Answer Sheet

Q1)

Overview:

XYZ is an online training provider. they have several main offices and a couple of branch offices.

Existing Environment

1) Their existing environment consist of an active directory domain named XYZ.com. This is being hosted on a Windows Server.

2) A set of web servers hosted on a VMware environment.

3) A set of Microsoft SQL server database servers hosted on physical servers

4) The company has also set up an Azure AD tenant.

5) Their subscription currently consists of Azure AD basic licences.

Network Infrastructure:

1) Each of the main offices has a data centre in place.

2) Each office also has a dedicated internet connection

Requirements

Planned Changes

1) The company wants to set up new office in London

2) All the sources for the London office will be hosted in Azure

3) The on-premises active directory will be synchronized to Azure AD

4)All client computers in the London office will be joined to the Azure AD domain.

Planned Azure Networking Infrastructure

Name
XYZ- London
XYZ- office
XYZ- client

The following subnets will be in place

Virtual Network Name	Subnet
XYZ-London	Subnet A
XYZ- London	Subnet B
XYZ- client	Subnet C
XYZ- office	Subnet D
XYZ- office	Subnet E

The following additional settings will be in place

1) Default routes in Azure will be used to route traffic

2) A peering connection will be established between the virtual networks XYZ-London and XYZ-office

3)The peering connection for XYZ-London will have remote gateways enabled

4) A private DNS zone will be created named XYZ local. the registration network will be set to the XYZ-client virtual network

The company has the following additional requirements:

1) A number of web apps will be deployed. The initial settings of the web apps will be the same.

2) The senior management needs to have the ability to view the costs for Azure resources from the prior week.

A Development team wants to use a serverless compute service that could be used in conjunction with the web applications when they are migrated to Azure. They decide to use the Azure function app service.

Would this fulfill the requirement?

✅ Correct

Explanation:-This is a serverless compute service that is available on the Azure platform

⚪ Incorrect

Q2)

Overview:

XYZ is an online training provider. they have several main offices and a couple of branch offices.

Existing Environment

1) Their existing environment consist of an active directory domain named XYZ.com. This is being hosted on a Windows Server.

2) A set of web servers hosted on a VMware environment.

3) A set of Microsoft SQL server database servers hosted on physical servers

4) The company has also set up an Azure AD tenant.

5) Their subscription currently consists of Azure AD basic licences.

Network Infrastructure:

1) Each of the main offices has a data centre in place.

2) Each office also has a dedicated internet connection

Requirements

Planned Changes

1) The company wants to set up new office in London

2) All the sources for the London office will be hosted in Azure

3) The on-premises active directory will be synchronized to Azure AD

4)All client computers in the London office will be joined to the Azure AD domain.

Planned Azure Networking Infrastructure

Name
XYZ- London
XYZ- office
XYZ- client

The following subnets will be in place

Virtual Network Name	Subnet
XYZ-London	Subnet A
XYZ- London	Subnet B
XYZ- client	Subnet C
XYZ- office	Subnet D
XYZ- office	Subnet E

The following additional settings will be in place

1. **Default routes in Azure will be used to route traffic**
2. **A peering connection will be established between the virtual networks XYZ-London and XYZ-office**
3. **The peering connection for XYZ-London will have remote gateways enabled**
4. **A private DNS zone will be created named XYZ local. the registration network will be set to the XYZ-client virtual network**

The company has the following additional requirements:

1. **A number of web apps will be deployed. The initial settings of the web apps will be the same.**
2. **The senior management needs to have the ability to view the costs for Azure resources from the prior week.**

A Development team wants to use a serverless compute service that could be used in conjunction with the web applications when they are migrated to Azure.

They decide to use the Azure CosmosDB service.

Would this fulfill the requirement?

- Correct
- ✅ Incorrect

Explanation:-This is a multi model database service and not a serverless compute service

---

Q3)

Your company uses Microsoft System Center Service Manager on its on-premises network. You plan to deploy several services to Azure. You need to recommend a solution to push Azure service health alerts to Service Manager.

What should you include in the recommendation?

- Azure Notification Hubs
- Azure Event Hubs
- ✅ IT Service Management Connector (ITSM)

Explanation:-Reference:https://docs. microsoft. com/en-us/azure/azure-monitor/platform/itsmc-overview

- Application Insights Connector

Q4)

You have an on-premises Hyper-V cluster. The cluster contains Hyper-V hosts that run Windows Server 2016 Datacenter. The hosts are licensed under a Microsoft Enterprise Agreement that has Software Assurance. The Hyper-V cluster hosts 30 virtual machines that run Windows Server 2012 R2. Each virtual machine runs a different workload. The workloads have predictable consumption patterns. You plan to replace the virtual machines with Azure virtual machines that run Windows Server 2016. The virtual machines will be sized according to the consumption pattern of each workload. You need to recommend a solution to minimize the compute costs of the Azure virtual machines.

Which two recommendations should you include in the solution? Each correct answer presents part of the solution.

- ✅ Purchase Azure Reserved Virtual Machine Instances for the Azure virtual machines
- Create a virtual machine scale set that uses autoscaling
- Configure a spending limit in the Azure account center
- Create a lab in Azure DevTest Labs and place the Azure virtual machines in the lab
- ✅ Activate Azure Hybrid Benefit for the Azure virtual machines

---

Q5)

You have an on-premises Active Directory forest and an Azure Active Directory (Azure AD) tenant. All Azure AD users are assigned a Premium P1 license. You deploy Azure AD Connect. Which two features are available in this environment that can reduce operational overhead for your company's help desk? Each correct answer presents a complete solution.

- Azure AD Privileged Identity Management policies
- access reviews
- ✅ self-service password reset

- Microsoft Cloud App Security Conditional Access App Control
- ✓ password writeback

Q6)

You are planning the implementation of an order processing web service that will contain microservices hosted in an Azure Service Fabric cluster. You need to recommend a solution to provide developers with the ability to proactively identify and fix performance issues. The developers must be able to simulate user connections to the order processing web service from the Internet, as well as simulate user transactions. The developers must be notified if the goals for the transaction response times are not met.

What should you include in the recommendation?

- container health
- Azure Network Watcher
- ✓ Application Insights
- Service Fabric Analytics

Q7)

You need to recommend a solution to generate a monthly report of all the new Azure Resource Manager resource deployments in your subscription.

What should you include in the recommendation?

- Azure Analysis Services
- ✓ Azure Activity Log

Explanation:-Through activity logs, you can determine:what operations were taken on the resources in your subscriptionwho started the operationwhen the operation occurredthe status of the operationthe values of other properties that might help you research the operationReference:https://docs. microsoft. com/en-us/azure/azure-resource-manager/resource-group-audit

- Azure Monitor action groups
- Azure Advisor

Q8)

You plan to deploy 200 Microsoft SQL Server databases to Azure by using Azure SQL Database and Azure SQL Database Managed Instance. You need to recommend a monitoring solution that provides a consistent monitoring approach for all deployments. The solution must meet the following requirements: Support current-state analysis based on metrics collected near real-time, multiple times per minute, and maintained for up to one-hour support longer-term analysis based on metrics collected multiple times per hour and maintained for up to two weeks. Support monitoring of the number of concurrent logins and concurrent sessions.

What should you include in the recommendation?

- dynamic management views
- trace flags
- ✓ Azure Monitor
- SQL Server Profiler

Q9)

WebDev01 is used only for testing purposes. You need to reduce the costs to host WebDev01.

What should you modify?

NOTE: To answer this question, sign in to the Azure portal and explore the Azure resource groups.

- the disk type of WebDev01
- the networking properties of WebDev01
- ✓ the storage type of the storage account

Explanation:-The storage type can be changed to Block blobs to save money. References:https://azure. microsoft. com/en-us/pricing/details/storage/

- the properties of the storage account

Q10)

A user named Steve-11234827@ExamUsers. com cannot modify the properties of the web app. You need to ensure that Steve-11234827@ExamUsers. com can modify web app properties.

What should you do? NOTE: To answer this question, sign in to the Azure portal and explore the Azure resource groups.

- Remove the resource lock from the resource group
- ✓ Remove the resource lock from the web app

Explanation:-As an administrator, you may need to lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting ormodifying critical resources. Note: resource - A manageable item that is available through Azure. Virtual machines, storage accounts, web apps, databases, and virtual networks are examplesof resources. References:https://docs. microsoft. com/sv-se/azure/azure-resource-manager/management/lock-resourceshttps://docs. microsoft. com/en-us/azure/azure-resource-manager/management/overview

- Modify the permissions on the web app
- Modify the permissions on the resource group

Q11)

You are designing an Azure web app. You need to ensure that users who have impaired vision can use the app.

Which reference material should you use when designing the app?

- Accessibility in Windows Dev Center
- Azure Application Architecture Guide
- ✅ Web Content Accessibility Guidelines

Explanation:- How Microsoft integrates accessibilityMicrosoft's obligation to accessibility is guided by three main principles: transparency, inclusivity and accountability. In developing our products and services, wetake into account leading global accessibility standards, including:EN 301 549U. S. Section 508Web Content Accessibility Guidelines (WCAG)References:https://www. microsoft. com/en-us/trust-center/compliance/accessibilityDesign for Identity and Security

- Cloud Application Architecture Guide

Q12)

You have an Azure subscription that contains a resource group named RG1. You create an Azure Active Directory (Azure AD) group named ResearchUsers that contains the user accounts of all researchers. You need to recommend a solution that meets the following requirements: The researchers must be allowed to create Azure virtual machines. The researchers must only be able to create Azure virtual machines by using specific Azure Resource Manager templates. Solution: On RG1, assign the Contributor role to the ResearchUsers group. Create a custom Azure Policy definition and assign the policy to RG1.

Does this meet the goal?

- ✅ Correct
- Incorrect

Q13)

A company named Contoso Ltd., has a single-domain Active Directory forest named contoso.com. Contoso is preparing to migrate all workloads to Azure. Contoso wants users to use single sign-on (SSO) when they access cloud-based services that integrate withAzure Active Directory (Azure AD). You need to identify any objects in Active Directory that will fail to synchronize to Azure AD due to formatting issues.

The solution must minimize costs.

What should you include in the solution?

- Azure Advisor
- ✅ Microsoft Office 365 IdFix
- Azure AD Connect Health
- Password Export Server version 3. 1 (PES v3. 1) in Active Directory Migration Tool (ADMT)

Q14)

You have an Azure subscription. You need to recommend a solution to provide developers with the ability to provision Azure virtual machines. The solution must meet the following requirements: Only allow the creation of virtual machines in specific regions. Only allow the creation of specific sizes of virtual machines.

What should include in the recommendation?

- conditional access policies
- ✅ Azure Policy
- Azure Resource Manager templates
- role-based access control (RBAC)

Q15)

Your network contains an on-premises Active Directory forest. You discover that when users change jobs within your company, the membership of the user groups are not being updated. As a result, users can access resources that are no longer relevant to their job. You plan to integrate Active Directory and Azure Active Directory (Azure AD) by using Azure AD Connect. You need to recommend a solution to ensure that group owners are emailed monthly about the group memberships they manage.

What should you include in the recommendation?

- ✅ Azure AD access reviews

Explanation:-Reference:https://docs. microsoft. com/en-us/azure/active-directory/governance/access-reviews-overview

- Tenant Restrictions
- Azure AD Identity Protection
- conditional access policies

Q16)

A company named Contoso, Ltd. has an Azure Active Directory (Azure AD) tenant that is integrated with Microsoft Office 365 and an Azure subscription. Contoso has an on-premises identity infrastructure. The infrastructure includes servers that run Active Directory Domain Services (AD DS), Active DirectoryFederation Services (AD FS), Azure AD Connect, and Microsoft Identity Manager (MIM). Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Active Directory forest and an Office 365 tenant.

Fabrikam has the same on-premises identity infrastructure as Contoso. A team of 10 developers from Fabrikam will work on an Azure solution that will be hosted in the Azure subscription of Contoso. The developers must be added to the Contributor role for a resource in the Contoso subscription. You need to recommend a solution to ensure that Contoso can assign the role to the 10 Fabrikam developers.

The solution must ensure that the Fabrikamdevelopers use their existing credentials to access resources.

What would you recommend?

- Configure an AD FS claims provider trust between the AD FS infrastructures of Fabrikam and Contoso.
- ✅ In the Azure AD tenant of Contoso, enable Azure Active Directory Domain Services (Azure AD DS). Create a one-way forest trust that uses selectiveauthentication between the Active Directory forests of Contoso and Fabrikam.

Explanation:-Trust configurations - Configure trust from managed forests(s) or domain(s) to the administrative forest* A one-way trust is required from production environment to the admin forest. * Selective authentication should be used to restrict accounts in the admin forest to only logging on to the appropriate production hosts. Reference: https://docs. microsoft. com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material

- In the Azure AD tenant of Contoso, create guest accounts for the Fabrikam developers.
- In the Azure AD tenant of Contoso, create cloud-only user accounts for the Fabrikam developers.

Q17)

You have a hybrid deployment of Azure Active Directory (Azure AD). You need to recommend a solution to ensure that the Azure AD tenant can be managed only from the computers on your on-premises network.

What should you include in the recommendation?

- Azure AD roles and administrators
- ✅ a conditional access policy
- Azure AD Application Proxy
- Azure AD Privileged Identity Management

Q18)

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains two administrative user accounts named Admin1 and Admin2. You create two Azure virtual machines named VM1 and VM2. You need to ensure that Admin1 and Admin2 are notified when more than five events are added to the security log of VM1 or VM2 during a period of 120 seconds.

The solution must minimize administrative tasks.

What should you create?

- two action groups and one alert rule
- ✅ one action group and one alert rule
- five action groups and one alert rule
- two action groups and two alert rules

Q19)

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains several administrative user accounts. You need to recommend a solution to identify which administrative user accounts have NOT signed in during the previous 30 days.

Which service should you include in the recommendation?

- Azure AD Identity Protection
- Azure Activity Log
- Azure Advisor
- ✅ Azure AD Privileged Identity Management (PIM)

Q20)

You manage a single-domain, on-premises Active Directory forest named contoso.com. The forest functional level is Windows Server 2016. You have several on-premises applications that depend on Active Directory. You plan to migrate the applications to Azure. You need to recommend an identity solution for the applications. The solution must meet the following requirements: Eliminate the need for hybrid network connectivity. Minimize management overhead for Active Directory.

What should you recommend?

- In Azure, deploy an additional child domain to the contoso. com forest.
- ✅ In Azure, deploy additional domain controllers for the contoso. com domain.
- Implement a new Active Directory forest in Azure.
- Implement Azure Active Directory Domain Services (Azure AD DS).

Q21)

You have an Azure subscription named Project1. Only a group named Project1admins is assigned roles in the Project1 subscription. The Project1 subscription contains all the resources for an application named Application1. Your company is developing a new application named Application2. The members of the Application2 development team belong to an Azure Active Directory (AzureAD) group named App2Dev. You identify the following requirements for Application2: The members of App2Dev must be prevented from changing the role assignments in Azure. The members of App2Dev must be able to create new Azure resources required by Application2. All the required role assignments for Application2 will be performed by the members of Project1admins. You need to recommend a solution for the role assignments of Application2.

Solution: In Project1, create a network security group (NSG) named NSG1. Assign Project1admins the Owner role for NSG1. Assign the App2Dev the Contributor role for NSG1.

Does this meet the goal?

Correct
Incorrect
Explanation:-You should use a separate subscription for Project2.

Q22)

You have an Azure subscription that contains a resource group named RG1. You create an Azure Active Directory (Azure AD) group named ResearchUsers that contains the user accounts of all researchers. You need to recommend a solution that meets the following requirements:The researchers must be allowed to create Azure virtual machines. The researchers must only be able to create Azure virtual machines by using specific Azure Resource Manager templates.

Solution: On RG1, assign a custom role-based access control (RBAC) role to the ResearchUsers group.

Does this meet the goal?

Correct
Incorrect
Explanation:-Instead: On RG1, assign the Contributor role to the ResearchUsers group. Create a custom Azure Policy definition and assign the policy to RG1.

Q23)

A company deploys Azure Active Directory (Azure AD) Connect to synchronize identity information from their on-premises Active Directory Domain Services (ADDS) directory to their Azure AD tenant. The identity information that is synchronized includes user accounts, credential hashes for authentication (password sync), and group membership. The company plans to deploy several Windows and Linux virtual machines (VMs) to support their applications. The VMs have the following requirements: Support domain join, LDAP read, LDAP bind, NTLM and Kerberos authentication, and Group Policy. Allow users to sign in to the domain using their corporate credentials and connect remotely to the VM by using Remote Desktop. You need to support the VM deployment.

Which service should you use?

Azure AD Domain Services
Explanation:-Azure AD Domain Services provides managed domain services such as domain join, group policy, LDAP, Kerberos/NTLM authentication that are fully compatiblewith Windows Server Active Directory. Reference:https://docs. microsoft. com/en-us/azure/active-directory-domain-services/active-directory-ds-overview
Azure AD Privileged Identity Management
Azure AD Managed Service Identity
Active Directory Federation Services (AD FS)

Q24)

Your company has deployed several virtual machines (VMs) on-premises and to Azure. Azure ExpressRoute has been deployed and configured for on-premises toAzure connectivity. Several VMs are exhibiting network connectivity issues. You need to analyze the network traffic to determine whether packets are being allowed or denied to the VMs.

Solution: Use the Azure traffic analytics solution in Azure Log Analytics to analyze the network traffic.

Does the solution meet the goal?

Correct
Incorrect
Explanation:-Instead use Azure Network Watcher to run IP flow verify to analyze the network traffic. Reference:https://docs. microsoft. com/en-us/azure/network-watcher/network-watcher-monitoring-overviewhttps://docs. microsoft. com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview

---

Q25)

Your company has deployed several virtual machines (VMs) on-premises and to Azure. Azure ExpressRoute has been deployed and configured for on-premises toAzure connectivity. Several VMs are exhibiting network connectivity issues. You need to analyze the network traffic to determine whether packets are being allowed or denied to the VMs.

Solution: Use Azure Network Watcher to run IP flow verify to analyze the network traffic.

Does the solution meet the goal?

Correct
Explanation:-The Network Watcher Network performance monitor is a cloud-based hybrid network monitoring solution that helps you monitor network performance betweenvarious points in your network infrastructure. It also helps you monitor network connectivity to service and application endpoints and monitor the performance ofAzure ExpressRoute. Note:IP flow verify checks if a packet is allowed or denied to or from a virtual machine. The information consists of direction, protocol, local IP, remote IP, local port, andremote port. If the packet is denied by a security group, the name of the rule that denied the packet is returned. While any source or destination IP can be chosen, IP flow verify helps administrators quickly diagnose connectivity issues from or to the internet and from or to the on-premises environment. IP flow verify looks at the rules for all Network Security Groups (NSGs) applied to the network interface, such as a subnet or virtual machine NIC. Traffic flow is then verified based on the configured settings to or from that network interface. IP flow verify is useful in confirming if a rule in a Network Security Group is blockingingress or egress traffic to or from a virtual machine. Reference:https://docs. microsoft. com/en-us/azure/network-watcher/network-watcher-monitoring-overviewhttps://docs. microsoft. com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview
Incorrect

Q26)

Your company has deployed several virtual machines (VMs) on-premises and to Azure. Azure ExpressRoute has been

deployed and configured for on-premises toAzure connectivity. Several VMs are exhibiting network connectivity issues. You need to analyze the network traffic to determine whether packets are being allowed or denied to the VMs.

Solution: Install and configure the Log Analytics and Dependency Agents on all VMs. Use the Wire Data solution in Azure Log Analytics to analyze the network traffic.

Does the solution meet the goal?

- Correct
- ✅ Incorrect

Explanation:-Instead use Azure Network Watcher to run IP flow verify to analyze the network traffic. Reference:https://docs. microsoft. com/en-us/azure/network-watcher/network-watcher-monitoring-overviewhttps://docs. microsoft. com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview

---

Q27)

Your network contains an on-premises Active Directory forest named contoso.com. The forest is synced to an Azure Active Directory (Azure AD) tenant namedcontoso.com and an Azure AD Domain Services (Azure AD DS) domain named contoso-aad. com. You have an Azure Storage account named Storage1 that contains a file share named Share1. You configure NTFS permissions on Share1. You plan to deploy a virtual machine that will be used by several users to access Share1. You need to ensure that the users can access Share1.

Which type virtual machine should you deploy?

- a virtual machine that runs Windows Server 2016 and is joined to the contoso. com domain
- a virtual machine that runs Windows 10 and is joined to the contoso-add. com domain
- a virtual machine that runs Windows 10 and is hybrid Azure AD joined to the contoso. com domain
- ✅ an Azure virtual machine that runs Windows Server 2016 and is joined to the contoso-adcom domain

Explanation:-You join the Windows Server virtual machine to the Azure AD DS-managed domain, here named contoso-aad. com. Note: Azure Files supports identity-based authentication over SMB (Server Message Block) (preview) through Azure Active Directory (Azure AD) Domain Services. Your domain-joined Windows virtual machines (VMs) can access Azure file shares using Azure AD credentials. Incorrect Answers:B, C: Azure AD authentication over SMB is not supported for Linux VMs for the preview release. Only Windows Server VMs are supported. Reference:https://docs. microsoft. com/en-us/azure/storage/files/storage-files-active-directory-enable#mount-a-file-share-from-a-domain-joined-vm

---

Q28)

Your company has an on-premises data center and an Azure subscription. The on-premises data center contains a Hardware Security Module (HSM). Your network contains an Active Directory domain that is synchronized to an Azure Active Directory (Azure AD) tenant. The company is developing an application named Application1. Application1 will be hosted in Azure by using 10 virtual machines that run Windows Server 2016. Five virtual machines will be in the West Europe Azure region and five virtual machines will be in the East US Azure region. The virtual machines will store sensitive company information. All the virtual machines will use managed disks. You need to recommend a solution to encrypt the virtual machine disks by using BitLocker Drive Encryption (BitLocker).

Solution: Deploy one Azure Key Vault to each region. Create two Azure AD service principals. Configure the virtual machines to use Azure Disk Encryption and specify a different service principal for the virtual machines in each region.

Does this meet the goal?

- Correct
- ✅ Incorrect

Explanation:-You would also have to import Import the security keys from the HSM into each Azure key vault. Reference:https://docs. microsoft. com/en-us/azure/security/azure-security-disk-encryption-prerequisites-aad

---

Q29)

Your company has an on-premises data center and an Azure subscription. The on-premises data center contains a Hardware Security Module (HSM). Your network contains an Active Directory domain that is synchronized to an Azure Active Directory (Azure AD) tenant. The company is developing an application named Application1. Application1 will be hosted in Azure by using 10 virtual machines that run Windows Server 2016. Five virtual machines will be in the West Europe Azure region and five virtual machines will be in the East US Azure region. The virtual machines will store sensitive company information. All the virtual machines will use managed disks. You need to recommend a solution to encrypt the virtual machine disks by using BitLocker Drive Encryption (BitLocker).

Solution: Export a security key from the on-premises HSM. Create one Azure AD service principal. Configure the virtual machines to use Azure Storage ServiceEncryption.

Does this meet the goal?

- Correct
- ✅ Incorrect

Explanation:-We use the Azure Premium Key Vault with Hardware Security Modules (HSM) backed keys. The Key Vault has to be in the same region as the VM that will be encrypted. Reference:https://www. ciraltos. com/azure-disk-encryption-v2/

Q30)

Your company has an on-premises data center and an Azure subscription. The on-premises data center contains a Hardware Security Module (HSM). Your network contains an Active Directory domain that is synchronized to an Azure Active Directory (Azure AD) tenant. The company is developing an application named Application1. Application1 will be hosted in Azure by using 10 virtual machines that run Windows Server 2016. Five virtual machines will be in the West Europe Azure region and five virtual machines will be in the East US Azure region. The virtual machines will store sensitive company information. All the virtual machines will use managed disks. You need to recommend a solution to encrypt the virtual machine disks by using BitLocker Drive Encryption (BitLocker).

Solution: Deploy one Azure key vault to each regionExport two security keys from the on-premises HSMImport the security

keys from the HSM into each Azure key vaultCreate two Azure AD service principalsConfigure the virtual machines to use Azure Disk EncryptionSpecify a different service principal for the virtual machines in each region.

Does this meet the goal?

✅ Correct

Explanation:-We use the Azure Premium Key Vault with Hardware Security Modules (HSM) backed keys. The Key Vault has to be in the same region as the VM that will be encrypted. Note: If you want to use a key encryption key (KEK) for an additional layer of security for encryption keys, add a KEK to your key vault. Use the Add-AzKeyVaultKeycmdlet to create a key encryption key in the key vault. You can also import a KEK from your on-premises key management HSM. Reference:https://www. ciraltos. com/azure-disk-encryption-v2/https://docs. microsoft. com/en-us/azure/security/azure-security-disk-encryption-prerequisites-aad

⚪ Incorrect

Q31)

Your company has deployed several virtual machines (VMs) on-premises and to Azure. Azure ExpressRoute has been deployed and configured for on-premises toAzure connectivity. Several VMs are exhibiting network connectivity issues. You need to analyze the network traffic to determine whether packets are being allowed or denied to the VMs. Solution: Use Azure Advisor to analyze the network traffic.

Does the solution meet the goal?

⚪ Correct

✅ Incorrect

Explanation:-Instead use Azure Network Watcher to run IP flow verify to analyze the network traffic. Note: Advisor is a personalized cloud consultant that helps you follow best practices to optimize your Azure deployments. It analyzes your resource configurationand usage telemetry and then recommends solutions that can help you improve the cost effectiveness, performance, high availability, and security of your Azureresources. With Advisor, you can:Get proactive, actionable, and personalized best practices recommendations. Improve the performance, security, and high availability of your resources, as you identify opportunities to reduce your overall Azure spend. Get recommendations with proposed actions inline. Reference:https://docs. microsoft. com/en-us/azure/advisor/advisor-overview

---

Q32)

Your network contains an Active Directory domain named contoso.com that is federated to an Azure Active Directory (Azure AD) tenant. The on-premises domain contains a VPN server named Server1 that runs Windows Server 2016. You have a single on-premises location that uses an address space of 172. 16. 0. 0/16. You need to implement two-factor authentication for users who establish VPN connections to Server1.

What should you include in the implementation?

⚪ In Azure AD, create a conditional access policy and a trusted named location

✅ Install and configure Azure MFA Server on-premises

Explanation:-You need to download, install and configure the MFA Server. Reference:https://docs. microsoft. com/en-us/azure/active-directory/authentication/howto-mfaserver-deploy

⚪ Configure an Active Directory Federation Services (AD FS) server on-premises

⚪ In Azure AD, configure the authentication methods. From the multi-factor authentication (MFA) service settings, create a trusted IP range

---

Q33)

The billing administrator at your company reports that a web app incurs high monthly costs in Azure. You discover that the web app is rarely used. You need to reduce the Azure hosting costs for the web app. What should you do?

NOTE: To answer this question, sign in to the Azure portal and explore the Azure resource groups.

⚪ Create a restriction policy

✅ Create a WebJob that runs daily

Explanation:-WebJobs is a feature of Azure App Service that enables you to run a program or script in the same context as a web app, API app, or mobile app. There is noadditional cost to use WebJobs. Incorrect Answers:A: A restriction policy would not address the costC, D: Both scaling out and scaling up would increase the cost. References:https://docs. microsoft. com/en-us/azure/app-service/webjobs-createDesign an Infrastructure Strategy

⚪ Modify the Scale out settings

⚪ Modify the Scale up settings

Q34)

You need to recommend a solution for the collection of security logs for the middle tier of the payment processing system.

What should you include in the recommendation?

⚪ Azure Event Hubs

⚪ AzureIncorrecttification Hubs

✅ the Azure Diagnostics agent

Explanation:-Scenario: Collect Windows security logs from all the middle-tier servers and retain the logs for a period of seven years. The Azure Diagnostics agent should be used when you want to archive logs and metrics to Azure storage. Reference:https://docs. microsoft. com/en-us/azure/azure-monitor/platform/agents-overview Determine Workload Requirements

⚪ the Microsoft Monitoring agent

Q35)

You need to recommend a solution for implementing the back-end tier of the payment processing system in Azure.

What should you include in the recommendation?

- an Azure SQL Database managed instance
- a SQL Server database on an Azure virtual machine
- ✓ an Azure SQL Database single database
- an Azure SQL Database elastic pool

Q36)

You need to recommend a solution for protecting the content of the payment processing system.

What should you include in the recommendation?

- Transparent Data Encryption (TDE)
- Azure Storage Service Encryption
- Always Encrypted with randomized encryption
- ✓ Always Encrypted with deterministic encryption

Q37)

Your company has an on-premises Active Directory Domain Services (AD DS) domain and an established Azure Active Directory (Azure AD) environment. Your company would like users to be automatically signed in to cloud apps when they are on their corporate desktops that are connected to the corporate network. You need to enable single sign-on (SSO) for company users.

Solution: Install and configure an Azure AD Connect server to use password hash synchronization and select the Enable single sign-on option.

Does the solution meet the goal?

- ✓ Correct
- Incorrect

Q38) You have an Azure subscription that contains a custom application named Application1. Application1 was developed by an external company named Fabrikam, Ltd. Developers at Fabrikam were assigned role-based access control (RBAC) permissions to the Application1 components. All users are licensed for the Microsoft 365E5 plan. You need to recommend a solution to verify whether the Fabrikam developers still require permissions to Application1. The solution must meet the following requirements: To the manager of the developers, send a monthly email message that lists the access permissions to Application1. If the manager does not verify access permission, automatically revoke that permission. Minimize development effort. What should you recommend?

- In Azure Active Directory (AD) Privileged Identity Management, create a custom role assignment for the Application1 resources
- Create an Azure Automation runbook that runs the Get-AzureADUserAppRoleAssignment cmdlet
- Create an Azure Automation runbook that runs the Get-AzureRmRoleAssignment cmdlet
- ✓ In Azure Active Directory (Azure AD), create an access review of Application1

Q39)

Your company has an on-premises Active Directory Domain Services (AD DS) domain and an established Azure Active Directory (Azure AD) environment. Your company would like users to be automatically signed in to cloud apps when they are on their corporate desktops that are connected to the corporate network. You need to enable single sign-on (SSO) for company users.

Solution: Install and configure an Azure AD Connect server to use pass-through authentication and select the Enable single sign-on option.

Does the solution meet the goal?

- ✓ Correct
- Incorrect

Q40)

Your company has an on-premises Active Directory Domain Services (AD DS) domain and an established Azure Active Directory (Azure AD) environment. Your company would like users to be automatically signed in to cloud apps when they are on their corporate desktops that are connected to the corporate network. You need to enable single sign-on (SSO) for company users.

Solution: Configure an AD DS server in an Azure virtual machine (VM). Configure bidirectional replication.

Does the solution meet the goal?

- Correct
- ✓ Incorrect

Q41)

You are designing a security solution for a company's Azure Active Directory (Azure AD). The company currently uses Azure AD Premium for all employees. Contractors will periodically access the corporate network based on demand. You must ensure that all employees and contractors are required to log on by using two-factor authentication.

The solution must minimize costs. You need to recommend a solution.

What should you recommend?

- Purchase Azure Multi-Factor Authentication licenses for the employees and the contractors
- Use the Multi-Factor Authentication provider in Azure and configure the usage model for each authentication type
- ✓ Use the Multi-Factor Authentication provider in Azure and configure the usage model for each enabled user
- Purchase Azure Multi-Factor Authentication licenses for the contractors only

---

Q42)

You have an Azure Active Directory (Azure AZD) tenant named contoso.com. The tenant contains a group named Group1. Group1 contains all the administrative user accounts. You discover several login attempts to the Azure portal from countries where administrative users do NOT work. You need to ensure that all login attempts to the Azure portal from those countries require Azure Multi-Factor Authentication (MFA).

Solution: Create an Access Review for Group1.

Does this solution meet the goal?

- Correct
- ✓ Incorrect

Q43)

You have an Azure Active Directory (Azure AZD) tenant named contoso.com. The tenant contains a group named Group1. Group1 contains all the administrative user accounts. You discover several login attempts to the Azure portal from countries where administrative users do NOT work. You need to ensure that all login attempts to the Azure portal from those countries require Azure Multi-Factor Authentication (MFA). Solution: You implement an access package.

Does this solution meet the goal?

- Correct
- ✓ Incorrect

Q44)

You have an Azure Active Directory (Azure AZD) tenant named contoso.com. The tenant contains a group named Group1. Group1 contains all the administrative user accounts. You discover several login attempts to the Azure portal from countries where administrative users do NOT work. You need to ensure that all login attempts to the Azure portal from those countries require Azure Multi-Factor Authentication (MFA). Solution: Implement Azure AD Privileged Identity Management.

Does this solution meet the goal?

- ✓ Correct
- Incorrect

Q45)

Your company has several Azure subscriptions that are part of a Microsoft Enterprise Agreement. The company's compliance team creates automatic alerts by using Azure Monitor. You need to recommend a solution to apply the alerts automatically when new subscriptions are added to the Enterprise Agreement.

What should you include in the recommendation?

- Azure Automation runbooks
- Azure Log Analytics alerts
- Azure Monitor action groups
- Azure Resource Manager templates
- ✓ Azure Policy

Q46)

You store web access logs data in Azure Blob storage. You plan to generate monthly reports from the access logs. You need to recommend an automated process to upload the data to Azure SQL Database every month.

What should you include in the recommendation?

- Microsoft SQL Server Migration Assistant (SSMA)
- ✓ Azure Data Factory
- Data Migration Assistant
- AzCopy

Q47)

Your company has the offices shown in the following table. The network contains an Active Directory domain named contoso.com that is synced to Azure Active Directory (Azure AD). All users connect to an application hosted in Microsoft 365. You need to recommend a solution to ensure that all the users use Azure Multi-Factor Authentication (MFA) to connect to the application from one of the offices.

What should you include in the recommendation?

- a named location and two Microsoft Cloud App Security policies

- a conditional access policy and two virtual networks
- a virtual network and two Microsoft Cloud App Security policies
- ✅ a conditional access policy and two named locations

Q48)

Your company has an on-premises Active Directory Domain Services (AD DS) domain and an established Azure Active Directory (Azure AD) environment. Your company would like users to be automatically signed in to cloud apps when they are on their corporate desktops that are connected to the corporate network. You need to enable single sign-on (SSO) for company users.

Solution: Install and configure an on-premises Active Directory Federation Services (AD FS) server with a trust established between the AD FS server and AzureAD.

Does the solution meet the goal?

- Correct
- ✅ Incorrect

Explanation:-Seamless SSO is not applicable to Active Directory Federation Services (ADFS). Instead install and configure an Azure AD Connect server. Reference:https://docs. microsoft. com/en-us/azure/active-directory/hybrid/how-to-connect-sso

---

Q49)

You have an Azure subscription that contains several resource groups, including a resource group named RG1. RG1 contains several business-critical resources. A user named admin1 is assigned the Owner role to the subscription. You need to prevent admin1 from modifying the resources in RG1.

The solution must ensure that admin1 can manage the resources in the other resource groups.

What should you use?

- a management group
- an Azure policy
- ✅ a custom role

Explanation:-Role-based access control (RBAC) focuses on user actions at different scopes. You might be added to the contributor role for a resource group, allowing you tomake changes to that resource group. Incorrect Answers:A: If your organization has many subscriptions, you may need a way to efficiently manage access, policies, and compliance for those subscriptions. Azuremanagement groups provide a level of scope above subscriptions. B: There are a few key differences between Azure Policy and role-based access control (RBAC). Azure Policy focuses on resource properties during deploymentand for already existing resources. Azure Policy controls properties such as the types or locations of resources. Unlike RBAC, Azure Policy is a default allow andexplicit deny system. D: Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheresto an organization's standards, patterns, and requirements. Reference:https://docs. microsoft. com/en-us/azure/role-based-access-control/overview

- an Azure blueprint

Q50)

A company has deployed several applications across Windows and Linux Virtual machines in Azure. Log Analytics is being used to send the required data for alerting purposes for Virtual Machines. You need to recommend which tables need to be queried for security-related queries.

Which of the following would you query for events from Windows Event Logs?

- Azure Activity
- Azure Diagnostics
- ✅ Event

Explanation:-This is also given in the Microsoft documentation, wherein you would use the Event Table for the queries on events from Windows Virtual machinesSince this is clearly mentioned, all other options are incorrectFor more information on collecting event data from windows virtual machines, please go ahead and visit the below URL. Reference:https://docs. microsoft. com/en-us/azure/azure-monitor/platform/data-sources-windows-events

- Syslog

Q51)

You have an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains a group named Group1. Group1 contains all the administrative user accounts. You discover several login attempts to the Azure portal from countries where administrative users do NOT work. You need to ensure that all login attempts to the Azure portal from those countries require Azure Multi-Factor Authentication (MFA).

Solution: Implement Azure AD Identity Protection for Group1.

Does this solution meet the goal?

- Correct
- ✅ Incorrect

Explanation:-Instead implement Azure AD Privileged Identity Management. Note: Azure Active Directory (Azure AD) Privileged Identity Management (PIM) is a service that enables you to manage, control, and monitor access to importantresources in your organization. Reference:https://docs. microsoft. com/en-us/azure/active-directory/privileged-identity-management/pim-configure

---

Q52)

You are designing a solution that will host 20 different web applications. You need to recommend a solution to secure the web applications with a firewall that protects against common web-based attacks including SQL injection, cross-site scripting attacks, and session hijacks.

The solution must minimize costs.

Which three Azure features should you recommend?

Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- VPN Gateway
- URL-based content routing
- Multi-site routing
- ✅ Web Application Firewall (WAF)

Explanation:-The web application firewall (WAF) in Azure Application Gateway helps protect web applications from common web-based attacks like SQL injection, cross-sitescripting attacks, and session hijacks. It comes preconfigured with protection from threats identified by the Open Web Application Security Project (OWASP) as thetop 10 common vulnerabilities. ExpressRoute connections do not go over the public Internet and thus can be considered more secure than VPN-based solutions. This allows ExpressRouteconnections to offer more reliability, faster speeds, lower latencies, and higher security than typical connections over the Internet. Reference:https://azure. microsoft. com/en-us/updates/application-gateway-web-application-firewall-in-public-preview/https://docs. microsoft. com/en-us/azure/security/fundamentals/overview

- ✅ Azure ExpressRoute

Explanation:-The web application firewall (WAF) in Azure Application Gateway helps protect web applications from common web-based attacks like SQL injection, cross-sitescripting attacks, and session hijacks. It comes preconfigured with protection from threats identified by the Open Web Application Security Project (OWASP) as thetop 10 common vulnerabilities. ExpressRoute connections do not go over the public Internet and thus can be considered more secure than VPN-based solutions. This allows ExpressRouteconnections to offer more reliability, faster speeds, lower latencies, and higher security than typical connections over the Internet. Reference:https://azure. microsoft. com/en-us/updates/application-gateway-web-application-firewall-in-public-preview/https://docs. microsoft. com/en-us/azure/security/fundamentals/overview

- ✅ Azure Application Gateway

Explanation:-The web application firewall (WAF) in Azure Application Gateway helps protect web applications from common web-based attacks like SQL injection, cross-sitescripting attacks, and session hijacks. It comes preconfigured with protection from threats identified by the Open Web Application Security Project (OWASP) as thetop 10 common vulnerabilities. ExpressRoute connections do not go over the public Internet and thus can be considered more secure than VPN-based solutions. This allows ExpressRouteconnections to offer more reliability, faster speeds, lower latencies, and higher security than typical connections over the Internet. Reference:https://azure. microsoft. com/en-us/updates/application-gateway-web-application-firewall-in-public-preview/https://docs. microsoft. com/en-us/azure/security/fundamentals/overview

---

Q53)

Your company has deployed several virtual machines (VMs) on-premises and to Azure. Azure ExpressRoute has been deployed and configured for on-premises toAzure connectivity. Several VMs are exhibiting network connectivity issues. You need to analyze the network traffic to determine whether packets are being allowed or denied to the VMs.

Solution: Install and configure the Microsoft Monitoring Agent and the Dependency Agent on all VMs. Use the Wire Data solution in Azure Monitor to analyze the network traffic.

Does the solution meet the goal?

- Correct
- ✅ Incorrect

Explanation:-Instead use Azure Network Watcher to run IP flow verify to analyze the network traffic. Note: Wire Data looks at network data at the application level, not down at the TCP transport layer. The solution doesn't look at individual ACKs and SYNs. Reference:https://docs. microsoft. com/en-us/azure/network-watcher/network-watcher-monitoring-overviewhttps://docs. microsoft. com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview

---

Q54)

A company has deployed several applications across Windows and Linux Virtual machines in Azure. Log Analytics is being used to send the required data for alerting purposes for Virtual Machines. You need to recommend which tables need to be queried for security-related queries.

Which of the following would you query for events from Linux system logging?

- Azure Activity
- Azure Diagnostics
- Event
- ✅ Syslog

Explanation:-This is also given in the Microsoft documentation, wherein you would use the Syslog Table for the queries on events from Linux Virtual machinesNote: Syslog is an event logging protocol that is common to Linux. Applications will send messages that may be stored on the local machine or delivered to aSyslog collector. When the Log Analytics agent for Linux is installed, it configures the local Syslog daemon to forward messages to the agent. The agent then sendsthe message to Azure Monitor where a corresponding record is created. Reference:https://docs. microsoft. com/en-us/azure/azure-monitor/platform/data-sources-syslog

---

Q55)

A company named Contoso, Ltd. has an Azure Active Directory (Azure AD) tenant that is integrated with Microsoft Office 365 and an Azure subscription. Contoso has an on-premises identity infrastructure. The infrastructure includes servers that run Active Directory Domain Services (AD DS), Active DirectoryFederation Services (AD FS), Azure AD Connect, and Microsoft Identity Manager (MIM). Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Active Directory forest and an Office 365 tenant. Fabrikam has the same on-premises identity infrastructure as Contoso. A team of 10 developers from Fabrikam will work on an Azure solution that will be hosted in the Azure subscription of Contoso. The developers must be added to the Contributor role for a resource in the Contoso subscription. You need to recommend a solution to ensure that Contoso can assign the role to the 10 Fabrikam developers.

The solution must ensure that the Fabrikamdevelopers use their existing credentials to access resources.

What should you recommend?

- Configure an AD FS relying party trust between the Fabrikam and Contoso AD FS infrastructures.
- Configure an organization relationship between the Office 365 tenants of Fabrikam and Contoso.
- In the Azure AD tenant of Contoso, create guest accounts for the Fabrikam developers.
- ✅ Configure a forest trust between the on-premises Active Directory forests of Contoso and Fabrikam.

Explanation:-Trust configurations - Configure trust from managed forests(s) or domain(s) to the administrative forestA one-way trust is required from production environment to the admin forest. Selective authentication should be used to restrict accounts in the admin forest to only logging on to the appropriate production hosts. References:https://docs. microsoft. com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material

---

Q56)

You have an Azure Active Directory (Azure AD) tenant named contoso.com that has a security group named Group1. Group1 is configured for assigned membership. Group1 has 50 members, including 20 guest users. You need to recommend a solution for evaluating the membership of Group1. The solution must meet the following requirements: The evaluation must be repeated automatically every three months. Every member must be able to report whether they need to be in Group1. Users who report that they do not need to be in Group1 must be removed from Group1 automatically users who do not report whether they need to be in Group1 must be removed from Group1 automatically.

What should you include in the recommendation?

- Implement Azure AD Identity Protection.
- ✅ Change the Membership type of Group1 to Dynamic User.

Explanation:-In Azure Active Directory (Azure AD), you can create complex attribute-based rules to enable dynamic memberships for groups. Dynamic group membershipreduces the administrative overhead of adding and removing users. When any attributes of a user or device change, the system evaluates all dynamic group rules in a directory to see if the change would trigger any group adds orremoves. If a user or device satisfies a rule on a group, they are added as a member of that group. If they no longer satisfy the rule, they are removed. References:https://docs. microsoft. com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership

- Create an access review.
- Implement Azure AD Privileged Identity Management.

Q57)

You have an Azure subscription named Project1. Only a group named Project1admins is assigned roles in the Project1 subscription. The Project1 subscription contains all the resources for an application named Application1. Your company is developing a new application named Application2. The members of the Application2 development team belong to an Azure Active Directory (AzureAD) group named App2Dev. You identify the following requirements for Application2: The members of App2Dev must be prevented from changing the role assignments in Azure. The members of App2Dev must be able to create new Azure resources required by Application2. All the required role assignments for Application2 will be performed by the members of Project1admins. You need to recommend a solution for the role assignments of Application2.

Solution: Create a new Azure subscription named Project2. Assign Project1admins the Owner role for the Project2 subscription. Assign App2Dev the Contributor role for the Project2 subscription.

Does this meet the goal?

- ✅ Correct
- Incorrect

Q58)

You have an Azure subscription named Project1. Only a group named Project1admins is assigned roles in the Project1 subscription. The Project1 subscription contains all the resources for an application named Application1. Your company is developing a new application named Application2. The members of the Application2 development team belong to an Azure Active Directory (AzureAD) group named App2Dev. You identify the following requirements for Application2: The members of App2Dev must be prevented from changing the role assignments in Azure. The members of App2Dev must be able to create new Azure resources required by Application2. All the required role assignments for Application2 will be performed by the members of Project1admins. You need to recommend a solution for the role assignments of Application2.

Solution: Create a new Azure subscription named Project2. Assign Project1admins the User Access Administrator role for the Project2 subscription. AssignApp2Dev the Owner role for the Project2 subscription.

Does this meet the goal?

- Correct
- ✅ Incorrect

Explanation:-Instead, assign Project1admins the Owner role for the Project2 subscription. Assign App2Dev the Contributor role for the Project2 subscription.

Q59)

You have an Azure subscription named Project1. Only a group named Project1admins is assigned roles in the Project1 subscription. The Project1 subscription contains all the resources for an application named Application1. Your company is developing a new application named Application2. The members of the Application2 development team belong to an Azure Active Directory (AzureAD) group named App2Dev. You identify the following requirements for Application2: The members of App2Dev must be prevented from changing the role assignments in Azure. The members of App2Dev must be able to create new Azure resources required by Application2. All the required role assignments for Application2 will be performed by the members of Project1admins. You need to recommend a solution for the role assignments of Application2.

Solution: In Project1, create a resource group named Application2RG. Assign Project1admins the Owner role for Application2RG. Assign App2Dev the Contributor role for Application2RG.

Does this meet the goal?

- Correct

Incorrect

Explanation:-You should use a separate subscription for Project2.

Q60)

You have an Azure subscription that contains a resource group named RG1. You create an Azure Active Directory (Azure AD) group named ResearchUsers that contains the user accounts of all researchers. You need to recommend a solution that meets the following requirements: The researchers must be allowed to create Azure virtual machines. The researchers must only be able to create Azure virtual machines by using specific Azure Resource Manager templates.

Solution: Create a lab in Azure DevTest Lab. Configure the DevTest Labs settings. Assign the DevTest Labs User role to the ResearchUsers group.

Does this meet the goal?

Correct

Incorrect

Explanation:-Instead: On RG1, assign the Contributor role to the ResearchUsers group. Create a custom Azure Policy definition and assign the policy to RG1.
