

SC-100 Microsoft Cybersecurity Architect

Practice Questions

[SC-100: Microsoft Cybersecurity Architect \(Pearson Practice Test\) - O'Reilly Online Learning \(oreilly.com\)](#)

Contents

Objective 1: Design a Zero Trust strategy and architecture	5
1. Factors included in Conditional Access	5
2. Entitle Management	5
3. The Cloud Adoption Framework (CAF).....	6
4. Microsoft Sentinel – Enable relevant data connectors	6
5. Azure Arc	7
6. Entitle Management	7
7. Microsoft Cybersecurity Reference Architecture (MCRA).....	8
8. Network Security Groups	8
9. Application Insights	9
10. Activity Logs track changes that are made to Azure resources.....	9
11. DMZ.....	10
12. The mean time to acknowledge (MTTA)	10
13. Designing security with resiliency in mind.....	10
14. Defender for Cloud.....	11
15. Logging Categories	11
16. Network Watcher	12
17. Conditional Access	13
18. Workflow automation tools	14
19. Zero Trust Rapid Modernization Plan (RaMP) components.....	14
20. Azure AD Privileged Identity Management includes the ability to create access reviews.....	15
21. Privileged Identity Management.....	15
22. The mean time to remediate (MTTR)	16
23. Access Packages	16
24. Foundational design principles included in a Zero Trust architecture	16

25. Azure Logic Apps is a resource type that allows you to create and run workflows	17
26. The Defender for Cloud Secure Score	17
27. Azure AD DS requires the use of Azure AD password hash synchronization with Azure AD Connect.	18
28. The company security policy states that authentication for cloud services must occur in the cloud.	18
29. Azure AD Pass-through Authentication.....	18
30. You are designing a hub and spoke network architecture for an Azure environment.....	19
31. Access reviews enable administrators and group owners to review membership and privileged role activation.....	19
32. A firewall can act as a Layer 7 IDS	20
33. Zero Trust principles.....	21
34. Report Reader	21
35. Azure Policy	22
36. Federated Authentication	22
Objective 2: Evaluate Governance Risk Compliance (GRC) technical strategies	22
1. Azure Policy	23
2. Secure Score	23
3. Risk Response.....	24
4. Threat intelligence in Sentinel.....	24
5. Azure Policy Effects	25
6. Azure Policy	26
7. Defender for Cloud.....	26
8. Rapid Modernization Plan (RaMP)	26
9. Azure Policy Effects	27
10. Defender for Cloud uses MITRE ATTACK framework.....	27
11. Workflow Automation is built into Defender for Cloud	28
12. Data sovereignty.....	29
13. Azure Automation	29
14. Azure Blueprints.....	29
15. Azure Landing Zone.....	29
16. Defender for Cloud provides continual assessment	30

17. Operational compliance processes and the appropriate tools	30
Objective 3 - Design security for infrastructure	31
1. The Security Compliance Toolkit	31
2. Key Vault Contributor	31
3. Shared access signatures	32
4. Remote Connectivity Options	35
5. Access to Azure SQL Database using private endpoints on a virtual network	40
6. For Linux VMs, you can deploy the Defender for Endpoint agent	49
7. Azure Policy	50
Next - Video#: Azure Update Manager with Azure Policies	50
8. System-assigned managed identity	50
9. App protection policy	51
10. Enroll the device	51
11. Defender for Cloud	52
12. Azure disk encryption	52
13. Security baseline	53
14. Defender for Identity	53
15. Security baseline	53
16. Defender for Cloud and vulnerability assessments	54
17. Security baseline	54
Objective 4: Design a strategy for data and applications	54
1. Azure AD B2B	55
2. VMs can use Azure Disk Encryption with customer-managed keys for encrypting data at rest	59
3. Microsoft Threat Modeling Tool	60
4. OWASP	61
5. Service and Type of Encryption	62
6. A sensitive information type with exact data match can use existing data to train the DLP policies.	62
7. Azure Application Gateway	62
8. Phases of the DevOps life cycle	63
9. DLP Policy components	63
10. Conditional Access App Control	64

11. Microsoft Purview Data Map	64
12. STRIDE	67
13. Mitigate SQL Injection – Azure Application Gateway.....	67
14. Microsoft Information Protection SDK.....	70
15. Principle of least privilege	71
16. Security strategy for Azure SQL Database.....	71
17. Data Classification Capability	72
18. Azure Front Door.....	72
19. Azure AD B2C	72
20. Trainable Classifier	73
21. Authenticate using a managed identity	73
22. A custom sensitive information type	74
Objective 5: Recommend security best practices and priorities.....	74
1. Requirements for a DevSecOps process	74
2. Zero Trust	78
3. OWASP threat modeling	79
4. Azure policy.....	81
5. DevSecOps: Security requirements.....	83
6. Azure AD Identity Protection	86
7. Microsoft Cloud Security Benchmark (MCSB).....	88
8. DevSecOps processes.....	90
9. DevSecOps: Security Requirements	93
10. Privileged Identity Management.....	97
11. Defender for Identity.....	99
12. Attack surface reduction rules	101
13. Designing security with a focus on protecting an organization from ransomware.	103
14. Defender for Identity.....	106
15. What are two security requirements that you should include in the operate phase of DevSecOps process?	106
16. The three principles of a Zero Trust approach to security	107
17. Two methods of preventing attackers from escalating privileges?.....	108
18. MITTRE ATT&CK Framework	108

19. Azure AD Application Proxy.....	111
20. Zero Trust Rapid Modernization Plan (RaMP).....	115
References.....	117

Objective 1: Design a Zero Trust strategy and architecture

1. Factors included in Conditional Access

Question 1 of 36

Question Id : SC-100-CP-1-030

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

- ☐ Data loss prevention
- ☒ Device compliance state
- ☒ Multifactor authentication
- ☐ Network security groups

Select 2 answers

You answered this question correctly.

Explanation:

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

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

2. Entitle Management

Question 2 of 36

Question Id : SC-100-CP-1-036

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

You answered this question correctly.

Explanation:

Access packages are created and reviewed using entitlement manager.

Review: <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)

Question 3 of 36

Question Id : SC-100-CP-1-005

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. x

Explanation:

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

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

4. Microsoft Sentinel – Enable relevant data connectors

Question 4 of 36

Question Id : SC-100-CP-1-021

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.**

You answered this question correctly. x

Explanation:

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

You answered this question correctly.

x

Explanation:

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. Entitle 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

You answered this question correctly.

x

Explanation:

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. Microsoft Cybersecurity Reference Architecture (MCRA)

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

You answered this question correctly.

×

Explanation:

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 answered this question correctly.

×

Explanation:

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>

9. Application Insights

Question 9 of 36

Question Id : SC-100-CP-1-017

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

You answered this question correctly.

×

Explanation:

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>

10. Activity Logs track changes that are made to Azure resources

You are planning the logging strategy for an application. You need to ensure that you can track change operations to resources deployed in your Azure subscription. Which logs should you monitor?

- ☒ Activity logs
- ☐ Application insight logs
- ☐ Azure Active Directory logs
- ☐ Resource logs

You answered this question correctly.

×

Explanation:

The Azure activity logs track changes that are made to Azure resources within a subscription at the control plane level.

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

11. DMZ

A **DMZ** is a type of network that exists between the Internet and a hub network to provide security segmentation between the two environments.

Possible answers : **perimeter,perimeter network,DMZ,demilitarized zone**

You answered this question correctly. ×

Explanation:

A DMZ or perimeter network is a type of network that exists between the Internet and a hub network that typically includes security services, such as a firewall, to protect the hub network from Internet traffic.

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

In this context the Hub Network is the LAN.

12. The mean time to acknowledge (MTTA)

The **MTTA** is the time between receiving an alert and a security analyst beginning their investigation.

Possible answers :

You answered this question correctly. ×

Explanation:

The mean time to acknowledge (MTTA) is how a security operations team measures the time between when systems generate an alert and the time that a security analyst begins their investigation of that alert.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-security-operations-strategy/2-understand-frameworks-processes-procedures>

13. Designing security with resiliency in mind

When **designing security with resiliency in mind**, which two goals should be included?

☐ Isolate all business functions.

☐ Isolate all technical functions.

☒ Prevent further damage.

☒ Protect critical operations.

Select 2 answers

You answered this question correctly. ×

Explanation:

During an incident, it is important to prevent further damage to the environment and protect the critical operations of the business.

Reference: <https://learn.microsoft.com/en-us/training/modules/build-overall-security-strategy-architecture/6-design-security-for-resiliency-strategy>

14. Defender for Cloud

You plan to deploy on Azure an application that meets PCI compliance. As part of the solution, you need to be able to create alerts and automate notifications based on this compliance. What should you use?

☒ Defender for Cloud

☐ Log Analytics

☐ Logic Apps

☐ Microsoft Sentinel

You answered this question correctly.

Explanation:

Defender for Cloud enables you to monitor the security posture of your Azure subscription based on the Microsoft Cloud Security Benchmark as well regulatory compliance standards, including those for PCI compliance.

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

15. Logging Categories

Drag the Azure logging category on the left to the correct definition on the right.

Correct Answers

Activity logs

Azure Active Directory reporting

Resource logs

Application Insights

Matching items here:

Change tracking for actions performed on resources deployed to Azure

Activity logs ✓

User sign-in activities

Azure Active Directory reporting ✓

Tracks operations that were performed by the individual Azure resource

Resource logs ✓

Application performance monitoring service for web developers

Application Insights ✓

You answered this question correctly.

Explanation:

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

16. Network Watcher

You manage a hybrid Azure/on-premises environment that is connected using a virtual private network (VPN). The VPN tunnel has failed, and you need to diagnose the connection issues. What should you use?

- ☐ Diagnostic logging
- ☐ Log Analytics
- ☐ Network Security Group flow logs

☒ Network Watcher

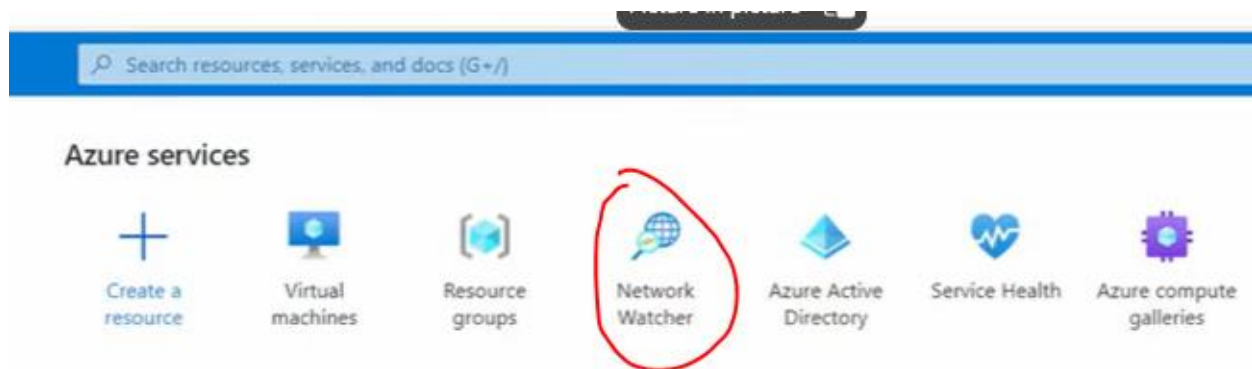
You answered this question correctly. x

Explanation:

The Network Watcher service includes a tool that provides VPN connection troubleshooting. This service can be used to diagnose IPsec and L2TP VPN tunnel connection issues.

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

[\(151\) What is Network Watcher and How Did It Get In My Subscription! - YouTube](#)



Network Watcher

Search

Filter for any field...

Subscription equals all Resource group equals all Location equals all Add filter

Showing 1 to 16 of 16 records.

Name	Subscription	Location	Resource group
NetworkWatcher_centralus	Microsoft Azure Sponsorship	Central US	NetworkWatcherRG
NetworkWatcher_centralus	Visual Studio Enterprise Subscr...	Central US	NetworkWatcherRG
NetworkWatcher_centralus	Pay-As-You-Go (MSDN)	Central US	NetworkWatcherRG
NetworkWatcher_eastus	Microsoft Azure Sponsorship	East US	NetworkWatcherRG
NetworkWatcher_eastus	Pay-As-You-Go (MSDN)	East US	NetworkWatcherRG
NetworkWatcher_eastus2	Microsoft Azure Sponsorship	East US 2	NetworkWatcherRG
NetworkWatcher_northeurope	Microsoft Azure Sponsorship	North Europe	NetworkWatcherRG
NetworkWatcher_northeurope	Visual Studio Enterprise Subscr...	North Europe	NetworkWatcherRG
NetworkWatcher_southcentralus	Microsoft Azure Sponsorship	South Central US	NetworkWatcherRG
NetworkWatcher_southeastasia	Pay-As-You-Go (MSDN)	Southeast Asia	NetworkWatcherRG
NetworkWatcher_westeurope	Microsoft Azure Sponsorship	West Europe	NetworkWatcherRG
NetworkWatcher_westus	Microsoft Azure Sponsorship	West US	NetworkWatcherRG
NetworkWatcher_westus	Pay-As-You-Go (MSDN)	West US	NetworkWatcherRG

17. Conditional Access

Question 17 of 36

Question Id : SC-100-CP-1-029

Conditional access provide(s) the ability to grant or deny access to cloud applications based on multiple requirements.

Possible answers : Conditional access, Conditional access policies

You answered this question correctly.

Explanation:

Conditional access allows you to create policies that specify multiple policies for the authentication process to succeed or require additional conditions to be met to allow a user to connect.

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

18. Workflow automation tools

Drag the workflow automation tool on the left to the correct definition on the right.

Correct Answers

Azure Logic Apps

Microsoft Defender for Cloud

Microsoft Sentinel

Matching items here:

Provides designer-based workflow automation using connectors.

Azure Logic Apps ✓

Can trigger workflow automation based on changes to regulatory compliance.

Microsoft Defender for Cloud ✓

Provides automation rules and playbooks to facilitate incident management and orchestrated response.

Microsoft Sentinel ✓

You answered this question correctly.

Explanation:

Reference: <https://learn.microsoft.com/en-us/training/modules/design-security-operations-strategy/6-evaluate-security-workflows>

19. Zero Trust Rapid Modernization Plan (RaMP) components

You are a designing the security architecture for a hybrid environment with Azure and on-premises resources. You need to include the Zero Trust Rapid Modernization Plan (RaMP) components in your design. What should you use?

☐ Cloud Adoption Framework (CAF)

☒ Microsoft Cybersecurity Reference Architectures (MCRA)

☐ Well-Architected Framework

☐ Zero-Trust Architecture

You answered this question correctly.

Explanation:

The Microsoft Cybersecurity Reference Architectures includes the Rapid Modernization Plan (RaMP), which includes specifics on security operations for a Zero Trust environment.

20. Azure AD Privileged Identity Management includes the ability to create access reviews

You are planning to review the privileged access of Azure resource roles. What should you use to create the access review?

- ☐ Conditional access
- ☐ Entitlement management
- ☐ Identity Protection

☒ Privileged Identity Management

You answered this question correctly. ×

Explanation:

Azure AD Privileged Identity Management includes the ability to create access reviews for Azure resource and Azure Active Directory role assignments.

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

21. Privileged Identity Management

You are planning a privileged identity strategy and need to ensure that privileged accounts have elevated permissions for only a specific period of time. What should you use?

- ☐ Conditional access
- ☐ Custom attributes
- ☐ Identity Protection

☒ Privileged Identity Management

You answered this question correctly. ×

Explanation:

Privileged Identity Management allows you to make roles eligible for assignment and then, when they are activated, the roles are only assigned for a configurable amount of time.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-identity-security-strategy/6-design-strategy-for-role-assignment-delegation>

22. The mean time to remediate (MTTR)

The **mean time to remediate** is the time between a security analyst beginning their investigation and when the incident is remediated.

Possible answers : **mean time to remediate, MTTR, time to remediate, time to resolution, mean time to resolution**

You answered this question correctly. ×

Explanation:

The mean time to remediate (MTTR) is the time period between when an analyst begins their investigation into an incident and when that incident has been remediated.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-security-operations-strategy/2-understand-frameworks-processes-procedures>

23. Access Packages

A(n) **Access package** is a feature of entitlement management that allows you to bundle group membership and application assignments together.

Possible answers :

You answered this question correctly. ×

Explanation:

Access packages are a feature of entitlement management that allow you to bundle group membership and application assignments together with policies and workflow approvals.

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

24. Foundational design principles included in a Zero Trust architecture

Which two **foundational design principles** are included in a Zero Trust architecture?

☒ Assume breach

☐ Defense in depth

☐ Multifactor authentication

☒ Verify explicitly

Select 2 answers

You answered this question correctly. ×

Explanation:

The three foundational principles of a Zero Trust architecture include are verify explicitly, use least-privilege access, and assume breach. Defense in depth and MFA might be components of the security architecture, but they are not specifically part of Zero Trust.

Reference: <https://learn.microsoft.com/en-us/training/modules/build-overall-security-strategy-architecture/2-zero-trust-overview>

25. Azure Logic Apps is a resource type that allows you to create and run workflows

You are planning to automate the notification workflow for new Azure resource events, and you need to identify a platform for creating and running workflows. What should you use?

☐ Defender for Cloud

☐ Graph API

☒ Logic Apps

☐ Sentinel

You answered this question correctly.

×

Explanation:

Azure Logic Apps is a resource type that allows you to create and run workflows that you design and create.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-security-operations-strategy/6-evaluate-security-workflows>

26. The Defender for Cloud Secure Score

A(n) provides a numerical value of the current configuration of resources in a subscription compared against the Center for Internet Security controls and external benchmarks.

Possible answers :

You answered this question correctly.

×

Explanation:

The Defender for Cloud Secure Score measures the existing configuration of resources against the Microsoft Cloud Security Benchmark and the Center for Internet Security controls to provide a point-in-time reference for how these resources are configured, with security in mind.

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

27. Azure AD DS requires the use of Azure AD password hash synchronization with Azure AD Connect.

You are planning a hybrid on-premises/Azure authentication strategy. The company plans to use Azure Active Directory Domain Services (Azure AD DS) and synchronize it with Azure Active Directory. Which cloud authentication method should you use?

☐ Azure AD cloud-only users

☒ Azure AD password hash synchronization

☐ Azure AD Pass-through Authentication

☐ Federated authentication

You answered this question correctly. ×

Explanation:

Azure AD DS requires the use of Azure AD password hash synchronization with Azure AD Connect. This allows the Azure AD DS service to synchronize with Azure AD.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-identity-security-strategy/4-recommend-secure-authentication-security-authorization-strategies>

28. The company security policy states that authentication for cloud services must occur in the cloud.

You are planning a hybrid on-premises/Azure authentication strategy. The company security policy states that authentication for cloud services must occur in the cloud. Which cloud authentication method should you use?

☐ Azure AD cloud-only users

☒ Azure AD password hash synchronization

☐ Azure AD Pass-through Authentication

☐ Federated authentication

You answered this question correctly. ×

Explanation:

To allow the authentication to stay in the cloud and not be transferred elsewhere, the password of the user account must be synchronized using Azure AD password hash synchronization.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-identity-security-strategy/4-recommend-secure-authentication-security-authorization-strategies>

29. Azure AD Pass-through Authentication

It requires an agent in the on-premises environment to perform the authentication with the local Active Directory domain controllers.

You are planning a hybrid on-premises/Azure authentication strategy. The company's security policy states that authentication must be performed in the on-premises Active Directory environment. Which cloud authentication method should you use?

- ☐ Azure AD cloud-only users
- ☐ Azure AD password hash synchronization
- ☒ Azure AD Pass-through Authentication
- ☐ Federated authentication

You answered this question correctly. x

Explanation:

Azure AD Pass-through Authentication requires an agent in the on-premises environment to perform the authentication with the local Active Directory domain controllers.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-identity-security-strategy/4-recommend-secure-authentication-security-authorization-strategies>

30. You are designing a hub and spoke network architecture for an Azure environment.

You are designing a hub and spoke network architecture for an Azure environment. You need to identify an available address space to use with the virtual networks. Which two address spaces can you assign to an Azure virtual network?

- ☒ 10.10.0.0/16
- ☐ 169.254.0.0/16
- ☒ 172.16.0.0/16
- ☐ 172.50.0.0/16

Select 2 answers

You answered this question correctly. x

Explanation:

The address spaces 10.10.0.0/16 and 172.16.0.0/16 fall into the RFC 1918 address ranges for private IP addresses and can be used with Azure virtual networks.

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

31. Access reviews enable administrators and group owners to review membership and privileged role activation

A(n) provides a way to ensure that only accounts that need access to a resource are members of a privileged group.

Possible answers :

You answered this question correctly. ×

Explanation:

An access review enables administrators and group owners to review membership and privileged role activation to ensure that users do not have excessive permissions over time.

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

32. A firewall can act as a Layer 7 IDS

You are designing a hybrid Azure/on-premises network. You need to ensure that all traffic traverses an intrusion detection system (IDS). What should you include in the design?

☐ Application gateway

☐ ExpressRoute

☒ Firewall

☐ Virtual network gateway

You answered this question correctly. ×

Explanation:

A firewall can act as a Layer 7 IDS. An application gateway only has a web application firewall and does not provide full IDS services. ExpressRoute and virtual network gateways do not provide any IDS capabilities.

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

33. Zero Trust principles

You are designing an architecture that follows the principles of Zero Trust. Drag the Zero Trust principle on the left to the correct definition on the right.

Correct Answers

Verify explicitly

Use least-privilege access

Assume breach

Matching items here:

Authenticate and authorize based on all available data points.

Verify explicitly ✓

Restrict access using just-in-time access.

Use least-privilege access ✓

Minimize segment access and blast radius.

Assume breach ✓

You answered this question correctly.

Explanation:

Reference: <https://learn.microsoft.com/en-us/training/modules/build-overall-security-strategy-architecture/2-zero-trust-overview>

34. Report Reader

You need to ensure that a security analyst can read the audit activity report in Azure AD. The analyst must not have more permissions than necessary to read the Azure AD audit logs. Which role should you assign to the analyst?

☒ Report Reader

☐ Global Reader

☐ Security Administrator

☐ Global Administrator

You answered this question correctly.

Explanation:

All four roles listed provide the ability to read the Azure AD audit log. However, the role that provides least privilege from those available is the Report Reader. All other roles would also allow read and/or change access to other audit logs and security configurations.

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

35. Azure Policy

Which Azure service provides methods to implement and manage governance, compliance reporting, security, and cost management?

- ☐ Azure Arc
- ☐ Azure Active Directory
- ☐ Azure Lighthouse
- ☒ Azure Policy

You answered this question correctly.

×

Explanation:

Azure Policy provides a way to implement and require resources to meet governance guidelines, enforce consistent deployments, and help organizations achieve regulatory compliance.

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

36. Federated Authentication

You are planning a hybrid authentication strategy using a third-party service for multifactor authentication. Which cloud authentication method should you use?

- ☐ Azure AD cloud-only users
- ☐ Azure AD password hash synchronization
- ☐ Azure AD Pass-through Authentication
- ☒ Federated authentication

You answered this question correctly.

×

Explanation:

Using a third-party service would require AD FS to transfer the authentication to the other identity provider.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-identity-security-strategy/4-recommend-secure-authentication-security-authorization-strategies>

Objective 2: Evaluate Governance Risk Compliance (GRC) technical strategies

1. Azure Policy

You are implementing security for resources in an Azure subscription. You need to ensure that all virtual machines have a specific extension installed. What should you use?

☐ Azure Advisor

☒ Azure Policy

☐ Defender for Cloud

☐ Microsoft Sentinel

You answered this question correctly. ×

Explanation:

Azure Policy enables you to create guardrails for your environment, including using the DeployIfNotExist effect type to deploy additional components.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-regulatory-compliance-strategy/5-design-validate-implementation-of-azure-policy>

2. Secure Score

Which component of Defender for Cloud provides insights into a key performance indicator related to how many security recommendations have been implemented for a subscription?

☐ Alerts

☒ Secure Score

☐ Security Posture

☐ Workload protection

You answered this question correctly. ×

Explanation:

Secure Score in Defender for Cloud provides you with a key performance indicator (KPI) related to how many recommendations have been implemented on a subscription.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-security-posture-recommend-technical-strategies-to-manage-risk/7-postures-use-secure-scores>

3. Risk Response

When planning to mitigate risks associated with known threats, in which phase of the risk management process would you tolerate or accept a known risk?

☐ Identification

☐ Assessment

☒ Response

☐ Monitoring

You answered this question correctly. ×

Explanation:

The risk management process has four phases: identification, assessment, response, and monitoring. Taking an action, even if the action is to accept the risk, is considered responding to the threat.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-security-posture-recommend-technical-strategies-to-manage-risk/6-interpret-technical-threat-intelligence-recommend-risk-mitigations>

4. Threat intelligence in Sentinel

Which tool in Microsoft Sentinel provides context, relevance, and priority to alerts?

☐ Analytics rules

☐ Hunting

☒ Threat intelligence

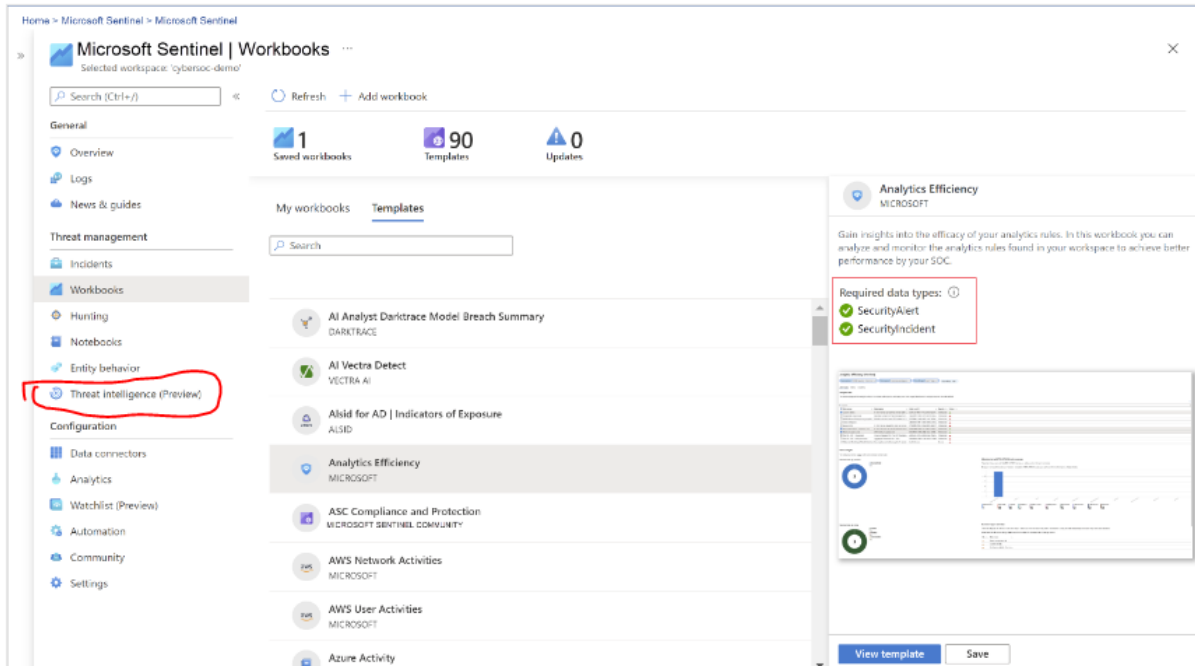
☐ Workbooks

You answered this question correctly. ×

Explanation:

Threat intelligence in Microsoft Sentinel provides additional information around an alert so that security advisors can come to a solution faster.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-security-posture-recommend-technical-strategies-to-manage-risk/6-interpret-technical-threat-intelligence-recommend-risk-mitigations>



[What is Microsoft Sentinel? | Microsoft Learn](#)

5. Azure Policy Effects

Question 5 of 17

Question Id : SC-100-CP-1-043

You are implementing security for resources in an Azure subscription. You need to ensure that each resource has a default cost center tag applied if the resource was deployed without a cost center tag. Which two Azure Policy effects should you use?

- ☒ Append
- ☐ Audit
- ☐ AuditIfNotExist
- ☒ DeployIfNotExist

Select 2 answers

You answered this question correctly.

Explanation:

Azure Policy enables you to create guardrails for your environment, including being able alter or add to a deployment when the request is submitted with the Modify, Append, or DeployIfNotExist policy effects.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-regulatory-compliance-strategy/5-design-validate-implementation-of-azure-policy>

Azure Policy enables you to create guardrails for your environment, including being able alter or add to a deployment when the request is submitted with the Modify, Append, or DeployIfNotExist policy effects.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-regulatory-compliance-strategy/5-design-validate-implementation-of-azure-policy>

6. Azure Policy

You are implementing security for resources in an Azure subscription. You need to ensure that storage accounts cannot be deployed with HTTPS disabled. What should you use?

☐ Azure Advisor

☒ Azure Policy

☐ Defender for Cloud

☐ Microsoft Sentinel

Azure Policy enables you to create guardrails for your environment, including blocking deployments that do not meet requirements.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-regulatory-compliance-strategy/5-design-validate-implementation-of-azure-policy>

7. Defender for Cloud

You are implementing security for resources in an Azure subscription that are subject to SOC TSP regulatory compliance. You need to identify recommendations and reports for the compliance of these resources. What should you use?

☐ Azure Advisor

☐ Azure Policy

☒ Defender for Cloud

☐ Microsoft Sentinel

Defender for Cloud provides a unified view of security, including reporting, recommendations, and compliance for an Azure subscription.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-regulatory-compliance-strategy/3-evaluate-infrastructure-compliance-use-microsoft-defender-for-cloud>

8. Rapid Modernization Plan (RaMP)

Question Id : SC-100-CP-1-046

helps you define how to establish a cloud security posture and provides guidance for deployment paths.

Rapid Modernization Plan (RaMP) can help you define your cloud security posture and provides deployment paths for various layers of cloud security.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-security-posture-recommend-technical-strategies-to-manage-risk/2-postures-use-benchmarks>

9. Azure Policy Effects

You are implementing security for resources in an Azure subscription. You need to ensure that Azure resource deployments using an Azure region that has not been approved are not deployed. Which Azure Policy component should you configure?

- ☐ Array
- ☐ Assignment
- ☒ Effect
- ☐ Location

Azure Policy enables you to create guardrails for your environment, including being able to deny a deployment based on an Azure region using the Deny effect in the policy definition.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-regulatory-compliance-strategy/5-design-validate-implementation-of-azure-policy>

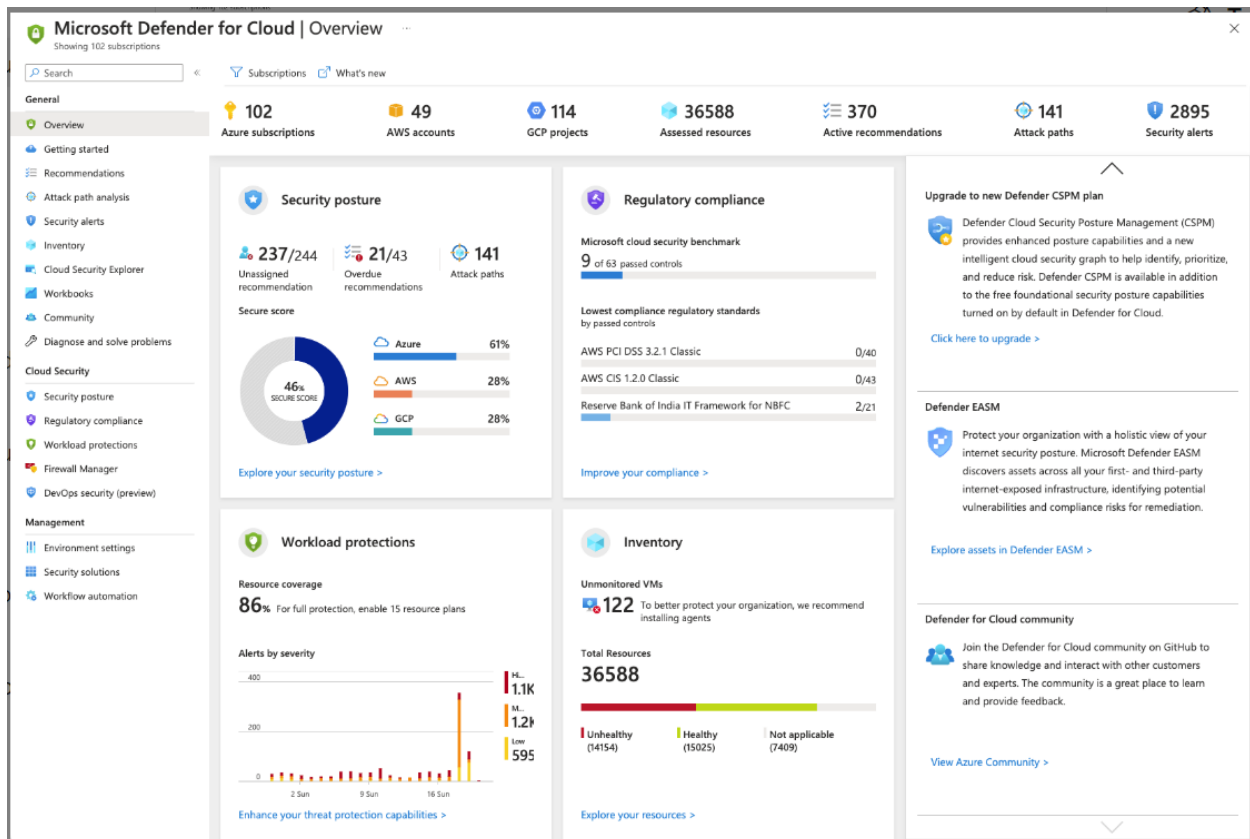
10. Defender for Cloud uses MITRE ATTACK framework

Which framework does Defender for Cloud use to allow you to identify security recommendations based on specific tactics?

- ☐ Cloud Adoption Framework
- ☒ MITRE ATTACK
- ☐ MITRE DEFEND
- ☐ Well-Architected Framework

Defender for Cloud correlates recommendations to increase your security posture and provides a reference to the MITRE Attack framework for these recommendations.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-security-posture-recommend-technical-strategies-to-manage-risk/3-postures-use-microsoft-defender-for-cloud>



[Review cloud security posture in Microsoft Defender for Cloud - Microsoft Defender for Cloud | Microsoft Learn](#)

11. Workflow Automation is built into Defender for Cloud

You need to configure an email notification when a new recommendation appears in Defender for Cloud. What should you configure?

- ☐ Azure Functions
- ☐ Azure Monitor
- ☐ Workbooks
- ☒ Workflow Automation

Workflow Automation is built into Defender for Cloud and allows you to create remediation logic, including email notifications.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-security-posture-recommend-technical-strategies-to-manage-risk/4-hygiene-of-cloud-workloads>

12. Data sovereignty

Data sovereignty mandates that data is stored in and under the legal jurisdiction of the country or region where the data is located.

Data sovereignty is part of a design solution involving where data will be stored and how the storage place affects the laws for that data.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-regulatory-compliance-strategy/6-design-for-data-residency-requirements>

13. Azure Automation

You are planning operational compliance for an organization. You need to ensure that security updates are scheduled and applied to virtual machines. Which tool should you use?

- ☐ Azure Advisor
- ☒ Azure Automation
- ☐ Azure Blueprints
- ☐ Azure Policy

Azure Automation accounts allow you to schedule and implement patch management for virtual machines.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-regulatory-compliance-strategy/2-interpret-compliance-requirements-their-technical-capabilities>

14. Azure Blueprints

Azure Blueprints bundle Azure Resource Manager templates, Azure Policy, and role assignments into a single container.

Azure Blueprints bundle together ARM templates, Azure policy definitions and assignments, and RBAC roles into a single solution.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-regulatory-compliance-strategy/6-design-for-data-residency-requirements>

15. Azure Landing Zone

An Azure **landing zone** is a multi-subscription diagram of an Azure environment that plans for security and other aspects of the Well-Architected Framework at enterprise scale.

An Azure landing zone (LZ) defines the subscription layout for resources according to the Well-Architected Framework.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-security-posture-recommend-technical-strategies-to-manage-risk/5-design-security-for-azure-landing-zone>

16. Defender for Cloud provides continual assessment

Which tool should you use to continually assess the resources in a subscription for security configuration and vulnerability issues?

- ☐ Azure Advisor
- ☐ Azure Policy
- ☒ Defender for Cloud
- ☐ Microsoft Sentinel

Defender for Cloud provides continual assessment of the resources and configuration of those resources in a subscription.

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-security-posture-recommend-technical-strategies-to-manage-risk/3-postures-use-microsoft-defender-for-cloud>

17. Operational compliance processes and the appropriate tools

Drag each operational compliance process to the appropriate tool to use to configure that process.

Correct Answers

- Patch management
- Policy enforcement
- Environment configuration
- Resource configuration

Matching items here:

- Azure Automation
- Patch management ✓**
- Azure Policy
- Policy enforcement ✓**
- Azure Blueprints
- Environment configuration ✓**
- Desired State Configuration
- Resource configuration ✓**

Reference: <https://learn.microsoft.com/en-us/training/modules/evaluate-regulatory-compliance-strategy/2-interpret-compliance-requirements-their-technical-capabilities>

Objective 3- Design security for infrastructure

1. The Security Compliance Toolkit

You are defining the baseline for endpoints. You need to test and edit the Microsoft-recommended baselines for Windows clients. What should you use?

- ☐ Azure Advisor
- ☐ Defender for Cloud
- ☐ Microsoft Purview
- ☒ Security Compliance Toolkit

The Security Compliance Toolkit allows you to test and edit the Microsoft-provided security baselines and customize them for your environment.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-strategy-for-secure-server-client-endpoints/2-specify-security-baselines-for-server-client-endpoints>

2. Key Vault Contributor

- ☐ Contributor
- ☐ Owner
- ☐ Key Vault Administrator
- ☒ Key Vault Contributor

The Key Vault Contributor role provides management access to Key Vault but not access to the data stored in Key Vault.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-strategy-for-secure-server-client-endpoints/6-design-strategy-manage-secrets-keys-certificates>

3. Shared access signatures

- ☐ Access keys
- ☐ Azure AD service principal
- ☐ Managed identity
- ☒ Shared access signature

A shared access signature (SAS) in a storage account can be set with an expiration date so that a new SAS token is required to access the storage account.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-strategy-for-secure-paas-iaas-saas-services/8-specify-security-requirements-for-storage-workloads>

Dashboard > Storage accounts >

Create storage account

The default deployment model is Resource Manager, which supports the latest Azure features. You may choose to deploy using the classic deployment model instead. [Choose classic deployment model](#)

Storage account name *	<input type="text" value="trevorsul"/>
	✖ The storage account name 'trevor' is already taken.
Location *	<input type="text" value="(US) West US 2"/>
Performance ⓘ	<input checked="" type="radio"/> Standard <input type="radio"/> Premium
Account kind ⓘ	<input type="text" value="StorageV2 (general purpose v2)"/>
Replication ⓘ	<input type="text" value="Read-access geo-redundant storage (RA-GRS)"/>
Blob access tier (default) ⓘ	<input type="radio"/> Cool <input checked="" type="radio"/> Hot

Dashboard > **trevorsullivan5**
Storage account

Search (Ctrl+/) « Open in Explorer → Move ↕ Refresh | Delete | Feedback

Overview

Activity log

Tags

Diagnose and solve problems

Access Control (IAM)

Data transfer

Events

Storage Explorer (preview)

Settings

Access keys

Essentials

Resource group ([change](#))
[storage](#)

Status
Primary: Available, Secondary: Available

Location
West US 2, West Central US

Subscription ([change](#))
[Trevor Sullivan Subscription](#)

Subscription ID

Performance/Access tier
Standard/Hot

Replication
Read-access geo-redundant storage (RA-GRS)

Account kind
StorageV2 (general purpose v2)

Classic alerts in Azure Monitor is announced to retire in 2021, it is recommended that you upgrade your classic alert rules to retain alerting functionality with the new alerting platform. For more information, see [Continue alerting with ARM storage accounts](#).

Dashboard > **trevorsullivan5** | Shared access signature

Storage account

Search (Ctrl+/) «

Events

Storage Explorer (preview)

Settings

Access keys

Geo-replication

CORS

Configuration

Encryption

Shared access signature

Firewalls and virtual networks

Private endpoint connections

A shared access signature (SAS) is a URI that grants restricted access rights to Azure Storage resources. You can provide a shared access signature to clients who should not be trusted with your storage account key but whom you wish to delegate access to certain storage account resources. By distributing a shared access signature URI to these clients, you grant them access to a resource for a specified period of time.

An account-level SAS can delegate access to multiple storage services (i.e. blob, file, queue, table). Note that stored access policies are currently not supported for an account-level SAS.

[Learn more](#)

Allowed services ⓘ

☒ Blob ☒ File ☒ Queue ☒ Table

Allowed resource types ⓘ

☐ Service ☐ Container ☐ Object

Allowed permissions ⓘ

☒ Read ☒ Write ☒ Delete ☒ List ☒ Add ☒ Create ☒ Update ☒ Process

Dashboard > trevorsullivan5

trevorsullivan5 | Shared access signature

Storage account

Search (Ctrl+/) <<

events

Storage Explorer (preview)

Settings

- Access keys
- Geo-replication
- CORS
- Configuration
- Encryption
- Shared access signature**
- Firewalls and virtual networks

An account-level SAS can delegate access to multiple storage services (i.e. blob, file, queue, table). Note that stored access policies are currently not supported for an account-level SAS.

[Learn more](#)

Allowed services ⓘ

☒ Blob ☐ File ☐ Queue ☐ Table

Allowed resource types ⓘ

☐ Service ☒ Container ☒ Object

Allowed permissions ⓘ

☒ Read ☐ Write ☐ Delete ☐ List ☐ Add ☐ Create ☐ Update ☐ Process

Blob versioning permissions ⓘ

☒ Enables deletion of versions

Allowed permissions ⓘ

☒ Read ☐ Write ☐ Delete ☐ List ☐ Add ☐ Create ☐ Update ☐ Process

Blob versioning permissions ⓘ

☒ Enables deletion of versions

Start and expiry date/time ⓘ

Start

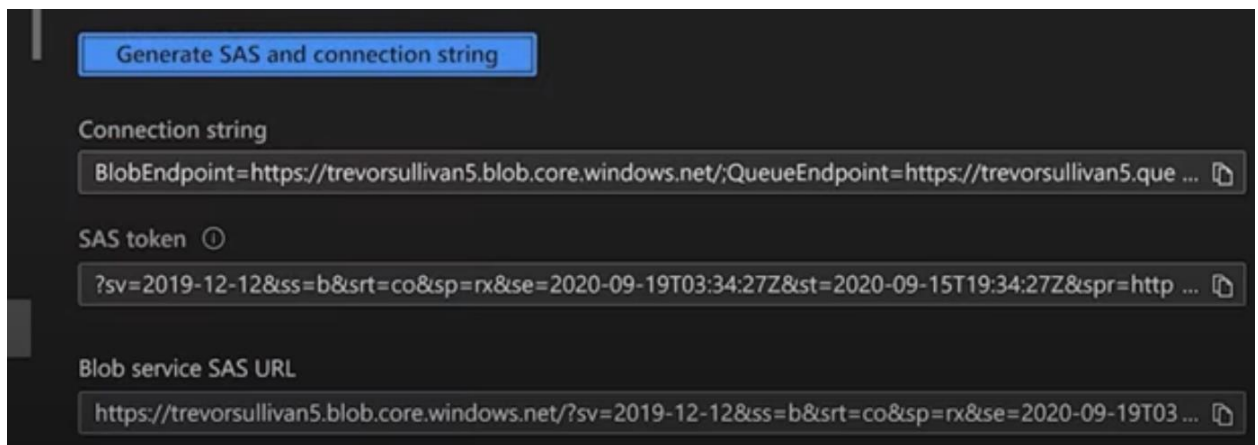
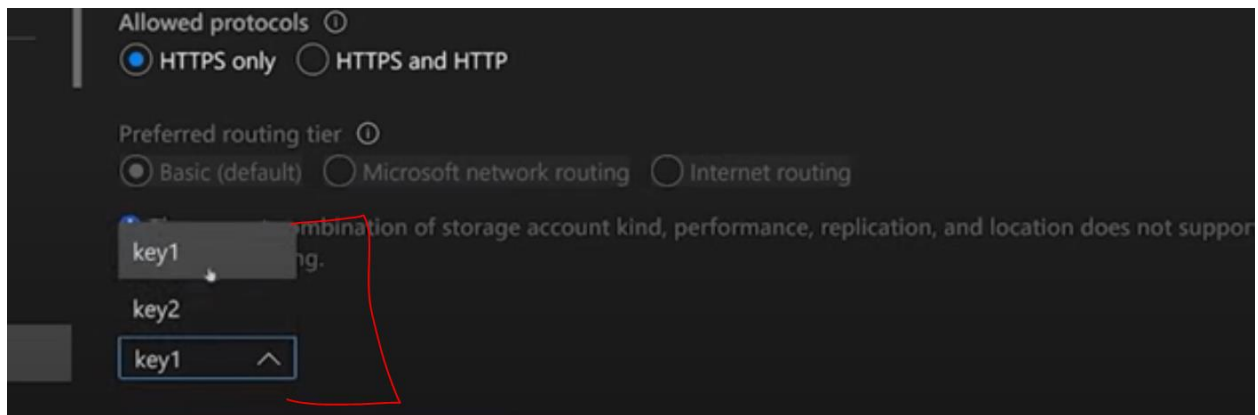
End

(UTC-07:00) Mountain Time (US & Canada)

Allowed IP addresses ⓘ

Allowed protocols ⓘ

☒ HTTPS only ☐ HTTPS and HTTP



<https://www.youtube.com/watch?v=OPX1eW1sCGg>

4. Remote Connectivity Options

Drag each remote connectivity option for a Windows virtual machine on the left to the correct definition on the right.

Correct Answers

Azure Bastion

Just-in-time VM access

Traditional RDP

Matching items here:

HTML5-based web client that uses port 443 externally

Azure Bastion ✓

Dynamically creates a network security group rule to allow remote desktop access with a prompt for justification

Just-in-time VM access ✓

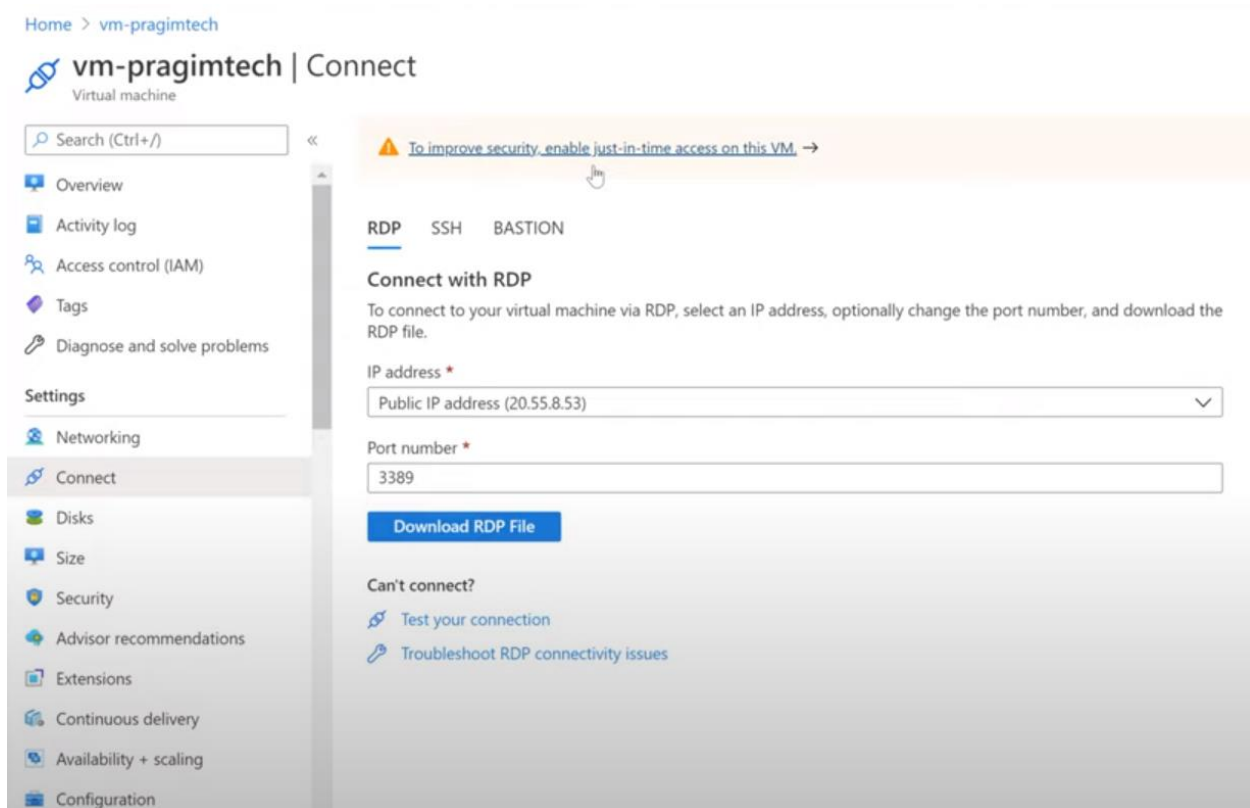
Requires an open port on a network security group to allow remote desktop access

Traditional RDP ✓

Azure Bastion uses an HTML5 connection in a web browser to remotely access the desired VM. JIT VM access, part of Defender for Servers, dynamically creates an NSG rule and has a prompt for why you are connecting to the VM. Traditional RDP requires port 3389 to be open in the NSG.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-strategy-for-secure-server-client-endpoints/7-secure-remote-access>

Azure vm just in time access | azure vm jit | azure jit vm access



vm-pragimtech | Networking

Virtual machine

Search (Ctrl+I)

Attach network interface

Detach network interface

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Networking

Connect

Disks

Size

Security

Advisor recommendations

Extensions

Continuous delivery

Availability + scaling

Configuration

vm-pragimtech447

IP configuration ⓘ

ipconfig1 (Primary)

Network Interface: vm-pragimtech447

Effective security rules

Topology

Virtual network/subnet: rg-test-vnet/default

NIC Public IP: 20.55.8.53

NIC Private IP: 10.0.0.4

Accelerated networking: Disabled

Inbound port rules

Outbound port rules

Application security groups

Load balancing

Network security group vm-pragimtech-nsg (attached to network interface: vm-pragimtech447)

Impacts 0 subnets, 1 network interfaces

Add inbound port rule

Priority	Name	Port	Protocol	Source	Destination	Action
100	Port_3389	3389	Any	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Home > vm-pragimtech

vm-pragimtech | Connect

Virtual machine

Search (Ctrl+I)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Networking

Connect

Disks

Size

Security

Advisor recommendations

Extensions

Continuous delivery

Availability + scaling

Configuration

Identity

This VM has a just-in-time access policy. Select "Request access" before connecting.

RDP

SSH

BASTION

Connect with RDP

You need to request access to connect to your virtual machine. Select an IP address, optionally change the port number, and select "Request access". [Learn more](#)

IP address *

Public IP address (20.55.8.53)

Port number *

3389

Source IP ⓘ

My IP

Other IP/IPv6

All configured IPv6s

Request access

Download RDP file anyway

Can't connect?

Test your connection

Troubleshoot RDP connectivity issues

Request access

vm-pragimtech

×

Please select the ports that you would like to open per virtual machine.

Port	Toggle	Allowed Source IP	IP Range	Time range (hours)
vm-pragimtech				
3389	<div>OnOff</div>	<div>My IP:IP Range</div>	No range	<div><div></div>3</div>

vm-pragimtech447

IP configuration ⓘ

ipconfig1 (Primary) ▾

Network Interface: vm-pragimtech447 [Effective security rules](#) [Topology](#)

Virtual network/subnet: rg-test-vnet/defaultNIC Public IP: 20.55.8.53NIC Private IP: 10.0.0.4Accelerated networking: Disabled

[Inbound port rules](#) [Outbound port rules](#) [Application security groups](#) [Load balancing](#)

Network security group vm-pragimtech-nsg (attached to network interface: vm-pragimtech447)
Impacts 0 subnets, 1 network interfaces

Add inbound port rule

Priority	Name	Port	Protocol	Source	Destination	Action	
100	SecurityCenter-JITRule-1590718750-2DF78...	3389	Any	82.129.70.111	10.0.0.4	Allow	...
1000	SecurityCenter-JITRule_1590718750_9E0...	3389	Any	Any	10.0.0.4	Deny	...
1001	Port_3389	3389	Any	Any	Any	Allow	...
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	...
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow	...
65500	DenyAllInBound	Any	Any	Any	Any	Deny	...

vm-pragimtech | Configuration

Virtual machine

[Save](#) [Discard](#)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Networking
- Connect
- Disks
- Size
- Security
- Advisor recommendations
- Extensions
- Continuous delivery
- Availability + scaling
- Configuration**

Just-in-time VM access

To improve security, enable a just-in-time access.

[Enable just-in-time](#)

i Just-in-time VM access secures your VM's management ports and grants access on-demand, for a limited time period, to pre-approved IP addresses. [Learn more about just-in-time access](#)

Licensing

☒ I confirm I have an eligible Windows 10 license with multi-tenant hosting rights. *

[Review multi-tenant hosting rights for Windows 10 compliance](#)

Proximity placement group

Proximity placement group ⓘ

No proximity placement groups found

i Proximity placement group can only be updated when the virtual machine is deallocated.

Host

vm-pragimtech | Networking

Virtual machine

[Attach network interface](#) [Detach network interface](#)

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Networking**
- Connect
- Disks
- Size
- Security
- Advisor recommendations
- Extensions
- Continuous delivery
- Availability + scaling
- Configuration

vm-pragimtech447

IP configuration ⓘ
ipconfig1 (Primary)

Network Interface: vm-pragimtech447 [Effective security rules](#) [Topology](#)
Virtual network/subnet: rg-test-vnet/default NIC Public IP: 20.55.8.53 NIC Private IP: 10.0.0.4 Accelerated networking: Disabled

[Inbound port rules](#) [Outbound port rules](#) [Application security groups](#) [Load balancing](#)

Network security group vm-pragimtech-nsg (attached to network interface: vm-pragimtech447)
Impacts 0 subnets, 1 network interfaces

[Add inbound port rule](#)

Priority	Name	Port	Protocol	Source	Destination	Action
1000	SecurityCenter-JITRule_1590718750_0BF	3389	Any	Any	10.0.0.4	Deny
1001	Port_3389	3389	Any	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

<https://www.youtube.com/watch?v=l-geFrA73mw&t=335s>

5. Access to Azure SQL Database using private endpoints on a virtual network

You are designing connectivity for a developer who works from various remote locations. The developer needs their device to have access to Azure SQL Database using private endpoints on a virtual network. What should you do?

- ☐ Deploy an Azure Bastion host in the same virtual network as the private endpoint.
- ☐ Deploy a network security group and associate it with the network interface of the private endpoint.
- ☒ Deploy a virtual network gateway and configure a point-to-site VPN.
- ☐ Deploy a virtual network gateway and configure a site-to-site VPN.

If the developer will be in different remote locations, a P2S VPN would allow the developer to connect securely regardless of their location. Because Azure SQL Database is using a private endpoint, it would not be accessible to the public and must be on the network.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-strategy-for-secure-server-client-endpoints/7-secure-remote-access>

Azure Point-to-Site VPN with Azure AD Authentication and MFA

<https://www.youtube.com/watch?v=Ur0WNjnXJrU>

Point to Site Authentication Methods

Certificate

- Self-signed or from an enterprise certificate authority.

RADIUS

- Integration with Windows Active Directory.

Azure AD authentication

- Supports MFA

Step 1: Deploy the Gateway

The image consists of two screenshots from the Azure portal. The top screenshot shows the 'New' page with a search bar containing 'vnet gateway'. Below the search bar, a list of categories is visible: 'Get started', 'Recently created', 'AI + Machine Learning', 'Analytics', 'Blockchain', and 'Compute'. To the right, there are three featured services: 'Windows Server 2016 Datacenter', 'Ubuntu Server 18.04 LTS', and 'Web App'. The bottom screenshot shows the 'Create virtual network gateway' page. The 'Resource group' is 'WestNetworkRG'. Under 'Instance details', the 'Name' is 'WestGW1', 'Region' is '(US) West US', 'Gateway type' is 'VPN', 'VPN type' is 'Route-based', 'SKU' is 'VpnGw1', and 'Generation' is 'Generation1'. The 'Virtual network' is 'WestVNet'. The 'Gateway subnet address range' is '10.1.3.0/24'. Under 'Public IP address', the 'Create new' radio button is selected. A mouse cursor is pointing at the 'Create new' radio button.

New

Create a resource

Home

Dashboard

All services

FAVORITES

Windows Virtual Desktop

Application Insights

App Services

Automation Accounts

Log Analytics workspaces

Recovery Services vaults

Get started

Recently created

AI + Machine Learning

Analytics

Blockchain

Compute

Windows Server 2016 Datacenter
Quickstarts + tutorials

Ubuntu Server 18.04 LTS
Learn more

Web App
Quickstarts + tutorials

Create virtual network gateway

Resource group ⓘ WestNetworkRG (derived from virtual network's resource group)

Instance details

Name * WestGW1 ✓

Region * (US) West US ✓

Gateway type * ⓘ ☒ VPN ☐ ExpressRoute

VPN type * ⓘ ☒ Route-based ☐ Policy-based

SKU * ⓘ VpnGw1 ✓

Generation ⓘ Generation1 ✓

Virtual network * ⓘ WestVNet ✓
[Create virtual network](#)


Only virtual networks in the currently selected subscription and region are listed.


Gateway subnet address range * ⓘ 10.1.3.0/24 ✓
10.1.3.0 - 10.1.3.255 (256 addresses)


Public IP address



Public IP address * ⓘ ☒ Create new ☐ Use existing

Public IP address name *


Generation  Generation1

Virtual network *  WestVNet
[Create virtual network](#)

 Only virtual networks in the currently selected subscription and region are listed.

Gateway subnet address range *  10.1.254.0/27 
 10.1.254.0 - 10.1.254.31 (32 addresses)

Public IP address

Public IP address *  ☒ Create new ☐ Use existing

Public IP address name * WestGW1

Public IP address SKU Basic

Assignment ☒ Dynamic ☐ Static

Step 2: Give admin consent

Dashboard > ciralto (Default Directory) > **Enterprise applications** All applications
 ciralto (Default Directory) - Azure Active Directory

Overview

- Overview
- Diagnose and solve problems

Manage

- All applications
- Application proxy
- User settings
- Collections

Security

- Conditional Access
- Consent and permissions

Activity

- Sign-ins
- Usage & Insights (Preview)

+ New application | Columns | Got feedback?

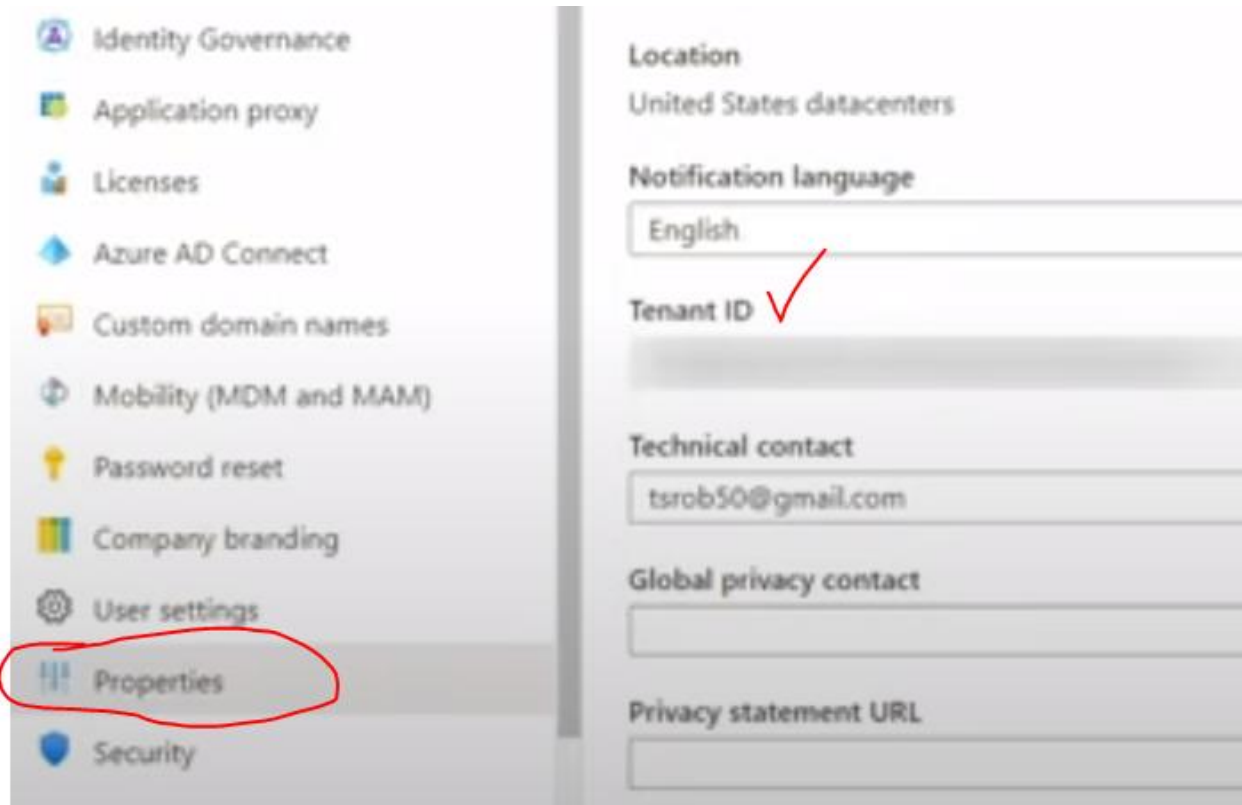
Try out the new Enterprise Apps search preview! Click to enable the preview. →

Application Type: Enterprise Applications | Applications status: Any | Application visibility: Any

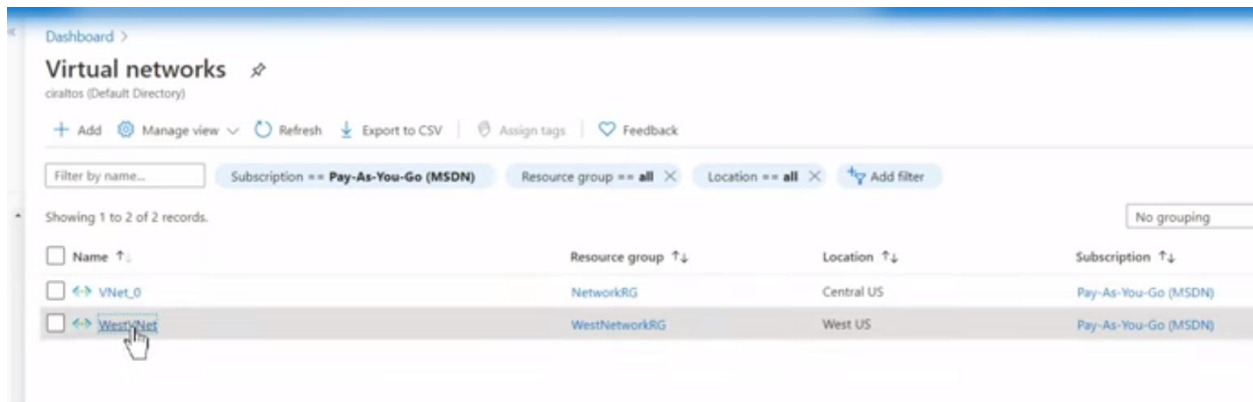
First 50 shown, to search all of your applications, enter a display name or the application ID.

Name	Homepage URL	Object ID
Access To Log Analytics	http://localhost:3000/login	
Azure DevOps	http://azure.com/devops	
Azure VPN	https://www.microsoft.com	
CirTestKeyVault	http://www.fakeurl.com	
CloudynAzureCollector	https://azureeaaccount1cloudyn.onmicrosoft...	
CollabDBService		
Common Data Service	http://www.microsoft.com/dynamics/crm	
Cynga Auditor		

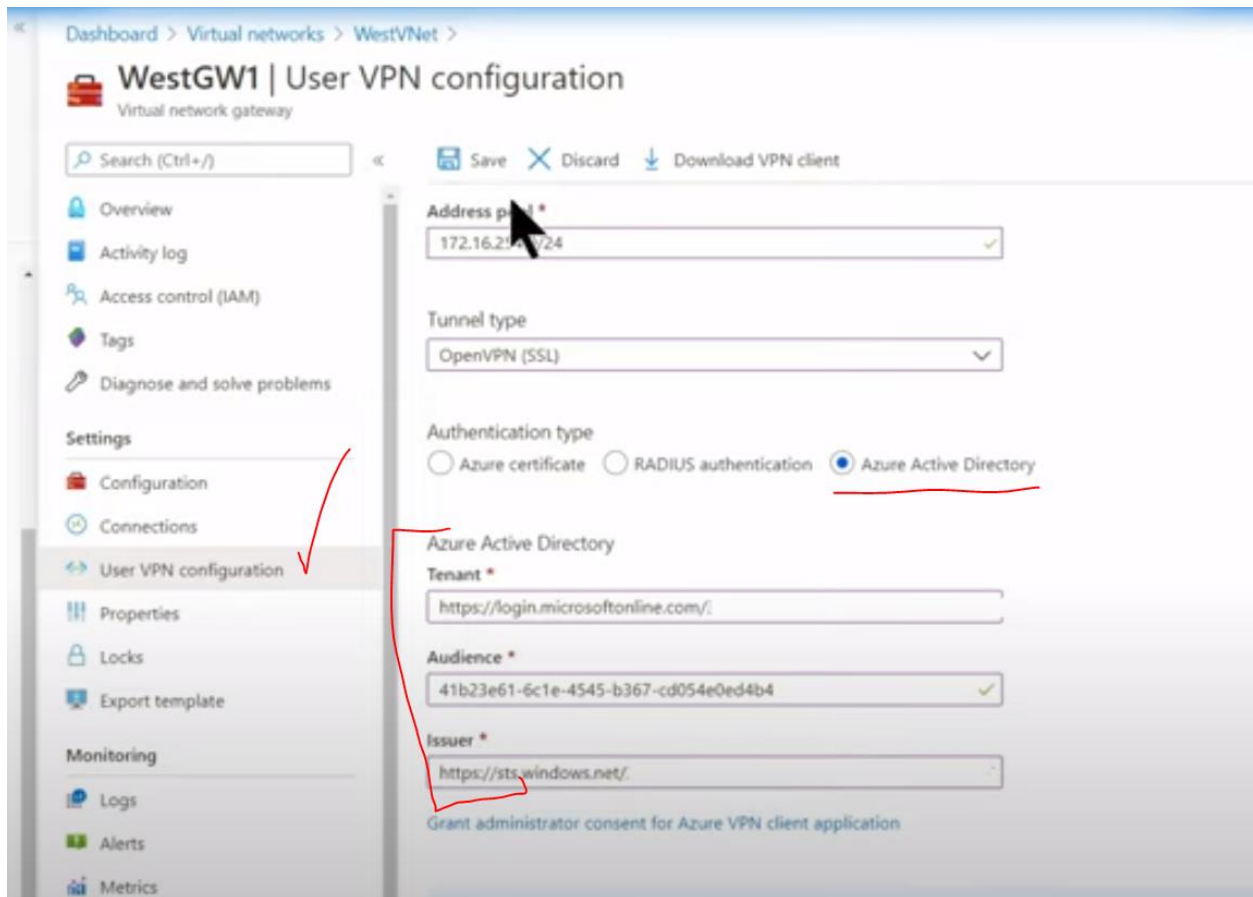
Need the tenant ID



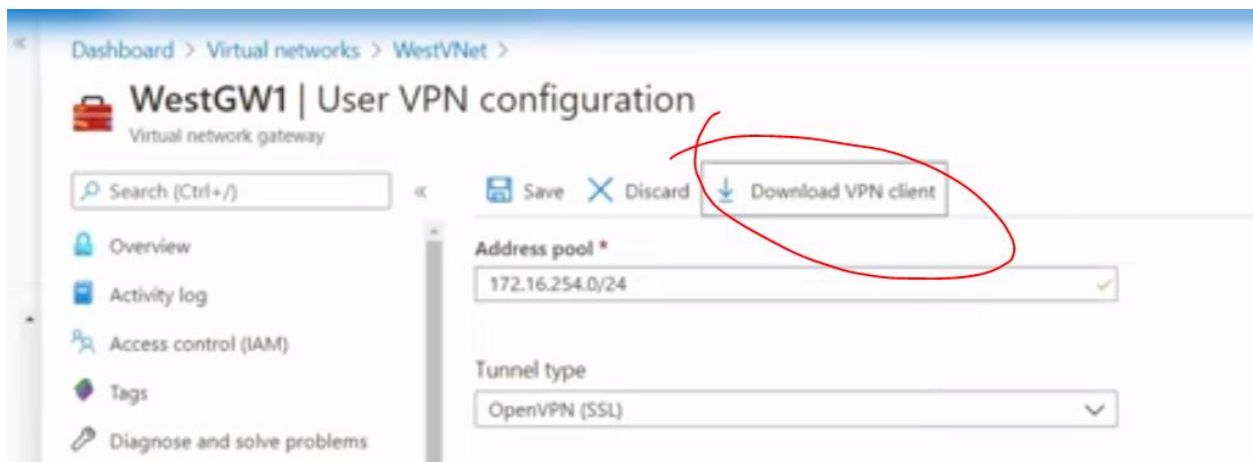
Step 3: Create the P2S Connection

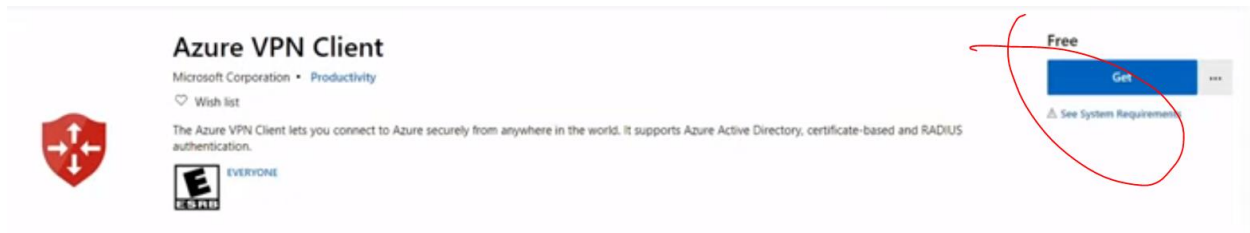


The above is the Vnet where we created the Gateway.

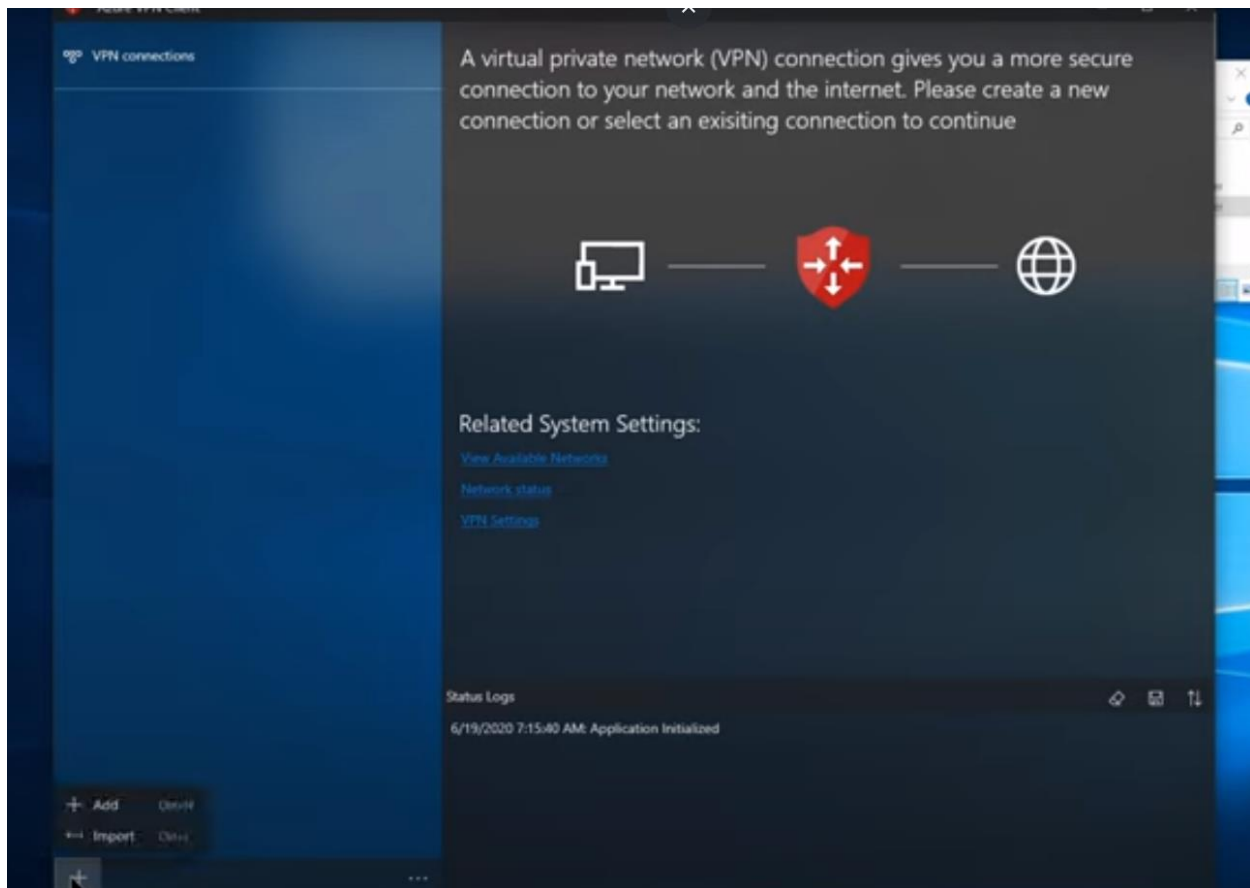


Configure the Client now





You can get it from the MS Store.



Connection Name

WestVNet

VPN Server

azuregateway-b1090031-f185-43f0-ae30-edd

Server Validation

Certificate Information

DigiCert Global Root CA

Server Secret

.....

Client Authentication

Authentication Type

Azure Active Directory

Tenant

https://login.microsoft

Audience

41b23e61-6c1e-4545-b

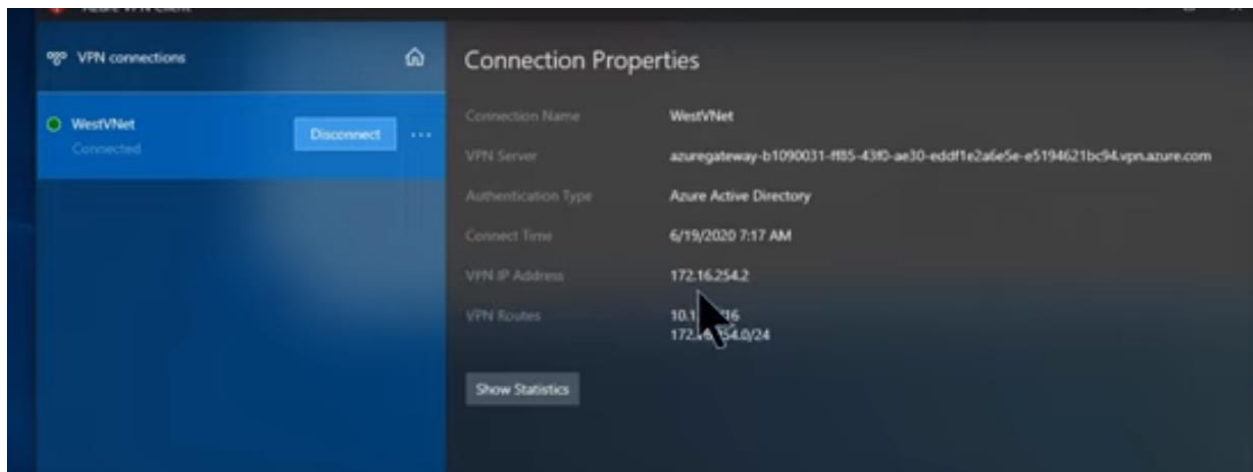
Issuer

https://sts.windows.net,

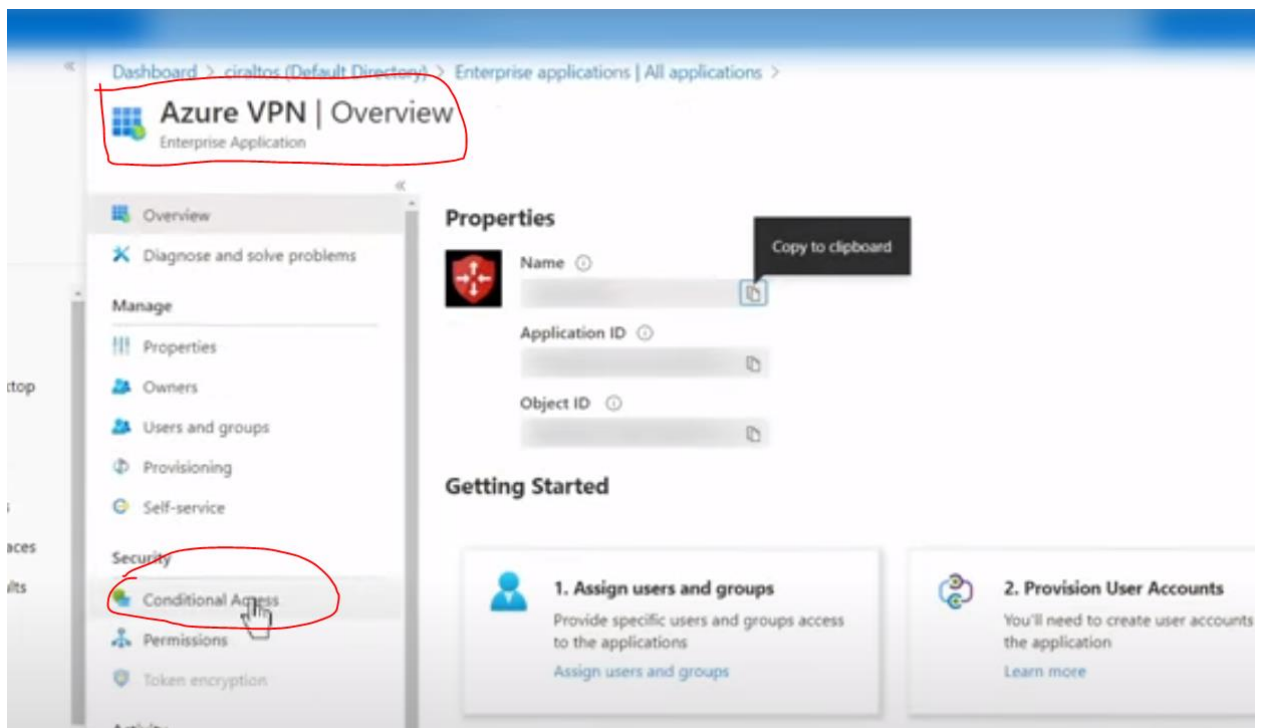
Clear Saved Account

Save

Cancel



Enable MFA



Dashboard > cirtos (Default Directory) > Enterprise applications | All applications > Azure VPN | Conditional Access >

New

Conditional access policy

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

VPNMFA ✓

Assignments

Users and groups ☒ >

All users ✓

Cloud apps or actions ☒ >

1 app included ✓

Conditions ⓘ >

0 conditions selected

Access controls

Grant ⓘ

1 control selected MFA >

Session ⓘ >

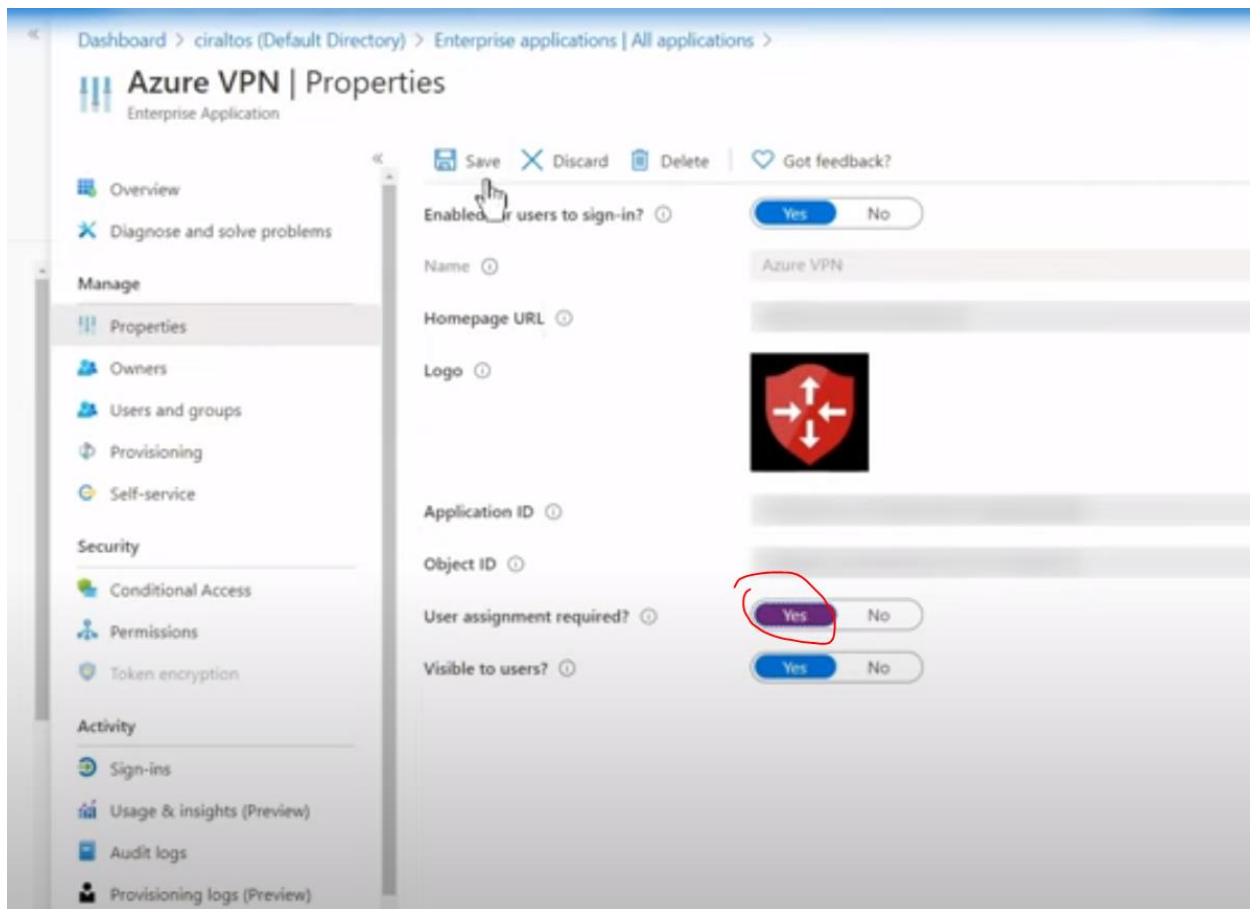
0 controls selected

Enable policy

Report-only ☒ On ☐ Off

Create

Restrict VPN to a Group



<https://www.youtube.com/watch?v=Ur0WNjnXJrU>

6. For Linux VMs, you can deploy the Defender for Endpoint agent

You are configuring a security baseline for Linux virtual machines in Azure. You need to identify a solution to protect the VM from viruses and malware. What should you do?

- ☐ Configure Azure Disk Encryption on the operating system disk.
- ☐ Configure a network security group on the VM network interface.
- ☐ Deploy a firewall to the same virtual network as the VM.
- ☒ Deploy the Microsoft Defender for Endpoint agent.

For Linux VMs, you can deploy the Defender for Endpoint agent to protect the machine from viruses and malware.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-strategy-for-secure-paas-iaas-saas-services/3-specify-security-baselines-for-iaas-services>

7. Azure Policy

You are configuring a security baseline for Azure Kubernetes Services (AKS) in Azure. You need to extend the Gatekeeper admission controller enforcements in AKS. What should you configure?

- ☒ Azure Policy
- ☐ Azure Container Registry
- ☐ DaemonSet
- ☐ Vulnerability assessments

Azure Policy extends the Gatekeeper service in AKS to apply at-scale enforcements and safeguards for an AKS cluster.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-strategy-for-secure-paas-iaas-saas-services/10-specify-security-requirements-for-container-orchestration>

Next- Video#: Azure Update Manager with Azure Policies

<https://www.youtube.com/watch?v=Da1EsoAzUoY>

8. System-assigned managed identity

You deploy Azure Key Vault in your subscription and import a trusted certificate. You need to ensure that an application running in a virtual machine can retrieve the certificate from Key Vault. The access must not allow users to retrieve the certificate. What two actions should you perform?

- ☐ Create a new application registration.
- ☐ Create a new enterprise application.
- ☒ Create a new Key Vault access policy.
- ☒ Create a system-assigned managed identity.

A system-assigned managed identity should be created on the VM, and a new access policy should be created using that same identity with the appropriate permissions.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-strategy-for-secure-server-client-endpoints/6-design-strategy-manage-secrets-keys-certificates>

9. App protection policy

Your organization has a bring-your-own-device policy for employees. Employees need to access Outlook using their mobile devices without enrolling the devices. What should you do?

☒ Create a new app protection policy.

☐ Create a new configuration policy.

☐ Create a new compliance policy.

☐ Create a device enrollment policy.

An app protection policy can protect registered applications by requiring security features on the applications even if a device is not enrolled.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-strategy-for-secure-server-client-endpoints/4-specify-security-requirements-for-mobile-devices-clients>

10. Enroll the device

☐ Create a new app protection policy.

☐ Create a new configuration policy.

☐ Create a new compliance policy.

☒ Enroll the device.

The device of a new employee will not be enrolled. For the existing configuration and compliance policies to apply, the device must be enrolled.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-strategy-for-secure-server-client-endpoints/4-specify-security-requirements-for-mobile-devices-clients>

11. Defender for Cloud

You are designing security for PaaS services in Azure. Which service provides guidance and recommendations for these services based on the Center for Internet Security (CIS)?

☐ Azure App Services

☒ Defender for Cloud

☐ Defender for Office 365

☐ Microsoft Sentinel

Defender for Cloud provides guidance and recommendations from the Center for Internet Security (CIS) for various PaaS services in Azure.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-strategy-for-secure-paas-iaas-saas-services/2-specify-security-baselines-for-paas-services>

12. Azure disk encryption

You are configuring a security baseline for Linux virtual machines in Azure. You need to ensure that VMs are encrypted using dm-crypt. What should you configure?

☒ Azure Disk Encryption

☐ Azure Key Vault

☐ Azure Storage Account

☐ Defender for Cloud

Azure Disk Encryption uses dm-crypt to encrypt the operating system and data disks on a Linux VM.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-strategy-for-secure-paas-iaas-saas-services/3-specify-security-baselines-for-iaas-services>

13. Security baseline

You need to create and apply a group of configuration settings for mobile devices. What should you create?

- ☐ App protection policy
- ☐ Compliance policy
- ☐ Conditional access policy
- ☒ Security baseline

A security baseline defines the security configuration for client devices, including mobile devices.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-strategy-for-secure-server-client-endpoints/2-specify-security-baselines-for-server-client-endpoints>

14. Defender for Identity

Defender for can monitor your domain controllers and analyze the data for attacks and threats.

Defender for Identity has a sensor that can be installed on AD DS domain controllers that can capture and parse network traffic and Windows events for attacks and threats.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-strategy-for-secure-server-client-endpoints/5-specify-requirements-active-directory-domain-services>

15. Security baseline

You are configuring a security baseline for Windows virtual machines in Azure. You need to ensure that VMs are encrypted using BitLocker. What should you configure?

- ☒ Azure Disk Encryption
- ☐ Azure Key Vault
- ☐ Azure Storage Account
- ☐ Defender for Cloud

Azure Disk Encryption uses BitLocker to encrypt the operating system and data disks on a Windows VM.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-strategy-for-secure-paas-iaas-saas-services/3-specify-security-baselines-for-iaas-services>

16. Defender for Cloud and vulnerability assessments

Defender for Cloud can provide recommendations and alerts, and it can perform **vulnerability assessments** for PaaS services such as Azure SQL Database and Azure Container Registry.

Defender for Cloud can provide recommendations and alerts, and it can perform vulnerability assessments for PaaS services such as Azure SQL Database and Azure Container Registry.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-strategy-for-secure-paas-iaas-saas-services/2-specify-security-baselines-for-paas-services>

17. Security baseline

You are configuring a security baseline for Windows virtual machines in Azure. You need to identify a solution to protect the VM from viruses and malware. What should you do?

- ☐ Configure Azure Disk Encryption on the operating system disk.
- ☐ Configure a network security group on the VM network interface.
- ☐ Deploy a firewall to the same virtual network as the VM.
- ☒ Deploy the Microsoft Antimalware for Azure VM extension.

For Windows VMs, you can deploy the Microsoft Antimalware for Azure extension to the VM to protect the machine from viruses and malware.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-strategy-for-secure-paas-iaas-saas-services/3-specify-security-baselines-for-iaas-services>

Objective 4: Design a strategy for data and applications

1. Azure AD B2B

You are designing identity security for an application. You need to allow access to other organizations using their identity systems. What should you use?

☒ Azure AD B2B

☐ Azure AD B2C

☐ Managed identities

☐ Third-party services

You answered this question correctly.

Explanation:

Azure AD B2B allows you to connect with other organizations and use their identity systems to configure authentication for your application.
Reference: <https://learn.microsoft.com/en-us/training/modules/specify-security-requirements-for-applications/5-standard-for-onboarding-new-application>

Azure AD B2B, also known as Azure AD Business-to-Business collaboration, is a feature within Microsoft Entra External ID that allows organizations to securely share resources and collaborate with external users. This means you can invite partners, vendors, or customers to access your applications and services without needing to create accounts within your own Azure Active Directory (Azure AD) tenant.

Here are some key benefits of using Azure AD B2B:

Simplified collaboration: External users can access your resources using their existing credentials, eliminating the need for them to create new accounts or manage multiple passwords.

Increased security: Azure AD B2B provides granular access controls, allowing you to grant specific permissions to external users based on their needs. Additionally, you can leverage multi-factor authentication (MFA) to further enhance security.

Reduced costs: By avoiding the need to create and manage additional user accounts, Azure AD B2B can help you save time and money.

Improved user experience: External users can access your resources from any device, anywhere in the world. They also have a single sign-on (SSO) experience, meaning they can access all their authorized resources without having to re-enter their credentials.

Here are some of the ways Azure AD B2B can be used:

- Share files and folders with external collaborators.
- Grant access to internal applications and services.

- Enable external users to participate in Teams meetings.
- Invite partners to collaborate on projects.
- Provide customer support through Azure AD B2B guest accounts.

If you are looking for a secure and efficient way to collaborate with external users, Azure AD B2B is a great option.

Here are some additional resources you may find helpful:


- Microsoft Entra B2B collaboration overview: <https://learn.microsoft.com/en-us/entra/external-id/what-is-b2b>
- What Is Microsoft Azure AD B2B?: <https://learn.microsoft.com/en-us/entra/external-id/add-users-administrator>
- Azure AD, B2B, B2C Puzzled Out - What is Azure Active Directory?: <https://learn.microsoft.com/en-us/entra/external-id/hybrid-cloud-to-on-premises>

External collaboration settings

The screenshot displays the 'External collaboration settings' page in the Microsoft Azure portal. The page is titled 'External Identities | External collaboration settings' and is for the tenant 'SeoRod Consulting INC. - Microsoft Entra ID'. The left sidebar contains a navigation menu with options like Overview, Cross-tenant access settings, All identity providers, External collaboration settings (selected), Diagnose and solve problems, Self-service sign up, Custom user attributes, All API connectors, Custom authentication extensions (Preview), User flows, Subscriptions, Linked subscriptions, Lifecycle management, Terms of use, Access reviews, and Troubleshooting + Support. The main content area shows a notification about moving the email one-time passcode for guests to All Identity Providers. Below this, there are three main sections: 'Guest invite settings' with radio button options for guest user access (selected: 'Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)'), 'Guest invite restrictions' with radio button options for who can invite guest users (selected: 'Only users assigned to specific admin roles can invite guest users'), and 'Enable guest self-service sign up via user flows' with a toggle set to 'No'. The 'External user leave settings' section has a toggle set to 'Yes'. The 'Collaboration restrictions' section has a warning icon and text about cross-tenant access settings, with radio button options for invitation restrictions (selected: 'Allow invitations to be sent to any domain (most inclusive)').


External Identities | Cross-tenant access settings

Organizational settings **Default settings** Microsoft cloud settings

 [Modifying default settings impact all collaboration with other Microsoft Entra tenants. Click here to learn how to identify your existing inbound and outbound collaborations.](#)


Default settings apply to all external Microsoft Entra tenants not listed on the organizational settings tab. These default settings can be modified but not deleted.
[Learn more](#)

Inbound access settings

 Edit inbound defaults

Type	Applies to	Status
B2B collaboration	External users and groups	All allowed
B2B collaboration	Applications	All allowed
B2B direct connect	External users and groups	All blocked
B2B direct connect	Applications	All blocked
Trust settings	N/A	Disabled


Outbound access settings

 Edit outbound defaults

Type	Applies to	Status
B2B collaboration	Users and groups	All allowed
B2B collaboration	External applications	All allowed

External Identities | All identity providers

Home > SeoRod Consulting INC. | External Identities > External Identities

 **External Identities | All identity providers** ...

SeoRod Consulting INC. - Microsoft Entra ID

Overview

Cross-tenant access settings

All identity providers

External collaboration settings

Diagnose and solve problems

Self-service sign up

Custom user attributes

All API connectors

Custom authentication extensions (Preview)

User flows

Subscriptions

Linked subscriptions

Lifecycle management

Terms of use

Access reviews

Troubleshooting + Support

New support request

Configured identity providers

Name

Microsoft Entra ID

Microsoft Account

Email one-time passcode

SAML/WS-Fed identity providers

Display name

Configuration

You have not added a SAML/WS-Fed identity provider

57

What is Azure B2C?

Azure Active Directory B2C (Azure AD B2C) is a customer identity access management (CIAM) solution offered by Microsoft. It helps organizations manage the sign-up, sign-in, and access for external users, typically customers, partners, or consumers, to their web and mobile applications.

Here are some key features of Azure AD B2C:

- White-labeled authentication: Customize the user experience with your own branding and colors.
- Multiple sign-in options: Support social login with Facebook, Google, Twitter, etc.
- Multi-factor authentication (MFA): Enhance security by requiring a second factor of authentication.
- Self-service password reset: Allow users to reset their passwords without needing assistance from IT.
- Conditional access policies: Grant access to specific users based on pre-defined conditions.
- Scalability: Support millions of users and billions of authentications per day.

Here are some of the benefits of using Azure AD B2C:

- Improved user experience: A more personalized and convenient experience for your customers.
- Increased security: Enhanced security with features like MFA and conditional access.
- Reduced costs: Reduced IT overhead by eliminating the need to manage user accounts manually.
- Faster time to market: Quickly launch new applications and services without needing to build your own authentication infrastructure.

Here are some of the use cases for Azure AD B2C:

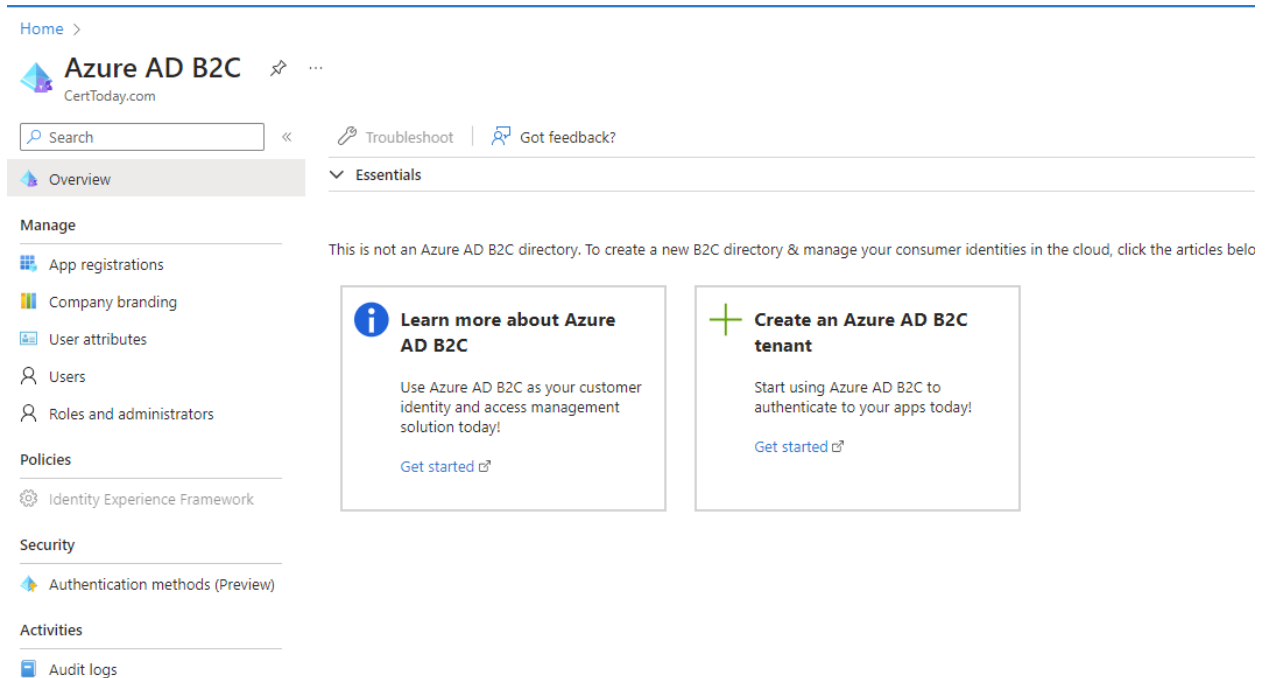
- E-commerce websites: Allow customers to sign up, sign in, and manage their accounts.
- Online gaming platforms: Enable players to create accounts, manage profiles, and make purchases.
- Mobile apps: Securely authenticate users and provide access to content and features.
- Customer portals: Provide a self-service portal for customers to access account information and request support.

Here are some additional resources you may find helpful:

- Azure Active Directory B2C documentation: <https://learn.microsoft.com/en-us/azure/active-directory-b2c/>

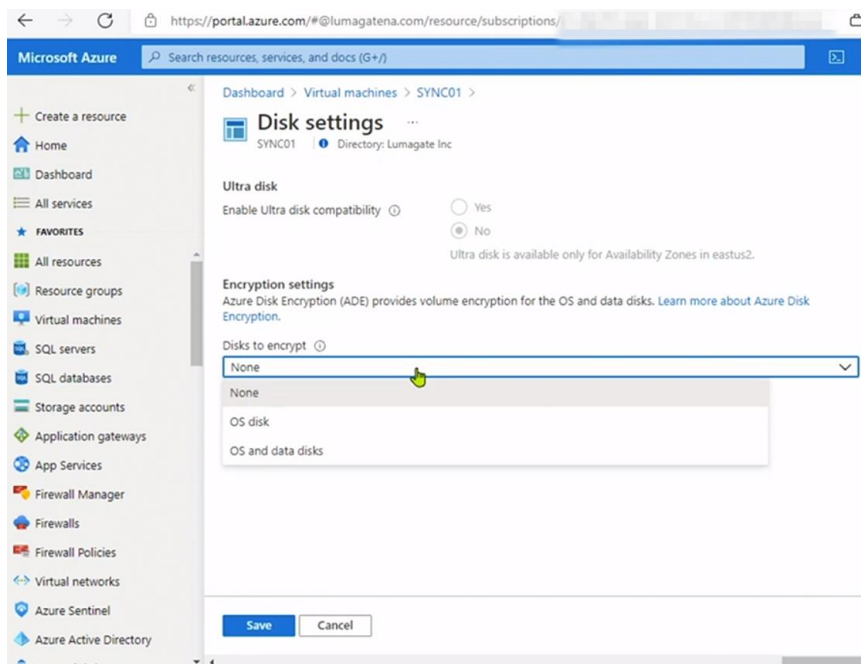
- What is Azure Active Directory B2C?: <https://learn.microsoft.com/en-us/entra/architecture/resilience-b2c>
- Azure AD B2C Pricing: <https://azure.microsoft.com/en-us/pricing/details/active-directory-external-identities/>

I hope this information gives you a good overview of Azure AD B2C. Please let me know if you have any other questions.



2. VMs can use Azure Disk Encryption with customer-managed keys for encrypting data at rest

Figure: VM Disk Encryption



3. Microsoft Threat Modeling Tool

You are designing identity security for an application. You need to analyze and mitigate security issues for the application. What should you use?

- ☐ Defender for Cloud
- ☐ Microsoft Sentinel
- ☒ Microsoft Threat Modeling Tool
- ☐ OWASP Ruleset

Microsoft Threat Modeling Tool helps you design an application, analyze threats, and mitigate any identified security issues.

Reference: <https://learn.microsoft.com/en-us/training/modules/specify-security-requirements-for-applications/4-understand-application-threat-modeling>

2- Evaluate the application design progressively

Analyze application components and connections and their relationships. Threat modeling is a crucial engineering exercise that includes defining security requirements, identifying and mitigating threats, and validating those mitigations. This technique can

be used at any stage of application development or production, but it's most effective during the design stages of a new functionality.

Popular methodologies include:

- [STRIDE](#):
 - Spoofing
 - Tampering
 - Repudiation
 - Information Disclosure
 - Denial of Service
 - Elevation of Privilege

Microsoft Security Development Lifecycle uses STRIDE and provides a tool to assist with this process. For more information, see [Microsoft Threat Modeling Tool](#).

- [Open Web Application Security Project \(OWASP\)](#) has documented a threat modeling approach for applications.

Integrate threat modeling through automation using secure operations. Here are some resources:

- Toolkit for [Secure DevOps on Azure](#).
- [Guidance on DevOps pipeline security](#) by OWASP.

4. OWASP

The [OWASP](#) has documented a threat modeling approach for web applications.

Possible answers : [OWASP](#), [Open Web App Security Project](#), [Open Web Application Security Project](#)

The Open Web Application Security Project (OWASP) has documented a threat modeling approach for web applications.

Reference: <https://learn.microsoft.com/en-us/training/modules/specify-security-requirements-for-applications/4-understand-application-threat-modeling>

5. Service and Type of Encryption

Drag the Azure service type on the left to the correct data security action on the right.

Correct Answers

App Service

Database

Storage account

Matching items here:

Request encryption for client connection requests.

App Service ✓

Require transparent data encryption to be enabled.

Database ✓

Use Azure Storage Service Encryption for data at rest.

Storage account ✓

6. A sensitive information type with exact data match can use existing data to train the DLP policies.

You need to identify information that might be stored in documents that contain employee IDs. The solution must include using existing data to inform the data loss prevention policies. What should you create?

☐ Encryption keys

☐ Role-based access control

☒ Sensitive information types

☒ Exact data match

Reference: <https://learn.microsoft.com/en-us/training/modules/design-strategy-for-securing-data/3-to-identify-protect-sensitive-data>

7. Azure Application Gateway

Azure Application Gateway is a region-based service that can be deployed in front of web applications to provide load balancing and web application firewall (WAF) capabilities.

Possible answers : Azure Application Gateway, Application Gateway, App Gateway, AppGW

Azure Application Gateway provides load balancing and WAF services at a regional level.

Reference: <https://learn.microsoft.com/en-us/training/modules/specify-security-requirements-for-applications/5-standard-for-onboarding-new-application>

8. Phases of the DevOps life cycle

Place the phases of the DevOps life cycle in the correct sequence.

Correct Answers

Plan

Develop

Deliver

Operate

Matching items here:

#1

Plan ✓

#2

Develop ✓

#3

Deliver ✓

#4

Operate ✓

The four phases of the DevOps life cycle are Plan, Develop, Deliver, and Operate.
Reference: <https://learn.microsoft.com/en-us/training/modules/specify-security-requirements-for-applications/2-specify-security-strategy-apis>

9. DLP Policy components

You are creating data loss prevention policies for your organization. Which two components should you include in a policy?

☐ Encryption keys

☐ Role-based access control

☒ Sensitive information types

☒ Sensitivity labels

A policy can include sensitive information types, sensitivity labels, retention labels, and trainable classifiers.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-strategy-for-securing-data/3-to-identify-protect-sensitive-data>

10. Conditional Access App Control

Your organization uses a third-party cloud application. You need to ensure that authentication sessions are routed through Azure AD. What should you use?

☒ Conditional Access App Control

☐ Defender for Cloud

☐ Information Protection

☐ Microsoft Sentinel

Conditional Access App Control allows you to force authentication through Azure AD Conditional Access before accessing the third-party app.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-strategy-for-securing-data/3-to-identify-protect-sensitive-data>

11. Microsoft Purview Data Map

Your organization uses Azure Data Lake, Azure Files, and Azure SQL Database. You need to identify sensitive data and automatically apply labels to content. What should you use?

☐ Rights Management Connector

☐ Defender for Cloud

☒ Microsoft Purview Data Map

☐ Microsoft Sentinel

You answered this question correctly.

Explanation:

Microsoft Purview Data Map can identify sensitive information and automatically apply labeling to that information.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-strategy-for-securing-data/3-to-identify-protect-sensitive-data>

Microsoft Purview Data Map: Discovering and Governing Your Enterprise Data

Microsoft Purview Data Map is a cloud-native platform that helps organizations discover, classify, and govern data across their entire data estate, both on-premises and in the cloud. It plays a crucial role in data governance by providing a centralized view of your data landscape, enabling you to:

Discover data:

- Automatically scan and identify sensitive data across various data sources, including databases, file systems, and cloud applications.
- Catalog data assets with detailed information such as data lineage, ownership, and access controls.
- Identify and track data movement across your organization.

Classify data:

- Apply sensitivity labels to data based on its business value and regulatory compliance requirements.
- Leverage built-in classification rules or create custom rules to meet your specific needs.
- Automate data classification for improved efficiency and consistency.

Govern data:

- Enforce access controls to ensure that only authorized users can access sensitive data.
- Monitor data usage and activity to detect suspicious behavior or data breaches.
- Implement data lifecycle management policies to ensure that data is retained and disposed of according to legal and regulatory requirements.

Benefits of using Microsoft Purview Data Map:

- Improved data visibility: Gain a comprehensive understanding of your data landscape and identify data assets that may be hidden or forgotten.
- Enhanced data security: Protect sensitive data by applying appropriate access controls and classification labels.
- Simplified data governance: Streamline your data governance processes with automated discovery, classification, and monitoring capabilities.
- Reduced compliance risk: Meet regulatory compliance requirements by ensuring that your data is managed responsibly.
- Cost optimization: Identify and eliminate unused or redundant data to reduce storage costs.

Microsoft Purview Data Map is a valuable tool for any organization that needs to improve its data governance practices. It helps you to discover, classify, and govern your data effectively, leading to better data security, compliance, and cost management.

Here are some additional resources that you may find helpful:

- Microsoft Purview Data Map documentation: <https://learn.microsoft.com/en-us/purview/concept-elastic-data-map>
- Benefits of using Microsoft Purview Data Map: <https://learn.microsoft.com/en-us/training/purview/>

- Microsoft Purview pricing: <https://azure.microsoft.com/en-us/pricing/details/purview/>

I hope this information gives you a good overview of Microsoft Purview Data Map.

Please let me know if you have any other questions.

Microsoft Purview Data Map Demo Videos

Here are some helpful demo videos about Microsoft Purview Data Map:

Official Microsoft Purview Videos:

- Microsoft Purview: Data Governance Made Easy
(<https://m.youtube.com/watch?v=Sb9uJLtXDGo>) This video provides a brief overview of Microsoft Purview and its key features, including Data Map.
- Microsoft Purview Data Map: Discover, Classify, and Govern Your Data
(<https://m.youtube.com/watch?v=27bA4KFiEKk>) This video demonstrates how you can use Purview Data Map to discover, classify, and govern your data across various sources.
- Microsoft Purview Data Map: Quickstart #5 - Data Map and Register Sources
(<https://m.youtube.com/watch?v=2O8oSKeB1Xq>) This video provides a step-by-step guide on how to set up Purview Data Map and register your data sources.

Additional Videos:

- Azure Purview | Map, Discover, and Find Insights Across Data Sources
(<https://m.youtube.com/watch?v=27bA4KFiEKk>) This video by Microsoft MVP Wolfgang Platz provides a comprehensive overview of Azure Purview, including Data Map, data lineage, and data catalog features.
- Learn Live - Microsoft Purview Data Governance
(<https://m.youtube.com/watch?v=Sb9uJLtXDGo>) This video by Microsoft MVP Thomas Maurer goes through a live demonstration of Purview Data Governance features, including Data Map and data lineage.
- How to explore your data estate using the Microsoft Purview data catalog
(<https://m.youtube.com/watch?v=cNCehZcePug>) This video by Microsoft Azure Data & AI MVP Mark Kromer focuses on exploring your data estate using the Purview Data Catalog, which is closely integrated with Data Map.

Other Resources:

- Microsoft Purview Data Map documentation: <https://learn.microsoft.com/en-us/purview/concept-elastic-data-map>

- Microsoft Purview Data Map quickstart: <https://m.youtube.com/watch?v=2O8oSKeB1Xg>
- Microsoft Purview Data Map best practices: <https://learn.microsoft.com/en-us/purview/concept-elastic-data-map>

These resources should provide you with a good understanding of Microsoft Purview Data Map and how it can be used to discover, classify, and govern your data.

12. STRIDE

Drag each STRIDE category on the left to the correct definition on the right.

Correct Answers	Matching items here:
Spoofing	Accessing and using another user's authentication information Spoofing ✓
Tampering	Maliciously modifying data Tampering ✓
Repudiation	Performing an action without a way to trace it Repudiation ✓
Information disclosure	Exposing information to users who do not have proper authorization Information disclosure ✓
Denial of Service	Denying availability to valid users Denial of Service ✓
Elevation of Privilege	Escalating permissions to a higher level than they should be for the user Elevation of Privilege ✓

Reference: <https://learn.microsoft.com/en-us/training/modules/specify-security-requirements-for-applications/4-understand-application-threat-modeling>

13. Mitigate SQL Injection – Azure Application Gateway

You deploy an application to an Azure app service. You need to mitigate the threat of SQL injection on the app. What should you do?

- ☒ Deploy Azure Application Gateway
- ☐ Deploy Azure Firewall
- ☐ Configure a private endpoint on the app service
- ☐ Enable TLS on the app service

Reference: <https://learn.microsoft.com/en-us/training/modules/specify-security-requirements-for-applications/5-standard-for-onboarding-new-application>

Deploying an Azure Application Gateway

There are several ways to deploy an Azure Application Gateway, depending on your familiarity with Azure and your desired level of automation. Here are three common methods:

1. Azure portal:

This is the simplest method and is suitable for beginners. However, it can be time-consuming for complex deployments.

Steps:

1. Open the Azure portal and navigate to Create a resource.
2. Search for "Application Gateway" and select it.
3. Choose the desired pricing tier (Basic, Standard, or WAF) and resource group.
4. Configure the application gateway settings, including:
 - Name
 - Location
 - Virtual network and subnet
 - Public IP address
 - Frontend IP configurations
 - Backend pools and backend address pools
 - Routing rules and listeners
5. Review your settings and click Create.

2. Azure Resource Manager (ARM) templates:

This method is more efficient for deploying complex application gateways and allows for greater control over the configuration. However, it requires familiarity with ARM templates.

Steps:

1. Create an ARM template for your application gateway using a text editor or IDE.
2. Define the desired configuration in the template, including the same settings as the Azure portal method.
3. Use the Azure CLI or PowerShell to deploy the template.

3. Infrastructure as Code (IaC) tools:

IaC tools like Terraform or Bicep offer a declarative way to manage your application gateway infrastructure. This method is ideal for automating deployments and ensuring consistency across environments.

Steps:

1. Define the desired application gateway configuration in your IaC code.
2. Run the IaC code to deploy the application gateway.

Additional resources:

- Deploy an application gateway using the Azure portal: <https://learn.microsoft.com/en-us/training/modules/configure-azure-application-gateway/>
- Deploy an application gateway using ARM templates: <https://learn.microsoft.com/en-us/azure/templates/microsoft.network/applicationgateways>
- Deploy an application gateway using Terraform: https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/resources/application_gateway
- Microsoft Azure Application Gateway documentation: <https://learn.microsoft.com/en-us/azure/application-gateway/>

Tips:

- Start with a simple configuration and gradually add complexity as needed.
- Use Azure Resource Manager templates or IaC tools to automate deployments.
- Test your application gateway thoroughly before deploying it to production.
- Monitor your application gateway performance and usage.

Remember, the specific steps may vary depending on your specific needs and environment.

Aquí te dejo algunas opciones de video demo en Youtube acerca de Azure Application Gateway:

Español:

- Microsoft Azure Application Gateway - Tutorial en Español (<https://m.youtube.com/watch?v=DjNPHetdIQo>)
- Configuración paso a paso de Azure Application Gateway (<https://m.youtube.com/watch?v=8DcTdlKTM64>)
- Aplicación Gateway en Azure | Configuración Básica (<https://m.youtube.com/watch?v=S0SumOE0AaY>)

Inglés:

- Microsoft Azure Application Gateway: Load-Balancing Solution (<https://m.youtube.com/watch?v=8DcTdIKTM64>)
- Azure Application Gateway Demo Setup - Code Samples (<https://m.youtube.com/watch?v=DjNPHetdIQo>)
- Microsoft Azure Application Gateway: Discover, Classify, and Govern Your Data (<https://m.youtube.com/watch?v=DjNPHetdIQo>)

Además de los videos, también te dejo algunos recursos adicionales que te pueden ser útiles:

- Microsoft Azure Application Gateway documentation: <https://learn.microsoft.com/en-us/training/modules/configure-azure-application-gateway/>
- Deploy an application gateway using the Azure portal: <https://learn.microsoft.com/en-us/training/modules/configure-azure-application-gateway/>
- Deploy an application gateway using ARM templates: <https://learn.microsoft.com/en-us/azure/templates/microsoft.network/applicationgateways>
- Microsoft Azure Application Gateway best practices: <https://learn.microsoft.com/en-us/training/modules/configure-azure-application-gateway/>

Espero que esta información te sea de utilidad.

14. Microsoft Information Protection SDK

Your organization uses third-party apps and services that store sensitive data. You need to identify and apply sensitivity labels to the data stored in these services. What should you use?

- ☐ Defender for Cloud
- ☐ Microsoft Defender for Cloud Apps
- ☒ Microsoft Information Protection SDK
- ☐ Microsoft Sentinel

Microsoft Information Protection SDK allows you to extend sensitivity labels to third-party apps and services.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-strategy-for-securing-data/3-to-identify-protect-sensitive-data>

15. Principle of least privilege

Which security methodology limits the damage that a single account can do?

- ☐ Defense in depth
- ☐ Escalation of privilege
- ☒ Principle of least privilege
- ☐ Repudiation

The principle of least privilege limits the damage that a single account can do in an environment.

Reference: <https://learn.microsoft.com/en-us/training/modules/specify-security-requirements-for-applications/4-understand-application-threat-modeling>

16. Security strategy for Azure SQL Database

You are designing a data security strategy for Azure SQL Database. Which two actions should you include?

- ☐ Ensure that Azure Disk Encryption uses keys from Azure Key Vault.
- ☒ Ensure that dynamic data masking is configured for users.
- ☐ Ensure that Service Fabric secrets are stored in a managed hardware security module (HSM).
- ☒ Ensure that transparent data encryption (TDE) is enabled.

TDE and dynamic data masking should both be configured for Azure SQL Database in a security baseline.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-strategy-for-securing-data/2-prioritize-mitigating-threats-to-data>

17. Data Classification Capability

Drag the data classification capability on the left to the correct definition on the right.

Correct Answers

Sensitive information type

Trainable classifiers

Data classification

Policies

Matching items here:

Uses a built-in or customized regular expression with keywords, confidence levels, and proximity.

Sensitive information type ✓

Uses pattern matching to identify possible sensitive data.

Trainable classifiers ✓

Items that have been identified with an appropriate sensitivity label.

Data classification ✓

The defined behavior after data has been classified with a sensitivity label.

Policies ✓

18. Azure Front Door

is a global service that can be deployed in front of web applications to provide load balancing and web application firewall (WAF) capabilities.

Azure Front Door provides load balancing and WAF services at a global level.

Reference: <https://learn.microsoft.com/en-us/training/modules/specify-security-requirements-for-applications/5-standard-for-onboarding-new-application>

19. Azure AD B2C

You are designing identity security for an application. You need to allow external access for users with their personal Microsoft accounts. What should you use?

☐ Azure AD B2B

☒ Azure AD B2C

☐ Managed identities

☐ Third-party services

Azure AD B2C allows you to connect with external users via their personal accounts, including Microsoft accounts.

Reference: <https://learn.microsoft.com/en-us/training/modules/specify-security-requirements-for-applications/5-standard-for-onboarding-new-application>

20. Trainable Classifier

You need to identify information using examples of data that might be sensitive instead of using pattern matching. What should you use?

- ☐ A custom sensitive information type
- ☒ A trainable classifier
- ☐ A sensitivity label
- ☐ A retention label

You can use a trainable classifier with sample data rather than using pattern matching to identify sensitive information.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-strategy-for-securing-data/3-to-identify-protect-sensitive-data>

21. Authenticate using a managed identity

Which method provides a secure access strategy with auditing for Azure SQL Database?

- ☒ Authenticate using a managed identity
- ☐ Authenticate using a connection string
- ☐ Connect using a private endpoint
- ☐ Connect using the public DNS name

Authenticating with an identity provides secure access and an audit trail for the identity.

Reference: <https://learn.microsoft.com/en-us/training/modules/specify-security-requirements-for-applications/5-standard-for-onboarding-new-application>

22. A custom sensitive information type

You need to identify information that might be stored in documents that contain employee IDs. What should you create?

☒ A custom sensitive information type

☐ A trainable classifier

☐ A sensitivity label

☐ A retention label

A custom sensitive information type allows you to identify data based on a pattern and confidence level that you set.

Reference: <https://learn.microsoft.com/en-us/training/modules/design-strategy-for-securing-data/3-to-identify-protect-sensitive-data>

Objective 5: Recommend security best practices and priorities

1. Requirements for a DevSecOps process

You are designing the requirements for a DevSecOps process for your organization. What are two security requirements that you should include in the plan and develop phase?

☐ Application security testing

☒ Pre-commit hooks

☒ Threat modeling

☐ Security acceptance testing

Threat modeling and pre-commit hooks should be included as part of a CI/CD DevSecOps process for application development.

Reference: <https://learn.microsoft.com/en-us/training/modules/recommend-secure-methodology-using-cloud-adoption-framework-caf/2-recommend-devsecops-process>

Pre-commit hooks are scripts that run automatically before you commit your code to a version control system (VCS), like Git. They act as a last line of defense before your

code goes live, helping to ensure that it meets certain coding standards and quality criteria.

Here are some key points about pre-commit hooks:

What they do:

- Pre-commit hooks can perform various tasks, including:
 - Running linters and code formatters: These tools check your code for stylistic errors and enforce consistent formatting.
 - Running unit tests: These tests verify that your code is functionally correct.
 - Checking for security vulnerabilities: These tools scan your code for potential security risks.
 - Validating commit messages: These tools ensure that your commit messages are clear and informative.
- They can be configured to run locally on your machine or on a remote CI/CD server.
- They can be written in various scripting languages, such as Python, Ruby, and JavaScript.
- They can be customized to meet your specific project requirements.

Benefits:

- Improved code quality: Pre-commit hooks help you identify and fix errors and inconsistencies in your code before you commit it.
- Increased efficiency: By automating repetitive tasks like code formatting and linting, pre-commit hooks can save you time and effort.
- Enhanced collaboration: Pre-commit hooks can help to ensure that everyone on your team is following the same coding standards.
- Reduced risk of errors: By catching errors before they are committed, pre-commit hooks can help to prevent bugs and security vulnerabilities.

Examples of popular pre-commit hooks:

- Black: A Python code formatter.
- Flake8: A Python linter and code checker.
- Prettier: A code formatter for various languages.
- ESLint: A JavaScript linter and code checker.
- Git hooks: A framework for managing pre-commit hooks.

How to get started:

- There are various tools and libraries available for managing pre-commit hooks. Some popular options include:
 - pre-commit: A Python framework for managing pre-commit hooks.
 - husky: A Git hook management tool.
 - lint-staged: A tool for running linters on staged files.
- Start by researching and choosing a suitable pre-commit hook management tool for your project.
- Define the desired pre-commit hook tasks and configure them in your project's settings.
- Test your pre-commit hooks to ensure they are working correctly.

Overall, pre-commit hooks are a valuable tool for improving code quality, increasing efficiency, and fostering collaboration within your team. By taking the time to set up and use pre-commit hooks effectively, you can significantly enhance your development workflow and deliver better quality software.

Threat Modeling

Threat Modeling Explained

Threat modeling is a proactive approach to identifying and mitigating security risks in your system. It involves analyzing your system from an attacker's perspective, considering how they might exploit vulnerabilities to achieve their goals. By identifying these potential threats, you can take steps to prevent them from happening.

Here are some key points about threat modeling:

What it is:

- A structured process for identifying, analyzing, and mitigating security threats in a system.
- Helps you identify vulnerabilities, attack vectors, and potential impacts of security breaches.
- Can be applied to various systems, including applications, websites, networks, and software.

Benefits:

- Improved security: Proactively identifies and mitigates security risks before they can be exploited.
- Reduced costs: Saves money by preventing security breaches and data breaches.

- Increased compliance: Helps you comply with industry regulations and standards.
- Better decision-making: Provides insights into security risks to inform security investments and resource allocation.

Key steps of the threat modeling process:

1. Define the scope: What system or application are you modeling?
2. Identify assets: What data or resources need protection?
3. Identify threats: What are the potential threats to your assets?
4. Identify vulnerabilities: What are the weaknesses that could allow attackers to exploit your system?
5. Analyze attack vectors: How could attackers exploit vulnerabilities to reach your assets?
6. Evaluate risks: How likely are the threats to occur and what is the potential impact?
7. Mitigate risks: Implement controls to prevent or mitigate the identified threats.
8. Document and maintain: Document your threat model and update it regularly as your system evolves.

Popular threat modeling methods:

- STRIDE: Spoofing, Tampering, Repudiation, Information Disclosure, Denial-of-service, Elevation of privilege.
- PASTA: Process, Attack Surface, Threat Actors, Security Architecture.
- Trike: Attacker Motivation, Capabilities, Targets.

Resources:

- OWASP Threat Dragon: <https://www.threatdragon.com/>
- Microsoft Threat Modeling Tool: <https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-getting-started>
- SANS Security Reading Room - Threat Modeling: <https://www.sans.org/white-papers/1646/>

By understanding and implementing threat modeling practices, you can significantly improve your security posture and protect your valuable assets from potential threats.

2. Zero Trust

A(n) **Zero Trust** approach to security is defined as part of the Microsoft Cybersecurity Reference Architecture (MCRA).

Possible answers : **Zero Trust**

You answered this question correctly.

Explanation:

A Zero Trust security approach is recommended as part of the Microsoft Cybersecurity Reference Architecture (MCRA).

Reference: <https://learn.microsoft.com/en-us/training/modules/use-microsoft-cybersecurity-reference-architecture-azure-security-benchmarks/4-recommend-for-zero-trust-security>

Zero Trust: Never Trust, Always Verify

What is Zero Trust?

Zero Trust is a security framework that assumes no user or device is inherently trustworthy, inside or outside the network. It requires continuous verification and authorization for every access request, regardless of its origin. This approach contrasts with the traditional perimeter-based security model, which relies on implicit trust within the network and focuses on securing the network boundary.

Key principles of Zero Trust:

- Least privilege access: Users are granted only the minimum access necessary to perform their specific tasks.
- Continuous verification: Users and devices are constantly verified and authorized using multiple factors, including multi-factor authentication and risk-based assessments.
- Micro-segmentation: The network is divided into smaller segments with limited access controls, minimizing the impact of a breach.
- Data-centric security: Sensitive data is protected wherever it resides, not just at the network edge.

Benefits of Zero Trust:

- Improved security: Reduces the risk of successful cyberattacks by minimizing the attack surface and eliminating implicit trust.
- Increased agility: Enables secure access to applications and resources from anywhere, on any device.
- Enhanced compliance: Helps meet regulatory requirements for data security and privacy.

- Reduced costs: Eliminates the need for expensive perimeter security solutions.

Implementing Zero Trust:

- Identify your assets and risks: Determine what data and resources need protection and what the potential threats are.
- Implement multi-factor authentication: Require additional factors beyond passwords for user authentication.
- Segment your network: Divide your network into smaller zones with restricted access.
- Use a cloud-based identity platform: This provides centralized management of user identities and access controls.
- Monitor and audit activity: Continuously monitor activity and log data for potential threats.

Resources:

- Microsoft Zero Trust guidance: <https://learn.microsoft.com/en-us/azure/security/fundamentals/zero-trust>
- National Institute of Standards and Technology (NIST) Zero Trust Architecture: <https://www.cisa.gov/zero-trust-maturity-model>
- Zero Trust Security Alliance: <https://cloudsecurityalliance.org/zt/>

Zero Trust is a critical security strategy in today's dynamic threat landscape. By adopting a Zero Trust approach, you can significantly improve your security posture and protect your valuable assets from unauthorized access.

3. OWASP threat modeling

You are designing the security requirements for a web application. You need to identify a sample of nontechnical questions to begin defining the requirements. What should you use?

- ☐ Microsoft Cloud Security Benchmark (MCSB)
- ☐ Microsoft Cybersecurity Reference Architecture (MCRA)
- ☒ OWASP threat modeling
- ☐ Microsoft Sentinel

OWASP threat modeling provides simple nontechnical questions that can help you begin the process of defining security requirements for a web app.

Reference: <https://learn.microsoft.com/en-us/training/modules/recommend-secure-methodology-using-cloud-adoption-framework-caf/2-recommend-devsecops-process>

OWASP Threat Modeling: Proactively Securing Your Applications

Threat modeling is a crucial practice in software development, helping you identify and mitigate potential security risks before they can be exploited by attackers. OWASP (Open Web Application Security Project) provides a framework and methodologies specifically tailored to web applications, making it an invaluable tool for developers and security professionals.

What is OWASP Threat Modeling?

OWASP Threat Modeling is a structured approach to identifying, analyzing, and mitigating security threats in web applications. It leverages methodologies like STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial-of-Service, and Elevation of Privilege) and PASTA (Process, Attack Surface, Threat Actors, Security Architecture) to systematically assess vulnerabilities and attack vectors.

Benefits of OWASP Threat Modeling:

- Improved security: Proactive identification and mitigation of security risks before they can be exploited.
- Reduced costs: Saving money by preventing security breaches and data leaks.
- Enhanced compliance: Helping organizations comply with industry regulations and standards.
- Better decision-making: Providing insights into security risks to inform security investments and resource allocation.

Key Steps of OWASP Threat Modeling:

1. Define the scope: Identify the web application or system you are modeling.
2. Identify assets: Recognize the data and resources that need protection within the application.
3. Decompose the application: Break down the application into its functionality and components for detailed analysis.
4. Identify threats: Using STRIDE or similar methodologies, brainstorm potential threats to each identified asset.
5. Identify vulnerabilities: Analyze each component for weaknesses that could enable attackers to exploit the identified threats.

6. Analyze attack vectors: Determine the sequence of steps an attacker might take to exploit vulnerabilities and access the assets.
7. Evaluate risks: Assess the likelihood of each threat occurring and its potential impact on the assets.
8. Mitigate risks: Implement controls and countermeasures to address the identified vulnerabilities and mitigate the associated risks.
9. Document and maintain: Document your threat model and update it regularly to reflect changes in the application and its environment.

OWASP Resources:

- OWASP Threat Dragon: https://owasp.org/www-community/Threat_Modeling
- STRIDE Methodology: https://owasp.org/www-community/Threat_Modeling_Process
- PASTA Methodology: https://owasp.org/www-pdf-archive/AppSecEU2012_PASTA.pdf
- OWASP Threat Dragon Guide: https://owasp.org/www-community/Threat_Modeling

By embracing OWASP Threat Modeling, you can proactively secure your web applications and build a more resilient and robust software ecosystem. Remember, security is not just a feature, it's a fundamental building block of any successful application.

4. Azure policy

You are designing the asset protection requirements for your cloud environment. You need to be able to audit and automatically remediate any servers that do not have the Log Analytics agent installed on them. What should you use?

☒ Azure Policy

☐ Bicep

☐ Resource locks

☐ Microsoft Sentinel

You answered this question correctly.

Explanation:

Azure Policy allows you to create policies that audit and automatically deploy other templates if something does not already exist.
Reference: <https://learn.microsoft.com/en-us/training/modules/recommend-secure-methodology-using-cloud-adoption-framework-caf/3-recommend-methodology-for-asset-protection>

Azure Policy: Enforcing Governance and Compliance in the Cloud

Azure Policy is a powerful tool within the Azure platform that helps organizations enforce governance and compliance requirements for their cloud resources. It allows administrators to define rules and conditions that govern the creation, deployment, and operation of resources within their Azure subscriptions.

Here are some key features and benefits of Azure Policy:

Features:

- Policy definitions: These pre-built or custom rules define what is allowed and not allowed within your Azure environment.
- Policy effects: These specify what happens when a policy rule is violated, such as denying the creation of a resource, logging a warning, or automatically remediating the issue.
- Policy initiatives: These group related policy definitions for easier management and enforcement.
- Compliance assessment: Provides visibility into compliance with your defined policies and identifies any violations.
- Audit logging: Tracks policy activity and resource changes to ensure accountability and transparency.

Benefits:

- Enforces governance: Ensures resources are provisioned and configured according to organizational standards and best practices.
- Improves compliance: Helps meet regulatory requirements and industry standards.
- Reduces risks: Minimizes the chances of security vulnerabilities and configuration errors.
- Automates enforcement: Automates policy enforcement, freeing up administrative time and resources.
- Enhances consistency: Ensures consistent configuration across all resources within a subscription.

Types of Azure Policy definitions:

- Regulatory compliance: These policies are designed to meet specific regulatory requirements, such as PCI DSS or HIPAA.
- Resource governance: These policies enforce best practices for resource usage and configuration.
- Security: These policies help improve security posture by restricting access and enabling essential security features.

- Cost management: These policies optimize resource utilization and help control cloud spending.

Getting started with Azure Policy:

- Identify your governance and compliance requirements.
- Review the built-in Azure Policy definitions for relevant options.
- Create custom policy definitions to address specific needs.
- Assign policies to subscriptions, resource groups, or individual resources.
- Monitor policy compliance and address any violations.

Resources:

- Azure Policy documentation: <https://learn.microsoft.com/en-us/training/modules/configure-azure-policy/>
- List of built-in policy definitions: <https://learn.microsoft.com/en-us/azure/governance/policy/samples/>
- Azure Policy best practices: <https://learn.microsoft.com/en-us/training/modules/configure-azure-policy/>

By implementing Azure Policy effectively, organizations can enhance their cloud governance and compliance posture, leading to a more secure, efficient, and cost-effective Azure environment.

5. DevSecOps: Security requirements

You are designing the requirements for a DevSecOps process for your organization. What are two security requirements that you should include in the build and test phase?

☐ Application security testing

☐ Dependency management

☒ Infrastructure scanning

☒ Security acceptance testing

Select 2 answers

You answered this question correctly.

Explanation:

Infrastructure scanning and security acceptance testing should be included as part of a CI/CD DevSecOps process for application development. Reference: <https://learn.microsoft.com/en-us/training/modules/recommend-secure-methodology-using-cloud-adoption-framework-caf/2-recommend-devsecops-process>

DevSecOps: Security Requirements

DevSecOps is a software development methodology that integrates security practices throughout the entire software development lifecycle (SDLC), from planning and design to deployment and operation. This approach aims to shift security from being an afterthought to a core part of the development process, resulting in more secure and reliable software.

Security requirements in DevSecOps can be broadly categorized into three main types:

1. Procedural Requirements:

- Security training: All team members involved in the SDLC should receive regular security training to stay updated on current threats and best practices.
- Threat modeling: Conduct threat modeling exercises to identify potential vulnerabilities and attack vectors early in the development process.
- Security testing: Integrate automated and manual security testing tools throughout the SDLC to identify and fix vulnerabilities.
- Security code reviews: Conduct regular code reviews with a focus on security best practices and coding standards.
- Vulnerability management: Implement a process for identifying, tracking, and remediating vulnerabilities in a timely manner.
- Incident response: Develop and test an incident response plan to effectively respond to security incidents.

2. Technical Requirements:

- Secure coding practices: Developers should follow secure coding practices to minimize the introduction of vulnerabilities into the code.
- Static code analysis: Integrate static code analysis tools to identify potential security vulnerabilities before code is deployed.
- Dynamic application security testing (DAST): Conduct DAST scans to identify vulnerabilities that can be exploited during runtime.
- Software composition analysis (SCA): Identify and manage vulnerabilities in open-source libraries and dependencies.
- Infrastructure as code (IaC) security: Secure your infrastructure by using IaC tools and enforcing security best practices.
- Encryption: Use encryption to protect sensitive data at rest and in transit.

- Identity and access management (IAM): Implement strong IAM controls to restrict access to resources based on the principle of least privilege.

3. Cultural and Organizational Requirements:

- Security champions: Identify and empower security champions within the organization to advocate for security practices.
- Security awareness: Promote a culture of security awareness among all team members.
- Shared responsibility: Define clear roles and responsibilities for security throughout the SDLC.
- Continuous monitoring: Continuously monitor systems and applications for suspicious activity.
- Metrics and reporting: Track security metrics and report on progress regularly.
- Automation: Automate security tasks wherever possible to improve efficiency and consistency.

The specific security requirements for your organization will depend on various factors, such as your industry, regulatory compliance needs, and risk tolerance. However, implementing these general categories of security requirements can significantly improve the security posture of your DevSecOps practices and deliver more secure software.

Additional Resources:

- OWASP DevSecOps Verification Standard: <https://owasp.org/www-project-devsecops-verification-standard/>
- NIST DevSecOps Framework: <https://csrc.nist.gov/projects/devsecops/publications>
- Microsoft DevSecOps Guide: <https://learn.microsoft.com/en-us/training/modules/introduction-to-secure-devops/>

6. Azure AD Identity Protection

Your organization is defining security policies for a migration to the cloud. You need to recommend a tool to use for identifying the use of stolen account credentials. What should you use?

☒ Azure AD Identity Protection

☐ Defender for Identity

☐ Defender for Office 365

☐ Microsoft Sentinel

You answered this question correctly.

Explanation:

Azure AD Identity Protection provides insights for stolen account credentials.

Reference: <https://learn.microsoft.com/en-us/training/modules/use-microsoft-cybersecurity-reference-architecture-azure-security-benchmarks/3-recommend-for-protecting-from-insider-external-attacks>

Azure Active Directory Identity Protection

Azure AD Identity Protection is a comprehensive identity security solution that helps organizations prevent, detect, and respond to identity-based threats. It utilizes machine learning algorithms and real-time risk assessments to identify suspicious activity and protect against compromised identities.

Key features of Azure AD Identity Protection:

Prevention:

- Conditional Access: Enforces granular access controls based on user identity, location, device, and risk level.
- Multi-Factor Authentication (MFA): Requires an additional verification factor beyond username and password for secure logins.
- Password Protection: Enforces strong password policies and prevents password spraying attacks.
- Identity Risk Detection: Analyzes user behavior and identifies anomalies that might indicate compromised identities.
- Account Security: Protects against account takeover attempts and automatically blocks suspicious activities.

Detection:

- Real-time Risk Assessments: Continuously evaluates user sign-in attempts and assigns a risk level based on various factors.

- Sign-in Logs: Provides detailed information about user sign-in attempts, including location, device, and risk level.
- User Risk Profiles: Analyzes user behavior and assigns a risk score based on their activity patterns.
- Machine Learning: Utilizes advanced algorithms to detect unusual and potentially malicious activities.

Response:

- Adaptive Authentication: Automatically prompts users for MFA or blocks access based on the assessed risk level.
- Investigation Tools: Provides tools to investigate suspicious activities and identify the root cause of security incidents.
- Automated Remediation: Automatically blocks compromised accounts or takes corrective actions based on predefined policies.
- Reporting and Alerts: Generates reports and sends alerts about suspicious activities and security incidents.

Benefits of using Azure AD Identity Protection:

- Improved security: Protects against a wide range of identity-based threats, including phishing attacks, account takeover attempts, and password spraying.
- Reduced risk of data breaches: Identifies and mitigates threats before they can lead to data breaches and other security incidents.
- Enhanced compliance: Helps organizations comply with industry regulations and data privacy laws.
- Increased user productivity: Seamless and secure access to applications and resources without compromising security.
- Reduced administrative overhead: Automates security tasks and simplifies threat detection and response.

Getting started with Azure AD Identity Protection:

- Enable Identity Protection in your Azure AD tenant.
- Configure conditional access policies to enforce MFA and other access controls.
- Implement strong password policies and enforce regular password changes.
- Monitor user activity and investigate suspicious activity alerts.
- Utilize reporting tools to gain insights into identity-related risks.

Resources:

- Azure AD Identity Protection documentation: <https://learn.microsoft.com/en-us/defender-for-identity/what-is>
- Azure AD Conditional Access documentation: <https://learn.microsoft.com/en-us/entra/identity/conditional-access/>
- Azure AD Multi-Factor Authentication documentation: <https://learn.microsoft.com/en-us/entra/identity/authentication/>

By implementing Azure AD Identity Protection, organizations can significantly enhance their security posture and protect their valuable assets from identity-based threats.

7. Microsoft Cloud Security Benchmark (MCSB)

Your organization is defining security policies for a migration to the cloud. Which resource should you recommend to use for technical and nontechnical security controls?

- ☐ Cloud Adoption Framework (CAF)
- ☒ Microsoft Cloud Security Benchmark (MCSB)
- ☐ Microsoft Cybersecurity Reference Architecture (MCRA)
- ☐ Well-Architected Framework (WAF)

You answered this question correctly.

Explanation:

Microsoft Cloud Security Benchmark (MCSB) provides both technical and nontechnical security controls to follow for best practices in the cloud.

Reference: <https://learn.microsoft.com/en-us/training/modules/use-microsoft-cybersecurity-reference-architecture-azure-security-benchmarks/2-recommend-for-cybersecurity-capabilities-controls>

Microsoft Cloud Security Benchmark (MCSB)

The Microsoft Cloud Security Benchmark (MCSB) is a comprehensive guidance document that provides best practices and recommendations for securing your workloads, data, and services across Azure and your multi-cloud environment. It serves as a successor to the Azure Security Benchmark (ASB), which was rebranded in October 2022 to offer a broader scope encompassing multi-cloud security considerations.

Key features of MCSB:

- Prescriptive best practices: Offers prescriptive guidance on securing your cloud resources with actionable recommendations.

- Multi-cloud focus: Expands beyond Azure to address security considerations for multi-cloud deployments.
- Control mapping: Maps controls to relevant regulations and compliance requirements, facilitating compliance efforts.
- Risk-based prioritization: Categorizes controls based on their risk impact, allowing for effective prioritization.
- Continuous improvement: Regularly updated to reflect evolving technologies and security threats.

MCSB structure:

- Control categories: Organized into six main categories:
 - Identity and Access Management
 - Network Security
 - Data Protection
 - Endpoint Security
 - Infrastructure Security
 - Threat Protection and Detection
- Controls: Each category encompasses specific controls with detailed descriptions, implementation guidance, and resources.
- Compliance mappings: Controls are mapped to relevant compliance standards and regulations, such as HIPAA, PCI DSS, and SOC 2.

Benefits of using MCSB:

- Improved security posture: Provides a comprehensive roadmap for securing your cloud environment and mitigating security risks.
- Enhanced compliance: Helps you comply with industry regulations and data privacy laws.
- Reduced costs: Optimizes security investments by focusing on the most critical controls.
- Increased agility: Enables secure and efficient cloud deployments.
- Standardized approach: Offers a consistent and repeatable approach to cloud security across your organization.

How to use MCSB:

- Review the MCSB document and familiarize yourself with the controls.
- Assess your current security posture against the MCSB controls.
- Identify and prioritize the controls that are most relevant to your organization and risk profile.

- Implement the prioritized controls and measure your progress.
- Monitor your cloud environment for threats and vulnerabilities.
- Regularly review and update your security posture based on the latest MCSB guidance and evolving security threats.

Resources:

- MCSB documentation: <https://learn.microsoft.com/en-us/security/benchmark/azure/overview>
- MCSB control mapping tool: <https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/azure-purview-security-baseline>
- MCSB quick start guide: <https://learn.microsoft.com/en-us/purview/concept-elastic-data-map>

By adopting MCSB as your cloud security framework, you can significantly improve your security posture, ensure compliance, and gain the confidence to fully leverage the power of cloud computing.

8. DevSecOps processes

Drag the DevSecOps processes into the correct order.

Correct Answers

Plan and develop

Commit the code

Build and test

Go to production

Operate

Matching items here:

#1

Plan and develop ✓

#2

Commit the code ✓

#3

Build and test ✓

#4

Go to production ✓

#5

Operate ✓

You answered this question correctly.

Explanation:

Reference: <https://learn.microsoft.com/en-us/training/modules/recommend-secure-methodology-using-cloud-adoption-framework-caf/2-recommend-devsecops-process>

DevSecOps Processes: Integrating Security Throughout the SDLC

DevSecOps is a software development methodology that integrates security practices throughout the entire Software Development Life Cycle (SDLC), from planning and design to deployment and operation. This shift left-shifts security from being an afterthought to a core part of the development process, leading to more secure and reliable software.

Key DevSecOps Processes:

1. Planning and Design:

- Security requirements definition: Identify and document security requirements for the planned software.
- Threat modeling: Analyze potential threats and vulnerabilities early in the development process.
- Secure architecture design: Design a secure architecture that mitigates identified threats and vulnerabilities.
- Secure coding guidelines: Define secure coding practices and standards for developers to follow.

2. Development:

- Static code analysis: Integrate static code analysis tools to identify potential vulnerabilities in the code.
- Dynamic application security testing (DAST): Conduct DAST scans to identify vulnerabilities that can be exploited during runtime.
- Software composition analysis (SCA): Identify and manage vulnerabilities in open-source libraries and dependencies.
- Integration security testing: Test the security of integrations between different components of the software.
- Automated security testing: Integrate security testing tools into the CI/CD pipeline for continuous feedback.

3. Deployment and Operation:

- Vulnerability scanning: Continuously scan deployed systems for vulnerabilities.
- Security configuration management: Manage and enforce security configurations for deployed systems.
- Identity and access management (IAM): Implement IAM controls to restrict access to resources based on the principle of least privilege.

- Log management and monitoring: Monitor system logs and events for suspicious activity.
- Incident response: Develop and test an incident response plan to effectively respond to security incidents.

4. Communication and Collaboration:

- Security awareness training: Provide regular security training to all team members involved in the SDLC.
- Security champions: Appoint security champions to advocate for security best practices.
- Security communication channels: Establish clear communication channels for reporting security incidents and concerns.
- Security metrics and reporting: Track security metrics and report on progress regularly.
- Shared responsibility: Define clear roles and responsibilities for security throughout the SDLC.

Benefits of Implementing DevSecOps Processes:

- Improved security posture: Early detection and mitigation of security risks throughout the development process.
- Reduced costs: Lower costs associated with fixing vulnerabilities later in the development cycle.
- Faster time to market: By addressing security concerns early, releases can be made faster and more consistently.
- Enhanced compliance: Easier compliance with industry regulations and data privacy laws.
- Increased accountability: Security becomes a shared responsibility, leading to better ownership and accountability.

Getting Started with DevSecOps Processes:

- Assess your current security practices and identify areas for improvement.
- Develop a plan for integrating security into your SDLC.
- Start small and gradually implement DevSecOps practices.
- Invest in training and tools to support your DevSecOps efforts.
- Measure your progress and continuously improve your DevSecOps practices.

Resources:

- OWASP DevSecOps Verification Standard: <https://owasp.org/www-project-devsecops-verification-standard/>: <https://owasp.org/www-project-devsecops-verification-standard/>
- NIST DevSecOps Framework: <https://csrc.nist.gov/projects/devsecops/publications>: <https://csrc.nist.gov/projects/devsecops/publications>

- Microsoft DevSecOps Guide: <https://learn.microsoft.com/en-us/training/modules/introduction-to-secure-devops/>: <https://learn.microsoft.com/en-us/training/modules/introduction-to-secure-devops/>

By integrating DevSecOps processes into your software development lifecycle, you can significantly improve the security of your applications and deliver reliable software that meets your business needs.

9. DevSecOps: Security Requirements

You are designing the requirements for a DevSecOps process for your organization. What are two security requirements that you should include in the go to production phase?

☐ Application security testing

☒ Configuration checks

☐ Threat modeling

☒ Smoke tests

Select 2 answers

You answered this question correctly.

Explanation:

Configuration checks and smoke tests should be included as part of a CI/CD DevSecOps process for application development.

Reference: <https://learn.microsoft.com/en-us/training/modules/recommend-secure-methodology-using-cloud-adoption-framework-caf/2-recommend-devsecops-process>

DevSecOps: Security Requirements

DevSecOps integrates security practices into the entire software development lifecycle (SDLC), from planning and design to deployment and operation. This approach requires clear and comprehensive security requirements to guide development efforts and ensure the overall security posture of the software.

Here are some key categories of security requirements in DevSecOps:

Procedural Requirements:

- Security training: All team members involved in the SDLC, including developers, operations, and security professionals, must receive ongoing security training to stay up-to-date on current threats and best practices.
- Threat modeling: Conduct threat modeling exercises early in the development process to identify potential vulnerabilities and attack vectors.

- Security testing: Integrate security testing tools and methodologies throughout the SDLC, including static code analysis, dynamic application security testing (DAST), and software composition analysis (SCA).
- Secure coding practices: Developers should follow secure coding practices and standards to minimize the introduction of vulnerabilities into the code.
- Vulnerability management: Implement a process for identifying, tracking, and remediating vulnerabilities in a timely manner.
- Incident response: Develop and test an incident response plan to effectively respond to security incidents.

Technical Requirements:

- Access control and role-based permissions: Implement access control mechanisms to restrict access to resources based on the principle of least privilege.
- Data encryption: Encrypt sensitive data at rest and in transit to protect against unauthorized access.
- Secure configuration management: Use configuration management tools to ensure consistency and enforce security configurations across all systems and applications.
- Multi-factor authentication (MFA): Implement MFA for all user accounts to enhance security and prevent unauthorized access.
- Network segmentation: Segment your network to restrict the potential impact of security breaches.
- Logging and monitoring: Implement comprehensive logging and monitoring systems to detect suspicious activity and identify potential security incidents.

Operational Requirements:

- Security incident and event management (SIEM): Implement a SIEM solution to collect and analyze security data from various sources to identify and respond to security incidents effectively.
- Security posture management (SPM): Utilize SPM tools to continuously assess and monitor the security posture of your systems and applications.
- Vulnerability scanning and penetration testing: Conduct regular vulnerability scans and penetration tests to identify and address vulnerabilities before they can be exploited by attackers.
- Security audits and assessments: Perform periodic security audits and assessments to identify and address weaknesses in your security controls and processes.

- Compliance requirements: Ensure your systems and applications comply with relevant industry regulations and data privacy laws.

Additional Considerations:

- DevSecOps tools and platforms: Utilize DevSecOps tools and platforms to automate security tasks and integrate security practices seamlessly into the development pipeline.
- Security champions: Appoint security champions within your organization to advocate for security best practices and promote a culture of security awareness.
- Continuous improvement: Continuously review and update your security requirements and practices to adapt to evolving threats and technologies.

By establishing and effectively implementing comprehensive security requirements, you can ensure that security is woven into the fabric of your DevSecOps practices, leading to the development of more secure and reliable software.

Here are some resources that you may find helpful:

- OWASP DevSecOps Verification Standard: <https://owasp.org/www-project-application-security-verification-standard/>
- NIST DevSecOps Framework: <https://csrc.nist.gov/projects/devsecops>
- Microsoft DevSecOps Guide: <https://learn.microsoft.com/en-us/training/modules/introduction-to-secure-devops/>

Smoke Tests

Smoke Tests: Verifying Basic Functionality

Smoke tests are preliminary tests performed to quickly confirm that the basic functionality of a system or application works correctly. They are typically quick and automated, focusing on verifying the system's core features and ensuring it is ready for further testing.

Key characteristics of smoke tests:

- Minimal scope: They focus on verifying critical functionality rather than comprehensively testing all features.
- Fast execution: They are designed to be quick and automated, taking minutes rather than hours or days.
- Early execution: They are typically performed before more extensive testing, often as part of the continuous integration (CI) pipeline.

- Pass/fail criteria: They provide a simple pass/fail result, indicating whether the system is functioning at a basic level.

Benefits of smoke testing:

- Early detection of critical issues: Identifying and addressing critical issues before investing resources in extensive testing.
- Improved build quality: Ensuring that builds are stable and ready for further testing, leading to more efficient development cycles.
- Reduced testing time: Focusing on essential functionality saves time and resources compared to comprehensive testing.
- Proactive problem identification: Proactively identifying potential problems before they manifest as larger issues.
- Increased confidence: Providing confidence that the system is ready for further testing and potential deployment.

Use cases for smoke tests:

- After code changes: To ensure that new code hasn't introduced regressions or broken existing functionality.
- Before manual testing: To save time and resources by focusing manual testing on areas with a higher risk of problems.
- After deployments: To verify that the system has deployed successfully and is functioning as expected.

Examples of smoke tests:

- Web application: Checking that the homepage loads correctly, verifying user login functionality, and confirming basic navigation.
- Mobile app: Ensuring the app launches successfully, testing basic features like touch input and gestures, and verifying data persistence.
- API endpoint: Sending basic requests to the API and verifying the response status codes and data format.

Best practices for smoke testing:

- Automate smoke tests: Utilize automation tools to run smoke tests consistently and efficiently.
- Focus on critical functionality: Prioritize tests that cover the core features of the system.
- Keep tests simple and concise: Avoid complex test cases that add unnecessary time and complexity.
- Use clear pass/fail criteria: Establish clear criteria for determining test success or failure.

- Integrate smoke tests into the CI pipeline: Run smoke tests automatically as part of the build process.
- Review and update smoke tests regularly: Ensure smoke tests are relevant and reflect changes in the system functionality.

By incorporating smoke testing into your development process, you can improve the quality and efficiency of your testing efforts, detect critical issues early, and ensure a stable and reliable system for your users.

10. Privileged Identity Management

You are designing an authorization strategy for an organization. You need to protect privileged accounts that can access security events and notifications. Administrators must provide justification when accessing these tools. What should you use?

- ☐ Conditional Access
- ☐ Role-based access control
- ☐ Privileged access workstations
- ☒ Privileged Identity Management

You answered this question correctly.

Explanation:

Privileged Identity Management allows you to protect elevated access and can require justification when activating elevated roles.

Reference: <https://learn.microsoft.com/en-us/training/modules/use-microsoft-cybersecurity-reference-architecture-azure-security-benchmarks/2-recommend-for-cybersecurity-capabilities-controls>

Azure Privileged Identity Management (PIM)

Azure Privileged Identity Management (PIM) helps organizations manage, control, and monitor privileged access to Azure resources. It provides a comprehensive solution for minimizing the risks associated with granting excessive and unnecessary administrative access.

Key benefits of Azure PIM:

Enhanced security:

- Reduces the attack surface: Limits the number of users with permanent privileged access, minimizing the potential impact of compromised accounts.
- Provides time-based or approval-based access: Enables just-in-time access for specific tasks, reducing the risk of privilege misuse.

- Enforces multi-factor authentication (MFA) for privileged access: Adds an extra layer of security to prevent unauthorized access.

Improved control and auditability:

- Centralizes management of privileged roles: Offers a single platform to manage all privileged identities and access assignments.
- Provides detailed audit logs: Enables tracking and monitoring of privileged access activities for compliance and security investigations.
- Supports role-based access control (RBAC): Allows granular control over access to specific resources and operations.

Increased agility and efficiency:

- Streamlines the process for granting and revoking access: Enables on-demand access for authorized users without manual intervention.
- Automates routine tasks: Reduces manual administrative overhead and improves operational efficiency.
- Supports integration with existing tools and processes: Integrates seamlessly with other Azure security solutions and identity management systems.

Key features of Azure PIM:

- Azure AD roles and Azure resources: Enables managing privileged access to Azure AD roles and Azure resources, such as virtual machines, storage accounts, and databases.
- Time-based access: Allows granting access for a specific duration, minimizing the time window for potential misuse.
- Approval-based access: Requires approval from designated reviewers before granting access, adding an extra layer of control.
- Emergency access: Enables temporary access for urgent situations with automatic expiration.
- Reports and monitoring: Provides detailed insights into privileged access activity and trends.

Getting started with Azure PIM:

- Enable Azure PIM in your Azure subscription.
- Identify and assign Azure AD roles and resource roles.
- Configure time-based or approval-based access for privileged roles.
- Enable MFA for privileged identities.
- Monitor access activity and investigate suspicious events.

Resources:

- Azure PIM documentation: <https://learn.microsoft.com/en-us/training/modules/azure-ad-privileged-identity-management/>
- Azure PIM quick start guide: <https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-how-to-add-role-to-user>
- Azure PIM best practices: <https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-how-to-activate-role>

By implementing Azure PIM, organizations can significantly improve their security posture, ensure compliance with regulations, and gain better control over privileged access to their Azure resources.

11. Defender for Identity

You are designing security for an organization. You need to identify a way to monitor brute-force attempts such as password sprays. What should you use?

- ☐ Defender for Cloud
- ☒ Defender for Identity
- ☐ Defender for Information Protection
- ☐ Defender for Microsoft 365

You answered this question correctly.

Explanation:

Defender for Identity includes the ability to monitor account access attempts, including password spray attempts.

Reference: <https://learn.microsoft.com/en-us/training/modules/recommend-ransomware-strategy-by-using-microsoft-security-best-practices/3-protect-assets-from-ransomware-attacks>

Defender for Identity: Enhanced Security for Your Hybrid Identity Landscape

Microsoft Defender for Identity is a cloud-based security solution designed to protect your hybrid identity environment, including on-premises Active Directory and cloud identities. It provides advanced threat detection and response capabilities to help you identify and mitigate security risks associated with compromised identities.

Key Features:

- Identity-based threat detection and response: Utilizes advanced machine learning and analytics to identify anomalous user behavior and suspicious activities, such as lateral movement, privilege escalation attempts, and password spraying attacks.

- Automated investigation and remediation: Automates investigation workflows and provides recommendations for remediating identified threats, reducing the time and resources required to respond to security incidents.
- Real-time visibility and monitoring: Offers a centralized dashboard for monitoring user activity, identifying suspicious events, and investigating potential threats in real-time.
- Risk-based prioritization: Prioritizes alerts based on their potential risk level, enabling security teams to focus their efforts on the most critical threats.
- Integration with other security solutions: Integrates with other Microsoft security solutions, such as Azure Sentinel and Microsoft Defender for Cloud, providing a comprehensive view of your security posture and a coordinated response to threats.

Benefits:

- Enhanced security posture: Proactively identifies and mitigates identity-based threats before they can cause significant damage.
- Reduced risk of data breaches: Protects your sensitive data from unauthorized access by compromised identities.
- Improved compliance: Helps organizations comply with industry regulations and data privacy laws related to identity security.
- Increased operational efficiency: Automates security tasks and reduces the workload on security teams.
- Better decision-making: Provides actionable insights into identity-related risks to inform security decisions.

Use Cases:

- Protecting privileged accounts: Monitor and control access to privileged accounts to prevent misuse and unauthorized access.
- Detecting and responding to insider threats: Identify anomalous user behavior that might indicate malicious insider activity.
- Responding to password spraying attacks: Detect and block attempts to crack user passwords using automated tools.
- Investigating suspicious activity: Analyze user activity logs to identify potential security incidents and investigate the root cause.
- Meeting compliance requirements: Demonstrate compliance with industry regulations and data privacy laws by implementing appropriate identity security controls.

Getting Started:

- Enable Defender for Identity in your Microsoft Defender for Cloud workspace.

- Connect your on-premises Active Directory environment to Defender for Identity.
- Configure threat detection rules and alerts.
- Monitor user activity and investigate suspicious events.
- Utilize the provided tools and insights to respond to identified threats.

Resources:

- Defender for Identity documentation: <https://learn.microsoft.com/en-us/defender-for-identity/what-is>
- Defender for Identity quick start guide: <https://learn.microsoft.com/en-us/defender-for-identity/deploy-defender-identity>
- Defender for Identity best practices: <https://learn.microsoft.com/en-us/azure/sentinel/best-practices>

By implementing Defender for Identity, organizations can significantly improve their identity security posture and gain a comprehensive view of their hybrid identity environment. This can help them proactively detect and respond to identity-based threats, protect sensitive data, and meet compliance requirements.

12. Attack surface reduction rules

You are designing security for an organization. You need to block common attack techniques such as advanced macro activity and process injection. What should you use?

- ☐ Azure Policy
- ☒ Attack surface reduction rules
- ☐ Defender for Cloud
- ☐ Defender for Cloud Apps

You answered this question correctly.

Explanation:

Attack surface reduction rules can help protect an endpoint against common attack techniques.

Reference: <https://learn.microsoft.com/en-us/training/modules/recommend-ransomware-strategy-by-using-microsoft-security-best-practices/4-recommend-microsoft-ransomware>

Attack Surface Reduction Rules: Protecting Your Endpoints

Attack surface reduction rules (ASR) are a powerful security feature within Microsoft Defender for Endpoint that helps administrators proactively reduce the attack surface and mitigate potential security risks on endpoints. These rules can be configured to restrict specific functionalities, block malicious behaviors, and limit interactions with potentially unsafe resources.

Key features of ASR:

- **Predefined rules:** ASR offers a set of predefined rules that address common attack vectors, such as blocking executable files from specific locations or preventing the execution of scripts.
- **Custom rules:** Organizations can create custom rules tailored to their specific security needs and risk profile.
- **Granular control:** ASR allows for granular control over rule application, enabling administrators to target specific groups of users or devices.
- **Auditing and reporting:** ASR provides detailed audit logs and reports on rule activity, enabling administrators to track the effectiveness of these rules and identify potential security incidents.

Benefits of using ASR:

- **Reduced attack surface:** Limits the attack surface available for malicious actors, making it more difficult for them to exploit vulnerabilities.
- **Improved security posture:** Proactively mitigates potential security risks and reduces the likelihood of successful attacks.
- **Enhanced compliance:** Helps organizations comply with industry regulations and data privacy laws that require specific security controls.
- **Reduced operational overhead:** Automates security tasks and simplifies the process of implementing security controls.
- **Improved visibility and control:** Provides greater visibility into endpoint activity and enables administrators to take corrective action when necessary.

Use cases for ASR:

- **Blocking untrusted applications:** Prevent the execution of untrusted or potentially harmful applications from running on endpoints.
- **Restricting access to specific locations:** Block access to websites, folders, or drives that might contain malicious content.

- Preventing script execution: Limit the execution of scripts, such as PowerShell scripts, to help mitigate script-based attacks.
- Disabling unnecessary functionalities: Disable features or functionalities that are not essential for user productivity but can be exploited by attackers.
- Protecting sensitive data: Restrict access to sensitive data and resources to minimize the potential impact of data breaches.

Getting started with ASR:

- Enable ASR in Microsoft Defender for Endpoint.
- Review and configure the predefined rules.
- Create custom rules if needed.
- Assign rules to specific groups of users or devices.
- Monitor ASR activity and investigate suspicious events.

Resources:

- Attack Surface Reduction Rules documentation: <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction?view=o365-worldwide>
- Attack Surface Reduction Rules best practices: <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction?view=o365-worldwide>
- Microsoft Defender for Endpoint documentation: <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/?view=o365-worldwide>

By implementing Attack Surface Reduction Rules effectively, organizations can significantly improve their endpoint security posture and proactively mitigate potential threats before they can cause harm.

13. Designing security with a focus on protecting an organization from ransomware.

You are designing security with a focus on protecting an organization from ransomware. What are two methods of preventing attackers from getting in?

☒ Endpoint security

☐ Data protection

☒ Remote access security

☐ Secure backups

Select 2 answers

You answered this question correctly.

Explanation:

Endpoint security and remote access security are two key methods of preventing attackers from getting in and accessing an organization's system.

Reference: <https://learn.microsoft.com/en-us/training/modules/recommend-ransomware-strategy-by-using-microsoft-security-best-practices/1-introduction>

Designing Security with a Focus on Protecting an Organization from Ransomware

Ransomware is a serious and evolving threat that can have devastating consequences for organizations. To effectively protect against ransomware attacks, it's crucial to design security with this specific threat in mind. Here are some key principles for designing security with a focus on protecting against ransomware:

Defense in Depth:

- Implement a layered security approach: Employ multiple security controls at different layers of the IT infrastructure, including network, endpoint, application, and data layers.
- Focus on prevention: Prioritize preventing ransomware infections in the first place by strengthening perimeter defenses, hardening systems, and implementing security awareness training for employees.
- Implement data backups and recovery solutions: Ensure regular backups of critical data are stored offline and encrypted. Develop and test a comprehensive incident response plan for efficient recovery in case of an attack.

Least Privilege:

- Grant users access based on the principle of least privilege: Users should only have the minimum access necessary to perform their job duties. This minimizes the potential impact of compromised accounts.
- Implement multi-factor authentication (MFA): Require MFA for all user accounts, including privileged accounts. This adds an extra layer of security and makes it harder for attackers to gain access.

Network Security:

- Segment your network: Divide your network into smaller segments to limit the lateral movement of attackers if they compromise a system.
- Filter network traffic: Implement network security controls to block access to malicious websites and prevent unauthorized data exfiltration.
- Monitor network activity: Continuously monitor network traffic for suspicious activity that might indicate a ransomware attack.

Endpoint Security:

- Deploy endpoint security solutions: Utilize endpoint detection and response (EDR) solutions to detect and respond to ransomware attacks on individual devices.
- Keep systems updated: Apply security patches and updates promptly to close vulnerabilities that attackers could exploit.
- Restrict software installation: Implement policies to control which applications users can install on their devices.
- Disable unnecessary features and functionalities: Disable features and functionalities that are not essential for user productivity but can be exploited by attackers.

Data Security:

- Encrypt sensitive data: Encrypt sensitive data at rest and in transit to protect it from unauthorized access.
- Implement data loss prevention (DLP): Use DLP tools to prevent unauthorized data exfiltration.
- Monitor data access: Monitor access to sensitive data to detect suspicious activity.

Security Awareness and Training:

- Provide regular security awareness training to employees: Educate employees about ransomware threats and best practices for protecting against them.
- Phishing simulations: Conduct phishing simulations to test employee awareness and identify areas for improvement.
- Incident reporting: Encourage employees to report suspicious activity immediately to the security team.

Continuous Improvement:

- Regularly assess your security posture: Conduct periodic security assessments to identify vulnerabilities and weaknesses in your defenses.
- Test your incident response plan: Regularly test your incident response plan to ensure it is effective in responding to ransomware attacks.

- Stay informed about evolving threats: Continuously update your security posture and awareness training to keep up with the latest ransomware threats and techniques.

By implementing these security principles and adopting a proactive approach to ransomware protection, organizations can significantly reduce the risk of falling victim to a ransomware attack and minimize the potential damage if an attack occurs.

14. Defender for Identity

Your organization is defining security policies for a migration to the cloud. You need to recommend a tool to use for identifying privileged accounts that might be compromised. What should you use?

☐ Azure AD Identity Protection

☒ Defender for Identity

☐ Defender for Office 365

☐ Microsoft Sentinel

You answered this question correctly.

Explanation:

Defender for Identity includes tools to identify whether a privileged account has been compromised.

Reference: <https://learn.microsoft.com/en-us/training/modules/use-microsoft-cybersecurity-reference-architecture-azure-security-benchmarks/3-recommend-for-protecting-from-insider-external-attacks>

15. What are two security requirements that you should include in the operate phase of DevSecOps process?

You are designing the requirements for a DevSecOps process for your organization. What are two security requirements that you should include in operate phase?

☐ Application security testing

☒ Penetration testing

☒ Threat intelligence

☐ Smoke tests

Select 2 answers

You answered this question correctly.

Explanation:

Penetration testing and threat intelligence should be included as part of a CI/CD DevSecOps process for application development.

Reference: <https://learn.microsoft.com/en-us/training/modules/recommend-secure-methodology-using-cloud-adoption-framework-caf/2-recommend-devsecops-process>

16. The three principles of a Zero Trust approach to security

What are the three principles of a Zero Trust approach to security?

☒ Assume compromise

☒ Implement the principle of least privilege

☐ Network segmentation

☒ Verify explicitly

17. Two methods of preventing attackers from escalating privileges?

You are designing security with a focus on protecting an organization from ransomware. What are two methods of preventing attackers from escalating privileges?

☐ Data protection

☒ Detection and response

☐ Endpoint security

☒ Privileged access strategy

Select 2 answers

You answered this question correctly.

Explanation:

Detection and response and a privileged access strategy both fall in the category of preventing attackers from escalating their privileges if they are able to gain access to a system.

Reference: <https://learn.microsoft.com/en-us/training/modules/recommend-ransomware-strategy-by-using-microsoft-security-best-practices/1-introduction>

18. MITRE ATT&CK Framework

Your organization is defining security policies for a migration to the cloud. Which resource should you recommend to use to help in planning detailed security control planning like threat detection coverage?

☐ Cloud Adoption Framework (CAF)

☒ MITRE ATT&CK Framework

☐ Microsoft Cybersecurity Reference Architecture (MCRA)

☐ Well-Architected Framework (WAF)

You answered this question correctly.

Explanation:

The MITRE ATT&CK Framework provides a detailed list of security controls and attack vectors that can be used for planning.

Reference: <https://learn.microsoft.com/en-us/training/modules/use-microsoft-cybersecurity-reference-architecture-azure-security-benchmarks/3-recommend-for-protecting-from-insider-external-attacks>

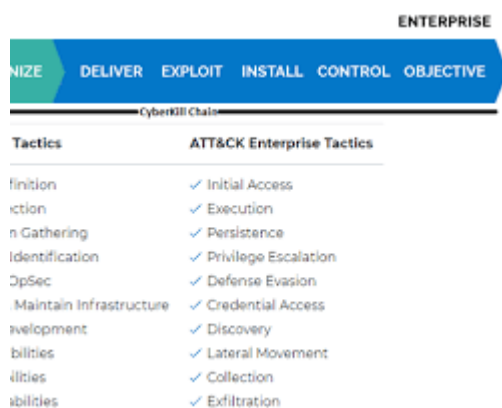
The MITRE ATT&CK framework is a knowledge base of adversary tactics, techniques, and procedures (TTPs) used in cyberattacks. It is a valuable resource for security professionals to understand how attackers operate and to develop effective defenses.

Opens in a new window  www.trellix.com

MITRE ATT&CK framework

The MITRE ATT&CK framework is organized into three high-level phases:

- Pre-attack: This phase includes activities that attackers perform before they have gained access to a system or network, such as reconnaissance and vulnerability scanning.



[Opens in a new window](#)  [sentinet.pl](https://www.sentinet.pl)

Preattack phase in MITRE ATT&CK framework

- Execution: This phase includes activities that attackers perform after they have gained access to a system or network, such as lateral movement, privilege escalation, and data exfiltration.



[Opens in a new window](#) 

www.sentinelone.com

Execution phase in MITRE ATT&CK framework

- Defense evasion: This phase includes activities that attackers perform to evade detection and analysis, such as clearing logs and disabling security tools.



[Opens in a new window](#)

www.blackberry.com

Defense evasion phase in MITRE ATT&CK framework

Within each phase, the MITRE ATT&CK framework is further divided into tactics, techniques, and procedures. Tactics are broad categories of activities that attackers perform, such as reconnaissance or privilege escalation. Techniques are specific methods that attackers use to perform a tactic, such as using a phishing email to steal credentials or exploiting a vulnerability to gain remote access to a system. Procedures are step-by-step instructions for performing a technique.

The MITRE ATT&CK framework is constantly being updated to reflect new TTPs that are being used by attackers. It is a valuable resource for security professionals to stay up-to-date on the latest threats and to develop effective defenses.

Here are some of the benefits of using the MITRE ATT&CK framework:

- Improved understanding of attacker behavior: The MITRE ATT&CK framework provides a comprehensive view of how attackers operate, from reconnaissance to data exfiltration. This understanding can help security professionals to develop more effective defenses.
- Improved threat detection and response: The MITRE ATT&CK framework can be used to identify and prioritize threats. This can help security teams to respond to incidents more quickly and effectively.
- Improved security posture: The MITRE ATT&CK framework can be used to identify security gaps and vulnerabilities. This can help organizations to improve their overall security posture.

19. Azure AD Application Proxy

You are designing security for a legacy web app that does not directly support Azure AD authentication. You need to ensure that users can access the application by using Azure AD for authentication. What should you use?

☒ Azure AD Application Proxy

☐ Azure Bastion

☐ Application Gateway

☐ Azure Front Door

You answered this question correctly.

Explanation:

Azure AD Application Proxy allows you to forward authentication requests to Azure AD even if the legacy application does not directly support or integrate with Azure AD.

Reference: <https://learn.microsoft.com/en-us/training/modules/recommend-ransomware-strategy-by-using-microsoft-security-best-practices/4-recommend-microsoft-ransomware>

Azure AD Application Proxy: Securely Access On-Premises Apps from the Cloud

Azure AD Application Proxy provides a secure and centralized way for users to access on-premises applications remotely through the Azure cloud. It eliminates the need for complex VPN configurations and provides a seamless user experience.

Key features of Azure AD Application Proxy:

- Secure access: Applications are accessed through the Azure cloud, removing the need to expose them directly to the internet.
- Single sign-on (SSO): Users can sign in to applications with their Azure AD credentials, eliminating the need for separate logins.
- Multi-factor authentication (MFA): Supports MFA for added security.
- Pre-authentication: Allows administrators to control who can access applications before authentication.
- Conditional access: Enables granular control over access to applications based on various conditions, such as user location, device type, and risk level.
- Reporting and monitoring: Provides detailed reports and logs to track application usage and identify potential security incidents.

Benefits of using Azure AD Application Proxy:

- Improved security: By eliminating the need to expose applications directly to the internet, Azure AD Application Proxy reduces the attack surface and minimizes the risk of unauthorized access.
- Enhanced user experience: Users can access applications from anywhere with an internet connection, without the need for VPNs.
- Reduced administrative overhead: Azure AD Application Proxy simplifies the process of managing and securing on-premises applications.
- Increased compliance: Supports compliance with industry regulations and data privacy laws.
- Centralized management: Provides a single platform for managing access to all on-premises applications.

Use cases for Azure AD Application Proxy:

- Remote access for employees: Enables employees to access on-premises applications from remote locations or home offices.
- Partner access: Provides secure access to on-premises applications for partners and vendors.
- Legacy application access: Allows users to access older applications that are not internet-ready.
- Mergers and acquisitions: Simplifies the process of integrating applications after mergers and acquisitions.

Getting started with Azure AD Application Proxy:

- Enable Azure AD Application Proxy in your Azure subscription.
- Configure your on-premises application connectors.
- Publish your on-premises applications to Azure AD.
- Assign users and groups access to published applications.
- Test access to applications and configure conditional access policies (optional).

Resources:

- Azure AD Application Proxy documentation: <https://learn.microsoft.com/en-us/training/modules/configure-azure-ad-application-proxy/>
- Azure AD Application Proxy quick start guide: <https://learn.microsoft.com/en-us/entra/identity/app-proxy/application-proxy-add-on-premises-application>
- Azure AD Application Proxy best practices: <https://learn.microsoft.com/en-us/training/modules/configure-azure-ad-application-proxy/>

By implementing Azure AD Application Proxy, organizations can securely and easily grant their users remote access to on-premises applications, enhancing user productivity and improving security posture.

Azure Front Door

Azure Front Door: A Modern Cloud CDN for Global Application Delivery

Azure Front Door is a modern cloud content delivery network (CDN) service offered by Microsoft Azure. It provides fast, reliable, and secure delivery of your web applications, static content, and APIs to users around the world.

Key features of Azure Front Door:

- Global network of edge locations: Leverages a geographically distributed network of edge locations to deliver content closer to users, minimizing latency and improving performance.
- High availability: Offers high availability and redundancy to ensure continuous uptime and service delivery.
- Automatic load balancing: Routes traffic automatically across available edge locations to optimize performance and prevent overloading individual servers.
- Web application firewall (WAF): Provides built-in protection against common web application attacks, such as SQL injection and cross-site scripting (XSS).
- URL routing and rewrite: Allows you to customize URL paths and redirect traffic based on specific rules.
- Traffic management: Enables you to manage traffic based on various factors, such as user location, time of day, and origin.
- Detailed analytics and reporting: Provides insights into traffic patterns, performance metrics, and security events.

Benefits of using Azure Front Door:

- Improved performance: Delivers content faster to users around the world, resulting in improved user experience and reduced bounce rates.
- Reduced costs: Offloads traffic from your origin servers, leading to cost savings on infrastructure and bandwidth.
- Increased scalability: Easily scales to accommodate spikes in traffic without impacting performance.

- Enhanced security: Protects your applications from web attacks with built-in WAF capabilities.
- Simplified deployment and management: Offers a user-friendly interface and integration with other Azure services.

Use cases for Azure Front Door:

- Delivering static content: Images, videos, JavaScript files, and other static content can be cached at edge locations for faster loading times.
- Hosting web applications: Web applications can be served through Azure Front Door to improve performance and scalability.
- Protecting applications from DDoS attacks: Azure Front Door can absorb large volumes of attack traffic, protecting your applications from downtime.
- Serving APIs: APIs can be exposed through Azure Front Door to ensure fast and reliable access for developers.
- Delivering global content: Content can be localized and delivered to users in different regions with the appropriate language and cultural settings.

Getting started with Azure Front Door:

- Create an Azure Front Door profile in your Azure subscription.
- Configure your origin servers and define routing rules.
- Enable additional features such as WAF and routing policies (optional).
- Monitor performance metrics and analyze traffic patterns.

Resources:

- Azure Front Door documentation: <https://learn.microsoft.com/en-us/azure/frontdoor/>
- Azure Front Door quick start guide: <https://learn.microsoft.com/en-us/training/modules/intro-to-azure-front-door/>
- Azure Front Door best practices: <https://learn.microsoft.com/en-us/azure/web-application-firewall/afds/waf-front-door-best-practices>

By implementing Azure Front Door, organizations can significantly improve the performance, scalability, and security of their global web applications and content delivery. This can lead to a better user experience, increased business agility, and improved cost efficiency.

20. Zero Trust Rapid Modernization Plan (RaMP)

You are designing the security requirements for an organization. You need to accelerate and prioritize the security solution. What should you use

- ☐ Cloud Adoption Framework
- ☐ Microsoft Cloud Security Benchmark
- ☐ Well Architected Framework
- ☒ Zero Trust Rapid Modernization Plan (RaMP)

You answered this question correctly.

Explanation:

The Zero Trust RaMP is included with the Microsoft Cybersecurity Reference Architecture to help prioritize and accelerate a security modernization.

Reference: <https://learn.microsoft.com/en-us/training/modules/use-microsoft-cybersecurity-reference-architecture-azure-security-benchmarks/5-recommend-for-zero-trust-rapid-modernization-plan>

Zero Trust Rapid Modernization Plan (RaMP)

The Zero Trust Rapid Modernization Plan (RaMP) is a Microsoft-developed initiative designed to help organizations quickly and efficiently implement key layers of protection aligned with Zero Trust principles. It offers a practical and actionable approach to modernize security and IT infrastructure by focusing on specific initiatives rather than detailed configuration steps for various technologies.

Key benefits of RaMP:

- **Faster implementation:** Compared to traditional deployment methodologies, RaMP enables faster adoption of Zero Trust principles by focusing on essential initiatives and providing pre-defined implementation paths.
- **Reduced complexity:** By streamlining the implementation process and offering pre-configured solutions, RaMP minimizes the complexity associated with Zero Trust adoption.
- **Improved security posture:** Implementing key Zero Trust principles through RaMP strengthens the overall security posture of your organization by reducing risk and improving access controls.
- **Increased efficiency:** By focusing on specific initiatives and leveraging pre-defined solutions, RaMP allows organizations to achieve Zero Trust goals with greater efficiency and resource optimization.

- Aligned with best practices: RaMP incorporates best practices and recommendations for Zero Trust implementation, ensuring alignment with industry standards and leading security frameworks.

RaMP Initiatives:

- Identity and Access Management: This initiative focuses on securing user identities and implementing multi-factor authentication (MFA) to ensure only authorized users access resources.
- Endpoint Security: This initiative aims to harden endpoints and implement endpoint detection and response (EDR) solutions to protect against malware and other threats.
- Application Security: This initiative focuses on securing applications and APIs through access control mechanisms, vulnerability management, and web application firewalls (WAFs).
- Network Security: This initiative aims to segment your network and implement intrusion detection/prevention systems (IDS/IPS) to restrict lateral movement and minimize attack surfaces.
- Data Security: This initiative focuses on protecting sensitive data through encryption, data loss prevention (DLP), and robust access controls.

Implementation approach:

1. Assess your current security posture: Evaluate your existing security controls and identify gaps in alignment with Zero Trust principles.
2. Prioritize RaMP initiatives: Based on your assessment, prioritize the RaMP initiatives that offer the most significant impact and address critical security gaps.
3. Leverage pre-defined solutions: Utilize pre-configured solutions and templates available within RaMP to simplify deployment and reduce configuration complexity.
4. Customize and adapt: While leveraging pre-defined solutions, adapt them to your specific organizational context and security requirements.
5. Measure and monitor progress: Continuously monitor the effectiveness of your RaMP implementation and adjust your approach as needed to ensure ongoing improvement.

Resources:

- Zero Trust Rapid Modernization Plan (RaMP) overview: <https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-ramp-overview>
- Zero Trust Rapid Modernization Plan (RaMP) technical guidance: <https://github.com/NZMSA>

- Microsoft Zero Trust documentation: <https://learn.microsoft.com/en-us/security/zero-trust/>

By adopting the Zero Trust Rapid Modernization Plan, organizations can accelerate their journey towards a more secure and resilient IT environment aligned with Zero Trust principles. This can lead to significant security improvements, increased operational efficiency, and improved user experience.

References

[SC-100: Microsoft Cybersecurity Architect \(Pearson Practice Test\) - O'Reilly Online Learning \(oreilly.com\)](#)

<https://learn.microsoft.com/en-us/shows/exam-readiness-zone/preparing-for-sc-100-design-solutions-that-align-with-security-best-practices-and-priorities>

[Configure encryption at rest \(linkedin.com\)](#)