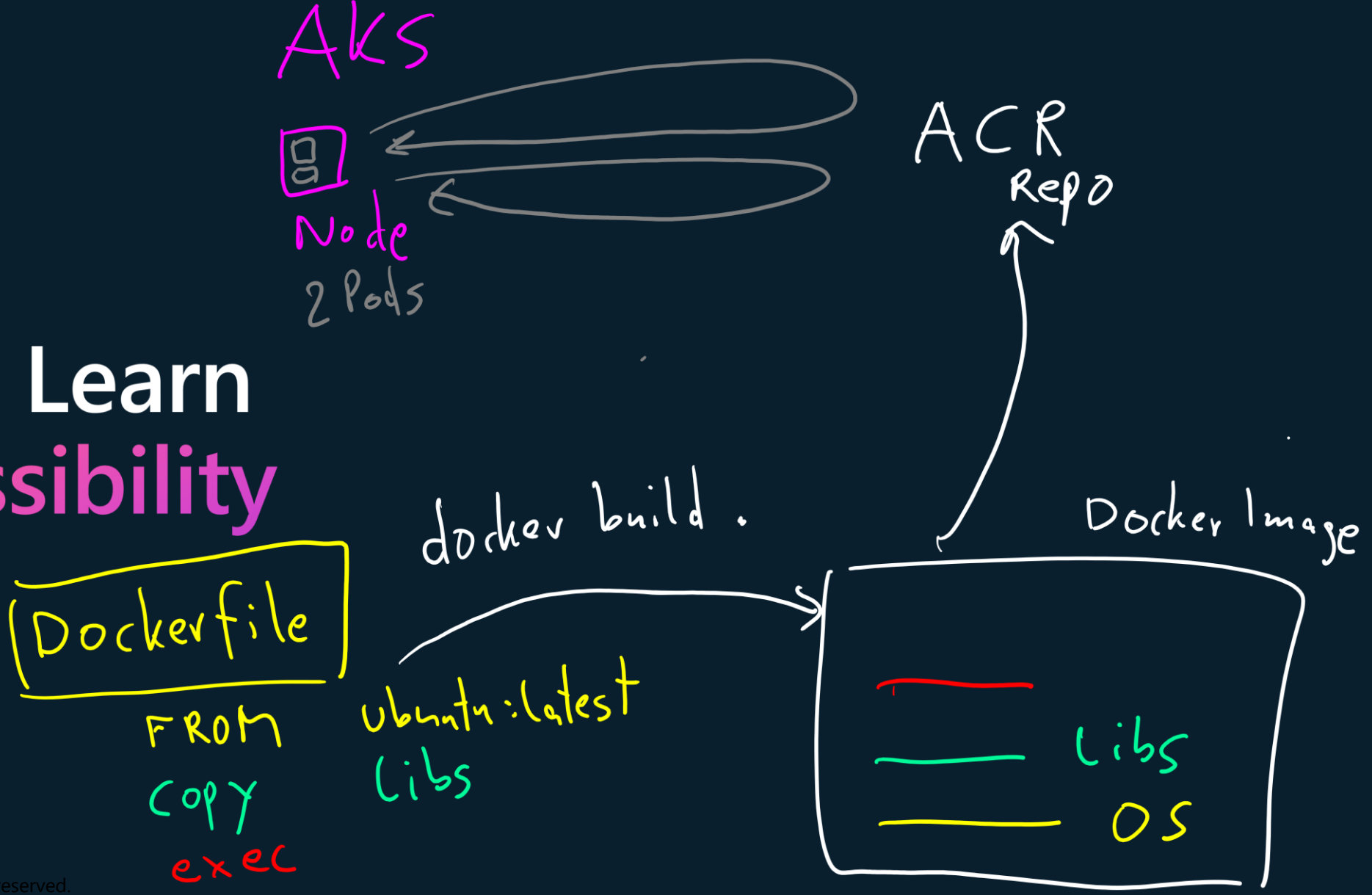
Microsoft

Microsoft Learn
Spark possibility



Microsoft

AZ-500

Microsoft Azure Security Technologies

Agenda

1 Manage identity and access

2 Secure networking

3 Secure compute, storage, and databases

4 Manage security operations

Cosmos DB

Leslie Lamport

LaTeX

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

Learning Objectives

After completing this learning path, you will be able to:

1. Strengthen compute security through Azure Bastion, AKS configurations, container monitoring, and advanced encryption techniques.

2. Enhance storage security with tailored access controls, protective measures against threats, and multiple encryption strategies.

3. Bolster Azure SQL Database protection through authentication, auditing, data classification, and advanced encryption recommendations.

Secure compute, storage, and databases

Secure compute, storage, and databases

1. Plan and implement advanced security for compute
2. Plan and implement security for storage
3. Plan and implement security for Azure SQL Database and Azure SQL Managed Instance

Plan and implement advanced security for compute

Plan and implement compute advanced security

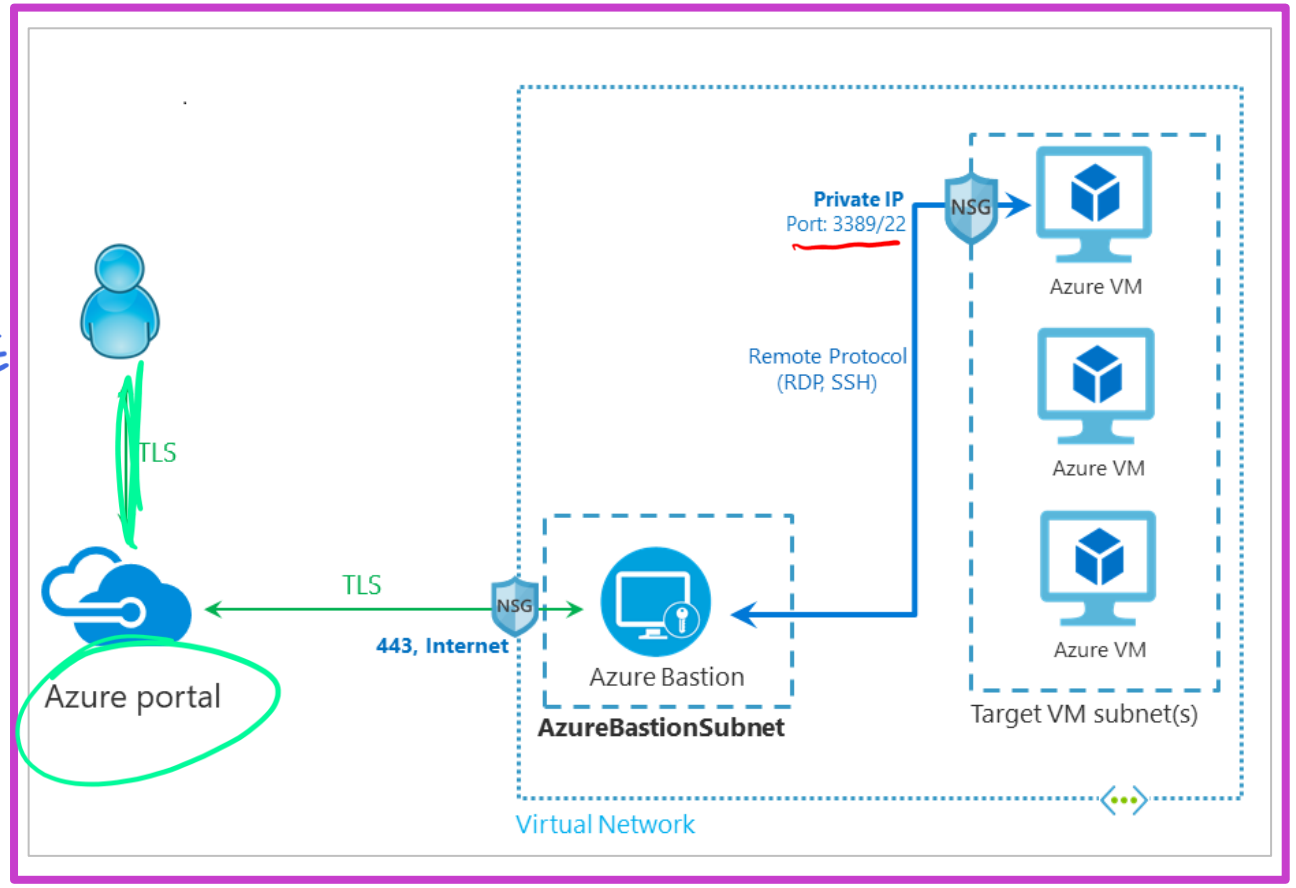
1. Plan and implement remote access to public endpoints, including Azure Bastion and just-in-time (JIT) VM access
2. Configure network isolation for Azure Kubernetes Service (AKS)
3. Secure and monitor AKS
4. Configure authentication for AKS
5. Configure security monitoring for Azure Container Instances (ACIs)
6. Configure security monitoring for Azure Container Apps (ACAs)
7. Manage access to Azure Container Registry (ACR)
8. Configure disk encryption, including Azure Disk Encryption (ADE), encryption as host, and confidential disk encryption
9. Recommend security configurations for Azure API Management

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

Remember these key points while you plan and implement remote access to public endpoints:

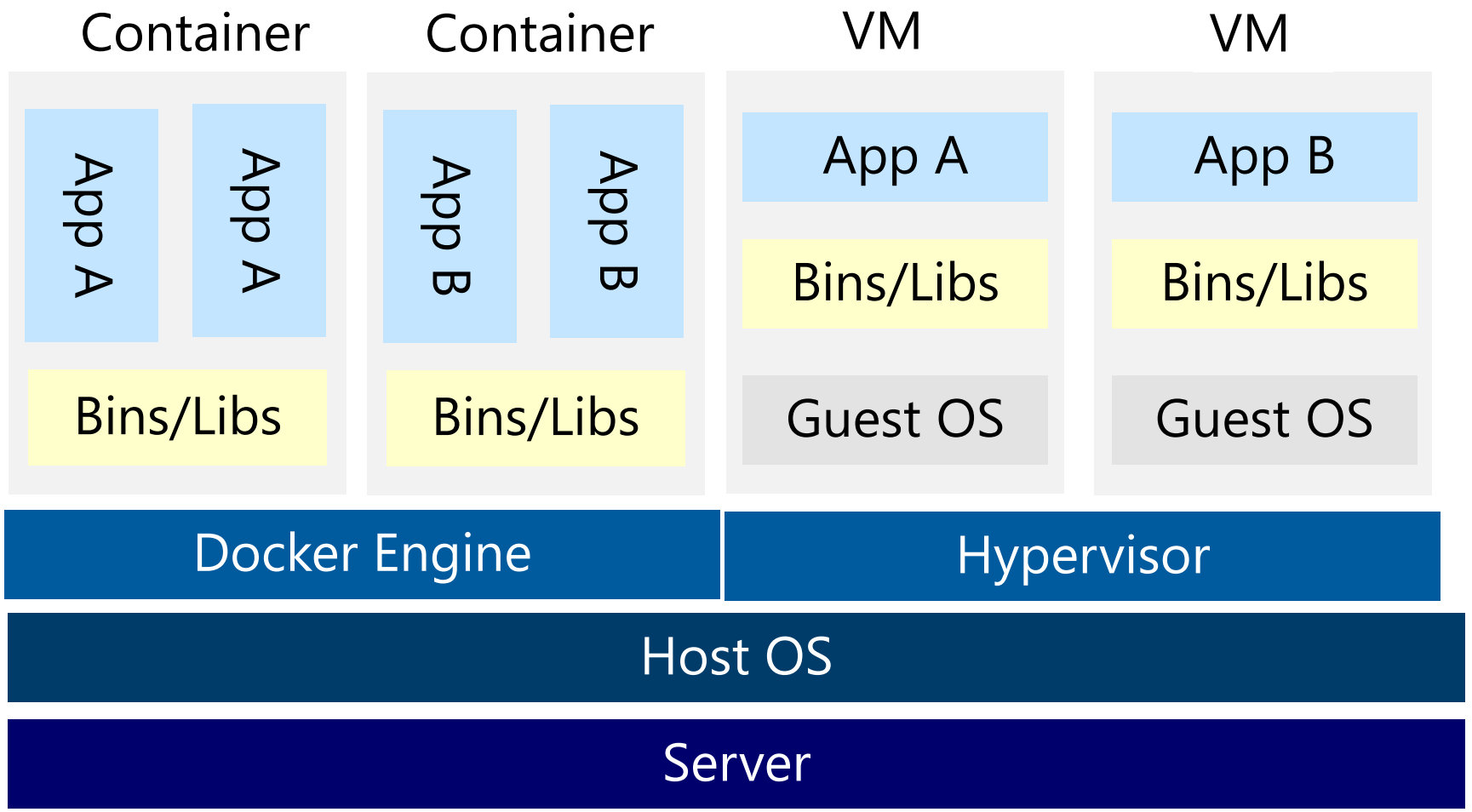
Azure Bastion

- Enables secure RDP/SSH sessions over TLS without public IP on Azure VM.
- Comes in two SKUs: Basic and Standard, ensuring secure perimeter deployments.
- Supports manual scaling and minimizes RDP/SSH exposure online.



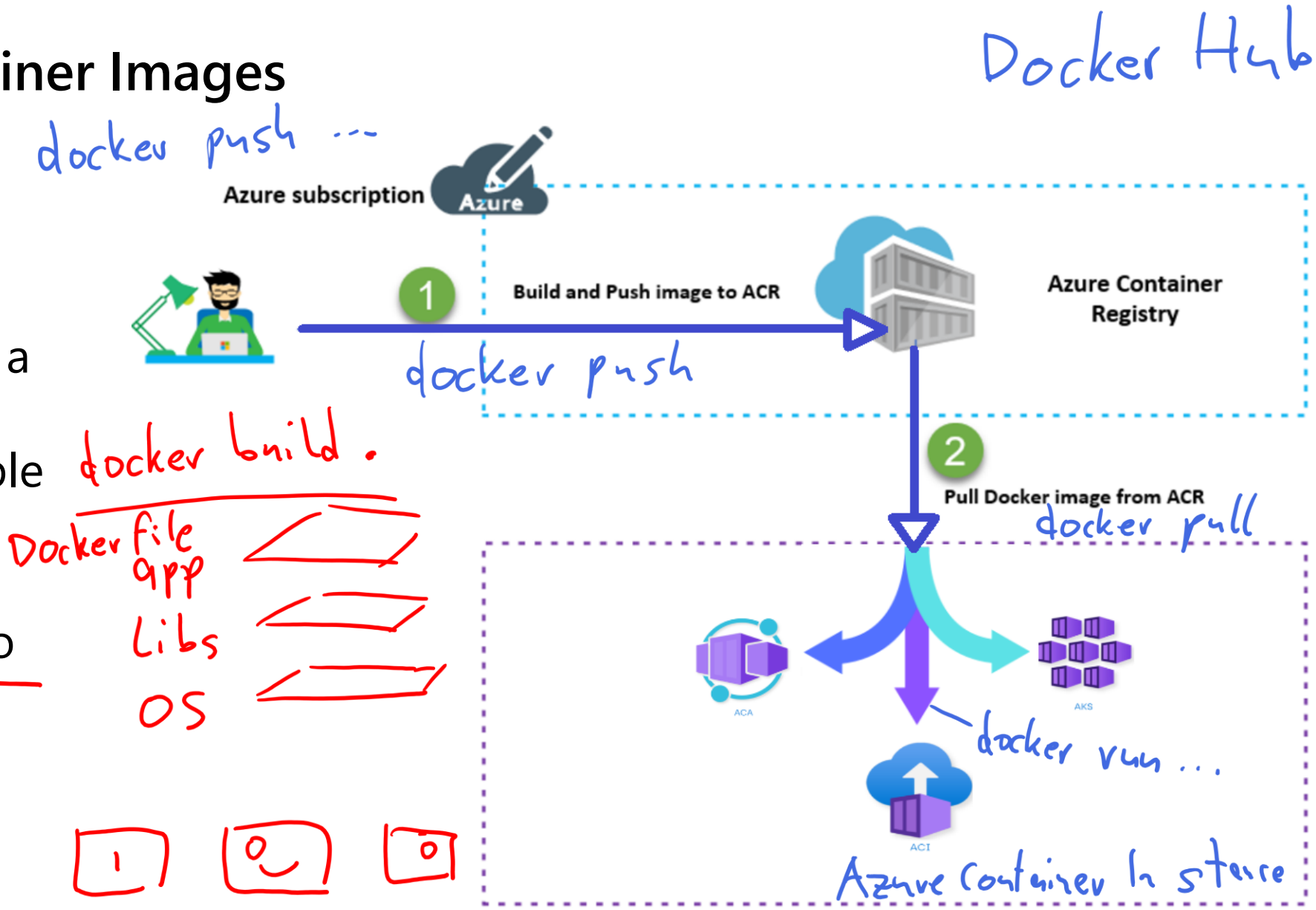
Compare Containers to Virtual Machines

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



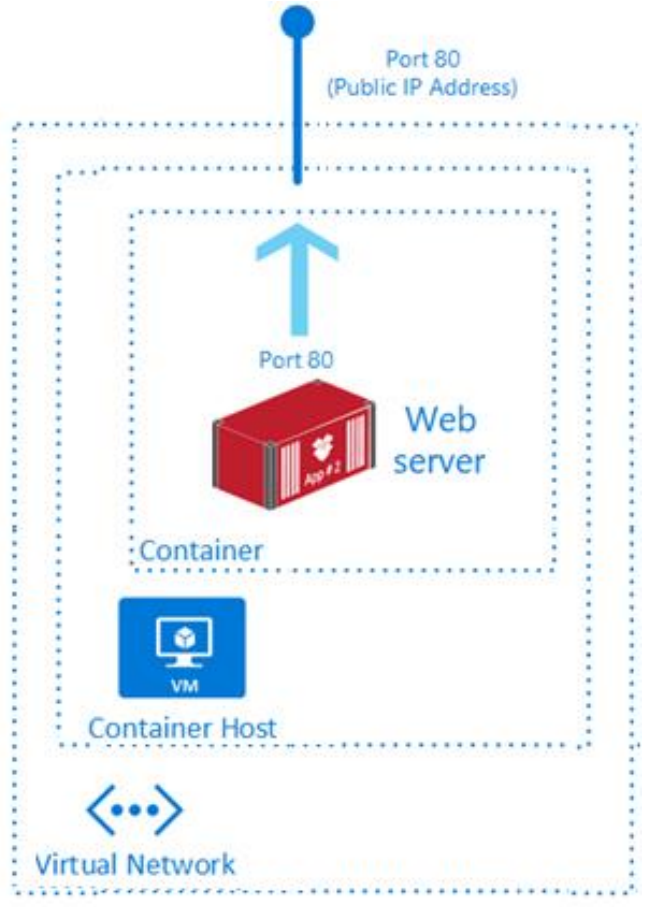
Understand Container Images

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



Review Azure Container Instances

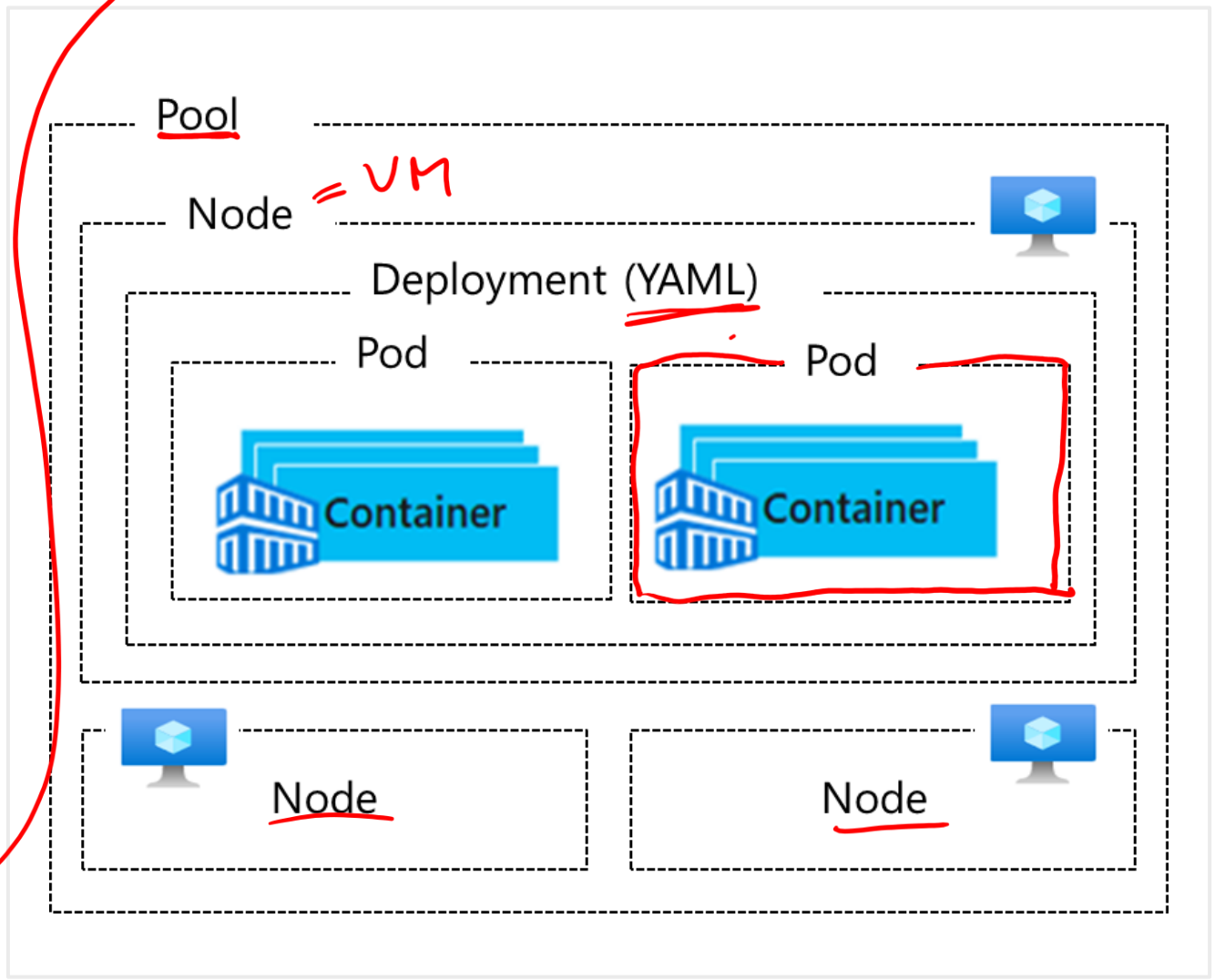
- PaaS Service
- Fast startup times
- Public IP connectivity and DNS name
- Isolation features
- Custom sizes
- Persistent storage
- Linux and Windows Containers
- Co-scheduled Groups
- Virtual network Deployment



Fastest way to run a container in Azure without provisioning a VM

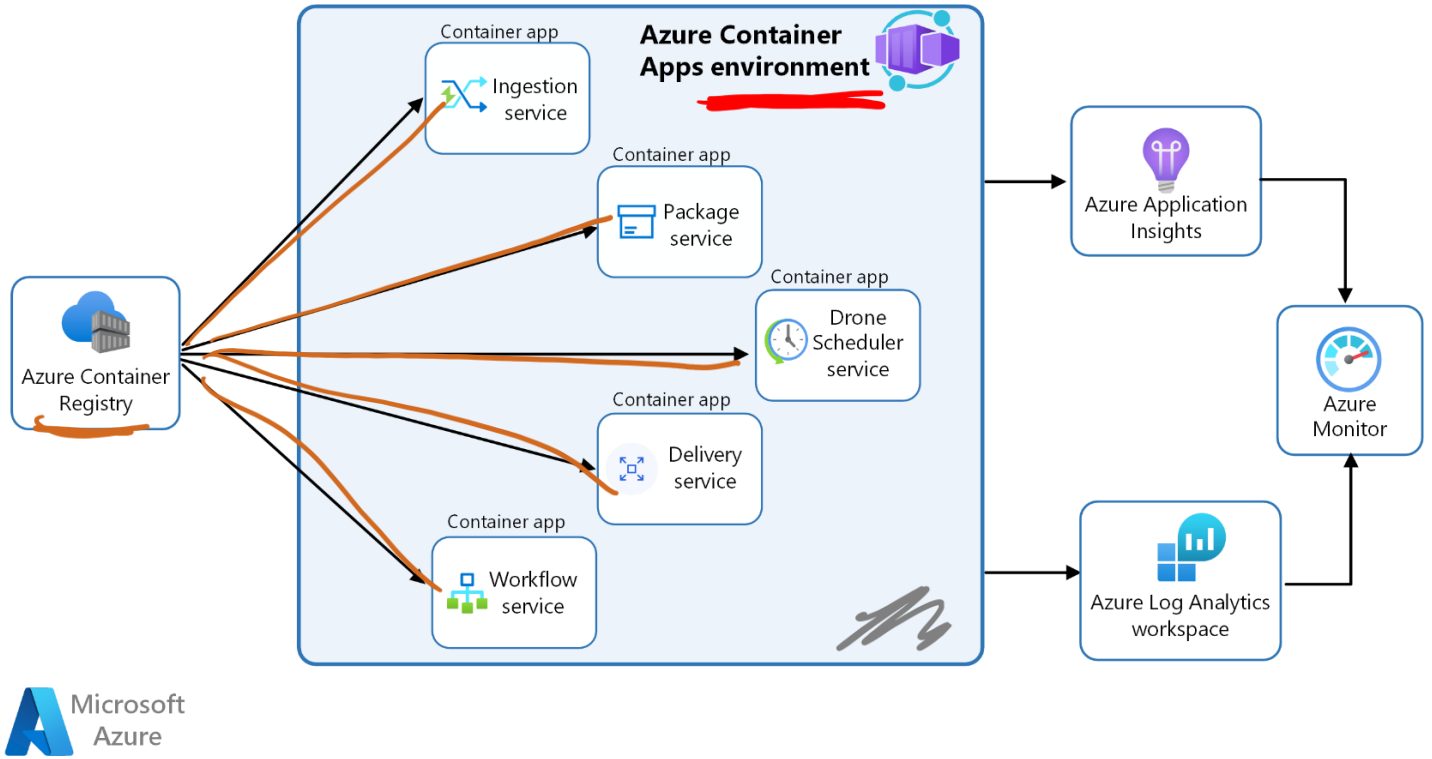
Understand AKS Terminology

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



Manage Containers with Azure Container Apps

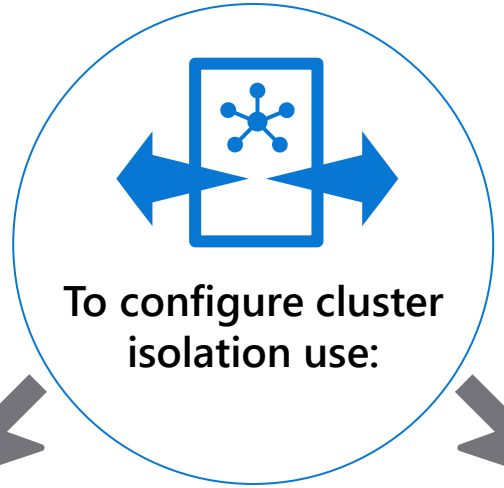
- Alternative to Azure Kubernetes Service – manages container orchestration
- The Container App environment creates a secure boundary around the apps and jobs
- The Container App runtime manages the environment (OS upgrades, scaling, versioning, and failover)



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.

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.

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.

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.

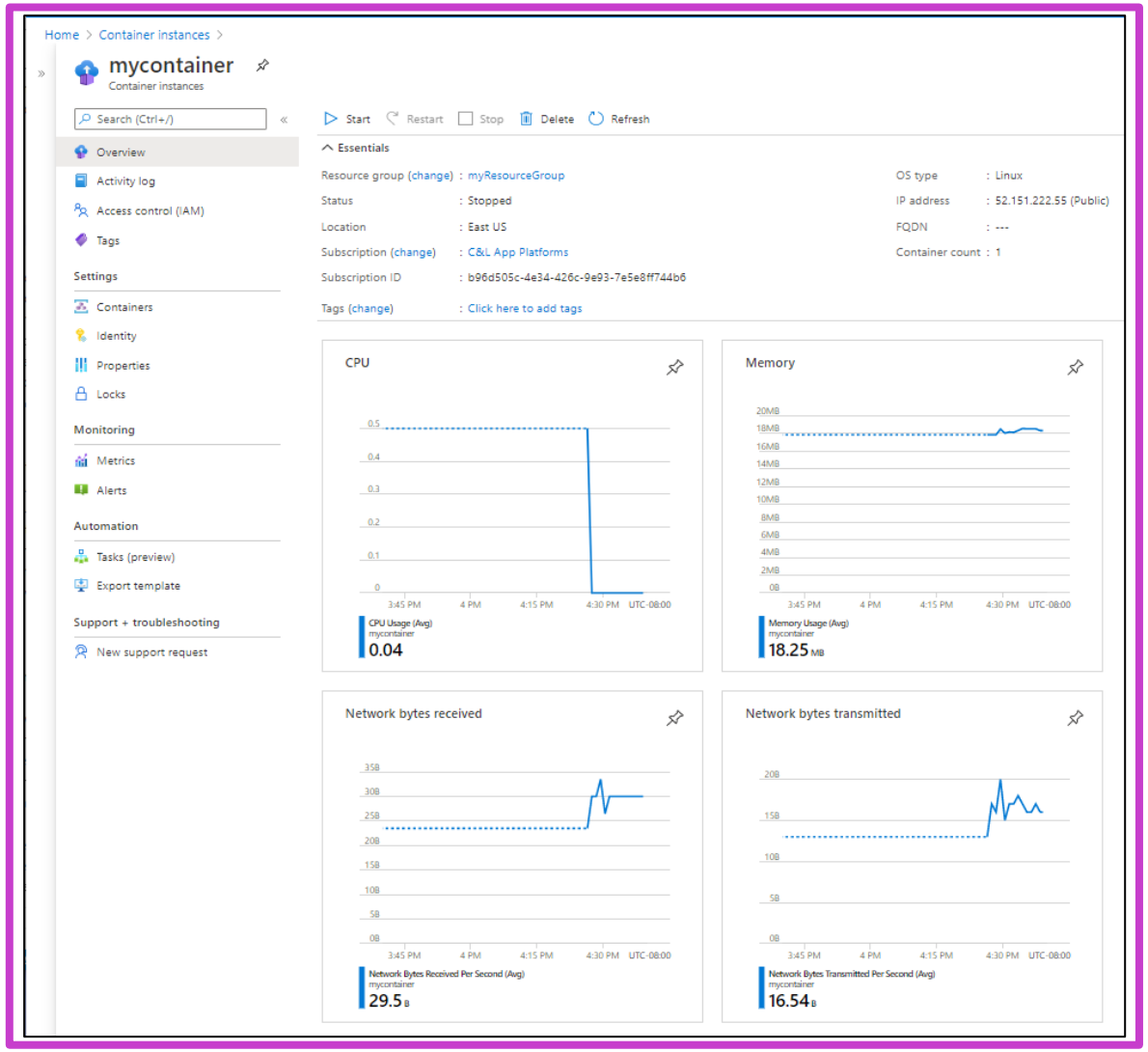
Remember these limitations:

- 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.

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.

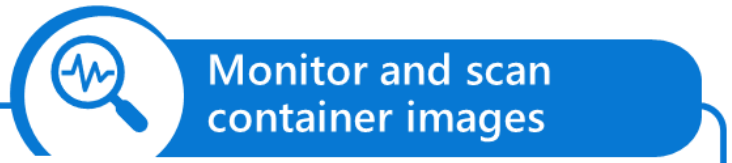


Get metrics - Azure CLI

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

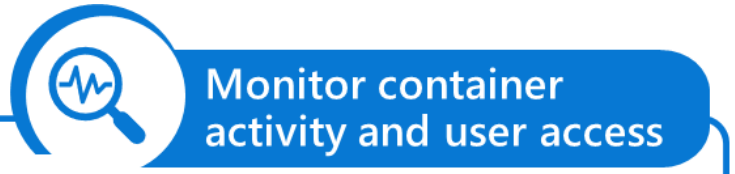
```
CONTAINER_GROUP=$(az container show --
resource-group <resource-group> --name
<container-group> --query id --output tsv)
```

Configure security monitoring for Azure Container Apps



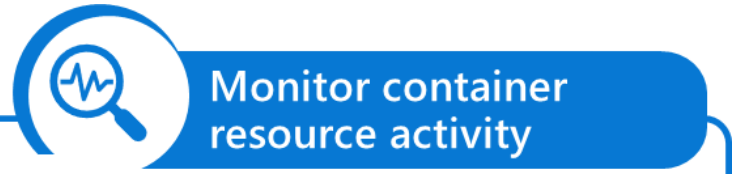
Monitor and scan container images

- 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.

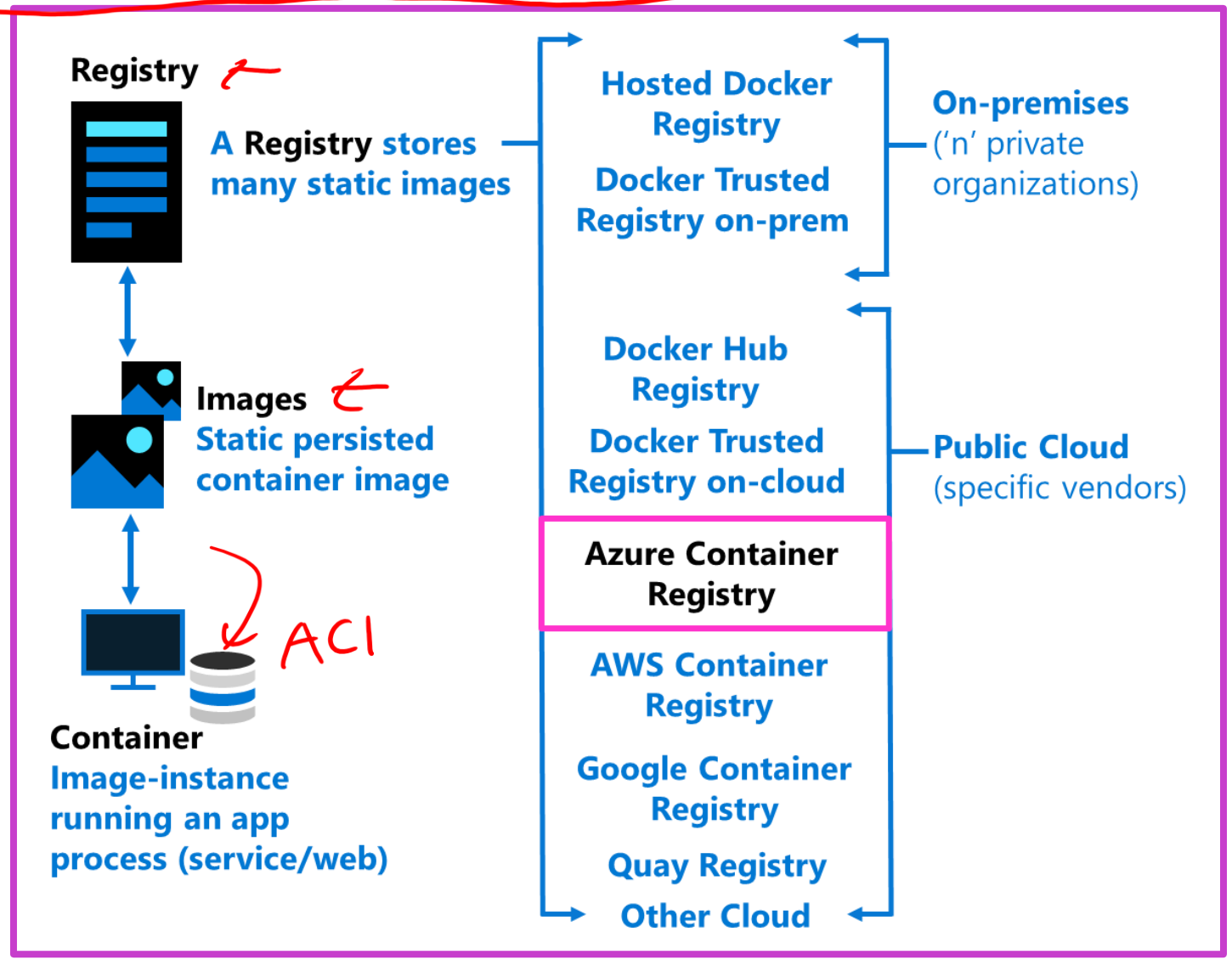


Monitor container resource activity

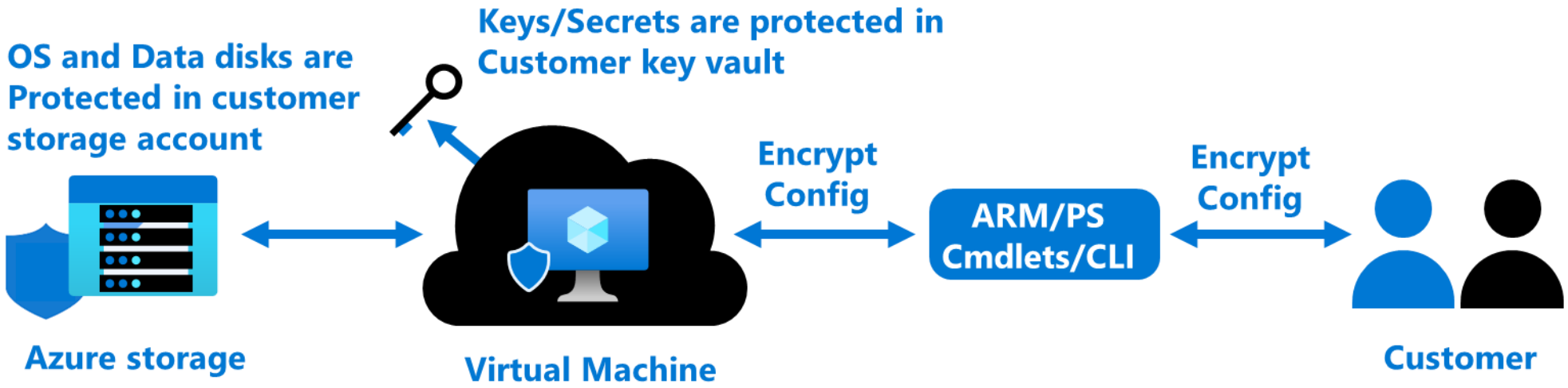
- Monitor your resource activity such as files and other resources that your containers access.
- Use Azure Monitor for the collection of metrics, activity logs, and diagnostic logs.
- Review metrics for performance statistics for different resources and the operating system inside a VM.

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



Configure disk encryption, including Azure Disk Encryption (ADE), encryption as 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

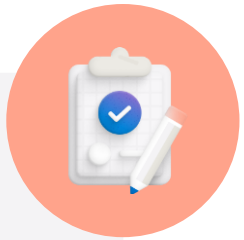
Security configurations for Azure API Management

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.

Additional Study – Container Security



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

Module Review Questions

- Core Cloud Services – Azure compute options
- Build and store container images with Azure Container Registry (Exercise)
- Build a containerized web application with Docker (Exercise)
- Introduction to Docker containers
- Run Docker containers with Azure Container Instances (Exercise)
- Azure Kubernetes Service Workshop (Exercise)

Plan and implement security for storage

Plan and implement storage security

1. Configure access control for storage accounts
2. Manage life cycle for storage account access keys
3. Select and configure an appropriate method for access to Azure Files
4. Select and configure an appropriate method for access to Azure Blob Storage
5. Select and configure an appropriate method for access to Azure Tables
6. Select and configure an appropriate method for access to Azure Queues
7. Select and configure appropriate methods for protecting against data security threats, including soft delete, backups, versioning, and immutable storage
8. Configure Bring your own key (BYOK)
9. Enable double encryption at the Azure Storage infrastructure level

Azure Storage

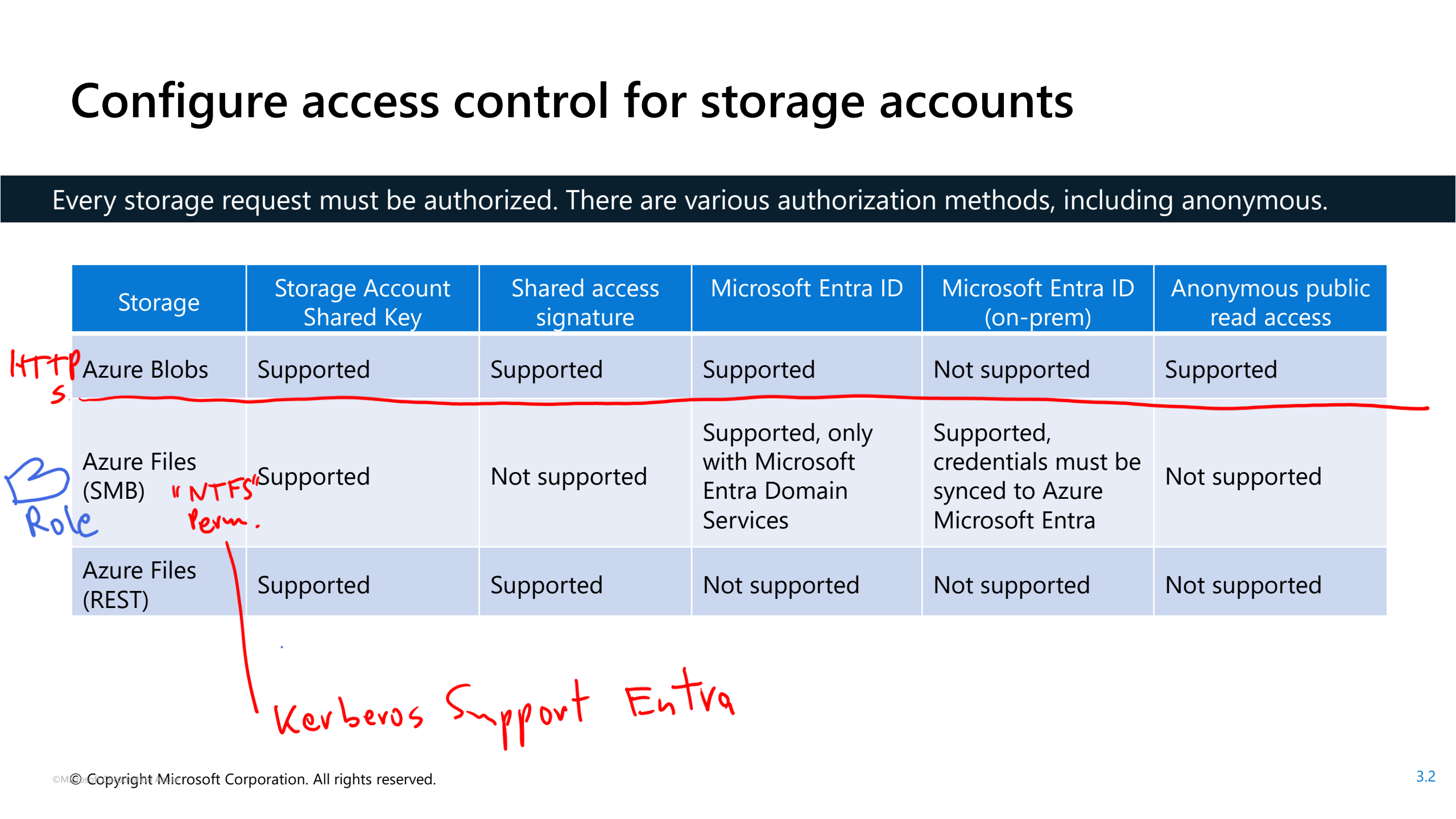
Azure Storage emphasizes security within its cloud storage platform, ensuring data protection and access control through various mechanisms:

- Encrypts data at rest and supports client-side encryption for comprehensive security.
- Offers multiple authorization methods, including Microsoft Entra ID and shared access signatures.
- Provides identity-based authentication over Server Message Block (SMB) and redundancy options to ensure data durability.

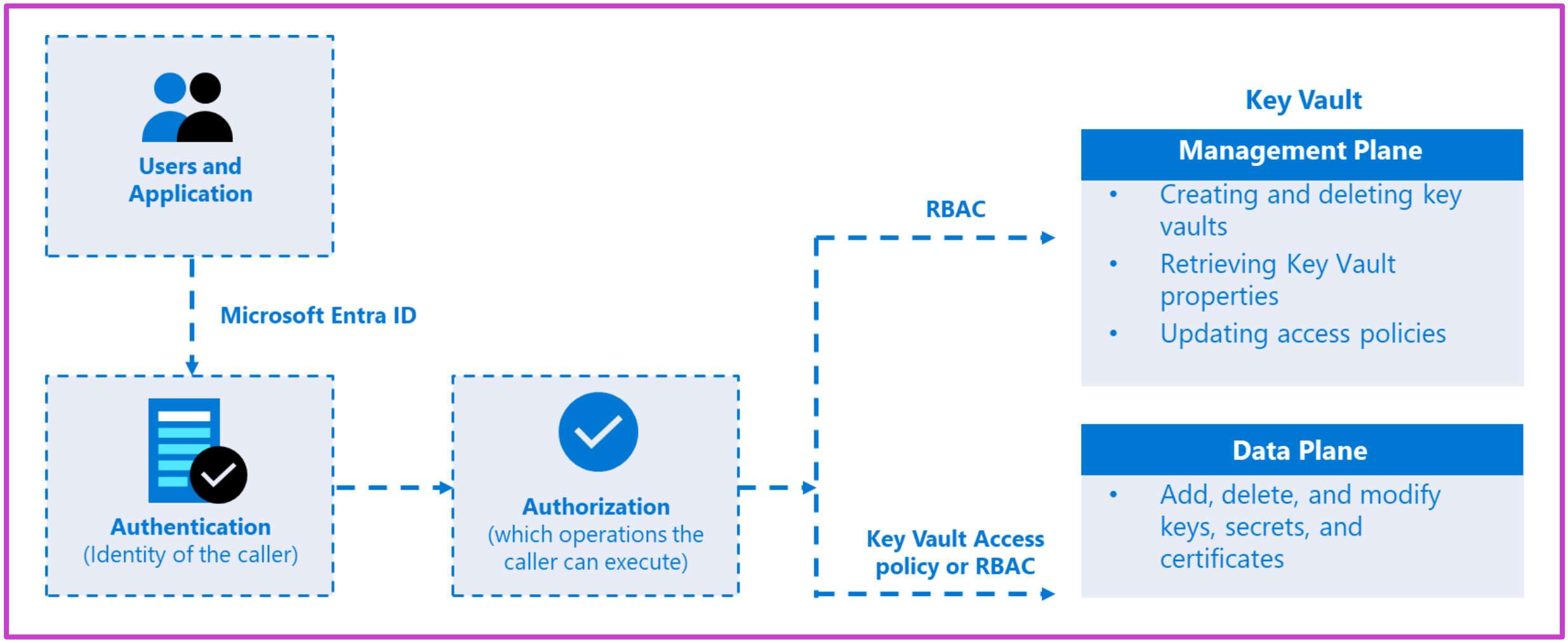
Configure access control for storage accounts

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

Storage	Storage Account Shared Key	Shared access signature	Microsoft Entra ID	Microsoft Entra ID (on-prem)	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 Azure Microsoft Entra	Not supported
Azure Files (REST)	Supported	Supported	Not supported	Not supported	Not supported

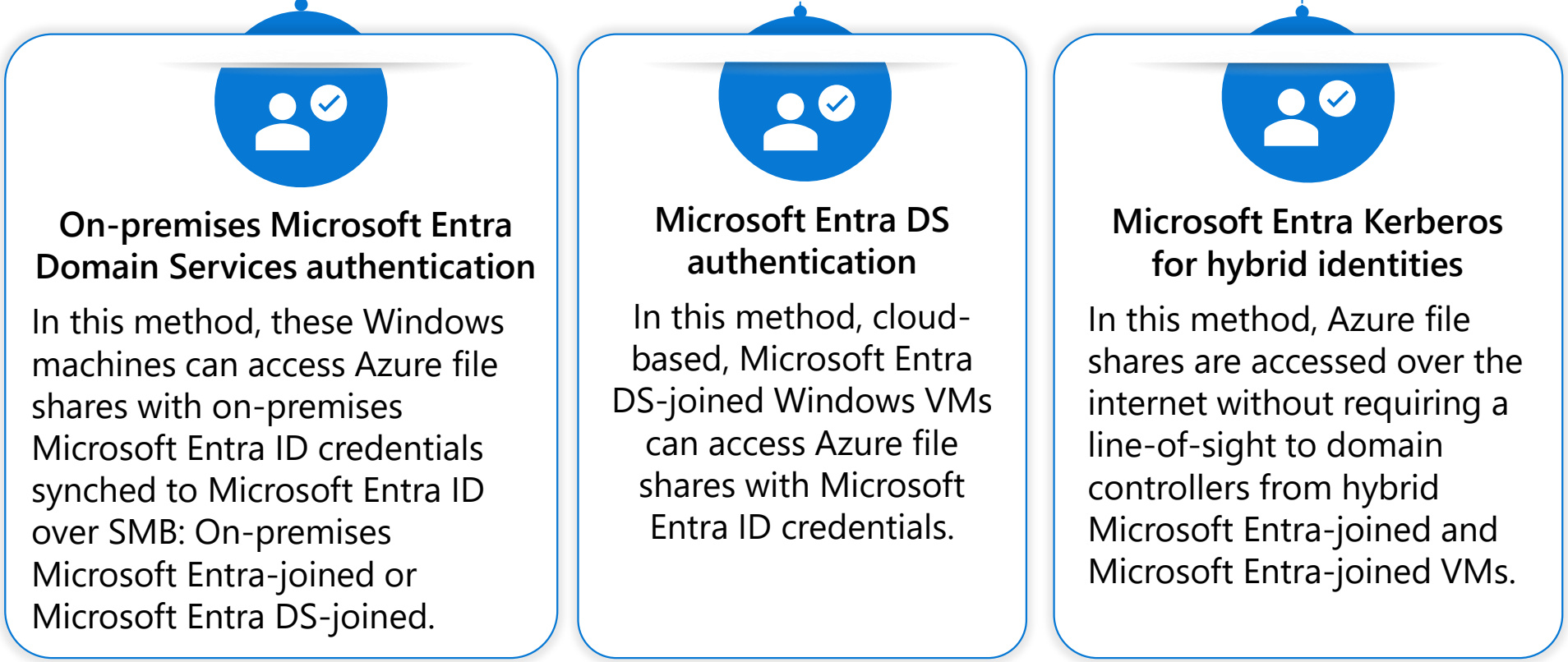


Manage life cycle for storage account access keys



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 Microsoft Entra Domain Services authentication

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

Microsoft Entra DS authentication

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

Microsoft Entra Kerberos for hybrid identities

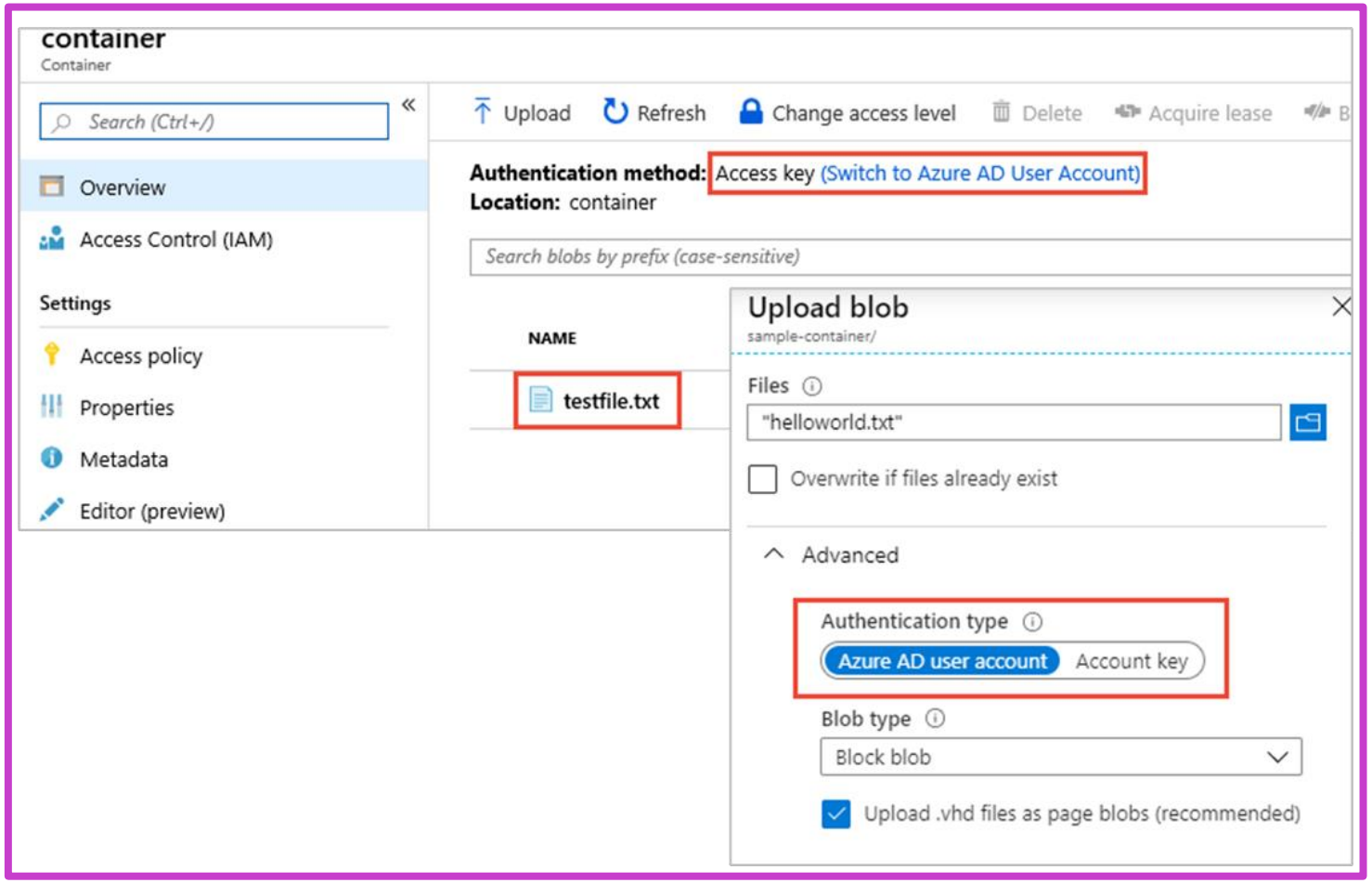
In this method, Azure file shares are accessed over the internet without requiring a line-of-sight to domain controllers from hybrid Microsoft Entra-joined and Microsoft Entra-joined VMs.

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

To authorize blob data access in Azure, specific permissions are required, typically provided through Azure role-based access control (Azure RBAC).

Permissions needed to access blob data:

- Use the account access key
- Use your Microsoft Entra ID account
- Determine the current authentication method
- Authenticate with the account access key
- Authenticate with your Microsoft Entra ID
- Specify how to authorize a blob upload operation
- Default to Microsoft Entra ID authorization in the Azure portal



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.

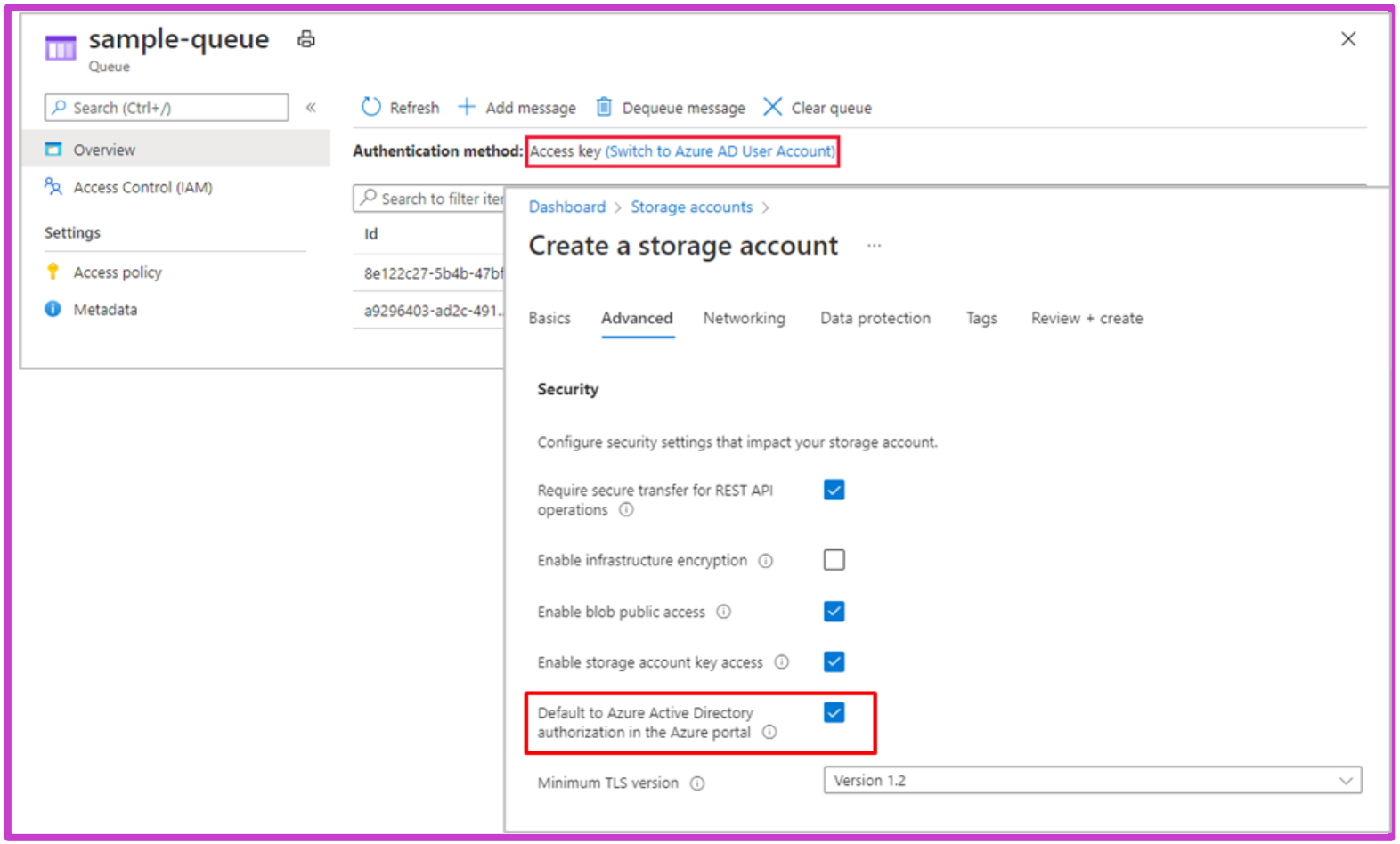
The authorization phase necessitates assigning specific Azure roles to the security principal; these roles, provided by Azure Storage, dictate the permissions the principal possesses for table data access.

Select and configure an appropriate method for Azure Queues

To authorize queue data access in Azure, specific permissions are needed, usually given through Azure role-based access control (Azure RBAC).

Permissions needed to access queue data:

- Use the account access key
- Use your Microsoft Entra ID account
- Determine the current authentication method
- Authenticate with the account access key
- Authenticate with your Microsoft Entra ID account
- Default to Microsoft Entra ID authorization in the Azure portal



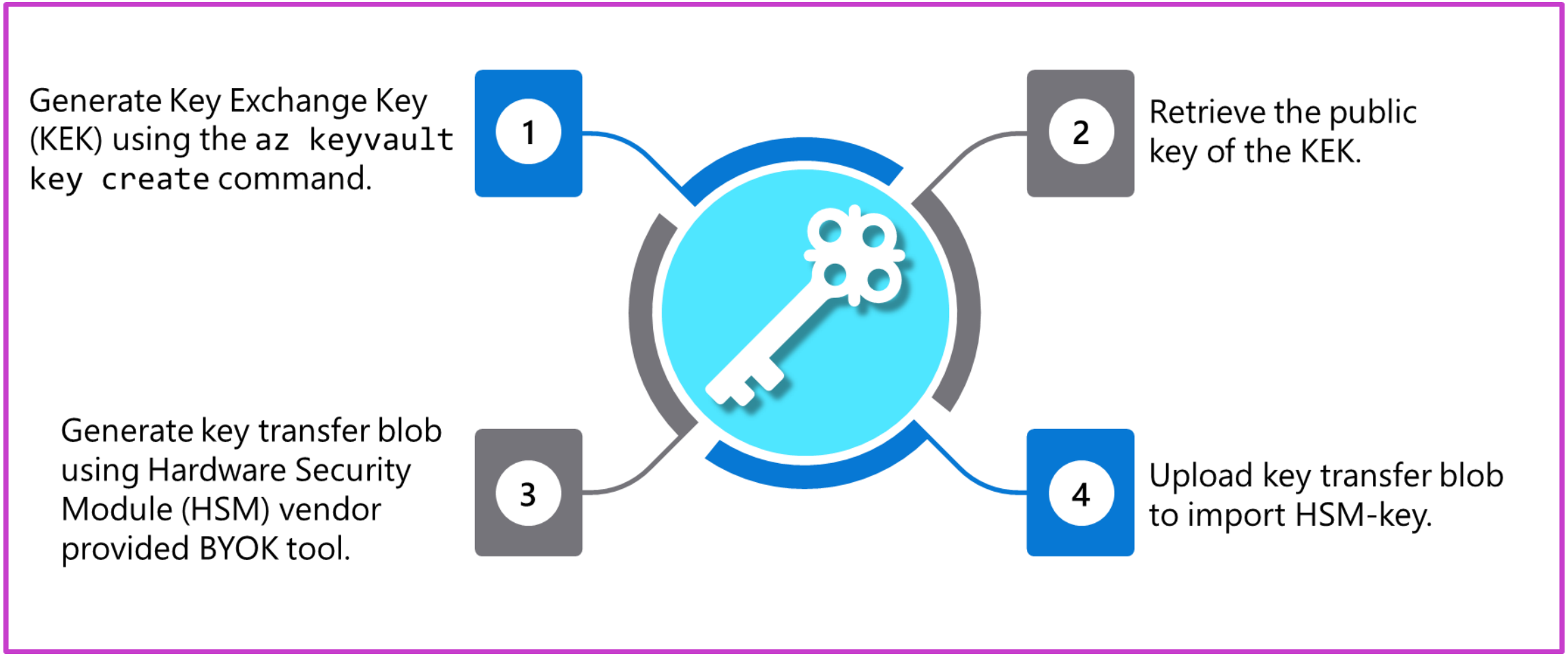
Data protection overview

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.

Bring your own key specification (BYOK)



Enable infrastructure encryption for double encryption of data

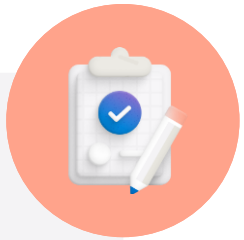
- **Azure Storage Encryption**: Uses 256-bit AES and is FIPS 140-2 compliant; optional infrastructure-level double encryption adds an additional security layer.
- **Infrastructure Encryption**: Encrypts data twice with distinct algorithms and keys, applicable to entire storage accounts or specific scopes.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

Demonstrations: Storage Security

1. Generate SAS tokens
2. Key rollover
3. Storage access policies
4. Microsoft Entra ID user account authentication
5. Storage endpoints

Additional Study – Storage Security



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

Module Review Questions

- Core Cloud Services – Azure data storage options
- Create an Azure Storage account (Exercise)
- Control access to Azure Storage with shared access signatures (Exercise)
- Store and share files in your application with Azure Files (Exercise)
- Secure your Azure Storage account

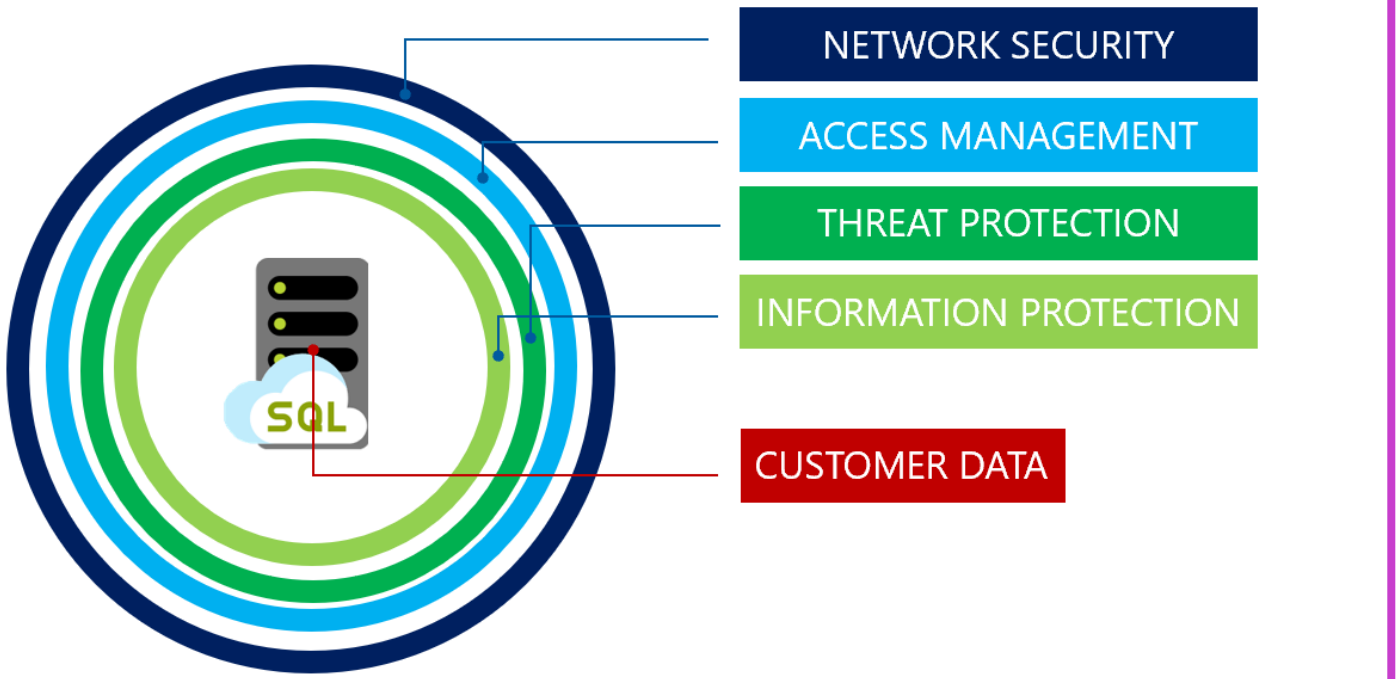
Plan and implement security for Azure SQL Database and Azure SQL Managed Instance

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

1. Azure SQL Database and SQL Managed Instance security
2. Enable database authentication by using Microsoft Entra ID
3. Enable database auditing
4. Identify use cases for the Microsoft Purview governance portal
5. Implement data classification of sensitive information by using the Microsoft Purview governance portal
6. Plan and implement dynamic masking
7. Implement Transparent Database Encryption (TDE)
8. Recommend when to use Azure SQL Database Always Encrypted

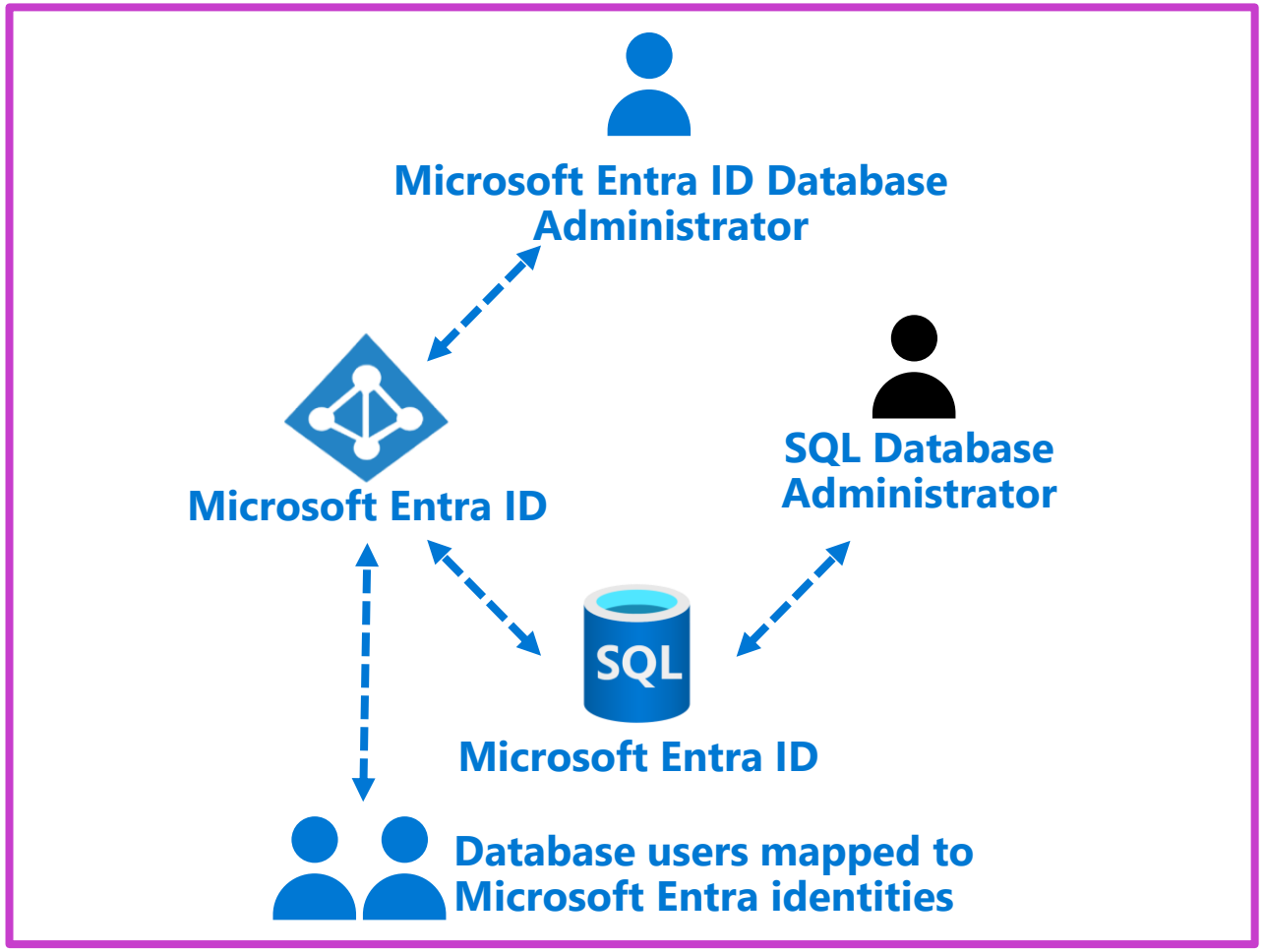
Azure SQL Database and SQL Managed Instance security

- 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.



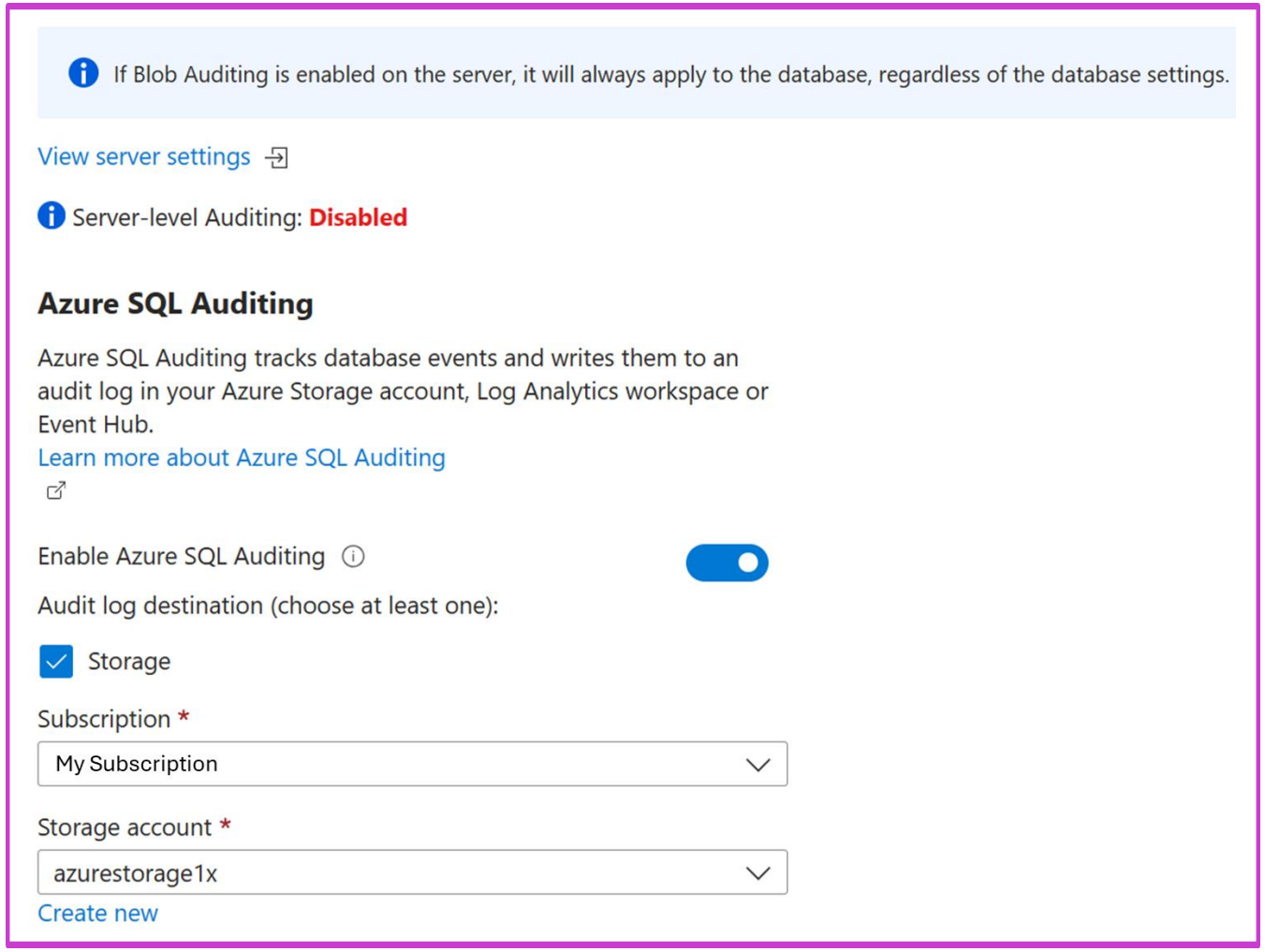
Enable database authentication by using Microsoft Entra ID

- An alternative to SQL Server authentication
- Helps stop the proliferation of user identities across database servers
- Allows password rotation in a single place
- Customers can manage database permissions using external (Microsoft Entra ID) groups

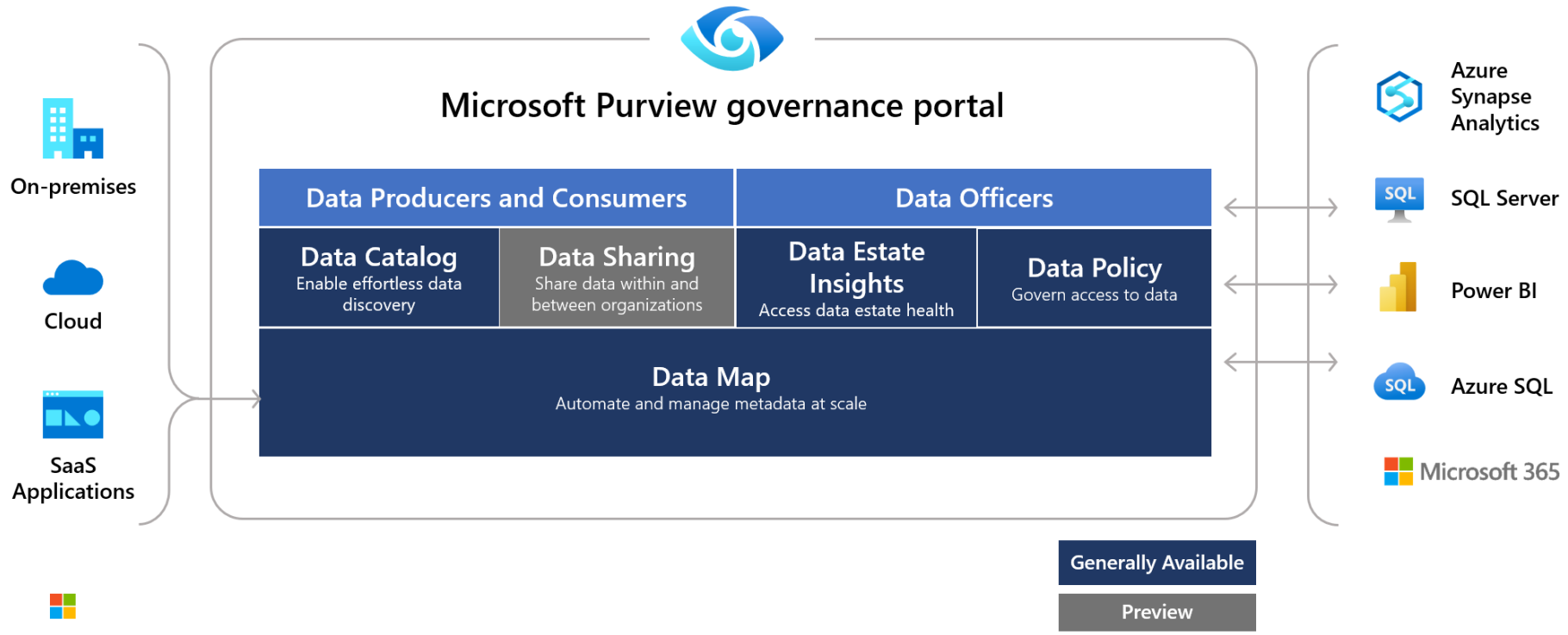


Enable database auditing

- Retain an audit trail of selected events
- Report on database activity and analyze results
- Configure policies for the server or database level
- Configure audit log destination
- A new server policy applies to all existing and newly created databases



Microsoft Purview governance



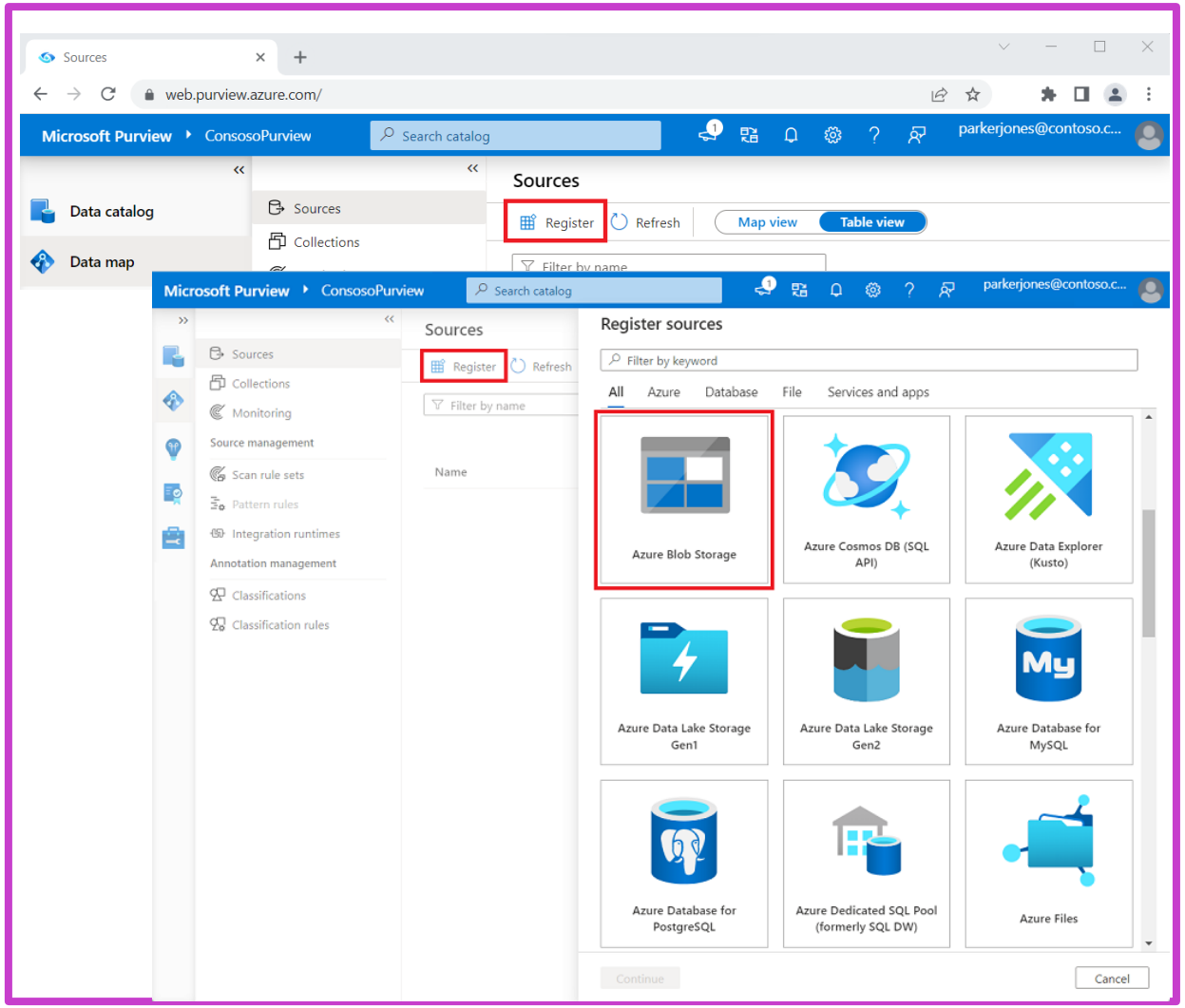
Microsoft Purview's solutions in the governance portal provide a unified data governance service that helps you manage your on-premises, multicloud, and software-as-a-service (SaaS) data.

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.

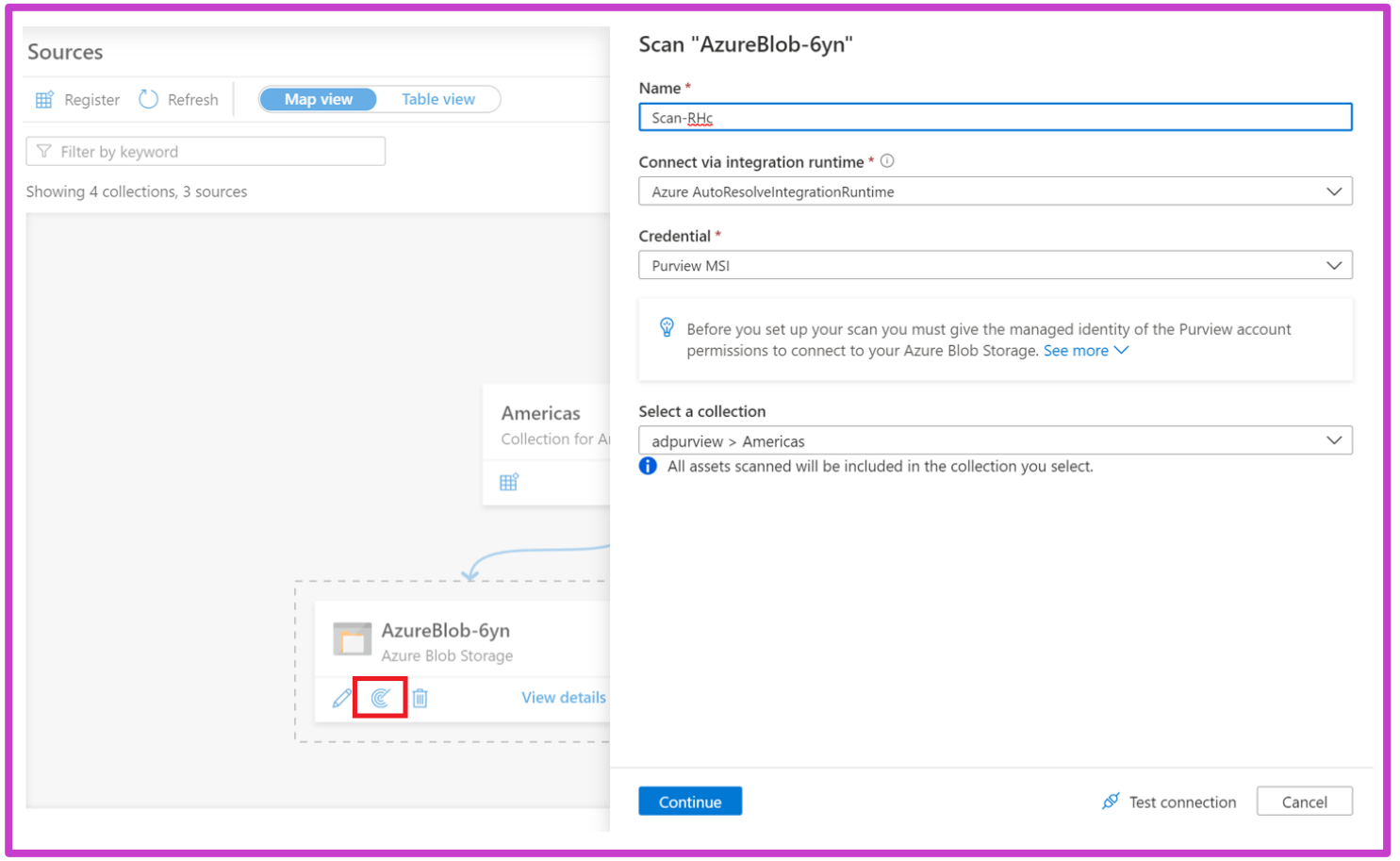


Microsoft Purview governance-Scan and ingestion

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.

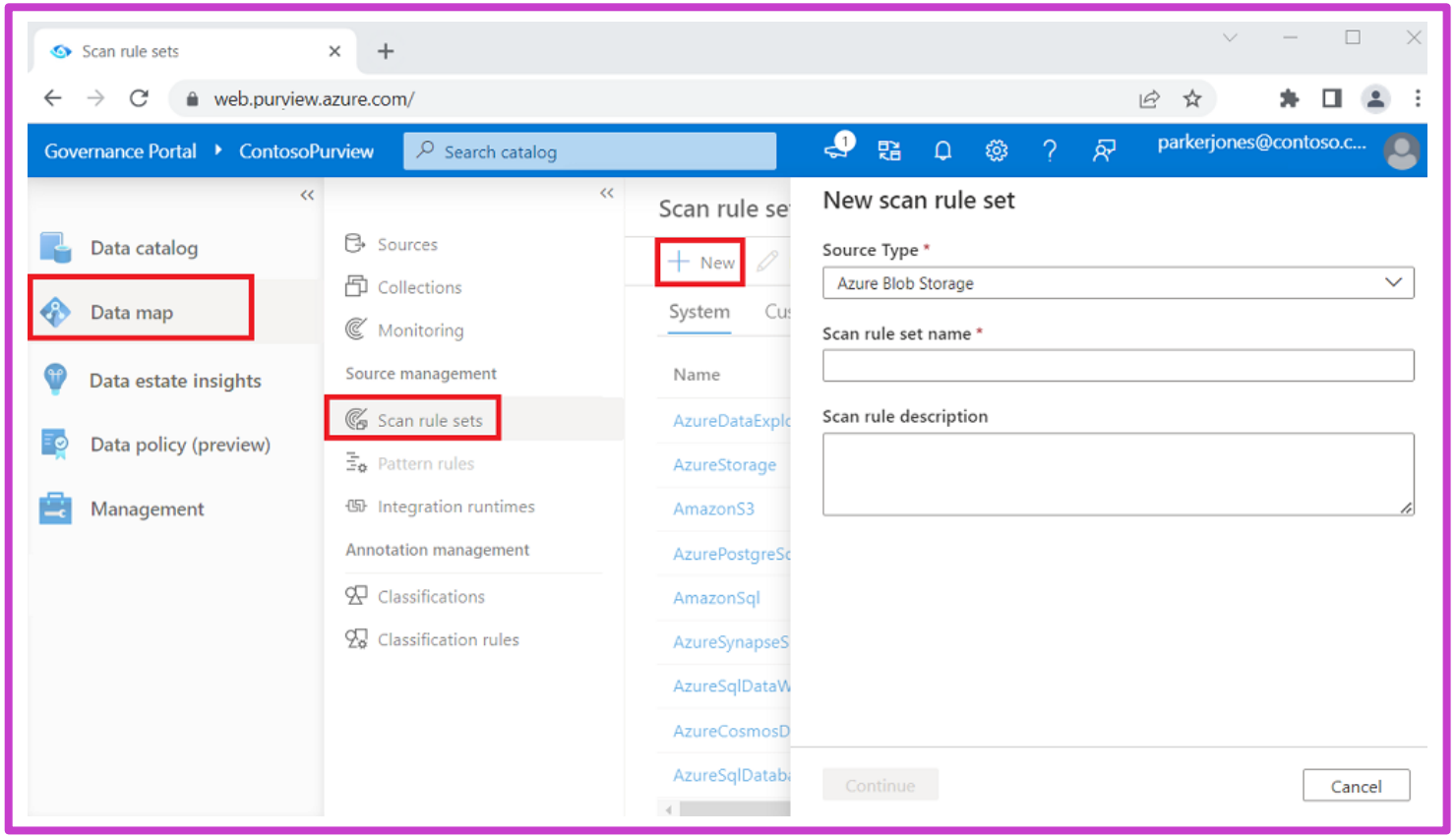


Microsoft Purview governance-Create a scan rule set

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.

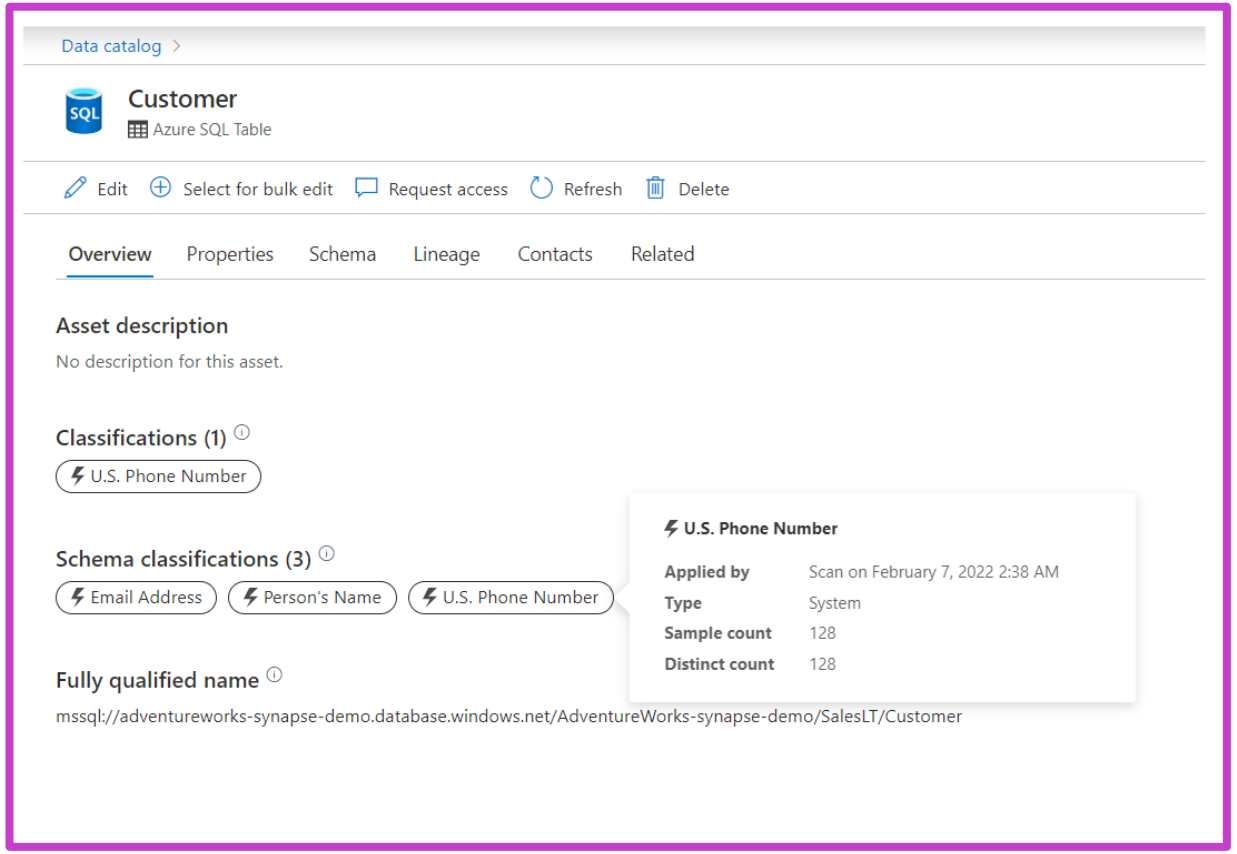


Microsoft Purview governance-Data classification

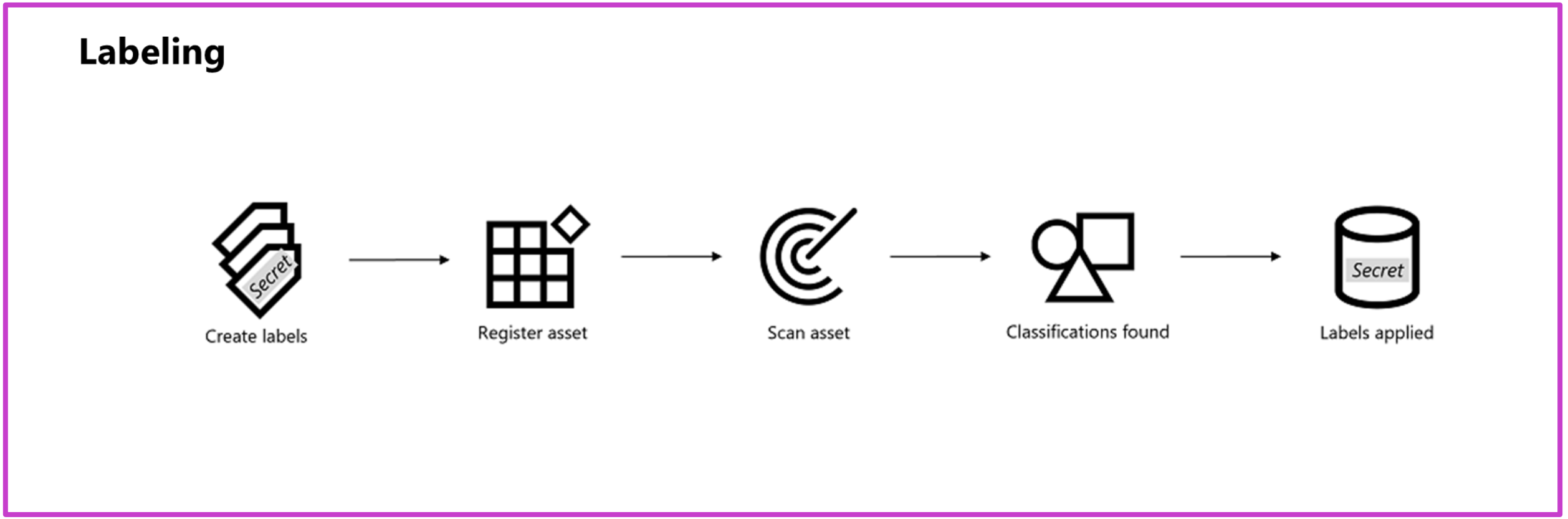
Apply classifications

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.

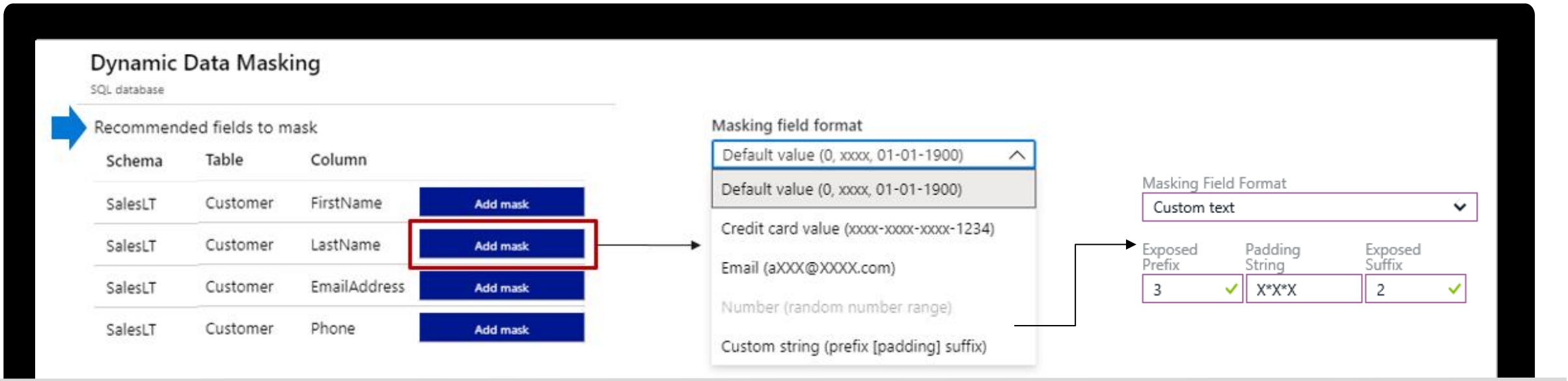


Labeling in the Microsoft Purview Data Map



- 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.

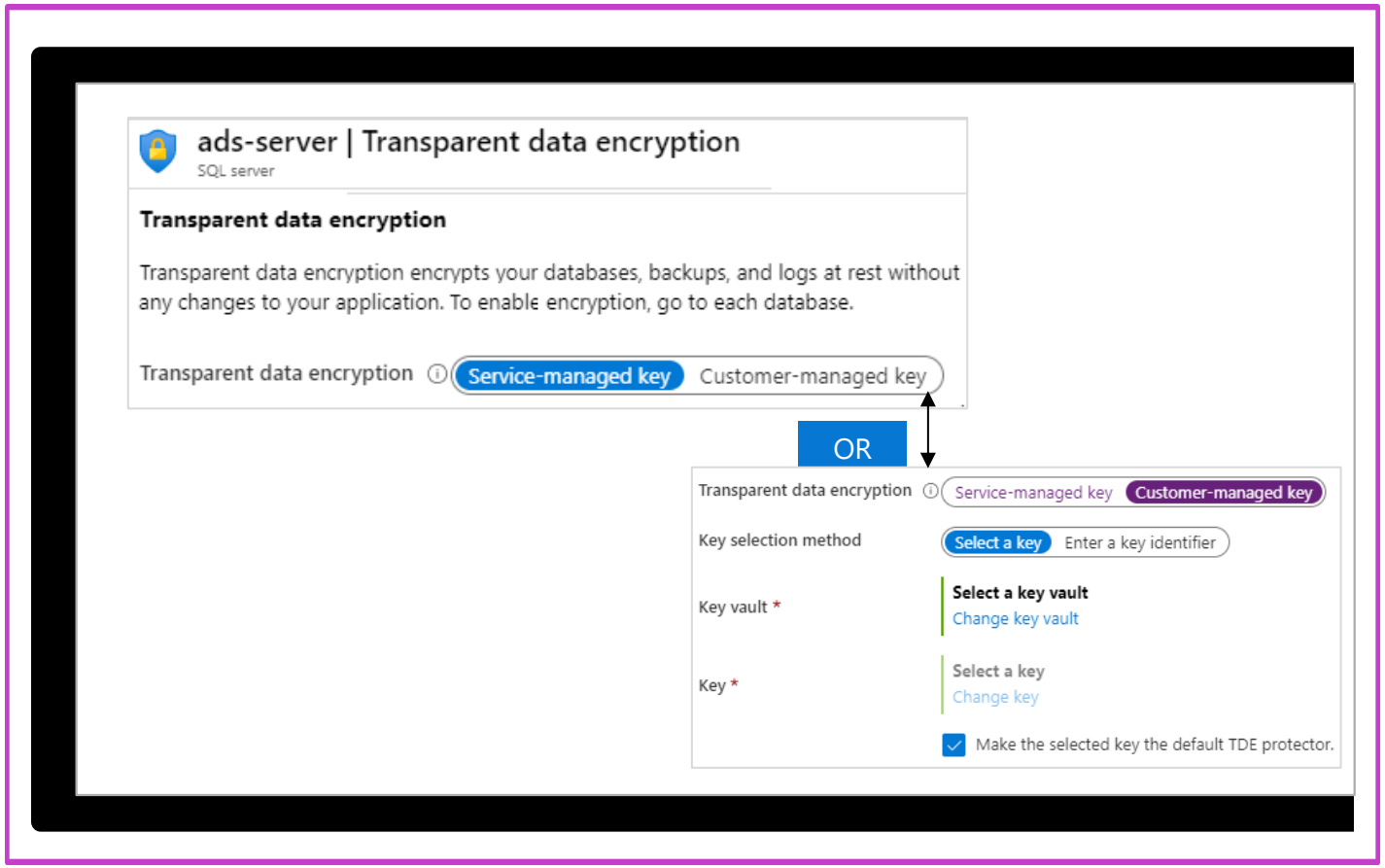
Plan and implement dynamic masking



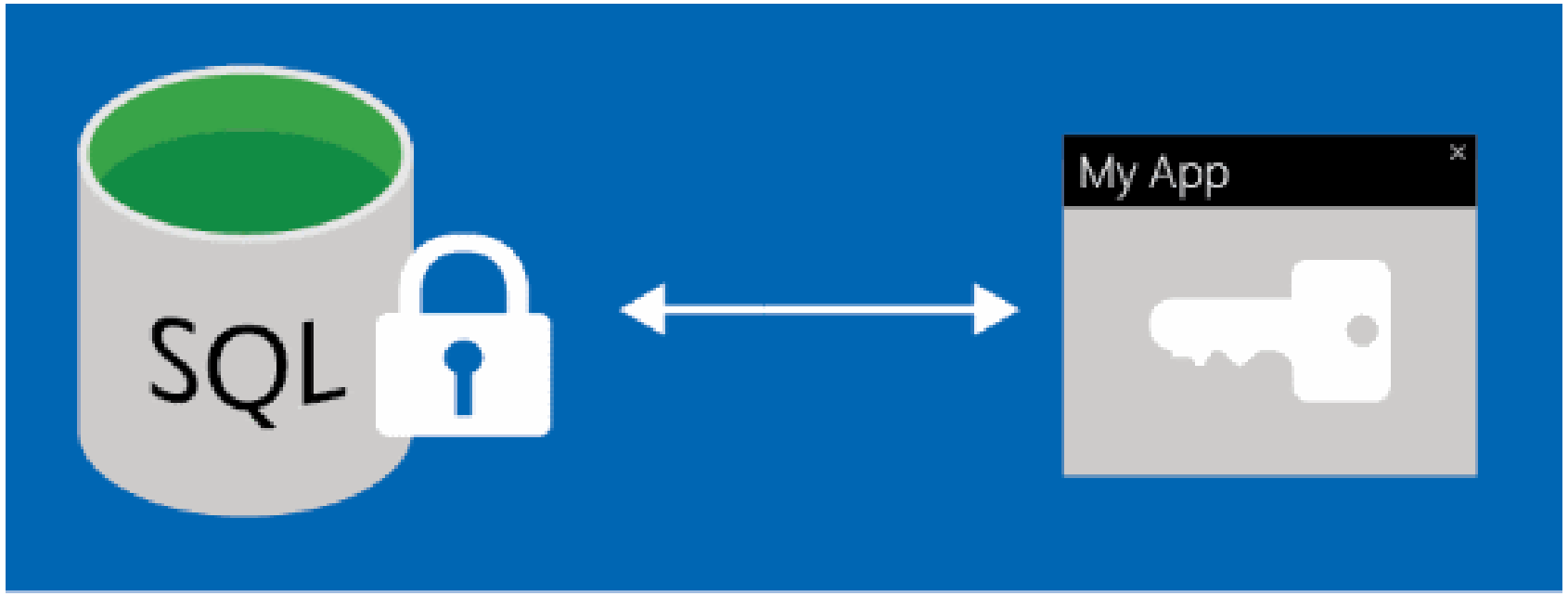
- Masks sensitive data for non-privileged users
- Administrators are excluded; you can add others
- Rules apply the masking logic; several formats are available

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, and Azure Synapse Analytics



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.

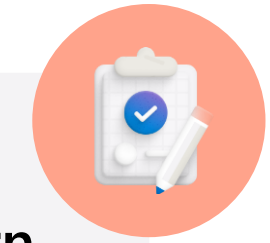
Always Encrypted – Implementation

Backup ?

Demonstrations: Database Security

1. Advanced Data Security and Auditing
2. Diagnostics
3. Microsoft Entra Authentication

Additional Study – Database Security



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

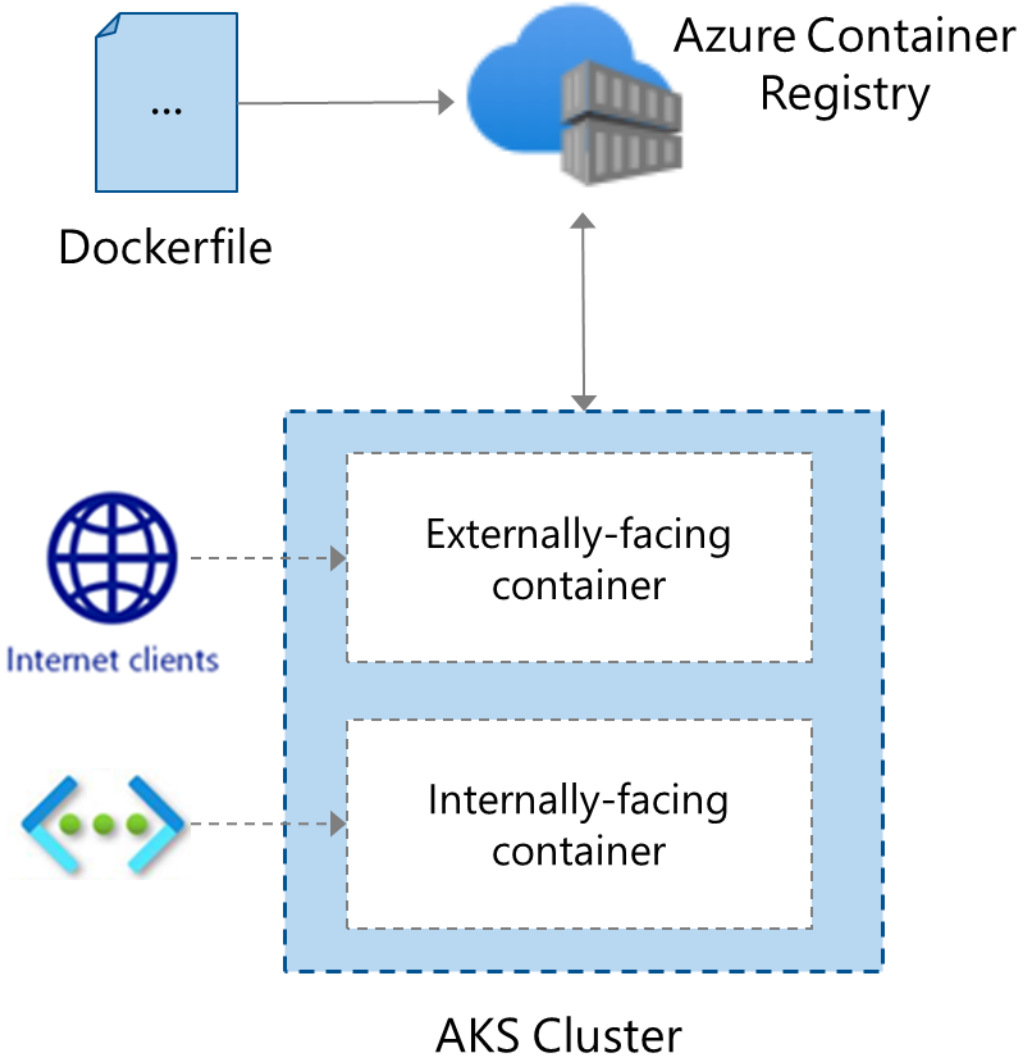
Module Review Questions

- Provision an Azure SQL database to store application data (Exercise)
- Secure your Azure SQL Database (Exercise)
- Configure security policies to manage data (Exercise)
- Migrate your relational data stored in SQL Server to Azure SQL Database (Exercise)

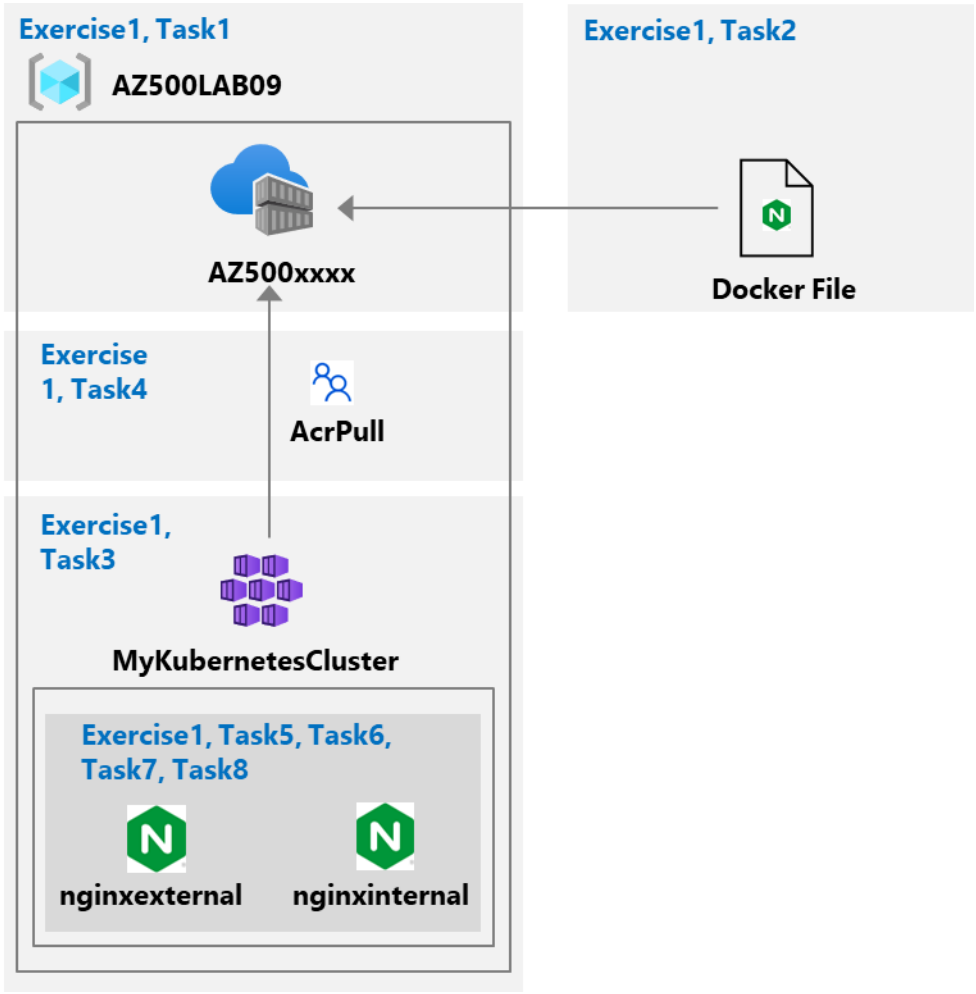
Module Labs

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



Lab 04 – Configuring and securing ACR and AKS



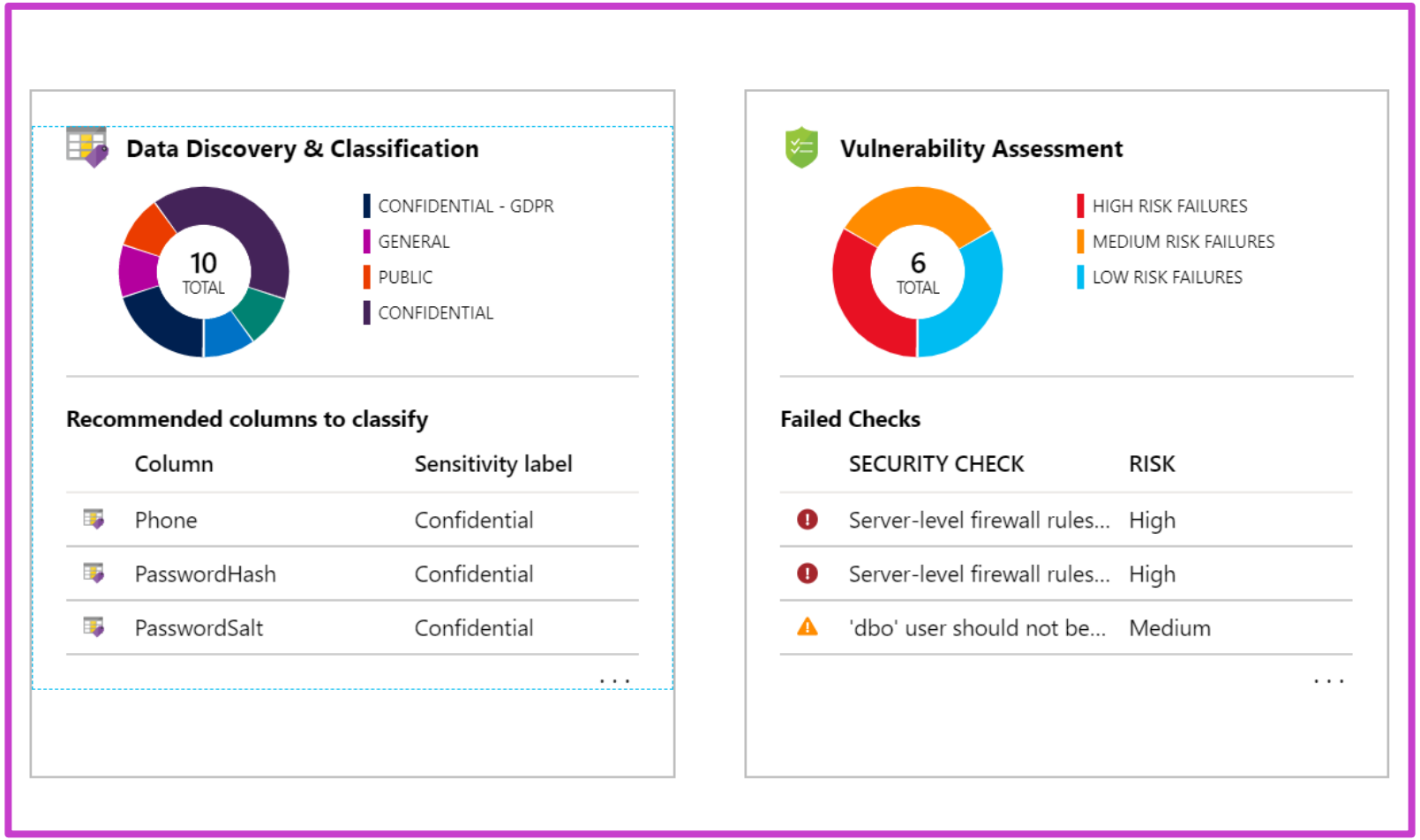
Lab 05 – Securing Azure SQL Database

Deploy an Azure SQL Database

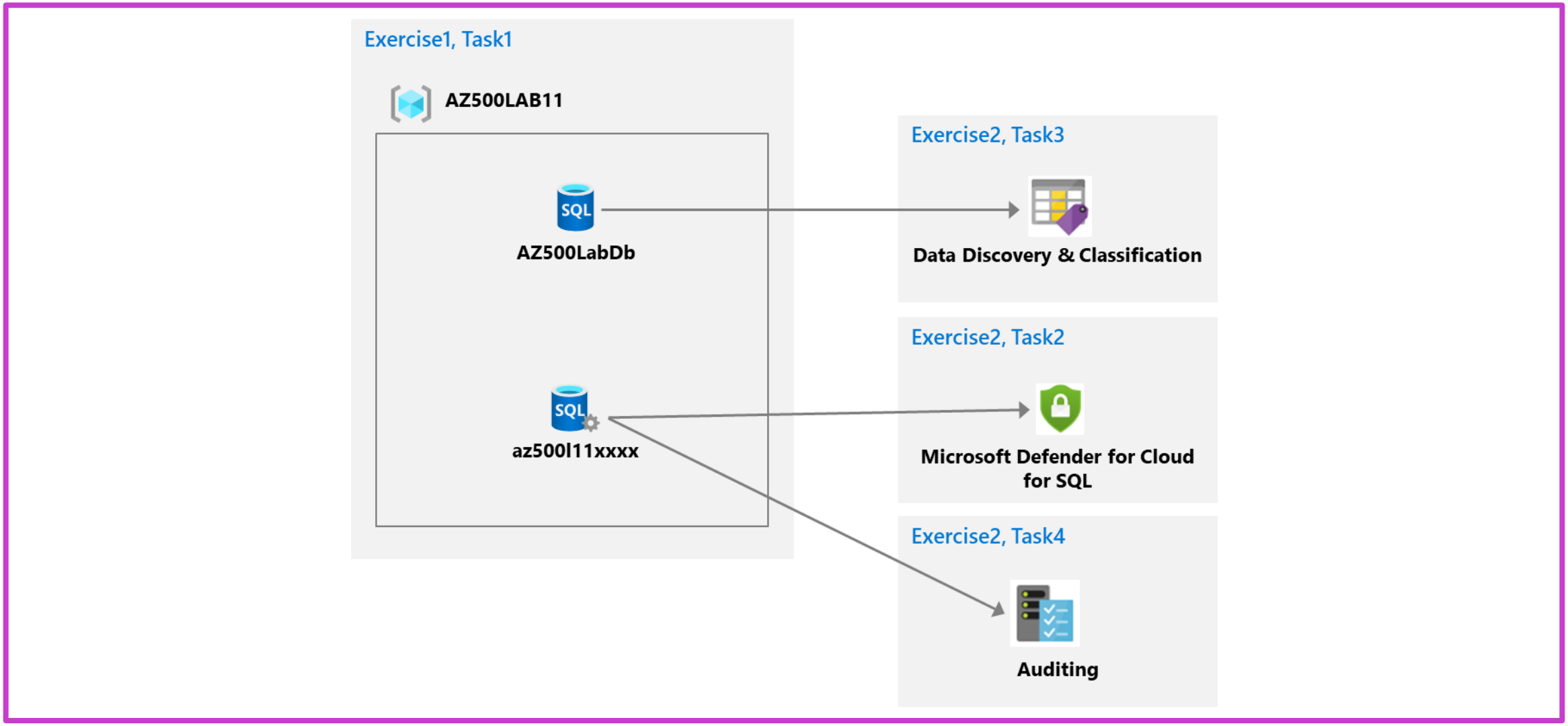
Configure Advanced Data Protection

Configure Data Classification

Configure Auditing



Lab 05 – Securing Azure SQL Database



Lab 06 – Service Endpoints and Securing Storage

Create a virtual network with a Public and Private subnet

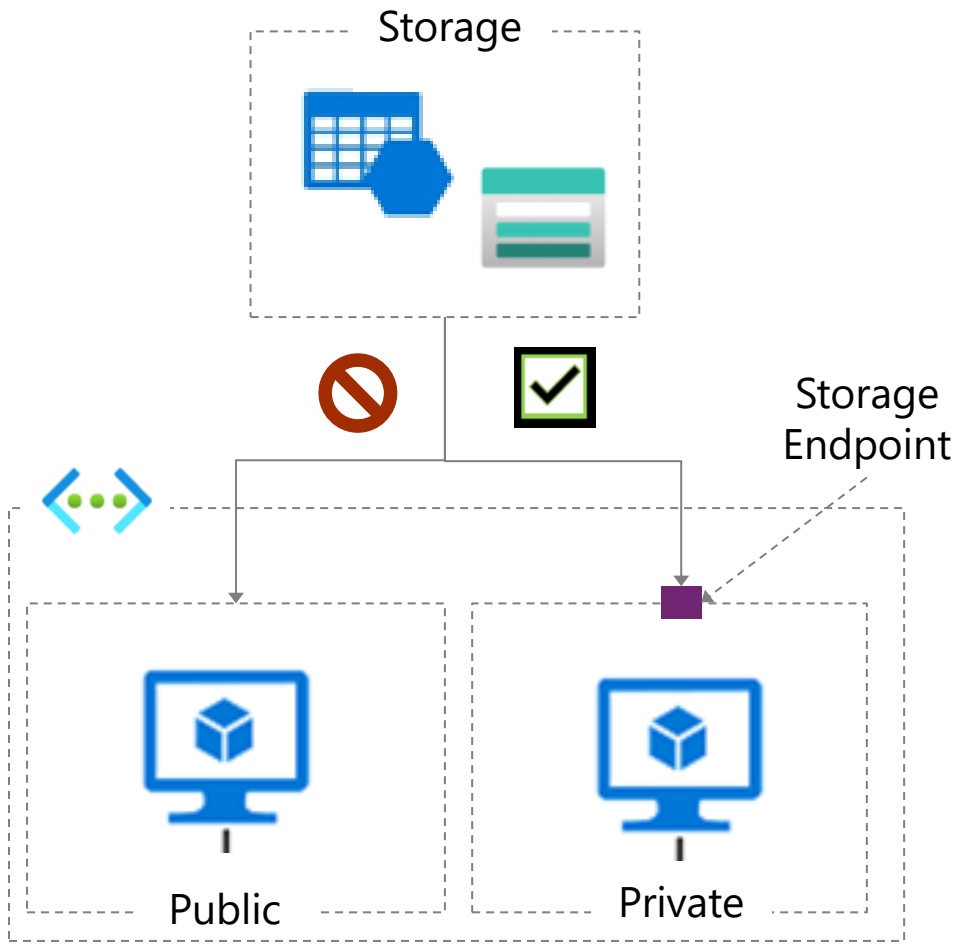
Create a storage endpoint for the Private subnet

Create a storage account with a file share

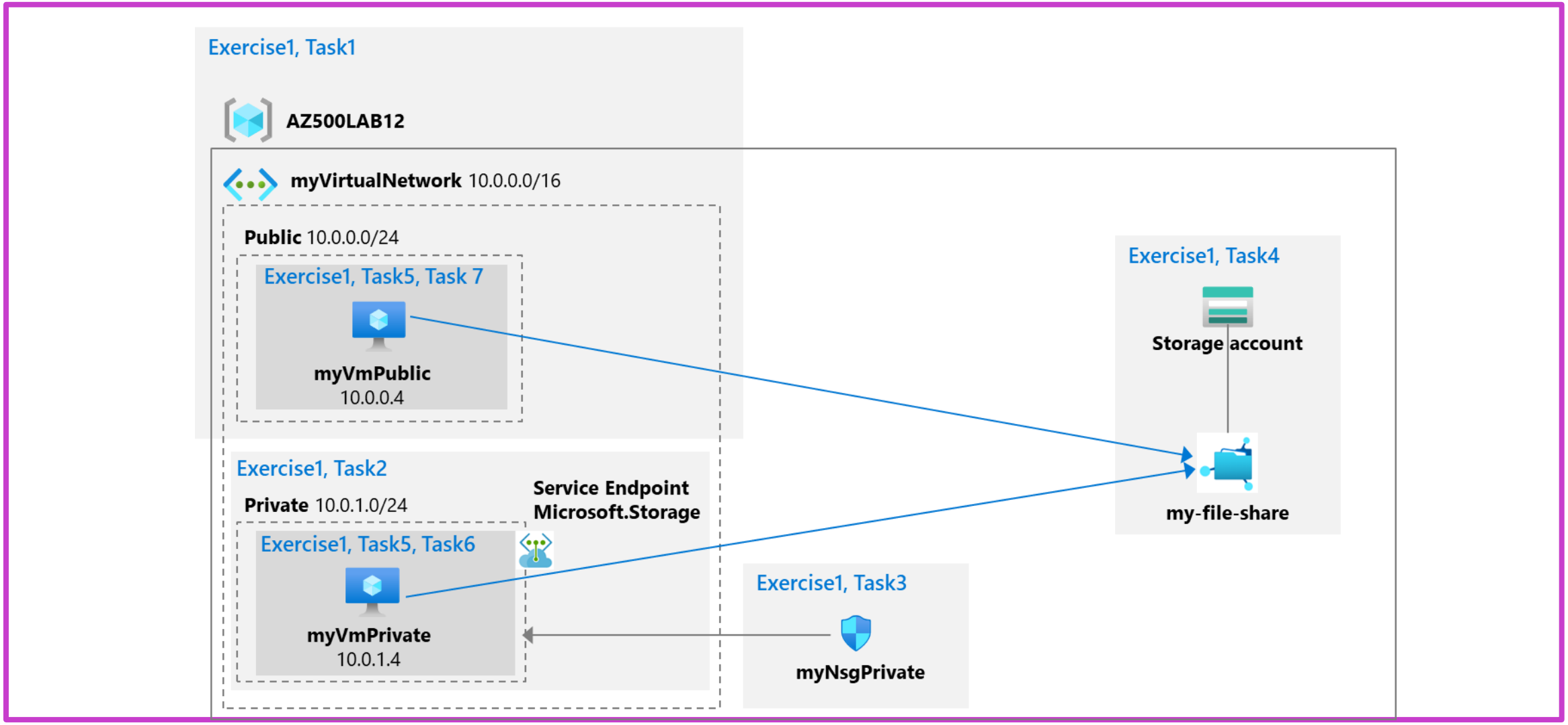
Configure a NSG with rules to allow access to storage and internet

Confirm storage access from the private subnet

Confirm storage access is denied from the public subnet



Lab 06 – Service Endpoints and Securing Storage



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

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.

End of presentation