AZ-500 3 - Manage Security Operations

Test ID: 195407318

Question #1 of 25

Question ID: 1416309

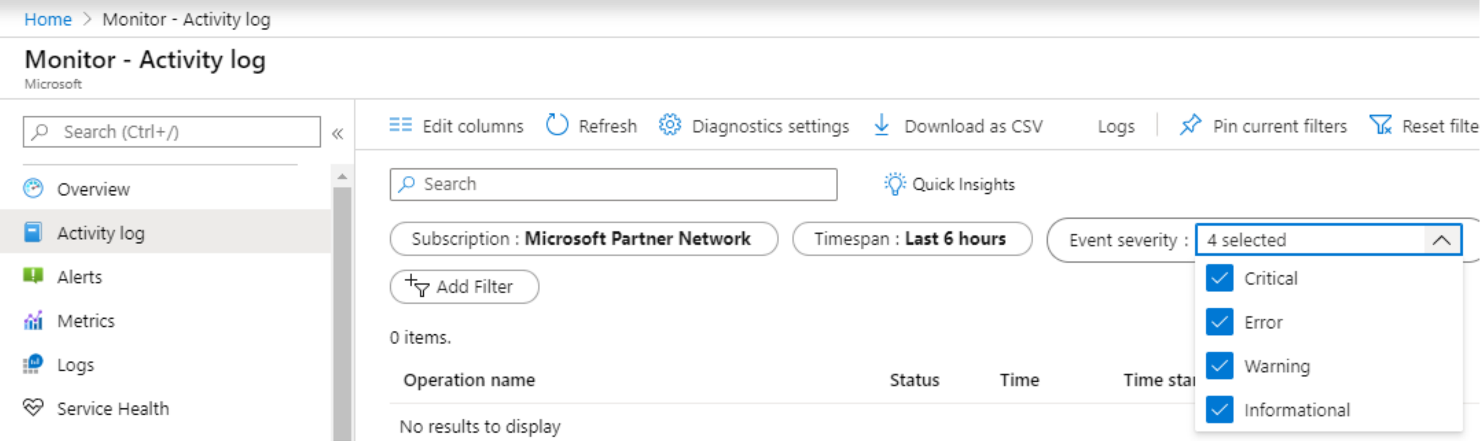
You need to troubleshoot how a user was able to modify resources in a resource group. You notice that resources were modified at least six months ago. You need to look back in the logs as far as you can.

How long are Activity Logs kept in a Subscription?

- ✓ **A)** 90 days
- ✗ **B)** 365 days
- ✗ **C)** Until resource will be deleted
- ✗ **D)** 180 days

Explanation

Activity Logs are kept for 90 days by default. You can search the Activity log in the Azure Portal by choosing Monitor > Activity Log based on subscription, timespan, severity, or resource group.



Subscription : **Microsoft Partner Network**

Timespan : **Last 6 hours**

Event severity : 4 selected

☑ Critical
☑ Error
☑ Warning
☑ Informational

0 items.

No results to display

You can also use the **Get-AzLog** cmdlet to retrieve log entries. The following retrieves log entries from the resource group named **NutexResource** for the past 21 days:

```
Get-AzLog -ResourceGroup ExampleGroup -StartTime (Get-Date).AddDays(-21)
```

Objective:

Manage security operations

Sub-Objective:

Monitor security by using Azure Monitor

References:

Azure > View activity logs to monitor actions on resources

Question #2 of 25

Question ID: 1380983

You are working on the Enterprise Security team for your company. A junior administrator created 263 Windows Server virtual machines (VMs) across five regions with the default configuration. The auditor team detected that your company underwent a brute-force password attack and other cyber-criminal attacks from all over the world.

Where can you find this information?

- ✓ **A)** Security Center - Security alerts map
- ✗ **B)** Security Center - Adaptive application controls
- ✗ **C)** NSG flow logs
- ✗ **D)** Security Center - Identity & Access

Explanation

You should use the security alerts map in Security Center. The security alerts map helps you identify threats against your environment. For example, you can identify if a threat is part of a botnet and where that threat is coming from. Security Center uses data from multiple sources within Microsoft to build this map. To see current threats, open Security Center. In the left pane of the dashboard, under Threat Protection select Security alerts map.

You should not use NSG flow logs. This option can allow investigating of network logs, but the investigation must be performed manually.

You should not use Security Center - Adaptive application controls. Adaptive application controls help you deal with malicious and/or unauthorized software, by allowing only specific applications to run on your VMs/servers. This option in Security Center will not map out threats against your environment.

You should not use Security Center - Identity & Access. This option in Security Center identifies security vulnerabilities in your environment. It provides recommendations that can harden and protect your resources. This option in Security Center will not map out threats against your environment.

Objective:
Manage security operations

Sub-Objective:
Monitor security by using Azure Security Center

References:

Azure > Security Center > Security alerts map and threat intelligence

---

Question #3 of 25

Question ID: 1380978

You are working as an Enterprise Azure administrator. You modified some policies created by the Security Center Standard Plan. Some policies should apply automatically.

What do you need to do first to apply policies automatically?

- ✗ **A)** Define a remediation task.
- ✓ **B)** Create a managed identity.
- ✗ **C)** Modify policies to use the AuditIfNotExists feature.
- ✗ **D)** Define the scope of the assignment.

Explanation

You should create a managed identity. Policies with the deployIfNotExists need to access to your Azure resources using the managed identity. Managed identity assigned to a specific resource allows one to modify another resource and, in this way, apply policies.

You should not define a remediation task. – It will not apply policies but only can define another task to do.

You should not define the scope of the assignment. It will not apply policies but change the scope of working this policy.

You should not modify policies to use the AuditIfNotExists feature. It will not apply policies, and this property is already set, just because the default behavior is to audit not to make changes.

Objective:
Manage security operations

Sub-Objective:
Monitor security by using Azure Security Center

References:

Azure > Governance > Policy > Remediate non-compliant resources with Azure Policy

Question #4 of 25

Question ID: 1380970

You are part of the Azure Security team at the Nutex Corporation. Nutex wants to create effective baselines to monitor the health of Azure resources. You are tasked with configuring Azure Monitor metric alerts that meet the following criteria:

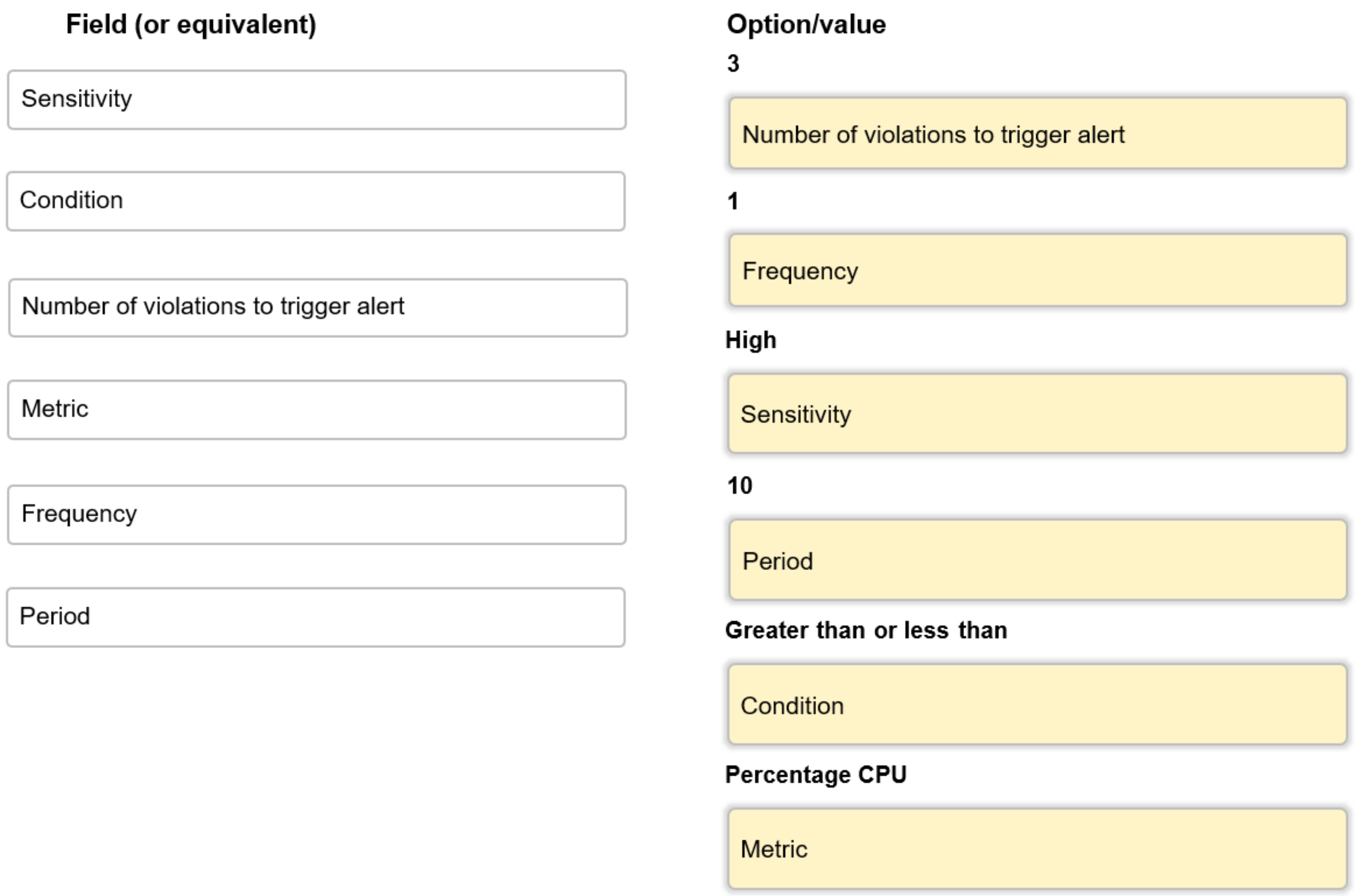
- Alerts must be generated based on the metrics' historical behavior and identify patterns and anomalies.
- Alerts must be generated for the smallest deviation from the normal value.
- Alerts must be generated only after three deviations from the normal value.
- Alert must be generated by checking values once every 10 minutes.

Match the fields (or equivalents) to create alerts in Azure on the left with the option or value to be specified on the right.

{UCMS id=5126276068147200 type=Activity}

Explanation

You would map the fields with their option or value as follows:



Field (or equivalent)

- Sensitivity
- Condition
- Number of violations to trigger alert
- Metric
- Frequency
- Period

Option/value	
3	Number of violations to trigger alert
1	Frequency
High	Sensitivity
10	Period
Greater than or less than	Condition
Percentage CPU	Metric

Metric alerts can be created for platform metrics, custom metrics, popular logs from Azure Monitor converted to metrics, and Application Insights metrics. Metric alerts are set for the metrics of a target resource. When the metric meets the condition and the expectancy you set for the alert, alerts are generated. Azure checks the metrics at regular intervals. Metric alerts can be created on the Azure Monitor – Alerts page. Metric alerts use the following fields:

Condition – This field specifies the upper and/or lower threshold value of the metric, below or above which alerts must be triggered. The options are: greater than the upper threshold or lower than the lower threshold (default), greater than the upper threshold, and lower than the lower threshold. In this case, greater than or less than.

Sensitivity – This field controls the level of deviations from the upper or lower thresholds. The options available are High (alert rule will be triggered on the smallest deviation), Medium (fewer alerts than with high sensitivity (default)), and Low (alert rule will only trigger on large deviations). In this case, it is set to High.

Metric – Metrics are used as Dimensions when creating a rule. For example, Percentage CPU usage or Percentage Memory usage. In this case, it is Percentage CPU.

Frequency – This field represents how frequently in the “period” the metric alert checks if the conditions are met. This is usually less than the period. In this case, 1.

Period – This field is the time measurement of how far back to go to check for metrics. In this case, 10 minutes.

Number of violations to trigger the alert is an advanced setting that lets you define the minimum number of deviations required within a certain time window to generate an alert (the default time window is four deviations in 20 minutes). In this case, 3.

Objective:
Manage security operations

Sub-Objective:
Monitor security by using Azure Monitor

References:

Microsoft Azure > Azure Monitor > Understand how metric alerts work in Azure Monitor

Microsoft Azure > Azure Monitor > Metric Alerts with Dynamic Thresholds in Azure Monitor

Microsoft Azure > Azure Monitor > Create, view, and manage metric alerts using Azure Monitor

Microsoft Tech Community > Getting started with Azure Monitor Dynamic Thresholds

---

Question #5 of 25

Question ID: 1380985

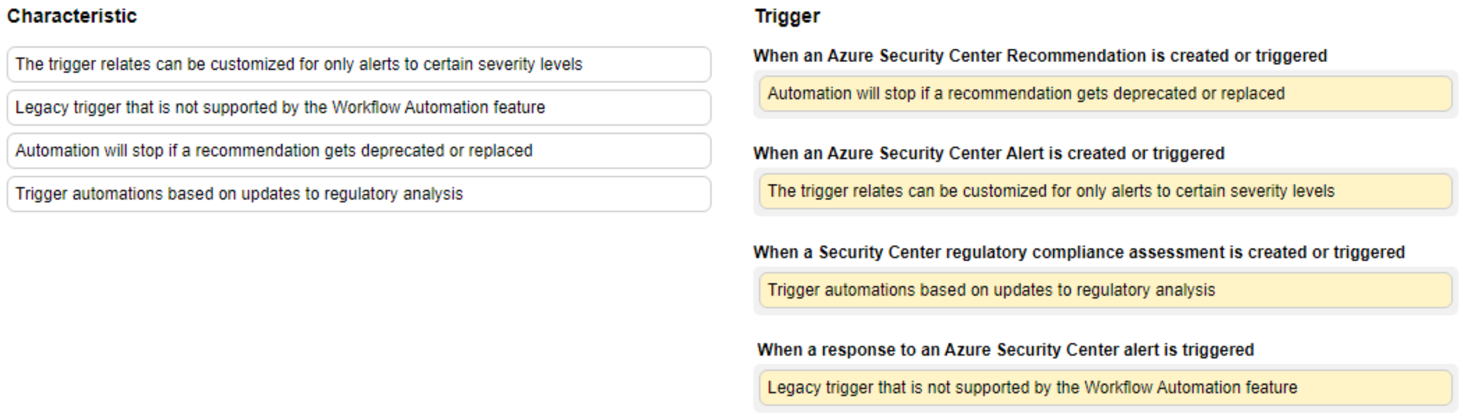
Your company has a developed a security program that includes multiple workflows for incident response. These processes include notifying the IT department, launching the change management process, and applying a remedy. You would like to automate as many steps as possible. You create a workflow automation for a Logic App in Security Center that will run when trigger conditions are met.

Match the proper Security Center trigger that is supported by the logic app designer.

{UCMS id=6254981318443008 type=Activity}

Explanation

You should choose the following:



Characteristic

- The trigger relates can be customized for only alerts to certain severity levels
- Legacy trigger that is not supported by the Workflow Automation feature
- Automation will stop if a recommendation gets deprecated or replaced
- Trigger automations based on updates to regulatory analysis

Trigger

When an Azure Security Center Recommendation is created or triggered

Automation will stop if a recommendation gets deprecated or replaced

When an Azure Security Center Alert is created or triggered

The trigger relates can be customized for only alerts to certain severity levels

When a Security Center regulatory compliance assessment is created or triggered

Trigger automations based on updates to regulatory analysis

When a response to an Azure Security Center alert is triggered

Legacy trigger that is not supported by the Workflow Automation feature

The "**When a response to an Azure Security Center alert is triggered**" trigger is not supported by the logic app designer. This is a legacy trigger that cannot launch logic apps in the Workflow Automation feature. You should use one of the following triggers:

- **When an Azure Security Center Recommendation is created or triggered**
- **When an Azure Security Center Alert is created or triggered**
- **When a Security Center regulatory compliance assessment is created or triggered**

If you use the **"When an Azure Security Center Recommendation is created or triggered"** trigger, your automation will stop working. You will need to update the trigger if the logic app relies on a recommendation that becomes deprecated or replaced.

If you use the **"When an Azure Security Center Alert is created or triggered"** trigger, you will be able to customize the trigger so that it relates only to alerts with the severity levels that you specify.

If you use the **"When a Security Center regulatory compliance assessment is created or triggered"** trigger, trigger automations are based on any changes made to regulatory compliance assessments.

Objective:

Manage security operations

Sub-Objective:

Monitor security by using Azure Security Center

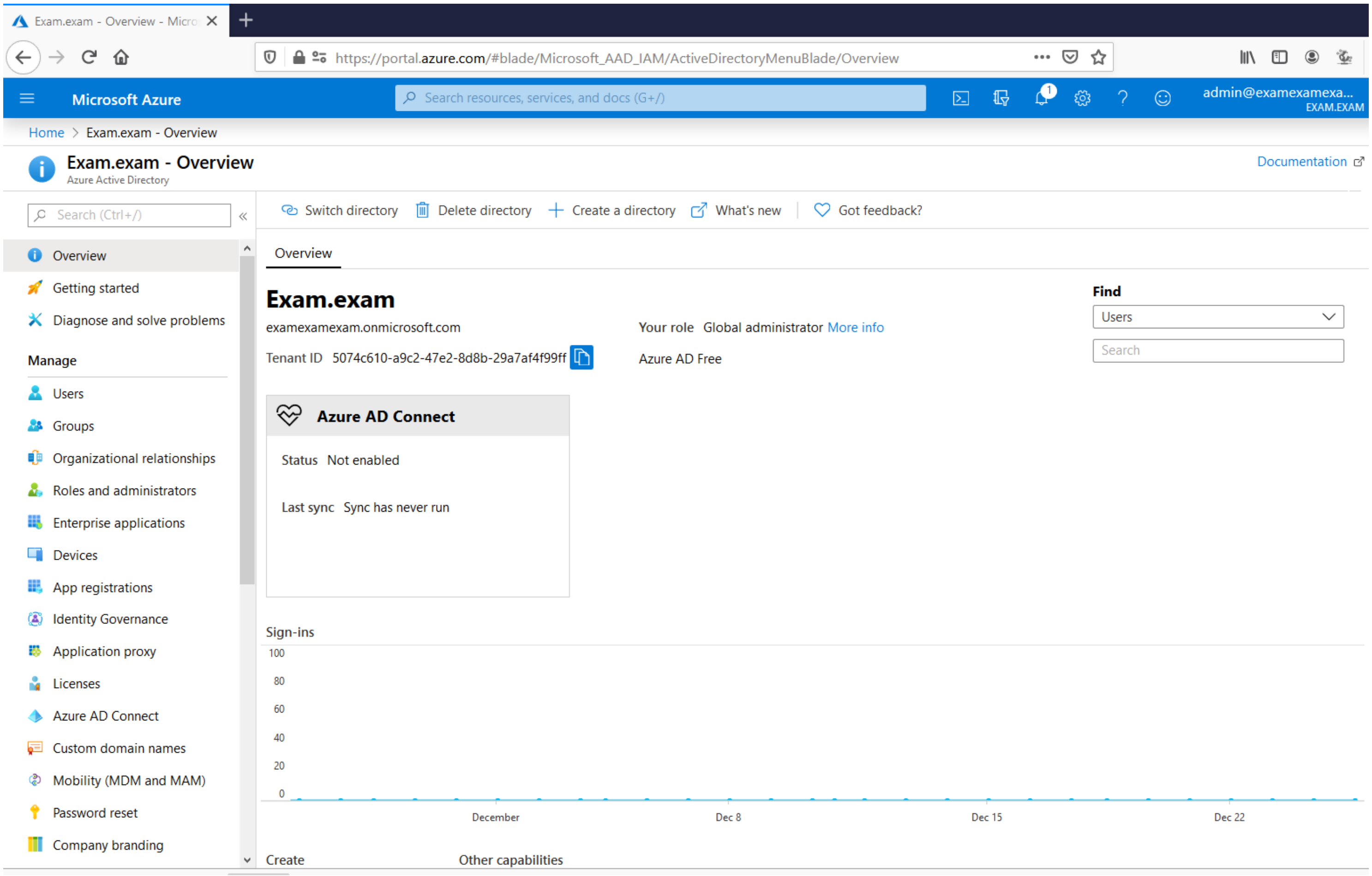
References:

Workflow automation in Azure Security Center | Microsoft Docs

Question #6 of 25

Question ID: 1380980

You are working as an Enterprise Azure Administrator. You just created a new Azure Subscription. The following displays your Azure Active Directory blade:



Exam.exam

examexamexam.onmicrosoft.com

Tenant ID 5074c610-a9c2-47e2-8d8b-29a7af4f99ff

Your role Global administrator More info

Azure AD Free

Azure AD Connect

Status Not enabled

Last sync Sync has never run

You need to enable Just in Time (JIT) VM Administration for VM01 and VM03. What steps do you need to perform?

✗ **A)** Upgrade to Azure Active Directory P1 plan.

✗ **B)** Upgrade to Azure Active Directory P2 plan.

✓ **C)** Enable JIT for VM01 and VM03.

✗ **D)** Add user group to the Contributors role of VM01 and VM03.

✓ **E)** Upgrade to Standard tier of Security Center.

Explanation

You should upgrade to Standard tier of Security Center. The Just in Time (JIT) feature is available on the Standard tier of the Security Center.

You should enable JIT for VM01 and VM03. In this way, we give access using JIT strategy to the selected VMs.

You should not upgrade to the Azure Active Directory P1 or P2 plan. Azure Active Directory P1 or P2 Plan is not necessary to run JIT functionality.

You should not add user group to the Contributors role of VM01 and VM03. This privilege is too wide in this scenario. In this way, we can give access without JIT functionality.

Objective:
Manage security operations

Sub-Objective:
Monitor security by using Azure Security Center

References:

Azure > Security Center > Manage virtual machine access using just-in-time

Question #7 of 25

Question ID: 1416310

You have created a security policy in Azure Security Center. You notice that your environment does not follow the policy that you created. You want to add a custom initiative to your subscription.

Which of the following are true regarding custom initiatives?

- ✗ **A)** A custom standards must be added at the resource group level for them to be evaluated and displayed in Security Center.
- ✗ **B)** Creating new initiatives requires subscription contributor credentials
- ✗ **C)** Microsoft recommends that a custom initiative use the narrowest scope required for the assignment
- ✓ **D)** Recommendations for your custom initiative appear if your environment does not follow your defined policies

Explanation

Recommendations for your custom initiative appear if your environment does not follow your defined policies.

Microsoft recommends custom initiative use the widest scope, not narrowest scope, required for the assignment.

To create new initiatives requires subscription owner credentials, not contributor credentials.

Custom standards must be added at the subscription level (or higher), not the resource group level, for them to be evaluated and displayed in Security Center.

Objective:

Manage security operations

Sub-Objective:

Monitor security by using Azure Security Center

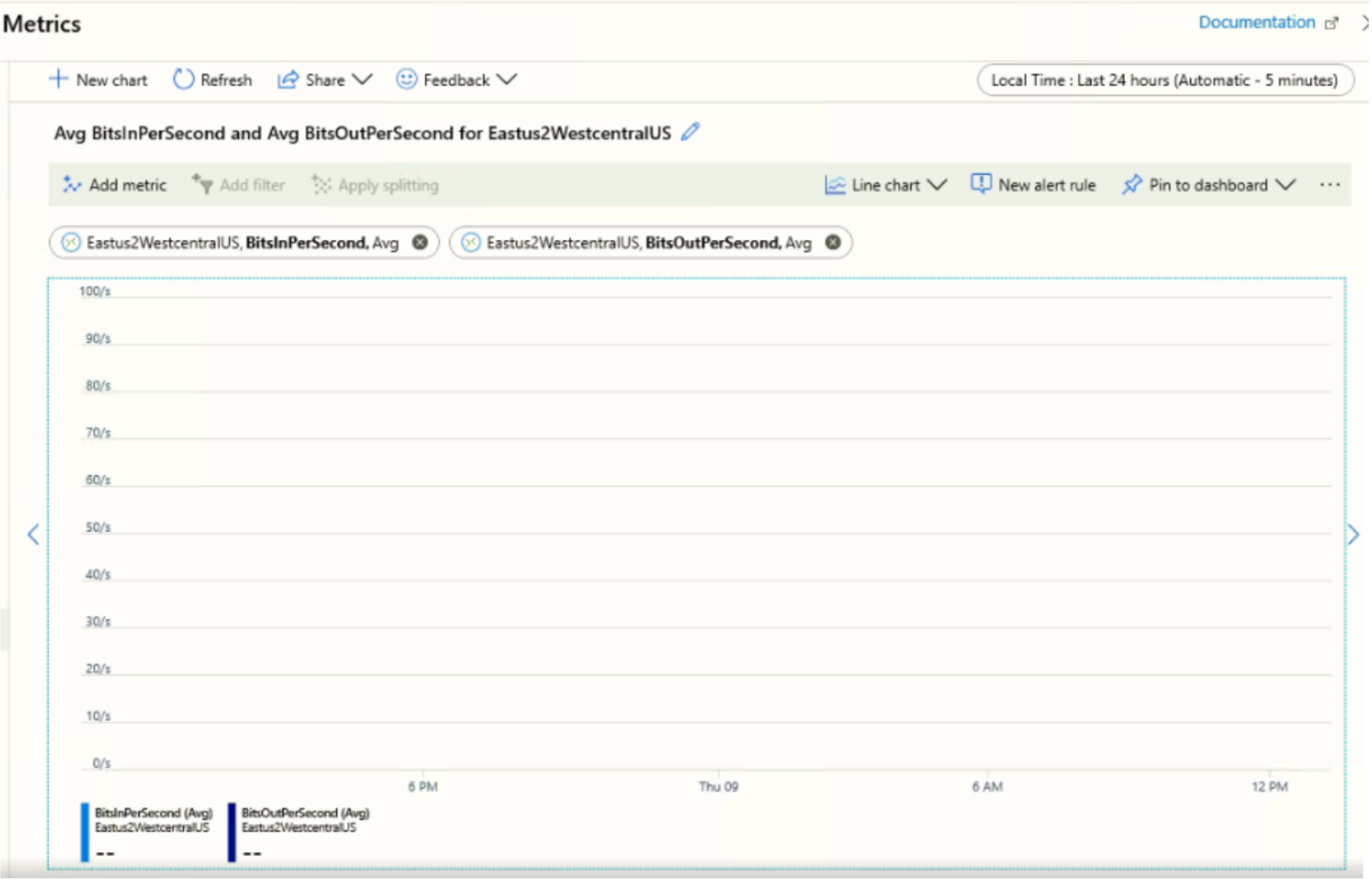
References:

Azure > Security Center > Using custom security policie

Question #8 of 25

Question ID: 1380969

The audit department found an unused connection in Virtual Network Gateway. You checked the metrics and saw the following:



It would be best if you implemented a solution informs you when any traffic appears on this connection.

What should you do?

- ✗ **A)** Use an Azure Firewall
- ✗ **B)** Configure a network security group
- ✗ **C)** Use Network Watcher
- ✓ **D)** Use an alert Rule

Explanation

It would be best if you used an alert rule. With an alert rule, you can be informed by email when the metric will reach a value. You can set an alert value on any of the metrics the connection.

Network Watcher can capture the traffic or check the connection, but you would still need an alert rule to be notified.

You should not use an Azure Firewall and/or network security group. You can block access to a connection with Azure Firewall or a network security group.

Objective:
Manage security operations

Sub-Objective:
Monitor security by using Azure Monitor

References:

Azure > Overview of alerts in Microsoft Azure

Question #9 of 25

Question ID: 1380982

You are working on the Enterprise Security team for your company. You need to check and verify whether NSG rules applied to virtual machines are equivalent. Which option should you use?

- ✗ **A)** Security Center - Security alerts map
- ✗ **B)** NSG flow logs
- ✓ **C)** Security Center - Adaptive network hardening
- ✗ **D)** Security Center - Adaptive application controls

Explanation

You should use Security Center - Adaptive Network Hardening. You can use network security groups (NSG) to filter traffic, which can improve security. You may want to improve security by hardening the NSG rules based on traffic patterns. Security Center - Adaptive Network Hardening can recommend how to harden the NSG rules. For example, you may have an NSG rule to allow traffic from 192.168.1.0/24 on port 22. The Adaptive Network Hardening's recommendation, based on the analysis, would be to narrow the range and allow traffic from 192.168.1.0/29 – which is a much narrower IP range – and to deny all other traffic to that port.

You should not use NSG flow logs. This option can allow investigating of network logs for suspicious traffic, but the investigation must be manually done.

You should not use Security Center - Security alert map. The security alerts map helps you identify threats against your environment. For example, you can identify if a threat is part of a botnet and where that threat is coming from. Security Center uses data from multiple sources within Microsoft to build this map. The security alert map will not harden your NSG rules.

You should not use Security Center - Adaptive application controls. This feature in Security Center helps you deal with malicious and/or unauthorized software by allowing only specific applications to run on your VMs/servers. Adaptive application controls will not harden your NSG rules.

Objective:
Manage security operations

Sub-Objective:
Monitor security by using Azure Security Center

References:

Azure > Security Center > Adaptive Network Hardening in Azure Security Center

Azure > Security Center > Adaptive application controls

Question #10 of 25

Question ID: 1380973

You are a cloud architect at Nutex Corporation. You have created three virtual machines in the following groups and locations:

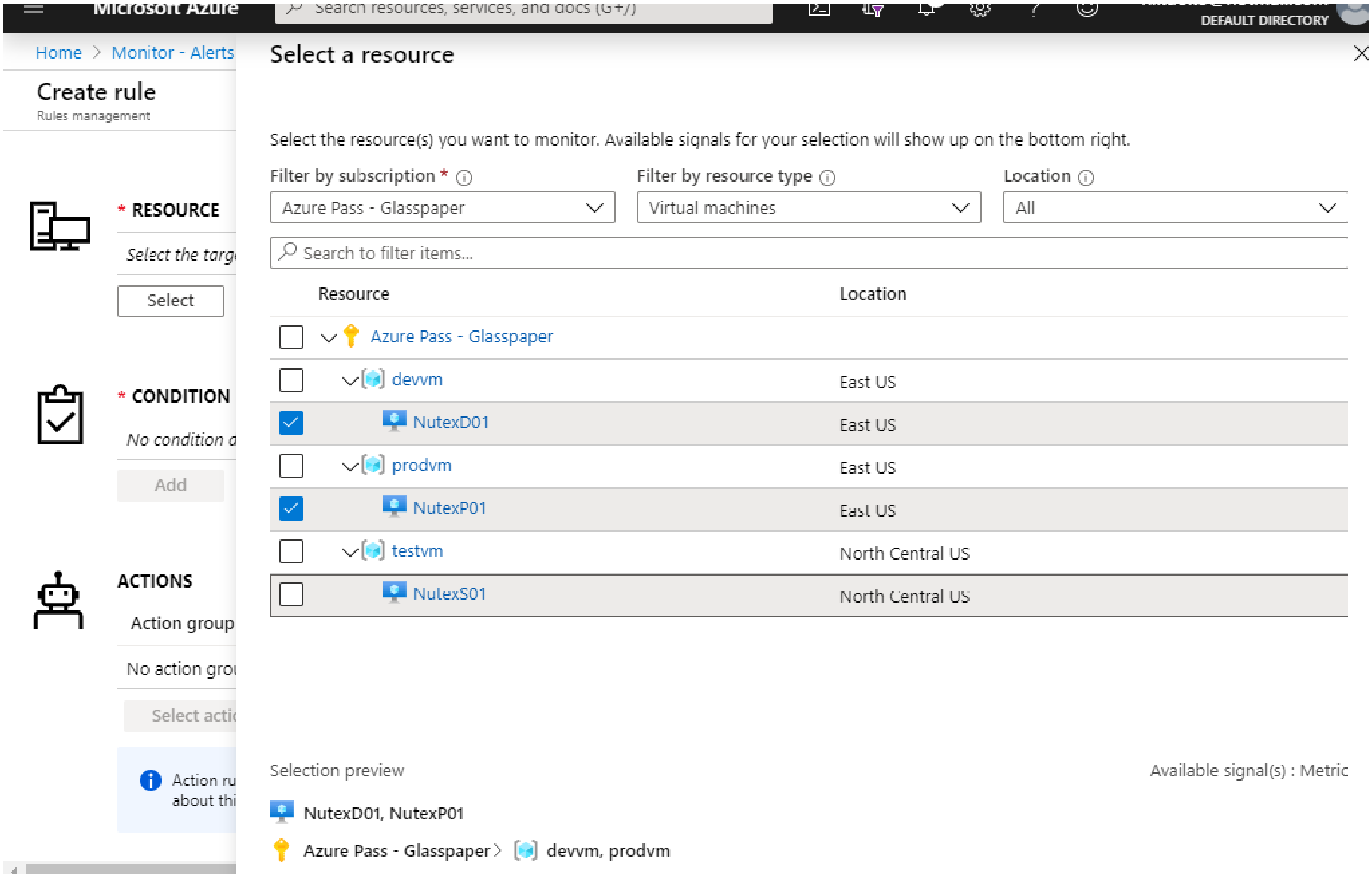
VM Name	Resource group	Location
NutexD01	devvm	East US
NutexP01	prodvm	East US
NutexS01	testvm	North Central US

You need to configure metric alerts for these virtual machines. Which solution will be the most efficient to implement?

- ✗ **A)** Configure one alert for the devvm and testvm resource groups, and one alert for the prodvm resource group.
- ✗ **B)** Configure three alerts per virtual machine.
- ✗ **C)** Configure one alert for all three virtual machines.
- ✓ **D)** Configure one alert for NutexD01 and NutexP01, and one alert rule for NutexS01.

Explanation

You would configure one alert for NutexD01 and NutexP01 and one alert rule for NutexS01. Because the NutexD01 and NutexP01 resources are in the same location, they can be grouped into one alert (as shown in the image):



Select a resource

Select the resource(s) you want to monitor. Available signals for your selection will show up on the bottom right.

Filter by subscription *: Azure Pass - Glasspaper
Filter by resource type: Virtual machines
Location: All

Search to filter items...

	Resource	Location
□	Azure Pass - Glasspaper	
□	devvm	East US
☑	NutexD01	East US
□	prodvm	East US
☑	NutexP01	East US
□	testvm	North Central US
□	NutexS01	North Central US

Selection preview

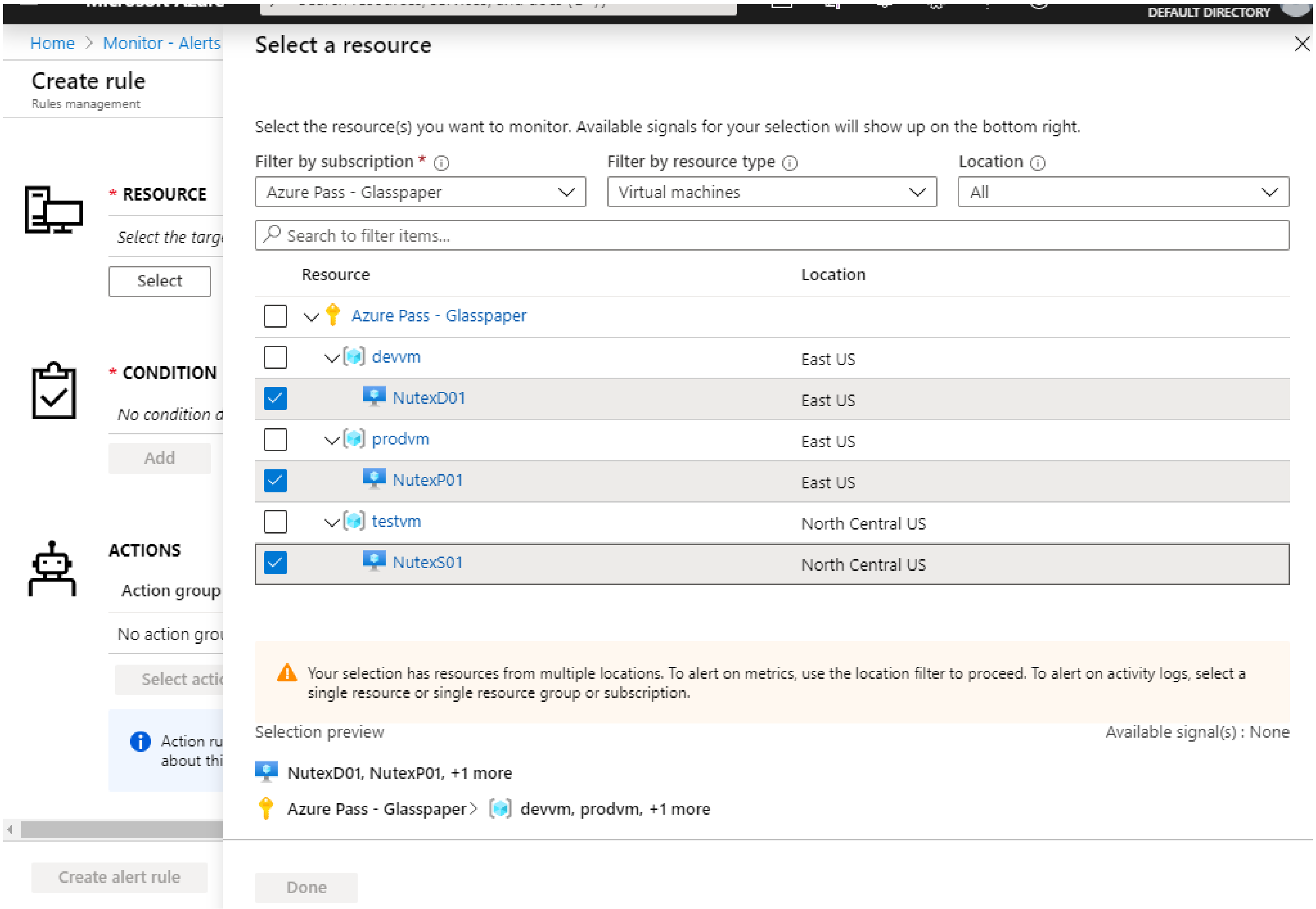
Available signal(s) : Metric

NutexD01, NutexP01

Azure Pass - Glasspaper > devvm, prodvm

NutexS01 is another location and thus would need a different alert than NutexD01 and NutexP01.

You would not configure one alert for all three virtual machines because the virtual machines are in different locations and it is not possible to group them, as shown in the image:



Home > Monitor - Alerts

Create rule

Rules management

* RESOURCE

Select the targ

Select

* CONDITION

No condition a

Add

ACTIONS

Action group

No action grou

Select acti

Action ru
about thi

Create alert rule

Select a resource

Select the resource(s) you want to monitor. Available signals for your selection will show up on the bottom right.

Filter by subscription *: Azure Pass - Glasspaper

Filter by resource type: Virtual machines

Location: All

Search to filter items...

	Resource	Location
□	Azure Pass - Glasspaper	
□	devvm	East US
☑	NutexD01	East US
□	prodvm	East US
☑	NutexP01	East US
□	testvm	North Central US
☑	NutexS01	North Central US

⚠ Your selection has resources from multiple locations. To alert on metrics, use the location filter to proceed. To alert on activity logs, select a single resource or single resource group or subscription.

Selection preview

Available signal(s) : None

NutexD01, NutexP01, +1 more

Azure Pass - Glasspaper > devvm, prodvm, +1 more

Done

You would not configure three alerts for every virtual machine because that is not the optimal solution as described above.

You would not configure one alert for the devvm and testvm resource groups and one alert for the prodvm resource group. The virtual machines in the devm and testvm resource groups are in different locations and cannot work together, as shown in the image.

Objective:

Manage security operations

Sub-Objective:

Monitor security by using Azure Monitor

References:

Microsoft Azure > Blog > Monitoring > Monitor at scale in Azure Monitor with multi-resource metric alerts

Question #11 of 25

Question ID: 1380988

You have noticed that malicious attackers have accessed your network resources. You want to automate and orchestrate a response to potentially dangerous threats in your Azure environment.

What should you configure in Azure Sentinel to respond to the threats?

- ✗ **A)** logic app
- ✓ **B)** playbook
- ✗ **C)** alert
- ✗ **D)** event

Explanation

You should create a playbook. A playbook consists of one or more logic apps that can be run automatically or manually when you receive an alert. When an alert is sent to Azure Sentinel, a playbook can be automatically run.

A logic app is a cloud service that can automate or schedule tasks. You can create logic apps for other services, but you must associate a logic app with a playbook with Azure Sentinel. In Azure Sentinel, the playbook, not the logic app, responds to the alert.

You would not create an alert. The alert should be configured elsewhere in Security Center. Azure Sentinel allows you to see insights and visibility of the alerts.

You would not create an event. The event would be written to a log that could be read by other services.

Objective:
Manage security operations

Sub-Objective:
Monitor security by using Azure Sentinel

References:

Home > Azure > Azure Sentinel > Logic Apps vs Playbooks and new Sentinel incident trigger

Azure > Azure Sentinel > Tutorial: Set up automated threat responses in Azure Sentinel

Question #12 of 25

Question ID: 1380986

You are working with the enterprise security team. The CEO asked you to advise the most powerful tool that can detect possible volatilities in your company. You need to cover Windows Server 2012 R2 and Linux servers.

Which of the following is the best tool to recommend?

- ✗ **A)** Microsoft Defender Advanced Threat Protection
- ✓ **B)** Azure Sentinel
- ✗ **C)** Azure Advanced Threat Protection (ATP)
- ✗ **D)** Azure Security Center

Explanation

Azure Sentinel is the most powerful tool to detect abnormal behaviors in not only the cloud environment but on-premises as well. It is based on Workspaces where logs are stored. Azure Sentinel allows you to collect data from all users, devices, applications on-premises, or in multiple clouds. When paired with Microsoft analytics. It can find undetected threats while minimizing false positives.

At the time of this writing, Microsoft Defender Advanced Threat Protection (ATP) and Azure Advanced Threat Protection do not support Linux operating systems. Advanced Threat Protection collects usage data and can safeguard your enterprise against threats, but is not as powerful as Azure Sentinel in finding undetected threats and volatilities.

Azure Security Center is a less powerful service than Azure Sentinel but does allow you to spot abnormalities.

Azure Security Center is a security information event management (SIEM) and security orchestration automated response (SOAR) solution while Security Center is not.

Objective:
Manage security operations

Sub-Objective:
Monitor security by using Azure Sentinel

References:

Azure > What is Azure Sentinel?

Azure > Microsoft Defender Advanced Threat Protection with Azure Security Center

Microsoft Blog > Threat hunting in Azure Advanced Threat Protection (ATP)

Question #13 of 25

Question ID: 1380993

You want to have the company’s Azure Architect sketch a project’s design parameters with a repeatable Azure resource that implements and adheres to the company’s standards and requirements.

You need to assign Jeff the following permissions regarding Azure Blueprints.

- Create new blueprint, but not create new assignments
- Create support tickets
- View role and role assignments
- Create deployments

Which role should you assign adhering to the principle of least privilege?

✗ **A)** Owner

✗ **B)** Contributor

✗ **C)** Blueprint Contributor

✓ **D)** Blueprint Operator

Explanation

A Blueprint Operator cannot create new blueprints but can assign existing blueprints. A Blueprint Operator has the following permissions:

Task	Permissions
Read roles and role assignments	Microsoft.Authorization/*/read
Create and manage blueprint assignments.	Microsoft.Blueprint/blueprintAssignments/*
Retrieves or lists resource groups.	Microsoft.Resources/subscriptions/resourceGroups/read
Create and manage a deployment	Microsoft.Resources/deployments/*
Create and update a support ticket	Microsoft.Support/*

A Blueprint Contributor cannot assign blueprints but can manage blueprint definitions. A Blueprint Contributor has the following permissions.

Task	Permissions
Read roles and role assignments	Microsoft.Authorization/*/read
Create and manage blueprint definitions or blueprint artifacts.	Microsoft.Blueprint/blueprints/*
Retrieves or lists resource group	Microsoft.Resources/subscriptions/resourceGroups/read
Create and manage a deployment	Microsoft.Resources/deployments/*
Create and update a support ticket	Microsoft.Support/*

A Contributor cannot assign blueprint permissions but can create and delete blueprint definitions. A Contributor can grant full access to someone else to manage all resources. However, you can not assign roles in Azure RBAC.

An Owner can create and manage resources of all types, including blueprints. An Owner can assign roles in Azure RBAC and grant full access to manage all resources.

Objective:
Manage security operations

Sub-Objective:
Configure security policies

References:

Azure > Governance > Blueprints > What is Azure Blueprints?

Question #14 of 25

Question ID: 1380971

You are working on the Enterprise Security team, and you need to configure an alert that sends you an email when new resources appear that are not compliant with policy1512.

Which custom log search do you choose?

✗ **A)**

```
let policyDefId = 'policy1512’; AzureActivity | where Category ==
'Policy' and Level != 'Informational' | extend
p=todynamic(Properties) | extend
policies=todynamic(tostring(p.policies)) | mvexpand policy =
policies | where policy.policyDefinitionName in (policyDefId) |
distinct ResourceId
```

✗ **B)**

```
AzureActivity | where Category == 'Policy' and Level !=
'Informational' | extend p=todynamic(Properties) | extend
policies=todynamic(tostring(p.policies)) | mvexpand policy =
policies | where p.isComplianceCheck == 'False
```

✗ **C)**
```
AzureActivity | where Category == 'Policy' and Level !=
'Informational' | extend p=todynamic(Properties) | extend
policies=todynamic(tostring(p.policies)) | mvexpand policy =
policies | summarize resource_count=count() by
tostring(policy.policyDefinitionName)
```

✓ **D)**
```
let policyDefId = 'policy1512'; AzureActivity | where Category ==
'Policy' and Level != 'Informational' | extend
p=todynamic(Properties) | extend
policies=todynamic(tostring(p.policies)) | mvexpand policy =
policies | where policy.policyDefinitionName in (policyDefId) and
p.isComplianceCheck == 'False'
```

Explanation

You can receive an alert on any newly added non-compliant resources detected by specific policy on a Log Analytics workspace by using the `let` command in the Kusto query language. The following query retrieves all non-compliant resources with policy1512:

```
let policyDefId = 'policy1512'; AzureActivity | where Category == 'Policy' and Level !=
'Informational' | extend p=todynamic(Properties) | extend
policies=todynamic(tostring(p.policies)) | mvexpand policy = policies | where
policy.policyDefinitionName in (policyDefId) and p.isComplianceCheck == 'False'
```

This query can be created on the Log Analytics workspace by clicking on the **Alerts** blade in Azure Monitor, and clicking **New Alert Rules**. You can add conditions in the query by selecting **Custom log search**.

You should not use the following query:

```
let policyDefId = 'policy1512’; AzureActivity | where Category == 'Policy' and Level !=
'Informational' | extend p=todynamic(Properties) | extend
policies=todynamic(tostring(p.policies)) | mvexpand policy = policies | where
policy.policyDefinitionName in (policyDefId) | distinct ResourceId
```

This query sends an alert for all compliant and non-compliant resources for policy1512. We just want to be alerted when a non-compliant resource is added.

You should not use the following query:

```
AzureActivity | where Category == 'Policy' and Level != 'Informational' | extend
p=todynamic(Properties) | extend policies=todynamic(tostring(p.policies)) | mvexpand policy =
policies | summarize resource_count=count() by tostring(policy.policyDefinitionName)
```

Although this query sends an alert for all non-compliant resources, it is not specific to policy1512.

You should not use the following query:

```
AzureActivity | where Category == 'Policy' and Level != 'Informational' | extend
p=todynamic(Properties) | extend policies=todynamic(tostring(p.policies)) | mvexpand policy =
policies | where p.isComplianceCheck == 'False
```

This query sends an alert for all new non-compliant resources, but not specific to policy1512.

Objective:
Manage security operations

Sub-Objective:
Monitor security by using Azure Monitor

References:

Microsoft > How to Create Azure Monitor Alerts for Non-Compliant Azure Policies

---

Question #15 of 25

Question ID: 1380974

Nutex Corporation recently deployed several web applications to the Azure platform. They need to detect problems in real time in order to resolve problems before their customers notice. An alert should be raised when a web server has returned 404: not found or 500: internal server error responses.

What should you recommend in Azure Monitor?

- ✓ **A)** Log
- ✗ **B)** Activity log
- ✗ **C)** Metric
- ✗ **D)** Service Health

Explanation

You would choose Log because Log alerts are based on what is written to log files. For example, a Log alert can notify you when a web server has returned a 404 or 500 response.

You would not choose Activity log because it notifies you when Azure resources change state. For example, an Activity log alert can notify you when a resource is deleted or created.

You would not choose Metric because it provides an alert trigger when a specified numerical threshold is exceeded. For example, a Metric alert can notify you when CPU usage is greater than 85 percent.

You would not choose Service Health because it informs you about issues in Azure services which may affect you in the future.

Objective:
Manage security operations

Sub-Objective:
Monitor security by using Azure Monitor

References:

Microsoft Azure > Azure Monitor > Overview of alerts in Microsoft Azure

---

Question #16 of 25

Question ID: 1380990

You have noticed that malicious attackers have accessed your network resources. You want to automate and orchestrate a response to potentially dangerous threats in your Azure environment.

What should you configure in Azure Sentinel to respond to the threats?

Choose the appropriate steps and place them in the correct order.

{UCMS id=4656991550046208 type=Activity}

Explanation

You should choose the following:

1. Configure a playbook
2. Create a Logic App
3. Configure triggers
4. From the **Alerts** tab, run the playbook

You should create a playbook. A playbook consists of one or more logic apps that can be run automatically or manually when you receive an alert. When an alert is sent to Azure Sentinel, a playbook can be automatically run. In Azure Sentinel, you can select **Playbooks** under **Configuration** to create a playbook. You will then have to specify a logic app or multiple logic apps.

A logic app is a cloud service that can automate or schedule tasks. You can create logic apps for other services, but you must associate a logic app with a playbook with Azure Sentinel. In Azure Sentinel, the playbook, not the logic app, responds to the alert.

You will then specify the connectors and triggers in the playbook. You can select **When a response to an Azure Sentinel alert is triggered** to have a playbook respond to an alert. Triggers and connectors can specify actions, logic conditions, or loops. For example, if an alert triggers a runbook, you could have a logic app that first creates a record, calls another logic app that posts a message, and then creates a condition. The condition may check if the alert is from a blocked user or blocked IP. If the condition is true, you could take a set of actions. If the condition is false, you could take a set of less drastic measures.

If you can run a playbook manually or on-demand from the **Alerts** tab, click on a specific alert and run the playbook you want.

You cannot run a Logic App or trigger a specific alert from the **Alerts** tab.

Objective:
Manage security operations

Sub-Objective:
Configure security policies

References:

Azure > Azure Sentinel > Tutorial: Set up automated threat responses in Azure Sentinel

Question #17 of 25

Question ID: 1380972

You are working on the Enterprise Security team, and you need to configure an alert that sends you an email every day with all non-compliant resources with a resource count.

Which query will you use?

✗ **A)** `AzureActivity | where Category == 'Policy' and Level != 'Informational' | extend p=todynamic(Properties) | extend policies=todynamic(tostring(p.policies)) | mvexpand policy = policies | where p.isComplianceCheck == 'False`

✗ **B)** `where Category == 'Policy' and Level != 'Informational' | extend p=todynamic(Properties) | extend policies=todynamic(tostring(p.policies)) | mvexpand policy = policies | summarize resource_count=count() by tostring(policy.policyDefinitionName)`

✓ **C)** `AzureActivity | where Category == 'Policy' and Level != 'Informational' | extend p=todynamic(Properties) | extend policies=todynamic(tostring(p.policies)) | mvexpand policy = policies | summarize resource_count=count() by tostring(policy.policyDefinitionName)`

✗ **D)** `where Category == 'Policy' and Level != 'Informational' | extend p=todynamic(Properties) | extend policies=todynamic(tostring(p.policies)) | mvexpand policy = policies | where p.isComplianceCheck == 'False`

Explanation

You should use the following query to retrieve all non-compliant resources:

```
AzureActivity | where Category == 'Policy' and Level != 'Informational' | extend
p=todynamic(Properties) | extend policies=todynamic(tostring(p.policies)) | mvexpand policy =
policies | summarize resource_count=count() by tostring(policy.policyDefinitionName)
```

This query gives a resource count of resources that match a policy definition name. Queries of the log can be created on the Log Analytics workspace by clicking on the **Alerts** blade in Azure Monitor, and clicking **New Alert Rules**. You can add conditions in the query by selecting **Custom log search**.

The following query is incorrect because it lists all new non-compliant resources:

```
AzureActivity | where Category == 'Policy' and Level != 'Informational' | extend
p=todynamic(Properties) | extend policies=todynamic(tostring(p.policies)) | mvexpand policy =
policies | where p.isComplianceCheck == 'False’
```

You should not use either of the following queries because they do not contain the `AzureActivity` keyword:

```
where Category == 'Policy' and Level != 'Informational' | extend p=todynamic(Properties) | extend
policies=todynamic(tostring(p.policies)) | mvexpand policy = policies | summarize
resource_count=count() by tostring(policy.policyDefinitionName)
```

```
where Category == 'Policy' and Level != 'Informational' | extend p=todynamic(Properties) | extend
policies=todynamic(tostring(p.policies)) | mvexpand policy = policies | where
```

```
p.isComplianceCheck == 'False
```

Objective:

Manage security operations

Sub-Objective:

Monitor security by using Azure Monitor

References:

Microsoft > How to Create Azure Monitor Alerts for Non-Compliant Azure Policies

Question #18 of 25

Question ID: 1380977

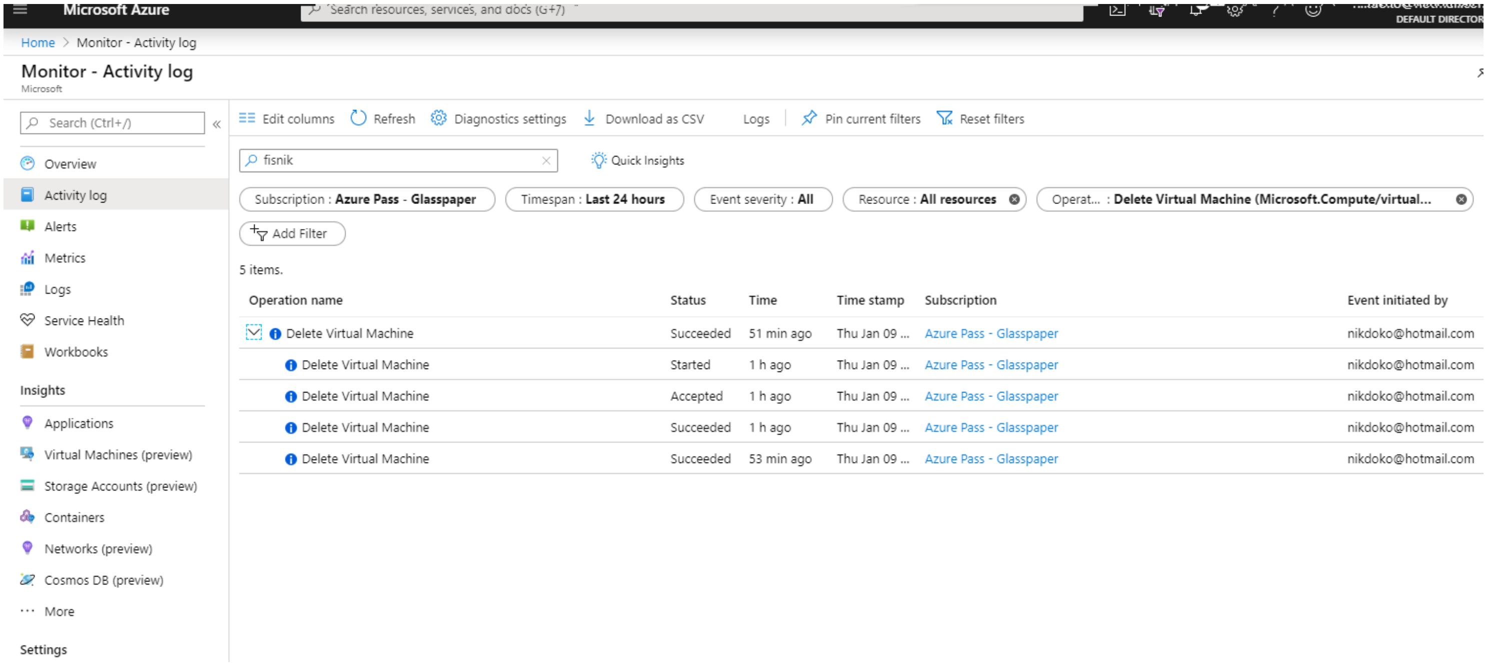
Nutex Corporation recently deployed several virtual machines (VMs) to the Azure platform. You have many users assigned to the Owner role. You have an urgent need to find which user deleted a virtual machine in the past 24 hours.

What should you recommend?

- ✗ **A)** Azure Advisor
- ✓ **B)** Activity log
- ✗ **C)** Azure Resource logs
- ✗ **D)** Azure Monitor metrics

Explanation

You would choose Activity log as it contains a record of all create, update, delete, and action operations performed through Resource Manager, as shown in the graphic. Additionally, it contains logs for Resource Health, Alert, Autoscale, Recommendation, Security, and Policy.



fisnik

Subscription : **Azure Pass - Glasspaper** | Timespan : **Last 24 hours** | Event severity : **All** | Resource : **All resources** | Operat... : **Delete Virtual Machine (Microsoft.Compute/virtual...**

5 items.

Operation name	Status	Time	Time stamp	Subscription	Event initiated by
Delete Virtual Machine	Succeeded	51 min ago	Thu Jan 09 ...	Azure Pass - Glasspaper	nikdoko@hotmail.com
Delete Virtual Machine	Started	1 h ago	Thu Jan 09 ...	Azure Pass - Glasspaper	nikdoko@hotmail.com
Delete Virtual Machine	Accepted	1 h ago	Thu Jan 09 ...	Azure Pass - Glasspaper	nikdoko@hotmail.com
Delete Virtual Machine	Succeeded	1 h ago	Thu Jan 09 ...	Azure Pass - Glasspaper	nikdoko@hotmail.com
Delete Virtual Machine	Succeeded	53 min ago	Thu Jan 09 ...	Azure Pass - Glasspaper	nikdoko@hotmail.com

You would not choose Azure Resource logs because they provide insight only into operations that were performed within an Azure resource.

You would not choose Azure Monitor metrics because that provides numerical values for resource performances and not information about deleting a resource.

You would not choose Azure Advisor because its purpose is to investigate your resources and recommend solutions that can help you improve the cost effectiveness, performance, high availability, and security of your Azure resources.

Objective:

Manage security operations

Sub-Objective:

Monitor security by using Azure Monitor

References:

Microsoft Azure > Azure Monitor > View and retrieve Azure Activity log events

Question #19 of 25

Question ID: 1380989

You are a cloud architect at Nutex Corporation which uses Azure for all of their resources. You need to implement restrictions to enforce their standards for allowed resource types.

What do you need to implement to make sure that your infrastructure stays compliant with the corporate standards?

- ✓ **A)** A new Azure Policy
- ✗ **B)** Azure AD Privileged Identity Management
- ✗ **C)** A Conditional Access policy
- ✗ **D)** Role-based access control (RBAC)

Explanation

You would choose to implement a new policy. Policies add protection and allow auditing, and ensure that only approved locations and SKUs are used. RBAC policies, along with Azure Policy, can provide governance around your environment, ensuring users have adequate rights but still adhere to the organization’s cloud policies.

You would not choose a Conditional Access policy. Conditional Access in Azure AD controls access to cloud apps based on specific conditions, such as sign-in risk, location, or device, and enforces requirements, such as multi-factor authentication.

You would not choose Azure AD Privileged Identity Management because it is a service that enables you to manage, control, and monitor access to important resources in your organization.

You would not choose role-based access control (RBAC) because it is an authorization system that provides access management of Azure resources.

Objective:
Manage security operations

Sub-Objective:
Configure security policies

References:

Microsoft Azure > Governance > Policy > Tutorial: Create and manage policies to enforce compliance > Implement a new custom policy

Question #20 of 25

Question ID: 1380979

You are part of the Azure Security team at the Nutex Corporation. Your team is tasked with configuring Just-in-Time (JIT) VM access to improve the security of management access to VMs. You must also allow any time access to VMs from remote management administrators.

Which of the following statements about configuring JIT VM access are TRUE? (Select all that apply.)

- ✓ **A)** JIT access to VMs can be audited from the Azure portal.
- ✗ **B)** The JIT access feature interrupts ongoing connections after the connections exceed the Max request time value of the JIT VM access rule.
- ✓ **C)** JIT access can be configured to allow or deny a specific list of IP addresses.
- ✓ **D)** Enabling JIT VM access requests adds appropriate JIT-specific security rules to the NSG configuration of the VM.

Explanation

The following statements are true:

- Enabling JIT VM access requests adds appropriate JIT-specific security rules to the NSG configuration of the VM.
- JIT access can be configured to allow or deny a specific list of IP addresses.
- JIT access to VMs can be audited from the Azure portal.

When you enable JIT VM access requests, this action adds appropriate JIT-specific security rules to the NSG configuration of the VM. When a JIT VM access request is enabled, Azure first checks whether the users trying to connect in the JIT time window have the necessary Azure RBAC permissions. Next, Azure automatically adds JIT-specific rules in the NSGs of the VM to allow access. When the allowed time limit (Max request time) is reached, NSGs will automatically revert to the original state (without the JIT-specific rules).

JIT access can allow or deny a specific list of IP addresses. With JIT access, ports on a VM can be locked down by any IP address users are trying to connect from (per request option), or for a specific IP address range or CIDR block.

You can use the Azure portal to audit JIT access to VMs. To view the JIT-specific activity on a VM, on the **Security Center – Just in time VM access** blade, open the "…" menu for a VM and select **Activity Log** from the shortcut menu. Activity logs contain the audit trail for all JIT-based accesses requested for the VM.

The JIT access feature doest not interrupt ongoing connections after the connections exceed the Max request time value of the JIT VM access rule. Ongoing connections are NOT interrupted. Azure does not allow new connections from the specified IP addresses after the Max request time value has been exceeded, from the time the access was requested.

Azure creates “deny all inbound traffic” rules with lower priority to deny all incoming connections. The “deny all inbound traffic” rules are added as low priority to ensure that no allow rules are overturned. These deny rules deny traffic to VMs after the Max request time has been exceeded.

Objective:

Manage security operations

Sub-Objective:

Monitor security by using Azure Security Center

References:

Microsoft Azure > Security Center > Manage virtual machine access using just-in-time > Configure JIT access from an Azure VM's page

RebelAdmin > Step-by-Step Guide to setup Just-in-Time VM Access in Azure

Microsoft Blogs > Harden Your Azure Infrastructure Using Azure Security Center Just-In-Time VM Acces

4sysops > Use Just-in-Time Access to protect your Azure VMs

Aidan Finn > Azure Bastion For Secure SSH/RDP in Preview

YouTube video > Azure Security Center – Just-in-Time Network Access

---

Question #21 of 25

Question ID: 1380987

The company that you are working for has Enterprise Agreement Azure Subscription with 240 subscriptions and has 200 Azure administrators in the US, Europe, Middle East, Africa, and Asia. You need to store Azure Activity Logs for 365 days. The solution must be easy to use for auditors to see detailed diagnostic and auditing information for Azure resources. You must have the possibility to create alerts based on log search and integrate with Azure Sentinel.

What solution do you suggest?

- ✗ **A)** Use Storage Account
- ✗ **B)** Use Azure Shared File System
- ✗ **C)** Use Event Hub
- ✓ **D)** Use Log Analytics Workspace

Explanation

You should choose the Log Analytics workspace. You can export the Activity Log to Log Analytics workspace, Event Hub, or a storage account. Log Analytics Workspace is the most powerful of those solutions. You can use it to collect resource logs and analyze the logs with other monitoring data collected by queries in Azure Monitor Logs. The Log Analytics platform allows you to search logs and integrate Log Analytics Workspace with Azure

Sentinel SIEM. You can create alerts based on searches. You can use the alerts to be notified of critical conditions or patterns identified in your resource logs. Results of log queries can be pin to an Azure dashboard, included in a workbook, or stored in an interactive report. These features would be helpful for auditors to see detailed diagnostic and auditing information from Azure resources.

Log Analytics workspaces in the Standalone or Per Node pricing tiers have user-configurable retention of up to 2 years so you can store an Activity Log for 365 days. However, the cost of storing data in a Log Analytics workspace is more expensive than storing that data in a storage account.

You can use a storage account to archive the Activity Log if you plan to retain your log data longer than 90 days (with full control over the retention policy) for audit, static analysis, or backup. Archiving the Activity Log is helpful, but you would need to use the Log Analytics workspace in Azure Monitor to provide detailed auditing and diagnostic information. You can use the Activity Log stored in the storage account in the Log Analytics workspace. Storing the Activity Log in a storage account does not allow an auditor to search the logs in an easy way.

You should not use Azure Event Hub in this scenario. If you need to store Activity Log events for 90 days or less, you could stream the Activity Log to Event Hub. Event Hub can receive and process millions of events per second. Event Hub is ideal for logging to a third party system or a telemetry system. In this scenario, you would need to use the Log Analytics workspace in Azure Monitor to provide detailed auditing and diagnostic information. Storing the Activity Log in the Event Hub does not allow an auditor to search the logs in an easy way.

You cannot export Activity Logs to Azure Shared File System.

Objective:
Manage security operations

Sub-Objective:
Monitor security by using Azure Sentinel

References:

Azure > Archive Azure resource logs to storage account

Azure > Collect Azure platform logs in Log Analytics workspace in Azure Monitor

Azure > Export Azure Activity log to storage or Azure Event Hubs

---

Question #22 of 25

Question ID: 1380992

You want to have the company’s Azure Architect sketch a project’s design parameters with a repeatable Azure resource that implements and adheres to the company’s standards and requirements.

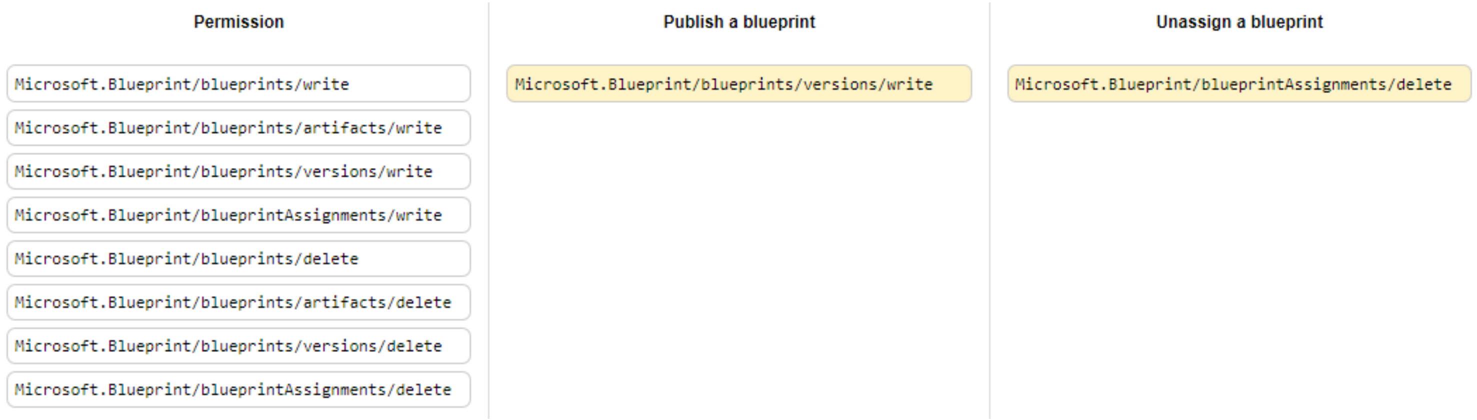
You need to assign the Architect and her subordinates permissions in Azure Blueprints.

Assign the appropriate permission to the appropriate task.

{UCMS id=5958920985116672 type=Activity}

Explanation

You should choose the following:



Permission	Publish a blueprint	Unassign a blueprint
Microsoft.Blueprint/blueprints/write	Microsoft.Blueprint/blueprints/versions/write	Microsoft.Blueprint/blueprintAssignments/delete
Microsoft.Blueprint/blueprints/artifacts/write		
Microsoft.Blueprint/blueprints/versions/write		
Microsoft.Blueprint/blueprintAssignments/write		
Microsoft.Blueprint/blueprints/delete		
Microsoft.Blueprint/blueprints/artifacts/delete		
Microsoft.Blueprint/blueprints/versions/delete		
Microsoft.Blueprint/blueprintAssignments/delete		

To create an Azure Blueprint, you will need to have the write permission. The following lists the tasks that require write permissions:

Task	Permissions
Create a blueprint definition	`Microsoft.Blueprint/blueprints/write`
Create artifacts on a blueprint definition	`Microsoft.Blueprint/blueprints/artifacts/write`
Publish a blueprint	`Microsoft.Blueprint/blueprints/versions/write`

When you save a blueprint definition on a management group or subscription scope, the blueprint definition permissions must be granted or inherited on that management group or subscription scope.

You will need the following permissions to delete blueprints:

`Microsoft.Blueprint/blueprints/delete`

`Microsoft.Blueprint/blueprints/artifacts/delete`

`Microsoft.Blueprint/blueprints/versions/delete`

To unassign a blueprint, you will need `Microsoft.Blueprint/blueprintAssignments/write` permissions.

To assign a blueprint, you will need `Microsoft.Blueprint/blueprintAssignments/delete` permissions.

Objective:
Manage security operations

Sub-Objective:

Configure security policies

References:

Azure > Governance > Blueprints > What is Azure Blueprints?

Question #23 of 25

Question ID: 1380976

You are working on your company's enterprise security team. The company that you are working for has Enterprise Agreement Azure Subscription with 240 subscriptions and has 200 Azure administrators in the US Region, in the US, Europe, the Middle East, Africa, and Asia. You need to store Azure Activity logs for 365 days.

The solution must be as inexpensive as possible. What do you suggest using?

- ✗ **A)** Use Azure Shared File System
- ✗ **B)** Use Log Analytics Workspace
- ✗ **C)** Use Event Hub
- ✓ **D)** Use Storage Account

Explanation

You should use a storage account. You can export Activity Log to Log Analytics workspace, Event Hub, and a storage account. Using a storage account to archiving the Activity Log would be the least expensive if you plan to retain your log data longer than 90 days (with full control over the retention policy) for audit, static analysis, or backup. If you need to store Activity Log events for 90 days or less, you could stream the Activity Log to Event Hub. You could also copy Activity Log events to a Log Analytics workspace where it can be analyzed by Azure Monitor.

Log Analytics workspaces in the Standalone or Per Node pricing tiers have user-configurable retention of up to 2 years so you can store an Activity Log for 365 days. However, the cost of storing data in a Log Analytics workspace is more expensive than storing that data in a storage account.

You cannot export Activity Logs to Azure Shared File System.

Objective:

Manage security operations

Sub-Objective:

Monitor security by using Azure Monitor

References:

Azure > Archive Azure resource logs to storage account

Azure > Collect Azure platform logs in Log Analytics workspace in Azure Monitor

Azure > Export Azure Activity log to storage or Azure Event Hubs

Azure > Manage usage and costs with Azure Monitor Logs

Question #24 of 25

Question ID: 1380991

You want to have the company's Azure Architect sketch a project's design parameters with a repeatable Azure resource that implements and adheres to the company's standards and requirements.

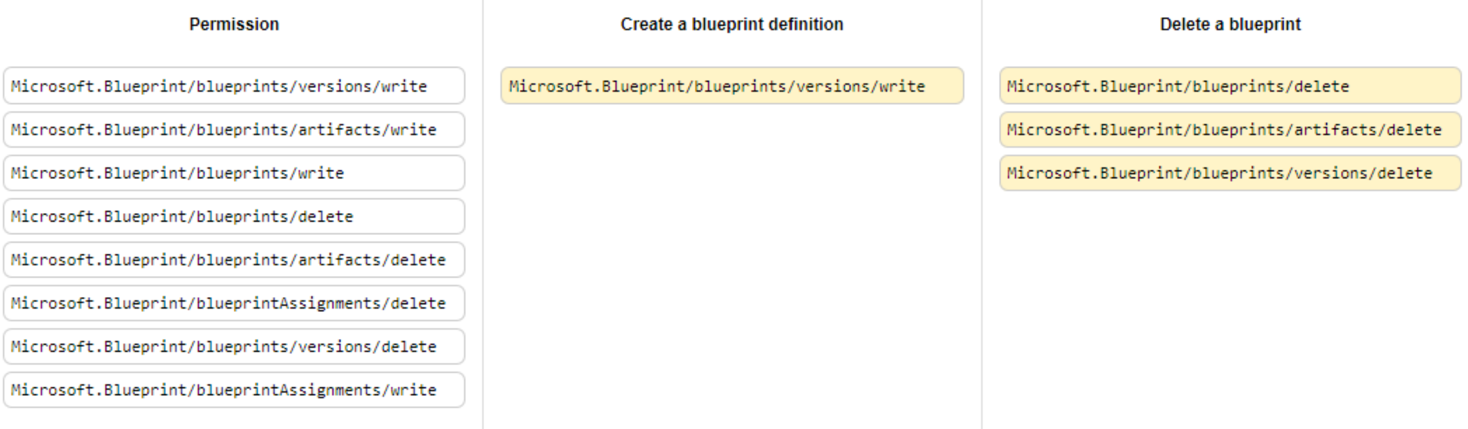
You need to assign the Architect and her subordinates permissions in Azure Blueprints.

Assign the appropriate permission to the appropriate task.

{UCMS id=4857734655639552 type=Activity}

Explanation

You should choose the following:



Permission	Create a blueprint definition	Delete a blueprint
Microsoft.Blueprint/blueprints/versions/write	Microsoft.Blueprint/blueprints/versions/write	Microsoft.Blueprint/blueprints/delete
Microsoft.Blueprint/blueprints/artifacts/write		Microsoft.Blueprint/blueprints/artifacts/delete
Microsoft.Blueprint/blueprints/write		Microsoft.Blueprint/blueprints/versions/delete
Microsoft.Blueprint/blueprints/delete		
Microsoft.Blueprint/blueprints/artifacts/delete		
Microsoft.Blueprint/blueprintAssignments/delete		
Microsoft.Blueprint/blueprints/versions/delete		
Microsoft.Blueprint/blueprintAssignments/write		

To create an Azure Blueprint, you will need to have the write permission. The following lists the tasks that require write permissions:

Task	Permissions
Create a blueprint definition	`Microsoft.Blueprint/blueprints/write`
Create artifacts on a blueprint definition	`Microsoft.Blueprint/blueprints/artifacts/write`
Publish a blueprint	`Microsoft.Blueprint/blueprints/versions/write`

When you save a blueprint definition on a management group or subscription scope, the blueprint definition permissions must be granted or inherited on that management group or subscription scope.

You will need the following permissions to delete blueprints:

`Microsoft.Blueprint/blueprints/delete`

`Microsoft.Blueprint/blueprints/artifacts/delete`

`Microsoft.Blueprint/blueprints/versions/delete`

To unassign a blueprint, you will need `Microsoft.Blueprint/blueprintAssignments/write` permissions.

To assign a blueprint, you will need `Microsoft.Blueprint/blueprintAssignments/delete` permissions.

Objective:
Manage security operations

Sub-Objective:
Configure security policies

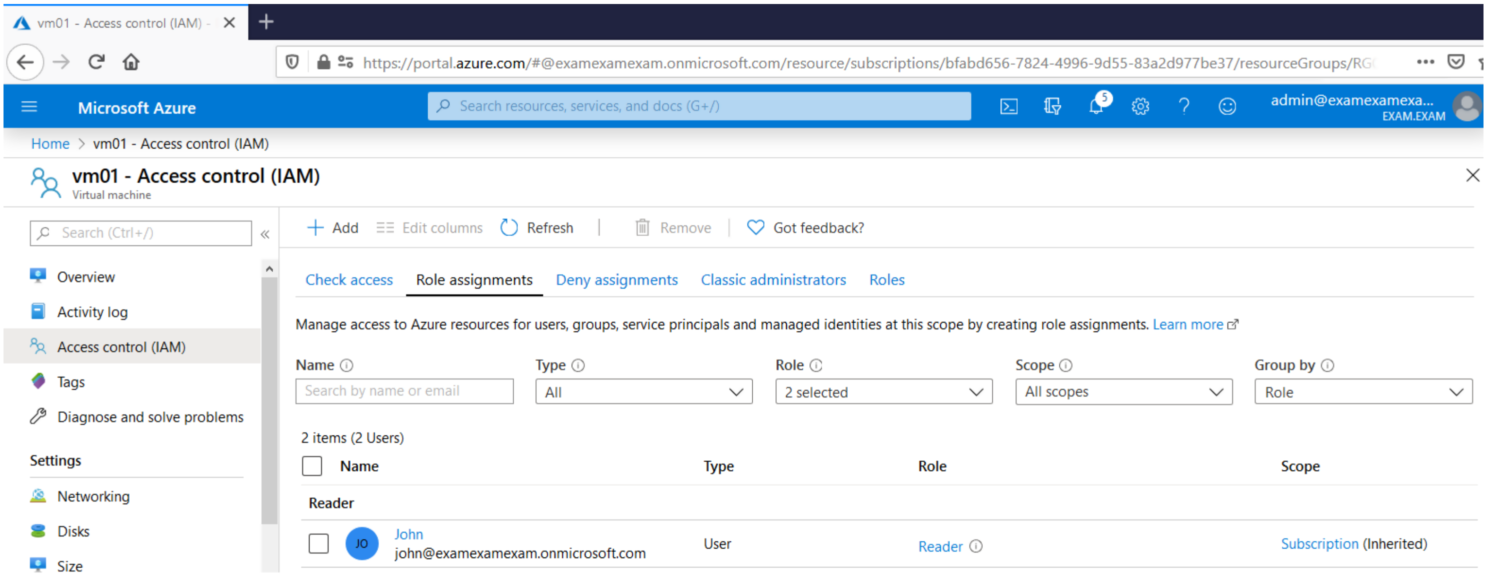
References:

Azure > Governance > Blueprints > What is Azure Blueprints?

Question #25 of 25

Question ID: 1380981

You are working as an Enterprise Azure administrator. The assistant administrator, John, reports that he cannot access the virtual machine named VM01 via just-in-time (JIT). JIT was enabled via Security Center. You checked IAM roles for VM01. The following graphic displays the IAM roles for VM01.


vm01 - Access control (IAM)
https://portal.azure.com/#@examexamexam.onmicrosoft.com/resource/subscriptions/bfabd656-7824-4996-9d55-83a2d977be37/resourceGroups/RG
Microsoft Azure
Search resources, services, and docs (G+/)
admin@examexamexa...
EXAM.EXAM
Home > vm01 - Access control (IAM)
Virtual machine
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Networking
Disks
Size
+ Add
Edit columns
Refresh
Remove
Got feedback?
Check access
Role assignments
Deny assignments
Classic administrators
Roles

vm01 - Access control (IAM)

Manage access to Azure resources for users, groups, service principals and managed identities at this scope by creating role assignments. Learn more

Name	Type	Role	Scope	Group by
Search by name or email	All	2 selected	All scopes	Role

2 items (2 Users)

□	Name	Type	Role	Scope
	Reader			
□	JO John john@examexamexam.onmicrosoft.com	User	Reader	Subscription (Inherited)

What do you need to make sure that John can manage virtual machine access using JIT?

- ✗ **A)** Set managed identity on VM01 for John.
- ✓ **B)** Add `jitNetworkAccessPolicies` in the scope of VM01 for John.
- ✗ **C)** Add the Avere Operator role in the scope of VM01 for John.
- ✗ **D)** Add the User Access Administrator role in the scope of VM01 for John.

Explanation

You should add `jitNetworkAccessPolicies` in the scope of VM01 for John.Permissions needed to use JIT are `Microsoft.Compute/virtualMachines/read` and `Microsoft.Security/locations/jitNetworkAccessPolicies/initiate/action`.

You should not set managed identity to on VM01 for John. Managed identity can be assigned to the resources. They are not set for users This action will not work.

You should not add the Avere Operator role in the scope of VM01 for John. This role is used by the Avere vFXT cluster to manage the cluster. This action will not work.

You should not add the User Access Administrator role in the scope of VM01 for John. It will allow John to Administration other users, but not resolve the issue.

Objective:

Manage security operations

Sub-Objective:

Monitor security by using Azure Security Center

References:

Azure > Security Center > Manage virtual machine access using just-in-time