Microsoft

Tag 3

AZ-500 Microsoft Azure Security Technologies

Guten Morgen!

© Copyright Microsoft Corporation. All rights reserved.

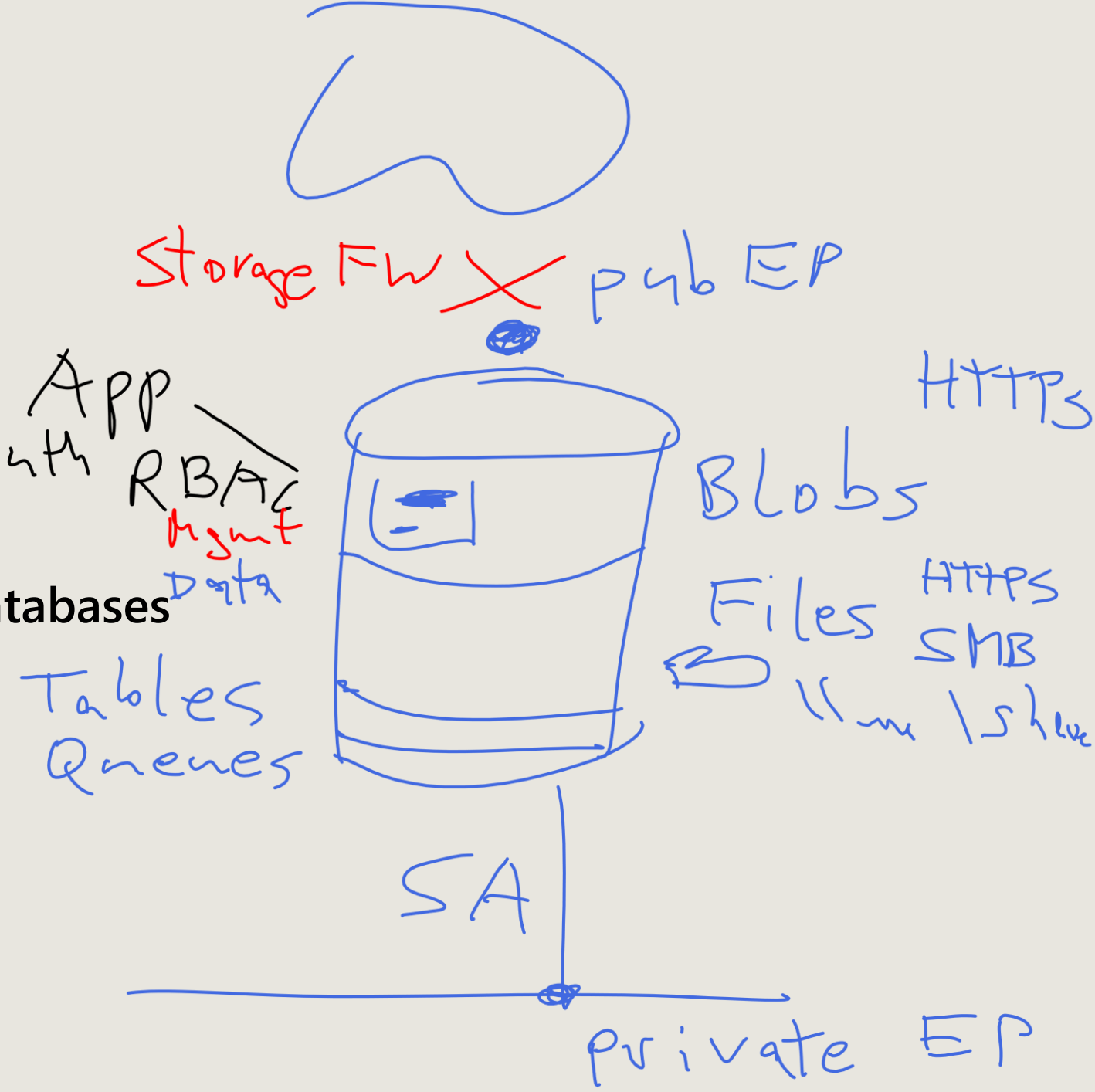
Agenda

1 Manage identity and access

2 Secure networking

3 Secure compute, storage, and databases

4 Manage security operations



© Copyright Microsoft Corporation. All rights reserved.

Learning Path: Secure compute, storage, and databases

Plan and implement advanced security for compute

Plan and implement security for storage

Plan and implement security for Azure SQL Database and Azure SQL Managed Instance

Module labs

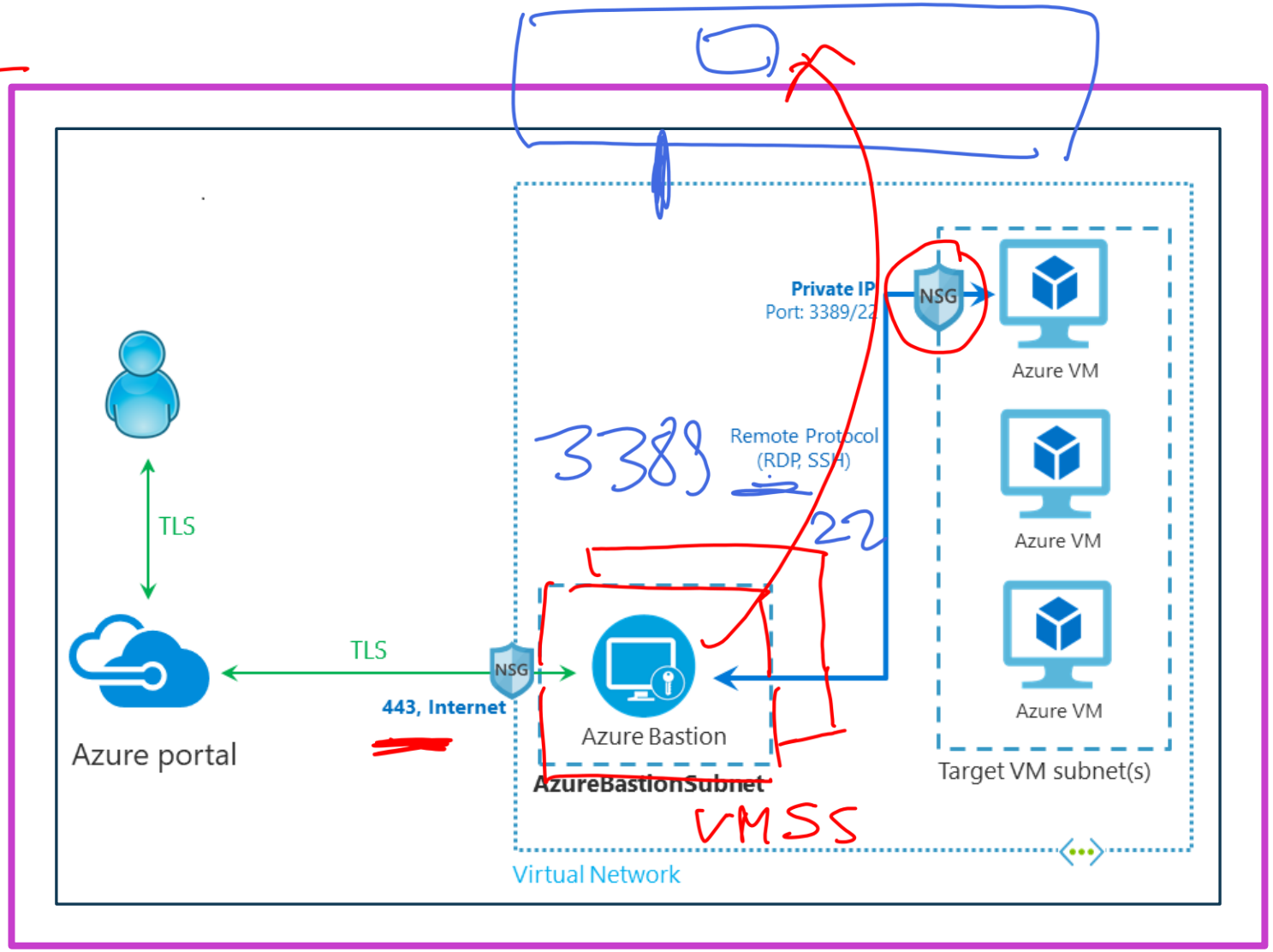
© Copyright Microsoft Corporation. All rights reserved.

Plan and implement advanced security for compute

© Copyright Microsoft Corporation. All rights reserved.

Plan and implement remote access to public endpoints, including Azure Bastion

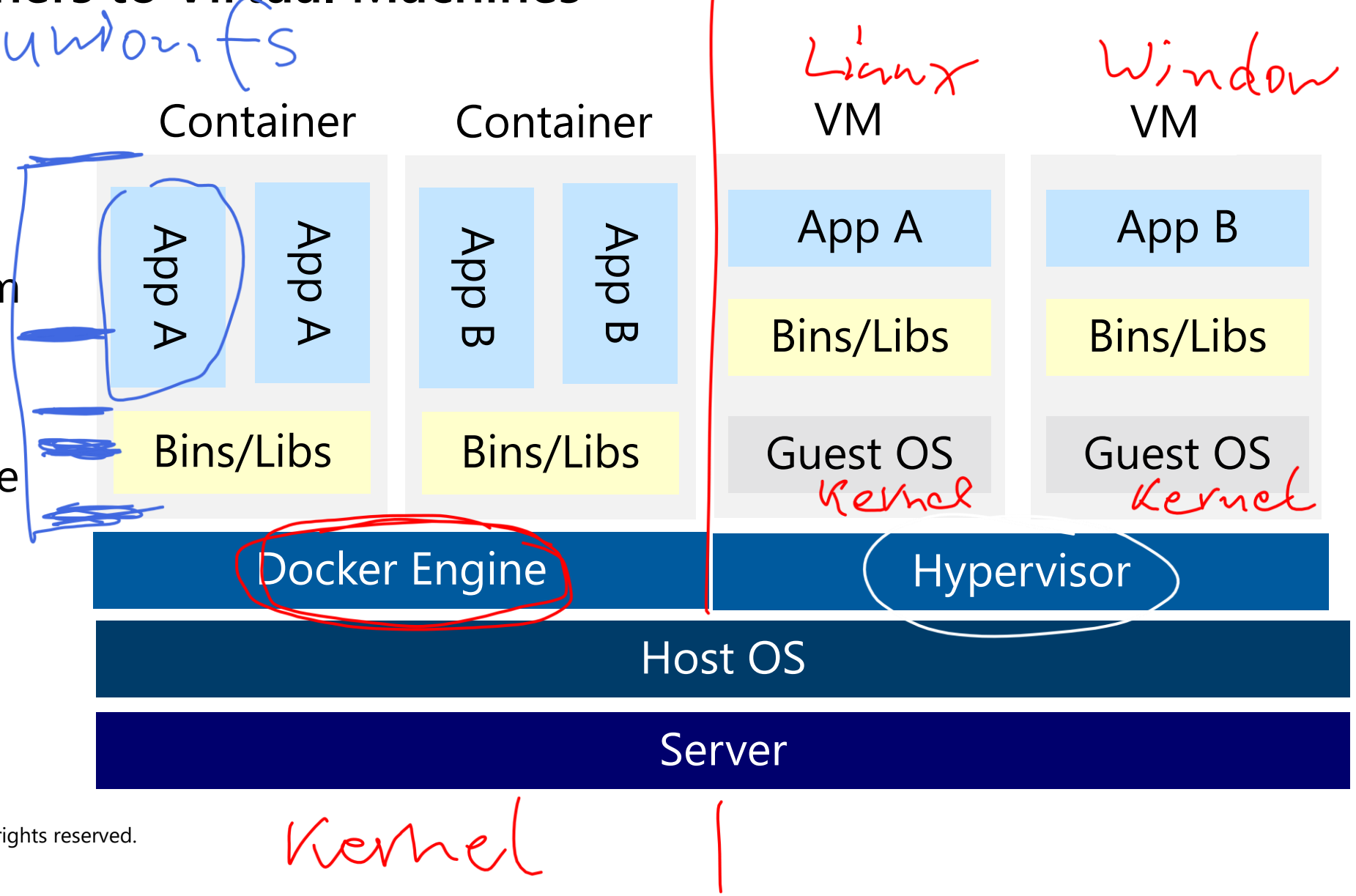
- Secure VM Access: Azure Bastion provides agentless RDP/SSH over TLS using private IPs, eliminating public exposure.
- SKU-Based Features: Developer is basic, Standard adds scaling, Premium enables session recording and private-only mode.
- Simplified Management: No public IPs, NSGs, or separate bastion hosts needed for secure connectivity.
- Scalability & Redundancy: Standard+ supports host scaling; availability zones are in preview for select regions.



© Copyright Microsoft Corporation. All rights reserved.

Compare Containers to Virtual Machines

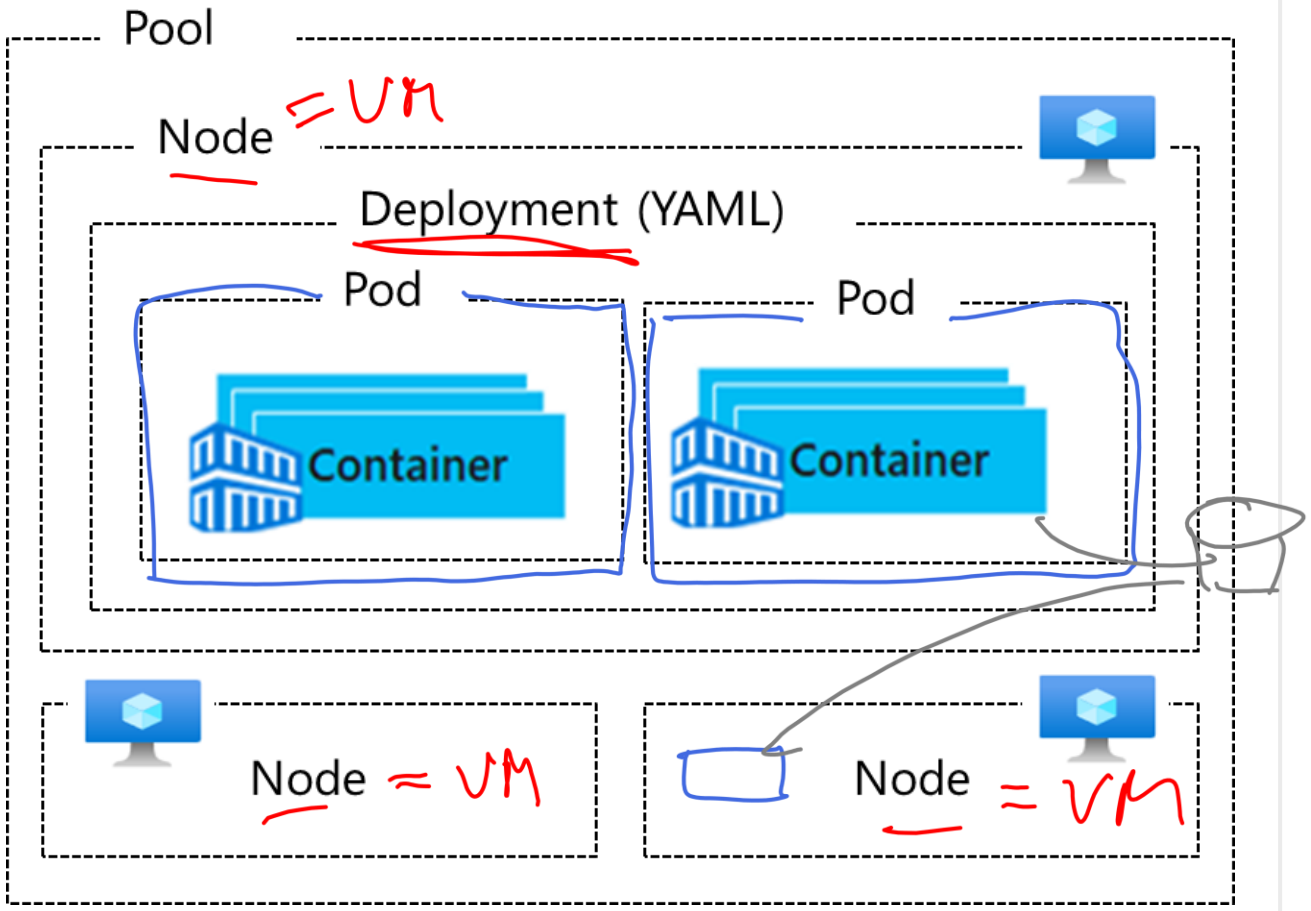
- Isolation
- Operating System
- Deployment
- Persistent storage
- Fault tolerance



© Copyright Microsoft Corporation. All rights reserved.

Understand AKS Terminology

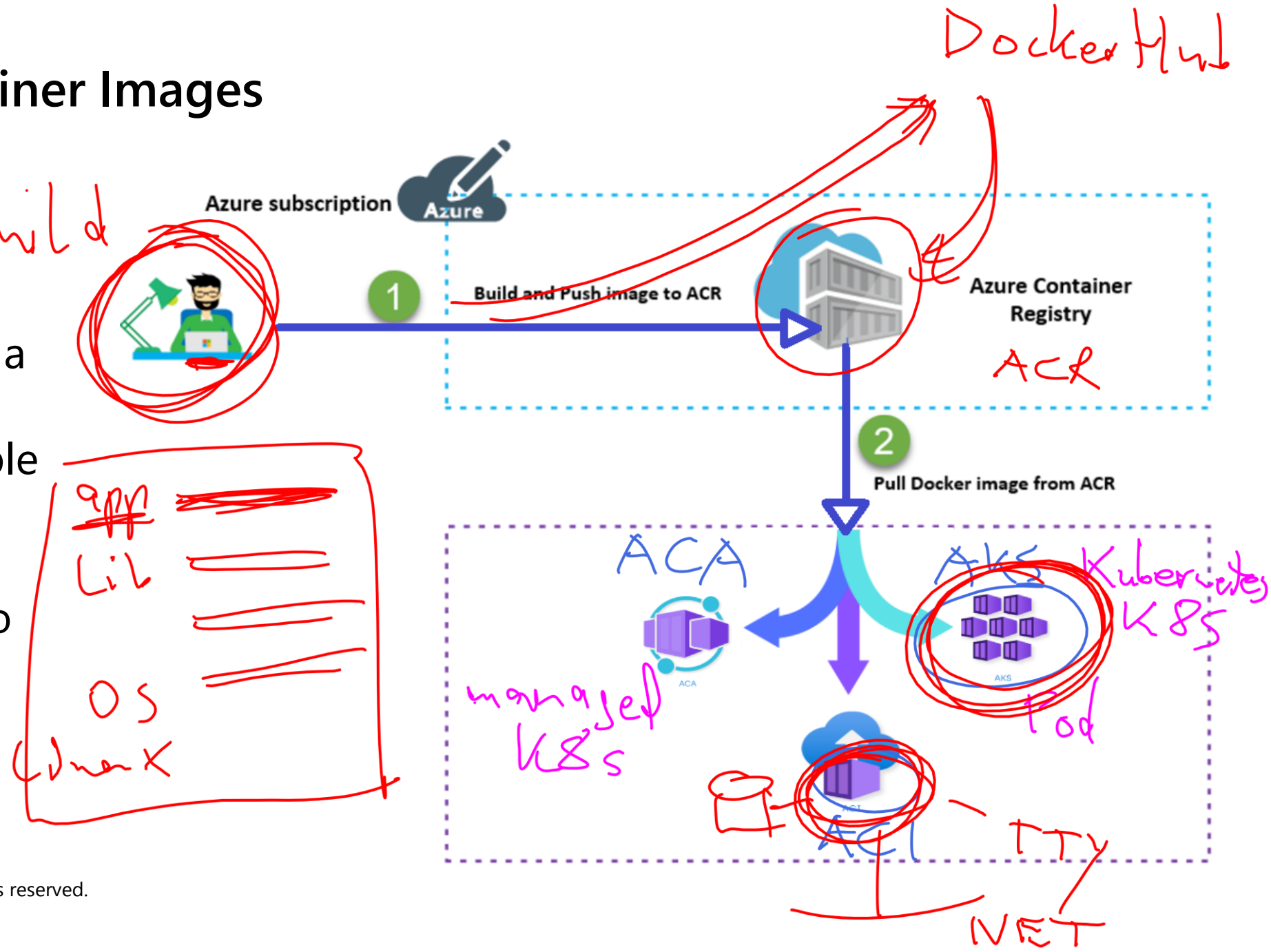
Term	Description
Pools	Groups of nodes with identical configurations
Nodes	Individual VMs running containerized applications
Pods	Single instance of an application. A pod can contain multiple containers
Deployment	One or more identical pods managed by Kubernetes
Manifest	YAML file describing a deployment



© Copyright Microsoft Corporation. All rights reserved.

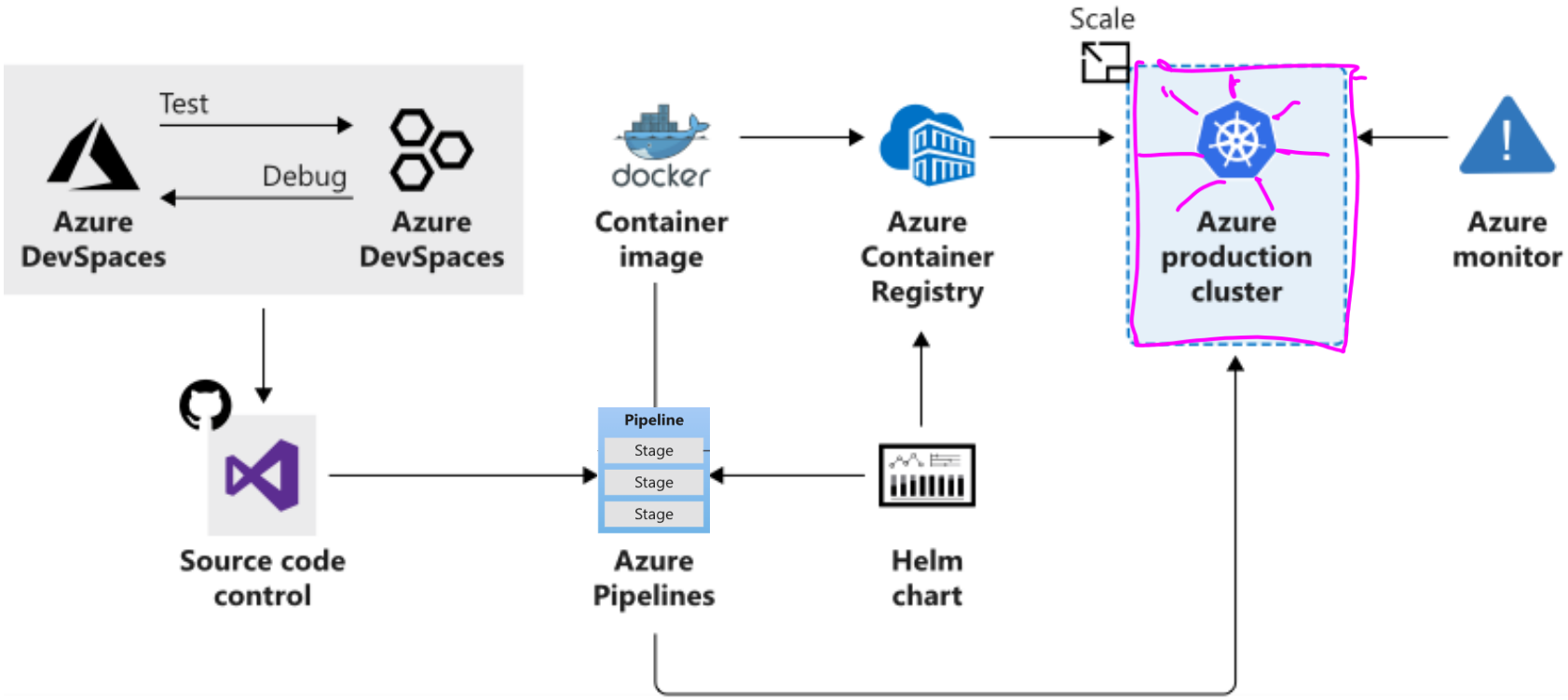
Understand Container Images

A container image is a lightweight, standalone, executable package of software that encapsulates everything needed to run an application.



© Copyright Microsoft Corporation. All rights reserved.

Azure Kubernetes Service



Manages health monitoring and maintenance

Performs simple cluster scaling

Enables nodes to be fully managed by Microsoft

You're responsible only for managing the agent nodes

You pay only for the agent nodes

© Copyright Microsoft Corporation. All rights reserved.

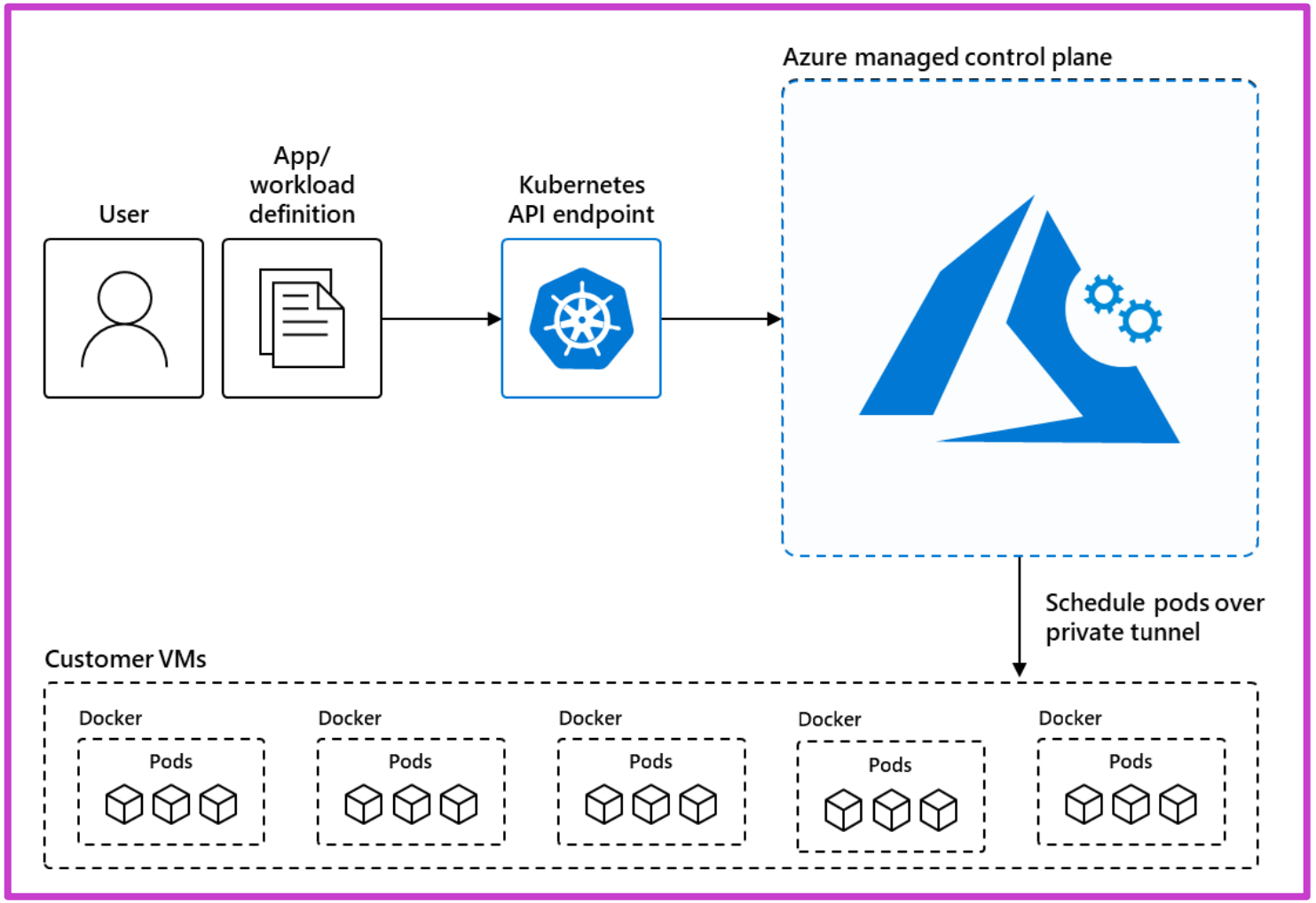
Compare container management solutions

	Azure Container Apps	Azure Kubernetes Service
Overview	Simplifies the deployment and management of microservices-based applications by abstracting away the underlying infrastructure.	Simplifies deploying a managed Kubernetes cluster in Azure by offloading the operational overhead to Azure.
Deployment	PaaS experience.	Offers more control and customization.
Management	Fully managed by Azure.	Partially managed by Azure (control plane).
Scalability	HTTP-based autoscaling and event-driven scaling.	Horizontal pod autoscaling and cluster autoscaling.
Use Cases	Rapid scaling and simplified management.	Complex, long-running applications that require full Kubernetes features.
Integration	Azure Logic Apps, Functions, and Event Grid for event-driven architecture.	Azure Policy for Kubernetes, Azure Monitor for containers, and Azure Defender for Kubernetes for comprehensive security and governance.

© Copyright Microsoft Corporation. All rights reserved.

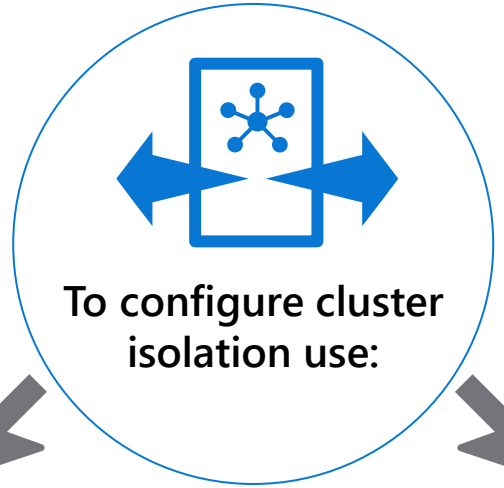
Azure Kubernetes Service (AKS)

- AKS simplifies Kubernetes management, providing high availability, scalability, and integration with DevOps tools.
- Azure manages AKS control plane for free, focusing on health monitoring and maintenance; users pay for nodes.
- AKS use cases include microservices, secure DevOps, data streaming, and running Windows containers.



© Copyright Microsoft Corporation. All rights reserved.

Configure network isolation for Azure Kubernetes Service



Logical isolation

- Has high pod density
- Additional security features, like Kubernetes RBAC for nodes, efficiently block exploit
- For true security when running hostile multi-tenant workloads, you should only trust a hypervisor.

Physical isolation

- Has low pod density
- it adds management and financial overhead.
- Use only for hostile multi-tenant workloads
- For other scenarios, it is recommended to use Logical Isolation.

© Copyright Microsoft Corporation. All rights reserved.

Secure and monitor AKS

Use Microsoft Defender for Containers to protect AKS by:

Environment hardening: Defender for Containers continuously assesses clusters to provide visibility into misconfigurations and guidelines to help mitigate identified threats.

Vulnerability assessment: Vulnerability assessment and management tools for images are stored in ACR registries and runs in Azure Kubernetes Service.

Run-time threat protection for nodes and clusters: Threat protection for clusters and Linux nodes generates security alerts for suspicious activities.

© Copyright Microsoft Corporation. All rights reserved.

Configure authentication for AKS

To configure authentication for AKS:

- Configure Microsoft Entra ID authentication for AKS clusters with OpenID Connect.
- Enable AKS-managed Microsoft Entra ID Integration on your existing Kubernetes RBAC-enabled cluster.
- Upgrade to AKS-managed Microsoft Entra ID Integration if you have legacy Azure AD Integration.
- Use kubelogin to access the cluster with non-interactive service principal sign-in.
- Use Conditional Access to control access while integrating Microsoft Entra ID with your AKS cluster.
- Use Privileged Identity Management (PIM) for just-in-time requests for cluster access control.

Remember these limitations:

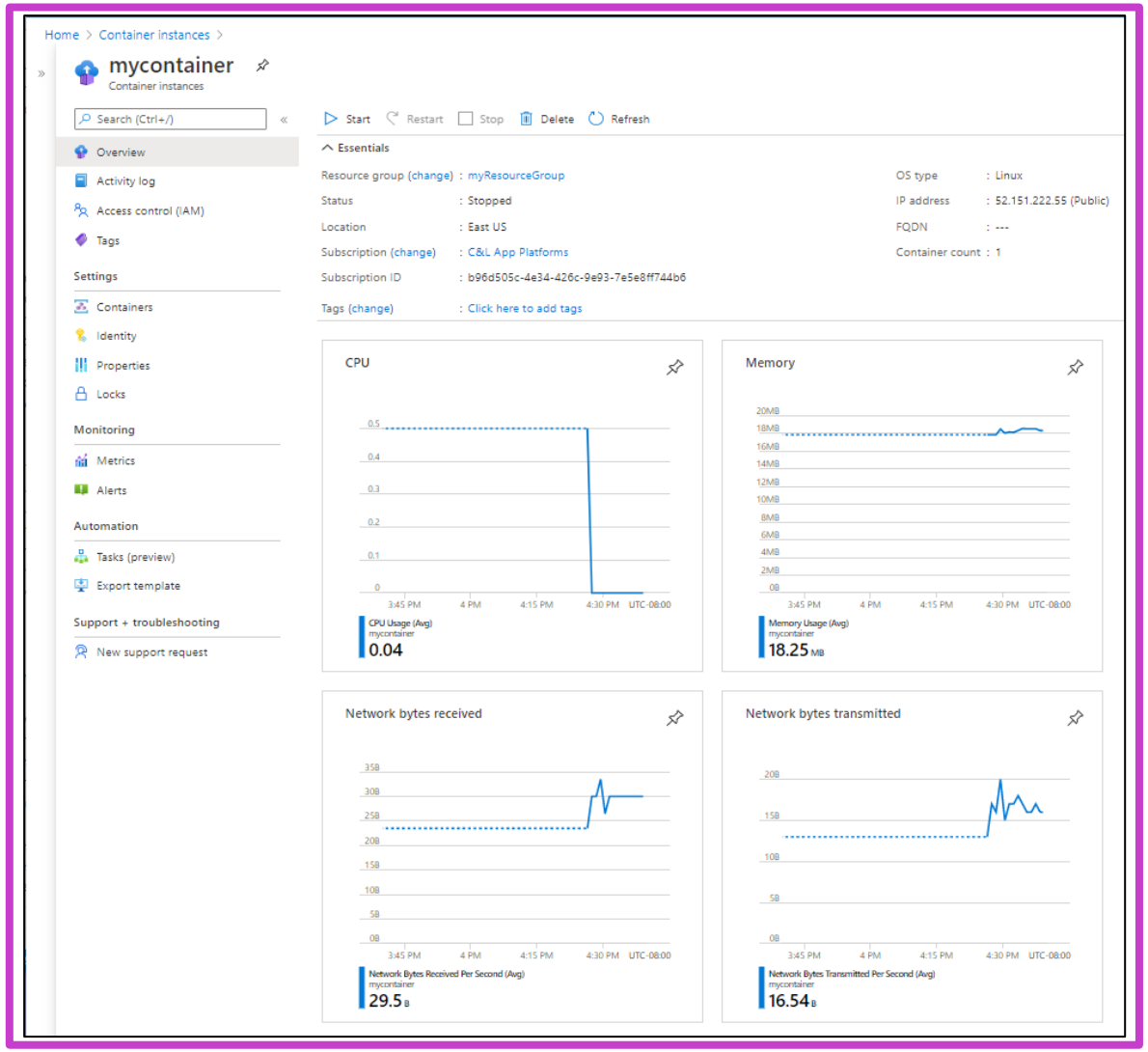
- You can't disable AKS-managed Microsoft Entra ID integration.
- You can't change an AKS-managed Microsoft Entra ID integrated cluster to legacy AAD.
- AKS-managed Microsoft Entra ID integration doesn't support clusters that are not Kubernetes RBAC-enabled.

© Copyright Microsoft Corporation. All rights reserved.

Configure security monitoring for Azure Container Instances

Get metrics - Azure portal

- When a container group is made, Azure Monitor data is in the Azure portal.
- Metrics are on the **Overview** page, with pre-created charts for each metric.



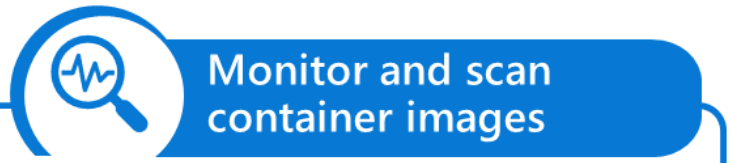
Get metrics - Azure CLI

- Metrics for container instances can also be gathered using the Azure CLI.
- First, get the ID of the container group using the following command:

```
CONTAINER_GROUP=$(az container show --
resource-group <resource-group> --name
<container-group> --query id --output tsv)
```

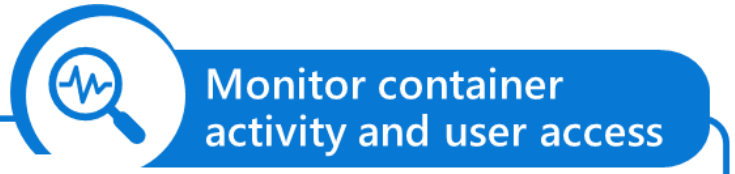
© Copyright Microsoft Corporation. All rights reserved.

Configure security monitoring for Azure Container Apps



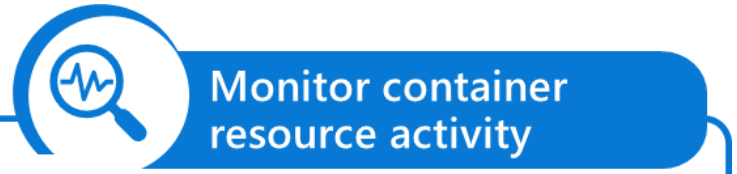
Monitor and scan container images

- Use solutions to scan container images in a private registry and identify potential vulnerabilities.
- Solutions include Microsoft Defender for Cloud's integrated Qualys scanner, Twistlock, and Aqua Security.



Monitor container activity and user access

- Monitor activity and user access to your container ecosystem consistently to identify suspicious or malicious activities.
- Use container monitoring solutions provided by Azure, such as Container Insights.



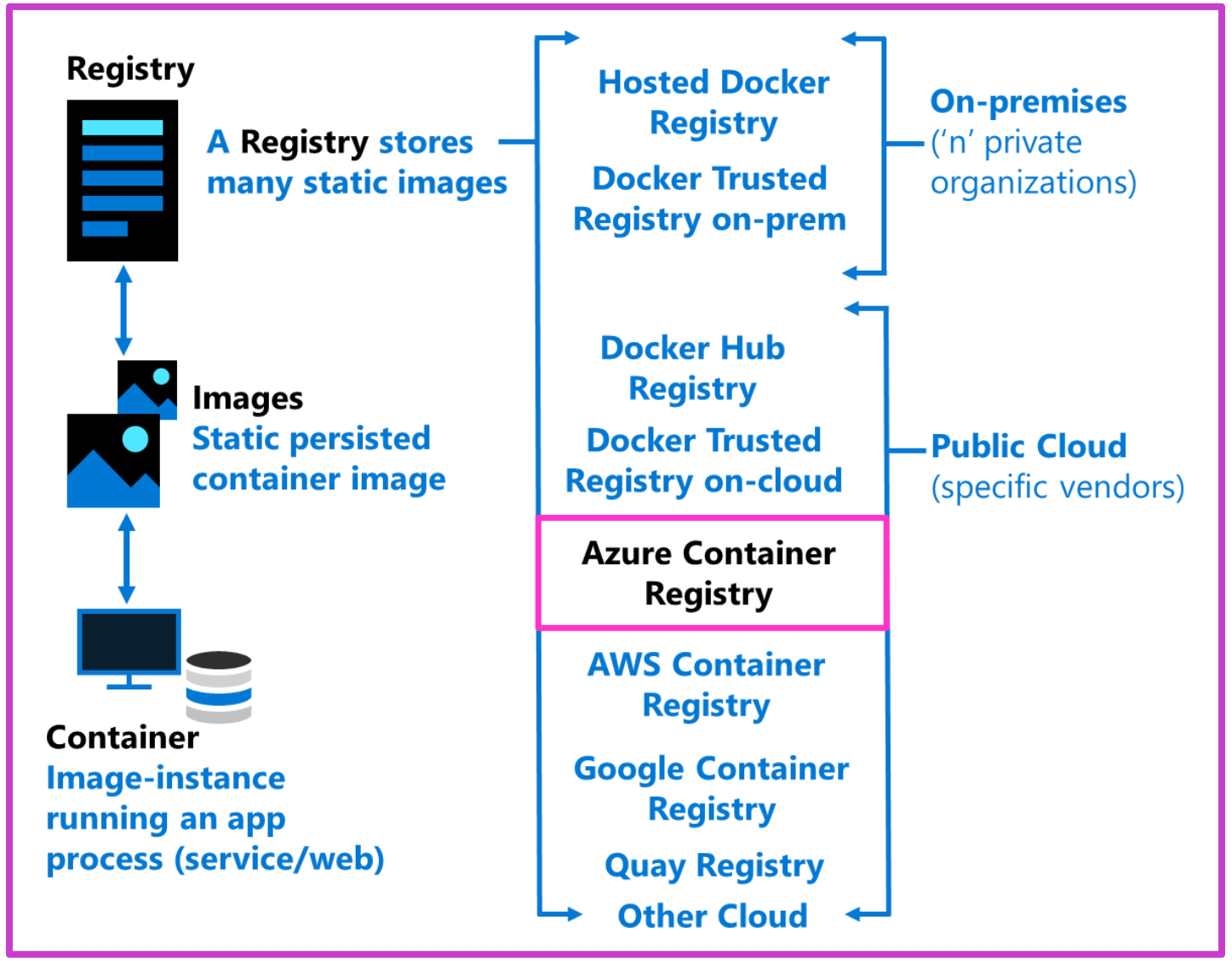
Monitor container resource activity

- Monitor your resource activity such as files and other resources that your containers access.
- Use Azure Monitor for the collection of metrics, activity logs, and diagnostic logs.
- Review metrics for performance statistics for different resources and the operating system inside a VM.

© Copyright Microsoft Corporation. All rights reserved.

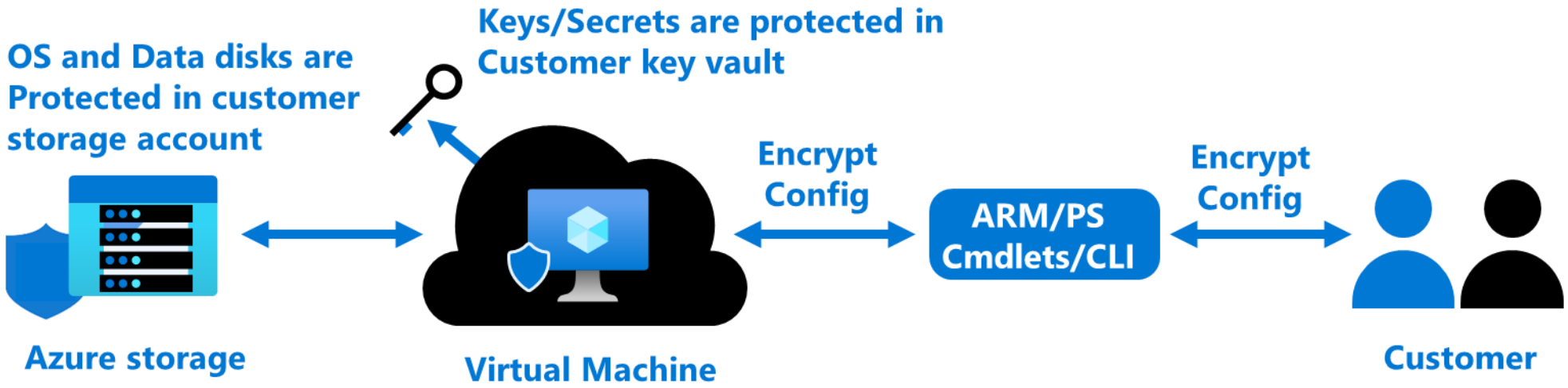
Manage access to an Azure Container Registry

- Docker registry service
- Private and hosted in Azure
- Build, store, and manage images
- Push and pull with the Docker CLI or the Azure CLI
- Access with Microsoft Entra ID
- RBAC to assign permissions
- Automate using DevOps



© Copyright Microsoft Corporation. All rights reserved.

Configure disk encryption, including Azure Disk Encryption (ADE), encryption at host, and confidential disk encryption



Provides encryption of the operating system and data disks

Windows VMs (BitLocker) and Linux VMs (DM-Crypt)

Stores encryption keys in a customer-managed key vault

© Copyright Microsoft Corporation. All rights reserved.

Security configurations for Azure API Management

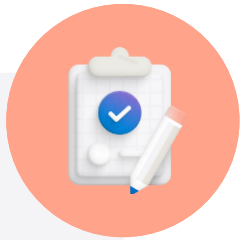
Use the following Azure security baseline for API Management:

Azure security baseline for API Management

- Azure security baseline for API Management incorporates Microsoft cloud security benchmark v1.0 guidance.
- The benchmark offers Azure security recommendations, categorized by controls, tailored for API Management.
- Microsoft Defender for Cloud enables monitoring, listing Azure Policy definitions for compliance, with some recommendations dependent on paid Defender plans for specific security scenarios.

© Copyright Microsoft Corporation. All rights reserved.

Additional Study – Planning and Implementing Advanced Security for Compute



Microsoft Learn Modules (docs.microsoft.com/Learn)

Module Review Questions

- Secure Remote Access to Virtual Machines: Implement Azure Bastion and Just-in-Time (JIT) access to protect VMs from unauthorized access.
- Secure Azure Kubernetes Service (AKS):Configure network isolation, authentication, and continuous security monitoring for AKS clusters.
- Monitor Azure Containers: Enable security monitoring for Azure Container Instances (ACIs) and Azure Container Apps (ACAs).
- Manage Azure Container Registry (ACR) Access: Securely manage access to ACR using role-based access control (RBAC) and network rules.
- Implement Disk and API Security:
  Configure Azure Disk Encryption (ADE), host encryption, and secure Azure API Management.

© Copyright Microsoft Corporation. All rights reserved.

Plan and implement security for storage

© Copyright Microsoft Corporation. All rights reserved.

Configure access control for storage accounts

Every storage request must be authorized. There are various authorization methods, including anonymous.

Storage	Storage Account Shared Key	Shared access signature	Microsoft Entra ID	Active Directory Domain Services (on-prem ADDS)	Anonymous public read access
Azure Blobs	Supported	Supported	Supported	Not supported	Supported
Azure Files (SMB)	Supported	Not supported	Supported, only with Microsoft Entra Domain Services	Supported, credentials must be synced to Microsoft Entra ID	Not supported
Azure Files (REST)	Supported	Supported	Supported	Not supported	Not supported
Azure Queues	Supported	Supported	Supported	Not supported	Not supported
Azure Tables	Supported	Supported	Supported	Not supported	Not supported

© Copyright Microsoft Corporation. All rights reserved.

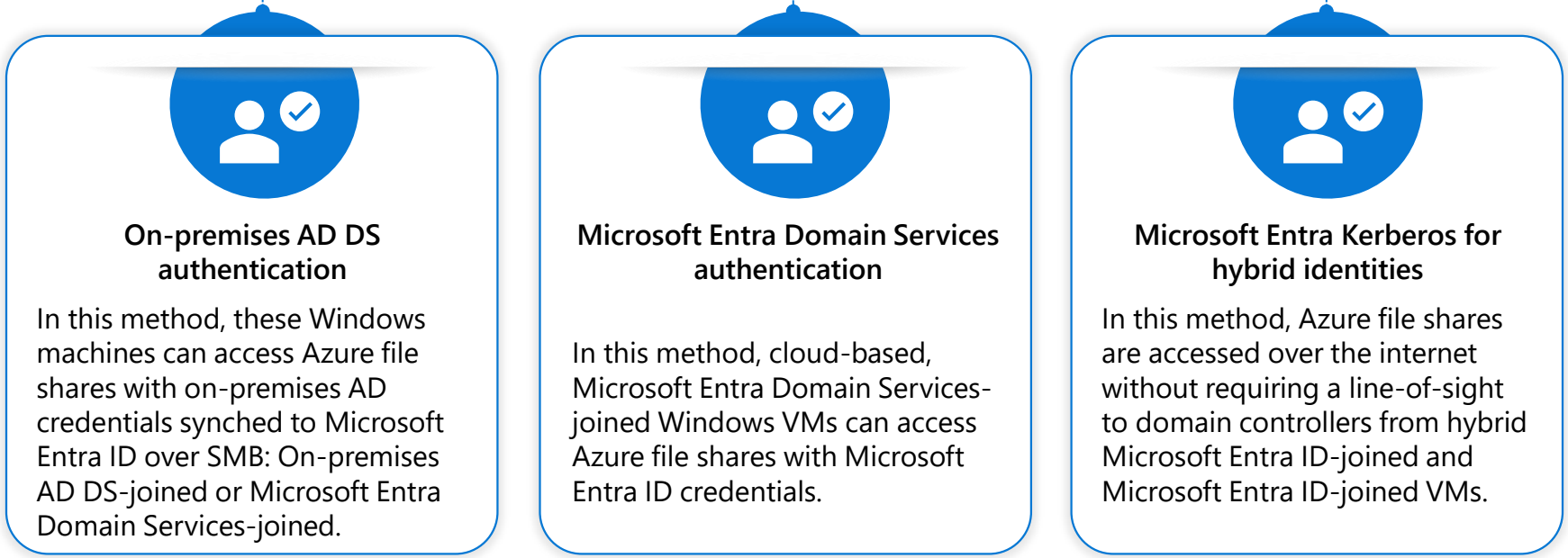
Manage storage account access keys

- Key Management: Use Azure Key Vault to securely manage, rotate, and protect storage access keys.
- Enhanced Authorization: Leverage Microsoft Entra ID and managed identities for superior security over shared keys.
- Key Rotation and Monitoring: Regularly rotate keys, set expiration policies, and monitor compliance using Azure Policy.

© Copyright Microsoft Corporation. All rights reserved.

Select and configure an appropriate method for access to Azure Files

Azure Files supports identity-based authentication for Windows file shares over Server Message Block (SMB) through the following methods. You can only use one method per storage account.



On-premises AD DS authentication

In this method, these Windows machines can access Azure file shares with on-premises AD credentials synched to Microsoft Entra ID over SMB: On-premises AD DS-joined or Microsoft Entra Domain Services-joined.

Microsoft Entra Domain Services authentication

In this method, cloud-based, Microsoft Entra Domain Services-joined Windows VMs can access Azure file shares with Microsoft Entra ID credentials.

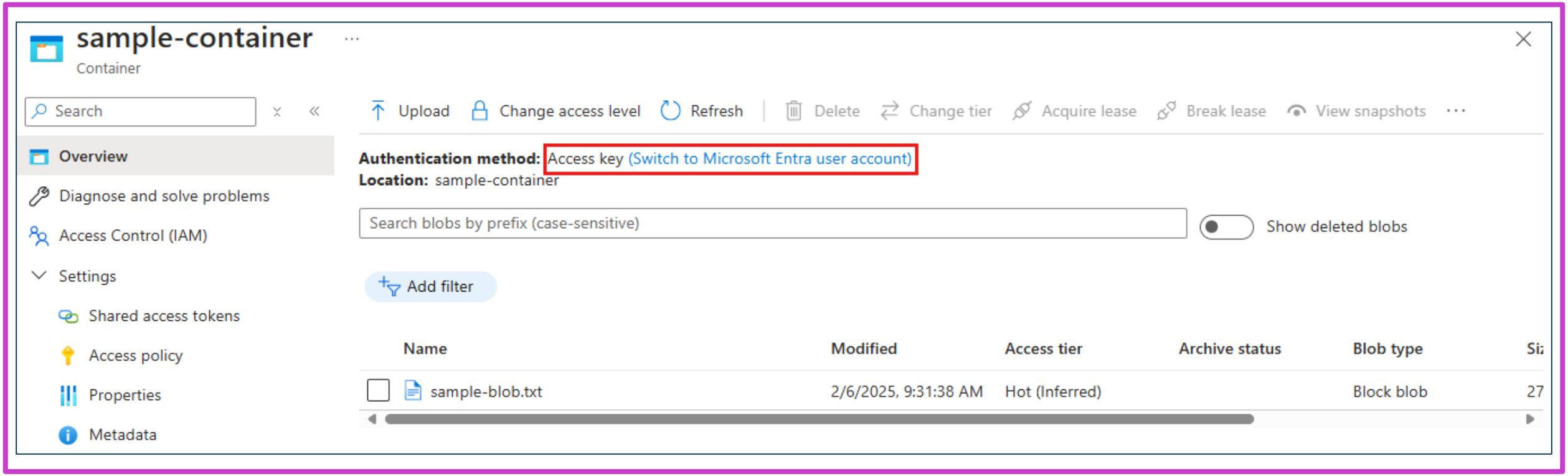
Microsoft Entra Kerberos for hybrid identities

In this method, Azure file shares are accessed over the internet without requiring a line-of-sight to domain controllers from hybrid Microsoft Entra ID-joined and Microsoft Entra ID-joined VMs.

Note: Azure Files supports the NFS protocol supporting Linux.

© Copyright Microsoft Corporation. All rights reserved.

Select and configure an appropriate methods for access to Azure Blob Storage



- Access blob data via Azure portal using Microsoft Entra account or storage account key.
- Permissions managed through Azure RBAC roles for accessing blob data.
- Switch authentication methods or specify authorization for blob uploads.

© Copyright Microsoft Corporation. All rights reserved.

Select and configure an appropriate method for access to Azure Tables

Remember the following considerations while configuring access to Azure Tables:

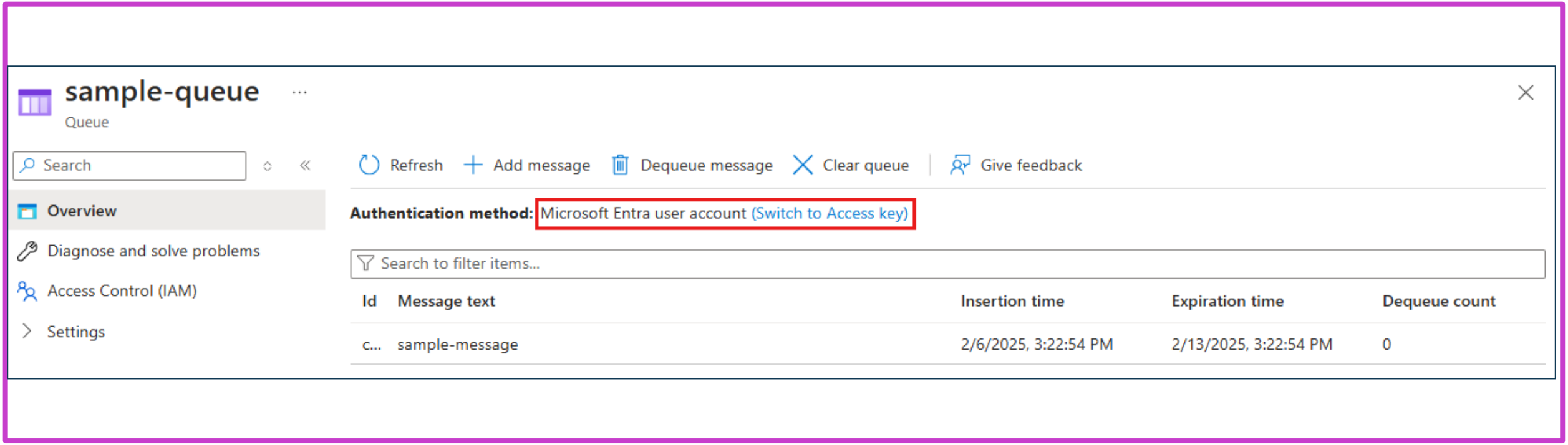
Accessing a table resource involves a two-step process in Microsoft Entra ID:
1. Authentication of the security principal's identity to get an OAuth 2.0 token
2. Using the token for authorizing access through the Table service

For authentication, applications running within Azure entities (e.g., Azure VM, Azure Functions) can utilize a managed identity to request an OAuth 2.0 access token.

The authorization phase necessitates assigning specific Azure roles to the security principal; these roles, provided by Azure Storage, dictate the permissions the principal possesses for table data access.

© Copyright Microsoft Corporation. All rights reserved.

Authorize access to queue data in the Azure portal



- Queue Data Access: The Azure portal accesses queue data using either a Microsoft Entra account or a storage account access key.
- Permissions & Authentication: Azure RBAC roles define access; users can switch authentication methods based on their permissions.
- Default Authentication: Microsoft Entra authorization can be set as the default but can be overridden if needed.

© Copyright Microsoft Corporation. All rights reserved.

Data protection overview

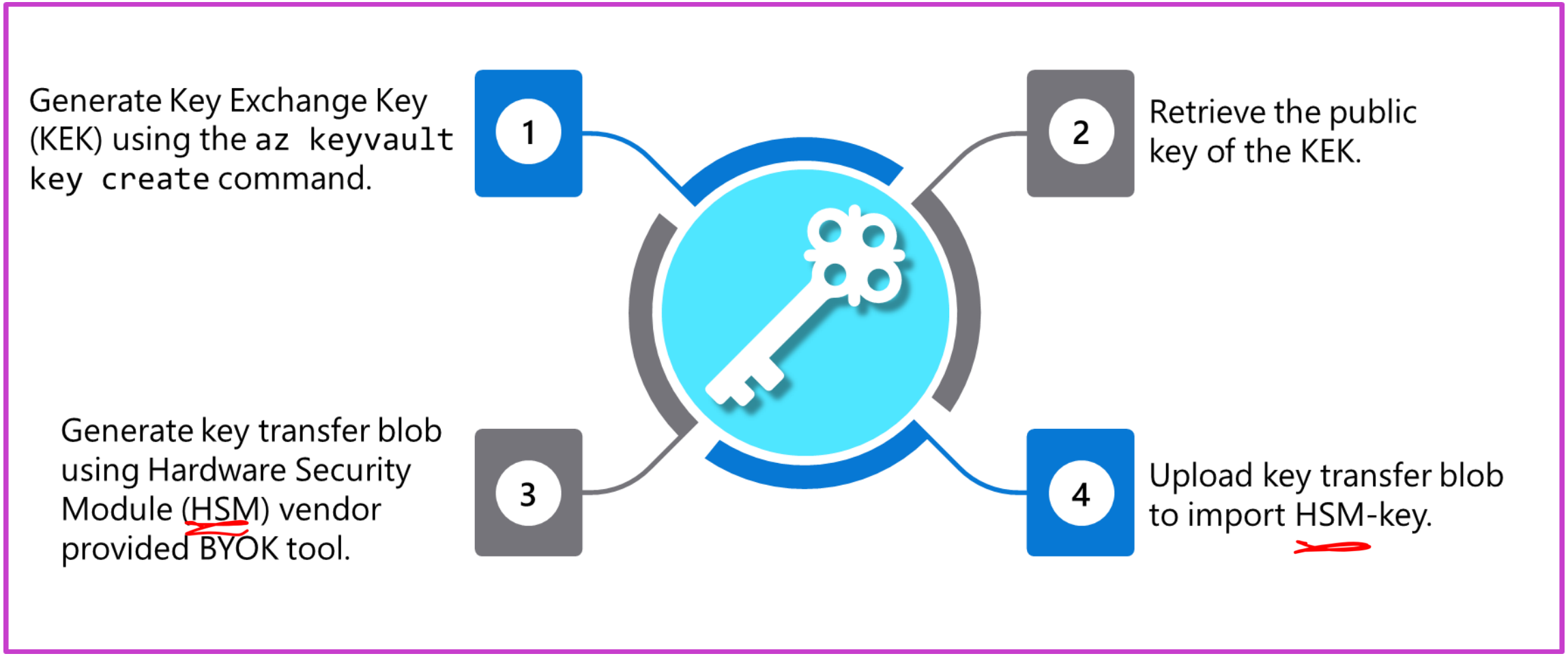
Recommendations for basic data protection

If you're looking for basic data protection coverage for your storage account and the data that it contains, then Microsoft recommends taking the following steps to begin with:

- Setting up Azure Resource Manager lock to avoid deletions or changes.
- Activating container soft delete for recovery of deleted content.
- Preserving blob state periodically:
    - In Blob Storage: use blob versioning for overwrite events.
    - In Azure Data Lake: utilize manual snapshots for data milestones.

© Copyright Microsoft Corporation. All rights reserved.

Bring your own key specification (BYOK)



© Copyright Microsoft Corporation. All rights reserved.

Enable infrastructure encryption for double encryption of data

- Azure Storage Encryption: Uses 256-bit AES and is FIPS 140-2 compliant; optional infrastructure-level double encryption adds an additional security layer.
- Infrastructure Encryption: Encrypts data twice with distinct algorithms and keys, applicable to entire storage accounts or specific scopes.
- Key Management: Service-level supports both Microsoft and customer-managed keys; infrastructure-level strictly uses Microsoft-managed keys.

Important: Infrastructure encryption is advised for compliance-driven double encryption needs. However, for most cases, Azure Storage encryption alone is typically sufficient and beneficial.

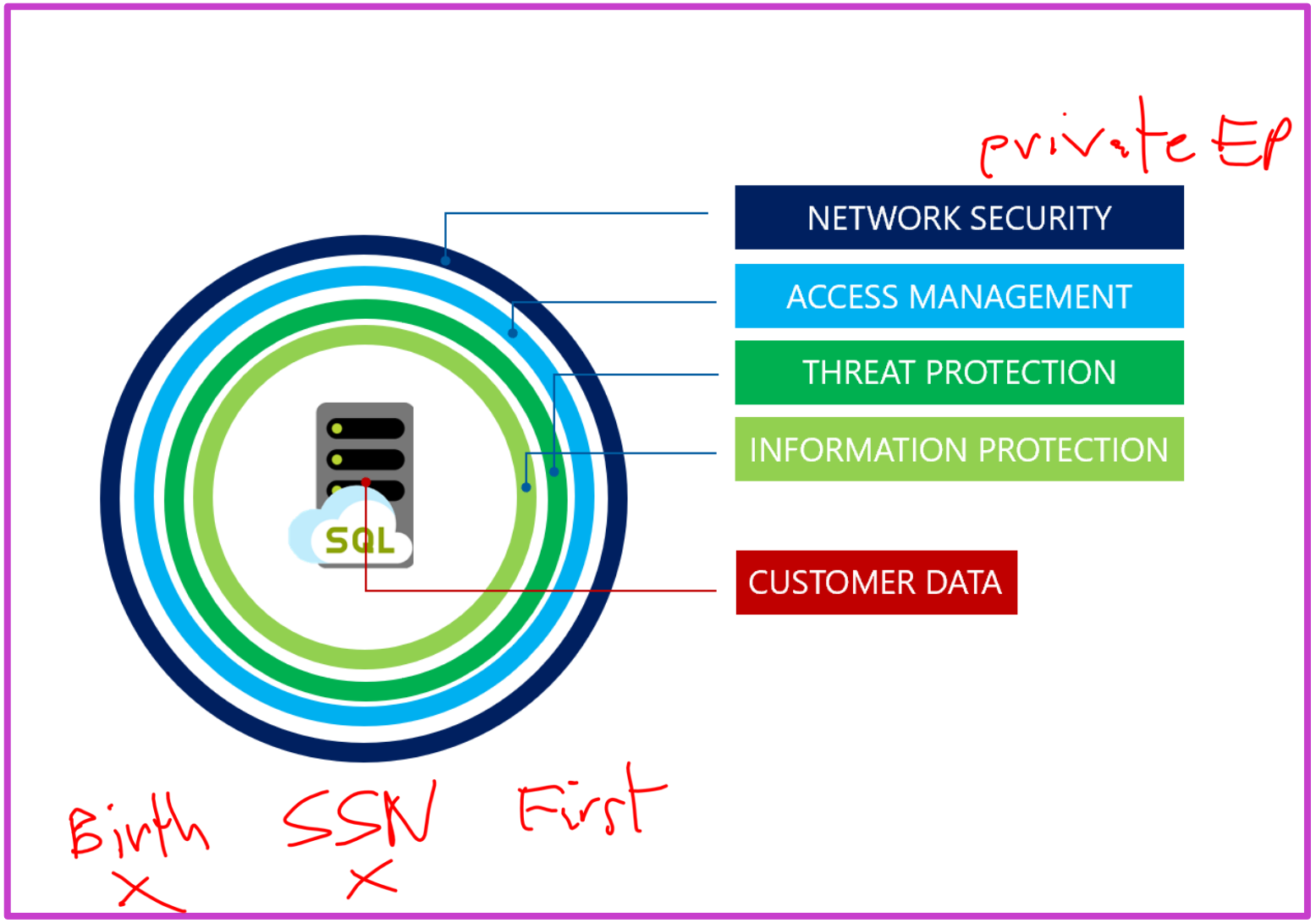
© Copyright Microsoft Corporation. All rights reserved.

Plan and implement security for Azure SQL Database and Azure SQL Managed Instance

© Copyright Microsoft Corporation. All rights reserved.

Azure SQL Database and SQL Managed Instance security

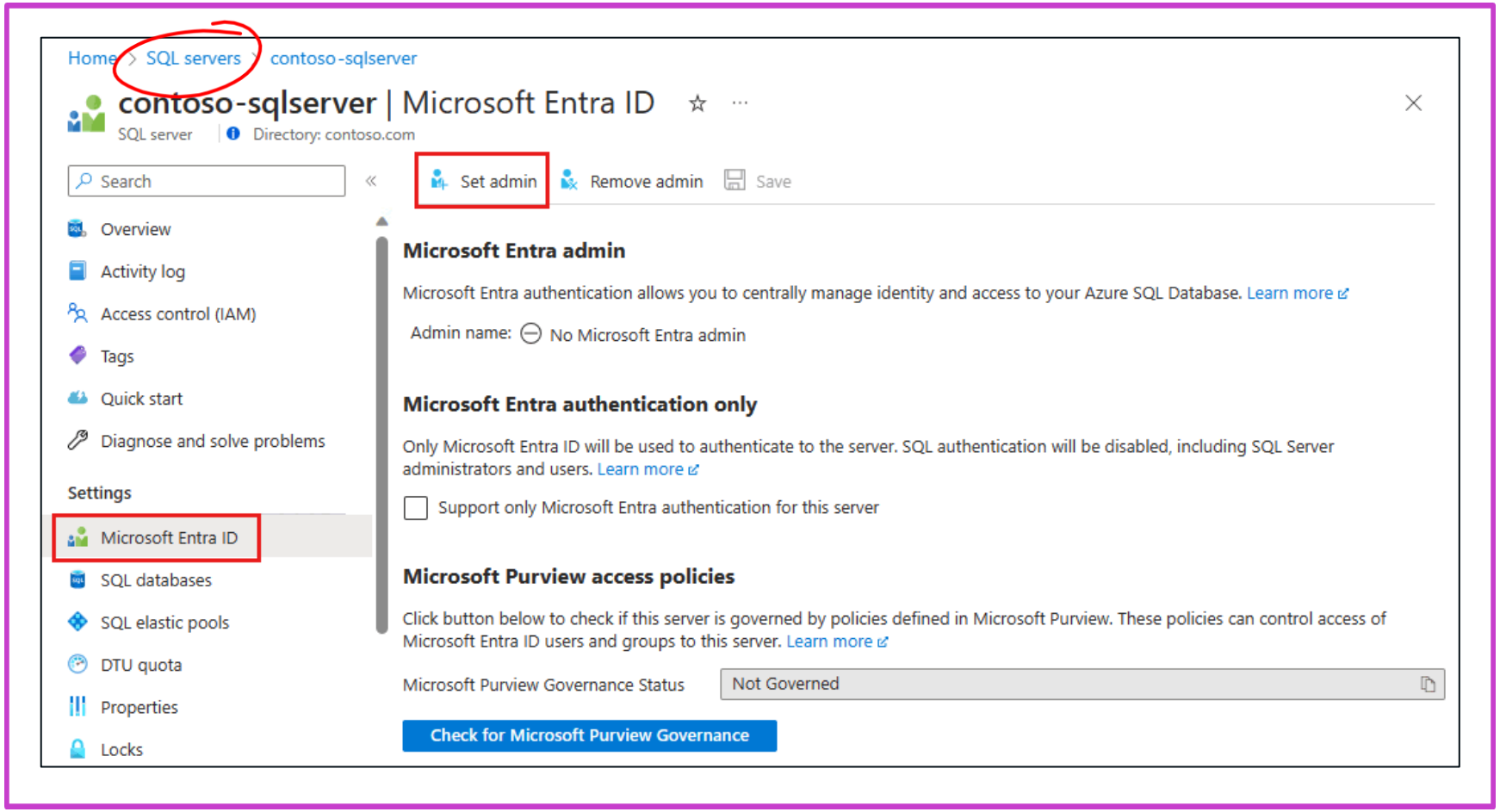
- Implements firewalls, IP and virtual network rules for robust network security.
- Supports SQL, Microsoft Entra authentication, and Windows authentication for secure access management.
- Uses encryption for data in transit and at rest and offers advanced threat protection.



© Copyright Microsoft Corporation. All rights reserved.

Enable Microsoft Entra database authentication

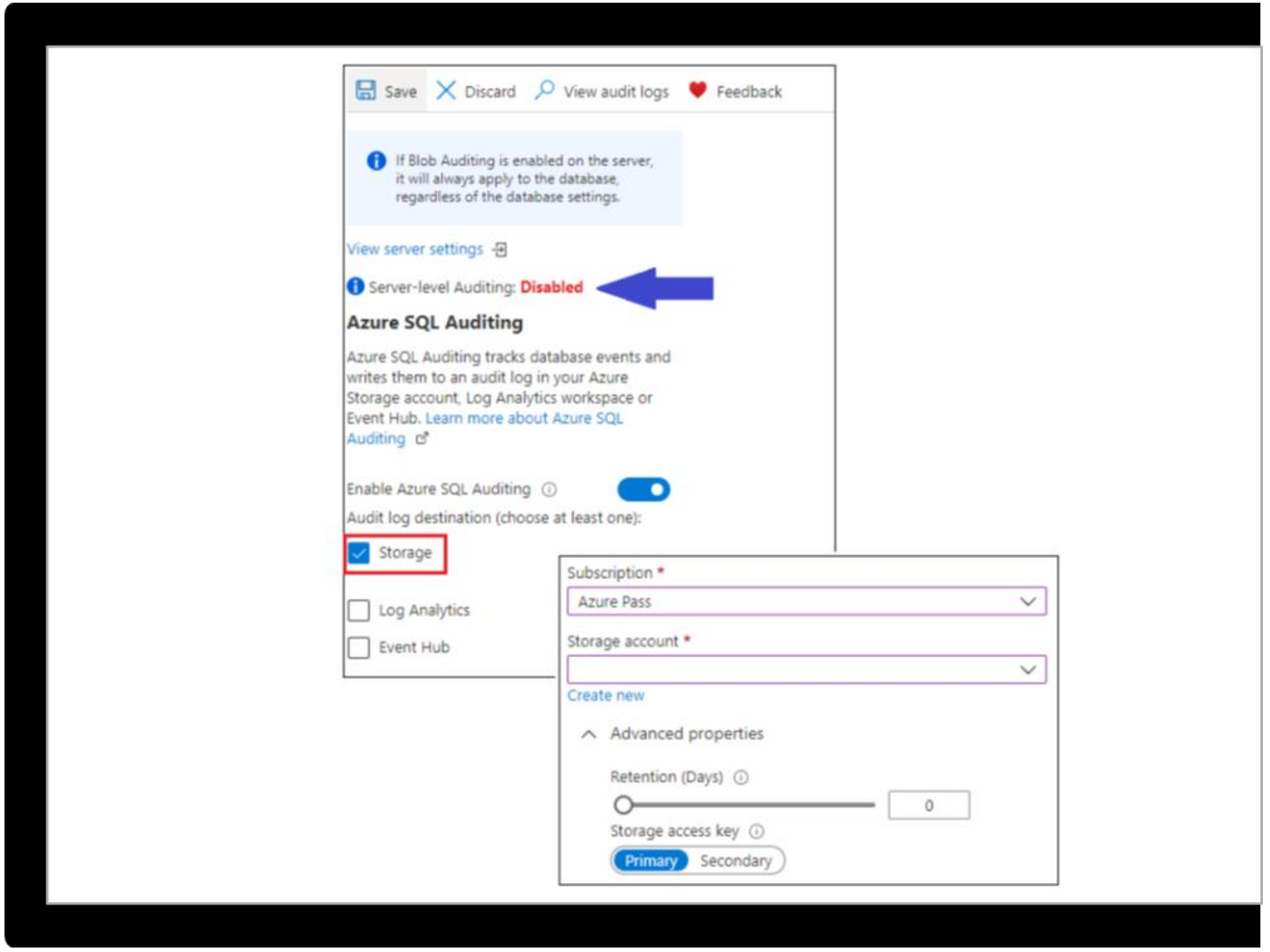
- Use Microsoft Entra ID for authentication with Azure SQL Database, Managed Instance, and Synapse Analytics.
- Ensure proper setup with a Microsoft Entra tenant, admin configuration, and permissions.
- Enable secure connections using Microsoft Entra authentication, MFA, and client integration.



© Copyright Microsoft Corporation. All rights reserved.

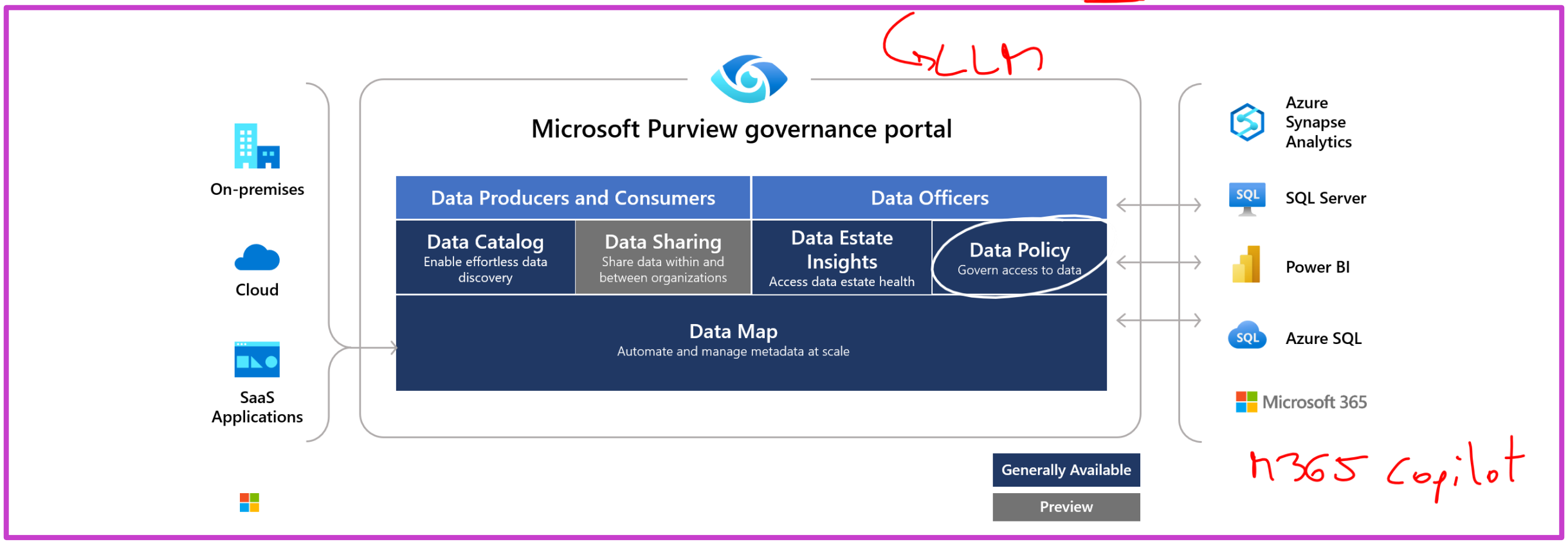
Enable database auditing

- Tracks database events to audit logs in Azure Storage, Log Analytics, or Event Hubs.
- Supports compliance, activity monitoring, and identifying security threats or suspicious database activity.
- Has limitations with Synapse pools, managed identities, and network-restricted storage accounts.



© Copyright Microsoft Corporation. All rights reserved.

Microsoft Purview governance



Microsoft Purview's solutions in the governance portal provide a unified data governance service that helps you manage your on-premises, multicloud, and software-as-a-service (SaaS) data.

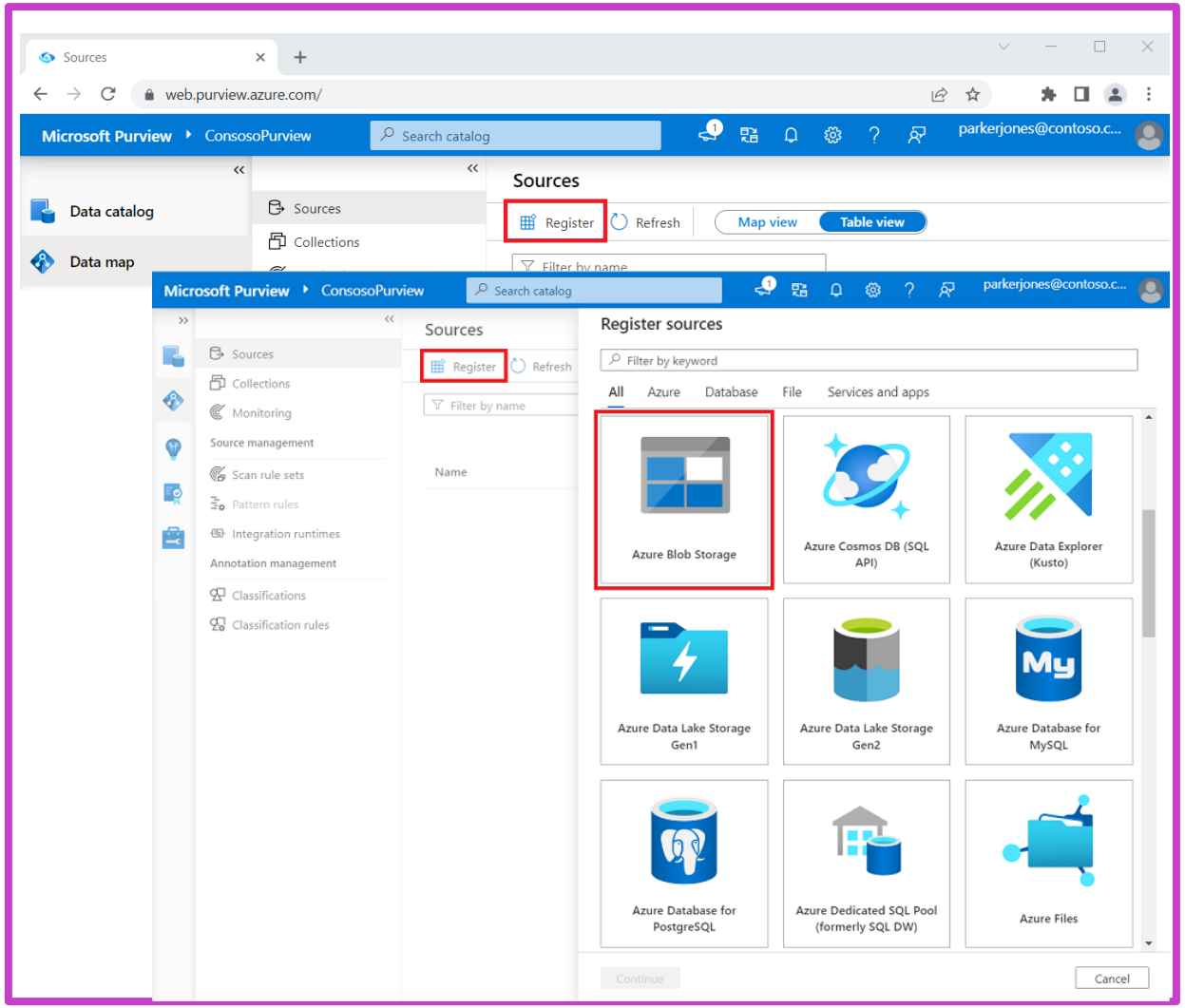
© Copyright Microsoft Corporation. All rights reserved.

Microsoft Purview governance-Register your data source

Registering a new source

In Microsoft Purview, after you register your data source, you can scan your source to capture technical metadata, extract schema, and apply classifications to your data.

- Registering a data source in Microsoft Purview associates its address with a Data Map collection.
- During registration, choose from system classifications or use custom ones for scanning.
- This process enables organized data management and classification in Purview.



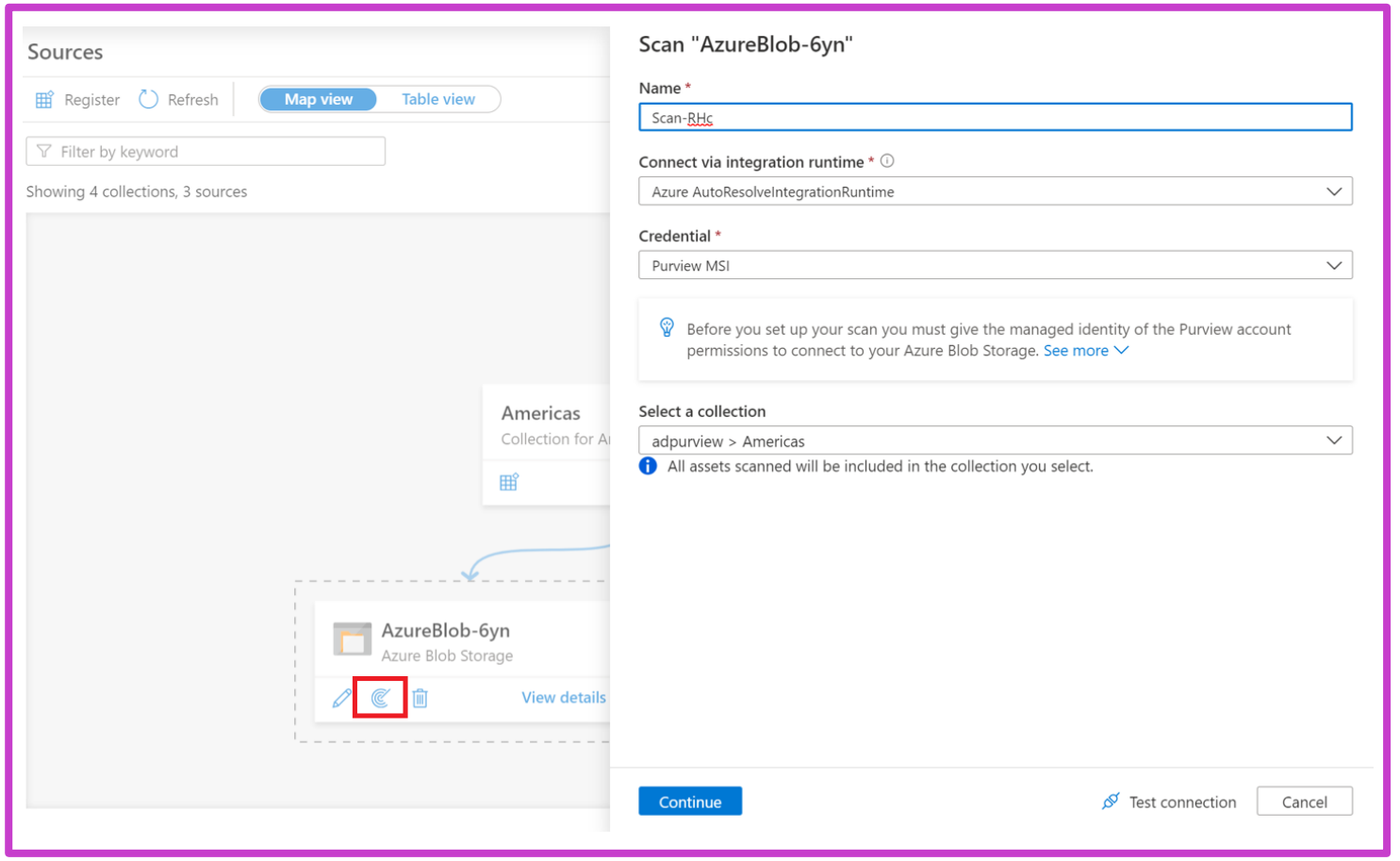
© Copyright Microsoft Corporation. All rights reserved.

Microsoft Purview governance-Scan and ingestion

Scans and ingestion

In Microsoft Purview, scanning and ingestion link your account to data sources. This populates the data map and catalog, simplifying data exploration and management

- Scanning connects to data sources, gathers technical metadata and schema, and applies classifications and sensitivity labels, offering flexible scheduling options.
- Ingestion populates the data map and integrates data source and lineage information, allowing for lineage tracking.
- Lineage information is added to existing sources or creates new ones during lineage ingestion.



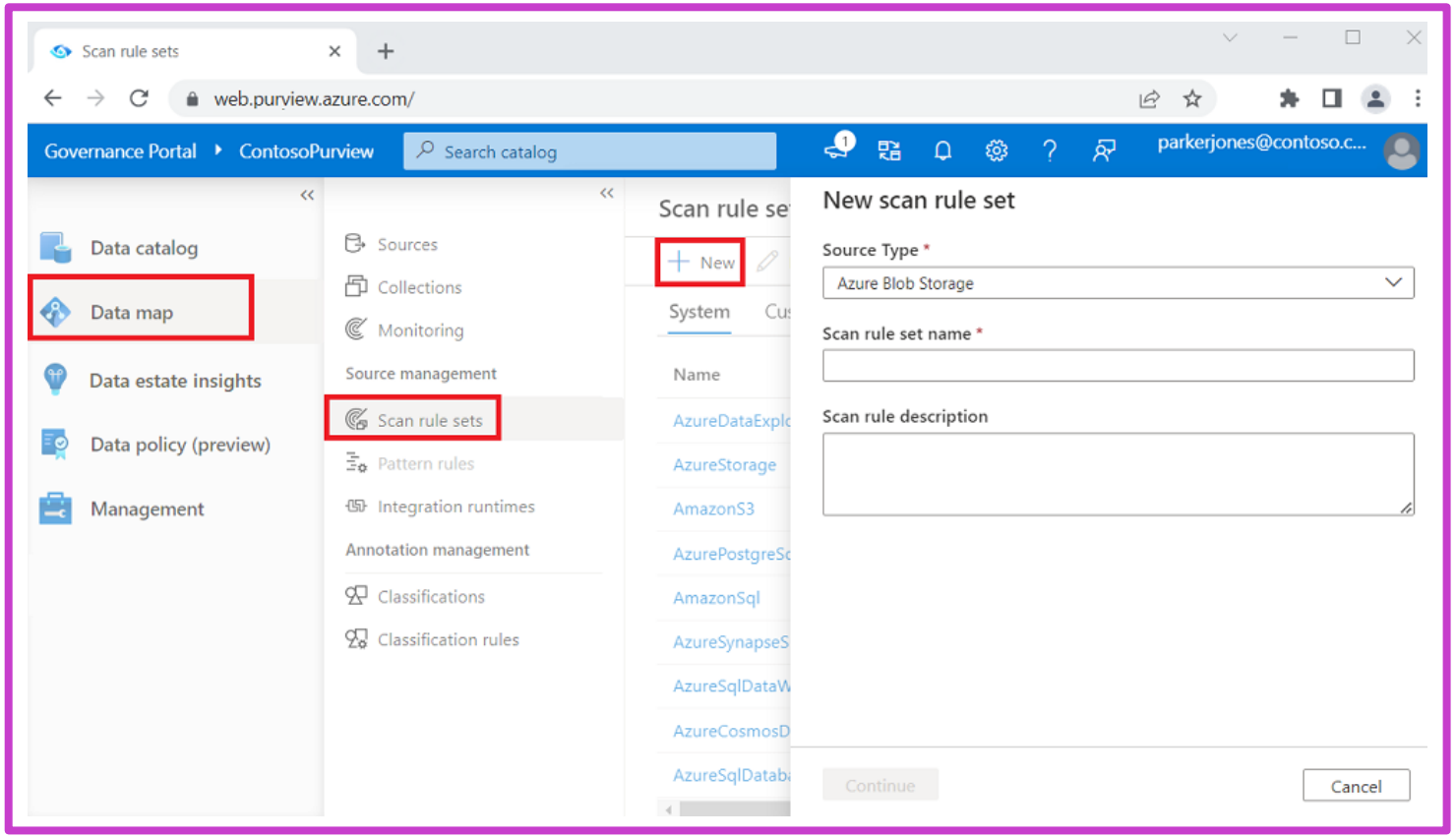
© Copyright Microsoft Corporation. All rights reserved.

Microsoft Purview governance-Create a scan rule set

Scan rule set

In a Microsoft Purview catalog, you can create scan rule sets to enable you to quickly scan data sources in your organization.

- Scan rule sets group scan rules for easy association with scans.
- Default sets can be created for various data source types and used company-wide.
- Users with permissions can craft custom rule sets for specific business requirements.



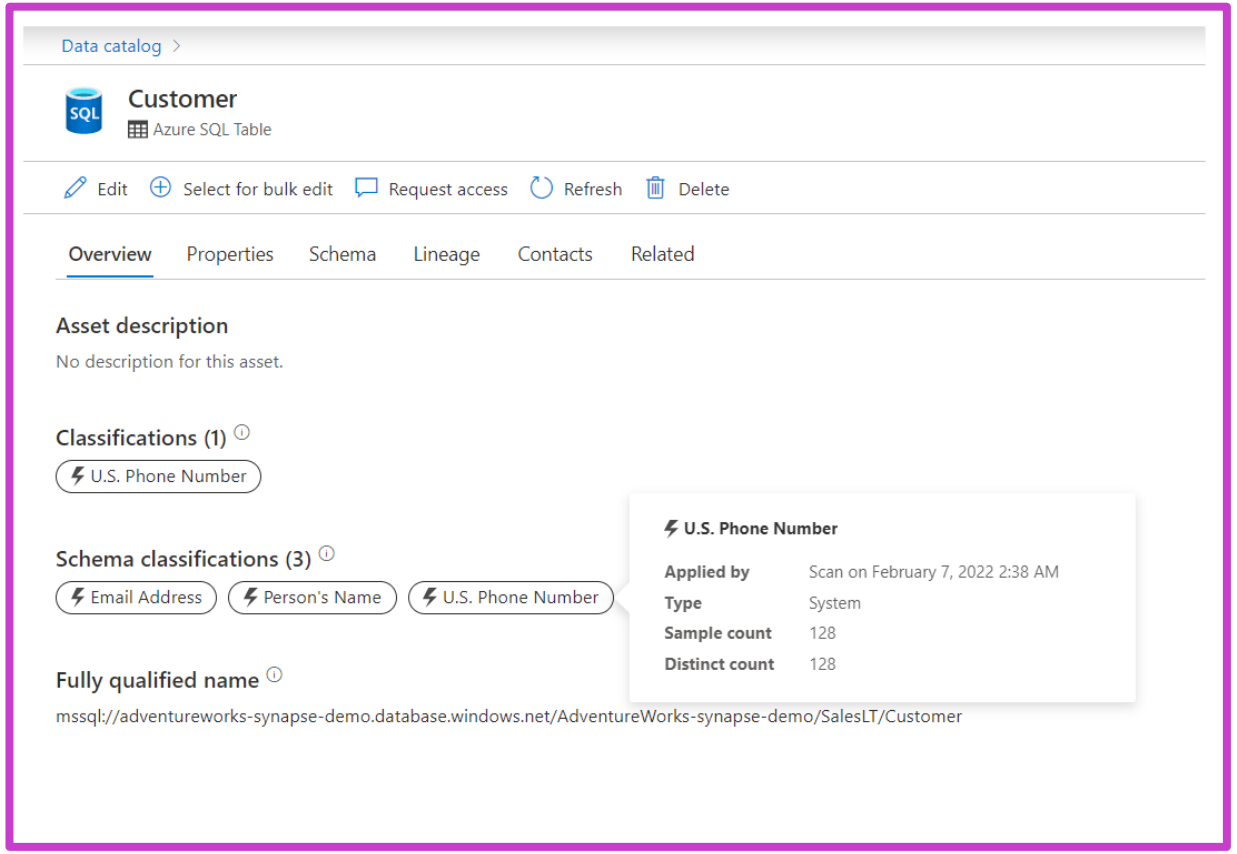
© Copyright Microsoft Corporation. All rights reserved.

Microsoft Purview governance-Data classification

Apply classifications

Data classification in the Microsoft Purview governance portal is a way of categorizing data assets by assigning unique logical tags or classes to the data assets.

- Microsoft Purview's data classification relies on business context, enabling asset categorization like Passport Numbers, Driver's License Numbers, Credit Card Numbers, SWIFT (Society for Worldwide Interbank Financial Telecommunications Codes), and similar data types.
- Classification aids in understanding, searching, and governing data, assessing associated risks, and implementing protective measures.
- Purview's automated classification offers 200+ system classifications, with options for customizing and editing in the governance portal.



© Copyright Microsoft Corporation. All rights reserved.

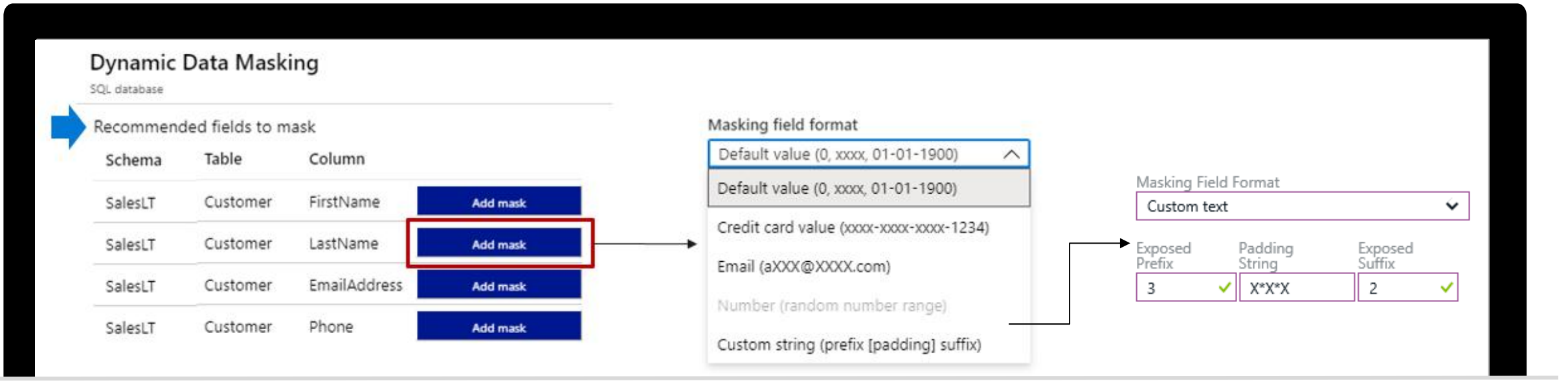
Labeling in the Microsoft Purview Data Map

Labeling

- Collaboration inside/outside the organization means data roams across devices and services, needing security aligned with policies.
- Sensitivity labels help secure data by indicating its sensitivity level, aiding in compliance without exposing actual data.
- Labels like 'highly confidential' identify document sensitivity (e.g., containing social security and credit card numbers) without revealing specifics.

© Copyright Microsoft Corporation. All rights reserved.

Plan and implement dynamic masking

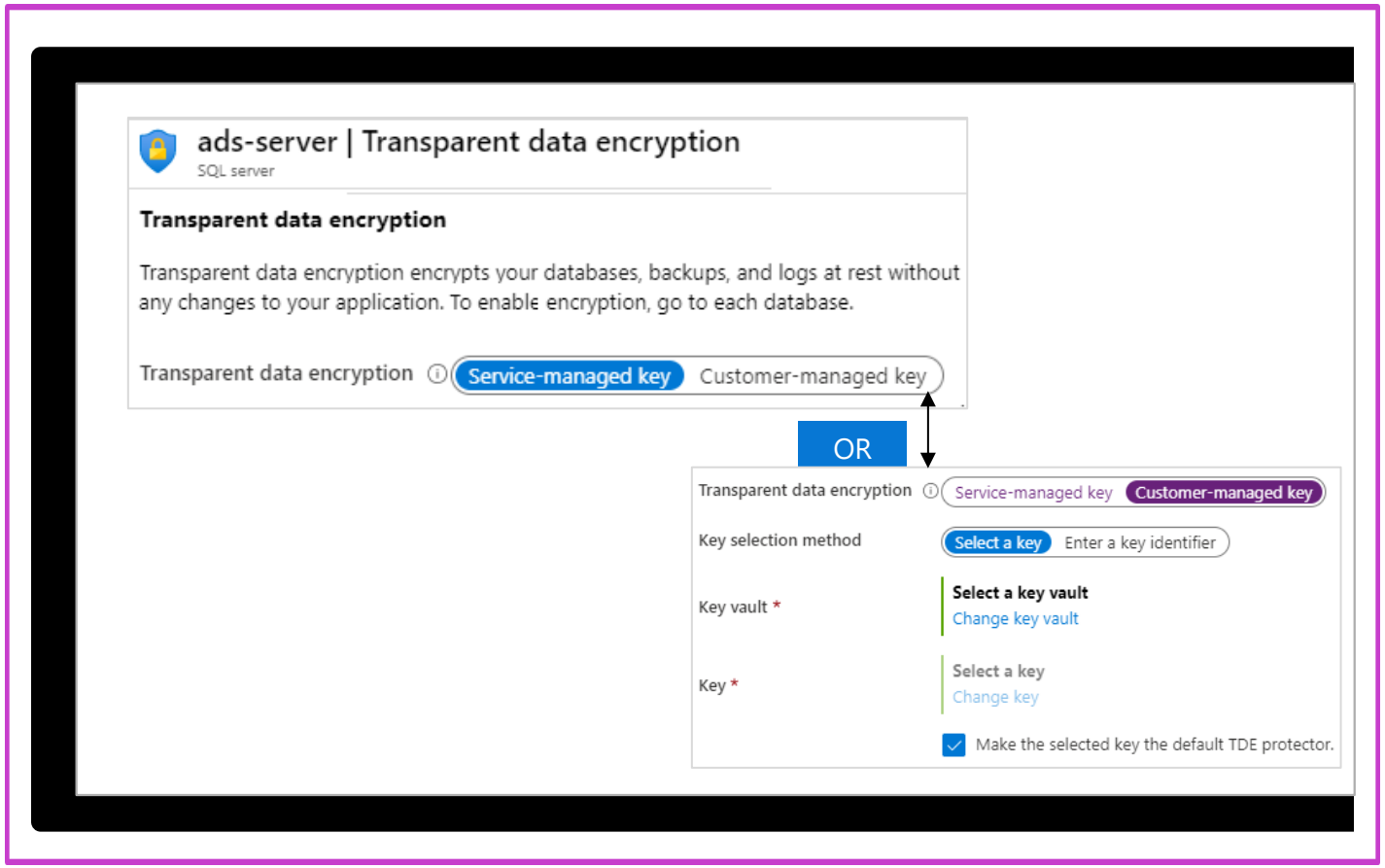


- Masks sensitive data for non-privileged users
- Administrators are excluded; you can add others
- Rules apply the masking logic; several formats are available

© Copyright Microsoft Corporation. All rights reserved.

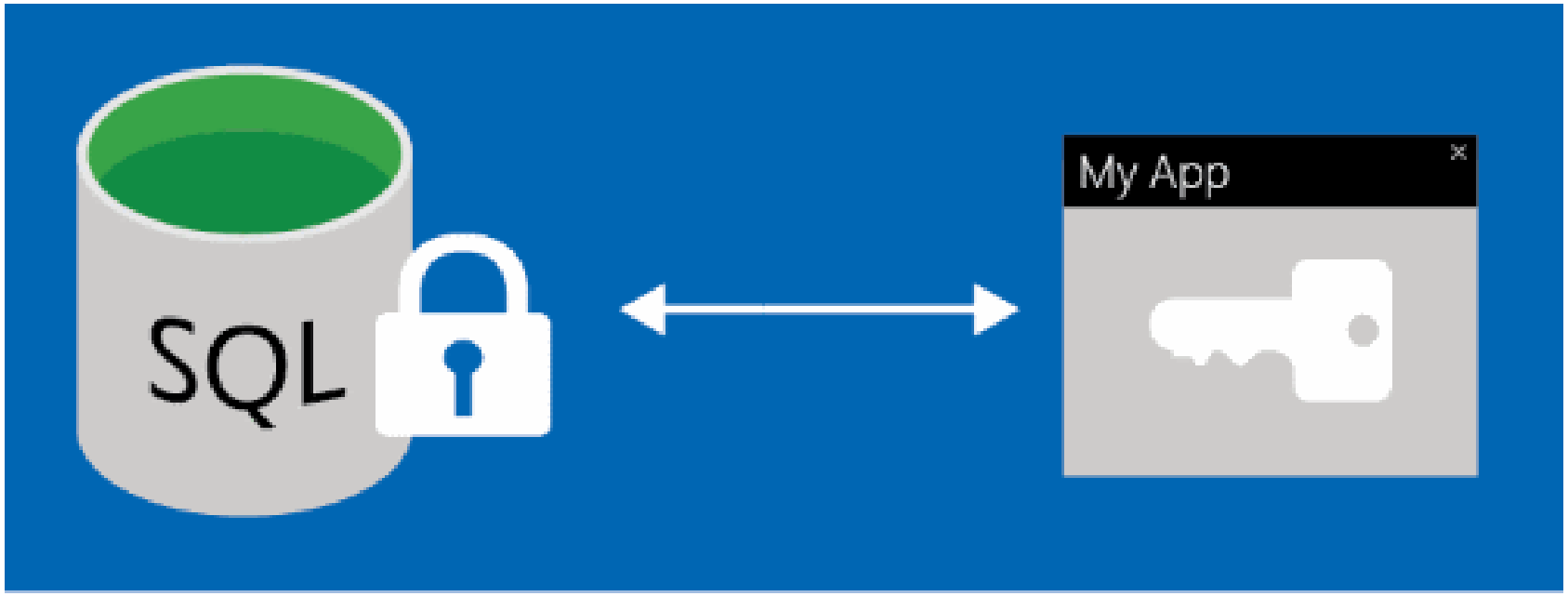
Implement Transparent Data Encryption (TDE)

- Protects databases, backups, and logs at rest – server level
- Real-time page level encryption and decryption – service or customer managed keys
- Supports Azure SQL Database (enabled by default), SQL Managed Instance, SQL Server on VM (IaaS SQL Server), and Azure Synapse Analytics



© Copyright Microsoft Corporation. All rights reserved.

Recommend when to use Azure SQL Database Always Encrypted



- Always Encrypted protects sensitive data in Azure SQL platforms.
- Clients encrypt data in applications without revealing encryption keys to Database Engine.
- Ensures data owner visibility while preventing unauthorized access, reducing data theft risks.

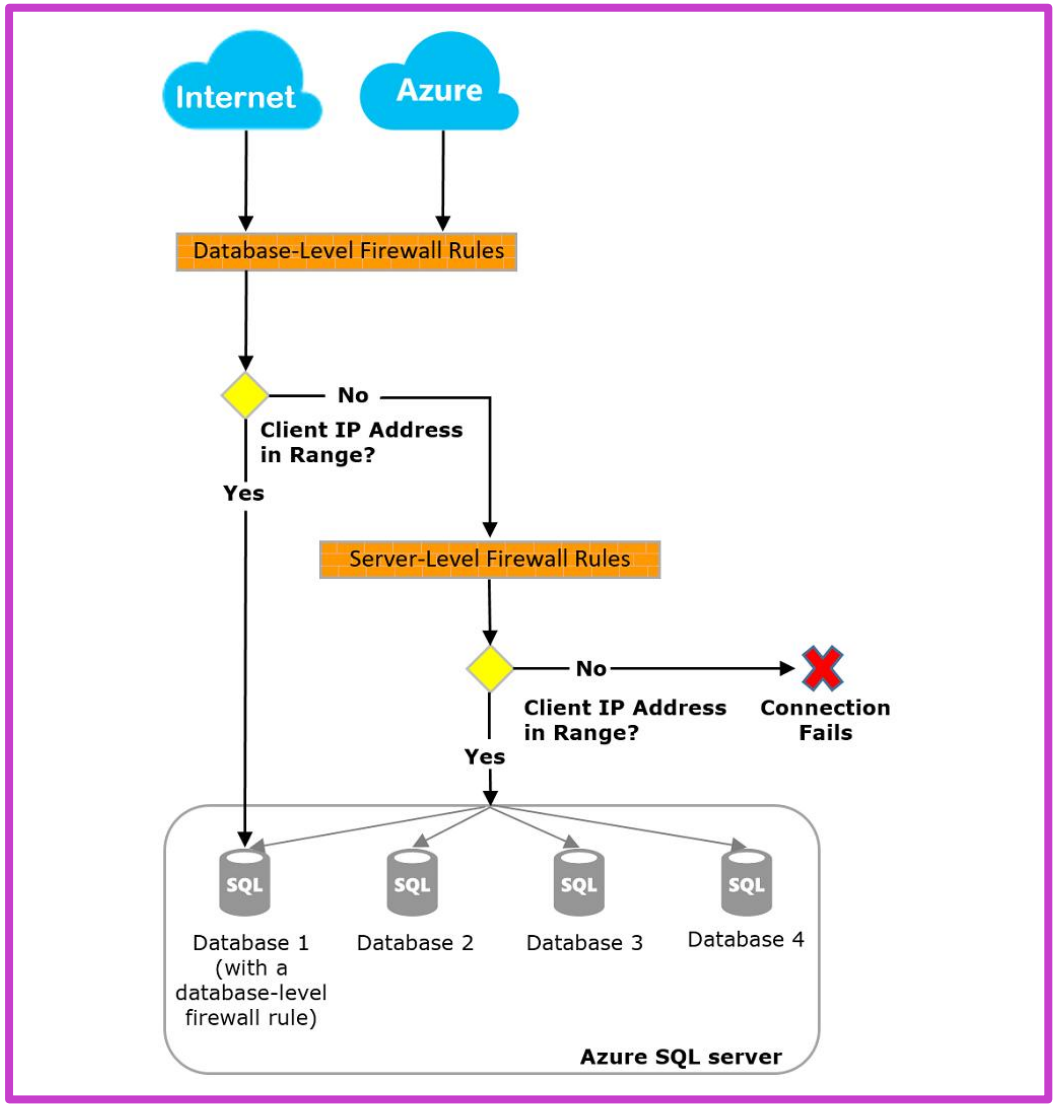
© Copyright Microsoft Corporation. All rights reserved.

Recommend when to use Always Encrypted

© Copyright Microsoft Corporation. All rights reserved.

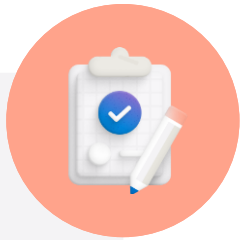
Implement an Azure SQL Database firewall

- Azure SQL Database and Synapse Analytics block public endpoint access by default with firewalls.
- Use server-level or database-level IP firewall rules to manage database access securely.
- Firewall rules can be configured via Azure portal, PowerShell, CLI, or Transact-SQL.



© Copyright Microsoft Corporation. All rights reserved.

Additional Study – Planning and Implementing Security for Azure SQL Database and Azure SQL Managed Instance



Microsoft Learn Modules (docs.microsoft.com/Learn)

Module Review Questions

- Enable Microsoft Entra Database Authentication: Secure database access using Microsoft Entra ID for identity-based authentication.
- Enable Database Auditing: Track and log database activities to ensure security compliance.
- Implement Dynamic Data Masking: Protect sensitive data by masking it from unauthorized users.
- Apply Transparent Data Encryption (TDE): Encrypt SQL databases at rest to protect data.
- Use Always Encrypted for Sensitive Data: Encrypt sensitive data in use to protect it from unauthorized access.

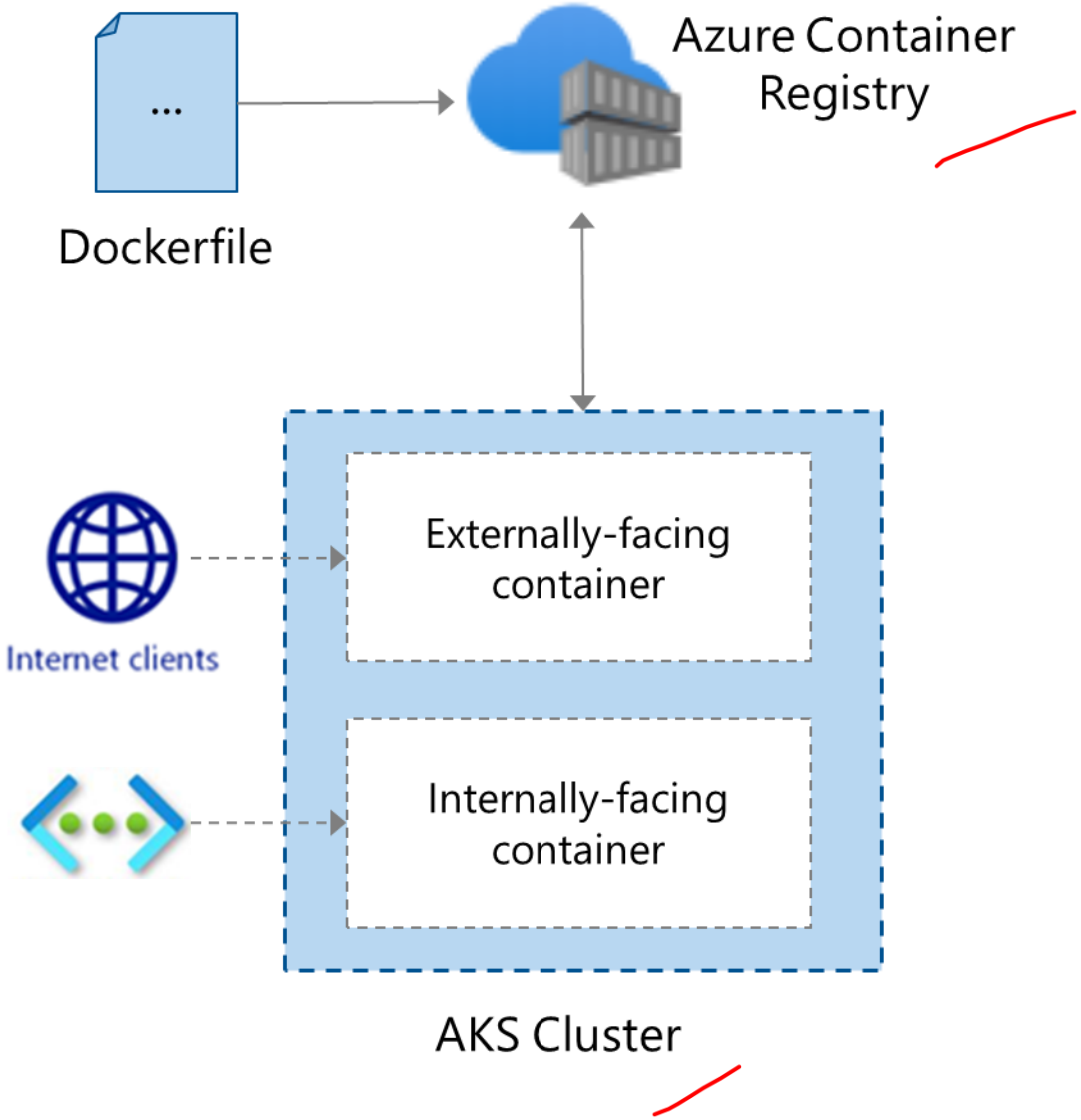
© Copyright Microsoft Corporation. All rights reserved.

Module Labs

© Copyright Microsoft Corporation. All rights reserved.

Lab 04 – Configuring and securing ACR and AKS

- Create an Azure Container Registry
- Create a Dockerfile, build a container and push it to ACR
- Create an Azure Kubernetes Service
- Give AKS permission to access the ACR
- Deploy an external facing container and test
- Deploy an internal facing container and test

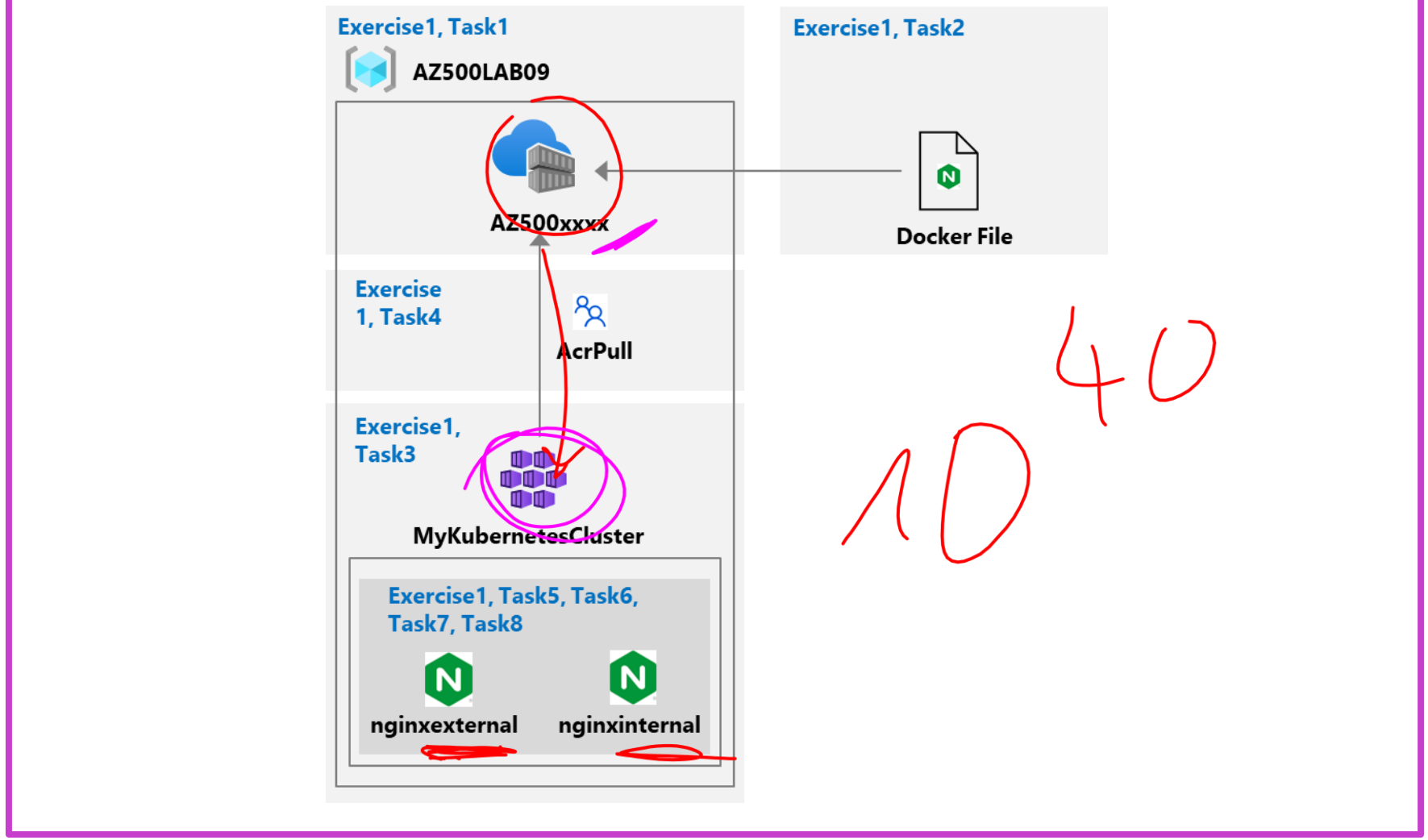


© Copyright Microsoft Corporation. All rights reserved.

Lab 04 – Configuring and securing ACR and AKS

This exercise teaches students how to deploy a proof of concept with Azure Container Registry and Azure Kubernetes Service by building images with Dockerfile, storing them in ACR, configuring AKS, and securing container app access

[Launch this Exercise in GitHub]



© Copyright Microsoft Corporation. All rights reserved.

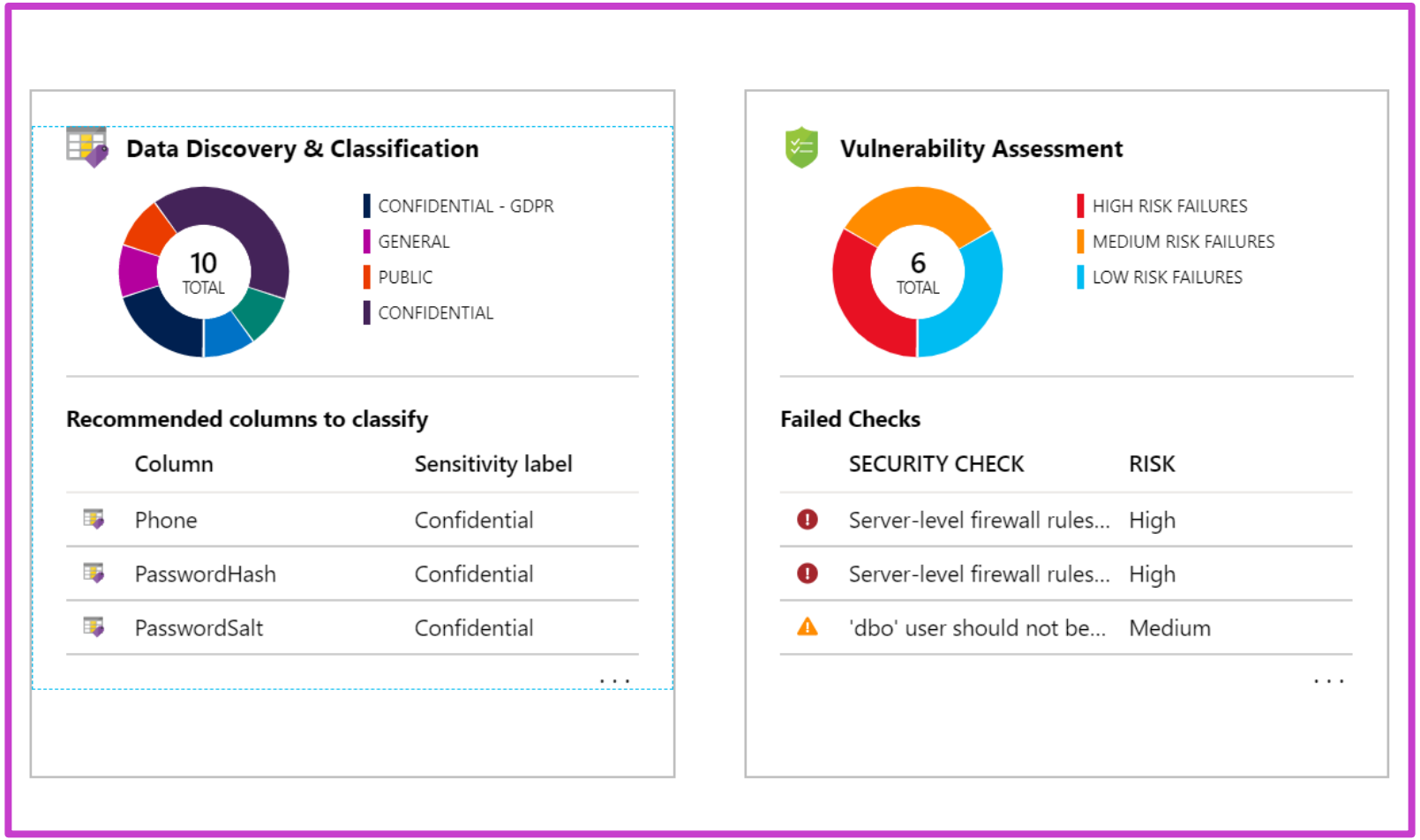
Lab 05 – Securing Azure SQL Database

Deploy an Azure SQL Database

Configure Advanced Data Protection

Configure Data Classification

Configure Auditing

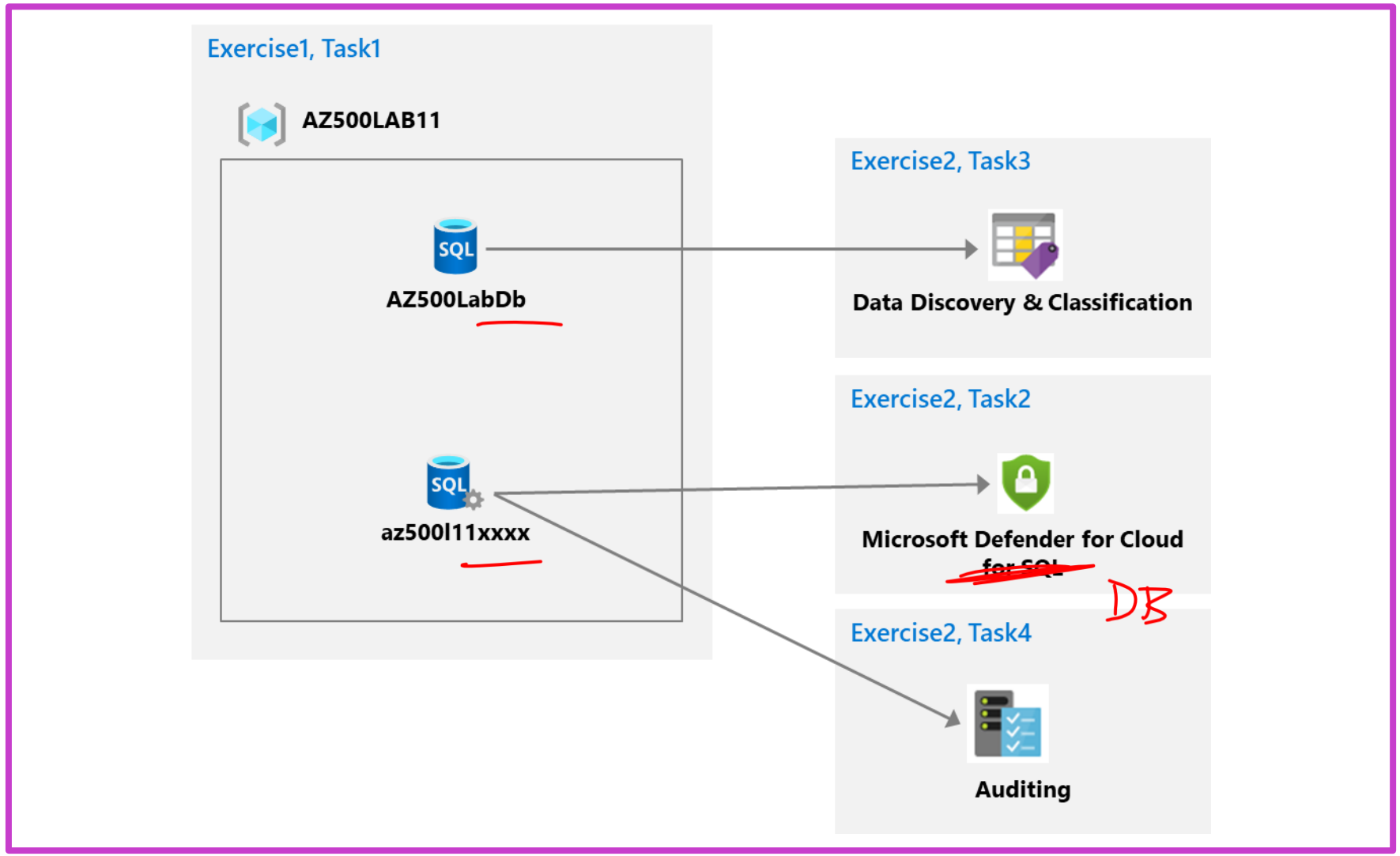


© Copyright Microsoft Corporation. All rights reserved.

Lab 05 – Securing Azure SQL Database

This exercise teaches students to review Azure SQL Database security features, including attack protection, data classification, and auditing of servers, queries, and events.

[Launch this Exercise in GitHub]



© Copyright Microsoft Corporation. All rights reserved.

Lab 06 – Service Endpoints and Securing Storage

Create a virtual network with a Public and Private subnet

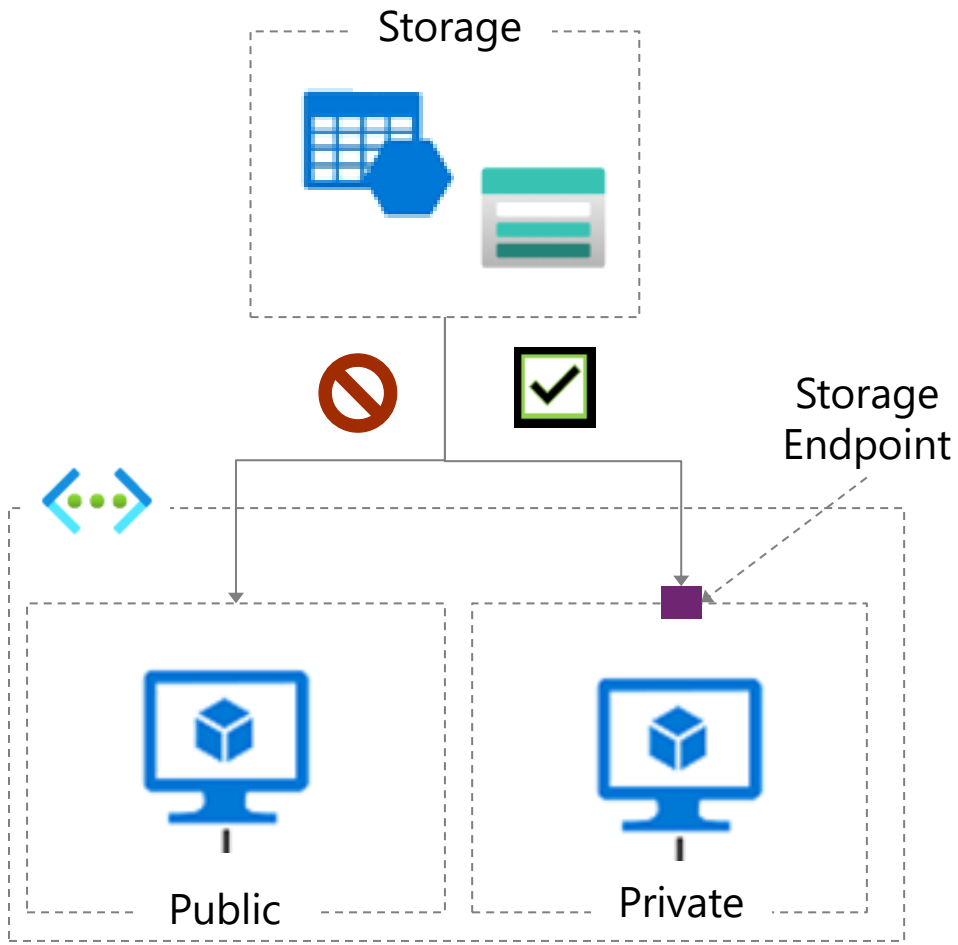
Create a storage endpoint for the Private subnet

Create a storage account with a file share

Configure a NSG with rules to allow access to storage and internet

Confirm storage access from the private subnet

Confirm storage access is denied from the public subnet

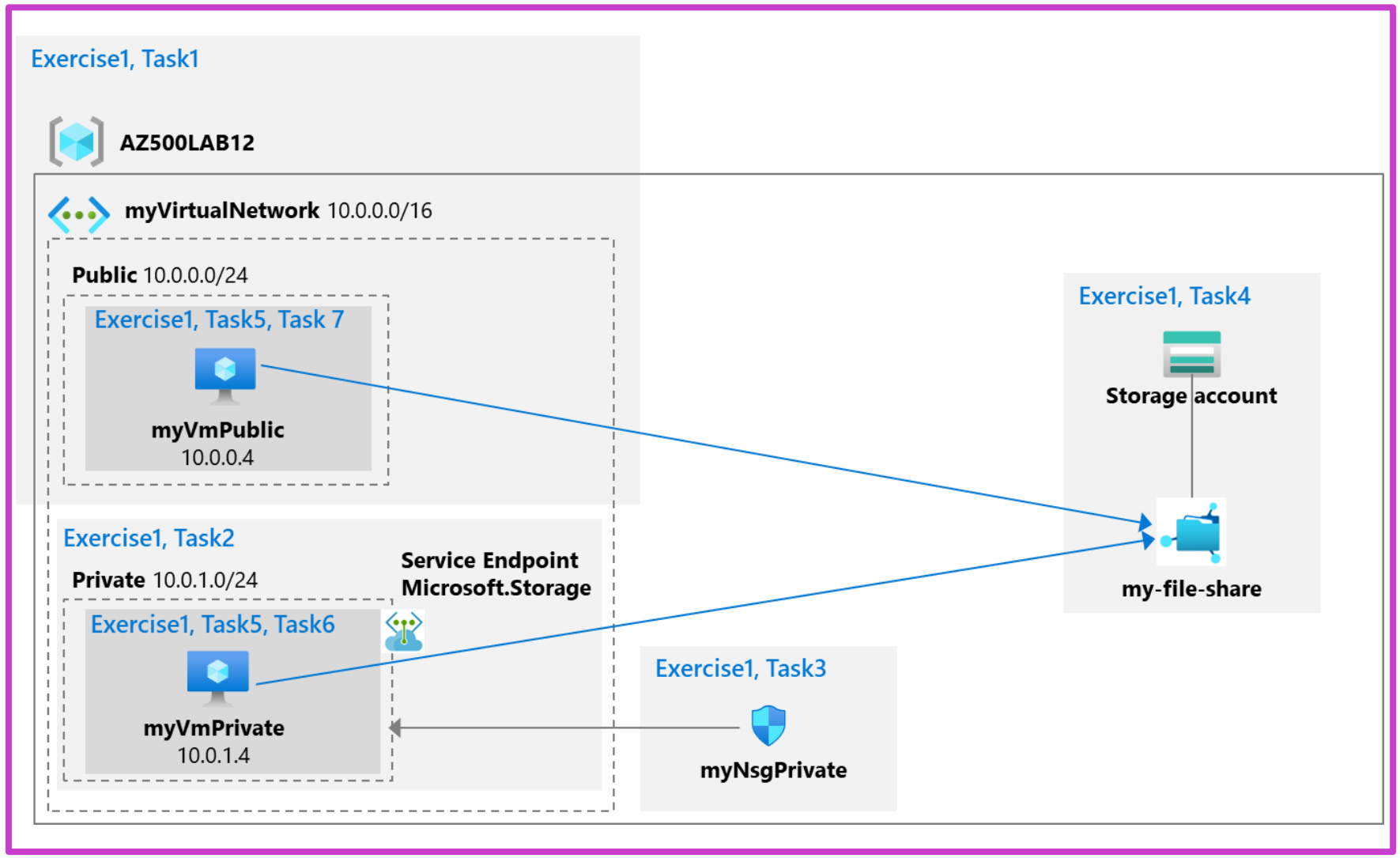


© Copyright Microsoft Corporation. All rights reserved.

Lab 06 – Service Endpoints and Securing Storage

This exercise teaches students how to create a proof of concept to secure Azure file shares by configuring a storage endpoint for Azure backbone traffic, restricting subnet access, and blocking external resources.

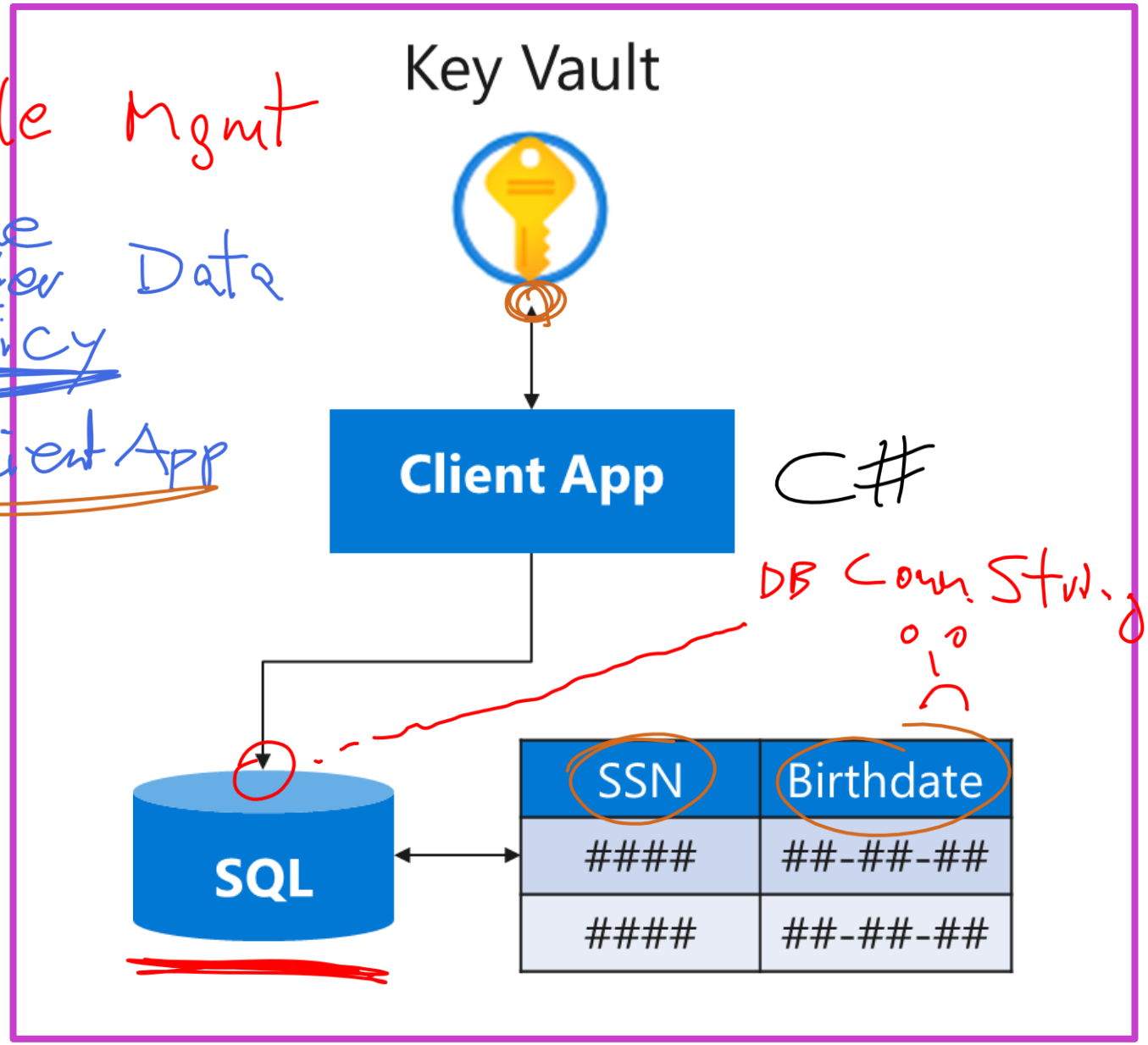
[Launch this Exercise in GitHub]



© Copyright Microsoft Corporation. All rights reserved.

Lab 07 – Key Vault

- Create a Key Vault and configure permissions
- Add a key and a secret to the vault
- Register a client app that uses the key
- Create a SQL database
- Encrypt columns in a table
- Build a console app to test the encryption

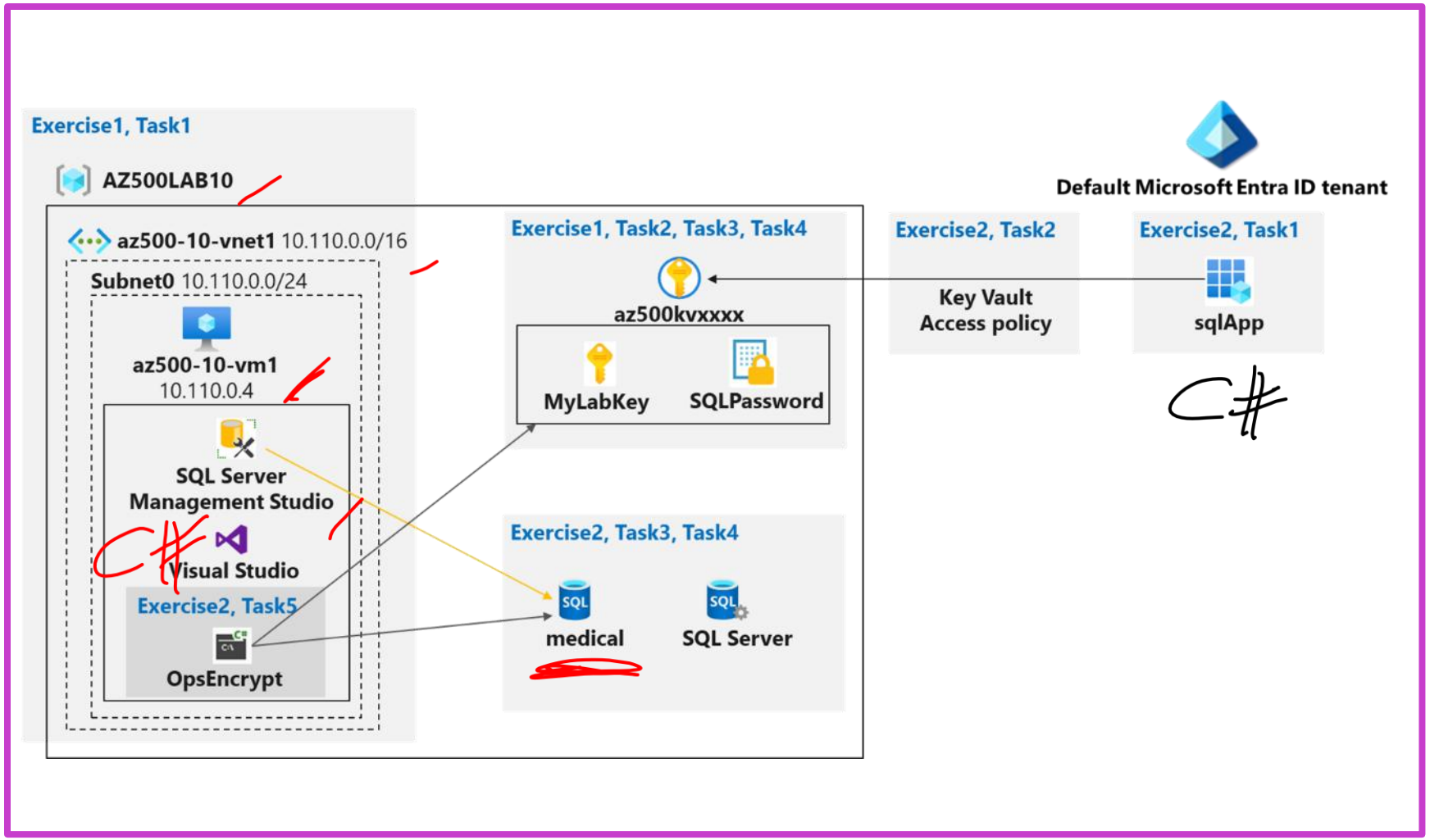


© Copyright Microsoft Corporation. All rights reserved.

Lab 07 – Key Vault

This exercise teaches students how to create an Azure Key Vault and store keys and secrets in the vault, create a SQL Database, and encrypt the content of columns in database tables by using Always Encrypted.

[Launch this Exercise in GitHub]



© Copyright Microsoft Corporation. All rights reserved.

Knowledge check

1 **How does scanning in Microsoft Purview handle classifications and sensitivity labels?**

- ☐ It ignores them during the scanning process
- ☑ It applies them to the gathered technical metadata and schema
- ☐ It deletes them from the system

2 **Which Azure service provides serverless, automatic, and scalable data encryption for data at rest?**

- ☐ Azure Key Vault
- ☑ Azure Storage Service Encryption
- ☐ Azure Sentinel

3 **In Azure SQL Database, what is Transparent Data Encryption (TDE) used for?**

- ☐ Managing access control for Azure SQL Database
- ☑ Encrypting data at rest and in motion
- ☐ Automatically scaling the database resources

© Copyright Microsoft Corporation. All rights reserved.

Learning Path Recap

In this learning path, we:

Implemented advanced compute security with Azure Bastion, JIT, AKS isolation, authentication, and encryption techniques.

Established robust storage security through access controls, data protection methods, and advanced encryption techniques.

Enhanced Azure SQL Database security via Microsoft Entra ID authentication, auditing, data classification, and encryption methods.

© Copyright Microsoft Corporation. All rights reserved.

End of presentation

© Copyright Microsoft Corporation. All rights reserved.