**Your company is migrating to the cloud and wants to replicate its on-premise  
Question 1**

**Question**

INCORRECT

**You would like to implement a hub-and-spoke VNet peering connection between two of your virtual networks, VNet1 in the East US region and VNet2 in the East US-2 region, using a network virtual appliance (NVA).**

**You have deployed VNet3 to serve as the network hub, and a custom Linux virtual machine in VNet3 to serve as the NVA.**

**How should you configure the peering connections between the VNets with this particular hub-and-spoke architecture?**

Configure all peering connections to allow forwarded traffic.

Configure peering connections directed to the hub network (VNet3) to allow gateway transit.

Configure peering connections directed to the spoke networks (VNet1 and VNet2) to use remote gateways.

Configure peering connections directed to the hub network (VNet3) to use remote gateways. Configure all other peering connections to allow gateway transit.

**Explanation**

If you require connectivity between spokes, consider deploying an Azure Firewall or other network virtual appliance. Then create routes to forward traffic from the spoke to the firewall or network virtual appliance, which can then route to the second spoke. In this scenario, you must configure the peering connections to allow forwarded traffic.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke?tabs=cli>

Something wrong with this question?

**Question 2**

**Question**

INCORRECT

**You want to connect the Azure VNets for three separate branch offices. You are designing a hub and spoke model network topology to do this. The central hub will serve as a firewall between the different locations during backend communication, and also a central location for disaster recovery backup storage.**

**Now you are considering whether to connect your hub-and-spoke model with VNet peering connections or Azure VPN Gateways. Each option has its own benefits.**

**Which statements comparing VNet peering and VPN Gateways in a hub-and-spoke model are correct? (Choose 3 answers)**

If you implement the model with Azure VPN Gateways, all VNets **can be cross-region.**

If you implement the model with VNet peering connections, the VNets **can be cross-region with Global VNet Peering.**

Whether the connections are made with Azure VPN Gateways or VNet peering connections, the VNets can be **within different Azure subscriptions** and associated **with separate Azure AD tenants**.

If you implement the model with Azure VPN Gateways, all VNets **can be in different regions**.

If you implement the model with VNet peering connections, the VNets **must be in the same region**.

If you implement the model with Azure VPN Gateways, the VNets can be **within different Azure subscriptions** that are **associated with the same Azure tenant.**

If you implement the VNets with VNet peering connections, the VNets can be **within different Azure subscriptions** and **associated with separate Azure AD tenants**.

**Explanation**

You could accomplish this network topology using VNet peering or Azure VPN Gateways, but each option has its requirements and limitations.

1. Connecting via VNet peering would require a router to be deployed in the central hub VNet, but this is not required for VNG connections.
2. VNet peering works both across separate tenants and subscriptions.
3. Hostname resolution is not possible for VMs connecting from different VNets through a peering connection. Azure DNS is required for these VMs to connect. However, name resolution is possible through a VNG connection.
4. VNets must be connected via Global VNet Peering.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: [/course/azure-network-connectivity-name-resolution/virtual-network-peering/](https://cloudacademy.com/course/azure-network-connectivity-name-resolution/virtual-network-peering/)

**Covered in this lecture**

**[Virtual Network Peering](https://cloudacademy.com/course/azure-network-connectivity-name-resolution/virtual-network-peering/)**

[Course](https://cloudacademy.com/course/azure-network-connectivity-name-resolution/virtual-network-peering/)

**[Azure Network Connectivity and Name Resolution](https://cloudacademy.com/course/azure-network-connectivity-name-resolution/virtual-network-peering/)**

[Time](https://cloudacademy.com/course/azure-network-connectivity-name-resolution/virtual-network-peering/)

**[4m 26s](https://cloudacademy.com/course/azure-network-connectivity-name-resolution/virtual-network-peering/)**

**Question 6**

**Question**

INCORRECT

**You have deployed a new virtual machine (VM1) to availability Set 1 (AS1) in VNet1. After the deployment, you realize you deployed it to the wrong availability set and VNet.**

**You need the VM to be located in a different availability set named AS2.**

**How can you fix this issue?**

Delete VM1 and recreate it to deploy within AS2.

Change the state of VM1 to Stopped (Deallocated). Then migrate VM1 to AS2 by updating the settings within Azure Portal.

Change the state of VM1 to Stopped (Deallocated). Ensure you have the proper permissions to move resources between the two availability sets. Then migrate VM1 to AS2 by updating the settings within Azure Portal.

Ensure you have the proper permissions to move resources between the two availability sets. Then migrate VM1 to AS2 by updating the settings within Azure Portal.

**Explanation**

Once you deploy a virtual machine as a standalone VM, or to an availability set, the VM's status cannot be changed. It will always be standalone or within the selected availability set. The only way to fix the issue, assuming no other services are being used that is to delete and recreate the VM.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: [/course/azure-resource-manager-virtual-machines/demo-add-three-vms-to-availability-set-1/](https://cloudacademy.com/course/azure-resource-manager-virtual-machines/demo-add-three-vms-to-availability-set-1/)

**Question 3**

**Question**

CORRECT

**You are investigating Azure Storage replication options to discover when you get the read and write access to the remote replica.**

**Which statement regarding read and write access to Azure Storage replicas is correct?**

No matter which replication option you've selected for your Azure Storage account, you gain read and write access to the remote replica when you initiate failover.

If you have configured RA-GRS replication for your Azure Storage account, you always have read and write access to the Azure Storage account's replica.

No matter which replication option you've selected, once Azure fails over to the account's remote sites, then you are granted write access to the replicated data.

If you have configured GRS or RA-GRS replication for your Azure Storage account, you always have read and write access to the Azure Storage account's replica.

**Explanation**

With GRS and other replication options, only Microsoft can declare a disaster and failover the remote sites, then you will get read and write access to data. Until then you don't have access to the remote site's data for the read/write operations. You only have access to the remote copy for read operations when using RA-GRS.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://docs.microsoft.com/en-us/azure/storage/storage-redundancy>

Something wrong with this question?

**Question 4**

**Question**

CORRECT

**You need to create Azure resource templates to automate the deployment of resources. At the same time, you need to ensure that anyone can differentiate between resources created for development or production. Which of the below template features can help people identify the purpose of deployed resources in this way?**

tags

resources

$schema

contentversion

**Explanation**

Tags can be used in templates to differentiate resources. For example, you can add a tag with a name of “Environment.” You can then assign values of “Production” to production-based instances and “Development” to development-based instances

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-template-tags>

Something wrong with this question?

**Question 5**

**Question**

CORRECT

**You have begun migrating your existing applications from on-premise servers to resources on an Azure Virtual Network. The on-premise network and Azure are currently connected via ExpressRoute. You need to ensure the ExpressRoute connection is healthy at all times. What Network Watcher service can you utilize to monitor the connection?**

Connection Monitor (formerly Network Performance Monitor)

Traffic Analytics

VPN Troubleshoot

Connection Monitor (Classic)

**Explanation**

The new Connection Monitor (formerly the Network Performance Monitor service) is a cloud-based hybrid network monitoring solution that helps you monitor network performance between various points in your network infrastructure. It also helps you monitor network connectivity to service and application endpoints and monitor the performance of Azure ExpressRoute.

Please note that Azure also has a legacy service that is also named Connection Monitor, but this has been changed to Connection Monitor Classic.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://docs.microsoft.com/en-us/azure/azure-monitor/insights/network-performance-monitor?toc=%2fazure%2fnetwork-watcher%2ftoc.json>

Something wrong with this question?

**Question 6**

**Question**

INCORRECT

**You have deployed a new virtual machine (VM1) to availability Set 1 (AS1) in VNet1. After the deployment, you realize you deployed it to the wrong availability set and VNet.**

**You need the VM to be located in a different availability set named AS2.**

**How can you fix this issue?**

Delete VM1 and recreate it to deploy within AS2.

Change the state of VM1 to Stopped (Deallocated). Then migrate VM1 to AS2 by updating the settings within Azure Portal.

Change the state of VM1 to Stopped (Deallocated). Ensure you have the proper permissions to move resources between the two availability sets. Then migrate VM1 to AS2 by updating the settings within Azure Portal.

Ensure you have the proper permissions to move resources between the two availability sets. Then migrate VM1 to AS2 by updating the settings within Azure Portal.

**Explanation**

Once you deploy a virtual machine as a standalone VM, or to an availability set, the VM's status cannot be changed. It will always be standalone or within the selected availability set. The only way to fix the issue, assuming no other services are being used that is to delete and recreate the VM.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: [/course/azure-resource-manager-virtual-machines/demo-add-three-vms-to-availability-set-1/](https://cloudacademy.com/course/azure-resource-manager-virtual-machines/demo-add-three-vms-to-availability-set-1/)

Something wrong with this question?

**Question 7**

**Question**

CORRECT

**You want to configure an Azure storage account to be accessible from only one Virtual Network in your Azure Virtual Network (VNet). The storage account should not be accessible from other networks or regions across your company's Azure subscription.**

**What should you do to implement this requirement?**

Activate the Secure transfer required option.

Add a network security group.

Create a VNet service endpoint.

Deploy Azure Traffic Manager.

**Explanation**

Virtual Network (VNet) service endpoint provides secure and direct connectivity to Azure services over an optimized route over the Azure backbone network. Endpoints allow you to secure your critical Azure service resources to only your virtual networks. Service Endpoints enable private IP addresses in the VNet to reach the endpoint of an Azure service without needing a public IP address on the VNet.

You should not activate the Secure transfer required option because this option forces all inbound and outbound traffic into the storage account to be secured over HTTPS instead of also allowing HTTP.

You should not add a network security group because this would limit access to resources within a VNet through filters such as IP filters and role-based access control (RBAC). It does apply to a single storage account.

You should not deploy Azure Traffic Manager because it is used to control the inbound and outbound flow of traffic for Azure networks. It does not apply to a single storage account.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview>

Something wrong with this question?

**Question 8**

**Question**

INCORRECT

**You are reviewing the specifications for a new solution, and it lists "a managed layer 7 load balancer."**

**Which of the following services will be included in your design?**

Azure Application Gateway

Azure Load Balancer

A custom virtual appliance

Azure Traffic Manager

**Explanation**

The OSI model defines layer 7 as an application layer. That includes protocols such as FTP, HTTP(S), STMP, etc.

Application Gateway is a layer 7 load balancer for HTTP(S) based traffic.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-introduction>

Something wrong with this question?

**Question 9**

**Question**

INCORRECT

**You are the owner of a resource group that contains the following Azure resources:**

* **VNet1, which contains Subnet1. Subnet1 is assigned a routing table, and a network security group named NSG-1.**
* **SubNet1 contains an ARM virtual machine 1 with a private IP address only.**

**VM-Database1 needs to connect to an on-premises static IP address (216.3.128.12) to request software updates. You do not want to reveal the IP address of the ARM virtual machine 1. All inbound traffic aside from the software updates should be blocked.**

**Which steps should you take to allow the database to connect successfully for updates while limiting threats? (Choose 2 answers.)**

Deploy a private load balancer associated with the ARM virtual machine.

Deploy a NAT gateway associated with Subnet1.

Update NSG-1 to allow outbound traffic to and from 216.3.128.12 over port 443. Include no other rules allowing traffic.

Update NSG-1 to allow outbound traffic to 216.3.128.12 over port 443. Include no other rules allowing traffic.

**Explanation**

Network security group security rules are evaluated by priority using the 5-tuple information (source, source port, destination, destination port, and protocol) to allow or deny the traffic. A flow record is created for existing connections. Communication is allowed or denied based on the connection state of the flow record. The flow record allows a network security group to be stateful.

Deploy a Network Address Translation or NAT gateway to enable Source Network Address Translation (SNAT). As Microsoft explains in its documentation:

*Source Network Address Translation (SNAT) rewrites the source of a flow to originate from a different IP address and/or port. Typically, SNAT is used when a private network needs to connect to a public host over the internet. SNAT allows multiple compute resources within the private VNet to use the same single Public IP address or set of IP addresses (prefix) to connect to the internet.*

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://docs.microsoft.com/en-us/azure/virtual-network/nat-gateway/nat-gateway-resource#source-network-address-translation>

Something wrong with this question?

**Question 10**

**Question**

CORRECT

**Which of the following can be used to easily remove a resource lock?**

ResourceId

ApplicationId

UserId

SystemId

**Explanation**

An easy way to remove a resource lock is to specify the ResourceId associated with the lock.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://blogs.msdn.microsoft.com/cloud_solution_architect/2015/06/18/lock-down-your-azure-resources/>

Something wrong with this question?

**Question 11**

**Question**

INCORRECT

**A company is planning to implement agile methodologies for one of their projects. The project will have the development environment as an app service hosted in Azure. Which of the following implementations would align with their agile practices?**

For the app service in Azure, configure the deployment source to any source code repository. Also ensure the deployment credentials are set. Ensure the right source code URL is set.

Set up Traffic Manager to route the different requests of the development environments from the different development teams.

Setup separate subscriptions for each development team and let each team connect their source code repository to the separate subscriptions

Setup a separate virtual machine for each developer and ensure they make their code changes to each virtual machine separately.

**Explanation**

For Agile practices, continuous integration is the key. Hence developers would want to ensure that all merged changes to the main trunk of their source code repository gets pushed to the development environment accordingly. This can be done by configuring the deployment source of the app service to the desired source code repository. Also ensure the deployment credentials are set. Ensure the right source code URL is set.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://docs.microsoft.com/en-us/azure/app-service-web/app-service-deploy-local-git>

Something wrong with this question?

**Question 12**

**Question**

CORRECT

**When using Azure Resource Manager (ARM) templates, what feature enables you to control resource properties during deployment in your organization?**

Active Directory

API Management

Azure Policy

Resource tags

**Explanation**

Resource policies enable you to establish conventions for resources in your organization. By defining conventions, you can control costs and more easily manage your resources. For example, you can specify that only certain types of virtual machines are allowed, or you can require that all resources have a particular tag.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-policy>

Something wrong with this question?

**Question 13**

**Question**

CORRECT

**You are a cost-sensitive IT administrator, and want to turn off your virtual machines at night to save money. What is a recommended method to do this?**

Create an operating system script that will turn off instances at the OS level, resulting in the VM state "Stopped."

Stop VMs from the Azure portal or using Azure Automation, resulting in the VM state "Stopped (Deallocated)"

Shutting down your VMs either through an operating system script or using the Azure Portal will work, as long as the VM state is "Stopped" or "Stopped (Deallocated).

Stop VMs using Azure Command Line Interface, resulting in the VM state "Stopped."

**Explanation**

If an only if the status of the VM says “stopped (deallocated),” then you are not billed. If it says “stopped allocated,” you’re still being billed for allocated virtual cores.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://blogs.technet.microsoft.com/gbanin/2015/04/22/difference-between-the-states-of-azure-virtual-machines-stopped-and-stopped-deallocated/>

Something wrong with this question?

**Question 14**

**Question**

INCORRECT

**Your company is being audited, and an external accountant needs access to review a blob container in the Blob service within one specific Azure storage account.**

**You currently use Azure Active Directory to control access to the blob storage resources in question. However, you have been told you need to provide the accountant with immediate access to review the blob container in the storage account without any further information.**

**How can you provide necessary access, but also limit it to the container in question?**

Provide the accountant with read-only access to the specific Azure Blob container with a service-level shared access signature token to expire at the end of the business day. Specify the HTTPS protocol is required to accept requests.

Assign the accountant a guest role in Azure Active Directory with read-only access to the specific Azure Blob storage service in the Azure Storage account.

Provide the accountant with read-only access to the specific Azure Blob container with a user-delegation shared access signature token to expire at the end of the business day. Allow all read requests but limit write requests to LIST and GET. Specify the HTTPS protocol is required to accept requests.

Provide the accountant with contributor role access to the storage account using Azure AD role-based access control (RBAC).

**Explanation**

In this case, Azure Storage's Shared Access Signature (SAS) is the best tool to provide limited, authorized access to the necessary blob resources. Remember, SAS allows two levels of access: service-level, which limits access to one type of storage within the Azure storage account, such as Blob, Table, Queue or File storage, and account level, which provides access to all storage types in a single account. The service level also allows you to limit access to specific containers, or even specific blobs, and control the actions that can be performed on the blobs by selecting approved common permission types such as read, write, list, or process.

You cannot provide a user-delegated SAS in this case because you do not know if the accountant has Azure AD credentials, which are required for this type of SAS.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://docs.microsoft.com/en-us/azure/storage/common/storage-dotnet-shared-access-signature-part-1#shared-access-signature-parameters>

Something wrong with this question?

**Question 15**

**Question**

CORRECT

**Which of the following Azure VPN solutions uses VPN over SSTP (Secure Socket Tunneling Protocol) and can be used to connect to a Virtual Network (VNet) from a remote location like a hotel or home office by establishing the connection from the client computer?**

Site-to-Site (S2S)

Point-to-Site (P2S)

SSTP-to-VNet

Multi-site

**Explanation**

A P2S connection is established by the client computer (a home office PC for example) to connect to a VNnet using a VPN connection over SSTP.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways>

Something wrong with this question?

**Question 16**

**Question**

CORRECT

**You would like to implement a Hub-and-Spoke VNet peering connection between two existing VNets in the East US region, (VNet 1 and VNet2), without using a network virtual appliance. You want resources in VNet1 and VNet2 to be able to communicate.**

**You have deployed VNet3 in the East US region that will serve as a hub between the other VNets. VNet1 and VNet2 should be able to communicate with each other through VNet3 using a VPN virtual network gateway.**

**Which VNet peering connections should be configured to allow all forwarded traffic? (Choose 2 answers.)**

VNet1 to VNet3 peering connection with traffic forwarded enabled.

VNet2 to VNet3 peering connection with traffic forwarded enabled

Only peering connections directed to VNet3 as the hub

Only peering connections directed to VNet1 and VNet2 as the spokes

**Explanation**

To implement a Hub-and-Spoke VNet peering connection between two existing VNets in the East US region without using a network virtual appliance, you can use a VPN virtual network gateway to connect the spoke VNets (VNet1 and VNet2) to the hub VNet (VNet3).

To allow all forwarded traffic between the VNets, you should configure the following VNet peering connections:

VNet1 to VNet3 peering connection with traffic forwarded enabled.

VNet2 to VNet3 peering connection with traffic forwarded enabled.

By enabling traffic forwarding, you allow traffic to be routed through the peering connection, which enables communication between resources in the spoke VNets (VNet1 and VNet2) through the hub VNet (VNet3) using the VPN virtual network gateway.

You can also configure spokes to use the hub gateway to communicate with remote networks. To allow gateway traffic to flow from spoke to hub and connect to remote networks, you must:

* Configure the peering connection in the hub to allow gateway transit.
* Configure the peering connection in each spoke to use remote gateways.
* Configure all peering connections to allow forwarded traffic.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke?tabs=cli>

Something wrong with this question?

**Question 17**

**Question**

INCORRECT

**What major directory roles are available in Azure AD? (Choose 3 answers)**

User

Administrator

Global Administrator

Limited Administrator

**Explanation**

Administrator and Guest are not Directory roles in Azure AD.  User, Global Administrator, and Limited Administrator are the three major Directory roles in Azure AD.  Limited Administrator can be broken out into various types of "sub-administrators."

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: [/azure/azure-active-directory-security-course/manage-access-to-azure-ad.html](https://cloudacademy.com/azure/azure-active-directory-security-course/manage-access-to-azure-ad.html)

Something wrong with this question?

**Question 18**

**Question**

INCORRECT

**Which statement regarding Azure Network Watcher's IP Flow Verify is correct?**

It can test packet flow between any two Azure endpoints.

It checks network security group for any rule(s) that deny the connection.

It reviews all NSG rules associated with either connection endpoint.

It verifies both directions of traffic simultaneously.

**Explanation**

IP Flow Verify tests if packets flow between a VM and a second endpoint only. It checks for any NSG rules which deny the connection. It only reviews one direction at a time, and for NSG rules associated with one connection point at a time.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview>

**Covered in this lecture**

**[Summary](https://cloudacademy.com/course/managing-connectivity-azure-network-watcher/summary/)**

[Course](https://cloudacademy.com/course/managing-connectivity-azure-network-watcher/summary/)

**[Managing Connectivity with Azure Network Watcher](https://cloudacademy.com/course/managing-connectivity-azure-network-watcher/summary/)**

[Time](https://cloudacademy.com/course/managing-connectivity-azure-network-watcher/summary/)

**[2m 31s](https://cloudacademy.com/course/managing-connectivity-azure-network-watcher/summary/)**

Something wrong with this question?

**Question 19**

**Question**

CORRECT

**What Azure network resource can allow or deny layer-3 traffic based on a series of security rules, and can also be directly applied to virtual machines, subnets, or network interface cards attached to virtual machines?**

Network Security Groups

Access Control Lists

Azure Firewalls

Application Gateways

**Explanation**

A network security group (NSG) contains a list of security rules that allow or deny network traffic to resources connected to Azure Virtual Networks (VNet). NSGs can be associated to subnets, individual VMs (classic), or individual network interfaces (NIC) attached to VMs (Resource Manager). When an NSG is associated to a subnet, the rules apply to all resources connected to the subnet. Traffic can further be restricted by also associating an NSG to a VM or NIC.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-nsg>

Something wrong with this question?

**Question 20**

**Question**

CORRECT

**The following is a subsection of an ARM template to deploy a Windows VM. In order to create the network interface you need a public IP Address and a Virtual Network. Which of the answers below belong in the dependsOn array to accomplish that objective?**

**...**

**{**

**"apiVersion": "2016-03-30",**

**"type": "Microsoft.Network/networkInterfaces",**

**"name": "[variables('nicName')]",**

**"location": "[resourceGroup().location]",**

**"dependsOn": [**

**\_\_\_\_FILL\_IN\_THE\_BLANK\_\_\_\_**

**"[resourceId('Microsoft.Network/virtualNetworks/', variables('virtualNetworkName'))]"**

**],**

**...**

"[resourceId('Microsoft.Network/publicIPAddresses/', variables('publicIPAddressName'))]",

"[resourceId('Microsoft.Network/networkInterfaces/', variables('nicName'))]"

"[reference(variables('publicIPAddressName')).dnsSettings.fqdn]"

"[resourceId('Microsoft.Storage/storageAccounts/', variables('storageAccountName'))]",

**Explanation**

The dependsOn property of a resource will allow you to delay the creation of a resource until another exists.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-authoring-templates>

Something wrong with this question?

**Question 21**

**Question**

CORRECT

**By default, Azure Virtual Machine operating system disks enable host caching for read and write disk I/O operations. What benefit does this provide?**

It allows the VM to effectively manage a large quantity of requests and store the data ephemerally.

It allows the VM to load balance CPU-intensive operation.

It allows VM operating systems to use extensive and complex encryption techniques by default.

It allows the VM operating system to support read and write disk I/O operations required for vertical and horizontal scaling.

**Explanation**

Operating system disks by default have enabled Host Caching for Read/Write disk I/O operations, since we can expect a fair amount of activity on this disk when the VM is being used. Data disks however have Host Caching disabled which really leaves it up to you to determine how often read/write operations occur and set caching appropriately. There’s no one shoe fits all, and so you have to use your own best judgment.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://docs.microsoft.com/en-us/azure/storage/storage-premium-storage-performance#disk-caching>

Something wrong with this question?

**Question 22**

**Question**

CORRECT

**A company needs to connect their on-premise data center to Azure. They want to have a dedicated connection and at the same time want to have a failover connection. They don’t mind having a drop in latency when it comes to the failover connection. They also have around 500+ employees who will need to use this connection. Which of the following connection types would you use?**

Site-to-Site for the main and failover connection.

Site-to-Site for the main and Point-to-Site for the failover connection.

ExpressRoute for the main connection and Site-to-Site for the failover connection.

Site-to-Site for the main and ExpressRoute for the failover connection.

**Explanation**

An ExpressRoute connection behaves like a dedicated connection between your on-premise data center and Azure**.**You can establish multiple connections betweenyour on-premise data center and Azure. In the failover connection, since the company does not mind a drop in latency, they can opt for a Site-to-Site VPN connection. This type of model is often used for a primary and failover connection from on-premise data centers and Azure**.**

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://docs.microsoft.com/en-us/azure/expressroute/expressroute-howto-coexist-resource-manager>

Something wrong with this question?

**Question 23**

**Question**

INCORRECT

**Your IT consulting business has recently partnered with two other businesses in different regions of the country. Each of your three offices has resources deployed in Microsoft Azure cloud.**

**Although you plan to eventually merge your separate offices into a single Azure AD tenant, you would like to connect several VNets in your separate subscriptions beforehand with your existing, separate Azure AD tenants in place.**

**What Azure solution is the easiest way to accomplish this?**

Create VNet peering connection

Create Virtual Network Gateways

Create a DNS zone with split-horizon view

Create a VNet-to-VNet VPN

**Explanation**

Microsoft Azure has steadily increased the compatibility of VNet Peering connections so that the previous generation solution, known as either Virtual Network Gateways or VPN Gateways, are used for in fewer scenarios now. VNet Peering connections can now connect VNets within separate subscriptions also within separate Azure AD tenants.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: [/course/azure-network-connectivity-name-resolution/virtual-network-gateways/](https://cloudacademy.com/course/azure-network-connectivity-name-resolution/virtual-network-gateways/)

**Covered in this lecture**

**[Virtual Network Gateways](https://cloudacademy.com/course/azure-network-connectivity-name-resolution/virtual-network-gateways/)**

[Course](https://cloudacademy.com/course/azure-network-connectivity-name-resolution/virtual-network-gateways/)

**[Azure Network Connectivity and Name Resolution](https://cloudacademy.com/course/azure-network-connectivity-name-resolution/virtual-network-gateways/)**

[Time](https://cloudacademy.com/course/azure-network-connectivity-name-resolution/virtual-network-gateways/)

**[5m 19s](https://cloudacademy.com/course/azure-network-connectivity-name-resolution/virtual-network-gateways/)**

Something wrong with this question?

**Question 24**

**Question**

CORRECT

**Your company has an application where users upload images and they're processed with different filters. The app is currently on-premises and you must design a solution in Azure.**

**The solution should minimize management effort, it should allow for deployments to be promoted, and the image processing code should run as a separate process from the web application.**

**Which option is best?**

WebJobs

IaaS VMs

Azure HPC

Azure HDInsight

**Explanation**

WebJobs is a feature of Azure App Service that enables you to run a program or script in the same context as a web app, API app, or mobile app, but as a separate process. And using App Services will minimize management, and web apps support deployment slots, allowing for deployment promotion.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://docs.microsoft.com/en-us/azure/app-service-web/websites-dotnet-webjobs-sdk>

Something wrong with this question?

**Question 25**

**Question**

INCORRECT

**Which of the following choices are true about Azure Storage encryption at rest? (Choose 2 answers)**

Azure Storage encryption is two-way encryption with asymmetric keys.

Azure Storage encryption is managed transparently by Azure.

Azure Storage encryption is one-way encryption with asymmetric keys.

Azure Storage encryption is two-way encryption with symmetric keys.

**Explanation**

Azure Storage encryption uses two-way symmetric keys and managed transparently by Azure and thus both parties have access to the secret key hence the symmetric nature.  Asymmetric key encryption (such as public/private key cryptography) is not valid in Azure Storage encryption.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: [/azure/microsoft-azure-security-solutions-course/data-security.html](https://cloudacademy.com/azure/microsoft-azure-security-solutions-course/data-security.html)

Something wrong with this question?

**Question 26**

**Question**

CORRECT

**Which standalone application provides a graphical interface for working with Azure Storage data on a Windows, OS X, or Linux machine?**

Microsoft Azure Storage Emulator

Microsoft Azure Storage Explorer

Windows Performance Monitor

IOSTAT

**Explanation**

Microsoft Azure Storage Explorer (Preview) is a free, standalone app from Microsoft that enables you to work graphically with Azure Storage data on Windows, OS X, and Linux. It also provides several ways to connect to your storage account (e.g., by subscription or through the storage emulator).

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://azure.microsoft.com/en-us/documentation/articles/vs-azure-tools-storage-manage-with-storage-explorer/>

Something wrong with this question?

**Question 27**

**Question**

CORRECT

**You are implementing Azure Backup to back up a group of VMs. If any VM suffers an outage or data corruption, you would like to restore the entire VM.**

**Your VMs require Managed SSD disk storage. When configuring the staging location for these VMs, how can you guarantee any restored VM through Azure Backup has the same storage configuration as the original VM?**

Check that a premium storage account with local redundant storage exists in the same region as the VM and Recovery Service Vault. Make sure Azure Storage Service Encryption has never been enabled on this storage account.

Check that a standard storage account endpoint with zone-redundant storage (ZRS) exists in the same resource group as the VM and Recovery Service Vault. Make sure Azure Storage Service Encryption has never been enabled on this storage account.

Check that a standard storage account with read-access globally redundant storage (RA\_GRS) exists in the same availability zone as the VM and Recovery Service Vault. Make sure Azure Disk Encryption is not currently enabled on this account

Check that a standard storage account with local redundant storage exists in the same region as the VM and Recovery Service Vault. Make sure Client-side Encryption is not currently enabled on this storage account.

**Explanation**

There are several factors to keep in mind here related to requirements for a VM restore through Azure Backup.

* The storage tier of the staging location determines the storage tier of the restored VM.
* The only redundancy option that offers premium is Local Redundant Storage, and you need a premium storage account for the VM.
* When your VM uses managed disks, the storage account acting as the staging location cannot have Azure Storage Service Encryption enabled at any time.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: [/course/implementing-azure-backup/16-recovering-an-entire-vm/](https://cloudacademy.com/course/implementing-azure-backup/16-recovering-an-entire-vm/)

Something wrong with this question?

**Question 28**

**Question**

INCORRECT

**Which AKS Service type supports public IP addresses and port numbers to allow direct access to AKS nodes by incoming traffic?**

ClusterIP Service type

NodePort Service type

LoadBalancer Service type

ExternalName Service type

**Explanation**

NodePort Service type supports public IP addresses and port numbers to enable direct access to AKS nodes by incoming traffic. This configuration requires an IP address for each AKS node.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://learn.microsoft.com/en-us/azure/aks/concepts-network>

Something wrong with this question?

**Question 29**

**Question**

INCORRECT

**A company hosts a web-based .Net application in Azure. They require that whenever an abnormal activity occurs, such as high page request rate, a custom application is notified so that it can be handled accordingly. Which option below meets this requirement?**

Create an alert in the Azure dashboard and configure the email alert. Ensure the custom application consumes the email alerts.

Create a custom powershell utility to check the the application request rate and then alerts the custom application accordingly.

Create an alert and use the Webhook functionality to send the notification to the custom application.

Create a custom utility that monitors and checks the application request rate and then sends the alert to the custom application.

**Explanation**

Webhooks allow one to route an Azure alert notification to other systems for post-processing or custom actions. A lot of custom systems support webhooks, hence this is the ideal implementation to alert third party systems to any irregularities generated by alerts in Azure.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/insights-webhooks-alerts>

Something wrong with this question?

**Question 30**

**Question**

CORRECT

**You are designing a transactional records management application for a small investment firm. It runs on memory-optimized virtual machines, which receive messages via Service Bus.**

**The virtual machines are grouped into a scale set with the following Scale Out rules:**

1. **Scale out one VM if CPU utilization is above 60 percent.**
2. **Scale out two VMs if CPU utilization is above 80 percent.**
3. **Scale out one VM if disk writes per second reach 65 percent capacity.**
4. **Scale out two VMs if disk writes per second reach 85 percent capacity.**
5. **Scale out one VM if message queue length reaches more than 1500.**
6. **Scale out two VMs if message queue length reaches more than 2500.**

**The following Scale In rules are also applied:**

1. **Scale in one VM if CPU utilization drops below 35 percent.**
2. **Scale in two VMs if CPU utilization drops below 20 percent.**

**Currently, your application is at 65 percent CPU utilization, disk writes per second are at 78 percent capacity, and the message queue length is 3000 messages.**

**Based on these metrics, what scaling action(s) will your application perform?**

Scale out two virtual machines.

Scale in one virtual machine.

Scale out one virtual machine.

Scale in two virtual machines.

**Explanation**

First and foremost, scale-out operations always have priority over scale-in operations. Anytime that multiple scale-out operations conflict with one another, the rule that takes precedence will be the one that initiates the largest increase in the number of instances. When it comes to scale-in conflicts, the rule that initiates the smallest decrease in the number of instances will take precedence.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-autoscale-overview#:~:text=An%20Azure%20virtual%20machine%20scale,the%20performance%20of%20your%20application.>

Something wrong with this question?

**Question 31**

**Question**

CORRECT

**Which Azure Storage service is designed for large-scale, offline data migration intended to help businesses migrate their data onto the Azure cloud?**

AzCopy

Azure Data Box

Azure Storage Explorer

StorSimple

**Explanation**

The Microsoft Azure Data Box cloud solution lets you send terabytes of data into Azure in a quick, inexpensive, and reliable way. The secure data transfer is accelerated by shipping you a proprietary Data Box storage device. Each storage device has a maximum usable storage capacity of 80 TB and is transported to your data center through a regional carrier. The device has a rugged casing to protect and secure data during the transit.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://docs.microsoft.com/en-us/azure/databox/data-box-overview>

Something wrong with this question?

**Question 32**

**Question**

CORRECT

**You suspect hackers and bots have been attacking your application's network. What Azure Network Watcher network monitoring or analysis tool would best fit your needs?**

Connection Monitor

Network Performance Monitor

Security Group View

Traffic Analytics

**Explanation**

Traffic analytics is a cloud-based solution that provides visibility into user and application activity in cloud networks. Traffic analytics analyzes Network Watcher network security group (NSG) flow logs to provide insights into traffic flow in your Azure cloud.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics>

Something wrong with this question?

**Question 33**

**Question**

CORRECT

**You want to create an alert for a virtual machine (VM) named VM1 that will be fired when the VMs central processing unit (CPU) usage is greater than 95 percent for at least 10 minutes for action group 1.**

**Which of the following command parts should be placed in the blanks below?**

az monitor metrics alert \_\_\_\_\_\_ -n A1 -g RG1 -- \_\_\_\_\_\_\_\_\_\_ "avg Percentage CPU > 95"

-- \_\_\_\_\_\_\_\_\_\_ 10m -- action AG1

create, condition, window-size

list, description, action

show, scopes, evaluation-frequency

create, description, name

**Explanation**

You should use the az monitor metrics alert "create" command to create the metric-based rule, the "condition" parameter to specify the condition that triggers the rule, and the "window-size" option to define a time window in which the value of the condition is aggregated.

"List" lists alert rules.

"Description" creates a free-text description of the rule.

"Action" defines an action group associated with an alert and is already defined as "AG1" in this example.

"Show" refers to showing a specific alert rule.

"Scopes" defines an action group associated with an alert.

"Evaluation-frequency" defines the frequency at which measured values are calculated.

"Name" assigns a name to the rule.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://learn.microsoft.com/en-us/cli/azure/monitor/metrics/alert?view=azure-cli-latest>

Something wrong with this question?

**Question 34**

**Question**

INCORRECT

**Your team is spending too much time recovering from unplanned events, specifically when small resource updates occur that disrupt service operations, or noncompliant resources are created.**

**You want to automate a process to review log data related to resource updates, to detect anomalies within the updates. You would like to utilize live dashboards to evaluate the log data quickly. What type of logs would you analyze, and with what Azure service?**

Process activity logs with Azure Event Hub.

Process diagnostic logs with Log Analytics.

Process application logs with tables in Azure Storage.

Process diagnostic logs with Power BI.

**Explanation**

Azure offers activity logs to help you track subscription level operations on resources, such as creating or updates resources. Azure Event Hubs allows you to receive thousands of log events per second and detect anomalies, and it also provides live dashboards as well.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview-activity-logs>

Something wrong with this question?

**Question 35**

**Question**

CORRECT

**Your organization's expenses have increased as operations have expanded. You need to identify expenses for Azure resources used by the IT and Development departments of your organization.**

**Which Azure service or tool should you use to better understand your organization's resource expenses by department?**

Azure Advisor

Azure Budget

Azure Price Calculator

Azure Resource Tags

**Explanation**

Another way to track Azure costs is by using tags. Tags can be applied to Azure resources as a means of grouping them for things like cost tracking. Tags can be applied based on department, project, environment, or any other purpose.

Each tag is a name/value pair where the name defines the type, or category of the tag, and the value identifies a specific instance of that type. For example, a tag name could be a department, and values could then be IT and Development.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags>

Something wrong with this question?

**Question 36**

**Question**

CORRECT

**A company wants to use Azure blob storage. For disaster recovery purposes, data copies should be maintained in different regions. In the event of heavy traffic, the company would like to partially offload read requests to a secondary region. As an Azure administrator, what can you do to achieve this requirement?**

Create the Azure Storage account with the default settings. Copy the data within blob storage to another region. Create a PowerShell script to synchronize the data.

Create the Azure Storage account with the default settings. Copy the data within blob storage to another region. Create a program to synchronize the data because PowerShell cannot be used with blob storage service.

Create the Azure Storage account with the replication attribute set to read-access geo-redundant storage (RA-GRS).

Create the Azure Storage account with the replication attribute set to geo-redundant storage.

**Explanation**

When a storage account is created, one can select the following replication options: Locally redundant storage (LRS), Zone-redundant storage (ZRS), geo-redundant storage (GRS),  or read-access geo-redundant storage (RA-GRS). The read-access geo-redundant storage allows copies of blob storage to be replicated to various regions. It also allows for a read-only copy to be accessed from another region.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://docs.microsoft.com/en-us/azure/storage/storage-redundancy>

Something wrong with this question?

**Question 37**

**Question**

CORRECT

**Your organization has a Microsoft 365 tenant and an Azure Active Directory (Azure AD) tenant named organization1.com. The company uses several Azure Files shares. Each share is assigned to a different department in the organization. The department attribute in Azure AD is populated for all users.**

**You need to ensure that the users can access the departmental file shares. Your solution must minimize administrative effort.**

**Which types of groups should you use? (Choose 2 answers)**

A security group that uses the dynamic membership type

A distribution group

A Microsoft 365 group that uses the dynamic membership type

A Microsoft 365 group that uses the assigned membership type

**Explanation**

You should use a security group that uses the dynamic membership type and a Microsoft 365 group that uses the dynamic membership type because these are groups that use dynamic membership rules and therefore reduce the cost of access management by providing attribute-based membership and access to resources. Membership rules allow for the membership and resulting access to be granted and removed automatically.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership>

Something wrong with this question?

**Question 38**

**Question**

INCORRECT

**Your application requires a high number of IOPS to satisfy minimum performance thresholds. You have selected Premium disks, and are now reviewing replication options.**

**Which replication options offer the most redundancy, based on your selection of Premium disks? (Choose 2 answers)**

LRS

GRS

RA-GRS

ZRS

**Explanation**

Azure Premium Disk Storage currently supports only locally redundant storage (LRS). Block blob storage accounts support locally redundant storage (LRS) and zone redundant storage (ZRS) in certain regions.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://learn.microsoft.com/en-us/azure/storage/common/storage-redundancy>

Something wrong with this question?

**Question 39**

**Question**

INCORRECT

**You want your application tier to automatically scale based on changes in demand. After reviewing usage reports with your historic CPU metrics, you know your baseline traffic will require three VM instances. However, the workload can randomly spike to triple the baseline amount.**

**You want to configure auto scaling to respond quickly to increases in traffic and respond gradually to decreases. The application tier is the only tier that needs to auto scale. You would like to ensure your instances remain available in the event of data center maintenance or a data center outage.**

**How can you accomplish this?**

Create a Virtual Machine Scale Set and set the "Limit to Single Placement Group" to 'true,' and enable Auto Scaling. Set your minimum number of instances to '3', and your maximum to '9'. Set your scale-out rate to '2', and scale-in rate to '1'.

Create a Virtual Machine Scale Set and set the "Limit to Single Placement Group" to 'false,' and enable Auto Scaling. Set your minimum number of instances to '3', and your maximum to '9'. Set your scale-out rate to '1', and scale-in rate to '2'.

Create a Virtual Machine Scale Set and set the "Limit to Single Placement Group" to 'true,' and enable Auto Scaling. Configure three fault domains and ten update domains for your scale set. Set your minimum number of instances to '3', and your maximum to '12'. Set your scale-out rate to '2', and scale-in rate to '1'.

Create a Virtual Machine Scale Set and set the "Limit to Single Placement Group" to 'false,' and enable Auto Scaling. Set your minimum number of instances to '3', and your maximum to '12'. Set your scale-out rate to '1', and scale-in rate to '2'.

**Explanation**

The key concerns in the question are:

* The minimum should be set to 3, with a maximum of 9.
* Your scale-out rate should be higher than your scale-in rate.
* You do not need to configure the number of fault domains and update domains in a Scale Set.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: [/course/azure-resource-manager-virtual-machines/demo-implement-vm-scaleset-autoscaling-1/](https://cloudacademy.com/course/azure-resource-manager-virtual-machines/demo-implement-vm-scaleset-autoscaling-1/)

Something wrong with this question?

**Question 40**

**Question**

CORRECT

**Several Azure resources that you own were recently deleted from a production environment.**

**Your company's IT staff includes several hundred people, including temporary staff whose roles and authorized permissions quickly change from project to project.**

**As an Azure Resource Owner at a resource group scope, what steps are you authorized to take to best prevent deletion of Azure resources deployed in production environments, and resources deployed in the future?**

Automate an Azure AD Connect sync on a weekly basis. Institute conditional access requirements for all authorized devices, and require MFA based on role.

Assign a resource lock to each deployed resource you own and include resource locks for your resources in production environment ARM templates.

Update the Azure resource policy to each resource you own and include the policy for your resources in production environment ARM templates.

Update the Azure resource policies for all resources that directly handle ARM templates to prevent accidental resource deletion.

**Explanation**

To correctly answer this question, you should have a basic understanding of common roles in Microsoft Azure, the scope of actions those roles can perform, and what each service or mechanism involved in the question can accomplish.

As a Resource Owner, you would not necessarily be able to change policy or implement locks at the subscription level. You are also not likely to be able to institute more stringent requirements in Azure AD to require conditional access and MFA.

You can assign resource policies to your current resources, and include them in templates, but this will not actually prevent resource deletion. Resource locks are the only tool at your disposal to address the problem directly with your level of authority.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: [/course/managing-azure-subscriptions-resource-groups/resource-locks/](https://cloudacademy.com/course/managing-azure-subscriptions-resource-groups/resource-locks/)

Something wrong with this question?

**Question 41**

**Question**

INCORRECT

**Your work for a company with an Azure subscription.**

**You have created multiple management groups under your Root Management Group. You are modifying the management groups and want to unlink a subscription and a management group without deleting either the subscription or the management group.**

**Which PowerShell cmdlet should you use?**

Remove\_AzManagementGroup

Remove\_AzManagementGroupSubscription

Update\_AzManagmentGroup

New\_AzManagementGroupDeployment

**Explanation**

The Remove-AzManagementGroupSubscription cmdlet removes a Subscription from a Management Group, as in the example below.

Remove-AzManagementGroupSubscription -GroupName "TestGroup" -SubscriptionId 2120692d-35c3-44c8-81f5-631fa7351726

The cmdlet does not delete the subscription or the management group.

You would not use the Remove\_AzManagementGroup cmdlet because it would delete the management group.

You would not use the Update\_AzManagmentGroup cmdlet because it is used to update parameters such as the management group display name.

You would not use the New\_AzManagementGroup cmdlet because it is used to add a deployment to a management group.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://learn.microsoft.com/en-us/powershell/module/az.resources/remove-azmanagementgroupsubscription?view=azps-9.2.0&viewFallbackFrom=azps-5.8.0&tryIt=true&source=docs#code-try-1>

Something wrong with this question?

**Question 42**

**Question**

INCORRECT

**You are building a group of 10 virtual machines and putting them into an availability set to ensure high availability.  You configure the maximum number of fault domains available in your desired region, which is three.  How many of your virtual machines will end up in the first fault domain?**

4

3

5

10

**Explanation**

The maximum number of fault domains available are 3, but depends on the region. When the number of virtual machines exceeds the number of fault domains, and their number is for example 3, the 4th VM will be placed into the first fault domain, while the 5th VM will be placed into the second domain, etc. Hence the 10th VM will end up in the first fault domain.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/manage-availability>

Something wrong with this question?

**Question 43**

**Question**

INCORRECT

**You are an Azure administrator for a company with 10 different departments.**

**The company has an Azure subscription that contains 400 virtual machines (VMs). Users in each department use only their department's virtual machines.**

**You need to apply resource tags for each department to the virtual machines.**

**Which of these should you use? (Choose two answers.)**

App registrations

Azure Advisor

PowerShell

Azure Resource Manager (ARM) templates

**Explanation**

You should use PowerShell or ARM templates to apply tags to VMs which will allow you to create reports and dashboards for alerts and management.

You should not use app registrations to apply tags because app registrations apply to separate slots or environments in App Service deployments.

You should not use Azure Advisor because it is a tool for use in evaluating your Azure environment and not for tagging resources.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/decision-guides/resource-tagging/>

Something wrong with this question?

**Question 44**

**Question**

INCORRECT

**What is not a requirement to deploy Azure AD Join?**

An Azure AD subscription

An Azure AD Premium subscription

Mobile device management

A deployment of Azure AD Connect

**Explanation**

To deploy Azure AD Join for any set of users you need the following:

* An Azure AD subscription.
* An Azure AD Premium subscription, such as mobile device management auto-enrollment, if you require more capabilities.
* Mobile device management--for example, a Microsoft Intune subscription, mobile device management for Office 365, or any of the partner mobile device management vendors that integrate with Azure AD.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://azure.microsoft.com/en-us/documentation/articles/active-directory-azureadjoin-windows10-devices/>

Something wrong with this question?

**Question 45**

**Question**

INCORRECT

**want to connect the Azure VNets for three separate branc Azure virtual machines (VMs) for a new web service. You now want to add these virtual machines to fault domains in an availability set. When you attempt to do this in the portal, you receive an error message preventing you from completing the task.**

**What is the reason for this?**

You did not check the required “Standalone” parameter in Azure Portal

You may not add running standalone VMs to availability sets

The VMs operating system is not compatible with fault domains.

The availability set has to be paused or stopped before standalone VMs can be added.

**Explanation**

Creating an Availability Set is a pretty simple, straightforward process. However, the caveat is getting your VMs to be part of an availability set. If you have existing VMs that are not part of an availability set, we refer to these as Standalone VMs. You may not simply take standalone VMs and move them into availability sets because this has to be done at the time of VM creation.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4354831/)

Learn more: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/change-availability-set>

**Covered in this lecture**

**[DEMO: Deploying and Connecting to a Windows Virtual Machine via the Azure Portal](https://cloudacademy.com/course/getting-started-with-azure-virtual-machines-988/demo-deploying-and-connecting-to-a-windows-virtual-machine-via-the-azure-portal/)**

[Course](https://cloudacademy.com/course/getting-started-with-azure-virtual-machines-988/demo-deploying-and-connecting-to-a-windows-virtual-machine-via-the-azure-portal/)

**[Getting Started with Azure Virtual Machines](https://cloudacademy.com/course/getting-started-with-azure-virtual-machines-988/demo-deploying-and-connecting-to-a-windows-virtual-machine-via-the-azure-portal/)**

[Time](https://cloudacademy.com/course/getting-started-with-azure-virtual-machines-988/demo-deploying-and-connecting-to-a-windows-virtual-machine-via-the-azure-portal/)

**[26m 18s](https://cloudacademy.com/course/getting-started-with-azure-virtual-machines-988/demo-deploying-and-connecting-to-a-windows-virtual-machine-via-the-azure-portal/)**

**Question 1**

**Question**

INCORRECT

**You are a start-up company currently hosting two small web applications, Web App 1 and Web App 2, on Azure Web Apps. Your Web Apps run on three instances on a Basic app service plan. You need to manage both web apps to meet the following requirements:**

* **Allow Web App 1 to scale from 5-8 instances based on application workload, as traffic for this web app is growing.**
* **Maintain Web App 2 on three separate instances, as this application is also growing more popular. However, Web App 2 does not require scaling capabilities yet.**

**What steps would be most cost-effective and meet your application requirements?**

Move Web App 1 to a separate Standard app service plan. Configure auto scaling for Web App 1 between a range of 5 to 8 instances based on application metrics. Keep your existing Basic app service plan for Web App 2.

Scale up to a Premium app service plan. Leave Web App 2 as it is currently configured. Configure auto scaling for Web App 1 between a range of 5 to 8 instances based on application metrics.

Move Web App 1 to a separate Premium app service plan. Configure auto scaling for Web App 1 between a range of 5 to 8 instances based on application metrics. Scale your Basic app service plan down to a Shared service plan for Web App 2.

Move Web App 1 to a separate Premium app service plan. Configure auto scaling for Web App 1 between a range of 5 to 8 instances based on application metrics. Scale up your existing service plan from Basic to Standard for Web App 2.

**Explanation**

App Service plans are containers for the apps that you deploy in App Service. App Service plans are offered in different tiers, with more functionality provided by higher, more expensive tiers. The following list highlights some of the distinctions between the available tiers:

* Free (Windows only): Run a small number of apps for free
* Shared (Windows only): Run more apps and provides support for custom domains
* Basic: Run unlimited apps and scale up to three instances with built-in load balancing
* Standard: The first tier that is recommended for production workloads. It scales up to ten (10) instances with Autoscaling support and VNet integration to access resources in your Azure virtual networks without exposing them to the internet
* Premium: Scale up to 20 instances and additional storage over the standard tier
* Isolated: Scale up to 100 instances, runs inside of an Azure Virtual Network isolated from other customers, and supports private access use cases

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more: [/lab/deploying-monitoring-azure-app-service-web-apps/creating-azure-app-service-plan/](https://cloudacademy.com/lab/deploying-monitoring-azure-app-service-web-apps/creating-azure-app-service-plan/)

**Question 2**

**Question**

CORRECT

**You have specified auto scaling rules for an image processing application hosted on virtual machines. The application receives messages from Azure storage queues when images need to be processed.**

**The virtual machines are grouped into a scale set with the following Scale Out rules:**

1. **Scale out one VM if CPU utilization is above 60 percent.**
2. **Scale out two VMs if CPU utilization is above 80 percent.**
3. **Scale out one VM if disk writes per second reach 65 percent capacity.**
4. **Scale out two VMs if disk writes per second reach 85 percent capacity.**
5. **Scale out one VM if the message queue length reaches more than 700.**
6. **Scale out two VMs if the message queue reaches more than 1000.**

**The following Scale In rules are also applied:**

1. **Scale in one VM if CPU utilization drops below 35 percent.**
2. **Scale in two VMs if CPU utilization drops below 20 percent.**
3. **Scale in one VM if your message queue has fewer than 100 messages.**

**The app's CPU utilization is currently at 30 percent, and the message queue contains 735 messages.**

**Based on these metrics, what auto scaling action(s) will your application perform?**

It will scale out one virtual machine.

It will scale up one virtual machine.

It will scale in one virtual machine.

It will scale down one virtual machine.

**Explanation**

First and foremost, scale-out operations always have priority over scale-in operations. Anytime that multiple scale-out operations conflict with one another, the rule that takes precedence will be the one that initiates the largest increase in the number of instances. When it comes to scale-in conflicts, the rule that initiates the smallest decrease in the number of instances will take precedence. So, it will scale out one virtual machine due to the number of messages in the message queue.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more: [/course/advanced-vm-management-in-azure-1020/virtual-machines-scale-sets/](https://cloudacademy.com/course/advanced-vm-management-in-azure-1020/virtual-machines-scale-sets/)

**Question 3**

**Question**

INCORRECT

**A company's app hosted in Azure is using the App Service. They want this app to interface with another application in another domain. Which of the below configurations will make this possible?**

Enable CORS for the App Service.

Enable Autoscale for the App Service.

Enable OAuth for the App Service.

Enable API Definition for the App Service.

**Explanation**

App Service offers support for Cross Origin Resource Sharing (CORS), which enables JavaScript clients to make cross-domain calls to APIs that are hosted in API apps. App Service lets you configure CORS access to your API without writing any code in your API.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more:

**Question 4**

**Question**

INCORRECT

**A company's current on-premise application runs on TCP protocol. The company has decided to move this application to Azure, and to use a cloud-based load balancer of some kind set up in Azure for the application. How would you efficiently set up a load balancer for this application?**

Create an Application Gateway. Add the necessary configuration to load balance the application based on the TCP protocol.

Create a NAT Instance. Route the traffic via the NAT instance to a custom load balancer.

Use Azure Load Balancer with the necessary configuration to load balance the application based on the TCP protocol.

Use Azure Load Balancer, but change the application to use the HTTP protocol since there is no support for TCP in Azure Load Balancers.

**Explanation**

Since the application works on the TCP protocol, Azure Load Balancer is a logical choice because it works at the TCP level. Application Gateway can also manage load balancing, but is designed for layer 7 or HTTP/HTTPS traffic. Hence that would not be suited for this requirement.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more: <https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview>

**Covered in this lecture**

**[AWS API Gateway, VPC Private Links, and NLBs](https://cloudacademy.com/course/course-automatically-created-2018-10-02-113135226141/c3l9-apigateway2/)**

[Course](https://cloudacademy.com/course/course-automatically-created-2018-10-02-113135226141/c3l9-apigateway2/)

**[.Net Microservices - Build Deployment and Hosting - Course Two](https://cloudacademy.com/course/course-automatically-created-2018-10-02-113135226141/c3l9-apigateway2/)**

[Time](https://cloudacademy.com/course/course-automatically-created-2018-10-02-113135226141/c3l9-apigateway2/)

**[23m 16s](https://cloudacademy.com/course/course-automatically-created-2018-10-02-113135226141/c3l9-apigateway2/)**

**Question 5**

**Question**

INCORRECT

**Your Chief Technology officer wants to manage the Azure Virtual Machine (VM) infrastructure by establishing a baseline, high-level standard of quality for all the resources in your environment.**

**What tool can be used to implement this request?**

VM Access extension

Azure VM agent extension

PowerShell DSC

Bitlocker

**Explanation**

Configuration Management deals with establishing a baseline, high-level standard of quality for all the resources in your environment. In this scenario, you will want to maintain the highest level of quality and serviceability of your virtual machines. There are several Configuration Management options in the Portal. PowerShell Desired State Configuration is one such tool. Different Configuration Management tools have different ways of implementing this desired state file, however, most tools are based on industry standards such as MOF or the Managed Object Format (MOF).

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more: <https://msdn.microsoft.com/en-us/powershell/dsc/overview>

**Question 6**

**Question**

CORRECT

**A company is hosting a set of resources using Azure Storage services. An external vendor needs temporary access to these resources. Which of the options below is recommended to provide access?**

Create a Virtual machine, copy the data and then provide access to the data.

Copy the data to another storage account and provide the necessary access.

Provide the storage account keys to the vendor so that they can access the resources.

Create a Shared Access Signature and provide it to the vendor.

**Explanation**

A shared access signature is a safe way to provide access to external parties for resources hosted in a storage account. It is not recommended to provide direct access keys to the person for accessing the relevant data in the storage account. Instead, you can create a shared access signature that provides delegated access to resources in your storage account.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more: <https://docs.microsoft.com/en-us/azure/storage/storage-dotnet-shared-access-signature-part-1>

**Question 7**

**Question**

CORRECT

**Reviewing your recently launched application, you notice several changes that could affect performance or security. You are concerned that the IT management team is not reviewing corporate requirements in these areas.**

**You want to automate a process to review Azure resources, including storage accounts and VMs, against the rules you specify. You want to be automatically notified of any noncompliance.**

**What steps can you take to accomplish this goal?**

Create resource policies with Azure Policy.

Implement 'Read-Only' resource locks.

Create alerts using Azure Log Analytics.

Initialize change tracking with Azure Automation and Log Analytics.

**Explanation**

Azure Policy is the only option that allows you to specify requirements and review resources against those requirements.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more: [/course/managing-azure-subscriptions-resource-groups/resource-policies/](https://cloudacademy.com/course/managing-azure-subscriptions-resource-groups/resource-policies/)

**Question 8**

**Question**

CORRECT

**Your organization wants to secure customer personal data stored within your Azure Virtual Machine (VM) environment. You suggest Azure Disk Encryption, which is an option available to both Linux and Windows VMs.**

**While the encryption process is actually pretty straightforward, and is as easy as deploying a VM extension in PowerShell, what is one caveat to the process that adds a level of complexity?**

Bitlocker enabled and Azure Backup Service are mutually exclusive processes.

Bitlocker is ineffective at encrypting the operating system.

A mechanism must be in place to manage the encryption keys for the encrypted disk.

The process of creating the encryption keys is complex.

**Explanation**

The one caveat to the Bitlocker process that adds a somewhat difficult level of complexity is managing the encryption keys that go along with encrypting your disk. After all, if you lock something away, someone has to keep track of the keys to reopen it. The good news is Azure provides what is called the Azure Key Vault service which is used to help you manage and control your disk-encryption keys and secrets used by cloud applications and services.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more: <https://docs.microsoft.com/en-us/azure/key-vault/key-vault-whatis>

**Question 9**

**Question**

CORRECT

**Your company would like your physical on-premise OLTP and OLAP database servers to failover to ARM virtual machines, in the event of a disaster. All servers must have managed disks. OLTP servers require premium SSD disks, while OLAP require standard SSD disks.**

**They have drawn up the following requirements:**

1. **OLTP databases require a minimal RTO.**
2. **OLAP databases require a minimal RPO.**
3. **The ARM virtual machines would need to be entirely replicated on Azure before failback to on-premise servers are initiated.**
4. **The ARM virtual machines backups would need to be able to survive a regional outage.**

**Which Azure services will you need to configure to correctly implement this disaster recovery plan? (Choose 3 answers)**

Azure Site Recovery

Azure Storage

Azure Stack Edge

Azure Backup

**Explanation**

All of the services would be necessary except for Azure Stack Edge.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more: [/course/designing-an-azure-compute-infrastructure/azure-backup/](https://cloudacademy.com/course/designing-an-azure-compute-infrastructure/azure-backup/)

**Question 10**

**Question**

INCORRECT

**Five developers in your company need to be able to connect to several application tier VMs. Your management team is concerned about security and doesn't want everyone to have access to all of the VMs. Which of the following network connections would be best in this scenario?**

A point-to-site VPN

A point-to-point VPN

A site-to-site VPN

An ExpressRoute connection

**Explanation**

Point-to-site VPNs allow you to connect a single client to a virtual network. You can create multiple point-to-site VPNs to assist in these types of situations, and for just a few connections this makes for a viable option. However, once you need a large number of connections, you'll want to consider a site-to-site VPN.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more: <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways#site-to-site-and-multi-site-connections>

**Question 11**

**Question**

INCORRECT

**Which statement regarding best practices to address transient errors in Azure Storage is *incorrect*?**

Retrying the failed operation is recommended.

Azure Storage Emulator is useful for debugging your storage service in a simulated environment.

Unbound parallelism in requests can cause your application to error or fail.

The linear approach is recommended in favor of an exponential backoff approach in addressing these error types.

**Explanation**

The linear approach will retry the same request over and over again with a fixed time duration between attempts, or worse, no delay at all, which can and often will have the effect of swamping an already overburdened service with additional requests.

At best, the continued stress will cause the service to take longer to recover; at worst, it will fall over in the face of a request load it simply can't handle. A better solution is to use an exponential backoff strategy where retries occur a fixed number of times with an increasing delay placed between each subsequent request.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more: <https://docs.microsoft.com/en-us/azure/storage/blobs/storage-performance-checklist#timeout-and-server-busy-errors>

**Question 12**

**Question**

CORRECT

**What extension should be enabled for Azure Scale sets to auto scale based on in-guest virtual machine metrics?**

Azure Diagnostics Extension

Azure DCS Extension

Azure VM Extension

Azure Custom Script Extension

**Explanation**

Automatic scaling can only be done if metrics collection is successful on each virtual machine in the scale set. The Azure Diagnostics Extension provides the monitoring and diagnostics capabilities that meet the metrics collection needs of the autoscale resource.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more:

**Question 13**

**Question**

CORRECT

**Your organization wants to connect two Azure networks using an Azure VPN Gateway. Which connection method can you implement to meet this requirement?**

An Azure Hybrid network

An Azure Accelerated Network

A VNet Peering connection

A VNet-to-VNet connection

**Explanation**

VNet Peering is an Azure-to-Azure connection which does not have to use VPN Gateways for connectivity across Azure VNets. If you did want to use Azure VPN Gateways, like in the case of on-premises connectivity, you can still do this between two Azure networks in what's called a VNet-to-VNet connection. VNet-to-VNet connectivity utilizes the Azure VPN gateways to connect two or more virtual networks together securely with IPsec/IKE S2S VPN tunnels.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more:

**Question 14**

**Question**

INCORRECT

**Your company is migrating to the cloud and wants to replicate its on-premises network in Azure. The company plans to use Azure Virtual Networks to place resources in virtual networks and subnets.**

**You are working on the design for the company IP address schema and need to map out which ranges can be assigned to the HR department.**

* **The HR department has a subnet with an address range of 10.3.0.0/16.**

**Which IP address can be dynamically assigned to the HR department?**

10.3.0.2

10.3.255.254

10.3.255.255

10.3.0.1

**Explanation**

Any address in the range of 10.3.04 through 10.3.255.254 is available for assignment.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more:

**Question 15**

**Question**

CORRECT

**You would like to implement a hub-and-spoke VNet peering connection between two of your virtual networks, VNet1 in the East US region and VNet2 in the East US-2 region, using a network virtual appliance (NVA).**

**You have deployed VNet3 to serve as the network hub, and a custom Linux virtual machine in VNet3 to serve as the NVA.**

**How should you configure route tables to support communication between the VNets with this particular hub-and-spoke architecture?**

Create route tables with user-defined routes in VNet1 and VNet2 listing the Linux VM router as a next hop.

Create route tables with user-defined routes in VNet1 and VNet2 listing the VNet3 CIDR block address range as the destination.

Create route tables with user-defined routes in VNet1 and VNet2 listing an internal load balancer in VNet3 as a next hop.

Create a route table for VNet1 with user-defined routes to the VNet2 CIDR block range. Create a second route table for VNet2 with user-defined routes to the VNet1 CIDR block range.

**Explanation**

To create a Hub-and-Spoke VNet peering connection with an NVA, you would need to:

* Create a peering connection between the destination VNets with forwarded traffic enabled.
* Deploy a Linux VM to a separate hub VNet.
* Create route tables with user-defined routes in the destination VNets.
* Include the Linux VM in the hub VNet as a next hop.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more:

**Question 16**

**Question**

CORRECT

**Your company has virtual machines hosted in Azure as well as on premise, and needs to share files across the virtual machines. Which storage option would best meet this requirement?**

Store the files using Blob storage.

Store the files using File storage.

Store the files using Table storage.

Store the files using Queue storage.

**Explanation**

Azure File storage is specifically meant for File shares, in contrast to other storage services. The Azure File service exposes file shares using the standard SMB 2.1 protocol. Even files from on-premise locations can be copied to the Azure file storage service and subsequently can be accessed by the virtual machines hosted in Azure.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more:

**Question 17**

**Question**

INCORRECT

**Your budget limits you to five application tier VMs without any ability to scale. You need to keep all VMs within one region, based on your current customer base's location. Given these limitations, you still want to limit the effects of Azure server maintenance or data center outages as much as possible.**

**How should you configure your resources to support this?**

Create an availability set and configure three fault domains and five update domains within it. Deploy your VMs into the availability set.

Create one availability set within a VNet. Configure five placement groups in the availability set. Deploy one VM in each placement group.

Create an availability set and configure five fault domains and five update domains. Deploy the VMs into the availability set.

Create two availability sets in separate resource groups in the same VNet. Configure three fault domains and update domains in one availability set, and two fault domains and update domains in the other availability set. Deploy three VMs in one availability set, and two VMs in the other availability set.

**Explanation**

Availability Sets offer an increased amount of availability and fault tolerance by dividing VMs into separate fault domains and update domains. Multiple availability sets can be launched within the same virtual network, but are limited to a maximum of three fault domains per availability set.

Placement groups are designed for Virtual Machine Scale Sets and cannot be launched inside availability sets.

Another key factor to bear in mind - creating two availability sets with separate fault domains in the same region does not increase your availability because although the availability sets are separate, they are linked to the same data center.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more:

**Question 18**

**Question**

INCORRECT

**An Azure subscription named Subscription 1 contains three resource groups named Development, Test, and Production. Two users, Thomas and Guy, are assigned to an Azure Active Directory group named Group 1.**

**All members of Group 1 can perform all read and write operations on all virtual machines in the Development and Test resource groups. However, they are prevented from performing any operations on virtual machines in the Production resource group through NotActions.**

**Guy is also assigned a second custom resource role, called ProductionVM\_Review. The ProductionVM\_Review role allows him to perform all read operations on all virtual machines in the Production resource group.**

**If Guy tries to perform a programmatic read operation on all virtual machines within Subscription 1, which of the following outcomes will occur?**

Azure Active Directory will allow the operation on all virtual machines.

Azure Active Directory will allow the operation on virtual machines for the Development and Test resource groups only.

Azure Active Directory will allow the operation on virtual machines for the Production resource group only.

Azure Active Directory will deny the operation on all virtual machines.

**Explanation**

Guy has two assigned roles that apply to him, where the NotActions of one role contradict the Actions of the other. So which wins?

Actions overrule NotActions, so Guy will be able to perform the read operation on all virtual machines, including those in the Production resource group.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more:

**Question 19**

**Question**

CORRECT

**Which Microsoft Azure Active Directory solution should you use to enable a cloud identity management solution for your consumer-facing web and mobile applications?**

Azure Active Directory B2C

Azure Active Directory

Azure Active Directory Domain Services

Azure Multi-Factor Authentication

**Explanation**

In the past, application developers who wanted to sign up and sign in consumers to their applications would have written their own code. And they would have used on-premises databases or systems to store usernames and passwords. Azure Active Directory B2C offers developers a better way to integrate consumer identity management into their applications with the help of a secure, standards-based platform and a rich set of extensible policies. When you use Azure Active Directory B2C, your consumers can sign up for your applications by using their existing social accounts (Facebook, Google, Amazon, LinkedIn) or by creating new credentials (email address and password, or username and password); we call the latter "local accounts."

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more:

**Question 20**

**Question**

INCORRECT

**Which feature in Azure AD allows you to restrict access to devices and applications based on predefined rules?**

Role-Based Access and Control (RBAC)

Multi-Factor Authentication (MFA)

Conditional Access

Azure AD Connect

**Explanation**

Conditional Access allows you to restrict access to devices and applications based on predefined rules.  RBAC only controls user access to resources.  MFA deals with authenticating user sign-in, and Azure AD Connect is a tool for Synchronizing On-premises Identity with Azure AD and monitoring.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more:

**Question 21**

**Question**

INCORRECT

**There are several virtual machines (VMs) deployed in your Azure subscription. The VMs are connected to different virtual networks (VNets). You have configured custom filtering rules on the VNets.**

**You deploy an additional VM named VM02 in a new VNet named VNet02. VM02 is experiencing connectivity issues. You use Network Watcher to troubleshoot connectivity.**

**Which cmdlets should you use to determine which filtering rule is causing the issue? (Choose 2 answers)**

Get-AzEffectiveNetworkSecurityGroup

Get-AzNetworkSecurityGroup

Test-AzNetworkWatcherIPFlow

Test-AzNetworkWatcherConnectivity

**Explanation**

To determine why the rules in Test network communication are allowing or preventing communication, you should review the effective security rules for the network interface with Get-AzEffectiveNetworkSecurityGroup:

Get-AzEffectiveNetworkSecurityGroup `

  -NetworkInterfaceName myVm `

  -ResourceGroupName myResourceGroup

The Get-AzEffectiveNetworkSecurityGroup cmdlet tests the outbound connection from the source VM and source port to the destination IP address and port using the Transmission Control Protocol (TCP). If any of the filtering rules block traffic between the endpoints that you configured in the invocation of the cmdlet, it returns the name of the network security group (NSG) that contains the filtering rule that denied the communication.

You should also use the Test-AzNetworkWatcherIPFlow cmdlet for a specified VM resource and a packet with specified direction using local and remote, IP addresses and ports to return whether the packet is allowed or denied.

For example, the following command gets the Network Watcher in West Central US for this subscription, then gets the VM and its associated Network Interfaces. Then for the first Network Interface, runs Test-AzNetworkWatcherIPFlow using the first IP from the first Network Interface for an outbound connection to an IP on the internet:

$nw = Get-AzResource | Where-Object {$\_.ResourceType -eq "Microsoft.Network/networkWatchers" -and $\_.Location -eq "WestCentralUS" }

$networkWatcher = Get-AzNetworkWatcher -Name $nw.Name -ResourceGroupName $nw.ResourceGroupName

$VM = Get-AzVM -ResourceGroupName testResourceGroup -Name VM0

$Nics = Get-AzNetworkInterface | Where-Object { $vm.NetworkProfile.NetworkInterfaces.Id -contains $\_.Id }

Test-AzNetworkWatcherIPFlow -NetworkWatcher $networkWatcher -TargetVirtualMachineId $VM.Id -Direction Outbound -Protocol TCP -LocalIPAddress $nics[0].IpConfigurations[0].PrivateIpAddress -LocalPort 6895 -RemoteIPAddress 204.79.197.200 -RemotePort 80

You should not use the Get-AzNetworkSecurityGroup cmdlet because it shows details about a specific NSG but does not provide information about the rules that affect the VM.

You should not use the Test-AzNetworkWatcherConnectivity cmdlet because it tests the outbound connectivity between a VM and a specific destination. It does not provide the name of the NSG that denied communication.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more:

**Question 22**

**Question**

CORRECT

**A company needs to connect their on-premise data centers to Azure. They have huge workloads that need to regularly transfer between on premise data centers and Azure. The company wants to avoid sending data over the public internet for security reasons. Which of the following connections should the company opt for to establish this connection?**

Create a Site-to-Site connection

Create a Point-to-Site connection

Create an ExpressRoute connection

Create a VNet-to-VNet connection

**Explanation**

An ExpressRoute connection behaves like a dedicated connection between your on-premise data center and Azure**.**TheSite-to-Site and Point-to-Site connections have to traverse the internet, and hence are not ideal when you have high workloads that need to be transferred between the on-premise and Azure location.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more:

**Question 23**

**Question**

CORRECT

**You are a systems architect for an organization with a Microsoft Azure infrastructure.**

**To maintain corporate compliance certifications, you must ensure that any new virtual machines are only created in approved Azure regions.**

**What should you do?**

Create an Azure management group.

Enforce conditional access policy in Azure Active Directory (AD).

Define and deploy a custom Azure Policy template.

Define and deploy an Azure Automation Desired State Configuration (DSC).

**Explanation**

You should define and deploy a custom Azure Policy by using JSON and Azure PowerShell. Azure Resource Manager includes a number of predefined policy templates that cover various governance use cases. However, you can also build a custom templated and upload it to Azure to make it available in your subscriptions.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more:

**Question 24**

**Question**

INCORRECT

**Which Azure service can provide performance metrics of not only solutions deployed on Azure, but also solutions hosted on-premise as well as Google Cloud and Amazon Web Services?**

Azure Application Insights

Azure Monitor

Azure Log Analytics

Azure Network Watcher

**Explanation**

Application Insights can monitor Azure deployments, as well as applications deployed within GCP, AWS and on-premise.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more: [/course/designing-for-azure-operations/designing-for-azure-operations-section1-4-app-monitoring/](https://cloudacademy.com/course/designing-for-azure-operations/designing-for-azure-operations-section1-4-app-monitoring/)

**Covered in this lecture**

**[App Monitoring](https://cloudacademy.com/course/designing-for-azure-operations/designing-for-azure-operations-section1-4-app-monitoring/)**

[Course](https://cloudacademy.com/course/designing-for-azure-operations/designing-for-azure-operations-section1-4-app-monitoring/)

**[Designing for Azure Operations](https://cloudacademy.com/course/designing-for-azure-operations/designing-for-azure-operations-section1-4-app-monitoring/)**

[Time](https://cloudacademy.com/course/designing-for-azure-operations/designing-for-azure-operations-section1-4-app-monitoring/)

**[2m 29s](https://cloudacademy.com/course/designing-for-azure-operations/designing-for-azure-operations-section1-4-app-monitoring/)**

**Question 25**

**Question**

CORRECT

**Which Azure tool is a cloud-based, command-line service for copying and migrating data between Azure Storage accounts?**

AzCopy

Import/Export Service

Azure Data Box

Azure Storage Explorer

**Explanation**

AzCopy is a Windows command-line utility. There are multiple uses for AzCopy. For example, you can copy data into your Blob storage account from your existing general-purpose storage accounts. Additionally, you can upload data from your on-premises storage devices into your Blob storage account.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more: <https://azure.microsoft.com/en-us/documentation/articles/storage-blob-storage-tiers/#evaluating-and-migrating-to-blob-storage-accounts>

**Question 26**

**Question**

CORRECT

**If you want to review detailed information about what incoming requests have been allowed or denied by network security groups on a per-rule basis, what Network Watcher service will best assist you?**

NSG Flow Logs

Diagnostic Logs

Network Performance Monitor

IP Flow Verify

**Explanation**

Network security group (NSG) flow logs are a feature of Network Watcher that allows you to view information about ingress and egress IP traffic through an NSG.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more: <https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-overview>

**Question 27**

**Question**

INCORRECT

**You have a Linux Azure Container Group with a Single Container Instance named myCon2. The container instance uses a Docker image that has an application that uses the local file system to store users' data. Persistent storage is required to support the application.**

**You want to configure interactive persistent storage for myCon2.**

**Which of these should you use?**

Azure secret volume

Azure file share

Azure blob storage

Azure table storage

**Explanation**

By default, Azure Container Instances are stateless. If the container is restarted, crashes, or stops, all of its state is lost. To persist state beyond the lifetime of the container, you must mount a volume from an external store. As shown in this article, Azure Container Instances can mount an Azure file share created with Azure Files. Azure Files offers fully managed file shares hosted in Azure Storage that are accessible via the industry standard Server Message Block (SMB) protocol. Using an Azure file share with Azure Container Instances provides file-sharing features similar to using an Azure file share with Azure virtual machines.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more: <https://learn.microsoft.com/en-us/azure/container-instances/container-instances-volume-azure-files>

**Question 27**

**Question**

INCORRECT

**You have a Linux Azure Container Group with a Single Container Instance named myCon2. The container instance uses a Docker image that has an application that uses the local file system to store users' data. Persistent storage is required to support the application.**

**You want to configure interactive persistent storage for myCon2.**

**Which of these should you use?**

Azure secret volume

Azure file share

Azure blob storage

Azure table storage

**Explanation**

By default, Azure Container Instances are stateless. If the container is restarted, crashes, or stops, all of its state is lost. To persist state beyond the lifetime of the container, you must mount a volume from an external store. As shown in this article, Azure Container Instances can mount an Azure file share created with Azure Files. Azure Files offers fully managed file shares hosted in Azure Storage that are accessible via the industry standard Server Message Block (SMB) protocol. Using an Azure file share with Azure Container Instances provides file-sharing features similar to using an Azure file share with Azure virtual machines.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more: <https://learn.microsoft.com/en-us/azure/container-instances/container-instances-volume-azure-files>

**Question 28**

**Question**

CORRECT

**What is the function of the outputs section of an Azure Resource Monitor template?**

It specifies the resources to deploy.

It returns values from deployed resources.

It defines previously used values.

It lists additional available resources.

**Explanation**

The outputs section returns values from any resources that have been deployed.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more: <https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/best-practices>

**Question 29**

**Question**

INCORRECT

**When running multiple environments of a given Azure App Service application, what deployment slot option allows you to test configuration elements and ensure that your application works as expected before being pushed to production?**

Swap with Preview

Staging Swap

Check 'Slot Setting' box

Swap App Settings

**Explanation**

Swap with preview, or multi-phase swap, simplify validation of slot-specific configuration elements, such as connection strings. For mission-critical workloads, you want to validate that the app behaves as expected when the production slot's configuration is applied, and you must perform such validation before the app is swapped into production. Swap with preview is what you need.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more: <https://docs.microsoft.com/en-us/azure/app-service-web/web-sites-staged-publishing>

**Question 30**

**Question**

CORRECT

**You would like to implement a Hub-and-Spoke VNet peering connection between two existing VNets in the East US region, (VNet 1 and VNet2), without using a network virtual appliance. You want resources in VNet1 and VNet2 to be able to communicate.**

**You have deployed VNet3 in the East US region that will serve as a hub between the other VNets. VNet1 and VNet2 should be able to communicate with each other through VNet3 using a VPN virtual network gateway.**

**Which VNet peering connections should be configured to allow gateway transit?**

All peering connections between the hub and spokes

No peering connections

Only peering connections directed to VNet3 as the hub

Only peering connections directed to VNet1 and VNet2 as the spokes

**Explanation**

Suppose you have several spokes that need to connect with each other. In that case, you'll run out of possible peering connections quickly, because the number of virtual network peerings per virtual network is limited. (For more information, see Networking limits. In this scenario, consider using user-defined routes (UDRs) to force traffic destined to a spoke to be sent to Azure Firewall or a network virtual appliance acting as a router at the hub. This change will allow the spokes to connect to each other.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more: <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke?tabs=cli>

**Question 31**

**Question**

INCORRECT

**Your company has resources in both Azure Infrastructure as a Service (IaaS) and on-premises architectures. You have an existing Azure Files Network File System version 4.1 (NFSv4.1). You have been asked to migrate the local-redundant storage (LRS) to zone-redundant storage (ZRS).**

**You want to maintain maximum control over the migration, and it must be completed by a date specified by management.**

**You need to select a supported method to complete the migrations.**

**What should you do?**

Request a live migration.

Perform the migration using PowerShell.

Perform a manual migration.

Perform the migration via the Azure portal.

**Explanation**

A manual migration from LRS to ZRS is the method for migrating Azure File Network File System version 4.1 NFSv4.1 shares in this scenario. A manual migration provides more flexibility and control than a conversion. You can use this option if you need the migration to be complete by a specific date, or if conversion is not supported for your scenario. Manual migration is also useful when moving a storage account to another region. See Move an Azure Storage account to another region for more details.

You must perform a manual migration if:

* You want to migrate your storage account to a different region.
* Your storage account is a block blob account.
* Your storage account includes data in the archive tier and rehydrating the data is not desired.

You should not request a live migration in this scenario because Azure Files NFSv4.1 share migrations are not supported.

It is not possible to perform the migration from LRS to ZRS using PowerShell because it supports only LRS to GRS and LRS to RA-GRS migrations.

The Azure Portal supports LRS migrations to geo-redundant (GRS) and read-access geo-redundant (RA-GRS) storage.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more: <https://learn.microsoft.com/en-us/azure/storage/common/redundancy-migration?tabs=portal#customer-initiated-conversion-preview>

**Question 32**

**Question**

INCORRECT

**You are designing a new photo editing and photo-sharing application that is integrated with social media. The storage type used for the application is critical.**

**The storage type must be ideal for frequent access, and be responsive to rapid read and write requests. In the event of a failure of some kind, you want to make sure customers can still view existing photos without interruption.**

**What storage option meets your requirements?**

Hot Page Blob Storage with RA-GRS replication

Hot Append Blob Storage with ZRS replication

Hot Block Blob Storage with GRS replication

Hot Block Blob Storage with RA-GRS replication

**Explanation**

The key to this question is understanding what strengths each type of blob storage offers, as well as the differences between the replication options and how they work.

Page blobs are the ideal type of blob storage because their strength is responding to large amounts of random read and write requests. Block and Append blobs have other strengths.

Next, zone redundant storage (ZRS), globally redundant storage, and read-access global redundant storage each replicate data across multiple areas. ZRS across zones, GRS and RA-GRS across regions. However, the objects within ZRS and GRS are not immediately accessible, but objects within RA-GRS are because it includes a readable secondary version of files on standby.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more: <https://docs.microsoft.com/en-us/azure/storage/common/storage-designing-ha-apps-with-ragrs?toc=%2fazure%2fstorage%2fqueues%2ftoc.json>

**Question 33**

**Question**

INCORRECT

**You have several VMs and the traffic to them needs to be filtered through a custom firewall virtual appliance. Which of the following is the best way to direct traffic through the virtual appliance before it reaches your virtual machines?**

User-defined routes

Network security groups

Azure Traffic Manager

Azure Application Gateway

**Explanation**

A user-defined route will allow you to filter traffic through a virtual appliance.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more: <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview>

**Question 34**

**Question**

INCORRECT

**Which of the following is not part of the default metrics for Azure Virtual machines when using the Azure Monitor service?**

PercentageCPU

Disk Read Bytes

Memory Consumed

Network Out

**Explanation**

The following are the valid metrics available for the Microsoft.Compute/virtualMachines resource:

1. Percentage CPU - The percentage of allocated compute units that are currently in use by the virtual machine(s)
2. Disk Read Bytes - Total bytes read from disk during monitoring period
3. Network Out - The number of bytes out on all network interfaces by the virtual machine(s) (Outgoing Traffic)

Even though memory consumption is not one of Azure Monitor's default metrics, you can always use the diagnostic extension available for virtual machines to pick up the memory consumption metrics.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more: <https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-supported-metrics#microsoftcomputevirtualmachines>

**Question 35**

**Question**

INCORRECT

**What should you do to configure gateway traffic to flow from spoke to hub and connect to remote networks?**

Allow all peering connections between the hub and spokes

Allow no peering connections

Configure the peering connection in the hub to allow gateway transit, and then configure the peering connection in each spoke to use remote gateways.

Configure the peering connection in the hub to allow gateway transit, the peering connection in each spoke to use remote gateways, and configure all peering connections to allow forwarded traffic.

**Explanation**

You can configure spokes to use the hub gateway to communicate with remote networks. To allow gateway traffic to flow from spoke to hub and connect to remote networks, you must:

* Configure the peering connection in the hub to allow gateway transit.
* Configure the peering connection in each spoke to use remote gateways.
* Configure all peering connections to allow forwarded traffic.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more: <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/hub-spoke?tabs=cli>

**Question 36**

**Question**

CORRECT

**You have a large amount (100 TB) of archival data that needs to be retained for several years, due to compliance requirements. You determined that Azure Storage is the best data storage solution for this dataset. Your office is connected to the internet over a low bandwidth connection that is heavily utilized. What Azure storage tool could help you move this data to Azure?**

Azure Storage Explorer

Azure CLI / Azure PowerShell

AzCopy

Azure Import/Export

**Explanation**

The Azure Import/Export service allows you to securely transfer large amounts of data to Azure blob storage by shipping hard disk drives to an Azure data center. You can also use this service to transfer data from Azure blob storage to hard disk drives and ship to your on-premises site. This service is suitable in situations where you want to transfer several terabytes (TB) of data to or from Azure, but uploading or downloading over the network is infeasible due to limited bandwidth or high network costs.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more: <https://docs.microsoft.com/en-us/azure/storage/storage-import-export-service>

**Question 37**

**Question**

CORRECT

**Your IT landscape in Azure consists of both Linux and Windows virtual machines. You configured consistent backup of Windows VMs with Azure Backup using Volume Shadow Copy Service (VSS).**

**Now you want to configure application consistent backup on the Azure Linux virtual machines. What statement below about Azure Backup on Linux virtual machines is correct?**

Linux has built in VSS that Azure Backup agent can utilize.

Linux does not require any additional configuration since backup is done transparently for the application.

Using Azure Backup on Linux requires custom pre- and post-scripts to complete application consistent backup.

Azure Backup provides scripts for open source operating systems like Linux.

**Explanation**

Azure Backup relies on the framework which can execute pre and post which will ensure that the application is consistent during every backup.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more: <https://docs.microsoft.com/en-us/azure/backup/backup-azure-vms-introduction>

**Question 38**

**Question**

INCORRECT

**You plan to use an Azure Resource Manager (ARM) template to create a Windows virtual machine.**

**You have used the automation script option and received the template from an existing resource group with one virtual machine.**

**You want to reuse this template in other deployments.**

**What should you do to ensure that all of the resources in the template will use the same location as the resource group?**

First, create a resource group in the target location by using the New-AzResourceGroup cmdlet. Then use the New-AZResourceGroupDeployment cmdlet using the newly created resource group.

Change the template file and update each location parameter with the value [resourceGroup().location].

In the Azure portal create a resource group in the target location. Then use the NewAZResourceGroupDeployment cmdlet using the newly created resource group.

Edit the parameters file and add a new parameter named location of type string with the default value of [resourceGroup().location].

**Explanation**

You should change the template file and update each location parameter with the value [resourceGroup().location]. The resourceGroup() function retrieves the resource group object that will be used to deploy the template. All resources in the template will then use the same location as the resource group.

You should not use the New-AzResourceGroup cmdlet with the location parameter to create a resource group in the target location and then use the New-AzResourceGroupDeployment cmdlet using the newly created resource group.

You should not use the Azure portal, create a resource group in the desired location, then use the New-AzResrouceGroupDeployment cmdlet using the newly created resource group. If the resource group is deployed in a different location to the location configured in the template file, the resources will be deployed in different locations.

You should not edit the parameters file and add a new parameter name location of type string with the default value [resourceGroup().location]. You also need to update the location parameter in the template file with the value [parameters('location')].

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more: <https://learn.microsoft.com/en-us/azure/azure-resource-manager/templates/syntax>

**Question 39**

**Question**

INCORRECT

**Which statements regarding resource tagging is false? (Choose 2 answers)**

Tagging a resource requires write access permission for the resource type.

Tags to a resource group are inherited by resources within the group

Tags cannot be applied to Azure Classic deployment resources.

After a resource group has been tagged, any new resources added to the resource group inherit the resource group's tags.

**Explanation**

Tags added to a resource group are not inherited by resources within the group, and will not be inherited by new resources added to the resource group.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more: [/course/managing-azure-subscriptions-resource-groups/move-resources/](https://cloudacademy.com/course/managing-azure-subscriptions-resource-groups/move-resources/)

**Question 40**

**Question**

CORRECT

**There are several mission-critical network connections between Azure IaaS Virtual Machines and Azure service endpoints in your Azure production environment. The connection health between these VMs and Azure endpoints needs to be continuously, automatically checked, and provide an alert if specific metrics approach unhealthy thresholds.**

**Which Azure Network Watcher feature would be ideal in this case?**

Connection Troubleshoot

IP Flow Verify

Connection Monitor

Traffic Analytics

**Explanation**

The connection monitor capability monitors communication at a regular interval and informs you of reachability, latency, and network topology changes between the VM and the endpoint. For example, you might have a web server VM that communicates with a database server VM. Someone in your organization may, unknown to you, apply a custom route or network security rule to the web server or database server VM or subnet.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more: <https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview>

**Question 41**

**Question**

INCORRECT

**Your subscription includes an Azure resource group named Resource Group1 with the following resources:**

* **vNet1 with a CIDR block 10.0.0.0/24 and vNet2 with a CIDR block 10.0.1.0/24**
* **There is a peering connection between vNet1 and vNet2**
* **vNet1 contains Subnet1 with CIDR range 10.0.0.32/27**
* **Subnet1 in vNet1 contains 2 Azure virtual machines with the following IP addresses**
  + **VM1 (10.0.0.35)**
  + **VM2 (10.0.0.36)**

**You must implement a new peering connection between vNet1 and vNet3. However, the vNet3 CIDR block (10.0.0.32/27) that overlaps with the CIDR block of Subnet 1.**

**What steps will you need to complete in order before you can create a peering connection between vNet1 and vNet3?**

1. Delete the peering connection between vNet1 and vNet2.
2. Terminate VM1 and VM2 virtual machines.
3. Delete Subnet1.
4. Modify the vNet1 CIDR block.
5. Terminate VM1 and VM2 virtual machines.
6. Delete Subnet1.
7. Modify the vNet1 CIDR block.
8. Delete the peering connection between vNet1 and vNet2.
9. Terminate VM1 and VM2 virtual machines.
10. Delete Resource Group1.
11. Terminate VM1 and VM2 virtual machines.
12. Delete Resource Group1.
13. Delete Subnet1.

**Explanation**

Once you have created a peering connection between two VNets, you cannot edit the address ranges for either VNet. If you need to edit the address range for any reason, you need to delete the peering connection first.

If you need to remove IP addresses from your CIDR block that are currently assigned to a subnet, the subnet needs to be deleted first, and for a subnet to be deleted, it needs to be empty.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more: [/course/azure-network-connectivity-name-resolution/virtual-network-peering/](https://cloudacademy.com/course/azure-network-connectivity-name-resolution/virtual-network-peering/)

**Question 42**

**Question**

CORRECT

**What does placing your virtual machines into an availability set accomplish regarding failures or outages?**

It limits the impact of potential physical hardware failures.

It prevents hardware failures.

It may limit the impact of network outages in the future.

It protects your application from failures, power outages or anything else.

**Explanation**

Placing two or more VMs in an availability set provides redundancy for them, and limits the impact of potential physical hardware failures.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more: <https://azure.microsoft.com/en-us/documentation/articles/automation-troubleshooting-automation-errors/>

**Question 43**

**Question**

INCORRECT

**Your manager has asked for advice on how best to fire off a console app that will nightly pick up some files that are uploaded to a Web App hosted on App Service and add them to Blob Storage. Cost and management effort are a concern.**

**Given what you know, which service would work best?**

WebJobs

Azure Logic Apps

Azure Functions

Azure Automation

**Explanation**

While there are multiple answers that would work, the answer that would be considered the "best" is the use of WebJobs.

WebJobs will have access to the files on the servers without any additional configuration. That will keep management and cost down.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more: <https://docs.microsoft.com/en-us/azure/app-service-web/web-sites-create-web-jobs>

**Question 44**

**Question**

CORRECT

**You recently implemented a new security and cost management policy. This implementation included the following tasks:**

* **Azure AD records were synced with on-premises Active Directory records;**
* **Resource owners implemented "Read Only" and "CanNotDelete" resource locks.**
* **All resources have been tagged based according to their project, environment, and cost center.**

**Now you are running into the following problem:**

* **Employees and Azure services with correctly configured read and write access permissions in Azure AD can no longer perform certain actions, such as listing relevant files in a storage container.**

**Based on the new security policy implementations, where would you check first?**

Review the resource policies in Azure Portal.

Review the most recent updates in Azure Active Directory.

Review the resource tags in Azure Portal.

Review the resource locks in Azure Portal.

**Explanation**

Each of the issues is documented directly in connection with Azure Resource Locks, so this would be the first place to check.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more: <https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources#how-locks-are-applied>

**Question 45**

**Question**

INCORRECT

**You have a two-tier application hosted within VNet-01 with an CIDR block of 10.0.0.0/16 and the following resource configurations:**

* **The front end is hosted on a VM named "VM\_Front" within a public subnet. The public subnet has an IP address range of 10.0.2.0/24. VM\_Front has a private IP address of 10.0.2.5, and a public IP address of 192.168.50.2.**
* **The backend is hosted on a second VM named VM\_Back within a private subnet. The private subnet has an IP address range of 10.0.3.0/24. VM\_Back has a private IP address of 10.0.3.4.**
* **A public load balancer with a private IP address of 10.0.1.6 and a public IP address of 172.16.50.35.**

**You are configuring a final rule for a network security group (NSG) associated with resources in the private subnet where VM\_Back is deployed. This final rule should block all traffic from the public subnet. Traffic from the public subnet that does not meet any of the NSG Allow rules would be processed by this rule.**

**Which NSG rule parameters below would meet the requirements for this NSG rule?**

Inbound Rule

Source: 10.0.2.0/24

Source Port: 0-65535

Destination: 10.0.3.4

Destination Port: 0-65535

Protocol: ANY

Priority: 4096

Action: Deny

Outbound Rule

Source: 10.0.2.0/24

Source Port: 0-65535

Destination: 10.0.3.4

Destination Port: 0-65535

Protocol: ANY

Priority: 20

Action: Deny

Inbound Rule

Source: 10.0.0.0/16

Source Port: \*

Destination: 10.0.3.4

Destination Port: \*

Protocol: ANY

Priority: 4096

Action: Deny

Outbound Rule

Source: 0.0.0.0/0

Source Port: \*

Destination: 10.0.3.4

Destination Port: \*

Protocol: ANY

Priority: 20

Action: Deny

**Explanation**

The correct NSG rule configuration is:

* Inbound Rule
* Source: 10.0.2.0/24
* Source Port: 0-65535
* Destination: 10.0.3.4
* Destination Port: 0-65535
* Protocol: ANY
* Priority: 4096
* Action: Deny

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357153/)

Learn more: [/course/implementing-azure-network-security/configuring-security-rules-in-an-nsg/](https://cloudacademy.com/course/implementing-azure-network-security/configuring-security-rules-in-an-nsg/)

**Question 1**

**Question**

CORRECT

**Which statement regarding Azure Network Watcher's IP Flow Verify is correct?**

It can test packet flow between any two Azure endpoints.

It checks network security group for any rule(s) that deny the connection.

It reviews all NSG rules associated with either connection endpoint.

It verifies both directions of traffic simultaneously.

**Explanation**

IP Flow Verify tests if packets flow between a VM and a second endpoint only. It checks for any NSG rules which deny the connection. It only reviews one direction at a time, and for NSG rules associated with one connection point at a time.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more: <https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview>

**Question 2**

**Question**

CORRECT

**Which AKS Service type supports public IP addresses and port numbers to allow direct access to AKS nodes by incoming traffic?**

ClusterIP Service type

NodePort Service type

LoadBalancer Service type

ExternalName Service type

**Explanation**

NodePort Service type supports public IP addresses and port numbers to enable direct access to AKS nodes by incoming traffic. This configuration requires an IP address for each AKS node.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more: <https://learn.microsoft.com/en-us/azure/aks/concepts-network>

**Question 3**

**Question**

CORRECT

**Your company is being audited, and an external accountant needs access to review a blob container in the Blob service within one specific Azure storage account.**

**You currently use Azure Active Directory to control access to the blob storage resources in question. However, you have been told you need to provide the accountant with immediate access to review the blob container in the storage account without any further information.**

**How can you provide necessary access, but also limit it to the container in question?**

Provide the accountant with read-only access to the specific Azure Blob container with a service-level shared access signature token to expire at the end of the business day. Specify the HTTPS protocol is required to accept requests.

Assign the accountant a guest role in Azure Active Directory with read-only access to the specific Azure Blob storage service in the Azure Storage account.

Provide the accountant with read-only access to the specific Azure Blob container with a user-delegation shared access signature token to expire at the end of the business day. Allow all read requests but limit write requests to LIST and GET. Specify the HTTPS protocol is required to accept requests.

Provide the accountant with contributor role access to the storage account using Azure AD role-based access control (RBAC).

**Explanation**

In this case, Azure Storage's Shared Access Signature (SAS) is the best tool to provide limited, authorized access to the necessary blob resources. Remember, SAS allows two levels of access: service-level, which limits access to one type of storage within the Azure storage account, such as Blob, Table, Queue or File storage, and account level, which provides access to all storage types in a single account. The service level also allows you to limit access to specific containers, or even specific blobs, and control the actions that can be performed on the blobs by selecting approved common permission types such as read, write, list, or process.

You cannot provide a user-delegated SAS in this case because you do not know if the accountant has Azure AD credentials, which are required for this type of SAS.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 4**

**Question**

CORRECT

**You are investigating Azure Storage replication options to discover when you get the read and write access to the remote replica.**

**Which statement regarding read and write access to Azure Storage replicas is correct?**

No matter which replication option you've selected for your Azure Storage account, you gain read and write access to the remote replica when you initiate failover.

If you have configured RA-GRS replication for your Azure Storage account, you always have read and write access to the Azure Storage account's replica.

No matter which replication option you've selected, once Azure fails over to the account's remote sites, then you are granted write access to the replicated data.

If you have configured GRS or RA-GRS replication for your Azure Storage account, you always have read and write access to the Azure Storage account's replica.

**Explanation**

With GRS and other replication options, only Microsoft can declare a disaster and failover the remote sites, then you will get read and write access to data. Until then you don't have access to the remote site's data for the read/write operations. You only have access to the remote copy for read operations when using RA-GRS.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 5**

**Question**

CORRECT

**Which of the following statements correctly describes the difference between role-based access controls (RBAC) and resource locks?**

Resource locks apply a restriction across all users and roles

RBAC applies a restriction across all users and roles

Resource locks apply a restriction to users only

RBAC applies a restriction to roles only.

**Explanation**

Unlike RBAC, management locks apply a restriction across all users and roles.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 6**

**Question**

CORRECT

**Your IT consulting business has recently partnered with two other businesses in different regions of the country. Each of your three offices has resources deployed in Microsoft Azure cloud.**

**Although you plan to eventually merge your separate offices into a single Azure AD tenant, you would like to connect several VNets in your separate subscriptions beforehand with your existing, separate Azure AD tenants in place.**

**What Azure solution is the easiest way to accomplish this?**

Create VNet peering connection

Create Virtual Network Gateways

Create a DNS zone with split-horizon view

Create a VNet-to-VNet VPN

**Explanation**

Microsoft Azure has steadily increased the compatibility of VNet Peering connections so that the previous generation solution, known as either Virtual Network Gateways or VPN Gateways, are used for in fewer scenarios now. VNet Peering connections can now connect VNets within separate subscriptions also within separate Azure AD tenants.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 7**

**Question**

INCORRECT

**You need to back up a VM using Azure Backup immediately, so you need to create a Recovery Service Vault. The general steps are listed below, in no particular order.**

1. **Assign a backup policy to the VM**
2. **Configure replication redundancy level.**
3. **Manually initiate the first backup.**
4. **Assign a resource group and location.**
5. **Configure the backup policy.**

**Which answer numerically lists the steps to back up a virtual machine in the correct order?**

4-2-5-1-3

4-5-1-2-3

2-5-1-4-3

5-1-2-4-3

**Explanation**

The correct order of execution is:

1. Assign a resource group and location.
2. Configure replication redundancy level.
3. Configure the backup policy.
4. Assign a backup policy to the VM.
5. Manually initiate the first backup.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 8**

**Question**

INCORRECT

**You have a microservice application hosted on Azure App Services named Azure Service Environment 1. The application communicates with on-premise database servers and data analysis applications. You need to find an effective monitoring solution to do the following:**

1. **Monitor performance of Azure Service Environment 1 and the on-premise database servers.**
2. **Provide alerts when communication between the on-premise database and Azure Service Environment 1 is disrupted.**
3. **Provide quantitative data regarding customer usage.**

**What Azure services or features within Azure App Service can meet all your requirements?**

Azure Application Insights

Azure Monitor

Azure App Service Diagnostic Logs

Azure App Service Metrics

**Explanation**

Application Insights can collect data from applications in Azure, running on-premise, or on other clouds. The integration with Azure Web Apps makes it exceptionally easy to use in Azure.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 9**

**Question**

INCORRECT

**You have successfully containerized your application within an Azure Container Registry, created an image of your application and pushed it into the container registry. You have also created an AKS cluster. Now you want to deploy the containerized application onto your AKS cluster.**

**Which three steps do you need to complete? (Choose 3 answers)**

Get credentials to authenticate **kubectl** commands sent to the Kubernetes cluster.

Create a manifest file declaring the required Kubernetes resources.

Create the resources in the cluster

Create a service principal to allow your cluster to interact with Azure resources

**Explanation**

You would need to complete all of the following steps in order to deploy your application to an AKS cluster except for creating a service principal. This step must already be completed in order for your AKS cluster to be provisioned and ready to host your application. You can also have AKS create a service principal for you using Azure CLI or Azure Portal.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 10**

**Question**

INCORRECT

**Which of the following statements is incorrect regarding a resource policy created using Azure Policy?**

Azure Policy scans Azure resources for noncompliance with defined resource policies.

It applies to Azure resources, not Azure subscribers or users.

Once a policy is created, it applies to both new and existing resources.

Users can search through Azure policy with custom policy queries.

**Explanation**

Azure Policy creates policies to define Azure resources only. Once a policy is created, it applies to new, updated and existing resources. The service scans hourly to detect noncompliance, but it does not support custom policy queries.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 11**

**Question**

CORRECT

**You want to create ARM templates to provision virtual machines with secure passwords that are not visible in the ARM template file.**

**Which service below can help you accomplish this task?**

Azure Active Directory

VM Agents

Multi-factor Authentication

Azure Key Vault

**Explanation**

The Azure Key Vault can be used to securely retrieve a password as a parameter to the Azure template. You need to create a vault and a secret using this service, then ensure that **enabledForTemplateDeployment** is set to true, and then reference the VaultID and the secretname in the template.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 12**

**Question**

CORRECT

**A company is using Azure Active Directory (Azure AD). The company has an assigned Global administrator and does not want someone else to have that level of access in Azure AD.**

**However, they want to allow a new employee to manage groups, user accounts, and service requests. Which of the following roles should be assigned to the new employee?**

Resource administrator

Billing administrator

Service administrator

User administrator

**Explanation**

Azure Active Directory has the following roles available:

1. Global administrator - This role has access to all administrative features.
2. Billing administrator - This role allows a user to manage subscriptions.
3. Service administrator - The service administrator manages requests and monitors the health of designated services.
4. User administrator - This role manages groups, user accounts, and service requests.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 13**

**Question**

CORRECT

**A company is planning to implement agile methodologies for one of their projects. The project will have the development environment as an app service hosted in Azure. Which of the following implementations would align with their agile practices?**

For the app service in Azure, configure the deployment source to any source code repository. Also ensure the deployment credentials are set. Ensure the right source code URL is set.

Set up Traffic Manager to route the different requests of the development environments from the different development teams.

Setup separate subscriptions for each development team and let each team connect their source code repository to the separate subscriptions

Setup a separate virtual machine for each developer and ensure they make their code changes to each virtual machine separately.

**Explanation**

For Agile practices, continuous integration is the key. Hence developers would want to ensure that all merged changes to the main trunk of their source code repository gets pushed to the development environment accordingly. This can be done by configuring the deployment source of the app service to the desired source code repository. Also ensure the deployment credentials are set. Ensure the right source code URL is set.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 14**

**Question**

INCORRECT

**A company's Azure environment consists of two virtual networks (VNets) with the following typology:**

**prod-vnet: 9 virtual machines (VMs)**

**dev-vnet: 9 virtual machines (VMs)**

**The VMs in the prod-vnet should run continuously. The VMs in the dev-vnet are used only between 6:00 A.M. and 6:00 P.M. local time.**

**You need to automate the shutdown and startup of the dev-vnet VMs to reduce the organization's monthly Azure costs.**

**Which Azure feature should you use?**

Azure Automation Desired State Configuration (DSC)

Azure Auto-Shutdown

Azure Change Tracking

Azure Automation runbook

**Explanation**

Azure Automation runbook is an Azure Automation management solution that allows you to publish PowerShell or Python scripts in Azure and optionally schedule Azure to run them automatically. In this case, the best practice is to write a PowerShell workflow script that automates VM startup and shutdown. You should then bind the script to two Azure Automation schedules: one to describe shutdown and one to describe startup time.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 15**

**Question**

CORRECT

**A company wants to use Azure blob storage. For disaster recovery purposes, data copies should be maintained in different regions. In the event of heavy traffic, the company would like to partially offload read requests to a secondary region. As an Azure administrator, what can you do to achieve this requirement?**

Create the Azure Storage account with the default settings. Copy the data within blob storage to another region. Create a PowerShell script to synchronize the data.

Create the Azure Storage account with the default settings. Copy the data within blob storage to another region. Create a program to synchronize the data because PowerShell cannot be used with blob storage service.

Create the Azure Storage account with the replication attribute set to read-access geo-redundant storage (RA-GRS).

Create the Azure Storage account with the replication attribute set to geo-redundant storage.

**Explanation**

When a storage account is created, one can select the following replication options: Locally redundant storage (LRS), Zone-redundant storage (ZRS), geo-redundant storage (GRS),  or read-access geo-redundant storage (RA-GRS). The read-access geo-redundant storage allows copies of blob storage to be replicated to various regions. It also allows for a read-only copy to be accessed from another region.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 16**

**Question**

CORRECT

**You need to investigate unexpected errors caused by requests initiated by web applications hosted on Azure. You suspect errors were caused by several types of resources, including compute, storage, notifications, and key management.**

**The best course of action is to compile all the data and then create queries to analyze the data manually.**

**What type of log data should you review first, and what service should you use to review the data?**

Review diagnostic logs with Log Analytics

Review activity logs with Azure Event Hub

Review application logs with Azure Queue Storage

Review boot diagnostic logs with Azure Table Storage

**Explanation**

To determine the right type of data to analyze, the key factor is that the errors were likely within requests from Azure services, which are actions tracked by diagnostic logs. It would also not be application logs, in this case, because the errors involve multiple types of resources, not just compute resources.

To determine the best service, the ability to create queries of log data is offered specifically by Log Analytics.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 17**

**Question**

CORRECT

**Which of the following choices are true about Azure Storage encryption at rest? (Choose 2 answers)**

Azure Storage encryption is two-way encryption with asymmetric keys.

Azure Storage encryption is managed transparently by Azure.

Azure Storage encryption is one-way encryption with asymmetric keys.

Azure Storage encryption is two-way encryption with symmetric keys.

**Explanation**

Azure Storage encryption uses two-way symmetric keys and managed transparently by Azure and thus both parties have access to the secret key hence the symmetric nature.  Asymmetric key encryption (such as public/private key cryptography) is not valid in Azure Storage encryption.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 18**

**Question**

CORRECT

**A client has an Azure Site-to-Site (S2S) connection between an on-premises location and an Azure virtual network (VNet) using a RouteBased Azure VPN gateway. This client has a requirement for all Internet-bound traffic from virtual machines (VMs) on their Azure VNet to be routed back to the on-premises location for auditing. Which of the following solutions would best meet the requirement?**

Create Point-to-Site (P2S) connections between the VMs and client machines at the on-premises location

Configure forced tunneling to route Internet-bound traffic from the VMs to the on-premises location

Create another S2S connection between the on-premises location and VNet using a PolicyBased VPN gateway

Add the “GatewaySubnet” to a network security group (NSG) with a rule to disallow all internet bound traffic

**Explanation**

Forced tunneling can be used with Azure S2S connections and RouteBased (not PolicyBased) VPN gateways to route Internet-bound traffic from a VNet to an on-premises location for inspection and auditing. According to Microsoft recommendations, the “GatewaySubnet” should not be part of an NSG.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 19**

**Question**

CORRECT

**A company is planning to deploy a set of web servers and database servers. They want to ensure high availability through availability sets. Which of the following is the recommended design practice to use?**

Place the web servers and database servers in the same availability set.

Place half of the web servers and half of the database servers in one availability set, and the other half in another availability set.

Place all the web servers in one availability set and the database servers in another availability set.

Have an availability set for each web server and database server.

**Explanation**

The best design practice when it comes to availability sets is to place the servers which serve the same purpose in one availability set. So application servers and web servers should be placed in their own availability sets. This ensures that each tier in your application will have at least one Virtual machine running at any point in time.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 20**

**Question**

INCORRECT

**An Azure subscription named Subscription 1 contains three resource groups named Development, Test, and Production. Thomas, Logan, and Guy have been assigned roles via role-based access controls (RBAC) to access Subscription 1 resources.**

* **Logan can perform all read and write operations on all compute and storage resources within the Development and Test resource groups.**
* **Guy is an owner of the Development and Test resource groups.**
* **Thomas is an owner of Subscription 1.**

**If necessary, who would be able to delete the entire Development resource group and all resources within it?**

Both Guy and Thomas

Only Thomas

Only Guy

Both Logan and Guy

**Explanation**

With role-based access controls (RBAC), the permissions applied at a certain scope apply to all child resources within that scope. This means a subscription owner also has owner permissions for all resource groups and resources within the subscription.

As such, both Guy and Thomas could complete the task required in the question below.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 21**

**Question**

CORRECT

**You suspect hackers and bots have been attacking your application's network. What Azure Network Watcher network monitoring or analysis tool would best fit your needs?**

Connection Monitor

Network Performance Monitor

Security Group View

Traffic Analytics

**Explanation**

Traffic analytics is a cloud-based solution that provides visibility into user and application activity in cloud networks. Traffic analytics analyzes Network Watcher network security group (NSG) flow logs to provide insights into traffic flow in your Azure cloud.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 22**

**Question**

CORRECT

**You are the owner of a resource group that contains the following Azure resources:**

* **VNet1, which contains Subnet1. Subnet1 is assigned a routing table, and a network security group named NSG-1.**
* **SubNet1 contains an ARM virtual machine 1 with a private IP address only.**

**VM-Database1 needs to connect to an on-premises static IP address (216.3.128.12) to request software updates. You do not want to reveal the IP address of the ARM virtual machine 1. All inbound traffic aside from the software updates should be blocked.**

**Which steps should you take to allow the database to connect successfully for updates while limiting threats? (Choose 2 answers.)**

Deploy a private load balancer associated with the ARM virtual machine.

Deploy a NAT gateway associated with Subnet1.

Update NSG-1 to allow outbound traffic to and from 216.3.128.12 over port 443. Include no other rules allowing traffic.

Update NSG-1 to allow outbound traffic to 216.3.128.12 over port 443. Include no other rules allowing traffic.

**Explanation**

Network security group security rules are evaluated by priority using the 5-tuple information (source, source port, destination, destination port, and protocol) to allow or deny the traffic. A flow record is created for existing connections. Communication is allowed or denied based on the connection state of the flow record. The flow record allows a network security group to be stateful.

Deploy a Network Address Translation or NAT gateway to enable Source Network Address Translation (SNAT). As Microsoft explains in its documentation:

*Source Network Address Translation (SNAT) rewrites the source of a flow to originate from a different IP address and/or port. Typically, SNAT is used when a private network needs to connect to a public host over the internet. SNAT allows multiple compute resources within the private VNet to use the same single Public IP address or set of IP addresses (prefix) to connect to the internet.*

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 23**

**Question**

CORRECT

**Your organization’s system administrator has deployed two standalone Azure virtual machines (VMs) for a new web service. You now want to add these virtual machines to fault domains in an availability set. When you attempt to do this in the portal, you receive an error message preventing you from completing the task.**

**What is the reason for this?**

You did not check the required “Standalone” parameter in Azure Portal

You may not add running standalone VMs to availability sets

The VMs operating system is not compatible with fault domains.

The availability set has to be paused or stopped before standalone VMs can be added.

**Explanation**

Creating an Availability Set is a pretty simple, straightforward process. However, the caveat is getting your VMs to be part of an availability set. If you have existing VMs that are not part of an availability set, we refer to these as Standalone VMs. You may not simply take standalone VMs and move them into availability sets because this has to be done at the time of VM creation.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 24**

**Question**

CORRECT

**You want to connect the Azure VNets for three separate branch offices. You are designing a hub and spoke model network topology to do this. The central hub will serve as a firewall between the different locations during backend communication, and also a central location for disaster recovery backup storage.**

**Now you are considering whether to connect your hub-and-spoke model with VNet peering connections or Azure VPN Gateways. Each option has its own benefits.**

**Which statements comparing VNet peering and VPN Gateways in a hub-and-spoke model are correct? (Choose 3 answers)**

If you implement the model with Azure VPN Gateways, all VNets **can be cross-region.**

If you implement the model with VNet peering connections, the VNets **can be cross-region with Global VNet Peering.**

Whether the connections are made with Azure VPN Gateways or VNet peering connections, the VNets can be **within different Azure subscriptions** and associated **with separate Azure AD tenants**.

If you implement the model with Azure VPN Gateways, all VNets **can be in different regions**.

If you implement the model with VNet peering connections, the VNets **must be in the same region**.

If you implement the model with Azure VPN Gateways, the VNets can be **within different Azure subscriptions** that are **associated with the same Azure tenant.**

If you implement the VNets with VNet peering connections, the VNets can be **within different Azure subscriptions** and **associated with separate Azure AD tenants**.

**Explanation**

You could accomplish this network topology using VNet peering or Azure VPN Gateways, but each option has its requirements and limitations.

1. Connecting via VNet peering would require a router to be deployed in the central hub VNet, but this is not required for VNG connections.
2. VNet peering works both across separate tenants and subscriptions.
3. Hostname resolution is not possible for VMs connecting from different VNets through a peering connection. Azure DNS is required for these VMs to connect. However, name resolution is possible through a VNG connection.
4. VNets must be connected via Global VNet Peering.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 25**

**Question**

CORRECT

**You would like to implement a Hub-and-Spoke VNet peering connection between two existing VNets in the East US region, (VNet 1 and VNet2), without using a network virtual appliance. You want resources in VNet1 and VNet2 to be able to communicate.**

**You have deployed VNet3 in the East US region that will serve as a hub between the other VNets. VNet1 and VNet2 should be able to communicate with each other through VNet3 using a VPN virtual network gateway.**

**Which VNet peering connections should be configured to allow all forwarded traffic? (Choose 2 answers.)**

VNet1 to VNet3 peering connection with traffic forwarded enabled.

VNet2 to VNet3 peering connection with traffic forwarded enabled

Only peering connections directed to VNet3 as the hub

Only peering connections directed to VNet1 and VNet2 as the spokes

**Explanation**

To implement a Hub-and-Spoke VNet peering connection between two existing VNets in the East US region without using a network virtual appliance, you can use a VPN virtual network gateway to connect the spoke VNets (VNet1 and VNet2) to the hub VNet (VNet3).

To allow all forwarded traffic between the VNets, you should configure the following VNet peering connections:

VNet1 to VNet3 peering connection with traffic forwarded enabled.

VNet2 to VNet3 peering connection with traffic forwarded enabled.

By enabling traffic forwarding, you allow traffic to be routed through the peering connection, which enables communication between resources in the spoke VNets (VNet1 and VNet2) through the hub VNet (VNet3) using the VPN virtual network gateway.

You can also configure spokes to use the hub gateway to communicate with remote networks. To allow gateway traffic to flow from spoke to hub and connect to remote networks, you must:

* Configure the peering connection in the hub to allow gateway transit.
* Configure the peering connection in each spoke to use remote gateways.
* Configure all peering connections to allow forwarded traffic.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 26**

**Question**

INCORRECT

**A company currently has an on-premise setup which manages identity stores in Active Directory. They want to extend their on-premise solution to Azure. They do not want to maintain two separate passwords, one for the on-premise store and the other for the console used to login into Azure. Which of the following can be used to ensure this requirement can be fulfilled?**

Use an Active Directory Federation server, which will use WS-Federation to ensure single-sign on for both on-premise and Azure.

Use an Active Directory Federation server which will use OpenID Connect protocol to ensure single-sign on for both on-premise and Azure.

Use an Active Directory Federation server which will use SAML protocol to ensure single-sign on for both on-premise and Azure.

Use a custom connector which will provide single sign on for both Active Directory on-premise and Azure.

**Explanation**

The Security Assertion Markup Language (SAML)-based claims authentication can be used for configuring single sign on between on-premise Active Directory and other web based providers. Active Directory Federation services can be setup on-premise which can be configured to use SAML. Active Directory Federation will work with Azure via tokens, and provide a single-sign on feature for users.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 27**

**Question**

CORRECT

**You are looking for cost savings in your Azure compute resources, and have identified a default VM scale set running daily batch processes during non-business hours is a fairly large expense. These batch processes are not mission-critical to your daily operation, and occasional interruptions will not have any consequence on the business.**

**What cost-saving method could you implement?**

Replacing the existing VM scale set with Reserved VMs

Replacing the existing VM scale set with Azure Functions

Replacing the existing VM scale set with Azure App Service

Replacing the existing VM scale set with 'Low Priority' VM scale set

**Explanation**

Low-priority VMs are cheaper, but can be terminated at any time by Azure. They are ideal for this type of use case, but not to support applications that must persist reliably and be highly available.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 28**

**Question**

CORRECT

**Which Azure Storage service is designed for large-scale, offline data migration intended to help businesses migrate their data onto the Azure cloud?**

AzCopy

Azure Data Box

Azure Storage Explorer

StorSimple

**Explanation**

The Microsoft Azure Data Box cloud solution lets you send terabytes of data into Azure in a quick, inexpensive, and reliable way. The secure data transfer is accelerated by shipping you a proprietary Data Box storage device. Each storage device has a maximum usable storage capacity of 80 TB and is transported to your data center through a regional carrier. The device has a rugged casing to protect and secure data during the transit.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 29**

**Question**

INCORRECT

**You want to assign a role-based access control (RBAC) role to a user in the Azure Portal. Consider the following steps listed below:**

1. **Select the user**
2. **Open Access Control (IAM) and select 'Add Role Assignment'**
3. **Open Azure Resource Manager and select 'Add Role Assignment'**
4. **Provide Reason for Assignment**
5. **Select the role**
6. **Save**
7. **Select Eligible or Permanent**

**Assuming you have the necessary permissions, which answer lists the necessary steps to assign an RBAC role to a user in the correct order?**

2 - 1 - 5 - 6

3 - 1 - 5 - 6

2 - 1 - 5 - 7 - 6

2 - 1 - 5 - 7 - 4 - 6

**Explanation**

In Access control (IAM), you can Add permissions to the resources. To assign a role to a user, you simply select the desired Role, Assign access to an Azure AD user, group, or application, Select the user from the list, and click Save.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 30**

**Question**

CORRECT

**Which standalone application provides a graphical interface for working with Azure Storage data on a Windows, OS X, or Linux machine?**

Microsoft Azure Storage Emulator

Microsoft Azure Storage Explorer

Windows Performance Monitor

IOSTAT

**Explanation**

Microsoft Azure Storage Explorer (Preview) is a free, standalone app from Microsoft that enables you to work graphically with Azure Storage data on Windows, OS X, and Linux. It also provides several ways to connect to your storage account (e.g., by subscription or through the storage emulator).

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 31**

**Question**

INCORRECT

**As your company's IT Security Manager, you want to integrate security monitoring services on corporate virtual and on-premise hardware such as employee laptops, virtual machines, mobile devices and so on. To address your company's concerns, you are reviewing Microsoft Defender for Cloud capabilities.**

**Microsoft Defender for Cloud can monitor which of the following types of computers?**

Azure-hosted virtual machines with Windows and Linux operating systems

Azure-hosted virtual machines with Windows and Linux operating systems, and non-Azure virtual machines with Windows operating systems

Azure-hosted virtual machines with Windows and Linux operating systems, and on-premise computers with Windows operating systems

Azure-native virtual machines, non-Azure virtual machines, and on-premise computers with Windows and Linux operating systems

**Explanation**

Microsoft Defender for Cloud can monitor virtual machines in the Azure Cloud and virtual machines hosted outside of the Azure cloud, as well as on-premise computers. Endpoint protection integrates with Linux and Windows operating systems.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 32**

**Question**

CORRECT

**Which of the following statements about Azure VPN Gateways and subnets is false?**

When creating on-premises to virtual network (VNet) connections, there cannot be overlapping subnet address ranges

VPN Gateways require a specific gateway subnet that must be named GatewaySubnet

Virtual machines cannot be deployed on a gateway subnet

When creating VNet-to-VNet connections there can be overlapping subnet address ranges

**Explanation**

There cannot be overlapping subnet address ranges in either on-premises to VNet connections or VNet-to-VNet connections. VPN Gateways require a specific gateway subnet that must be named GatewaySubnet and virtual machines cannot be deployed on the gateway subnet.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 33**

**Question**

CORRECT

**Your application requires a high number of IOPS to satisfy minimum performance thresholds. You have selected Premium disks, and are now reviewing replication options.**

**Which replication options offer the most redundancy, based on your selection of Premium disks? (Choose 2 answers)**

LRS

GRS

RA-GRS

ZRS

**Explanation**

Azure Premium Disk Storage currently supports only locally redundant storage (LRS). Block blob storage accounts support locally redundant storage (LRS) and zone redundant storage (ZRS) in certain regions.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 34**

**Question**

CORRECT

**What Azure network resource can allow or deny layer-3 traffic based on a series of security rules, and can also be directly applied to virtual machines, subnets, or network interface cards attached to virtual machines?**

Network Security Groups

Access Control Lists

Azure Firewalls

Application Gateways

**Explanation**

A network security group (NSG) contains a list of security rules that allow or deny network traffic to resources connected to Azure Virtual Networks (VNet). NSGs can be associated to subnets, individual VMs (classic), or individual network interfaces (NIC) attached to VMs (Resource Manager). When an NSG is associated to a subnet, the rules apply to all resources connected to the subnet. Traffic can further be restricted by also associating an NSG to a VM or NIC.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 35**

**Question**

CORRECT

**You are reviewing the specifications for a new solution, and it lists "a managed layer 7 load balancer."**

**Which of the following services will be included in your design?**

Azure Application Gateway

Azure Load Balancer

A custom virtual appliance

Azure Traffic Manager

**Explanation**

The OSI model defines layer 7 as an application layer. That includes protocols such as FTP, HTTP(S), STMP, etc.

Application Gateway is a layer 7 load balancer for HTTP(S) based traffic.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 35**

**Question**

CORRECT

**You are reviewing the specifications for a new solution, and it lists "a managed layer 7 load balancer."**

**Which of the following services will be included in your design?**

Azure Application Gateway

Azure Load Balancer

A custom virtual appliance

Azure Traffic Manager

**Explanation**

The OSI model defines layer 7 as an application layer. That includes protocols such as FTP, HTTP(S), STMP, etc.

Application Gateway is a layer 7 load balancer for HTTP(S) based traffic.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 35**

**Question**

CORRECT

**You are reviewing the specifications for a new solution, and it lists "a managed layer 7 load balancer."**

**Which of the following services will be included in your design?**

Azure Application Gateway

Azure Load Balancer

A custom virtual appliance

Azure Traffic Manager

**Explanation**

The OSI model defines layer 7 as an application layer. That includes protocols such as FTP, HTTP(S), STMP, etc.

Application Gateway is a layer 7 load balancer for HTTP(S) based traffic.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 35**

**Question**

CORRECT

**You are reviewing the specifications for a new solution, and it lists "a managed layer 7 load balancer."**

**Which of the following services will be included in your design?**

Azure Application Gateway

Azure Load Balancer

A custom virtual appliance

Azure Traffic Manager

**Explanation**

The OSI model defines layer 7 as an application layer. That includes protocols such as FTP, HTTP(S), STMP, etc.

Application Gateway is a layer 7 load balancer for HTTP(S) based traffic.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 35**

**Question**

CORRECT

**You are reviewing the specifications for a new solution, and it lists "a managed layer 7 load balancer."**

**Which of the following services will be included in your design?**

Azure Application Gateway

Azure Load Balancer

A custom virtual appliance

Azure Traffic Manager

**Explanation**

The OSI model defines layer 7 as an application layer. That includes protocols such as FTP, HTTP(S), STMP, etc.

Application Gateway is a layer 7 load balancer for HTTP(S) based traffic.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 35**

**Question**

CORRECT

**You are reviewing the specifications for a new solution, and it lists "a managed layer 7 load balancer."**

**Which of the following services will be included in your design?**

Azure Application Gateway

Azure Load Balancer

A custom virtual appliance

Azure Traffic Manager

**Explanation**

The OSI model defines layer 7 as an application layer. That includes protocols such as FTP, HTTP(S), STMP, etc.

Application Gateway is a layer 7 load balancer for HTTP(S) based traffic.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 35**

**Question**

CORRECT

**You are reviewing the specifications for a new solution, and it lists "a managed layer 7 load balancer."**

**Which of the following services will be included in your design?**

Azure Application Gateway

Azure Load Balancer

A custom virtual appliance

Azure Traffic Manager

**Explanation**

The OSI model defines layer 7 as an application layer. That includes protocols such as FTP, HTTP(S), STMP, etc.

Application Gateway is a layer 7 load balancer for HTTP(S) based traffic.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 35**

**Question**

CORRECT

**You are reviewing the specifications for a new solution, and it lists "a managed layer 7 load balancer."**

**Which of the following services will be included in your design?**

Azure Application Gateway

Azure Load Balancer

A custom virtual appliance

Azure Traffic Manager

**Explanation**

The OSI model defines layer 7 as an application layer. That includes protocols such as FTP, HTTP(S), STMP, etc.

Application Gateway is a layer 7 load balancer for HTTP(S) based traffic.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 35**

**Question**

CORRECT

**You are reviewing the specifications for a new solution, and it lists "a managed layer 7 load balancer."**

**Which of the following services will be included in your design?**

Azure Application Gateway

Azure Load Balancer

A custom virtual appliance

Azure Traffic Manager

**Explanation**

The OSI model defines layer 7 as an application layer. That includes protocols such as FTP, HTTP(S), STMP, etc.

Application Gateway is a layer 7 load balancer for HTTP(S) based traffic.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 35**

**Question**

CORRECT

**You are reviewing the specifications for a new solution, and it lists "a managed layer 7 load balancer."**

**Which of the following services will be included in your design?**

Azure Application Gateway

Azure Load Balancer

A custom virtual appliance

Azure Traffic Manager

**Explanation**

The OSI model defines layer 7 as an application layer. That includes protocols such as FTP, HTTP(S), STMP, etc.

Application Gateway is a layer 7 load balancer for HTTP(S) based traffic.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 35**

**Question**

CORRECT

**You are reviewing the specifications for a new solution, and it lists "a managed layer 7 load balancer."**

**Which of the following services will be included in your design?**

Azure Application Gateway

Azure Load Balancer

A custom virtual appliance

Azure Traffic Manager

**Explanation**

The OSI model defines layer 7 as an application layer. That includes protocols such as FTP, HTTP(S), STMP, etc.

Application Gateway is a layer 7 load balancer for HTTP(S) based traffic.

[**Bookmark**](https://cloudacademy.com/exam/results/36231/4357260/)

Learn more:

**Question 21**

**Question**

INCORRECT

**Your organization has a custom line-of-business (LOB) application that uses several Azure resources. All of the LOB application resources are in the same resource group.**

**You want to create a template for the resource group currently being used by the LOB application.**

**What should you do?**

Use the Get-AzResourceGroupDeployment cmdlet.

Use the Export-AzResrouceGroup cmdlet.

Use the Save-AzResourceGroupDeploymentTemplate cmdlet.

Use the Get-AzResourceGroupDeploymentOperation cmdlet.

**Explanation**

You should use the Save-AzResourceGroupDeploymentTemplate cmdlet because it saves a resource group deployment template to a JSON file, as in the following example:

Save-AzResourceGroupDeploymentTemplate -DeploymentName "TestDeployment" -ResourceGroupName "TestGroup"

This command gets the deployment template from TestDeployment and saves it as a JSON file in the current directory so that it can be reused for the target resources needed for the LOB application.

You should not use the Get-AzResourceGroupDeployment cmdlet because it returns the deployment history for a resource group.

You should not use the Export-AzResrouceGroup cmdlet because it will export all resources in the resource group as a template.

You should not use the Get-AzResourceGroupDeploymentOperation cmdlet because this command returns all operations performed during a deployment.

Learn more: <https://learn.microsoft.com/en-us/powershell/module/az.resources/save-azresourcegroupdeploymenttemplate?view=azps-9.2.0>

**Question 22**

**Question**

INCORRECT

**You have had to troubleshoot several issues related to network interfaces, and spent a great deal of time completing this task. Which service within Azure Network Watcher allows you to review recent activity to check for issues with network interfaces more quickly?**

Diagnostic Logs

NSG Flow Logs

Next Hop

Connection Monitor

**Explanation**

 The Diagnostic logs capability provides a single interface to enable and disable network resource diagnostic logs for any existing network resource that generates a diagnostic log. You can view diagnostic logs using tools such as Microsoft Power BI and Azure Log Analytics.

Learn more: <https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview#logs>

**Question 24**

**Question**

INCORRECT

**You want to configure a recovery service vault for your on-premise server backup as well as VM disks. What steps are required for on-premise servers that are not required for Azure VMs? (Choose 2 answers)**

Install a recovery service agent

Register your on-premise server

Configure a backup policy

Configure the vault storage replication

**Explanation**

To back up an on-prem server with Azure Backup, the Recovery Services Agent must be downloaded and installed on the on-prem server being backed up. Additionally, the server being backed up must first be registered with the vault so that it can communicate with it securely.

Learn more: [/course/implementing-azure-backup/12-backing-up-on-prem-servers/](https://cloudacademy.com/course/implementing-azure-backup/12-backing-up-on-prem-servers/)

**Question 30**

**Question**

INCORRECT

**You need to cut your product development and product resource budget by a significant amount in the next fiscal quarter. You think there are ways to save by terminating underutilized resources, or reducing costs for heavily-used resource types.**

**You do not currently have the time or resources to dedicate to a substantial cost analysis project. You need to obtain intelligent insights related to your historic budget allocations in a very short window of time with minimal administration required.**

**To analyze your resource spend automatically for potential cost-saving opportunities, what Azure tool or service should you use?**

Resource Tags

Azure Cost Management

Log Alerts

Azure Advisor

**Explanation**

Any of these mechanisms offers potential as a cost-saving or cost-tracking tool to a skillful administrator. The question is, which resource allows you the largest amount of insights with minimal investment of time or staff? Resource tags can be great if you have time to apply them all. Log alerts could be useful if you were interested in current, at-the-moment spending rather than historical spend. The same is true of Azure Cost Management, which provides a wide variety of general and detailed reports and filtering options, but do you have time to read them? Maybe not.

In this situation, Azure Advisor is the best choice because it quickly analyzes a short period of historic spend across your resources and provides quick, actionable feedback on ways to save money.

Learn more: <https://docs.microsoft.com/en-us/azure/advisor/advisor-overview>

**Question 44**

**Question**

INCORRECT

**Your team is spending too much time recovering from unplanned events, specifically when small resource updates occur that disrupt service operations, or noncompliant resources are created.**

**You want to automate a process to review log data related to resource updates, to detect anomalies within the updates. You would like to utilize live dashboards to evaluate the log data quickly. What type of logs would you analyze, and with what Azure service?**

Process activity logs with Azure Event Hub.

Process diagnostic logs with Log Analytics.

Process application logs with tables in Azure Storage.

Process diagnostic logs with Power BI.

**Explanation**

Azure offers activity logs to help you track subscription level operations on resources, such as creating or updates resources. Azure Event Hubs allows you to receive thousands of log events per second and detect anomalies, and it also provides live dashboards as well.

Learn more: <https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview-activity-logs>