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 4

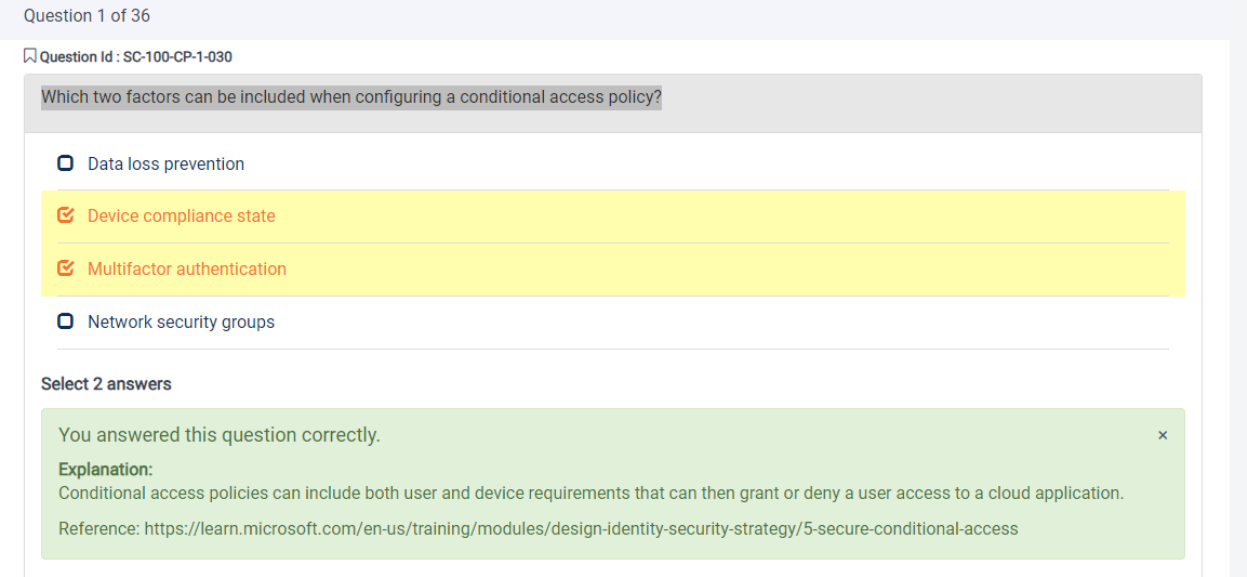
1. Factors included in Conditional Access 4
2. Entitle Management 4
3. The Cloud Adoption Framework (CAF) 5
4. Microsoft Sentinel – Enable relevant data connectors 5
5. Azure Arc 6
6. Entitle Management 6
7. Microsoft Cybersecurity Reference Architecture (MCRA) 7
8. Network Security Groups 7
9. Application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

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

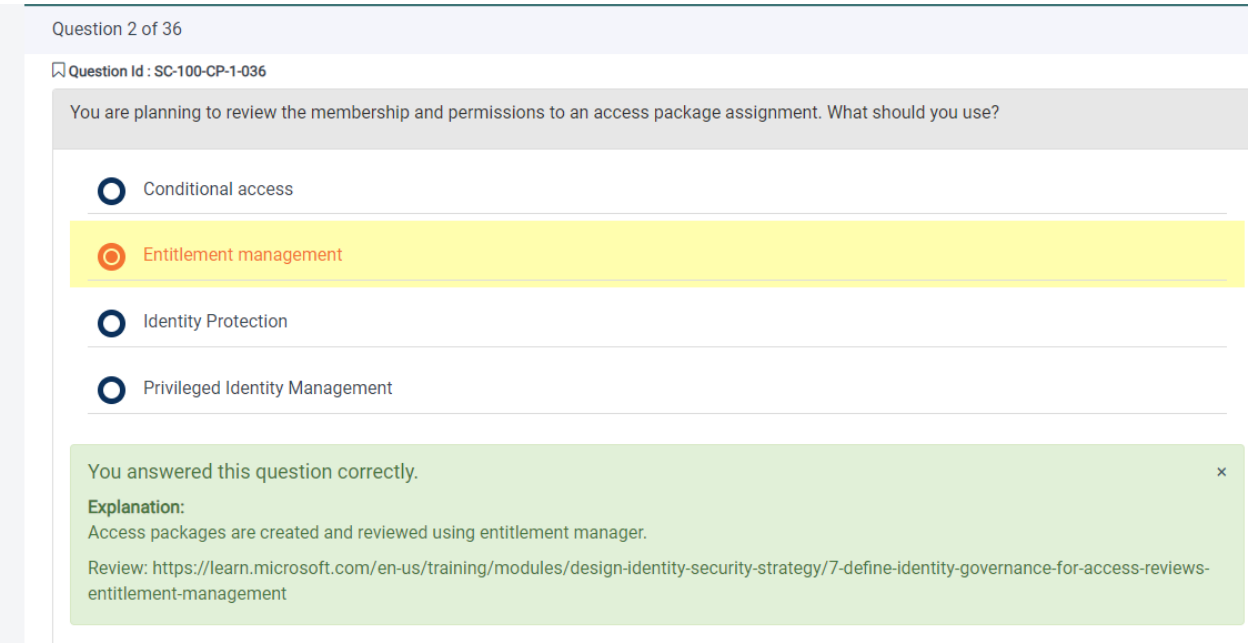
17. Operational compliance processes and the appropriate tools 29
Objective 3 - Design security for infrastructure 30
1. The Security Compliance Toolkit 30
2. Key Vault Contributor 30
3. Shared access signatures 31
4. Remote Connectivity Options 34
5. Access to Azure SQL Database using private endpoints on a virtual network 39
Next 6. For Linux VMs, you can deploy the Defender for Endpoint agent 48
7. Azure Policy 49
8. System-assigned managed identity 49
9. App protection policy 50
10. Enroll the device 50
11. Defender for Cloud 51
12. Azure disk encryption 51
13. Security baseline 52
14. Defender for Identity 52
15. Security baseline 52
16. Defender for Cloud and vulnerability assessments 53
17. Security baseline 53
References 53

Objective 1: Design a Zero Trust strategy and architecture

1. Factors included in Conditional Access



2. Entitle 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. ×

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. ×

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. ×

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. ×

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 _____ 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

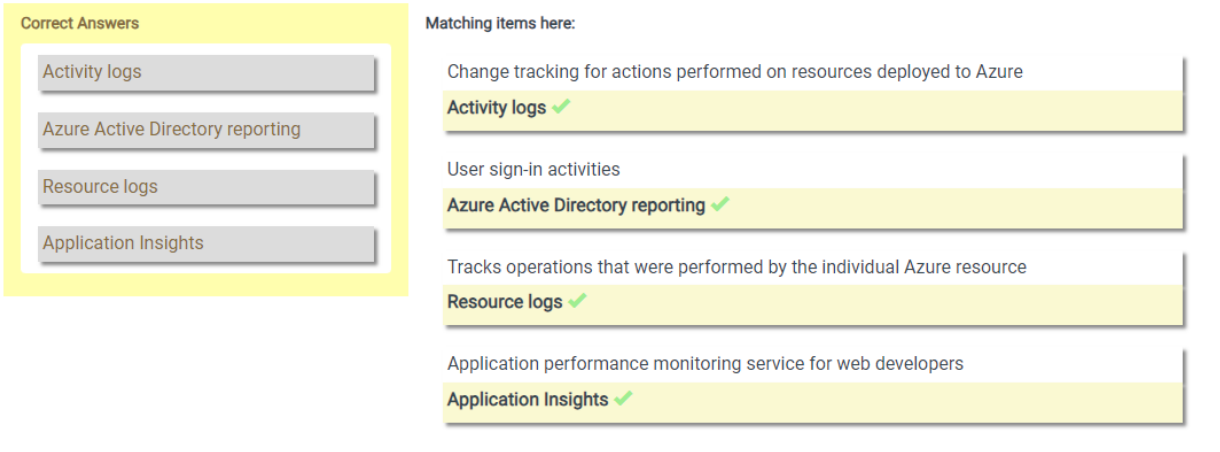
You answered this question correctly. ×

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.



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?

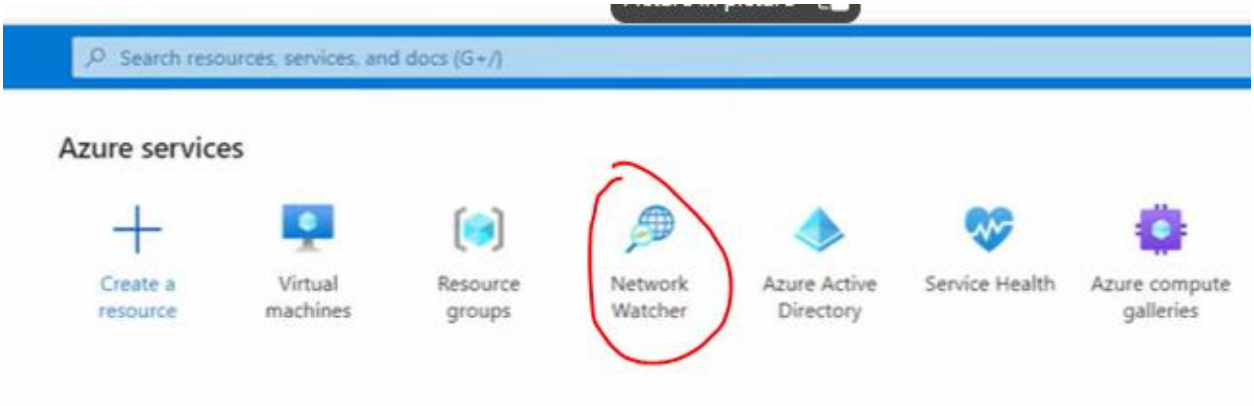
- Diagnostic logging
- Log Analytics
- Network Security Group flow logs
- Network Watcher

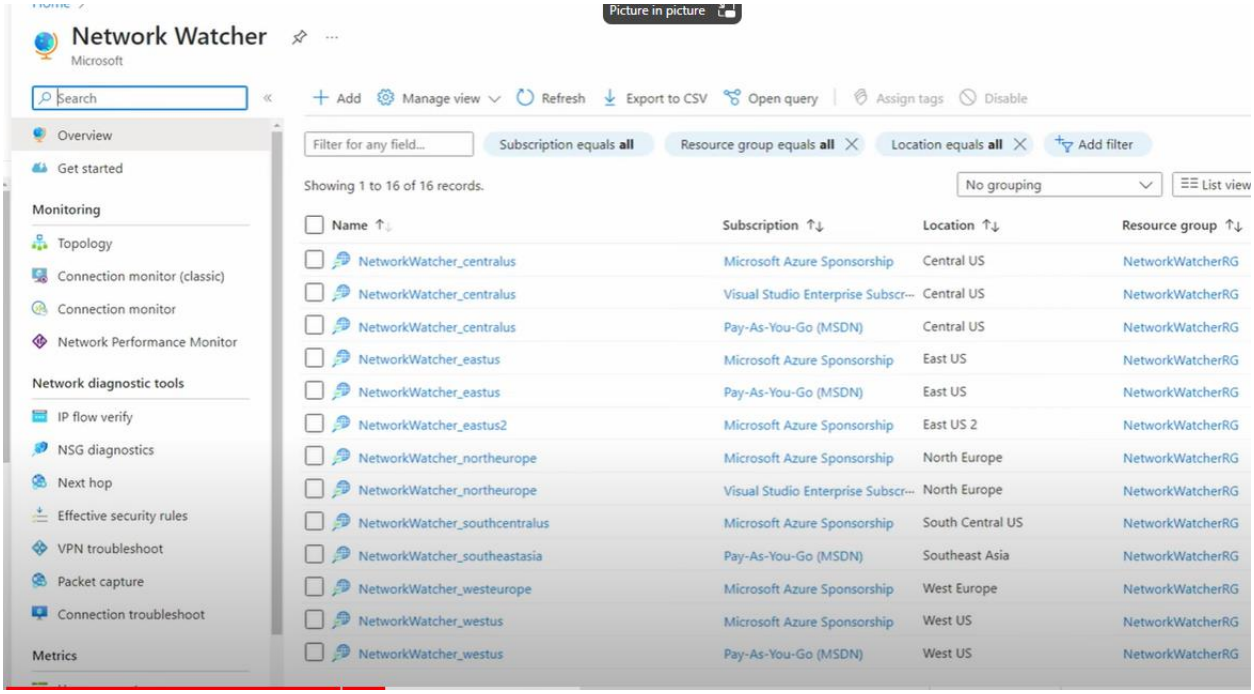
You answered this question correctly. ×

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]





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

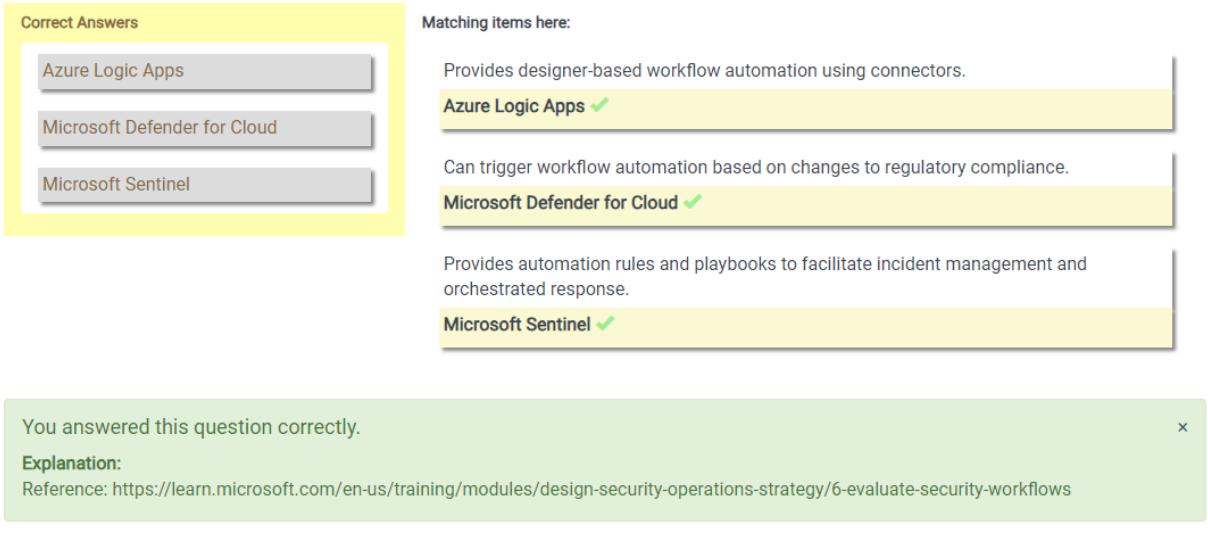
You answered this question correctly. ×

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.



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?

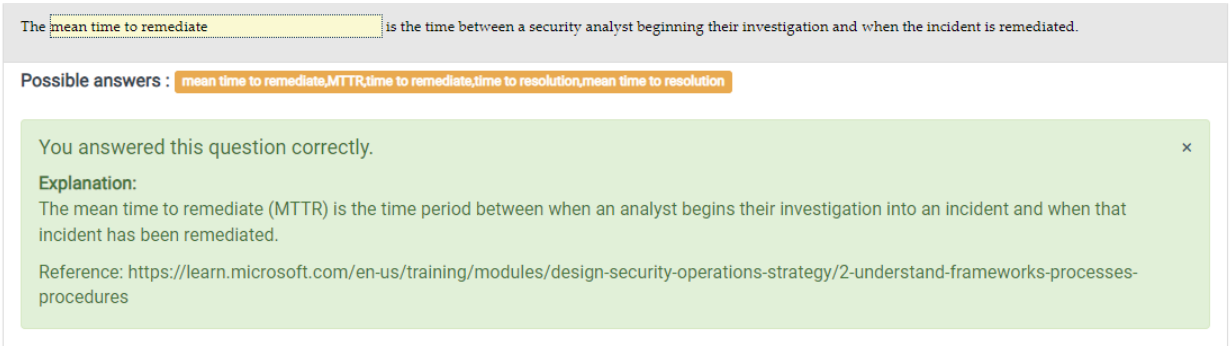
- Conditional access
- Custom attributes
- Identity Protection
- Privileged Identity Management

You answered this question correctly. ×

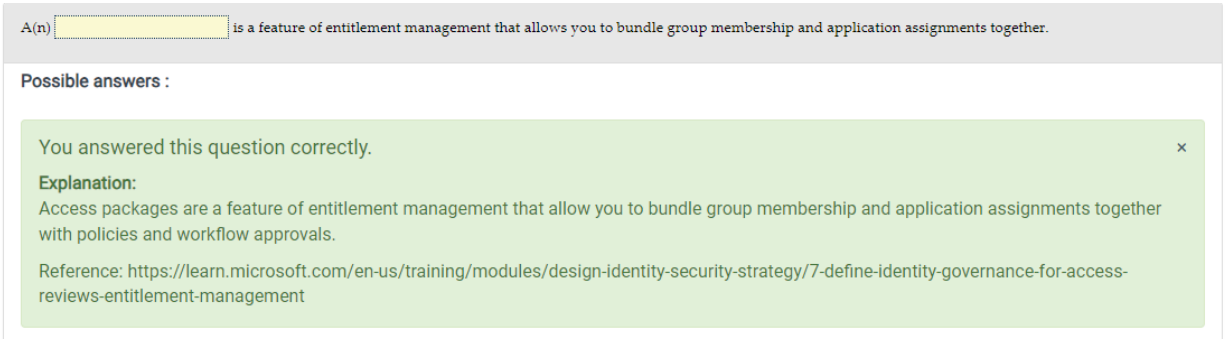
Explanation:
Privileged Identity Management allows you to make roles eligible for assignment and then, when they are activated, the roles are only assigned for a configurable amount of time.

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

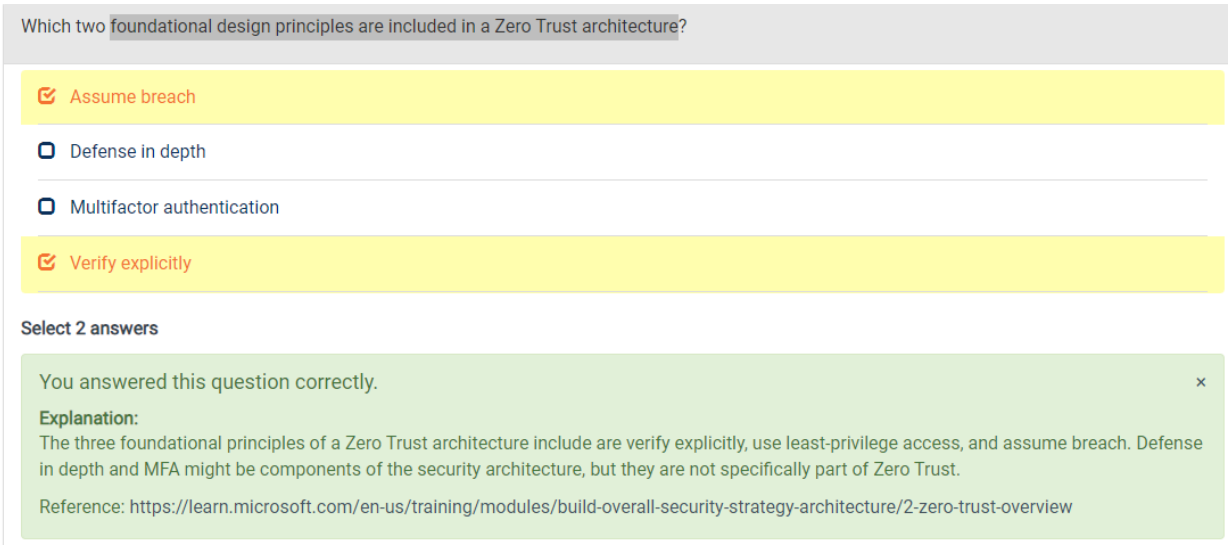
22. The mean time to remediate (MTTR)



23. Access Packages



24. Foundational design principles included in a Zero Trust architecture



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. ×

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?

- [x] 10.10.0.0/16
- [ ] 169.254.0.0/16
- [x] 172.16.0.0/16
- [ ] 172.50.0.0/16

Select 2 answers

You answered this question correctly. ×

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

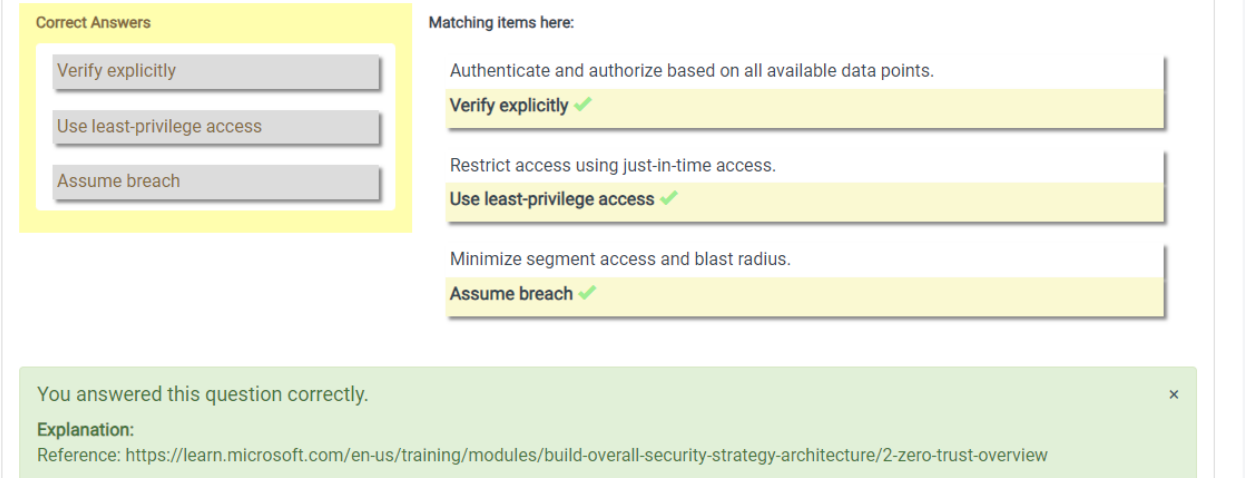
You answered this question correctly. ×

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.



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 associates 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

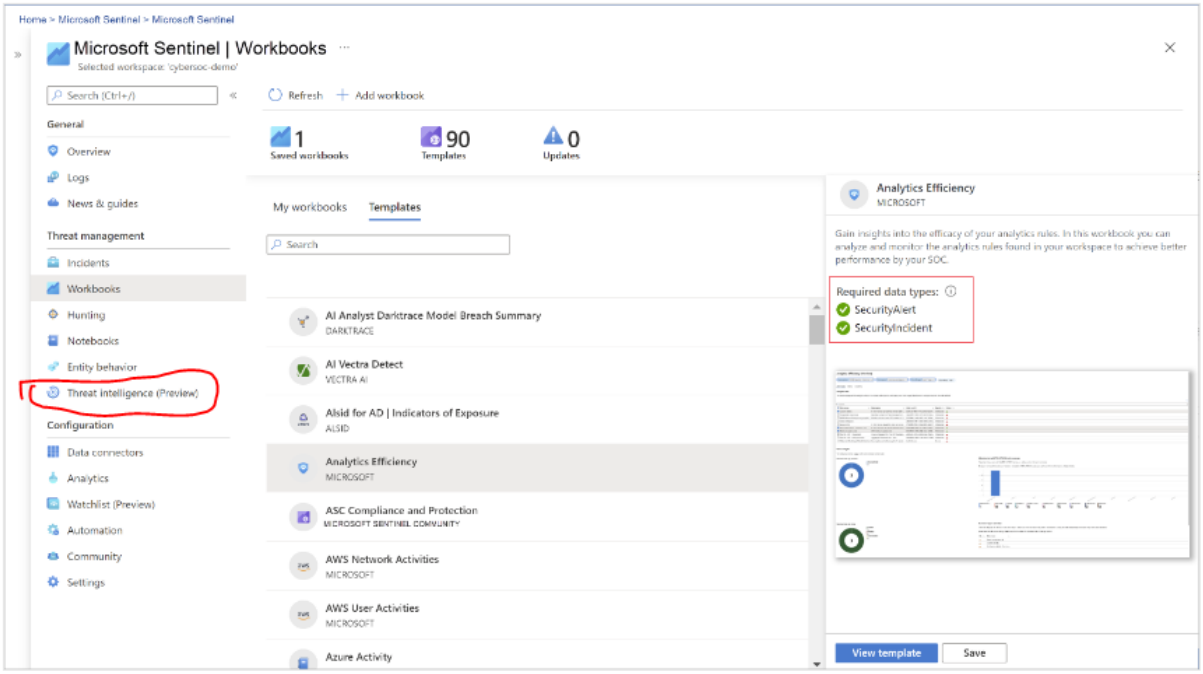
4. Threat intelligence in Sentinel

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?

- [x] Append
- [ ] Audit
- [ ] AuditIfNotExist
- [x] DeployIfNotExist

Select 2 answers

You answered this question correctly.

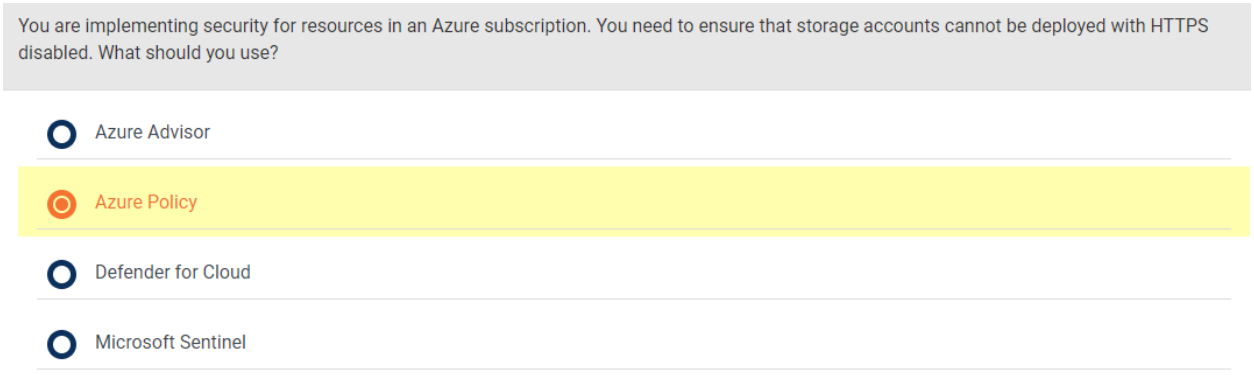
Explanation:
Azure Policy enables you to create guardrails for your environment, including being able alter or add to a deployment when the request is submitted with the Modify, Append, or DeployIfNotExist policy effects.

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

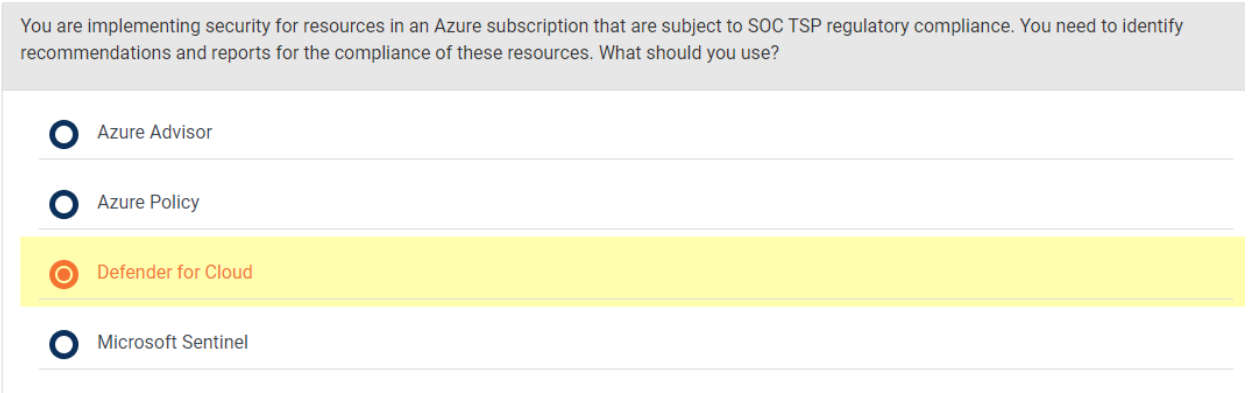
6. Azure Policy



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

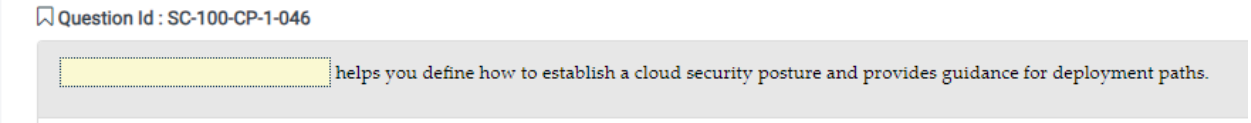
7. Defender for Cloud



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

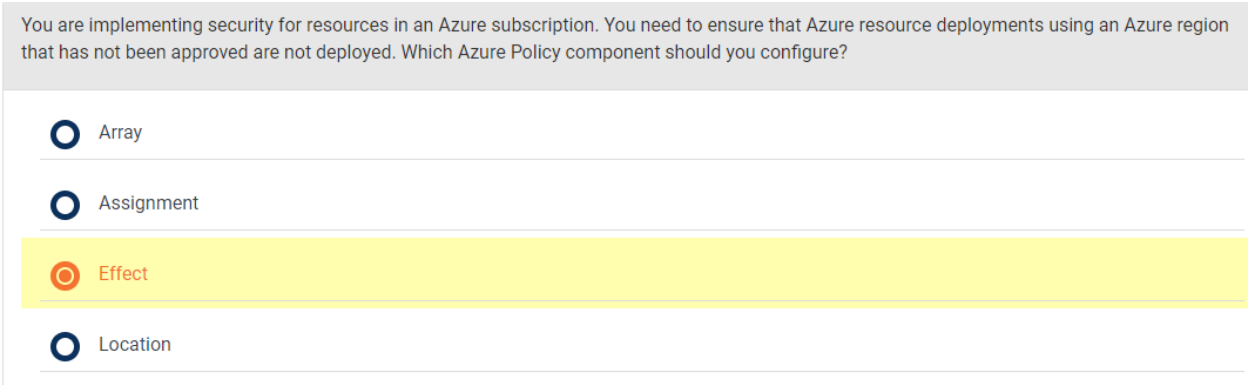
8. Rapid Modernization Plan (RaMP)



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

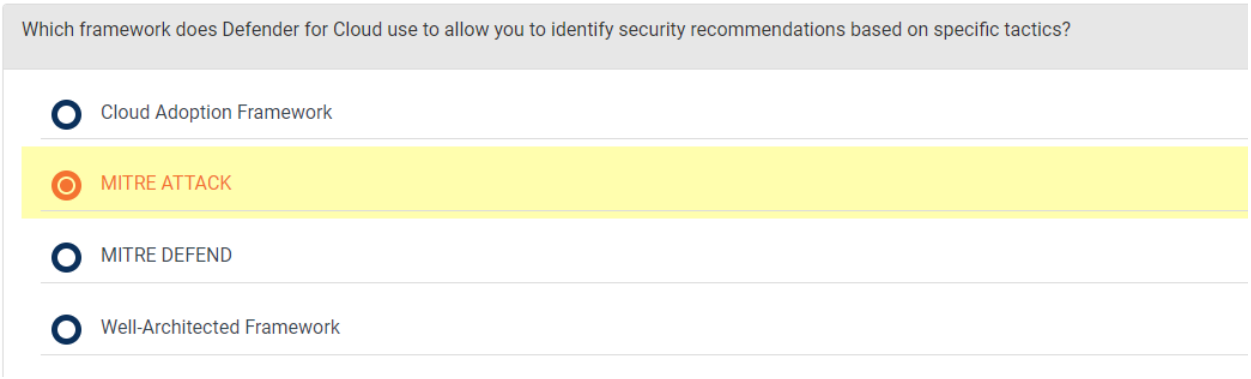
9. Azure Policy Effects



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.

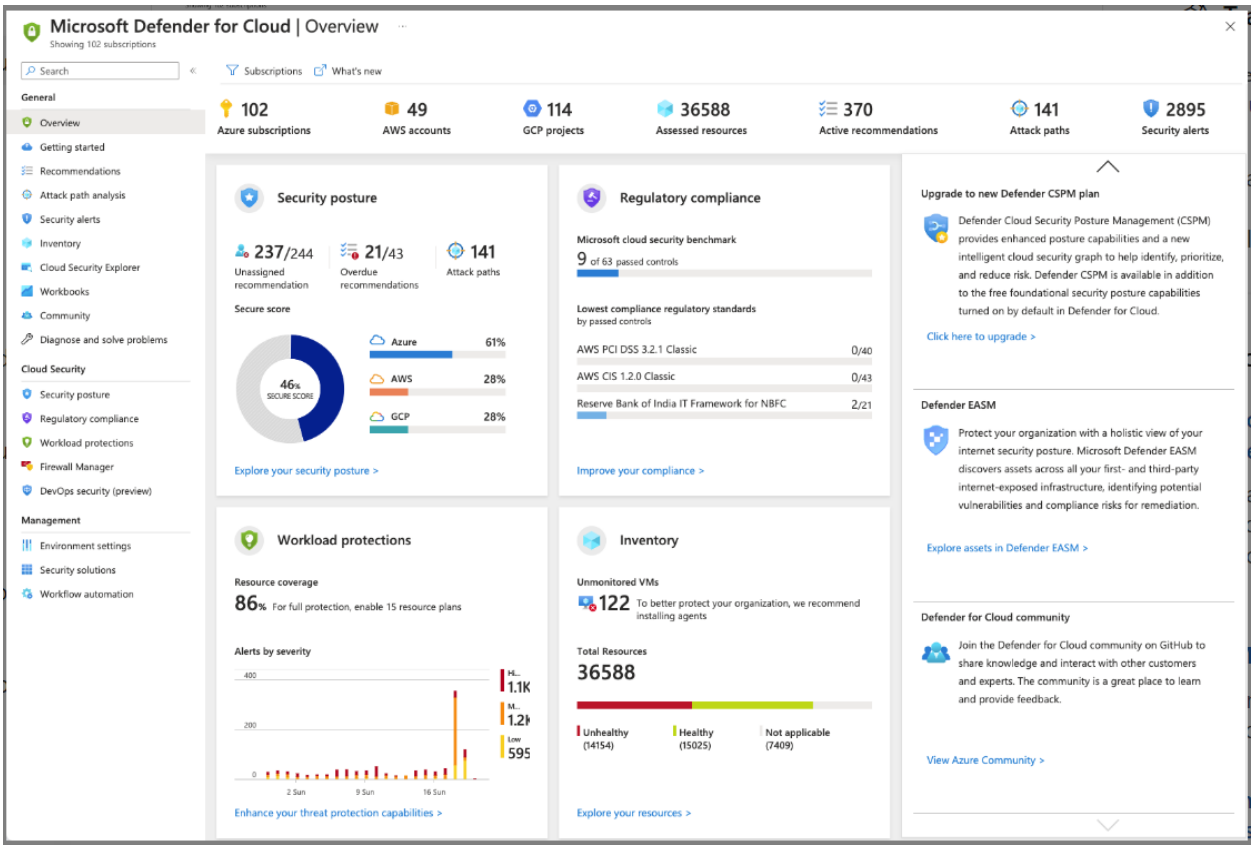
Reference: https://learn.microsoft.com/en-us/training/modules/evaluate-regulatory-compliance-strategy/5-design-validate-implementation-of-azure-policy

10. Defender for Cloud uses MITTRE ATTACK framework



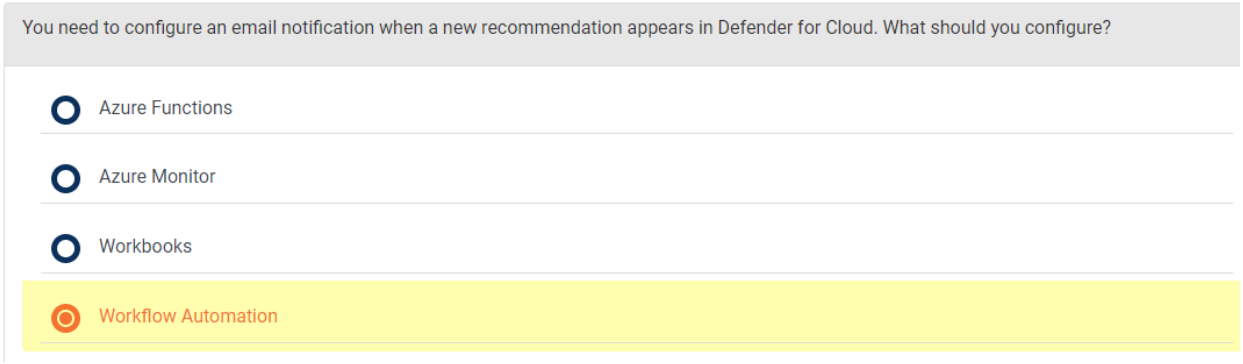
Defender for Cloud correlates recommendations to increase your security posture and provides a reference to the MITRE Attack framework for these recommendations.

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



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

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

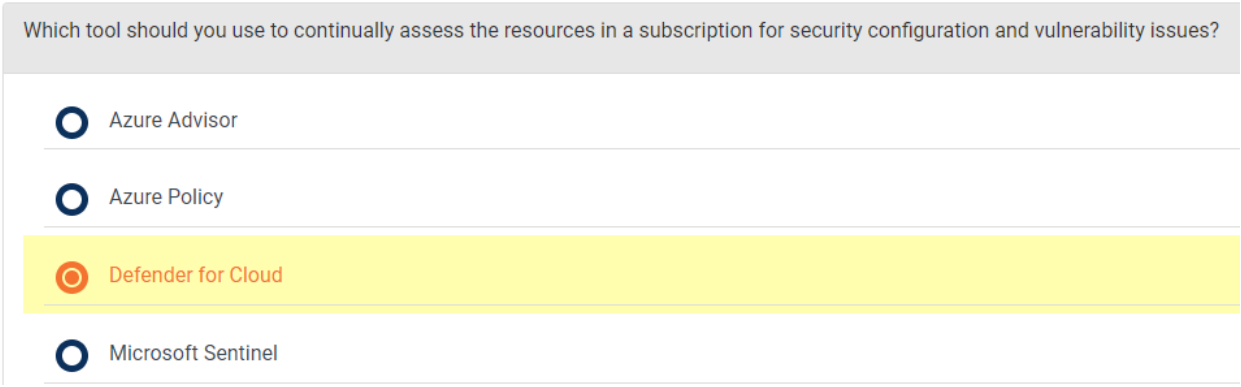
15. Azure Landing Zone

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

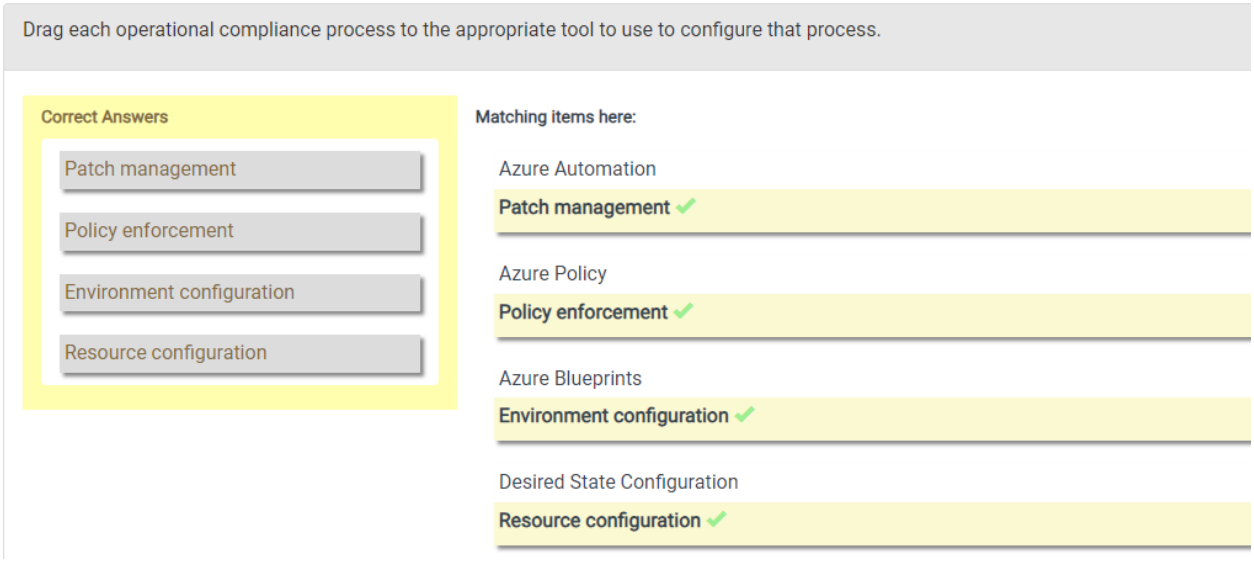
16. Defender for Cloud provides continual assessment



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

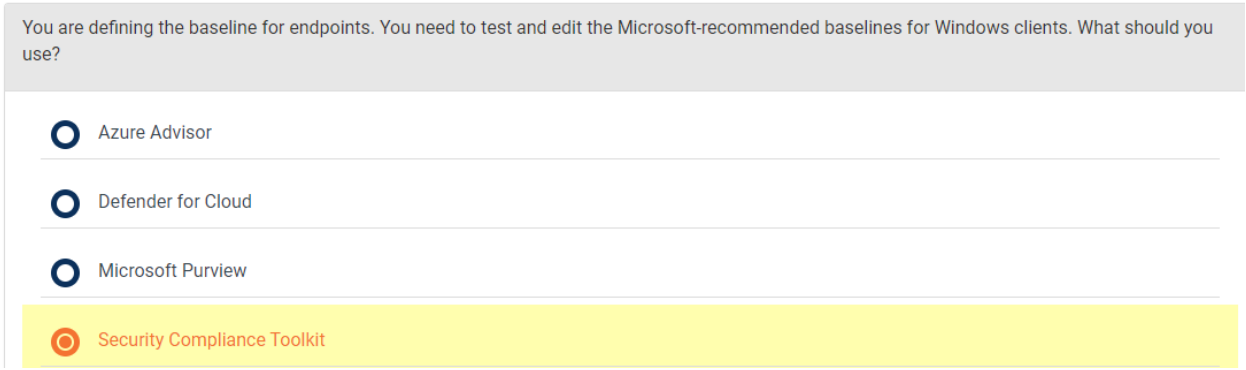
17. Operational compliance processes and the appropriate tools



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

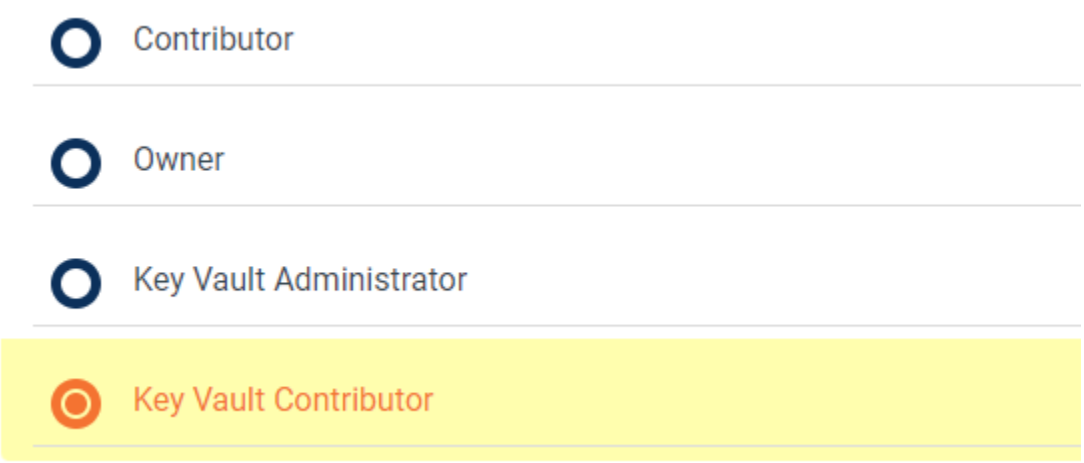
1. The Security Compliance Toolkit



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

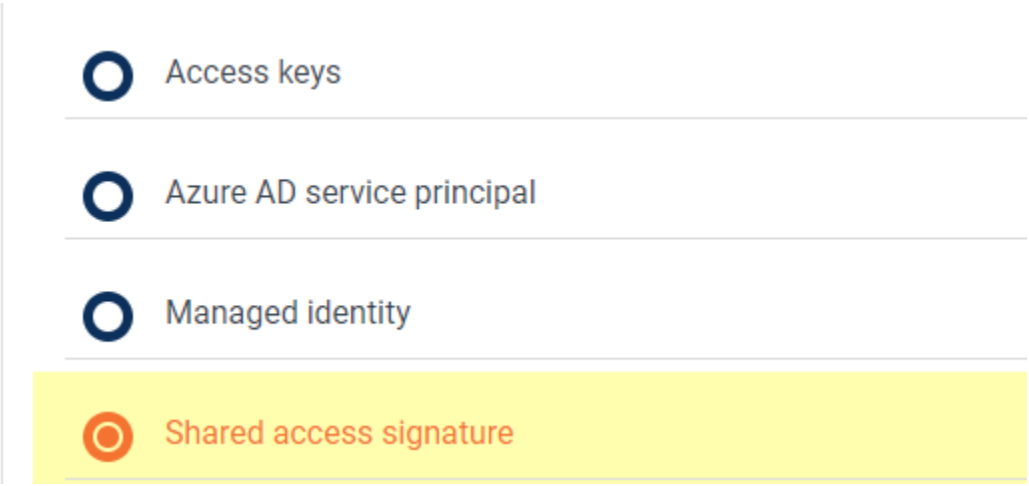
2. Key Vault Contributor



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

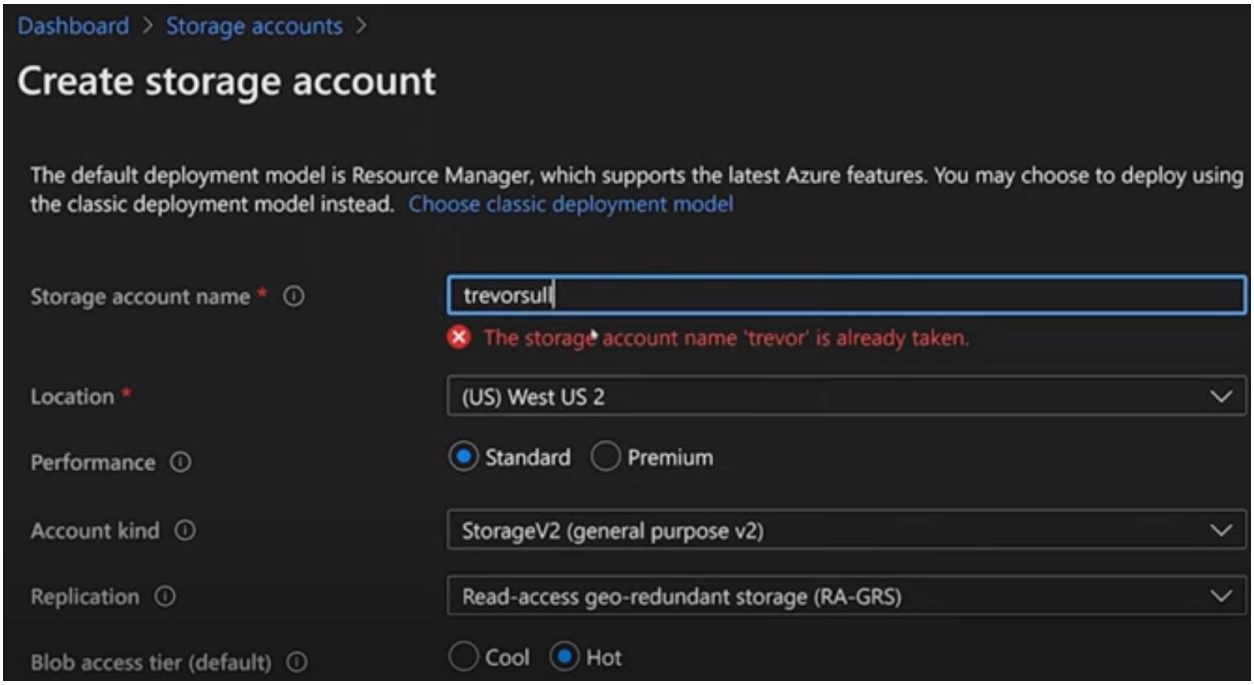
Reference: https://learn.microsoft.com/en-us/training/modules/design-strategy-for-secure-server-client-endpoints/6-design-strategy-manage-secrets-keys-certificates

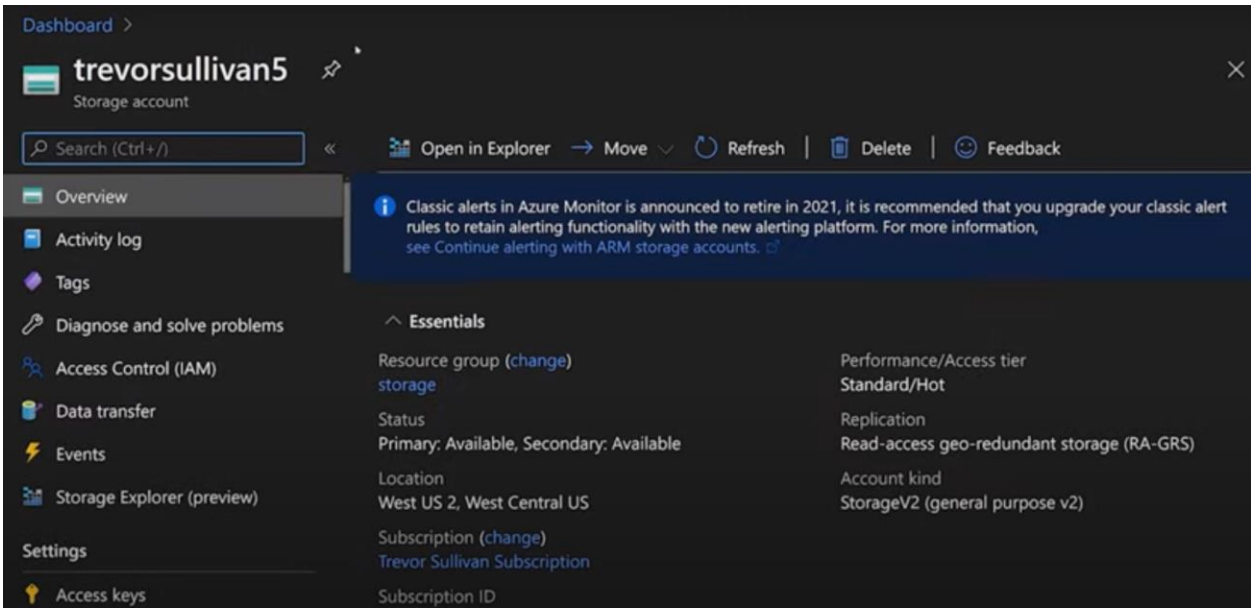
3. Shared access signatures

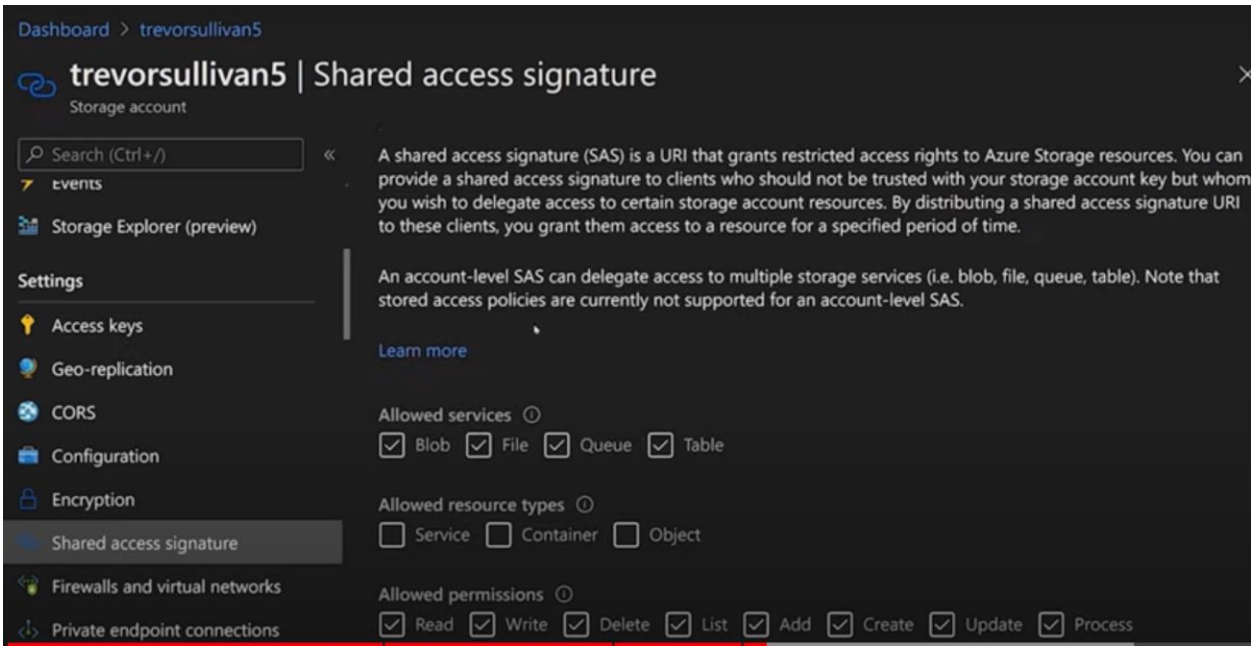


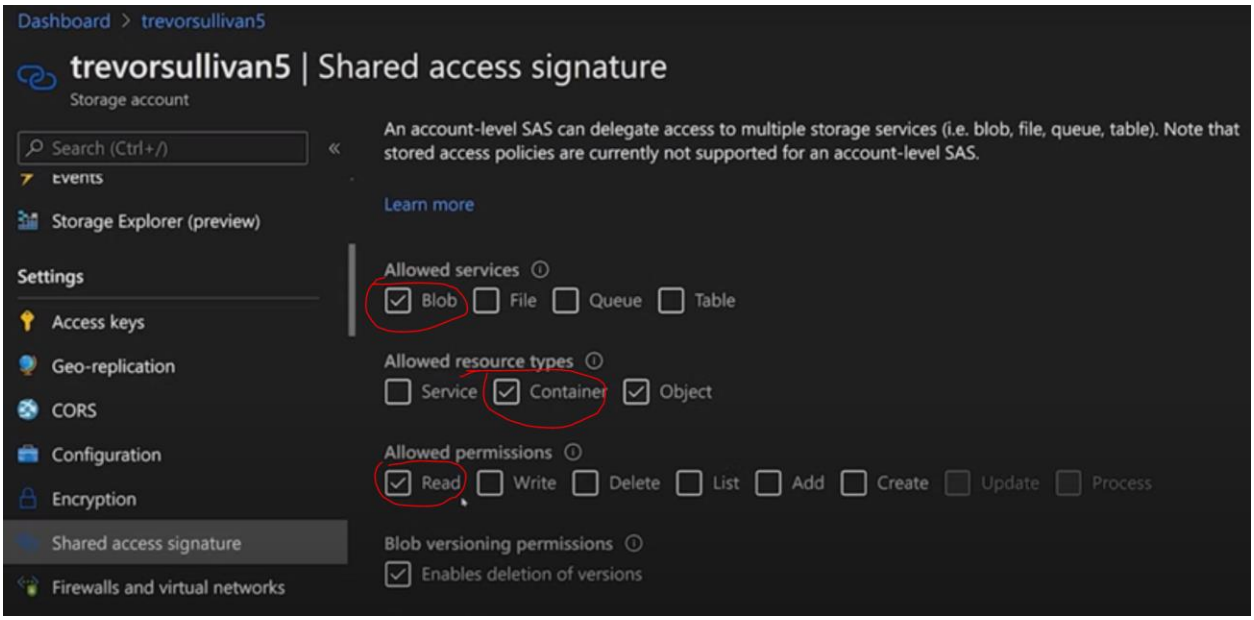
A shared access signature (SAS) in a storage account can be set with an expiration date so that a new SAS token is required to access the storage account.

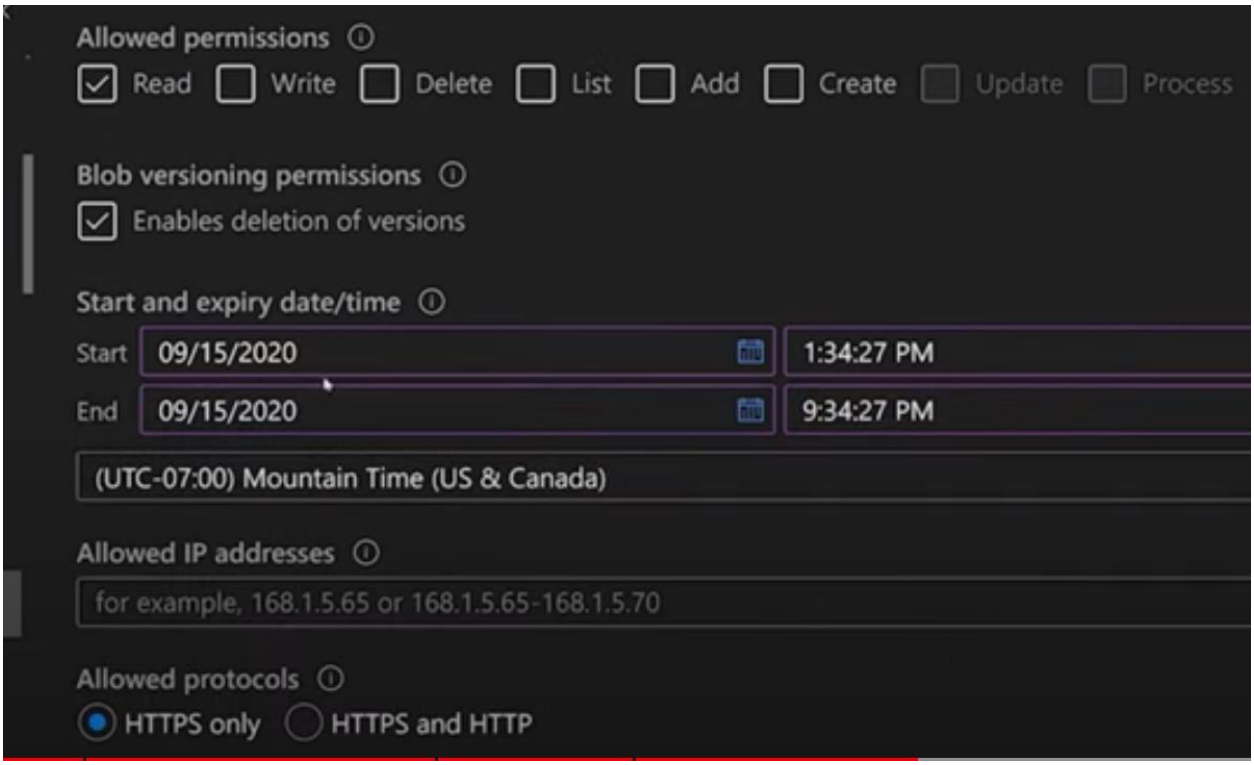
Reference: https://learn.microsoft.com/en-us/training/modules/design-strategy-for-secure-paas-iaas-saas-services/8-specify-security-requirements-for-storage-workloads

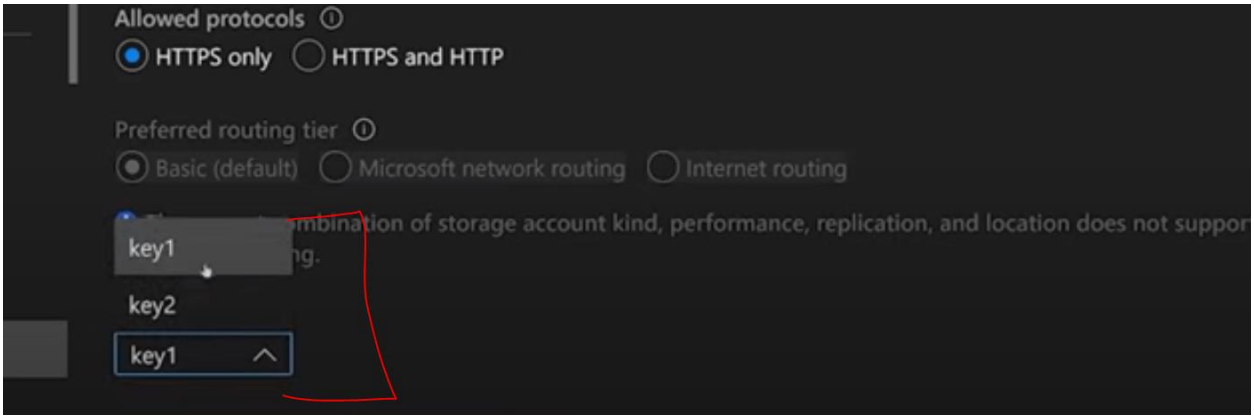


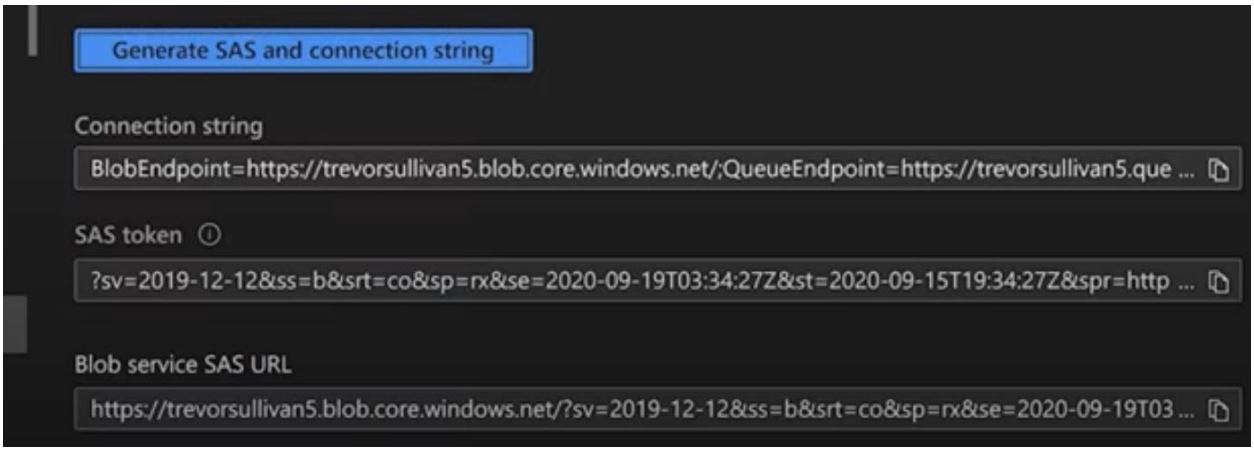

Dashboard
trevorsullivan5
Storage account
Search (Ctrl+/)
Open in Explorer
Move
Refresh
Delete
Feedback
Overview
Activity log
Tags
Diagnose and solve problems
Access Control (IAM)
Data transfer
Events
Storage Explorer (preview)
Settings
Access keys
Classic alerts in Azure Monitor is announced to retire 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.
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)


Dashboard
trevorsullivan5
trevorsullivan5 | Shared access signature
Storage account
Search (Ctrl+/)
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

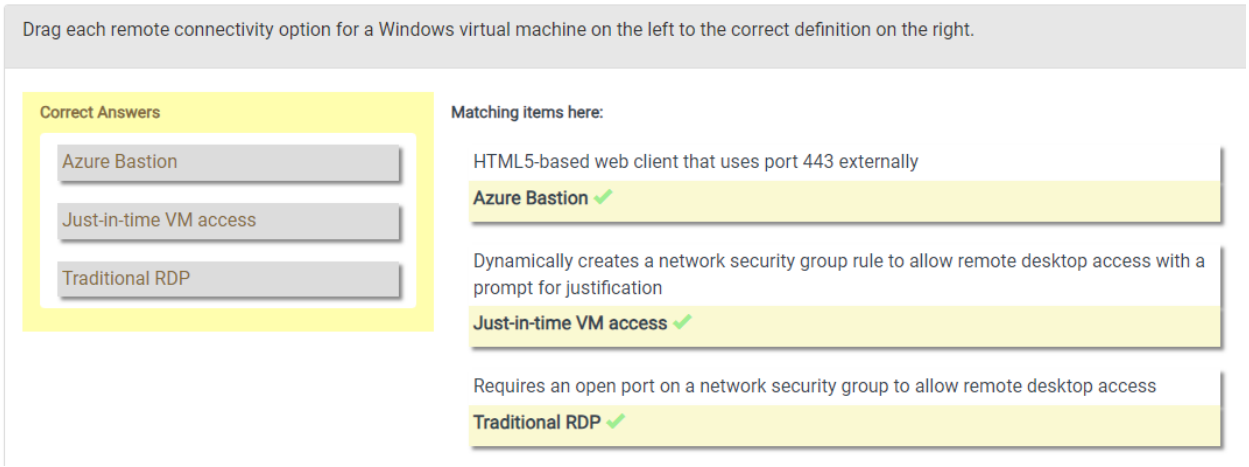

Allowed permissions
Read
Write
Delete
List
Add
Create
Update
Process
Blob versioning permissions
Enables deletion of versions
Start and expiry date/time
Start
09/15/2020
1:34:27 PM
End
09/15/2020
9:34:27 PM
(UTC-07:00) Mountain Time (US & Canada)
Allowed IP addresses
for example, 168.1.5.65 or 168.1.5.65-168.1.5.70
Allowed protocols
HTTPS only
HTTPS and HTTP





https://www.youtube.com/watch?v=0PX1eW1sCGg

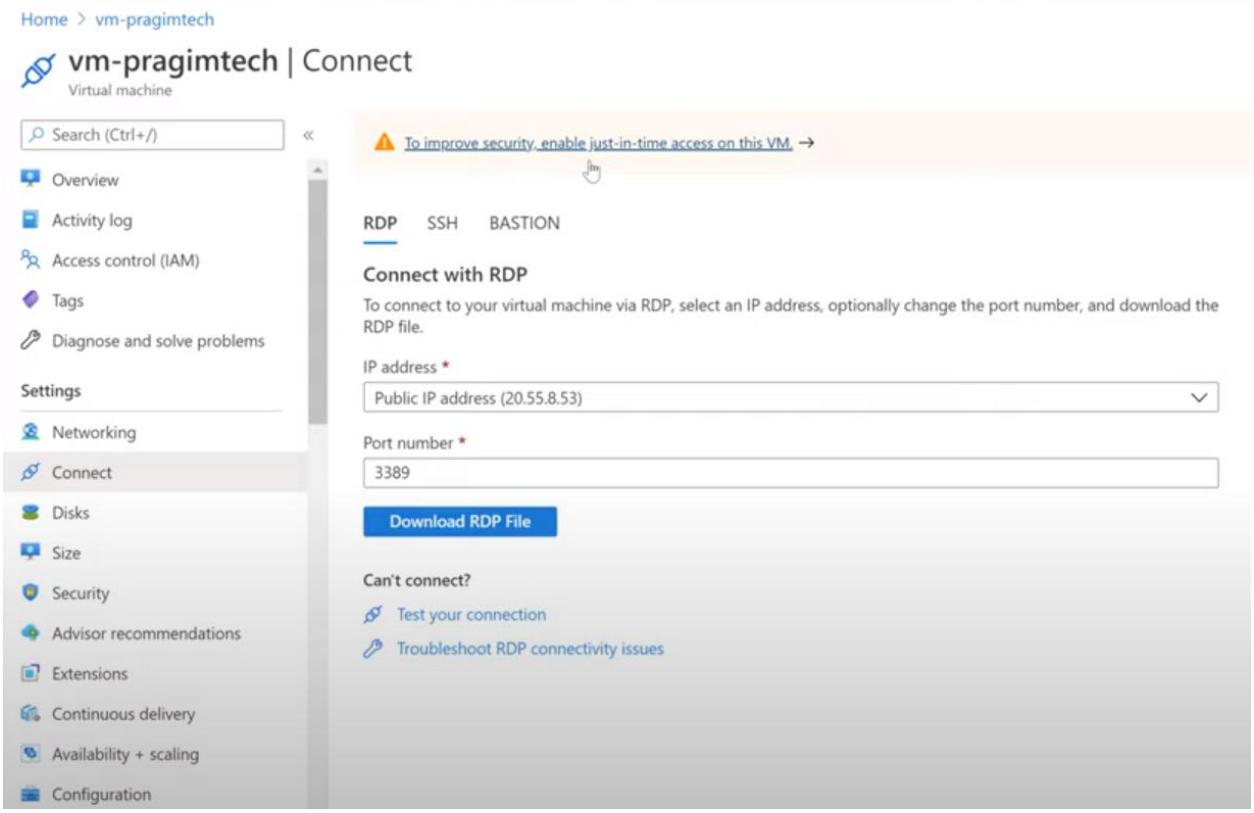
4. Remote Connectivity Options

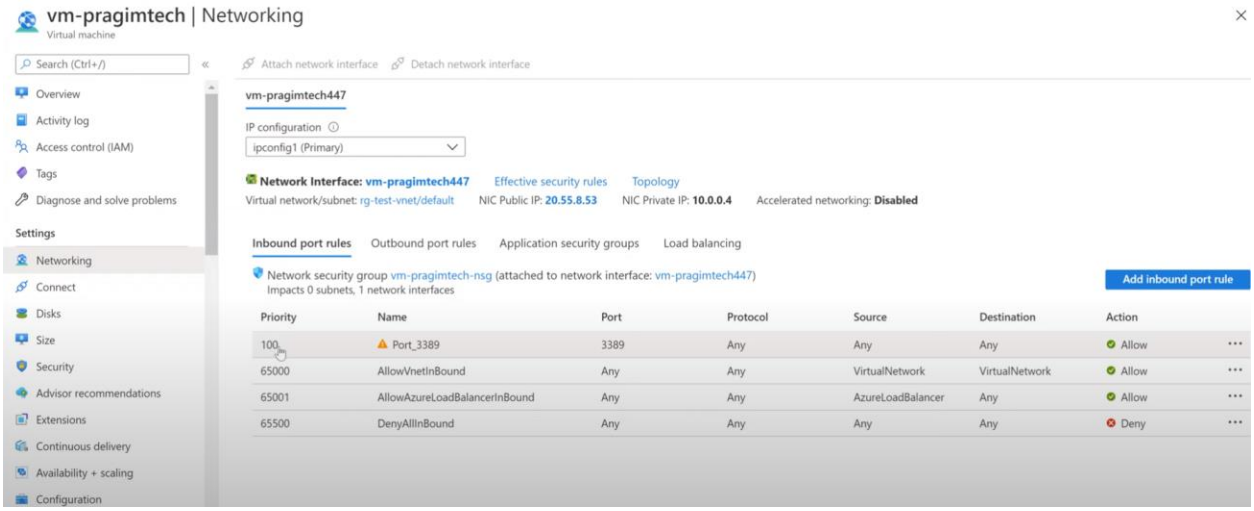


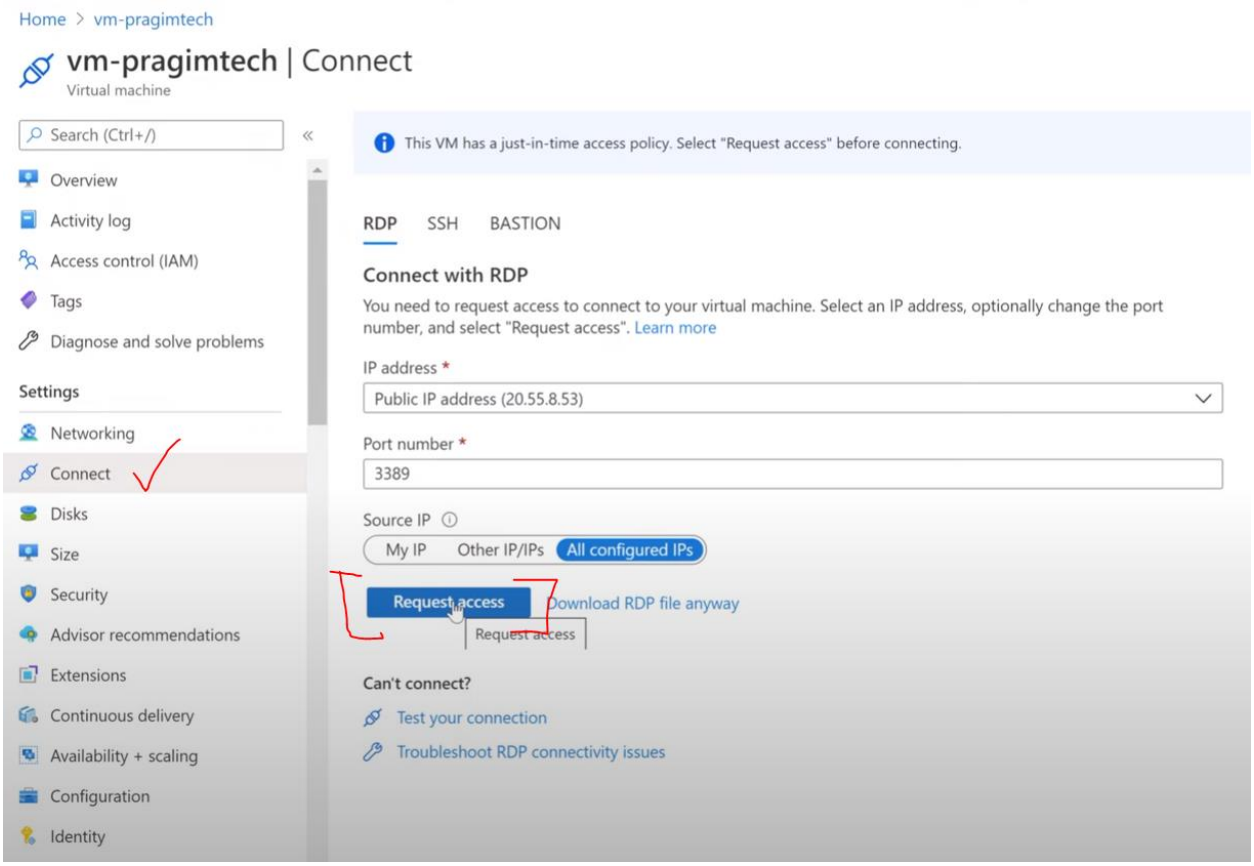
Azure Bastion uses an HTML5 connection in a web browser to remotely access the desired VM. JIT VM access, part of Defender for Servers, dynamically creates an NSG rule and has a prompt for why you are connecting to the VM. Traditional RDP requires port 3389 to be open in the NSG.

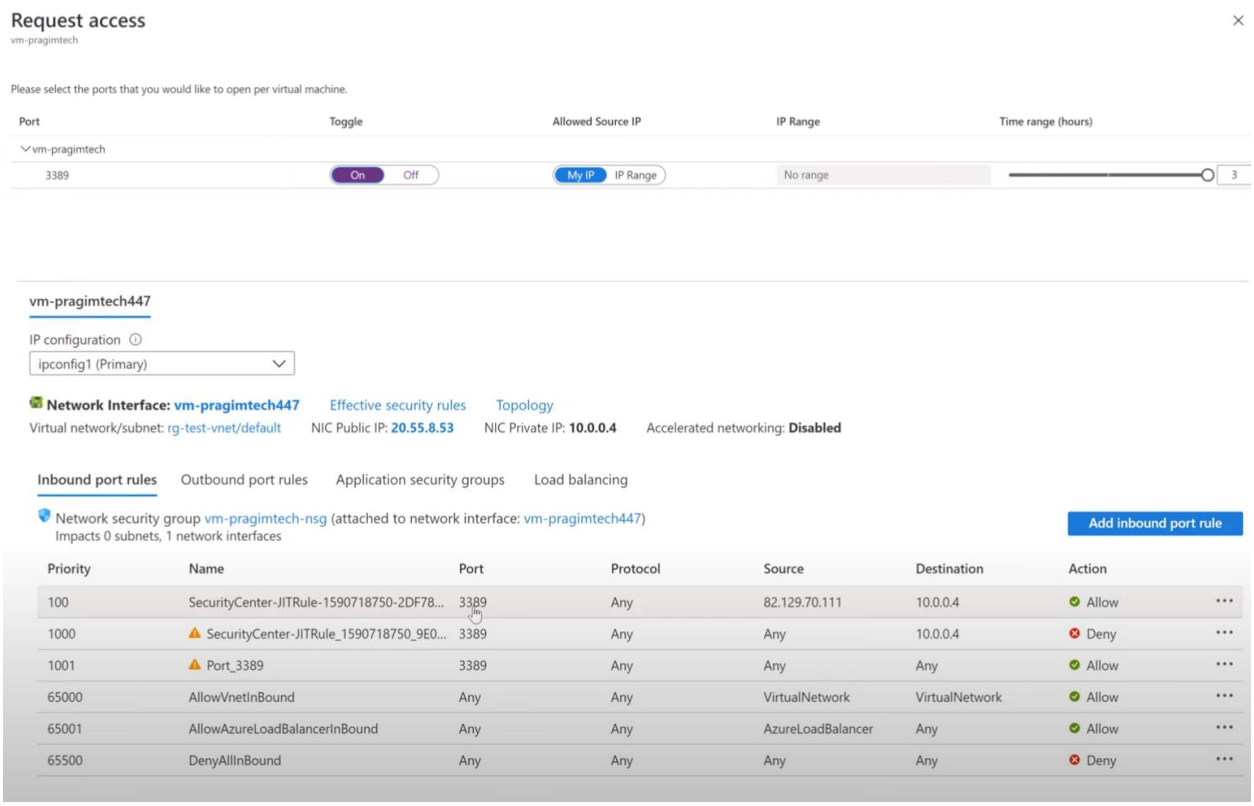
Reference: https://learn.microsoft.com/en-us/training/modules/design-strategy-for-secure-server-client-endpoints/7-secure-remote-access

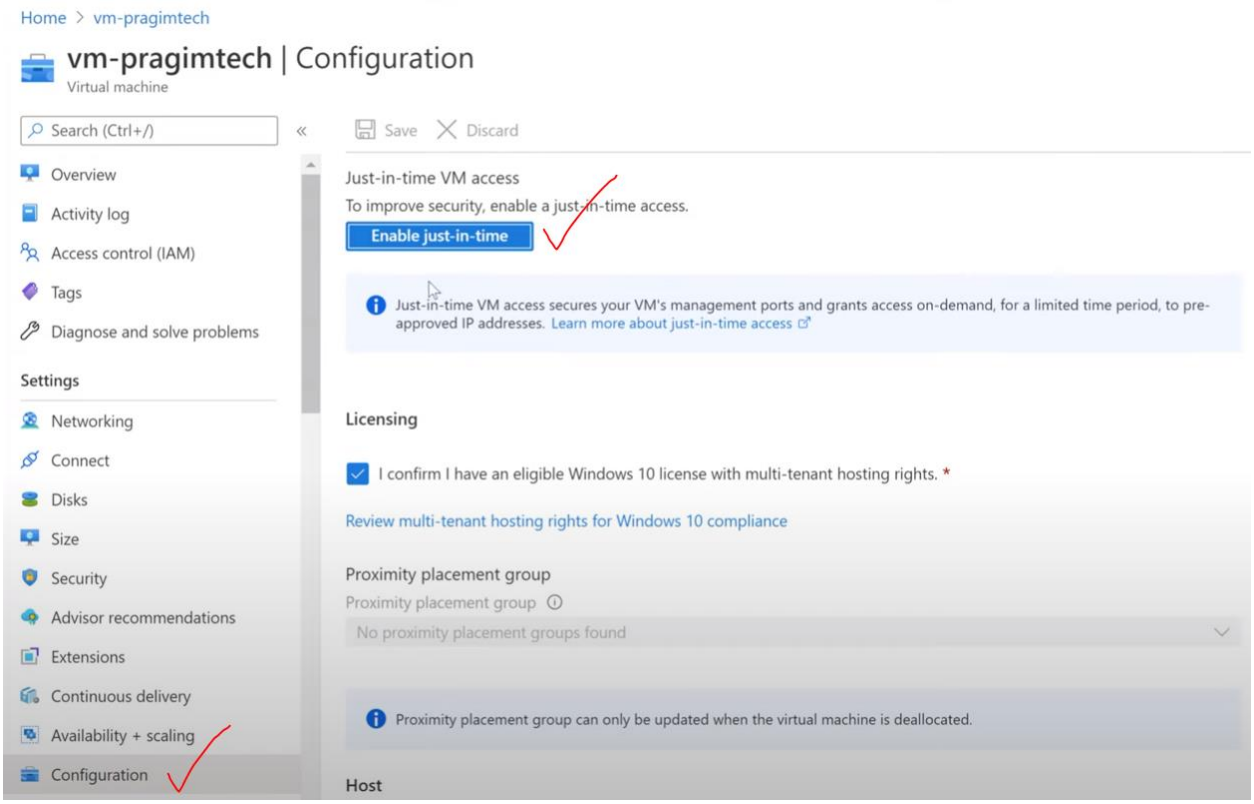
Azure vm just in time access | azure vm jit | azure jit vm access

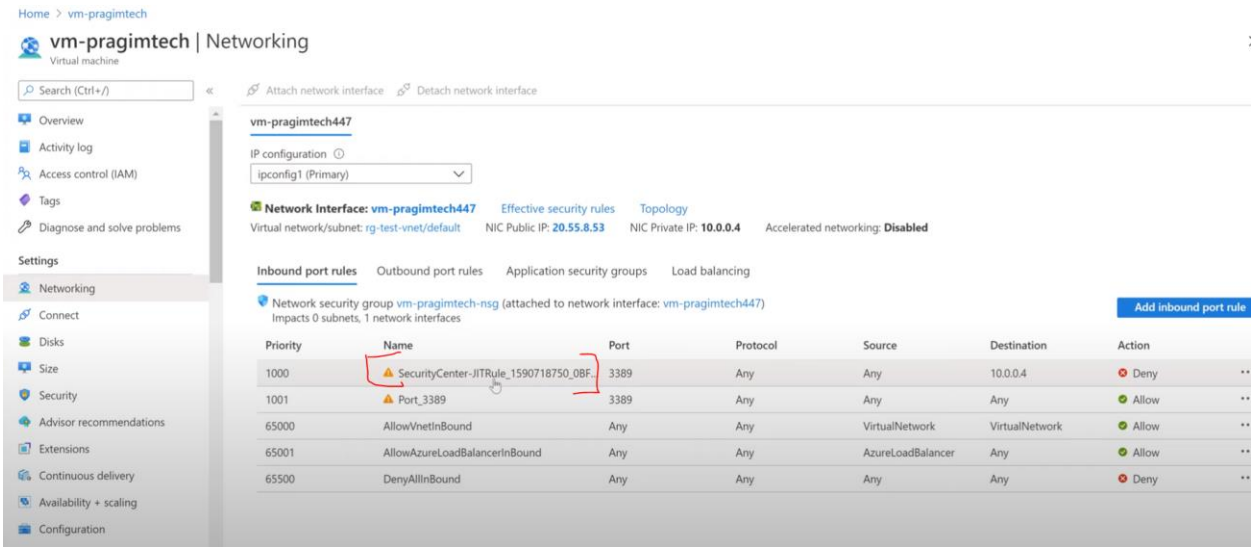



vm-pragimtech | Networking
Virtual machine
Search (Ctrl+/)
Attach network interface
Detach network interface
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Networking
Connect
Disks
Size
Security
Advisor recommendations
Extensions
Continuous delivery
Availability + 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+/)
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/IPs
All configured IPs
Request access
Download RDP file anyway
Request access
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
On
Off
My IP
IP Range
No range
3
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
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





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.

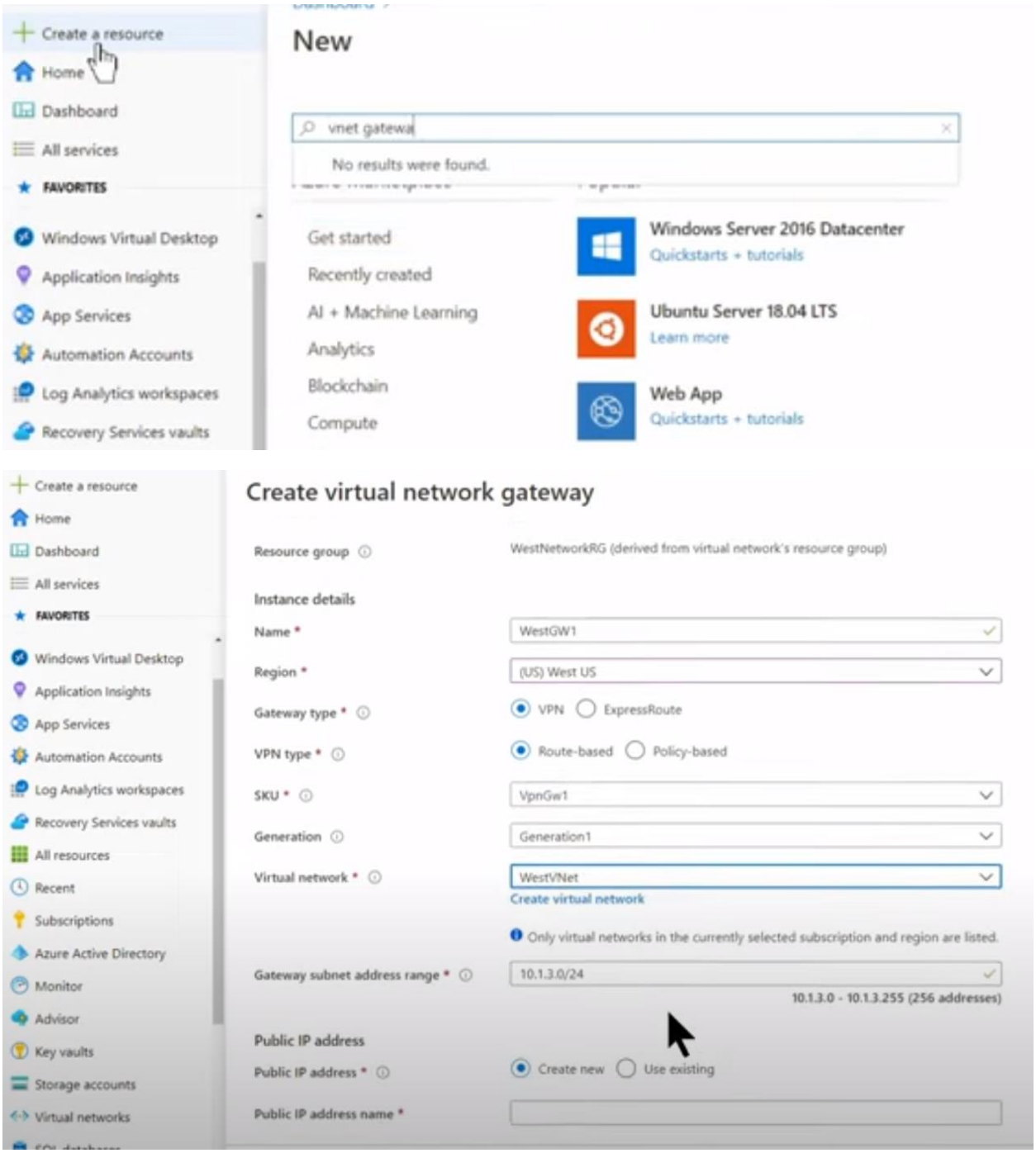
If the developer will be in different remote locations, a P2S VPN would allow the developer to connect securely regardless of their location. Because Azure SQL Database is using a private endpoint, it would not be accessible to the public and must be on the network.

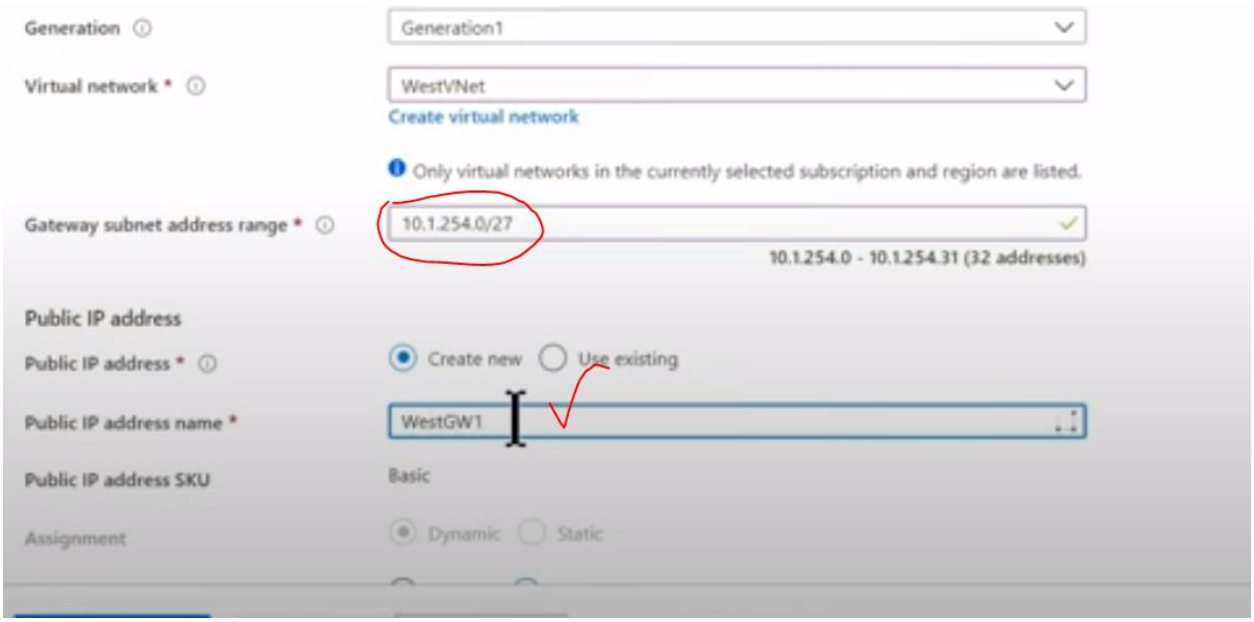
Reference: https://learn.microsoft.com/en-us/training/modules/design-strategy-for-secure-server-client-endpoints/7-secure-remote-access

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

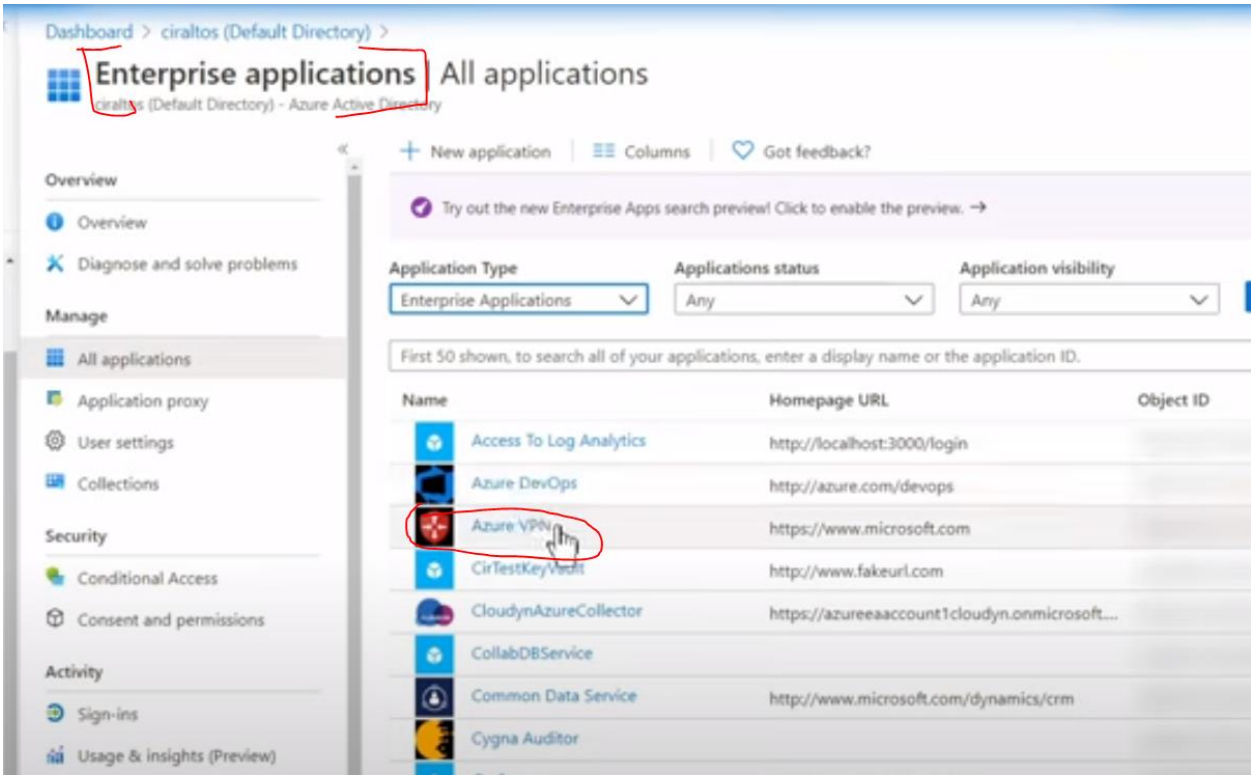
https://www.youtube.com/watch?v=Ur0WNjnXJrU

Step 1: Deploy the Gateway

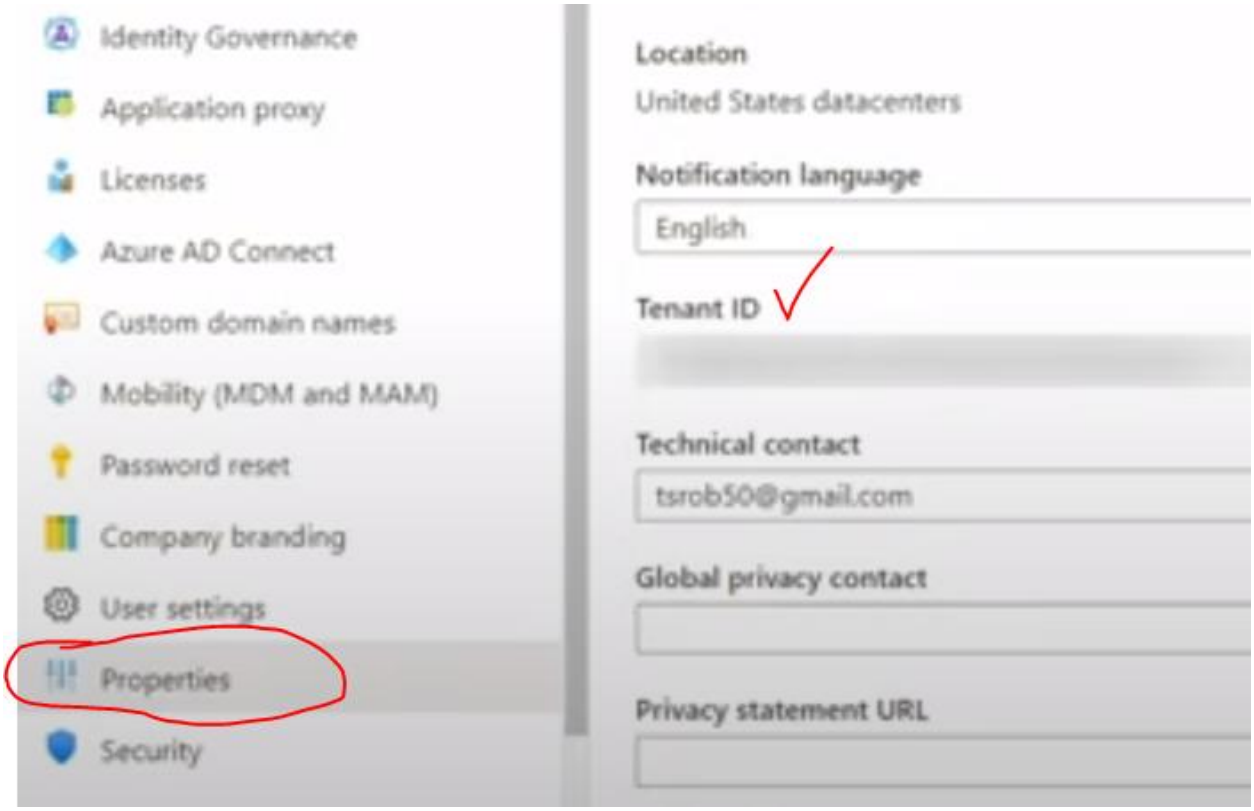

Create a resource
Home
Dashboard
All services
FAVORITES
Windows Virtual Desktop
Application Insights
App Services
Automation Accounts
Log Analytics workspaces
Recovery Services vaults
New
vnet gatewa
No results were found.
Get started
Recently created
AI + Machine Learning
Analytics
Blockchain
Compute
Windows Server 2016 Datacenter
Quickstarts + tutorials
Ubuntu Server 18.04 LTS
Learn more
Web App
Quickstarts + tutorials
Create a resource
Home
Dashboard
All services
FAVORITES
Windows Virtual Desktop
Application Insights
App Services
Automation Accounts
Log Analytics workspaces
Recovery Services vaults
All resources
Recent
Subscriptions
Azure Active Directory
Monitor
Advisor
Key vaults
Storage accounts
Virtual networks
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 *



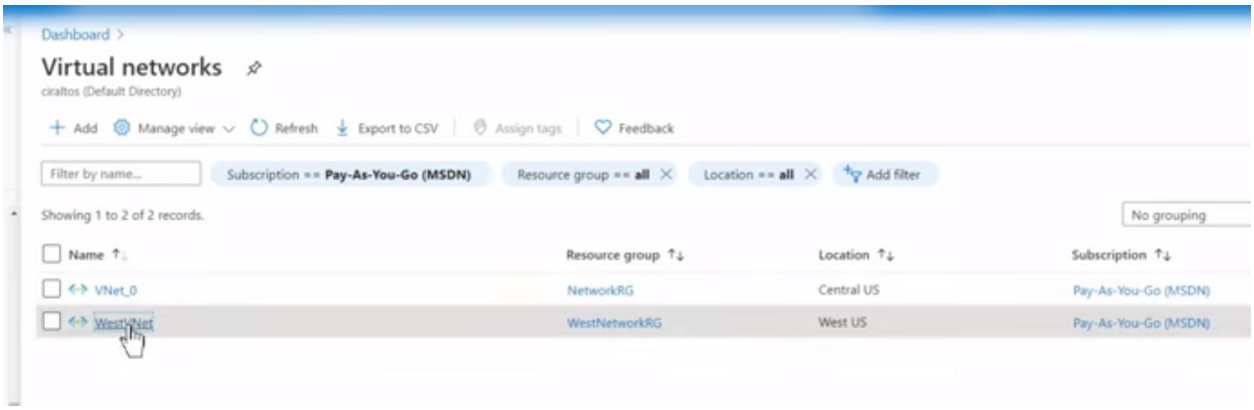
Step 2: Give admin consent



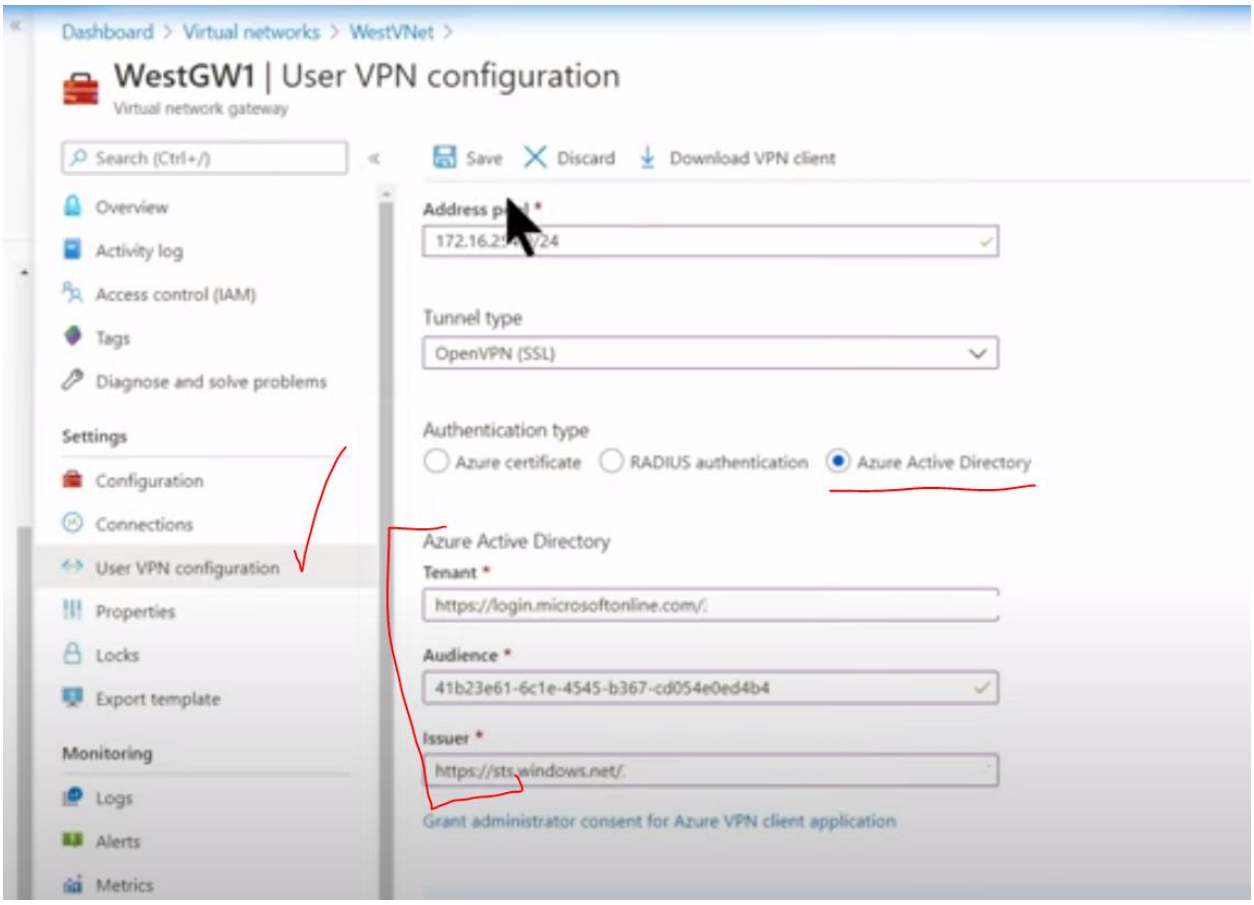
Need the tenant ID



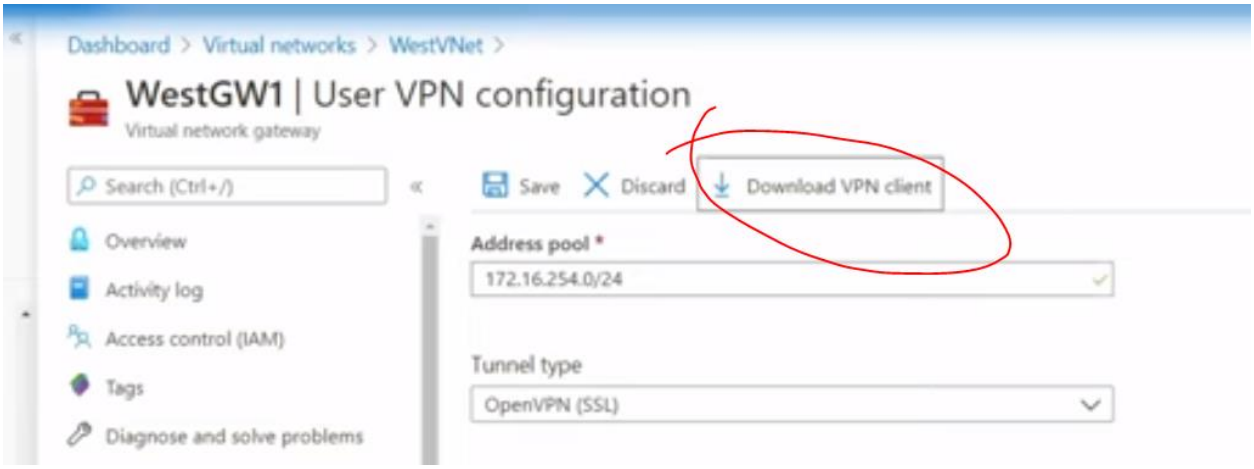
Step 3: Create the P2S Connection

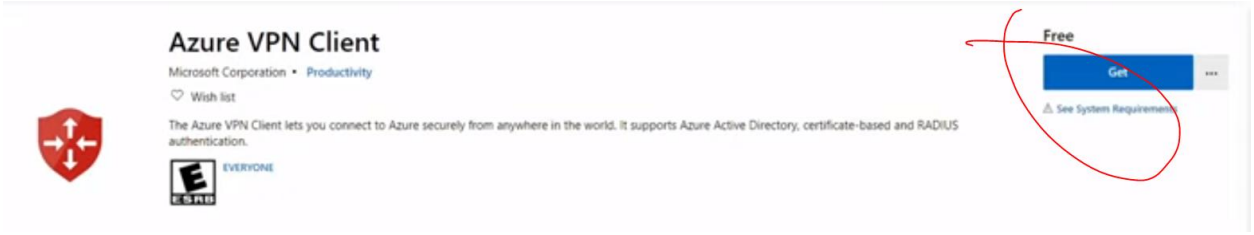


The above is the Vnet where we created the Gateway.

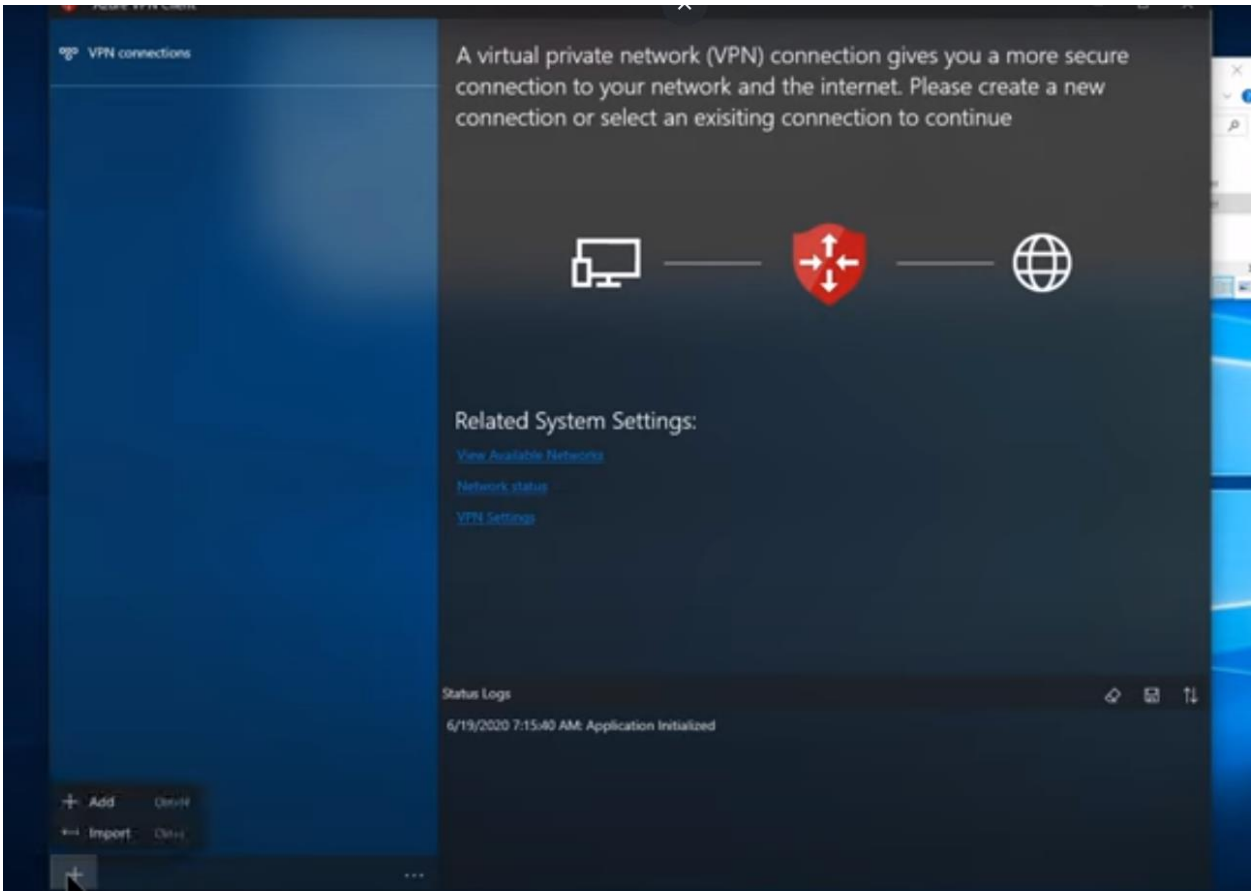


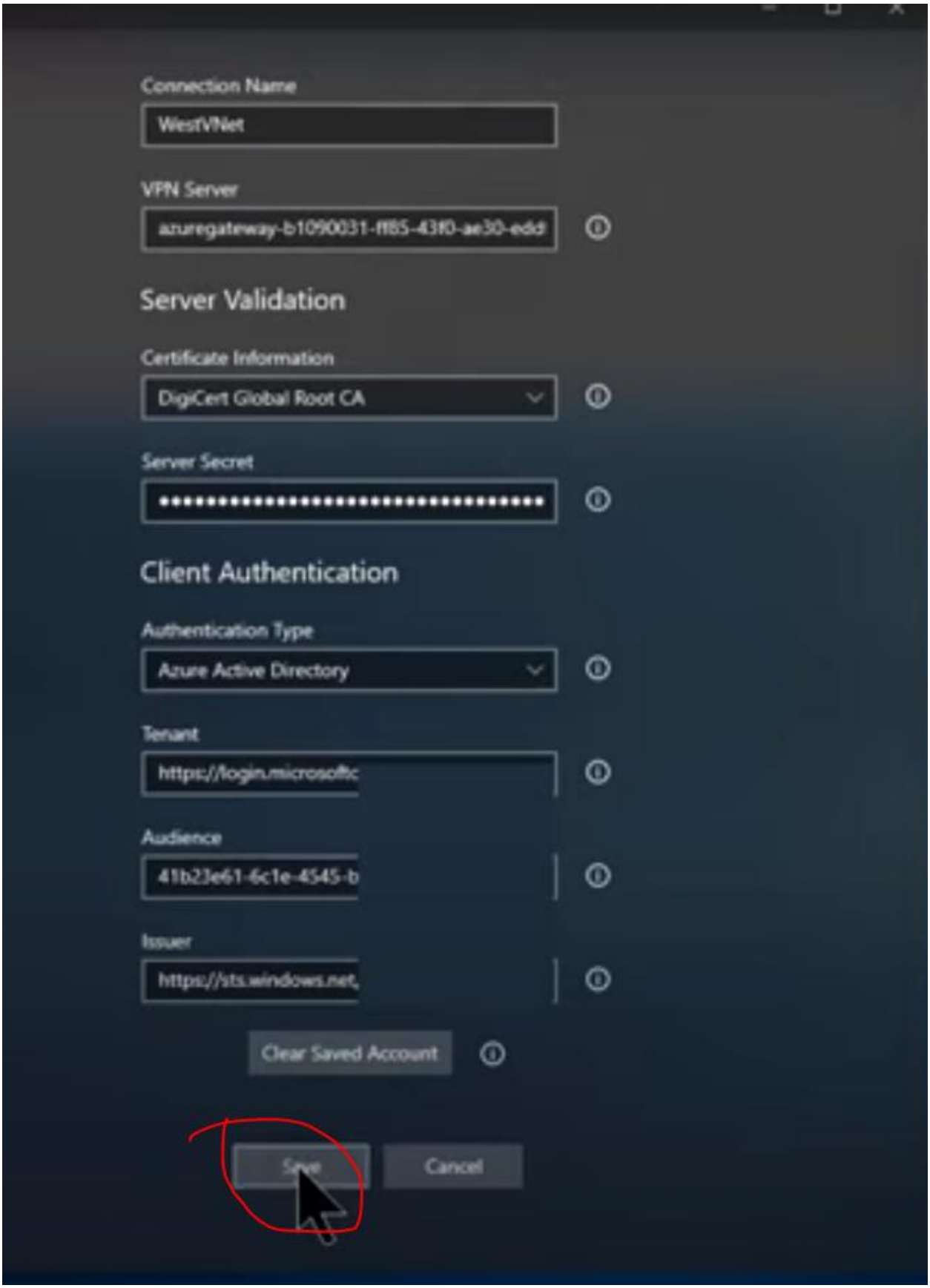
Configure the Client now

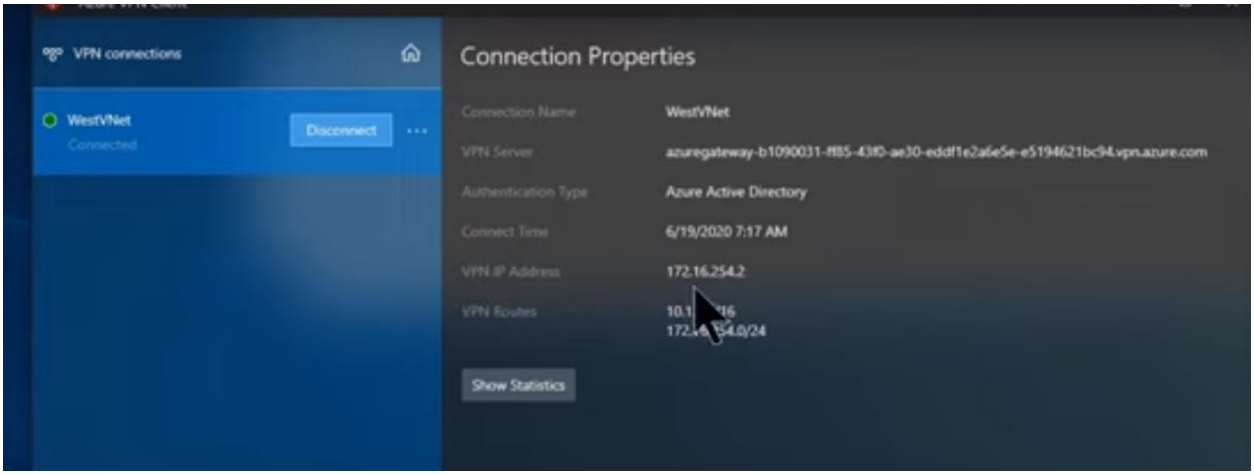




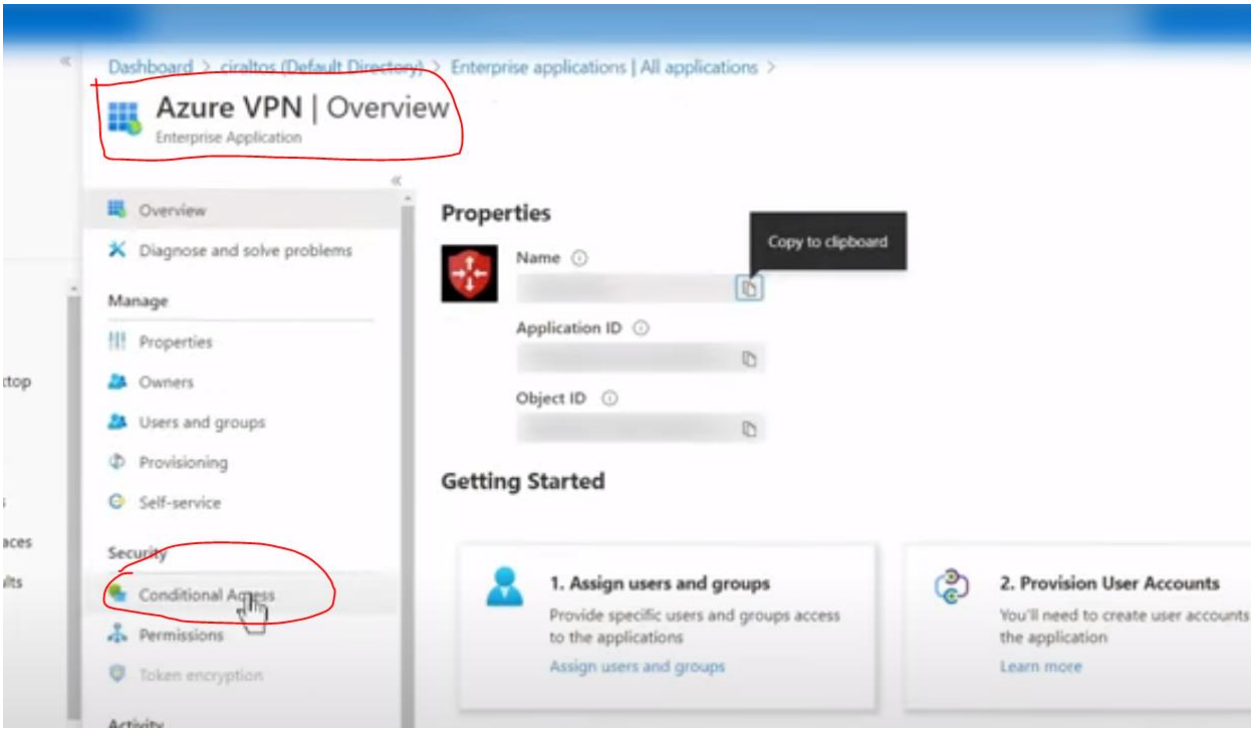
You can get it from the MS Store.

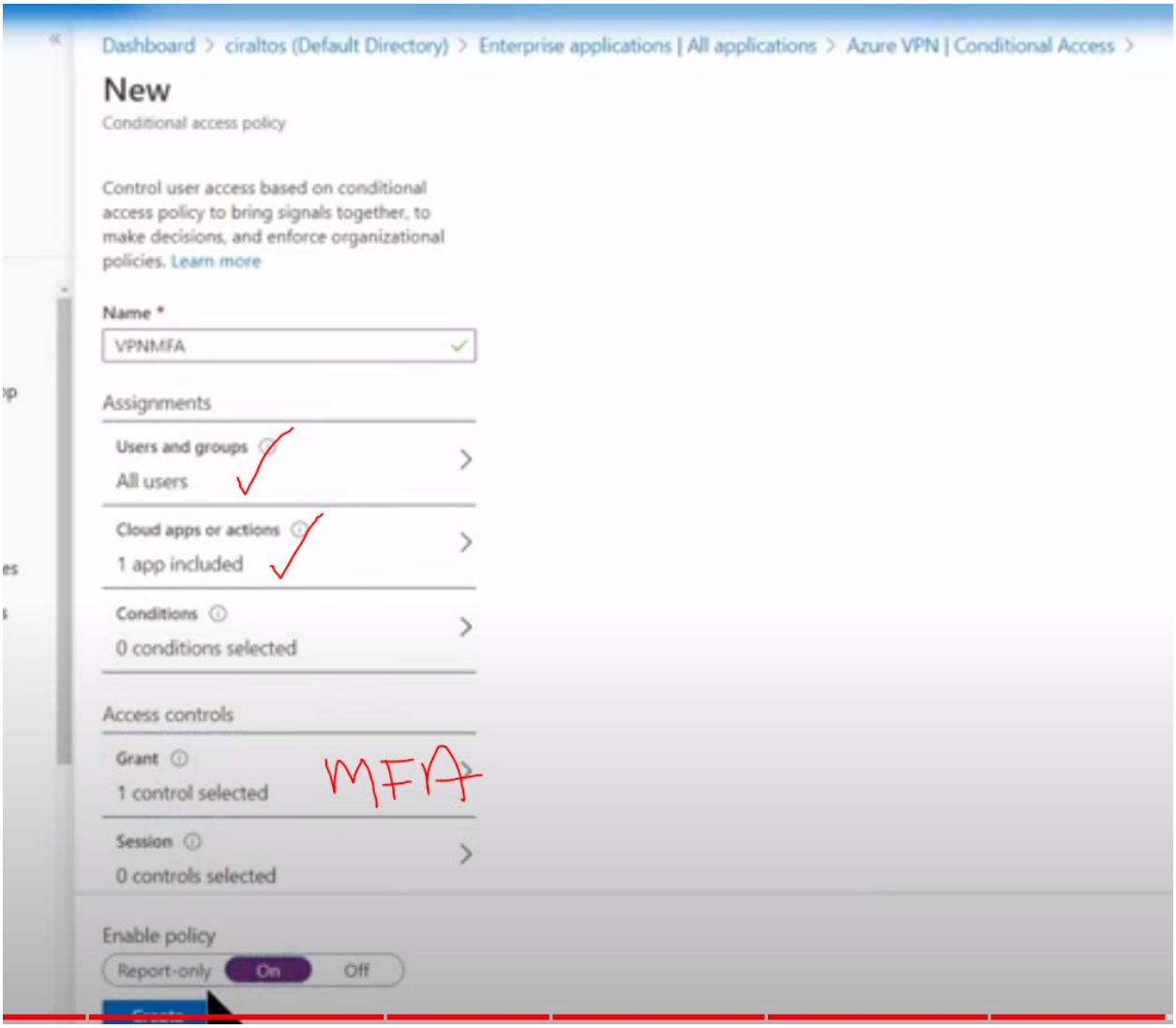



Connection Name
WestVNet
VPN Server
azuregateway-b1090031-ff85-43f0-ae30-edd
Server Validation
Certificate Information
DigiCert Global Root CA
Server Secret
Client Authentication
Authentication Type
Azure Active Directory
Tenant
https://login.microsoftc
Audience
41b23e61-6c1e-4545-b
Issuer
https://sts.windows.net,
Clear Saved Account
Save
Cancel

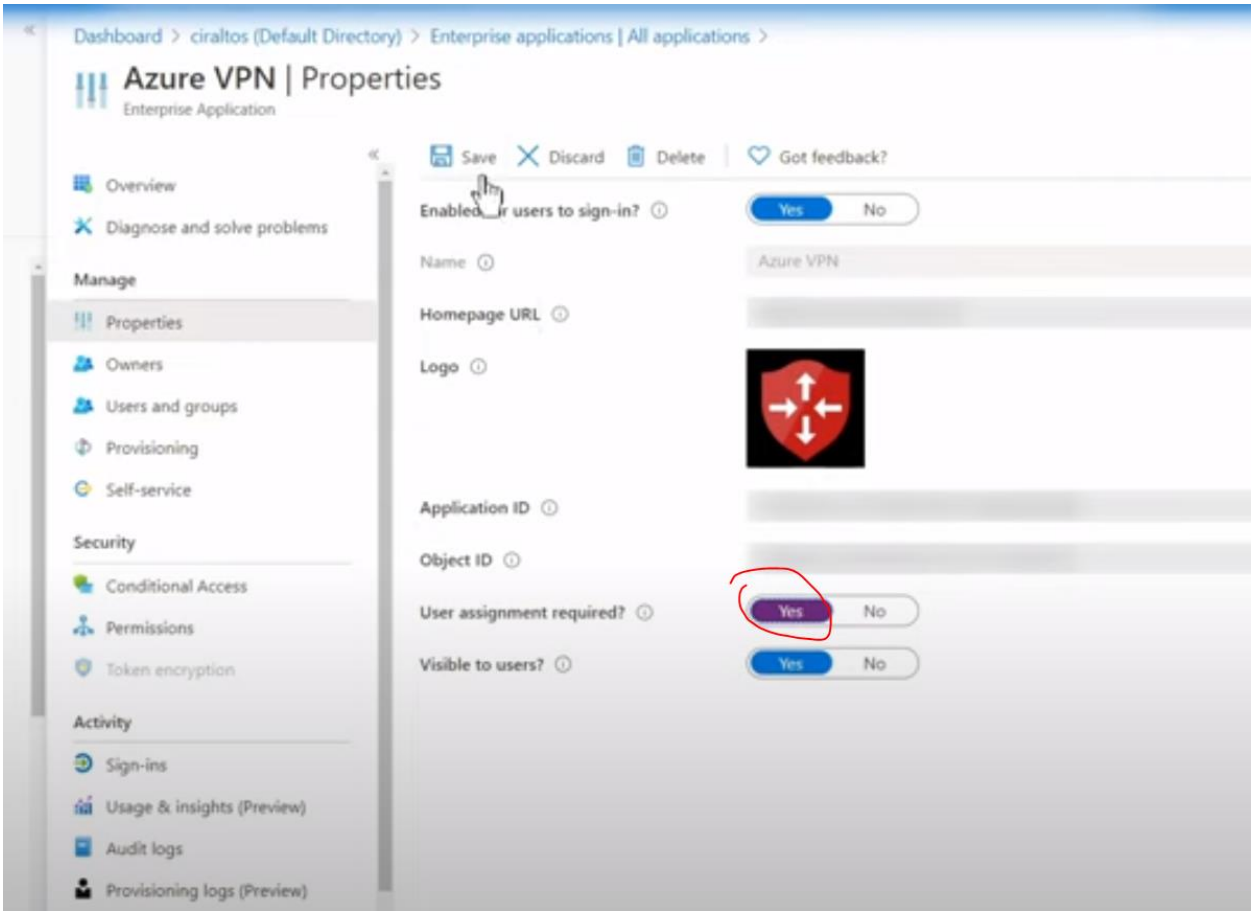

VPN connections
WestVNet
Connected
Disconnect
Connection Properties
Connection Name
WestVNet
VPN Server
azuregateway-b1090031-ff85-43f0-ae30-eddf1e2a6e5e-e5194621bc94.vpn.azure.com
Authentication Type
Azure Active Directory
Connect Time
6/19/2020 7:17 AM
VPN IP Address
172.16.254.2
VPN Routes
Show Statistics

Enable MFA


Dashboard > cjraltos (Default Directory) > Enterprise applications | All applications >
Azure VPN | Overview
Enterprise Application
Overview
Diagnose and solve problems
Manage
Properties
Owners
Users and groups
Provisioning
Self-service
Security
Conditional Access
Permissions
Token encryption
Properties
Name
Copy to clipboard
Application ID
Object ID
Getting Started
1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups
2. Provision User Accounts
You'll need to create user accounts the application
Learn more



Restrict VPN to a Group



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

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

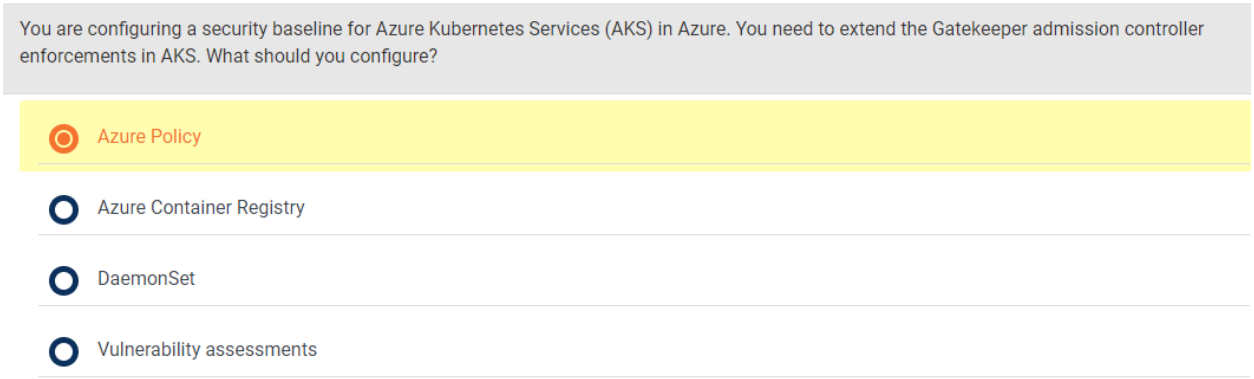
You are configuring a security baseline for Linux virtual machines in Azure. You need to identify a solution to protect the VM from viruses and malware. What should you do?

- 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

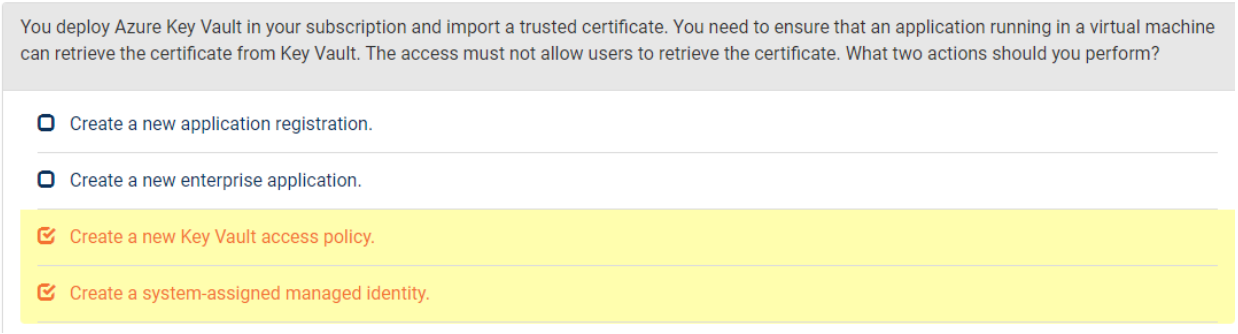
7. Azure Policy



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

8. 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

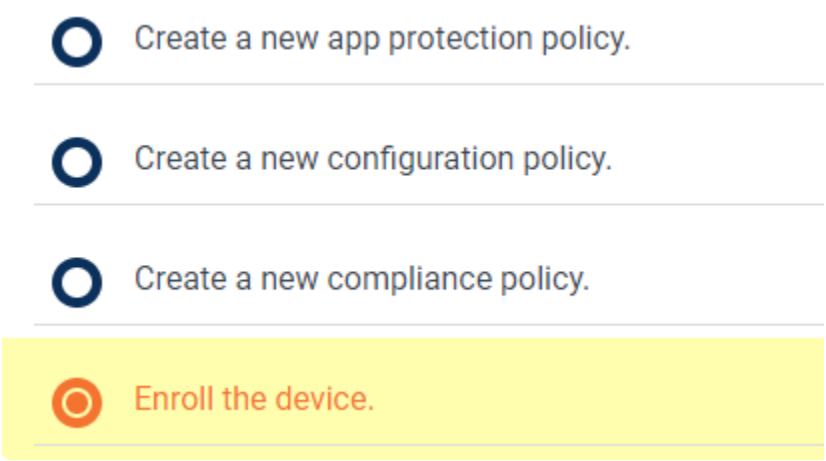
Your organization has a bring-your-own-device policy for employees. Employees need to access Outlook using their mobile devices without enrolling the devices. What should you do?

- 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



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

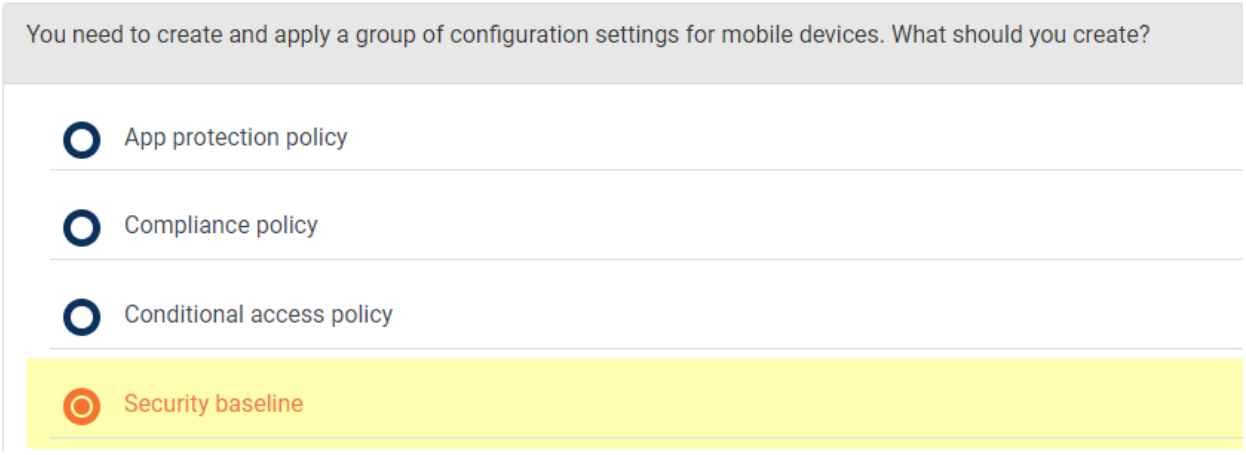
You are configuring a security baseline for Linux virtual machines in Azure. You need to ensure that VMs are encrypted using dm-crypt. What should you configure?

- 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

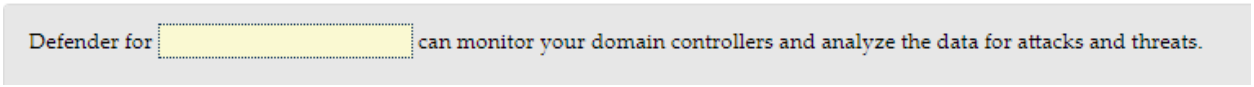
13. Security baseline



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

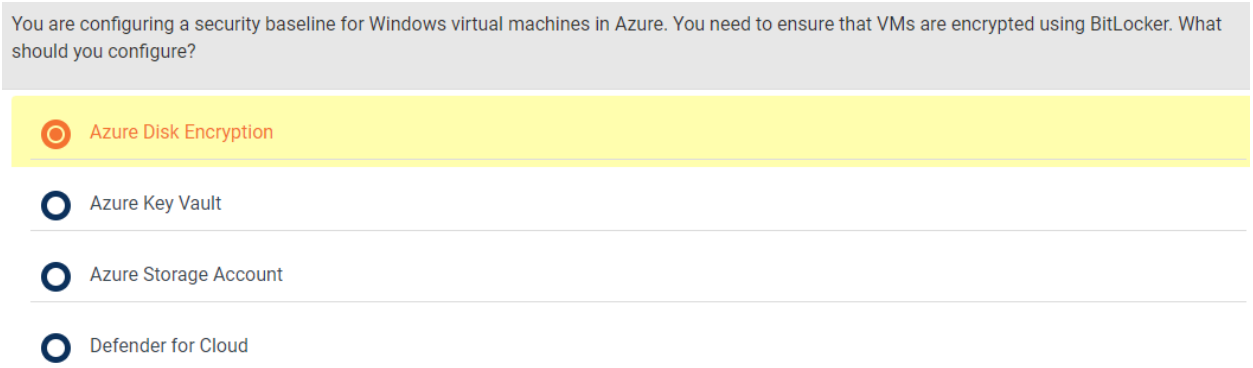
14. Defender for Identity



Defender for 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

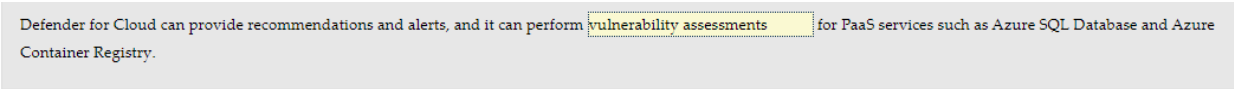
15. Security baseline



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

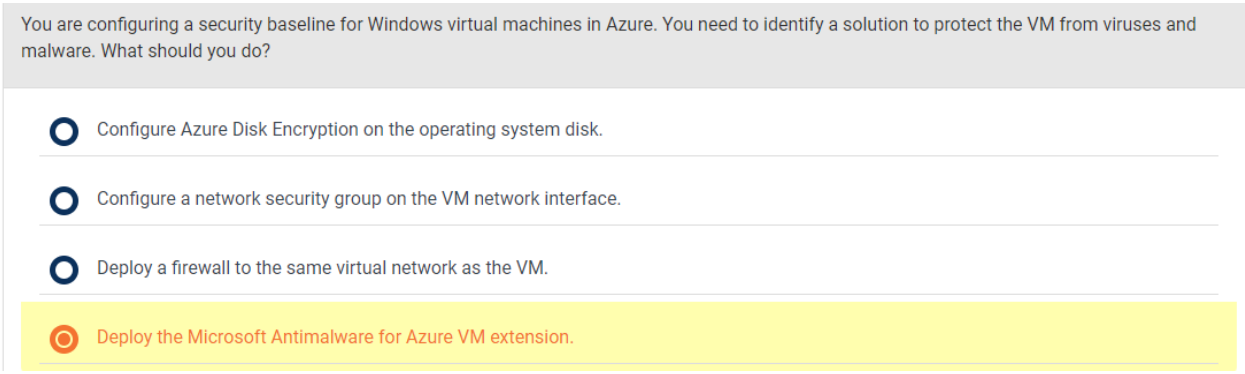
16. Defender for Cloud and vulnerability assessments



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.

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



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

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