DUMPSBOSS.COM

Microsoft Azure Security Technologies

Microsoft AZ-500

Version Demo

Total Demo Questions: 20

Total Premium Questions: 623

Buy Premium PDF

https://dumpsboss.com

support@dumpsboss.com

Topic Break Down

Topic	No. of Questions
Topic 2, New Update	287
Topic 3, Case Study 1	2
Topic 4, Case Study 2	3
Topic 5, Case Study 3	4
Topic 6, Case Study 4	3
Topic 7, Case Study 5	5
Topic 8, Case Study 6	2
Topic 9, Case Study 7	2
Topic 10, Case Study 8	3
Topic 11, Mixed Questions	312
Total	623

QUESTION NO: 1

You are collecting events from Azure virtual machines to an Azure Log Analytics workspace.

You plan to create alerts based on the collected events.

You need to identify which Azure services can be used to create the alerts.

Which two services should you identify? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Azure Monitor

B. Azure Security Center

C. Azure Analysis Services

D. Azure Sentinel

E. Azure Advisor

ANSWER: A D

QUESTION NO: 2 - (HOTSPOT)

HOTSPOT

Your company has an Azure subscription named Subscription1 that contains the users shown in the following table.

Name	Role
User1	Global administrator
User2	Billing administrator
User3	Owner
User4	Account Admin

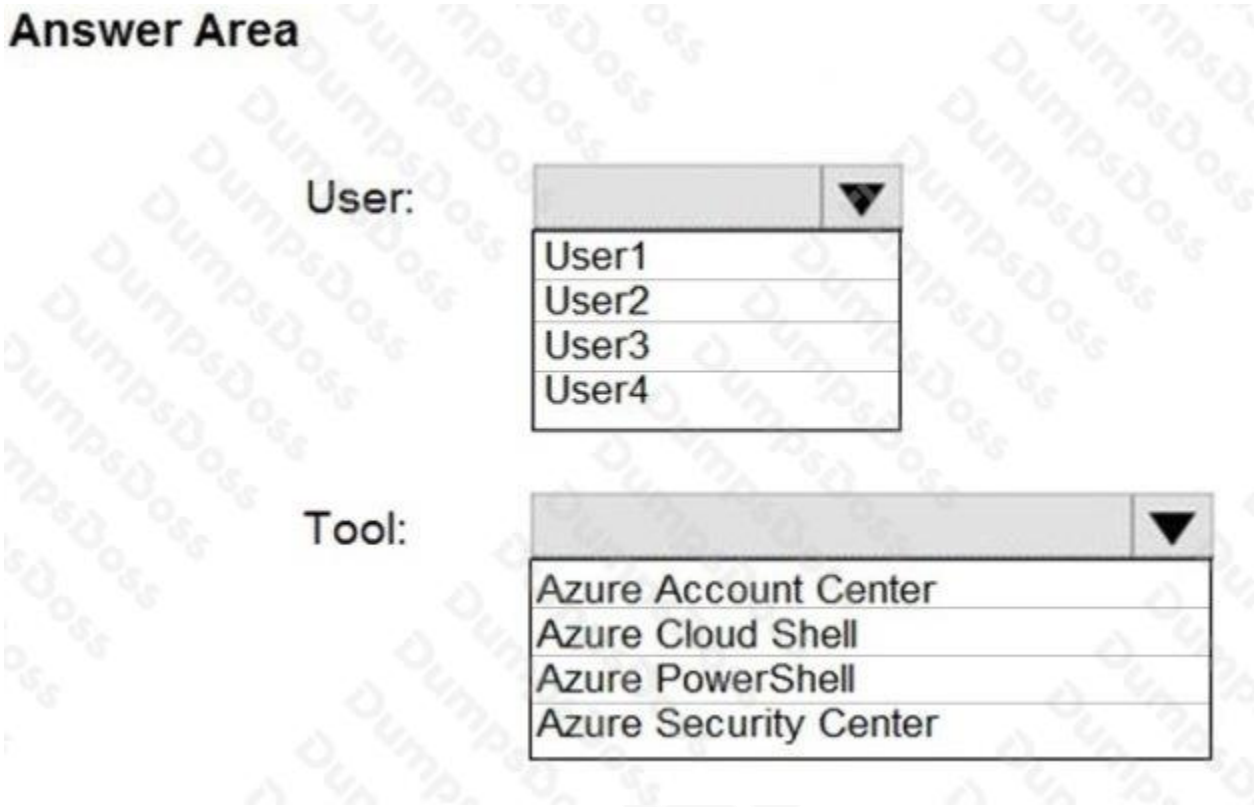
The company is sold to a new owner.

The company needs to transfer ownership of Subscription1.

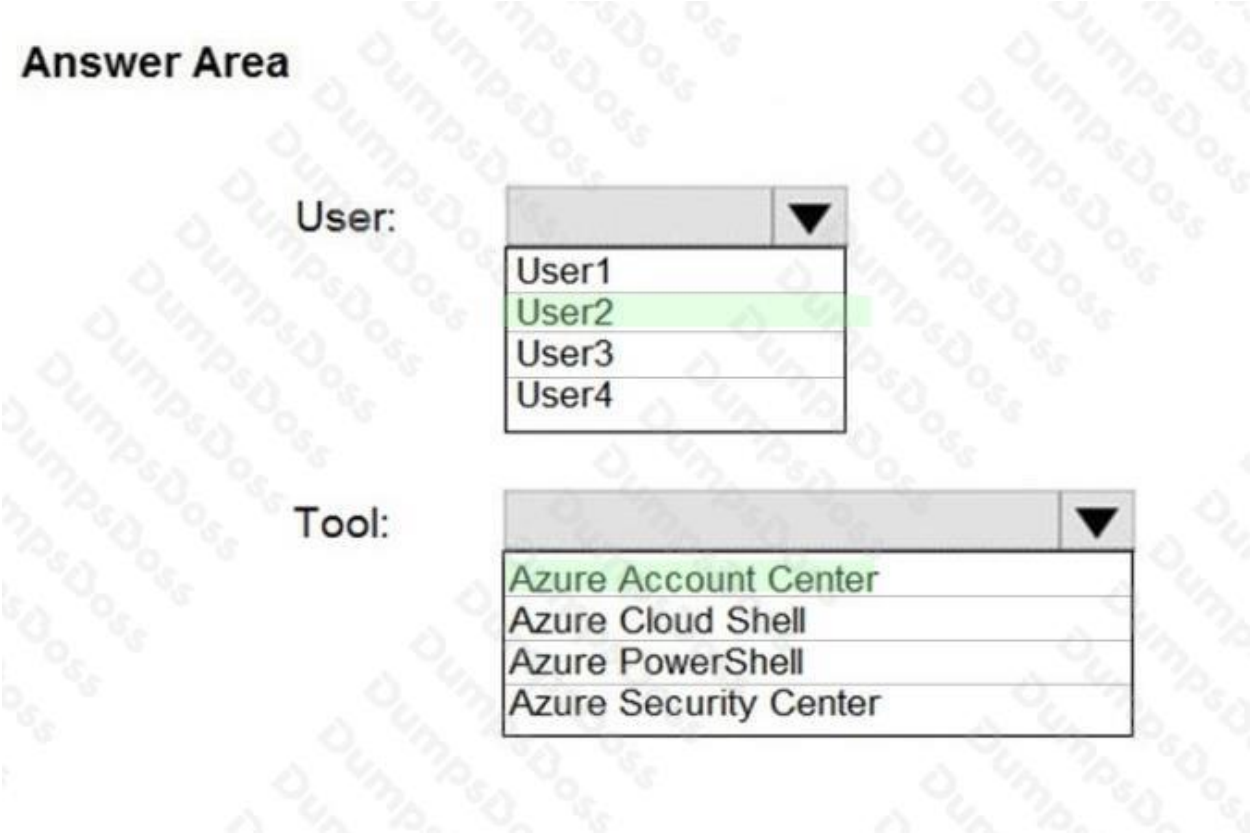
Which user can transfer the ownership and which tool should the user use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



ANSWER:



Explanation:

Box 1; User2

Billing Administrator

Select Transfer billing ownership for the subscription that you want to transfer.

Enter the email address of a user who's a billing administrator of the account that will be the new owner for the subscription.

Box 2: Azure Account Center Azure Account Center can be used.

Reference:

https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer#transfer-billing-ownership-of-an-azure-subscription

QUESTION NO: 3

You have an Azure Sentinel workspace.

You need to create a playbook.

Which two triggers will start the playbook? Each correct answer presents a complete solution,

NOTE: Each correct selection is worth one point.

A. An Azure Sentinel scheduled query rule is executed.

B. An Azure Sentinel data connector is added.

C. An Azure Sentinel alert is generated.

D. An Azure Sentinel hunting query result is returned.

E. An Azure Sentinel incident is created.

ANSWER: C E

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

QUESTION NO: 4

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 configuration policies in Microsoft Intune

B. an Azure Desired State Configuration (DSC) virtual machine extension

C. application security groups

D. device compliance policies in Microsoft Intune

ANSWER: B

Explanation:

The primary use case for the Azure Desired State Configuration (DSC) extension is to bootstrap a VM to the Azure Automation State Configuration (DSC) service. The service provides benefits that include ongoing management of the VM configuration and integration with other operational tools, such as Azure Monitoring. Using the extension to register VM's to the service provides a flexible solution that even works across Azure subscriptions.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-overview

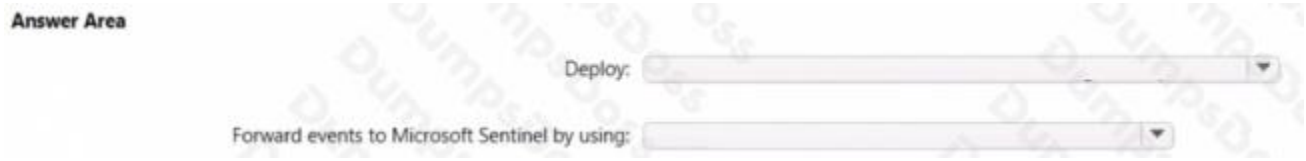
QUESTION NO: 5 - (SIMULATION)

You have a Microsoft Sentinel deployment.

You need to connect a third-party security solution to the deployment. The third-party solution will send Common Event Format (CER-formatted messages.

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

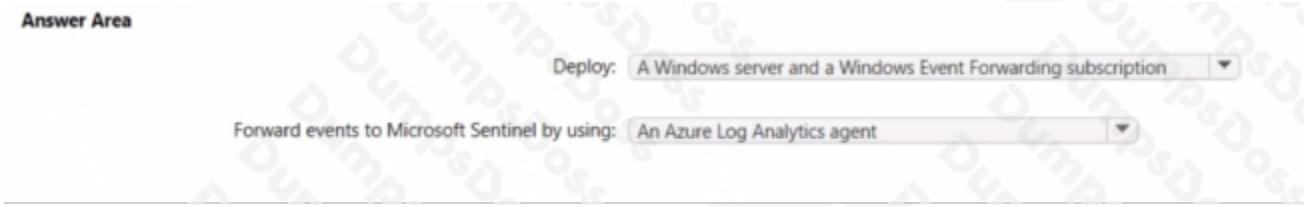
NOTE: Each correct selection is worth one point.



ANSWER: SeetheanswerbelowatExplanation.

Explanation:

Answer is as image below.



QUESTION NO: 6

You have an Azure Active Directory (Azure AD) tenant and a root management group.

You create 10 Azure subscriptions and add the subscriptions to the rout management group.

You need to create an Azure Blueprints definition that will be stored in the root management group.

What should you do first?

A. Add an Azure Policy definition to the root management group.

B. Modify the role-based access control (RBAC) role assignments for the root management group.

C. Create a user-assigned identity.

D. Create a service principal.

ANSWER: B

Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/role-based-access-control/elevate-access-global-admin

QUESTION NO: 7

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. Configure Azure Active Directory (Azure AD) Identity Protection.

B. From Microsoft Defender for Cloud, configure adaptive application controls.

C. Apply an Azure policy to RGI.

D. Apply a resource lock to RGI.

ANSWER: B

Explanation:

Microsoft Defender for Cloud helps you prevent, detect, and respond to threats. Defender for Cloud gives you increased visibility into, and control over, the security of your Azure resources. It provides integrated security monitoring and policy management across your Azure subscriptions. It helps detect threats that might otherwise go unnoticed, and works with a broad ecosystem of security solutions.

Defender for Cloud helps you optimize and monitor the security of your virtual machines by:

https://learn.microsoft.com/en-us/azure/security/fundamentals/virtual-machines-overview

QUESTION NO: 8

Your network contains an Active Directory forest named contoso.com. You have an Azure Active 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.

A. the Domain Admins group in Active Directory

B. the Security administrator role in Azure AD

C. the Global administrator role in Azure AD

D. the User administrator role in Azure AD

E. the Enterprise Admins group in Active Directory

ANSWER: C E

Explanation:

Reference: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions

QUESTION NO: 9

You have an Azure subscription named Sub1.

In Azure Security Center, you have a workflow automation named WF1. WF1 is configured to send an email message to a user named User1.

You need to modify WF1 to send email messages to a distribution group named Alerts.

What should you use to modify WF1?

A. Azure Application Insights

B. Azure Monitor

C. Azure Logic Apps Designer

D. Azure DevOps

ANSWER: C

Explanation:

Reference: https://docs.microsoft.com/en-us/azure/security-center/workflow-automation https://docs.microsoft.com/en-us/learn/modules/resolve-threats-with-azure-security-center/6-exercise-configure-playbook

QUESTION NO: 10 - (HOTSPOT)

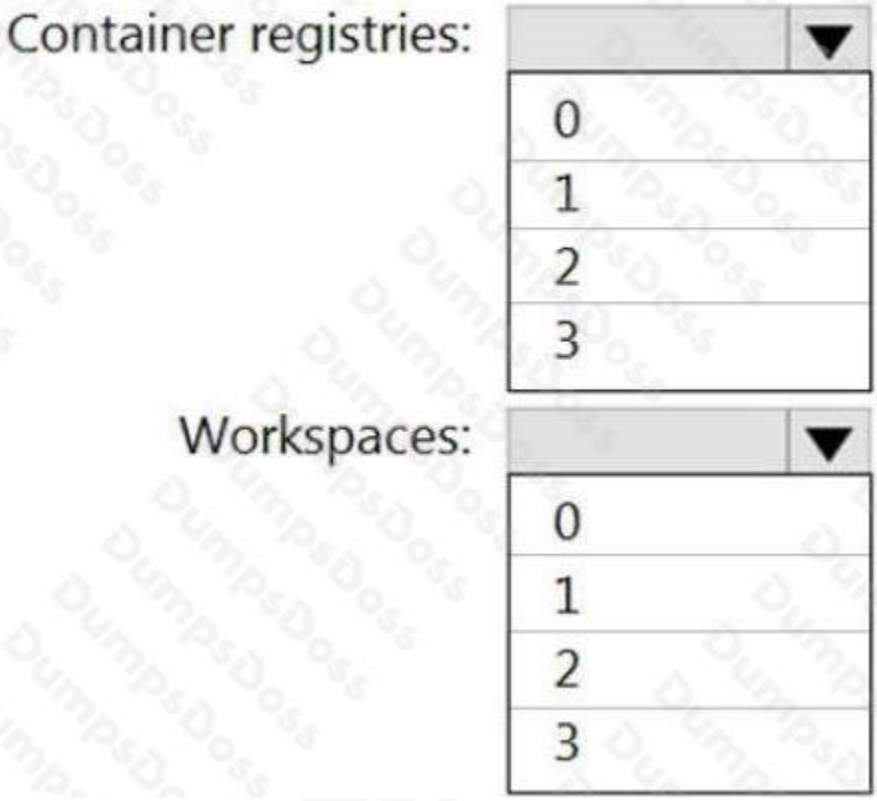
HOTSPOT

You need to configure support for Azure Sentinel notebooks to meet the technical requirements.

What is the minimum number of Azure container registries and Azure Machine Learning workspaces required?

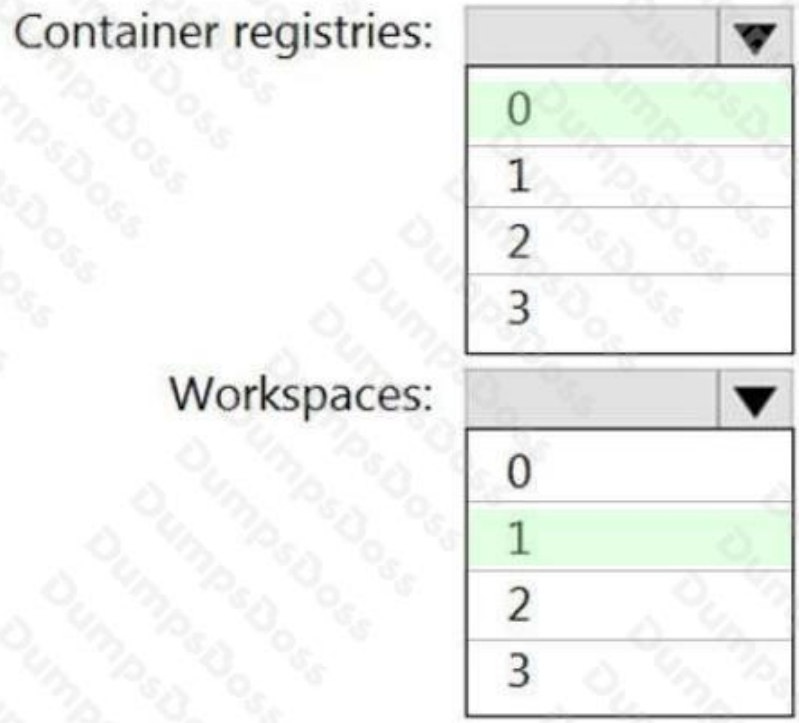
Hot Area:

Answer Area



ANSWER:

Answer Area



Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/notebooks

QUESTION NO: 11

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.

A. AcrQuarantineReader

B. Contributor

C. AcrPush

D. AcrImageSigner

E. AcrQuarantineWriter

ANSWER: C D

Explanation:

References:

https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust

https://docs.microsoft.com/en-us/azure/container-registry/container-registry-roles

QUESTION NO: 12

You have an Azure subscription that contains a web app named App1.

Users must be able to select between a Google identity or a Microsoft identity when authenticating to App1.

You need to add Google as an identity provider in Azure AD.

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

Each correct selection is worth one point

A. a tenant name

B. a tenant ID

C. the endpoint URL Of an application

D. a client ID

E. a client secret

ANSWER: D E

Explanation:

https://learn.microsoft.com/en-us/azure/app-service/configure-authentication-provider-google

QUESTION NO: 13 - (DRAG DROP)

DRAG DROP

You have five Azure subscriptions linked to a single Azure Active Directory (Azure AD) tenant.

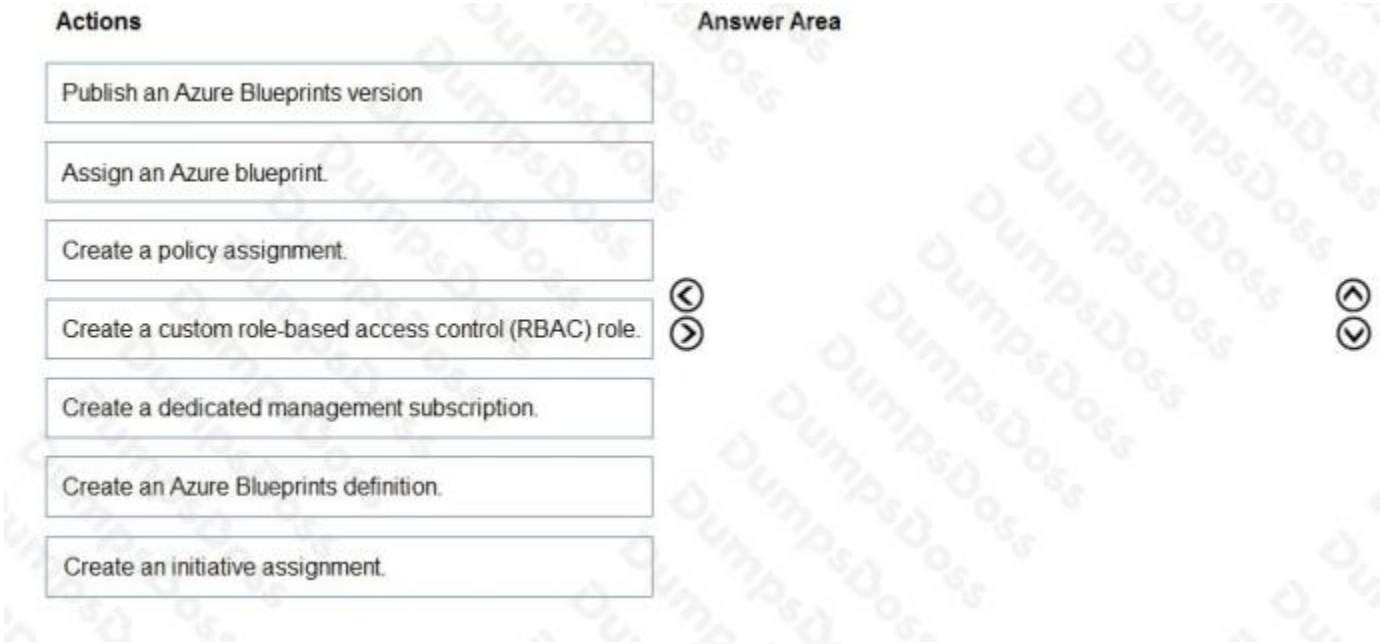
You create an Azure Policy initiative named SecurityPolicyInitiative1.

You identify which standard role assignments must be configured on all new resource groups.

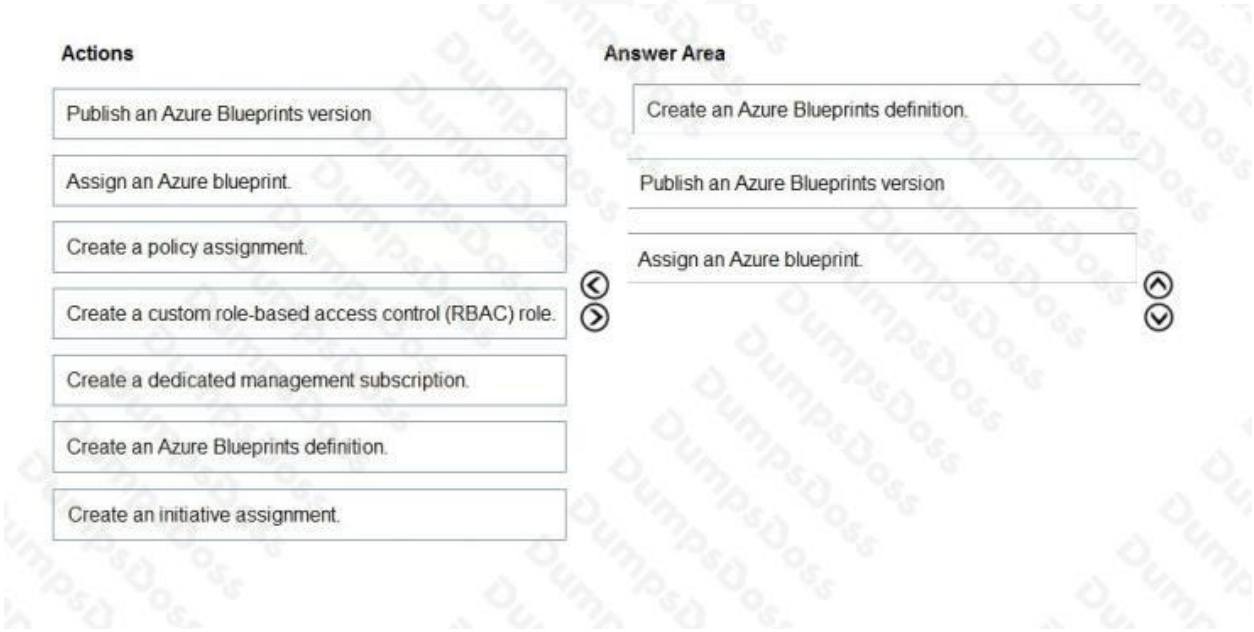
You need to enforce SecurityPolicyInitiative1 and the role assignments when a new resource group is created.

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

Select and Place:



ANSWER:



Explanation:

Reference:

https://docs.microsoft.com/en-us/azure/governance/blueprints/create-blueprint-portal https://docs.microsoft.com/en-us/azure/azure-australia/azure-policy

QUESTION NO: 14

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?

A. VM3 only

B. VM1 and VM3 only

C. VM3 and VM4 only

D. VM1, VM2, VM3, and VM4

ANSWER: D

Explanation:

When automatic provisioning is enabled, Security Center provisions the Microsoft Monitoring Agent on all supported Azure VMs and any new ones that are created.

Supported Operating systems include: Ubuntu 14.04 LTS (x86/x64), 16.04 LTS (x86/x64), and 18.04 LTS (x64) and Windows Server 2008 R2, 2012, 2012 R2, 2016, version 1709 and 1803.

Reference:

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

QUESTION NO: 15 - (SIMULATION)

You have an Azure subscription that contains an instance of Azure Firewall Standard named AzFWL You need to identify whether you can use the following features with AzFW1:

• TLS inspection

• Threat intelligence

• The network intrusion detection and prevention systems (IDPS)

What can you use?

A. TLS inspection only

B. threat intelligence only

C. TLS inspection and the IDPS only

D. threat intelligence and the IDPS only

E. TLS inspection, threat intelligence, and the IDPS

ANSWER: E

QUESTION NO: 16 - (DRAG DROP)

DRAG DROP

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

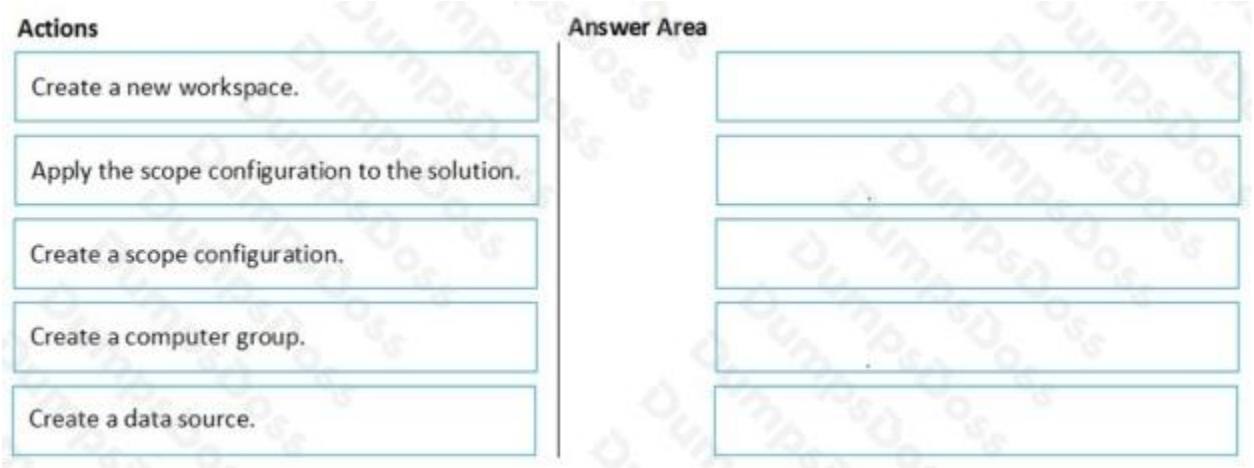
You have 500 Azure virtual machines that run Windows Server 2016 and are enrolled in LAW1.

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

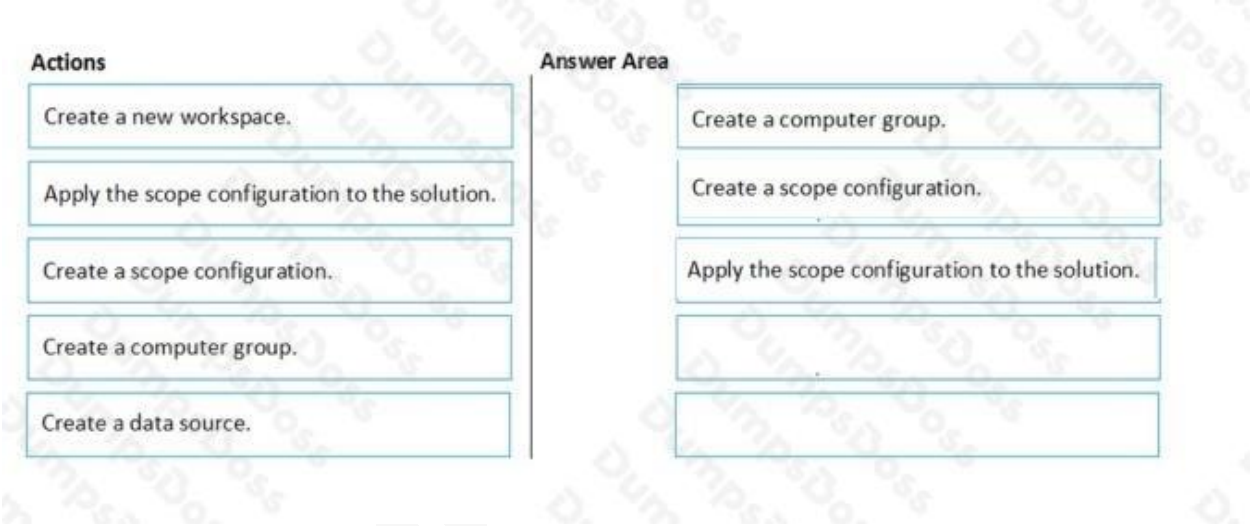
You need to ensure that System Update Assessment-related logs are uploaded to LAW1 from 100 of the virtual machines only.

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.

Select and Place:



ANSWER:



Explanation:

Reference: https://docs.microsoft.com/en-us/azure/azure-monitor/insights/solution-targeting

QUESTION NO: 17

You want to gather logs from a large number of Windows Server 2016 computers using Azure Log Analytics.

You are configuring an Azure Resource Manager template to deploy the Microsoft Monitoring Agent to all the servers automatically.

Which of the following should be included in the template? (Choose all that apply.)

A. WorkspaceID

B. AzureADApplicationID

C. WorkspaceKey

D. StorageAccountKey

ANSWER: A C

Explanation:

Reference:

https://blogs.technet.microsoft.com/manageabilityguys/2015/11/19/enabling-the-microsoft-monitoring-agent-in-windows-json-templates/

QUESTION NO: 18

You have an Azure subscription that contains an Azure key vault and an Azure Storage account. The key vault contains customer-managed keys. The storage account is configured to use the customer-managed keys stored In the key vault.

You plan to store data in Azure by using the following services:

* Azure Files

* Azure Blob storage

* Azure Log Analytics

* Azure Table storage

* Azure Queue storage

Which two services data encryption by using the keys stored in the key vault? Each correct answer present a complete solution.

NOTE: Each correct selection is worth one point.

A. Queue storage

B. Table storage

C. Azure Files

D. Blob storage

ANSWER: A C

Explanation:

https://docs.microsoft.com/en-us/azure/storage/common/account-encryption-key-create?tabs=portal

QUESTION NO: 19

You have an Azure AD tenant that contains 500 users and an administrative unit named AU1.

From the Azure Active Directory admin center, you plan to add the users to AU1 by using Bulk add members.

You need to create and upload a file for the bulk add.

What should you include in the file?

A. only the display name of each user

B. only the user principal name (UPN) of each user

C. only the object identifier of each user

D. only the user principal name (UPN) and object identifier of each user

E. Only the user principal name (UPN) and display name of each user

ANSWER: E

QUESTION NO: 20

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 configuration policies in Microsoft Intune

B. an Azure Desired State Configuration (DSC) virtual machine extension

C. security policies in Azure Security Center

D. Azure Logic Apps

ANSWER: B

Explanation:

The primary use case for the Azure Desired State Configuration (DSC) extension is to bootstrap a VM to the Azure Automation State Configuration (DSC) service. The service provides benefits that include ongoing management of the VM configuration and integration with other operational tools, such as Azure Monitoring. Using the extension to register VM's to the service provides a flexible solution that even works across Azure subscriptions.

Reference: https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-overview