Denzel Frimpong
Student ID#:
D485 Cloud Security

Cloud Security Implementation Plan

A. Executive Summary

SWBTL LLC's Microsoft Azure cloud environment exhibits numerous securities issues and fails to meet the company's business needs. The following points details the discrepancies between the current security environment and the company's business requirements:

1. **Compliance with Applicable Regulations and Standards:** SWBTL LLC holds contracts with the U.S. government and processes card transactions daily. Therefore, it must adhere to the Federal Information Security Modernization Act (FISMA) and the Payment Card Industry Data Security (PCI DSS). Presently, SWBTL LLC's existing cloud environment does not meet these regulatory requirements.
2. **Azure Resource Groups and Azure Role-based Access Control (RBAC):** SWBTL LLC requires that departmental resources be accessible only to users within the respective department, adhering to the principle of least privilege. However, the current cloud environment does not meet this requirement.
3. **Azure Key Vaults and Encryption of Data-at-Rest and Data-in-Transit:** Currently, There are no services in place to encrypt data-at-rest or data-in-

transit. Azure key Vaults can be utilized to secure encryption keys when implementing services like Azure Disk Encryption and Azure SQL Database TDE for data-at-rest. For Data-in-transit, Azure Key Vaults enforce transport-level encryption to safeguard data transferred between Azure Key Vault and Clients.

4. **Backups:** SWBTL LLC has specific business requirements for backups, including their frequency, retention, and recovery objectives. Currently, there are no policies or configurations in places that meet these requirements.
5. **Vulnerability Scanning:** The current vulnerability scans are outdated, and it is unclear whether they include the cloud environment.

Overall, SWBTL LLC's cloud environment lacks the essential security controls needed to meet its business requirements and comply with regulations and standards. The company must implement corrective actions to secure the cloud environment properly.

B. Proposed Course of Action

The recommended course of action for SWBTL LLC involves adopting Microsoft's Azure Government Infrastructure as a Service (IaaS) solution. This will provide the company with a FEDRAMP/FedRamp+ authorized product that is also approved at DOD Impact Level (IL) 5. Additionally, this service model aligns with the company's needs by enabling the deployment and management of multiple operating systems, virtual machines, and custom applications, all supported by on-demand compute, storage, and network resources.

Applicable regulatory compliance directives include the following:

- **Federal Information Security Modernization Act (FISMA):** As a U.S government contractor, SWBTL LLC must adhere to the information security standards and guidelines mandated by FISMA, which includes those developed by the national Institute of Standards and Technology (NIST) (NIST, 2016).
- **Federal Risk and Authorization Management program (FedRAMP):** This program utilizes NIST standards to establish uniform security requirements for cloud services (FedRAMP, n.d.). Microsoft Azure Government aligns its controls with NIST Sp 800-53 Rev. 5 to achieve compliance and FedRAMP authorization (Microsoft, 2024).
- **Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG):** Developed and maintained by the DoD's Defense Information Systems Agency (DISA), this guide outlines security requirements for cloud solutions. Compliance with these SRG and DoD FedRAMP+ controls grants cloud solutions a DoD provisional authorization. The Microsoft Azure Government solution, for instance, is classified as DoD Impact Level 5 (IL 5) (Microsoft, 2023).
- **Payment Card Industry Data Security Standard (PCI DSS):** PCI DSS applies to any organization that stores, processes, or transmits cardholder data. According to the Company Overview and Requirements are relevant to SWBTL LLC handles card transactions daily. Therefore, PCI DSS requirements are relevant to SWBTL LLC, The operational aspects of their systems involved in processing transactions (PCI Security Standards Council, 2018).

Security Benefits of Microsoft Azure government IaaS:

The Microsoft Azure government IaaS solution offers numerous security advantages. The following outline the benefits essential for SWBTL LLC:

- Azure Resource manager: This solution allows for the creation and management of resource groups. It also includes a tagging feature to identify resources associated with these groups.
- Azure RBAC: This service manages access to resources by restricting permissions based on a need-to-know basis. Implementing Azure RBAC ensures that the principle of least privilege is upheld.
- Encryption in Transit: Azure Storage allows data encryption during transit using transport-level encryption, wire encryption, and client-side encryption.
- Encryption at Rest: Azure Storage enables data encryption at rest through storage service encryption, client-side encryption, Azure Disk Encryption, and Azure SQL Database Transparent Data Encryption (TDE).
- Azure Backup: This solution offers backup services that allow authorized users to back up and restore virtual machines, files, folders, SQL databases, and more. This service is crucial for securely recovering any lost data following accidental deletion (Microsoft, 2022).

Security Challenges of Microsoft Azure Government IaaS:

Despite the many security benefits of the Microsoft Azure Government IaaS solution, a significant challenge is the potential misconfiguration of security controls in the cloud environment. Security is a shared responsibility between the cloud service provider (CSP) and the customer. This underscores the necessity for customers to implement security controls according to industry's best practices and to thoroughly test these controls for

quality assurance. Improper implementation of security controls can have serious consequences for confidentiality, integrity, and availability of the cloud environment.

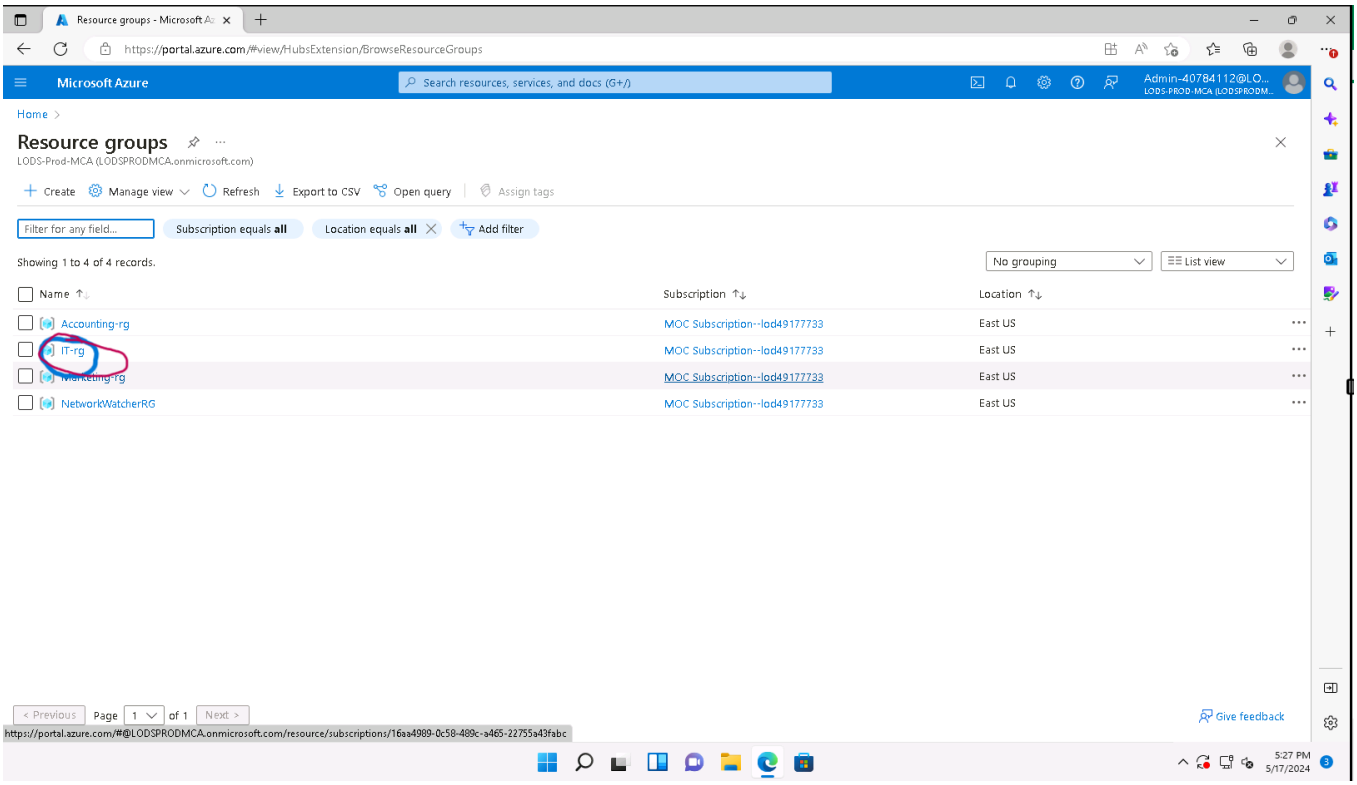
C. Role-Based Access Control

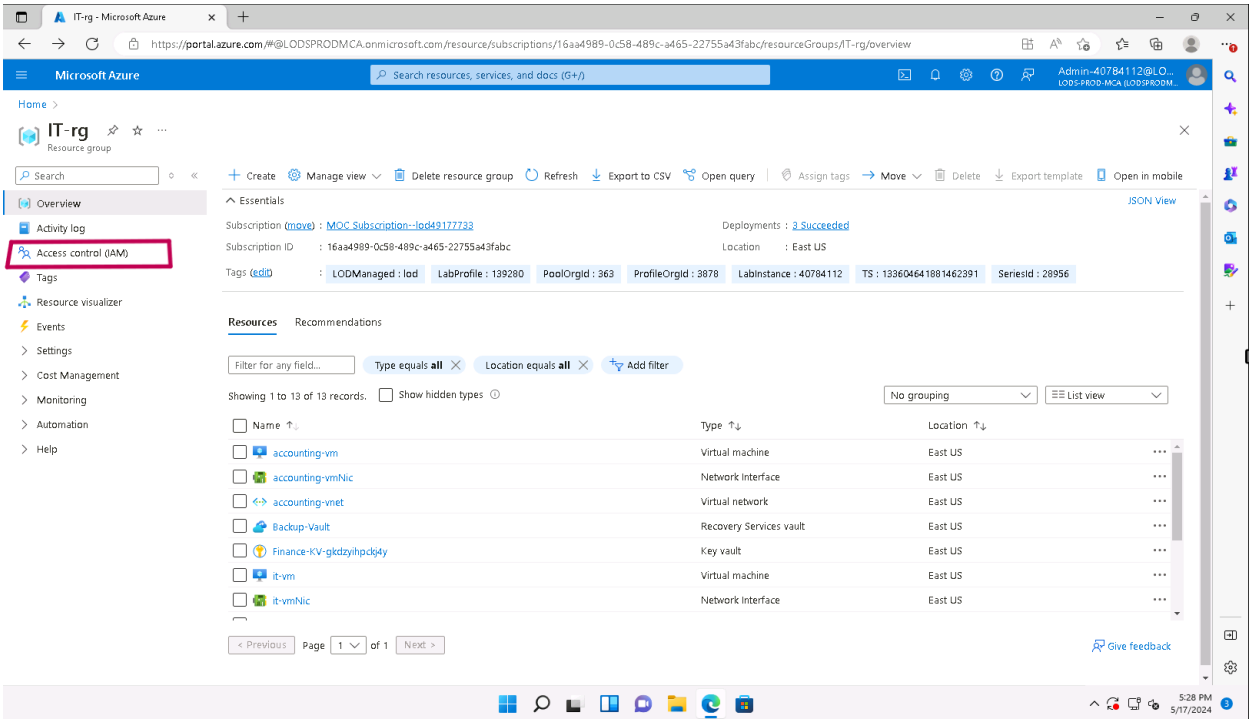
The following three recommendations can be implemented for RBAC:

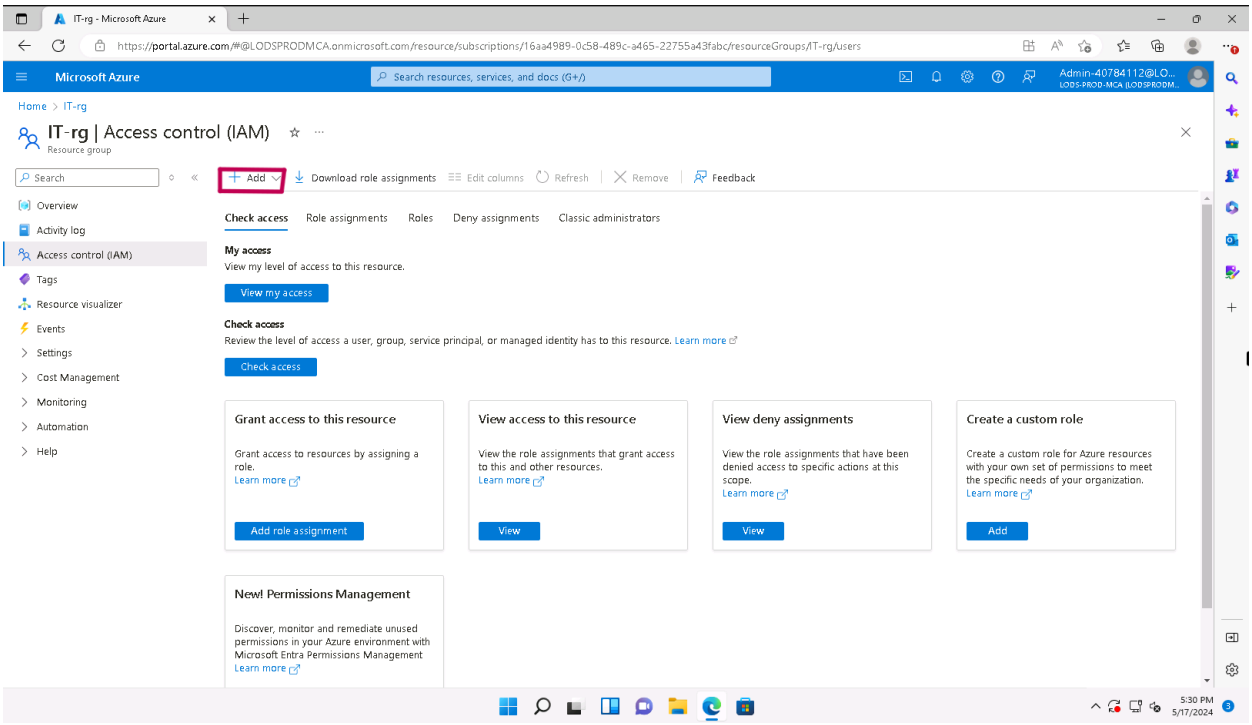
1. To enforce the principle of least privilege, the Accounting Department at SWBTL LLC Accounting Department at SWBTL LLC should not access to the resources of the IT or Marketing Departments. Similarly, the IT and Marketing Departments should only have access to their own respective resources.
2. To enforce the principle of least privilege, the Microsoft Azure Government IaaS cloud solution includes built-in roles, such as “Contributor,” that can be assigned to different departments.
3. These roles, along with the departmental users assigned to them, should be reviewed and updated regularly in accordance with regulatory timeframes.

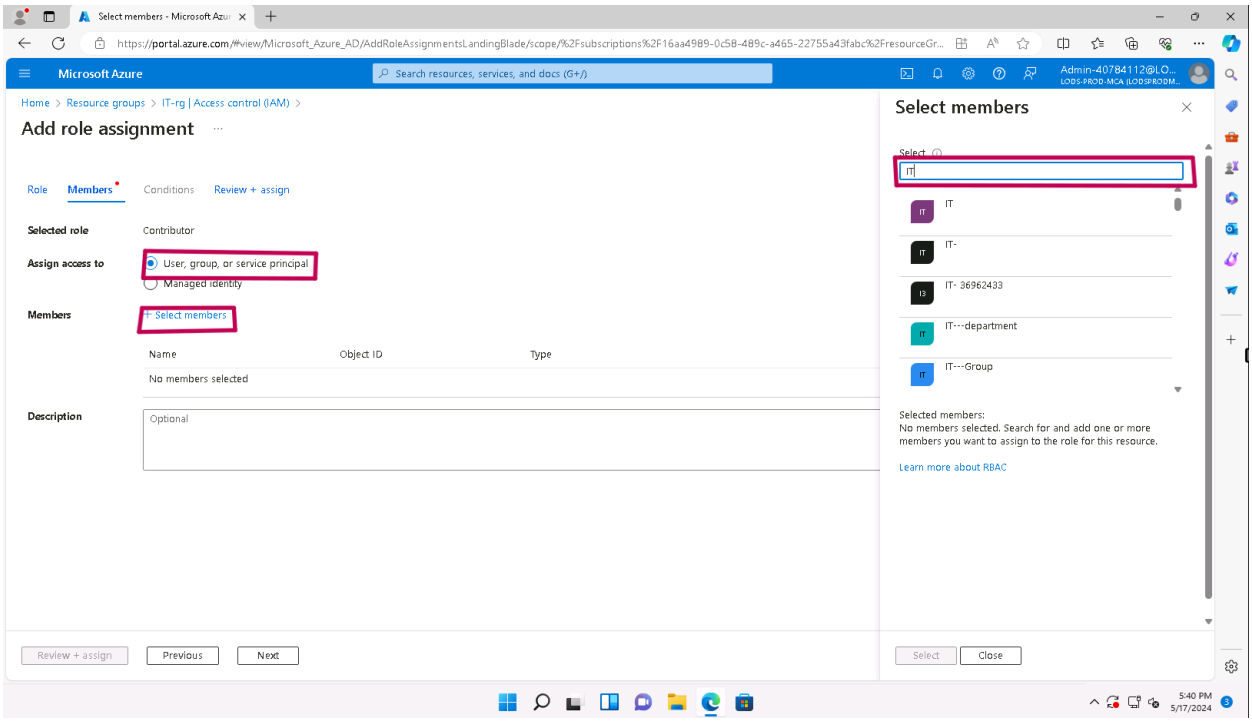
The following screenshots illustrate the complete steps for configuring RBAC for the IT Department, beginning with the Resource Groups area. These steps will then be repeated for the Accounting and Marketing Departments.

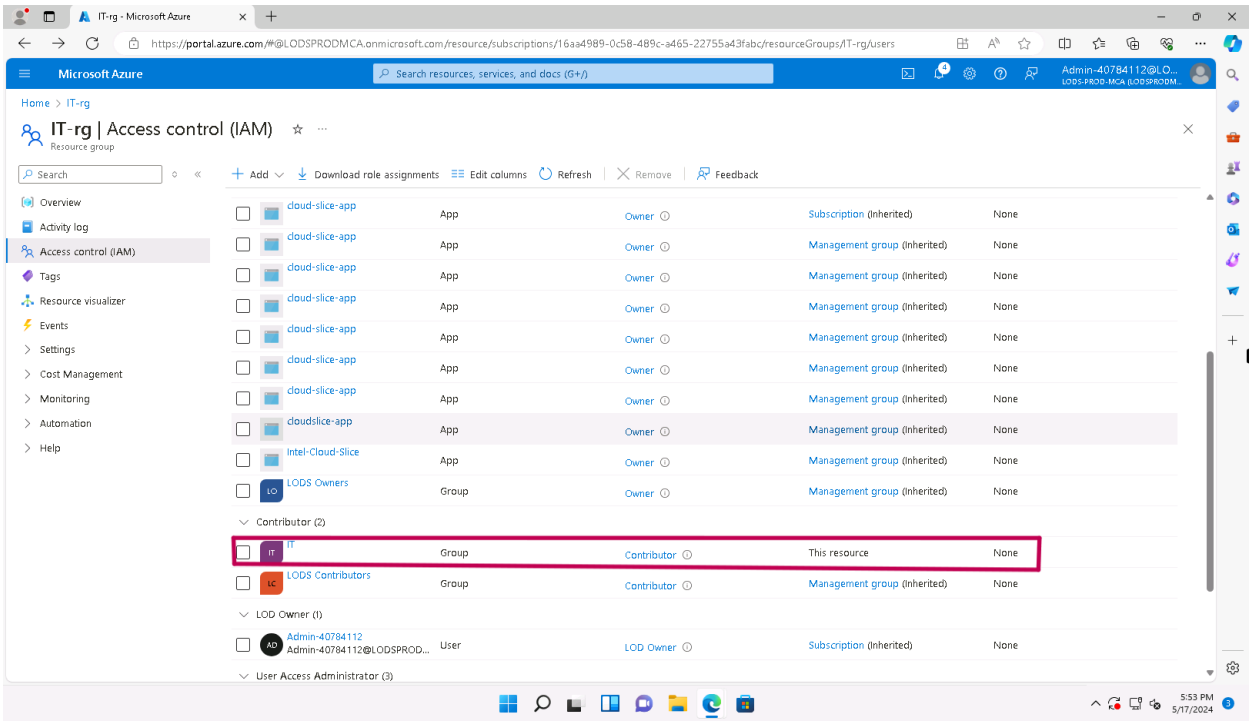
IT Department:


Resource groups - Microsoft Azure
https://portal.azure.com/#view/HubsExtension/BrowseResourceGroups
Microsoft Azure
Search resources, services, and docs (G+/)
Admin-40784112@LO...
LODS-PROD-MCA (LODSPRODM...
Home
Resource groups
LODS-Prod-MCA (LODSPRODMCA.onmicrosoft.com)
Create
Manage view
Refresh
Export to CSV
Open query
Assign tags
Filter for any field...
Subscription equals all
Location equals all
Add filter
Showing 1 to 4 of 4 records.
No grouping
List view
Name
Subscription
Location
Accounting-rg
MOC Subscription--lod49177733
East US
IT-rg
MOC Subscription--lod49177733
East US
Marketing-rg
MOC Subscription--lod49177733
East US
NetworkWatcherRG
MOC Subscription--lod49177733
East US
< Previous
Page 1 of 1
Next >
Give feedback
https://portal.azure.com/#@LODSPRODMCA.onmicrosoft.com/resource/subscriptions/16aa4989-0c58-489c-a465-22755a43fabc
5:27 PM
5/17/2024

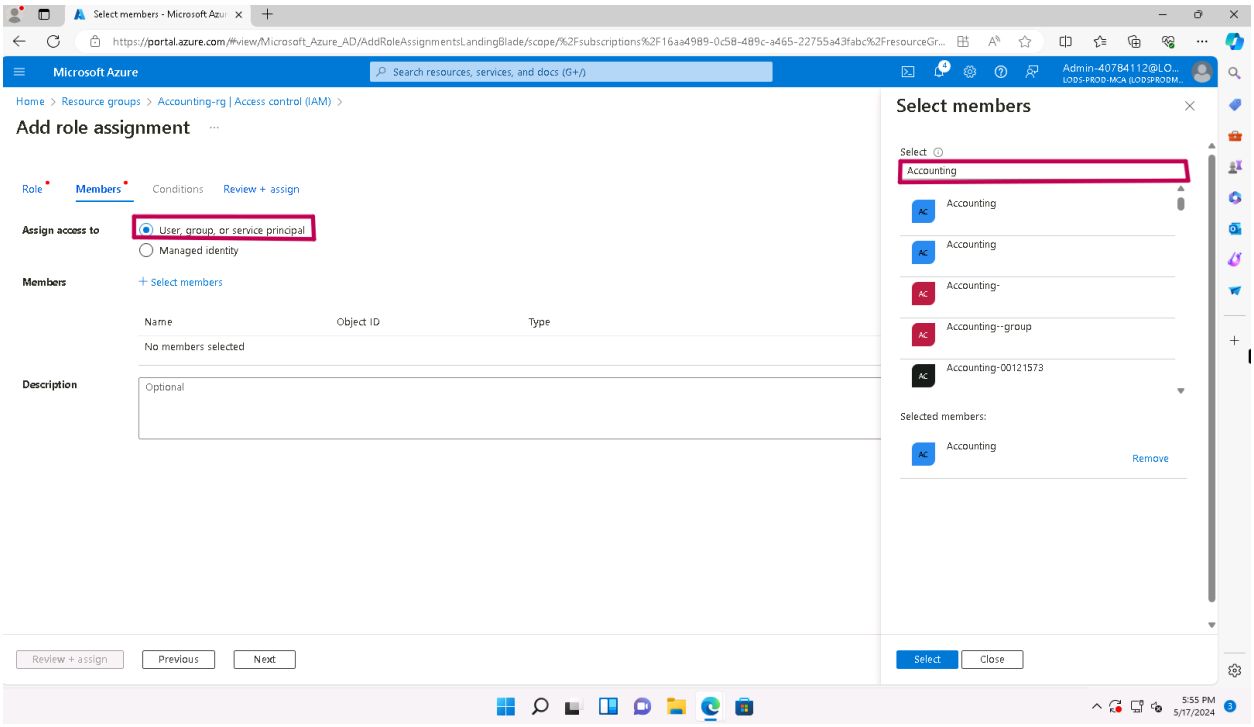

IT-rg - Microsoft Azure
https://portal.azure.com/#@LODSPRODMCA.onmicrosoft.com/resource/subscriptions/16aa4989-0c58-489c-a465-22755a43fabc/resourceGroups/IT-rg/overview
Microsoft Azure
Search resources, services, and docs (G+/)
Admin-40784112@LO...
LODS-PROD-MCA (LODSPRODM...
Home
IT-rg
Resource group
Search
Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Events
Settings
Cost Management
Monitoring
Automation
Help
Create
Manage view
Delete resource group
Refresh
Export to CSV
Open query
Assign tags
Move
Delete
Export template
Open in mobile
Essentials
JSON View
Subscription (move) : MOC Subscription--lod49177733
Deployments : 3 Succeeded
Subscription ID : 16aa4989-0c58-489c-a465-22755a43fabc
Location : East US
Tags (edit) : LODManaged : lod
LabProfile : 139280
PoolOrgId : 363
ProfileOrgId : 3878
LabInstance : 40784112
TS : 1336046418814623 91
SeriesId : 28956
Resources
Recommendations
Filter for any field...
Type equals all
Location equals all
Add filter
Showing 1 to 13 of 13 records.
Show hidden types
No grouping
List view
Name
Type
Location
accounting-vm
Virtual machine
East US
accounting-vmNic
Network Interface
East US
accounting-vnet
Virtual network
East US
Backup-Vault
Recovery Services vault
East US
Finance-KV-gkdzyihpckj4y
Key vault
East US
it-vm
Virtual machine
East US
it-vmNic
Network Interface
East US
< Previous
Page 1 of 1
Next >
Give feedback
5:28 PM
5/17/2024

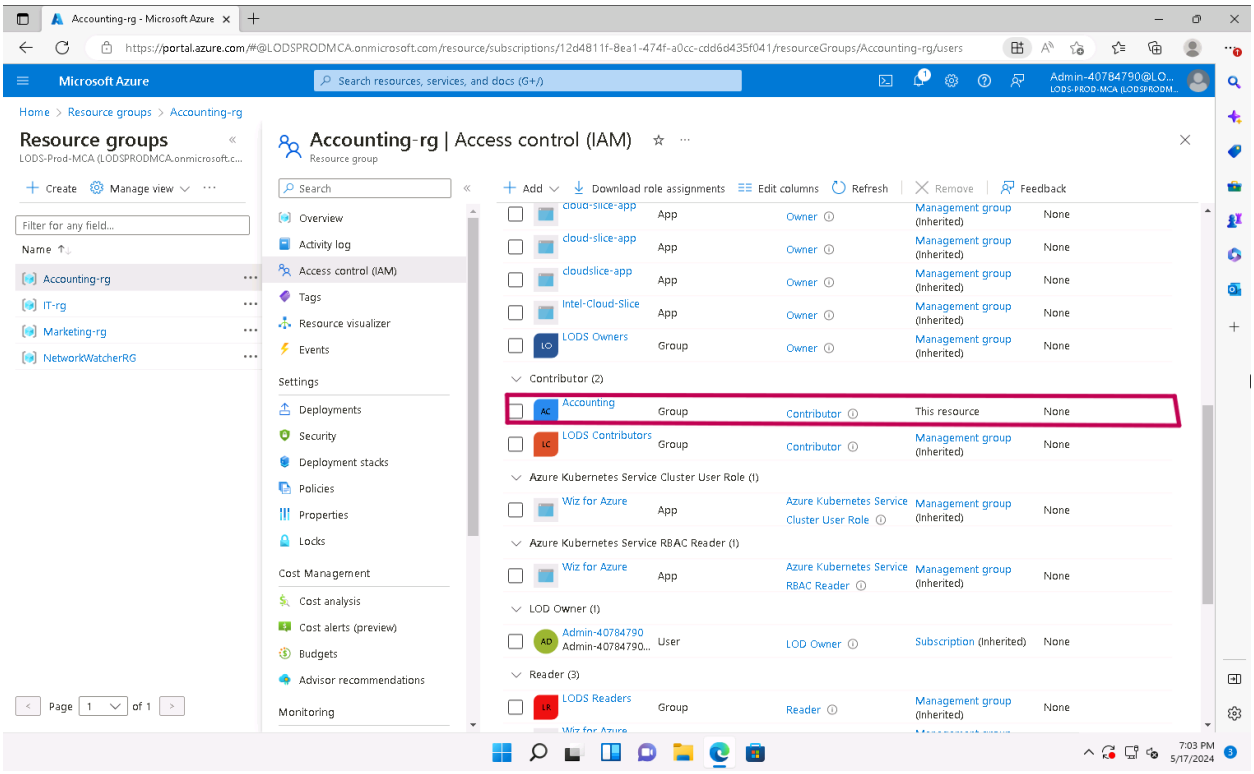

IT-rg - Microsoft Azure
Microsoft Azure
Search resources, services, and docs (G+/)
Home > IT-rg
IT-rg | Access control (IAM)
Resource group
Add
Download role assignments
Edit columns
Refresh
Remove
Feedback
Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Events
Settings
Cost Management
Monitoring
Automation
Help
Check access
Role assignments
Roles
Deny assignments
Classic administrators
My access
View my level of access to this resource.
View my access
Check access
Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more
Check access
Grant access to this resource
Grant access to resources by assigning a role.
Learn more
Add role assignment
View access to this resource
View the role assignments that grant access to this and other resources.
Learn more
View
View deny assignments
View the role assignments that have been denied access to specific actions at this scope.
Learn more
View
Create a custom role
Create a custom role for Azure resources with your own set of permissions to meet the specific needs of your organization.
Learn more
Add
New! Permissions Management
Discover, monitor and remediate unused permissions in your Azure environment with Microsoft Entra Permissions Management
Learn more


Select members - Microsoft Azu
Microsoft Azure
Search resources, services, and docs (G+/)
Home > Resource groups > IT-rg | Access control (IAM) >
Add role assignment
Role
Members
Conditions
Review + assign
Selected role
Contributor
Assign access to
User, group, or service principal
Managed identity
Members
+ Select members
Name
Object ID
Type
No members selected
Description
Optional
Review + assign
Previous
Next
Select members
Select
IT
IT
IT-
IT- 36962433
IT---department
IT---Group
Selected members:
No members selected. Search for and add one or more members you want to assign to the role for this resource.
Learn more about RBAC
Select
Close

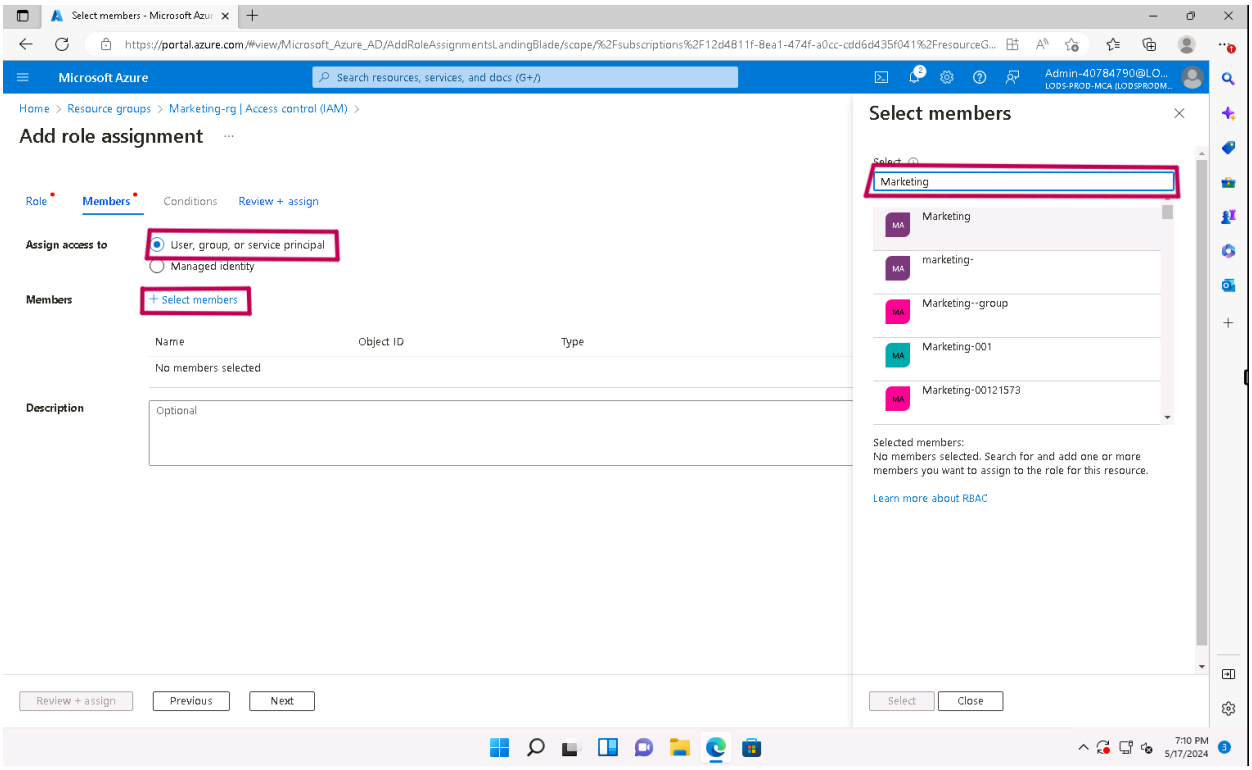


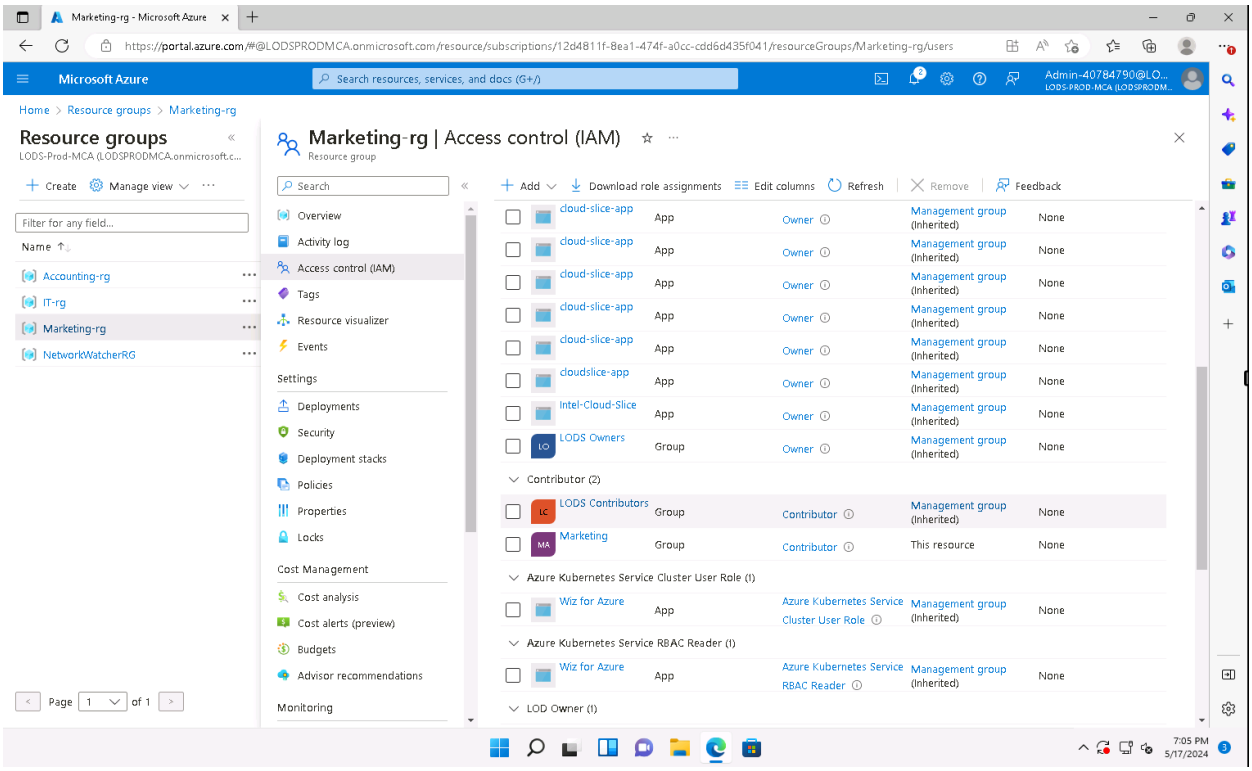
Accounting Department:





Marketing Department:





D. Encryption

Two best practices to implement in relation to Azure key Vaults includes the following:

- Key Rotation Policy: A policy should be set up automatically generate new keys after a specified period. This ensures the company's encryption keys remain secure.
- Resource Group Isolation: Each Resource Group should have its own dedicated Key Vault, ensuring that only users with access to those Resource Groups can access their respective departmental Key Vaults.

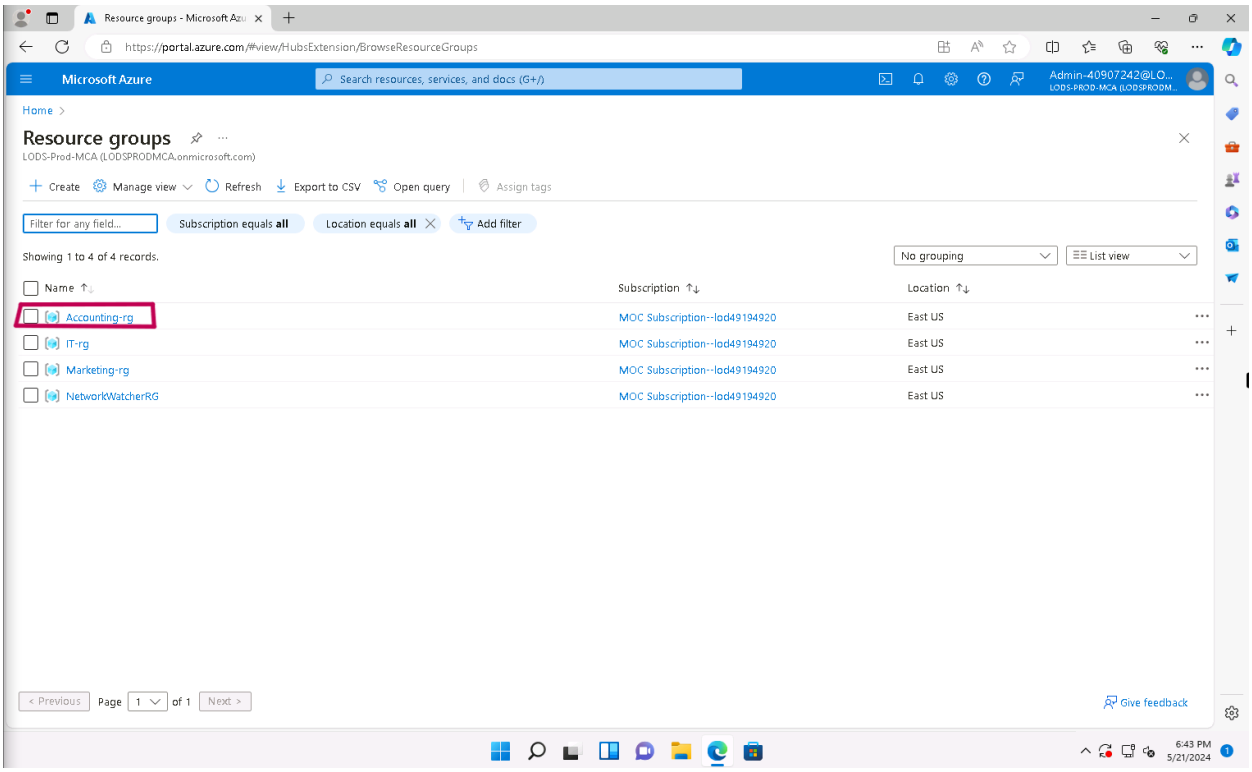
Two recommendations for using Key Vaults to encrypt both data at rest and data in transit are as follows:

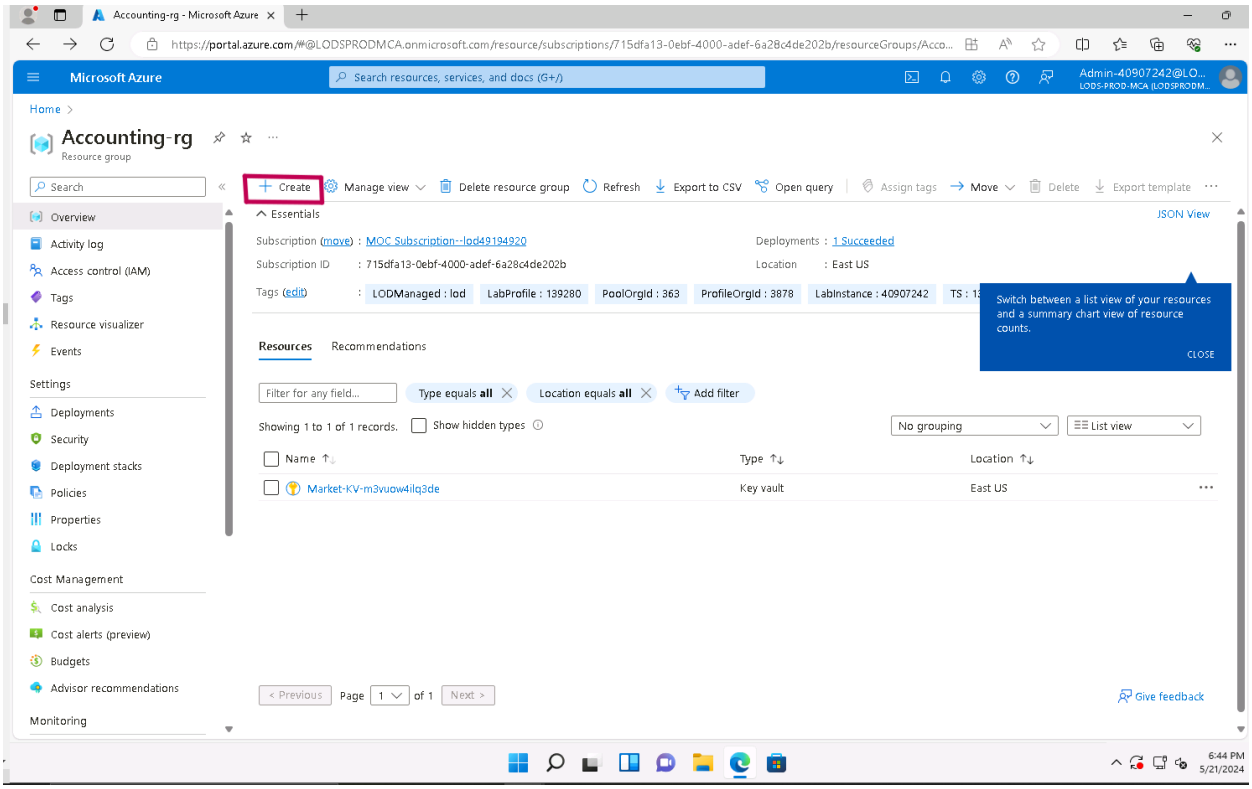
- Data in transit: Azure Key Vaults apply transport-level encryption to protect data transmitted between the Key Vault and Clients.

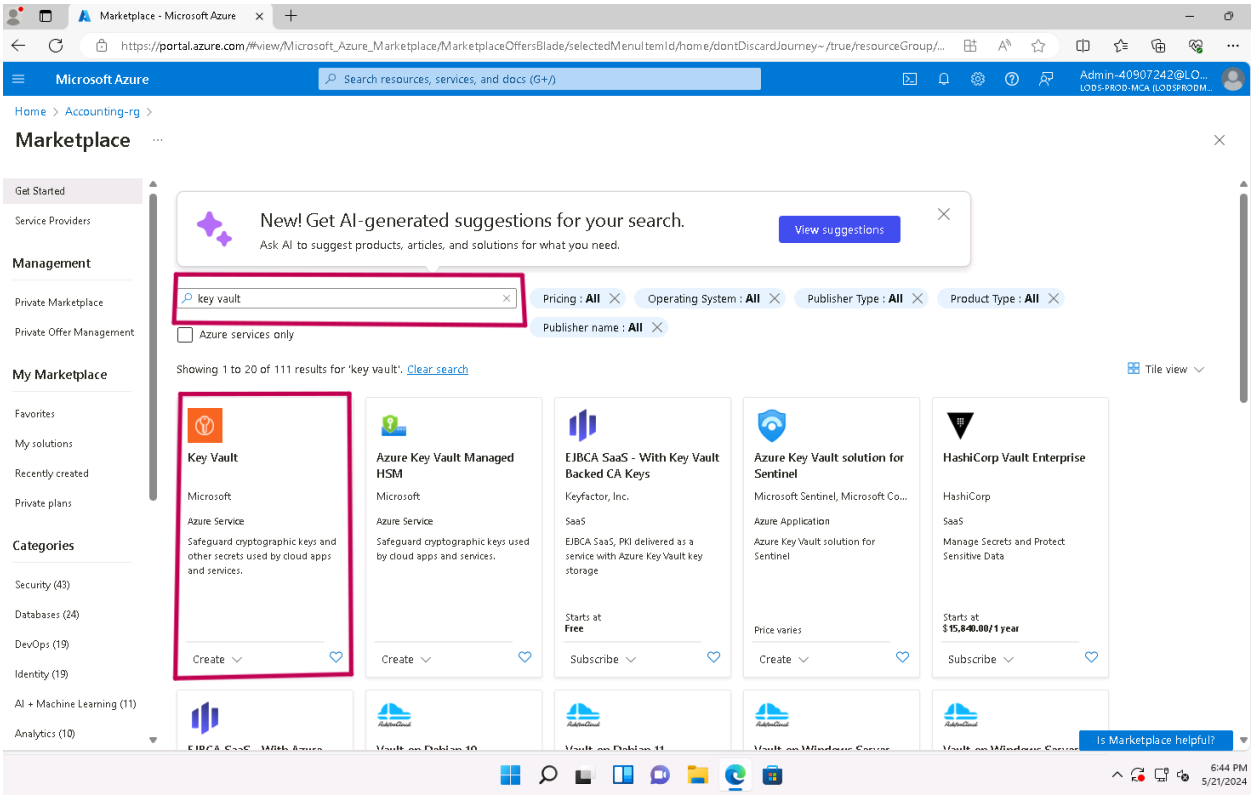
- Data at rest: Azure Key Vaults can be utilized to safeguard encryption keys when using Azure Disk Encryption and Azure SQL Data Transparent Data Encryption services for securing data at rest.

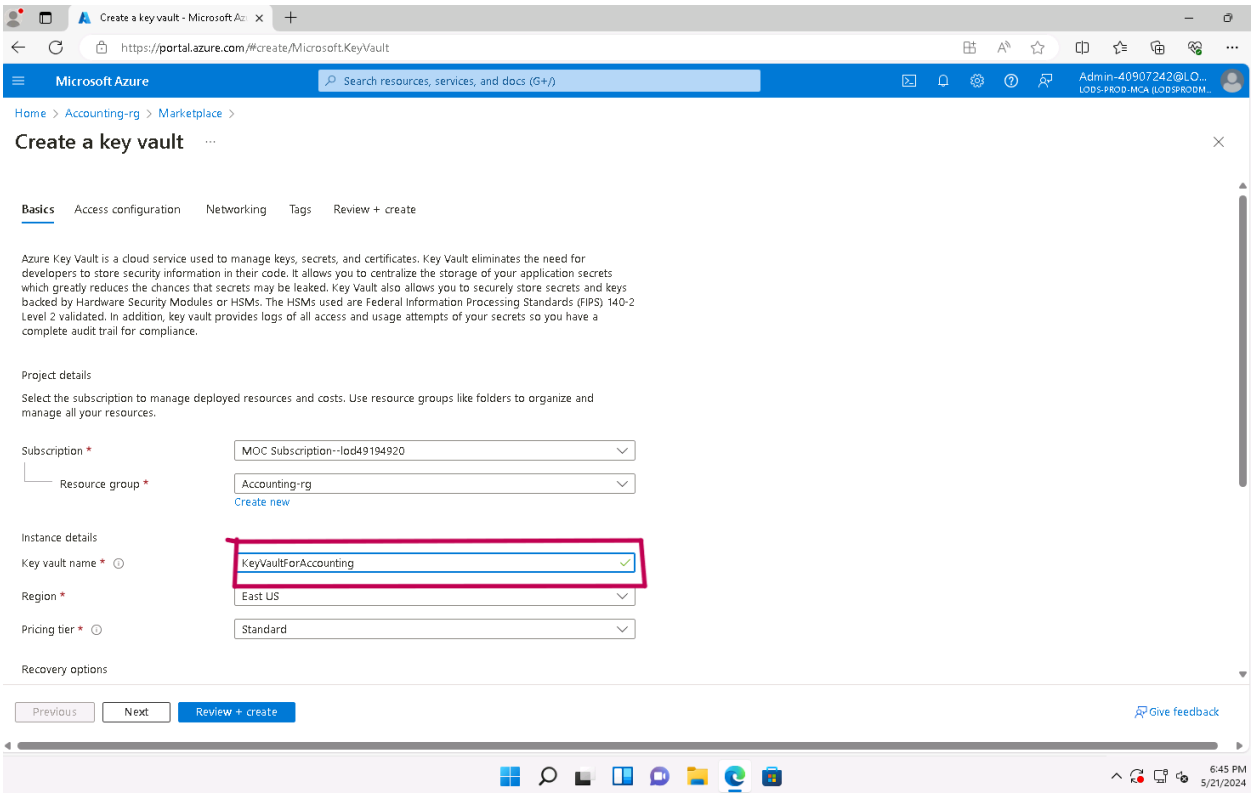
The following screenshots demonstrate the complete steps to configure Key Vaults for the Accounting Department, beginning with the Resource Groups area. These steps will then be repeated for the IT and Marketing Departments:

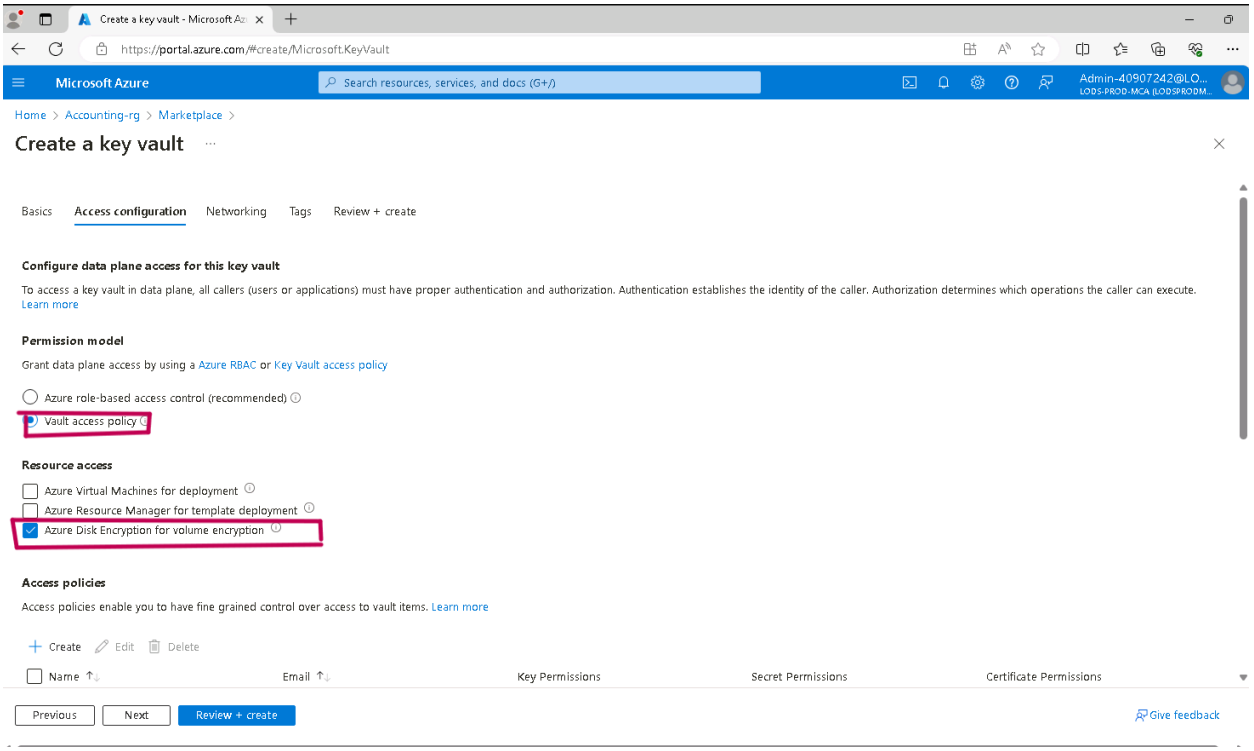
Accounting Department:

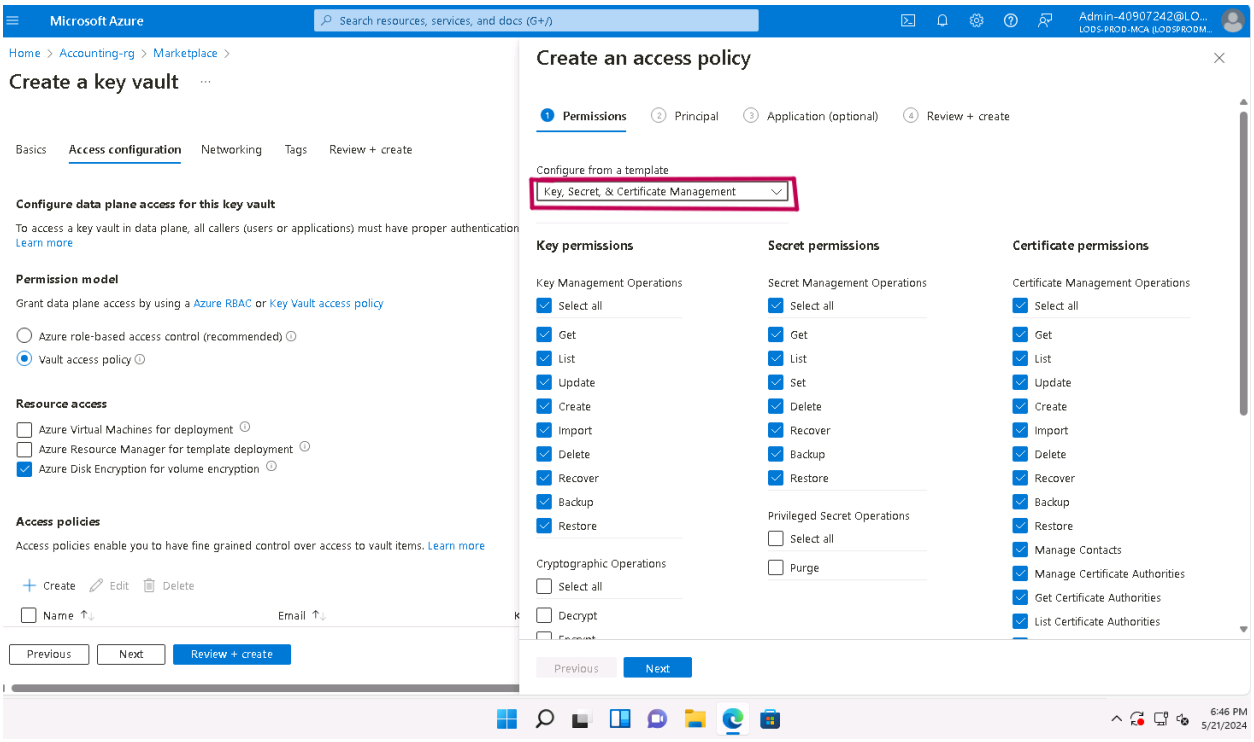


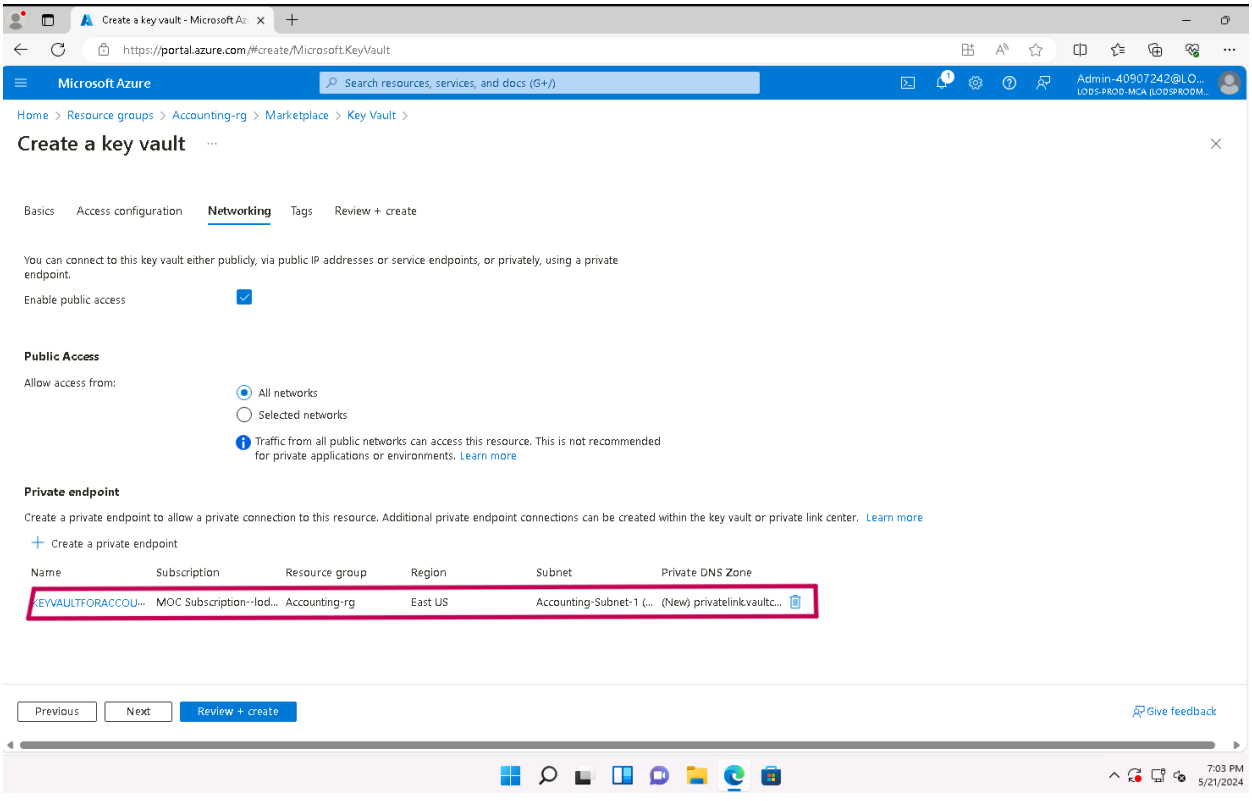

Accounting-rg - Microsoft Azure
Microsoft Azure
Search resources, services, and docs (G+/)
Home
Accounting-rg
Resource group
Create
Manage view
Delete resource group
Refresh
Export to CSV
Open query
Assign tags
Move
Delete
Export template
Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Events
Settings
Deployments
Security
Deployment stacks
Policies
Properties
Locks
Cost Management
Cost analysis
Cost alerts (preview)
Budgets
Advisor recommendations
Monitoring
Essentials
JSON View
Subscription (move) : MOC Subscription--lod49194920
Subscription ID : 715dfa13-0ebf-4000-adef-6a28c4de202b
Tags (edit) : LODManaged : lod
LabProfile : 139280
PoolOrgId : 363
ProfileOrgId : 3878
LabInstance : 40907242
Deployments : 1 Succeeded
Location : East US
Switch between a list view of your resources and a summary chart view of resource counts.
CLOSE
Resources
Recommendations
Filter for any field...
Type equals all
Location equals all
Add filter
Showing 1 to 1 of 1 records.
Show hidden types
No grouping
List view
Name
Type
Location
Market-KV-m3vuow4ilq3de
Key vault
East US
< Previous
Page 1 of 1
Next >
Give feedback
6:44 PM
5/21/2024

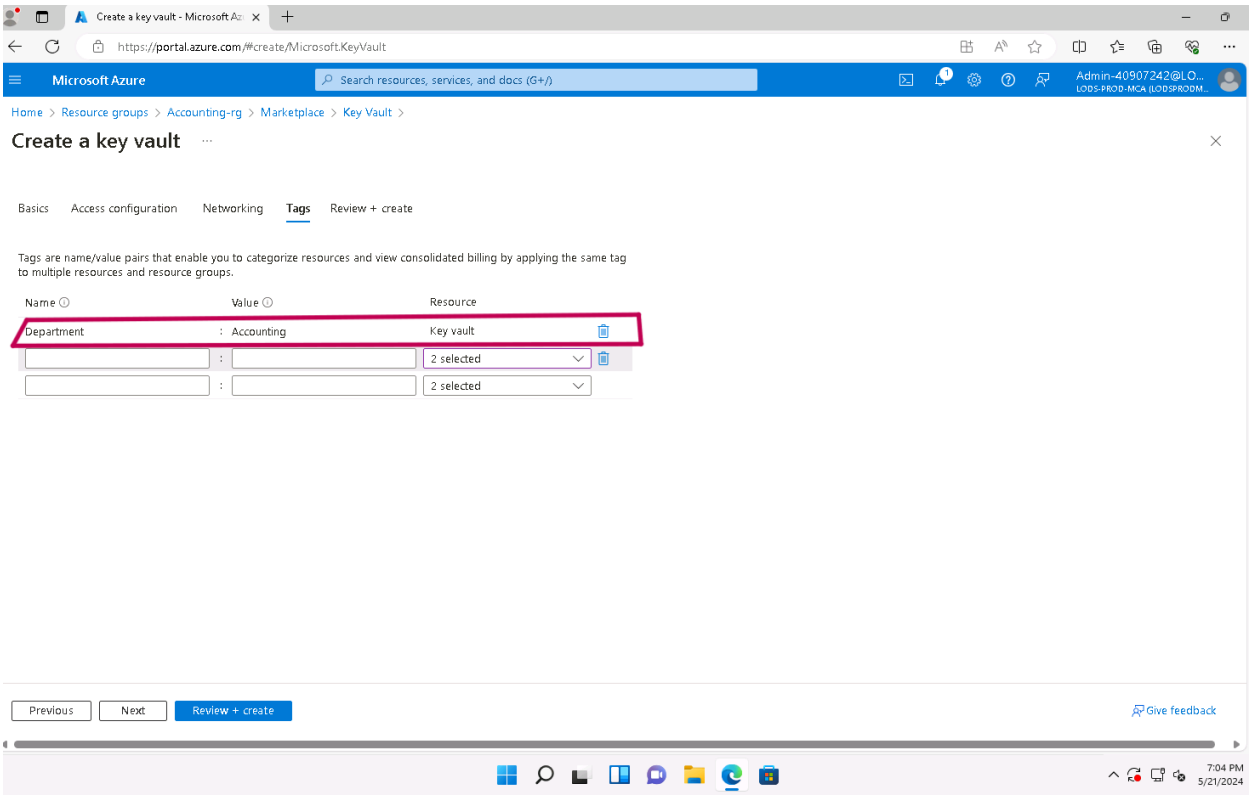

Marketplace - Microsoft Azure
Microsoft Azure
Search resources, services, and docs (G+/)
Home > Accounting-rg >
Marketplace
Get Started
Service Providers
Management
Private Marketplace
Private Offer Management
My Marketplace
Favorites
My solutions
Recently created
Private plans
Categories
Security (43)
Databases (24)
DevOps (19)
Identity (19)
AI + Machine Learning (11)
Analytics (10)
New! Get AI-generated suggestions for your search.
Ask AI to suggest products, articles, and solutions for what you need.
View suggestions
key vault
Azure services only
Pricing : All
Operating System : All
Publisher Type : All
Product Type : All
Publisher name : All
Showing 1 to 20 of 111 results for 'key vault'. Clear search
Tile view
Key Vault
Microsoft
Azure Service
Safeguard cryptographic keys and other secrets used by cloud apps and services.
Create
Azure Key Vault Managed HSM
Microsoft
Azure Service
Safeguard cryptographic keys used by cloud apps and services.
Create
EJBCA SaaS - With Key Vault Backed CA Keys
Keyfactor, Inc.
SaaS
EJBCA SaaS, PKI delivered as a service with Azure Key Vault key storage
Starts at
Free
Subscribe
Azure Key Vault solution for Sentinel
Microsoft Sentinel, Microsoft Co...
Azure Application
Azure Key Vault solution for Sentinel
Price varies
Create
HashiCorp Vault Enterprise
HashiCorp
SaaS
Manage Secrets and Protect Sensitive Data
Starts at
$15.840.00/1 year
Subscribe
Is Marketplace helpful?
6:44 PM
5/21/2024

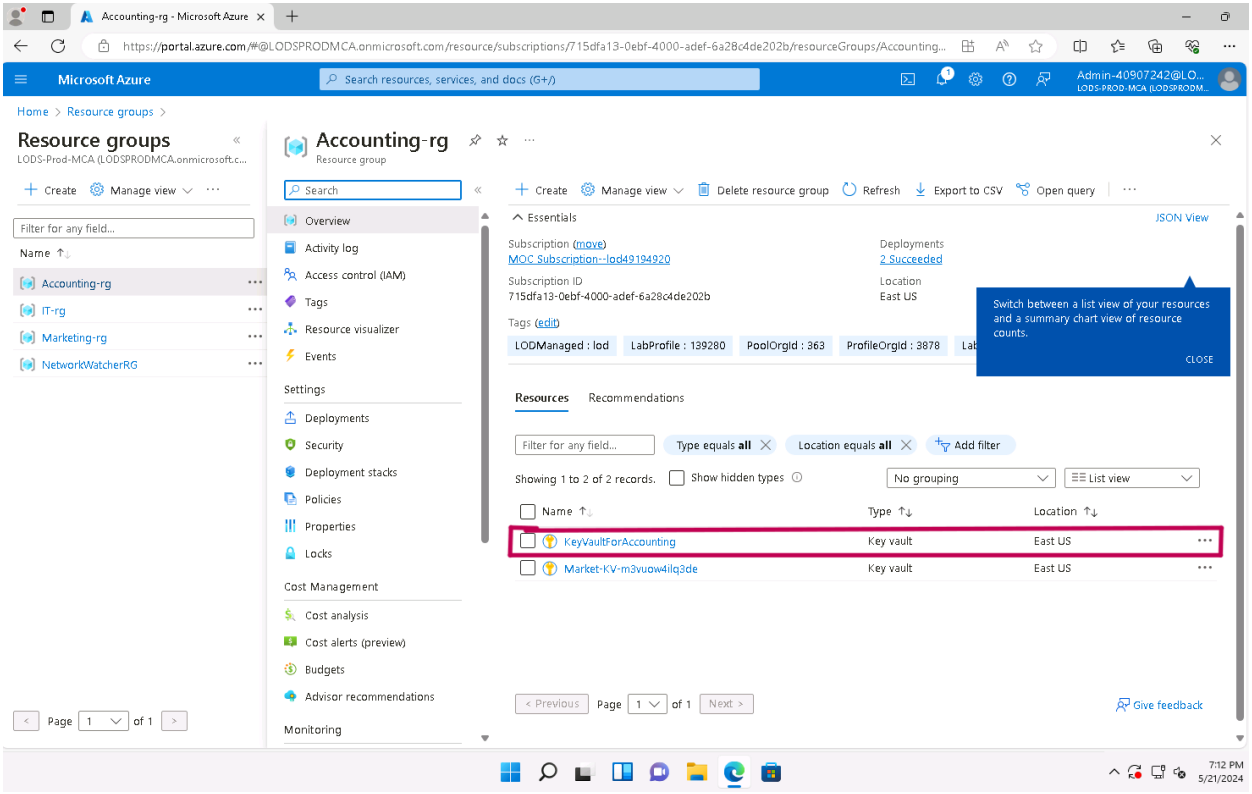

Create a key vault - Microsoft Az
https://portal.azure.com/#create/Microsoft.KeyVault
Microsoft Azure
Search resources, services, and docs (G+/)
Admin-40907242@LO...
LODS-PROD-MCA (LODSPRODM...
Home > Accounting-rg > Marketplace >
Create a key vault
Basics
Access configuration
Networking
Tags
Review + create
Azure Key Vault is a cloud service used to manage keys, secrets, and certificates. Key Vault eliminates the need for developers to store security information in their code. It allows you to centralize the storage of your application secrets which greatly reduces the chances that secrets may be leaked. Key Vault also allows you to securely store secrets and keys backed by Hardware Security Modules or HSMs. The HSMs used are Federal Information Processing Standards (FIPS) 140-2 Level 2 validated. In addition, key vault provides logs of all access and usage attempts of your secrets so you have a complete audit trail for compliance.
Project details
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.
Subscription *
MOC Subscription--lod49194920
Resource group *
Accounting-rg
Create new
Instance details
Key vault name *
KeyVaultForAccounting
Region *
East US
Pricing tier *
Standard
Recovery options
Previous
Next
Review + create
Give feedback
6:45 PM
5/21/2024


Create a key vault - Microsoft Az
https://portal.azure.com/#create/Microsoft.KeyVault
Microsoft Azure
Search resources, services, and docs (G+/)
Admin-40907242@LO...
LODS-PROD-MCA (LODSPRODM...
Home > Accounting-rg > Marketplace >
Create a key vault
Basics
Access configuration
Networking
Tags
Review + create
Configure data plane access for this key vault
To access a key vault in data plane, all callers (users or applications) must have proper authentication and authorization. Authentication establishes the identity of the caller. Authorization determines which operations the caller can execute.
Learn more
Permission model
Grant data plane access by using a Azure RBAC or Key Vault access policy
Azure role-based access control (recommended)
Vault access policy
Resource access
Azure Virtual Machines for deployment
Azure Resource Manager for template deployment
Azure Disk Encryption for volume encryption
Access policies
Access policies enable you to have fine grained control over access to vault items. Learn more
Create
Edit
Delete
Name
Email
Key Permissions
Secret Permissions
Certificate Permissions
Previous
Next
Review + create
Give feedback

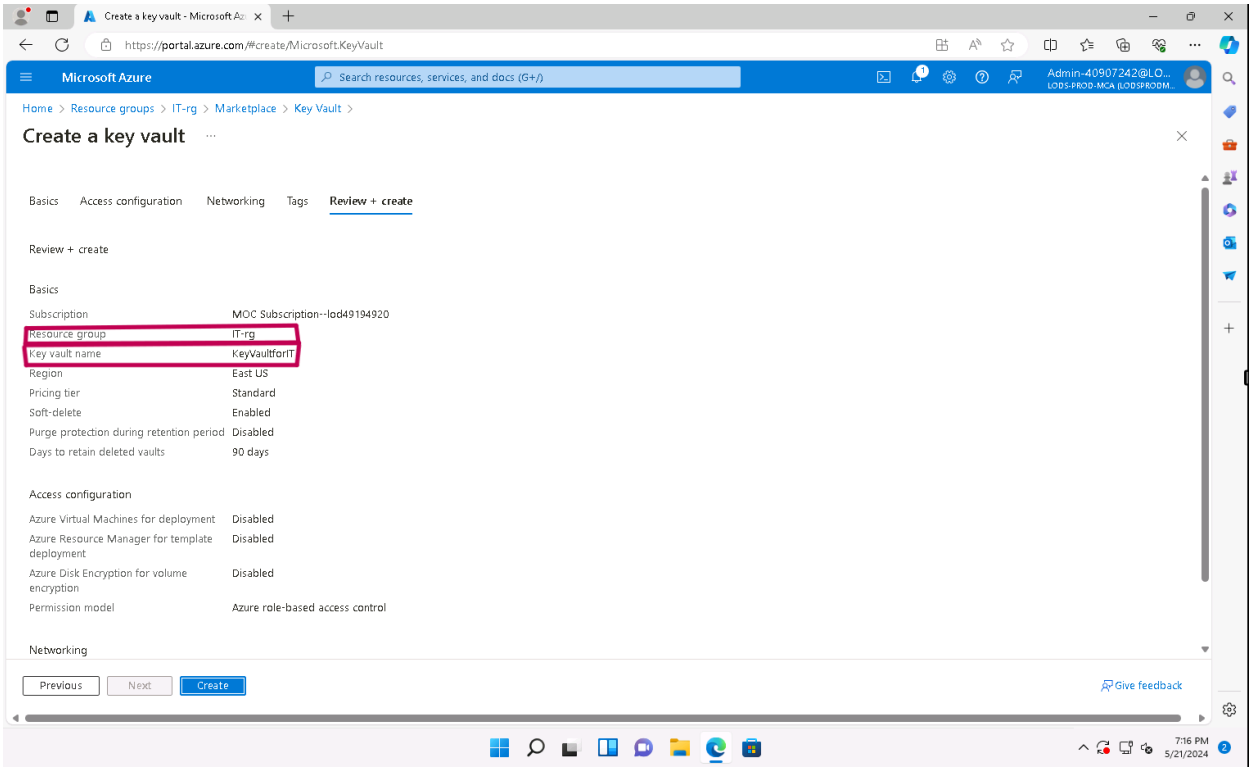

Microsoft Azure
Search resources, services, and docs (G+/)
Admin-40907242@LO...
LODS-PROD-MCA (LODSPRODM...
Home > Accounting-rg > Marketplace >
Create a key vault
Basics
Access configuration
Networking
Tags
Review + create
Configure data plane access for this key vault
To access a key vault in data plane, all callers (users or applications) must have proper authentication
Learn more
Permission model
Grant data plane access by using a Azure RBAC or Key Vault access policy
Azure role-based access control (recommended)
Vault access policy
Resource access
Azure Virtual Machines for deployment
Azure Resource Manager for template deployment
Azure Disk Encryption for volume encryption
Access policies
Access policies enable you to have fine grained control over access to vault items. Learn more
Create
Edit
Delete
Name
Email
Previous
Next
Review + create
Create an access policy
Permissions
Principal
Application (optional)
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
Decrypt
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
List Certificate Authorities
Previous
Next
6:46 PM
5/21/2024

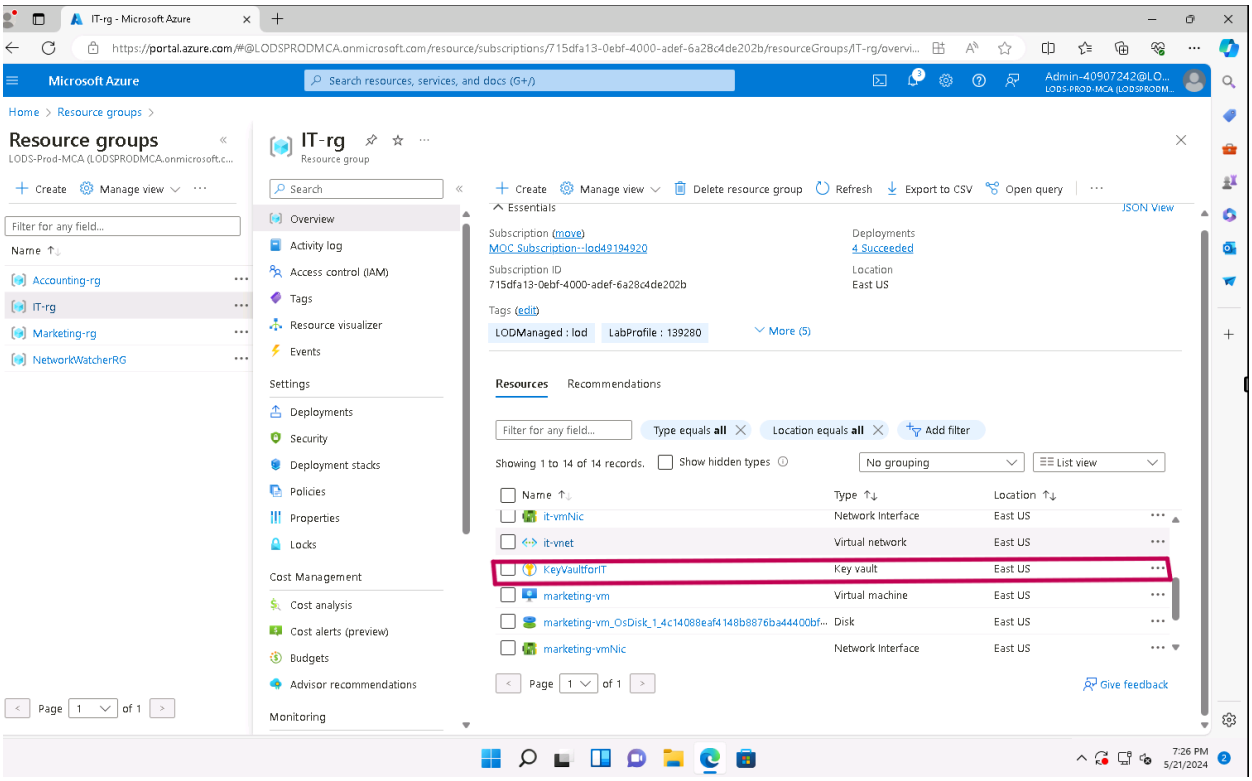

Create a key vault - Microsoft Az
https://portal.azure.com/#create/Microsoft.KeyVault
Microsoft Azure
Search resources, services, and docs (G+/)
Admin-40907242@LO...
LODS-PROD-MCA (LODSPRODM...
Home > Resource groups > Accounting-rg > Marketplace > Key Vault >
Create a key vault
Basics
Access configuration
Networking
Tags
Review + create
You can connect to this key vault either publicly, via public IP addresses or service endpoints, or privately, using a private endpoint.
Enable public access
Public Access
Allow access from:
All networks
Selected networks
Traffic from all public networks can access this resource. This is not recommended for private applications or environments. Learn more
Private endpoint
Create a private endpoint to allow a private connection to this resource. Additional private endpoint connections can be created within the key vault or private link center. Learn more
Create a private endpoint
Name
Subscription
Resource group
Region
Subnet
Private DNS Zone
KEYVAULTFORACCOU...
MOC Subscription--lod...
Accounting-rg
East US
Accounting-Subnet-1 (...
(New) privatelink.vaultc...
Previous
Next
Review + create
Give feedback
7:03 PM
5/21/2024


Create a key vault - Microsoft Az
https://portal.azure.com/#create/Microsoft.KeyVault
Microsoft Azure
Search resources, services, and docs (G+/)
Admin-40907242@LO...
LODS-PROD-MCA (LODSPRODM...
Home > Resource groups > Accounting-rg > Marketplace > Key Vault >
Create a key vault
Basics
Access configuration
Networking
Tags
Review + create
Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups.
Name
Value
Resource
Department : Accounting Key vault
2 selected
2 selected
Previous
Next
Review + create
Give feedback
7:04 PM
5/21/2024

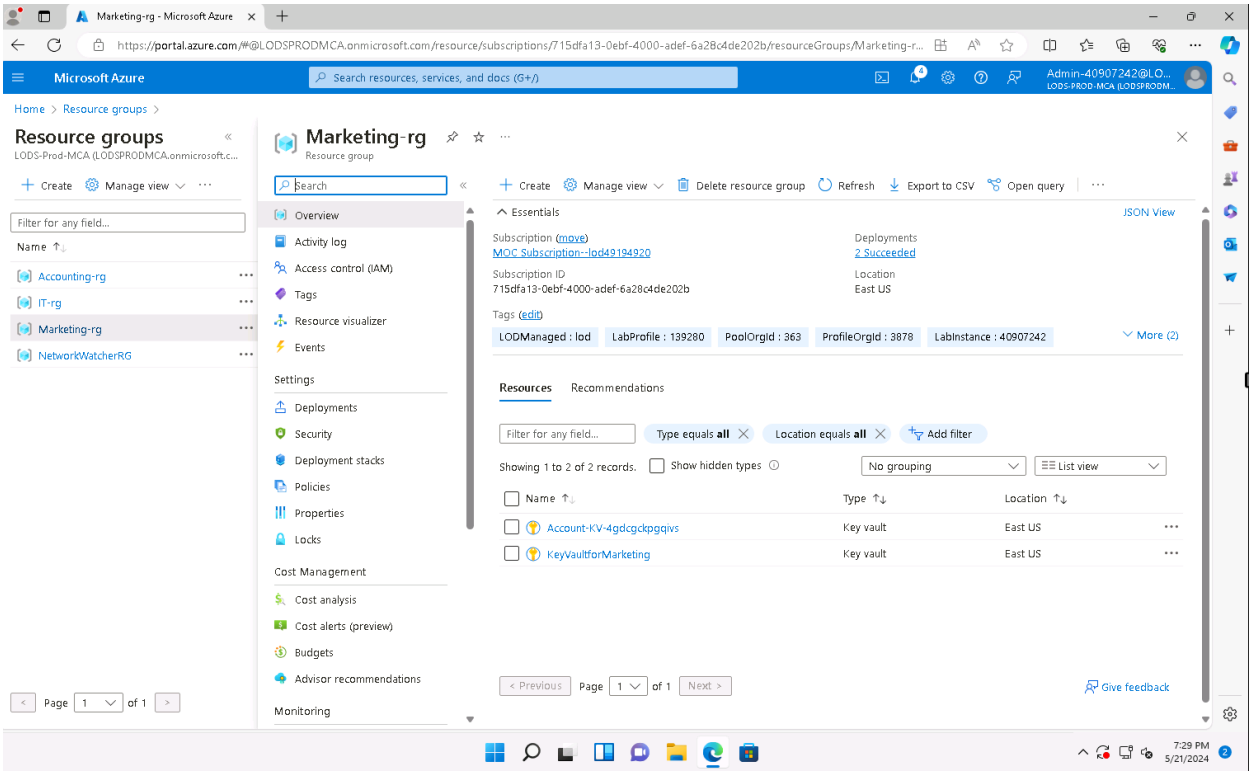

Accounting-rg - Microsoft Azure
https://portal.azure.com/#@LODSPRODMCA.onmicrosoft.com/resource/subscriptions/715dfa13-0ebf-4000-adef-6a28c4de202b/resourceGroups/Accounting...
Microsoft Azure
Search resources, services, and docs (G+/)
Admin-40907242@LO...
LODS-PROD-MCA (LODSPRODM...
Home > Resource groups >
Resource groups
LODS-Prod-MCA (LODSPRODMCA.onmicrosoft.c...
Create
Manage view
Filter for any field...
Name
Accounting-rg
IT-rg
Marketing-rg
NetworkWatcherRG
Page 1 of 1
Accounting-rg
Resource group
Search
Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Events
Settings
Deployments
Security
Deployment stacks
Policies
Properties
Locks
Cost Management
Cost analysis
Cost alerts (preview)
Budgets
Advisor recommendations
Monitoring
Create
Manage view
Delete resource group
Refresh
Export to CSV
Open query
Essentials
JSON View
Subscription (move)
MOC Subscription--lod49194920
Subscription ID
715dfa13-0ebf-4000-adef-6a28c4de202b
Deployments
2 Succeeded
Location
East US
Tags (edit)
LODManaged : lod
LabProfile : 139280
PoolOrgId : 363
ProfileOrgId : 3878
Switch between a list view of your resources and a summary chart view of resource counts.
CLOSE
Resources
Recommendations
Filter for any field...
Type equals all
Location equals all
Add filter
Showing 1 to 2 of 2 records.
Show hidden types
No grouping
List view
Name
Type
Location
KeyVaultForAccounting
Key vault
East US
Market-KV-m3vuow4ilq3de
Key vault
East US
< Previous
Page 1 of 1
Next >
Give feedback
7:12 PM
5/21/2024

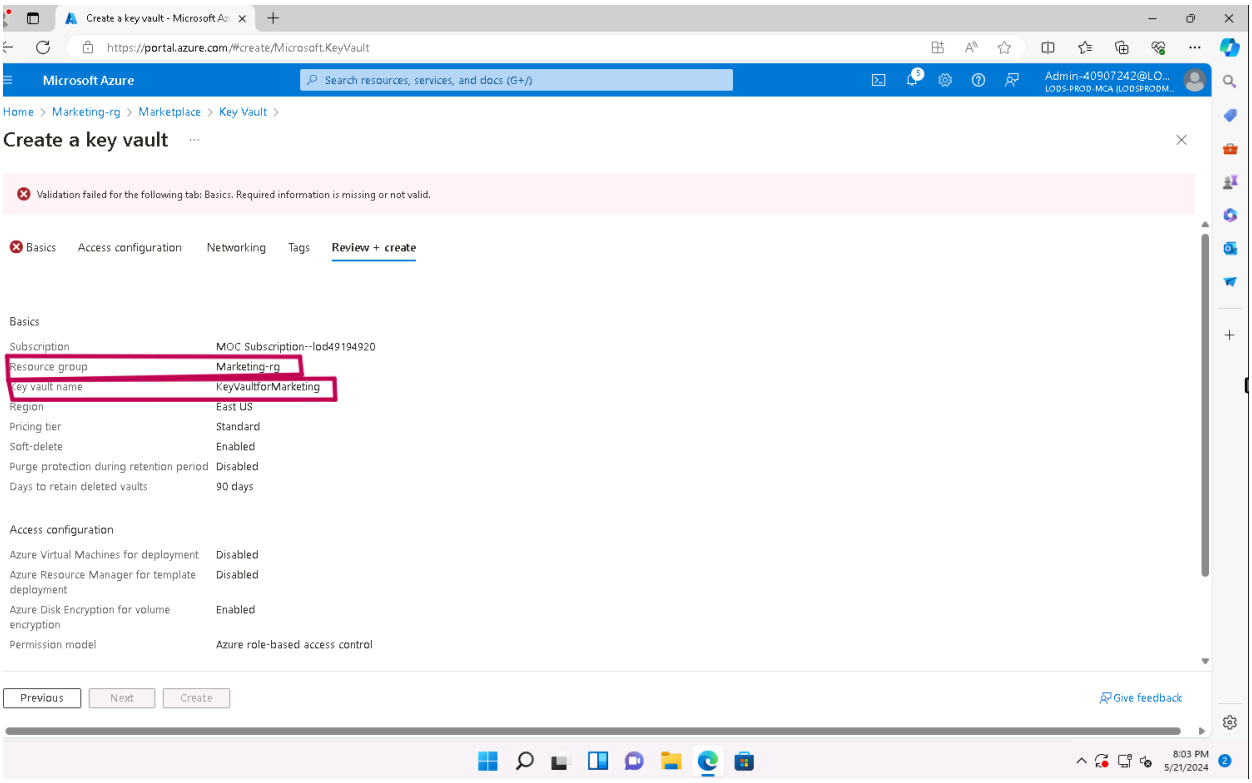
IT Department:





Marketing Department:

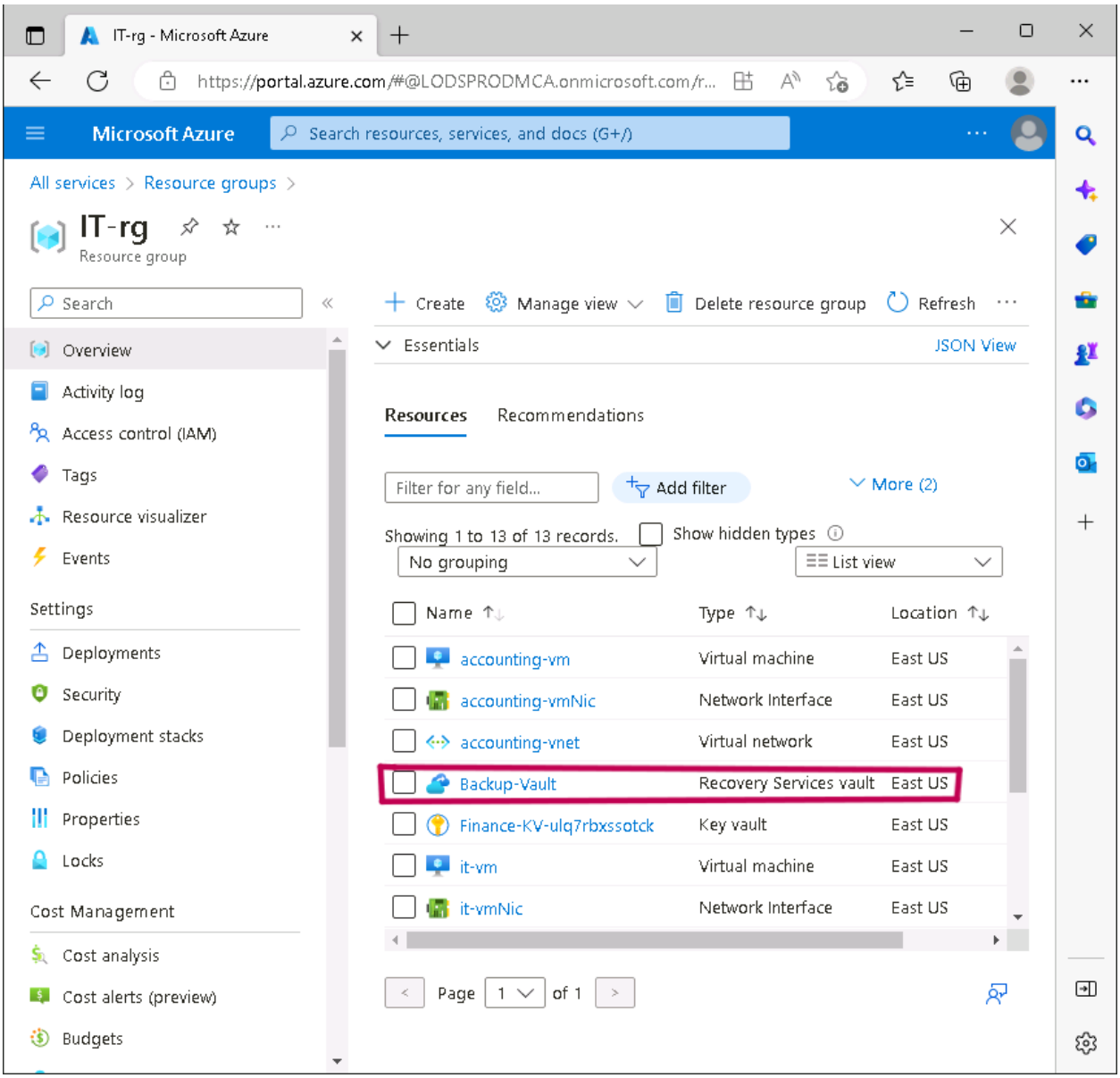


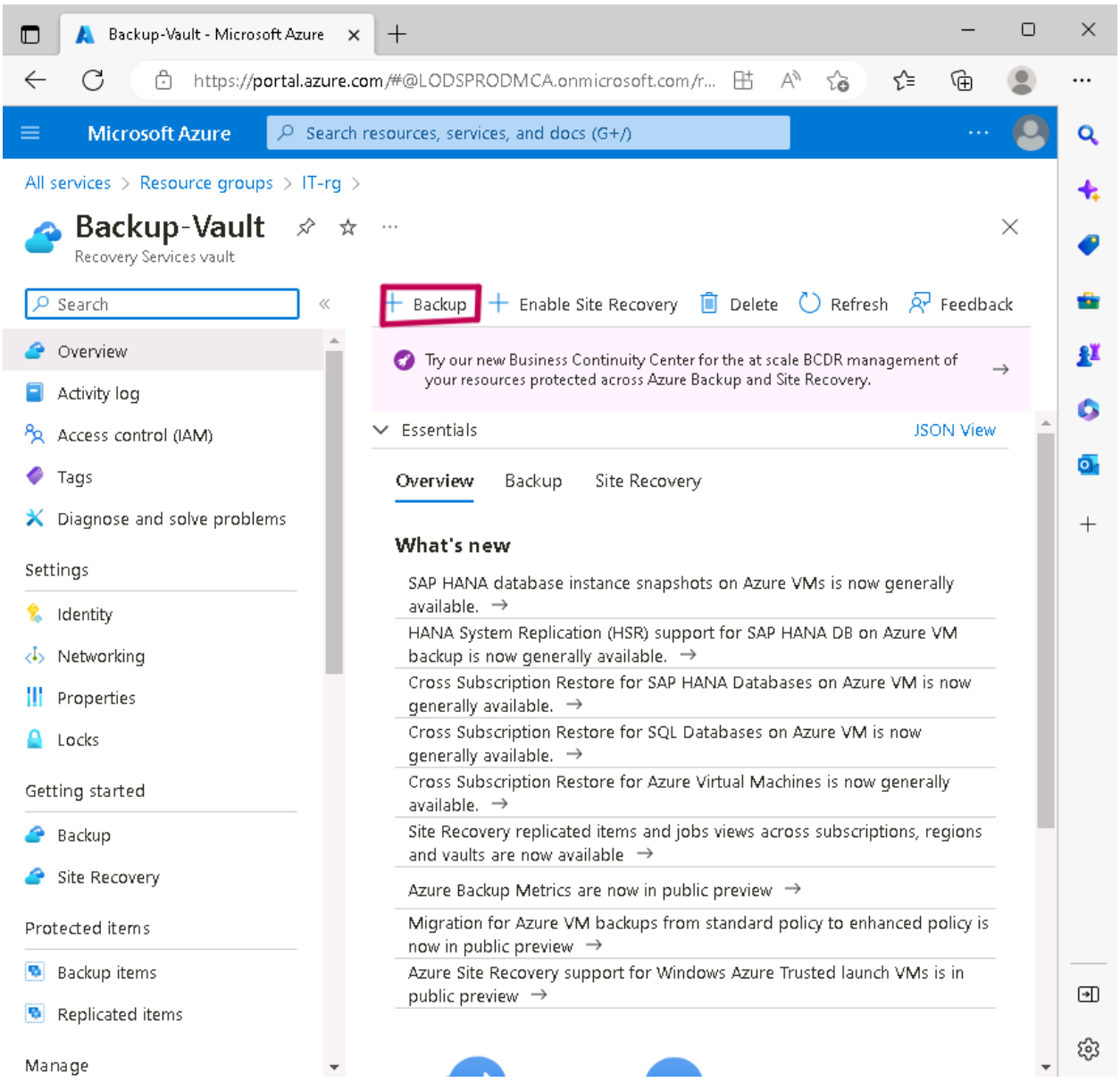


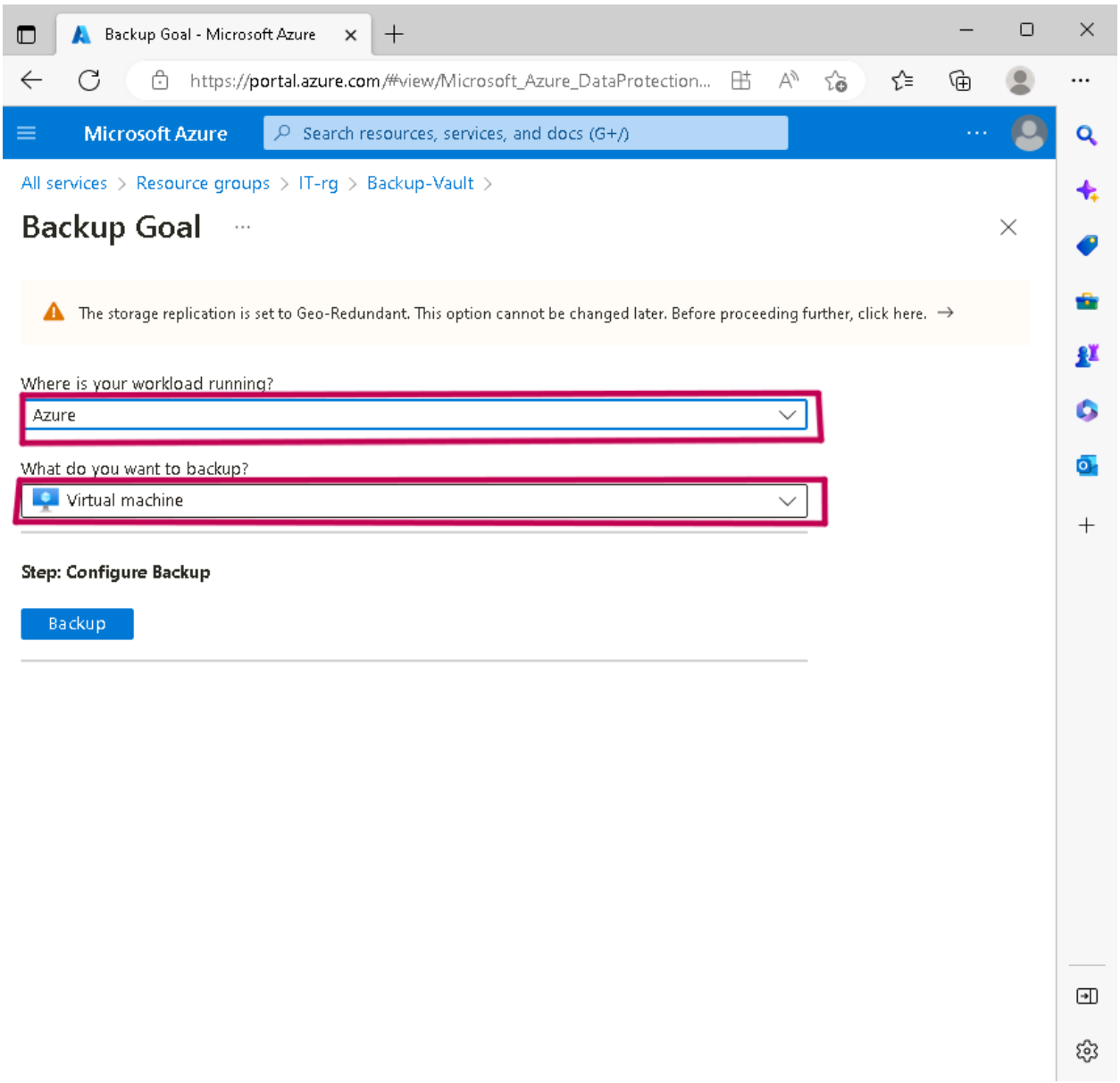
E. Backups

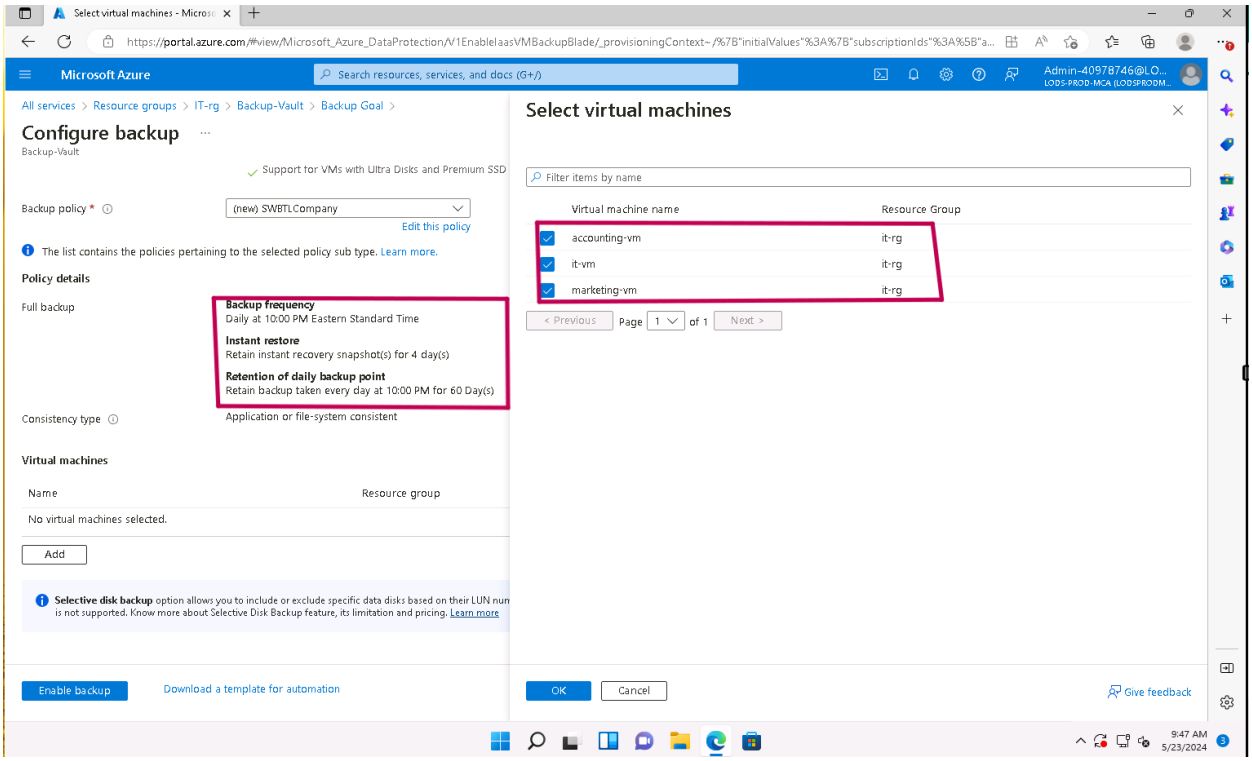
Configuration of File Backup Settings:

- The creation of a new backup policy includes the following:
    - Policy Name: SWBTLCompany
    - Recovery Point Objective (RPO): 1 day
    - Time Conducted: 10 P.M Eastern Time (ET)
    - Retention:
        - Instant Recovery Snapshots: 4 days
        - Daily Backup Points: 60 days


IT-rg - Microsoft Azure
https://portal.azure.com/#@LODSPRODMCA.onmicrosoft.com/r...
Microsoft Azure
Search resources, services, and docs (G+/)
All services > Resource groups >
IT-rg
Resource group
Search
Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Events
Settings
Deployments
Security
Deployment stacks
Policies
Properties
Locks
Cost Management
Cost analysis
Cost alerts (preview)
Budgets
Create
Manage view
Delete resource group
Refresh
Essentials
JSON View
Resources
Recommendations
Filter for any field...
Add filter
More (2)
Showing 1 to 13 of 13 records.
Show hidden types
No grouping
List view
Name
Type
Location
accounting-vm
Virtual machine
East US
accounting-vmNic
Network Interface
East US
accounting-vnet
Virtual network
East US
Backup-Vault
Recovery Services vault
East US
Finance-KV-ulq7rbxssotck
Key vault
East US
it-vm
Virtual machine
East US
it-vmNic
Network Interface
East US
Page
1
of 1


Backup-Vault - Microsoft Azure
https://portal.azure.com/#@LODSPRODMCA.onmicrosoft.com/r...
Microsoft Azure
Search resources, services, and docs (G+/)
All services > Resource groups > IT-rg >
Backup-Vault
Recovery Services vault
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Identity
Networking
Properties
Locks
Getting started
Backup
Site Recovery
Protected items
Backup items
Replicated items
Manage
Backup
Enable Site Recovery
Delete
Refresh
Feedback
Try our new Business Continuity Center for the at scale BCDR management of your resources protected across Azure Backup and Site Recovery.
Essentials
JSON View
Overview
Backup
Site Recovery
What's new
SAP HANA database instance snapshots on Azure VMs is now generally available.
HANA System Replication (HSR) support for SAP HANA DB on Azure VM backup is now generally available.
Cross Subscription Restore for SAP HANA Databases on Azure VM is now generally available.
Cross Subscription Restore for SQL Databases on Azure VM is now generally available.
Cross Subscription Restore for Azure Virtual Machines is now generally available.
Site Recovery replicated items and jobs views across subscriptions, regions and vaults are now available
Azure Backup Metrics are now in public preview
Migration for Azure VM backups from standard policy to enhanced policy is now in public preview
Azure Site Recovery support for Windows Azure Trusted launch VMs is in public preview


Backup Goal - Microsoft Azure
https://portal.azure.com/#view/Microsoft_Azure_DataProtection...
Microsoft Azure
Search resources, services, and docs (G+/)
All services > Resource groups > IT-rg > Backup-Vault >
Backup Goal
The storage replication is set to Geo-Redundant. This option cannot be changed later. Before proceeding further, click here. →
Where is your workload running?
Azure
What do you want to backup?
Virtual machine
Step: Configure Backup
Backup



The configuration outlined above are consistent with the company's business needs, as specified in the requirements documentation:

- The IT department is tasked with executing and verifying backups
- Each cloud server have a RPO of 1 day
- Backups conducted daily at 10 P.M ET
- Instant Recovery Snapshots for 4 days
- Daily backup points for 60 days
- Backup policy name is "SWBTLCompany"

F. Security Responsibilities

A significant advantage of selecting the Microsoft Azure Government IaaS cloud solution is its FedRAMP authorization. The FedRAMP document, known as the Control Implentation Summary (CIS) and Customer Responsibility Matrix (CRM), outlines the security responsibilities of Cloud Service Provider (CSP), which in this case is Azure, and the customer, SWBTL LLC. With an IaaS cloud solution, SWBTL LLC assumes greater responsibility for security controls compared to Platform as a Service (PaaS) and Software as a Service (SaaS) Solutions.

Here are three potential risks SWBTL LLC might face with an IaaS service model:

- One risk is the misconception that all security controls are fully managed by the CSP, Microsoft. This misunderstanding can result in security gaps and noncompliance issues, potentially causing significant impact on the company if it solely relies on the CSP for security.
- A second risk involves the company being unaware of its responsibilities regarding security controls. This lack of understanding can result in security gaps and noncompliance issues, which may significantly impact the company. Even minor issues can escalate into major problems over time.
- A third risk is the assumption that implementing these security controls will be straightforward and can be handled by any employee. This misconception might lead to the realization that the company lacks staff with the necessary expertise, or it may result in assigning the task to

underqualified personnel. This could lead to improperly implemented security controls. The impact of this risk can vary from low to high, depending on the approach the company takes.

Here are three suggestions to guarantee adherence to the company's cloud security standards:

- Encrypting data both at rest and during transit is crucial, particularly for cardholder information. Since SWBTL LLC handles transactions, encrypting this data is necessary to maintain PCI DSS compliance (PCI Security Standards Council, 2018).
- Security audits and compliance checks: SWBTL LLC needs to conduct internal audits and compliance reviews to identify any weaknesses in their security measures. Alternatively, the company could hire a Third-Party Assessment Organization to perform these evaluations.
- Access control policy: SWBTL LLC should adopt Role-Based Access Control (RBAC) in alignment with the principle of least privilege. This approach to access management will help ensure the company's compliance with FISMA and NIST standards.

G. Threats and Countermeasures

Here are three potential threats to the company's updated cloud solution, along with corresponding mitigation strategies:

- Unauthorized access to data: both insider and outsider threats can compromise data by violating the Need to Know (NTK) principle and the confidentiality component of the CIA triad. Such breaches can result in significant data leaks, damage the company's reputation, and incur financial penalties. To mitigate this threat, a combination of security tools and access control policies should be employed. Implementing a web application firewall (WAF) can restrict access to the cloud environment based on IP address, location, and other criteria. Additionally, configuring Role-Based Access Control (RBAC) according to the principle of the least privilege ensures users have only the necessary access to perform their job functions.
- Cloud Misconfigurations: The complexity of cloud environments means that lacking expert management can have severe consequences. Accidental misconfigurations can result in the previously mentioned threats. To mitigate this risk, conducting regular audits and compliance checks is essential to identify and rectify any security gaps.

F. Sources

FedRAMP. (n.d.). program Basics | FedRAMP.gov. www.fedramp.gov https.fedramp.gov/program-basics/

NIST. (2016, November 30). FISMA Background – NIST Risk Management Framework | CSRC | CSRC. CSRC | NIST. https://csrc.nist.gov/projects/risk-management/fisma-background

Microsoft. (2024, February 6). Regulatory Compliance details for NIST SP 800-53 Rev. 5 (Azure Government) – Azure policy. Learn.micorsoft.com. https://learn.microsoft.com/en-us/azure/goverance/plocy/samples/gov-nist-sp-800-53-r5

Microsoft. (2022, November 15). Introductions to Azure security. Learn.micorsoft.com. https://learn.mictosoft.com/en-uas/azure/security/fundamentals/overview