Reference:
https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-managementgroups/

QUESTION 13
You are testing an Azure Kubernetes Service (AKS) cluster. The cluster is configured as shown in the exhibit. (Click the Exhibit tab.)

BASICS

Subscription	Microsoft Azure Sponsorship
Resource group	AzureBackupRG_eastus2_1
Region	East US
Kubernetes cluster name	akscluster2
Kubernetes version	1.1 1.5
DNS name prefix	akscluster2
Node count	3
Node size	Standard_DS2_v2
Virtual nodes (preview)	Disabled

AUTHENTICATION

Enable RBAC	No

NETWORKING

HTTP application routing	Yes
Network configuration	Basic

MONITORING

Enable container monitoring	No

TAGS

You plan to deploy the cluster to production. You disable HTTP application routing.

You need to implement application routing that will provide reverse proxy and TLS termination for AKS services by using a single IP address.

What should you do?

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

Correct Answer: A
Explanation:
An ingress controller is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services.

References:
https://docs.microsoft.com/en-us/azure/aks/ingress-tls

QUESTION 14
From Azure Security, 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?

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

Correct Answer: A
Explanation:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/action-groups
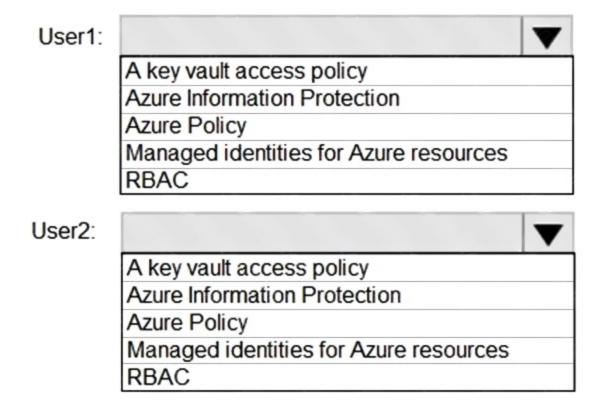
QUESTION 15
HOTSPOT
You have an Azure key vault.

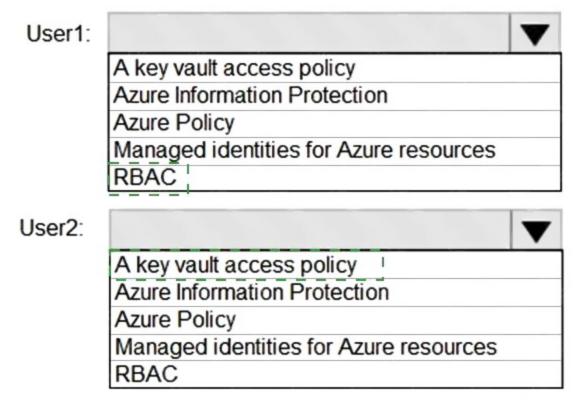You need to delegate administrative access to the key vault to meet the following requirements:

▪ Provide a user named User1 with the ability to set advanced access policies for the key vault.
▪ Provide a user named User2 with the ability to add and delete certificates in the key vault.
▪ Use the principle of least privilege.

What should you use to assign access to each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

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

Correct Answer:

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 16
DRAG DROP
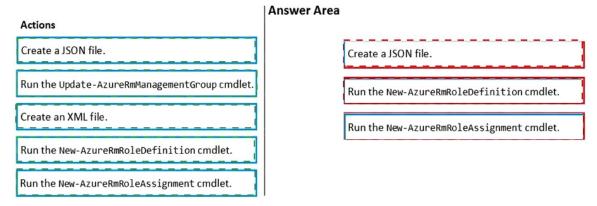You have an Azure subscription named Sub1.

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

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

Answer Area

Correct Answer:

QUESTION 17
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?

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

Correct Answer: B
Explanation:
Adaptive application control is an intelligent, automated end-to-end application whitelisting solution from Azure Security Center. It helps you control which applications can run on your Azure and non-Azure VMs (Windows and Linux), which, among other benefits, helps harden your VMs against malware. Security Center uses machine learning to analyze the applications running on your VMs and helps you apply the specific whitelisting rules using this intelligence.

Reference:
https://docs.microsoft.com/en-us/azure/security-center/security-center-adaptive-application

QUESTION 18
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.