SC-200 Q&As

Microsoft Security Operations Analyst

Pass Microsoft SC-200 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/sc-200.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers

QUESTION 1

HOTSPOT

You have a Microsoft Sentinel workspace named sws1.

You plan to create an Azure logic app that will raise an incident in an on-premises IT service management system when an incident is generated in sws1.

You need to configure the Microsoft Sentinel connector credentials for the logic app. The solution must meet the following requirements:

1.

Minimize administrative effort.

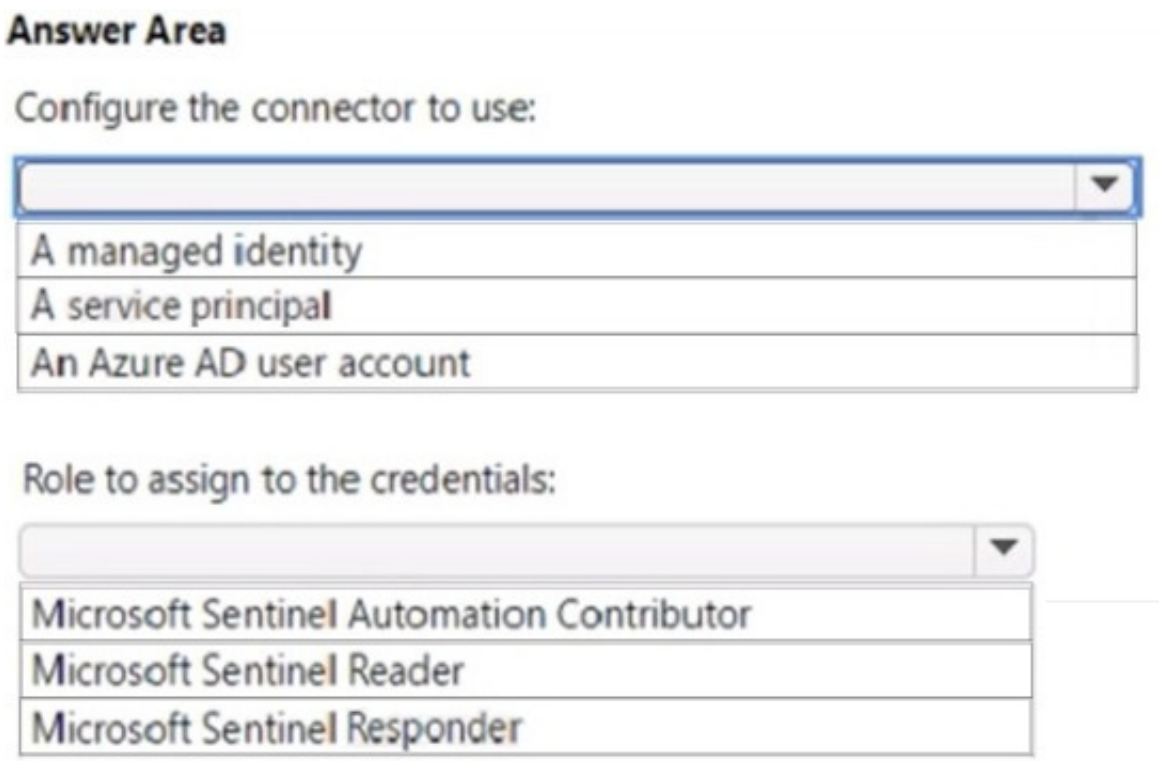
2.

Use the principle of least privilege.

How should you configure the credentials? To answer, select the appropriate options in the answer area.

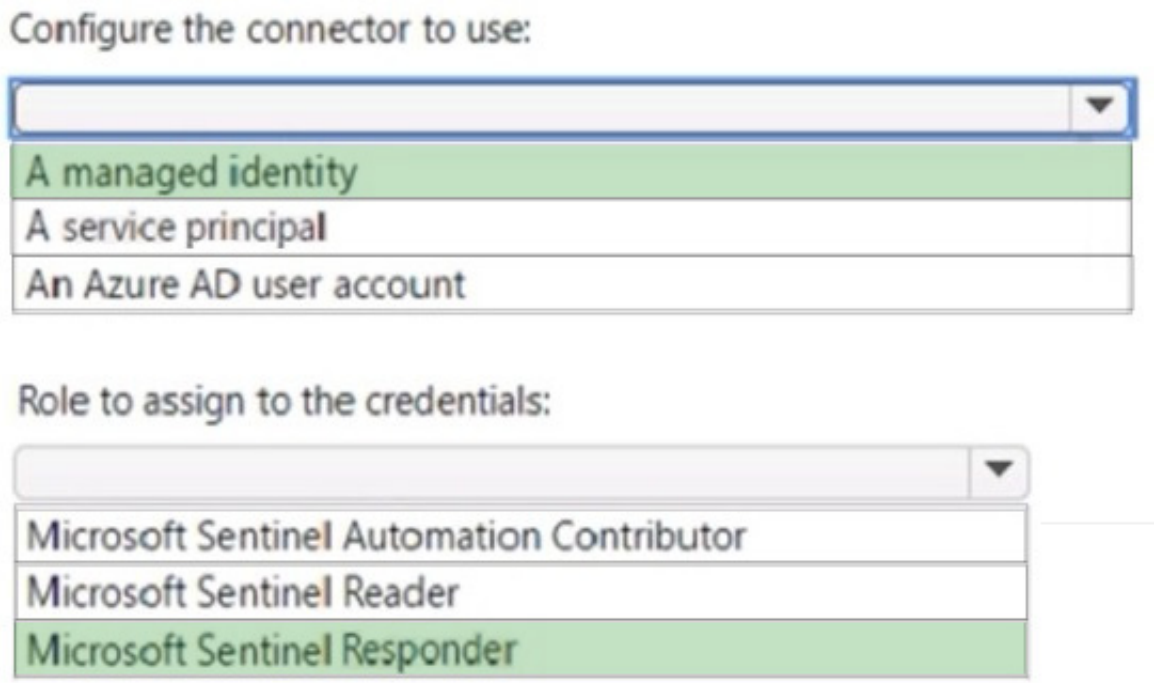
NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

Answer Area



Box 1: A managed identity Managed Identity for Azure Sentinel Logic Apps connector With the availability of Managed Identity for the Azure Sentinel connector, you can give permissions directly to the playbook (Logic App workflow resource), so Sentinel connector actions will operate on its behalf, as if it were an independent object which has permissions on Azure Sentinel. This lowers the number of identities you have to manage and gives the power to give access directly to the resource that operates.

Incorrect:

The service principal connection type allows us to create a registered application and use it as the identity behind the connector. You can define what this app can do, who can access it and what resources can this app access. It\\'s easy to delete it or replace its credentials if it\\'s suspected to have been compromised. For these reasons it\\'s great from a security perspective, but it still requires managing as another identity in the cloud that has credentials and permissions which potentially others can use.

Many would prefer not to authenticate with a user to a tool that generates automated actions. It is harder to audit (for example, using the incident table) which actions have been taken on behalf of a user and which are made by the playbook. It also makes less sense to see, for example, new comments that were generated by a playbook, but appear as if a user is their author. Also, if a user leaves the organization, you need to update all the connections that use its identity.

Box 2: Azure Sentinel Responder role

Reference: https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/what-s-new-managed-identity-for-azure-sentinel-logic-apps/ba-p/2068204

QUESTION 2

You have an Azure subscription that uses Microsoft Defender for Cloud and contains 100 virtual machines that run Windows Server.

You need to configure Defender for Cloud to collect event data from the virtual machines. The solution must minimize administrative effort and costs.

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

NOTE: Each correct selection is worth one point.

A. From the workspace created by Defender for Cloud, set the data collection level to Common.

B. From the Microsoft Endpoint Manager admin center, enable automatic enrollment.

C. From the Azure portal, create an Azure Event Grid subscription.

D. From the workspace created by Defender for Cloud, set the data collection level to All Events.

E. From Defender for Cloud in the Azure portal, enable automatic provisioning for the virtual machines.

Correct Answer: AE

A (not D): What event types are stored for "Common" and "Minimal"?

The Common and Minimal event sets were designed to address typical scenarios based on customer and industry standards for the unfiltered frequency of each event and their usage.

*

Common - A set of events that satisfies most customers and provides a full audit trail.

This set is intended to provide a full user audit trail, including events with low volume. For example, this set contains both user logon events (event ID 4624) and user logoff events (event ID 4634). We include auditing actions like security

group changes, key domain controller Kerberos operations, and other events that are recommended by industry organizations.

*

Minimal

*

All events

QUESTION 3

You have a third-party security information and event management (SIEM) solution.

You need to ensure that the SIEM solution can generate alerts for Azure Active Directory (Azure AD) sign-events in near real time.

What should you do to route events to the SIEM solution?

A. Create an Azure Sentinel workspace that has a Security Events connector.

B. Configure the Diagnostics settings in Azure AD to stream to an event hub.

C. Create an Azure Sentinel workspace that has an Azure Active Directory connector.

D. Configure the Diagnostics settings in Azure AD to archive to a storage account.

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/overview-monitoring

QUESTION 4

HOTSPOT

You have an Azure DevOps organization that contains an Azure Repos repository named Repo1 and is onboarded to Microsoft Defender for DevOps.

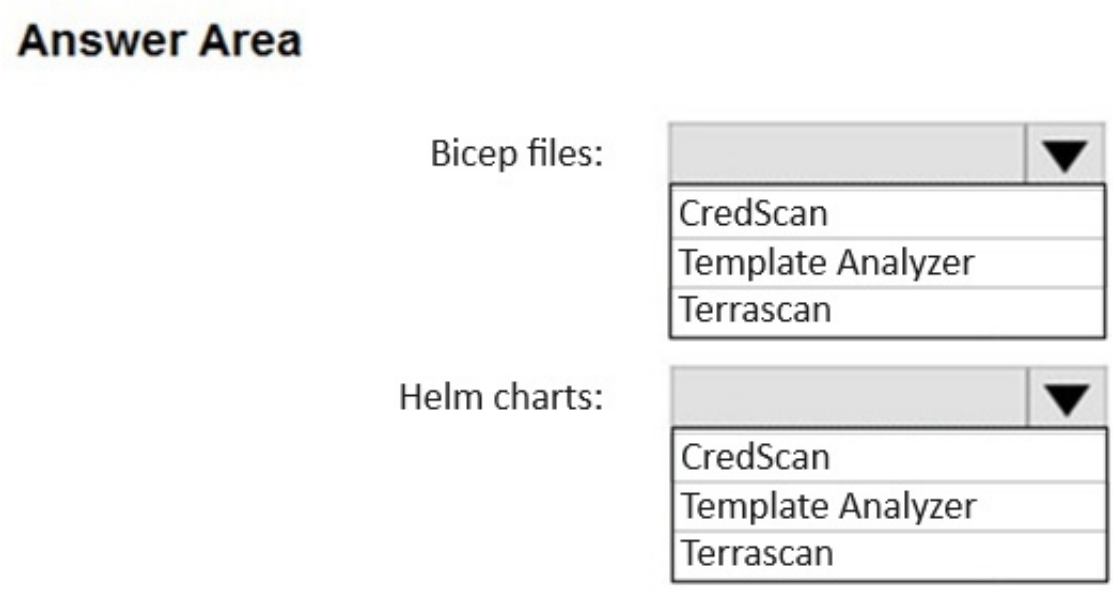
You create infrastructure as code (IaC) files and store them in Repo1. The IaC files are formatted as Bicep files and Helm charts.

You need to configure Defender for DevOps to identify misconfigurations in the IaC files.

Which scanning tool should you use for each type of files? To answer, select the appropriate options in the answer area.

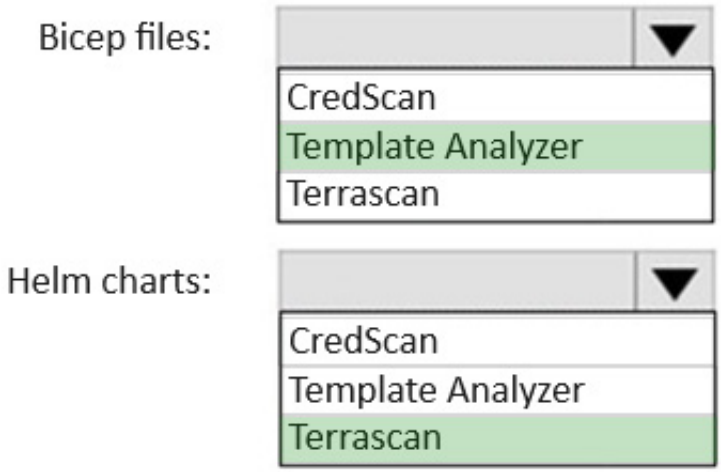
NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

Answer Area



QUESTION 5

You have an Azure subscription that uses Microsoft Sentinel.

You need to minimize the administrative effort required to respond to the incidents and remediate the security threats detected by Microsoft Sentinel.

Which two features should you use? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Microsoft Sentinel bookmarks

B. Azure Automation runbooks

C. Microsoft Sentinel automation rules

D. Microsoft Sentinel playbooks

E. Azure Functions apps

Correct Answer: CD

Reference: https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook?tabs=LAC

QUESTION 6

You have a Microsoft 365 E5 subscription that uses Microsoft Defender XDR and contains a user named User1.

You need to ensure that User1 can manage Microsoft Defender XDR custom detection rules and Endpoint security policies. The solution must follow the principle of least privilege.

Which role should you assign to User1?

A. Security Administrator

B. Security Operator

C. Cloud Device Administrator

D. Desktop Analytics Administrator

Correct Answer: A

QUESTION 7

You need to deploy the native cloud connector to Account 1 to meet the Microsoft Defender for Cloud requirements. What should you do in Account1 first?

A. Create an AWS user for Defender for Cloud.

B. Configure AWS Security Hub.

C. Deploy the AWS Systems Manager (SSM) agent.

D. Create an Access control (IAM) role for Defender for Cloud.

Correct Answer: A

Dynamic scaled onboarding of AWS EC2 instances to Azure Arc using Ansible

Create an AWS identity

In order for Terraform to create resources in AWS, we will need to create a new AWS IAM role with appropriate permissions and configure Terraform to use it.

Scenario: Automate the deployment of the Azure Connected Machine agent for Azure Arc-enabled servers to the existing and future resources of Account1.

Fabrikam has an Amazon Web Services (AWS) account named Account1. Account1 contains 100 Amazon Elastic Compute Cloud (EC2) instances that run a custom Windows Server 2022. The image includes Microsoft SQL Server 2019 and

does NOT have any agents installed.

Reference:

https://github.com/microsoft/azure_arc/blob/main/docs/azure_arc_jumpstart/azure_arc_servers/scaled_deployment/aws_scaled_ansible/_index.md

QUESTION 8

HOTSPOT

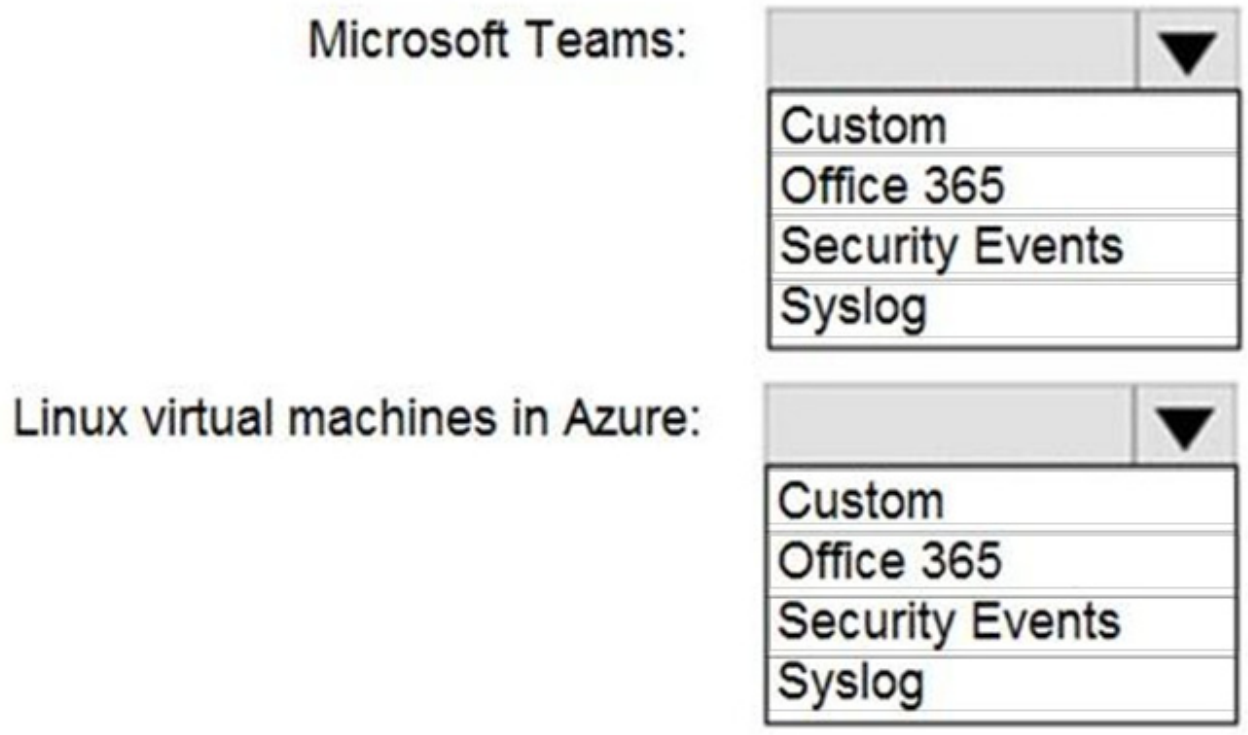
You deploy Azure Sentinel.

You need to implement connectors in Azure Sentinel to monitor Microsoft Teams and Linux virtual machines in Azure. The solution must minimize administrative effort.

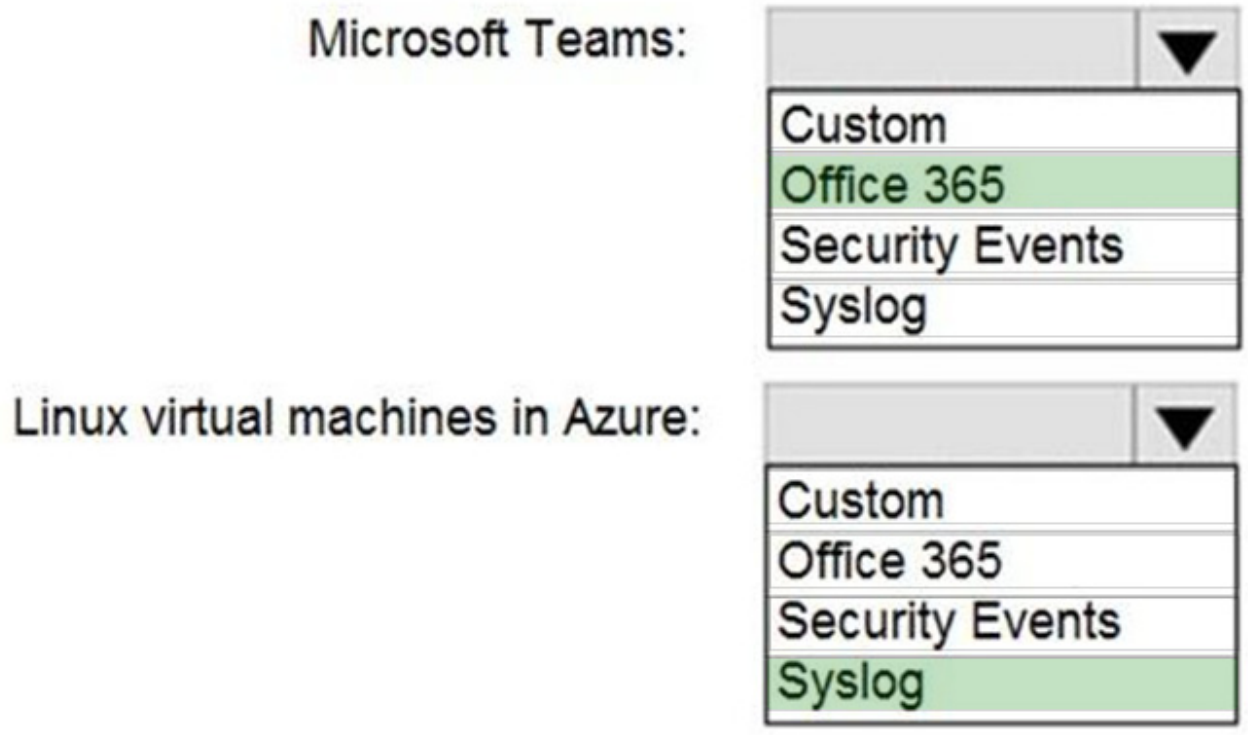
Which data connector type should you use for each workload? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Reference: https://docs.microsoft.com/en-us/azure/sentinel/connect-office-365 https://docs.microsoft.com/en-us/azure/sentinel/connect-syslog

QUESTION 9

HOTSPOT

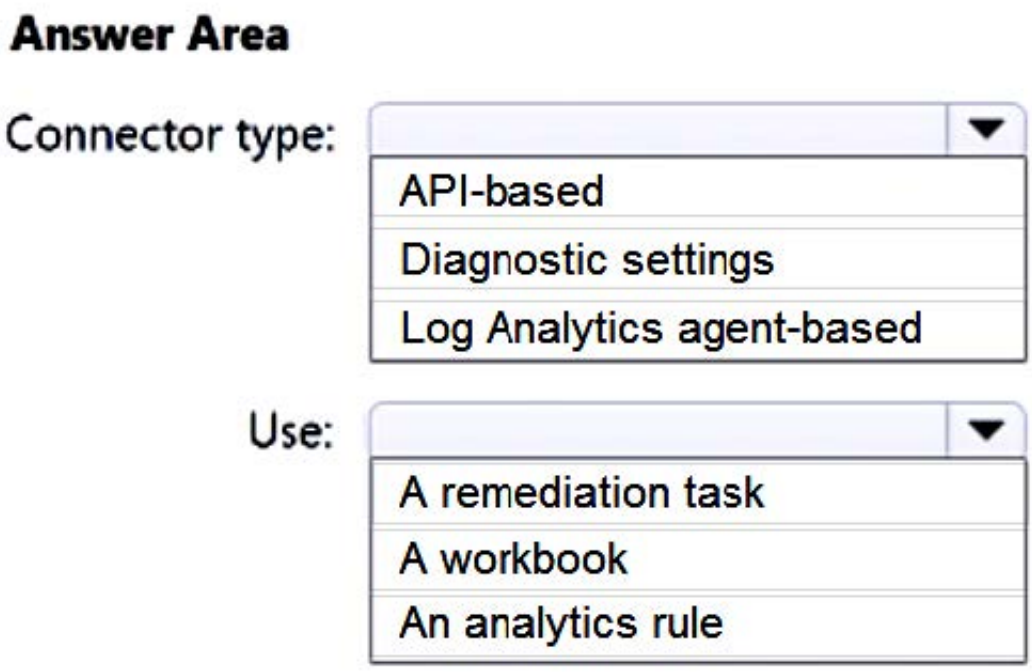
You have four Azure subscriptions. One of the subscriptions contains a Microsoft Sentinel workspace.

You need to deploy Microsoft Sentinel data connectors to collect data from the subscriptions by using Azure Policy. The solution must ensure that the policy will apply to new and existing resources in the subscriptions.

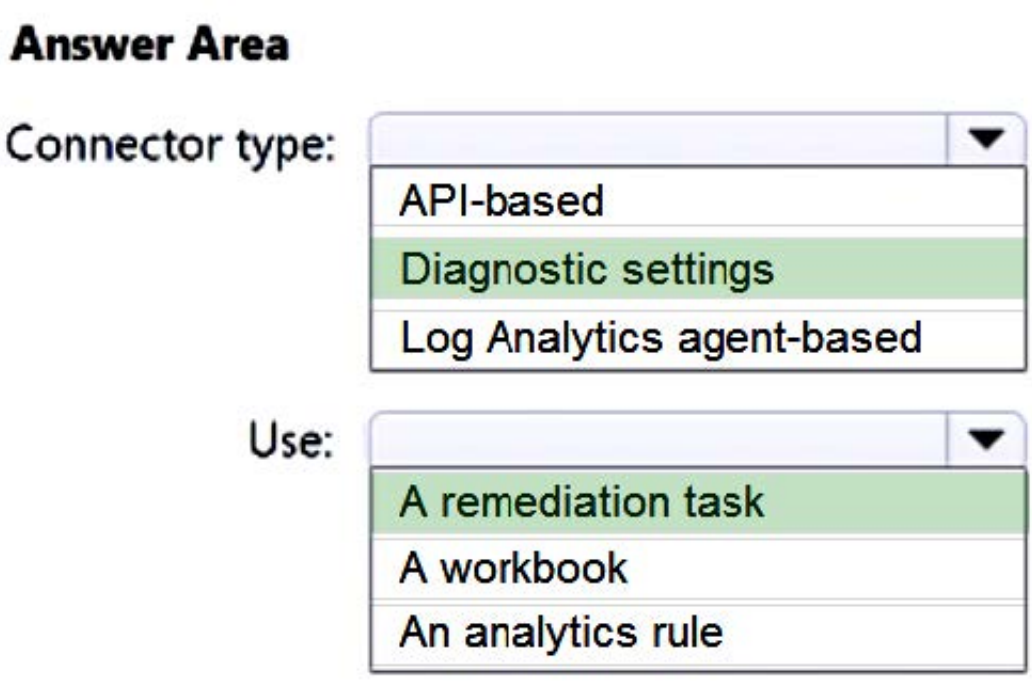
Which type of connectors should you provision, and what should you use to ensure that all the resources are monitored? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



The policy will be applied to resources added in the future. To apply the policy on your existing resources as well, select the Remediation tab and mark the Create a remediation task check box https://learn.microsoft.com/en-us/azure/sentinel/connect-services-diagnostic-setting-based

QUESTION 10

HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint.

You have the on-premises devices shown in the following table.

Name	Management state	Operating system
Device1	Onboarded to and managed by using Microsoft Defender for Endpoint	Windows Server 2022
Device2	Discovered by Microsoft Defender for Endpoint and unmanaged	Linux

You are preparing an incident response plan for devices infected by malware. You need to recommend response actions that meet the following requirements:

1.

Block malware from communicating with and infecting managed devices.

2.

Do NOT affect the ability to control managed devices.

Which actions should you use for each device? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

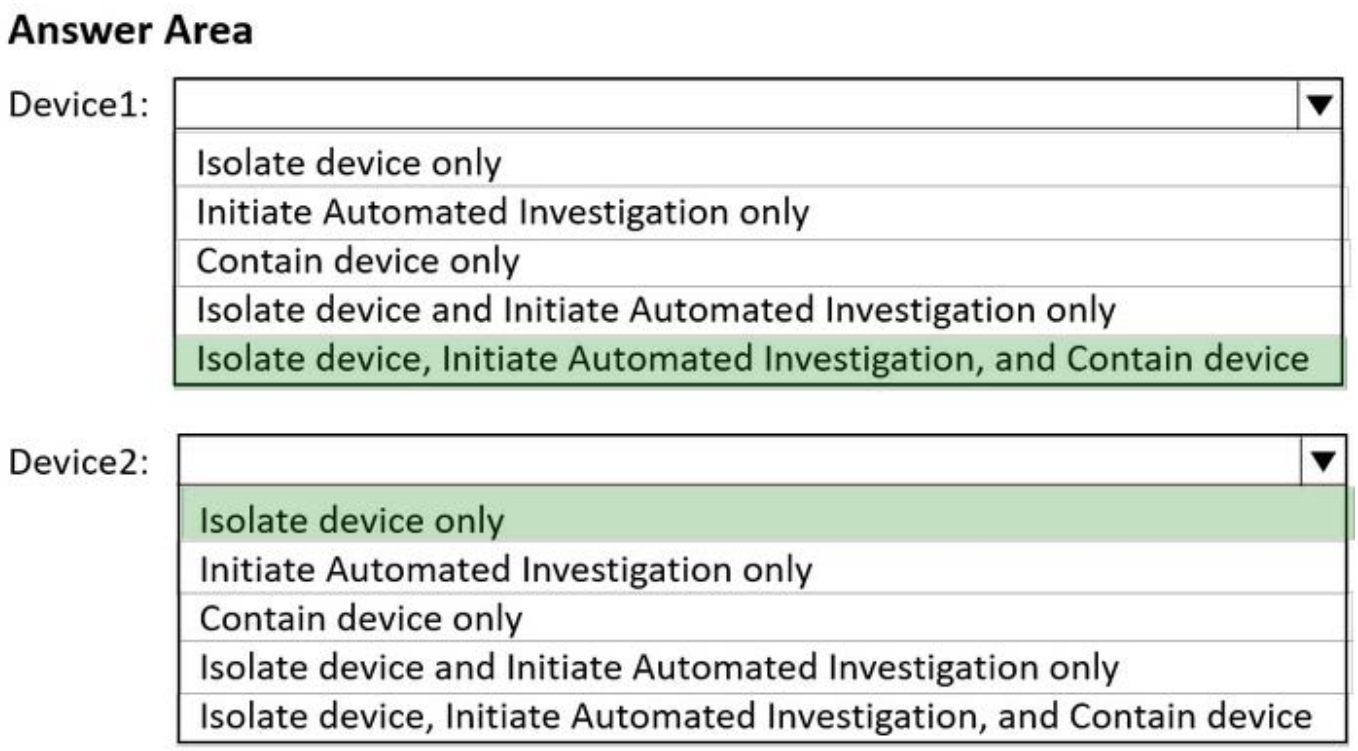
Device1:

- Isolate device only
- Initiate Automated Investigation only
- Contain device only
- Isolate device and Initiate Automated Investigation only
- Isolate device, Initiate Automated Investigation, and Contain device

Device2:

- Isolate device only
- Initiate Automated Investigation only
- Contain device only
- Isolate device and Initiate Automated Investigation only
- Isolate device, Initiate Automated Investigation, and Contain device

Correct Answer:



QUESTION 11

HOTSPOT

You have an Azure subscription that contains a user named User1 and a Microsoft Sentinel workspace named WS1.

You deploy Advanced Security Information Model (ASIM) authentication parsers to WS1.

You need to use the parsers to query the authentication events generated by User1 during the last 24 hours. The solution must maximize the performance of the query.

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

NOTE: Each correct selection is worth one point.

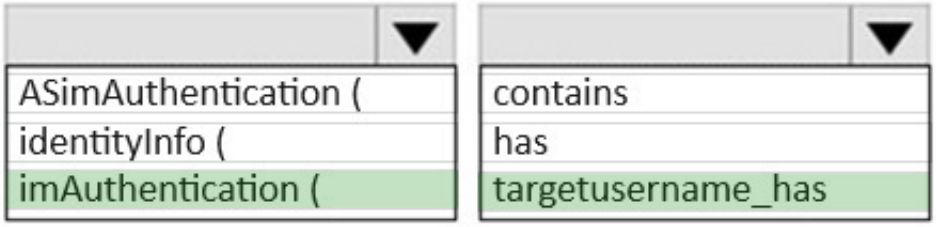
Hot Area:

Answer Area


```
= 'user1', starttime = ago(1d), endtime=now())
```

Correct Answer:

Answer Area

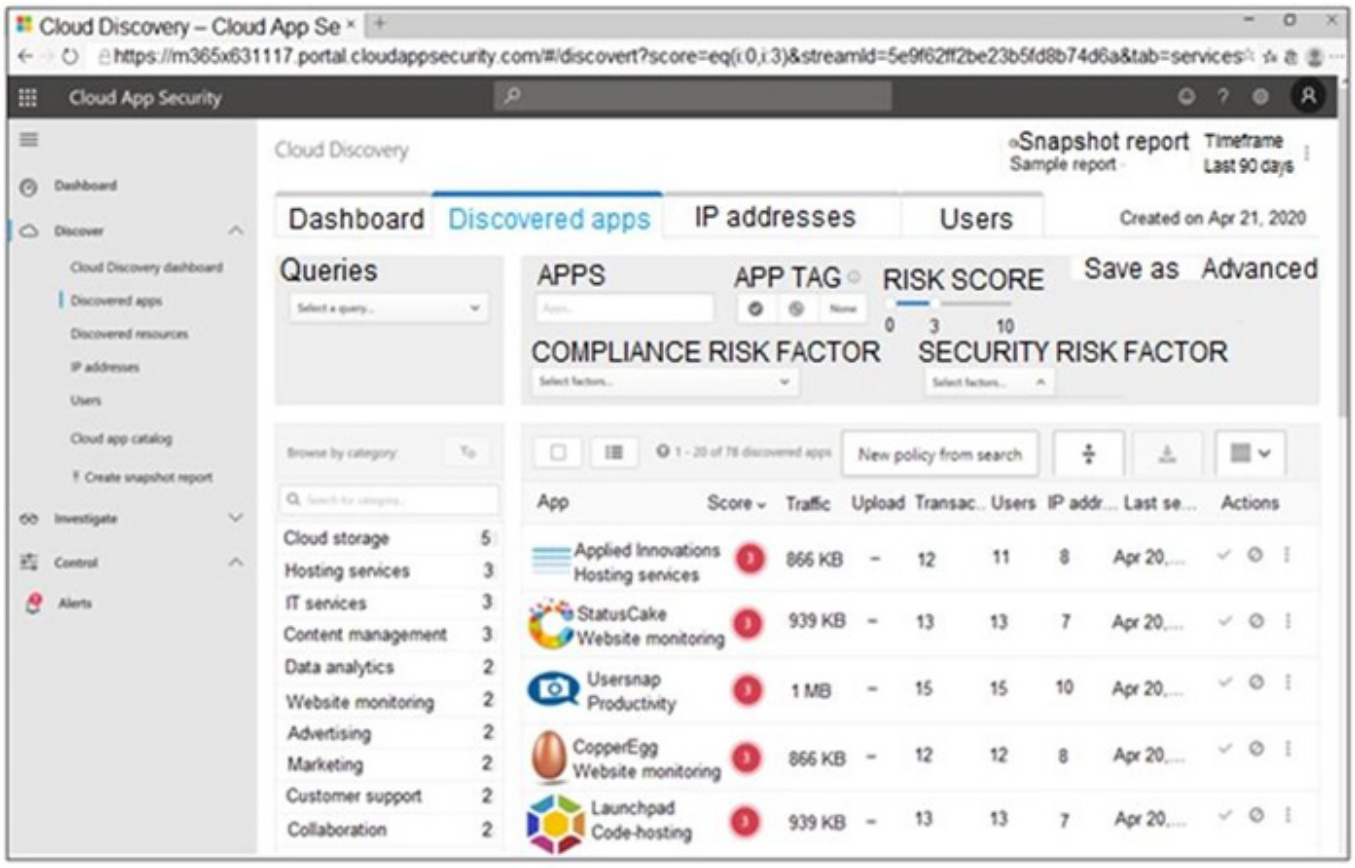



```
= 'user1', starttime = ago(1d), endtime=now())
```

QUESTION 12

DRAG DROP

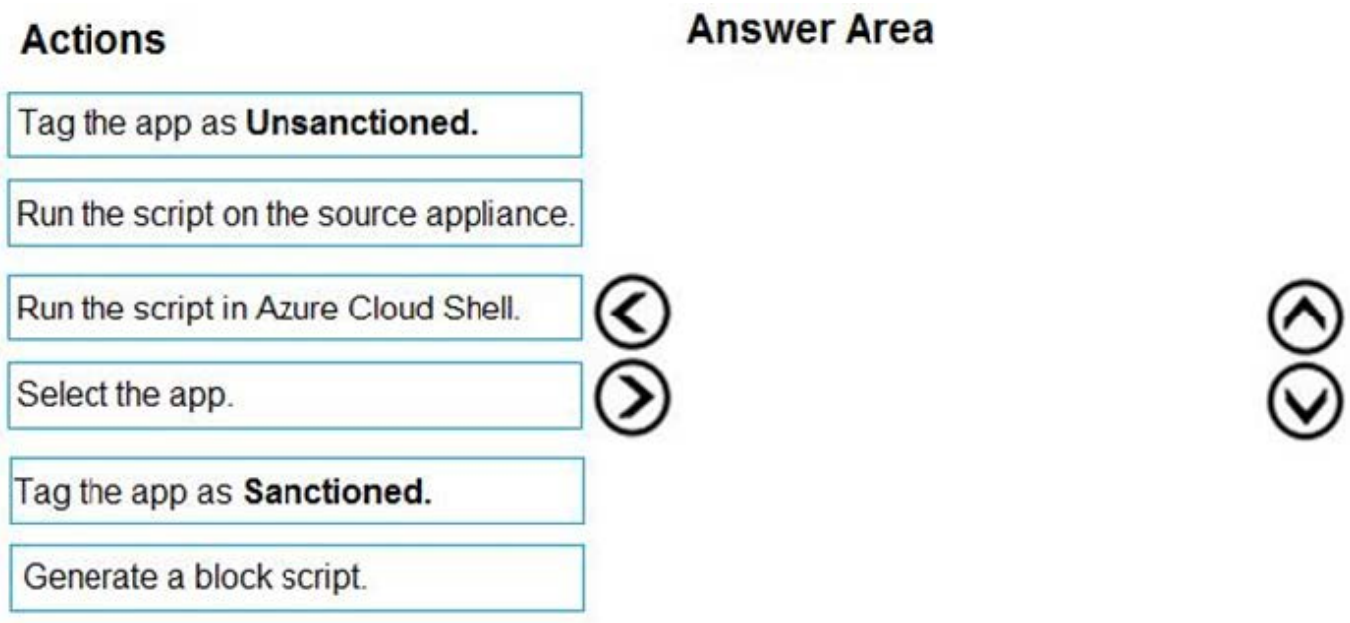
You open the Cloud App Security portal as shown in the following exhibit.



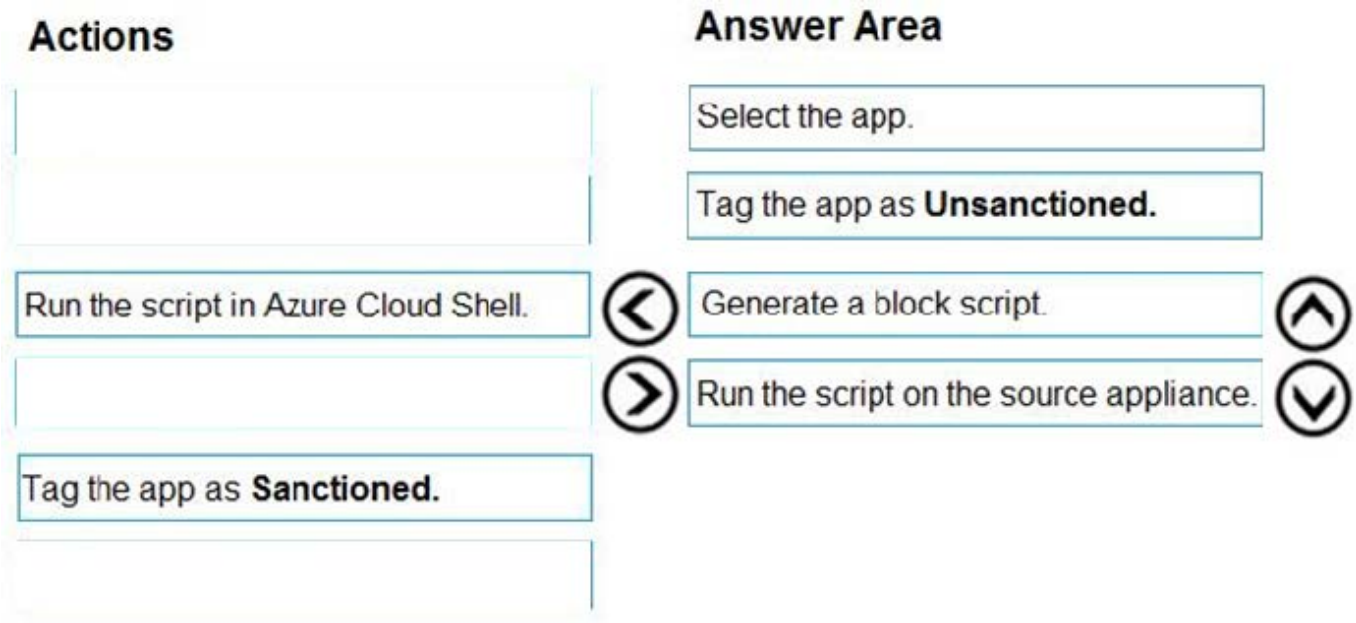
You need to remediate the risk for the Launchpad app.

Which four 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:



Correct Answer:



Reference: https://docs.microsoft.com/en-us/cloud-app-security/governance-discovery

QUESTION 13

You need to recommend a solution to meet the technical requirements for the Azure virtual machines. What should you include in the recommendation?

A. just-in-time (JIT) access

B. Azure Defender

C. Azure Firewall

D. Azure Application Gateway

Correct Answer: B

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

QUESTION 14

You are investigating an incident in Azure Sentinel that contains more than 127 alerts.

You discover eight alerts in the incident that require further investigation.

You need to escalate the alerts to another Azure Sentinel administrator.

What should you do to provide the alerts to the administrator?

A. Create a Microsoft incident creation rule

B. Share the incident URL

C. Create a scheduled query rule

D. Assign the incident

Correct Answer: D

Reference: https://docs.microsoft.com/en-us/azure/sentinel/investigate-cases

QUESTION 15

You recently deployed Azure Sentinel.

You discover that the default Fusion rule does not generate any alerts. You verify that the rule is enabled.

You need to ensure that the Fusion rule can generate alerts.

What should you do?

A. Disable, and then enable the rule.

B. Add data connectors

C. Create a new machine learning analytics rule.

D. Add a hunting bookmark.

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/azure/sentinel/connect-data-sources

Latest SC-200 Dumps SC-200 Study Guide SC-200 Exam Questions