# KTest

更に上のクオリティ　更に上のサービス

# 問題集

http://www.ktest.jp

1年で無料進級することに提供する

**Exam : AZ-500**

**Title :** Microsoft Azure Security Technologies

**Version :** DEMO

1. Topic 1, Litware, inc

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 |

**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 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.

You need to meet the identity and access requirements for Group1.
What should you do?
A. Add a membership rule to Group1.
B. Delete Group1. Create a new group named Group1 that has a membership type of Office 365. Add users and devices to the group.
C. Modify the membership rule of Group1.
D. Change the membership type of Group1 to Assigned. Create two groups that have dynamic memberships. Add the new groups to Group1.
**Answer:** D
**Explanation:**
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership
Scenario:
Litware identifies the following identity and access requirements: All San Francisco users and their devices must be members of Group1.
The tenant currently contain this group:

| 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. |

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-create-azure-portal

2.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.
**Answer:** D
**Explanation:**
https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-dnat

3.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.
**Answer:** C
**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.
Reference: https://docs.microsoft.com/en-us/azure/security-center/security-center-pricing

4.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.
**Answer:** BE
**Explanation:**
Refer https://docs.microsoft.com/en-us/azure/app-service/app-service-web-configure-tls-mutual-auth

5.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.

```
{
  "Name": "Role1",
  "Id": "11111111-1111-1111-1111-111111111111",
  "IsCustom" : true,
  "Description": "VM storage operator"
  "Actions" : [
```

| | |
|---|---|
| "Microsoft.Compute/ | disks/*", |
| "Microsoft.Resources/ | storageAccounts/*", |
| "Microsoft.Storage/ | virtualMachines/disks/*", |

```
        ],
  "NotActions": [
                ],
  "AssignableScopes" : [
```

"/"
"/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4/resourceGroups/Resource Group1"
"/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4

```
                    ]
}
```

**Answer:**

```
{
  "Name": "Role1",
  "Id": "11111111-1111-1111-1111-111111111111",
  "IsCustom" : true,
  "Description": "VM storage operator"
  "Actions" : [
```

| | |
|---|---|
| "Microsoft.Compute/ | disks/*", |
| "Microsoft.Resources/ | storageAccounts/*", |
| "Microsoft.Storage/ | virtualMachines/disks/*", |

```
        ],
  "NotActions": [
                ],
  "AssignableScopes" : [
```

"/"
"/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4/resourceGroups/Resource Group1"
"/subscriptions/43894a43-17c2-4a39-8cfc-3540c2653ef4

```
                    ]
}
```

**Explanation:**

1) Microsoft.Compute/
2) disks
3) /subscrption/{subscriptionId}/resourceGroups/{Resource Group Id}
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.