SC-100 Q&As

Microsoft Cybersecurity Architect

Pass Microsoft SC-100 Exam with 100% Guarantee

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

https://www.pass4itsure.com/sc-100.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

Your company has a third-party security information and event management (SIEM) solution that uses Splunk and Microsoft Sentinel.

You plan to integrate Microsoft Sentinel with Splunk.

You need to recommend a solution to send security events from Microsoft Sentinel to Splunk.

What should you include in the recommendation?

A. a Microsoft Sentinel data connector

B. Azure Event Hubs

C. a Microsoft Sentinel workbook

D. Azure Data Factory

Correct Answer: A

Microsoft Sentinel Add-On for Splunk allows Azure Log Analytics and Microsoft Sentinel users to ingest security logs from Splunk platform using the Azure HTTP Data Collector API. Reference: https://splunkbase.splunk.com/app/5312/

QUESTION 2

HOTSPOT

Your company wants to optimize using Azure to protect its resources from ransomware.

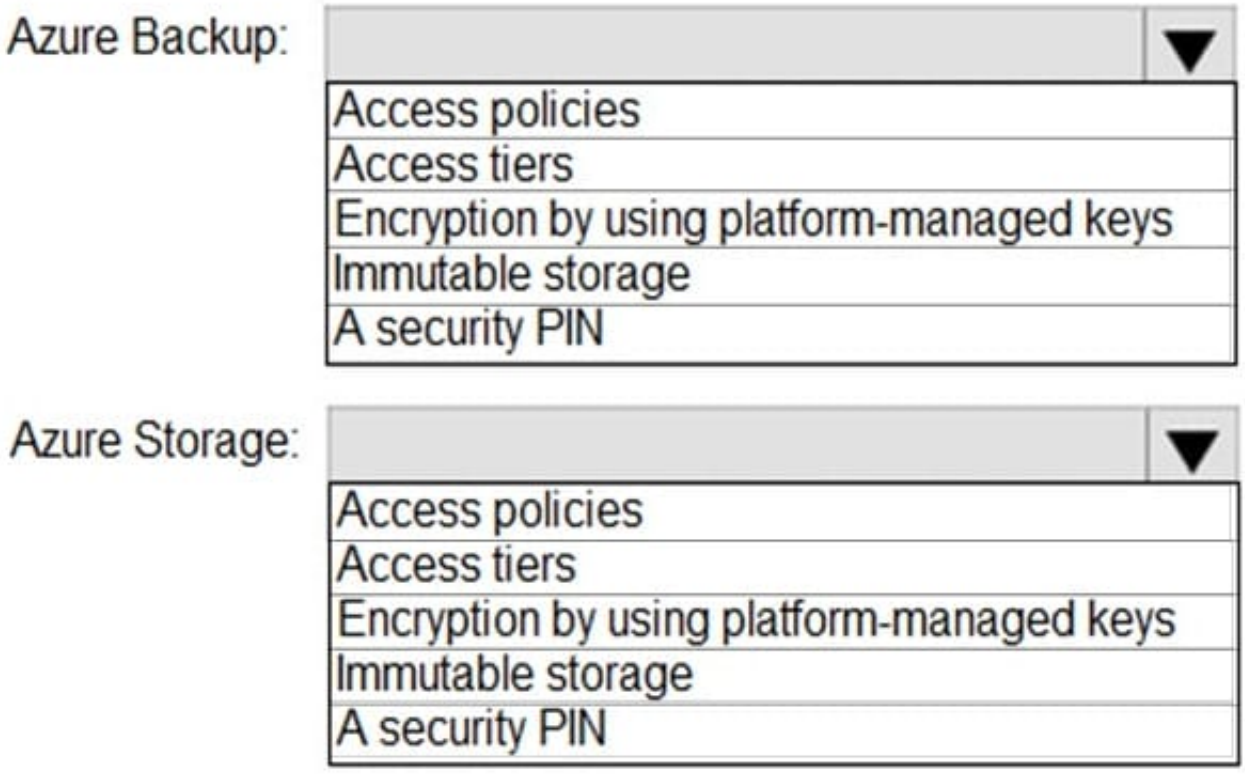
You need to recommend which capabilities of Azure Backup and Azure Storage provide the strongest protection against ransomware attacks. The solution must follow Microsoft Security Best Practices.

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

NOTE: Each correct selection is worth one point.

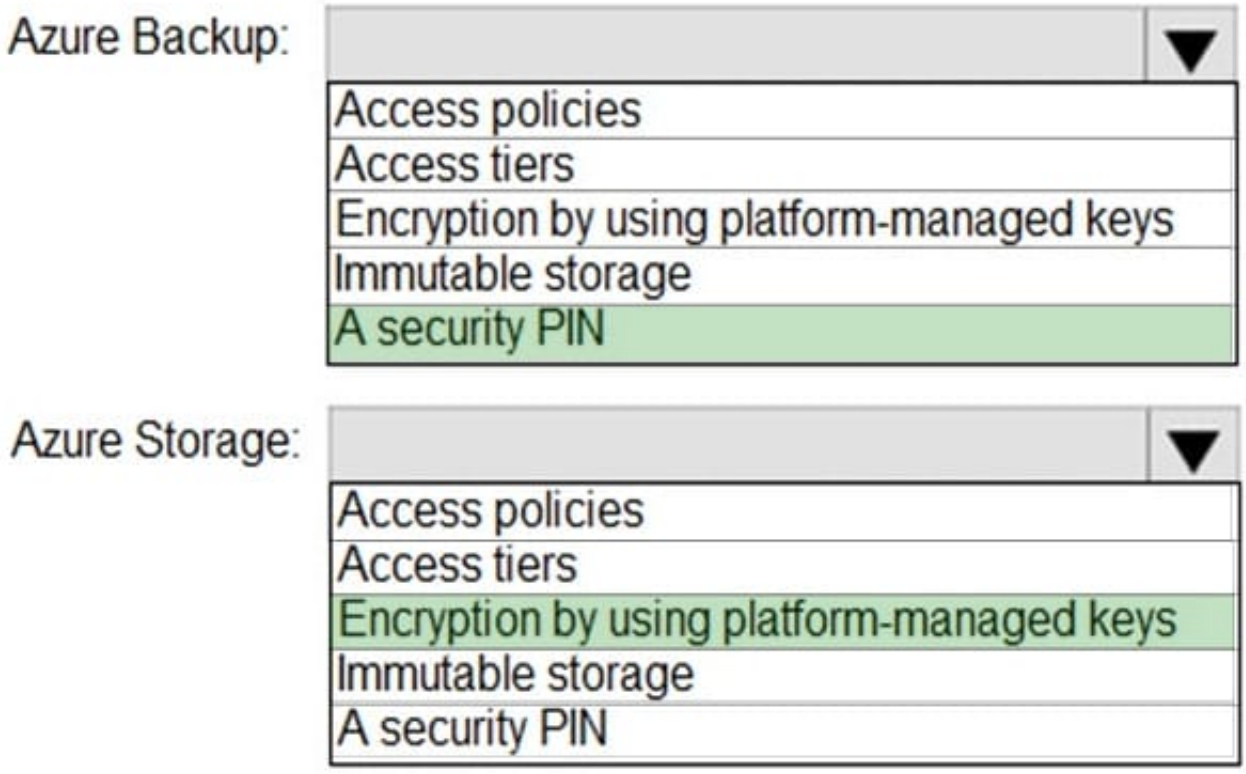
Hot Area:

Answer Area



Correct Answer:

Answer Area



Box 1: A security PIN

Azure Backup

The best way to prevent falling victim to ransomware is to implement preventive measures and have tools that protect your organization from every step that attackers take to infiltrate your systems.

You can reduce your on-premises exposure by moving your organization to a cloud service.

Checks have been added to make sure only valid users can perform various operations. These include adding an extra layer of authentication. As part of adding an extra layer of authentication for critical operations, you\\'re prompted to enter a

security PIN before modifying online backups.

Box 2: Encryption by using platform-managed keys

Ensure backup data is encrypted.

By default, backup data at rest is encrypted using platform-managed keys (PMK). For vaulted backups, you can choose to use customer-managed keys (CMK) to own and manage the encryption keys yourself. Additionally, you can configure

encryption on the storage infrastructure using infrastructure-level encryption, which along with CMK encryption provides double encryption of data at rest.

Reference:

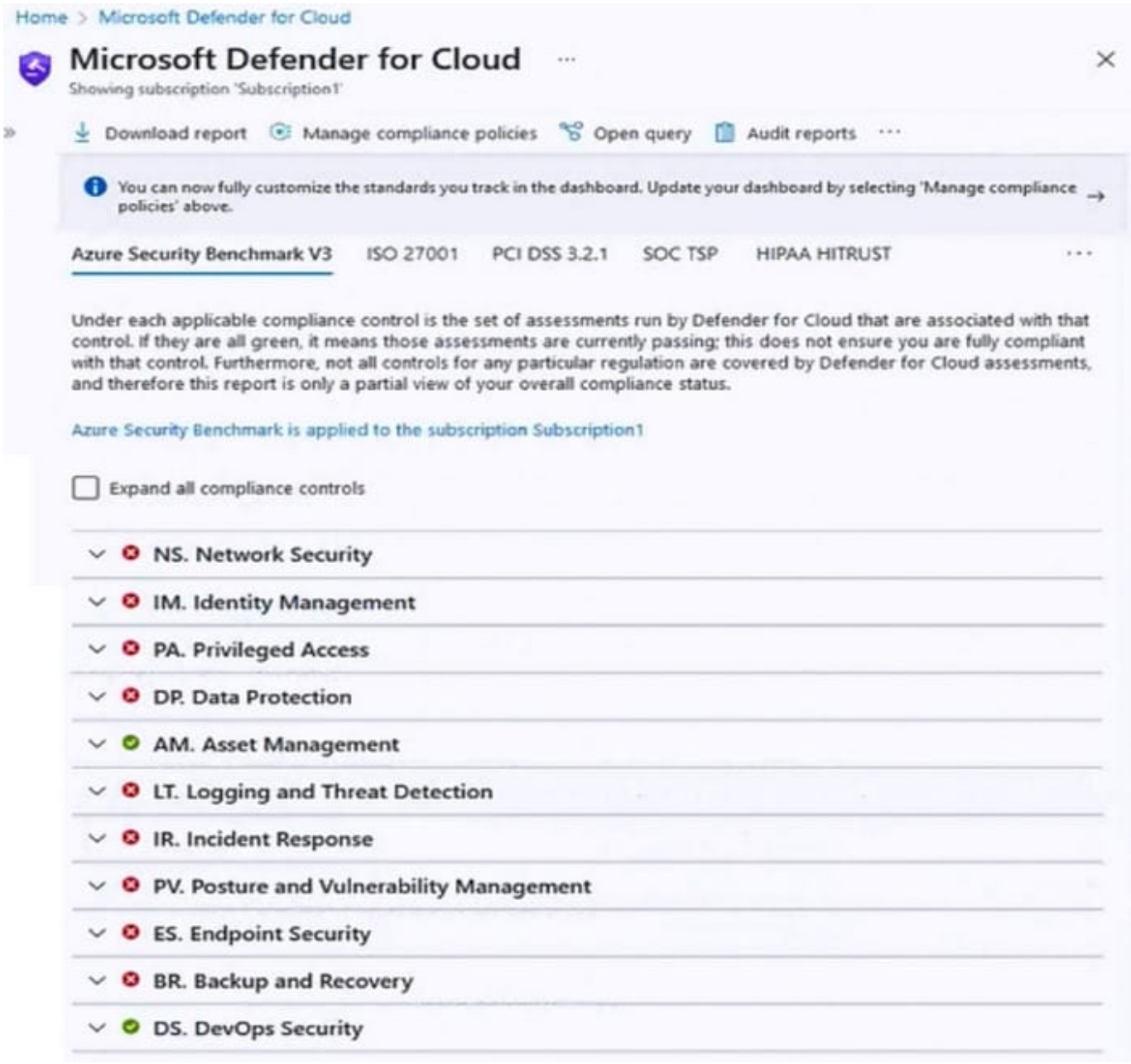
https://learn.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware

https://learn.microsoft.com/en-us/azure/backup/protect-backups-from-ransomware-faq

QUESTION 3

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

You are evaluating the Azure Security Benchmark V3 report as shown in the following exhibit.



You need to verify whether Microsoft Defender for servers is installed on all the virtual machines that run Windows.
Which compliance control should you evaluate?

A. Asset Management

B. Posture and Vulnerability Management

C. Data Protection

D. Endpoint Security

E. Incident Response

Correct Answer: D

Microsoft Defender for servers compliance control installed on Windows

Defender for clout "Endpoint Security" azure security benchmark v3

Endpoint Security covers controls in endpoint detection and response, including use of endpoint detection and response (EDR) and anti-malware service for endpoints in Azure environments.

Security Principle: Enable Endpoint Detection and Response (EDR) capabilities for VMs and integrate with SIEM and security operations processes.

Azure Guidance: Azure Defender for servers (with Microsoft Defender for Endpoint integrated) provides EDR capability to prevent, detect, investigate, and respond to advanced threats.

Use Microsoft Defender for Cloud to deploy Azure Defender for servers for your endpoint and integrate the alerts to your SIEM solution such as Azure Sentinel.

Incorrect:

Not A: Asset Management covers controls to ensure security visibility and governance over Azure resources, including recommendations on permissions for security personnel, security access to asset inventory, and managing approvals for

services and resources (inventory, track, and correct).

Not B: Posture and Vulnerability Management focuses on controls for assessing and improving Azure security posture, including vulnerability scanning, penetration testing and remediation, as well as security configuration tracking, reporting,

and correction in Azure resources.

Not C: Data Protection covers control of data protection at rest, in transit, and via authorized access mechanisms, including discover, classify, protect, and monitor sensitive data assets using access control, encryption, key and certificate

management in Azure.

Not E: Incident Response covers controls in incident response life cycle - preparation, detection and analysis, containment, and post-incident activities, including using Azure services such as Microsoft Defender for Cloud and Sentinel to

automate the incident response process.

Reference: https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-endpoint-security

QUESTION 4

Your company has on-premises Microsoft SQL Server databases.

The company plans to move the databases to Azure.

You need to recommend a secure architecture for the databases that will minimize operational requirements for patching and protect sensitive data by using dynamic data masking. The solution must minimize costs.

What should you include in the recommendation?

A. SQL Server on Azure Virtual Machines

B. Azure Synapse Analytics dedicated SQL pools

C. Azure SQL Database

Correct Answer: C

Explanation:

Azure SQL Database, Azure SQL Managed Instance, and Azure Synapse Analytics support dynamic data masking. Dynamic data masking limits sensitive data exposure by masking it to non-privileged users.

Azure SQL Database is cheaper as its offer DTU\\'s based tier and also vCore based for more intensive workflow.

Hovewer, Managed Instance offers almost ~100% compatibility with on-prem Microsoft SQL Server.

Incorrect:

Not A: SQL Server does not support dynamic data masking.

Not B: Synapse Analytics is more expensive compared to Azure SQL Database.

Reference:

https://docs.microsoft.com/en-us/azure/azure-sql/database/dynamic-data-masking-overview?view=azuresql

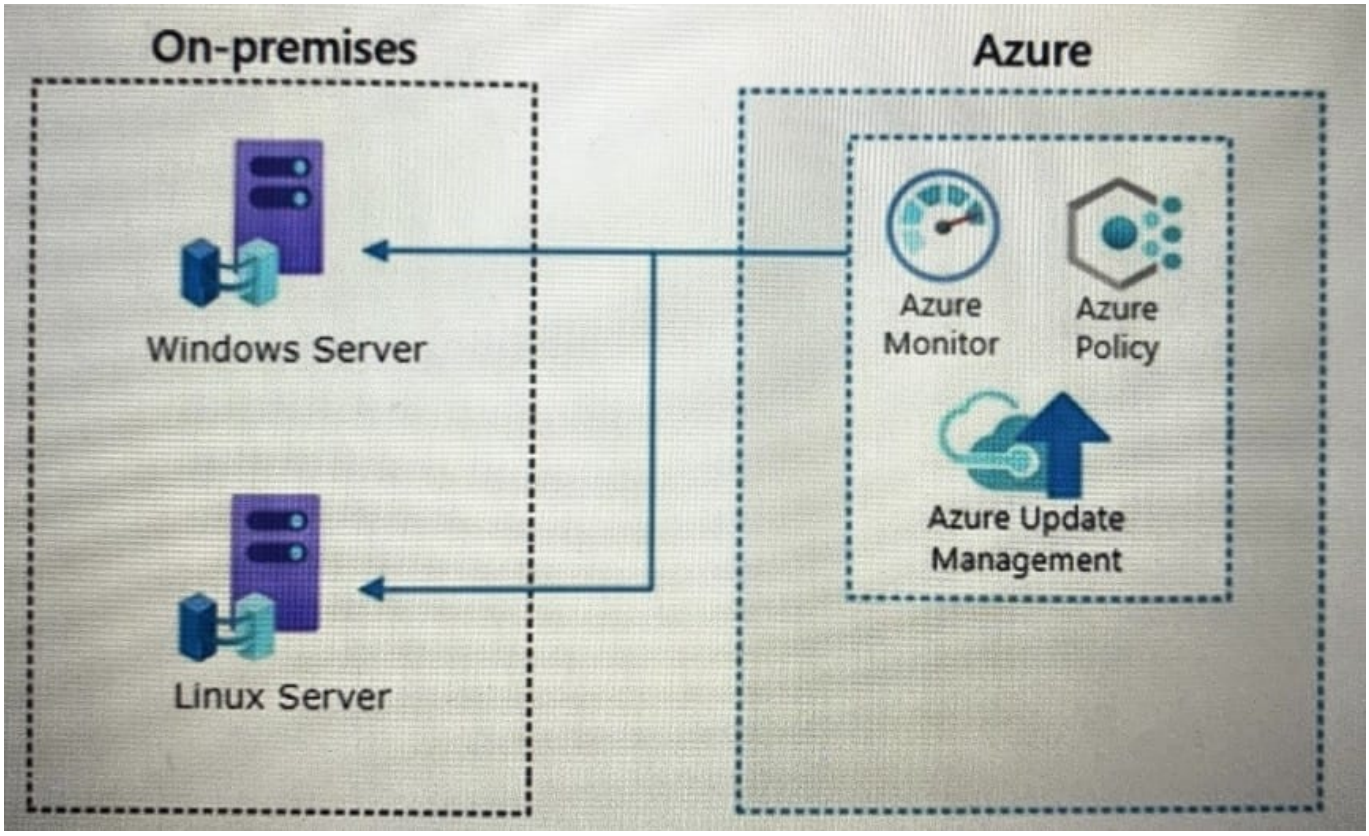
https://learn.microsoft.com/en-us/answers/questions/1057631/azure-sql-db-vs-azure-sql-managed-instance-cost

QUESTION 5

Your company has a hybrid cloud infrastructure.

Data and applications are moved regularly between cloud environments.

The company\\'s on-premises network is managed as shown in the following exhibit.



You are designing security operations to support the hybrid cloud infrastructure. The solution must meet the following requirements:

1.

Govern virtual machines and servers across multiple environments.

2.

Enforce standards for all the resources across all the environments by using Azure Policy.

Which two components should you recommend for the on-premises network? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. on-premises data gateway

B. Azure VPN Gateway

C. guest configuration in Azure Policy

D. Azure Arc

E. Azure Bastion

Correct Answer: CD

C: Azure Policy\\'s guest configuration feature provides native capability to audit or configure operating system settings as code, both for machines running in Azure and hybrid Arc-enabled machines. The feature can be used directly per-

machine, or at-scale orchestrated by Azure Policy.

Configuration resources in Azure are designed as an extension resource. You can imagine each configuration as an additional set of properties for the machine. Configurations can include settings such as:

Operating system settings Application configuration or presence Environment settings Configurations are distinct from policy definitions. Guest configuration utilizes Azure Policy to dynamically assign configurations to machines.

D: Azure Arc is a bridge that extends the Azure platform to help you build applications and services with the flexibility to run across datacenters, at the edge, and in multicloud environments.

Microsoft recently [2019/2020] released Azure Arc, which unlocks new hybrid scenarios for organizations by bringing new Azure services and management features to any infrastructure.

By the time of writing this post, the public preview supports the following operating systems:

Windows Server 2012 R2 and newer

Ubuntu 16.04 and 18.04

Register the required Resource Providers in Azure

First, we need to register the required resource providers in Azure. Therefore, take the following steps:

Open a browser and navigate to the Azure portal at: https://portal.azure.com/

Login with your administrator credentials.

Open Cloud Shell in the top right menu, and add the following lines of code to register the Microsoft.HybridCompute and the Microsoft.GuestConfiguration resource providers:

Register-AzResourceProvider -ProviderNamespace Microsoft.HybridCompute

Register-AzResourceProvider -ProviderNamespace Microsoft.GuestConfiguration

This will result in the following output:

```
Azure:/
PS Azure:\> Register-AzResourceProvider -ProviderNamespace Microsoft.HybridCompute

ProviderNamespace : Microsoft.HybridCompute
RegistrationState : Registering
ResourceTypes     : {machines, operations}
Locations         : {West US 2, West Europe, Southeast Asia}


Azure:/
PS Azure:\> Register-AzResourceProvider -ProviderNamespace Microsoft.GuestConfiguration

ProviderNamespace : Microsoft.GuestConfiguration
RegistrationState : Registering
ResourceTypes     : {guestConfigurationAssignments, software, softwareUpdates, softwareUpdateProfile…}
Locations         : {East US 2, South Central US}
```

Note that the resource providers are only registered in specific locations.

(Networking

During installation and runtime, the agent requires connectivity to Azure Arc service endpoints. If outbound connectivity is blocked by the firewall, make sure that the following URLs are not blocked:

Required Azure service endpoints include:

Guest Configuration)

Incorrect:

Not A, Not B: Connect the on-premises machine to Azure Arc

To connect the on-premises machine to Azure Arc, we first need install the agent on the on-premises machine (not any Gateways).

Not E: Azure Bastion now supports connectivity to Azure virtual machines or on-premises resources via specified IP address.

Azure Bastion is a fully managed service that provides more secure and seamless Remote Desktop Protocol (RDP) and Secure Shell Protocol (SSH) access to virtual machines (VMs) without any exposure through public IP addresses.

Reference: https://techcommunity.microsoft.com/t5/azure-developer-community-blog/azure-arc-for-servers-getting-started/ba-p/1262062

https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/manage/hybrid/server/best-practices/arc-policies-mma

https://docs.microsoft.com/en-us/azure/governance/policy/concepts/guest-configuration

SC-100 PDF Dumps SC-100 Practice Test SC-100 Braindumps