Cloud Security Implementation Plan

Jamal Rizki

SWBLT LLC Cloud Migration

A. Executive Summary

SWBTL LLC began as a small regional delivery service provider and has since evolved into a nationwide service provider with over 2,000 employees. The company's infrastructure is currently hosted in four data centers located in the United States. Over time these systems have become increasingly costly, as SWBTL does not own the data centers and is instead leasing them from a third party. Other concerns the company currently faces include an unreliable service and a threat surface potentially vulnerable to cyberattacks. The company must also comply with FISMA and PCI DSS regulations and has a NIST SP 800-53 audit approaching. Due to these factors, the company has decided to transition to the cloud. To begin this transition, the company will focus on the Marketing, Accounting, and IT departments, using Microsoft Azure as the service provider.

B. Proposed Course of Action

To best meet SWBTL LLC's requirements, the implementation of an Infrastructure as a Service (IaaS) model is the best course of action. This is due to the company's need to deploy and manage virtual machines and

operating systems, provision compute and storage resources, and integrate custom applications.

Regulatory compliance requirements include adhering to FISMA for government contracts, PCI DSS for the processing of credit card data, and NIST SP 800-53 guidance controls for the upcoming assessment. Microsoft Azure allows SWBTL to scale rapidly, it also reduces the associated costs by provisioning only the minimum resources required, and it also integrates seamlessly with the existing Active Directory configuration the company uses. In addition, Azure offers strong encryption services for both data in transit and at rest, as well as the management of passwords, credentials, and secrets through Azure Key Vault. Challenges to this migration include the complex process of transferring large volumes of data, ensuring that data remains secure and is accessible only to authorized parties, and establishing suitable backup and recovery processes to minimize risks at all stages of the migration and beyond.

C1. Analysis and Recommendations

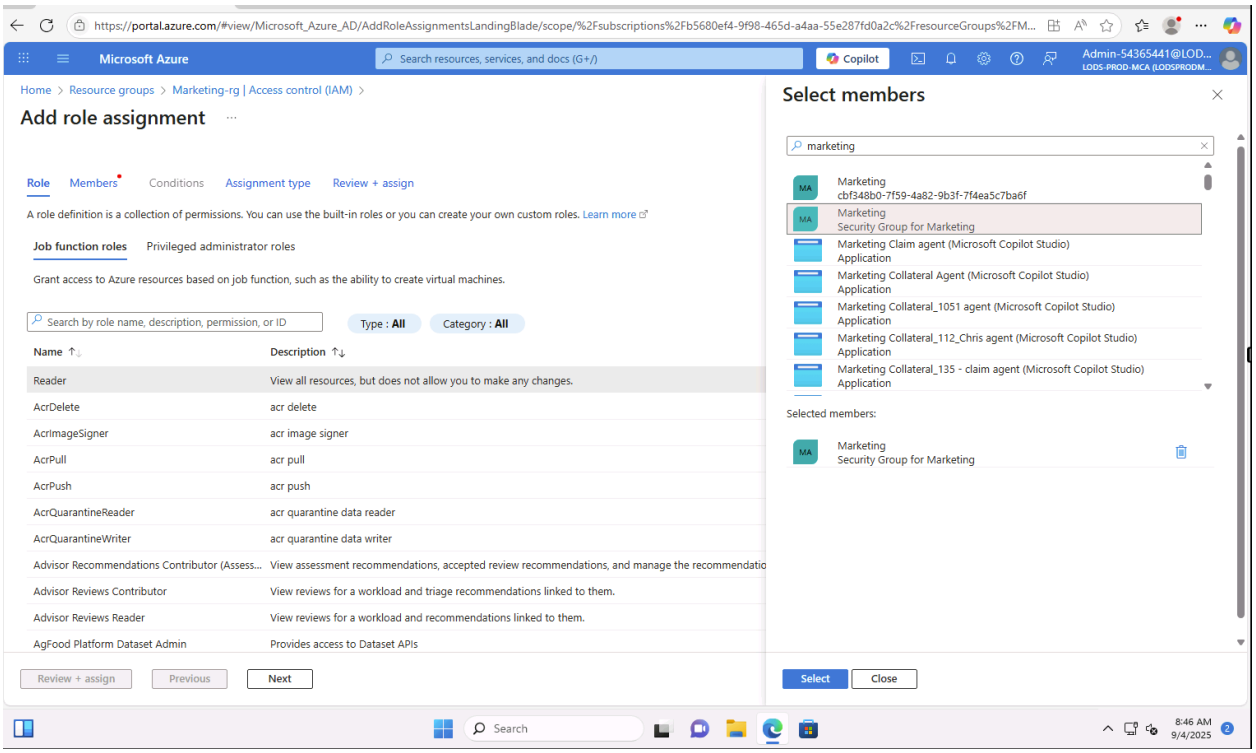
Currently the role-based access controls at SWBTL are not aligning with the principles of least privilege best practices. There are many configurations where the roles are set to be broader than necessary.

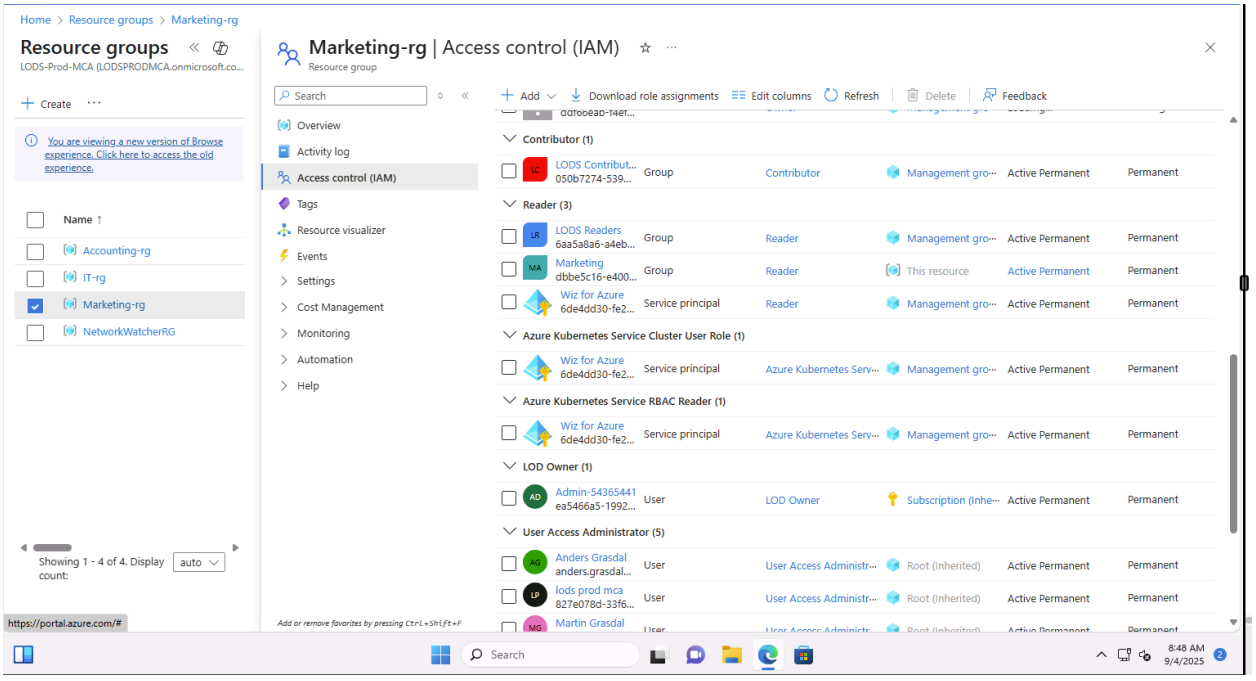
Three recommendations to address these flaws are:

1. Assign roles based on departmental function – Assigning basic Reader permissions to departments that only interact with the resources at a low level. The Marketing and Accounting departments should be restricted from altering resources to avoid accidental or intentional changes.
2. Implement least privilege across departments - Each department should be isolated from the others to avoid unauthorized access to or altering of another department's resources.
3. Remove unnecessary management or subscription-level access - Default permissions at the subscription or administrative level could allow users to bypass departmental boundaries.

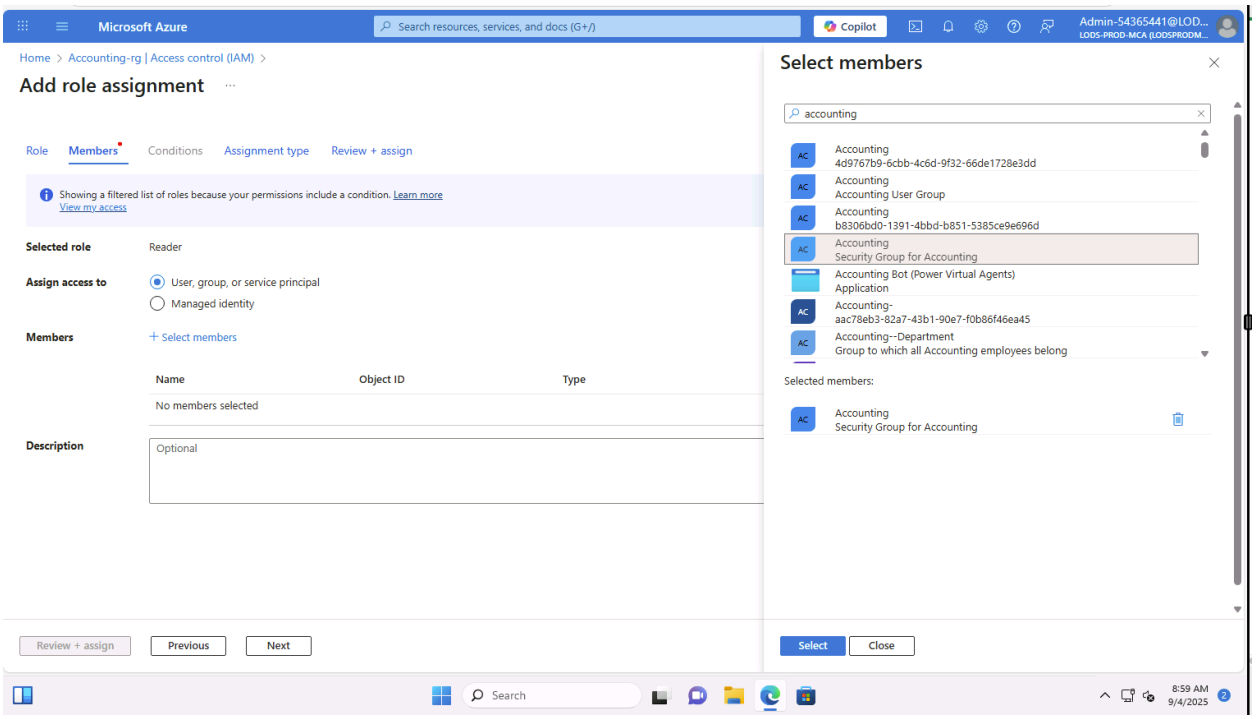
C2. Updated Configurations

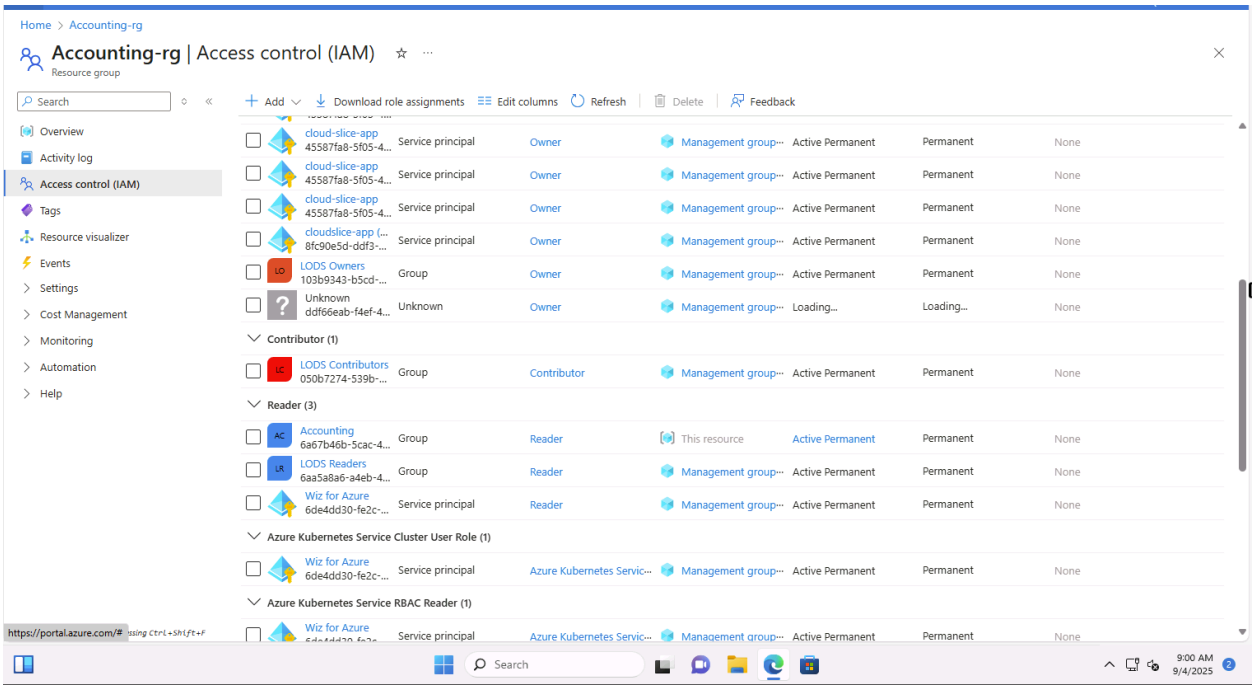
Marketing – The Marketing security group was assigned the role of Reader. This provides visibility of resources without allowing any modifications.



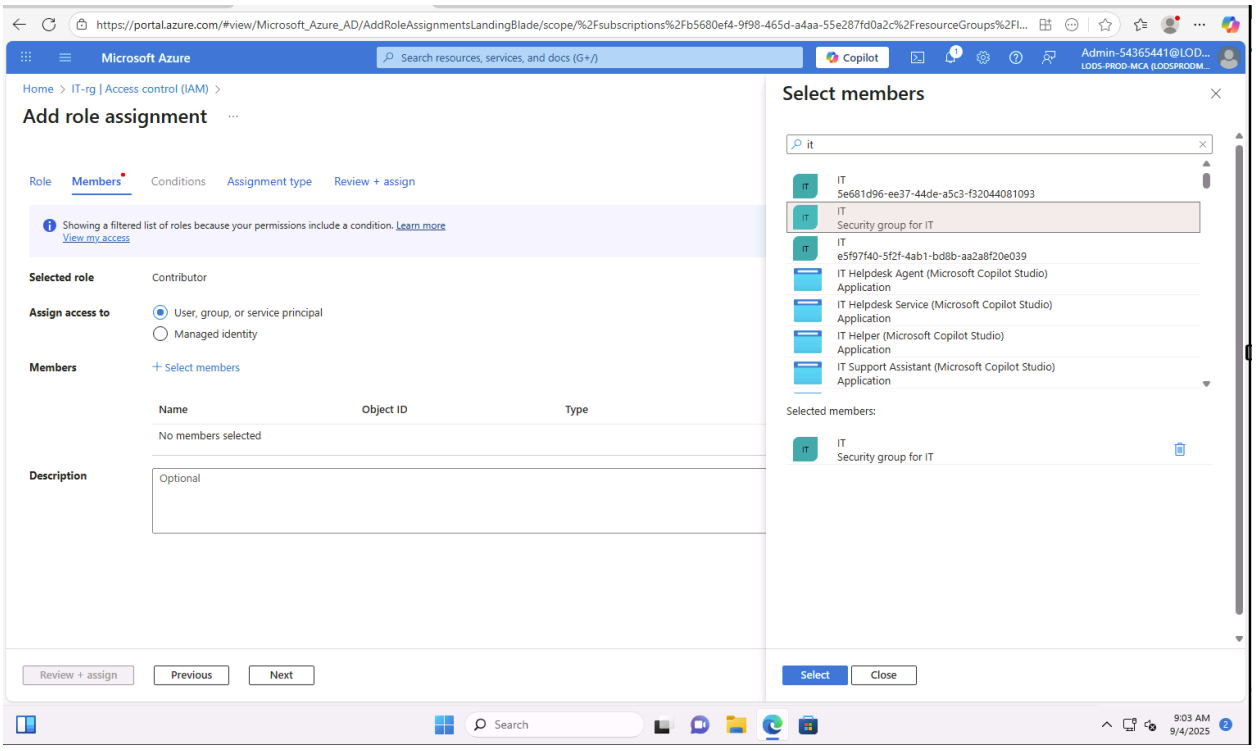


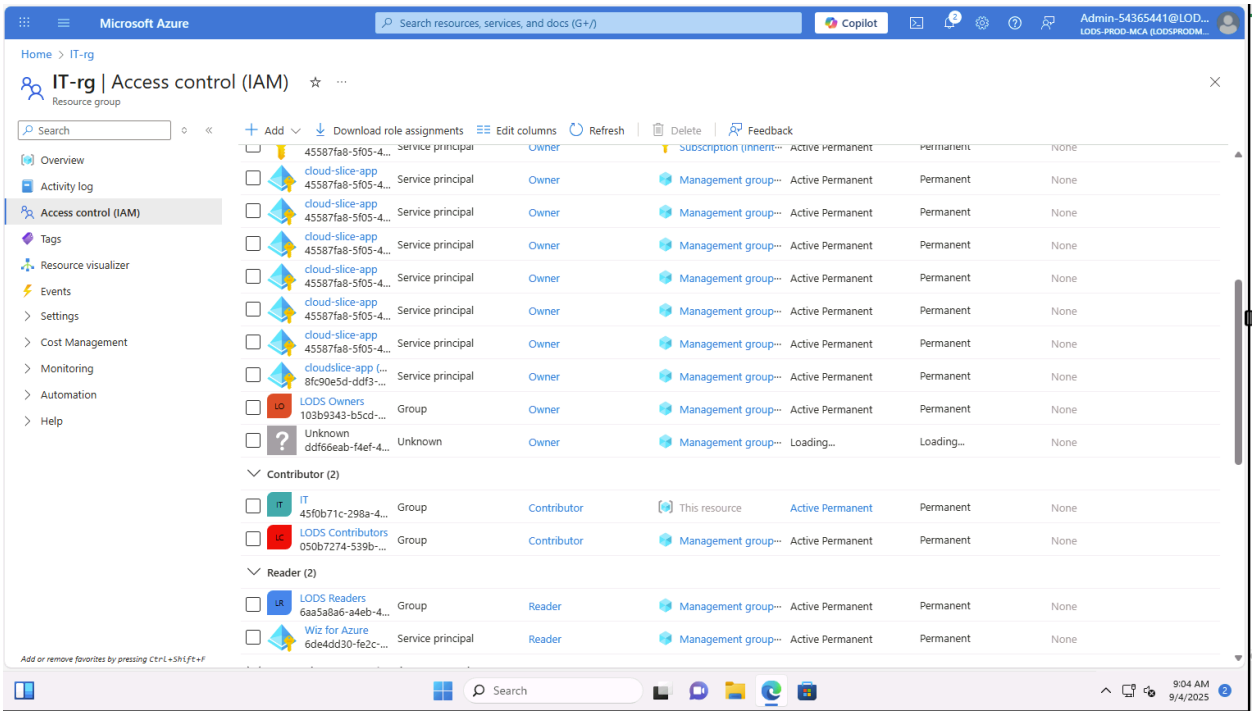
Accounting – The Accounting security group was assigned the role of Reader. This provides visibility of resources without allowing any modifications.





IT– The IT security group was assigned the role of Contributor. This allows changes and modifications to resources but not permissions to assign or alter roles.



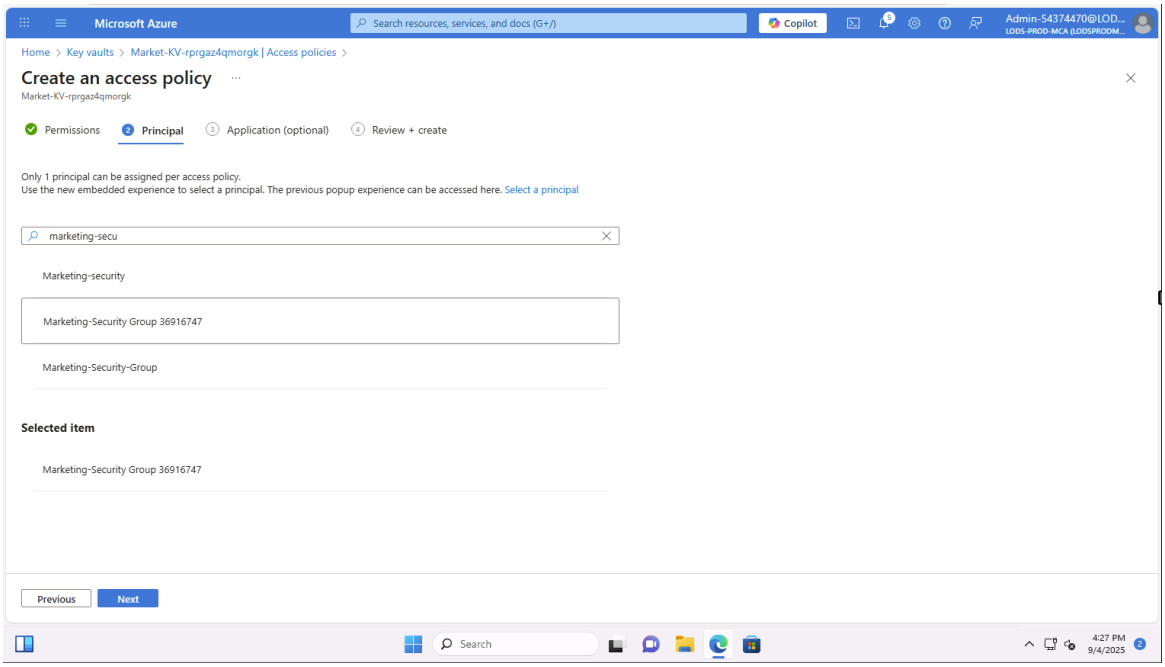


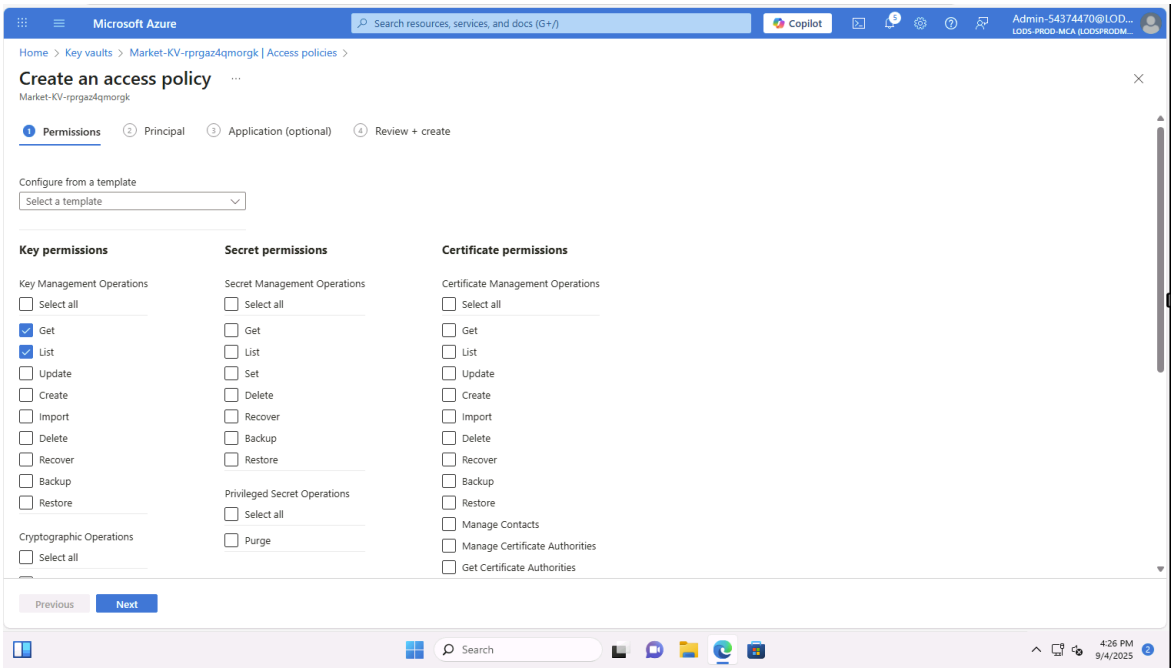
D1. Implementation of Best Practices

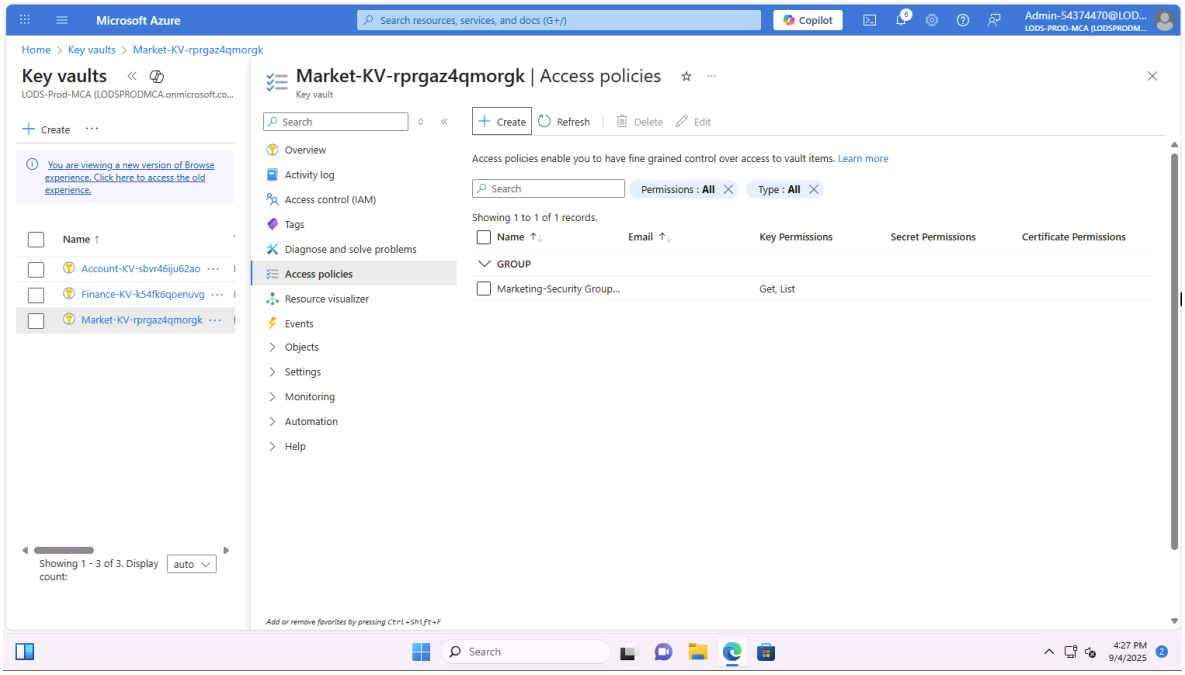
Access Policies - Access policies were implemented using the principles of least privilege. For both Marketing and Accounting groups, only the Get and List permissions were granted. For IT, the Key, Secret, and Certificate template was applied, giving the IT department broader permissions. This also aligns with the RBAC policies implemented earlier.

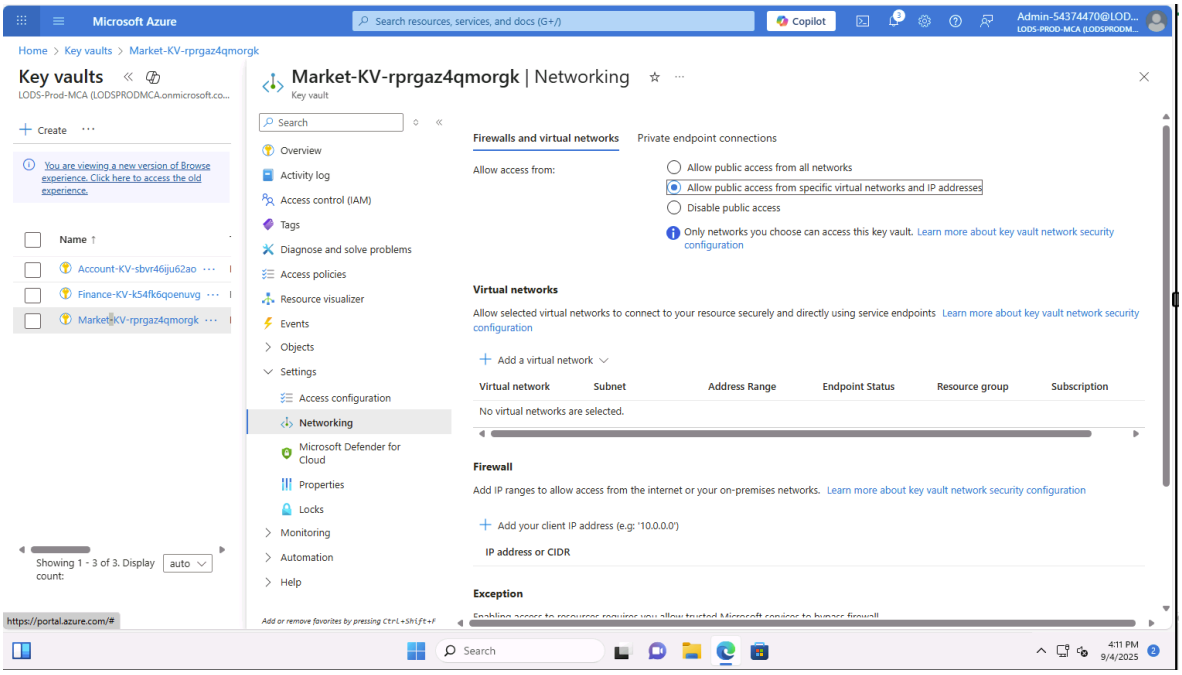
Network Access – Access policies should be granular and allow only authorized access. Configuring network settings to allow access only from required subnets and virtual networks helps prevent broad public access.

Marketing resource group:

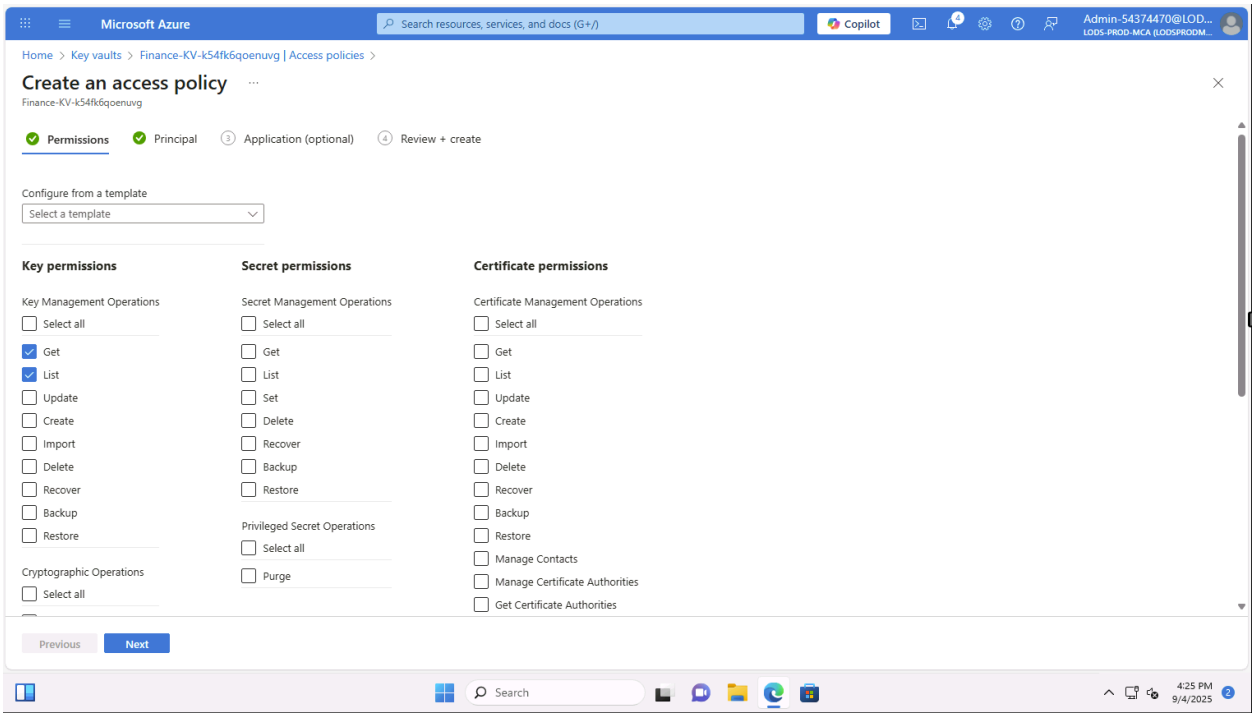

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Admin-54374470@LOD...
LODS-PROD-MCA (LODSPRODM...
Home > Key vaults > Market-KV-rprgaz4qmorgk | Access policies >
Create an access policy
Market-KV-rprgaz4qmorgk
Permissions
Principal
Application (optional)
Review + create
Only 1 principal can be assigned per access policy.
Use the new embedded experience to select a principal. The previous popup experience can be accessed here. Select a principal
marketing-secu
Marketing-security
Marketing-Security Group 36916747
Marketing-Security-Group
Selected item
Marketing-Security Group 36916747
Previous
Next
Search
4:27 PM
9/4/2025

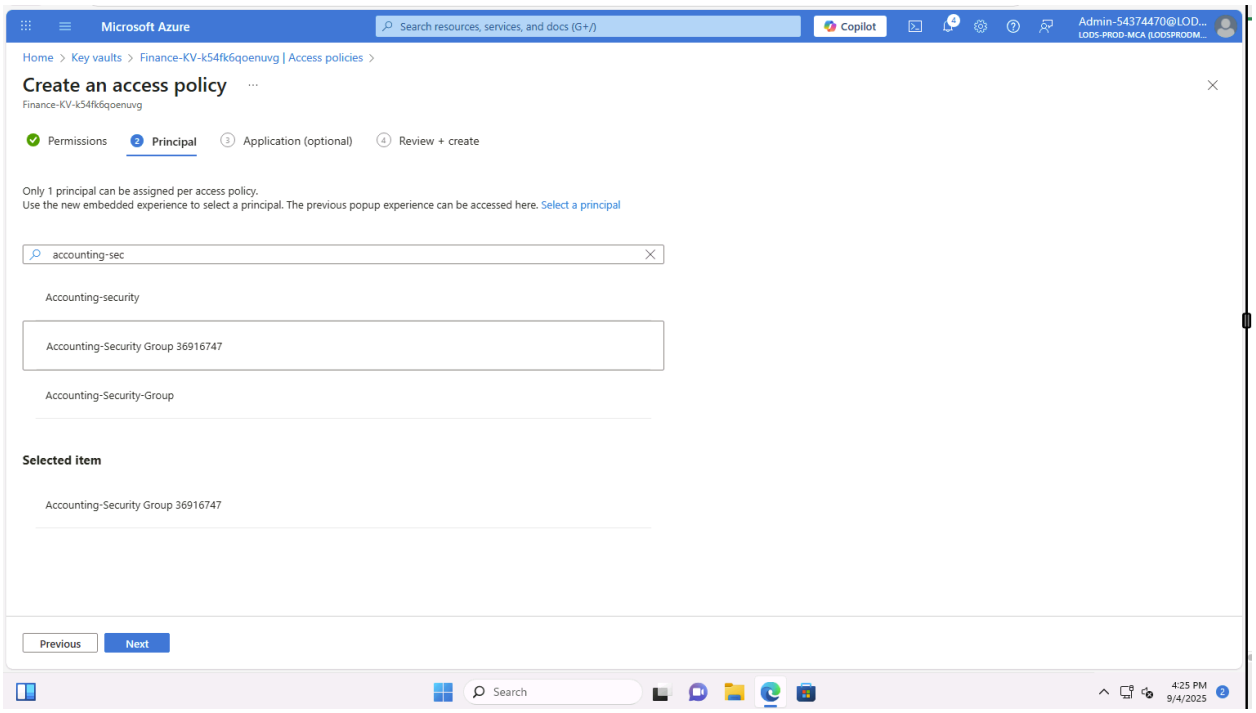

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Admin-54374470@LOD...
LODS-PROD-MCA (LODSPRODM...
Home > Key vaults > Market-KV-rprgaz4qmorgk | Access policies >
Create an access policy
Market-KV-rprgaz4qmorgk
Permissions
Principal
Application (optional)
Review + create
Configure from a template
Select a template
Key permissions
Key Management Operations
Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Cryptographic Operations
Select all
Secret permissions
Secret Management Operations
Select all
Get
List
Set
Delete
Recover
Backup
Restore
Privileged Secret Operations
Select all
Purge
Certificate permissions
Certificate Management Operations
Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Manage Contacts
Manage Certificate Authorities
Get Certificate Authorities
Previous
Next
Search
4:26 PM
9/4/2025

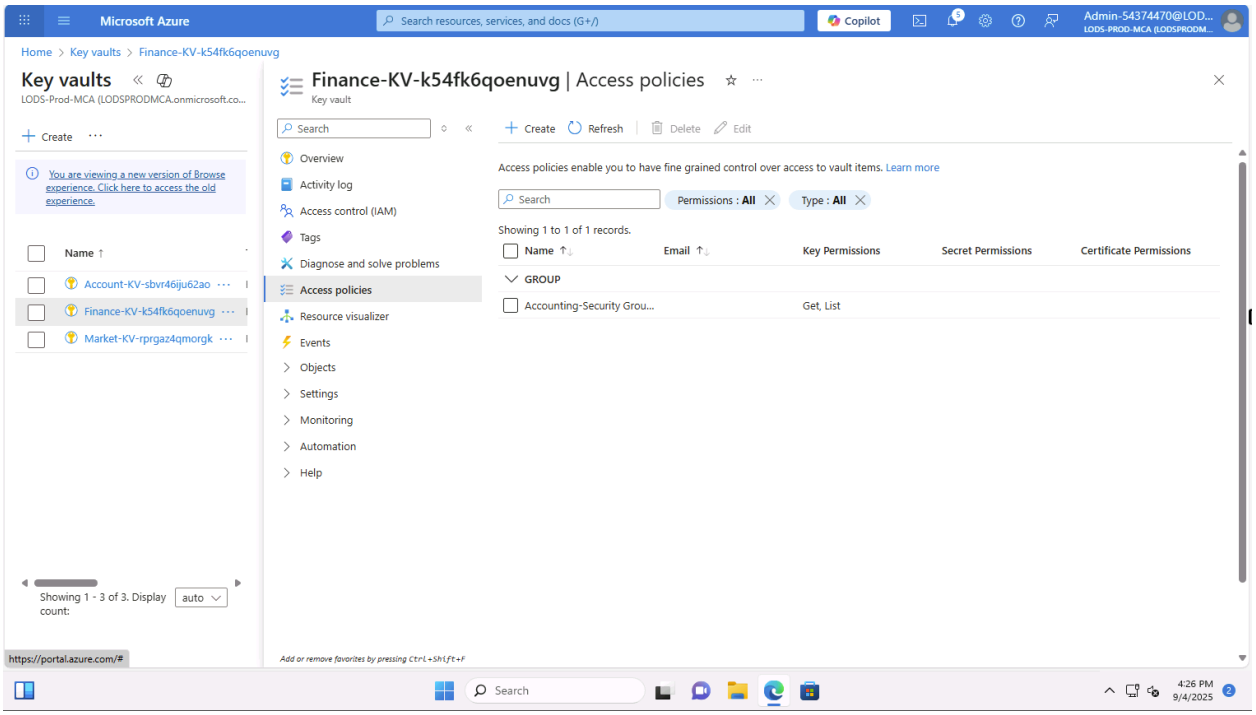

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Admin-54374470@LOD...
LODS-PROD-MCA (LODSPRODM...
Home > Key vaults > Market-KV-rprgaz4qmorgk
Key vaults
LODS-Prod-MCA (LODSPRODMCA.onmicrosoft.co...
Create
You are viewing a new version of Browse experience. Click here to access the old experience.
Name
Account-KV-sbvr46iju62ao
Finance-KV-k54fk6qoenuvg
Market-KV-rprgaz4qmorgk
Showing 1 - 3 of 3. Display count: auto
Market-KV-rprgaz4qmorgk | Access policies
Key vault
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Access policies
Resource visualizer
Events
Objects
Settings
Monitoring
Automation
Help
Create
Refresh
Delete
Edit
Access policies enable you to have fine grained control over access to vault items. Learn more
Search
Permissions : All
Type : All
Showing 1 to 1 of 1 records.
Name
Email
Key Permissions
Secret Permissions
Certificate Permissions
GROUP
Marketing-Security Group...
Get, List
Add or remove favorites by pressing Ctrl+Shift+F
Search
4:27 PM
9/4/2025

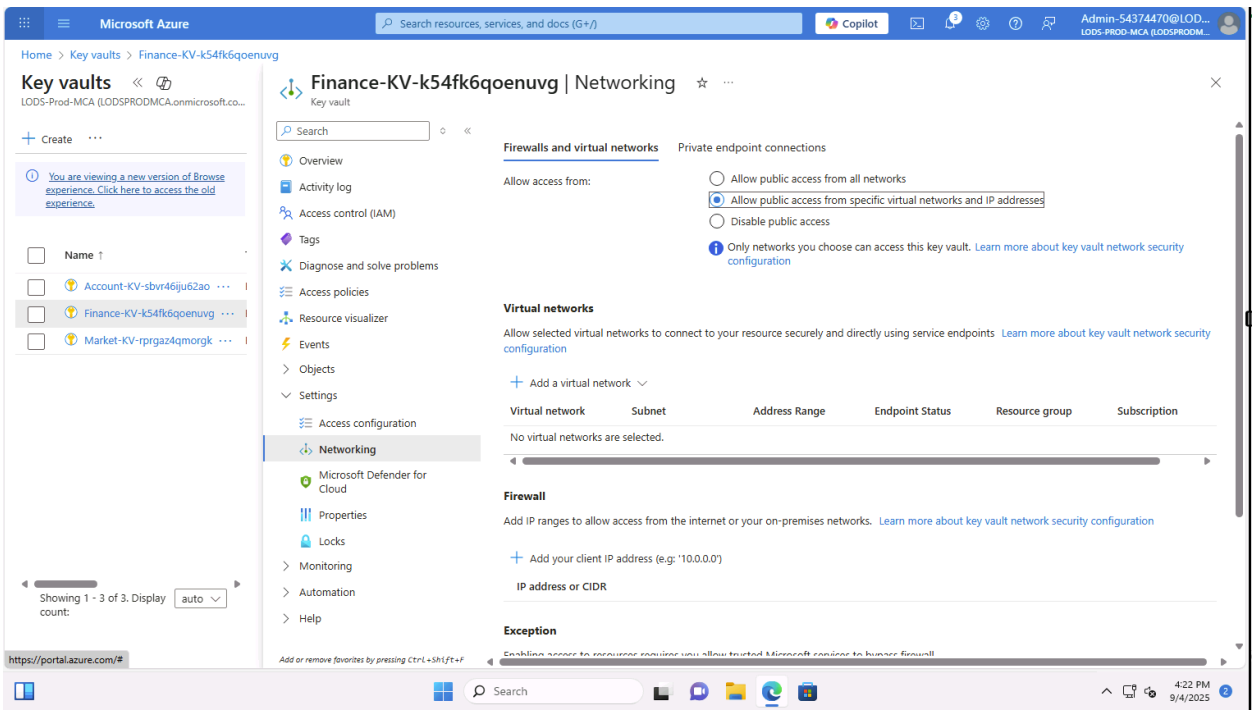

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Admin-54374470@LOD...
LODS-PROD-MCA (LODSPRODM...
Home > Key vaults > Market-KV-rprgaz4qmorgk
Key vaults
LODS-Prod-MCA (LODSPRODMCA.onmicrosoft.co...
Create
You are viewing a new version of Browse experience. Click here to access the old experience.
Name
Account-KV-sbvr46iju62ao
Finance-KV-k54fk6qoenuvg
Market-KV-rprgaz4qmorgk
Showing 1 - 3 of 3. Display count: auto
Market-KV-rprgaz4qmorgk | Networking
Key vault
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Access policies
Resource visualizer
Events
Objects
Settings
Access configuration
Networking
Microsoft Defender for Cloud
Properties
Locks
Monitoring
Automation
Help
Firewalls and virtual networks
Private endpoint connections
Allow access from:
Allow public access from all networks
Allow public access from specific virtual networks and IP addresses
Disable public access
Only networks you choose can access this key vault. Learn more about key vault network security configuration
Virtual networks
Allow selected virtual networks to connect to your resource securely and directly using service endpoints Learn more about key vault network security configuration
Add a virtual network
Virtual network
Subnet
Address Range
Endpoint Status
Resource group
Subscription
No virtual networks are selected.
Firewall
Add IP ranges to allow access from the internet or your on-premises networks. Learn more about key vault network security configuration
Add your client IP address (e.g. '10.0.0.0')
IP address or CIDR
Exception
https://portal.azure.com/#
Add or remove favorites by pressing Ctrl+Shift+F
Search
4:11 PM
9/4/2025

Finance resource group:

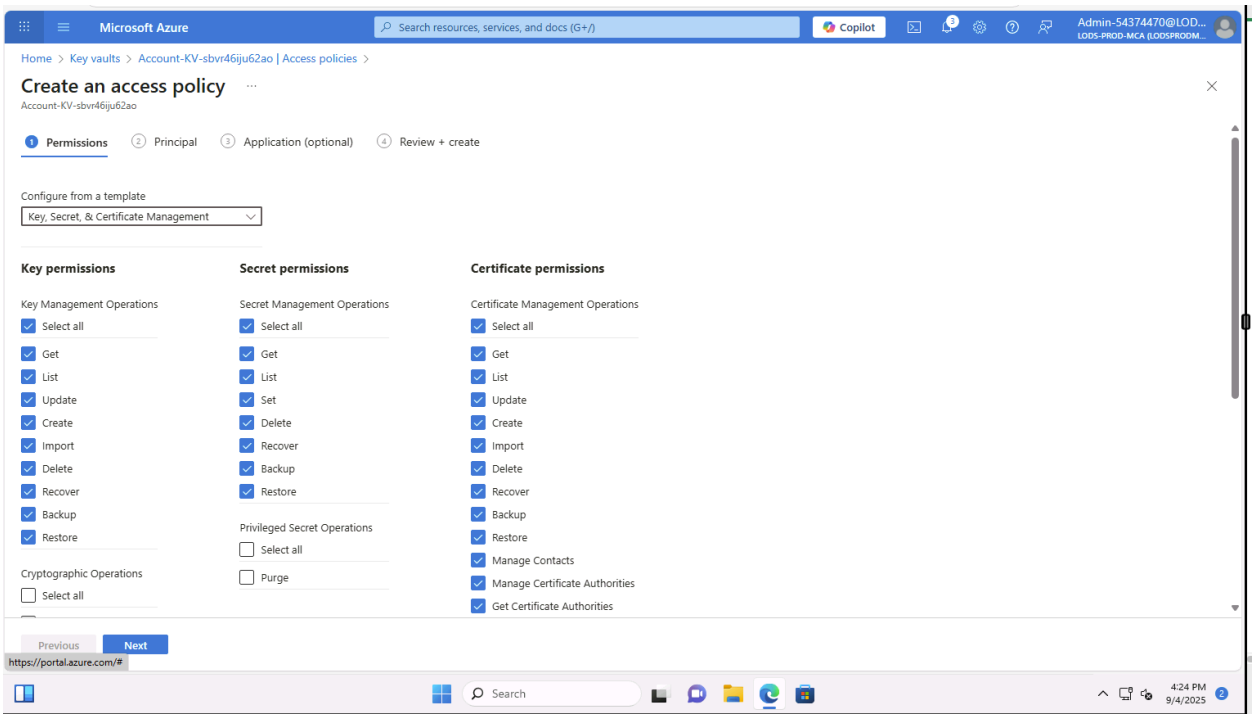


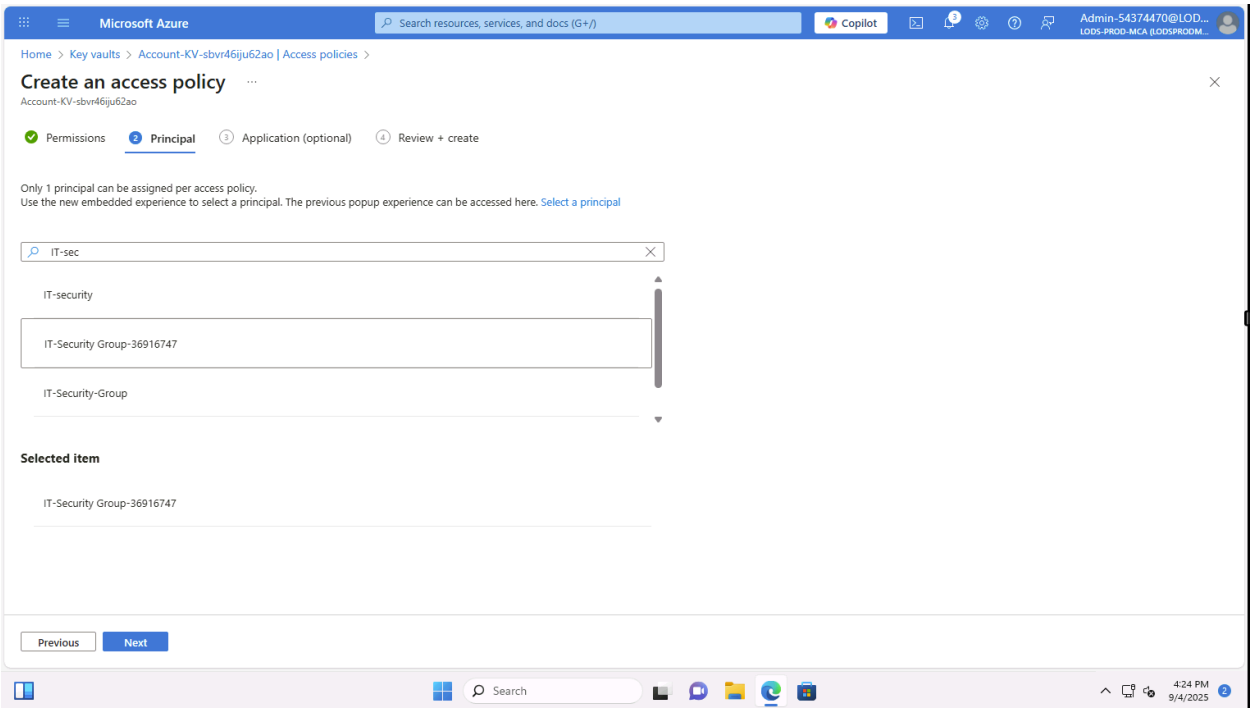


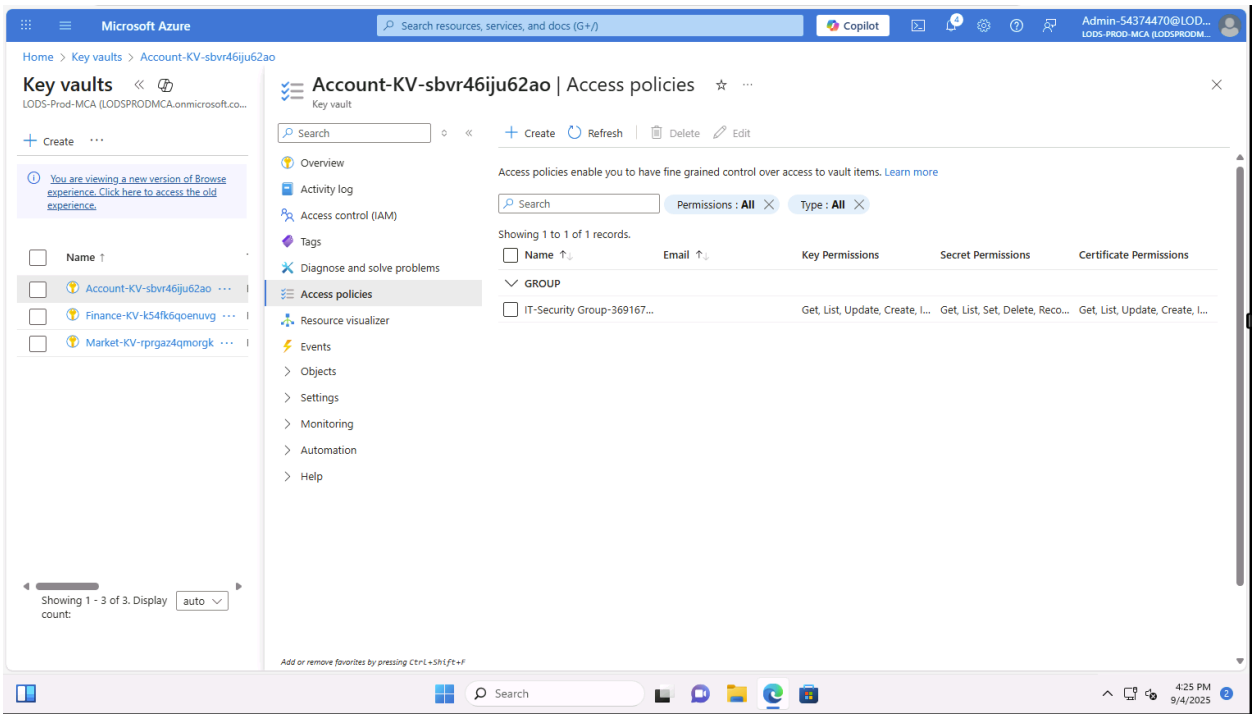


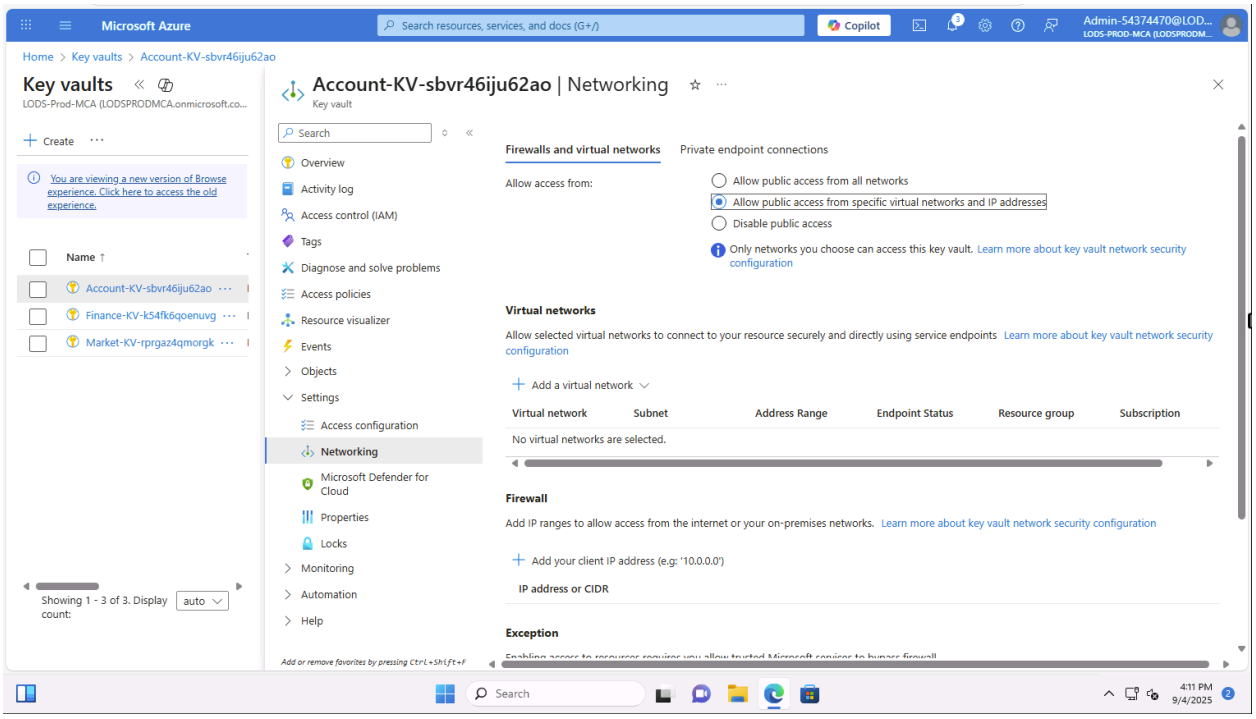


IT resource group:


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Admin-54374470@LOD...
LODS-PROD-MCA (LODSPRODM...
Home > Key vaults > Account-KV-sbvr46iju62ao | Access policies >
Create an access policy
Account-KV-sbvr46iju62ao
1 Permissions
2 Principal
3 Application (optional)
4 Review + create
Configure from a template
Key, Secret, & Certificate Management
Key permissions
Key Management Operations
Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Cryptographic Operations
Select all
Secret permissions
Secret Management Operations
Select all
Get
List
Set
Delete
Recover
Backup
Restore
Privileged Secret Operations
Select all
Purge
Certificate permissions
Certificate Management Operations
Select all
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Manage Contacts
Manage Certificate Authorities
Get Certificate Authorities
Previous
Next
https://portal.azure.com/#
Search
4:24 PM
9/4/2025


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Admin-54374470@LOD...
LODS-PROD-MCA (LODSPRODM...
Home > Key vaults > Account-KV-sbvr46iju62ao | Access policies >
Create an access policy
Account-KV-sbvr46iju62ao
Permissions
2 Principal
3 Application (optional)
4 Review + create
Only 1 principal can be assigned per access policy.
Use the new embedded experience to select a principal. The previous popup experience can be accessed here. Select a principal
IT-sec
IT-security
IT-Security Group-36916747
IT-Security-Group
Selected item
IT-Security Group-36916747
Previous
Next
Search
4:24 PM
9/4/2025





D2. Encryption Recommendations

Data at rest – Azure Key Vaults can store and manage encryption keys, secrets, and certificates for services such as Storage Blobs, Databases, and Virtual Machines. The use of Key Vault ensures sensitive data is kept secure and also helps the company meet compliance goals.

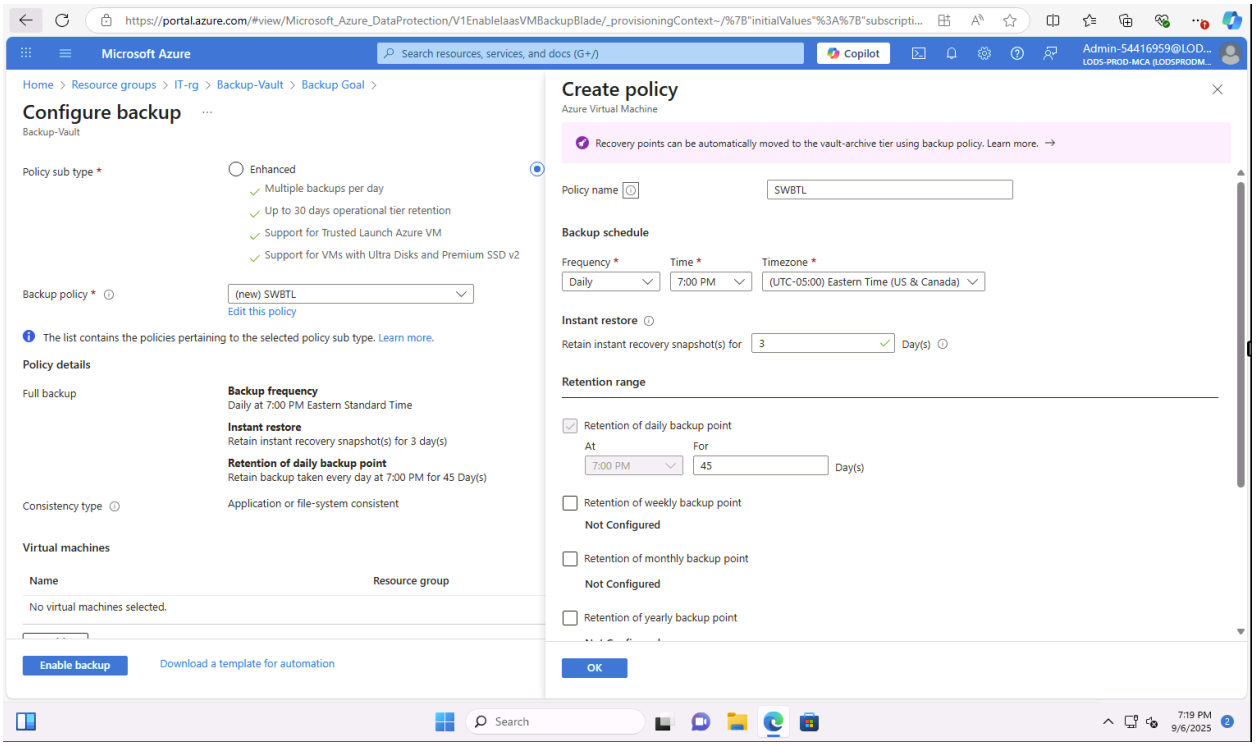
Data in transit – Azure Key Vault can store and manage SSL/TLS certificates. This protects data in transit by preventing it from being intercepted or tampered with during communication between applications and services.

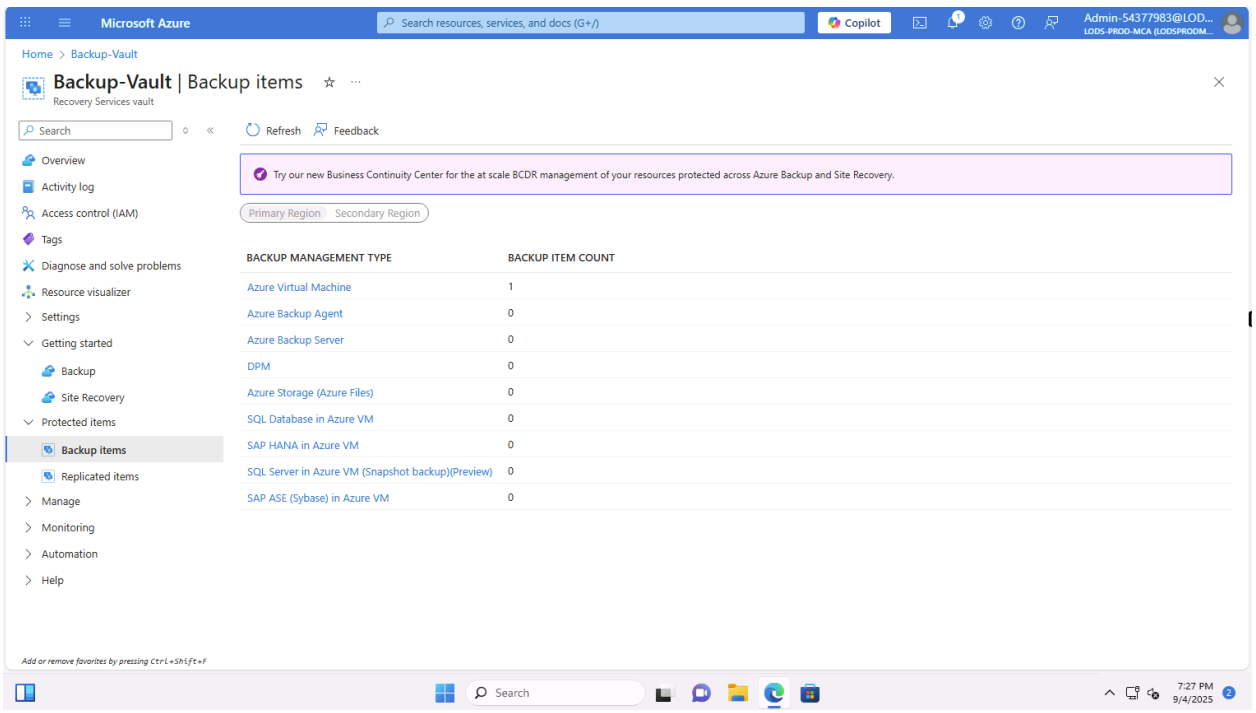
E1. Azure Cloud Backups

I configured two different backup settings in the IT-rg Resource group including:

Virtual machine backup:

- Created a new policy named SWBTL
- Configured a daily backup at 7:00 PM EST.
- The backup retention period is set for 45-days
- Instant restore is set to 3 days

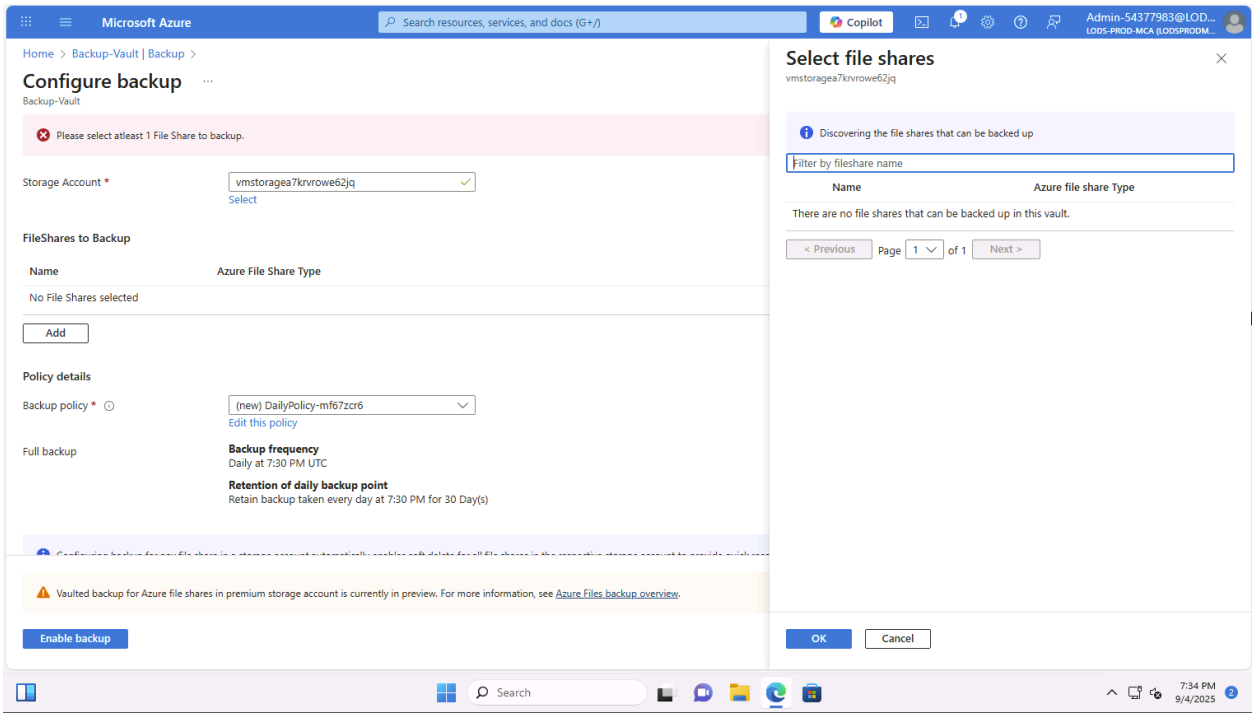




File Share Backup:

The second example demonstrates a file share backup:

- Scheduled a daily backup at 7:30 pm UTC time
- Set backup retention period for 30-days
- As no file shares are currently available in the environment, the configuration demonstrates how it would be implemented at a future date.



E2. Supporting Business Requirements

The backup configurations implemented support business requirements by strengthening disaster recovery and regulatory compliance. They also protect against data loss caused by intentional or

unintentional errors and safeguard the company from system failures. These align with the requirements of SWBTL, including a 45-day backup policy, RPO of one day with daily backups scheduled, and snapshots maintained for 3 days.

F1. Shared Responsibility

With Infrastructure as a Service (IaaS), the cloud provider is responsible for securing the hosts, network, and datacenters, while the customer is responsible for managing the operating system, controls, applications, identity and access management (IAM) policies, data, and devices (Microsoft, n.d).

Applicable Risks

1. Broken access controls - Misconfigured access controls can allow unauthorized users to exfiltrate data or launch cyberattacks. This represents a high risk because it directly compromises the confidentiality and integrity of company data.
2. Data loss - Proper storage and backup policies are the responsibility of the company. The impact is high due to its effect on data availability in the event of downtime or data loss.

3. Compliance issues - Without the correct compliance measures, the company faces a medium to high impact if it fails to meet applicable regulatory standards.

Recommendations

1. Strong IAM policies - Use MFA, Principles of least privilege and conditional access policies to prevent unauthorized access
2. Strong Backup policies - Schedule and asses backup policies regularly to ensure data security
3. Continuous monitoring - Use tools, manual and automated monitoring solutions to meet compliance needs. (Microsoft, n.d).

G. Cloud Threats and Mitigation Tactics

Some potential threat vectors and migration tactics are:

1. Data Breaches – Misconfigurations can include weak access controls, flaws in software configurations, and unauthorized data exfiltration from storage accounts.
    - Mitigation countermeasures – This includes encryption of data, effective use of firewalls and IAM policies, and monitoring of suspicious behavior patterns.

2. Insider threats – Employees may intentionally or unintentionally cause system disruptions.
    - Mitigation countermeasures – Implementing robust access controls and maintaining the principle of least privilege best practices.
3. Account hijacking – If a bad actor compromises a user account it could lead to unauthorized access to data and resources.
    - Mitigation countermeasures – Adhering to granular access policies limits the attack surface should an account be compromised. Multifactor authentication can help prevent initial access.

References

Microsoft. Shared responsibility in the cloud. (n.d.). Retrieved September 5, 2025, from https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

Microsoft. Cloud adoption framework: Secure methodology in Azure. (n.d.). Retrieved September 5, 2025, from https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/govern/monitor-cloud-governance