Number: AZ-500
Passing Score: 800
Time Limit: 120 min

**AZ-500**



**Website:** https://vceplus.com
**VCE to PDF Converter:** https://vceplus.com/vce-to-pdf/
**Facebook:** https://www.facebook.com/VCE.For.All.VN/
**Twitter :** https://twitter.com/VCE_Plus

https://www.vceplus.com/

**Microsoft Azure Security Technologies (beta)**

**Question Set 1**

**QUESTION 1**
**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?

A.  Yes
B.  No

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:
To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately effects all of the shared access signatures associated with it.

References: https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy

**QUESTION 2**

**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 (AzureAD).

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?

A. Yes
B. No

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:
Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.

Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions: ▪
Create Azure Virtual Network.
▪ Create a custom DNS server in the Azure Virtual Network.

▪ Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.
▪ Configure forwarding between the custom DNS server and your on-premises DNS server.

References: https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network **QUESTION 3**
**Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.**

**After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.**

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

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?

A. Yes
B. No

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:
You can connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.

Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions: ▪
Create Azure Virtual Network.
▪ Create a custom DNS server in the Azure Virtual Network.
▪ Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.
▪ Configure forwarding between the custom DNS server and your on-premises DNS server.

References: https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network

**QUESTION 4**
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?

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

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:
Password hash synchronization requires the least effort regarding deployment, maintenance, and infrastructure. This level of effort typically applies to organizations that only need their users to sign in to Office 365, SaaS apps, and other Azure AD-based resources. When turned on, password hash synchronization is part of the Azure AD Connect sync process and runs every two minutes.

Incorrect Answers:
A: A federated authentication system relies on an external trusted system to authenticate users. Some companies want to reuse their existing federated system investment with their Azure AD hybrid identity solution. The maintenance and management of the federated system falls outside the control of Azure AD. It's up to the organization by using the federated system to make sure it's deployed securely and can handle the authentication load.

C: For pass-through authentication, you need one or more (we recommend three) lightweight agents installed on existing servers. These agents must have access to your on-premises Active Directory Domain Services, including your on-premises AD domain controllers. They need outbound access to the Internet and access to your domain controllers. For this reason, it's not supported to deploy the agents in a perimeter network.

Pass-through Authentication requires unconstrained network access to domain controllers. All network traffic is encrypted and limited to authentication requests.

References: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

**QUESTION 5**
Your network contains an on-premises Active Directory domain named corp.contoso.com.

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

You sync all on-premises identities to Azure AD.

You need to prevent users who have a `givenName` attribute that starts with `TEST` from being synced to Azure AD. The solution must minimize administrative effort.

What should you use?

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

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:
Use the Synchronization Rules Editor and write attribute-based filtering rule.

References: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration

**QUESTION 6**
Your company plans to create separate subscriptions for each department. Each subscription will be associated to the same Azure Active Directory (Azure AD) tenant.

You need to configure each subscription to have the same role assignments.

What should you use?

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

**Correct Answer:** C
**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:
The Azure AD Privileged Identity Management (PIM) service also allows Privileged Role Administrators to make permanent admin role assignments.

References:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-add-role-to-user

**Testlet 1**

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question on this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next sections of the exam. After you begin a new section, you cannot return to this section.

**To start the case study**

To display the first question on this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question. **Overview**

Litware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.

**Existing Environment**

Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.

Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the Litware employees and their devices. Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.

The tenant contains the groups shown in the following table.

| 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 Subent0. |
| 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 |

Litware identifies the following identity and access requirements:

▪ All San Francisco users and their devices must be members of Group1.
▪ The members of Group2 must be assigned the Contributor role to Resource Group2 by using a permanent eligible assignment.
▪ Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the users' behalf.

**Platform Protection Requirements**

Litware identifies the following platform protection requirements:

▪ Microsoft Antimalware must be installed on the virtual machines in Resource Group1.
▪ The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.
▪ Azure AD users must be to authenticate to AKS1 by using their Azure AD credentials.
▪ Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.
▪ A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in Resource Group1. Role1 must be available only for Resource Group1.

**Security Operations Requirements**

Litware must be able to customize the operating system security configurations in Azure Security Center.

**QUESTION 1**
You need to ensure that users can access VM0. The solution must meet the platform protection requirements.

What should you do?

A. Move VM0 to Subnet1.
B. On Firewall, configure a network traffic filtering rule.
C. Assign RT1 to AzureFirewallSubnet.
D. On Firewall, configure a DNAT rule.

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:
Azure Firewall has the following known issue:
Conflict with Azure Security Center (ASC) Just-in-Time (JIT) feature.

If a virtual machine is accessed using JIT, and is in a subnet with a user-defined route that points to Azure Firewall as a default gateway, ASC JIT doesn't work. This is a result of asymmetric routing – a packet comes in via the virtual machine public IP (JIT opened the access), but the return path is via the firewall, which drops the packet because there is no established session on the firewall.

Solution: To work around this issue, place the JIT virtual machines on a separate subnet that doesn't have a user-defined route to the firewall.

Scenario:

| | | |
|---|---|---|
| | | 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. |

Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.

| 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. |

References:
https://docs.microsoft.com/en-us/azure/firewall/overview

**Question Set 2**

**QUESTION 1**
You have Azure Resource Manager templates that you use to deploy Azure virtual machines.

You need to disable unused Windows features automatically as instances of the virtual machines are provisioned.

What should you use?

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

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:
You can use Azure Automation State Configuration to manage Azure VMs (both Classic and Resource Manager), on-premises VMs, Linux machines, AWS VMs, and on-premises physical machines.

Note: Azure Automation State Configuration provides a DSC pull server similar to the Windows Feature DSC-Service so that target nodes automatically receive configurations, conform to the desired state, and report back on their compliance. The built-in pull server in Azure Automation eliminates the need to set up and maintain your own pull server. Azure Automation can target virtual or physical Windows or Linux machines, in the cloud or on-premises.

References: https://docs.microsoft.com/en-us/azure/automation/automation-dsc-getting-started

**QUESTION 2** 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.

**Hot Area:**

```
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",
      "roleDefinitionIds" : [
      "/providers/microsoft.authorization/roleDefinitions/12345678-1234-5678-abcd-012345678910"
      ],
      "name" : "customExtension",
      "deployment" : {
          "properties" : {
      "mode": "incremental",
      "parameters" : {
      },
      "[      ▼    ]": [
```

| existenceCondition |
| resources |
| template |

```
      ]
      }
      }
    }
  }
}
```

**Correct Answer:**

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
        ]
      }
    }
  }
}
```

**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:

Box 1: DeployIfNotExists
DeployIfNotExists executes a template deployment when the condition is met.

Box 2: Template

The details property of the DeployIfNotExists effects has all the subproperties that define the related resources to match and the template deployment to execute.
Deployment [required]

This property should include the full template deployment as it would be passed to the Microsoft.Resources/deployment

References: https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects

## QUESTION 3

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

You need to use the auto-generated service principal to authenticate to the Azure Container Registry.

What should you create?

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

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:
When you create an AKS cluster, Azure also creates a service principal to support cluster operability with other Azure resources. You can use this auto-generated service principal for authentication with an ACR registry. To do so, you need to create an Azure AD role assignment that grants the cluster's service principal access to the container registry.

References: https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-auth-aks

## QUESTION 4

You have an 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?

A. VM1 only

B. VM1, VM2, and VM3 only

C. VM1, VM2, VM3, and VM4

D. VM1 and VM4 only

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:
Note: Create a workspace
▪ In the Azure portal, click All services. In the list of resources, type Log Analytics. As you begin typing, the list filters based on your input. Select Log Analytics. ▪ Click Create, and then select choices for the following items:

Provide a name for the new Log Analytics workspace, such as DefaultLAWorkspace. OMS workspaces are now referred to as Log Analytics workspaces.

Select a Subscription to link to by selecting from the drop-down list if the default selected is not appropriate.

For Resource Group, select an existing resource group that contains one or more Azure virtual machines.

Select the Location your VMs are deployed to. For additional information, see which regions Log Analytics is available in.

Incorrect Answers:

B, C: A Log Analytics workspace provides a geographic location for data storage. VM2 and VM3 are at a different location.

D: VM4 is a different resource group.

References: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/manage-access

**Testlet 1**

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question on this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next sections of the exam. After you begin a new section, you cannot return to this section.

**To start the case study**
To display the first question on this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question. **Overview**

Litware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.

**Existing Environment**

Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.

Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the Litware employees and their devices. Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.

The tenant contains the groups shown in the following table.

| 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 Subent0. |
| 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 |

Litware identifies the following identity and access requirements:

- All San Francisco users and their devices must be members of Group1.
- The members of Group2 must be assigned the Contributor role to Resource Group2 by using a permanent eligible assignment.
- Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the users' behalf.

**Platform Protection Requirements**

Litware identifies the following platform protection requirements:

- Microsoft Antimalware must be installed on the virtual machines in Resource Group1.
- The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.
- Azure AD users must be to authenticate to AKS1 by using their Azure AD credentials.
- Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.
- A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in Resource Group1. Role1 must be available only for Resource Group1.

**Security Operations Requirements**

Litware must be able to customize the operating system security configurations in Azure Security Center.

**QUESTION 1**
You need to ensure that you can meet the security operations requirements.

What should you do first?

A. Turn on Auto Provisioning in Security Center.
B. Integrate Security Center and Microsoft Cloud App Security.
C. Upgrade the pricing tier of Security Center to Standard.
D. Modify the Security Center workspace configuration.

**Correct Answer:** C
**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:
The Standard tier extends the capabilities of the Free tier to workloads running in private and other public clouds, providing unified security management and threat protection across your hybrid cloud workloads. The Standard tier also adds advanced threat detection capabilities, which uses built-in behavioral analytics and machine learning to identify attacks and zero-day exploits, access and application controls to reduce exposure to network attacks and malware, and more.

Scenario: Security Operations Requirements

Litware must be able to customize the operating system security configurations in Azure Security Center.

References:
https://docs.microsoft.com/en-us/azure/security-center/security-center-pricing

**Question Set 2**

**QUESTION 1**
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 first?

A. Create a custom sensitive information type.
B. Elevate access for global administrators in Azure AD.
C. Upgrade the pricing tier of the Security Center to Standard.
D. Enable integration with Microsoft Cloud App Security.

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:
First, you need to create a new sensitive information type because you can't directly modify the default rules.

References: https://docs.microsoft.com/en-us/office365/securitycompliance/customize-a-built-in-sensitive-information-type

**QUESTION 2** 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.

**Hot Area:**

## Answer Area

```
let timeframe = 3d;
SecurityEvent
| where TimeGenerated > ago(3d)
| where AcccountType == 'User' and ▼ ==4625
                                    ActivityID
                                    DataType
                                    EventID
                                    QuantityUnit

| Summarie failed_login_attempts= ▼
                                    Count(),
                                    Countif(),
                                    Makeset(),
                                    Split(),

    latest_failed_login=arg_max(TimeGenerated by Account
| where failed login attempts > 5
```

**Correct Answer:**

## Answer Area

```
let timeframe = 3d;
SecurityEvent
| where TimeGenerated > ago(3d)
| where AcccountType == 'User' and [_____ ▼] ==4625
```

| ActivityID |
| DataType |
| **EventID** |
| QuantityUnit |

```
| Summarie failed_login_attempts= [_____ ▼]
```

| **Count(),** |
| Countif(), |
| Makeset(), |
| Split(), |

```
            latest_failed_login=arg_max(TimeGenerated by Account
| where failed login attempts > 5
```

**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:

The following example identifies user accounts that failed to log in more than five times in the last day, and when they last attempted to log in.

let timeframe = 1d;
SecurityEvent
| where TimeGenerated > ago(1d)
| where AccountType == 'User' and EventID == 4625 // 4625 - failed log in
| summarize failed_login_attempts=count(), latest_failed_login=arg_max(TimeGenerated, Account) by Account
| where failed_login_attempts > 5

| project-away Account1

References: https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/examples

**QUESTION 3**
You have an Azure subscription named Sub1.

In Azure Security Center, you have a security playbook named Play1. Play1 is configured to send an email message to a user named User1.

You need to modify Play1 to send email messages to a distribution group named Alerts.

What should you use to modify Play1?

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

**Correct Answer:** D
**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:
You can change an existing playbook in Security Center to add an action, or conditions. To do that you just need to click on the name of the playbook that you want to change, in the Playbooks tab, and Logic App Designer opens up.

References: https://docs.microsoft.com/en-us/azure/security-center/security-center-playbooks

**QUESTION 4**
You create a new Azure subscription.

You need to ensure that you can create custom alert rules in Azure Security Center.

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

**NOTE:** Each correct selection is worth one point.

A. Onboard Azure Active Directory (Azure AD) Identity Protection.

B. Create an Azure Storage account.
C. Implement Azure Advisor recommendations.
D. Create an Azure Log Analytics workspace.
E. Upgrade the pricing tier of Security Center to Standard.

**Correct Answer:** BD
**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:
D: You need write permission in the workspace that you select to store your custom alert.

References: https://docs.microsoft.com/en-us/azure/security-center/security-center-custom-alert

**QUESTION 5**
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?

A. Log
B. Log (Saved Query)
C. Metric
D. Activity Log

**Correct Answer:** C

**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:
Metric alerts in Azure Monitor provide a way to get notified when one of your metrics cross a threshold. Metric alerts work on a range of multi-dimensional platform metrics, custom metrics, Application Insights standard and custom metrics.

Note: Signals are emitted by the target resource and can be of several types. Metric, Activity log, Application Insights, and Log.

References:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-metric

**Testlet 1**

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question on this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next sections of the exam. After you begin a new section, you cannot return to this section.

**To start the case study**
To display the first question on this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question. **Overview**

Litware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.

**Existing Environment**

Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.

Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the Litware employees and their devices. Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.

The tenant contains the groups shown in the following table.

| 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 Subent0. |
| 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 |

Litware identifies the following identity and access requirements:

▪ All San Francisco users and their devices must be members of Group1.
▪ The members of Group2 must be assigned the Contributor role to Resource Group2 by using a permanent eligible assignment.
▪ Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the users' behalf.

**Platform Protection Requirements**

Litware identifies the following platform protection requirements:

▪ Microsoft Antimalware must be installed on the virtual machines in Resource Group1.
▪ The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.
▪ Azure AD users must be to authenticate to AKS1 by using their Azure AD credentials.
▪ Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.
▪ A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in Resource Group1. Role1 must be available only for Resource Group1.

**Security Operations Requirements**

Litware must be able to customize the operating system security configurations in Azure Security Center.

**QUESTION 1**
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.

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

**Correct Answer:** AC
**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:
A: To configure Certificates for use in Azure Websites Applications you need to upload a public Certificate.

C: Over time, multiple versions of TLS have been released to mitigate different vulnerabilities. TLS 1.2 is the most current version available for apps running on Azure App Service.

Incorrect Answers:
B: We need support the http url as well.

Note:

WebApp1 is an Azure web app that is
accessible by using https://litwareinc.com
and http://www.litwareinc.com.

**Question Set 2**

## QUESTION 1
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?

A.  an application permission without admin consent
B.  a delegated permission without admin consent
C.  a delegated permission that requires admin consent
D.  an application permission that requires admin consent

**Correct Answer:** B
**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:
Delegated permissions - Your client application needs to access the web API as the signed-in user, but with access limited by the selected permission. This type of permission can be granted by a user unless the permission requires administrator consent.

Incorrect Answers:
A, D: Application permissions - Your client application needs to access the web API directly as itself (no user context). This type of permission requires administrator consent and is also not available for public (desktop and mobile) client applications.

References: https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-access-web-apis

## QUESTION 2
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. a redirect URI
B. a reply URL
C. a key
D. an application ID

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:
For Native Applications you need to provide a Redirect URI, which Azure AD will use to return token responses.

References: https://docs.microsoft.com/en-us/azure/active-directory/develop/v1-protocols-oauth-code

**QUESTION 3**
From the Azure portal, you are configuring an Azure policy.

You plan to assign policies that use the `DeployIfNotExist`, `AuditIfNotExist`, `Append`, and `Deny` effects.

Which effect requires a managed identity for the assignment?

A. `AuditIfNotExist`

B. `Append`

C. `DeployIfNotExist`

D. `Deny`

**Correct Answer:** C
**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:

When Azure Policy runs the template in the deployIfNotExists policy definition, it does so using a managed identity.

References: https://docs.microsoft.com/bs-latn-ba/azure/governance/policy/how-to/remediate-resources

**QUESTION 4**
HOTSPOT

You need to create an Azure key vault. The solution must ensure that any object deleted from the key vault be retained for 90 days.

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

**NOTE:** Each correct selection is worth one point.

**Hot Area:**

## Answer Area

New-AzureRmKeyVault  -VaultName 'KeyVault1' -ResourceGroupName 'RG1'

-Location 'East US'

| -EnabledForDeployment |
| -EnablePurgeProtection |
| -Tag |

| -Confirm |
| -DefaultProfile |
| -EnableSoftDelete |
| -SKU |

**Correct Answer:**

## Answer Area

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

    -Location 'East US'  [ ▼ ]              [ ▼ ]
                         -EnabledForDeployment    -Confirm
                         -EnablePurgeProtection   -DefaultProfile
                         -Tag                     -EnableSoftDelete
                                                  -SKU
```
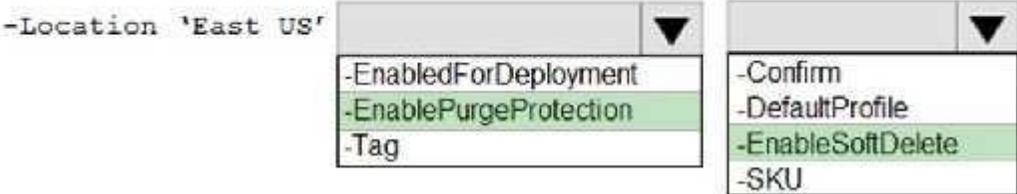
**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:

Box 1: -EnablePurgeProtection
If specified, protection against immediate deletion is enabled for this vault; requires soft delete to be enabled as well.

Box 2: -EnableSoftDelete
Specifies that the soft-delete functionality is enabled for this key vault. When soft-delete is enabled, for a grace period, you can recover this key vault and its contents after it is deleted.

References: https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/new-azurermkeyvault

**QUESTION 5**
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?

A. In Azure AD, create a role.
B. In Azure Key Vault, create a key.
C. In Azure Key Vault, create an access policy.
D. In Azure AD, enable Azure AD Application Proxy.

**Correct Answer:** A
**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:
Azure Key Vault provides a way to securely store credentials and other keys and secrets, but your code needs to authenticate to Key Vault to retrieve them. Managed identities for Azure resources overview makes solving this problem simpler, by giving Azure services an automatically managed identity in Azure Active Directory (Azure AD). You can use this identity to authenticate to any service that supports Azure AD authentication, including Key Vault, without having any credentials in your code.

Example: How a system-assigned managed identity works with an Azure VM
After the VM has an identity, use the service principal information to grant the VM access to Azure resources. To call Azure Resource Manager, use role-based access control (RBAC) in Azure AD to assign the appropriate role to the VM service principal. To call Key Vault, grant your code access to the specific secret or key in Key Vault.

References: https://docs.microsoft.com/en-us/azure/key-vault/quick-create-net

https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-

resources/overview

**QUESTION 6**
You have an Azure SQL database.

You implement Always Encrypted.

You need to ensure that application developers can retrieve and decrypt data in the database.

Which two pieces of information should you provide to the developers? Each correct answer presents part of the solution.

**NOTE:** Each correct selection is worth one point.

A. a stored access policy
B. a shared access signature (SAS)

C. the column encryption key

D. user credentials

E. the column master key

**Correct Answer:** CE
**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:
Always Encrypted uses two types of keys: column encryption keys and column master keys. A column encryption key is used to encrypt data in an encrypted column. A column master key is a key-protecting key that encrypts one or more column encryption keys.

References: https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine

**QUESTION 7**
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?

A. SQL Login

B. Active Directory – Universal with MFA support

C. Active Directory – Integrated

D. Active Directory – Password

**Correct Answer:** C
**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:
Azure AD can be the initial Azure AD managed domain. Azure AD can also be an on-premises Active Directory Domain Services that is federated with the Azure AD.

Using an Azure AD identity to connect using SSMS or SSDT
The following procedures show you how to connect to a SQL database with an Azure AD identity using SQL Server Management Studio or SQL Server Database Tools.

Active Directory integrated authentication
Use this method if you are logged in to Windows using your Azure Active Directory credentials from a federated domain.

1. Start Management Studio or Data Tools and in the Connect to Server (or Connect to Database Engine) dialog box, in the Authentication box, select Active Directory - Integrated. No password is needed or can be entered because your existing credentials will be presented for the connection.
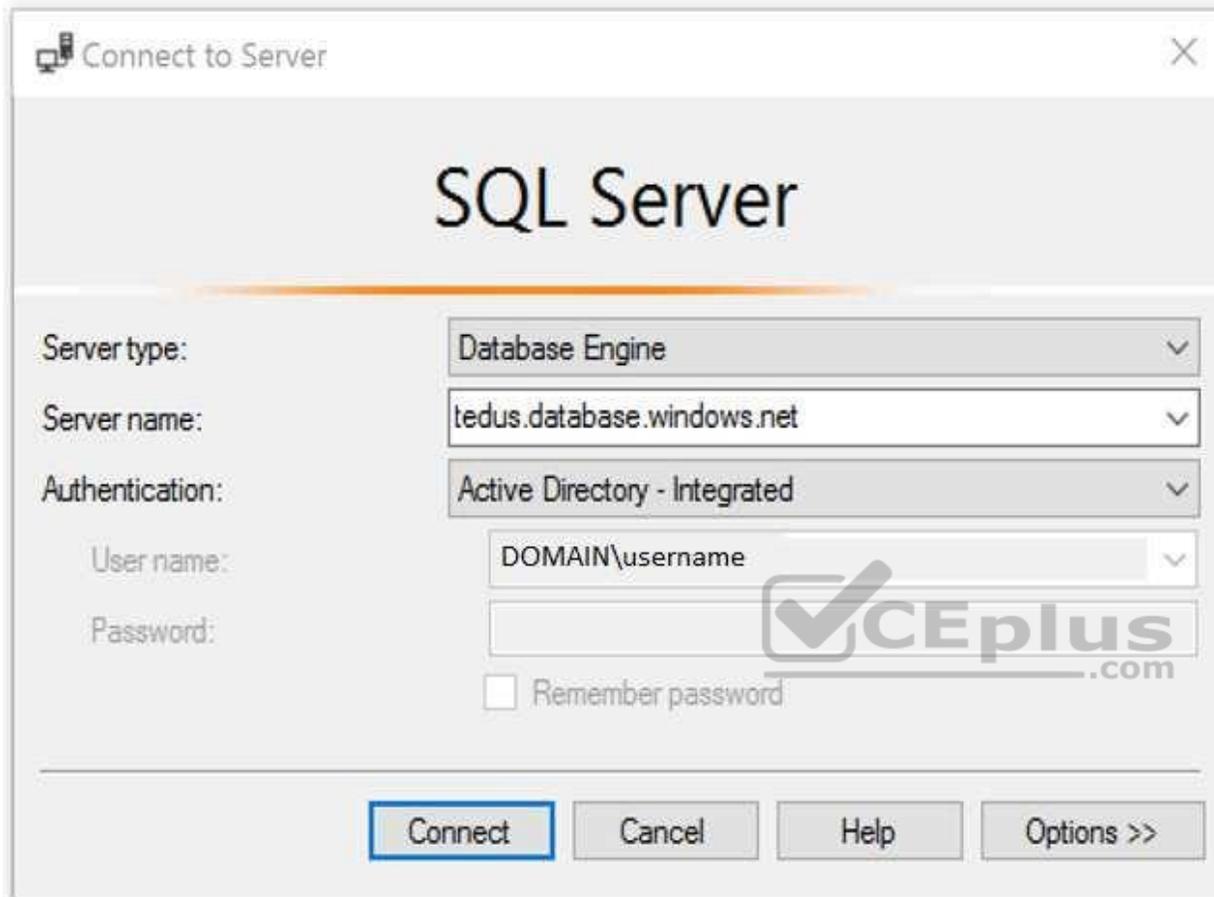
2.      Select the Options button, and on the Connection Properties page, in the Connect to database box, type the name of the user database you want to connect to. (The AD domain name or tenant ID" option is only supported for Universal with MFA connection options, otherwise it is greyed out.)

References: https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/sql-database/sql-database-aad-authentication-configure.md

**QUESTION 8**
Your company uses Azure DevOps.

You need to recommend a method to validate whether the code meets the company's quality standards and code review standards.

What should you recommend implementing in Azure DevOps?

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

**Correct Answer:** C
**Section: [none]**
**Explanation**

**Explanation/Reference:**
Explanation:
Branch policies help teams protect their important branches of development. Policies enforce your team's code quality and change management standards.

References: https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies?view=azure-devops&viewFallbackFrom=vsts