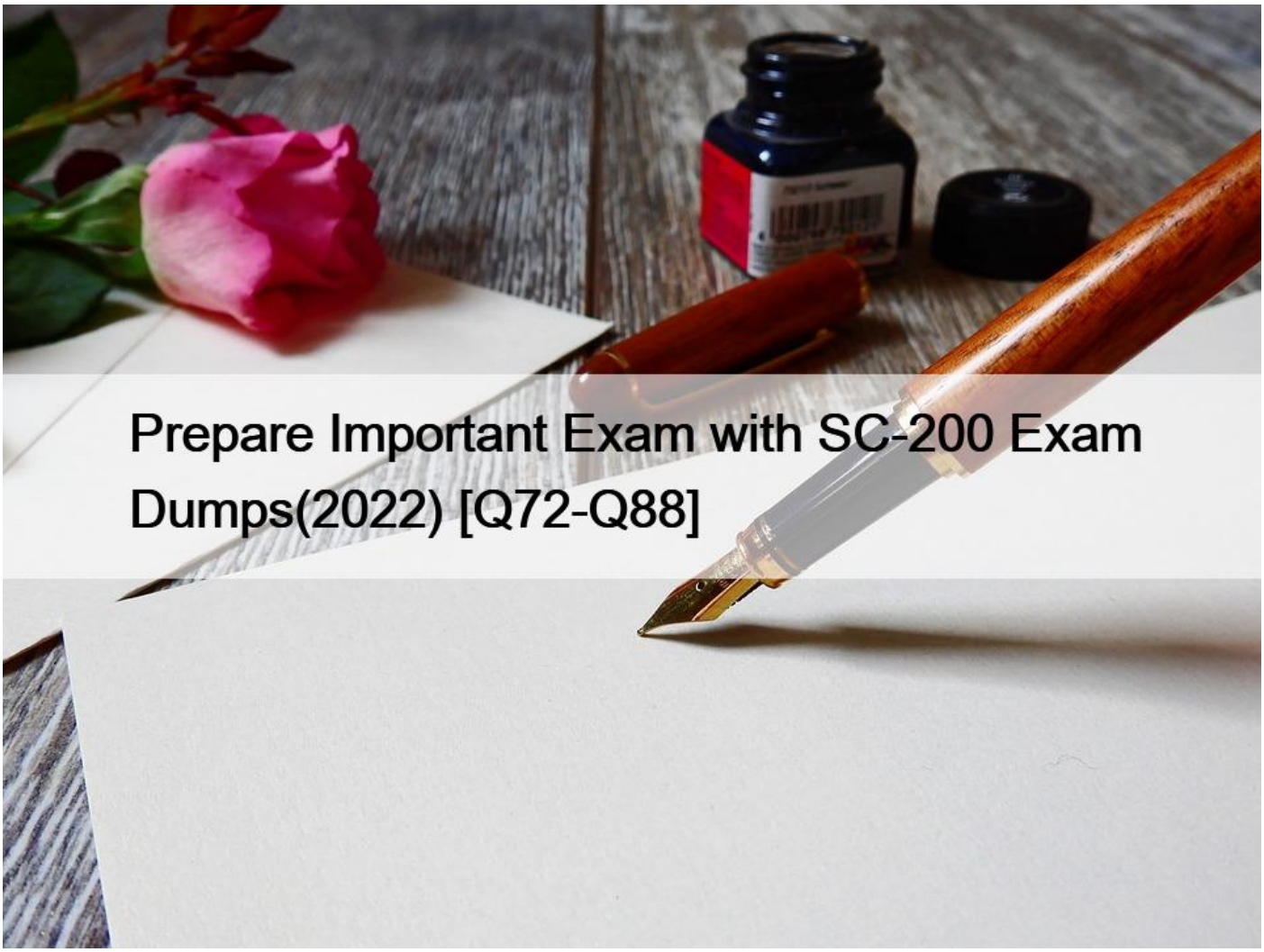
Prepare Important Exam with SC-200 Exam Dumps(2022) [Q72-Q88



Prepare Important Exam with SC-200 Exam Dumps(2022)
Pass Exam Questions Efficiently With SC-200 Questions

Microsoft SC-200 Exam Syllabus Topics:

TopicDetailsTopic 1- Identify the prerequisites for a data connector- Configure detection alerts in Azure AD Identity Protection
Topic 2- Mitigate threats using Azure Defender- Identify and remediate security risks using Secure ScoreTopic 3- Identify and remediate security risks related to Azure Active Directory- Remediate incidents by using Azure Defender recommendations
Topic 4- Identify and remediate security risks related to Conditional Access events- manage data retention, alert notification, and advanced featuresTopic 5- Identify and remediate security risks related to sign-in risk policies- Identify data sources to be ingested for Azure Sentinel

NEW QUESTION 72

You have an Azure subscription that has Microsoft Defender for Cloud enabled.

You have a virtual machine that runs Windows 10 and has the Log Analytics agent installed.

You need to simulate an attack on the virtual machine that will generate an alert.

What should you do first?
* Run the Log Analytics Troubleshooting Tool.
* Copy a executable and rename the file as ASC_AlerTest_662jf10N,exe
* Modify the settings of the Microsoft Monitoring Agent.
* Run the MMASetup executable and specify the -foo argument

NEW QUESTION 73

You need to use an Azure Resource Manager template to create a workflow automation that will trigger an automatic remediation when specific security alerts are received by Azure Security Center.

How should you complete the portion of the template that will provision the required Azure resources? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

```
"resources": [
  {
    "type": "                                    /automations",
                Microsoft.Automation
                Microsoft.Logic
                Microsoft.Security
    "apiVersion": "2019-01-01-preview",
    "name": "[parameters('name')]",
    "location": "[parameter                    ]",
    "properties": {
      "descri      on": "[format(variables('description'), '{0}', parameters
('subscriptionId'))]",
      "isEnabled": true,
      "actions": [
        {
          "actionType": "LogicApp",
          "logicAppResourceId": "[resourceId('ITEM2/workflows', parameters
('appName'))]",
          "uri": "[listCallbackURL(resourceId(parameters('subscriptionId'),
parameters('resourceGroupName'), '                    /workflows/triggers',
                Microsoft.Automation
                Microsoft.Logic
                Microsoft.Security
parameters('appName'), 'manual'), '2019-05-01').value]"
        }
      ],
```

Reference:

https://docs.microsoft.com/en-us/azure/security-center/quickstart-automation-alert

NEW QUESTION 74

You have an Azure subscription that has Azure Defender enabled for all supported resource types.

You create an Azure logic app named LA1.

You plan to use LA1 to automatically remediate security risks detected in Azure Security Center.

You need to test LA1 in Security Center.

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

NOTE: Each correct selection is worth one point.

Answer Area

Set the LA1 trigger to:

- When an Azure Security Center Recommendation is created or triggered
- When an Azure Security Center Alert is created or triggered
- When a response to an Azure Security Center alert is triggered

Trigger the execution of LA1 from:

- Recommendations
- Workflow automation

Reference:

https://docs.microsoft.com/en-us/azure/security-center/workflow-automation#create-a-logic-app-and-define-when-it-should-automatically-run

NEW QUESTION 75

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 are configuring Microsoft Defender for Identity integration with Active Directory.

From the Microsoft Defender for identity portal, you need to configure several accounts for attackers to exploit.

Solution: From Azure Identity Protection, you configure the sign-in risk policy.

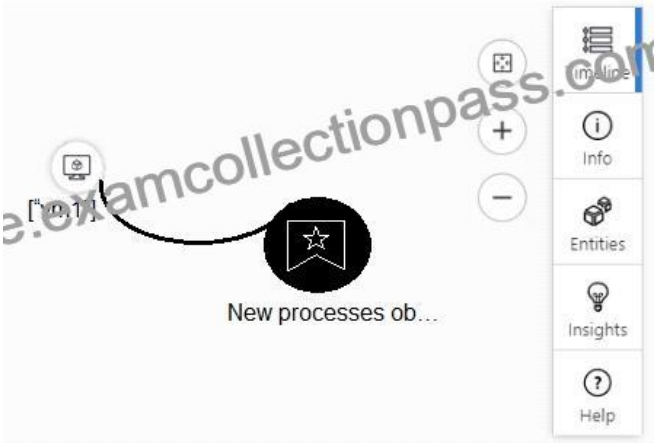
Does this meet the goal?
* Yes
* No
Section: [none]

Explanation/Reference:

https://docs.microsoft.com/en-us/defender-for-identity/manage-sensitive-honeytoken-accounts

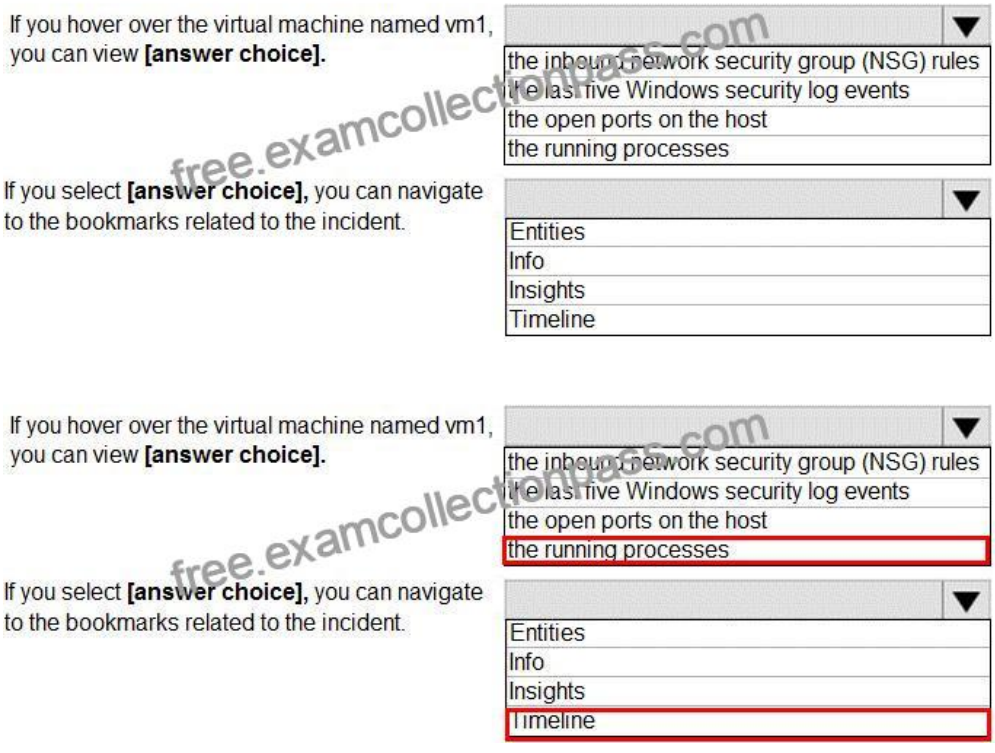
NEW QUESTION 76

From Azure Sentinel, you open the Investigation pane for a high-severity incident as shown in the following exhibit.



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.



Reference:

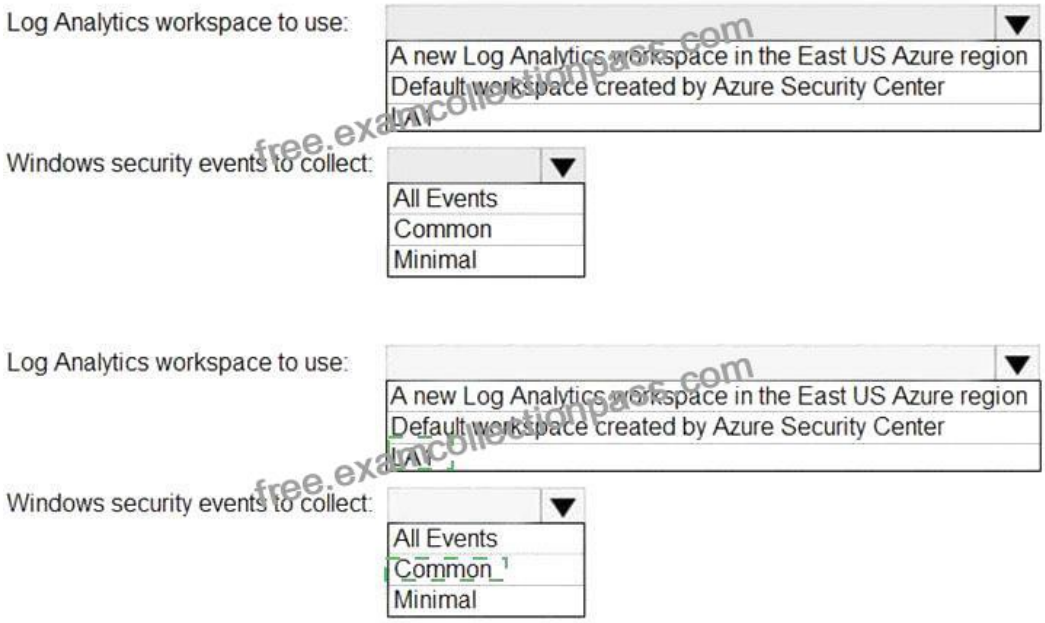
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-investigate-cases#use-the-investigation-graph-to-deep-dive

NEW QUESTION 77

You need to implement Azure Defender to meet the Azure Defender requirements and the business requirements.

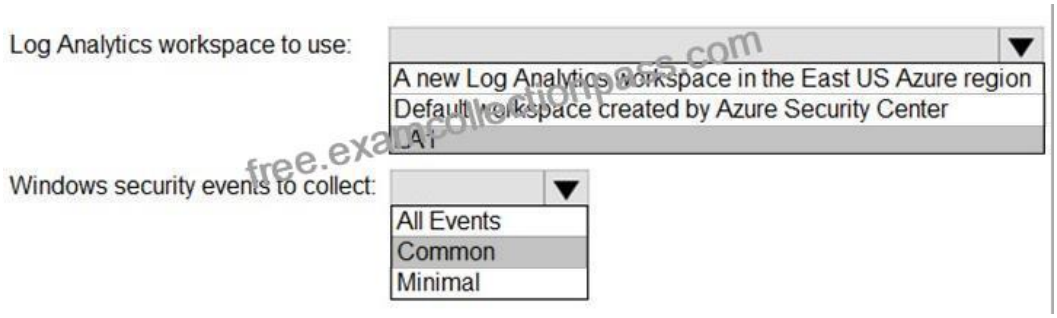
What should you include in the solution? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Explanation

Graphical user interface, application Description automatically generated



NEW QUESTION 78

You have an existing Azure logic app that is used to block Azure Active Directory (Azure AD) users. The logic app is triggered manually.

You deploy Azure Sentinel.

You need to use the existing logic app as a playbook in Azure Sentinel.

What should you do first?
* And a new scheduled query rule.
* Add a data connector to Azure Sentinel.
* Configure a custom Threat Intelligence connector in Azure Sentinel.
* Modify the trigger in the logic app.

Section: [none]

NEW QUESTION 79

Your company uses Azure Sentinel.

A new security analyst reports that she cannot assign and dismiss incidents in Azure Sentinel. You need to resolve the issue for the analyst. The solution must use the principle of least privilege. Which role should you assign to the analyst?
* Logic App Contributor
* Azure Sentinel Contributor
* Azure Sentinel Reader
* Azure Sentinel Responder

NEW QUESTION 80

You implement Safe Attachments policies in Microsoft Defender for Office 365.

Users report that email messages containing attachments take longer than expected to be received.

You need to reduce the amount of time it takes to deliver messages that contain attachments without compromising security. The attachments must be scanned for malware, and any messages that contain malware must be blocked.

What should you configure in the Safe Attachments policies?
* Dynamic Delivery
* Replace
* Block and Enable redirect
* Monitor and Enable redirect

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments?view=o365-worldwide

NEW QUESTION 81

You receive an alert from Azure Defender for Key Vault.

You discover that the alert is generated from multiple suspicious IP addresses.

You need to reduce the potential of Key Vault secrets being leaked while you investigate the issue. The solution must be implemented as soon as possible and must minimize the impact on legitimate users.

What should you do first?
* Modify the access control settings for the key vault.
* Enable the Key Vault firewall.
* Create an application security group.

* Modify the access policy for the key vault.

Explanation/Reference:

Reference:

https://docs.microsoft.com/en-us/azure/security-center/defender-for-key-vault-usage

NEW QUESTION 82

You receive a security bulletin about a potential attack that uses an image file.

You need to create an indicator of compromise (IoC) in Microsoft Defender for Endpoint to prevent the attack.

Which indicator type should you use?

* a URL/domain indicator that has Action set to Alert only
* a URL/domain indicator that has Action set to Alert and block
* a file hash indicator that has Action set to Alert and block
* a certificate indicator that has Action set to Alert and block

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/indicator-file?view=o365-worldwide

NEW QUESTION 83

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?

* Playbooks
* Analytics
* Threat intelligence
* Incidents

Section: [none]

Explanation/Reference:

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

NEW QUESTION 84

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 are configuring Azure Sentinel.

You need to create an incident in Azure Sentinel when a sign-in to an Azure virtual machine from a malicious IP address is detected.

Solution: You create a Microsoft incident creation rule for a data connector.

Does this meet the goal?
* Yes
* No
Section: [none]

Explanation/Reference:

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

NEW QUESTION 85

You need to remediate active attacks to meet the technical requirements.

What should you include in the solution?
* Azure Automation runbooks
* Azure Logic Apps
* Azure Functions
* Azure Sentinel livestreams
Section: [none]

Explanation/Reference:

https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks

NEW QUESTION 86

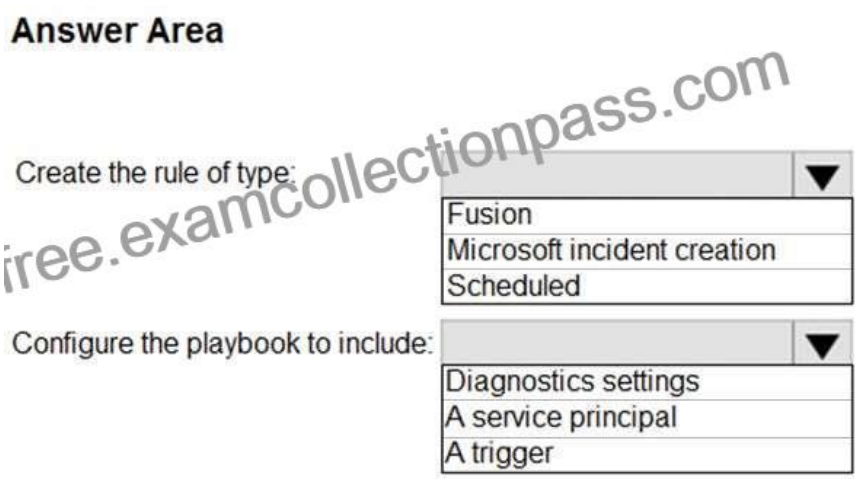
HOTSPOT

You need to create the analytics rule to meet the Azure Sentinel requirements.

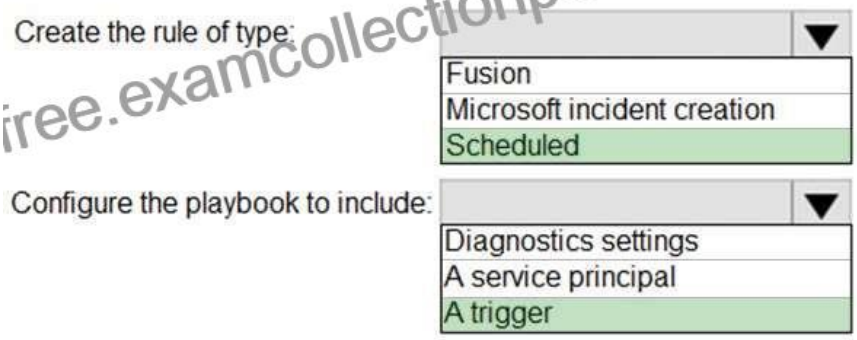
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area



Section: [none]

Explanation/Reference:

https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom#set-automated-responses-and- create-the-rule

https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook Question Set 3

NEW QUESTION 87

You are configuring Microsoft Cloud App Security.

You have a custom threat detection policy based on the IP address ranges of your company’s United States-based offices.

You receive many alerts related to impossible travel and sign-ins from risky IP addresses.

You determine that 99% of the alerts are legitimate sign-ins from your corporate offices.

You need to prevent alerts for legitimate sign-ins from known locations.

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

NOTE: Each correct selection is worth one point.
* Override automatic data enrichment.
* Add the IP addresses to the corporate address range category.
* Increase the sensitivity level of the impossible travel anomaly detection policy.
* Add the IP addresses to the other address range category and add a tag.
* Create an activity policy that has an exclusion for the IP addresses.

NEW QUESTION 88

You are configuring Azure Sentinel.

You need to send a Microsoft Teams message to a channel whenever a sign-in from a suspicious IP address is detected.

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

NOTE: Each correct selection is worth one point.
* Add a playbook.
* Associate a playbook to an incident.
* Enable Entity behavior analytics.
* Create a workbook.
* Enable the Fusion rule.

Explanation/Reference:

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

Exam SC-200: Microsoft Security Operations Analyst **The content of this exam was updated on July 23, 2021.**

The Microsoft Security Operations Analyst collaborates with organizational stakeholders to secure information technology systems for the organization. Their goal is to reduce organizational risk by rapidly remediating active attacks in the environment, advising on improvements to threat protection practices, and referring violations of organizational policies to appropriate stakeholders. Responsibilities include threat management, monitoring, and response by using a variety of security solutions across their environment. The role primarily investigates, responds to, and hunts for threats using Microsoft Azure Sentinel, Azure Defender, Microsoft 365 Defender, and third-party security products. Since the Security Operations Analyst consumes the operational output of these tools, they are also a critical stakeholder in the configuration and deployment of these technologies.

Part of the requirements for: Microsoft Certified: Security Operations Analyst Associate

Download exam skills outline

SC-200 Questions - Truly Beneficial For Your Microsoft Exam:
https://www.examcollectionpass.com/Microsoft/SC-200-practice-exam-dumps.html]