



AZ- 500.examcollection.premium.exam.117q AZ-500

AZ-500

Microsoft Azure Security Technologies

Version 5.0

This file was created using

VCE Simulator

from

Avanset.com

Score: 800/1000
Version:
Time Limit: 120 Minutes

Manage identity and access

Case Study (1 questions)

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.

Name	Type	Description
Group1	Security group	A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources.
Group2	Security group	A group that has the Dynamic User membership type and contains the Chicago IT team

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

Name	Type	Description
VNet1	Virtual network	VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet.
VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.
VM1	Virtual machine	VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subnet0.
SQLDB1	Azure SQL Database	SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1.
WebApp1	Web app	WebApp1 is an Azure web app that is accessible by using https://litwareinc.com and http://www.litwareinc.com .
Resource Group1	Resource group	Resource Group1 is a resource group that contains VNet1, VM0, and VM1.
Resource Group2	Resource group	Resource Group2 is a resource group that contains shared IT resources.

Azure Security Center is set to the Free tier.

Planned changes

Litware plans to deploy the Azure resources shown in the following table.

Name	Type	Description
Firewall1	Azure Firewall	An Azure firewall on VNet1.
RT1	Route table	A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0.
AKS1	Azure Kubernetes Service (AKS)	A managed AKS cluster

Identity and Access Requirements

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 able 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.

Data and Application Requirements

Litware identifies the following data and applications requirements:

The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials.

WebApp1 must enforce mutual authentication.

General Requirements

Litware identifies the following general requirements:

Whenever possible, administrative effort must be minimized.

Whenever possible, use of automation must be minimized.

Question 1

You need to meet the identity and access requirements for Group1.

What should you do?

- ☐ Add a membership rule to Group1.
- ☐ Delete Group1. Create a new group named Group1 that has a membership type of Office 365. Add users and devices to the group.
- ☐ Modify the membership rule of Group1.
- ☐ Change the membership type of Group1 to Assigned. Create two groups that have dynamic memberships. Add the new groups to Group1.

Case Study (1 questions)

Case Study

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.

Existing Environment

Azure AD

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

Name	City	Role
User1	Montreal	Global administrator
User2	MONTREAL	Security administrator
User3	London	Privileged role administrator
User4	Ontario	Application administrator
User5	Seattle	Cloud application administrator
User6	Seattle	User administrator
User7	Sydney	Reports reader
User8	Sydney	None
User9	Sydney	Owner

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

Name	Membership type	Dynamic membership rule
Group1	Dynamic user	<code>user.city -contains "ON"</code>
Group2	Dynamic user	<code>user.city -match "*on"</code>

Sub1

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

User9 creates the virtual networks shown in the following table.

Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.

Name	Set on	Lock type
Lock1	RG1	Delete
Lock2	RG2	Read-only
Lock3	RG3	Delete
Lock4	RG3	Read-only

Sub1 contains the Azure policies shown in the following table.

Policy definition	Resource type	Scope
Allowed resource types	networkSecurityGroups	RG4
Not allowed resource types	virtualNetworks/subnets	RG5
Not allowed resource types	networkSecurityGroups	RG5
Not allowed resource types	virtualNetworks/virtualNetworkPeerings	RG6

Sub2

Sub2 contains the virtual networks shown in the following table.

Name	Subnet
VNetwork1	Subnet11, Subnet12, and Subnet13
VNetwork2	Subnet21

Sub2 contains the virtual machines shown in the following table.

Name	Network interface	Application security group	Connected to
VM1	NIC1	ASG1	Subnet11
VM2	NIC2	ASG2	Subnet11
VM3	NIC3	None	Subnet12
VM4	NIC4	ASG1	Subnet13
VM5	NIC5	None	Subnet21

All virtual machines have 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.

Name	Associated to
NSG1	NIC2
NSG2	Subnet11
NSG3	Subnet13
NSG4	Subnet21

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

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

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

Priority	Port	Protocol	Source	Destination	Action
100	80	TCP	Internet	VirtualNetwork	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

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

Priority	Port	Protocol	Source	Destination	Action
100	Any	TCP	ASG1	ASG1	Allow
150	Any	Any	ASG2	VirtualNetwork	Allow
200	Any	Any	Any	Any	Deny
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

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

Priority	Port	Protocol	Source	Destination	Action
100	Any	Any	Any	Any	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

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

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	Any	Internet	Allow
65500	Any	Any	Any	Any	Deny

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.

Question 2

You need to ensure that User2 can implement PIM.

What should you do first?

- ☐ Assign User2 the Global administrator role.
- ☐ Configure authentication methods for contoso.com.
- ☐ Configure the identity secure score for contoso.com.
- ☐ Enable multi-factor authentication (MFA) for User2.

(27 questions)**Question 3**

Your network contains an Active Directory forest named contoso.com. You have an Azure Directory (Azure AD) tenant named contoso.com.

You plan to configure synchronization by using the Express Settings installation option in Azure AD Connect.

You need to identify which roles and groups are required to perform the planned configuration. The solution must use the principle of least privilege.

Which two roles and groups should you identify? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- ☐ the Domain Admins group in Active Directory
- ☐ the Security administrator role in Azure AD
- ☐ the Global administrator role in Azure AD
- ☐ the User administrator role in Azure AD
- ☐ the Enterprise Admins group in Active Directory

Question 4

HOTSPOT

You create and enforce an Azure AD Identity Protection user risk policy that has the following settings:

Assignment: Include Group1, Exclude Group2

Conditions: Sign-in risk of Medium and above

Access: Allow access, Require password change

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Member of	Mobile phone	Multi-factor authentication (MFA) status
User1	Group1	123 555 7890	Disabled
User2	Group1, Group2	None	Enabled
User3	Group1	123 555 7891	Required

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
If User1 signs in from an unfamiliar location, he must change his password.	☐	☐
If User2 signs in from an anonymous IP address, she must change her password.	☐	☐
If User3 signs in from a computer containing malware that is communicating with known bot servers, he must change his password.	☐	☐

Question 5

You plan to use Azure Resource Manager templates to perform multiple deployments of identically configured Azure virtual machines. The password for the administrator account of each deployment is stored as a secret in different Azure key vaults.

You need to identify a method to dynamically construct a resource ID that will designate the key vault containing the appropriate secret during each deployment. The name of the key vault and the name of the secret will be provided as inline parameters.

What should you use to construct the resource ID?

- ☐ a key vault access policy
- ☐ a linked template
- ☐ a parameters file
- ☐ an automation account

Question 6

Your network contains an Active Directory forest named contoso.com. The forest contains a single domain.

You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

You plan to deploy Azure AD Connect and to integrate Active Directory and the Azure AD tenant.

You need to recommend an integration solution that meets the following requirements:

Ensures that password policies and user logon restrictions apply to user accounts that are synced to the tenant

Minimizes the number of servers required for the solution.

Which authentication method should you include in the recommendation?

- ☐ federated identity with Active Directory Federation Services (AD FS)
- ☐ password hash synchronization with seamless single sign-on (SSO)
- ☐ pass-through authentication with seamless single sign-on (SSO)

Question 7

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 a hybrid configuration of Azure Active Directory (Azure AD).

You have an Azure HDInsight cluster on a virtual network.

You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials.

You need to configure the environment to support the planned authentication.

Solution: You create a site-to-site VPN between the virtual network and the on-premises network.

Does this meet the goal?

- ☐ Yes
- ☐ No

Question 8

HOTSPOT

You have an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Role	Sign in frequency
User1	Password administrator	Sign in every work day
User2	Password administrator	Sign in bi-weekly
User3	Global administrator, Password administrator	Signs in every month

You configure an access review named Review1 as shown in the following exhibit.

Create an access review

Access reviews enable reviewers to attest to whether users still need to be in a role.

* Review name

Review1

Description ⓘ

* Start date

2019-03-01

Frequency

One time

Duration (in days) ⓘ

1

End ⓘ

Never

End by

Occurrences

* Number of times

0

* End date

2019-03-20

Users

Scope ☒ Everyone

* Review role membership

Password administrator

Reviewers

Reviewers Members(self)

Upon completion settings

Auto apply results to resource ⓘ

Should reviewer not respond ⓘ Take recommendations

Advanced settings

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

User3 can perform Review1 for

▼

User3 only
User1 and User2 only
User1, User2, and User3

If User2 fails to complete Review1 by March 20, 2019

▼

The Password administrator role will be revoked from User2
User2 will retain the Password administrator role
User3 will receive a confirmation request

Question 9

HOTSPOT

You have an Azure subscription named Sub 1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Role
User1	Global administrator
User2	Security administrator
User3	Security reader
User4	License administrator

Each user is assigned an Azure AD Premium P2 license.

You plan to onboard and configure Azure AD Identity Protection.

Which users can onboard Azure AD Identity Protection, remediate users, and configure policies? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Users who can onboard Azure AD Identity Protection:

	▼
User1 only	
User1 and User2 only	
User1, User2, and User3 only	
User1, User2, User3, and User4 only	

Users who can remediate users and configure policies:

	▼
User1 and User2 only	
User1 and User3 only	
User1, User2, and User3 only	
User1, User2, User3, and User4	

Question 10

DRAG DROP

You create an Azure subscription with Azure AD Premium P2.

You need to ensure that you can use Azure Active Directory (Azure AD) Privileged Identity Management (PIM) to secure Azure AD roles.

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.

Actions

Discover privileged roles.

Sign up PIM for Azure AD roles.

Consent to PIM.

Discover resources.

Verify your identity by using multi-factor authentication (MFA).

Answer Area

Question 11

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 a hybrid configuration of Azure Active Directory (Azure AD).

You have an Azure HDInsight cluster on a virtual network.

You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials.

You need to configure the environment to support the planned authentication.

Solution: You deploy an Azure AD Application Proxy.

Does this meet the goal?

- ☐ Yes
- ☐ No

Question 12

HOTSPOT

Your company has two offices in Seattle and New York. Each office connects to the Internet by using a NAT device. The offices use the IP addresses shown in the following table.

Location	IP address space	Public NAT segment
Seattle	10.10.0.0/16	190.15.1.0/24
New York	172.16.0.0/16	194.25.2.0/24

The company has an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Multi-factor authentication (MFA) status
User1	Enabled
User2	Enforced

The MFA service settings are configured as shown in the exhibit. (Click the Exhibit tab.)

trusted ips ([learn more](#))

☒ Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

10.10.0.0/16
194.25.2.0/24

verification options ([learn more](#))

Methods available to users:

- ☒ Call to phone
- ☒ Text message to phone
- ☐ Notification through mobile app
- ☐ Verification code from mobile app or hardware token

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

NOTE: Each correct selection is worth one point.

Answer Area

	Yes	No
If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone.	☐	☐
If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app.	☐	☐
If User2 signs in to Azure from a device in the New York office, User1 must be authenticated by using a phone	☐	☐

Question 13

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?

- ☐ Synchronization Rules Editor
- ☐ Web Service Configuration Tool
- ☐ Azure Portal
- ☐ Active Directory Users and Computers

Question 14

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 a hybrid configuration of Azure Active Directory (Azure AD).

You have an Azure HDInsight cluster on a virtual network.

You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials.

You need to configure the environment to support the planned authentication.

Solution: You deploy the On-premises data gateway to the on-premises network.

Does this meet the goal?

- ☐ Yes
- ☐ No

Question 15

HOTSPOT

You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Member of	Multi-factor authentication (MFA) status
User1	Group1, Group2	Disabled
User2	Group2	Disabled

The tenant contains the named locations shown in the following table.

Name	IP address range	Trusted location
Seattle	193.77.10.0/24	Yes
Boston	154.12.18.0/24	No

You create the conditional access policies for a cloud app named App1 as shown in the following table.

Name	Include	Exclude	Condition	Grant
Policy1	Group1	Group2	Locations: Boston	Block access
Policy2	Group1	None	Locations: Any location	Grant access, Require multi-factor authentication
Policy3	Group2	Group1	Locations: Boston	Block access
Policy4	User2	None	Locations: Any location	Grant access, Require multi-factor authentication

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can access App1 from an IP address of 154.12.18.10.	☐	☐
User2 can access App1 from an IP address of 193.77.10.15.	☐	☐
User2 can access App1 from an IP address of 154.12.18.34.	☐	☐

Question 16

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 regenerate the access keys.

Does this meet the goal?

- ☐ Yes
- ☐ No

Question 17

You have a hybrid configuration of Azure Active Directory (Azure AD). You have an Azure SQL Database instance that is configured to support Azure AD authentication.

Database developers must connect to the database instance and authenticate by using their on-premises Active Directory account.

You need to ensure that developers can connect to the instance by using Microsoft SQL Server Management Studio. The solution must minimize authentication prompts.

Which authentication method should you recommend?

- ☐ Active Directory - Password
- ☐ Active Directory - Universal with MFA support
- ☐ SQL Server Authentication
- ☐ Active Directory - Integrated

Question 18

DRAG DROP

You need to configure an access review. The review will be assigned to a new collection of reviews and reviewed by resource owners.

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.

Actions**Answer Area**

Create an access review program.

Set Reviewers to Selected users.

Create an access review audit.

Create an access review control.

Set Reviewers to Group owners.

Set Reviewers to Members.



Question 19

HOTSPOT

You have an Azure Container Registry named Registry1.

You add role assignment for Registry1 as shown in the following table.

User	Role
User1	AcrPush
User2	AcrPull
User3	AcrImageSigner
User4	Contributor

Which users can upload images to Registry1 and download images from Registry1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Upload images:

▼

User1 only
User1 and User4 only
User1, User3, and User4
User1, User2, User3, and User4

Download images:

▼

User2 only
User1 and User2 only
User2 ad User4 only
User1, User2, and User4
User1, User2, User3, and User4

Question 20

DRAG DROP

You are implementing conditional access policies.

You must evaluate the existing Azure Active Directory (Azure AD) risk events and risk levels to configure and implement the policies.

You need to identify the risk level of the following risk events:

Users with leaked credentials

Impossible travel to atypical locations

Sign-ins from IP addresses with suspicious activity

Which level should you identify for each risk event? To answer, drag the appropriate levels to the correct risk events. Each level 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.

Levels**Answer Area****High**

Impossible travel to atypical locations:

Low

Users with leaked credentials:

Medium

Sign-ins from IP addresses with suspicious activity:

Question 21

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 a hybrid configuration of Azure Active Directory (Azure AD).

You have an Azure HDInsight cluster on a virtual network.

You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials.

You need to configure the environment to support the planned authentication.

Solution: You deploy Azure Active Directory Domain Services (Azure AD DS) to the Azure subscription.

Does this meet the goal?

- ☐ Yes
- ☐ No

Question 22

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?

- ☐ Azure Security Center
- ☐ Azure Policy
- ☐ Azure AD Privileged Identity Management (PIM)
- ☐ Azure Blueprints

Question 23

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 create a new stored access policy.

Does this meet the goal?

- ☐ Yes
- ☐ No

Question 24

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?

- ☐ Yes
- ☐ No

Question 25

HOTSPOT

You create a new Azure subscription that is associated to a new Azure Active Directory (Azure AD) tenant.

You create one active conditional access policy named Portal Policy. Portal Policy is used to provide access to the Microsoft Azure Management cloud app.

The Conditions settings for Portal Policy are configured as shown in the Conditions exhibit. (Click the Conditions tab.)

The screenshot displays the 'Portal Policy' configuration page in the Azure portal, with the 'Conditions' tab selected. The page is divided into three main sections: 'Portal Policy', 'Conditions', and 'Locations'.

- Portal Policy:** Contains the policy name 'Portal Policy', a list of assignments (Users and groups: All users; Cloud apps: 1 app included; Conditions: 1 condition selected), and access controls (Grant: 2 controls selected; Session: 0 controls selected).
- Conditions:** Shows the configuration for the selected condition. It includes sections for 'Device platforms' (Not configured), 'Locations' (1 included), 'Client apps (preview)' (Not configured), and 'Device state (preview)' (Not configured).
- Locations:** Provides options to control user access based on their physical location. It includes a 'Configure' toggle set to 'Yes', an 'Include' section with radio buttons for 'Any location', 'All trusted locations', and 'Selected locations' (which is selected), and a list of selected locations including 'Contoso'.

The Grant settings for Portal Policy are configured as shown in the Grant exhibit. (Click the Grant tab.)

Portal Policy

Info
Delete

* Name

Assignments

Users and groups ⓘ
All users

Cloud apps ⓘ
1 app included

Conditions ⓘ
1 condition selected

Access controls

Grant ⓘ
2 controls selected

Session ⓘ
0 controls selected

Grant

Select the controls to be enforced.

☐ Block access
☒ Grant access

☒ Require multi-factor authentication ⓘ
☐ Require device to be marked as compliant ⓘ
☐ Require Hybrid Azure AD joined device ⓘ
☒ Require approved client app ⓘ
[See list of approved client apps](#)

For multiple controls
☐ Require all the selected controls
☒ Require one of the selected controls

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

NOTE: Each correct selection is worth one point.

Answer area

Statements	Yes	No
Users from the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	☐	☐
Users from the Contoso named location must use multi-factor authentication (MFA) to access the web services hosted in the Azure subscription.	☐	☐
Users external to the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	☐	☐

Question 26

You have an Azure subscription.

You create an Azure web app named Contoso1812 that uses an S1 App service plan.

You create a DNS record for `www.contoso.com` that points to the IP address of Contoso1812.
You need to ensure that users can access Contoso1812 by using the `https://www.contoso.com` URL.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- ☐ Turn on the system-assigned managed identity for Contoso1812.
- ☐ Add a hostname to Contoso1812.
- ☐ Scale out the App Service plan of Contoso1812.
- ☐ Add a deployment slot to Contoso1812.
- ☐ Scale up the App Service plan of Contoso1812.
- ☐ Upload a PFX file to Contoso1812.

Question 27

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 create a lock on Sa1.

Does this meet the goal?

- ☐ Yes
- ☐ No

Question 28

You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

An administrator named Admin1 has access to the following identities:

An OpenID-enabled user account

A Hotmail account

An account in contoso.com

An account in an Azure AD tenant named fabrikam.com

You plan to use Azure Account Center to transfer the ownership of Sub1 to Admin1.

To which accounts can you transfer the ownership of Sub1?

- ☐ contoso.com only
- ☐ contoso.com, fabrikam.com, and Hotmail only
- ☐ contoso.com and fabrikam.com only
- ☐ contoso.com, fabrikam.com, Hotmail, and OpenID-enabled user account

Question 29**HOTSPOT**

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Member of	Multi-factor authentication (MFA) status
User1	None	Disabled
User2	Group1	Disabled
user3	Group1	Enforced

Azure AD Privileged Identity Management (PIM) is enabled for the tenant.

In PIM, the Password Administrator role has the following settings:

Maximum activation duration (hours): 2
 Send email notifying admins of activation: Disable
 Require incident/request ticket number during activation: Disable
 Require Azure Multi-Factor Authentication for activation: Enable
 Require approval to activate this role: Enable
 Selected approver: Group1

You assign users the Password Administrator role as shown in the following table.

Name	Assignment type
User1	Active
User2	Eligible
user3	Eligible

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

NOTE: Each correct selection is worth one point.

Answer area

Statements	Yes	No
When User1 signs in, the user is assigned the Password Administrator role automatically.	☐	☐
User2 can request to activate the Password Administrator role.	☐	☐
If User3 wants to activate the Password Administrator role, the user can approve their own request.	☐	☐

Implement platform protection

Case Study (3 questions)

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.

Name	Type	Description
Group1	Security group	A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources.
Group2	Security group	A group that has the Dynamic User membership type and contains the Chicago IT team

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

Name	Type	Description
VNet1	Virtual network	VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet.
VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.
VM1	Virtual machine	VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subnet0.
SQLDB1	Azure SQL Database	SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1.
WebApp1	Web app	WebApp1 is an Azure web app that is accessible by using https://litwareinc.com and http://www.litwareinc.com .
Resource Group1	Resource group	Resource Group1 is a resource group that contains VNet1, VM0, and VM1.
Resource Group2	Resource group	Resource Group2 is a resource group that contains shared IT resources.

Identity and Access Requirements

Azure Security Center is set to the Free tier.

Planned changes

Litware plans to deploy the Azure resources shown in the following table.

Name	Type	Description
Firewall1	Azure Firewall	An Azure firewall on VNet1.
RT1	Route table	A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0.
AKS1	Azure Kubernetes Service (AKS)	A managed AKS cluster

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 able 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.

Data and Application Requirements

Litware identifies the following data and applications requirements:

The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials.

WebApp1 must enforce mutual authentication.

General Requirements

Litware identifies the following general requirements:

Whenever possible, administrative effort must be minimized.

Whenever possible, use of automation must be minimized.

Question 30

You need to ensure that users can access VM0. The solution must meet the platform protection requirements.

What should you do?

- ☐ Move VM0 to Subnet1.
- ☐ On Firewall, configure a network traffic filtering rule.
- ☐ Assign RT1 to AzureFirewallSubnet.
- ☐ On Firewall, configure a DNAT rule.

Question 31

HOTSPOT

You need to deploy Microsoft Antimalware to meet the platform protection requirements.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Create a custom policy definition that has effect set to:

▼

Append
Deny
DeployIfNotExists

Create a policy assignment and modify:

▼

The Create a Managed Identify setting
The exclusion settings
The scope

Question 32

DRAG DROP

You need to deploy AKS1 to meet the platform protection requirements.

Which four 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.

NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.

Actions

Deploy an AKS cluster.

Create a client application.

Create a server application.

Create an RBAC binding.

Create a custom RBAC role.

Answer Area

Case Study (5 questions)

Case Study

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.

Existing Environment

Azure AD

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

Name	City	Role
User1	Montreal	Global administrator
User2	MONTREAL	Security administrator
User3	London	Privileged role administrator
User4	Ontario	Application administrator
User5	Seattle	Cloud application administrator
User6	Seattle	User administrator
User7	Sydney	Reports reader
User8	Sydney	None
User9	Sydney	Owner

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

Name	Membership type	Dynamic membership rule
Group1	Dynamic user	<code>user.city -contains "ON"</code>
Group2	Dynamic user	<code>user.city -match "*on"</code>

Sub1

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

User9 creates the virtual networks shown in the following table.

Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.

Name	Set on	Lock type
Lock1	RG1	Delete
Lock2	RG2	Read-only
Lock3	RG3	Delete
Lock4	RG3	Read-only

Sub1 contains the Azure policies shown in the following table.

Policy definition	Resource type	Scope
Allowed resource types	networkSecurityGroups	RG4
Not allowed resource types	virtualNetworks/subnets	RG5
Not allowed resource types	networkSecurityGroups	RG5
Not allowed resource types	virtualNetworks/virtualNetworkPeerings	RG6

Sub2

Sub2 contains the virtual networks shown in the following table.

Name	Subnet
VNetwork1	Subnet11, Subnet12, and Subnet13
VNetwork2	Subnet21

Sub2 contains the virtual machines shown in the following table.

Name	Network interface	Application security group	Connected to
VM1	NIC1	ASG1	Subnet11
VM2	NIC2	ASG2	Subnet11
VM3	NIC3	None	Subnet12
VM4	NIC4	ASG1	Subnet13
VM5	NIC5	None	Subnet21

All virtual machines have 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.

Name	Associated to
NSG1	NIC2
NSG2	Subnet11
NSG3	Subnet13
NSG4	Subnet21

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

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

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

Priority	Port	Protocol	Source	Destination	Action
100	80	TCP	Internet	VirtualNetwork	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

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

Priority	Port	Protocol	Source	Destination	Action
100	Any	TCP	ASG1	ASG1	Allow
150	Any	Any	ASG2	VirtualNetwork	Allow
200	Any	Any	Any	Any	Deny
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

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

Priority	Port	Protocol	Source	Destination	Action
100	Any	Any	Any	Any	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

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

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	Any	Internet	Allow
65500	Any	Any	Any	Any	Deny

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.

Question 33

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.

Answer Area

Statements	Yes	No
From VM1, you can successfully ping the public IP address of VM2. ☐	☐	☐
From VM1, you can successfully ping the private IP address of VM3. ☐	☐	☐
From VM1, you can successfully ping the private IP address of VM5. ☐	☐	☐

Question 34**HOTSPOT**

You are evaluating the security of VM1, VM2, and VM3 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.

Answer area

	Yes	No
From the Internet, you can connect to the web server on VM1 by using HTTP. ☐	☐	☐
From the Internet, you can connect to the web server on VM2 by using HTTP. ☐	☐	☐
From the Internet, you can connect to the web server on VM3 by using HTTP. ☐	☐	☐

Question 35

You need to meet the technical requirements for VNetwork1.

What should you do first?

- ☐ Create a new subnet on VNetwork1.
- ☐ Remove the NSGs from Subnet11 and Subnet13.
- ☐ Associate an NSG to Subnet12.
- ☐ Configure DDoS protection for VNetwork1.

Question 36

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.

Answer Area

Group1:

	▼
No members	
Only User2	
Only User2 and User4	
User1, User2, User3, and User4	

Group2:

	▼
No members	
Only User3	
Only User1 and User3	
User1, User2, User3, and User4	

Question 37

HOTSPOT

You are evaluating the effect of the application security groups on 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.

Answer area	Statements	Yes	No
	From VM1, you can successfully ping the private IP address of VM4.	☐	☐
	From VM2, you can successfully ping the private IP address of VM4.	☐	☐
	From VM1, you can connect to the web server on VM4.	☐	☐

(32 questions)

Question 38

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 use Azure Security Center for the centralized policy management of three Azure subscriptions.

You use several policy definitions to manage the security of the subscriptions.

You need to deploy the policy definitions as a group to all three subscriptions.

Solution: You create an initiative and an assignment that is scoped to a management group.

Does this meet the goal?

- ☐ Yes
☐ No

Question 39

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?

- ☐ device configuration policies in Microsoft Intune
- ☐ an Azure Desired State Configuration (DSC) virtual machine extension
- ☐ application security groups
- ☐ device compliance policies in Microsoft Intune

Question 40

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. The subscription contains 50 virtual machines that run Windows Server 2012 R2 or Windows Server 2016.

You need to deploy Microsoft Antimalware to the virtual machines.

Solution: You add an extension to each virtual machine.

Does this meet the goal?

- ☐ Yes
- ☐ No

Question 41

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 use Azure Security Center for the centralized policy management of three Azure subscriptions.

You use several policy definitions to manage the security of the subscriptions.

You need to deploy the policy definitions as a group to all three subscriptions.

Solution: You create a policy definition and assignments that are scoped to resource groups.

Does this meet the goal?

- ☐ Yes
- ☐ No

Question 42

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 use Azure Security Center for the centralized policy management of three Azure subscriptions.

You use several policy definitions to manage the security of the subscriptions.

You need to deploy the policy definitions as a group to all three subscriptions.

Solution: You create a resource graph and an assignment that is scoped to a management group.

Does this meet the goal?

- ☐ Yes
- ☐ No

Question 43

HOTSPOT

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

Name	Resource group	Status
VM1	RG1	Stopped (Deallocated)
VM2	RG2	Stopped (Deallocated)

You create the Azure policies shown in the following table.

Policy definition	Resource type	Scope
Not allowed resource types	virtualMachines	RG1
Allowed resource types	virtualMachines	RG2

You create the resource locks shown in the following table.

Name	Type	Created on
Lock1	Read-only	VM1
Lock2	Read-only	RG2

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
You can start VM1.	☐	☐
You can start VM2.	☐	☐
You can create a virtual machine in RG2.	☐	☐

Question 44

HOTSPOT

You have an Azure subscription. The subscription contains Azure virtual machines that run Windows Server 2016.

You need to implement a policy to ensure that each virtual machine has a custom antimalware virtual machine extension installed.

How should you complete the policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

```
{
  "if" : {
    "allof": [
      {
        "field" : "type",
        "equals": "Microsoft.Compute/virtualMachines"
      }
      {
        "field" : "Microsoft.Compute/imageSKU",
        "equals" : "2016-Datacenter",
      }
    ]
  },
  "then" : {
    "effect" : "
    Append
    Deny
    DeployIfNotExists
    ",
    "details" : {
      "type" : "Microsoft.GuestConfiguration/guestConfigurationAssignments",
      "roleDefinitionsIds" : [
        "/providers/microsoft.authorization/roleDefinitions/12345678-1234-5678-abcd-012345678910"
      ],
      "name" : "customExtension",
      "deployment" : {
        "properties" : {
          "mode": "incremental",
          "parameters" : {
            "
            existenceCondition
            resources
            template
            ": {
          }
        }
      }
    }
  }
}
```

Question 45

You are securing access to the resources in an Azure subscription.

A new company policy states that all the Azure virtual machines in the subscription must use managed disks.

You need to prevent users from creating virtual machines that use unmanaged disks.

What should you do?

- ☐ Azure Monitor
- ☐ Azure Policy
- ☐ Azure Security Center
- ☐ Azure Service Health

Question 46

HOTSPOT

You create resources in an Azure subscription as shown in the following table.

Name	Type	Region
RG1	Resource group	West Europe
VNET1	Azure virtual network	West Europe
Contoso1901	Azure Storage account	West Europe

VNET1 contains two subnets named Subnet1 and Subnet2. Subnet1 has a network ID of 10.0.0.0/24. Subnet2 has a network ID of 10.1.1.0/24.

Contoso1901 is configured as shown in the exhibit. (Click the Exhibit tab.)

```
PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet

ByPass          : Logging, Metrics
DefaultAction    : Deny
IpRules          : [193.77.0.0/16,...]
VirtualNetworkRules : [/subscriptions/a90c8c8f-d8bc-4112-abfb-dac4906573dd/resourceGroups/RG1/providers/Microsoft.Network/virtualNetworks/VNET1/subnets/Subnet1,...]

PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet.IpRules

Action IPAddressOrRange
-----
Allow  193.77.0.0/16

PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet.IpRules

Action VirtualNetworkResourceId          State
-----
Allow  /subscriptions/a90c8c8f-d8bc-4112-abfb-dac4906573dd/resourceGroups/RG1/providers/Microsoft.Network/virtualNetworks/VNET1/subnets/Subnet1 Succeeded

PS C:\> _
```

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

NOTE: Each correct selection is worth one point.

Answer area

Statements	Yes	No
An Azure virtual machine on Subnet1 can access data in Contoso1901.	☐	☐
An Azure virtual machine on Subnet2 can access data in Contoso1901.	☐	☐
A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901.	☐	☐

Question 47

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

Name	Region	Subnet
VNET1	West US	Subnet11 and Subnet12
VNET2	West US 2	Subnet21
VNET3	East US	Subnet31

The subscription contains the virtual machines shown in the following table.

Name	Network interface	Connected to
VM1	NIC1	Subnet11
VM2	NIC2	Subnet11
VM3	NIC3	Subnet12
VM4	NIC4	Subnet21
VM5	NIC5	Subnet31

On NIC1, you configure an application security group named ASG1.

On which other network interfaces can you configure ASG1?

- ☐ NIC2 only
- ☐ NIC2, NIC3, NIC4, and NIC5
- ☐ NIC2 and NIC3 only
- ☐ NIC2, NIC3, and NIC4 only

Question 48

DRAG DROP

You have an Azure subscription named Sub1.

You have an Azure Active Directory (Azure AD) group named Group1 that contains all the members of your IT team.

You need to ensure that the members of Group1 can stop, start, and restart the Azure virtual machines in Sub1. The solution must use the principle of least privilege.

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.

Actions	Answer Area
Create a JSON file.	
Run the Update-AzureRmManagementGroup cmdlet.	
Create an XML file.	
Run the New-AzureRmRoleDefinition cmdlet.	
Run the New-AzureRmRoleAssignment cmdlet.	

Question 49

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. The subscription contains 50 virtual machines that run Windows Server 2012 R2 or Windows Server 2016.

You need to deploy Microsoft Antimalware to the virtual machines.

Solution: You connect to each virtual machine and add a Windows feature.

Does this meet the goal?

- ☐ Yes
☐ No

Question 50

You have the Azure virtual machines shown in the following table.

Name	Operating system	State
VM1	Windows Server 2008 R2 Service Pack 1 (SP1)	Running
VM2	Windows Server 2012 R2	Running
VM3	Windows Server 2016	Stopped
VM4	Ubuntu Server 18.04 LTS	Running

For which virtual machine can you enable Update Management?

- ☐ VM2 and VM3 only
- ☐ VM2, VM3, and VM4 only
- ☐ VM1, VM2, and VM4 only
- ☐ VM1, VM2, VM3, and VM4
- ☐ VM1, VM2, and VM3 only

Question 51

You have an Azure subscription that contains a user named User1 and an Azure Container Registry named ConReg1.

You enable content trust for ContReg1.

You need to ensure that User1 can create trusted images in ContReg1. The solution must use the principle of least privilege.

Which two roles should you assign to User1? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- ☐ AcrQuarantineReader
- ☐ Contributor
- ☐ AcrPush
- ☐ AcrImageSigner
- ☐ AcrQuarantineWriter

Question 52

DRAG DROP

You have an Azure subscription that contains the following resources:

A virtual network named VNET1 that contains two subnets named Subnet1 and Subnet2.

A virtual machine named VM1 that has only a private IP address and connects to Subnet1.

You need to ensure that Remote Desktop connections can be established to VM1 from the internet.

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.

Actions

Configure a network security group (NSG).

Create a network rule collection.

Create a NAT rule collection.

Create a new subnet.

Deploy Azure Application Gateway.

Deploy Azure Firewall.

Answer Area

Question 53

You have the Azure virtual machines shown in the following table.

Name	Operating system	Region	Resource group
VM1	Windows Server 2012	East US	RG1
VM2	Windows Server 2012 R2	West Europe	RG1
VM3	Windows Server 2016	West Europe	RG2
VM4	Red Hat Enterprise Linux 7.4	East US	RG2

You create an Azure Log Analytics workspace named Analytics1 in RG1 in the East US region.

Which virtual machines can be enrolled in Analytics1?

- ☐ VM1 only
- ☐ VM1, VM2, and VM3 only
- ☐ VM1, VM2, VM3, and VM4
- ☐ VM1 and VM4 only

Question 54

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 use Azure Security Center for the centralized policy management of three Azure subscriptions.

You use several policy definitions to manage the security of the subscriptions.

You need to deploy the policy definitions as a group to all three subscriptions.

Solution: You create a policy initiative and assignments that are scoped to resource groups.

Does this meet the goal?

- ☐ Yes
- ☐ No

Question 55

From Azure Security Center, you create a custom alert rule.

You need to configure which users will receive an email message when the alert is triggered.

What should you do?

- ☐ From Azure Monitor, create an action group.
- ☐ From Security Center, modify the Security policy settings of the Azure subscription.
- ☐ From Azure Active Directory (Azure AD), modify the members of the Security Reader role group.
- ☐ From Security Center, modify the alert rule.

Question 56

You have an Azure subscription named Sub1. Sub1 contains a virtual network named VNet1 that contains one subnet named Subnet1.

Subnet1 contains an Azure virtual machine named VM1 that runs Ubuntu Server 18.04.

You create a service endpoint for MicrosoftStorage in Subnet1.

You need to ensure that when you deploy Docker containers to VM1, the containers can access Azure Storage resources by using the service endpoint.

What should you do on VM1 before you deploy the container?

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

Question 57

HOTSPOT

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

Name	Operating system	Region	Resource group
VM1	Windows Server 2012	East US	RG1
VM2	Windows Server 2012 R2	West US	RG1
VM3	Windows Server 2016	West US	RG2
VM4	Ubuntu Server 18.04 LTS	West US	RG2
VM5	Red Hat Enterprise Linux 7.4	East US	RG1
VM6	CentOS 7.5	East US	RG1

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.

Answer Area

Update1:

▼

VM2 only
VM4 only
VM1 and VM2 only
VM1, VM2, VM4, VM5, and VM6

Update2:

▼

VM5 only
VM1 and VM5 only
VM4 and VM5 only
VM1, VM2, and VM5 only
VM1, VM2, VM3, VM4, and VM5

Question 58

DRAG DROP

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

Name	Region	Description
HubVNet	East US	HubVNet is a virtual network connected to the on-premises network by using a site-to-site VPN that has BGP route propagation enabled. HubVNet contains subnets named HubVNetSubnet0 and GatewaySubnet. Virtual network gateway is connected to GatewaySubnet.
SpokeVNet	East US	SpokeVNet is a virtual network connected to HubVNet by using VNet peering. SpokeVNet contains subnets named SpokeVNetSubnet0 and AzureFirewallSubnet.

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.

Subnets	Answer Area
AzureFirewallSubnet	RT1:
GatewaySubnet	RT2:
SpokeVNetSubnet0	

Question 59

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.

Answer Area

User1:

▼

A key vault access policy
Azure Information Protection
Azure Policy
Managed identities for Azure resources
RBAC

User2:

▼

A key vault access policy
Azure Information Protection
Azure Policy
Managed identities for Azure resources
RBAC

Question 60

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

Basics

Subscription	Azure Pass - Sponsorship
Resource group	RG1
Region	(US) East US
Kubernetes cluster name	AKScluster
Kubernetes version	1.12.8
DNS name prefix	AKScluster
Node count	3
Node size	Standard_DS_v2

Scale

Virtual nodes	Disabled
VM scale sets (preview)	Disabled

Authentication

Enable RBAC	No
-------------	----

Networking

HTTP application routing	No
Network configuration	Basic

Monitoring

Enable container monitoring	No
-----------------------------	----

Tags

(none)

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?

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

Question 61

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?

- ☐ an Azure Active Directory (Azure AD) group
- ☐ an Azure Active Directory (Azure AD) role assignment
- ☐ an Azure Active Directory (Azure AD) user
- ☐ a secret in Azure Key Vault

Question 62

You plan to deploy Azure container instances.

You have a containerized application that validates credit cards. The application is comprised of two containers: an application container and a validation container.

The application container is monitored by the validation container. The validation container performs security checks by making requests to the application container and waiting for responses after every transaction.

You need to ensure that the application container and the validation container are scheduled to be deployed together. The containers must communicate to each other only on ports that are not externally exposed.

What should you include in the deployment?

- ☐ application security groups
- ☐ network security groups (NSGs)
- ☐ management groups
- ☐ container groups

Question 63

You are configuring and securing a network environment.

You deploy an Azure virtual machine named VM1 that is configured to analyze network traffic.

You need to ensure that all network traffic is routed through VM1.

What should you configure?

- ☐ a system route
- ☐ a network security group (NSG)
- ☐ a user-defined route

Question 64

You have 15 Azure virtual machines in a resource group named RG1.

All virtual machines run identical applications.

You need to prevent unauthorized applications and malware from running on the virtual machines.

What should you do?

- ☐ Apply an Azure policy to RG1.
- ☐ From Azure Security Center, configure adaptive application controls.
- ☐ Configure Azure Active Directory (Azure AD) Identity Protection.
- ☐ Apply a resource lock to RG1.

Question 65

DRAG DROP

You are configuring network connectivity for two Azure virtual networks named VNET1 and VNET2.

You need to implement VPN gateways for the virtual networks to meet the following requirements:

VNET1 must have six site-to-site connections that use BGP.

VNET2 must have 12 site-to-site connections that use BGP.

Costs must be minimized.

Which VPN gateway SKU should you use for each virtual network? To answer, drag the appropriate SKUs to the correct networks. Each SKU 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.

SKUs		Answer Area	
Basic	VpnGw1	VNET1:	
VpnGw2	VpnGw3	VNET2:	

Question 66

You have an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry.

You need to use automatically generated service principal for the AKS cluster to authenticate to the Azure Container Registry.

What should you create?

- ☐ a secret in Azure Key Vault
- ☐ a role assignment
- ☐ an Azure Active Directory (Azure AD) user
- ☐ an Azure Active Directory (Azure AD) group

Question 67

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.

Name	Network interface	Application security group assignment	IP address
VM1	NIC1	AppGroup12	10.0.0.10
VM2	NIC2	AppGroup12	10.0.0.11
VM3	NIC3	AppGroup3	10.0.0.100
VM4	NIC4	AppGroup4	10.0.0.200

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.

Answer Area

NSGs:

	▼
1	
2	
3	
4	

Network security rules:

	▼
1	
2	
3	
4	

Question 68

HOTSPOT

You have two Azure virtual machines in the East US2 region as shown in the following table.

Name	Operating system	Type	Tier
VM1	Windows Server 2008 R2	A3	Basic
VM2	Ubuntu 16.04-DAILY-LTS	L4s	Standard

You deploy and configure an Azure Key vault.

You need to ensure that you can enable Azure Disk Encryption on VM1 and VM2.

What should you modify on each virtual machine? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

VM1:

	▼
The operating system version	
The tier	
The type	

VM2:

	▼
The operating system version	
The tier	
The type	

Question 69**HOTSPOT**

You have a network security group (NSG) bound to an Azure subnet.

You run Get-AzureRmNetworkSecurityRuleConfig and receive the output shown in the following exhibit.

```

Name           : DenyStorageAccess
Description    :
Protocol      : *
SourcePortRange : {*}
DestinationPortRange : {*}
SourceAddressPrefix : {*}
DestinationAddressPrefix : {Storage}
SourceApplicationSecurityGroups : []
DestinationApplicationSecurityGroups : []
Access        : Deny
Priority       : 105
Direction     : Outbound

Name           : StorageEA2Allow
ProvisioningState : Succeeded
Description    :
Protocol      : *
SourcePortRange : {*}
DestinationPortRange : {443}
SourceAddressPrefix : {*}
DestinationAddressPrefix : {Storage/EastUS2}
SourceApplicationSecurityGroups : []
DestinationApplicationSecurityGroups : []
Access        : Allow
Priority       : 104
Direction     : Outbound

Name           : Contoso_FTP
Description    :
Protocol      : TCP
SourcePortRange : {*}
DestinationPortRange : {21}
SourceAddressPrefix : {1.2.3.4/32}
DestinationAddressPrefix : {10.0.0.5/32}
SourceApplicationSecurityGroups : []
DestinationApplicationSecurityGroups : []
Access        : Allow
Priority       : 504
Direction     : Inbound

```

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

Traffic destined for an Azure Storage account is **[answer choice]**.

	▼
able to connect to East US	
able to connect to East US 2	
able to connect to West Europe	
prevented from connecting to all regions	

FTP connections from 1.2.3.4 to 10.0.0.10/32 are **[answer choice]**.

	▼
allowed	
dropped	
forwarded	

Manage security operations

Case Study (2 questions)

Case Study

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.

Existing Environment

Azure AD

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

Name	City	Role
User1	Montreal	Global administrator
User2	MONTREAL	Security administrator
User3	London	Privileged role administrator
User4	Ontario	Application administrator
User5	Seattle	Cloud application administrator
User6	Seattle	User administrator
User7	Sydney	Reports reader
User8	Sydney	None
User9	Sydney	Owner

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

Name	Membership type	Dynamic membership rule
Group1	Dynamic user	<code>user.city -contains "ON"</code>
Group2	Dynamic user	<code>user.city -match "*on"</code>

Sub1

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

User9 creates the virtual networks shown in the following table.

Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.

Name	Set on	Lock type
Lock1	RG1	Delete
Lock2	RG2	Read-only
Lock3	RG3	Delete
Lock4	RG3	Read-only

Sub1 contains the Azure policies shown in the following table.

Policy definition	Resource type	Scope
Allowed resource types	networkSecurityGroups	RG4
Not allowed resource types	virtualNetworks/subnets	RG5
Not allowed resource types	networkSecurityGroups	RG5
Not allowed resource types	virtualNetworks/virtualNetworkPeerings	RG6

Sub2

Sub2 contains the virtual networks shown in the following table.

Name	Subnet
VNetwork1	Subnet11, Subnet12, and Subnet13
VNetwork2	Subnet21

Sub2 contains the virtual machines shown in the following table.

Name	Network interface	Application security group	Connected to
VM1	NIC1	ASG1	Subnet11
VM2	NIC2	ASG2	Subnet11
VM3	NIC3	None	Subnet12
VM4	NIC4	ASG1	Subnet13
VM5	NIC5	None	Subnet21

All virtual machines have 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.

Name	Associated to
NSG1	NIC2
NSG2	Subnet11
NSG3	Subnet13
NSG4	Subnet21

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

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

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

Priority	Port	Protocol	Source	Destination	Action
100	80	TCP	Internet	VirtualNetwork	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

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

Priority	Port	Protocol	Source	Destination	Action
100	Any	TCP	ASG1	ASG1	Allow
150	Any	Any	ASG2	VirtualNetwork	Allow
200	Any	Any	Any	Any	Deny
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

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

Priority	Port	Protocol	Source	Destination	Action
100	Any	Any	Any	Any	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

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

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	Any	Internet	Allow
65500	Any	Any	Any	Any	Deny

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.

Question 70

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.

Answer Area

Virtual networks that User2 can modify:

▼

VNET4 only
VNET4 and VNET1 only
VNET4, VNET3, and VNET1 only
VNET4, VNET3, VNET2, and VNET1

Virtual networks that User2 can delete:

▼

VNET4 only
VNET4 and VNET1 only
VNET4, VNET3, and VNET1 only
VNET4, VNET3, VNET2, and VNET1

Question 71

HOTSPOT

You assign User8 the Owner role for RG4, RG5, and RG6.

In which resource groups can User8 create virtual networks and NSGs? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

User8 can create virtual networks in:

	▼
RG4 only	
RG6 only	
RG4 and RG6 only	
RG4, RG5, and RG6	

User8 can create NSGs in:

	▼
RG4 only	
RG4 and RG5 only	
RG4 and RG6 only	
RG4, RG5, and RG6	

Case Study (1 questions)

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.

Name	Type	Description
Group1	Security group	A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources.
Group2	Security group	A group that has the Dynamic User membership type and contains the Chicago IT team

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

Name	Type	Description
VNet1	Virtual network	VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet.
VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.
VM1	Virtual machine	VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subnet0.
SQLDB1	Azure SQL Database	SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1.
WebApp1	Web app	WebApp1 is an Azure web app that is accessible by using https://litwareinc.com and http://www.litwareinc.com .
Resource Group1	Resource group	Resource Group1 is a resource group that contains VNet1, VM0, and VM1.
Resource Group2	Resource group	Resource Group2 is a resource group that contains shared IT resources.

Azure Security Center is set to the Free tier.

Planned changes

Litware plans to deploy the Azure resources shown in the following table.

Name	Type	Description
Firewall1	Azure Firewall	An Azure firewall on VNet1.
RT1	Route table	A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0.
AKS1	Azure Kubernetes Service (AKS)	A managed AKS cluster

Identity and Access Requirements

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 able 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.

Data and Application Requirements

Litware identifies the following data and applications requirements:
The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials.
WebApp1 must enforce mutual authentication.

General Requirements

Litware identifies the following general requirements:
Whenever possible, administrative effort must be minimized.
Whenever possible, use of automation must be minimized.

Question 72

You need to ensure that you can meet the security operations requirements.

What should you do first?

- ☐ Turn on Auto Provisioning in Security Center.
- ☐ Integrate Security Center and Microsoft Cloud App Security.
- ☐ Upgrade the pricing tier of Security Center to Standard.
- ☐ Modify the Security Center workspace configuration.

(21 questions)

Question 73

You are troubleshooting a security issue for an Azure Storage account.

You enable the diagnostic logs for the storage account.

What should you use to retrieve the diagnostics logs?

- ☐ the Security & Compliance admin center
- ☐ SQL query editor in Azure
- ☐ File Explorer in Windows
- ☐ AzCopy

Question 74

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.

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

Question 75

You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

You are assigned the Global administrator role for the tenant. You are responsible for managing Azure Security Center settings.

You need to create a custom sensitivity label.

What should you do?

- ☐ Create a custom sensitive information type.
- ☐ Elevate access for global administrators in Azure AD.
- ☐ Change Azure Security Center to use Standard-tier pricing.
- ☐ Enable integration with Microsoft Cloud App Security.

Question 76

You have 10 virtual machines on a single subnet that has a single network security group (NSG).

You need to log the network traffic to an Azure Storage account.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- ☐ Install the Network Performance Monitor solution.
- ☐ Enable Azure Network Watcher.
- ☐ Enable diagnostic logging for the NSG.
- ☐ Enable NSG flow logs.
- ☐ Create an Azure Log Analytics workspace.

Question 77

You have an Azure subscription named Sub1 that contains an Azure Log Analytics workspace named LAW1.

You have 100 on-premises servers that run Windows Server 2012 R2 and Windows Server 2016. The servers connect to LAW1. LAW1 is configured to collect security-related performance counters from the connected servers.

You need to configure alerts based on the data collected by LAW1. The solution must meet the following requirements:

Alert rules must support dimensions.

The time it takes to generate an alert must be minimized.

Alert notifications must be generated only once when the alert is generated and once when the alert is resolved.

Which signal type should you use when you create the alert rules?

- ☐ Log
- ☐ Log (Saved Query)
- ☐ Metric
- ☐ Activity Log

Question 78

You company has an Azure Active Directory (Azure AD) tenant named contoso.com.

You plan to create several security alerts by using Azure Monitor.

You need to prepare the Azure subscription for the alerts.

What should you create first?

- ☐ An Azure Storage account
- ☐ an Azure Log Analytics workspace
- ☐ an Azure event hub
- ☐ an Azure Automation account

Question 79

You are troubleshooting a security issue for an Azure Storage account.

You enable the diagnostic logs for the storage account.

What should you use to retrieve the diagnostics logs?

- ☐ the Security & Compliance admin center
- ☐ Azure Security Center
- ☐ Azure Cosmos DB explorer
- ☐ AzCopy

Question 80

HOTSPOT

You are configuring just in time (JIT) VM access to a set of Azure virtual machines.

You need to grant users PowerShell access to the virtual machine by using JIT VM access.

What should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Permission that must be granted to users on VM:

	▼
Read	
Update	
View	
Write	

TCP port that must be allowed:

	▼
22	
25	
3389	
5986	

Question 81

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

Name	Resource group
VM1	RG1
VM2	RG2
VM3	RG1
VM4	RG2

You need to ensure that the virtual machines in RG1 have the Remote Desktop port closed until an authorized user requests access.

What should you configure?

- ☐ Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
- ☐ an application security group
- ☐ Azure Active Directory (Azure AD) conditional access
- ☐ just in time (JIT) VM access

Question 82

HOTSPOT

You plan to use Azure Monitor Logs to collect logs from 200 servers that run Windows Server 2016.

You need to automate the deployment of the Log Analytics Agent to all the servers by using an Azure Resource Manager template.

How should you complete the template? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

```
{
  "type" : "Microsoft.Compute/virtualMachines/extensions",
  "name" : "[concat(parameter('vmname'), /OMSExtension)]",
  "apiVersion" : "[variables('apiVersion')]",
  "location" : "[resourceGroup().location]",
  "dependsOn" : [
    "[concat('Microsoft.Compute/virtualMachines/', parameters('vmName'))]"
  ],
  "properties" : {
    "publisher" : "Microsoft.EnterpriseCloud.Monitoring",
    "type" : "MicrosoftMonitoringAgent",
    "typeHandlerVersion" : "1.0",
    "autoUpgradeMinorVersion" : true,
    "settings" : {
      "[variable('var1')]" : "[variable('var1')]"
      "AzureADApplicationID"
      "WorkspacelD"
      "WorkspaceName"
      "WorkspaceURL"
    },
    "protectedSettings" : {
      "[variable('var2')]" : "[variable('var2')]"
      "AzureADApplicationSecret"
      "StorageAccountKey"
      "WorkspacelD"
      "WorkspaceKey"
    }
  }
}
```

Question 83

DRAG DROP

You have an Azure subscription named Sub1 that contains an Azure Log Analytics workspace named LAW1.

You have 500 Azure virtual machines that run Windows Server 2016 and are enrolled in LAW1.

You plan to add the System Update Assessment solution to LAW1.

You need to ensure that System Update Assessment-related logs are uploaded to LAW1 from 100 of the virtual machines only.

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.

Actions

Create a new workspace.

Apply the scope configuration to the solution.

Create a scope configuration.

Create a computer group.

Create a data source.

Answer Area

Question 84

HOTSPOT

You suspect that users are attempting to sign in to resources to which they have no access.

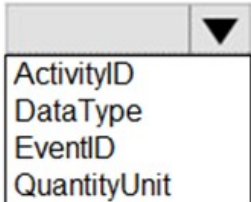
You need to create an Azure Log Analytics query to identify failed user sign-in attempts from the last three days. The results must only show users who had more than five failed sign-in attempts.

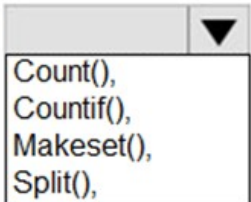
How should you configure the query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

```

let timeframe = 3d;
SecurityEvent
| where TimeGenerated > ago(3d)
| where AccountType == 'User' and  == 4625

| summarize failed_login_attempts= 

latest_failed_login=arg_max(TimeGenerated, Account) by Account
| where failed_login_attempts > 5

```

Question 85

HOTSPOT

You have an Azure subscription named Sub1. Sub1 has an Azure Storage account named Storage1 that contains the resources shown in the following table.

Name	Type
Container1	Blob container
Share1	File share

You generate a shared access signature (SAS) to connect to the blob service and the file service.

Which tool can you use to access the contents in Container1 and Share1 by using the SAS? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Tools for Container1:

	▼
Robocopy.exe	
Azure Storage Explorer	
File Explorer	

Tools for Share1:

	▼
Robocopy.exe	
Azure Storage Explorer	
File Explorer	

Question 86

You have an Azure Storage account named storage1 that has a container named container1.

You need to prevent the blobs in container1 from being modified.

What should you do?

- ☐ From container1, change the access level.
- ☐ From container1, add an access policy.
- ☐ From container1, modify the Access Control (IAM) settings.
- ☐ From storage1, enable soft delete for blobs.

Question 87

HOTSPOT

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

Name	Type	Region	Resource group
SQL1	Azure SQL database	East US	RG1
Analytics1	Azure Log Analytics workspace	East US	RG1
Analytics2	Azure Log Analytics workspace	East US	RG2
Analytics3	Azure Log Analytics workspace	West Europe	RG1

You create the Azure Storage accounts shown in the following table.

Name	Region	Resource group	Storage account type	Access tier (default)
Storage1	East US	RG1	Blob	Cool
Storage2	East US	RG2	General purpose V1	<i>Not applicable</i>
Storage3	West Europe	RG1	General purpose V2	Hot

You need to configure auditing for SQL1.

Which storage accounts and Log Analytics workspaces can you use as the audit log destination? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Storage accounts that can be used as the audit log destination:

▼

☐ Storage1 only
☐ Storage2 only
☐ Storage1 and Storage2 only
☐ Storage1, Storage2, and Storage3

Log Analytics workspaces that can be used as the audit log destination:

▼

☐ Analytics1 only
☐ Analytics1 and Analytics2 only
☐ Analytics1 and Analytics3 only
☐ Analytics1, Analytics2, and Analytics3

Question 88

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.

Settings**Answer Area**

Activity log

Logs

Metrics

Service Health

Identify the user who deleted a virtual machine three weeks ago:

Query the security events of a virtual machine that runs Windows Server 2016:

Question 89

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

Name	Operating system
VM1	Windows Server 2016
VM2	Ubuntu Server 18.04 LTS

From Azure Security Center, you turn on Auto Provisioning.

You deploy the virtual machines shown in the following table.

Name	Operating system
VM3	Windows Server 2016
VM4	Ubuntu Server 18.04 LTS

On which virtual machines is the Log Analytics agent installed?

- ☐ VM3 only
- ☐ VM1 and VM3 only
- ☐ VM3 and VM4 only
- ☐ VM1, VM2, VM3, and VM4

Question 90

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

Name	Operating system
VM1	Windows Server 2016
VM2	Ubuntu Server 18.04 LTS

From Azure Security Center, you turn on Auto Provisioning.

You deploy the virtual machines shown in the following table.

Name	Operating system
VM3	Windows Server 2016
VM4	Ubuntu Server 18.04 LTS

On which virtual machines is the Microsoft Monitoring agent installed?

- ☐ VM3 only
- ☐ VM1 and VM3 only
- ☐ VM3 and VM4 only
- ☐ VM1, VM2, VM3, and VM4

Question 91

HOTSPOT

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

Name	Type	Resource group
RG1	Resource group	<i>Not applicable</i>
VM1	Virtual machine	RG1
VM2	Virtual machine	RG1
ActionGroup1	Action group	RG1

VM1 and VM2 are stopped.

You create an alert rule that has the following settings:

Resource: RG1

Condition: All Administrative operations

Actions: Action groups configured for this alert rule: ActionGroup1

Alert rule name: Alert1

You create an action rule that has the following settings:

Scope: VM1

Filter criteria: Resource Type = "Virtual Machines"

Define on this scope: Suppression

Suppression config: From now (always)

Name: ActionRule1

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

Note: Each correct selection is worth one point.

Answer area

Statements	Yes	No
If you start VM1, an alert is triggered.	☐	☐
If you start VM2, an alert is triggered.	☐	☐
If you add a tag to RG1, an alert is triggered.	☐	☐

Question 92

You company has an Azure subscription named Sub1. Sub1 contains an Azure web app named WebApp1 that uses Azure Application Insights. WebApp1 requires users to authenticate by using OAuth 2.0 client secrets.

Developers at the company plan to create a multi-step web test app that preforms synthetic transactions emulating user traffic to Web App1.

You need to ensure that web tests can run unattended.

What should you do first?

- ☐ In Microsoft Visual Studio, modify the .webtest file.
- ☐ Upload the .webtest file to Application Insights.
- ☐ Register the web test app in Azure AD.
- ☐ Add a plug-in to the web test app.

Question 93

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?

- ☐ Azure DevOps
- ☐ Azure Application Insights
- ☐ Azure Monitor
- ☐ Azure Logic Apps Designer

Secure data and applications

Case Study (3 questions)

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.

Name	Type	Description
Group1	Security group	A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources.
Group2	Security group	A group that has the Dynamic User membership type and contains the Chicago IT team

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

Name	Type	Description
VNet1	Virtual network	VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet.
VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.
VM1	Virtual machine	VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subnet0.
SQLDB1	Azure SQL Database	SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1.
WebApp1	Web app	WebApp1 is an Azure web app that is accessible by using https://litwareinc.com and http://www.litwareinc.com .
Resource Group1	Resource group	Resource Group1 is a resource group that contains VNet1, VM0, and VM1.
Resource Group2	Resource group	Resource Group2 is a resource group that contains shared IT resources.

Azure Security Center is set to the Free tier.

Planned changes

Litware plans to deploy the Azure resources shown in the following table.

Name	Type	Description
Firewall1	Azure Firewall	An Azure firewall on VNet1.
RT1	Route table	A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0.
AKS1	Azure Kubernetes Service (AKS)	A managed AKS cluster

Identity and Access Requirements

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 able 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.

Data and Application Requirements

Litware identifies the following data and applications requirements:

The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials.

WebApp1 must enforce mutual authentication.

General Requirements

Litware identifies the following general requirements:

Whenever possible, administrative effort must be minimized.

Whenever possible, use of automation must be minimized.

Question 94

DRAG DROP

You need to configure SQLDB1 to meet the data and application requirements.

Which three actions should you recommend be performed in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions**Answer Area**

From the Azure portal, create an Azure AD administrator for LitwareSQLServer1.

In SQLDB1, create contained database users.

Connect to SQLDB1 by using Microsoft SQL Server Management Studio (SSMS).

In Azure AD, create a system-assigned managed identity.

In Azure AD, create a user-assigned managed identity.



Question 95

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.

Answer Area

```
{
  "Name": "Role1",
  "Id": "11111111-1111-1111-1111-111111111111",
  "IsCustom" : true,
  "Description": "VM storage operator"
  "Actions" : [
    [
      "Microsoft.Compute/",
      "Microsoft.Resources/",
      "Microsoft.Storage/"
    ],
    [
      "disks/*",
      "storageAccounts/*",
      "virtualMachines/disks/*",
    ],
  ],
  "NotActions": [
    ],
  "AssignableScopes" : [
    [
      "/"
      "/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4/resourceGroups/Resource Group1"
      "/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4"
    ]
  ]
}
```

Question 96

You need to configure WebApp1 to meet the data and application requirements.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- ☐ Upload a public certificate.
- ☐ Turn on the HTTPS Only protocol setting.
- ☐ Set the Minimum TLS Version protocol setting to 1.2.
- ☐ Change the pricing tier of the App Service plan.
- ☐ Turn on the Incoming client certificates protocol setting.

(21 questions)

Question 97

HOTSPOT

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

Name	Type
User1	Azure Active Directory (Azure AD) user
User2	Azure Active Directory (Azure AD) user
Group1	Azure Active Directory (Azure AD) group
Vault1	Azure key vault

User1 is a member of Group1. Group1 and User2 are assigned the Key Vault Contributor role for Vault1.

On January 1, 2019, you create a secret in Vault1. The secret is configured as shown in the exhibit.
(Click the Exhibit tab.)

Create a secret

Upload options

Manual

* Name 

Password1

* Value

• • • • • • • • • •

Content type (optional)

Set activation date?  ☒

Activation Date

2019-03-01



12:00:00 AM

(UTC+02:00) --- Current Time Zone ---

Set expiration Date?  ☒

Expiration Date

2020-03-01



12:00:00 AM

(UTC+02:00) --- Current Time Zone ---

Enabled?

Yes

No

User2 is assigned an access policy to Vault1. The policy has the following configurations:

Key Management Operations: Get, List, and Restore

Cryptographic Operations: Decrypt and Unwrap Key

Secret Management Operations: Get, List, and Restore

Group1 is assigned an access to Vault1. The policy has the following configurations:

Key Management Operations: Get and Recover

Secret Management Operations: List, Backup, and Recover

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

Answer Area

	Statements	Yes	No
	On January 1, 2019, User1 can view the value of Password1.	☐	☐
	On June 1, 2019, User2 can view the value of Password1.	☐	☐
	On June 1, 2019, User1 can view the value of Password1.	☐	☐

Question 98

You have an Azure subscription that contains a virtual machine named VM1.

You create an Azure key vault that has the following configurations:

Name: Vault5

Region: West US

Resource group: RG1

You need to use Vault5 to enable Azure Disk Encryption on VM1. The solution must support backing up VM1 by using Azure Backup.

Which key vault settings should you configure?

- ☐ Access policies
- ☐ Secrets
- ☐ Keys
- ☐ Locks

Question 99

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?

- ☐ branch folders
- ☐ branch permissions
- ☐ branch policies
- ☐ branch locking

Question 100

Your company has an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

The company develops an application named App1. App1 is registered in Azure AD.

You need to ensure that App1 can access secrets in Azure Key Vault on behalf of the application users.

What should you configure?

- ☐ an application permission without admin consent
- ☐ a delegated permission without admin consent
- ☐ a delegated permission that requires admin consent
- ☐ an application permission that requires admin consent

Question 101

HOTSPOT

You have an Azure Active Directory (Azure AD) tenant named contoso1812.onmicrosoft.com that contains the users shown in the following table.

Name	Username	Type
User1	User1@contoso1812.onmicrosoft.com	Member
User2	User2@contoso1812.onmicrosoft.com	Member
User3	User3@contoso1812.onmicrosoft.com	Member
User4	User4@outlook.com	Guest

You create an Azure Information Protection label named Label1. The Protection settings for Label1 are configured as shown in the exhibit. (Click the Exhibit tab.)

Protection

Contoso1812 - Azure Information Protection

Protections settings ⓘ

Azure (cloud key)

HYOK (AD RMS)

Select the protection action type ⓘ

- ☒ Set permissions
- ☐ Set user-defined permissions (Preview)

USERS**PERMISSIONS****AuthenticatedUsers****Viewer****User1@contoso1812.onmicrosoft.com****Co-Author****User2@contoso1812.onmicrosoft.com****Reviewer**[+Add permissions](#)

Label1 is applied to a file named File1.

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can print File1.	☐	☐
User3 can read File1.	☐	☐
User4 can print File1.	☐	☐

Question 102

HOTSPOT

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

Name	Use condition	Label is applied	Pattern	Case sensitivity
Label1	Condition1	Automatically	White	On
Label2	Condition2	Automatically	Black	Off

You have the Azure Information Protection policies as shown in the following table.

Name	Applies to	Use label	Set the default label
Global	<i>Not applicable</i>	<i>None</i>	None
Policy1	User1	Label1	None
Policy2	User1	Label2	None

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.

Answer Area

If User1 creates a Microsoft Word file that includes the text "Black and White", the file will be assigned:

▼

No label

Label1 only

Label2 only

Label1 and Label2

If User1 creates a Microsoft Notepad file that includes the text "Black or white", the file will be assigned:

▼

No label

Label1 only

Label2 only

Label1 and Label2

Question 103

You have an Azure web app named webapp1.

You need to configure continuous deployment for webapp1 by using an Azure Repo.

What should you create first?

- ☐ an Azure Application Insights service
- ☐ an Azure DevOps organization
- ☐ an Azure Storage account
- ☐ an Azure DevTest Labs lab

Question 104

You have an Azure subscription that contains an Azure key vault named Vault1.

In Vault1, you create a secret named Secret1.

An application developer registers an application in Azure Active Directory (Azure AD).

You need to ensure that the application can use Secret1.

What should you do?

- ☐ In Azure AD, create a role.
- ☐ In Azure Key Vault, create a key.
- ☐ In Azure Key Vault, create an access policy.
- ☐ In Azure AD, enable Azure AD Application Proxy.

Question 105

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.

Answer Area

```
New-AzKeyVault -VaultName 'KeyVault1' -ResourceGroupName 'RG1'
```

```
-Location 'East US'
```

	▼
-EnabledForDeployment	
-EnablePurgeProtection	
-Tag	

	▼
-Confirm	
-DefaultProfile	
-EnableSoftDelete	
-SKU	

Question 106

DRAG DROP

Your company has an Azure Active Directory (Azure AD) tenant named contoso.com.

The company is developing an application named App1. App1 will run as a service on server that runs Windows Server 2016. App1 will authenticate to contoso.com and access Microsoft Graph to read directory data.

You need to delegate the minimum required permissions to App1.

Which three actions should you perform in sequence from the Azure portal? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions**Answer Area**

Question 107

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.

Name	Type	Description
CosmosDBAccount1	Azure Cosmos DB account	A Cosmos DB account containing a database Named CosmosDB1 that serves as a back-end tier of the application
WebApp1	Azure web app	A web app configured to serve as the middle tier of the application

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.

Answer Area

CosmosDB1: ▼

- Authenticate Azure AD users and generate resource tokens.
- Authenticate Azure AD users and relay resource tokens.
- Create database users and generate resource tokens.

WebApp1: ▼

- Authenticate Azure AD users and generate resource tokens.
- Authenticate Azure AD users and relay resource tokens.
- Create database users and generate resource tokens.

Question 108

DRAG DROP

You have an Azure subscription named Sub1. Sub1 contains an Azure virtual machine named VM1 that runs Windows Server 2016.

You need to encrypt VM1 disks by using Azure Disk Encryption.

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.

Actions	Answer Area
Run Set -AzStorageAccount.	
Create an Azure key vault.	
Configure access policies for the Azure key vault.	
Configure secrets for the Azure key vault.	
Run Set -AzVMDiskEncryptionExtension.	

Question 109

Your company has an Azure subscription named Sub1 that is associated to an Azure Active Directory Azure (Azure AD) tenant named contoso.com.

The company develops a mobile application named App1. App1 uses the OAuth 2 implicit grant type to acquire Azure AD access tokens.

You need to register App1 in Azure AD.

What information should you obtain from the developer to register the application?

- ☐ a redirect URI
- ☐ a reply URL
- ☐ a key
- ☐ an application ID

Question 110

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 stored access policy
- ☐ a shared access signature (SAS)
- ☐ the column encryption key
- ☐ user credentials
- ☐ the column master key

Question 111

You have a hybrid configuration of Azure Active Directory (Azure AD).

All users have computers that run Windows 10 and are hybrid Azure AD joined.

You have an Azure SQL database that is configured to support Azure AD authentication.

Database developers must connect to the SQL database by using Microsoft SQL Server Management Studio (SSMS) and authenticate by using their on-premises Active Directory account.

You need to tell the developers which authentication method to use to connect to the SQL database from SSMS. The solution must minimize authentication prompts.

Which authentication method should you instruct the developers to use?

- ☐ SQL Login
- ☐ Active Directory – Universal with MFA support
- ☐ Active Directory – Integrated
- ☐ Active Directory – Password

Question 112

You have an Azure subscription named Sub1 that contains the Azure key vaults shown in the following table:

Name	Region	Resource group
Vault1	West Europe	RG1
Vault2	East US	RG1
Vault3	West Europe	RG2
Vault4	East US	RG2

In Sub1, you create a virtual machine that has the following configurations:

Name: VM1

Size: DS2v2

Resource group: RG1

Region: West Europe

Operating system: Windows Server 2016

You plan to enable Azure Disk Encryption on VM1.

In which key vaults can you store the encryption key for VM1?

- ☐ Vault1 or Vault3 only
- ☐ Vault1, Vault2, Vault3, or Vault4
- ☐ Vault1 only
- ☐ Vault1 or Vault2 only

Question 113

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

Name	Type	Region	Resource group
Sa1	Azure Storage account	East US	RG1
VM1	Azure virtual machine	East US	RG2
KV1	Azure key vault	East US 2	RG1
SQL1	Azure SQL database	East US 2	RG2

You need to ensure that you can provide VM1 with secure access to a database on SQL1 by using a contained database user.

What should you do?

- ☐ Enable a managed service identity on VM1.
- ☐ Create a secret in KV1.
- ☐ Configure a service endpoint on SQL1.
- ☐ Create a key in KV1.

Question 114

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?

- ☐ AuditIfNotExist
- ☐ Append
- ☐ DeployIfNotExist
- ☐ Deny

Question 115

You have an Azure SQL Database server named SQL1.

You turn on Advanced Threat Protection for SQL1 to detect all threat detection types.

Which action will Advanced Threat Protection detect as a threat?

- ☐ A user updates more than 50 percent of the records in a table.
- ☐ A user attempts to sign in as `SELECT * FROM table1`.
- ☐ A user is added to the `db_owner` database role.
- ☐ A user deletes more than 100 records from the same table.

Question 116**HOTSPOT**

You have an Azure subscription that contains an Azure key vault named Vault1.

On January 1, 2019, Vault1 stores the following secrets.

```
Enabled      : False
Expires      :
NotBefore    : 5/1/19 12:00:00 AM
Created      : 12/20/18 2:55:00 PM
Updated      : 12/20/18 2:55:00 PM
ContentType  :
Tags         :
TagTable     :
VaultName    : vault1
Name         : Password1
Version      :
Id           : https://vault1.vault.azure.net:443/secrets/Password1
```

```
Enabled      : True
Expires      : 5/1/19 12:00:00 AM
NotBefore    : 3/1/19 12:00:00 AM
Created      : 12/20/18 3:00:00 PM
Updated      : 12/20/18 3:00:00 PM
ContentType  :
Tags         :
TagsTable    :
VaultName    : vault1
Name         : Password2
Version      :
Id           : https://vault1.vault.azure.net:443/secrets/Password2
```

Which can each secret be used by an application? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Password1: ▼

Never

Always

Only after May 1, 2019

Password2: ▼

Never

Always

Only between March 1, 2019 and May 1. 2019

Question 117

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.

Actions

Run Set-AzureRmKeyVaultAccessPolicy

Create an Azure Automation account.

Import PowerShell modules to the Azure Automation account.

Create a user-assigned managed identity.

Create a connection resource in the Azure Automation account.

Answer Area