AZ-500$^{\text{Q\&As}}$

Microsoft Azure Security Technologies

Pass Microsoft AZ-500 Exam with 100% Guarantee

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 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?

A. Yes

B. No

Correct Answer: A

You don\\'t need a VPN with OnPrem to connect to HDInsights. It would be relevant if you need connection between HDInsights and onPrem servers and/or want to remove/restric public traffic.

HDIsights can be accessed from internet no matters of the authentication method.

https://learn.microsoft.com/en-us/azure/hdinsight/hdinsight-virtual-network-architecture

Now you want to connects HDI with on-prem AD DS identities.

The only supported way is to use Azure AD DS (An Azure Service, different from your onprem AD DS).

Azure AD DS needs AD connect with PHS from On-Prem AD DS to Azure AD. You are in Hybrid config so already setup AD Connects.

Azure AD DS is deplpoyed in a VNEt and needs to be Perred with HDInsights VNet. That\\'s it.

https://learn.microsoft.com/en-us/azure/hdinsight/domain-joined/apache-domain-joined-create-configure-enterprise-security-cluster

QUESTION 2

You have a Azure subscription.

You enable Azure Active Directory (Azure AD) Privileged identify (PIM). Your company\\'s security policy for administrator accounts has the following conditions:

1.

The accounts must use multi-factor authentication (MFA).

2.

The account must use 20-character complex passwords.

3.

The passwords must be changed every 180 days.

4.

The account must be managed by using PIM.

You receive alerts about administrator who have not changed their password during the last 90 days. You need to minimize the number of generated alerts. Which PIM alert should you modify?

A. Roles don\\'t require multi-factor authentication for activation.

B. Administrator aren\\'t using their privileged roles

C. Roles are being assigned outside of Privileged identity Management

D. Potential stale accounts in a privileged role.

Correct Answer: D

Reference: https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-configure-security-alerts?tabs=new

QUESTION 3

Your company\\'s Azure subscription includes a hundred virtual machines that have Azure Diagnostics enabled.

You have been tasked with analyzing the security events of a Windows Server 2016 virtual machine. You have already accessed Azure Monitor.

Which of the following options should you use?

A. Application Log

B. Metrics

C. Activity Log

D. Logs

Correct Answer: D

Log Integration collects Azure diagnostics from your Windows virtual machines, Azure activity logs, Azure Security Center alerts, and Azure resource provider logs. This integration provides a unified dashboard for all your assets, whether they\\'re on-premises or in the cloud, so that you can aggregate, correlate, analyze, and alert for security events.

Reference: https://docs.microsoft.com/en-us/azure/security/azure-log-audit

QUESTION 4

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:

1.

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

2.

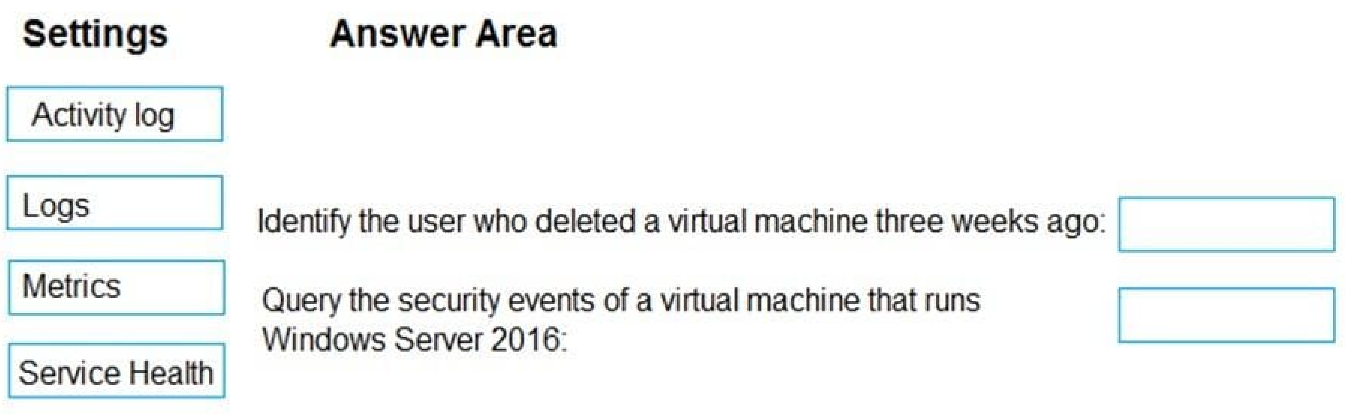
Query the security events of a virtual machine that runs Windows Server 2016.

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.

Select and Place:



Settings

Activity log

Logs

Metrics

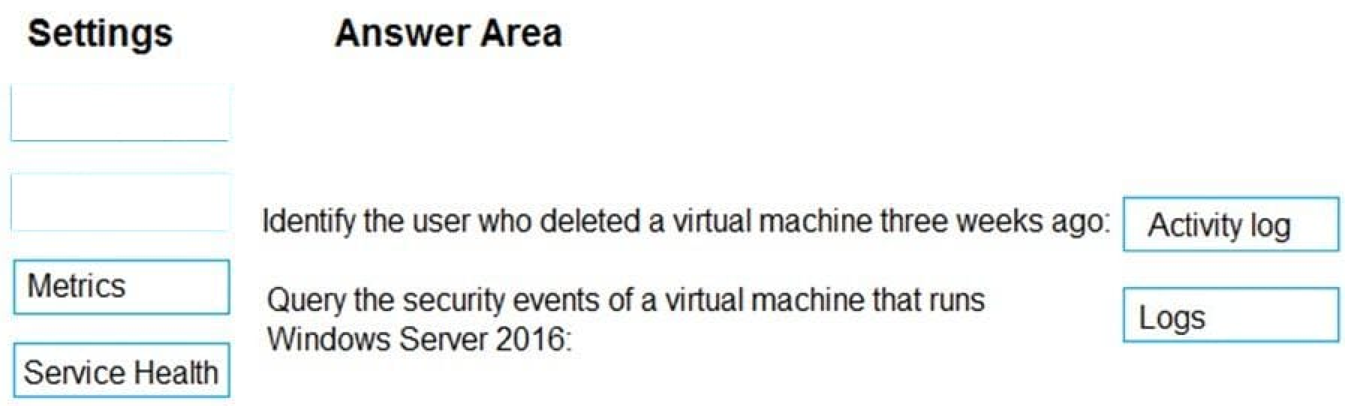
Service Health

Answer Area

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

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

Correct Answer:



Settings	Answer Area	
	Identify the user who deleted a virtual machine three weeks ago:	Activity log
Metrics	Query the security events of a virtual machine that runs Windows Server 2016:	Logs
Service Health		

Box1: Activity log Azure activity logs provide insight into the operations that were performed on resources in your subscription. Activity logs were previously known as "audit logs" or "operational logs," because they report control-plane events for your subscriptions.

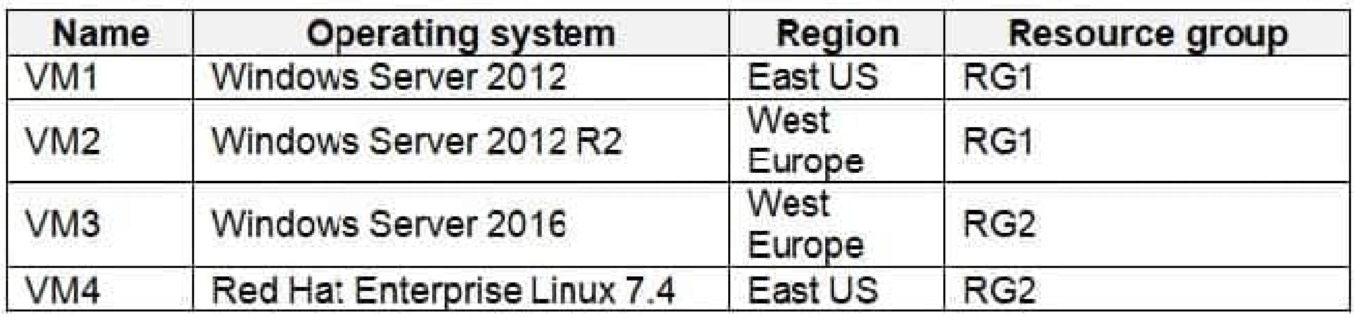
Activity logs help you determine the "what, who, and when" for write operations (that is, PUT, POST, or DELETE).

Box 2: Logs Log Integration collects Azure diagnostics from your Windows virtual machines, Azure activity logs, Azure Security Center alerts, and Azure resource provider logs. This integration provides a unified dashboard for all your assets, whether they\\'re on-premises or in the cloud, so that you can aggregate, correlate, analyze, and alert for security events.

References: https://docs.microsoft.com/en-us/azure/security/azure-log-audit

QUESTION 5

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: C

Note: Create a workspace

1.

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.

2.

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