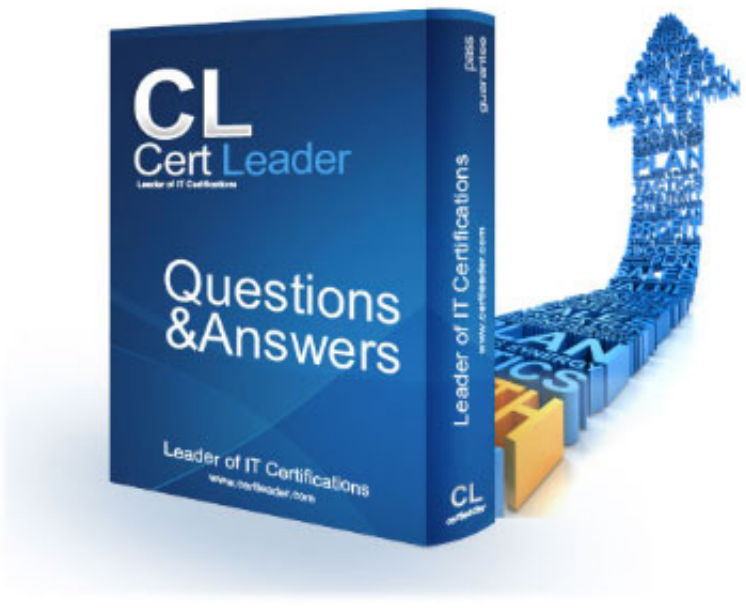
az-500 Dumps

Microsoft Azure Security Technologies

https://www.certleader.com/az-500-dumps.html



NEW QUESTION 1
You need to meet the identity and access requirements for Group1.
What should you do?

A. Add a membership rule to Group1.
B. Delete Group1. Create a new group named Group1 that has a membership type of Office 365. Add users and devices to the group.
C. Modify the membership rule of Group1.
D. Change the membership type of Group1 to Assigne
E. Create two groups that have dynamic membership
F. Add the new groups to Group1.

Answer: B

Explanation:
Incorrect Answers:
A, C: You can create a dynamic group for devices or for users, but you can't create a rule that contains both users and devices.
D: For assigned group you can only add individual members. Scenario:
Litware identifies the following identity and access requirements: All San Francisco users and their devices must be members of Group1. The tenant currently contain this group:

References:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-create-azure-portal
Testlet 2
This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question on this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next sections of the exam. After you begin a new section, you cannot return to this section.
To start the case study
To display the first question on this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.
Overview
Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York. The company hosts its entire server infrastructure in Azure.
Contoso has two Azure subscriptions named Sub1 and Sub2. Both subscriptions are associated to an Azure Active Directory (Azure AD) tenant named contoso.com.
Technical requirements
Contoso identifies the following technical requirements:
Deploy Azure Firewall to VNetWork1 in Sub2.
Register an application named App2 in contoso.com.
Whenever possible, use the principle of least privilege.
Enable Azure AD Privileged Identity Management (PIM) for contoso.com
Contoso.com contains the users shown in the following table.

Contoso.com contains the security groups shown in the following table.

Sub1
Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.

User2 creates the virtual networks shown in the following table.

Sub1 contains the locks shown in the following table.

Sub1 contains the Azure policies shown in the following table.

Sub2

Sub2 contains the virtual machines shown in the following table.

All virtual machines have the public IP addresses and the Web Server (IIS) role installed. The firewalls for each virtual machine allow ping requests and web requests.
Sub2 contains the network security groups (NSGs) shown in the following table.

NSG1 has the inbound security rules shown in the following table.

NSG2 has the inbound security rules shown in the following table.

NSG3 has the inbound security rules shown in the following table.

NSG4 has the inbound security rules shown in the following table.

NSG1, NSG2, NSG3, and NSG4 have the outbound security rules shown in the following table.

Contoso identifies the following technical requirements:
* Deploy Azure Firewall to VNetwork1 in Sub2.
* Register an application named App2 in contoso.com.
* Whenever possible, use the principle of least privilege.
* Enable Azure AD Privileged Identity Management (PIM) for contoso.com.m.

NEW QUESTION 2
You need to ensure that User2 can implement PIM.
What should you do first?

A. Assign User2 the Global administrator role.

B. Configure authentication methods for contoso.com.
C. Configure the identity secure score for contoso.com.
D. Enable multi-factor authentication (MFA) for User2.

Answer: A

Explanation:
To start using PIM in your directory, you must first enable PIM.
1. Sign in to the Azure portal as a Global Administrator of your directory.
You must be a Global Administrator with an organizational account (for example, @yourdomain.com), not a Microsoft account (for example, @outlook.com), to enable PIM for a directory.
Scenario: Technical requirements include: Enable Azure AD Privileged Identity Management (PIM) for contoso.com References:
https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-getting-started

NEW QUESTION 3
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure Subscription named Sub1.
You have an Azure Storage account named Sa1 in a resource group named RG1.
Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies. You discover that unauthorized users accessed both the file service and the blob service.
You need to revoke all access to Sa1. Solution: You generate new SASs. Does this meet the goal?

A. Yes
B. No

Answer: B

Explanation:
Instead you should create a new stored access policy.
To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately affects all of the shared access signatures associated with it.
References:
https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy

NEW QUESTION 4
Your network contains an on-premises Active Directory domain named corp.contoso.com.
You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com. You sync all on-premises identities to Azure AD.
You need to prevent users who have a givenName attribute that starts with TEST from being synced to Azure AD. The solution must minimize administrative effort.
What should you use?

A. Synchronization Rules Editor
B. Web Service Configuration Tool
C. the Azure AD Connect wizard
D. Active Directory Users and Computers

Answer: A

Explanation:
Use the Synchronization Rules Editor and write attribute-based filtering rule.
References:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration

NEW QUESTION 5
Your company plans to create separate subscriptions for each department. Each subscription will be associated to the same Azure Active Directory (Azure AD) tenant.
You need to configure each subscription to have the same role assignments. What should you use?

A. Azure Security Center
B. Azure Blueprints
C. Azure AD Privileged Identity Management (PIM)
D. Azure Policy

Answer: C

Explanation:
The Azure AD Privileged Identity Management (PIM) service also allows Privileged Role Administrators to make permanent admin role assignments.
References:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-add-role-to-user

NEW QUESTION 6
HOTSPOT
What is the membership of Group1 and Group2? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: User1, User2, User3, User4
Contains "ON" is true for Montreal (User1), MONTREAL (User2), London (User 3), and Ontario (User4) as string and regex operations are not case sensitive.
Box 2: Only User3
Match "*on" is only true for London (User3).
Scenario:
Contoso.com contains the users shown in the following table.

Contoso.com contains the security groups shown in the following table.

References:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership

NEW QUESTION 7
HOTSPOT
You are evaluating the security of the network communication between the virtual machines in Sub2. For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.
Hot Area:

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Yes
NSG1 has the inbound security rules shown in the following table.

NSG2 has the inbound security rules shown in the following table.

Box 2: Yes
Box 3: No Note:
Sub2 contains the virtual machines shown in the following table.

Sub2 contains the network security groups (NSGs) shown in the following table.

Question Set 3

NEW QUESTION 8
You have an Azure subscription named Sub1. Sub1 contains a virtual network named VNet1 that contains one subnet named Subnet1.
You create a service endpoint for Subnet1.
Subnet1 contains an Azure virtual machine named VM1 that runs Ubuntu Server 18.04.
You need to deploy Docker containers to VM1. The containers must be able to access Azure Storage resources and Azure SQL databases by using the service endpoint.

A. Create an application security group and a network security group (NSG).
B. Edit the docker-compose.yml file.
C. Install the container network interface (CNI) plug-in.

Answer: C

Explanation:
The Azure Virtual Network container network interface (CNI) plug-in installs in an Azure Virtual Machine. The plug-in supports both Linux and Windows platform. The plug-in assigns IP addresses from a virtual network to containers brought up in the virtual machine, attaching them to the virtual network, and connecting them directly to other containers and virtual network resources. The plug-in doesn’t rely on overlay networks, or routes, for connectivity, and provides the same performance as virtual machines.
The following picture shows how the plug-in provides Azure Virtual Network capabilities to Pods:

References:
https://docs.microsoft.com/en-us/azure/virtual-network/container-networking-overview

NEW QUESTION 9
You have Azure Resource Manager templates that you use to deploy Azure virtual machines.
You need to disable unused Windows features automatically as instances of the virtual machines are provisioned. What should you use?

A. device compliance policies in Microsoft Intune
B. Azure Automation State Configuration
C. application security groups
D. Azure Advisor

Answer: B

Explanation:
You can use Azure Automation State Configuration to manage Azure VMs (both Classic and Resource Manager), on-premises VMs, Linux machines, AWS VMs, and on-premises physical machines.
Note: Azure Automation State Configuration provides a DSC pull server similar to the Windows Feature DSC-Service so that target nodes automatically receive configurations, conform to the desired state, and report back on their compliance. The built-in pull server in Azure Automation eliminates the need to set up and maintain your own pull server. Azure Automation can target virtual or physical Windows or Linux machines, in the cloud or on-premises.
References:
https://docs.microsoft.com/en-us/azure/automation/automation-dsc-getting-started

NEW QUESTION 10
DRAG DROP
You have an Azure subscription that contains the virtual networks shown in the following table.

The Azure virtual machines on SpokeVNetSubnet0 can communicate with the computers on the on-premises network. You plan to deploy an Azure firewall to HubVNet.
You create the following two routing tables:
RT1: Includes a user-defined route that points to the private IP address of the Azure firewall as a next hop address RT2: Disables BGP route propagation and defines the private IP address of the Azure firewall as the default gateway
You need to ensure that traffic between SpokeVNetSubnet0 and the on-premises network flows through the Azure firewall.
To which subnet should you associate each route table? To answer, drag the appropriate subnets to the correct route tables. Each subnet may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.
Select and Place:

A. Mastered
B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 10
You are configuring an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry.
You need to use the auto-generated service principal to authenticate to the Azure Container Registry. What should you create?

A. an Azure Active Directory (Azure AD) group
B. an Azure Active Directory (Azure AD) role assignment
C. an Azure Active Directory (Azure AD) user
D. a secret in Azure Key Vault

Answer: B

Explanation:
When you create an AKS cluster, Azure also creates a service principal to support cluster operability with other Azure resources. You can use this auto-generated service principal for authentication with an ACR registry. To do so, you need to create an Azure AD role assignment that grants the cluster's service principal access to the container registry.
References:
https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-auth-aks

NEW QUESTION 11
HOTSPOT
You have Azure virtual machines that have Update Management enabled. The virtual machines are configured as shown in the following table.

You schedule two update deployments named Update1 and Update2. Update1 updates VM3. Update2 updates VM6.
Which additional virtual machines can be updated by using Update1 and Update2? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Update1: VM1 and VM2 only
VM3: Windows Server 2016 West US RG2
Update2: VM4 and VM5 only VM6: CentOS 7.5 East US RG1
For Linux, the machine must have access to an update repository. The update repository can be private or public. References:
https://docs.microsoft.com/en-us/azure/automation/automation-update-management

NEW QUESTION 13
HOTSPOT
You have an Azure subscription named Sub1.
You create a virtual network that contains one subnet. On the subnet, you provision the virtual machines shown in the following table.

Currently, you have not provisioned any network security groups (NSGs). You need to implement network security to meet the following requirements:
Allow traffic to VM4 from VM3 only.
Allow traffic from the Internet to VM1 and VM2 only. Minimize the number of NSGs and network security rules.
How many NSGs and network security rules should you create? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

A. Mastered
B. Not Mastered

Answer: A

Explanation:
NSGs: 2
Network security rules: 3
Not 2: You cannot specify multiple service tags or application groups) in a security rule.
References:
https://docs.microsoft.com/en-us/azure/virtual-network/security-overview

NEW QUESTION 15
HOTSPOT
You have an Azure key vault.
You need to delegate administrative access to the key vault to meet the following requirements:
Provide a user named User1 with the ability to set advanced access policies for the key vault. Provide a user named User2 with the ability to add and delete certificates in the key vault. Use the principle of least privilege.
What should you use to assign access to each user? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

A. Mastered
B. Not Mastered

Answer: A

Explanation:
User1: RBAC

RBAC is used as the Key Vault access control mechanism for the management plane. It would allow a user with the proper identity to: set Key Vault access policies
create, read, update, and delete key vaults set Key Vault tags
Note: Role-based access control (RBAC) is a system that provides fine-grained access management of Azure resources. Using RBAC, you can segregate duties within your team and grant only the amount of access to users that they need to perform their jobs.
User2: A key vault access policy
A key vault access policy is the access control mechanism to get access to the key vault data plane. Key Vault access policies grant permissions separately to keys, secrets, and certificates.
References:
https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault

NEW QUESTION 18
You have an Azure virtual machines shown in the following table.

You create an Azure Log Analytics workspace named Analytics1 in RG1 in the East US region. Which virtual machines can be enrolled in Analytics1?

A. VM1 only
B. VM1, VM2, and VM3 only
C. VM1, VM2, VM3, and VM4
D. VM1 and VM4 only

Answer: A

Explanation:
Note: Create a workspace
In the Azure portal, click All services. In the list of resources, type Log Analytics. As you begin typing, the list filters based on your input. Select Log Analytics. Click Create, and then select choices for the following items:
Provide a name for the new Log Analytics workspace, such as DefaultLAWorkspace. OMS workspaces are now referred to as Log Analytics workspaces. Select a Subscription to link to by selecting from the drop-down list if the default selected is not appropriate.
For Resource Group, select an existing resource group that contains one or more Azure virtual machines.
Select the Location your VMs are deployed to. For additional information, see which regions Log Analytics is available in. Incorrect Answers:
B, C: A Log Analytics workspace provides a geographic location for data storage. VM2 and VM3 are at a different location.
D: VM4 is a different resource group. References:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/manage-access

NEW QUESTION 23
You are testing an Azure Kubernetes Service (AKS) cluster. The cluster is configured as shown in the exhibit. (Click the Exhibit tab.)

You plan to deploy the cluster to production. You disable HTTP application routing.
You need to implement application routing that will provide reverse proxy and TLS termination for AKS services by using a single IP address. What should you do?

A. Create an AKS Ingress controller.
B. Install the container network interface (CNI) plug-in.
C. Create an Azure Standard Load Balancer.
D. Create an Azure Basic Load Balancer.

Answer: A

Explanation:
An ingress controller is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services.
References:
https://docs.microsoft.com/en-us/azure/aks/ingress-tls

NEW QUESTION 28
HOTSPOT
Which virtual networks in Sub1 can User2 modify and delete in their current state? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: VNET4 and VNET1 only
RG1 has only Delete lock, while there are no locks on RG4. RG2 and RG3 both have Read-only locks.
Box 2: VNET4 only
There are no locks on RG4, while the other resource groups have either Delete or Read-only locks.
Note: As an administrator, you may need to lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. You can set the lock level to CanNotDelete or ReadOnly. In the portal, the locks are called Delete and Read-only respectively.

CanNotDelete means authorized users can still read and modify a resource, but they can't delete the resource.
ReadOnly means authorized users can read a resource, but they can't delete or update the resource. Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.
Scenario:
User2 is a Security administrator.
Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.
User2 creates the virtual networks shown in the following table.

Sub1 contains the locks shown in the following table.

References:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources
Testlet 2
This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question on this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next sections of the exam. After you begin a new section, you cannot return to this section.
To start the case study
To display the first question on this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.
Overview
Litware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.
Existing Environment
Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.
Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the Litware employees and their devices. Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.
The tenant contains the groups shown in the following table.

The Azure subscription contains the objects shown in the following table.

Azure Security Center is set to the Free tier.
Planned changes
Litware plans to deploy the Azure resources shown in the following table.

Litware identifies the following identity and access requirements:
All San Francisco users and their devices must be members of Group1.
The members of Group2 must be assigned the Contributor role to Resource Group2 by using a permanent eligible assignment.
Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the users' behalf.
Platform Protection Requirements
Litware identifies the following platform protection requirements:
Microsoft Antimalware must be installed on the virtual machines in Resource Group1.
The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role. Azure AD users must be to authenticate to AKS1 by using their Azure AD credentials.
Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.
A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in Resource Group1. Role1 must be available only for Resource Group1.
Security Operations Requirements
Litware must be able to customize the operating system security configurations in Azure Security Center.

NEW QUESTION 29
You have an Azure subscription named Sub1.
In Azure Security Center, you have a security playbook named Play1. Play1 is configured to send an email message to a user named User1. You need to modify Play1 to send email messages to a distribution group named Alerts.
What should you use to modify Play1?

A. Azure DevOps
B. Azure Application Insights
C. Azure Monitor
D. Azure Logic Apps Designer

Answer: D

Explanation:

You can change an existing playbook in Security Center to add an action, or conditions. To do that you just need to click on the name of the playbook that you want to change, in the Playbooks tab, and Logic App Designer opens up.
References:
https://docs.microsoft.com/en-us/azure/security-center/security-center-playbooks

NEW QUESTION 30
You create a new Azure subscription.
You need to ensure that you can create custom alert rules in Azure Security Center. Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Onboard Azure Active Directory (Azure AD) Identity Protection.
B. Create an Azure Storage account.
C. Implement Azure Advisor recommendations.
D. Create an Azure Log Analytics workspace.
E. Upgrade the pricing tier of Security Center to Standard.

Answer: BD

Explanation:
D: You need write permission in the workspace that you select to store your custom alert.
References:
https://docs.microsoft.com/en-us/azure/security-center/security-center-custom-alert

NEW QUESTION 31
DRAG DROP
You have an Azure subscription that contains 100 virtual machines. Azure Diagnostics is enabled on all the virtual machines. You are planning the monitoring of Azure services in the subscription.
You need to retrieve the following details:

Identify the user who deleted a virtual machine three weeks ago.
Query the security events of a virtual machine that runs Windows Server 2016.
What should you use in Azure Monitor? To answer, drag the appropriate configuration settings to the correct details. Each configuration setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.
Select and Place:

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box1: Activity log
Azure activity logs provide insight into the operations that were performed on resources in your subscription. Activity logs were previously known as “audit logs” or “operational logs,” because they report control-plane events for your subscriptions.
Activity logs help you determine the “what, who, and when” for write operations (that is, PUT, POST, or DELETE). Box 2: Logs
Log Integration collects Azure diagnostics from your Windows virtual machines, Azure activity logs, Azure Security Center alerts, and Azure resource provider logs. This integration provides a unified dashboard for all your assets, whether they're on-premises or in the cloud, so that you can aggregate, correlate, analyze, and alert for security events.
References:
https://docs.microsoft.com/en-us/azure/security/azure-log-audit
Testlet 1
This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question on this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next sections of the exam. After you begin a new section, you cannot return to this section.
To start the case study
To display the first question on this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.
Overview
Litware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.
Existing Environment
Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.
Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the Litware employees and their devices. Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.
The tenant contains the groups shown in the following table.

The Azure subscription contains the objects shown in the following table.

Azure Security Center is set to the Free tier.
Planned changes
Litware plans to deploy the Azure resources shown in the following table.

Litware identifies the following identity and access requirements:
All San Francisco users and their devices must be members of Group1.
The members of Group2 must be assigned the Contributor role to Resource Group2 by using a permanent eligible assignment.
Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the users' behalf.
Platform Protection Requirements
Litware identifies the following platform protection requirements:
Microsoft Antimalware must be installed on the virtual machines in Resource Group1.
The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role. Azure AD users must be to authenticate to AKS1 by using their Azure AD credentials.
Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.
A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in Resource Group1. Role1 must be available only for Resource Group1.
Security Operations Requirements
Litware must be able to customize the operating system security configurations in Azure Security Center.

NEW QUESTION 36
HOTSPOT
You need to create Role1 to meet the platform protection requirements.
How should you complete the role definition of Role1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Scenario: A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in Resource Group1. Role1 must be available only for Resource Group1.
Azure RBAC template managed disks "Microsoft.Storage/" References:
https://blogs.msdn.microsoft.com/azureedu/2017/02/11/new-managed-disk-storage-option-for-your-azure-vms/

NEW QUESTION 37
From the Azure portal, you are configuring an Azure policy.
You plan to assign policies that use the DeployIfNotExist, AuditIfNotExist, Append, and Deny effects. Which effect requires a managed identity for the assignment?

A. AuditIfNotExist
B. Append
C. DeployIfNotExist
D. Deny

Answer: C

Explanation:
When Azure Policy runs the template in the deployIfNotExists policy definition, it does so using a managed identity.
References:
https://docs.microsoft.com/bs-latn-ba/azure/governance/policy/how-to/remediate-resources

NEW QUESTION 39
HOTSPOT
You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com. You plan to implement an application that will consist of the resources shown in the following table.

Users will authenticate by using their Azure AD user account and access the Cosmos DB account by using resource tokens. You need to identify which tasks will be implemented in CosmosDB1 and WebApp1.
Which task should you identify for each resource? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

A. Mastered
B. Not Mastered

Answer: A

Explanation:
CosmosDB1: Create database users and generate resource tokens.
Azure Cosmos DB resource tokens provide a safe mechanism for allowing clients to read, write, and delete specific resources in an Azure Cosmos DB account according to the granted permissions.
WebApp1: Authenticate Azure AD users and relay resource tokens
A typical approach to requesting, generating, and delivering resource tokens to a mobile application is to use a resource token broker. The following diagram shows a high-level overview of how the sample application uses a resource token broker to manage access to the document database data:

References:
https://docs.microsoft.com/en-us/xamarin/xamarin-forms/data-cloud/cosmosdb/authentication

NEW QUESTION 40
HOTSPOT
You need to create an Azure key vault. The solution must ensure that any object deleted from the key vault be retained for 90 days.
How should you complete the command? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: -EnablePurgeProtection
If specified, protection against immediate deletion is enabled for this vault; requires soft delete to be enabled as well.
Box 2: -EnableSoftDelete
Specifies that the soft-delete functionality is enabled for this key vault. When soft-delete is enabled, for a grace period, you can recover this key vault and its contents after it is deleted.
References:
https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/new-azurermkeyvault

NEW QUESTION 42
You have an Azure SQL database.
You implement Always Encrypted.
You need to ensure that application developers can retrieve and decrypt data in the database.
Which two pieces of information should you provide to the developers? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. a stored access policy
B. a shared access signature (SAS)
C. the column encryption key
D. user credentials
E. the column master key

Answer: CE

Explanation:
Always Encrypted uses two types of keys: column encryption keys and column master keys. A column encryption key is used to encrypt data in an encrypted

column. A column master key is a key-protecting key that encrypts one or more column encryption keys.
References:
https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine

NEW QUESTION 44
DRAG DROP
You have an Azure subscription named Sub1 that contains an Azure Storage account named Contosostorage1 and an Azure key vault named Contosokeyvault1.
You plan to create an Azure Automation runbook that will rotate the keys of Contosostorage1 and store them in Contosokeyvault1.
You need to implement prerequisites to ensure that you can implement the runbook.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.
Select and Place:

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Step 1: Create an Azure Automation account
Runbooks live within the Azure Automation account and can execute PowerShell scripts.
Step 2: Import PowerShell modules to the Azure Automation account
Under ‘Assets’ from the Azure Automation account Resources section select ‘to add in Modules to the runbook. To execute key vault cmdlets in the runbook, we need to add AzureRM.profile and AzureRM.key vault.
Step 3: Create a connection resource in the Azure Automation account
You can use the sample code below, taken from the AzureAutomationTutorialScript example runbook, to authenticate using the Run As account to manage Resource Manager resources with your runbooks. The AzureRunAsConnection is a connection asset automatically created when we created ‘run as accounts’ above. This can be found under Assets -> Connections. After the authentication code, run the same code above to get all the keys from the vault.
$connectionName = "AzureRunAsConnection" try
{
# Get the connection "AzureRunAsConnection "
$servicePrincipalConnection=Get-AutomationConnection -Name $connectionName
"Logging in to Azure..." Add-AzureRmAccount `
-ServicePrincipal `
-TenantId $servicePrincipalConnection.TenantId `
-ApplicationId $servicePrincipalConnection.ApplicationId `
-CertificateThumbprint $servicePrincipalConnection.CertificateThumbprint
}
References:
https://www.rahulpnath.com/blog/accessing-azure-key-vault-from-azure-runbook/

NEW QUESTION 48
HOTSPOT
You have the Azure Information Protection conditions shown in the following table.

You have the Azure Information Protection labels shown in the following table.

You need to identify how Azure Information Protection will label files.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Label 2 only
How multiple conditions are evaluated when they apply to more than one label
1. The labels are ordered for evaluation, according to their position that you specify in the policy: The label positioned first has the lowest position (least sensitive) and the label positioned last has the highest position (most sensitive).
2. The most sensitive label is applied.
3. The last sublabel is applied.
Box 2: No Label
Automatic classification applies to Word, Excel, and PowerPoint when documents are saved, and apply to Outlook when emails are sent. Automatic classification does not apply to Microsoft Notepad.
References:
https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification

NEW QUESTION 50

Your company uses Azure DevOps.
You need to recommend a method to validate whether the code meets the company's quality standards and code review standards. What should you recommend implementing in Azure DevOps?

A. branch folders
B. branch permissions
C. branch policies
D. branch locking

Answer: C

Explanation:
Branch policies help teams protect their important branches of development. Policies enforce your team's code quality and change management standards.
References:
https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies?view=azure-devops&viewFallbackFrom=vsts

NEW QUESTION 52
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your az-500 Exam with Our Prep Materials Via below:

https://www.certleader.com/az-500-dumps.html