SC-200Q&As

Microsoft Security Operations Analyst

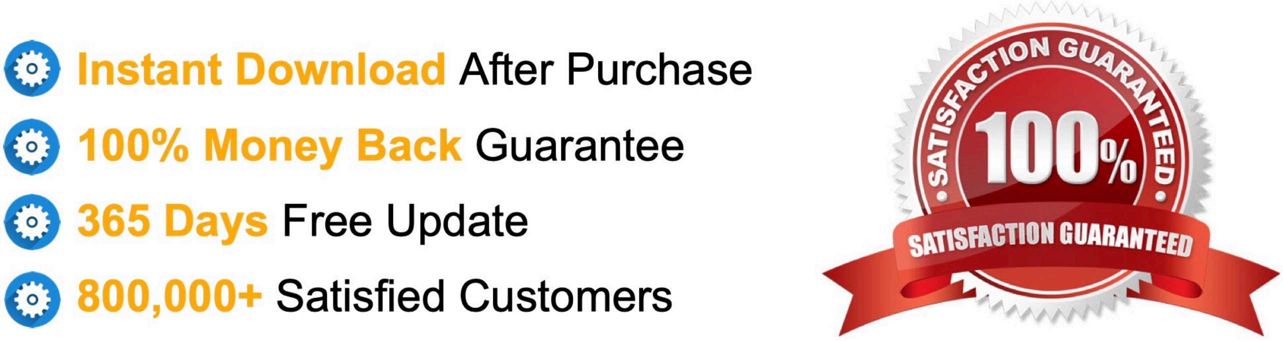
Pass Microsoft SC-200 Exam with 100% Guarantee

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

https://www.pass2lead.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
SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

You have an Azure Sentinel workspace.

You need to test a playbook manually in the Azure portal.

From where can you run the test in Azure Sentinel?

A. Playbooks

B. Analytics

C. Threat intelligence

D. Incidents

Correct Answer: D

Reference: https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook#run-a-playbook-on-demand

---

QUESTION 2

You have a Microsoft 365 subscription that uses Azure Defender.

You have 100 virtual machines in a resource group named RG1.

You assign the Security Admin roles to a new user named SecAdmin1.

You need to ensure that SecAdmin1 can apply quick fixes to the virtual machines by using Azure Defender. The solution must use the principle of least privilege.

Which role should you assign to SecAdmin1?

A. the Security Reader role for the subscription

B. the Contributor for the subscription

C. the Contributor role for RG1

D. the Owner role for RG1

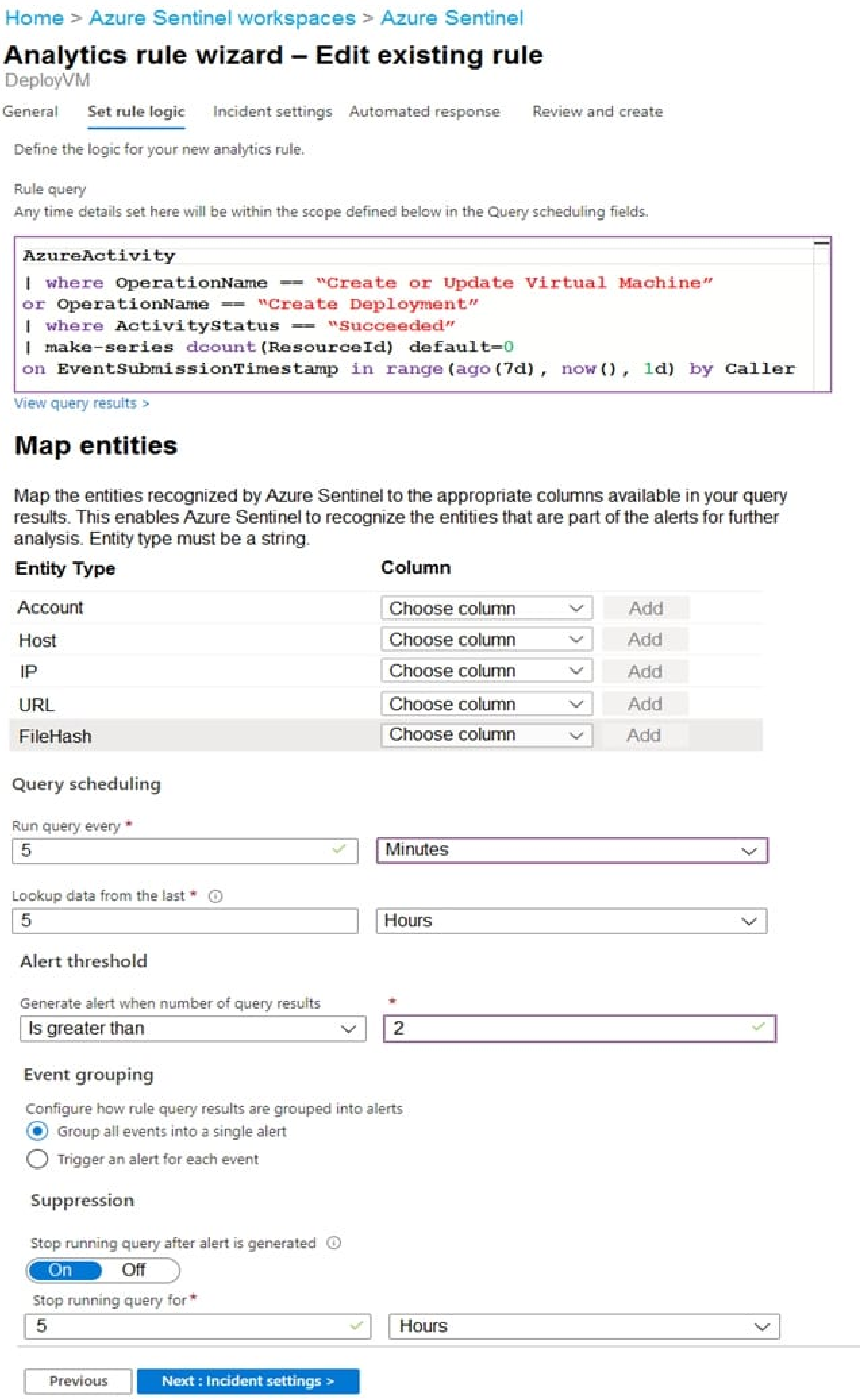
Correct Answer: C

QUESTION 3

HOTSPOT

You use Azure Sentinel to monitor irregular Azure activity.

You create custom analytics rules to detect threats as shown in the following exhibit.



Home > Azure Sentinel workspaces > Azure Sentinel

Analytics rule wizard – Edit existing rule

DeployVM

Define the logic for your new analytics rule.

Rule query

Any time details set here will be within the scope defined below in the Query scheduling fields.

```
AzureActivity
| where OperationName == "Create or Update Virtual Machine"
or OperationName == "Create Deployment"
| where ActivityStatus == "Succeeded"
| make-series dcount(ResourceId) default=0
on EventSubmissionTimestamp in range(ago(7d), now(), 1d) by Caller
```

View query results >

Map entities

Map the entities recognized by Azure Sentinel to the appropriate columns available in your query results. This enables Azure Sentinel to recognize the entities that are part of the alerts for further analysis. Entity type must be a string.

Entity Type	Column	
Account	Choose column	Add
Host	Choose column	Add
IP	Choose column	Add
URL	Choose column	Add
FileHash	Choose column	Add

Query scheduling

Run query every * 5 Minutes

Lookup data from the last * 5 Hours

Alert threshold

Generate alert when number of query results * Is greater than 2

Event grouping

Configure how rule query results are grouped into alerts

● Group all events into a single alert

○ Trigger an alert for each event

Suppression

Stop running query after alert is generated: On

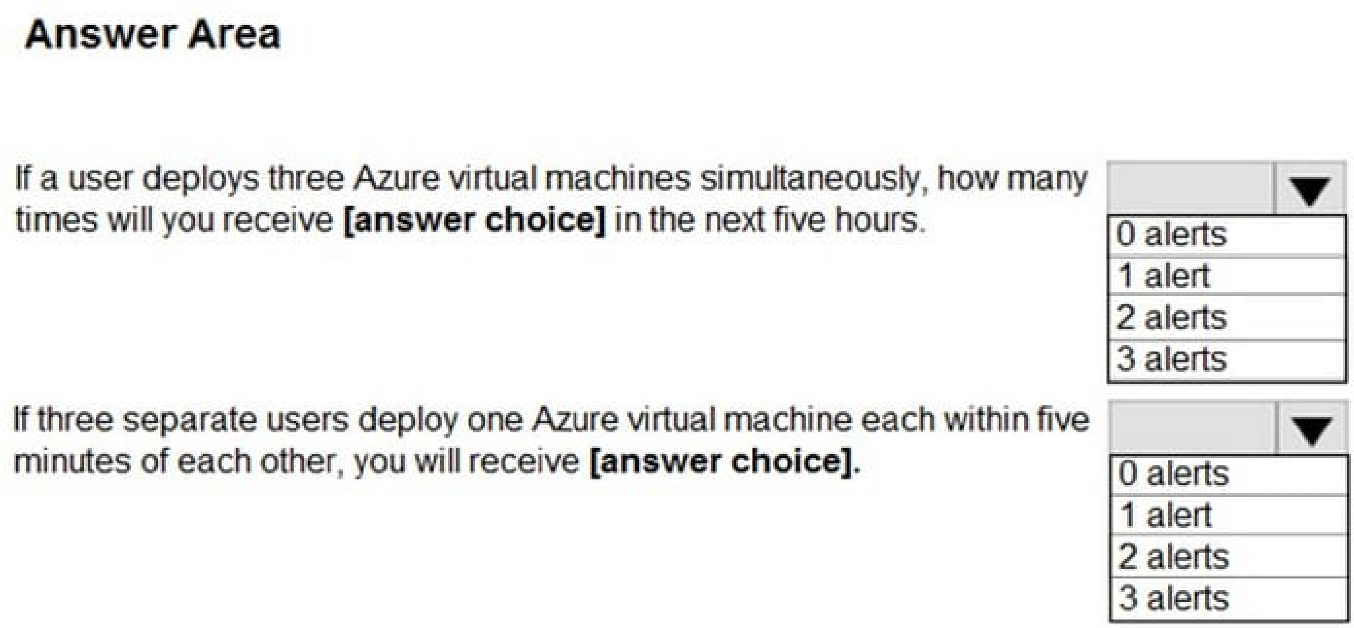
Stop running query for * 5 Hours

You do NOT define any incident settings as part of the rule definition.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

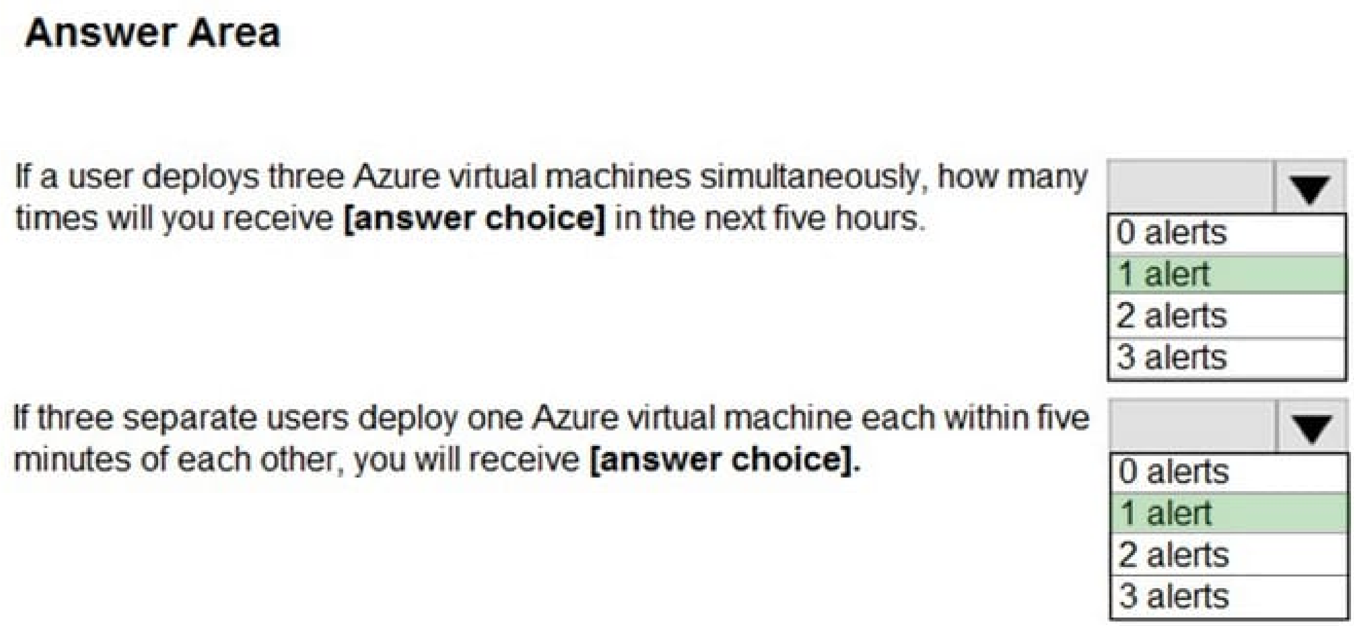
If a user deploys three Azure virtual machines simultaneously, how many times will you receive **[answer choice]** in the next five hours.

- 0 alerts
- 1 alert
- 2 alerts
- 3 alerts

If three separate users deploy one Azure virtual machine each within five minutes of each other, you will receive **[answer choice]**.

- 0 alerts
- 1 alert
- 2 alerts
- 3 alerts

Correct Answer:



Answer Area

If a user deploys three Azure virtual machines simultaneously, how many times will you receive **[answer choice]** in the next five hours.

- 0 alerts
- [✓ 1 alert]
- 2 alerts
- 3 alerts

If three separate users deploy one Azure virtual machine each within five minutes of each other, you will receive **[answer choice]**.

- 0 alerts
- [✓ 1 alert]
- 2 alerts
- 3 alerts

Reference: https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom

QUESTION 4

You have a Microsoft Sentinel workspace.

You receive multiple alerts for failed sign in attempts to an account.

You identify that the alerts are false positives.

You need to prevent additional failed sign-in alerts from being generated for the account. The solution must meet the following requirements:

1.

Ensure that failed sign-in alerts are generated for other accounts.

2.

Minimize administrative effort What should do?

A. Create an automation rule.

B. Create a watchlist.

C. Modify the analytics rule.

D. Add an activity template to the entity behavior.

Correct Answer: A

There are two methods for avoiding false positives:

Automation rules create exceptions without modifying analytics rules.

Scheduled analytics rules modifications permit more detailed and permanent exceptions.

Automation rules

Can apply to several analytics rules.

Keep an audit trail. Exceptions prevent incident creation, but alerts are still recorded for audit purposes.

Are often generated by analysts.

Allow applying exceptions for a limited time. For example, maintenance work might trigger false positives that outside the maintenance timeframe would be true incidents.

Incorrect:

Not A: Analytics rules modifications

Allow advanced boolean expressions and subnet-based exceptions.

Let you use watchlists to centralize exception management.

Typically require implementation by Security Operations Center (SOC) engineers.

Are the most flexible and complete false positive solution, but are more complex

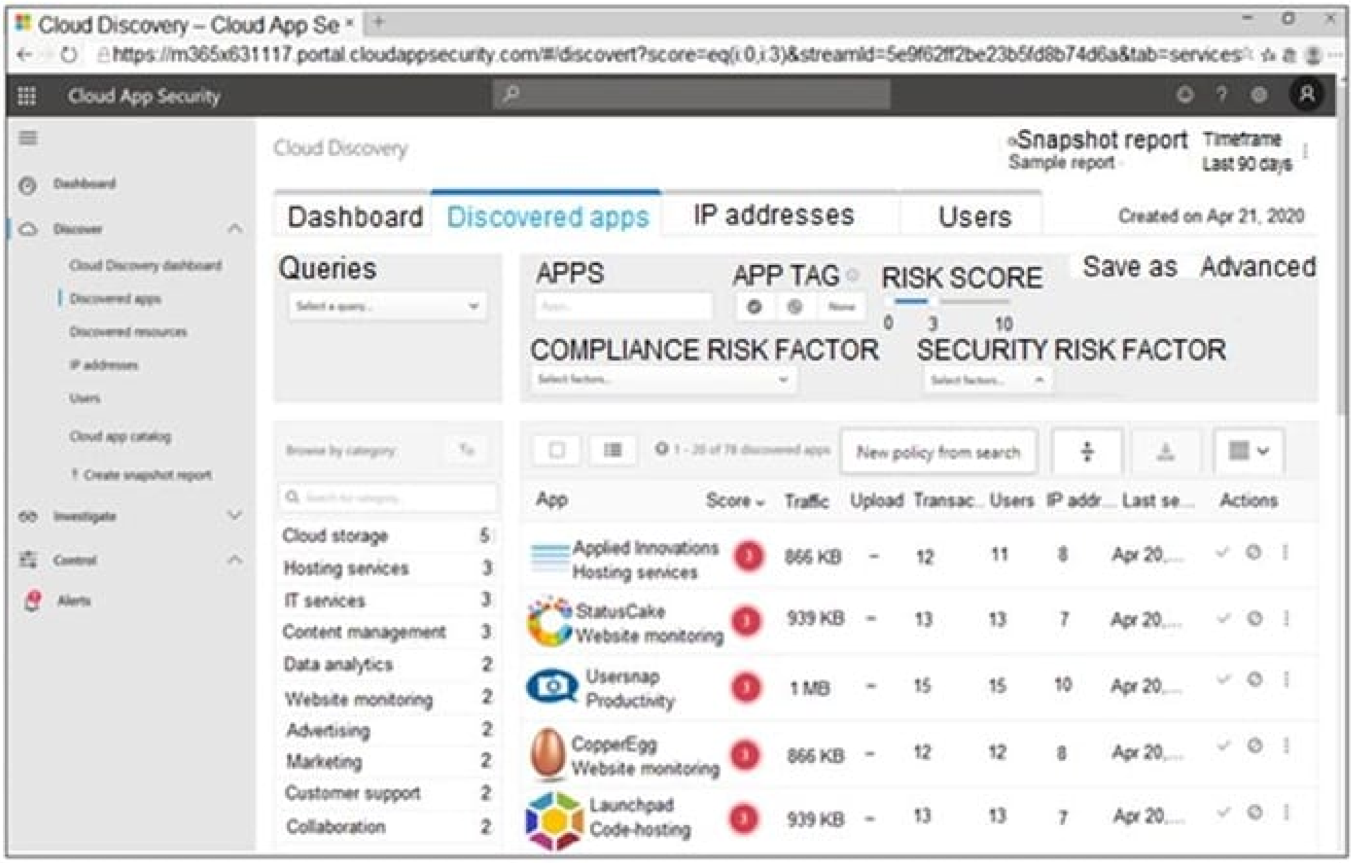
Reference:

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

QUESTION 5

DRAG DROP

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



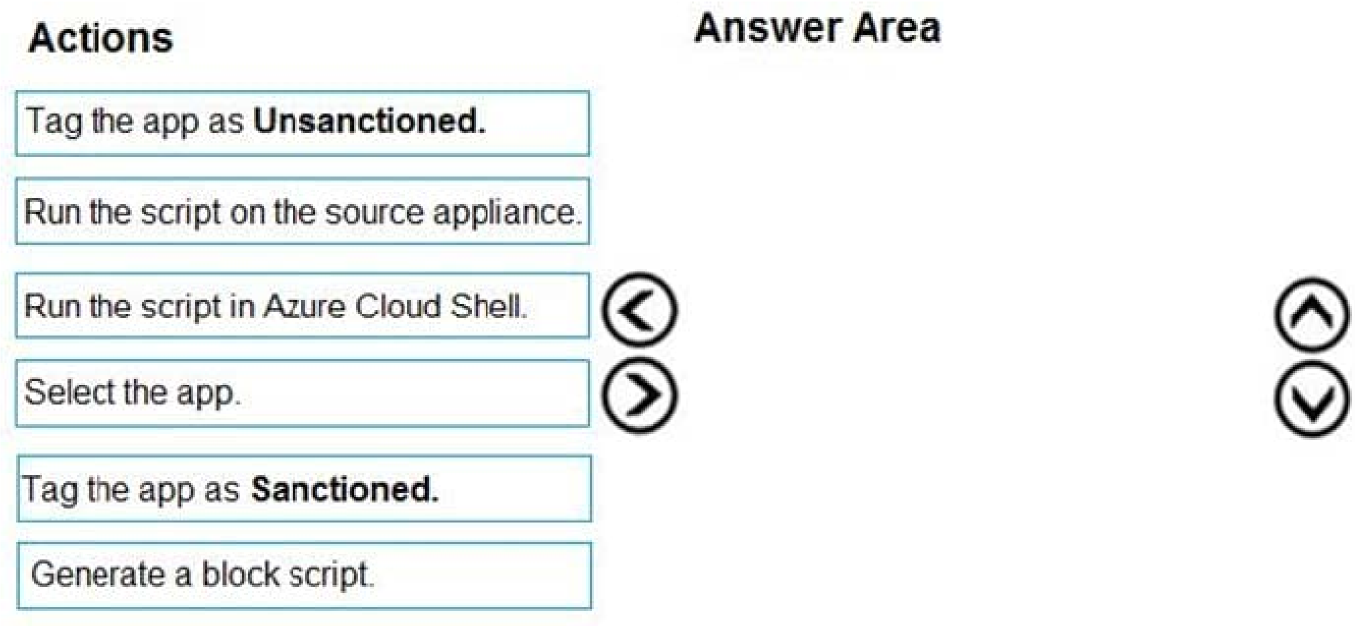
Cloud storage	5
Hosting services	3
IT services	3
Content management	3
Data analytics	2
Website monitoring	2
Advertising	2
Marketing	2
Customer support	2
Collaboration	2

App	Score	Traffic	Upload	Transac...	Users	IP addr...	Last se...	Actions
Applied Innovations Hosting services	[illegible]	866 KB	-	12	11	8	Apr 20,...	✓ ⊘ ⋮
StatusCake Website monitoring	[illegible]	939 KB	-	13	13	7	Apr 20,...	✓ ⊘ ⋮
Usersnap Productivity	[illegible]	1 MB	-	15	15	10	Apr 20,...	✓ ⊘ ⋮
CopperEgg Website monitoring	[illegible]	866 KB	-	12	12	8	Apr 20,...	✓ ⊘ ⋮
Launchpad Code-hosting	[illegible]	939 KB	-	13	13	7	Apr 20,...	✓ ⊘ ⋮

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:



Actions

Tag the app as **Unsanctioned.**

Run the script on the source appliance.

Run the script in Azure Cloud Shell.

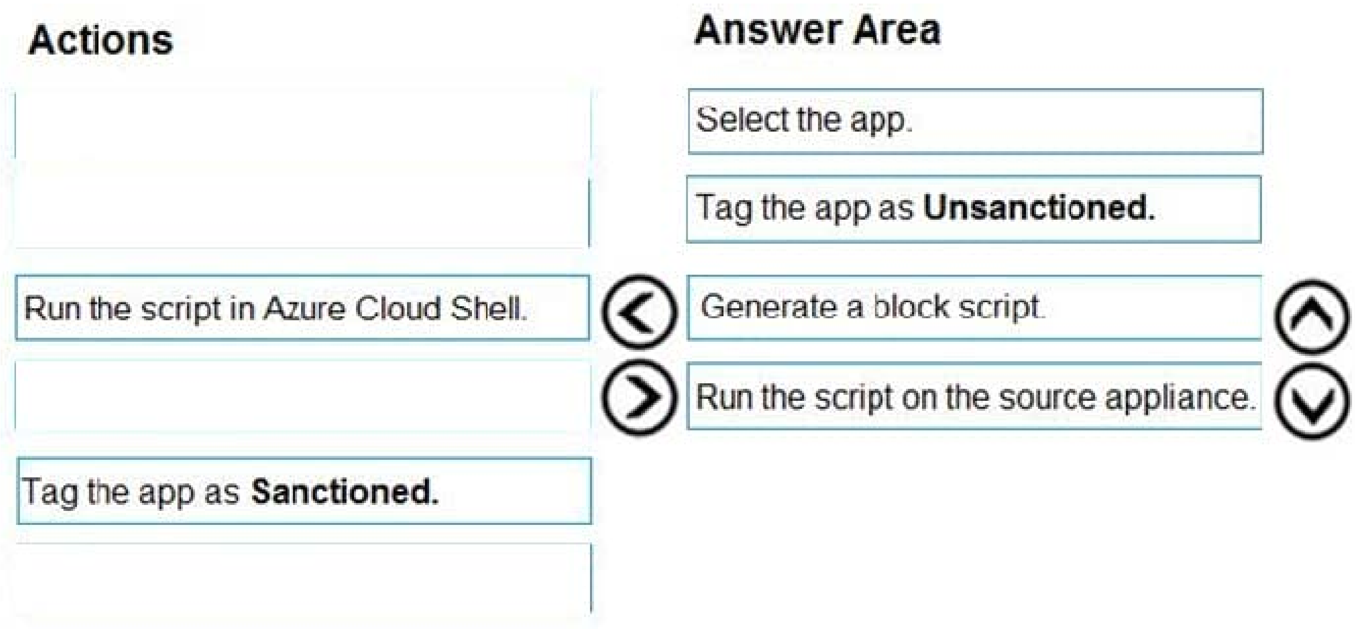
Select the app.

Tag the app as **Sanctioned.**

Generate a block script.

Answer Area

Correct Answer:



Actions

Run the script in Azure Cloud Shell.

Tag the app as **Sanctioned.**

Answer Area

Select the app.

Tag the app as **Unsanctioned.**

Generate a block script.

Run the script on the source appliance.

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

SC-200 PDF Dumps SC-200 Exam Questions SC-200 Braindumps