Practice Test Questions

Azure Fundamentals

Match each Azure Storage Blob access tier with its associated description.

To answer, drag the appropriate blob access tier to the appropriate feature. A tier may be used once, more than once, or not at all.

Drag and drop the answers

Incurs penalties for data deleted within 30 days.	Cool
Is not available at the account level.	Archive
Incurs the highest rehydration cost.	Archive

Archive | Cool | Hot

The cool storage tier incurs penalties for data deleted within 30 days.

The archive storage tier is not available at the account level.

The archive storage tier incurs the highest rehydration costs.

Azure Storage offers three pricing and availability tiers for blob storage. These tiers facilitate cost-effective storage based on how frequently data needs to be accessed.

Hot tier storage offers the highest performance and lowest access latencies but is the most expensive storage tier. This tier is intended to hold data that is accessed frequently.

The cool tier is designed to hold data that only requires infrequent access. Any data placed in the cool tier most be stored for at least 30 days. Moving or deleting data prior to this threshold results in penalties.

The archive tier is designed to hold data that rarely requires access. The archive tier is not available at the account level and is configured on the blob itself. This tier has the highest access latencies, and the process of retrieving the archived data for reading, also known as rehydration, incurs the highest costs.

References

Which two options can you use to connect Azure Virtual Networks (VNets) to each other? Each correct answer presents a complete solution.

Choose the correct answers

- Azure Traffic Manager
- Azure Front Door
- Azure ExpressRoute
- ✔ VNet peering
- ✔ VPN gateways

Explanation

You should use VNet peering or VPN gateways to connect Azure Virtual Networks (VNets) to each other. With VNet peering you can seamlessly connect two or more VNets in Azure, routing the traffic directly through the Microsoft backbone infrastructure. Alternatively, you can deploy VPN gateways in each VNet to connect them to each other over the public internet.

You should not use Azure ExpressRoute, Azure Front Door, or Azure Traffic Manager Gateways to connect Azure Virtual Networks (VNets) to each other. None of these enables VNet-to-VNet connectivity.

Azure ExpressRoute is a service that enables private connectivity between your on-premises network and Microsoft Azure or Microsoft 365.

Azure Front Door is a global endpoint that works at Layer 7 (HTTP/HTTPS) to enable fast, secure, and widely scalable Web applications.

Azure Traffic Manager is a DNS-based traffic load balancer that allows optimal distribution of traffic to Azure services spread across global Azure regions.

References

Which Azure component provides information about planned maintenance and advisories such as deprecated offerings?

Choose the correct answer

- Microsoft Defender for Cloud
- ✔ Azure Service Health
- Azure Monitor
- Azure Advisor

Azure Service Health provides information about planned maintenance and advisories such as deprecated offerings. This is provided through Azure status at the global level and Service Health at the individual service level. These are both components of Azure Service Health. Azure Service Health also includes Resource Health, which reports about individual resources through a configurable dashboard.

Azure Monitor does not provide information about planned maintenance and service advisories. Azure Monitor collects resource on applications, guest operating systems, resource operations, tenant-level services, and information about the health and operation of Azure.

Microsoft Defender for Cloud does not provide information about planned maintenance and service advisories. Microsoft Defender for Cloud is designed to help protect Azure cloud, non-Azure cloud, and hybrid computing resources through a set of security tools. Microsoft Defender for Cloud provides tools to help strengthen your organization's security posture, protect against threats, and quickly secure your computing environment.

Azure Advisor does not provide information about planned maintenance and service advisories. Azure Advisor analyzes your resource configuration to help you optimize your Azure deployments. It provides best practices recommendations regarding performance, security, and availability.

For each of the following statements, select Yes if the statement correctly describes the use of Azure Policy initiatives. Otherwise, select No.

Statement	Yes	No
An initiative is limited to being assigned to resource groups or subscriptions only.	○	◉
When an initiative assignment is evaluated, all of the policies in that initiative are evaluated.	◉	○
An initiative can only contain policies that are located in the same subscription.	◉	○

Explanation

An initiative is a collection of Azure policy definitions, which are usually grouped with the aim of achieving a single goal. Initiatives are used to simplify managing and assigning policies. The same initiative can be assigned to multiple scopes in order to include resources, resource groups, subscriptions, or management groups.

When an initiative assignment is evaluated, all of the policies in that initiative are evaluated. If you want to evaluate a policy by itself, you should either not assign the policy to an initiative or you should create an initiative that only contains that policy.

An initiative can only contain policies that are located in the same subscription. You can assign a single initiative to scopes across multiple subscriptions or management groups. However, you must create the policies and initiatives in the same subscription.

You manage a development team that needs to focus all its efforts on creating and maintaining application code. Your team does not have the resources to provision and scale the infrastructure your applications require to run. What should you do?

Choose the correct answer

- Automate virtual machine provisioning with Azure Quickstart Templates.
- Configure virtual machines and deploy application updates using Azure command-line interface (CLI).
- Containerize the apps and deploy a container cluster service.
- ✔ Create an Azure Functions subscription and upload your code.

Explanation

You should create an Azure Functions subscription and upload your code. Azure Functions is an example of serverless computing. In the serverless computing model, a customer can submit their application code to a cloud service provider (CSP) such as Azure. Azure provisions and maintains the servers and infrastructure required to run the application. This includes code backups, high availability features, and auto-scaling to meet increased workloads.

You should not containerize the app and deploy a container cluster service. Containers typically contain only the binaries and libraries to run a single app or service. However, a container is an infrastructure component, and the containers must be created, deployed, and periodically updated. Azure supports container clusters via the Azure Kubernetes Service (AKS).

You should not automate virtual machine provisioning with Azure Quickstart Templates. A template is a stored virtual machine configuration. Many organizations use templates to speed up the deployment of frequently used operating system configurations. Like containers, virtual machines are an infrastructure component.

You should not configure virtual machines and deploy application updates using Azure command-line interface (Azure CLI). The Azure CLI provides an automated way to control and automate many of the same tasks that can be performed through the Azure portal, such as creating and managing virtual machines, networking, storage, and more. In addition, the Azure CLI can be used to manage multiple Azure subscriptions and save time by avoiding the manual entry of repetitive commands.

How can Azure lower capital expenditure (CapEx) costs?

Choose the correct answer

- Azure reduces the amount of maintenance that is associated with the configuration of firewalls, which reduces costs.
- Azure allows you to reduce the level of IT staffing that is required to maintain on-premises applications and services.
- Azure allows you to pay annually to reduce overall costs that are associated with its platform-as-a-service (PaaS) offerings.
- ✔ Azure allows you to pay monthly based on usage rather than pay upfront for physical hardware.

Explanation

Azure allows you to pay for servers monthly based on usage, rather than pay upfront for physical hardware. CapEx refers to money that is spent up front on infrastructure hardware such as routers, switches, and servers. With a public cloud deployment in Azure, you only need to pay for the usage of these devices. This eliminates CapEx costs. With a hybrid cloud deployment in Azure, you can lower CapEx costs because you only need to pay for devices that are on-premises.

Azure does not necessarily allow you to reduce the level of IT staffing that is required to maintain on-premises applications and services. Although there is no need for hardware IT support in a public cloud deployment, the company still needs IT personnel to maintain its on-premises applications and services.

Azure does not allow you to pay annually to reduce the overall costs that are associated with its platform-as-a-service (PaaS) offerings. It allows you to pay annually for some infrastructure-as-a-service (IaaS) offerings, such as virtual machines (VMs), through reserved VM instances.

Azure does not reduce the amount of maintenance that is associated with configuring firewalls, which would reduce costs. Although Azure eliminates the need to perform physical cabling of networks, it still requires you to configure software.

You are researching governance methodologies in Azure. You want to understand role-based access security (RBAC), policies, initiatives, and locks.

You need to choose the type of resource or feature to use for different scenarios.

When should you use each resource or feature? To answer, drag the appropriate resource or feature to each scenario. A resource or feature may be used once, more than once, or not at all.

Drag and drop the answers

You want to ensure that only SQL Database instances can be added to a resource group named database-rg.	Policy
You want to ensure that only members of the Sales group can access virtual machines (VMs) in the sales-rg resource group.	RBAC
You want to prevent new resources from being added to a resource group by anyone.	Lock

Lock | Policy | RBAC | Initiative

Explanation

You should use a policy when you want to ensure that only SQL Database instances can be added to a resource group named database-rg. A policy definition is a JSON file that is assigned to a scope, such as a resource group. The JSON file defines the rules that are to be followed for certain resources.

You should use RBAC to ensure that only members of the Sales group can access VMs in the sales-rg resource group. RBAC assigns permissions that apply to users and groups.

You should use a lock when you want to prevent new resources from being added to a resource group by anyone. This helps prevent accidental modification of a resource group. The name of this lock setting is ReadOnly. In the Azure portal, this lock setting is referred to as Read-only.

You should not use an initiative in this scenario. An initiative allows you to manage a collection of policies.

To complete the statement in the answer area, select the appropriate option from the drop-down menu.

Choose the correct options

An Azure Initiative

is a collection of Azure policies targeted toward reaching a single overall goal.

Explanation

An Azure Initiative is a collection of Azure policies targeted toward reaching a single overall goal. This simplifies managing and assigning policy definitions by grouping a set of policies as a single item. The Initiative can then be assigned to a scope and applied to all resources contained in that scope.

An Azure Initiative does not provide a model that is used by Azure Resource Manager to deploy large numbers of identical resources. This describes a Resource Manager template, which contains resource and resource group definitions.

An Azure Initiative does not let you implement detailed granular resource access controls. This is done by assigning role-based access controls (RBACs) to users and groups over specified scopes. RBAC supports over 70 built-in roles.

An Azure Initiative does not integrate with Azure Advisor to provide best practices for optimization. Azure Advisor integrates with Microsoft Defender for Cloud to provide a consolidated view of recommendations for all Azure resources. It can help you improve cost effectiveness, performance, high availability, and security of Azure resources.

You build a new operational analytics solution in Azure using PostgreSQL as a relational database. The estimated monthly growth of your database is 20 Gb.

You need to ensure that your database can scale horizontally and support query parallelization for faster responses on a large dataset, without your team's involvement in database or operating system management.

Which deployment option of PostgreSQL in Azure should you use?

Choose the correct answer

- Azure database for PostgreSQL Single Server
- ✔ Azure database for PostgreSQL Hyperscale (Citus)
- Azure database for PostgreSQL Flexible Server
- PostgreSQL on Azure VMs

Explanation

You should use Azure database for PostgreSQL Hyperscale (Citus). This is a deployment option offered as a Platform-as-a-Service (PaaS) that can scale horizontally by breaking up large data tables into smaller chunks, called shards. Hyperscale (Citus) also enables query parallelization across multiple servers, providing greater performance on datasets of 100 Gb and above.

You should not use Azure database for PostgreSQL Flexible Server or Azure database for PostgreSQL Single Server. Both are PaaS offerings, so Microsoft fully manages database engine and the underlying infrastructure. Single server additionally features Advanced Threat Protection and geo-redundant disaster recovery capabilities, while Flexible server offers more granular access over database configuration and high availability across multiple availability zones. However, none of them is designed to scale horizontally to support accommodation of large datasets or provide query parallelization for a fast response in operational analytics scenarios.

You also should not use PostgreSQL on Azure VMs. This is an Infrastructure-as-a-Service (IaaS) based deployment, where you would need to configure and support the database and the operating system on an Azure VM manually.

Which Azure database product supports key-value and document data models and provides native support for NoSQL?

Choose the correct answer

- Azure SQL Database
- SQL Server on Virtual Machines (VMs)
- ✔ Azure Cosmos DB

Explanation

Azure Cosmos DB supports key-value and document data models and provides native support for Not Only SQL (NoSQL). Azure Cosmos DB is designed as a globally distributed database system with latency in the 99th percentile with less than 10-millisecond (ms) latencies for both reads and writes. In addition to NoSQL, it supports open source SQL (OSS) APIs for MongoDB, Cassandra, Gremlin, and SQL.

NoSQL is an alternative to traditional relational database models and supports a variety of data models such as key-value, document, columnar, and graph formats.

Azure SQL Database and SQL Server on VMs are relational database management systems (RDMS) and do not directly support NoSQL. Azure SQL Database is a cloud implementation of Microsoft SQL Server that lets you migrate on-premises SQL Server databases without having to change your applications. SQL Server on VMs gives you a cloud migration platform that supports Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, and Ubuntu Linux and lets you use bring your own license (BYOL) images.

You are going to start collecting data about your Azure infrastructure with Azure Monitor. Which type of data collection requires you to enable diagnostics?

Choose the correct answer

- Container workload performance
- Usage of Web applications
- Linux virtual machine (VM) health
- ✔ Event logs

Explanation

You must enable diagnostics to use Azure Monitor to collect event log data. In addition, you must enable diagnostics to collect other information such as performance counters and crash logs.

Usage of Web applications, Linux VM health, and container workload performance are all collected by default without having to enable diagnostics. Azure Monitor collects data automatically from a variety of sources, including:

- Application monitoring data
- Guest operating system monitoring data
- Azure resource monitoring data
- Azure subscription monitoring data
- Azure tenant monitoring data

Data collected includes real-time metrics and Azure monitor logs.

You deploy a business critical solution in Azure.

You need to ensure that your resources are replicated and hosted at least 200 miles away within the same geographic area, to minimize impact on your solution's availability in case of disaster.

Which configuration option should you use?

Choose the correct answer

- [x] Region pairs
- [ ] Resource groups
- [ ] Availability zones
- [ ] Availability sets

You should use region pairs. This option consists of two paired Azure datacenters in the same geographic area at least 300 miles away. Using region pairs reduces the likelihood of interruptions in both regions at once in case of a disaster.

You should not use availability sets. This option ensures that your virtual machine remains operational in case of planned or unplanned maintenance events and hardware failures. However, it is effective only within the boundaries of a single datacenter and cannot provide the required redundancy in a region.

You should not use availability zones. This option enables physical separation of zones within a single or multiple datacenters in the same Azure region. It provides higher redundancy than availability sets, but it still does not meet the requirements of at least a 200-mile separation between replicated solution resources.

You should not use resource groups. A resource group is a logical container that holds related Azure resources that share the same lifecycle. It does not provide any resource redundancy capability as required in this scenario.

Which two solutions should you use to transfer an on-premises virtual hard disk (VHD) to Azure? Each correct answer presents a complete solution.

Choose the correct answers

- [x] AzCopy
- [ ] Azure Data Share
- [ ] Azure Files
- [x] Azure Storage Explorer

Explanation

You should use AzCopy or Azure Storage Explorer to transfer an on-premises VHD to Azure.

AzCopy is a command-line tool that can be used to upload and download data to and from Azure Blob storage. AzCopy can be used to transfer data within Azure storage accounts or between storage accounts. It supports both block blobs and page blobs.

You should also use Azure Storage Explorer. This is a graphical user interface (GUI) tool that you can use to manage your Azure Storage resources. With Storage Explorer, you can create and manage storage accounts, blobs, queues, tables, and files. You can also monitor your storage account metrics and access your stored data through the various Storage Explorer features.

You should not use Azure Data Share to transfer an on-premises VHD to Azure. Azure Data Share is a cloud-based storage service offered by Microsoft. It allows users to share data across multiple devices and applications. Data can be accessed by authorized users from any location, and it can be secured using user authentication and encryption.

You should not use Azure Files to transfer an on-premises VHD to Azure. Azure Files is a cloud file storage service from Microsoft Azure that operates like a traditional Server Message Block (SMB) or Network File System (NFS) file server. This makes Azure Files directly accessible by Windows, Linux, and macOS clients.

Your company uses Azure Blueprints to assist with its migration to Azure. User1 should be able to assign published blueprints.

You need to add User1 to the role-based access control (RBAC) role necessary to provide this permission. Your solution should follow the principle of least privilege.

Which role should you assign User1 to?

Choose the correct answer

- Blueprint Contributor
- Contributor
- Owner
- ✔ Blueprint Operator

Explanation

You should assign User1 to the Blueprint Operator role. Members of this role can assign existing published blueprints, but they cannot create new blueprint definitions.

You should not assign User1 to the Owner role. This would enable the user to assign published blueprints, however it would violate the principle of least privilege because the role includes all Azure Blueprint related permissions.

You should not assign User1 to the Contributor role. Members of this role can create and delete blueprint definitions, but they cannot assign published blueprints.

You should not assign User1 to the Blueprint Contributor role. This role enables users to manage but not assign blueprint definitions.

A coworker informs you of a planned Azure maintenance window. You attempt to verify this information using the tool shown in the Exhibit.

You are still uncertain whether the maintenance will impact services you use.

What should you do to determine how this maintenance might impact your organization?

Choose the correct answer

- Select the resource types for your account in Resource Health.
- Check the Azure status page for any planned maintenance outages.
- ✔ Verify any planned maintenance via the Service Health dashboard.
- Use Azure Monitor to view maintenance intervals for your resources.

Explanation

You should verify any planned maintenance via the Service Health dashboard. Azure Service Health is a service that helps you stay informed about the health and availability of your Azure resources. You can use Azure Service Health to get alerts when there are problems with your resources, and to see the status of your resources at a glance. With Azure Service Health, you can also quickly retrieve information about Microsoft's planned maintenance activities.

You should not check the Azure status page for any planned maintenance outages. Azure status is a website that provides information about the global availability and health of Microsoft Azure services. It will not show planned maintenance information for your organization.

You should not use Azure Monitor to view maintenance intervals for your resources. Azure Monitor is a service that allows you to collect, monitor, and analyze data from your resources in Azure. It provides insights into the performance and health of your applications, infrastructure, and network. With Azure Monitor, you can get notified about issues with your resources and take corrective action quickly. It will not show planned maintenance information for your organization.

You should not select the resource types for your account in Resource Health. Resource Health is a service you can use to retrieve status information for your organization's resources. However, Resource Health will not show planned maintenance information.

You need a security solution that helps provision, manage, and deploy Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates.

What should you use?

Choose the correct answer

- Microsoft Defender for Cloud
- Microsoft Defender for Identity
- Azure Information Protection (AIP)
- ✔ Key Vault

Explanation

You should use Key Vault. Key Vault helps provision, manage, and deploy both public and private SSL/TLS certificates.

Key Vault is used to securely store cryptographic keys and other secrets. Additional key vault features include:

- Securing storage and controlled access to token, password, certificates, API keys, and other secrets
- Creating and controlling encryption keys used to encrypt data
- Provisioning, managing, and deploying both public and private SSL/TLS certificates
- Storing secrets and keys protected by software or Federal Information Processing Standard (FIPS)140-2 Level 2 validated hardware security modules (HSMs).

Microsoft Defender for Identity (formerly Azure Advanced Threat Protection [ATP]) does not help provision, manage, and deploy SSL/TLS certificates. Microsoft Defender for Identity is a cloud-based security solution designed to detect and help identify advanced threats and help protect hybrid (cloud and on-premises) computing environments. Microsoft Defender for Identity also does the following:

- Monitor users, entity behavior, and activities
- Help protect user identities and credentials stored in Active Directory
- Provide clear incident information

AIP does not help provision, manage, and deploy SSL/TLS certificates. AIP enables an organization to organize and protect documents and emails through the use of labels. Labels can be applied manually by users or automatically through administrator-defined rules. The classifications make the data identifiable no matter where the data is stored or even if the data has been shared.

Microsoft Defender for Cloud does not help provision, manage, and deploy SSL/TLS certificates. Microsoft Defender for Cloud is designed to help protect Azure cloud, non-Azure cloud, and hybrid computing resources through a set of security tools. These include tools for monitoring the network to prevent, detect, and respond to potential security threats. Microsoft Defender for Cloud provides tools to help strengthen your organization's security posture, protect against threats, and quickly secure your computing environment. It makes it easier to manage your organization's security policies and compliance.

You need to deploy a serverless solution that meets the following requirements:

- Execution is triggered through an HTTP request.
- You pay only for the time that your code runs.
- You do not have to manage the application infrastructure.

Which Azure service should you use?

Choose the correct answer

- Azure SQL Database
- Azure Virtual Machine
- Azure Database for PostgreSQL
- ✔ Azure Functions

Explanation

You should use Azure Functions. This is a serverless platform that lets you execute your code when needed and pay for the actual runtime only, without worrying about configuration or management of the underlying physical and application infrastructure. Azure Functions can be triggered by various event types, including HTTP requests.

You should not use Azure Database for PostgreSQL. This is a relational DB based on the PostgreSQL Community Edition DB engine and offered as a Platform-as-a-Service (PaaS). It cannot be used to host and execute your code on-demand by HTTP requests. With Azure DB for PostgreSQL, you are billed hourly at a fixed rate based on the service tier and compute size selected.

You should not use Azure SQL Database. This is a relational database based on the Microsoft SQL server DB engine and provided as a PaaS. While Azure SQL DB offers the serverless pricing tier, it is intended for the automatic pausing of the database during inactive times, and you are still charged for the database storage. Azure SQL DB is not intended for running your custom code on demand and triggering its execution through HTTP requests.

You should not use Azure Virtual Machine (VM). This is an Infrastructure-as-a-Service (IaaS) offered in Azure, where Microsoft manages the underlying physical infrastructure, while you as a customer are responsible for the rest of the solution: from the operating system and application to data and access. You are billed for the computing resources allocated to the VM and cannot use it as a hosting platform for serverless applications.

You deploy two Azure virtual machines (VMs) running Windows Server 2016 and one VM running Ubuntu Linux. All three VMs and their resources are added to the same resource group. The VMs and the resource group are located in the same Azure region.

The test plan directs that you need to delete the resource group once the initial test cycle is completed.

What is the result of this action?

Choose the correct answer

- [x] All of the VMs contained in the resource group are deleted.
- [ ] Only resource metadata is deleted and the VMs are shut down.
- [ ] Only resource metadata is deleted with no impact on the VMs.
- [ ] Only resource metadata is deleted and access to the VMs is disabled.

Explanation

When a resource group is deleted, all of the resources contained in that resource group are also deleted, including VMs. Resource groups are used to group related resources for easier and more efficient management. Typically, resource groups are used to create a logical group of related resources with a similar lifecycle. The resource group stores metadata about the resources it contains, which can include resources from different Azure regions.

Deleting a resource group deletes the metadata of all contained resources, so that the VMs are not left in place in any state.

You are planning to use Azure for a cloud solution.

You need to choose the most appropriate tool for different scenarios.

Which tools should you use? To answer, drag the appropriate tool to each scenario. A tool may be used once, more than once, or not at all.

Drag and drop the answers

You want to see how much you can save over five years by moving your company's infrastructure to the Azure cloud.	Total Cost of Ownership (TCO) calculator
You want to set up an alert to send you and your coworker text messages when your Azure Resources use 90 percent of your company's monthly Azure budget.	Cost Management
You want to estimate the cost of deploying four virtual machines (VMs) and two SQL Database instances to Azure.	Azure pricing calculator

Azure pricing calculator | Cost Management | Total Cost of Ownership (TCO) calculator

Explanation

You should use the Total Cost of Ownership (TCO) calculator when you want to see how much you can save over five years by moving your company's infrastructure to the Azure cloud. This tool allows you to predict cost savings.

You should use the Cost Management tool when you want to set up an alert to send you and your coworker text messages when your Azure resources use 90 percent of your company's monthly Azure budget. This tool allows you to view historical breakdowns of how much Azure resources cost. You can also set up alerts that get triggered when costs exceed a budget threshold.

You should use the Azure pricing calculator when you want to estimate the cost of deploying four VMs and two SQL Database instances to Azure. This tool allows you to estimate the cost of deploying new resources to Azure.

A company wants to host data disks in the Azure cloud. The data disks must be available to other on-premises machines running Windows, Linux, and macOS using network sharing via Server Message Block (SMB) protocol. Data must be secure both at rest and in-transit.

You need to choose an appropriate storage product solution.

Which storage product should you use?

Choose the correct answer

- Disk storage
- Blob storage
- Archive storage
- File storage ✔

Explanation

You should use file storage. File storage meets all the scenario requirements. Access is provided to other VMs, as well as on-premises, through the use of the SMB protocol, REST, and native client libraries.

You should not use disk storage. Disk storage stores data as a virtual hard disk (VHD) that is available to the VM to which the disk is attached. This storage product does not provide any outside access.

You should not choose blob storage. Blob storage is designed for storing very large quantities of unstructured data. Outside access to application data is supported, but data is stored and accessed as block blobs.

You should not choose archive storage. This is provided as a low-cost storage option for data that is rarely accessed.

Which two options are examples of Conditional Access policies? Each correct answer presents a complete solution.

Choose the correct answers

- [ ] Enable self-service password reset
- [ ] Enable password writeback to on-premises
- [x] Require compliant devices
- [x] Block access by location
- [ ] Create dynamic groups

Explanation

Block access by location and Require compliant devices are examples of Conditional Access policies. Conditional Access policies specify the actions that must be completed or the conditions that must be met to grant access to the requested resource. With the Block access by location policy, you block access for traffic originating from specific countries / regions. With the Require compliant devices policy, you enable access to resources from devices that meet compliance requirements, such as having device encryption enabled or running on certain versions of operating systems.

Enable password writeback to on-premises and Enable self-service password reset are examples of Azure Active Directory (Azure AD) authentication settings. The Enable password writeback to on-premises setting lets your users change their password in Azure AD and replicate password changes back to the on-premises AD environment. The Enable self-service password reset setting reduces administrative effort and the workload on the help desk by allowing end users to unlock their accounts and reset their passwords through Azure AD's self-service functionality.

Create dynamic group is an action in Azure AD where you create a security group or Microsoft 365 group with dynamic group membership rules based on end user or device properties.

You want to perform automated deployments from Azure DevOps. Which of the following enables this process?

Choose the correct options

Azure App Service enables you to perform automated deployments from Azure DevOps.

Explanation

Azure App Service enables you to perform automated deployments from Azure DevOps. Azure App Service is a cloud platform for developing and hosting web applications and services. It enables you to build web apps with ASP.NET, Node.js, PHP, Python, or Ruby on Rails. You can also use Azure App Service to host static websites.

Azure DevOps is a cloud-based set of tools and services for software developers. It includes Continuous Integration/Continuous Delivery (CI/CD) pipelines, control repositories, Structured Query Language (SQL) databases, and container registries. The pipelines component in DevOps can be used to perform automated code deployments.

Azure Data Studio is a data management tool that enables you to connect to and query data stores, build visually stunning reports, and quickly develop custom analytic solutions. It includes built-in support for Azure SQL Database, Azure Cosmos DB, Azure Data Lake Store, and Azure HDInsight. You can also use it to connect to other popular data stores such as MySQL, PostgreSQL, and MongoDB. Azure Data Studio does not enable you to perform automated deployments from Azure DevOps.

Azure SQL is a family of cloud-based relational database services built on Microsoft SQL Server technologies. It offers high availability, scale, and global distribution while still providing the familiarity and compatibility of SQL Server. Azure SQL does not enable you to perform automated deployments from Azure DevOps.

You need to give all users in a group the ability to create and manage all types of Azure resources in a subscription. Rights granted to the users should be kept to a minimum.

Which built-in role-based access control (RBAC) role should you assign to the group?

Choose the correct answer

- Owner
- ✔ Contributor
- Reader
- User Access Administrator

Explanation

You should assign the Contributor role. This role meets the scenario requirements but it keeps the additional permissions allowed to a minimum. The Contributor role does not include the ability to grant access to others.

You should not assign the Owner role. This role would meet the requirement to create and manage resources but it assigns more permissions than required. The Owner role grants full access to all resources and the ability to delegate access to others.

You should not assign the Reader role. This role lets you view but not create or manage Azure resources.

You should not assign the User Access Administrator role. This role lets you manage user access to Azure resources but not create or manage the resources.

Azure RBAC supports over 70 built-in roles. Of these, Owner, Contributor, Reader, and User Access Administrator are the most commonly used.

Identify which statements accurately describe Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS).

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

Statement	Yes	No
The service provider is responsible for all infrastructure hardware in SaaS, PaaS, and IaaS.	◉	○
Creating a virtual machine (VM) running Windows Server 2016 is an example of PaaS.	○	◉
SaaS gives you a way to give users access to sophisticated applications in a pay-as-you-go environment.	◉	○

Explanation

The service provider is responsible for all infrastructure hardware in SaaS, PaaS, and IaaS. This is one of the key advantages of all cloud service models. Subscribers have access to the resources they need but do not have to worry about deploying or maintaining the resources.

Creating a VM running Windows Server 2016 is not an example of PaaS. It is an example of IaaS instead. PaaS is an application development environment that includes the operating system and development tools.

SaaS gives you a way to give users access to sophisticated applications in a pay-as-you-go environment. This gives you a cost-effective way of providing users with applications such as Customer Relationship Management (CRM) applications.

Which Azure resource can be deployed as Infrastructure-as-a-Service (IaaS)?

Choose the correct answer

- [x] Virtual machine (VM)
- [ ] Azure SQL Database
- [ ] Office 365
- [ ] API Management

Explanation

A VM is an example of IaaS because it simulates hardware. With IaaS, the user has full control over the operating system.

Azure SQL Database represents Platform-as-a-Service (PaaS). With PaaS, the user does not have full control over the operating system. The user has control of the PaaS application.

Office 365 represents Software-as-a-Service (SaaS). With SaaS, the user does not have full control over the operating system or an application. The user simply uses the application as a subscription service.

API Management represents PaaS. With PaaS, the user does not have full control over the operating system. The user has control of the PaaS application. An API is a set of operations exposed by an application or service. API Management allows you to provide a level of control to an API.

As part of a cloud migration, your Azure cloud implementation has been initially seeded with 100TB of data.

As the migration continues, you need to periodically migrate data to Azure using Server Message Block (SMB).

Which two solutions should you use to meet this requirement? Each correct answer presents a complete solution.

Choose the correct answers

- [x] Azure Files
- [x] Azure Data Box Gateway
- [ ] Azure Data Box Heavy
- [ ] Azure Data Share

You should use Azure Data Box Gateway to periodically migrate data to Azure using Server Message Block (SMB). Azure Data Box Gateway is a service that enables you to securely transfer large amounts of data to and from Azure Data Box. You can use the Gateway to replicate data between on-premises storage and Azure Data Box, or to transfer data into and out of Azure Storage accounts using your network. Data Box Gateway is a virtual appliance you run on-premises which presents an SMB endpoint to your users.

You should use Azure Files to periodically migrate data to Azure using SMB. Azure Files is a cloud file storage service from Microsoft that operates like a traditional file server. SMB is a file sharing protocol used on Windows operating systems. Using SMB with Azure Files, Windows and other SMB-capable clients can access shared files located in the cloud.

You should not use Azure Data Box Heavy to periodically migrate data to Azure using SMB. Azure Data Box Heavy is a physical data transfer service that allows you to copy large amounts of data (up to 100TB) from your on-premises data center to an Azure datacenter. The data is first transferred to an Azure Data Box appliance, which is then shipped to an Azure datacenter where it is imported into your storage account.

You should not use Azure Data Share to periodically migrate data to Azure using SMB. Azure Data Share is a cloud-based storage service offered by Microsoft. It allows users to share data across multiple devices and applications. Data can be accessed by authorized users from any location, and it can be secured using user authentication and encryption.

For each of the following statements regarding Azure virtual network peering, select Yes if the statement is true. Otherwise, select No.

Statement	Yes	No
Virtual network peering can be used to connect virtual networks across Azure regions.	◉	○
Virtual network peering can be used to transfer data between Azure Active Directory (Azure AD) tenants.	◉	○
Configuring peering requires a short downtime for the peered virtual networks.	○	◉

Explanation

Virtual network peering can be used to connect virtual networks across Azure regions. Azure Virtual Network (VNet) provides logically isolated, private networks in the cloud. By default, all resources on a virtual network can communicate with the internet. VNet also supports inbound connects using public IP addresses and Load Balancers. Virtual network peering is used to connect virtual networks within an Azure region. Peering between regions is also known as Global VNet Peering.

Virtual network peering can be used to transfer data between Azure AD tenants. Peering creates a high-bandwidth, low-latency connection between virtual networks. Transferring data between tenants, subscriptions, and deployment models is supported.

Configuring peering does not require any downtime for the peered virtual networks. Resources can continue to support inbound and outbound connections for the duration of the peering process.

Match each Azure solution to a scenario.

To answer, drag the appropriate solution to each scenario. A solution may be used once, more than once, or not at all.

Drag and drop the answers

Build a baseline behavioral profile of organizational entities to identify anomalous activity.	**Microsoft Sentinel**
Securely store a database connection string to avoid its accidental exposure in a web site's source code.	**Azure Key Vault**
Deny traffic to your Azure Virtual Network resources from known malicious IP addresses.	**Azure Firewall**

Microsoft Sentinel **Azure Key Vault**

Azure Monitor

Explanation

You should use Microsoft Sentinel to build a baseline behavioral profile of organizational entities to identify anomalous activity. Microsoft Sentinel is a security information and event manager (SIEM) platform that can analyze data across the enterprise to identify potential threats, including anomalous activities of users or applications, and help with a faster and smarter response.

You should use Azure Key Vault to securely store a database connection string to avoid its accidental exposure in a web site's source code. Key Vault is an Azure service that allows you securely store and access cryptographic keys, passwords, certificates, and other secrets. To avoid exposure of your backend database's connection string in a web application's source code, you can store it in Azure Key Vault and retrieve it in your application programmatically at run time.

You should use Azure Firewall to deny traffic to your Azure Virtual Network resources from known malicious IP addresses. Azure Firewall is a firewall as a service in Azure that can protect your resources. Through integration with Microsoft Threat Intelligence, Azure Firewall can identify and deny traffic to or from malicious IP addresses and domains.

You should not use Azure Monitor for any of the listed scenarios. Azure Monitor is a monitoring solution that can collect telemetry from your resources to analyze their performance, create alerts, and build dashboards with a system health overview of your Azure and on-premises environments.

For each of the following statements about Azure Virtual Desktop (AVD), select Yes if the statement is true. Otherwise, select No.

Statement	Yes	No
AVD supports Remote Desktop clients on MacOS and iOS.	◉	○
You are charged for the use of AVD on a monthly basis accordingly by active users.	○	◉
AVD users should exist in the same Windows Server Active Directory (AD) that is linked to Azure AD.	◉	○

Explanation

Azure Virtual Desktop (AVD) supports Remote Desktop clients on MacOS and iOS. Other supported platforms include Windows Desktop, Web, Android, and Microsoft Store Client.

You are not charged for the use of AVD on a monthly basis accordingly by active users. AVD is a service that does not require any additional licenses. You can use it with your existing Microsoft 365 or Windows per-user license. However, you are charged for the virtual machines where AVD runs.

AVD users should exist in the same Windows Server AD that is linked to Azure AD. AVD does not support the use of Microsoft accounts or Azure AD B2B when users are sourced from a separate Azure AD tenant.

Which Azure resource can be managed as Software-as-a-Service (SaaS)?

Choose the correct answer

- Azure SQL Database
- API Management
- ✔ Azure Internet-of-Things (IoT) Central
- Virtual machine (VM)

Explanation

Azure IoT Central can be managed as SaaS. With SaaS, the user does not have full control over the operating system or an application. The user simply uses the application as a subscription service. IoT Central is Microsoft's IoT service that makes it easy for users to manage and monitor IoT devices at scale.

VM cannot be managed as SaaS. VM represents Infrastructure-as-a-Service (IaaS) because it simulates hardware. With IaaS, the user has full control over the operating system.

Azure SQL Database cannot be managed as SaaS. Azure SQL Database represents Platform-as-a-Service (PaaS). With PaaS, the user does not have full control over the operating system. The user has control of the PaaS application.

API Management cannot be managed as SaaS. This represents PaaS. With PaaS, the user does not have full control over the operating system. The user has control of the PaaS application. An API is a set of operations exposed by an application or service. API Management allows you to provide a level of control to an API.

You work for a small company that hosts its own web server running Microsoft Internet Information Services (IIS) and email server running Microsoft Exchange. As demand on the web server increases, you want to add a secondary web server to spread out the traffic. As demand decreases, you want to decommission the web server to save energy and maintenance. You consider moving the current infrastructure to the cloud.

You need to determine the benefits of moving the infrastructure to the cloud.

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

Statement	Yes	No
You can use horizontal scaling for the web server.	◉	○
You can resize the disk on demand on mail server if e-mail messages increase.	◉	○
You eliminate the cost of having IT staff.	○	◉

Explanation

You can use horizontal scaling for the web server. With auto-scale, you can configure rules that monitor metrics such as requests, memory usage, and central processing unit (CPU) percentage to determine when Azure should automatically add and remove virtual machine (VM) instances.

You can resize the disk on demand on mail server if e-mail messages increase. Azure is elastic. It allows you to add more resources on demand, as needed.

You do not eliminate the cost of having IT staff by moving the infrastructure to the cloud. However, you can reduce IT costs associated with having expert IT staff. You still need IT staff to handle Infrastructure-as-a-Service (IaaS) tasks.

To improve performance of a mission-critical application, your organization has implemented cloud bursting. Which statement describes the benefit cloud bursting provides?

Choose the correct answer

- Additional virtual machines are added to, and removed from, a compute cluster based on workload.
- Compute, memory, and storage resources are added to cloud-based servers to increase capacity.
- Compute resources are distributed geographically to reduce the impact of power or connectivity failures.
- ✔ Cloud-based resources are provisioned when on-premises servers reach 100% resource capacity.

Explanation

When cloud bursting is configured, cloud-based resources are provisioned when on-premises servers reach 100% resource capacity. Cloud bursting is used in hybrid cloud models consisting of on-premises and cloud-based resources. In a cloud bursting scenario, when the on-premises compute infrastructure is saturated, cloud-based resources come online to address the increased workload.

Vertical scalability describes an environment where compute, memory, and storage resources are added to cloud-based servers to increase capacity. In this scenario, the number of compute nodes is minimized but the performance of each node is enhanced.

Horizontal scalability describes an environment where additional virtual machines are added to, and removed from, a compute cluster based on workload. This allows an application or service the ability to maintain performance during peak usage times, without requiring dedicated resources.

Cloud service providers (CSPs) use zones to distribute compute, storage, and networking resources geographically. This approach helps to reduce the impact of power or connectivity failures. Zones are also often referred to as availability zones.

You need to identify features of resource groups.

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

Statement	Yes	No
Locking a resource group as read-only locks all resources contained in the group.	◉	○
A resource group can contain resources from the same region as the resource group only.	○	◉
You can add a resource to or remove a resource from a resource group as long as the resource group is not locked.	◉	○
Resources can interact with other resources in a different resource group.	◉	○

Explanation

Locking a resource group as read-only locks all resources contained in the group. You can apply locks to a resource group or subscription to prevent deletion or make contained resources read-only. You can also apply locks directly to a resource.

A resource group can contain resources from any region, not just the region in which the resource group is located.

You can add a resource to or remove a resource from a resource group, except when the resource group is locked. You can also move resources between resource groups. A resource can reside in only one resource group at a time. Deleting a resource group will delete all resources contained in that group.

Resources can interact with other resources in a different resource group. The resource group creates a logical resource grouping primarily for management purposes and does not impact access between resources.

For each of the following statements about capital expenditures (CapEx) and operational expenditures (OpEx), select Yes if the statement is true. Otherwise, select No.

Statement	Yes	No
CapEx costs are fixed.	◉	○
Using CapEx for infrastructure spending is a good idea when the demand fluctuates or is unknown.	○	◉
The Pay-as-you-go consumption model qualifies as an OpEx.	◉	○

Explanation

CapEx costs are fixed. CapEx is an upfront cost, and you know exactly how much is being spent. Buying the servers and equipment for a datacenter is a CapEx.

Using CapEx for infrastructure spending is not a good idea when the demand fluctuates or is unknown. On the contrary; CapEx is appealing when you need to predict the cost before the start of a project and plan your expenses accordingly. When the demand fluctuates or is unknown, you should consider OpEx.

The Pay-as-you-go consumption model qualifies as an OpEx. With OpEx, there is no upfront cost and you pay for a service or product as you use it.

A company is deploying a critical business application on two virtual machines (VMs). The deployment needs to support:

- Highly available access
- Separate fault and update zones
- Minimal latency between instances

Most users who need to access the application are in the Azure East US 2 region.

Which configuration should the company use to deploy the solution?

Choose the correct answer

- Separate availability sets
- Separate resource groups in the same region
- ✔ Separate availability zones
- Separate regions in a regional pair

Explanation

The company should use separate availability zones. Regions that support availability zones, including East US 2, provide for three availability zones. Availability zones are deployed in separate datacenters, so interruptions in one availability zone, such as a storage device failure, do not impact the other availability zones. Each availability zone is a separate fault and update zone and has very low latency with other availability zones in the region.

The company should not use separate availability sets. Availability sets are separate deployments in the same datacenter, so they do not provide geographically separated fault or update zones. They do provide separate fault and update zones within a datacenter, but all resources are part of the same datacenter.

The company should not use separate resource groups. This does nothing to meet the scenario requirements. Resource groups are used to define logical resource groups for management purposes. Because both VMs are supporting the same application, it is recommended that both would be part of the same resource group.

The company should not use separate regions in a regional pair. This provides separate fault and update zones but does not minimize latency as required by the scenario.

A common solution would be to deploy the application across two or three availability zones and also configure replication with a regional pair. This provides high-availability and a higher level of support for disaster recovery.

To complete the statement in the answer area, select the appropriate option from the drop-down menu.

Choose the correct options

You use Azure Cost Management and Billing to create cost reports. To understand the data in a cost report, Microsoft recommends you implement [tags.]

Explanation

To understand the data in a cost report, Microsoft recommends you implement tags. Azure tags are labels that can be applied to Azure resources to help you organize and categorize them. You can apply as many tags as you want to a resource, and each tag can have a different key and value. For example, you could apply the tag "Name" with the value "MyWebApp" to an Azure Web App resource. Then, when viewing a list of resources, you could filter them by this tag to only see resources with the tag "Name" and the value "MyWebApp". In addition to cost reporting, tags can also be used in Azure Policy definitions to enforce compliance standards on your Azure resources.

Microsoft does not recommend you use Resource Manager to understand data in a cost report. Azure Resource Manager (ARM) is a management tool that helps you deploy and manage your Azure resources in a consistent, unified way. ARM provides role-based access control and auditing to help you keep control of your Azure environment.

Microsoft does not recommend you use management groups to understand data in a cost report. Management groups provide a hierarchy in Azure that enables you to organize resources and centrally manage access, policies, and compliance for those resources. You can create management groups at any level in the hierarchy, and then move resources into and out of management groups as needed.

Microsoft does not recommend you use resource groups to understand data in a cost report. Azure resource groups are used to manage Azure resources. You can group resources together in a resource group and then deploy, manage, and delete them together as a single unit. Resource groups also help you to control access to your resources. You can control who has access to what resource groups and what actions they can perform on the resources within the group.

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

Statement	Yes	No
A provided physical server is dedicated to your organization's workload only.	◉	○
You can share a provided physical server across your multiple Azure subscriptions.	○	◉
You are charged per number of virtual machines (VMs) deployed.	○	◉

Explanation

A provided physical server is dedicated to your organization's workload only. Azure Dedicated Hosts are isolated physical servers where you run your organization's workload only. They are not shared with any other Azure customers to meet corporate compliance guidelines and standards.

You cannot share provided physical servers across your multiple Azure subscriptions. The underlying physical hosts are single-tenant, so they are dedicated to one Azure subscription only.

You are not charged per number of VMs deployed. Azure Dedicated Hosts are charged per dedicated host, regardless of how many VMs you run on the host.

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

Statement	Yes	No
Azure Files can be accessed using the Server Message Block (SMB) protocol.	◉	○
Azure Files can be accessed using the Network File System (NFS) protocol.	◉	○
A shared access signature (SAS) is required to access Azure Files.	○	◉

Explanation

Azure Files can be accessed using the Server Message Block (SMB) protocol. Azure Files is a cloud file storage service from Microsoft Azure that operates like a traditional file server. SMB is a file sharing protocol used on Windows operating systems. Using SMB with Azure Files, Windows and other SMB-capable clients can access shared files located in the cloud.

Azure Files can be accessed using the Network File System (NFS) protocol. Network File System (NFS) is a file sharing protocol popular on Linux and UNIX-based systems.

A shared access signature (SAS) is not required to access Azure Files. A SAS is a unique identifier that you can use to authorize access to your Azure resources. A SAS contains all the information required to authenticate and access resources, including the resource Uniform Resource Identifier (URI), permissions, and expiry. You can create a SAS manually or programmatically.

Your company has a hybrid Azure cloud infrastructure in Virginia. It consists of Azure virtual machines (VMs), an App Service, a SQL Database instance, and an on-premises web server that hosts a Windows Communication Foundation (WCF) service. You consider using the Azure Service Health feature.

You need to determine the use cases for which Service Health is beneficial.

In which three use cases is Service Health beneficial? To answer, move the appropriate use cases from the list of possible use cases to the answer area and arrange them in any order.

Create a list in any order

Possible use cases

- You want to view App Service performance with Windows Task Manager.
- You want to receive an email when an unauthorized user attempts to access a VM.

Beneficial use cases

- You want to be notified if your App Service usage exceeds the usage quota.
- You want to respond to planned service outages in Virginia.
- You want to implement a webhook on your website to display health incidents.

Explanation

The following are good use cases for Service Health:

- You want to be notified if your App Service exceeds the usage quota.
- You want to respond to planned service outages in Virginia.
- You want to implement a webhook on your website to display health incidents.

Service Health notifies you if your App Service usage exceeds the usage quota. This is referred to as a health advisory.

Service Health allows you to respond to planned service outages in Virginia. It reports planned maintenance at its datacenters.

Service Health allows you to implement a webhook on your website to display health incidents. The payload is a JavaScript Object Notation (JSON) document. You know if the payload is a Service Health incident by inspecting the context.eventSource property and ensuring that its value is ServiceHealth.

Service Health does not allow you to receive emails when unauthorized users attempt to access a VM. Unauthorized login attempts are saved in resource logs.

Service Health does not allow you to view App Service performance with Windows Task Manager. Task Manager allows you to view performance on the local computer.

For each of the described scenarios, select the most appropriate Azure governance methodology.

To answer, select the most appropriate methodology from the drop-down menus.

Choose the correct options

Scenario	Methodology
You need to prevent any users from deleting resources from a subscription with contents spanning multiple resource groups.	Azure Locks
You need to use information from Azure Security Center to develop best practices recommendations for optimization.	Azure Advisor
You need to define a set of policies to help ensure compliance for resources contained in a resource group.	Initiative

Explanation

You should use Azure Locks to prevent any users from deleting resources from a subscription with contents spanning multiple resource groups. Locks can be applied to a subscription, a resource group, or a resource as CanNotDelete or ReadOnly. In this scenario, you would apply a CanNotDelete lock to the subscription which would, in turn, apply to all of the resource groups and resources contained in the subscription.

You should use Azure Advisor to use information from Azure Security Center to develop best practices recommendations for optimization. Azure Advisor provides a consolidated view of recommendations for all Azure resources to help improve the cost effectiveness, performance, high availability, and security of Azure resources.

You should use an Initiative to define a set of policies to help ensure compliance for resources contained in a resource group. An Azure Initiative is a collection of Azure policies targeted towards reaching a single overall goal. This simplifies managing and assigning policy definitions by grouping a set of policies as a single item. The Initiative can then be assigned to a scope and applied to all of the resources contained in that scope.

You should not use Azure Policies in any of the scenarios. You would use Azure Policies to define the policies that you would combine into a set as an Initiative.

You should not use role-based access controls (RBACs) in any of the scenarios. RBACs are used to define granular security for users and groups over management groups, subscriptions, resource groups, and resources.

What is the purpose of a resource group?

Choose the correct answer

- It defines initiatives that allow you to control the type of resources that can be deployed.
- ✔ It serves as a container for Azure resources like virtual machines (VMs) and web apps.
- It specifies the subscriptions that are allowed to create Azure resources.
- It is a collection of user and group accounts.

Explanation

A resource group serves as a container for Azure resources like VMs and web apps. You can then assign role-based access security (RBAC) permissions to a resource group to determine which users can access the Azure services.

A resource group does not define initiatives that allow you to control the type of resources that can be deployed. Azure Policy performs this function.

A resource group is not a collection of user and group accounts. Collections of users and groups are normally defined in Active Directory or a directory service.

A resource group does not specify the subscriptions that are allowed to create Azure resources. A subscription is essentially a billing unit.

Which example best describes authorization?

Choose the correct answer

- Students who enter their password to check their grades at university.
- ✔ People who present their birth certificate to prove that they are eligible to receive government age-based benefits.
- Banking customers who enter their personal identification number (PIN) number to log into an ATM.
- Passengers who present their driver's license to prove their identity before boarding a flight.

Explanation

Authentication is the process of proving that somebody is who they say they are, whereas authorization is the act of granting an authenticated person permission to do something.

People presenting their birth certificate to prove that they are eligible to receive government age-based benefits is a good example of authorization. Authorization is the process of verifying that an authenticated user has access to certain functions. In this scenario, the person is already authenticated and now the age on the birth certificate verifies that the user has a right to receive government age-based benefits.

Passengers presenting their driver's license to prove their identity before boarding a flight is not an example of authorization. It is an example of authentication. Authentication establishes the identity of a person. The picture on the driver's license helps to prove that the person who holds the license is the person whose picture is on the license, but it does not necessarily authorize the person to board the plane.

Banking customers entering their PIN number to withdraw money from an ATM is not an example of authorization. The PIN (and other passwords) are a form of authentication and ensure that the person who has the bank card is the person who owns the bank account, but it does not necessarily grant the user permission to do something.

Students entering their password to check their grades at university is not an example of authorization. The password helps to determine whether the person that is checking the grades is the actual student, but it does not authorize the authenticated party to do something.

Which statement best describes what a resource lock does to a virtual machine (VM)?

Choose the correct answer

- It allows the VM to be deleted, but not modified.
- ✔ It prevents the VM from being deleted.
- It forces the VM to be deleted within a specific time period.
- It forces the VM to be deleted immediately.

You are considering moving some of your applications to Azure as container instances. However, your manager wants you to explain to them about containers and their benefits first.

You need to explain containers to your manager.

Which four descriptions of containers are accurate? To answer, move the appropriate descriptions from the list of possible descriptions to the answer area and arrange them in any order.

Create a list in any order

Possible descriptions

- A container requires you to manually install dependencies.
- A container requires you to configure the host virtual machine.

Container descriptions

- A container can be accessed over the Internet by IP address or domain name.
- A container can run on Windows or Linux.
- A container can scale out as needed.
- A container represents a single app and its dependencies.

Explanation

A container can be accessed over the Internet by IP address or domain name. This is similar to a virtual machine (VM). With Azure Container Instances, you can specify the Domain Name Server (DNS) name label, allowing your container to be reachable at [dnsnamelabel].[region].azurecontainer.io.

A container can run on Windows or Linux. You specify the operating system when you create the container group. With Azure Container Instances, a container group is a group of containers that all run on the same host VM. This means that the group itself is tied to an operating system. So all containers in the container group share the same operating system.

A container can scale out as needed. You do not need to use custom scaling rules as you do with App Services.

A container represents a single app and its dependencies. This allows you to package, deploy, and manage the container as a unit.

A container does not require you to configure the host VM. Azure manages the host VM.

A container does not require you to manually install dependencies. A container represents a single app and its dependencies. The dependencies are installed automatically.

You are asked about the differences between Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS).

You need to explain what each service type means.

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

Statement	Yes	No
IaaS allows you to rent hardware and have control over the operating system (OS).	●	○
PaaS allows you to manage applications without controlling the underlying OS.	●	○
SaaS allows you to subscribe to software.	●	○

Explanation

IaaS allows you to rent hardware and have control over the OS. This includes virtual machines (VMs), storage, and virtual networks (VNets). With IaaS, you create the VMs, attach storage devices to them, and assign the VMs to VNets that you create. You control the applications that are installed on the VM. OS updates are automatically handled by Azure.

PaaS allows you to manage applications without controlling the underlying OS. This includes development frameworks and databases, such as Azure SQL Database. With PaaS, you do not create the VM. You only have control of the applications on the VM.

SaaS allows you to subscribe to software. An example is Office 365.

References

You are researching the governance methodologies in Azure. You want to understand role-based access security (RBAC), policies, initiatives, locks, and Azure Advisor.

You need to choose the type of resource or feature to use for different scenarios.

When should you use each resource or feature? To answer, drag the appropriate resource or feature to each scenario. A resource or feature may be used once, more than once, or not at all.

Drag and drop the answers

You want to control the users who are allowed to create virtual networks (VNets).	RBAC
You want to review security recommendations related to your deployed resources.	Advisor
You want to prevent virtual machines (VMs) from being deployed in a subscription.	Policy

RBAC | Advisor | Policy | Loc

Explanation

You should use RBAC to control the users who are allowed to create VNets. RBAC assigns permissions that apply to users and groups.

You should use Advisor to review security recommendations for your deployed resources. Advisor integrates with Security Center to allow you to detect issues before they occur. You can then view recommendations to help mitigate the threat.

You should use a policy in this scenario. A policy definition is a JSON file that is assigned to a scope, such as a resource group, or a subscription. The JSON file defines the rules that are to be taken for certain resources. You can use a policy to enforce rules that apply to ensure compliance and identify non-compliant resources, to define which resources have to be deployed and which do not, and to set the allowed size and configuration of the respective resource (e.g. size of a VM).

You should not use a lock when you want to prevent VMs from being deployed in a subscription. Resource locks help to prevent accidental modification or deletion of a resource, subscription, or resource group. You can create a Read-only resource lock at the subscription, resource group, or resource level. The lock level can be set to CanNotDelete or ReadOnly. If you create a lock at the subscription level, it prevents any kind of modification to the whole subscription. In this scenario, only resource of type VM has to be affected. Creating a policy is the correct approach.

You should not use an initiative in this scenario. An initiative allows you to manage a collection of policies.

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

Statement	Yes	No
ExpressRoute traffic is routed through a private connection.	◉	○
Traffic between peered virtual networks (VNets) is routed over the public internet.	○	◉
A VNet is created within the scope of a region.	◉	○

Explanation

ExpressRoute traffic is routed over a private connection. ExpressRoute is enabled through a connectivity provider at a co-location facility that lets you link your on-premises networks to Microsoft cloud services, such as Microsoft Azure and Microsoft 365.

Traffic between peered virtual networks (VNets) is not routed over the public internet. Instead, it is routed through the Microsoft backbone infrastructure without the involvement of the public internet.

A VNet is created within the scope of a region. A VNet is a regional resource. However, VNets from different regions can still be connected to each other via Global VNet peering using internal Microsoft connectivity in Azure or via VPN gateways using the public internet.

A company has an Azure Active Directory (Azure AD) Premium P1 subscription. The company has a hybrid environment that uses both Azure AD and on-premises federated AD using Active Directory Federation Services (AD FS).

The company is upgrading its security and must configure Azure AD self-service password reset (SSPR) and Multi-Factor Authentication (MFA). You need to identify the authentication types that are supported by both SSPR and MFA.

Which three authentication types are supported by both SSPR and MFA? Each correct answer presents a complete solution.

Choose the correct answers

- [ ] Security questions
- [ ] App password
- [x] Voice call
- [ ] Email address
- [x] Password
- [x] SMS

The authentication types supported by both SSPR and MFA are:

- Password
- SMS
- Voice call

Password refers to your Azure Active Directory (Azure AD) password. This authentication method cannot be disabled. You must know your current password to change your own password through SSPR. If SSPR has been configured properly, users whose passwords are not working can verify their identity through another device or phone number or answer security questions to set a new password.

You can use SMS to receive a verification code as a text message that you would then enter in the sign-in interface for authentication. With a voice call, you would answer the call and then press # for authentication.

In addition, Microsoft Authenticator app supports MFA and SSPF in public preview and OATH Hardware token supports SSPR and MFA in public preview.

Security questions and email addresses are supported authentication methods, but for SSPR only.

App password is supported for MFA, but not in all cases. App passwords are used to authenticate non-browser applications.

Match each Azure Cloud Adoption Framework (CAF) methodology with its description.

To answer, drag the appropriate methodology to each description. A methodology may be used once, more than once, or not at all.

Drag and drop the answers

Define the business justification and the expected outcomes of adoption.	Strategy
Align actionable adoption plans with business outcomes.	Plan
Prepare the cloud environment for the planned changes.	Ready
Develop new cloud-native or hybrid solutions.	Innovate

80%

Using the Strategy methodology, you define the business justification and expected outcomes of adoption. You should define and document your motivations behind cloud adoption, agree on specific business outcomes with stakeholders and executives, develop a business case to validate relevant financial models, and choose the right first project that can help to align motivations with required technical efforts.

Using the Plan methodology, you align actionable adoption plans with business outcomes. You create an inventory of your digital estate, establish plans for initial organizational alignment, and the ways to address skill readiness gaps. Eventually, you develop a cloud adoption plan to manage planned changes across the digital estate, organization, and skills.

Using the Ready methodology, you prepare the cloud environment for the planned changes. As a part of readiness preparation, you review the Azure setup guides, choose the most appropriate option for hosting your cloud workload, expand it to meet your cloud adoption plan's platform requirements, and validate your modifications against Azure best practices.

Using the Innovate methodology, you develop new cloud-native or hybrid solutions. Innovation can provide the greatest business value by unlocking new technical skills and expanding business capabilities. You should achieve consensus on the hypothetical business value, consider various tools from the Azure innovation guide, adopt best practices as a part of the cloud architecture, and enable an effective feedback loop throughout your cloud solution's development process.

Azure CAF brings together cloud adoption best practices and provides a set of tools, guidance, and narratives to drive desired business outcomes during your cloud adoption process. On top of the Strategy, Plan, Ready, and Innovation methodologies described above, CAF also includes Migrate, Govern, Manage, and Organize.

You need to compare the costs of running an application workload in Azure versus on-premises.

What should you do to ensure that you can use the Azure TCO calculator to complete this task?

Choose the correct answer

- [x] Define the server, database, storage, and networking workload.
- [ ] Create an authorized service account in Azure Active Directory (Azure AD).
- [ ] Initiate a paid Azure cloud subscription for your organization.
- [ ] Determine the app's compute, storage, and network requirements.

Explanation

You should define the server, database, storage, and networking workload. The Azure total cost of ownership (TCO) calculator is a tool that allows you to estimate the TCO for running your applications on Microsoft Azure. The calculator takes into account factors such as compute, storage, bandwidth, and management costs. You can also specify whether you want to run your applications in the cloud or on-premises. You can define your workload by specifying the server, database, storage, and networking resources that your application uses.

You do not need to create an authorized service account in Azure AD. The TCO calculator is free to use and it does not require you to use an Azure AD account. Azure AD accounts are used to facilitate authentication and authorization for access to your Azure resources.

You do not need to determine the app's compute, storage, and network requirements. This task is generally performed when the application is first deployed.

You do not need to initiate a paid Azure cloud subscription for your organization. The TCO calculator is free to use.

To complete the sentence, select the appropriate option from the drop-down menu.

Choose the correct options

Cloud computing is the delivery of computing services such as compute power, storage, software and analytics over the internet.

Explanation

Cloud computing is the delivery of computing services, such as compute power, storage, networking, software and analytics over the internet. You rent those computing resources from a cloud service provider and only pay for what you use.

CapEx is the spending of money on products and services upfront, and then deducting that expense from your tax bill over time. Setting up an on-premises datacenter is an example of CapEx.

OpEx is the spending of money on products and services and being billed for them as you use them. With OpEx, there are no upfront costs because you pay for the actual consumption. Use of Azure services is an example of OpEx.

Your company plans to use Azure Blueprints to support rapid deployment through built-in components and following organizational compliance.

Which statements accurately describe the features and functionality of Azure Blueprints?

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

Statement	Yes	No
When a blueprint is updated and the updated version is published, any assignments of the blueprint are updated automatically.	○	◉
When a blueprint is unassigned, all of the resources assigned by the blueprint remain in place, but blueprint resource locking is removed.	◉	○
When you delete a core blueprint, any assigned versions of the blueprint remain in place.	◉	○

Explanation

When a blueprint is updated and the updated version is published, any assignments of the blueprint are not updated automatically. You must update the blueprint assignment with the new updated version of the assignment.

When a blueprint is unassigned, all of the resources assigned by the blueprint remain in place, but blueprint resource locking is removed. This also results in the deletion of the blueprint assignment object.

When you delete a core blueprint, any assigned versions of the blueprint remain in place. A blueprint must be unassigned before it can be deleted.

A company is reviewing security for virtual machines (VMs) deployed on its hybrid cloud.

You need to identify security features provided through Microsoft Defender for Cloud.

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

Statement	Yes	No
Microsoft Defender for Cloud supports monitoring, security recommendations, and advanced threat protection for cloud and on-premises virtual machine (VM) resources.	●	○
Microsoft Defender for Cloud provides native integration with Microsoft Defender Antivirus in Windows.	●	○
Microsoft Defender for Cloud support is limited to Windows operating systems only.	○	●
Microsoft Defender for Cloud can automatically discover and assess security for new Azure resources as they are deployed.	●	○

Explanation

Microsoft Defender for Cloud supports monitoring, security recommendations, and advanced threat protection for cloud and on-premises VM resources. This means that resources and workloads are protected across a hybrid environment, whether or not they are deployed in Azure.

Microsoft Defender for Cloud provides native integration with Microsoft Defender Antivirus in Windows as well as other Microsoft security solutions, such as Microsoft Defender for Cloud Apps. These protections can be extended to other cloud and on-premises resources.

Microsoft Defender for Cloud support is not limited to Windows operating systems only. It supports Windows Server 2008 and later and multiple versions of eight Linux operating system distributions.

Microsoft Defender for Cloud can automatically discover and assess security for new Azure resources as they are deployed. Monitoring and discovery is a continuous process. For multi-cloud and hybrid environments protection can be extended with the help of AzureArc.

You deploy three virtual machines (VMs) to Azure as a three-tiered architecture. One VM hosts a front-end web application, one VM hosts a business application programming interface (API), and the other VM hosts a Microsoft SQL Server database. Only the front-end web application should be publicly accessible, and it should be accessible over HTTP on port 80. All three VMs must be accessible over Remote Desktop Protocol (RDP) on port 222. Only your account should be able to use RDP to access the VMs.

You need to determine how Network Security Groups (NSGs) can be used in this scenario.

Which two ways can NSG rules be used? Each correct answer presents a complete solution.

Choose the correct answers

- [ ] To ensure that only your account can use RDP to access the VMs
- [x] To ensure that only the front-end VM is publicly accessible over port 80
- [ ] To ensure that the front-end VM hosts only web applications
- [x] To ensure that all three VMs are accessible over port 222

Explanation

An NSG can ensure that all three VMs are accessible over port 222. An NSG acts like a firewall. It defines rules that allow or deny inbound and outbound traffic.

An NSG can ensure that only the front-end VM is publicly accessible over port 80. An NSG acts like a firewall. It defines rules that allow or deny inbound and outbound traffic.

An NSG cannot ensure that the front-end VM hosts only web applications. You cannot use an NSG to restrict applications on a VM. This is an IT management issue.

An NSG cannot ensure that only your account can use RDP to access the VMs. You cannot use an NSG to restrict user account access to a VM. You must use role-based access control (RBAC) to accomplish this.

Your company suffers a catastrophic web outage due to a misconfigured driver on a database server.

You need to find a cloud solution that allows the highly customized web application to run without requiring management of operating system settings or services. However, the company's web developers must be able to maintain customizations.

What should you do to meet these requirements?

Choose the correct answer

- Migrate the web app to serverless compute.
- Relocate the web app to an infrastructure as a service (IaaS) provider.
- ✔ Deploy the web app functionality using platform as a service (PaaS).
- Move the web app to a software as a service (SaaS) provider.

Explanation

You should deploy the web app functionality using platform as a service (PaaS). PaaS is a type of cloud computing that provides a platform for developers to build, run, and manage applications without the need for infrastructure management. PaaS includes all the tools and services required to develop, test, deploy, and scale applications. Typically, PaaS providers offer a wide variety of services, including databases, analytics, workflow engines, and more.

You should not move the web app to a software as a service (SaaS) provider. SaaS is software that is hosted on the cloud and available to customers over the Internet. Microsoft Office 365 is an example of SaaS.

You should not migrate the web app to serverless compute. In serverless computing, the customer simply submits their application code, and the cloud service provider (CSP) provisions and maintains the servers and infrastructure required to run an application. Azure Functions is an example of a serverless compute platform.

You should not relocate the web app to an infrastructure as a service (IaaS) provider. An IaaS solution will require the organization to manage the underlying OS and services. In IaaS, network, compute, and storage resources are offered by a cloud provider.

You work for a cloud solution provider. One of your company's clients considers moving its on-premises infrastructure to the cloud. However, the client wants a better understanding of the different models before it makes a decision. A third-party will not be involved.

You need to describe the advantages of the different cloud models.

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

Statement	Yes	No
The public cloud allows you to deploy resources without managing the underlying hardware.	◉	○
The hybrid cloud allows you to deploy resources with no capital expenditure and minimal IT expertise.	○	◉
The private cloud allows you to deploy resources by having minimal IT expertise.	○	◉

Explanation

The public cloud allows you to deploy resources without managing the underlying hardware. The servers, storage devices, and networking devices exist in Azure datacenters. You are only required to manage the configuration of those devices.

The hybrid cloud typically allows you to deploy resources with some capital expenditure. Capital expenditure (CapEx) involves spending money on physical resources up front. With the hybrid cloud, some resources exist in the cloud, while other resources usually exist on-premises. The CapEx costs come from the on-premises resources. Some hybrid deployments can also involve a combination of public and private clouds, which requires IT expertise.

The private cloud requires you to have IT expertise in order to deploy resources, unless you are using a third-party company as the private cloud provider. This is because on a private cloud that is not third-party hosted, you are responsible for managing the hardware, such as servers, storage devices, and networking devices, as well as for the configuration of these resources.

Which of the following allows you to assign permissions to users so that they can create resources in Azure?

Choose the correct answer

- Resource groups
- ✔ Role-based access control (RBAC)
- Initiatives
- Policies

Explanation

RBAC allows you to assign permissions to users so that they can create resources in Azure. This allows you to control which users are allowed to create resources.

Policies do not allow you to assign permissions to users. Policies allow you to specify what type of resources can be created.

Initiatives do not allow you to assign permissions to users. Initiatives allow you to group policies together.

Resource groups do not allow you to assign permissions to users. Resource groups allow you to group resources together.

References

To complete the sentence, select the appropriate option from the drop-down menu.

Choose the correct options

Defense in depth is a strategy to implement multiple layers of security to slow down an attack and provide early alert telemetry to act upon.

Explanation

Defense in depth is a strategy to implement multiple layers of security to slow down an attack and provide early alert telemetry to act upon. It removes reliance on any single layer of protection and ensures that if one layer is breached, a subsequent layer is already in place to prevent further exposure. In Azure, defense in depth consists of Physical Security, Identity & Access, Perimeter, Network, Compute, Application, and Data layers.

Application Insights is a feature of Azure Monitor that allows you to monitor your live applications. It can automatically detect performance anomalies, help to diagnose issues, and provide insight on how your app is being used.

Azure Cognitive Services are RESTful Application Programming Interfaces (APIs) and client library Software Development Kits (SDKs) that you can use to add cognitive features to your applications. Azure Cognitive Services provides pre-trained machine learning algorithms in the areas of vision, speech, language, decision, and search.

Customer Lockbox is an interface that lets Azure customers review and approve data access requests raised by Microsoft engineers. By default, the Microsoft support team has no access to customer data. Through the Customer Lockbox an engineer who performs troubleshooting can request such access. However, the final decision remains with the Azure customers who may authorize or reject access to their data in Azure.

Match each statement with the Azure compute service being described.

To answer, drag the appropriate type to each description. A service may be used once, more than once, or not at all.

Drag and drop the answers

Includes a virtual processor, memory, storage, and networking resources.	Azure Virtual Machines
Is a lightweight, virtualized application environment.	Container Instances
Includes the abstraction of servers, infrastructure, and operating systems.	Azure Functions

Explanation

Azure Virtual Machines includes a virtual processor, memory, storage, and networking resources. Azure Virtual Machines allows you to create and use virtual machines in the cloud. A virtual machine is created by software that emulates the characteristics of a real computer system, often allowing multiple virtual operating systems to run on one physical computer. Virtual machines are often used to create web servers, development environments, and testing environments. They can be customized to run specific operating systems and applications. Users can access their virtual machines using a remote desktop connection.

Container Instances is a lightweight, virtualized application environment. Containers provide many of the same benefits as virtual machines and are designed to be portable and largely self-contained. They are typically composed of the binaries and libraries required to run a single app or service. Due to their small footprint and compute/memory requirements, containers are typically faster and cheaper to deploy than comparable virtual machines. Docker is a popular container ecosystem.

Azure Functions includes the abstraction of servers, infrastructure, and operating systems. Functions provides a way to run small pieces of code, or "functions", in the cloud. Functions can be triggered by events, like a Hypertext Transfer Protocol (HTTP) request or a message in a queue, or they can run on a schedule. They are easy to write and use, and they scale automatically. You can also use Azure Functions to call other Azure services, like Storage or Cosmos DB.

Your company is reorganizing after acquiring a new company. Both your company and the new company have their own Azure Active Directory (Azure AD) tenants.

You need to determine what happens when you transfer the billing ownership of a subscription from an account in your Azure AD tenant to an account in another Azure AD tenant and associate the subscription with the new directory.

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

Statement	Yes	No
All users and groups with role-based access to manage the subscription lose their access.	◉	○
System-assigned Managed Identities are re-enabled automatically.	○	◉
Moving a subscription that owns an Azure Kubernetes Service (AKS) cluster causes the cluster to lose functionality.	◉	○

Explanation

When you transfer the billing ownership of a subscription from an account in your Azure AD tenant to an account in another Azure AD tenant, you are not required to associate the subscription with the new directory. If you choose to associate the subscription with the new directory, this results in several changes.

All users and groups with role-based access to manage the subscription lose their access. This also applies to any other service principals. RBAC assignments do not carry over when you associate the subscription with a new tenant. Classic subscription administrators such as Service Administrators and Co-administrators also lose access. The only user initially able to manage resources in the subscription is the user account that accepts the transfer.

System-assigned Managed Identities are not re-enabled automatically and must be re-enabled after the transfer. Any user-assigned Managed Identities must be recreated.

Moving a subscription that owns an Azure Kubernetes Service (AKS) cluster causes the cluster to lose functionality. This is due to lost service principal rights and lost role assignments.

For each of the following statements regarding consumption and fixed cost price models, select Yes if the statement is true. Otherwise, select No.

Statement	Yes	No
For organizations with consistent, high utilization, the consumption-based pricing model is the most efficient one.	○	◉
There are no upfront costs when using the consumption-based model.	◉	○
In the fixed price model, you pay for resources even if you do not use them.	◉	○

Explanation

For organizations with consistent, high utilization, the consumption-based pricing model is not the most efficient one. When you have a consistent need for compute, storage, and network resources, it is more cost-efficient to reserve resources using the fixed price model. When you enter a one-year or three-year commitment, Azure passes on significant discounts of up to 72%. Consumption-based pricing is better for periodic or one-off needs.

There are no upfront costs when using the consumption-based model. You create or launch the resources you need, and you are only charged for the usage amount. You know exactly what you will pay per unit of time or usage when you activate the resource.

In the fixed price model, you pay for resources even if you do not use them. This means that if you enter a one-year commitment for a server virtual machine, you will pay the same amount if the server is on for one hour a day or 24 hours a day.

Your company is planning a deployment using Azure Database for PostgreSQL. The deployment should meet the following requirements:

- Up to 10 TB storage
- Azure Premium Storage
- Point-in-time-restore for up to 35 days

You need to select the appropriate deployment and pricing tier to meet these requirements and minimize costs.

What should you select?

Choose the correct answer

- Azure Database for PostgreSQL Single Server Basic tier
- Azure Database for PostgreSQL Hyperscale (Citus)
- ✔ Azure Database for PostgreSQL Single Server General Purpose tier
- Azure Database for PostgreSQL Single Server Memory Optimized tier

Explanation

You should select Azure Database for PostgreSQL Single Server General Purpose tier. This is the most cost-effective option that meets all of the requirements. The General Purpose tier supports data storage of up to 16 TB and uses Azure Premium storage. Point-in-time restore is met by all Azure Database for PostgreSQL deployments.

You should not select Azure Database for PostgreSQL Single Server Basic tier. This option does not meet the storage size or storage type requirements. Storage is limited to 1TB and is limited to Azure Standard Storage.

You should not select Azure Database for PostgreSQL Single Server Memory Optimized tier. This option meets your requirements but is more expensive than the General Purpose pricing tier.

You should not select Azure Database for PostgreSQL Hyperscale (Citus) because of the cost of this option. You would use this option, for example, if you need to support horizontally scaled queries across multiple machines using sharding.

Your company is planning to move its infrastructure to the Azure cloud.

You need to explain the subscription model.

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

Statement	Yes	No
A subscription can contain one or more resource groups.	◉	○
A subscription can have only one license.	○	◉
Multiple subscriptions can be owned by a single organization.	◉	○

Explanation

A subscription can contain one or more resource groups. In Azure, a subscription determines how you are billed for resource usage. Before creating a resource in your subscription, you need to have a resource group. An example of a resource is a virtual machine (VM). You are billed based on the size of the VM and how long that VM is up and running.

A subscription can and almost always will have multiple licenses. Licenses are assigned to each user account.

Multiple subscriptions can be owned by a single organization. This allows for scenarios such as a development subscription and a production subscription.

You are planning to use Azure for your company's cloud infrastructure. You just learned that Azure supports Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) offerings.

You need to determine the resources that are available for each category.

Which resource does each type of infrastructure make available? To answer, select the appropriate resources from the drop-down menus.

Choose the correct options

SaaS: Outlook

PaaS: Azure SQL Database

IaaS: Virtual machine (VM)

Explanation

SaaS offers Outlook. With SaaS, you do not manage the operating system or an application, but you can manage the application's users.

PaaS offers Azure SQL Database. With PaaS, you do not manage the operating system, but you can manage the application that runs on the operating system.

IaaS offers a VM. With IaaS, you do not manage the physical hardware, but you can manage the operating system and configuration. With a VM, you have full control over the operating system and configuration, such as assigning an IP address to a virtual network adapter.

Skype is a SaaS offering because it only allows you to manage its users.

IoT Hub is a PaaS offering because it allows you to manage an application.

SQL Server 2016 on Linux is an IaaS offering because you can manage the Linux operating system.

What is the maximum length of time you can use the credits from an Azure free subscription before it expires?

Choose the correct answer

- 12 months
- 24 months
- ✔ 30 days
- 6 months

Explanation

A free Azure subscription is good for 30 days before you have to upgrade. The subscription includes $200 credit that can be used any time within the first 30 days. Any credit left over after the first 30 days does not carry over.

After using your credit or when your subscription expires, you can upgrade to Pay-As-You-Go for paid services. Services offered as free with the subscription, such as storage within limits, will continue to be free for 12 months.

References

In the Infrastructure-as-a-Service (IaaS) cloud service model, the subscriber is responsible for the management of which two components? Each correct answer presents part of the solution.

Choose the correct answers

- [ ] Virtualization
- [x] Operating system (OS)
- [ ] Physical Networking
- [ ] Storage
- [x] Applications

In the IaaS model, subscribers are responsible for management of:

- Applications
- Data
- Runtime
- Middleware
- OS

The service provider is responsible for:

- Virtualization
- Servers
- Storage
- Physical Networking

In the Platform-as-a-Service (PaaS) model, the subscriber is responsible for applications and data only. The service provider is responsible for all of these components in the Software-as-a-Service model.

Match each type of cloud computing with its description.

To answer, drag the appropriate type to each description. A type may be used once, more than once, or not at all.

Drag and drop the answers

Cloud resources are owned and operated by a service provider and delivered over the Internet.	Public cloud
Cloud resources are maintained on a private network and used exclusively by one business or organization.	Private cloud
This is a combination of on-premises infrastructure with a public cloud.	Hybrid cloud

Explanation

With a public cloud, cloud resources are owned and operated by a service provider and delivered over the Internet. The use of a public cloud does not require any upfront purchase of hardware or software because it is leased by the cloud service provider, and you pay only for the service you use.

With a private cloud, cloud resources are maintained on a private network and used exclusively by one business or organization. Resources are not shared with others as in a public cloud, so there is a higher level of control and privacy to meet specific business, legal, or security requirements.

A hybrid cloud is a combination of on-premises infrastructure with a public cloud. It allows organizations to run relevant services and solutions in the most appropriate location.

Match each Azure resource to a scenario.

To answer, drag the appropriate resource to each scenario. A resource may be used once, more than once, or not at all.

Drag and drop the answers

Migrate a workload from an on-premises Hyper-V host to Azure, still retaining full control over the operating system.	Azure Virtual Machine (VM)
Deploy a web application using Platform-as-a-Service (PaaS) for scalability and security.	Azure App Service
Build an event-driven solution and pay only for the time spent running your code.	Azure Functions

Explanation

You should use an Azure VM to migrate a workload from an on-premises Hyper-V host to Azure, still retaining full control over the operating system. Azure VM is an Infrastructure-as-a-Service (IaaS) offering that provides flexibility of virtualization with full control over the computing environment, without the need to buy and maintain physical hardware.

You should use Azure App Service to deploy a web application using PaaS for scalability and security. Using App Service allows you to focus on building your web solution, while Azure handles the management of the underlying infrastructure.

You should use Azure Functions to build an event-driven solution and pay only for the time spent running your code. Azure Functions is a serverless platform where execution of your code is triggered by a specific type of event. It uses a pay-per-use pricing model, so you are charged only for the run time of your code.

You should not use Azure Traffic Manager for any of these scenarios. Azure Traffic Manager is a DNS-based traffic load balancer that allows optimal distribution of traffic to Azure resources spread across various Azure regions and geographies.

For each of the following statements about shared responsibility in the cloud, select Yes if the statement is true. Otherwise, select No.

Statement	Yes	No
The customer always retains responsibility for the data.	◉	○
The responsibility for the management of accounts is transferred to the cloud provider.	○	◉
The responsibility for the operating system in Platform-as-a-Service (PaaS) is retained by the customer.	○	◉

Explanation

The customer always retains responsibility for the data. The cloud provider is always responsible for the underlying physical infrastructure. Additionally, the cloud provider may own upper-level components, such as the operating system in the case of PaaS deployment, or even the application itself as with Software-as-a-Service (SaaS) solutions. However, responsibility for the data, end-user devices, accounts, and access management is always retained by the customer.

The responsibility for the management of accounts is not transferred to the cloud provider. Whether the deployment type is Infrastructure-as-a-Service (IaaS), PaaS, SaaS, or an on-premises datacenter, the customer always retains responsibility for management of accounts. They decide how to provision end-user and system accounts, password complexity, and level of access, depending on the tools and interface enabled by their cloud providers.

The responsibility for the operating system in PaaS is not retained by the customer. In IaaS and on-premises deployments, the customer is responsible for the purchase, installation, configuration, and management of the operating system. However, in PaaS and SaaS deployments, ownership and responsibility are transferred to the cloud provider.

You are a cloud engineer for a retail company. You need to decide whether to use a public or a private cloud.

What is an advantage of using a public cloud over a private cloud?

Choose the correct answer

- Greater security is provided for tenant data.
- The environment supports a higher level of customization for each tenant.
- On-demand scalability allows business requirements to be met more efficiently.
- ✔ Costs are lower and spread among multiple tenants.

Explanation

An advantage of a public cloud over a private cloud is that costs are lower and spread among multiple tenants. This is possible because subscribing tenants share resources and the provider can take advantage of economies of scale. A public cloud also usually has a higher level of reliability because it is based on a larger network of servers.

A private cloud provides greater security than a public cloud for tenant data. A private cloud is based on a private network, including storage resources, and this means that access is limited to subscribing tenants. Tenants share storage resources on a public cloud and data is partitioned among them.

The public cloud environment does not support a higher level of customization for each tenant. There is a level of customization available, but this is somewhat limited by the shared environment. A high level of customization is a feature of private clouds because of the tenant's exclusive access.

On-demand scalability is a feature of both public and private clouds and is not an advantage of either over the other.

References

You deploy a new Linux virtual machine (VM) and then manually adjust its configuration in Azure portal to meet the requirements of your Development environment.

You need to capture changes made to the Development VM's configuration after the original deployment, so that you can reuse it as a template in the deployment of Test and Production VMs.

Which two actions can you perform to achieve your goal? Each correct answer presents a complete solution.

Choose the correct answers

- [x] Export the Azure Resource Manager (ARM) template from a resource group.
- [ ] Export the Azure Resource Manager (ARM) template before deployment.
- [ ] Export the Azure Resource Manager (ARM) template from deployment history.
- [x] Export the Azure Resource Manager (ARM) template from a resource.
- [ ] Replace the Development VM with a VM scale set.

Explanation

You should either export the ARM template from a resource or from a resource group. ARM templates can be used to represent the desired state of your Azure resources. They can be repeatedly and consistently deployed throughout the development lifecycle, so you could recreate the Test and Production instances. You can open the Development VM's settings directly in Azure portal or select it in its resource group list and then click the Export template menu item. Both options allow you to capture changes to the Development VM that were made after the original deployment.

You should not export the ARM template before deployment or export the ARM template from the deployment history. These two options only capture the state of the resource at the time of deployment. They do not include any manual changes made after the original deployment.

You also should not replace the Development VM with a VM scale set. A scale set can provide high availability to your application, automatically increasing or decreasing the number of VMs in response to demand or as per a defined schedule. However, it cannot capture the desired state of your Development VM and reuse it for deployment of the Test and Production instances.

Which Azure feature enhances manageability and reliability by provisioning virtual machine instances based on workload?

Choose the correct answer

- Availability zones
- ✔ Autoscale
- Serverless compute
- Site Recovery

Explanation

Azure autoscale enhances manageability and reliability by provisioning virtual machine instances based on workload. Azure autoscale is a feature of Microsoft Azure that creates and manages a pool of virtual machines to handle increased demand. When demand spikes, autoscale creates new virtual machines in the pool and, when demand subsides, it removes them. This ensures that you only pay for the compute resources you need.

Serverless compute does not enhance manageability and reliability by provisioning virtual machine instances based on workload. In serverless computing, the customer simply submits their application code, and the cloud service provider (CSP) provisions and maintains the servers and infrastructure required to run an application. Azure Functions is an example of a serverless compute platform.

Availability zones do not enhance manageability and reliability by provisioning virtual machine instances based on workload. An Azure availability zone is a physically separate zone within an Azure region. Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking. This allows Azure to offer zone-redundant services, meaning that if one zone becomes unavailable, your application can failover to another availability zone without interruption.

Site Recovery does not enhance manageability and reliability by provisioning virtual machine instances based on workload. Azure Site Recovery is a service that helps protect your on-premises workloads in the event of a disaster. It orchestrates replication of your data and applications to Azure, and then fails over to Azure when needed. You can use Site Recovery to recover from disasters like server or network outages, power outages, or even human error.

What is the advantage of moving your company's infrastructure to Azure by using a public cloud deployment model?

Choose the correct answer

- Legacy applications are easier to support.
- There are no operational expenditure (OpEx) costs.
- ✔ The company is able to scale up as needed with no capital expenditure (CapEx) required.
- The company has complete control of the resources that are used by the operating system.

Explanation

The company is able to scale up as needed with no CapEx required. CapEx refers to money that is spent on infrastructure hardware, such as routers, switches, and servers. With a public cloud deployment in Azure, you only need to pay for the usage of these devices. This eliminates CapEx costs.

There are OpEx costs. OpEx refers to money that is spent regularly and that is necessary for a company to operate. With a public cloud deployment model, OpEx costs are the monthly subscription fees.

Legacy applications are not easier to support with a public deployment model. Legacy applications sometimes require specific versions of hardware and operating systems. With Azure, you cannot control the version of the operating system or the hardware that hosts it. To support legacy applications, you might need to use a hybrid or private deployment model.

You do not have complete control of resources that are used by the operating system. The engineers at the Microsoft datacenter have complete control of the resources. To have complete control yourself, you should use a private deployment model that is not third-party hosted.

You need to determine the number of subscriptions that you have to create based on the requirements for each scenario.

How many subscriptions should you create? To answer, drag the appropriate number of subscriptions to each scenario. A number may be used once, more than once, or not at all.

Drag and drop the answers

Your company has three departments and two Azure administrators. Both administrators manage all departments. Each department must receive an Azure bill.	Three
Your company has two physical locations and one Azure administrator. The administrator manages both locations. Each location must receive an Azure bill.	Two
Your company has two divisions and two Azure administrators. Each administrator is responsible for a division. The company must receive one Azure bill.	One

Explanation

A single Azure account can create multiple subscriptions. Billing occurs at the subscription level.

You should create three subscriptions when your company has three departments that must each receive an Azure bill.

You should create two subscriptions when your company has two physical locations that must each receive a separate bill.

You should create one subscription when your company has two divisions that must share one Azure bill.

You need to understand Azure monitoring options.

Which monitoring feature should you use for each scenario? To answer, drag the appropriate feature to each scenario. A feature may be used once, more than once, or not at all.

Drag and drop the answers

You want to know how many times your web app has been unavailable during the past month.	Health history
You want you and your team members to receive a text message when Azure maintenance is planned.	Health alerts
You want to view the Azure features that are planned to be deprecated.	Health advisories

Explanation

You should monitor Health history to know how many times your web app has been unavailable during the past month. Health history keeps track of inactive events for 90 days.

You should use Health alerts when you want you and your team members to receive a text message when Azure maintenance is planned. Health alerts allow you to configure notifications that affect you.

You should monitor Health advisories to view the Azure features that are planned to be deprecated. Health advisories show you events that are of concern to you, such as when you exceed the usage quota or when a feature is about to be deprecated.

You should not monitor Planned maintenance. This shows you upcoming Azure maintenance that will affect your Azure services in the future. It does not send text messages.

You should not monitor Service issues. This shows you problems that affect you right now, such as by displaying a map of service outages.

Company A wants its development and QA departments to manage App Services, its IT and development departments to manage virtual machines (VMs), and its IT department to manage SQL Database instances. These departments should manage the corresponding resources in both the production and development environments.

Company B wants its development department to manage its own VMs and storage accounts, and its sales team to manage its own Machine Learning (ML) models.

Company C wants its IT department to manage SQL Server VMs that are in the production environment. It also wants to allow its development department to manage SQL Server VMs that host applications in the development environment.

You need to choose the most appropriate resource group organization for each company.

Which resource group organization should you use for each company? To answer, drag the appropriate company to each resource group organization. A company may be used once, more than once, or not at all.

Drag and drop the answers

Create a resource group for each department.	Company B
Create a resource group for each resource type.	Company A
Create a resource group for each environment.	Company C

Explanation

You should create a resource group for each department for Company B. For example, you can apply role-based access control (RBAC) permissions to ensure that only users in the development department can access resources in a development resource group that is named development-rg. The resources in this resource group include VMs and storage accounts.

You should create a resource group for each resource type for Company A. For example, you can create three resource groups that are named appservice-rg, vm-rg, and sql-rg to contain App Services instances, VMs, and SQL Database instances, respectively. You can then apply RBAC permissions to ensure that only specific users can access the resource groups. For example, only users in the development and QA departments can access resources in the appservice-rg group.

You should create a resource group for each environment for Company C. For example, you can create two resource groups that are named development-rg and production-rg to represent the development and production environments. The development environment VMs are placed in the development-rg group, and the production VMs are placed in the production-rg group. You can then apply RBAC permissions to ensure that only users in the development department can access the development-rg resource group and only users in the IT department can access the production-rg resource group.

A company wants to expand its cloud presence by deploying additional resources to Azure. The company plans to use templates based on existing resources to automate the deployment process. Ensuring consistent deployment is critical.

What should the company use?

Choose the correct answer

- Microsoft Defender for Cloud
- Azure Resource Groups
- Azure Monitor
- ✔ Azure Resource Manager

The company should use Azure Resource Manager to automate resource deployments using templates. Azure Resource Manager integrates with Azure portal, PowerShell, CLI, and REST API to perform deployment and management tasks. It gives you an easy way to deploy multiple resource instances or reliably redeploy resources. Using templates helps to ensure consistency.

The company should not use Azure Resource Groups. Resource groups provide a way to manage resources as a set. You can use Resource Manager to deploy resources as part of a group, but that functionality is not built into resource groups directly.

The company should not use Microsoft Defender for Cloud. Defender for Cloud does not provide the functionality to automate resource deployment. Microsoft Defender for Cloud is designed to help prevent attacks against resources. If an attack or intrusion does occur, Microsoft Defender for Cloud has tools to detect and respond to the event.

The company should not use Azure Monitor. Azure Monitor is designed to collect, analyze, and act on telemetry data from both Azure and on-premises environments. It does not provide deployment tools.

To complete the statement in the answer area, select the appropriate option from the drop-down menu.

Choose the correct options

Migrating to cloud services enables an organization to budget

infrastructure costs | as an operational expense.

Explanation

Migrating to cloud services enables an organization to budget infrastructure costs as an operational expense (OpEx). OpEx refers primarily to consumable items and pay-as-you-go resources. Cloud-based services operate on a consumption-based model and fall into the category of pay-as-you-go expenses.

Capital Expenses (CapEx) refer to (typically high-value) investments for fixed assets. From an information technology (IT) standpoint, this would include items such as on-premises servers, but it would also include other assets such as buildings, vehicles and equipment.

From a budgeting standpoint, a major difference between the two is that OpEx can be expensed immediately when the money is spent, while CapEx is usually depreciated over time.

Your company migrates virtual machines (VMs) from an on-premises datacenter to Azure. As a part of the migration, all existing physical servers in your data center are decommissioned. The migrated workload runs on Azure VMs.

Which are the two possible benefits of this cloud migration? Each correct answer presents part of the solution.

Choose the correct answers

- [ ] Ownership of physical infrastructure
- [ ] Reduced Service Level Agreement (SLA)
- [x] Absence of upfront costs for physical infrastructure
- [x] Pay-as-you-Go model
- [ ] Fixed recurrent costs

Explanation

The absence of upfront costs for physical infrastructure and the Pay-as-you-Go model are two possible benefits of this cloud migration. With cloud infrastructure, there are no upfront costs for cloud customers because the cost of hardware provisioning and ownership is taken care of by the cloud provider. As a client, you pay for the actual consumption of the selected cloud services and resources using a Pay-as-you-Go charging model.

The ownership of physical infrastructure, fixed recurrent costs, and a reduced Service Level Agreement (SLA) are not benefits of this cloud migration. As a cloud customer, you only lease cloud computing resources. Ownership of underlying physical hardware belongs to the actual cloud service provider. There are no fixed recurrent costs because you pay for the actual usage of cloud resources, which may vary depending on your solution's workload demand. As a part of this cloud migration, you are also very likely to get not a lower, but a higher SLA. Most Azure services and resources offer an SLA of 99.9% and above, which is much higher uptime than what is achievable at an on-premises datacenter.

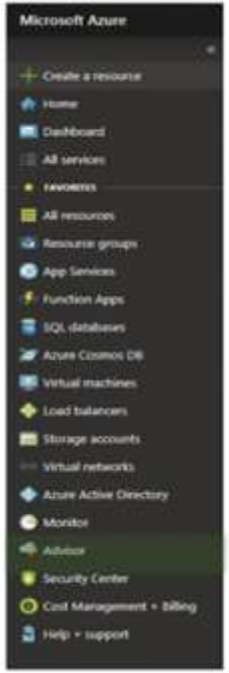
Your company is planning an Azure cloud deployment that must meet the following requirements:

- Improve the continuity of business-critical applications
- Improve application performance
- Detect threats and vulnerabilities
- Reduce overall Azure costs

You need to use a tool that will help you make these types of recommendations.

Which tool should you use? To answer, click the appropriate option in the answer area.

Select the correct area



Explanation

You should use Azure Advisor to collect the recommendations needed. You should run Advisor from the menu to launch Azure Advisor. The other menu selections will not provide the requested information.

Azure Advisor is a personal cloud consultant that provides the information you need to follow best practices and optimize Azure deployments. It can provide recommendations for proactive, actionable, and personalized best practices.

References

For each of the following statements about infrastructure as a service (IaaS) on Azure, select Yes if the statement is true. Otherwise, select No.

Statement	Yes	No
Azure IaaS provides and manages container orchestrators.	○	◉
Resources can be allocated on a pay-as-you-go basis, whenever needed.	◉	○
You are responsible for managing applications and middleware while Azure manages operating systems.	○	◉

Explanation

Azure infrastructure as a service (IaaS) does not provide and manage container orchestrators. This level of service is offered by Azure platform as a service (PaaS). Container orchestrators are tools that help manage and automate the deployment, scaling, and management of containerized applications. One of the most popular container orchestrators is Kubernetes. Kubernetes helps you manage your containerized applications by providing features like auto-scaling, self-healing, rolling updates, and more.

Azure IaaS allows resources to be allocated on a pay-as-you-go basis, whenever needed. Pay-as-you-go cloud services are those where you only pay for the resources that you consume. This can be a massive benefit for businesses of all sizes, as it enables them to control and predict their costs more accurately. Perhaps more importantly, it also allows businesses to scale their usage up or down as needed, without having to worry about overusing (and thus wasting) resources.

In Azure IaaS, you are responsible for managing applications, middleware, and operating systems. In IaaS, network, compute, and storage resources are offered by a cloud provider. However, an IaaS solution will require the subscriber to manage the underlying operating system and services.

To complete the sentence, select the appropriate option from the drop-down menu.

Choose the correct options

With Single Sign-On (SSO) , users can access all needed applications without being required to authenticate a second time.

With SSO, users can access all needed applications without being required to authenticate a second time. The user logs in only once, for example to Azure Active Directory (Azure AD), and that verified credential is then used for other apps in the form of authentication tickets or tokens.

Conditional access is the tool used by Azure AD to make decisions on whether to grant or block access to the requested resource. It enforces organizational policies that define actions to be completed or conditions to be met before access is authorized. For example, administrators may allow network traffic only from specific countries or regions.

MFA is a process where end users are prompted during their login process to provide additional forms of identification, such as a fingerprint, face scan, or the code sent to their mobile phone. It helps to minimize the vector of attacks because this additional factor is not something that can be easily obtained or duplicated.

RBAC is a system that provides fine-grained access management of your Azure resources. It lets you specify who has access to resources, what they can do with them, and the areas they have access to. For example, you may assign owner access to your project team members on the relevant resource group level.

You need to ensure consistent performance for users who access your application, which runs on customized Linux virtual machines.

What should you use to provision virtual machines automatically?

Choose the correct answer

- Availability zones
- Dedicated hosts
- ✔ Scale sets
- Functions

Explanation

You should use scale sets to provision virtual machines automatically. An Azure virtual machine scale set is a group of identical, autoscaling virtual machines in the Azure cloud. Virtual machine scale sets allow you to easily deploy and manage a large number of virtual machines as a single unit, making them ideal for scalable workloads like web servers, application servers, and batch processing jobs. You can create your own virtual machine scale sets from scratch or use pre-configured ones from the Azure Marketplace.

You should not use Functions to provision virtual machines automatically. Azure Functions is an example of serverless computing that allows a subscriber to submit their application code to a cloud service provider (CSP) such as Azure. Azure provisions and maintains the servers and infrastructure required to run the application. This includes code backups, high availability features, and auto-scaling to meet increased workloads.

You should not use availability zones to provision virtual machines automatically. Cloud service providers (CSPs) use availability zones to distribute compute, storage, and networking resources geographically. This approach helps to reduce the impact of power or connectivity failures.

You should not use dedicated hosts to provision virtual machines automatically. Azure Dedicated Hosts are physical servers that you lease from Microsoft. You get exclusive use of the server hardware and all the resources on it, including CPU, memory, storage and networking. This type of hosting is best for applications with high performance or compliance requirements that cannot be met by Azure's public cloud infrastructure.

To complete the statement in the answer area, select the appropriate option from the drop-down menu.

Choose the correct options

Azure Monitor begins collecting data | as soon as you add a resource to a new Azure subscription.

Explanation

Azure Monitor begins collecting data as soon as you add a resource to a new Azure subscription. Azure Monitor is enabled automatically for an Azure subscription and is ready to start collecting resource data, which includes metrics (numeric values) and logs organized into records.

There is no need to launch Azure Management Portal to start monitoring.

It is not necessary to enable diagnostics to start collecting data through Azure Monitor. You can use diagnostics to extend the data collected to include information such as performance counters, event logs, and crash dumps.

You do not need to create the metrics and logs data stores. These are created for you automatically.

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

Statement	Yes	No
Spot pricing provides access to discounted Azure compute resources.	◉	○
Spot virtual machines (VMs) use the standard service level agreement (SLA) for Azure VMs.	○	◉
You can set the maximum price that you agree to pay.	◉	○

Explanation

Spot pricing provides access to Azure compute resources at deep discounts when unused Azure capacity is available.

Spot VMs do not use the standard SLA for Azure VMs. There is no SLA for spot VMs because Azure allocates spot VMs only if there is an unused capacity available. If Azure needs the capacity back, spot VMs can be evicted with a 30-second notice.

You can set the maximum price that you agree to pay. Because spot VM prices vary based on available capacity, you can set the capped price. Your VMs are automatically evicted when the current spot price is higher than the maximum price you agree to pay or if Azure no longer has compute capacity available .

You are planning to move your company's web applications to Azure. You want to use Azure's security features.

You need to understand the difference between authentication and authorization in Azure.

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

Statement	Yes	No
Authentication ensures that the user name and password combination is correct.	◉	○
Authorization ensures that an account has sufficient permissions to access a resource.	◉	○
Authentication can use certificates to identify a person or service.	◉	○
Authorization can use passwords to identify a person.	○	◉

Explanation

Authentication ensures that the user name and password combination is correct. It establishes whether or not people are who they say they are, or whether a service is what it claims it is.

Authorization ensures that an account has sufficient permissions to access a resource. It determines the level of access afforded to a person or service. It can determine which data or resources a service or person is allowed to access.

Authentication can use certificates to identify a person or service. A certificate has an embedded key that identifies a person or service.

Authorization cannot use passwords to identify a person. This is referred to as authentication.

Your Azure tenant includes an Azure Virtual Network (VNet) with several internet-facing web servers. The web servers experience attacks that exhaust server resources and make the servers unavailable to legitimate users. You determine that the attacks are being launched from multiple locations.

You need to implement an Azure solution that:

- Detects and automatically tries to mitigate attacks.
- Generates alerts when an active attack is underway.

What is the best option to implement your solution?

Choose the correct answer

- [x] Azure DDoS Protection Standard
- [ ] Azure Application Security Groups (ASG)
- [ ] Azure Information Protection (AIP)
- [ ] Azure Firewall

Explanation

You should implement Azure DDoS Protection Standard. The type of attack described is a distributed denial of service (DDoS) attack. Azure DDoS Protection is designed to detect, prevent, and automatically mitigate against DDoS attacks. It uses automatic learning of per-customer traffic patterns to help to prevent false positives. The protection would apply to all devices on the virtual network (VNet) on which the web servers are deployed, not just the web servers.

You should not implement AIP as a protection against DDoS attacks. AIP provides a way to classify and organize documents and files through the use of labels. Optionally, it can add a layer of protection to documents and emails. It does not support the functionality to respond to a DDoS attack.

You should not implement Azure ASGs. ASGs let you group virtual machines (VMs) and define network security policies based on those groups. Configuring the web servers as ASGs, for example, does nothing to protect the web servers but lets you implement security protections that specifically target the web servers.

You should not implement Azure Firewall. You can use Azure Firewall to filter traffic between Azure virtual subnets and between Azure and an on-premises deployment. Azure Firewall can be implemented as a part of a security solution, but it does not have the capability to respond to and mitigate DDoS attacks.

Which two examples best describe multi-factor authentication (MFA)? Each correct answer presents a complete solution.

Choose the correct answers

- [x] You receive a text message with a code after you enter a username and password on a movie streaming site.
- [x] You insert your debit card into an ATM and then enter your personal identification number (PIN) to access your account.
- [ ] You specify an email address and password to access online banking.
- [ ] You draw a pattern on your phone to unlock it so that you can call your manager.

Explanation

Receiving a text message with a code after you enter a username and password on a movie streaming site is an example of MFA. MFA adds an additional layer of security because it requires two or more types of authentication, such as something you know, something you possess, and something you are. In this scenario, the username and password represent something you know. The phone that receives the text message with a code represents something you possess. Although some would argue that the code would also be something that you know, this type of double authentication is still often called MFA.

Inserting your debit card into an ATM and then entering your PIN to access your account is also a good example of MFA. This scenario uses two layers of security. The ATM card is something you possess, and the PIN is something you know.

Drawing a pattern on your phone to unlock it so that you can call your manager is not a good example of MFA. This represents one layer of authentication, which is something you know: the pattern.

Specifying an email address and password to access online banking is not a good example of MFA. This represents one layer of authentication, which is something you know: the email address and password.

What is the appropriate cloud service model for each scenario?

To answer, choose the most appropriate cloud service model for each scenario from the drop-down list.

Choose the correct options

A company needs to deploy an Ubuntu Linux virtual machine (VM) to run a resource-intensive data analysis application.	IaaS
A company needs to make productivity applications available to all employees, including those that work from home, on a pay-as-you-go basis.	SaaS
A company needs to develop a web app designed to run on both computers and mobile devices and manage the application lifecycle.	PaaS
A company needs to transition an on-premises data center to the cloud with minimal impact on users.	IaaS

Explanation

An Azure Ubuntu Linux virtual machine (VM) is an example of infrastructure as a service (IaaS). Azure provides the infrastructure on which the VM is deployed. Software and applications are the responsibility of the subscriber creating the VM.

A company would make productivity applications available to all employees through a software as a service (SaaS) subscription. This provides for easy access for all employees, including those who work from home. SaaS subscriptions are based on a pay-as-you-go billing model.

A platform as a service (PaaS) implementation would provide the environment needed to develop a web app designed to run on both computers and mobile devices. PaaS is specifically designed to provide an application design and development environment. This includes tools for managing the application lifecycle.

A company that needs to transition an on-premises data center to the cloud would use an IaaS deployment. Impact is minimized because the company can continue to use its existing applications, in most situations. This solution would let the company create additional VMs as necessary.

To complete the statement in the answer area, select the appropriate option from the drop-down menu.

Choose the correct options

An Azure Multi-factor Authentication (MFA) server is required

for authentication when supporting users located on on-premises Active Directory (AD) only.

Explanation

An MFA server is required for authentication when supporting users located on on-premises Active Directory only. Azure MFA Service (Cloud) does not support this configuration and requires Azure Active Directory (Azure AD) as a security component.

When supporting authentication for users located on Azure AD only, you must use Azure MFA Service (Cloud). This is not supported by an MFA server.

Support for authentication with both Azure AD and on-premises AD using Azure AD Connect or authentication with Azure AD and on-premises AD using federation with Active Directory Federation Services (AD FS) is provided by Azure MFA Service (Cloud) or Azure MFA Server. Azure MFA Service (Cloud) is recommended for new deployments that include Azure AD and federated users.

To complete the statement in the answer area, select the appropriate option from the drop-down menu.

Choose the correct options

Azure Advisor integrates with [Microsoft Defender for Cloud] to help

to prevent, detect, and respond to threats to Azure resources.

Explanation

Azure Advisor integrates with Microsoft Defender for Cloud to help to prevent, detect, and respond to threats to Azure resources. Azure Advisor analyzes resource configuration and usage telemetry to provide recommendations for:

- High availability
- Security
- Performance
- Cost

Security recommendations are available from the Security tab on the Advisor dashboard. Based on the data collected and analysis performed by Azure Advisor, Microsoft Defender for Cloud identifies potential security vulnerabilities and creates recommendations.

AIP is not integrated with Azure Advisor and does not provide for the remediation of security issues. AIP provides a way to classify and organize documents and files through the use of labels. Optionally, it can add a layer of protection to documents and emails.

Azure ATP is not integrated with Azure Advisor and does not provide for the remediation of security issues detected through Azure Advisor. Azure ATP uses information from on-premises Active Directory (AD) signals to identify, detect, and investigate advanced threats.

Azure Cloud Shell is a browser-accessible shell for running Azure CLI and Azure PowerShell commands. It provides an interface for running commands, but it is not integrated with Azure Advisor and does not support direct functionality based on Azure Advisor.

For each of the following statements regarding security benefits offered by Azure cloud, select Yes if the statement is true. Otherwise, select No.

Statement	Yes	No
Azure Active Directory (Azure AD) is used to manage API cryptographic keys.	○	●
Azure Storage encryption is enabled by default and cannot be disabled.	●	○
Azure ExpressRoute is used to secure traffic between virtual networks.	○	●

Explanation

Azure Active Directory (Azure AD) is not used to manage Application Programming Interface (API) cryptographic keys. Azure AD is a Microsoft's cloud-based identity and an access management service. It combines core directory services and helps you manage users, groups, and access to applications in your Azure subscription. Azure Key Vault would be the best choice for managing cryptographic keys and secrets.

Azure Storage encryption is enabled by default and cannot be disabled. Azure Storage encryption is a feature that encrypts your data using 256-bit Advanced Encryption Standard (AES) encryption before storing it in Azure Storage. Data is encrypted with a key that is unique to each storage account. You control who has access to the data and how it is used. Data remains encrypted while in transit between the customer's computer and Azure, and between Azure data centers.

Azure ExpressRoute is not used to secure traffic between virtual networks. Azure ExpressRoute is a private network connection between your organization and Microsoft Cloud services. It provides a more secure, reliable, and predictable way to connect to Microsoft Cloud services than connecting over the Internet. With ExpressRoute, you can establish connections to Azure services from your data center, office or on-premises environment.

You need to bring Azure Storage into your virtual network with a dedicated IP address.

Which solution should you use?

Choose the correct answer

- Peer your Azure virtual network (VNet) with an Azure Storage VNet.
- Create a private connection with Azure ExpressRoute.
- ✔ Create a private endpoint with Azure Private Link.
- Create a site-to-site VPN with Azure VPN Gateway.

Explanation

You should create a private endpoint with Azure Private Link. A private endpoint is a network interface that connects you privately and securely to a service powered by Azure Private Link. Private endpoints use a private Internet Protocol (IP) address from your VNet, and they communicate with the service over a secure connection. Traffic from a private endpoint to the service traverses over the Microsoft backbone network, eliminating exposure from the public internet.

You should not create a site-to-site VPN with Azure VPN Gateway. Azure VPN Gateway is a type of virtual network gateway that provides secure, private connections between organizations and their virtual networks. It is used to connect a customer's on-premises networks with Azure, or to securely connect multiple Azure VNets. Azure VPN Gateway supports both site-to-site and point-to-point VPN connections.

You should not create a private connection with Azure ExpressRoute. Azure ExpressRoute is a private network connection between your organization and Microsoft Cloud services. It provides a more secure, reliable, and predictable way to connect to Microsoft Cloud services than connecting over the internet. With ExpressRoute, you can establish connections to Azure services from your data center, office, or on-premises environment.

You should not peer your Azure VNet with an Azure Storage VNet. VNets provide logically isolated, private networks in the cloud. By default, all resources on a virtual network can communicate with the internet. VNets also support inbound connects using public IP addresses and Load Balancers. Virtual network peering is used to connect VNets within an Azure region.

Which resource is required to use Azure Cloud Shell?

Choose the correct answer

- [x] Storage account
- [ ] Virtual machine (VM)
- [ ] App Services web app
- [ ] Container

A storage account is required to use Azure Cloud Shell.

A VM is not required to use Azure Cloud Shell. A VM is a compute resource that you use as if you were working on a local computer.

An App Services web app allows you to deploy web applications to Azure. Azure Cloud Shell is a feature of the web-based Azure portal.

A container is similar to a VM with the exception that you cannot manage the operating system. A container allows you to deploy a self-contained application.

Your company is considering moving its on-premises infrastructure to Azure. Before doing so, you want to compare the cost savings, if any.

You need to choose the most appropriate cost savings estimation tool.

Which tool should you use?

Choose the correct answer

- [x] Total Cost of Ownership (TCO) calculator
- [ ] Azure Pricing Calculator
- [ ] Azure Advisor
- [ ] Cost Management

Explanation

You should use the TCO calculator. This calculator allows you to compare the difference in cost between your current on-premises infrastructure and your predicted cloud infrastructure. This calculator looks at on-premises hardware, electricity, IT labor, and software licensing, among other things. It then compares this cost to the assumed resources needed in Azure.

You should not use the Azure Pricing Calculator. This tool allows you to estimate the monthly cost of a planned cloud solution. You can add various resources to the calculator. Among other things, you can choose the region of the resources, and the number of instances of a resource to help estimate the cost. However, you cannot use this tool to estimate cost savings between an on-premises infrastructure and Azure.

You should not use Azure Advisor. This is a service that makes recommendations on performance, security, high availability, and cost by examining existing Azure resources. You cannot use this tool to estimate cost savings between an on-premises infrastructure and Azure.

You should not use Cost Management. This is a built-in service that gives you a breakdown of the usage and cost of your Azure resources. This allows you to see what is costing you money and how it compares against your budget. You cannot use this tool to estimate cost savings between an on-premises infrastructure and Azure.

To complete the statement in the answer area, select the appropriate option from the drop-down menu.

Choose the correct options

Creating highly portable, scalable app instances that include the binaries and libraries required to run can be done using [containers.]

Explanation

Creating highly portable, scalable app instances that only include the binaries and libraries required to run can be done using containers. Containers provide many of the same benefits as virtual machines and are designed to be portable and largely self-contained. They are typically composed of the binaries and libraries required to run a single app or service. Due to their small footprint and compute/memory requirements, containers are typically faster and cheaper to deploy than comparable virtual machines. Docker is a popular container ecosystem.

Creating highly portable, scalable app instances that only include the binaries and libraries required to run cannot be done using virtual desktop infrastructure (VDI). VDI uses virtual machines (VMs) to provide users with a virtual desktop that is stored centrally. VDI is designed to make creating, managing, and securing user desktops easier.

Creating highly portable, scalable app instances that only include the binaries and libraries required to run cannot be done using VMs. VMs are complete, self-contained operating systems. VMs include the base OS, drivers, services, as well as application binaries and support libraries. VMs typically offer more functionality and flexibility than containers.

A company is looking for solutions to help to lower cloud-related costs.

You need to identify tools and mechanisms that help save money.

To answer, select the appropriate cost control mechanism from the drop-down list.

Choose the correct options

Your company plans to commit to a three-year plan for virtual machines (VMs) and storage resources to receive a reduction in pay-as-you-go prices.	Azure Reservations
Your company plans to make use of a free SaaS solution that lets your company monitor, allocate, and optimize cloud spend in a multi-cloud environment.	Azure Cost Management
Your company wants to increase default limits on how many select resources of each type can be provisioned per Azure Region.	Azure Resource Manager (ARM)

Explanation

Your company plans to commit to a three-year plan for VMs and storage resources to receive a reduction in pay-as-you-go prices. This is an example of using Azure Reservations to cut costs. Cost savings can be significant for resources that use significant capacity or throughput or run for long periods of time. Azure Reservations can be applied to VMs, Blob storage data, Azure Cosmos DB, or SQL databases.

Your company plans to make use of a free SaaS solution that lets your company monitor, allocate, and optimize cloud spend in a multi-cloud environment. This is the role of Azure Cost Manager, which is provided at no cost to Azure customers and partners. It supports a multi-cloud environment to include Azure, AWS, and Google Cloud Platform.

Your company wants to increase default limits how many of select resources of each type can be provisioned per Azure Region. This can be accomplished with ARM. This lets you increase default limits but does not let you exceed hard limits.

None of the statements refers to the Azure TCO calculator. TCO calculator is used to estimate the cost savings you can get by migrating workloads to the cloud.

None of the statements refers to Azure spending limits. These are limits that are set on a subscription and set a hard limit on how much can be spent during a billing period. Once set, spending limits can be deleted but they cannot be increased.

Which statements accurately describe Azure PowerShell?

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

Statement	Yes	No
Azure PowerShell can be used to create scripts to automate Azure management tasks.	●	○
Azure PowerShell virtual machine (VM) management is limited to Windows VMs only.	○	●
Azure PowerShell can be run in a browser in the Azure Cloud Shell.	●	○
Azure Resource Manager templates use Azure PowerShell syntax.	○	●

Explanation

Azure PowerShell can be used to create scripts to automate Azure management tasks. It provides support for the concurrent execution of multiple scripts. Most tasks can be automated through the use of PowerShell scripts.

Azure PowerShell VM management is not limited to Windows VMs only. It can also be used to manage Linux and Mac OS VMs.

Azure PowerShell can be run in a browser in the Azure Cloud Shell or by connecting through Azure PowerShell. In addition to Azure PowerShell, Azure Cloud Shell supports Azure Command-line interface (CLI) and many programming languages.

Azure Resource Manager templates use basic JavaScript Object Notation (JSON) syntax with support for expressions and functions that extend JSON values. JSON is a language-independent data format that is supported by a variety of programming languages.

Compare using Azure PowerShell and Azure CLI for Azure management.

To answer, select the appropriate options from the drop-down menus.

Choose the correct options

Commands work the same on Mac, Linux, and Windows.	Both
Command execution supported in Azure Cloud Shell.	Both
Executes commands in an interactive environment.	Both
Supports an optional GUI interface.	Neither

Explanation

Commands work the same on Mac, Linux, and Windows with both Azure CLI and Azure PowerShell. Azure PowerShell works the same on all platform using .NET Core and the Az Module since PowerShell version 6.2.4.

Azure Cloud Shell supports both. Azure Cloud Shell is an interactive, browser-accessible shell environment. The first time you launch Cloud Shell, you are prompted to select your shell as either Bash or PowerShell. This becomes your default, but you can manually choose between Bash and PowerShell. Choose Bash to support Azure CLI commands and PowerShell to support Azure PowerShell commands.

Both Azure CLI and Azure PowerShell execute commands in an interactive command-line based environment. In most management situations, the choice between using Azure CLI and Azure PowerShell is one of personal preference.

Neither Azure CLI nor Azure PowerShell supports a GUI interface. They are both command-line only environments.

Your company is considering using a Platform-as-a-Service (PaaS) environment.

You need to determine the responsibilities of customer and provider for several components.

Which components would be the responsibility of the customer and which would be the responsibility of the provider? To answer, select the appropriate options from the drop-down menus.

Choose the correct options

Operating system	Provider
Data	Customer
Storage	Provider
Virtualization	Provider
Applications	Customer

Explanation

PaaS is an application design environment. The service provider is responsible for the underlying infrastructure. Development tools are provided for multiple platforms, including computers, mobile devices, and web apps.

In a PaaS environment the customer is responsible for managing:

- Applications
- Data

The provider is responsible for:

- Runtime
- Middleware
- Operating System
- Virtualization
- Servers
- Storage
- Networking

PaaS makes for a flexible development platform where the customer can focus on development rather than being concerned with managing the underlying platform.

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

Statement	Yes	No
All Azure resources support tags.	○	◉
Tags are name/value pairs.	◉	○
Tags applied to a resource group are inherited by its resources.	○	◉

Explanation

Not all Azure resources support tags. They cannot be applied to classic resources that existed before Microsoft introduced Azure Resource Manager (ARM), like Cloud Services. Also, they cannot be applied to some other Azure resources. For the latest updates on tag support, you should consult Microsoft documentation.

Tags are name/value pairs. Tag values are case-sensitive, while tag names are not. You apply tags to Azure resources, resource groups, or subscriptions using PowerShell, Azure Command Line Interface (CLI), in ARM templates or Azure portal. You can have as many as 50 tag name/value pairs.

Tags applied to a resource group are not inherited by its resources. They are also not inherited if they are applied at the Azure subscription level. To ensure that all the required resources are tagged, you either need to apply them manually or create an Azure policy that automatically applies required tags from resource groups or the subscription to resources during their deployment.

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

Statement	Yes	No
Locks can be applied in the context of specific users and roles.	○	◉
When multiple locks are applied at different scopes, the most restrictive inherited lock applies.	◉	○
A lock applies to all of the resources contained in a scope and any new resources added to the scope.	◉	○
Role-based access control (RBAC) roles take precedence over locks.	○	◉

Explanation

Locks cannot be applied in the context of specific users and roles. When a lock is applied to a scope or resource, it applies to all users and roles. Locks can be applied as CanNotDelete or ReadOnly. ReadOnly is more restrictive than CanNotDelete. In Azure portal the locks are referred to as Delete and Read-only.

When multiple locks are applied at different scopes, the most restrictive inherited lock applies. When a lock is applied at a scope, it applies to contained resources and scopes. Locks can be applied to the subscription, resource group, and resource scope.

A lock applies to all of the resources contained in a scope and any new resources added to the scope. The lock automatically applies to any resources contained in the scope and it is added to any resources added to or created in the scope.

RBAC roles do not take precedence over locks. Locks always take precedence.

A company subscribes to Azure as a platform for developing and deploying web apps. The company wants to keep initial expenses to a minimum. The company cannot use the free edition as it does not support many features required, so the company decides to go with Azure AD premium subscription.

You need to determine the features available to the company with Azure Active Directory (Azure AD) Premium P1 edition.

Which two features are supported by Azure AD Premium P1 edition? Each correct answer presents a complete solution.

Choose the correct answers

- [x] Role-based access control (RBAC)
- [x] Conditional Access
- [ ] Identity Protection
- [ ] Self-service entitlement management
- [ ] Privileged Identity Management (PIM), just-in-time access

Azure AD Premium P1 edition supports Role-based access control (RBAC) and Conditional Access. The Azure AD P1 supports most of premium features except a few including the ones marked as incorrect in this question.

Azure AD P1 license does not support Identity Protection, Self-service entitlement management and Privileged Identity Management (PIM), just-in-time access. These are included in Azure AD P2 license.

Azure AD comes in four editions: Free, Office 365, Premium P1, and Premium P2. The Free edition is included with a subscription of a commercial online service, e.g. Azure, Dynamics 365, Intune, and Power Platform

To complete the statement in the answer area, select the appropriate option from the drop-down menu.

Choose the correct options

Application Security Groups (ASGs) let you

organize similar servers so you can easily define and implement security policies based on those groups.

Explanation

ASGs let you organize similar servers so you can easily define and implement security policies based on those groups. ASGs let you apply security to the group as a whole.

ASGs do not let you directly allow or block connections to all servers running instances of the same server. ASGs can be used as a part of the solution, but this is not configured through ASGs. You could, for example, create an ASG and then create a Network Security Group (NSG), defining connection filters, and apply it to the ASG.

ASGs do not let you control user access to serverless applications. ASGs apply to server applications only. Access to serverless applications is managed through Azure Active Directory (Azure AD) and role-based access controls (RBACs).

ASGs do not let you define templates for the rapid deployment of application instances in an orchestrated environment. Azure provides various tools to facilitate rapid deployment, such as Azure DevTest Labs.

To complete the statement in the answer area, select the appropriate option from the drop-down menu.

Choose the correct options

Management groups let you organize multiple

subscriptions as a single management entity to facilitate easier management .

Explanation

Management groups let you organize multiple subscriptions as a single management entity to facilitate easier management. You can create managements groups in a hierarchical structure with the top level of the hierarchy at the tenant level and all of the subscriptions are contained in that tenant. Any conditions applied to a management group apply to all subscriptions contained in that management group object.

Management groups do not organize multiple Azure AD tenants as a single management entity to facilitate easier management. An Azure tenant is an organization's top-level Azure hierarchy. An organization will typically have one tenant and it can then have multiple subscriptions under that tenant. Azure does not provide a method for organizing multiple tenants into a single management entity.

Management groups do not organize multiple resource groups or resources for management. Neither can be added directly to a management group but are managed indirectly if the subscription in which they are contained is part of a management group.

Match each benefit of cloud computing with its description.

To answer, drag the appropriate benefit to each description. A benefit may be used once, more than once, or not at all.

Drag and drop the answers

Manually increasing or decreasing resources to meet a predictable workload	Scalability
Automatically increasing or decreasing resources to meet spikes and drops in demand	Elasticity
Speed and flexibility in allocation and deallocation of required resources	Agility

Scalability is the benefit of cloud computing that allows increasing or decreasing resources to meet a predictable workload. Scaling can be horizontal (scaling out), when you provision additional resources to function together as one unit like adding additional virtual machines (VMs), or vertical (scaling up), when you increase capacity of existing resources such as by adding more CPUs or memory to VMs.

Elasticity is the benefit of cloud computing that allows the automatic increase or decrease of resources to meet spikes and drops in demand. The distinction between scalability and elasticity is that the latter is always done automatically to meet sudden bursts in capacity demand, while the former addresses more predictable and even planned demand and workload requirements.

Agility is the benefit of cloud computing that enables speed and flexibility in allocation and deallocation of required resources. It allows deployment of required resources and services in minutes without manual administration of provisioning or deprovisioning processes.

High availability (HA) is the benefit of cloud computing that keeps resources and services functioning for long periods of time. Cloud service providers typically offer a service level agreement (SLA) that guarantees HA or uptime of resources and services as a percentage.

Which Azure management tool provides a graphic interface for deploying, managing, and monitoring Azure resources?

Choose the correct answer

- [x] Azure portal
- [ ] Azure Resource Manager
- [ ] Azure Command-line interface (CLI)
- [ ] Azure PowerShell

Azure portal provides a graphic interface for deploying, managing, and monitoring Azure resources. It can also be used to manage all aspects of your applications. Azure portal has a home view, which is the default view with menus, and a dashboard view, which gives you easy access to tools and information.

Azure PowerShell and Azure CLI are both command-line based management utilities and do not provide a graphic interface.

Azure Resource Manager is not used for managing and monitoring Azure resources. It is used to deploy resources based on templates and provides an easy way to deploy consistent instances of resources.

Which feature of Azure Monitor allows you to visually analyze telemetry data?

Choose the correct answer

- Alerts
- ✔ Application Insights
- Service Health
- Metrics

Explanation

Application Insights is a feature of Azure Monitor that allows you to visually analyze telemetry data. It is an Application Performance Management (APM) service that detects performance in real time. Developers can install a small instrumentation package in their web applications to send telemetry data to Azure. Administrators can then log in to the Azure portal and choose Application Insights under Azure Monitor.

Service Health does not analyze telemetry data. It tracks the state of Azure services. It allows administrators to be notified of events like planned maintenance or a service outage.

Metrics are numerical values that describe some aspect of the system, such as CPU time. Metrics are not an analysis feature.

Alerts do not analyze telemetry data. They allow you to configure actions that should be taken when specific conditions are met. For example, an alert can send you an email when the CPU for a virtual machine (VM) exceeds a certain threshold.

You need to enable data redundancy for your organization's cloud apps. Depending on the data, redundancy may be local only, or may require multiple copies stored in different locations.

Given the redundant storage descriptions below, which redundancy option is being described? To answer, select the appropriate redundancy option from the answer area.

Choose the correct options

It stores three data copies in each of two regions.	Geo-redundant storage (GRS)
It allows replicated data to be accessed in two zones.	Read-access GRS (RA-GRS)
It stores all replicas in one data center.	Locally redundant storage (LRS)

Azure geo-redundant storage (GRS) is a storage replication option for geo-redundant systems. It stores three copies of your data in each of two regions. Azure GRS makes sure that your data remains available even if there is a complete failure at one location. In the event of a localized failure or network outage, your applications can still access data from the second location.

Like GRS, read-access GRS (RA-GRS) is a service that creates geo-redundant replicas of your data in two separate Azure regions, so that your data is always available, even in the event of a regional outage. Unlike GRS, however, RA-GRS is a storage redundancy type that provides read access from both locations simultaneously.

Locally redundant storage (LRS) stores all replicas in one datacenter. LRS protects data locally by writing to three disks within the datacenter.

You have completed the migration of your organization's core servers and processes to cloud-based virtual machines. Your final project involves migrating a weekly batch-processing task that relies on operating system drivers to print PDF reports.

You need to meet this requirement while minimizing costs.

What should you do?

Choose the correct answer

- Configure virtual machine clusters to scale for batch processing.
- Execute the batch task on a dedicated virtual machine as needed.
- ✔ Run the batch processing task using spot instances.
- Migrate the batch processing to serverless compute.

You should run the batch processing task using spot instances. Spot virtual machines or instances can help reduce costs by taking advantage of unutilized compute capacity. Most cloud service providers (CSPs) offer this unused capacity at a significant discount, as it allows the provider to recover some of the costs associated with operating their infrastructure. Unlike a normal virtual machine, spot virtual machines do not offer guaranteed compute resources at a specified time. They are perfect for batch or other asynchronous processing that can occur on a flexible schedule. Microsoft offers this feature as Azure Spot Virtual Machines.

You should not migrate the batch processing to serverless compute. In serverless computing, the customer simply submits their application code, and the CSP maintains the servers and infrastructure required to run an application. Serverless computing does not provide access to a full operating system for printing.

You should not configure virtual machine clusters to scale for batch processing. Scaling allows resources to be consumed on an as-needed basis, based on workload. Though less expensive than operating a virtual machine full time, as scaling requires on-demand processing, it is often one of the most expensive cloud compute resources.

You should not execute the batch task on a dedicated virtual machine as needed. Powering on a dedicated batch virtual machine as needed is the second-best option in this scenario as compute charges are only calculated when the virtual machine is running. However, storage charges will be incurred regardless of whether or not a virtual machine is operational.

You work for a small college. The college has no more than 250 active students. You consider moving the college's infrastructure to the cloud.

You need to determine the type of subscription that you should use for different scenarios.

Which subscriptions should you use? To answer, drag the appropriate subscription to each scenario. A subscription may be used once, more than once, or not at all.

Drag and drop the answers

You want to evaluate Azure virtual machines (VMs) for 18 months.	Pay-As-You-Go
You want to purchase Azure virtual machines (VMs) and software licenses under one agreement.	Enterprise
You want to evaluate Azure App Services for six months.	Free

You should use a Pay-As-You-Go subscription when you want to evaluate Azure VMs for 18 months. A Pay-As-You-Go subscription charges you monthly for Azure resources.

You should use an Enterprise subscription when you want to purchase Azure VMs and software licenses under one agreement. This helps you save money.

You should use a Free subscription when you want to evaluate Azure App Services for six months. A Free subscription includes $200 credit that you can use for any service for 30 days. It also provides free access to Azure services for one year.

You should not use a Student subscription. This subscription is only available for students and for non-business purposes.

You are interviewing for a job as an entry level Azure administrator.

You need to describe regions.

Which three descriptions of regions are accurate? To answer, move the appropriate descriptions from the list of possible descriptions to the answer area and arrange them in any order.

Create a list in any order

Possible descriptions of regions

- Regions can span countries.
- Regions represent physical datacenters.

Descriptions of regions

- Regions are always paired with other regions.
- Regions contain one or more datacenters.
- Regions specify the location of resources.

Regions are always paired with other regions. The paired region is always in the same geography, such as the US, but it is always the farthest from the original region, at least 300 miles away. This allows for replication in a way such that civil unrest, large-scale power outages or natural disasters have minimal impact on Azure services.

Regions contain one or more datacenters. They represent an area within a geographical area, such as East US or West US.

Regions specify the location of resources. Although you cannot choose the exact datacenter for a deployed resource, you can choose its region. Azure then determines the physical data center where the resource is provisioned.

Regions cannot span countries. They are tied to a single country or geographical area.

Regions do not represent physical datacenters. They represent an area within a geographical area.

To complete the sentence, select the appropriate option from the drop-down menu.

Choose the correct options

Disaster Recovery is the ability to restore a cloud service in the wake of a catastrophic loss.

Disaster recovery is the ability to restore a cloud service in the wake of a catastrophic loss. Taking regular backups of important data and replicating your application across different regions are some of the disaster recovery measures that help you ensure that data remains safe and that your application's availability is not impacted after an unexpected disastrous event.

Agility is the ability to react quickly with allocation and deallocation of cloud resources. It allows deployment of required resources and services in minutes without manual administration of provisioning or deprovisioning processes.

High availability (HA) is the ability to keep cloud resources and services functioning for long periods of time. Cloud service providers typically offer a service level agreement (SLA) that guarantees HA or uptime of resources and services, as a percentage.

You create an Azure subscription.

You need to determine when you should use specific Azure management tools.

When should you use each tool? To answer, drag the appropriate tool to each scenario. A tool may be used once, more than once, or not at all.

Drag and drop the answers

You need to log in to Azure with the following cmdlet from your laptop without manually opening a web browser: Connect-AzAccount	Azure PowerShell
You need to log in to Azure with the following command from your laptop without manually opening a web browser: az login	Azure CLI
You want to run the following cmdlet in a scripting environment inside the browser: New-AzVm	Azure Cloud Shell

You should use Azure PowerShell when you need to log in to Azure with the following cmdlet from your laptop without manually opening a web browser:

```
Connect-AzAccount
```

Azure PowerShell is a module that you can install on your computer for Windows, Linux, or macOS. It allows you to use PowerShell cmdlets locally to administer Azure resources.

You should use Azure CLI when you need to log in to Azure with the following command from your laptop without manually opening a web browser:

```
az login
```

Azure CLI is a cross-platform command-line tool that allows you to manage Azure resources from your computer.

You should use Azure Cloud Shell when you need to run the following cmdlet in a scripting environment inside the browser:

```
New-AzVm
```

Azure Cloud Shell is a web-based tool that allows you to run PowerShell cmdlets or Azure CLI commands after you log in to the Azure portal.

Your company plans to deploy to the Azure cloud three virtual machines (VMs) and a Load Balancer. You want to estimate the cost of using all four resources before you create a subscription.

You need to choose the most appropriate cost estimation tool.

Which tool should you use?

Choose the correct answer

- Total Cost of Ownership (TCO) calculator
- Cost Management
- Azure Advisor
- ✔ Azure Pricing Calculator

You should use the Azure Pricing Calculator. This tool allows you to estimate the monthly cost of a cloud solution. You can add various resources to the calculator. Among other things, you can choose the region of the resources, and the number of instances of a resource to help estimate the cost.

You should not use the TCO calculator. This calculator allows you to compare the difference in cost between your current on-premises infrastructure and your predicted cloud infrastructure. This calculator looks at on-premises hardware, electricity, IT labor, and software licensing, among other things. It then compares this cost to the assumed resources needed in Azure. This cost does not accurately reflect the monthly cost for the Azure resources you plan to deploy.

You should not use Azure Advisor. This is a service that makes recommendations on performance, security, high availability, and cost by examining existing Azure resources. You must have an existing subscription to use Azure Advisor.

You should not use Cost Management. This is a built-in service that gives you a breakdown of the usage and cost of your Azure resource. This allows you to see what is costing you money and how it compares against your budget. You must have an existing subscription to use Cost Management.

For each of the following statements about Azure Distributed Denial of Service (DDoS) Protection, select Yes if the statement is true. Otherwise, select No.

Statement	Yes	No
Azure DDoS Protection Standard is enabled automatically.	○	◉
Azure DDoS Protection Standard provides protection against volumetric, protocol, and application layer attacks.	◉	○
Virtual networks from multiple subscriptions in your organization can link to the same Azure DDoS Protection plan.	◉	○

Azure DDoS Protection Standard is not set up automatically. Azure DDoS Protection is available as Basic and Standard. Basic is enabled automatically as part of the Azure platform. Standard provides additional protections compared to DDoS basic and can easily be enabled but does incur an additional charge to the subscription.

Azure DDoS Protection Standard provides protection against volumetric, protocol, and application layer attacks. A volumetric attack refers to an attempt to flood a network with what appears to be legitimate traffic, but at very high levels. Protocol attacks work by exploiting weaknesses in the layer 3 and layer 4 protocol stack. Application layer (resource layer) attacks target web application packets. Protection is provided for Azure Load Balancer, Azure Application Gateway, and Azure Service Fabric instances with associated public IP addresses. Protection is not provided for App Service Environments.

Virtual networks from multiple subscriptions in your organization can link to the same Azure DDoS Protection plan. The protection plan is associated with a subscription when it is created and will be billed to the associated subscription plan. A plan cannot be moved between subscriptions. Moving a plan would require you to delete the plan and then recreate the plan associated with a different subscription.

Identify the features of Azure Cloud Shell.

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

Statement	Yes	No
When running Azure PowerShell with Cloud Shell, both Linux-specific and Windows-specific functionality is available.	○	●
Cloud Shell times out after 20 minutes of inactivity.	●	○
Cloud Shell provides a way to run Azure Command-Line Interface (CLI) and Azure PowerShell on iOS and Android mobile devices.	●	○

Explanation

Azure Cloud Shell is an interactive, browser-accessible shell environment. When launching Cloud Shell, you need to select PowerShell to execute Azure PowerShell commands or Bash to execute Azure CLI commands. When running Azure PowerShell with Cloud Shell, Linux-specific functionality is available, but Windows-specific functionality is not. This is because Cloud Shell runs PowerShell 6 on a Linux container.

Cloud Shell times out with 20 minutes of inactivity.

Cloud Shell provides a way to run Azure CLI and Azure PowerShell on iOS and Android mobile devices. Cloud Shell can be accessed from Azure mobile app, among other features available on the app, to manage and monitor the Azure environment.

To complete the statement in the answer area, select the appropriate option from the drop-down menu.

Choose the correct options

A [standard general-purpose v2] storage account supports Blob, Queue, and Table Storage services.

Explanation

A standard general-purpose v2 storage account supports Blob, Queue, and Table Storage services. Azure standard general-purpose v2 storage accounts are cost-effective, secure, durable, and scalable storage solutions. They provide data protection and performance features to help you safely store and access your data. These storage account types are available in all public regions.

A premium block blobs storage account only supports the Blob Storage service. This account type does not support the Queue or Table storage services. Blobs are designed to store unstructured data.

A premium file shares only supports file shares. File shares are supported by Azure Files, which is a cloud file storage service that operates like a traditional Server Message Block (SMB) or Network File System (NFS) file server. This makes Azure Files directly accessible by Windows, Linux, and macOS clients.

A premium page blobs only supports page blob storage. An Azure page blobs is a type of storage blob that represents a continuous stream of bytes. Azure page blobs can be used to store any type of data and are especially well-suited for storing unstructured data, such as text or images.

You have been asked to develop cloud migration plans for your organization.

As part of this assignment, you need to identify the most cost-effective cloud service type for each department in the organization. The solution should minimize management overhead.

Given each department's requirements, which solution should you recommend? To answer, select the appropriate cloud service type from the drop-down menus.

Choose the correct options

Finance	Use provider-managed hardware to run a customized database.	IaaS
Sales	Use a provider-managed calendar to schedule appointments and meetings.	SaaS
Marketing	Use provider-managed business intelligence services to analyze marketing trends.	PaaS

The infrastructure as a service (IaaS) cloud service type will allow your organization to use provider-managed hardware to run a customized database. In IaaS, network, compute, and storage resources are offered by a cloud provider. These resources may be shared by multiple tenants, or they can be dedicated to a single tenant. Some cloud providers offer full data center IaaS solutions, including a physically secure room or building.

The software as a service (SaaS) cloud service type will allow your organization to use a provider-managed calendar to schedule appointments and meetings. SaaS is software that is hosted on the cloud and available to customers over the Internet. Microsoft Office 365 is an example of SaaS.

The platform as a service (PaaS) cloud service type will allow your organization to use provider-managed business intelligence services to analyze marketing trends. PaaS is a type of cloud computing that provides a platform for developers to build, run, and manage applications without the need for infrastructure management. Typically, PaaS providers offer a wide variety of services, including databases, analytics, workflow engines, and more.

You are researching the governance methodologies in Azure. You want to understand role-based access security (RBAC), policies, initiatives, and locks.

You need to choose the type of resource or feature to use for different scenarios.

When should you use each resource or feature? To answer, drag the appropriate resource or feature to each scenario. A resource or feature may be used once, more than once, or not at all.

Drag and drop the answers

You want to ensure that only virtual machines (VMs) of a specific size are deployed to a resource group.	Policy
You want to manage a collection of policy definitions.	Initiative
You want to prevent virtual machines (VMs) from being deleted by anyone after they are deployed.	Lock

Explanation

You should use a policy when you want to ensure that only VMs of a specific size are deployed to a resource group. A policy definition is a JSON file that is assigned to a scope, such as a resource group. The JSON file defines the rules that are to be used for certain resources. For example, you can create a rule to deny the creation of all VMs that are outside the sizes that you specify.

You should use an initiative when you want to manage a collection of policy definitions. This allows you to manage multiple policies as a whole, rather than individually. Similar to policies, you can assign initiatives to a scope, such as a resource group or subscription.

You should use a lock when you want to prevent VMs from being deleted by anyone after they are deployed. This helps to prevent accidental deletion of critical resources. The name of this lock setting is CanNotDelete. In the Azure portal, this lock setting is simply referred to as Delete.

You should not use Role-Based Access Control (RBAC) in this scenario. RBAC assigns permissions that apply to users and groups. In this scenario, you are applying settings to resources regardless of users and groups.

Your company plans to migrate applications and services to the cloud. You recommend for a hybrid cloud to be deployed. Why would you make this recommendation?

Choose the correct answer

- To consolidate all cloud resources in a single data center
- To ensure that charges are only incurred when cloud resources are utilized
- ✔ To augment on-premises resources by providing overflow capacity
- To eliminate the need for company-managed compute resources

Explanation

By implementing a hybrid cloud, your company can augment on-premises resources by providing overflow capacity. A hybrid cloud is the combination of two or more cloud models, such as public and private, and provides benefits from both models. It can give businesses the flexibility to use public cloud resources when they need them, while also keeping sensitive data and applications on-premises in a private cloud. A hybrid cloud can also help organizations manage peaks and valleys in traffic more efficiently. By using a hybrid cloud model, businesses do not have to overprovision computing resources in anticipation of high demand; they can simply bring in extra resources from the public cloud when they need them.

Implementing a hybrid cloud will not allow your company to consolidate all cloud resources in a single data center. This describes a public or a private cloud, either of which could support this requirement.

Implementing a hybrid cloud will not allow your company to ensure that charges are only incurred when cloud resources are utilized. This more accurately describes a public cloud, where resource elasticity allows storage and compute to be allocated on demand. This allows you to pay only for the resources you need when you need them.

Implementing a hybrid cloud will not allow your company to eliminate the need for company-managed compute resources. All cloud models will require your company to manage some aspect of compute resources.

You recently signed up for a free Azure subscription.

You need to familiarize yourself with the Azure portal UI.

Which UI elements best match the descriptions? To answer, select the appropriate UI elements from the drop-down menus.

Choose the correct options

A collection of customizable tiles that are displayed in the portal.	Dashboard
A panel that slides out in a navigation sequence.	Blade
A service that provides recommendations on high availability.	Azure Advisor

Explanation

A dashboard is a collection of customizable tiles that are displayed in the portal. You can add tiles, remove tiles, and reposition them as you wish. Each tile can represent a deployed resource, or even other elements such as a clock.

A blade is a panel that slides out in a navigation sequence. It represents a single level in a navigation hierarchy. Each blade provides either information or configuration options. Depending on which options you select, a new blade may open.

Azure Advisor is a service that provides recommendations on high availability. It also provides recommendations on cost, security, and performance. It analyzes the services that you deploy and tries to find ways to improve the usage of those services.

A resource panel is not a panel that slides out in a navigation sequence. It is the left-most panel in the portal. It lists the main resource types that are available.

Azure Marketplace does not provide recommendations on high availability. Azure Marketplace allows you to create new resources from a catalog.

Match each statement with the correct cloud model.

To answer, select the appropriate cloud models from the drop-down menus.

Choose the correct options

A company wants to deploy multiple servers to host web applications but wants to keep hardware costs and management costs to a minimum. The solution should be highly scalable.	Public model
A company needs to implement a solution where it maintains management control over hardware and infrastructure. The solution can be physically deployed offsite.	Private model
A company plans to use a custom software as a service (SaaS) application and wants to minimize costs. The company is legally required to maintain and secure all data onsite.	Hybrid model

Explanation

A company wants to deploy multiple servers to host web applications but wants to keep hardware costs and management costs to a minimum. The solution should be highly scalable. This describes a public model solution. A public cloud environment is one where the solution is managed by a provider. Most solutions are based on a multi-tenant model with the solution run in a shared environment with customer data partitioned to provide data security. Microsoft Azure is an example of a public cloud.

A company needs to implement a solution where it maintains management control over hardware and infrastructure. The solution can be physically deployed offsite. This describes a private model solution. A private cloud is one where an organization builds and maintains its own solution, either in its datacenter or hosted as dedicated resources by a solution provider. Services and infrastructure are hosted on a private network dedicated to that organization only. Government agencies and financial institutions often use the private cloud model.

A company plans to use a custom Software-as-a-Service (SaaS) application and wants to minimize costs. The company is legally required to maintain and secure all data onsite. This is best implemented as a hybrid model. A hybrid cloud combines features of public and private clouds. This provides a way to save costs by sharing less-secure solution needs in a public cloud and keeping high-risk, high-value resources internal to the network.

You plan to create an Azure subscription and take advantage of its Azure Active Directory (Azure AD) features. You plan to use the subscription for no more than one year.

You need to choose the least expensive license for each scenario.

Which license should you use? To answer, drag the appropriate license to each scenario. A license may be used once, more than once, or not at all.

Drag and drop the answers

You want to publish on-premises web apps using Azure AD.	Premium
You want to use on-premises directory synchronization.	Free
You want on-premises users to be able to reset their own passwords.	Premium

You should use the Premium license when you want to publish on-premises web apps using Azure AD. This functionality is provided by Azure AD Application Proxy.

You should use the Free license when you want to use on-premises directory synchronization. The Free license also supports single-sign on (SSO) and user and group management.

You should use the Premium license when you want on-premises users to be able to reset their own passwords. The self-service password reset feature is offered in the Office 365 Apps, Premium P1, and Premium P2 licenses.

You need to use Azure Cloud Shell to manage Linux virtual machines (VMs) that are already deployed and in use.

For each of the following management tools, select Yes if you can use the tool to manage Linux VMs in Cloud Shell. Otherwise, select No.

Management tools	Yes	No
Azure Command-line interface (CLI)	◉	○
Azure PowerShell	◉	○
Azure portal	○	◉

The Azure Cloud Shell supports the use of Azure CLI, Azure PowerShell, and Bash to manage Linux, Windows, and Mac OS VMs. Azure Cloud Shell also supports common programming languages.

You can access Cloud Shell through Azure portal or from shell.azure.com, but you cannot use Azure portal inside Cloud Shell.

Azure Cloud Shell lets you open an authenticated, browser-based management shell from virtually anywhere.

To complete the statement in the answer area, select the appropriate option from the drop-down menu.

Choose the correct options

A billing zone is a geographical grouping of Azure regions

used to determine billing based on [data transfers.]

A billing zone is a geographical grouping of Azure regions used to determine billing based on data transfers. Billing applies to both incoming and outgoing data and varies by billing zone. Data transfers between billing zones and regions in a zone are billed. Billing zones do not impact any other billing factors.

A billing zone is not used to determine billing based on hours of activity. Microsoft does bill based on usage, but this is not adjusted by zone.

A billing zone is not used to determine billing based on peak usage periods or resource deployment. These are not specific factors in billing and invoicing.

Your company wants to know which cloud deployment model would work best for them.

You need to choose the appropriate model for each scenario.

Which model should you use in each scenario? To answer, select the appropriate models from the drop-down menus.

Choose the correct options

Your company wants to create a virtual network with 10 virtual machines (VMs) and no capital expenditure (CapEx) costs.	Public
Your company wants to control the methods used to have a high level of security for its resources.	Private
Your company does not have IT experts or the money to purchase its own servers.	Public

You should use the public model when your company wants to create a virtual network with 10 VMs and no CapEx costs. CapEx involves spending money on physical resources up front. The public cloud allows you to deploy resources without managing the underlying hardware. The servers, storage devices, and networking devices exist in Azure datacenters. You are only required to manage the configuration of those devices, and that is why there are no CapEx costs.

You should use the private model when your company wants to control the methods used to have a high level of security for its resources. The private cloud allows you to deploy physical resources in a datacenter where you have access. This means that you can control the physical security of your resources.

You should use the public model when your company does not have IT experts or the money to purchase its own servers. The servers, storage devices, and networking devices exist and are maintained in Azure datacenters by the cloud service provider. You are only required to manage the configuration of those devices, and that is why there are no CapEx costs.

You should not use the hybrid model in any of the given scenarios. This model is a mixture of Azure cloud services and an on-premises infrastructure.

You work for a private equity firm in Richmond, Virginia. You are planning to deploy a virtual machine (VM) to Azure that allows developers to run a .NET Core web service. The client applications that access the web service are deployed at the firm. The developers inform you that any operating system can be used.

You need to use the Azure pricing calculator to determine the least expensive cost of the deployed VM.

Which settings should you select? To answer, select the appropriate settings from the drop-down menus.

Choose the correct options

You should set the Region to East US. East US is the closest region to Virginia that supports non-government deployments.

You should set the Operating System to Linux. Linux is less expensive than Windows. Because the developers use .NET Core, any operating system can be used.

You should set the Tier to Basic. Even though it is more expensive than Low Priority, you would not deploy a low priority VM in a scenario in which there will be only a single VM.

You should not set the Region to US Gov Virginia. Only government agencies and government contractors can use this region. In this scenario, your company is a private equity firm.

You should not set the Tier to Standard. This option is more expensive than Basic and Low Priority.

You should not set the Operating System to Windows. Windows is more expensive than Linux.

Your company wants to ensure that it meets its internal compliance goals and that Azure resources are compliant with company standards. This will include ongoing evaluation for compliance and the identification of non-compliant resources.

You need to recommend a solution.

What should you use?

Choose the correct answer

- [x] Azure Policy
- [ ] Azure Advisor
- [ ] Azure Monitor
- [ ] Role-based access control (RBAC)

You should use Azure Policy. Azure Policy lets a company enforce rules that apply to resources to help ensure compliance with company standards. Policies can also be used to ensure that resources meet service level agreement (SLA) requirements. Resources are evaluated based on policies and non-compliant resources are identified.

You should not use RBAC. RBAC lets you manage access to resources through built-in and custom roles applied to management groups, subscriptions, resource groups, and resources. Roles can be assigned to groups, users, other security principals, and managed identifies. RBAC has over 70 built-in roles.

You should not use Azure Advisor. Azure Advisor integrates with Azure Security Center to provide a consolidated view of recommendations for all Azure resources to help improve the cost effectiveness, performance, high availability, and security of Azure resources. It does not enable you to monitor and evaluate for compliance.

You should not use Azure Monitor. Azure Monitor provides a solution for collecting, analyzing, and acting on telemetry from cloud and on-premises environments, however it would not enable you to monitor for compliance with company standards.

You manage an Azure subscription for your company. At a meeting, someone asks you about the Azure pricing calculator.

What is the Azure pricing calculator used for?

Choose the correct answer

- Providing a real-time, up-to-the-minute view of what your Azure resources cost.
- Determining the annual costs associated with moving a physical infrastructure to the cloud.
- Determining which resources are costing your Azure subscription the most money.
- ✔ Estimating the monthly costs associated with using specific Azure resources.

The Azure pricing calculator is used for estimating the monthly costs associated with using specific Azure resources. With each resource that you add to the pricing calculator, you can choose its region, which also affects the price. For other resources, such as an Azure SQL Database, you can choose the number of instances and the type of each instance, which also affects the cost.

The Azure pricing calculator is not used for determining the annual costs associated with moving a physical infrastructure to the cloud. You would use the Azure Total Cost of Ownership (TCO) calculator if you wanted to perform this task.

The Azure pricing calculator does not allow you to determine which Azure resources are costing your subscription the most money. Azure Cost Management helps with this task.

The Azure pricing calculator does not provide a real-time, up-to-the-minute view of what your Azure resources cost. Azure Cost Management helps provide this data. However, it does not provide up-to-the-minute cost analysis. Estimated charges are updated six times per day.

You create an Azure subscription.

You need to determine when you should use specific Azure management tools.

When should you use each tool? To answer, drag the appropriate tool to each scenario. A tool may be used once, more than once, or not at all.

Drag and drop the answers

You need to log in to Azure with the following cmdlet from your laptop without manually opening a web browser: Connect-AzAccount	Azure PowerShell
You need to log in to Azure with the following command from your laptop without manually opening a web browser: az login	Azure CLI
You want to run the following cmdlet in a scripting environment inside the browser: New-AzVm	Azure Cloud Shell

You should use Azure PowerShell when you need to log in to Azure with the following cmdlet from your laptop without manually opening a web browser:

```
Connect-AzAccount
```

Azure PowerShell is a module that you can install on your computer for Windows, Linux, or macOS. It allows you to use PowerShell cmdlets locally to administer Azure resources.

You should use Azure CLI when you need to log in to Azure with the following command from your laptop without manually opening a web browser:

```
az login
```

Azure CLI is a cross-platform command-line tool that allows you to manage Azure resources from your computer.

You should use Azure Cloud Shell when you need to run the following cmdlet in a scripting environment inside the browser:

```
New-AzVm
```

Azure Cloud Shell is a web-based tool that allows you to run PowerShell cmdlets or Azure CLI commands after you log in to the Azure portal.

To complete the statement in the answer area, select the appropriate option from the drop-down menu.

Choose the correct options

A private cloud requires

the infrastructure to be on a private network.

Explanation

A private cloud's services and infrastructure are maintained on a private network. An organization can implement its own private cloud, but it is more common to subscribe to a private cloud hosted and managed by a third-party provider.

A private cloud does not require the use of custom developed software, although it may have custom software depending on the tenant's needs. It is common to find a mix of commercial applications with some custom applications.

A private cloud does not require data to be stored in an on-premises datacenter. It is possible to create a private cloud from an on-premises datacenter, but this is not a requirement.

A private cloud does not require each tenant to access applications and data through a different URL. A private cloud will have, by definition, a single tenant.

party service provider and shared with other organizations. You only pay for the compute power, storage, and networking resources you use.

What type of cloud computing is this an example of?

Choose the correct answer

- ○ Hybrid cloud
- ✔ Public cloud
- ○ Private cloud
- ○ On-premises datacenter

Explanation

This is an example of a public cloud computing. With a public cloud, the cloud resources (compute power, storage, networking) are owned and operated by the relevant cloud service provider and delivered over the Internet. You pay only for what you use. The underlying physical infrastructure of the public cloud is shared with other organizations, the so called cloud tenants.

This is not an example of hybrid cloud computing. With hybrid computing, you combine a private cloud with a public cloud. Private cloud infrastructure is not shared with other organizations and is used to host certain workloads, like highly sensitive data that cannot be stored on the shared infrastructure because of the regulatory requirements. Public cloud infrastructure can be used to host less sensitive solutions to enable flexible and cost-effective methods of running your workload.

This is not an example of a private cloud computing. In a private cloud, computing resources are used exclusively by one business or organization. Computing infrastructure may belong to your organization or a third-party service provider. However, the underlying infrastructure is not shared with other organizations, but dedicated solely to yours.

This is not an example of on-premises datacenter computing. An on-premises datacenter is typically used to build a private cloud because the hardware and software are located at your organization's own on-site datacenter and dedicated to your organization's workload only.

Which Azure security solution provides general security recommendations and suggests remediations to better secure your resources?

Choose the correct answer

- Azure Information Protection (AIP)
- Key Vault
- ✔ Microsoft Defender for Cloud
- Azure DDoS Protection Standard

Explanation

Microsoft Defender for Cloud provides security recommendations and suggests remediation actions, including suggestions for which remediations should take priority. Microsoft Defender for Cloud is designed to help to protect Azure cloud, non-Azure cloud, and hybrid computing resources through a set of security tools. These include tools for monitoring the network to prevent, detect, and respond to potential security threats. Microsoft Defender for Cloud provides tools to help to strengthen your organization's security posture, protect against threats, and quickly secure your computing environment. It makes it easier to manage your organization's security policies and compliance.

Azure DDoS Protection Standard does not provide general security and remediation recommendations. Azure DDoS Protection is designed specifically to provide defense against distributed denial of service (DDoS) attacks.

AIP does not provide security and remediation recommendations. AIP enables an organization to organize and protect documents and emails through the use of labels. Labels can be applied manually by users or automatically through administrator-defined rules. The classifications make the data identifiable no matter where the data is stored or even if the data has been shared.

Key Vault does not provide security and remediation recommendations. Key Vault is used to securely store cryptographic keys and other secrets. Key vault features include:

- Securely store and control access to tokens, passwords, certificates, API keys, and other secrets.
- Create and control encryption keys that are used to encrypt data.
- Provision, manage, and deploy both public and private SSL/TLS certificates.
- Store secrets and keys protected by software or FIPS 140-2 Level 2 validated hardware security modules (HSMs).

For each of the following statements regarding factors that affect costs in Azure, select Yes if the statement is true. Otherwise, select No.

Statement	Yes	No
Azure Advisor makes shutdown recommendations based on CPU and memory utilization over the last seven days.	○	◉
You can use Azure Advisor to reduce costs by resizing underutilized virtual machines.	◉	○
Tags can aid in cost management for your subscriptions, and each tag consists of a name, location, and value.	○	◉

Azure Advisor does not make shutdown recommendations based on Central Processing Unit (CPU) and memory utilization over the last seven days. Azure Advisor makes shutdown recommendations based on CPU and outbound network utilization.

Azure Advisor is a cloud service that helps you to optimize your Azure resources for cost, performance, and availability. It analyzes your resource configuration and usage telemetry to identify issues and recommend solutions that can help you improve efficiency and save money.

You can use Azure Advisor to reduce costs by resizing underutilized virtual machines. Advisor analyzes your resource usage and activity data, and then makes recommendations based on best practices from Microsoft. The recommendations are based on how you use Azure resources and services.

Tags can aid in cost management for your subscriptions; however, each tag consists only of a name and value pair. Azure tags are labels that can be applied to Azure resources to help you organize and categorize them. You can apply as many tags as you want to a resource, and each tag can have a different key and value. For example, you could apply the tag "Name" with the value "MyWebApp" to an Azure Web App resource. Tags do not include a location.

You need to understand Azure monitoring options.

Which monitoring feature should you use for each scenario? To answer, drag the appropriate feature to each scenario. A feature may be used once, more than once, or not at all.

Drag and drop the answers

You want to enable developers to improve app performance and usability.	Application Insights
You want to receive an email whenever the number of requests to a web app exceeds 10,000 within an hour.	Alerts
You want to view the number of virtual machines (VMs) that are currently down.	Resource Health

Explanation

You should use Application Insights to enable developers to improve app performance and usability. Application Insights monitors the availability, performance, and usage of web applications. It exposes an API so that developers can log data to Azure and evaluate performance bottlenecks and app usability.

You should use Alerts to receive an e-mail whenever the number of requests to a web app exceeds 10,000 within an hour. Alerts are notifications that you set up to be sent when a metric exceeds a certain threshold.

You should use Resource Health to view the number of VMs that are currently down. Resource Health displays a list of health issues that are related to a particular resource, such as whether a VM is available or not.

You should not use Metrics. Metrics simply tell you how a resource is performing and what it is consuming.

Your company uses management groups to manage resources in your Azure tenant more efficiently. User1 should be able to assign access and assign policies to management groups.

You need to determine which role-based access control (RBAC) role User1 should be added to. Your solution should follow the principle of least privilege.

Which role should you add User1 to?

Choose the correct answer

- Contributor
- ✔ User Access Administrator
- Management Group Contributor
- Owner

Explanation

You should add User1 to the User Access Administrator role. From the context of management groups, this role grants permissions to assign access and assign policies only.

You should not add User1 to the Owner role because this would grant them more permissions than necessary. Members of the Owner role can create, update, move, delete, and read management groups in addition to assigning access policies.

You should not add User1 to the Contributor or Management Group Contributor role. Neither of these roles would grant User1 permission to assign access or assign policies. Members of both roles can create, update, move, delete, and read management groups.

Which two organization-level insights can you derive from the Regulatory Compliance dashboard of Microsoft Defender for Cloud? Each correct answer presents part of the solution.

Choose the correct answers

- [ ] Overall secure score
- [ ] Mitigation steps for reported threats
- [x] Number of passing and failing assessments
- [x] Overall compliance score
- [ ] Security alerts ranked by severity

Explanation

On the Regulatory Compliance dashboard of Microsoft Defender for Cloud, you can find an overall compliance score and the number of passing and failing assessments. The overall compliance score provides insight into your organization's compliance posture against a supported set of standards and policies. Additionally, you get the status of all the assessments in the context of a particular standard or policy regulation, with the number of passed and failed assessments associated with each.

Security alerts ranked by severity and mitigation steps for reported threats are part of the Security Alerts section of Microsoft Defender for Cloud. This provides you with a unified view of all security alerts raised across your hybrid cloud workload. Security alerts are grouped by their severity level, as High Severity, Medium Severity, and Low Severity alerts. You can investigate the the root cause for each alert and manually apply recommended steps to mitigate the threat.

The overall secure score can be found in the Secure Score section of Microsoft Defender for Cloud. It is a single score shown as a percentage value that aggregates all the security findings across your resources, subscriptions, and organizations to provide you with a high-level assessment of the current security situation. The higher the overall secure score, the lower the identified security risk level.

Match each Azure resource with its use scenario.

To answer, drag the appropriate resource to each scenario. A resource may be used once, more than once, or not at all.

Drag and drop the answers

Fast migration of SQL Server from on-premises to Azure with retention of operating system access	SQL Server on Azure VMs
Cost-effective, serverless database with an intermittent usage pattern and a low compute utilization over time	Azure SQL Database
Life=and-shift of on-premises SQL Server with minimal changes to an Azure Platform-as-a-Service (PaaS) solution	Azure SQL Managed Instance

You should use SQL Server on Azure VMs for the fast migration of SQL Server from on-premises to Azure with retention of operating system access. This option enables lift-and-shift from an on-premises datacenter to Azure with ease, while maintaining 100 percent compatibility with SQL Server and providing full access to the database engine and operating system on the VM level.

You should use Azure SQL Database as a cost-effective, serverless database with an intermittent usage pattern and a low compute utilization over time. The serverless service tier of Azure SQL Database is optimized for scenarios with intermittent or unpredictable usage patterns. It automatically pauses the database during periods of inactivity and resumes it when activity returns, enabling per second billing for the actual amount of compute consumed.

You should use Azure SQL Managed Instance for the lift-and-shift of on-premises SQL Server with minimal changes to an Azure PaaS solution. Azure SQL Managed Instance has near 100 percent compatibility with the latest version of SQL Server Enterprise Edition, enabling frictionless migration to Azure with minimal application and database changes. At the same time, it is a PaaS offering, eliminating overhead for the management of underlying infrastructure.

You should not use Azure Database for PostgreSQL for any of the listed scenarios. Azure Database for PostgreSQL is a fully managed database service based on PostgreSQL Community Edition database engine. However, as a PaaS offering, it does not provide access to the operating system, is not compatible with SQL Server to provide a smooth lift-and-shift experience, and has no serverless tiers for the cost-effective hosting of a database with an intermittent usage pattern.

Which Azure service can use autoscale to add or remove resources as appropriate to minimize costs and ensure optimum performance levels?

Choose the correct answer

- Azure Advisor
- Azure Service Health
- ✔ Azure Monitor
- Microsoft Defender for Cloud

Azure Monitor can use autoscale to add or remove resources as appropriate to minimize costs and ensure performance. You can create rules based on metrics collected by Azure Monitor to match resources to an application load.

Azure Service Health does not use autoscale to match resources to load requirements. Azure Service Health provides information about issue and their impact and provides updates as issues are resolved. It can also keep you informed about service outages and planned maintenance.

Microsoft Defender for Cloud does not use autoscale to match resources to load requirements. Microsoft Defender for Cloud is designed to help protect Azure cloud, non-Azure cloud, and hybrid computing resources through a set of security tools. Microsoft Defender for Cloud provides tools to help strengthen your organization's security posture, protect against threats, and quickly secure your computing environment.

Azure Advisor does not use autoscale to match resources to load requirements. Azure Advisor analyzes your resource configuration to help you optimize your Azure deployments. It provides best practices recommendations regarding performance, security, and availability.

Your company deploys resources in Azure. According to the shared responsibility model, which task will you be required to perform?

Choose the correct answer

- Upgrade RAM on virtualization systems.
- Configure connectivity between regions.
- ✔ Install critical updates on virtual machines.
- Manage access to data center resources.

According to the shared responsibility model, you will install critical updates on virtual machines. The cloud shared responsibility model is a framework that delineates the roles and responsibilities of a cloud service provider (CSP) and its customers in managing data, applications, and infrastructure components stored in, or running on, the cloud. In the public cloud model, installing critical updates on a virtual machine would be managed by the customer.

According to the shared responsibility model, you will not manage access to data center resources. Data center access is typically tightly controlled, and all requests must be approved by the CSP. While on-premises, visitors have restricted access to only the required resources. This is done to ensure the security and availability of cloud resources.

According to the shared responsibility model, you will not configure connectivity between regions. Depending on the CSP, a region is a geographically constrained area where one or more data centers is located. The CSP is responsible for managing network connectivity between regions.

According to the shared responsibility model, you will not upgrade RAM on virtualization systems. The CSP always maintains responsibility for the physical compute, storage, and networking hardware it uses to offer its cloud services. In the event Random Access Memory (RAM) needs to be replaced or upgraded, the CSP performs this duty.

You are tasked with addressing performance issues on an Azure-based web server cluster.

You need to configure virtual machines to scale vertically.

What should you do to meet this requirement?

Choose the correct answer

- Allow additional virtual machines to be auto-deployed as needed.
- Configure the cluster to burst into a hybrid cloud.
- Migrate the server cluster to a Kubernetes cluster.
- ✔ Add compute and memory resources to each virtual machine.

You should add compute and memory resources to each virtual machine. When it comes to managing the resources required for virtual machines, you have several options for scaling performance on demand. Vertical scalability describes an environment where the number of compute nodes is minimized, but compute resources for each node are increased. For example, Random Access Memory (RAM), faster storage, and additional Central Processing Units (CPUs) are added to a single server to increase performance. Depending on the cloud service provider (CSP), this can either be done by modifying the instance or migrating to an instance that offers expanded resources.

You should not configure the cluster to burst into a hybrid cloud. Cloud bursting is used in hybrid cloud models consisting of on-premises and cloud-based resources. In a cloud bursting scenario, when the on-premises compute infrastructure is saturated, cloud-based resources come online to address the increased workload. This approach does not add compute or memory resources to existing virtual machines.

You should not allow additional virtual machines to be auto-deployed as needed. This describes horizontal scalability, where load is distributed across compute nodes that are added and removed as needed. This approach does not add compute or memory resources to existing virtual machines.

You should not migrate the server cluster to a Kubernetes cluster. Kubernetes is an orchestration tool that helps you manage your containerized applications by providing features like auto-scaling, self-healing, rolling updates, and more.

You are planning to create a cloud solution in Azure.

You need to choose the appropriate networking resources to deploy for certain scenarios.

Which resources should you deploy? To answer, select the appropriate resources from the drop-down menus.

Choose the correct options

Scenario	Resource
You want to allow inbound traffic to an Azure Virtual Machine (VM) from only specific IP addresses.	Network Security Group (NSG)
You want to prevent a malicious flood of HTTP traffic to a VM that hosts Internet Information Services (IIS).	Distributed Denial-of-Service (DDoS) Protection
You want to create a rule that restricts network traffic across subscriptions.	Azure Firewall

You should use an NSG to allow inbound traffic to an Azure VM from only specific IP addresses. An NSG allows or denies inbound traffic to an Azure resource. For example, you associate an NSG with a subnet, which is part of a virtual network (VNet). A VM can be attached to a VNet. The NSG can allow or deny traffic to that VM.

You should use DDoS Protection to prevent a malicious flood of HTTP traffic to a VM that hosts IIS. DDoS Protection helps prevent volumetric attacks, protocol attacks, and application layer attacks.

You should use Azure Firewall when you want to create a rule that restricts network traffic across subscriptions. It has built-in high availability. Rules are enforced and logged across subscriptions, which reduces management overhead.

Traffic Manager allows users to access Azure resources from a datacenter that is nearest to them by using Domain Name System (DNS). This service does not meet any of the requirements.

Application Gateway is a load balancing solution that uses routing to send HTTP traffic to a pool of backend instances. This service does not meet any of the requirements.

An NSG does not allow you to create a policy that restricts network traffic across subscriptions. An NSG can only protect resources in a single subscription.

Which setup represents a hybrid cloud model?

Choose the correct answer

- An Azure WebJob that makes calls to the Azure Representational State Transfer (REST) Application Program Interface (API)
- ✔ An Azure web Application Program Interface (API) that connects to an on-premises SQL Server database at an on-premises private datacenter
- An Azure Function that crawls the web for trending news
- An Azure web application that connects to an Azure SQL Database

Explanation

An Azure web API that connects to an on-premises SQL Server database represents a hybrid deployment model. A hybrid deployment model exists when Azure hosts some resources while your company hosts others. Hybrid deployments combine public and private cloud deployments, and the private cloud can be an on-premises private datacenter.

An Azure web application that connects to an Azure SQL Database does not represent a hybrid cloud deployment model. This represents a public cloud deployment model. No on-premises resources are used in this scenario. A public cloud deployment model occurs when resources are only deployed to the public cloud, such as Azure.

An Azure Function that crawls the web for trending news does not represent a hybrid deployment model. This represents a public deployment model. No on-premises resources are used in this scenario. In a public deployment model, only Azure resources are used.

An Azure WebJob that makes calls to the Azure REST API does not represent a hybrid deployment model. It represents a public cloud deployment model. A public cloud deployment model occurs when resources are only deployed to the public cloud, such as Azure.

Match each Microsoft cloud service with its cloud service type.

To answer, drag the appropriate type to each cloud service. A type may be used once, more than once, or not at all.

Drag and drop the answers

Azure Cosmos DB	PaaS
Azure Storage	IaaS
Microsoft Office 365	SaaS

Azure Cosmos DB is an example of platform as a service (PaaS). PaaS is a type of cloud computing that provides a platform for developers to build, run, and manage applications without the need for infrastructure management. Typically, PaaS providers offer a wide variety of services, including databases, analytics, workflow engines, and more.

Azure Storage is an example of infrastructure as a service (IaaS). In IaaS, network, compute, and storage resources are offered by a cloud provider. These resources may be shared by multiple tenants, or they can be dedicated to a single tenant. Some cloud providers offer full data center IaaS solutions, including a physically secure room or building.

Microsoft Office 365 is an example of software as a service (SaaS). SaaS is a type of subscription software that allows you to use the software from a remote location, often through the internet. It is popular with businesses because it allows them to avoid the cost and hassle of installing and maintaining software on their own systems.

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

Statement	Yes	No
You can transfer an existing subscription to a new Azure Active Directory (AD) tenant.	◉	○
Quotas for resources in Azure Resource Groups are per region rather than per subscription.	◉	○
A user can only be given access to one subscription.	○	◉

You can transfer an existing subscription to a new Azure AD tenant. When you transfer a subscription, all role-based access control (RBAC) role assignments are deleted from the source tenant. RBAC role assignments are not migrated to the destination tenant.

Quotas for resources in Azure Resource Groups are per region rather than per subscription. Limits for many resources are higher than traditional default limits for resources managed in Azure Resource Groups through Azure Resource Manager.

A user can be given access to multiple subscriptions and access resources in those subscriptions. However, a resource can belong to only one subscription.

To complete the sentence, select the appropriate option from the drop-down menu.

Choose the correct options

With serverless computing , developers deploy code and pay for its runtime only, without worrying about the provisioning, configuration and management of the underlying infrastructure.

With serverless computing, developers deploy code and pay for its run time only, without worrying about the provisioning, configuration, and management of the underlying infrastructure. A pay-per-execution model in serverless computing allows sub-second billing only for the time and resources required for the execution of code. All tasks related to the provisioning, configuration, and management of the underlying infrastructure are carried out by the cloud provider and are not visible to the developer.

With IaaS, the cloud service provider takes care of the the underlying physical infrastructure. However, as a customer, you are still responsible for the installation, configuration, and management of application components, such as the operating system, middleware, and applications. You can deploy your code, but IaaS billable charges would include the cost of all allocated compute resources.

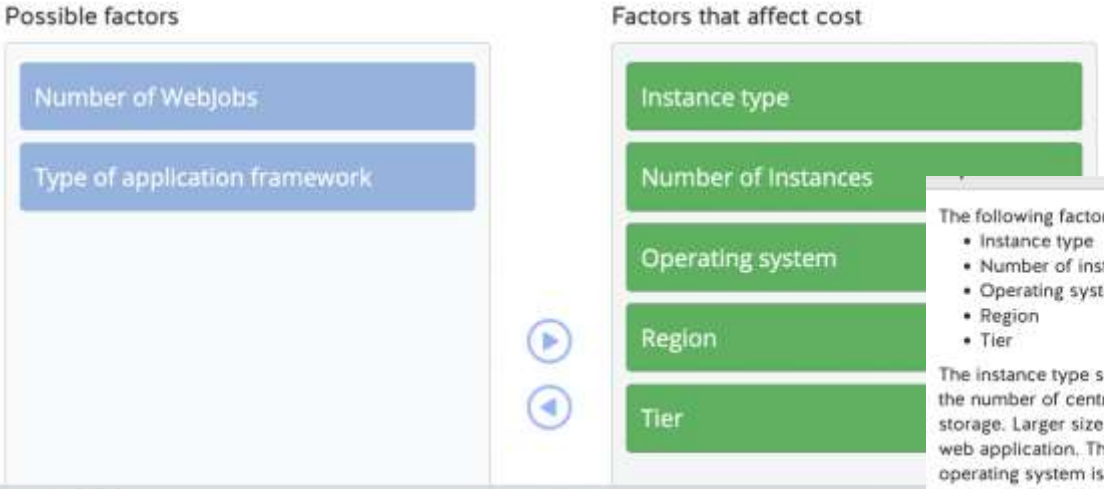
With SaaS, the cloud service provider is responsible for the provision and management of both physical and software components. As a customer, you cannot change the code of a SaaS solution, because control and responsibility is limited to data and access. SaaS solutions are typically licensed and charged through a monthly or annual subscription.

You are given approval to move your company's web application to Azure as an App Service. However, your manager wants to know the annual cost for such a move. You decide to use the Azure Pricing Calculator to estimate the cost.

You need to determine which factors affect the cost.

Which five factors affect the cost of an App Service? To answer, move the appropriate factors from the list of possible factors to the answer area and arrange them in any order.

Create a list in any order



The following factors affect the cost of an App Service web application in Azure:

- Instance type
- Number of instances
- Operating system
- Region
- Tier

The instance type specifies the size of the virtual machine (VM) that hosts the web application. Size refers to the number of central processing unit (CPU) cores, the amount of allocated memory, and the size of storage. Larger sizes increase the cost. The number of instances refers to the number of VMs that host the web application. The more instances, the higher the price. The operating system specifies whether the VM operating system is Windows or Linux. Linux is slightly cheaper than Windows. The region specifies the location of the deployed VM. Prices vary by geographical location. The tier allows you to choose whether you want a shared VM or an isolated VM. To use a shared VM, you must choose the Free or Shared tier. The Free tier does not incur a price.

The following factors do not affect cost: number of WebJobs and type of application framework. WebJobs are free because they run on the same host as the VM and in the same context as an App Service web application. The type of application framework, such as .NET Framework 2.0 or .NET Core has no effect on the price of a web application. Azure supports both.

Which Azure service is used to send an email to an administrator when a virtual machine (VM) is about to exceed its usage quota for the month?

Choose the correct answer

- Service Health
- Azure Monitor metrics
- Application Insights
- ✔ Azure Monitor alerts

Azure Monitor alerts allow an administrator to configure actions that should occur when specific conditions are met on the consumer side (conditions the consumer is responsible for). For example, alerts can be sent via an email when the CPU for a VM exceeds a certain threshold or resource usage quotas, such as CPU Credits Remaining for a VM, is reached.

Application Insights is an Application Performance Management (APM) service that detects performance in real-time. It allows cloud and on-premises applications to send telemetry data to Azure.

Service Health tracks the state of Azure services. It is used to notify administrators when certain events take place, for which the cloud provider is responsible. Examples are: planned maintenance or service outage. You can use Service Health alerts to send an email whenever an event occurs, that you are interested in.

Azure Monitor metrics are numerical values that describe some aspects of the system, such as Central Processing Unit (CPU) time. Metrics are not an analysis feature.

You move some Windows Server virtual machines (VMs) from your on-premises datacenter to Azure. Existing on-premises VMs are licensed by your company's active Microsoft Software Assurance agreement.

You need to reduce the cost of your Azure VMs.

What should you do?

Choose the correct answer

- Create VMs in availability sets.
- ✔ Enable the Azure Hybrid Benefit setting.
- Create VMs in availability zones.
- Deploy your VMs on an Azure Dedicated Host.

You should enable the Azure Hybrid Benefit setting. Activating this licensing option in the VM settings allows you to use existing Windows Server licenses, which are covered by the active Microsoft Software Assurance agreement, to run Windows VMs in Azure. You pay only for the VMs' infrastructure cost, which can be up to 40 percent of the regular cost.

You should not create VMs in availability sets or availability zones. Both would help you to achieve higher availability for your VMs. With availability sets, your VMs are automatically distributed across the fault domains within a datacenter to limit the impact of potential hardware, network, or power failures. Availability zones are physically separated zones in an Azure region that allow you to protect your VMs from the loss of entire datacenter.

You also should not deploy your VMs on an Azure Dedicated Host. Azure Dedicated Hosts provide physical servers dedicated to your organizational workload only and not shared with other Azure customers. You are charged at the host level, regardless of the number of VMs you deploy.

Which two locations are valid destinations for platform logs and metrics collected by Azure Monitor? Each correct answer presents a complete solution.

Choose the correct answers

- [ ] A Resource Health dashboard
- [ ] An Azure Advisor monitor
- [x] An Azure Log Analytics workspace
- [x] An Azure storage account

An Azure Log Analytics workspace is a valid destination for platform logs and metrics collected by Azure Monitor. An Azure Log Analytics workspace is a place in the cloud where you can collect and query your log data. You can use an Azure Log Analytics workspace to explore and analyze data from a variety of sources, including Azure services, on-premises systems, and other cloud providers.

An Azure storage account is a valid destination for platform logs and metrics collected by Azure Monitor. Azure Storage is a cloud-based storage service offered by Microsoft. It allows you to store data in the cloud for easy access from anywhere. You can use Azure Storage to store files, including photos, videos, and documents, to host websites and apps, and to store data for analytics purposes.

A Resource Health dashboard is not a valid destination for platform logs and metrics collected by Azure Monitor. Resource Health is a service you can use to get status information for your organization's resources.

An Azure Advisor monitor is not a valid destination for platform logs and metrics collected by Azure Monitor. Azure Advisor is a cloud service that helps you optimize your Azure resources for cost, performance, and availability. It analyzes your resource configuration and usage telemetry to identify issues and recommend solutions that can help you improve efficiency and save money.

Your Azure tenant includes several internet-facing web servers. The web servers rely on data stored on Azure SQL Database servers. The web servers are located in different virtual network (VNet) subnets. The database servers have their endpoint exposed to the subnets.

You need to implement detailed controls over the types of connections supported between the web servers and database servers. You want to minimize the efforts and costs necessary to implement and maintain your solution.

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

Choose the correct answers

- [ ] User Defined Routes (UDRs)
- [ ] Azure Firewall
- [ ] Azure Traffic Manager
- [x] Application Security Groups (ASGs)
- [x] Network Security Groups (NSGs)

You should include NSGs and ASGs in your solution.

In multi-tier architecture ASGs provide the possibility to group network interfaces of virtual machines (VMs) per service tier and give each service tier human readable labels, such as WebAccess or SQLTier. Such labels are easier to read and are more meaningful compared to IP addresses. As an example, when you configure an NSG filtering rule, instead of adding 10.0.0.0/24 you add ASG with the label WebAccess (which groups all the web servers in your web tier) as the destination. Instead of adding 10.0.1.0/24 you add ASG with the label SQLTier (which groups all your SQL servers in your backend tier) as the destination.

NSGs are specialized packet-filtering firewalls that let you define security rules to control traffic into and out of a VNet, between subnets, or per VM. You have the option of applying NSGs to ASGs to limit their filtering to servers in those ASGs. You would create the necessary ASGs first, add the desired servers to the respective ASGs, and then create your NSGs and apply filtering rules using the ASGs (as source or destination).

You should not include UDRs in your solution. UDRs are custom routing tables that are used to override and supplement the default routing tables in VNets.

You should not use Azure Firewall. Azure Firewall provides traffic filtering, similar to NSGs. Both services are not mutually exclusive; they can complement each other. Using Azure Firewall with NSGs can provide better defence-in-depth network security. Implementing Azure Firewall will result in additional costs and efforts for configuration and maintaining. In this scenario the costs and effort have to be minimized.

You should not include Azure Traffic Manager as a part of your solution. Azure Traffic Manager is a DNS-based traffic load balancer that lets you distribute traffic across global Azure regions. It does not provide the ability to filter traffic by connection.

A company is migrating several web apps from an on-premises private cloud deployment to Azure. The company wants to use Azure Active Directory (Azure AD) for authentication and authorization.

You need to determine if Azure AD will meet your authentication requirements.

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

Statement	Yes	No
Azure AD authentication and authorization support requires integration with an on-premises AD.	○	◉
Web apps must be registered with Azure AD to support authentication and authorization services.	◉	○
Azure AD supports authorization through the use of role-based access control (RBAC).	◉	○

Azure AD authentication and authorization support does not require integration with an on-premises AD. Integration is supported and might be applicable in a hybrid environment supporting both Azure and on-premises resources. When it is used with on-premises Active Directory Federation Services (AD FS), Azure AD hands off authentication to an AD FS server.

Web apps must be registered with Azure AD to support authentication and authorization services. Registration is through the Azure Management Portal.

Azure AD supports authorization through use of RBAC. RBAC is necessary to set up access permissions when using Azure AD for authentication and authorization.

Which two infrastructures are valid hybrid cloud infrastructures? Each correct answer presents part of the solution.

Choose the correct answers

- [x] On-premises infrastructure and public cloud
- [ ] On-premises infrastructure and private cloud
- [x] Private and public cloud
- [ ] Multiple public clouds
- [ ] Multiple private clouds

Explanation

A hybrid cloud is based on an on-premises architecture and a public cloud or a private cloud and a public cloud. This cloud model is most commonly used when leveraging benefits of running applications from a public cloud while providing additional security by storing data in a private cloud or an on-premises datacenter.

Multiple public clouds and multiple private clouds do not represent hybrid clouds. In each case, it is simply multiple instances of that cloud model.

While it is possible to have a federated configuration that includes an on-premises infrastructure and private cloud, this is not considered a hybrid cloud. This configuration might be used, for example, when transitioning from an on-premises to a cloud-based datacenter.

Your company has a new policy to restrict administrative access to resources at the resource group and resource scopes in a detailed, granular way. Access will be granted to various groups and individual users.

You need to implement the new policy.

What should you use?

Choose the correct answer

- Azure Advisor
- Locks
- ✔ Role-based access control (RBAC)
- Azure Policy

Explanation

You should use RBAC. RBAC supports various scopes, including management groups, subscriptions, resource groups, and resources. Roles can be assigned to groups, users, other security principals, and managed identifies. RBAC has over 70 built-in roles and supports the creation and assignment of custom roles.

You should not use Azure Policy. Azure Policy is used to enforce rules that apply to resources to help ensure compliance and to meet Service Level Agreement (SLA) requirements. Resources are evaluated based on policies, and non-compliant resources are identified.

You should not use Azure Advisor. Azure Advisor integrates with Azure Security Center to provide a consolidated view of recommendations for all Azure resources. It can help you improve the cost effectiveness, performance, high availability, and security of Azure resources.

You should not use Locks. Locks are used to limit access to a subscription, resource group, or resource by setting the access Lock level as CanNoDelete or ReadOnly. When a lock is set for a subscription or resource group, it applies to all of the resources contained in that scope. Locks apply to all users and roles and do not provide the granular control required by the scenario.