Exam SC-100 Microsoft Cybersecurity Architect

Contents

Review Questions.......1

1. Conditional Access policy.......1

2. Entitlement management.......2

3. The Cloud Adoption Framework (CAF).......2

4. Enable the relevant data connectors in Sentinel.......2

5. Azure Arc.......3

6. Entitlement Management.......3

7. MCRA – Microsoft Cybersecurity Reference Architecture.......4

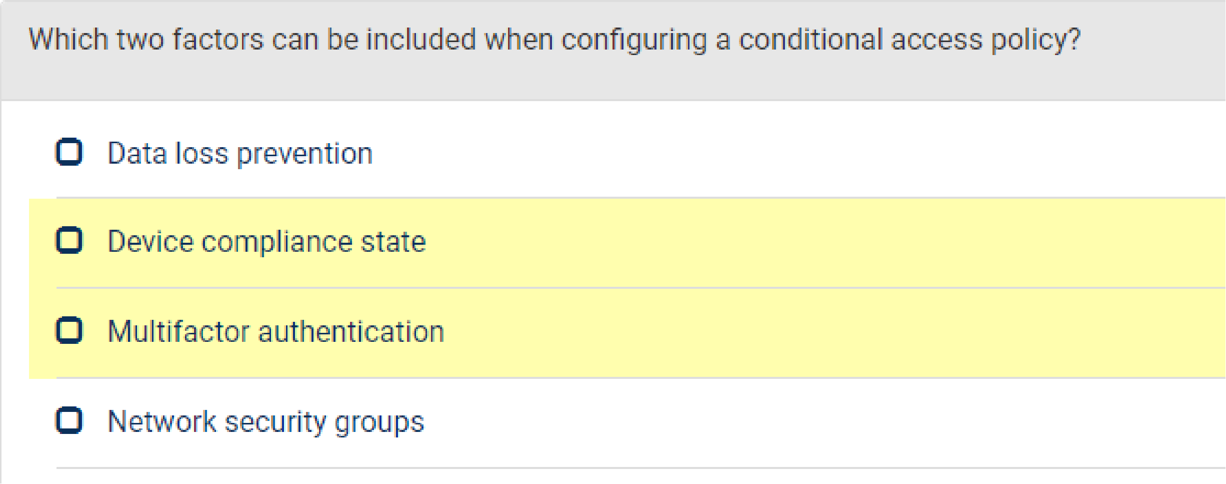
8. Network Security Groups.......4

10. Application Insights.......5

Additional References.......5

Review Questions

1. Conditional Access policy



Which two factors can be included when configuring a conditional access policy?

□ Data loss prevention

□ Device compliance state

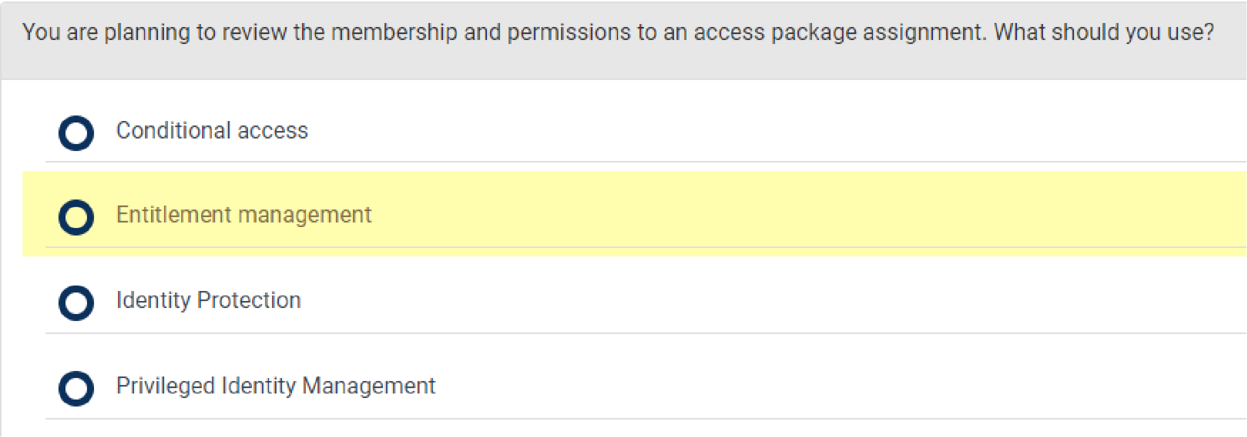
□ Multifactor authentication

□ Network security groups

Conditional access policies can include both user and device requirements that can then grant or deny a user access to a cloud application.

https://learn.microsoft.com/en-us/training/modules/design-identity-security-strategy/5-secure-conditional-access

2. Entitlement management



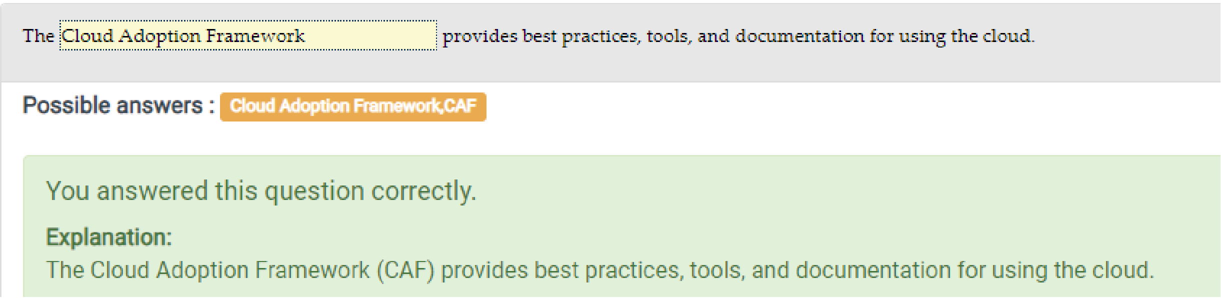
You are planning to review the membership and permissions to an access package assignment. What should you use?

- ○ Conditional access
- ○ Entitlement management
- ○ Identity Protection
- ○ Privileged Identity Management

Access packages are created and reviewed using entitlement manager.

https://learn.microsoft.com/en-us/training/modules/design-identity-security-strategy/7-define-identity-governance-for-access-reviews-entitlement-management

3. The Cloud Adoption Framework (CAF)



The Cloud Adoption Framework provides best practices, tools, and documentation for using the cloud.

Possible answers : Cloud Adoption Framework,CAF

You answered this question correctly.

Explanation:
The Cloud Adoption Framework (CAF) provides best practices, tools, and documentation for using the cloud.

https://learn.microsoft.com/en-us/training/modules/build-overall-security-strategy-architecture/4-develop-security-requirements-based-business-goals

4. Enable the relevant data connectors in Sentinel

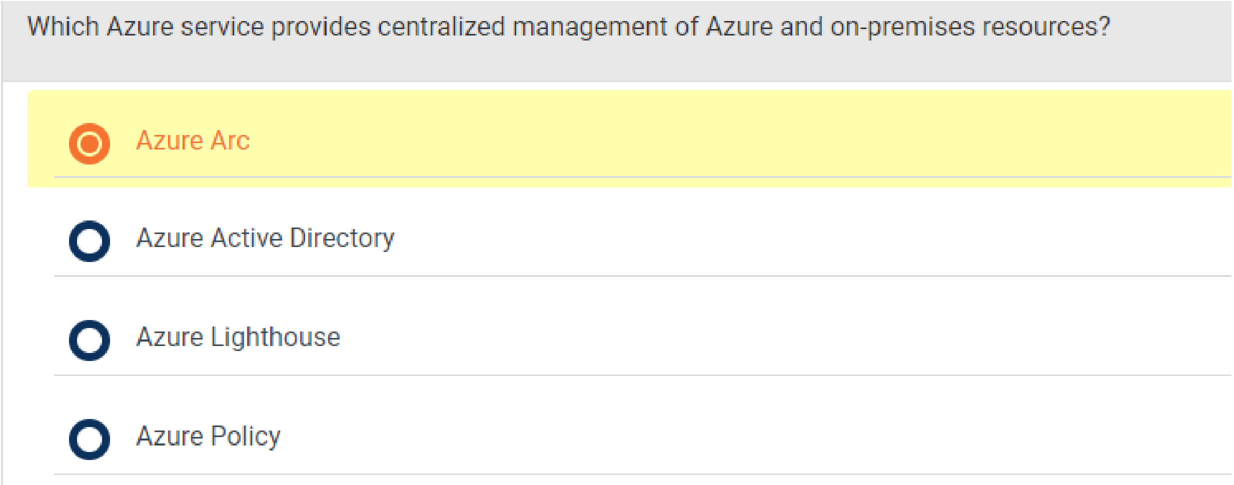
You are planning to use Microsoft Sentinel for visibility, automation, and orchestration of security monitoring. You need to ensure that you can establish visibility of third-party virtual appliances in Sentinel. What should you do?

- ○ Create an automation rule.
- ○ Create a playbook.
- ○ Enable incident notifications.
- ● Enable relevant data connectors.

To ensure visibility into third-party events and monitoring, the relevant data connector must be configured so that data is captured into the underlying Log Analytics workspace.

Reference: https://learn.microsoft.com/en-us/training/modules/design-security-operations-strategy/5-design-strategy-security-information-event-management

5. Azure Arc



Which Azure service provides centralized management of Azure and on-premises resources?

◉ Azure Arc

○ Azure Active Directory

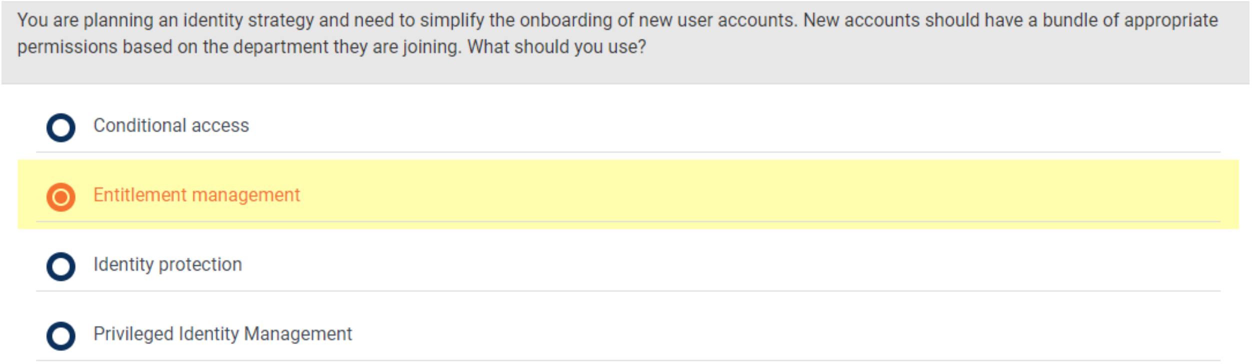
○ Azure Lighthouse

○ Azure Policy

Azure Arc provides hybrid management of resources, whether they are in Azure, on premises, or in other cloud environments.

Reference: https://learn.microsoft.com/en-us/training/modules/build-overall-security-strategy-architecture/7-design-for-hybrid-multi-tenant-environments

6. Entitlement Management



You are planning an identity strategy and need to simplify the onboarding of new user accounts. New accounts should have a bundle of appropriate permissions based on the department they are joining. What should you use?

○ Conditional access

◉ Entitlement management

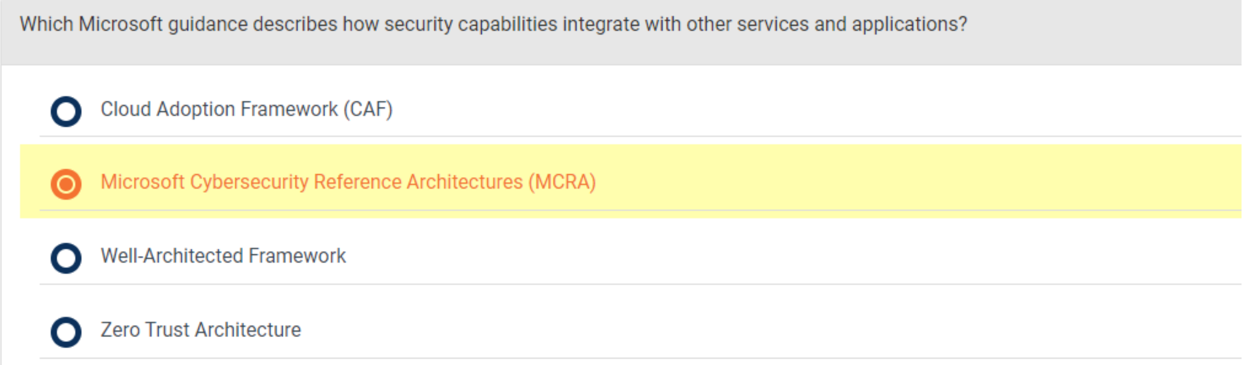
○ Identity protection

○ Privileged Identity Management

Entitlement management includes the ability to create access packages, which can be used to bundle group and permission membership for new and external users.

Reference: https://learn.microsoft.com/en-us/training/modules/design-identity-security-strategy/7-define-identity-governance-for-access-reviews-entitlement-management

7. MCRA – Microsoft Cybersecurity Reference Architecture



Which Microsoft guidance describes how security capabilities integrate with other services and applications?

○ Cloud Adoption Framework (CAF)

● Microsoft Cybersecurity Reference Architectures (MCRA)

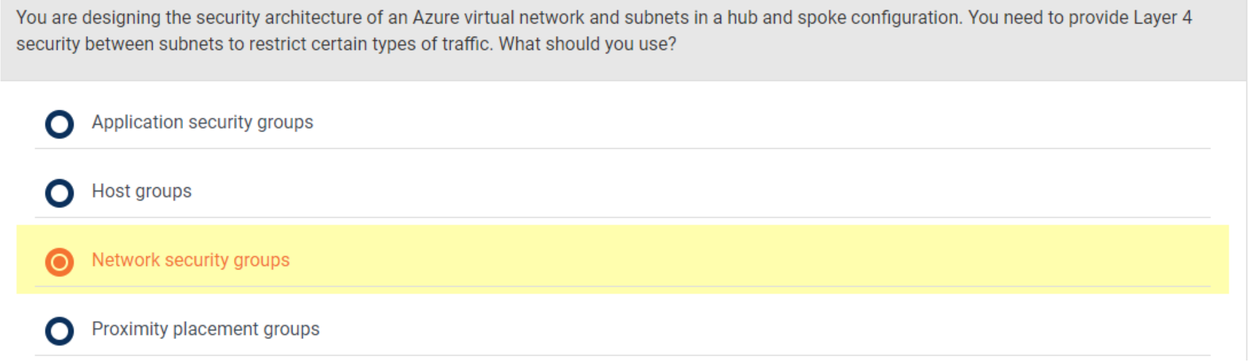
○ Well-Architected Framework

○ Zero Trust Architecture

The Microsoft Cybersecurity Reference Architectures (MCRA) describes how Microsoft security capabilities integrate with Microsoft services, including Azure and Office 365, as well as third-party applications.

Reference: https://learn.microsoft.com/en-us/training/modules/build-overall-security-strategy-architecture/3-develop-integration-points-architecture

8. Network Security Groups



You are designing the security architecture of an Azure virtual network and subnets in a hub and spoke configuration. You need to provide Layer 4 security between subnets to restrict certain types of traffic. What should you use?

○ Application security groups

○ Host groups

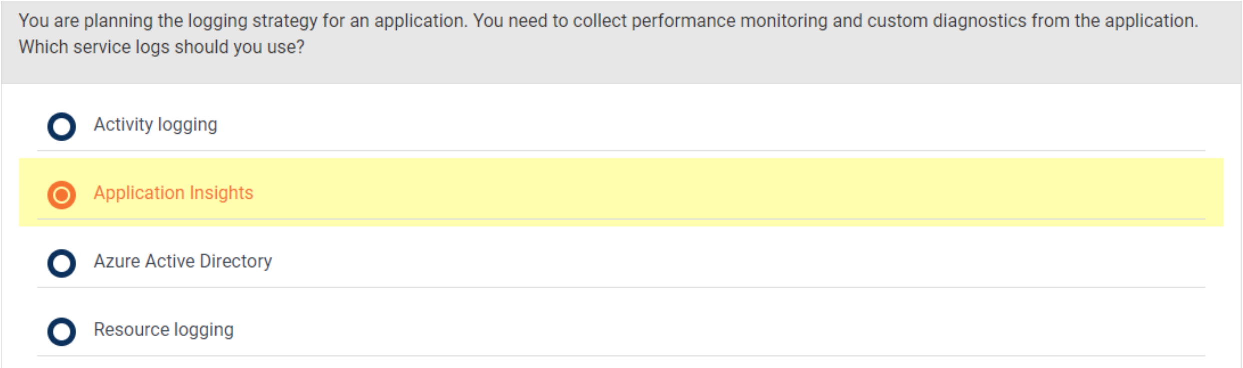
● Network security groups

○ Proximity placement groups

You should include network security groups between the subnets in order to filter traffic based on protocol, port, or IP address.

Reference: https://learn.microsoft.com/en-us/training/modules/build-overall-security-strategy-architecture/8-design-technical-governance-strategies-for-traffic-filtering-segmentation

10. Application Insights



You are planning the logging strategy for an application. You need to collect performance monitoring and custom diagnostics from the application. Which service logs should you use?

○ Activity logging

● Application Insights

○ Azure Active Directory

○ Resource logging

Azure Application Insight allows developers to capture exceptions and custom diagnostics for an application running on Azure.

Reference: https://learn.microsoft.com/en-us/training/modules/design-security-operations-strategy/3-design-log-audit-security-strategy

Additional References

https://learning.oreilly.com/certifications/9780137977697/