16.3.0

✗ **C** New-AzResourceGroupDeployment
This cmdlet deploys a template into an existing resource group. The template instead declares a resource group to create, which requires a subscription-scope deployment.

https://learn.microsoft.com/en-us/powershell/module/az.resources/new-azresourcegroupdeployment?view=azps-15.4.0

✓ **D** New-AzSubscriptionDeployment
This cmdlet deploys an ARM template at subscription scope, which is the required scope for creating the `Microsoft.Resources/resourceGroups` resource in the template. [9]

https://learn.microsoft.com/en-us/powershell/module/az.resources/new-azdeployment?view=azps-16.0.0

Dumpsgate

Question 50

Hotspot (dropdowns) · Domain: D3 Deploy and manage Azure compute resources › Automate deployment of resources by using Azure Resource Manager (ARM) templates or Bicep files

You have an Azure subscription that contains a resource group named RG1.

You plan to use an Azure Resource Manager (ARM) template named template1 to deploy resources. The solution must meet the following requirements:

Deploy new resources to RG1.

In RG1, delete resources that are not specified in the template.

How should you complete the command?

```
New-AzResourceGroupDeployment -TemplateUri
"https://contoso.com/template1" -TemplateParameterFile
params.json [Blank 1] RG1 -Mode [Blank 2]
```

Blank 1 (after params.json): -Name | -QueryString | -ResourceGroupName | -Tag

Blank 2 (after -Mode): All | Complete | Incremental

Answer

- Blank 1 (after params.json): **-ResourceGroupName**
- Blank 2 (after -Mode): **Complete**

Explanation

Use `-ResourceGroupName` to target the existing resource group RG1 for the deployment. Set `-Mode Complete` because complete mode removes resources in the target resource group that are not defined in the template, while still deploying the resources that are defined. This meets both requirements in the scenario.

https://learn.microsoft.com/en-us/azure/azure-resource-manager/deployment-modes
https://learn.microsoft.com/en-us/powershell/module/az.resources/new-azresourcegroupdeployment?view=azps-15.2.0
https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/deployment-complete-mode-deletion

✗ **Blank 1: -Name** -Name
`-Name` specifies the deployment name, not the resource group to which the template should be deployed. It would not identify RG1 as the deployment target.

https://learn.microsoft.com/en-us/powershell/module/az.resources/new-azresourcegroupdeployment?view=azps-15.2.0

✗ **Blank 1: -QueryString** -QueryString

`-QueryString` supplies a query string for a template URI; it does not select a resource group. The command needs the resource-group parameter to target RG1.

https://learn.microsoft.com/en-us/powershell/module/az.resources/new-azresourcegroupdeployment?view=azps-15.2.0

✓ **Blank 1: -ResourceGroupName** -ResourceGroupName
This parameter specifies the resource group for the deployment. Using it before `RG1` directs the template deployment to the required resource group.

https://learn.microsoft.com/en-us/powershell/module/az.resources/new-azresourcegroupdeployment?view=azps-15.2.0

✗ **Blank 1: -Tag** -Tag
`-Tag` applies tags to the deployment; it does not specify the resource group where resources should be deployed. It therefore cannot target RG1 in this command.

https://learn.microsoft.com/en-us/powershell/module/az.resources/new-azresourcegroupdeployment?view=azps-15.2.0

✗ **Blank 2: All** All
`All` is not the deployment mode that requests deletion of resources absent from the template. The required mode is `Complete`.

https://learn.microsoft.com/en-us/azure/azure-resource-manager/deployment-modes
https://learn.microsoft.com/en-us/powershell/module/az.resources/new-azresourcegroupdeployment?view=azps-15.2.0

✓ **Blank 2: Complete** Complete
Complete mode deploys the resources specified by the template and deletes existing resources in the target resource group that are not specified in the template. That matches the requirement for RG1.

https://learn.microsoft.com/en-us/azure/azure-resource-manager/deployment-modes
https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/deployment-complete-mode-deletion

✗ **Blank 2: Incremental** Incremental
Incremental mode deploys or updates resources specified in the template but leaves other resources in RG1 unchanged. It would not delete the resources that are absent from the template.

https://learn.microsoft.com/en-us/azure/azure-resource-manager/deployment-modes
https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/deployment-complete-mode-deletion

Question 51

Single choice · Domain: D3 Deploy and manage Azure compute resources › Create and configure virtual machines

You plan to deploy several Azure virtual machines that will run Windows Server in a virtual machine scale set by using an Azure Resource Manager template.

You need to ensure that NGINX is available on all the virtual machines after they are deployed.

What should you use?

A. the New-AzConfigurationAssignment cmdlet
B. Azure Application Insights
C. a Microsoft Intune device configuration profile
D. a Desired State Configuration (DSC) extension

Answer: D. a Desired State Configuration (DSC) extension

Dumpsgate

Free demo · full exam: 507 questions

Question 52

Single choice · Domain: D3 Deploy and manage Azure compute resources › Create and configure Azure App Service

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

Name	Location	Description
RG1	East US	Resource group
ASP1	East US	Azure App Service plan
ASP2	West Europe	Azure App Service plan
WebApp1	East US	Azure App Service web app in ASP1
Managed1	East US	Managed identity

```
$srcapp = Get-AzWebApp -ResourceGroupName RG1 -Name WebApp1
New-AzWebApp -ResourceGroupName RG1 -Name WebApp2 -Location "West Europe" -AppServicePlan ASP2 -SourceWebApp $srcapp
```

WebApp1 has the following configurations:

- Identity: Managed!
- Environment variable: EnvVar1
- Deployment slots: WebApp1 --slot1
- Backups: Perform a custom backup every two days

You clone WebApp1 by running the following commands.

Which configuration of WebApp1 is cloned to WebApp2?

A. Identity
B. Deployment slots
C. Backups
D. Environment variable

Answer: D. Environment variable

Explanation

The `New-AzWebApp` command creates WebApp2 from WebApp1 using `-SourceWebApp`, which copies supported app configuration, including application settings. The `EnvVar1` environment variable is an application setting, so it is cloned. The managed identity, deployment slots, and backup schedule are not cloned as part of this operation.

https://learn.microsoft.com/en-us/azure/app-service/app-service-web-app-cloning
https://learn.microsoft.com/en-us/azure/app-service/configure-common?view=migrate
https://learn.microsoft.com/en-us/azure/app-service/overview-managed-identity
https://learn.microsoft.com/en-us/azure/app-service/manage-backup

✗ **A** Identity
WebApp2 does not inherit WebApp1's managed identity through this cloning operation. A managed identity is associated with the individual app resource and must be configured for the new app as needed.

https://learn.microsoft.com/en-us/azure/app-service/app-service-web-app-cloning
https://learn.microsoft.com/en-us/azure/app-service/overview-managed-identity

✗ **B** Deployment slots
WebApp1's deployment slots are not cloned to WebApp2 by the command shown. Cloning the app does not create copies of its deployment slots.

https://learn.microsoft.com/en-us/azure/app-service/app-service-web-app-cloning

✗ **C** Backups
The custom backup schedule is not cloned to WebApp2. Backup configuration must be set up separately for the new app.

https://learn.microsoft.com/en-us/azure/app-service/app-service-web-app-cloning
https://learn.microsoft.com/en-us/azure/app-service/manage-backup

✓ **D** Environment variable
The environment variable is an app setting, and app settings are included among the configurations copied when cloning an App Service web app. Therefore, `EnvVar1` is cloned to WebApp2.

https://learn.microsoft.com/en-us/azure/app-service/app-service-web-app-cloning
https://learn.microsoft.com/en-us/azure/app-service/configure-common?view=migrate

Question 53

Multiple choice · Domain: D4 Implement and manage virtual networking › Configure secure access to virtual networks

Your organization is deploying a multi-tier application to Azure with a web tier and a database tier. The web servers must be isolated from direct internet access, while the database servers must only accept connections from the web tier. You need to implement network segmentation using Azure virtual networks and Network Security Groups (NSGs).

Which of the following configurations will meet these requirements? (Select all that apply.)

A. Create two subnets within a single virtual network: one for web servers and one for database servers. Apply an NSG to the database subnet that denies all inbound traffic except from the web subnet's address space.

B. Deploy the web servers and database servers in separate virtual networks and configure NSG rules to allow traffic only between the specific IP addresses of the web tier and database tier.

C. Place all servers in a single subnet with a single NSG that uses service tags to allow only HTTP and HTTPS traffic to reach any resources in the subnet.

D. Apply an NSG to the web subnet that denies all inbound traffic from the internet, then create a second NSG on the database subnet that denies all traffic except from the web subnet.

Answer: D. Apply an NSG to the web subnet that denies all inbound traffic from the internet, then create a second NSG on the database subnet that denies all traffic except from the web subnet.

Explanation

D addresses both requirements with separate subnet-level controls: the web subnet's NSG blocks inbound traffic from the internet, and the database subnet's NSG permits traffic only from the web subnet while denying other traffic. NSGs filter network traffic using rules, which makes them suitable for enforcing these tier-specific restrictions. The other choices either omit an explicit restriction on internet access to the web tier or do not restrict database access to the web tier.

https://learn.microsoft.com/en-us/security/zero-trust/azure-networking-segmentation

Free demo · full exam: 507 questions

https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-nsg

✗ **A** Create two subnets within a single virtual network: one for web servers and one for database servers. Apply an NSG to the database subnet that denies all inbound traffic except from the web subnet's address space.
The database subnet is restricted to traffic from the web subnet, but this configuration does not specify a rule blocking direct internet access to the web servers. It therefore does not meet both requirements.

https://learn.microsoft.com/en-us/azure/networking/design-guide/vnets-subnets
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-nsg

✗ **B** Deploy the web servers and database servers in separate virtual networks and configure NSG rules to allow traffic only between the specific IP addresses of the web tier and database tier.
This describes inter-tier allow rules, but it does not explicitly configure the required internet block on the web tier. Separate virtual networks alone do not establish that restriction; the web tier needs an NSG rule that blocks inbound internet traffic.

https://learn.microsoft.com/en-us/azure/networking/design-guide/vnets-subnets
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-nsg

✗ **C** Place all servers in a single subnet with a single NSG that uses service tags to allow only HTTP and HTTPS traffic to reach any resources in the subnet.
A single subnet and shared rule set do not isolate the web and database tiers. Allowing HTTP and HTTPS to resources in the subnet also does not ensure that the database accepts connections only from the web tier.

https://learn.microsoft.com/en-us/azure/networking/design-guide/flat-network
https://learn.microsoft.com/en-us/security/zero-trust/azure-networking-segmentation
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-nsg

✓ **D** Apply an NSG to the web subnet that denies all inbound traffic from the internet, then create a second NSG on the database subnet that denies all traffic except from the web subnet.
The web-subnet NSG blocks direct inbound access from the internet, and the database-subnet NSG limits database connections to the web subnet. This applies the required restrictions separately to each application tier.

https://learn.microsoft.com/en-us/troubleshoot/azure/virtual-network/virtual-network-troubleshoot-nsg-blocking-traffic
https://learn.microsoft.com/en-us/security/zero-trust/azure-networking-segmentation
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-nsg

Question 54

Single choice · Domain: D4 Implement and manage virtual networking › Configure name resolution and load balancing

Your organization is deploying a DNS-based load balancing solution to distribute traffic across multiple Azure regions for global application availability. Users should be directed to the region closest to them, and health checks must ensure unhealthy regions are removed from rotation. Which Azure service should you use?

A. Azure Traffic Manager with geographic routing policy and health probe configuration
B. Azure Load Balancer with cross-region load balancing rules
C. Azure Application Gateway with multi-region backend pools
D. Azure Front Door with Azure Firewall integrated for health monitoring
E. Azure ExpressRoute with traffic distribution policies

Answer: A. Azure Traffic Manager with geographic routing policy and health probe configuration

Free demo · full exam: 507 questions

Question 55

Single choice · Domain: D4 Implement and manage virtual networking › Configure secure access to virtual networks

Your organization is deploying a multi-tier application in Azure with web servers in one subnet and database servers in another subnet within the same virtual network. You need to ensure that only the web servers can initiate connections to the database servers on port 3306, while blocking all other traffic between the subnets. Which combination of Azure networking features should you implement?

A. Network Security Groups (NSGs) applied to the database subnet to allow inbound traffic only from the web server subnet on port 3306
B. A firewall rule in the virtual network settings to block subnet-to-subnet communication
C. User-defined routes (UDRs) configured to deny traffic between subnets
D. Virtual network peering between the two subnets to control traffic flow
E. An Azure Bastion host configured with network segmentation policies

Answer: A. Network Security Groups (NSGs) applied to the database subnet to allow inbound traffic only from the web server subnet on port 3306

Explanation

Apply an NSG to the database subnet and configure rules that allow inbound connections from the web-server subnet on TCP port 3306 while denying other traffic between the subnets. NSGs filter network traffic using rules that can specify source, destination, protocol, and port; ensure the rules account for any default rules that would otherwise allow traffic within the virtual network. [4, 9, 12]

https://learn.microsoft.com/azure/virtual-network/network-security-group-how-it-works
https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-nsg

✓ **A** Network Security Groups (NSGs) applied to the database subnet to allow inbound traffic only from the web server subnet on port 3306
An NSG on the database subnet can allow inbound TCP traffic from the web-server subnet to destination port 3306 and deny other traffic between the subnets. Configure rule priorities and any required deny rule so that default virtual-network traffic allowances do not permit other connections. [4, 9, 12]

https://learn.microsoft.com/azure/virtual-network/network-security-group-how-it-works
https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-filter-network-traffic
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-nsg

✗ **B** A firewall rule in the virtual network settings to block subnet-to-subnet communication
A virtual network does not provide the described general firewall-rule setting for controlling subnet traffic. Also, blocking all subnet-to-subnet communication would prevent the required web-server connections to the database on port 3306.

✗ **C** User-defined routes (UDRs) configured to deny traffic between subnets
UDRs determine where network traffic is routed; they are not the appropriate feature for enforcing this source-and-port-specific allow/deny policy. An NSG can filter the database-subnet traffic by source subnet and destination port.

✗ **D** Virtual network peering between the two subnets to control traffic flow
Virtual network peering connects separate virtual networks; the web and database subnets are already within the same virtual network. Peering provides connectivity rather than the required per-port traffic filtering. [10]

https://learn.microsoft.com/azure/virtual-network/virtual-network-peering-overview

✗ **E** An Azure Bastion host configured with network segmentation policies
Azure Bastion provides secure browser-based access to virtual machines for management; it does not enforce segmentation policies for application traffic between the web and database subnets. [6]

https://learn.microsoft.com/en-us/azure/bastion/design-architecture

Question 56

Multiple choice · Domain: D4 Implement and manage virtual networking › Configure and manage virtual networks in Azure

You are managing an Azure virtual network that uses on-premises network resources. You have deployed an Azure VPN Gateway to establish a secure connection between the on-premises network and your Azure VNet.

However, you notice that communication between on-premises resources and resources in the Azure VNet is intermittent and unreliable.

Which of the following steps should you take to troubleshoot and diagnose the VPN connection issue?

A. Check the local network gateway configuration to ensure the on-premises network address space is correctly defined
B. Verify that the VPN connection status in the Azure portal shows 'Connected'
C. Review network security group (NSG) rules on Azure subnets to ensure they permit traffic from on-premises address ranges
D. Delete and recreate the VPN gateway to reset the connection
E. Modify the Azure VNet address space to match the on-premises network exactly

Answer

- A. **Check the local network gateway configuration to ensure the on-premises network address space is correctly defined**
- B. **Verify that the VPN connection status in the Azure portal shows 'Connected'**
- C. **Review network security group (NSG) rules on Azure subnets to ensure they permit traffic from on- premises address ranges**

Explanation

For an intermittent site-to-site VPN, verify that the local network gateway describes the on-premises address space correctly and check the connection status in Azure to help identify tunnel connectivity problems. Also review NSG rules, because a connected VPN tunnel does not guarantee that subnet rules allow traffic between Azure and on-premises address ranges. These checks diagnose likely configuration and traffic-filtering causes without making disruptive changes.

https://learn.microsoft.com/en-us/troubleshoot/azure/vpn-gateway/vpn-gateway-troubleshoot
https://learn.microsoft.com/en-us/troubleshoot/azure/vpn-gateway/vpn-gateway-troubleshoot-site-to-site-disconnected-intermittently
https://learn.microsoft.com/en-us/troubleshoot/azure/virtual-network/virtual-network-troubleshoot-nsg-blocking-traffic

✓ **A** Check the local network gateway configuration to ensure the on-premises network address space is

correctly defined
The local network gateway represents the on-premises VPN device and its address prefixes in Azure. Incorrect or incomplete prefixes can cause traffic to be routed incorrectly, so checking this configuration is a relevant troubleshooting step.

https://learn.microsoft.com/en-us/troubleshoot/azure/vpn-gateway/vpn-gateway-troubleshoot
https://learn.microsoft.com/en-us/troubleshoot/azure/vpn-gateway/troubleshoot-vpn-tunnel-cannot-connect
https://learn.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal?WT.mc_id=AZ-MVP-5004796

✓ **B** Verify that the VPN connection status in the Azure portal shows 'Connected'
Checking the connection status helps determine whether the VPN tunnel is currently established and can expose connectivity interruptions. It is a useful diagnostic check for an intermittent connection, although it does not by itself confirm that all application traffic can pass.

https://learn.microsoft.com/en-us/troubleshoot/azure/vpn-gateway/vpn-gateway-troubleshoot
https://learn.microsoft.com/en-us/troubleshoot/azure/vpn-gateway/vpn-gateway-troubleshoot-site-to-site-disconnected-intermittently

✓ **C** Review network security group (NSG) rules on Azure subnets to ensure they permit traffic from on-premises address ranges
NSG rules can block traffic even when the VPN tunnel is connected. Reviewing the rules for the Azure subnets and confirming that they allow the relevant on-premises source ranges can identify a traffic-filtering cause.

https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-diagnose-on-premises-connectivity
https://learn.microsoft.com/en-us/troubleshoot/azure/virtual-network/virtual-network-troubleshoot-nsg-blocking-traffic

✗ **D** Delete and recreate the VPN gateway to reset the connection
Deleting and recreating the gateway is a disruptive change, not an appropriate initial diagnostic step for intermittent communication. Check the gateway configuration, connection status, and traffic rules first; resetting a gateway is a separate recovery action and is not the same as deleting and recreating it.

https://learn.microsoft.com/en-us/troubleshoot/azure/vpn-gateway/vpn-gateway-troubleshoot
https://learn.microsoft.com/en-us/azure/vpn-gateway/reset-gateway

✗ **E** Modify the Azure VNet address space to match the on-premises network exactly
The Azure VNet and on-premises network should use distinct, non-overlapping address spaces so that traffic can be routed between them. The local network gateway should instead be configured with the on-premises address prefixes; changing the VNet to match them would not be the correct fix.

https://learn.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal?WT.mc_id=AZ-MVP-5004796
https://learn.microsoft.com/azure/vpn-gateway/vpn-gateway-howto-vnet-vnet-resource-manager-portal

Free demo · full exam: 507 questions

Question 57

Single choice · Domain: D4 Implement and manage virtual networking › Configure and manage virtual networks in Azure

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

Name	Location	Description
VNet1	East US	Virtual network
Subnet1	East US	Subnet on VNet1
NIC1	East US	Network interface

You create a route table named RT1 in the East US Azure region. To which resources can you associate RT1?

A. VNet1 only
B. Subnet1 only
C. VNet1 and NIC1 only
D. Subnet1 and NIC1 only
E. VNet1, Subnet1, and NIC!

Answer: B. Subnet1 only

Explanation

Azure route tables are associated with subnets, not directly with virtual networks or network interfaces. RT1 is in East US, and Subnet1 is also in East US, so RT1 can be associated with Subnet1. Therefore, the correct answer is B.

https://learn.microsoft.com/en-us/azure/virtual-network/manage-route-table
https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-create-route-table

✗ **A** VNet1 only
A route table is not associated directly with a virtual network. It is associated with a subnet, so VNet1 alone is not a valid target.

https://learn.microsoft.com/en-us/azure/virtual-network/manage-route-table
https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-create-route-table

✓ **B** Subnet1 only
Route tables are associated with subnets. Subnet1 is in East US, the same region as RT1, so it can be associated with RT1.

https://learn.microsoft.com/en-us/azure/virtual-network/manage-route-table
https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-create-route-table

✗ **C** VNet1 and NIC1 only
Neither a virtual network nor a network interface is a direct association target for a route table. The route table must instead be associated with a subnet.

https://learn.microsoft.com/en-us/azure/virtual-network/manage-route-table
https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-create-route-table

✗ **D** Subnet1 and NIC1 only
Subnet1 can be associated with RT1, but NIC1 cannot be associated with a route table directly. This option therefore includes an invalid target.

https://learn.microsoft.com/en-us/azure/virtual-network/manage-route-table
https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-create-route-table

✗ **E** VNet1, Subnet1, and NIC1
Subnet1 is a valid association target, but VNet1 and NIC1 are not. A route table is associated with a subnet, not directly with its virtual network or a network interface.

https://learn.microsoft.com/en-us/azure/virtual-network/manage-route-table
https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-create-route-table

Question 58

Single choice · Domain: D4 Implement and manage virtual networking › Configure name resolution and load balancing

You have an Azure subscription that contains a virtual network named VNet1 and a virtual machine named VM1. VM1 runs Windows Server and is connected to VNet1.

You perform the following tasks:

- On VM1, you install the DNS Server role.
- On VM1, you create a standard primary DNS zone named zone1.com.
- From the Azure portal, you create an Azure DNS zone named zone2.com.
- From the Azure portal, you create an Azure Private DNS zone named zone3.com.

For which zones can you add a virtual network link to VNet1?

A. zone1.com only
B. zone2.com only
C. zone3.com only
D. zone2.com and zone3.com only
E. zone1.com, zone2.com, and zone3.com

Answer: C. zone3.com only

Explanation

A virtual network link to VNet1 can be created for zone3.com because it is an Azure Private DNS zone, and private DNS zones support links to virtual networks. The standard primary zone hosted on VM1 is a Windows DNS zone, not an Azure Private DNS zone. The Azure DNS zone zone2.com is a public DNS zone, which does not support Azure virtual network links.

https://learn.microsoft.com/en-us/azure/dns/private-dns-virtual-network-links
https://learn.microsoft.com/en-us/azure/dns/public-dns-overview
https://learn.microsoft.com/en-us/azure/dns/private-dns-overview/

✗ **A** zone1.com only
zone1.com is a standard primary zone hosted by the DNS Server role on VM1. It is not an Azure Private DNS zone, so you cannot add an Azure virtual network link to it.

https://learn.microsoft.com/en-us/azure/dns/private-dns-virtual-network-links

✗ **B** zone2.com only
zone2.com is an Azure DNS public zone. Public DNS zones do not have virtual network links; that linking feature is for Azure Private DNS zones.

https://learn.microsoft.com/en-us/azure/dns/private-dns-virtual-network-links
https://learn.microsoft.com/en-us/azure/dns/public-dns-overview

✓ **C** zone3.com only
zone3.com is an Azure Private DNS zone, and Azure Private DNS zones support virtual network links. Therefore, VNet1 can be linked to zone3.com.

https://learn.microsoft.com/en-us/azure/dns/private-dns-virtual-network-links
https://learn.microsoft.com/en-us/azure/dns/private-dns-overview/

✗ **D** zone2.com and zone3.com only
zone3.com supports a virtual network link because it is an Azure Private DNS zone. zone2.com is a public Azure DNS zone, which does not support that type of link.

https://learn.microsoft.com/en-us/azure/dns/private-dns-virtual-network-links
https://learn.microsoft.com/en-us/azure/dns/public-dns-overview

✗ **E** zone1.com, zone2.com, and zone3.com
Only zone3.com is an Azure Private DNS zone. zone1.com is hosted on VM1 as a Windows DNS zone, and zone2.com is an Azure public DNS zone; neither can be linked to VNet1 using Azure Private DNS virtual network links.

https://learn.microsoft.com/en-us/azure/dns/private-dns-virtual-network-links
https://learn.microsoft.com/en-us/azure/dns/public-dns-overview
https://learn.microsoft.com/en-us/azure/dns/private-dns-overview/

Dumpsgate

Question 59

Yes / No · Domain: D4 Implement and manage virtual networking › Configure and manage virtual networks in Azure

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

Name	IP address space	Location	Subnet	Peered with
VNet1	10.10.0.0/16	East US	Subnet11, Subnet12	VNet2
VNet2	172.16.0.0/16	West US	Subnet2	VNet1
VNet3	192.168.0.0/16	East US	Subnet3	None

The subscription contains the virtual machines shown in the following table.

Name	IP address	Connected to
VM11	10.10.1.10	Subnet11
VM12	10.10.2.10	Subnet12
VM2	172.16.1.10	Subnet2
VM3	192.168.1.10	Subnet3

You create the route tables shown in the following table.

Name	Associated with
RT1	Subnet11
RT2	Subnet2
RT3	Subnet3

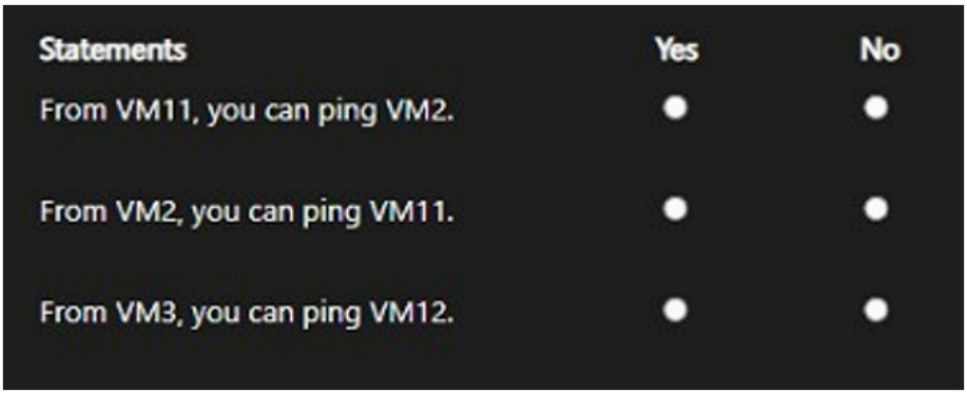
The route tables include the routes shown in the following table.

Name	In route table	Destination	Next hop type	Next hop address
Route1	RT1	192.168.0.0/16	Virtual appliance	192.168.1.10
Route2	RT2	10.10.1.0/24	None	Not applicable
Route3	RT3	10.10.0.0/16	Virtual appliance	10.10.2.10

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

NOTE: Each correct selection is worth one point.

Free demo · full exam: 507 questions



Statement	Yes	No
From VM11, you can ping VM2.	☐	☐
From VM2, you can ping VM11.	☐	☐
From VM3, you can ping VM12.	☐	☐

Answer

- From VM11, you can ping VM2. **No**
- From VM2, you can ping VM11. **No**
- From VM3, you can ping VM12. **No**

Explanation

All three statements are false. VM11 and VM2 are in peered VNets, but the route associated with VM2's subnet blackholes traffic destined for VM11's address, so ping cannot complete in either direction. VM3's VNet is not peered with VNet1, and the route in RT3 does not create connectivity to VM12.

https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/virtual-network-peering
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview?WT.mc_id=MVP_381754

✓ **Statement 1** From VM11, you can ping VM2. — No
VM11 can route toward VM2 through the VNet1–VNet2 peering, but a ping also requires a reply. RT2 is associated with VM2's subnet and has a route for 10.10.1.0/24 with next hop type None, which drops the reply traffic to VM11. Therefore, the ping cannot succeed.

https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/virtual-network-peering
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview?WT.mc_id=MVP_381754

✓ **Statement 2** From VM2, you can ping VM11. — No
RT2 is associated with VM2's subnet, and its 10.10.1.0/24 route has next hop type None. VM11's address, 10.10.1.10, matches that route, so traffic from VM2 to VM11 is dropped rather than sent over the peering.

https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/virtual-network-peering
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview?WT.mc_id=MVP_381754

✓ **Statement 3** From VM3, you can ping VM12. — No
VM3 is in VNet3, which is not peered with VNet1, where VM12 resides. RT3's route naming VM12 as a virtual-appliance next hop does not establish peering or otherwise provide a reachable path between the VNets, so VM3 cannot ping VM12.

https://learn.microsoft.com/azure/virtual-network/virtual-network-routing-appliance-overview

https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/virtual-network-peering
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview?WT.mc_id=MVP_381754

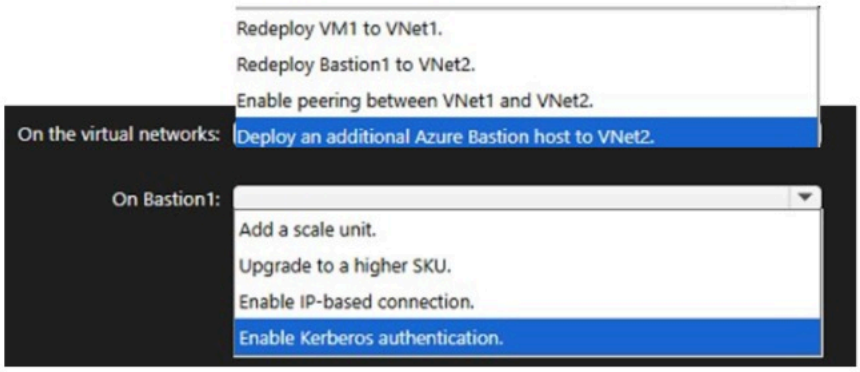
Question 60

Hotspot (dropdowns) · Domain: D4 Implement and manage virtual networking › Configure secure access to virtual networks

You have an Azure subscription that contains two virtual networks named VNet1 and VNet2. VNet1 contains multiple virtual machines and an Azure Bastion host named Bastion1 that uses the Standard SKU. VNet2 contains a virtual machine named VM1.

External users access the virtual machines on VNet1 by using Bastion1.

You need to use Bastion1 to provide RDP access to VM1. The solution must minimize costs and administrative effort.



On the virtual networks: Redeploy VM1 to VNet1. | Redeploy Bastion1 to VNet2. | Enable peering between VNet1 and VNet2. | Deploy an additional Azure Bastion host to VNet2.

On Bastion1: Add a scale unit. | Upgrade to a higher SKU. | Enable IP-based connection. | Enable Kerberos authentication.

Answer

- On the virtual networks: **Enable peering between VNet1 and VNet2.**
- On Bastion1: **Enable IP-based connection.**

Explanation

Enable VNet peering so Bastion1 in VNet1 can reach VM1 in VNet2 without moving resources or deploying another Bastion host. Then enable IP-based connection on Bastion1 so you can connect to VM1 by its IP address across the peered network. This reuses the existing Standard SKU host and avoids the added cost and administration of another host. [1][3]

https://learn.microsoft.com/en-us/azure/bastion/vnet-peering
https://learn.microsoft.com/en-us/azure/bastion/connect-ip-address?WT.mc_id=AZ-MVP-4038163

✗ **Box 1: Redeploy VM1 to VNet1.** Redeploy VM1 to VNet1.
Moving VM1 would require unnecessary deployment work and could disrupt the VM. VNet peering lets

Bastion1 reach a VM in VNet2 without moving it. [1]

https://learn.microsoft.com/en-us/azure/bastion/vnet-peering

✗ **Box 1: Redeploy Bastion1 to VNet2.** Redeploy Bastion1 to VNet2.
Redeploying Bastion1 would add administrative effort and could disrupt the existing users who rely on it to access VNet1. Peering allows the existing host in VNet1 to reach VM1 in VNet2. [1]

https://learn.microsoft.com/en-us/azure/bastion/vnet-peering

✓ **Box 1: Enable peering between VNet1 and VNet2.** Enable peering between VNet1 and VNet2.
VNet peering provides network connectivity between VNet1, where Bastion1 is deployed, and VNet2, where VM1 resides. This lets you reuse Bastion1 instead of relocating it or deploying another host. [1]

https://learn.microsoft.com/en-us/azure/bastion/vnet-peering

✗ **Box 1: Deploy an additional Azure Bastion host to VNet2.** Deploy an additional Azure Bastion host to VNet2.
A second Bastion host would add deployment, management, and hosting costs. Peering VNet2 with VNet1 and using Bastion1's IP-based connection capability avoids the additional host. [1][3]

https://learn.microsoft.com/en-us/azure/bastion/vnet-peering
https://learn.microsoft.com/en-us/azure/bastion/connect-ip-address?WT.mc_id=AZ-MVP-4038163

✗ **Box 2: Add a scale unit.** Add a scale unit.
Scale units increase Bastion capacity; they do not provide the network path or connection method needed to access VM1 in VNet2. The scenario calls for connectivity across the peered VNets, not more session capacity. [2]

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

✗ **Box 2: Upgrade to a higher SKU.** Upgrade to a higher SKU.
Bastion1 already uses the Standard SKU, which supports the required IP-based connection capability. An upgrade would add cost without being necessary for this scenario. [3][8]

https://learn.microsoft.com/en-us/azure/bastion/connect-ip-address?WT.mc_id=AZ-MVP-4038163
https://learn.microsoft.com/en-us/azure/bastion/bastion-sku-comparison?trk=public_post_comment-text

✓ **Box 2: Enable IP-based connection.** Enable IP-based connection.
IP-based connection lets Bastion connect to a target VM by its IP address, including a VM in a peered virtual network. Since Bastion1 already uses Standard, enabling this feature avoids upgrading or deploying another host. [3]

https://learn.microsoft.com/en-us/azure/bastion/connect-ip-address?WT.mc_id=AZ-MVP-4038163

✗ **Box 2: Enable Kerberos authentication.** Enable Kerberos authentication.
Kerberos changes the authentication options for Bastion connections; it does not establish connectivity between VNet1 and VNet2 or enable IP-based targeting of VM1. It does not address the requirement in this scenario. [11]

https://learn.microsoft.com/en-us/azure/bastion/kerberos-authentication-portal/?WT.mc_id=AZ-MVP-4038163

Question 61

Single choice · Domain: D4 Implement and manage virtual networking › Configure name resolution and load balancing

You have an Azure subscription that contains two virtual networks named VNet1 and VNet2. VNet1 contains two virtual machines named VM1 and VM2. VM1 and VM2 host an application named App1.

The resources on VNet2 only access App1 through the internal network.

You need to ensure that inbound traffic from VNet2 to App1 is evenly distributed between VM1 and VM2. The solution must ensure that the virtual machines are NOT exposed to the internet.

What should you use?

A. Azure Application Gateway
B. Azure Load Balancer
C. Azure Front Door
D. Azure Traffic Manager

Answer: B. Azure Load Balancer

Explanation

Use an Azure Load Balancer with an internal frontend to distribute VNet2's inbound traffic across VM1 and VM2. The internal frontend keeps the VMs off the internet while allowing access over the internal network; Azure Load Balancer provides traffic distribution to backend VMs. [3]

https://learn.microsoft.com/en-us/azure/load-balancer/components

✗ **A** Azure Application Gateway
Application Gateway can use a private frontend, so it can avoid exposing the VMs to the internet. However, it is an application-layer gateway for HTTP(S) traffic, and the scenario calls for distributing inbound traffic between the VMs without specifying application-layer routing. [1][7]

https://learn.microsoft.com/en-us/azure/application-gateway/configure-application-gateway-with-private-frontend-ip
https://learn.microsoft.com/en-us/azure/application-gateway/application-gateway-components

✓ **B** Azure Load Balancer
An internal Azure Load Balancer distributes traffic arriving at its private frontend across backend VMs. VNet2 can reach that frontend over the internal network, and the VMs do not need internet-facing endpoints. [3][6]

https://learn.microsoft.com/en-us/azure/load-balancer/components
https://learn.microsoft.com/en-us/azure/virtual-network/network-overview

✗ **C** Azure Front Door
Azure Front Door is designed for internet-facing application delivery, rather than distributing traffic from VNet2 through a private internal frontend. It does not meet the requirement to keep the VMs unexposed to the internet. [2]

https://learn.microsoft.com/en-us/azure/networking/design-guide/internet-ingress

✗ **D** Azure Traffic Manager
Traffic Manager uses DNS-based routing to direct clients to endpoints; it does not act as an internal traffic proxy that distributes each connection across VM1 and VM2. It therefore does not meet the stated internal load-balancing requirement. [5]

https://learn.microsoft.com/en-us/azure/traffic-manager/traffic-manager-how-it-works

Question 62

Single choice · Domain: D4 Implement and manage virtual networking › Configure name resolution and load balancing

You have an Azure subscription that uses the public IP addresses shown in the following table.

Name	IP version	SKU	IP address assignment	Availability zone
IP1	IPv6	Basic	Static	Not applicable
IP2	IPv6	Basic	Dynamic	Not applicable
IP3	IPv6	Standard	Static	Zone-redundant

You need to create a public Azure Standard Load Balancer.

Which public IP addresses can you use?

A. IP1 and IP3 only
B. IP1, IP2, and IP3
C. IP2 only
D. IP3 only

Answer: D. IP3 only

Explanation

A public Azure Standard Load Balancer requires a Standard SKU public IP address. IP1 and IP2 are Basic SKU addresses, so neither meets that requirement; IP2 is also dynamically assigned. IP3 is Standard SKU and statically assigned, so it is the only address in the table that can be used. [1][2]

https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-addresses/
https://learn.microsoft.com/en-us/azure/load-balancer/skus

✗ **A** IP1 and IP3 only
IP3 meets the requirement, but IP1 is a Basic SKU public IP address. A Standard Load Balancer requires a Standard SKU public IP address, so IP1 cannot be used for it. [1][2]

https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-addresses/
https://learn.microsoft.com/en-us/azure/load-balancer/skus

✗ **B** IP1, IP2, and IP3
IP3 is usable, but IP1 and IP2 are Basic SKU addresses, which are not compatible with a Standard Load Balancer. IP2 is additionally dynamically assigned, whereas IP3 is static. [1][2]

https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-addresses/
https://learn.microsoft.com/en-us/azure/load-balancer/skus

✗ **C** IP2 only
IP2 is a Basic SKU public IP address, so it cannot be used with a Standard Load Balancer. Its dynamic assignment is also unsuitable for the required Standard public IP configuration. [1][2]

https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-addresses/
https://learn.microsoft.com/en-us/azure/load-balancer/skus

✓ **D** IP3 only
IP3 is the only address in the table with the Standard SKU. It is statically assigned, so it meets the public IP requirements for the Standard Load Balancer. [1][2]

https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-addresses/

Free demo · full exam: 507 questions

https://learn.microsoft.com/en-us/azure/load-balancer/skus

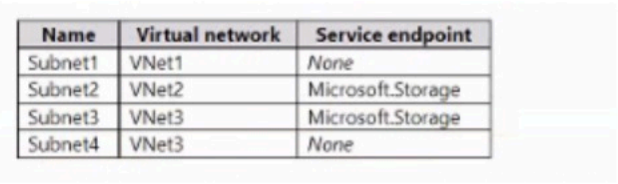
Question 63

Yes / No · Domain: D4 Implement and manage virtual networking › Configure secure access to virtual networks

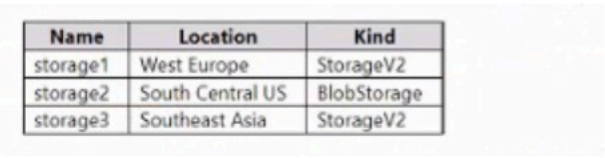
You have an Azure subscription that contains the virtual networks shown in the following table.

Name	Location
VNet1	West Europe
VNet2	Southeast Asia
VNet3	South Central US

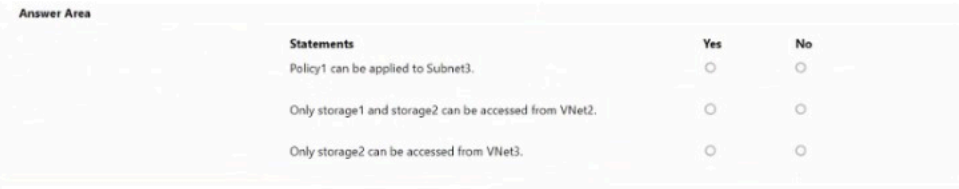
Name	Location
VNet1	West Europe
VNet2	Southeast Asia
VNet3	South Central US



Name	Virtual network	Service endpoint
Subnet1	VNet1	None
Subnet2	VNet2	Microsoft.Storage
Subnet3	VNet3	Microsoft.Storage
Subnet4	VNet3	None



Name	Location	Kind
storage1	West Europe	StorageV2
storage2	South Central US	BlobStorage
storage3	Southeast Asia	StorageV2



The subscription contains the subnets shown in the following table.

Name	Virtual network	Service endpoint
Subnet1	VNet1	None
Subnet2	VNet2	Microsoft.Storage
Subnet3	VNet3	Microsoft.Storage
Subnet4	VNet3	None

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

Name	Location	Kind
storage1	West Europe	StorageV2

storage2	South Central US	BlobStorage
storage3	Southeast Asia	StorageV2

You create a service endpoint policy named policy1 in the South Central US Azure region to allow connectivity to all the storage accounts in the subscription.

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

NOTE: Each correct selection is worth one point.

Statement	Yes	No
Policy1 can be applied to Subnet3.	☐	☐
Only storage1 and storage2 can be accessed from VNet2.	☐	☐
Only storage2 can be accessed from VNet3.	☐	☐

Answer

- Policy1 can be applied to Subnet3. **Yes**
- Only storage1 and storage2 can be accessed from VNet2. **No**
- Only storage2 can be accessed from VNet3. **No**

Explanation

Policy1 is in South Central US, so it can be associated with Subnet3 in VNet3, which is also in South Central US and has the Microsoft.Storage service endpoint enabled. Service endpoint policies are associated with subnets and can specify which storage accounts the subnet may access; this policy allows all three accounts, not just accounts in the subnet's region. VNet2 is in another region, so policy1 cannot be applied there, and its enabled storage endpoint does not restrict access to only storage1 and storage2.

https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoint-policies
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoint-policies-overview
https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security-virtual-networks

✓ **Statement 1** Policy1 can be applied to Subnet3.
Policy1 and VNet3 are both in South Central US, and Subnet3 has the Microsoft.Storage service endpoint required for a storage service endpoint policy. Therefore, policy1 can be applied to Subnet3.

https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoint-policies
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoint-policies-overview

✗ **Statement 2** Only storage1 and storage2 can be accessed from VNet2.
VNet2 is in Southeast Asia, so policy1, which is in South Central US, cannot be applied to its subnet. Subnet2 has the Microsoft.Storage service endpoint, and the statement is false because that endpoint does not limit access to only storage1 and storage2; storage3 is not excluded just because it is in Southeast Asia.

https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoint-policies
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoint-policies-overview
https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security-virtual-networks

✗ **Statement 3** Only storage2 can be accessed from VNet3.
Subnet3 in VNet3 has the Microsoft.Storage service endpoint and can use policy1, which is configured to allow connectivity to all the subscription's storage accounts. Because the policy is not limited to accounts in South Central US, access is not limited to storage2.

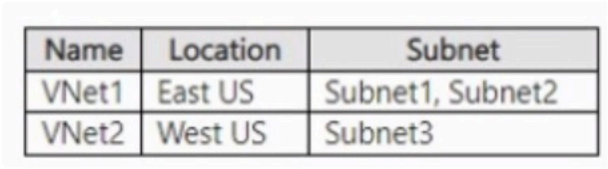
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoint-policies
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoint-policies-overview

Question 64

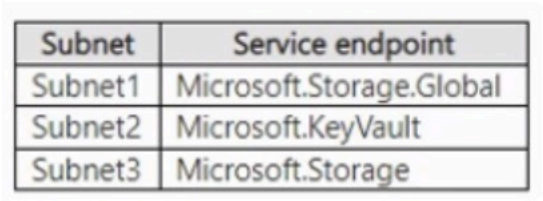
Yes / No · Domain: D4 Implement and manage virtual networking › Configure secure access to virtual networks

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

Name	Location	Subnet
VNet1	East US	Subnet1, Subnet2
VNet2	West US	Subnet3

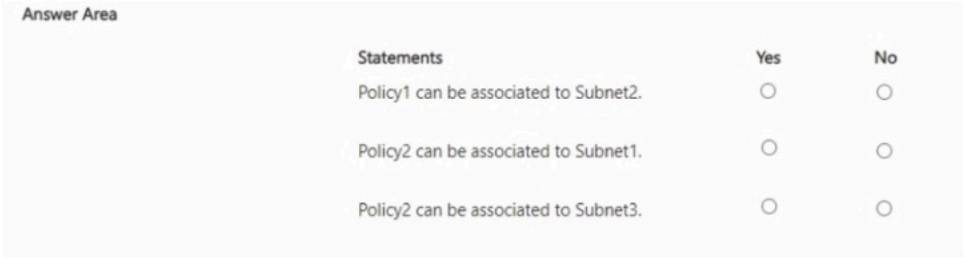


Name	Location	Subnet
VNet1	East US	Subnet1, Subnet2
VNet2	West US	Subnet3



Subnet	Service endpoint
Subnet1	Microsoft.Storage.Global
Subnet2	Microsoft.KeyVault
Subnet3	Microsoft.Storage

Name	Location
Policy1	East US
Policy2	West US



Answer Area

Statements	Yes	No
Policy1 can be associated to Subnet2.	○	○
Policy2 can be associated to Subnet1.	○	○
Policy2 can be associated to Subnet3.	○	○

You add a service endpoint to each subnet as shown in the following table.

Subnet	Service endpoint
Subnet1	Microsoft.Storage.Global
Subnet2	Microsoft.KeyVault
Subnet3	Microsoft.Storage

You create the service endpoint policies shown in the following table.

Name	Location
Policy1	East US
Policy2	West US

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

Statement	Yes	No
Policy1 can be associated to Subnet2.	☐	☐
Policy2 can be associated to Subnet1.	☐	☐
Policy2 can be associated to Subnet3.	☐	☐

Answer

- Policy1 can be associated to Subnet2. **No**
- Policy2 can be associated to Subnet1. **No**
- Policy2 can be associated to Subnet3. **Yes**

Explanation

A service endpoint policy can be associated only with a subnet in the same region, and service endpoint policies apply to Microsoft.Storage endpoints. Policy1 and Subnet2 are both in East US, but Subnet2 has a Microsoft.KeyVault endpoint, so that association is not valid. Policy2 is in West US, so it cannot be associated with Subnet1 in East US; it can be associated with Subnet3 in West US, which has a Microsoft.Storage endpoint.

https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoint-policies

✗ **Statement 1** Policy1 can be associated to Subnet2.
Although Policy1 and Subnet2 are both in East US, Subnet2 has a Microsoft.KeyVault service endpoint. Service endpoint policies apply to Microsoft.Storage endpoints, so this association is not valid.

https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoint-policies
https://learn.microsoft.com/en-us/azure/key-vault/general/overview-vnet-service-endpoints

✗ **Statement 2** Policy2 can be associated to Subnet1.
Policy2 is in West US, while Subnet1 is in the East US VNet. A service endpoint policy must be in the same region as the subnet with which it is associated, so this association is not valid.

https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoint-policies

✓ **Statement 3** Policy2 can be associated to Subnet3.
Policy2 and Subnet3 are both in West US, and Subnet3 has a Microsoft.Storage service endpoint. The region and endpoint requirements for associating the policy are met.

https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoint-policies

Dumpsgate

Question 65

Yes / No · Domain: D4 Implement and manage virtual networking › Configure secure access to virtual networks

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

Name	Operating system	Connects to
VM1	Windows Server 2019	Subnet1
VM2	Windows Server 2019	Subnet2

Name	Operating system	Connects to
VM1	Windows Server 2019	Subnet1
VM2	Windows Server 2019	Subnet2

VM1 and VM2 use public IP addresses. From Windows Server 2019 on VM1 and VM2, you allow inbound Remote Desktop connections.

Subnet1 and Subnet2 are in a virtual network named VNET1.

The subscription contains two network security groups (NSGs) named NSG1 and NSG2. NSG1 uses only the default rules.

NSG2 uses the default rules and the following custom incoming rule;

- Priority: 100
- Name: Rule1
- Port: 3389
- Protocol: TCP
- Source: Any
- Destination: Any
- Action: Allow

NSG1 is associated to Subnet1. NSG2 is associated to the network interface of VM2.

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

NOTE: Each correct selection is worth one point.

Statement	Yes	No
From the internet, you can connect to VM1 by using Remote Desktop.	☐	☐
From the internet, you can connect to VM2 by using Remote Desktop.	☐	☐
From VM1, you can connect to VM2 by using Remote Desktop.	☐	☐

Answer

- From the internet, you can connect to VM1 by using Remote Desktop. **No**
- From the internet, you can connect to VM2 by using Remote Desktop. **Yes**
- From VM1, you can connect to VM2 by using Remote Desktop. **Yes**

Explanation

VM1 is protected by NSG1 on Subnet1, and NSG1 has only the default inbound rules, which deny unsolicited internet traffic. VM2 has an NSG rule that allows TCP port 3389 from any source, so inbound Remote Desktop traffic is allowed both from the internet and from VM1. NSG1's default rule allows traffic within the virtual network, so VM1 can initiate an RDP connection to VM2 as well.

https://learn.microsoft.com/azure/virtual-network/network-security-group-how-it-works
https://learn.microsoft.com/en-us/azure/virtual-machines/troubleshooting/troubleshoot-rdp-nsg-problem
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-nsg

✗ **Statement 1** From the internet, you can connect to VM1 by using Remote Desktop. — No
NSG1 is associated with Subnet1 and uses only the default rules. Its default inbound rules deny traffic from the internet, so VM1's public IP address and enabled Windows Remote Desktop do not make the connection possible through the NSG.

https://learn.microsoft.com/azure/virtual-network/network-security-group-how-it-works
https://learn.microsoft.com/en-us/azure/virtual-machines/troubleshooting/troubleshoot-rdp-nsg-problem
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-nsg

✓ **Statement 2** From the internet, you can connect to VM2 by using Remote Desktop. — Yes
NSG2 is associated with VM2's network interface and has a priority 100 inbound rule allowing TCP port 3389 from any source to any destination. That rule allows internet-originated RDP traffic before the lower-priority default inbound deny rule is evaluated.

https://learn.microsoft.com/azure/virtual-network/network-security-group-how-it-works
https://learn.microsoft.com/en-us/azure/virtual-machines/troubleshooting/troubleshoot-rdp-nsg-problem
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-nsg

✓ **Statement 3** From VM1, you can connect to VM2 by using Remote Desktop. — Yes
VM1's outbound connection to VM2 is allowed by the default virtual-network outbound rule on NSG1. At VM2, NSG2's custom rule allows inbound TCP port 3389 from any source, including VM1, so the RDP connection is permitted.

https://learn.microsoft.com/azure/virtual-network/network-security-group-how-it-works
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-nsg

Free demo · full exam: 507 questions

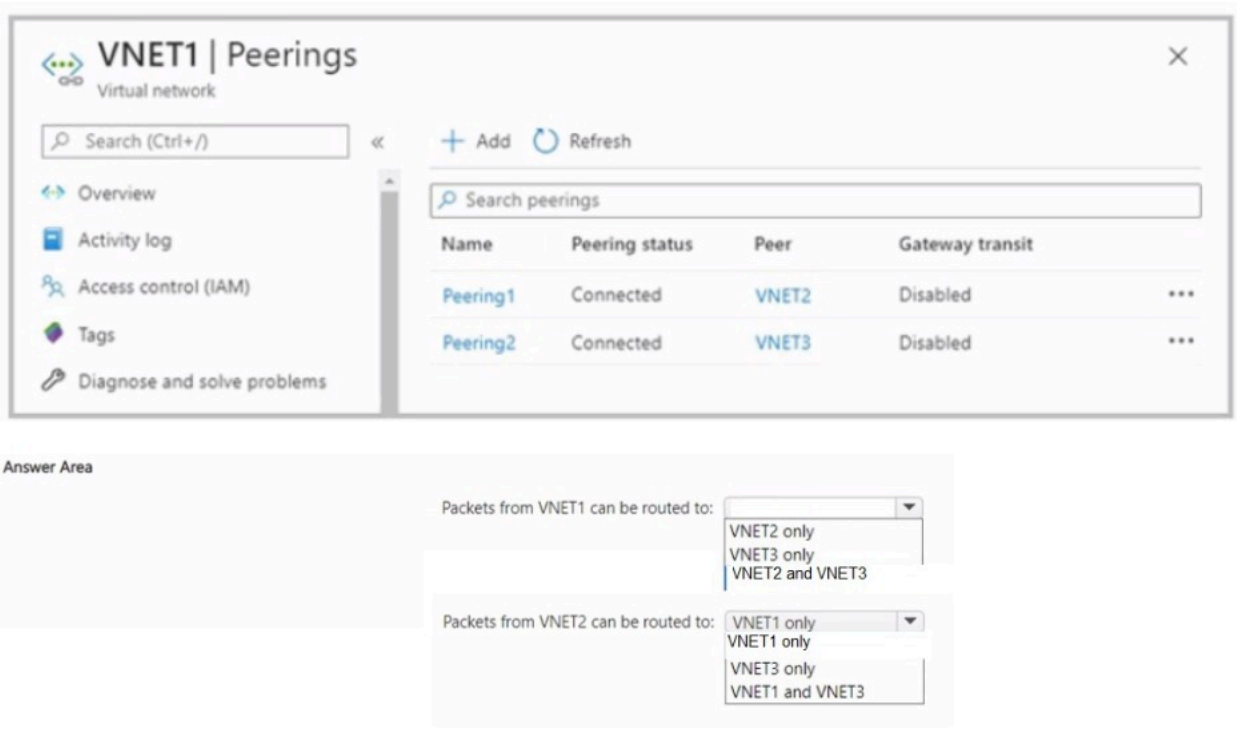
Question 66

Hotspot (dropdowns) · Domain: D4 Implement and manage virtual networking › Configure and manage virtual networks in Azure

You have an Azure subscription that contains three virtual networks named VNET1, VNET2, and VNET3.

Peering for VNET1 is configured as shown in the following exhibit.

Name	Peering status	Peer	Gateway transit
Peering1	Connected	VNET2	Disabled
Peering2	Connected	VNET3	Disabled



Packets from VNET1 can be routed to: VNET2 only | VNET3 only | VNET2 and VNET3

Packets from VNET2 can be routed to: VNET1 only | VNET3 only | VNET1 and VNET3

Answer

- Packets from VNET1 can be routed to: **VNET2 and VNET3**
- Packets from VNET2 can be routed to: **VNET1 only**

Explanation

VNET1 has connected, direct peerings with both VNET2 and VNET3, so it can route packets to each of them. VNET peering is not transitive: VNET2 cannot use its peering with VNET1 to reach VNET3, because VNET2 has no direct peering with VNET3. Therefore, packets from VNET2 can be routed to VNET1 only. [1]

https://learn.microsoft.com/azure/virtual-network/virtual-network-peering-overview

✗ **Box 1: VNET2 only** Packets from VNET1 can be routed to VNET2 only
VNET1 has a connected peering with VNET2, but it also has a connected peering with VNET3. Packets from VNET1 can therefore be routed to both peers, not just VNET2. [1]

https://learn.microsoft.com/azure/virtual-network/virtual-network-peering-overview

✗ **Box 1: VNET3 only** Packets from VNET1 can be routed to VNET3 only
VNET1 has a connected peering with VNET3, but it also has a connected peering with VNET2. Packets from VNET1 can therefore be routed to both peers, not just VNET3. [1]

https://learn.microsoft.com/azure/virtual-network/virtual-network-peering-overview

✓ **Box 1: VNET2 and VNET3** Packets from VNET1 can be routed to VNET2 and VNET3
The exhibit shows connected peerings from VNET1 to both VNET2 and VNET3. Each is a direct peering, so VNET1 can route packets to both networks. [1]

https://learn.microsoft.com/azure/virtual-network/virtual-network-peering-overview

✓ **Box 2: VNET1 only** Packets from VNET2 can be routed to VNET1 only
VNET2 is directly peered with VNET1. The peering from VNET1 to VNET3 does not give VNET2 a transitive route to VNET3, so VNET1 is the only listed destination VNET2 can reach. [1]

https://learn.microsoft.com/azure/virtual-network/virtual-network-peering-overview

✗ **Box 2: VNET3 only** Packets from VNET2 can be routed to VNET3 only
VNET2 has a direct peering with VNET1, not with VNET3. VNET2 cannot route through VNET1 to VNET3 because VNET peering does not provide transitive routing. [1]

https://learn.microsoft.com/azure/virtual-network/virtual-network-peering-overview

✗ **Box 2: VNET1 and VNET3** Packets from VNET2 can be routed to VNET1 and VNET3
VNET2 can reach VNET1 through their direct peering, but VNET1's separate peering with VNET3 does not make VNET3 reachable from VNET2. VNET peering is not transitive. [1]

https://learn.microsoft.com/azure/virtual-network/virtual-network-peering-overview

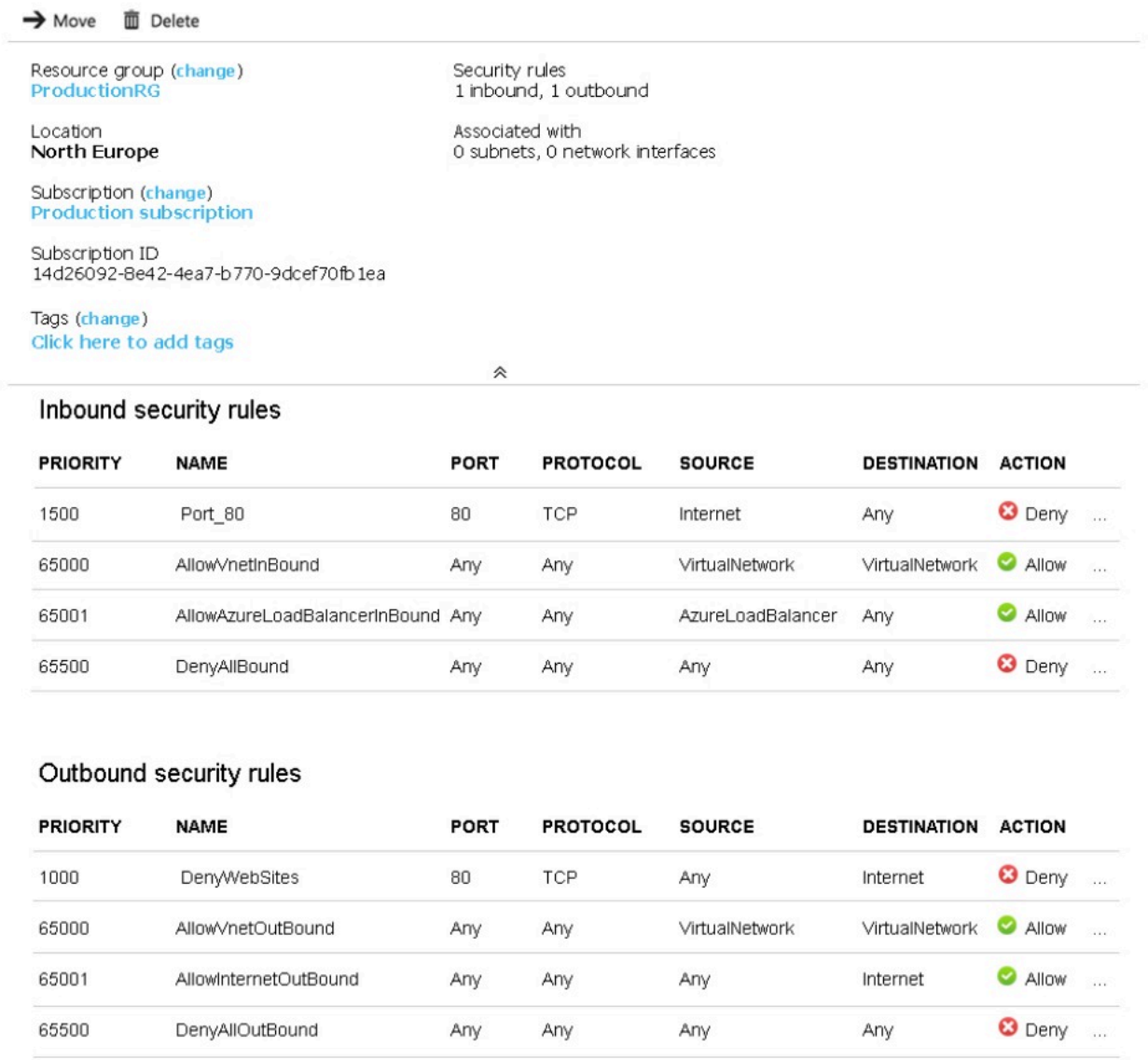
Question 67

Single choice · Domain: D4 Implement and manage virtual networking › Configure secure access to virtual networks

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

Free demo · full exam: 507 questions

Name	Type	Details
VNet1	Virtual network	*Not applicable*
Subnet1	Subnet	Hosted on VNet1
VM1	Virtual machine	On Subnet1
VM2	Virtual machine	On Subnet1



VM1 and VM2 are deployed from the same template and host line-of-business applications accessed by using Remote Desktop. You configure the network security group (NSG) shown in the exhibit. (Click the Exhibit button.) You need to prevent users of VM1 and VM2 from accessing websites on the Internet.

What should you do?

A. Associate the NSG to Subnet1.
B. Disassociate the NSG from a network interface.
C. Change the DenyWebSites outbound security rule.
D. Change the Port_80 inbound security rule

Answer: A. Associate the NSG to Subnet1.

Explanation

The exhibit shows that the NSG has no subnet or network-interface associations, so its outbound DenyWebSites rule is not currently applied to VM1 or VM2. Associate the NSG with Subnet1 to apply its outbound rules to both VMs, which share that subnet. The existing outbound rule denies TCP traffic on port 80 to the Internet; the inbound Port_80 rule does not control users' outbound website access.

https://learn.microsoft.com/azure/virtual-network/network-security-group-how-it-works
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-nsq

✓ **A** Associate the NSG to Subnet1.
The exhibit reports that the NSG is associated with 0 subnets and 0 network interfaces, so its rules are not applied to either VM. Associating it with Subnet1 applies the NSG's outbound rules to traffic from both VM1 and VM2, including the existing DenyWebSites rule.

https://learn.microsoft.com/azure/virtual-network/network-security-group-how-it-works
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-nsq

✗ **B** Disassociate the NSG from a network interface.
The exhibit shows that the NSG is associated with 0 network interfaces, so there is no network-interface association to remove. Disassociating it would not apply its outbound deny rule to the VMs.

https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface
https://learn.microsoft.com/azure/virtual-network/network-security-group-how-it-works

✗ **C** Change the DenyWebSites outbound security rule.
The NSG already has an outbound DenyWebSites rule for TCP port 80 to the Internet. The problem is that the NSG has no associations, so changing the rule alone would not make it apply to VM1 or VM2; associate the NSG with Subnet1 instead.

https://learn.microsoft.com/azure/virtual-network/network-security-group-how-it-works
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-nsq

✗ **D** Change the Port_80 inbound security rule
Port_80 is an inbound rule, while the requirement is to prevent the VMs from initiating access to Internet websites. The outbound DenyWebSites rule is the relevant rule, and the NSG must be associated with Subnet1 for its rules to apply.

https://learn.microsoft.com/azure/virtual-network/network-security-group-how-it-works
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-nsq

Free demo · full exam: 507 questions

Question 68

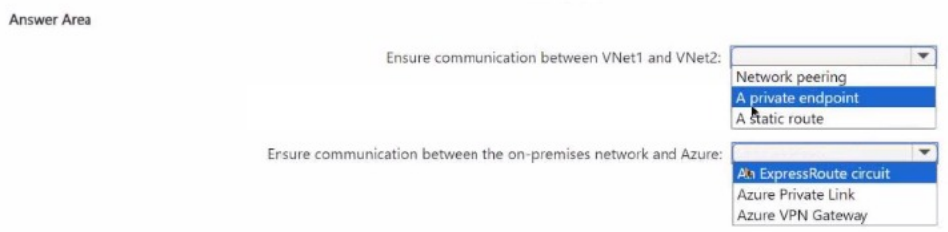
Hotspot (dropdowns) · Domain: D4 Implement and manage virtual networking › Configure and manage virtual networks in Azure

You have an on-premises network.

You have an Azure subscription that contains two virtual networks named VNet1 and VNet2. VNet1 uses an IP address space of 192.168.8.0/24. VNet2 uses an IP address space of 192.168.9.0/24.

You need to configure the virtual networks. The solution must meet the following requirements:

- Ensure that the resources on VNet1 can communicate with the resources on VNet2.
- Ensure that the resources on the on-premises network can communicate with Azure resources.
- Minimize costs.



Ensure communication between VNet1 and VNet2: Network peering | A private endpoint | A static route

Ensure communication between the on-premises network and Azure: An ExpressRoute circuit | Azure Private Link | Azure VPN Gateway

Answer

- Ensure communication between VNet1 and VNet2: **Network peering**
- Ensure communication between the on-premises network and Azure: **Azure VPN Gateway**

Explanation

Use network peering to connect VNet1 and VNet2, whose address spaces do not overlap, and enable communication between their resources over Azure networking. Use an Azure VPN Gateway for communication between the on-premises network and Azure; it provides site-to-site connectivity while avoiding the higher cost of ExpressRoute. These choices meet both connectivity requirements while minimizing costs. [1][3][8]

https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways
https://learn.microsoft.com/azure/virtual-network/virtual-network-peering-overview
https://learn.microsoft.com/en-us/azure/expressroute/plan-manage-cost

✓ **Box 1: Network peering** Network peering
VNet peering connects VNet1 and VNet2 so resources in each can communicate over Azure's network. Their address spaces (192.168.8.0/24 and 192.168.9.0/24) do not overlap, making peering suitable. [2][3]

https://learn.microsoft.com/en-us/azure/virtual-network/tutorial-connect-virtual-networks?tabs=portal
https://learn.microsoft.com/azure/virtual-network/virtual-network-peering-overview

✗ **Box 1: A private endpoint** A private endpoint
A private endpoint provides private access to a specific Azure service or resource; it does not connect the two virtual networks for general resource-to-resource communication. [11]

https://learn.microsoft.com/en-us/azure/private-link/private-endpoint-overview/

Free demo · full exam: 507 questions

✗ **Box 1: A static route** A static route
A static route can direct traffic along a path, but it does not itself establish the VNet-to-VNet connection required here. VNet peering is the direct choice for enabling communication between these networks. [3]

https://learn.microsoft.com/azure/virtual-network/virtual-network-peering-overview

✗ **Box 2: An ExpressRoute circuit** An ExpressRoute circuit
ExpressRoute can provide private connectivity between the on-premises network and Azure, but it is not the cost-minimizing option for this scenario. The question requires minimizing costs, and a site-to-site VPN is the appropriate lower-cost choice. [8][9]

https://learn.microsoft.com/en-us/azure/expressroute/plan-manage-cost
https://learn.microsoft.com/en-us/azure/networking/design-guide/hybrid-connectivity

✗ **Box 2: Azure Private Link** Azure Private Link
Azure Private Link gives private access to specific services, not general connectivity from the on-premises network to Azure resources. It does not meet the scenario's network-wide communication requirement. [11]

https://learn.microsoft.com/en-us/azure/private-link/private-endpoint-overview/

✓ **Box 2: Azure VPN Gateway** Azure VPN Gateway
An Azure VPN Gateway supports a site-to-site VPN connection between the on-premises network and an Azure virtual network. It provides the required hybrid connectivity without the higher cost associated with ExpressRoute. [1][8][9]

https://learn.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways
https://learn.microsoft.com/en-us/azure/expressroute/plan-manage-cost
https://learn.microsoft.com/en-us/azure/networking/design-guide/hybrid-connectivity

Question 69

Hotspot (dropdowns) · Domain: D4 Implement and manage virtual networking › Configure name resolution and load balancing

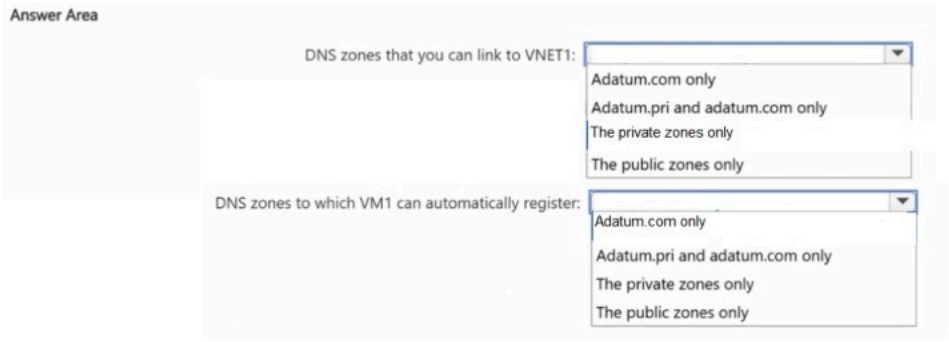
You have an Azure virtual machine that runs Windows Server and has the following configurations:

- Name:VM1
- Region: West US
- Connected to: VNET1
- Private IP address: 10.1.0.4
- Public IP address: 52.186.85.63
- DNS suffix in Windows Server Adatum.com

You create the Azure DNS zones shown in the following table.

Name	Type	Region
Adatum.pri	Private	West Europe
Contoso.pri	Private	Central US
Adatum.com	Public	West Europe
Contoso.com	Public	North Europe

Name	Type	Region
Adatum.pri	Private	West Europe
Contoso.pri	Private	Central US
Adatum.com	Public	West Europe
Contoso.com	Public	North Europe



You need to identify which DNS zones you can link to VNET1 and the DNS zones to which VM1 can automatically register.

Which zones should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

DNS zones that you can link to VNET1: Adatum.com only | Adatum.pri and adatum.com only | The private zones only | The public zones only

DNS zones to which VM1 can automatically register: Adatum.com only | Adatum.pri and adatum.com only | The private zones only | The public zones only

Answer

- DNS zones that you can link to VNET1: **The private zones only**
- DNS zones to which VM1 can automatically register: **The private zones only**

Explanation

Azure virtual network links are supported for private DNS zones, not public DNS zones, so VNET1 can be linked to the private zones regardless of their listed regions. VM automatic DNS registration is also a private DNS zone feature; public zones such as Adatum.com and Contoso.com are not eligible. Therefore, select “The private zones only” for both questions. [1][2][4]

https://learn.microsoft.com/en-us/azure/dns/private-dns-autoregistration
https://learn.microsoft.com/en-us/azure/dns/private-dns-overview/
https://learn.microsoft.com/en-us/azure/dns/private-dns-virtual-network-links

✗ **Box 1: Adatum.com only** Adatum.com only

Adatum.com is a public DNS zone, and public zones cannot be linked to VNET1 as Azure private DNS zones can. The listed private zones are the ones that can be linked.

https://learn.microsoft.com/en-us/azure/dns/private-dns-overview/
https://learn.microsoft.com/en-us/azure/dns/private-dns-virtual-network-links

✗ **Box 1: Adatum.pri and adatum.com only** Adatum.pri and adatum.com only

This includes Adatum.com, a public zone that cannot be linked to VNET1. It also leaves out Contoso.pri, which is a private zone and can be linked.

https://learn.microsoft.com/en-us/azure/dns/private-dns-overview/
https://learn.microsoft.com/en-us/azure/dns/private-dns-virtual-network-links

✓ **Box 1: The private zones only** The private zones only
Azure virtual network links are used with private DNS zones, so both Adatum.pri and Contoso.pri are eligible to link to VNET1. Their listed regions do not prevent the links; public zones are not linkable to a virtual network in this way.

https://learn.microsoft.com/en-us/azure/dns/private-dns-overview/
https://learn.microsoft.com/en-us/azure/dns/private-dns-virtual-network-links

✗ **Box 1: The public zones only** The public zones only
Public DNS zones are not linked to virtual networks using private DNS zone virtual network links. VNET1 can instead be linked to the private zones.

https://learn.microsoft.com/en-us/azure/dns/private-dns-overview/
https://learn.microsoft.com/en-us/azure/dns/private-dns-virtual-network-links

✗ **Box 2: Adatum.com only** Adatum.com only
Adatum.com is public, and Azure automatic registration of virtual machine records is a feature of private DNS zones, not public zones. The Windows DNS suffix shown does not make this public zone eligible for Azure private DNS auto-registration.

https://learn.microsoft.com/en-us/azure/dns/private-dns-autoregistration
https://learn.microsoft.com/en-us/azure/dns/private-dns-overview/

✗ **Box 2: Adatum.pri and adatum.com only** Adatum.pri and adatum.com only
Adatum.pri is private, but Adatum.com is public and is not eligible for Azure private DNS automatic registration. The correct category is private zones only, not this mix of private and public zones.

https://learn.microsoft.com/en-us/azure/dns/private-dns-autoregistration
https://learn.microsoft.com/en-us/azure/dns/private-dns-overview/

✓ **Box 2: The private zones only** The private zones only
Automatic registration of virtual machine records is available for private DNS zones when the applicable virtual network link is configured for registration. Public zones do not provide this private-zone registration feature.

https://learn.microsoft.com/en-us/azure/dns/private-dns-autoregistration
https://learn.microsoft.com/en-us/azure/dns/private-dns-overview/

✗ **Box 2: The public zones only** The public zones only
Azure virtual machine automatic registration is a private DNS zone feature, so neither public zone is eligible. The VM's public IP address does not change that distinction.

https://learn.microsoft.com/en-us/azure/dns/private-dns-autoregistration
https://learn.microsoft.com/en-us/azure/dns/private-dns-overview/

Question 70

Multiple choice · Domain: D5 Monitor and maintain Azure resources › Implement backup and recovery

You manage several virtual machines in Azure and need to implement a backup strategy. Your organization requires a Recovery Time Objective (RTO) of 2 hours and a Recovery Point Objective (RPO) of 1 hour. Current compliance policy mandates that backups must be retained for 7 years. You are evaluating Azure Backup and Azure Site Recovery as potential solutions.

Which of the following statements are true regarding these services and their suitability for this scenario? (Select all that apply.)

A. Azure Backup can meet the RPO requirement of 1 hour through scheduled daily backups, though meeting 7-year retention requires archival tier storage and extended retention settings.

B. Azure Site Recovery provides continuous replication with an RPO measured in minutes, which exceeds the 1-hour RPO requirement, and can help meet the 2-hour RTO through failover automation.

C. Azure Backup with hourly backup frequency and long-term retention policies can meet both the 1-hour RPO and 7-year retention requirements, though RPO depends on backup frequency configuration.

D. A combination of Azure Site Recovery for the RTO/RPO requirements and Azure Backup for the 7-year retention requirement would provide a comprehensive solution meeting all stated objectives.

Answer

- B. **Azure Site Recovery provides continuous replication with an RPO measured in minutes, which exceeds the 1-hour RPO requirement, and can help meet the 2-hour RTO through failover automation.**
- D. **A combination of Azure Site Recovery for the RTO/RPO requirements and Azure Backup for the 7-year retention requirement would provide a comprehensive solution meeting all stated objectives.**

Explanation

Azure Site Recovery is the appropriate service for the 1-hour RPO and 2-hour RTO because replication can provide recovery points measured in minutes, and failover plans can automate recovery steps. Azure Backup complements it by providing backup retention for long-term compliance, including a 7-year retention requirement. Daily backups alone do not meet a 1-hour RPO, and Azure VM Backup policies do not provide hourly recovery points at one-hour intervals.

https://learn.microsoft.com/en-us/azure/reliability/reliability-site-recovery
https://learn.microsoft.com/en-us/azure/site-recovery/site-recovery-overview
https://learn.microsoft.com/azure/backup/backup-azure-vm-backup-faq
https://learn.microsoft.com/en-us/azure/site-recovery/site-recovery-create-recovery-plans

✗ **A** Azure Backup can meet the RPO requirement of 1 hour through scheduled daily backups, though meeting 7-year retention requires archival tier storage and extended retention settings.
Daily backups can leave nearly a day between recovery points, so they cannot meet the 1-hour RPO. Long-term retention settings may address retention, but they do not fix that recovery-point gap.

https://learn.microsoft.com/azure/backup/backup-azure-vm-backup-faq

✓ **B** Azure Site Recovery provides continuous replication with an RPO measured in minutes, which exceeds the 1-hour RPO requirement, and can help meet the 2-hour RTO through failover automation.
Site Recovery replicates workloads and supports recovery points with an RPO measured in minutes, which is within the 1-hour limit. Recovery plans and failover automation can help achieve the 2-hour RTO,

Free demo · full exam: 507 questions

although actual recovery time depends on the environment and configuration.

https://learn.microsoft.com/en-us/azure/reliability/reliability-site-recovery
https://learn.microsoft.com/en-us/azure/site-recovery/site-recovery-overview
https://learn.microsoft.com/en-us/azure/site-recovery/site-recovery-create-recovery-plans

✗ **C** Azure Backup with hourly backup frequency and long-term retention policies can meet both the 1-hour RPO and 7-year retention requirements, though RPO depends on backup frequency configuration. Azure VM Backup policies do not offer backups at one-hour intervals; enhanced policies support intervals of several hours, while standard policies are daily. Long-term retention may support the retention objective, but backup frequency therefore cannot satisfy the stated 1-hour RPO.

https://learn.microsoft.com/en-us/azure/backup/backup-support-matrix-iaas
https://learn.microsoft.com/azure/backup/backup-azure-vm-backup-faq

✓ **D** A combination of Azure Site Recovery for the RTO/RPO requirements and Azure Backup for the 7-year retention requirement would provide a comprehensive solution meeting all stated objectives.
This approach assigns each requirement to the service suited to it: Site Recovery provides replication and failover capabilities for the RTO and RPO, while Azure Backup supplies long-term backup retention. Together they address the recovery objectives and the 7-year compliance requirement.

https://learn.microsoft.com/en-us/azure/reliability/reliability-site-recovery
https://learn.microsoft.com/en-us/azure/site-recovery/site-recovery-overview
https://learn.microsoft.com/azure/backup/backup-azure-vm-backup-faq
https://learn.microsoft.com/en-us/azure/site-recovery/site-recovery-create-recovery-plans

Dumpsgate

Question 71

Single choice · Domain: D5 Monitor and maintain Azure resources › Implement backup and recovery

Your organization requires that all virtual machine backups be retained for a minimum of 30 days and that you be able to restore an entire VM to a different Azure region in the event of a disaster. Which backup and recovery solution should you implement?

A. Azure Backup with Recovery Services vault configured for geo-redundant backup, cross-region restore enabled, and retention set to 30 days minimum
B. Azure Site Recovery replication to a secondary region with daily snapshots retained for 30 days
C. Managed disk snapshots stored in the same region with a 30-day lifecycle policy
D. Azure Backup with locally redundant storage and daily backup scheduling
E. Azure Storage Account copies to another region with blob versioning enabled

Answer: A. Azure Backup with Recovery Services vault configured for geo-redundant backup, cross-region restore enabled, and retention set to 30 days minimum

Explanation

Option A meets both requirements: Azure Backup can protect the VM with a Recovery Services vault, and its backup policy can retain recovery points for at least 30 days. With geo-redundant storage and cross-region restore enabled, you can restore the VM in a secondary Azure region if the primary region is unavailable. This combines backup retention with the requested regional recovery capability. [1][4][8]

https://learn.microsoft.com/en-us/azure/backup/backup-azure-backup-faq
https://learn.microsoft.com/en-us/azure/backup/backup-azure-recovery-services-vault-overview
https://learn.microsoft.com/en-us/azure/backup/about-azure-vm-restore

✓ **A** Azure Backup with Recovery Services vault configured for geo-redundant backup, cross-region

Free demo · full exam: 507 questions

restore enabled, and retention set to 30 days minimum
This option directly addresses both requirements: the backup policy can retain recovery points for at least 30 days, and cross-region restore lets you restore the VM in another Azure region. Geo-redundant backup supports storing backup data redundantly across regions. [1][4][8]

https://learn.microsoft.com/en-us/azure/backup/backup-azure-backup-faq
https://learn.microsoft.com/en-us/azure/backup/backup-azure-recovery-services-vault-overview
https://learn.microsoft.com/en-us/azure/backup/about-azure-vm-restore

✗ **B** Azure Site Recovery replication to a secondary region with daily snapshots retained for 30 days
Site Recovery is intended for replication and disaster recovery, rather than providing the Azure Backup retention solution requested here. The scenario specifically requires VM backups retained for at least 30 days, so Azure Backup with an appropriate retention policy is the better fit.

✗ **C** Managed disk snapshots stored in the same region with a 30-day lifecycle policy
The snapshots are stored in the same region, so a disaster affecting that region could make them unavailable. This does not meet the requirement to restore the VM to a different Azure region.

✗ **D** Azure Backup with locally redundant storage and daily backup scheduling
Daily backups alone do not ensure that recovery points are retained for at least 30 days; the policy must specify that retention. More importantly, locally redundant storage does not provide the geo-redundant backup and cross-region restore configuration required for regional disaster recovery. [1][4]

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

✗ **E** Azure Storage Account copies to another region with blob versioning enabled
Blob copies and versioning are not the Azure VM backup and restore solution described in the scenario. They do not by themselves provide Azure Backup recovery points with the required retention policy and a supported full-VM cross-region restore workflow.

Question 72

Single choice · Domain: D5 Monitor and maintain Azure resources › Monitor resources in Azure

You have deployed a web application on Azure App Service across three instances. Application logs show intermittent failures and slow response times during peak hours. You need to identify whether the issue is with a specific App Service instance, a backend resource, or the application code itself. Which combination of monitoring solutions should you implement?

A. Application Insights to track application performance and dependencies, plus App Service diagnostics logs to monitor instance-level health
B. Azure Monitor alerts configured to send email notifications whenever CPU usage exceeds 80 percent
C. Azure Resource Health to check the status of all App Service instances and Azure Service Health for platform events
D. Log Analytics workspace with queries for VM performance metrics only
E. Azure Advisor recommendations and Application Insights sampling at 10 percent

Answer: A. Application Insights to track application performance and dependencies, plus App Service diagnostics logs to monitor instance-level health

Explanation

Free demo · full exam: 507 questions

Application Insights can help identify application-code performance issues and slow or failing backend dependencies, while App Service diagnostics provide logs and instance-level information. Together, these tools best match the need to distinguish an affected App Service instance from a backend resource or the application itself. CPU alerts, platform health checks, VM-only queries, and Advisor recommendations do not provide this combination of diagnostic detail.

https://learn.microsoft.com/azure/app-service/overview-diagnostics
https://learn.microsoft.com/en-us/azure/app-service/troubleshoot-diagnostic-logs
https://learn.microsoft.com/en-us/azure/app-service/monitor-app-service
https://learn.microsoft.com/en-us/azure/azure-monitor/app/dependencies

✓ **A** Application Insights to track application performance and dependencies, plus App Service diagnostics logs to monitor instance-level health
Application Insights helps analyze application performance and dependency calls, which can reveal whether slow responses or failures originate in the code or a backend. App Service diagnostics add platform and instance-level diagnostic information, helping investigate whether a particular App Service instance is involved.

https://learn.microsoft.com/azure/app-service/overview-diagnostics
https://learn.microsoft.com/en-us/azure/app-service/troubleshoot-diagnostic-logs
https://learn.microsoft.com/en-us/azure/app-service/monitor-app-service
https://learn.microsoft.com/en-us/azure/azure-monitor/app/dependencies

✗ **B** Azure Monitor alerts configured to send email notifications whenever CPU usage exceeds 80 percent
A CPU threshold alert can notify you about one possible symptom, but it does not explain whether the cause is an individual instance, a backend dependency, or application code. It is therefore too narrow for the required investigation.

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

✗ **C** Azure Resource Health to check the status of all App Service instances and Azure Service Health for platform events
Service Health is useful for Azure platform incidents, but platform status checks alone do not diagnose application performance or dependency failures. This combination would not provide the application-level and instance diagnostic detail needed for the intermittent failures.

https://learn.microsoft.com/en-us/azure/service-health/

✗ **D** Log Analytics workspace with queries for VM performance metrics only
Queries limited to VM performance metrics do not cover the application's code execution or backend dependencies. They also do not fit the stated need to diagnose an App Service workload using application and App Service diagnostics.

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

✗ **E** Azure Advisor recommendations and Application Insights sampling at 10 percent
Advisor provides recommendations rather than the targeted, ongoing diagnostics needed to locate intermittent failures across instances, application code, and dependencies. Sampling only 10 percent can also leave less telemetry available for investigating intermittent events.

https://learn.microsoft.com/en-us/azure/advisor/advisor-reference-reliability-recommendations
https://learn.microsoft.com/en-us/azure/app-service/monitor-app-service
https://learn.microsoft.com/en-us/azure/azure-monitor/app/dependencies

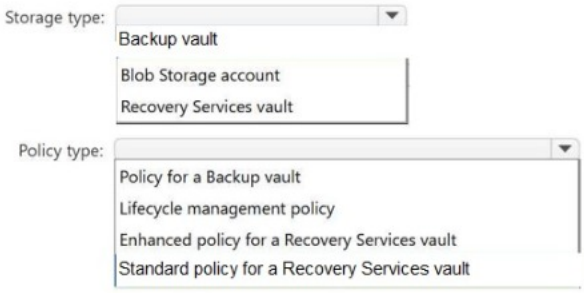
Question 73

Hotspot (dropdowns) · Domain: D5 Monitor and maintain Azure resources › Implement backup and recovery

You have an Azure subscription that contains a virtual machine named VM1. VM1 has Trusted Launch enabled. You need to recommend a backup solution for VM1. The solution must minimize administrative effort and costs. Which type of storage and which type of backup policy should you include in the recommendation? To answer, select

NOTE: Each correct selection is worth one point.

Answer Area



Storage type: Backup vault | Blob Storage account | Recovery Services vault

Policy type: Policy for a Backup vault | Lifecycle management policy | Enhanced policy for a Recovery Services vault | Standard policy for a Recovery Services vault

Answer

- Storage type: **Recovery Services vault**
- Policy type: **Enhanced policy for a Recovery Services vault**

Explanation

Choose a Recovery Services vault because it is the vault type used for Azure VM backup. VM1 has Trusted Launch enabled, so use the enhanced policy for a Recovery Services vault, which supports backing up Trusted Launch VMs. This uses Azure's VM backup service rather than requiring a separate Blob Storage configuration or lifecycle-management process. [1][2][4]

https://learn.microsoft.com/azure/backup/backup-azure-recovery-services-vault-overview
https://learn.microsoft.com/en-us/azure/backup/backup-support-matrix
https://learn.microsoft.com/en-us/azure/backup/backup-azure-vms-enhanced-policy?tabs=azure-portal&trk=article-ssr-frontend-pulse_little-text-block

✗ **Storage type: Backup vault** Backup vault
A Backup vault is used for other supported backup workloads, not the Azure VM backup choice required here. For VM1, use a Recovery Services vault and its VM backup policy options. [1][2]

https://learn.microsoft.com/azure/backup/backup-azure-recovery-services-vault-overview
https://learn.microsoft.com/en-us/azure/backup/backup-support-matrix

✗ **Storage type: Blob Storage account** Blob Storage account
A Blob Storage account is not the vault type to select for Azure VM backup. Using it would not provide the VM backup policy needed for this Trusted Launch VM. [1][3]

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

✓ **Storage type: Recovery Services vault** Recovery Services vault

Free demo · full exam: 507 questions

Recovery Services vaults support Azure VM backup. This is the appropriate storage type to pair with the VM backup policy for VM1. [1][2]

https://learn.microsoft.com/azure/backup/backup-azure-recovery-services-vault-overview
https://learn.microsoft.com/en-us/azure/backup/backup-support-matrix

✗ **Policy type: Policy for a Backup vault** Policy for a Backup vault
This policy belongs with a Backup vault, which is not the storage type for backing up this Azure VM. The VM backup selection should use a Recovery Services vault policy. [2]

https://learn.microsoft.com/en-us/azure/backup/backup-support-matrix

✗ **Policy type: Lifecycle management policy** Lifecycle management policy
A lifecycle management policy is for managing the lifecycle of blobs, not for configuring Azure VM backups. It would not provide the required backup policy for VM1. [5]

https://learn.microsoft.com/en-us/azure/backup/backup-overview?source=recommendations

✓ **Policy type: Enhanced policy for a Recovery Services vault** Enhanced policy for a Recovery Services vault
The enhanced Recovery Services vault policy supports backups of Trusted Launch VMs. It is therefore the compatible policy choice for VM1. [2][4]

https://learn.microsoft.com/en-us/azure/backup/backup-support-matrix
https://learn.microsoft.com/en-us/azure/backup/backup-azure-vms-enhanced-policy?tabs=azure-portal&trk=article-ssr-frontend-pulse_little-text-block

✗ **Policy type: Standard policy for a Recovery Services vault** Standard policy for a Recovery Services vault
The standard Recovery Services vault policy does not provide the required Trusted Launch VM backup support. Use the enhanced policy for this VM. [2][4]

https://learn.microsoft.com/en-us/azure/backup/backup-support-matrix
https://learn.microsoft.com/en-us/azure/backup/backup-azure-vms-enhanced-policy?tabs=azure-portal&trk=article-ssr-frontend-pulse_little-text-block

Question 74

Single choice · Domain: D5 Monitor and maintain Azure resources › Implement backup and recovery

You have two Azure virtual machines named VM1 and VM2. You have two Recovery Services vaults named RSV1 and RSV2.

VM2 is backed up to RSV1.

You need to back up VM2 to RSV2.

What should you do first?

A. From the VM2 blade, click Disaster recovery, click Replication settings, and then select RSV2 as the Recovery Services vault.

B. From the RSV1 blade, click Backup items and stop the VM2 backup.

C. From the RSV1 blade, click Backup Jobs and export the VM2 job.

D. From the RSV2 blade, click Backup. From the Backup blade, select the backup for the virtual machine, and then click Backup.

Answer: B. From the RSV1 blade, click Backup items and stop the VM2 backup.

Free demo · full exam: 507 questions

Dumpsgate

Question 75

Single choice · Domain: D5 Monitor and maintain Azure resources › Monitor resources in Azure

You have an Azure subscription. The subscription contains 10 virtual machines that run Windows Server.

Each virtual machine hosts a website in IIS and has the Azure Monitor Agent installed.

You need to collect the IIS logs from each virtual machine and store them in a Log Analytics workspace.

What should you configure first?

A. a data collection endpoint
B. VM insights
C. a private endpoint
D. Diagnostic settings
E. an Azure Monitor Private Link Scope (AMPLS)

Answer: A. a data collection endpoint

Explanation

Free demo · full exam: 507 questions

Configure a data collection endpoint (DCE) first. The Azure Monitor Agent uses data collection rules to collect and route IIS logs to the Log Analytics workspace, and a DCE provides the endpoint used for that collection path. VM insights and diagnostic settings do not configure collection of IIS logs from inside the Windows virtual machines.

https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/data-collection-endpoint-overview
https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-collection-rule-azure-monitor-agent?tabs=cli
https://learn.microsoft.com/en-us/azure/azure-monitor/vm/data-collection-iis
https://learn.microsoft.com/azure/azure-monitor/data-collection/data-collection-rule-structure

✓ **A** a data collection endpoint
A DCE provides an endpoint for Azure Monitor Agent data collection and is the required first configuration in this scenario. You can then configure a data collection rule to collect the IIS logs and send them to the Log Analytics workspace.

https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/data-collection-endpoint-overview
https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-collection-rule-azure-monitor-agent?tabs=cli
https://learn.microsoft.com/en-us/azure/azure-monitor/vm/data-collection-iis

✗ **B** VM insights
VM insights is used to monitor virtual-machine health and performance, not to define collection of IIS log files. IIS log collection requires configuring a data collection rule for the relevant log data.

https://learn.microsoft.com/en-us/azure/azure-monitor/vm/data-collection-iis
https://learn.microsoft.com/en-us/azure/azure-monitor/vm/monitor-virtual-machine-data-collection

✗ **C** a private endpoint
A private endpoint is used for private network connectivity to supported Azure services; it does not define which IIS logs the agent collects. The scenario does not specify a private connectivity requirement.

https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-network-configuration

✗ **D** Diagnostic settings
Diagnostic settings route Azure resource platform logs and metrics, rather than IIS logs generated inside the guest operating system. Use Azure Monitor Agent data collection configuration for the IIS logs.

https://learn.microsoft.com/en-us/azure/azure-monitor/agents/data-collection-rule-azure-monitor-agent?tabs=cli
https://learn.microsoft.com/en-us/azure/azure-monitor/vm/data-collection-iis

✗ **E** an Azure Monitor Private Link Scope (AMPLS)
An AMPLS is part of configuring private connectivity for Azure Monitor resources, not the configuration that specifies collection of IIS logs. No private-link requirement is stated in the scenario.

https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-network-configuration

Question 76

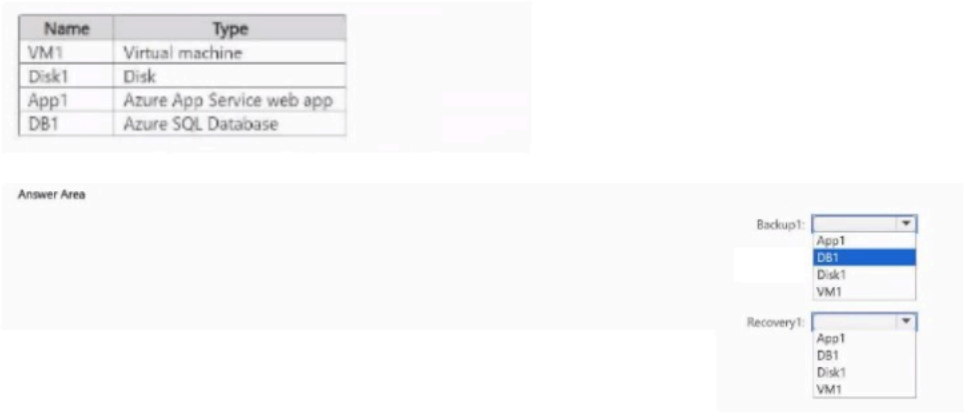
Hotspot (dropdowns) · Domain: D5 Monitor and maintain Azure resources › Implement backup and recovery

You have an Azure subscription that contains an Azure Backup vault named Backup1, a Recovery Services vault named Recovery1, and the resources shown in the following table.

Name	Type
VM1	Virtual machine
Disk1	Disk
App1	Azure App Service web app
DB1	Azure SQL Database

You plan to back up the resources.

Which resource can be backed up to Backup1, and which resource can be backed up to Recovery1? To answer, select the appropriate options in the answer area.



NOTE: Each correct selection is worth one point.

Backup1: App1 | DB1 | Disk1 | VM1
Recovery1: App1 | DB1 | Disk1 | VM1

Answer

- Backup1: **Disk1**
- Recovery1: **VM1**

Explanation

Backup1 is an Azure Backup vault, which supports backing up Azure managed disks, so Disk1 belongs there. Recovery1 is a Recovery Services vault, which supports Azure virtual machine backups, so VM1 belongs there. App1 and DB1 are not the resources to select for either vault in this scenario.

https://learn.microsoft.com/en-us/azure/backup/backup-support-matrix
https://learn.microsoft.com/en-us/azure/backup/backup-support-matrix-iaas
https://learn.microsoft.com/azure/backup/backup-azure-recovery-services-vault-overview
https://learn.microsoft.com/en-us/azure/backup/disk-backup-faq

✗ **Box 1: App1** App1 — Azure App Service web app
App Service web app backups use App Service backup functionality; App1 is not the resource to select for an Azure Backup vault. Disk1 is the supported resource for Backup1 in this question.

https://learn.microsoft.com/en-us/azure/backup/backup-support-matrix

✗ **Box 1: DB1** DB1 — Azure SQL Database
DB1 is an Azure SQL Database, not the Azure managed disk workload backed up to Backup1 in this scenario. Azure SQL Database backups are handled through its database backup features, rather than selecting DB1 for this vault assignment.

https://learn.microsoft.com/en-us/azure/backup/backup-support-matrix

✓ **Box 1: Disk1** Disk1 — Disk
Backup1 is an Azure Backup vault, which supports Azure Disk backup. Therefore, Disk1 is the correct resource for Backup1.

https://learn.microsoft.com/en-us/azure/backup/backup-support-matrix
https://learn.microsoft.com/en-us/azure/backup/disk-backup-faq

✗ **Box 1: VM1** VM1 — Virtual machine
VM1 is backed up using a Recovery Services vault, not the Azure Backup vault selected as Backup1 here. Recovery1 is the appropriate vault for VM1.

https://learn.microsoft.com/en-us/azure/backup/backup-support-matrix-iaas
https://learn.microsoft.com/azure/backup/backup-azure-recovery-services-vault-overview

✗ **Box 2: App1** App1 — Azure App Service web app
App1 is not the virtual machine workload to select for a Recovery Services vault in this scenario. Recovery1 is used for backing up VM1.

https://learn.microsoft.com/en-us/azure/backup/backup-support-matrix
https://learn.microsoft.com/azure/backup/backup-azure-recovery-services-vault-overview

✗ **Box 2: DB1** DB1 — Azure SQL Database
DB1 is an Azure SQL Database, not the virtual machine resource to select for Recovery1 in this question. Its database backups are handled through Azure SQL backup features.

https://learn.microsoft.com/en-us/azure/backup/backup-support-matrix
https://learn.microsoft.com/azure/backup/backup-azure-recovery-services-vault-overview

✗ **Box 2: Disk1** Disk1 — Disk
Disk1 is backed up using the Azure Backup vault, Backup1. Recovery1 is the vault to use for VM1 instead.

https://learn.microsoft.com/en-us/azure/backup/backup-support-matrix-iaas
https://learn.microsoft.com/azure/backup/backup-azure-recovery-services-vault-overview
https://learn.microsoft.com/en-us/azure/backup/disk-backup-faq

✓ **Box 2: VM1** VM1 — Virtual machine
Recovery Services vaults support Azure virtual machine backup. Therefore, VM1 is the correct resource for Recovery1.

https://learn.microsoft.com/en-us/azure/backup/backup-support-matrix-iaas
https://learn.microsoft.com/azure/backup/backup-azure-recovery-services-vault-overview

Question 77

Single choice · Domain: D5 Monitor and maintain Azure resources › Implement backup and recovery

You plan to back up an Azure virtual machine named VM1. You discover that the Backup Pre-Check status displays a status of Warning. What is a possible cause of the Warning status?

A. VM1 is stopped.
B. A Recovery Services vault is unavailable.
C. VM1 has an unmanaged disk.
D. VM1 does not have the latest version of the Azure VM Agent (WaAppAgentexe) installed.

Answer: D. VM1 does not have the latest version of the Azure VM Agent (WaAppAgentexe) installed.

Explanation

A Backup Pre-Check warning can indicate that VM1's Azure VM Agent is outdated. Updating the agent to the latest version can address this VM-side condition; therefore, option D is the possible cause in this scenario. [3] [7] [12]

https://learn.microsoft.com/en-us/azure/backup/quick-backup-vm-portal
https://learn.microsoft.com/en-us/azure/backup/backup-azure-vms-troubleshoot
https://learn.microsoft.com/en-us/azure/virtual-machines/extensions/agent-windows

✗ **A** VM1 is stopped.
A stopped VM is not the specific condition identified here: Azure VM Backup can back up a VM that is shut down. The outdated VM Agent is the possible cause of the Warning status in this question. [10]

https://learn.microsoft.com/azure/backup/backup-azure-vm-backup-faq

✗ **B** A Recovery Services vault is unavailable.
An unavailable vault would affect access to or execution of the backup operation; it is not the VM-side pre-check condition described here. The relevant possible cause is that VM1's Azure VM Agent is not up to date. [3]

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

✗ **C** VM1 has an unmanaged disk.
Having an unmanaged disk is not the possible pre-check warning cause identified in this scenario. The warning can instead arise because the Azure VM Agent installed on VM1 is outdated. [5] [7]

https://learn.microsoft.com/en-us/azure/backup/backup-support-matrix-iaas
https://learn.microsoft.com/en-us/azure/backup/backup-azure-vms-troubleshoot

✓ **D** VM1 does not have the latest version of the Azure VM Agent (WaAppAgentexe) installed.
An outdated Azure VM Agent can cause a Backup Pre-Check warning. Updating the agent to the latest version is the appropriate response to this warning condition. [3] [7] [12]

https://learn.microsoft.com/en-us/azure/backup/quick-backup-vm-portal
https://learn.microsoft.com/en-us/azure/backup/backup-azure-vms-troubleshoot
https://learn.microsoft.com/en-us/azure/virtual-machines/extensions/agent-windows

Free demo · full exam: 507 questions

Question 78

Single choice · Domain: D5 Monitor and maintain Azure resources › Monitor resources in Azure

You have an Azure subscription that contains a virtual network named VNet1.

VNet1 uses two ExpressRoute circuits that connect to two separate on-premises datacenters.

You need to create a dashboard to display detailed metrics and a visual representation of the network topology.

What should you use?

A. Azure Monitor Network Insights
B. Azure Virtual Network Watcher
C. Log Analytics
D. a Data Collection Rule (DCR)

Answer: A. Azure Monitor Network Insights

Explanation

Azure Monitor Network Insights is designed to provide a consolidated view of network resources, including detailed metrics and a visual topology. The ExpressRoute Network Insights experience applies to the circuits connecting VNet1 to the two on-premises datacenters, so it meets both requirements in the scenario. Use it rather than a general network troubleshooting tool or a data-collection configuration.

https://learn.microsoft.com/en-us/azure/expressroute/expressroute-network-insights

✓ **A** Azure Monitor Network Insights
ExpressRoute Network Insights provides a view of ExpressRoute resources with detailed monitoring metrics and a visual representation of the network topology. That combination matches the requested dashboard for VNet1 and its two ExpressRoute circuits.

https://learn.microsoft.com/en-us/azure/expressroute/expressroute-network-insights

✗ **B** Azure Virtual Network Watcher
Network Watcher provides network monitoring and troubleshooting capabilities, and its topology feature can visualize network resources. However, the scenario specifically calls for the detailed ExpressRoute metrics and topology dashboard provided by ExpressRoute Network Insights.

https://learn.microsoft.com/en-us/azure/network-watcher/network-insights-overview
https://learn.microsoft.com/EN-US/azure/network-watcher/network-insights-topology
https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-overview

✗ **C** Log Analytics
Log Analytics is used to query and analyze collected log data, not to provide the purpose-built ExpressRoute dashboard and visual network topology requested here. It would not be the direct service to choose for this requirement.

✗ **D** a Data Collection Rule (DCR)
A DCR specifies how Azure Monitor collects and processes monitoring data. It is a data-collection configuration, not a dashboard that displays ExpressRoute metrics and network topology.

https://learn.microsoft.com/en-us/azure/azure-monitor/data-collection/data-collection-rule-best-practices
https://learn.microsoft.com/en-us/azure/azure-monitor/data-collection/data-collection-rule-overview

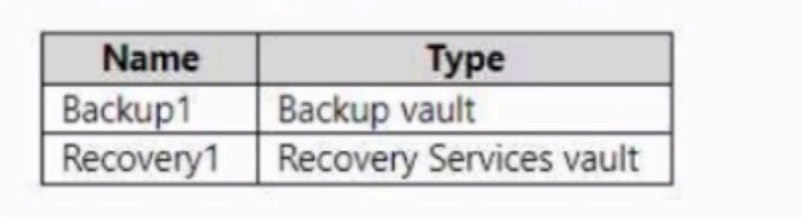
Free demo · full exam: 507 questions

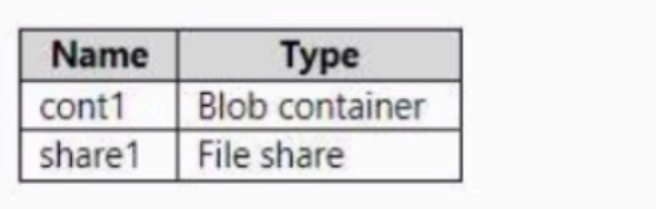
Question 79

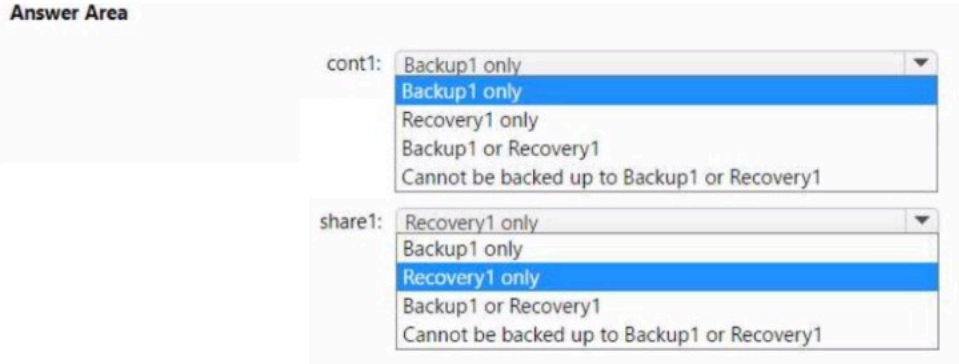
Hotspot (dropdowns) · Domain: D5 Monitor and maintain Azure resources › Implement backup and recovery

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

Name	Type
Backup1	Backup vault
Recovery1	Recovery Services vault







You create a storage account that contains the resources shown in the following table.

Name	Type
cont1	Blob container
share1	File share

To which vault can you back up cont1 and share1? To answer, select the appropriate options in the answer area.

NOTE: Each correct answer is worth one point.

cont1: Backup1 only | Recovery1 only | Backup1 or Recovery1 | Cannot be backed up to Backup1 or Recovery1

share1: Backup1 only | Recovery1 only | Backup1 or Recovery1 | Cannot be backed up to Backup1 or Recovery1

Free demo · full exam: 507 questions

Answer

- cont1: **Backup1 only**
- share1: **Recovery1 only**

Explanation

Back up cont1, the blob container, to Backup1 because Azure Blob backup uses a Backup vault. Back up share1, the Azure file share, to Recovery1 because Azure Files backup uses a Recovery Services vault. The two resource types therefore require different vault types in this scenario.

https://learn.microsoft.com/en-us/azure/backup/backup-azure-files
https://learn.microsoft.com/en-us/azure/backup/azure-file-share-backup-overview
https://learn.microsoft.com/en-us/azure/backup/blob-backup-configure-manage
https://learn.microsoft.com/en-us/azure/backup/blob-backup-overview

✓ **cont1: Backup1 only** Backup1 only
cont1 is a blob container, and Azure Blob backup is configured in a Backup vault. Backup1 is the only Backup vault listed, so it is the appropriate choice.

https://learn.microsoft.com/en-us/azure/backup/blob-backup-configure-manage
https://learn.microsoft.com/en-us/azure/backup/blob-backup-overview

✗ **cont1: Recovery1 only** Recovery1 only
Recovery1 is a Recovery Services vault, not a Backup vault. It is not the vault type used for backing up the blob container cont1.

https://learn.microsoft.com/en-us/azure/backup/blob-backup-configure-manage
https://learn.microsoft.com/en-us/azure/backup/blob-backup-overview
https://learn.microsoft.com/azure/backup/backup-azure-recovery-services-vault-overview

✗ **cont1: Backup1 or Recovery1** Backup1 or Recovery1
The two vault types are not interchangeable for this resource. Blob backup uses a Backup vault, so Recovery1 is not also an eligible option.

https://learn.microsoft.com/en-us/azure/backup/blob-backup-configure-manage
https://learn.microsoft.com/en-us/azure/backup/blob-backup-overview
https://learn.microsoft.com/azure/backup/backup-azure-recovery-services-vault-overview

✗ **cont1: Cannot be backed up to Backup1 or Recovery1** Cannot be backed up to Backup1 or Recovery1
Azure Blob backup is supported, and Backup1 is the required type of vault for it. Therefore cont1 can be backed up to one of the listed vaults.

https://learn.microsoft.com/en-us/azure/backup/blob-backup-configure-manage
https://learn.microsoft.com/en-us/azure/backup/blob-backup-overview

✗ **share1: Backup1 only** Backup1 only
share1 is an Azure file share, whose backup in this scenario uses a Recovery Services vault. Backup1 is a Backup vault, so it is not the appropriate vault for share1.

https://learn.microsoft.com/en-us/azure/backup/backup-azure-files
https://learn.microsoft.com/en-us/azure/backup/azure-file-share-backup-overview
https://learn.microsoft.com/azure/backup/backup-azure-recovery-services-vault-overview

✓ **share1: Recovery1 only** Recovery1 only
share1 is an Azure file share, and Azure Files backup uses a Recovery Services vault. Recovery1 is the only Recovery Services vault listed.

https://learn.microsoft.com/en-us/azure/backup/backup-azure-files
https://learn.microsoft.com/en-us/azure/backup/azure-file-share-backup-overview
https://learn.microsoft.com/azure/backup/backup-azure-recovery-services-vault-overview

✗ **share1: Backup1 or Recovery1** Backup1 or Recovery1
This choice incorrectly treats both vault types as suitable for the file share. For this scenario, Azure Files backup is performed through a Recovery Services vault, so Backup1 is not also an option.

https://learn.microsoft.com/en-us/azure/backup/backup-azure-files
https://learn.microsoft.com/en-us/azure/backup/azure-file-share-backup-overview

Free demo · full exam: 507 questions

https://learn.microsoft.com/azure/backup/backup-azure-recovery-services-vault-overview

✗ **share1: Cannot be backed up to Backup1 or Recovery1** Cannot be backed up to Backup1 or Recovery1
Azure file shares can be backed up, and Recovery1 is the appropriate Recovery Services vault listed for that purpose. The share is therefore not excluded from both vaults.

https://learn.microsoft.com/en-us/azure/backup/backup-azure-files
https://learn.microsoft.com/en-us/azure/backup/azure-file-share-backup-overview
https://learn.microsoft.com/azure/backup/backup-azure-recovery-services-vault-overview

---

Question 80

Single choice · Domain: D5 Monitor and maintain Azure resources › Implement backup and recovery

You have an Azure subscription that contains a virtual machine named VM1. You plan to configure Azure Site Recovery for VM1. You create a Recovery Services vault and enable replication for VM1.

You need to ensure that in the event of a failover. VM1 starts automatically in the target Azure region. What should you do?

A. Configure a recovery plan.
B. Configure an Azure logic app.
C. Create an Azure Automation account.
D. Enable Update Management for VM1.

Answer: A. Configure a recovery plan.

Explanation

Configure a recovery plan for VM1. Azure Site Recovery recovery plans orchestrate failover and can start the replicated VM in the target region as part of the failover process. This meets the requirement without adding a separate automation or update-management service. [1][2]

https://learn.microsoft.com/azure/site-recovery/recovery-plan-overview
https://learn.microsoft.com/en-us/azure/site-recovery/site-recovery-create-recovery-plans

✓ **A** Configure a recovery plan.
A recovery plan coordinates the failover steps for replicated machines, including starting VM1 in the target region when the plan is run. This is the Site Recovery feature intended to orchestrate recovery. [1] [2]

https://learn.microsoft.com/azure/site-recovery/recovery-plan-overview
https://learn.microsoft.com/en-us/azure/site-recovery/site-recovery-create-recovery-plans

✗ **B** Configure an Azure logic app.
A Logic App is not required to start a replicated VM as part of Site Recovery failover. Recovery plans provide the built-in failover orchestration needed in this scenario. [1]

https://learn.microsoft.com/azure/site-recovery/recovery-plan-overview

✗ **C** Create an Azure Automation account.
An Automation account can support custom runbook automation, but creating one alone does not configure VM1 to start during failover. A recovery plan is the relevant Site Recovery mechanism. [1][11]

https://learn.microsoft.com/azure/site-recovery/recovery-plan-overview
https://learn.microsoft.com/en-us/azure/site-recovery/site-recovery-runbook-automation

✗ **D** Enable Update Management for VM1.

Free demo · full exam: 507 questions

Update Management handles VM update operations; it does not orchestrate Site Recovery failover or start VM1 in the target region. [1]

https://learn.microsoft.com/azure/site-recovery/recovery-plan-overview

Dumpsgate