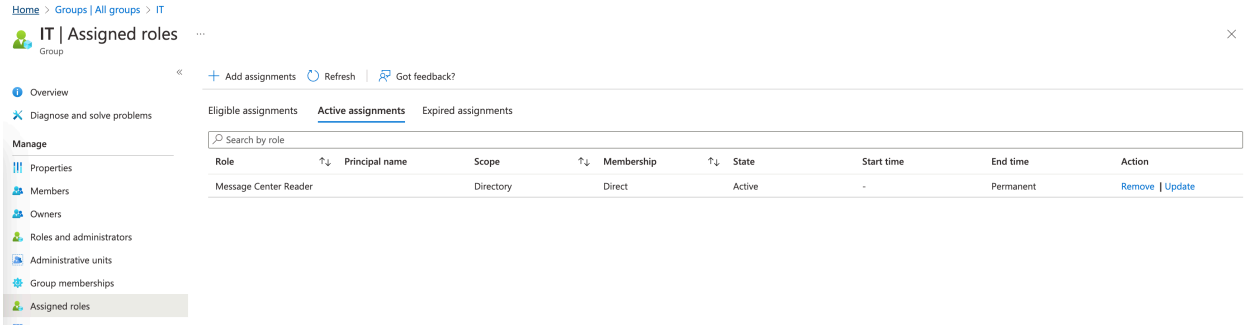
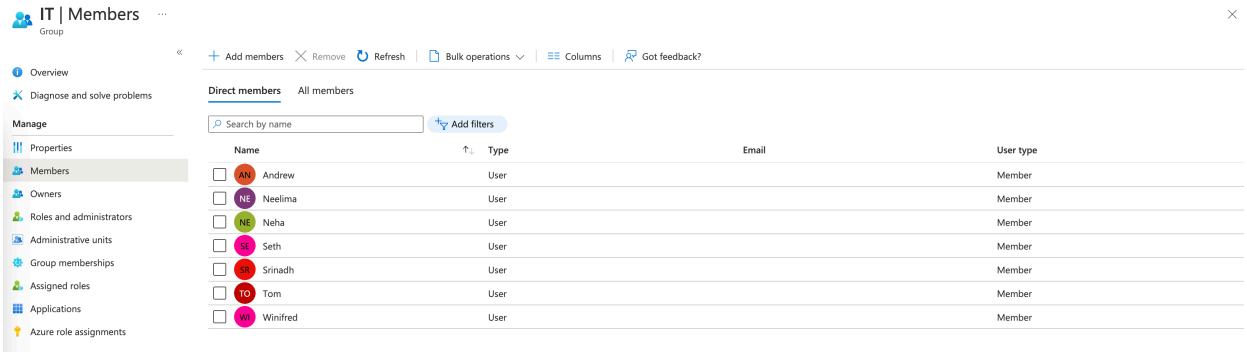
Attention students:

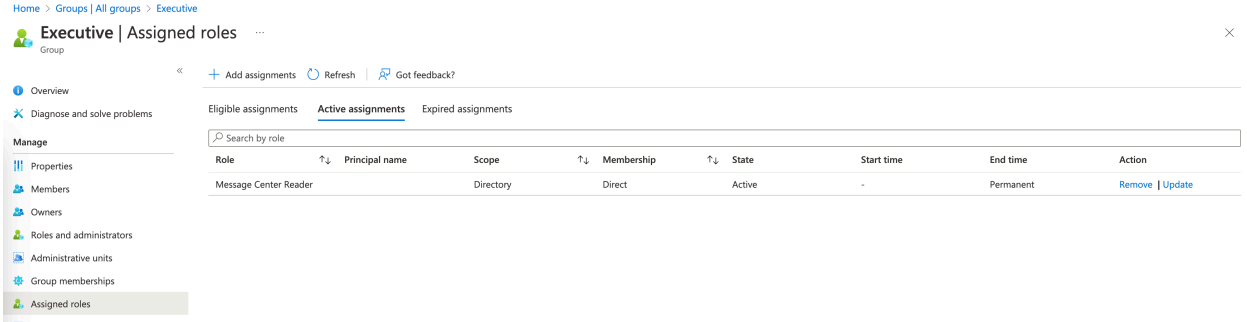
In order to demonstrate successful completion of all components in the project, please use screenshot(s) to show each completed action step as specified on the instructions page.

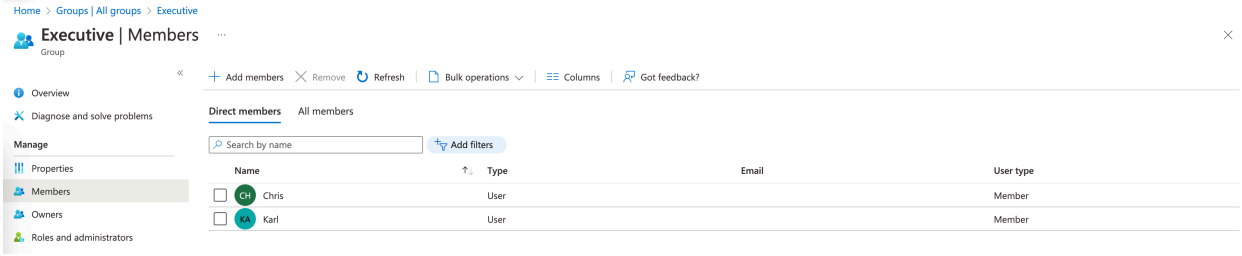
Identity and Access Management

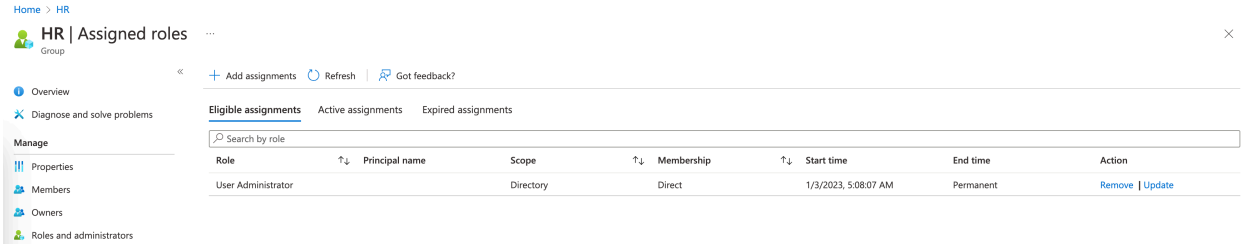
1. Proof of Assigned roles and AD assignments
    a. Andrew
    b. Chris
    c. Karl
    d. Lora
    e. Neelima
    f. Neha
    g. Seth
    h. Srinadh
    i. Tom
    j. Winifred

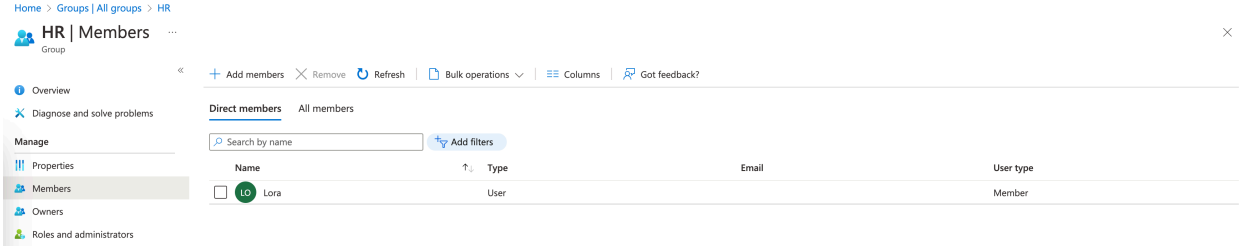


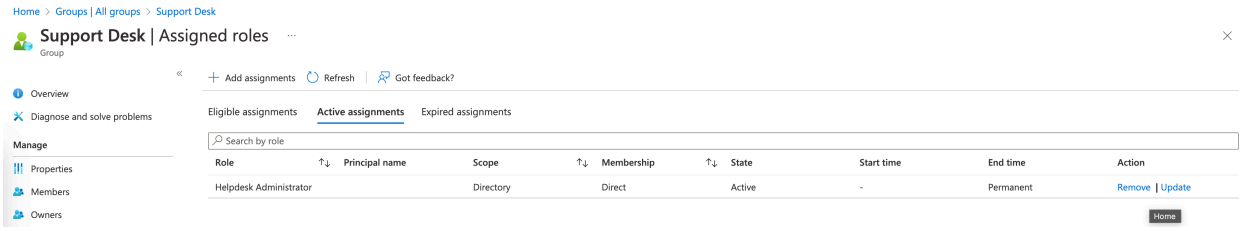


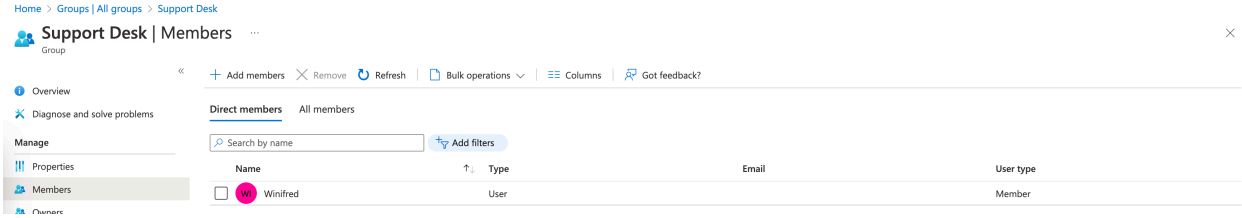



Home > Groups | All groups > Executive
Executive | Members
Group
Add members
Remove
Refresh
Bulk operations
Columns
Got feedback?
Overview
Diagnose and solve problems
Manage
Properties
Members
Owners
Roles and administrators
Direct members
All members
Search by name
Add filters
Name
Type
Email
User type
Chris
User
Member
Karl
User
Member

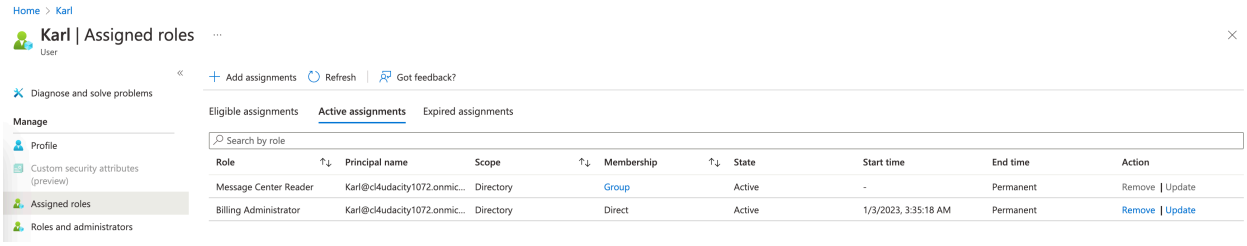

Home > HR
HR | Assigned roles
Group
Add assignments
Refresh
Got feedback?
Overview
Diagnose and solve problems
Manage
Properties
Members
Owners
Roles and administrators
Eligible assignments
Active assignments
Expired assignments
Search by role
Role
Principal name
Scope
Membership
Start time
End time
Action
User Administrator
Directory
Direct
1/3/2023, 5:08:07 AM
Permanent
Remove | Update


Home > Groups | All groups > HR
HR | Members
Group
Add members
Remove
Refresh
Bulk operations
Columns
Got feedback?
Overview
Diagnose and solve problems
Manage
Properties
Members
Owners
Roles and administrators
Direct members
All members
Search by name
Add filters
Name
Type
Email
User type
Lora
User
Member

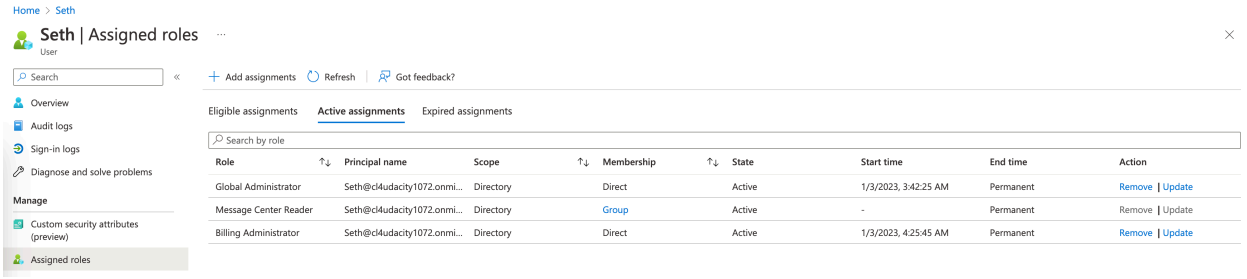

Home > Groups | All groups > Support Desk
Support Desk | Assigned roles
Group
Add assignments
Refresh
Got feedback?
Overview
Diagnose and solve problems
Manage
Properties
Members
Owners
Eligible assignments
Active assignments
Expired assignments
Search by role
Role
Principal name
Scope
Membership
State
Start time
End time
Action
Helpdesk Administrator
Directory
Direct
Active
-
Permanent
Remove | Update
Home


Home > Groups | All groups > Support Desk
Support Desk | Members
Group
Add members
Remove
Refresh
Bulk operations
Columns
Got feedback?
Overview
Diagnose and solve problems
Manage
Properties
Members
Direct members
All members
Search by name
Add filters
Name
Type
Email
User type
Winifred
User
Member

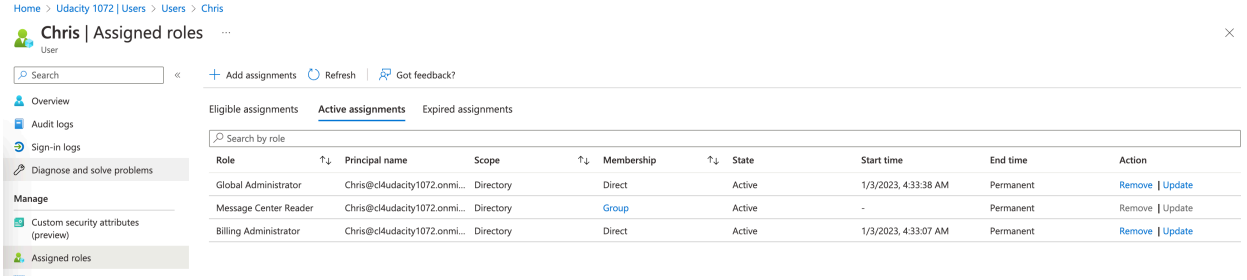
The COO will have the Billing Admin role active



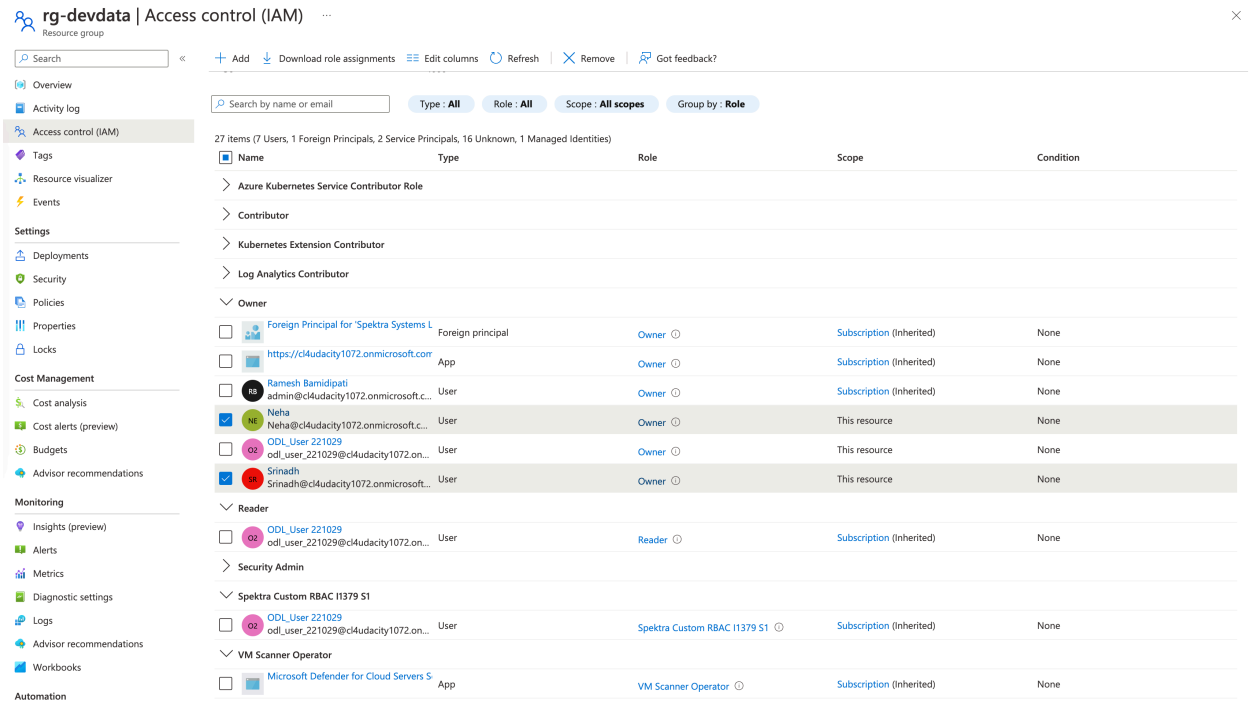
The Azure Architect will be eligible for the Global Admin and Billing admin roles



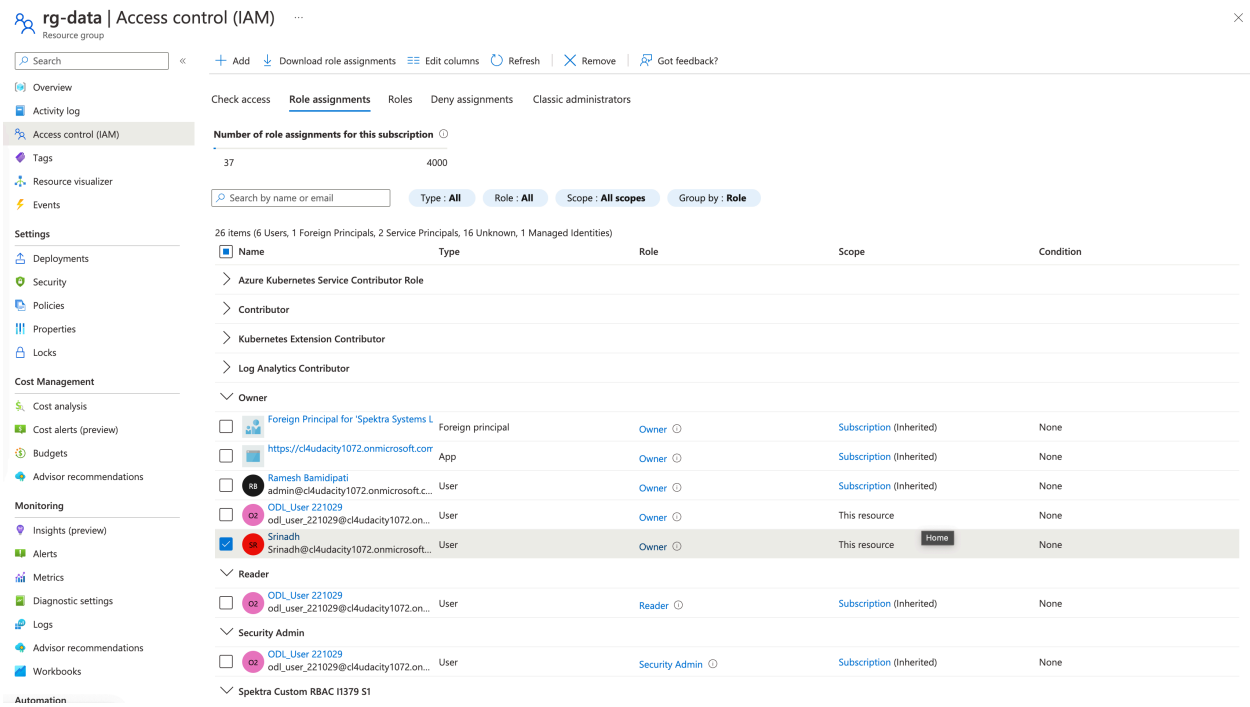
The CIO will not continually work in the environment however, they will need the same Azure AD access should the need arise to step in for the Azure Architect



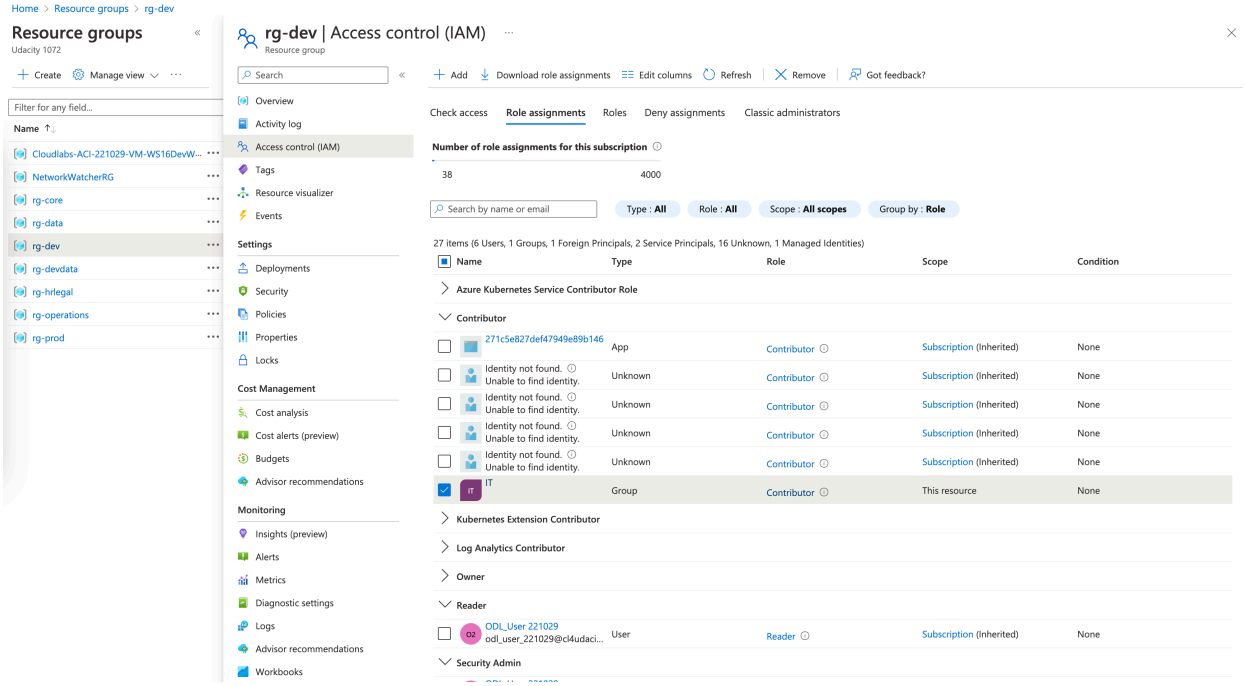
Development DBA will only need to access the Dev Database



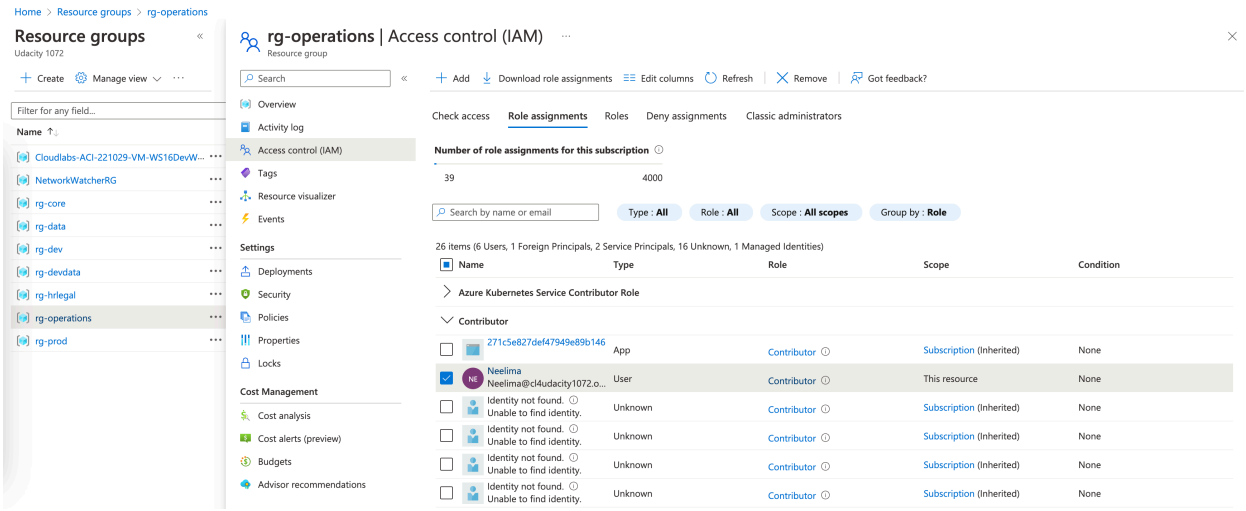
The lead DBA will need access to all SQL infrastructure and data

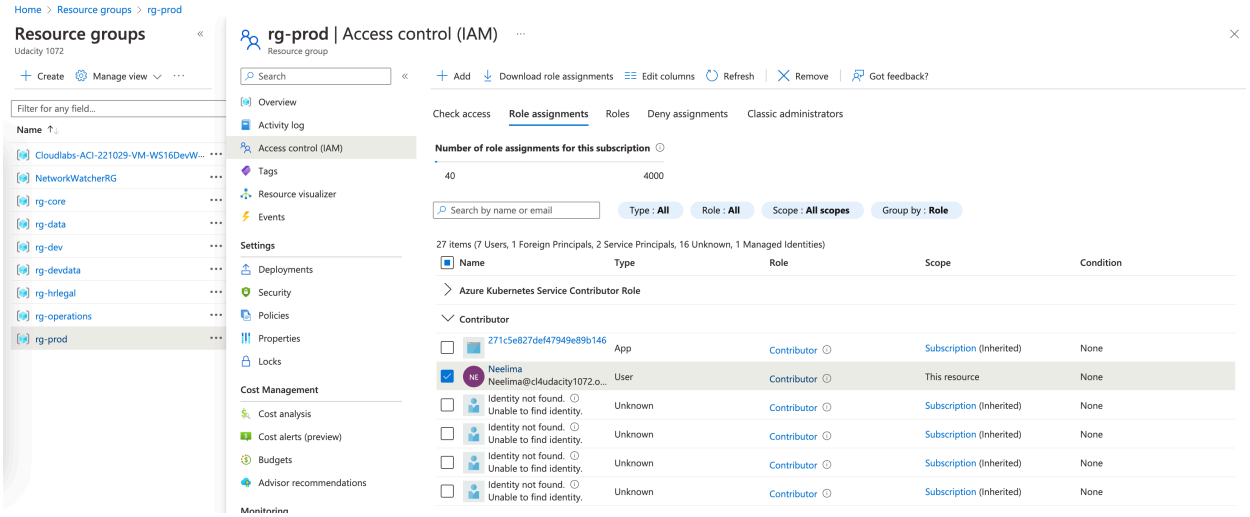


The IT Engineers will each need access to their assigned environments but will not need to provide this access to others

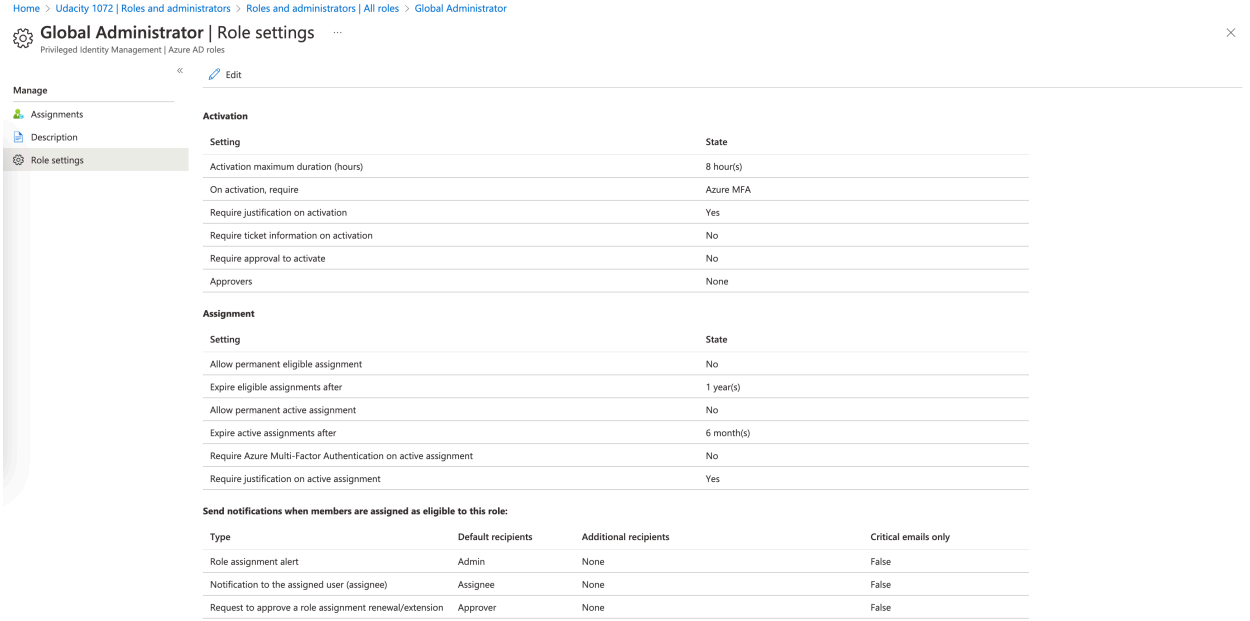


Development Lead will each need access to their assigned environments but will not need to provide this access to others

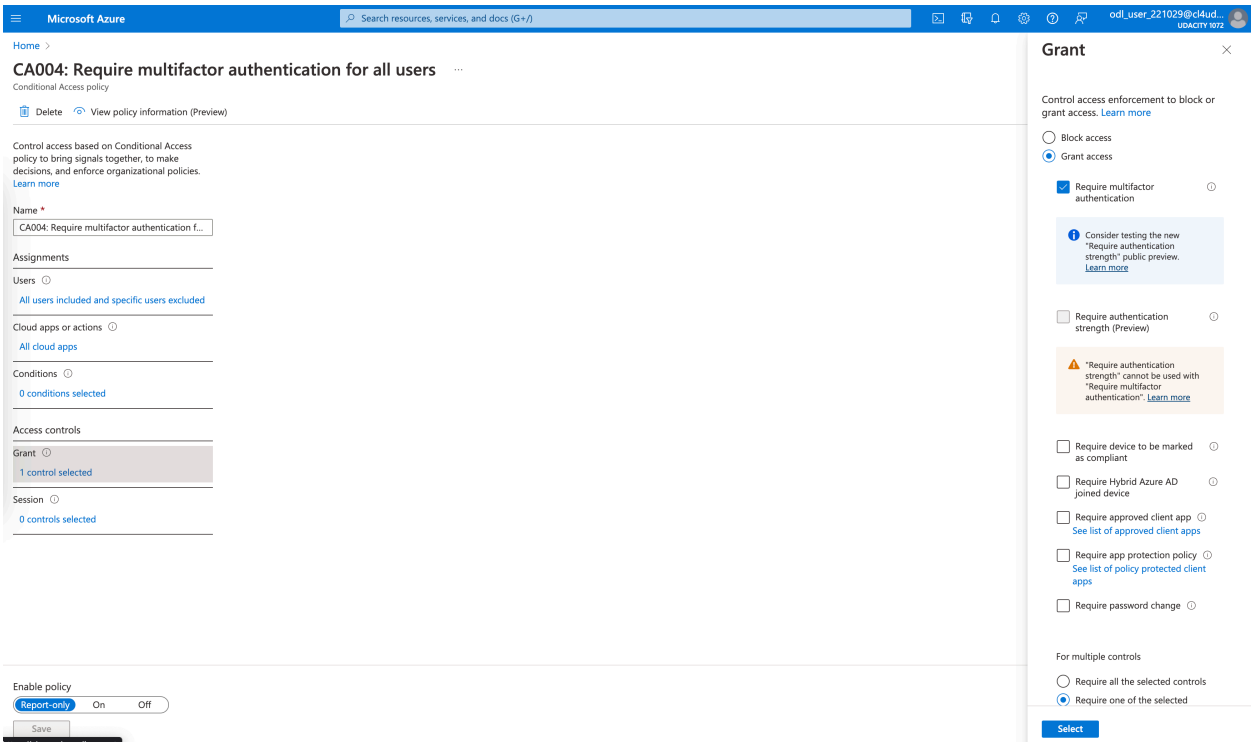




2. Proof of Global Administrator setting with duration, eligibility, expiration



3. Proof of Conditional Access policy all users



4. Proof of Multi-factor authentication(14 days, Charlotte office info)

Microsoft odl_user_221029@cl4udacity1072.onmicrosoft.com | ?

multi-factor authentication

users service settings

app passwords (learn more)

- ○ Allow users to create app passwords to sign in to non-browser apps
- ◉ Do not allow users to create app passwords to sign in to non-browser apps

trusted ips (learn more)

- ☑ Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

143.52.0.0/24

verification options (learn more)

Methods available to users:

- ☐ Call to phone
- ☑ Text message to phone
- ☑ Notification through mobile app
- ☑ Verification code from mobile app or hardware token

remember multi-factor authentication on trusted device (learn more)

- ☑ Allow users to remember multi-factor authentication on devices they trust (between one to 365 days)

Number of days users can trust devices for 14

NOTE: For the optimal user experience, we recommend using Conditional Access sign-in frequency to extend session lifetimes on trusted devices, locations, or low-risk sessions as an alternative to 'Remember MFA on a trusted device' settings. If using 'Remember MFA on a trusted device,' be sure to extend the duration to 90 or more days. Learn more about reauthentication prompts.

save

Manage advanced settings and view reports Go to the portal

Network Security

1. Bastion overview

Home > Bastions >

Create a Bastion ...

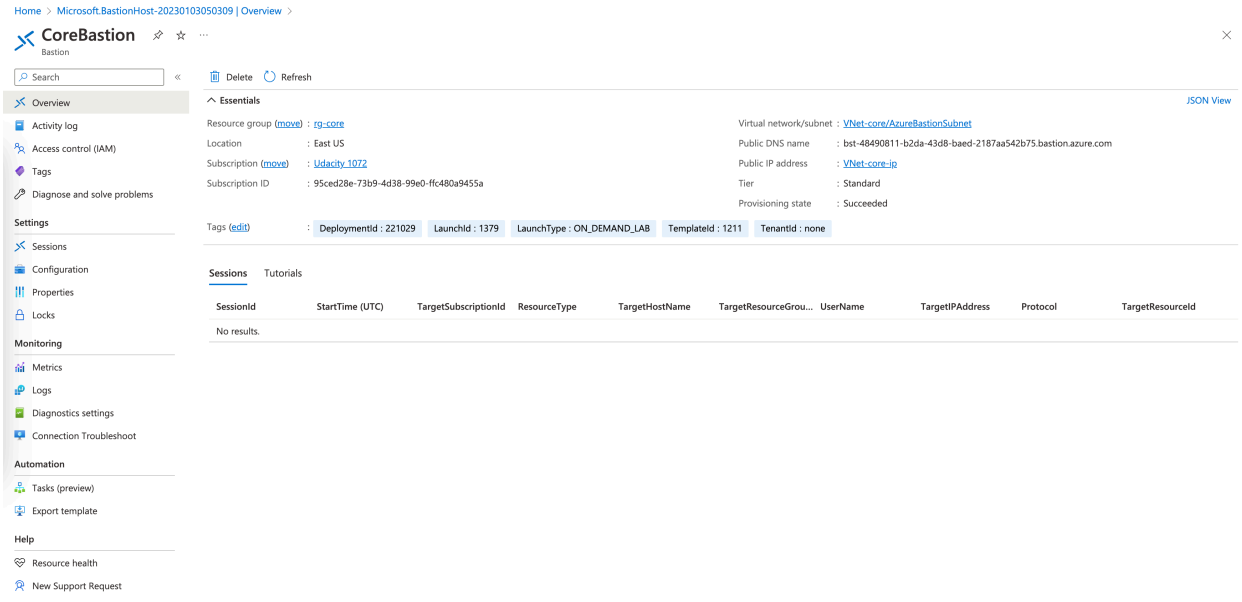
Validation passed

Basics Tags Advanced **Review + create**

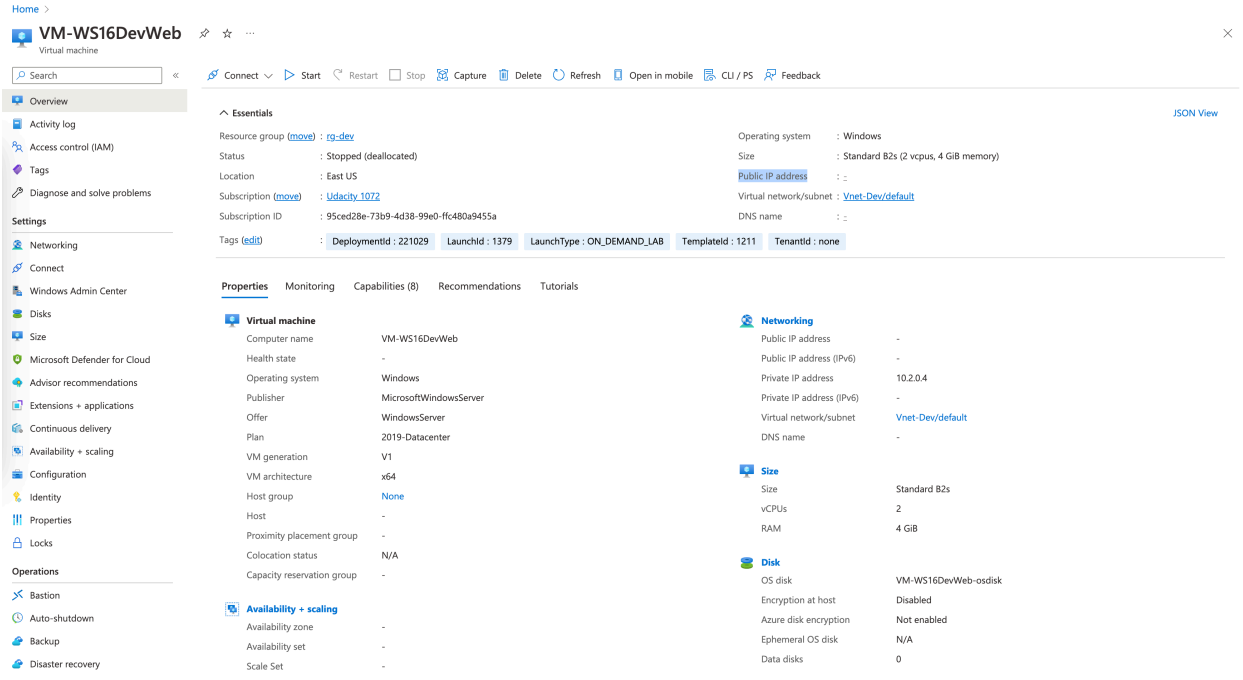
Summary

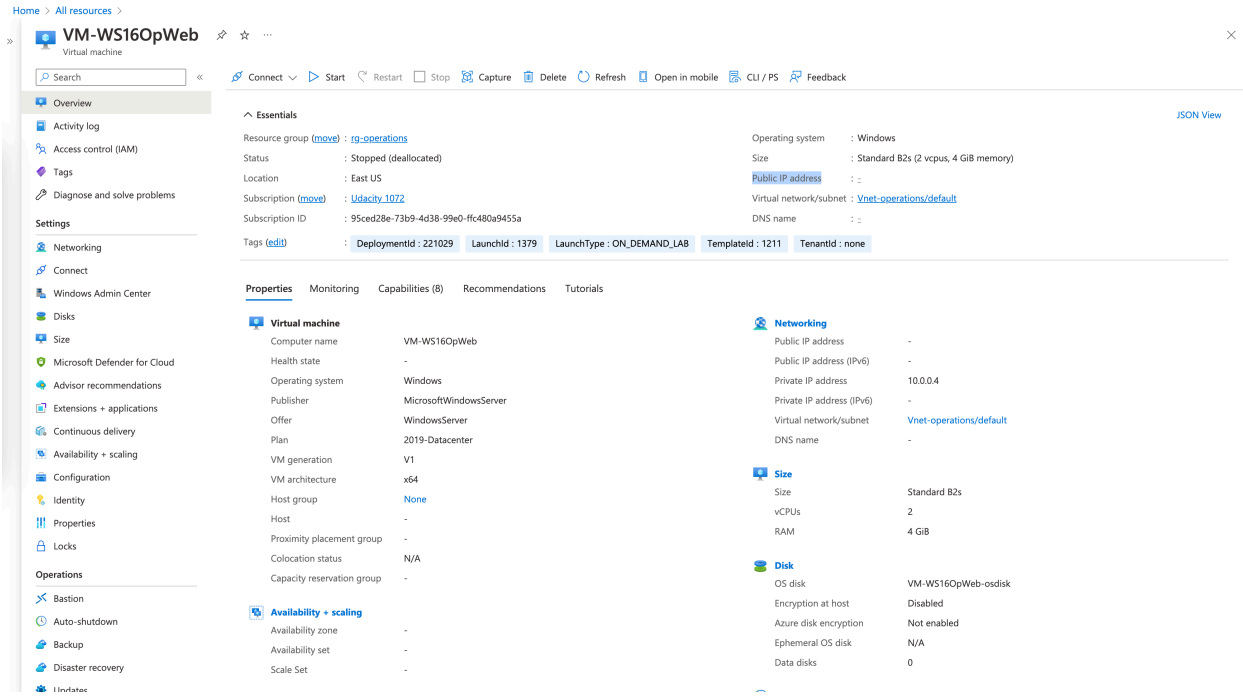
Basics

Name	CoreBastion
Subscription	Udacity 1072
Resource group	rg-core
Region	East US
Virtual network	VNet-core
Subnets	AzureBastionSubnet
Public IP address	VNet-core-ip
Tier	Standard
Instance count	2
Copy and paste	Enabled
IP-based connection	Disabled
Kerberos authentication (Preview)	Disabled
Shareable Link	Disabled
Native client support	Disabled



2. Proof of public IP addresses removed





VM-WS19HRL-Web

Virtual machine

Search

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Networking
- Connect
- Windows Admin Center
- Disks
- Size
- Microsoft Defender for Cloud
- Advisor recommendations
- Extensions + applications
- Continuous delivery
- Availability + scaling
- Configuration
- Identity
- Properties
- Locks

Operations

- Bastion
- Auto-shutdown
- Backup
- Disaster recovery
- Updates
- Inventory

Connect | Start | Restart | Stop | Capture | Delete | Refresh | Open in mobile | CLI / PS | Feedback

Essentials JSON View

Resource group (move)	: rg-hrlegal	Operating system	: Windows
Status	: Stopped (deallocated)	Size	: Standard B2s (2 vcpus, 4 GiB memory)
Location	: East US	Public IP address	: -
Subscription (move)	: Udacity 1072	Virtual network/subnet	: HRLegal/default
Subscription ID	: 95ced28e-73b9-4d38-99e0-ffc480a9455a	DNS name	: -

Tags (edit) : DeploymentId : 221029 | LaunchId : 1379 | LaunchType : ON_DEMAND_LAB | TemplateId : 1211 | TenantId : none

Properties | Monitoring | Capabilities (8) | Recommendations | Tutorials

Virtual machine

Computer name	VM-WS19HRL-Web
Health state	-
Operating system	Windows
Publisher	MicrosoftWindowsServer
Offer	WindowsServer
Plan	2019-Datacenter
VM generation	V1
VM architecture	x64
Host group	None
Host	-
Proximity placement group	-
Colocation status	N/A
Capacity reservation group	-

Availability + scaling

Availability zone	-
Availability set	-
Scale Set	-

Security type

Networking

Public IP address	-
Public IP address (IPv6)	-
Private IP address	10.0.0.4
Private IP address (IPv6)	-
Virtual network/subnet	HRLegal/default
DNS name	-

Size

Size	Standard B2s
vCPUs	2
RAM	4 GiB

Disk

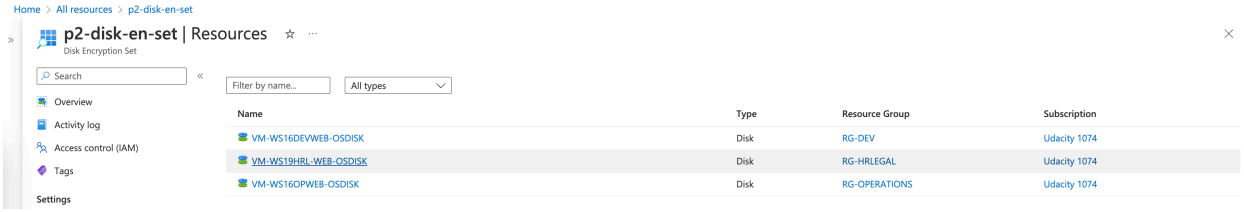
OS disk	VM-WS19HRL-Web-osdisk
Encryption at host	Disabled
Azure disk encryption	Not enabled
Ephemeral OS disk	N/A
Data disks	0

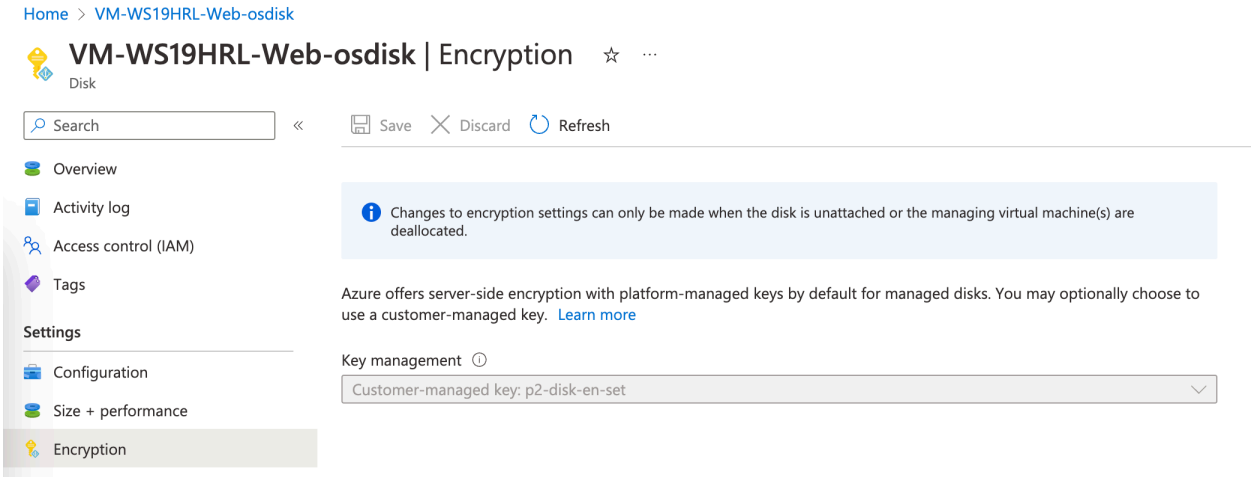
Auto-shutdown

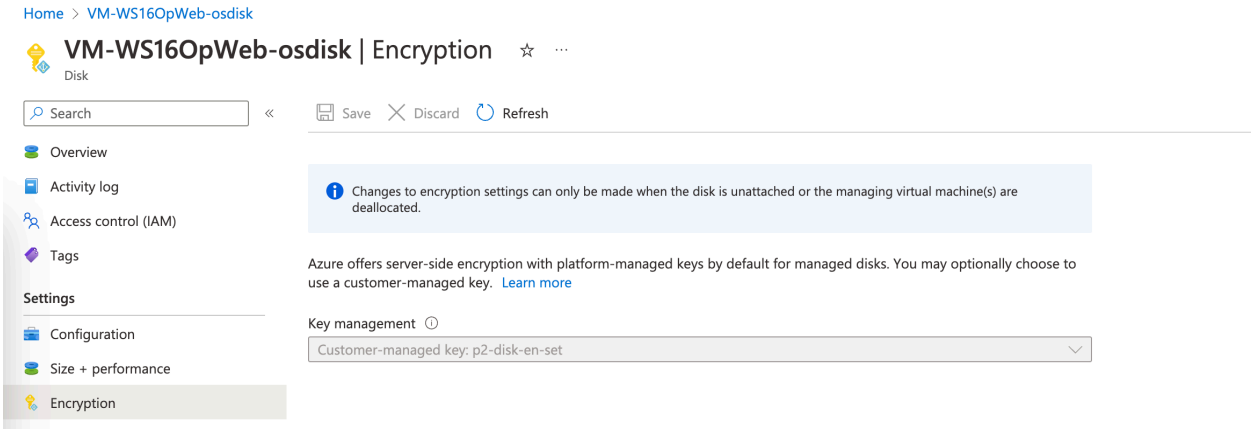
Auto-shutdown	Not enabled

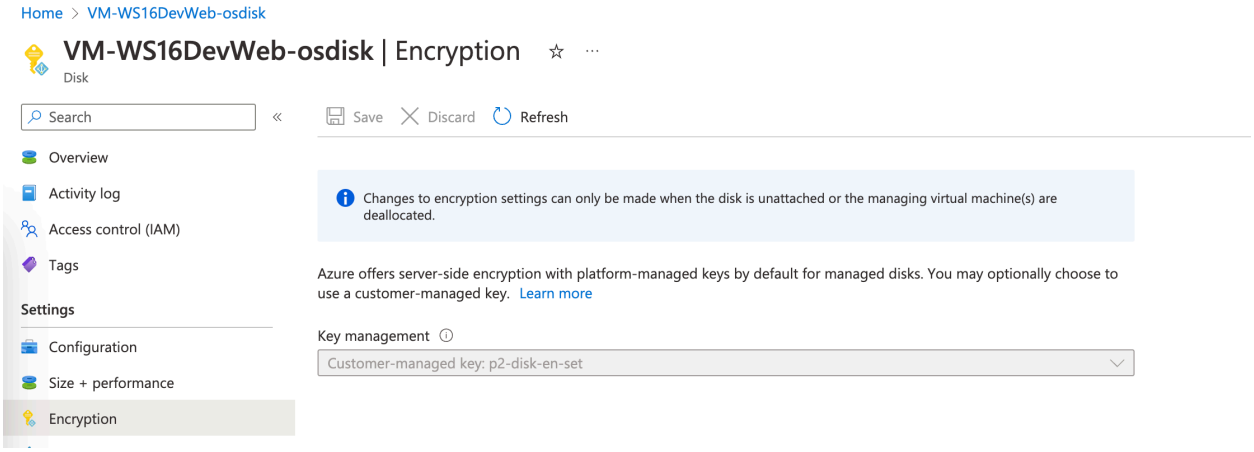
Data and Encryption

1. Proof of Encryption types for VM (devapp,OpWeb,HRL-App,OPApp, HRL-Web)

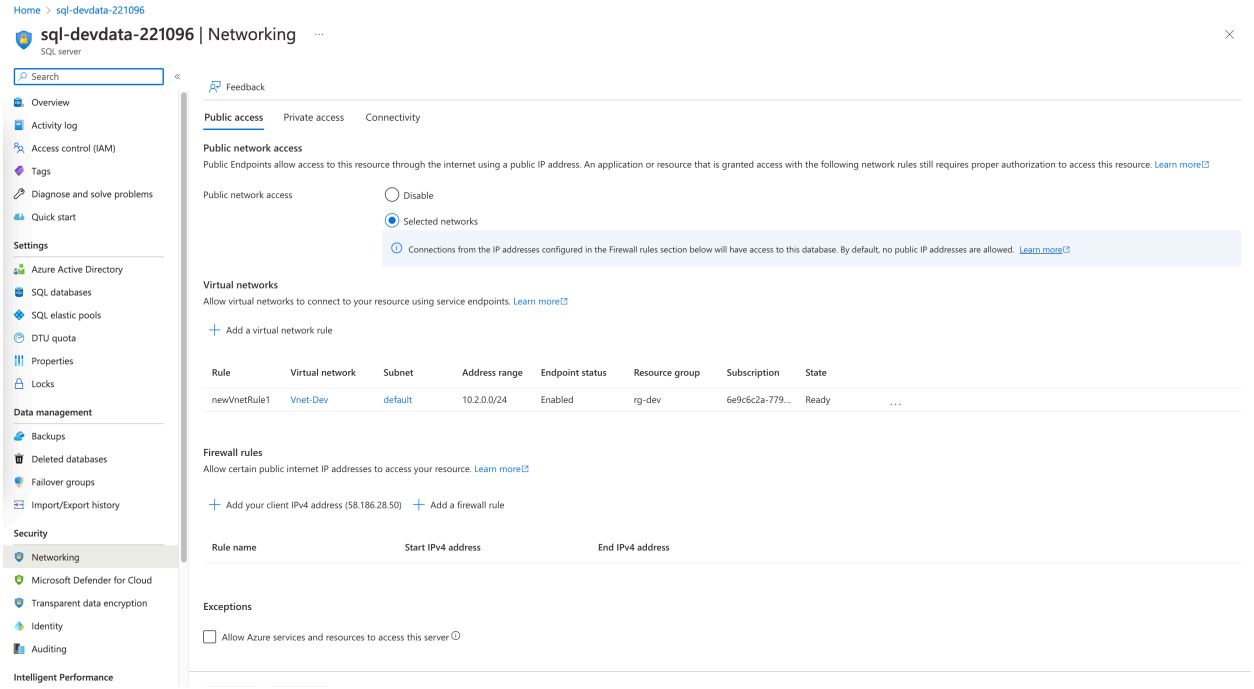


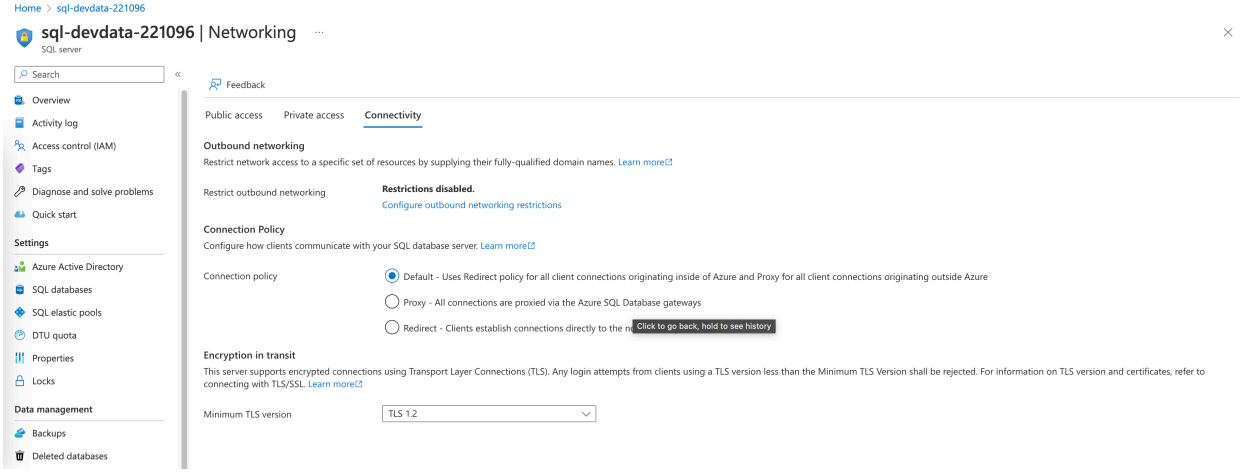


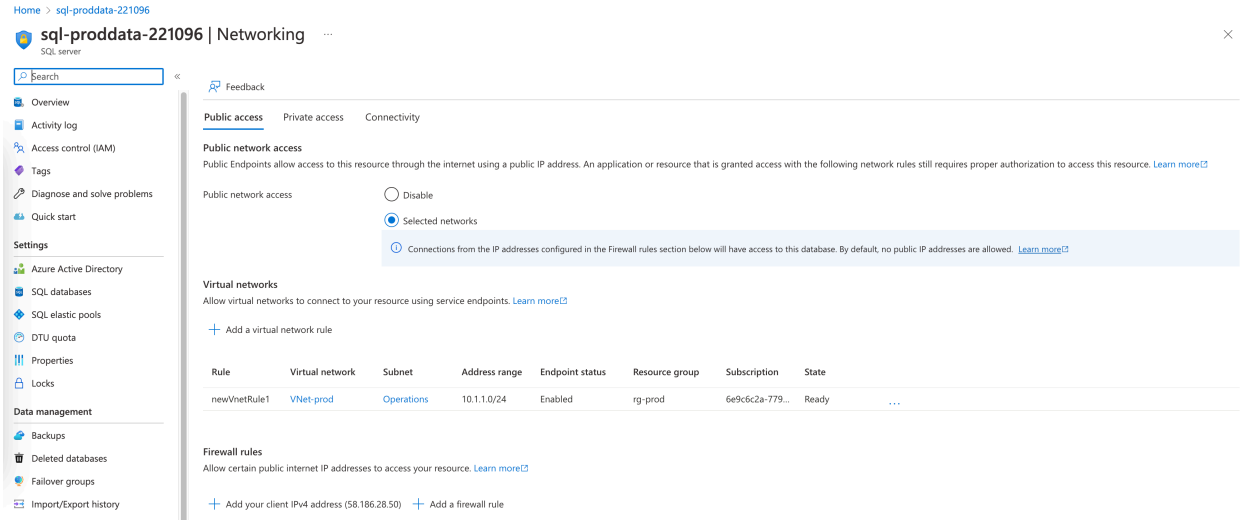


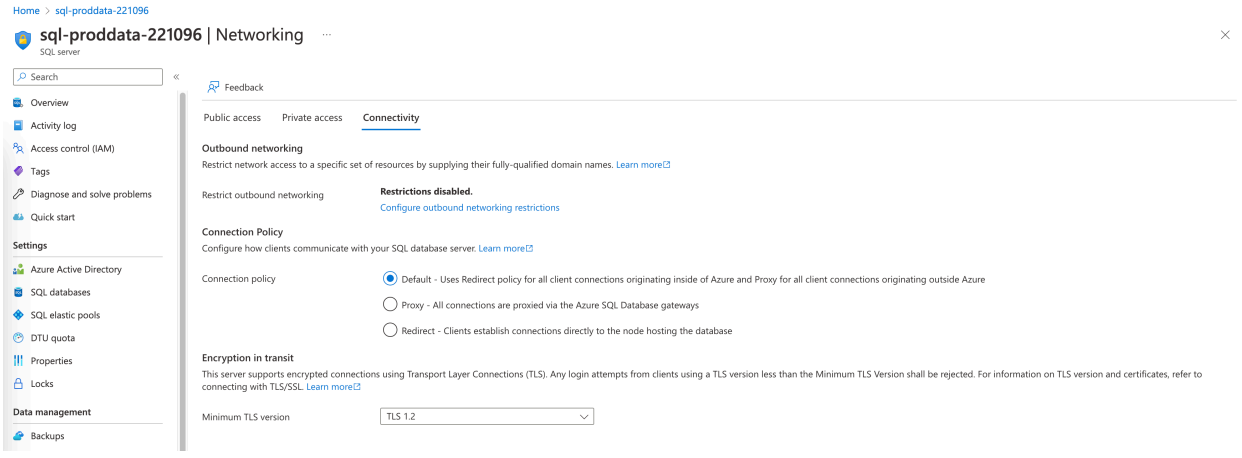


2. Firewalls and virtual networks page
    a. Proof of no public access and TLS for SQL servers(prod, dev)

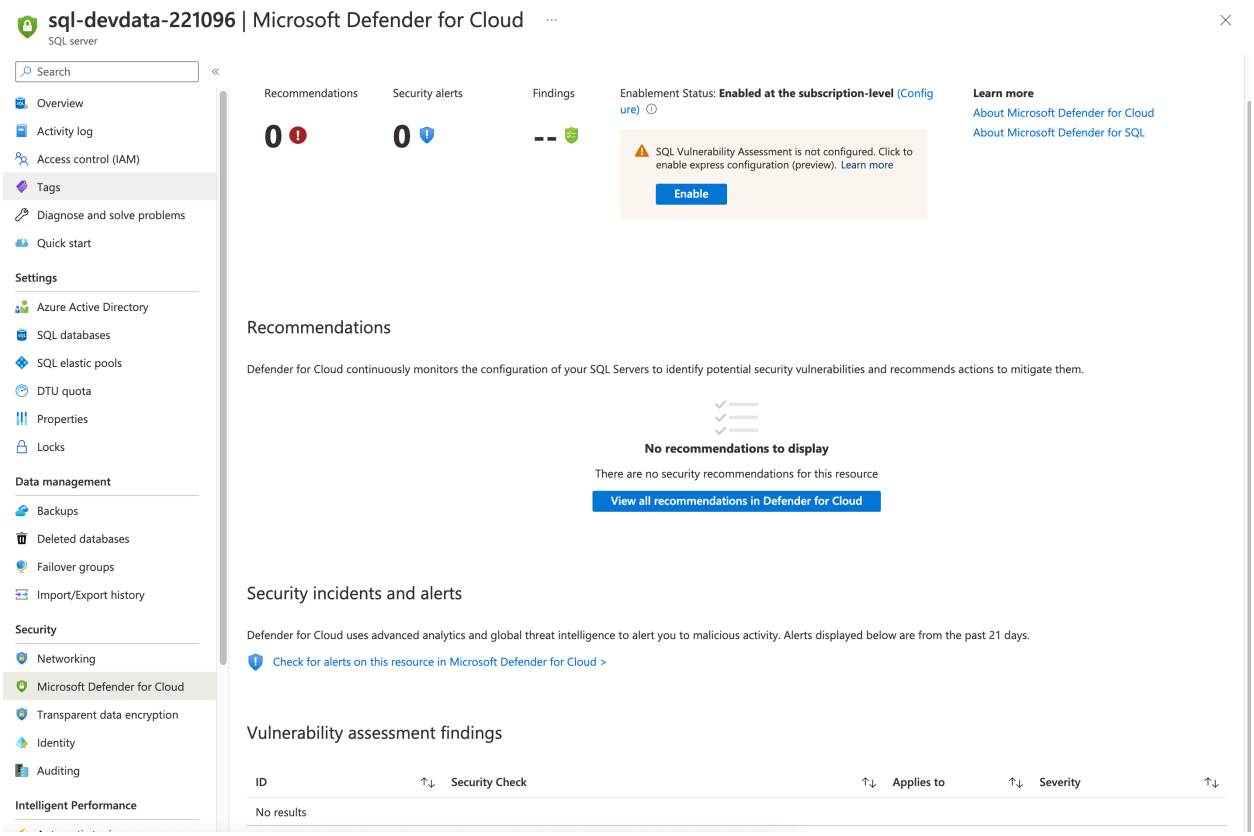


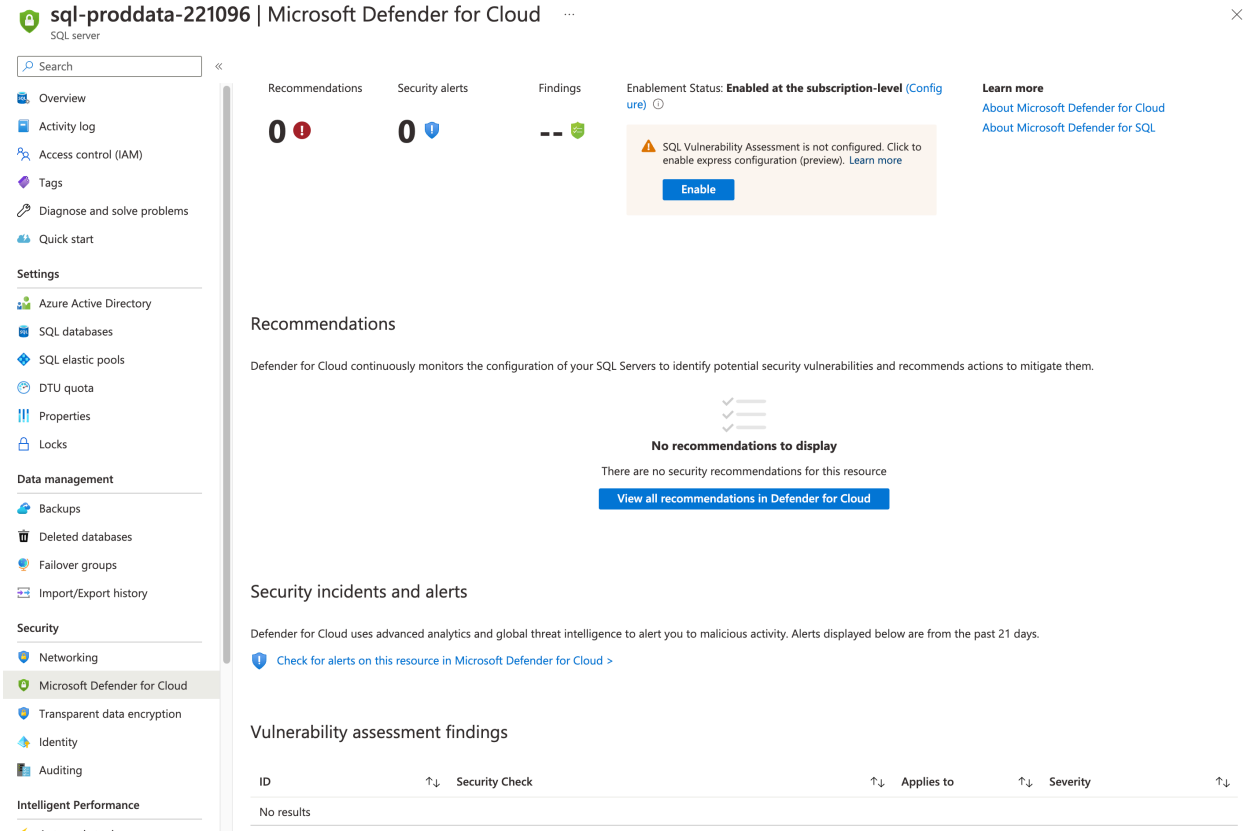




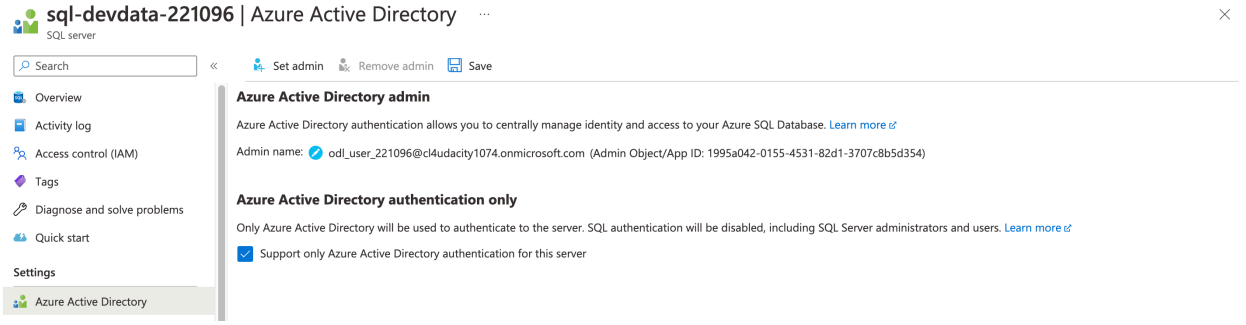


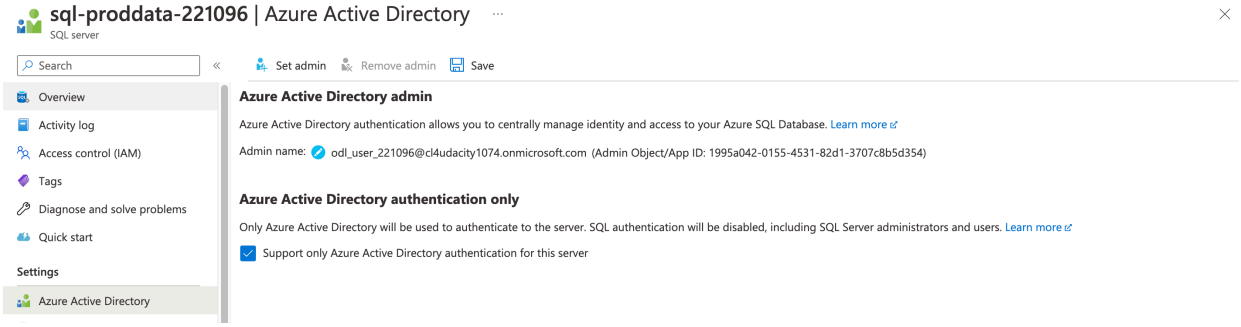
3. Proof of Azure Defender SQL server enabled(prod, dev)


sql-devdata-221096 | Microsoft Defender for Cloud
SQL server
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Quick start
Settings
Azure Active Directory
SQL databases
SQL elastic pools
DTU quota
Properties
Locks
Data management
Backups
Deleted databases
Failover groups
Import/Export history
Security
Networking
Microsoft Defender for Cloud
Transparent data encryption
Identity
Auditing
Intelligent Performance
Recommendations
0
Security alerts
0
Findings
--
Enablement Status: Enabled at the subscription-level (Configure)
SQL Vulnerability Assessment is not configured. Click to enable express configuration (preview). Learn more
Enable
Learn more
About Microsoft Defender for Cloud
About Microsoft Defender for SQL
Recommendations
Defender for Cloud continuously monitors the configuration of your SQL Servers to identify potential security vulnerabilities and recommends actions to mitigate them.
No recommendations to display
There are no security recommendations for this resource
View all recommendations in Defender for Cloud
Security incidents and alerts
Defender for Cloud uses advanced analytics and global threat intelligence to alert you to malicious activity. Alerts displayed below are from the past 21 days.
Check for alerts on this resource in Microsoft Defender for Cloud >
Vulnerability assessment findings
ID
Security Check
Applies to
Severity
No results



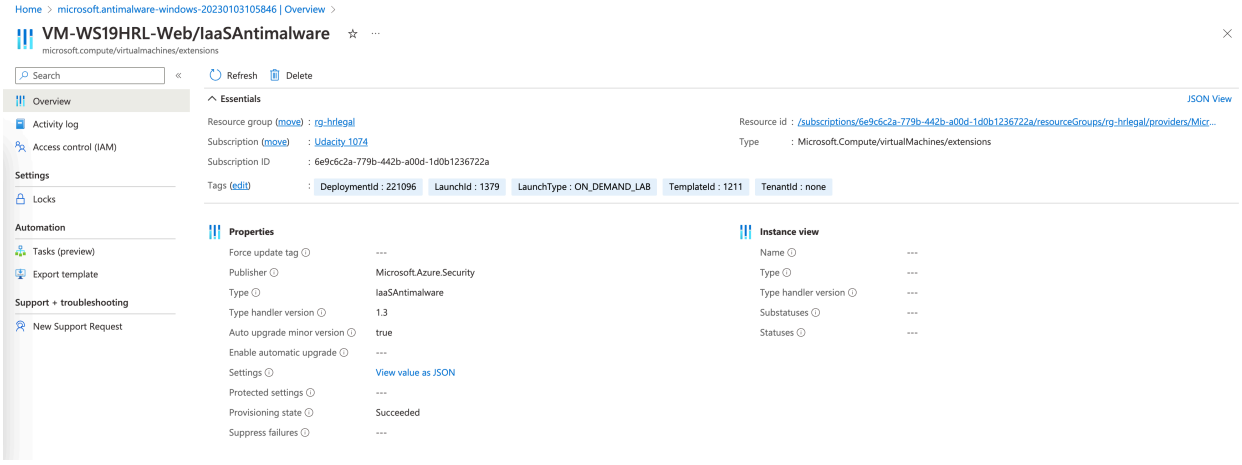
4. Proof of Azure AD authentication for SQL enabled(prod, dev)

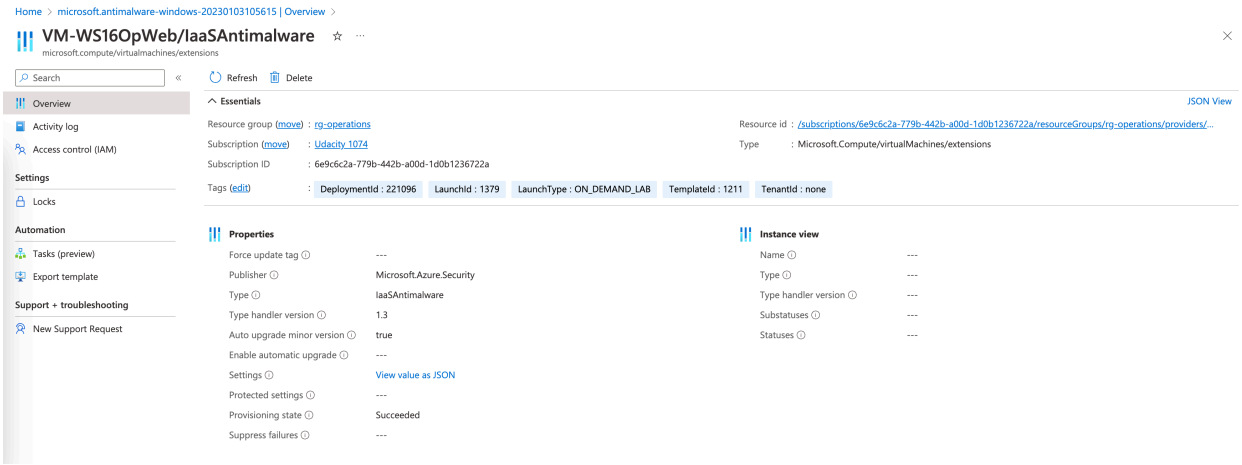


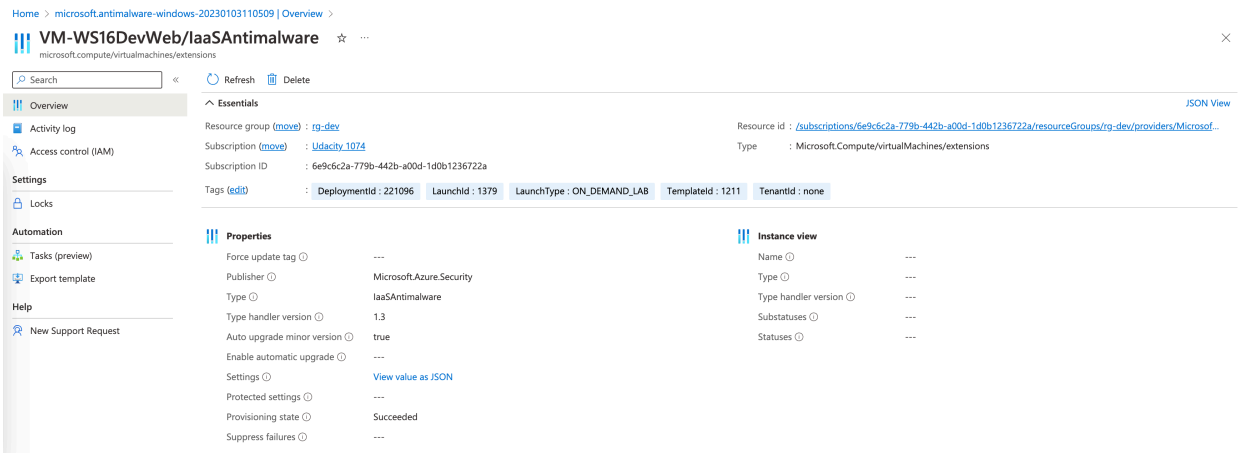

sql-proddata-221096 | Azure Active Directory
SQL server
Search
Set admin
Remove admin
Save
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Quick start
Settings
Azure Active Directory
Azure Active Directory admin
Azure Active Directory authentication allows you to centrally manage identity and access to your Azure SQL Database. Learn more
Admin name: odl_user_221096@cl4udacity1074.onmicrosoft.com (Admin Object/App ID: 1995a042-0155-4531-82d1-3707c8b5d354)
Azure Active Directory authentication only
Only Azure Active Directory will be used to authenticate to the server. SQL authentication will be disabled, including SQL Server administrators and users. Learn more
Support only Azure Active Directory authentication for this server

Cloud Protection

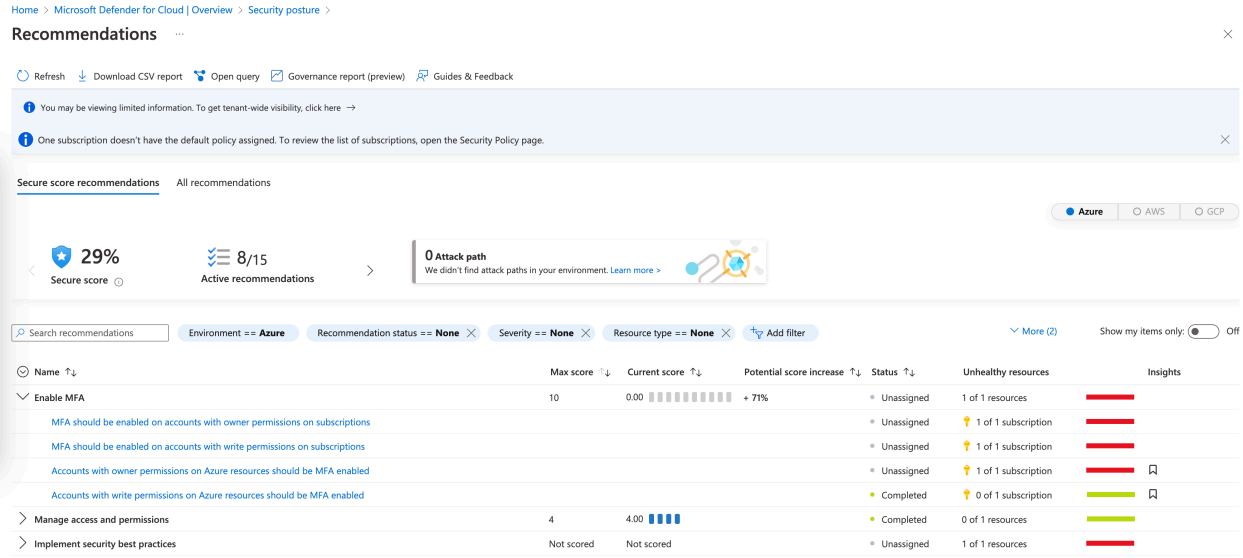
1. Proof of IaaSAntimalware enabled (devapp,OpApp,HRL-Web, HRL-App,OpWeb)





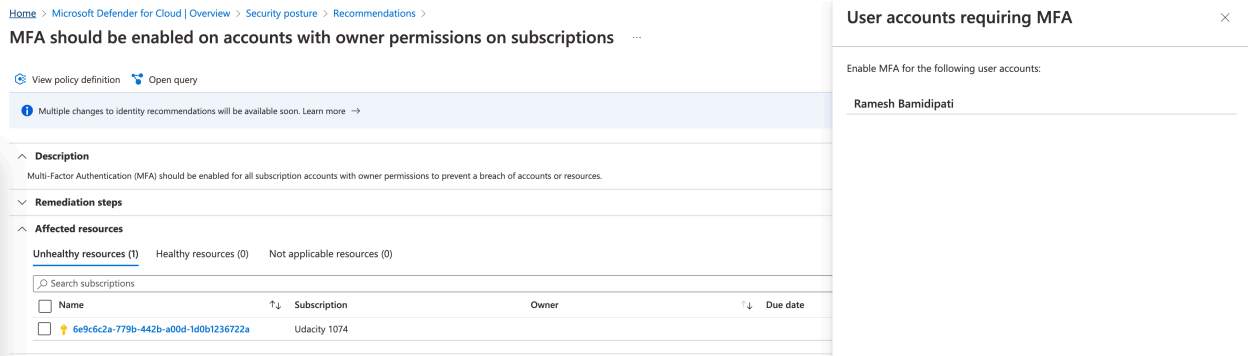


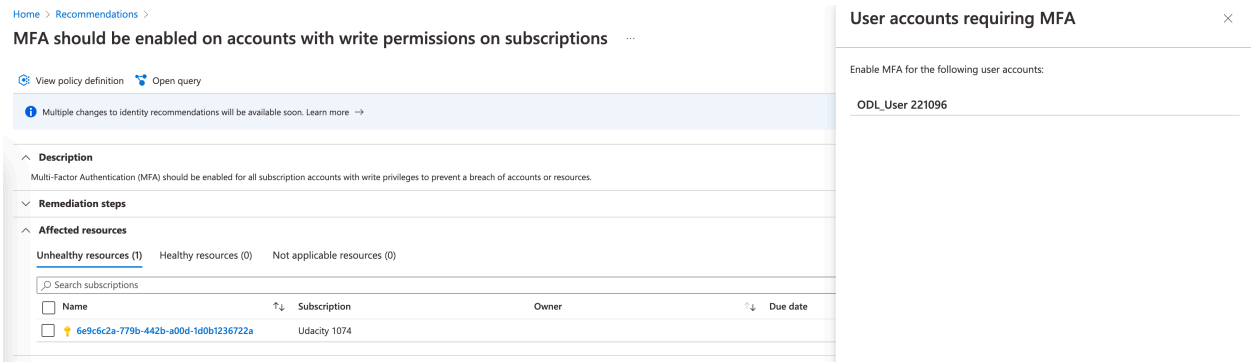
2. Recommendations



A. Based on the security score, the “Enable MFA” has the greatest impact on security (0/10 score).

1. MFA should be enabled on accounts with owner permissions on subscriptions
2. MFA should be enabled on accounts with write permissions on
3. Accounts with owner permissions on Azure resources should be MFA enabled
4. Accounts with write permissions on Azure resources should be MFA enabled



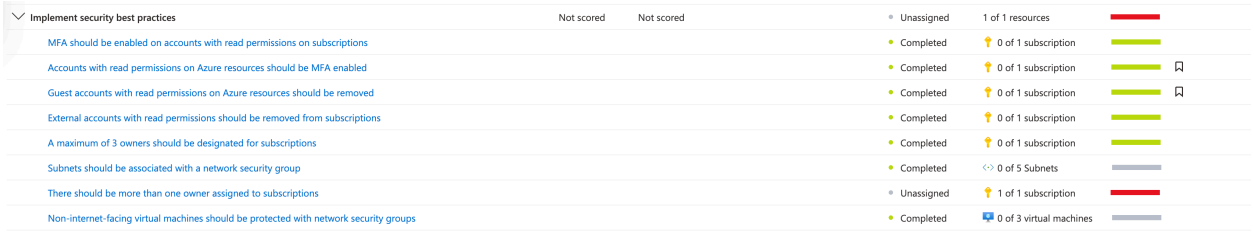


The MFA is disabled for the account Ramesh Bamidipati which has owner permissions and ODL_User 221096 which has write permissions.

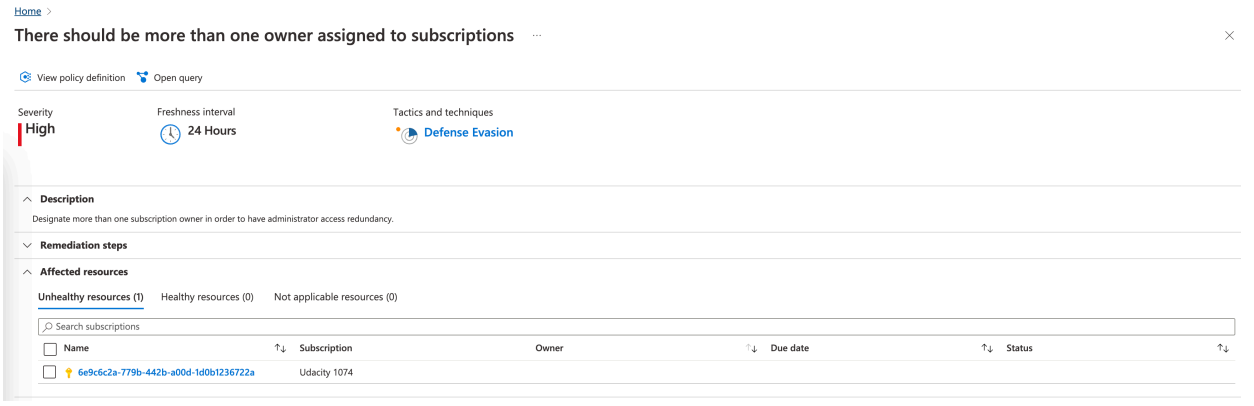
⇨ We should apply a Policy to enforce using MFA for all users (including owner, write role)

B. The “Manage access and permissions” is already solved (4/4 score)

C. Implement security best practices



There is 1 unresolve point in the best practices:

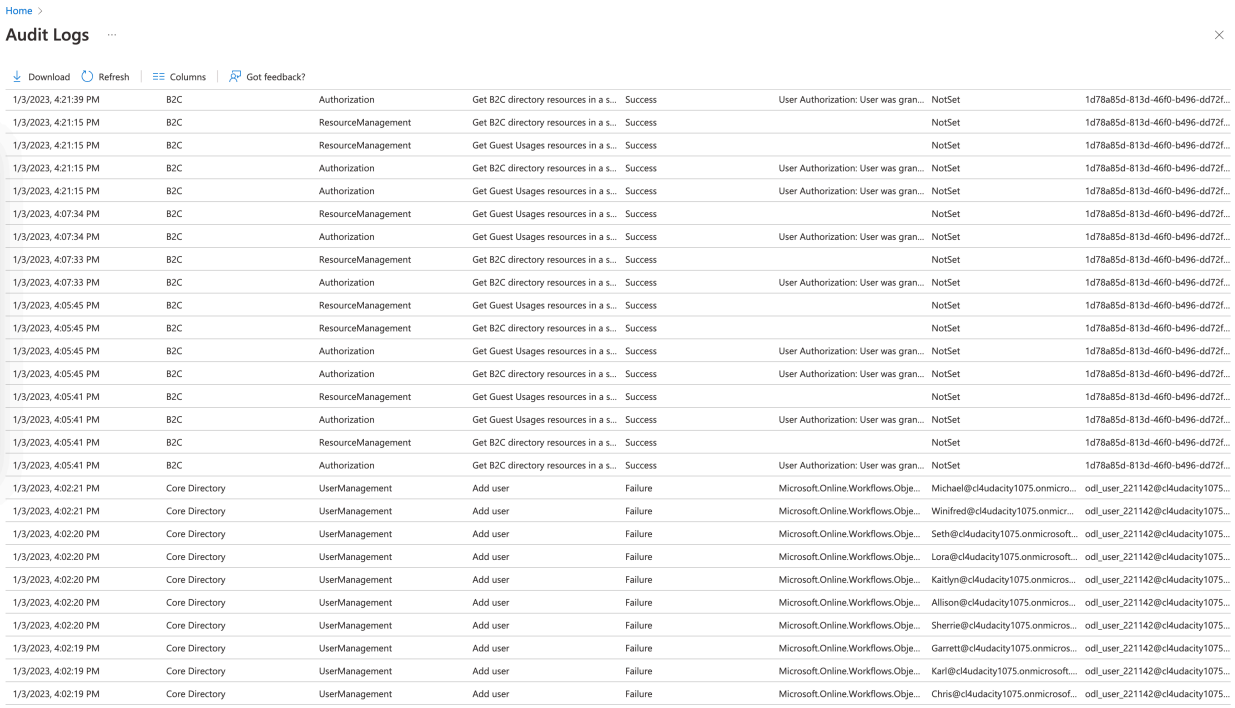


This point recommends having at least 2 users with owner role in a subscription. Designate more than one subscription owner in order to have administrator access redundancy so that if one of the owners forget or lost their password, or the account is hacked, etc. we still have at least 1 other owner.

To add assign an user as an owner, we can use the Access Control (IAM)

Monitoring

Identify 3 items from the Audit log and explain what each log shows.



Home >

Audit Logs ···

Download | Refresh | Columns | Got feedback?

1/3/2023, 4:21:39 PM	B2C	Authorization	Get B2C directory resources in a s...	Success	User Authorization: User was gran...	NotSet	1d78a85d-813d-46f0-b496-dd72f...
1/3/2023, 4:21:15 PM	B2C	ResourceManagement	Get B2C directory resources in a s...	Success		NotSet	1d78a85d-813d-46f0-b496-dd72f...
1/3/2023, 4:21:15 PM	B2C	ResourceManagement	Get Guest Usages resources in a s...	Success		NotSet	1d78a85d-813d-46f0-b496-dd72f...
1/3/2023, 4:21:15 PM	B2C	Authorization	Get B2C directory resources in a s...	Success	User Authorization: User was gran...	NotSet	1d78a85d-813d-46f0-b496-dd72f...
1/3/2023, 4:21:15 PM	B2C	Authorization	Get Guest Usages resources in a s...	Success	User Authorization: User was gran...	NotSet	1d78a85d-813d-46f0-b496-dd72f...
1/3/2023, 4:07:34 PM	B2C	ResourceManagement	Get Guest Usages resources in a s...	Success		NotSet	1d78a85d-813d-46f0-b496-dd72f...
1/3/2023, 4:07:34 PM	B2C	Authorization	Get Guest Usages resources in a s...	Success	User Authorization: User was gran...	NotSet	1d78a85d-813d-46f0-b496-dd72f...
1/3/2023, 4:07:33 PM	B2C	ResourceManagement	Get B2C directory resources in a s...	Success		NotSet	1d78a85d-813d-46f0-b496-dd72f...
1/3/2023, 4:07:33 PM	B2C	Authorization	Get B2C directory resources in a s...	Success	User Authorization: User was gran...	NotSet	1d78a85d-813d-46f0-b496-dd72f...
1/3/2023, 4:05:45 PM	B2C	ResourceManagement	Get Guest Usages resources in a s...	Success		NotSet	1d78a85d-813d-46f0-b496-dd72f...
1/3/2023, 4:05:45 PM	B2C	ResourceManagement	Get B2C directory resources in a s...	Success		NotSet	1d78a85d-813d-46f0-b496-dd72f...
1/3/2023, 4:05:45 PM	B2C	Authorization	Get Guest Usages resources in a s...	Success	User Authorization: User was gran...	NotSet	1d78a85d-813d-46f0-b496-dd72f...
1/3/2023, 4:05:45 PM	B2C	Authorization	Get B2C directory resources in a s...	Success	User Authorization: User was gran...	NotSet	1d78a85d-813d-46f0-b496-dd72f...
1/3/2023, 4:05:41 PM	B2C	ResourceManagement	Get Guest Usages resources in a s...	Success		NotSet	1d78a85d-813d-46f0-b496-dd72f...
1/3/2023, 4:05:41 PM	B2C	Authorization	Get Guest Usages resources in a s...	Success	User Authorization: User was gran...	NotSet	1d78a85d-813d-46f0-b496-dd72f...
1/3/2023, 4:05:41 PM	B2C	ResourceManagement	Get B2C directory resources in a s...	Success		NotSet	1d78a85d-813d-46f0-b496-dd72f...
1/3/2023, 4:05:41 PM	B2C	Authorization	Get B2C directory resources in a s...	Success	User Authorization: User was gran...	NotSet	1d78a85d-813d-46f0-b496-dd72f...
1/3/2023, 4:02:21 PM	Core Directory	UserManagement	Add user	Failure	Microsoft.Online.Workflows.Obje...	Michael@cl4udacity1075.onmicro...	odl_user_221142@cl4udacity1075...
1/3/2023, 4:02:21 PM	Core Directory	UserManagement	Add user	Failure	Microsoft.Online.Workflows.Obje...	Winifred@cl4udacity1075.onmicr...	odl_user_221142@cl4udacity1075...
1/3/2023, 4:02:20 PM	Core Directory	UserManagement	Add user	Failure	Microsoft.Online.Workflows.Obje...	Seth@cl4udacity1075.onmicrosoft...	odl_user_221142@cl4udacity1075...
1/3/2023, 4:02:20 PM	Core Directory	UserManagement	Add user	Failure	Microsoft.Online.Workflows.Obje...	Lora@cl4udacity1075.onmicrosoft...	odl_user_221142@cl4udacity1075...
1/3/2023, 4:02:20 PM	Core Directory	UserManagement	Add user	Failure	Microsoft.Online.Workflows.Obje...	Kaitlyn@cl4udacity1075.onmicros...	odl_user_221142@cl4udacity1075...
1/3/2023, 4:02:20 PM	Core Directory	UserManagement	Add user	Failure	Microsoft.Online.Workflows.Obje...	Allison@cl4udacity1075.onmicros...	odl_user_221142@cl4udacity1075...
1/3/2023, 4:02:20 PM	Core Directory	UserManagement	Add user	Failure	Microsoft.Online.Workflows.Obje...	Sherrie@cl4udacity1075.onmicros...	odl_user_221142@cl4udacity1075...
1/3/2023, 4:02:19 PM	Core Directory	UserManagement	Add user	Failure	Microsoft.Online.Workflows.Obje...	Garrett@cl4udacity1075.onmicros...	odl_user_221142@cl4udacity1075...
1/3/2023, 4:02:19 PM	Core Directory	UserManagement	Add user	Failure	Microsoft.Online.Workflows.Obje...	Karl@cl4udacity1075.onmicrosoft....	odl_user_221142@cl4udacity1075...
1/3/2023, 4:02:19 PM	Core Directory	UserManagement	Add user	Failure	Microsoft.Online.Workflows.Obje...	Chris@cl4udacity1075.onmicrosof...	odl_user_221142@cl4udacity1075...

- Audit Log 1: Add User

Home >

Audit Logs

Download | Refresh | Columns | Got feedback?

1/3/2023, 4:21:39 PM	B2C	Authorization	Get B2C directory resources in a s...	Su
1/3/2023, 4:21:15 PM	B2C	ResourceManagement	Get B2C directory resources in a s...	Su
1/3/2023, 4:21:15 PM	B2C	ResourceManagement	Get Guest Usages resources in a s...	Su
1/3/2023, 4:21:15 PM	B2C	Authorization	Get B2C directory resources in a s...	Su
1/3/2023, 4:21:15 PM	B2C	Authorization	Get Guest Usages resources in a s...	Su
1/3/2023, 4:07:34 PM	B2C	ResourceManagement	Get Guest Usages resources in a s...	Su
1/3/2023, 4:07:34 PM	B2C	Authorization	Get Guest Usages resources in a s...	Su
1/3/2023, 4:07:33 PM	B2C	ResourceManagement	Get B2C directory resources in a s...	Su
1/3/2023, 4:07:33 PM	B2C	Authorization	Get B2C directory resources in a s...	Su
1/3/2023, 4:05:45 PM	B2C	ResourceManagement	Get Guest Usages resources in a s...	Su
1/3/2023, 4:05:45 PM	B2C	ResourceManagement	Get B2C directory resources in a s...	Su
1/3/2023, 4:05:45 PM	B2C	Authorization	Get Guest Usages resources in a s...	Su
1/3/2023, 4:05:45 PM	B2C	Authorization	Get B2C directory resources in a s...	Su
1/3/2023, 4:05:41 PM	B2C	ResourceManagement	Get Guest Usages resources in a s...	Su
1/3/2023, 4:05:41 PM	B2C	Authorization	Get Guest Usages resources in a s...	Su
1/3/2023, 4:05:41 PM	B2C	ResourceManagement	Get B2C directory resources in a s...	Su
1/3/2023, 4:05:41 PM	B2C	Authorization	Get B2C directory resources in a s...	Su
1/3/2023, 4:02:21 PM	Core Directory	UserManagement	Add user	Fa
1/3/2023, 4:02:21 PM	Core Directory	UserManagement	Add user	Fa
1/3/2023, 4:02:20 PM	Core Directory	UserManagement	Add user	Fa
1/3/2023, 4:02:20 PM	Core Directory	UserManagement	Add user	Fa
1/3/2023, 4:02:20 PM	Core Directory	UserManagement	Add user	Fa
1/3/2023, 4:02:20 PM	Core Directory	UserManagement	Add user	Fa
1/3/2023, 4:02:20 PM	Core Directory	UserManagement	Add user	Fa
1/3/2023, 4:02:19 PM	Core Directory	UserManagement	Add user	Fa
1/3/2023, 4:02:19 PM	Core Directory	UserManagement	Add user	Fa
1/3/2023, 4:02:19 PM	Core Directory	UserManagement	Add user	Fa

Audit Log Details

Activity | Target(s) | Modified Properties

Activity

Date	1/3/2023, 4:02 PM
Activity Type	Add user
Correlation ID	4365043b-a2ea-423c-9233-8fab24742f19
Category	UserManagement
Status	failure
Status reason	Microsoft.Online.Workflows.ObjectAlreadyExistsException
User Agent	

Initiated by (actor)

Type	User
Display Name	
Object ID	3dd42e03-5778-4f7d-82b2-0c609087a755
IP address	20.127.52.190
User Principal Name	odl_user_221142@cl4udacity1075.onmicrosoft.com

Additional Details

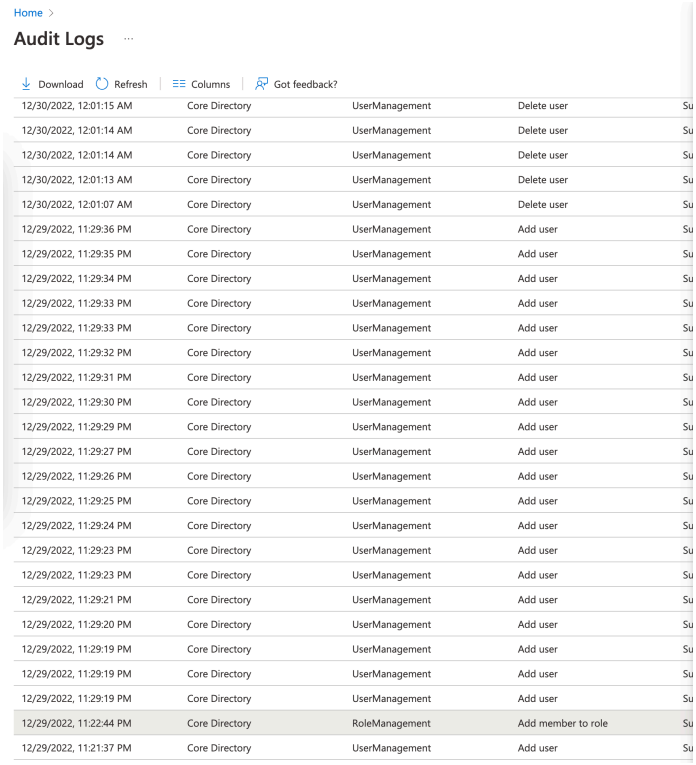
User-Agent	Swagger-Codegen/1.4.0.0/csharp

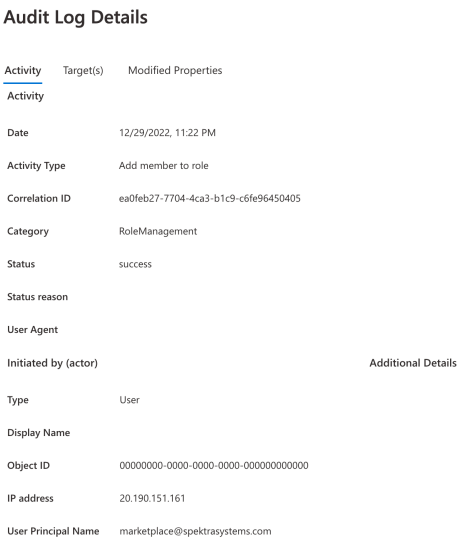
Activity | Target(s) | **Modified Properties**

Target	Property Name	Old Value	New Value
Michael@...	AccountEnabled	[]	[true]
Michael@...	City	[]	["Detroit"]
Michael@...	Department	[]	["IT"]
Michael@...	DisplayName	[]	["Michael"]
Michael@...	JobTitle	[]	["Support Desk Admin"]
Michael@...	MailNickname	[]	["Michael"]
Michael@...	StsRefreshToke...	[]	["2023-01-03T09:02:21Z"]
Michael@...	UserPrincipalN...	[]	["Michael@cl4udacity1075.onmicrosoft.com"]
Michael@...	UserType	[]	["Member"]
Michael@...	Included Updat...		"AccountEnabled, City, Department, DisplayName, JobTitle, MailNickname, StsRefreshTokensValidFrom, UserPrincipalName, UserType"
Michael@...	MethodExecuti...		"Microsoft.Online.Workflows.ObjectAlreadyExistsException"

⇨ A new user is added to the AAD, we can see the details of the action including datetime, IP address, status of the action,... The logs also shows the details of the event, in this case is the details of the user

- Audit Log 2: Add Member to Role

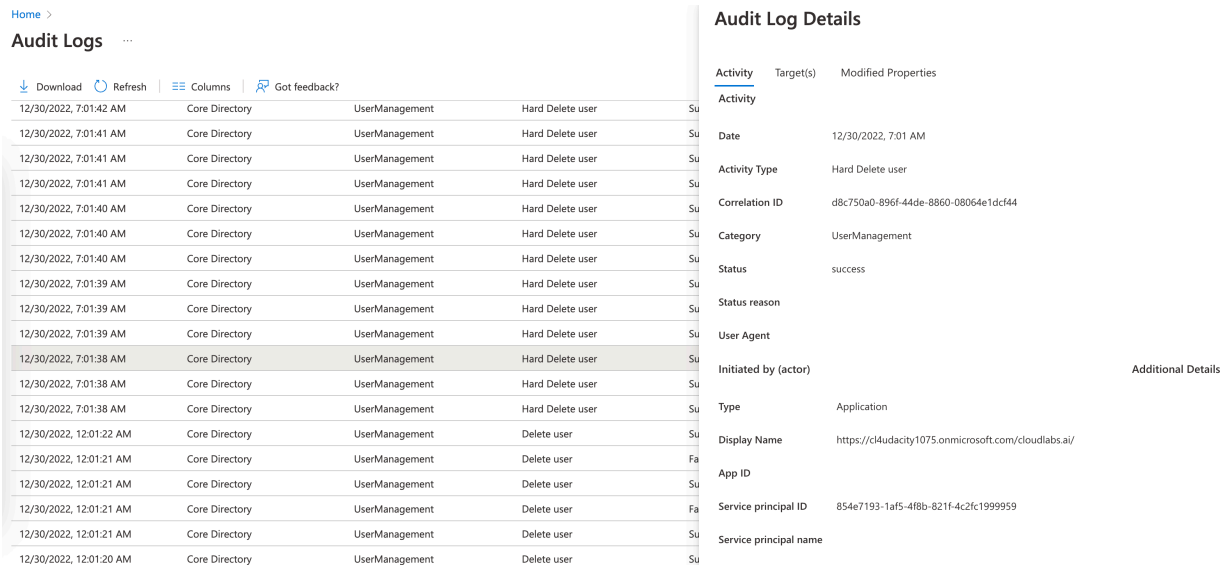




Target	Property Name	Old Value	New Value
odl_user_2...	Role.ObjectID		"0e599a48-f786-4c28-baad-20968d5427aa"
odl_user_2...	Role.DisplayNa...		"Global Administrator"
odl_user_2...	Role.TemplateId		"62e90394-69f5-4237-9190-012177145e10"
odl_user_2...	Role.WellKnow...		"TenantAdmins"

⇨ Beside the general information, this log shows us there are 2 roles (Global Admin, Tenant Admin) assigned to user odl_user_220700

- Audit Log 2: Add Member to Role



Target

Type	User
Id	67f5367e-d50f-43fa-827c-2bb38377d177
Display Name	
User Principal Name	67f5367ed50f43fa827c2bb38377d177Chris@cl4udacity1075.onmicrc

⇨ This log shows us the the user with ID 67f5367e-d50f-43fa-827c-2bb38377d177 is hard deleted. The log contains additional info like time, action type, status of the action, category, etc.

1. Proof of Azure SQL auditing with Log analytics (devdata,proddata)

sql-devdata-221096 | Auditing

SQL server

Search

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Quick start

Settings

Azure Active Directory
SQL databases
SQL elastic pools
DTU quota
Properties
Locks

Data management

Backups
Deleted databases
Failover groups
Import/Export history

Security

Networking
Microsoft Defender for Cloud
Transparent data encryption

Save | Discard | Feedback

Azure SQL Auditing

Azure SQL Auditing tracks database events and writes them to an audit log in your Azure Storage account, Log Analytics workspace or Event Hub. Learn more about Azure SQL Auditing

Enable Azure SQL Auditing

Audit log destination (choose at least one):

- [ ] Storage
- [x] Log Analytics

Subscription *

Udacity 1074

Log Analytics *

p3-log-analytics(eastus)

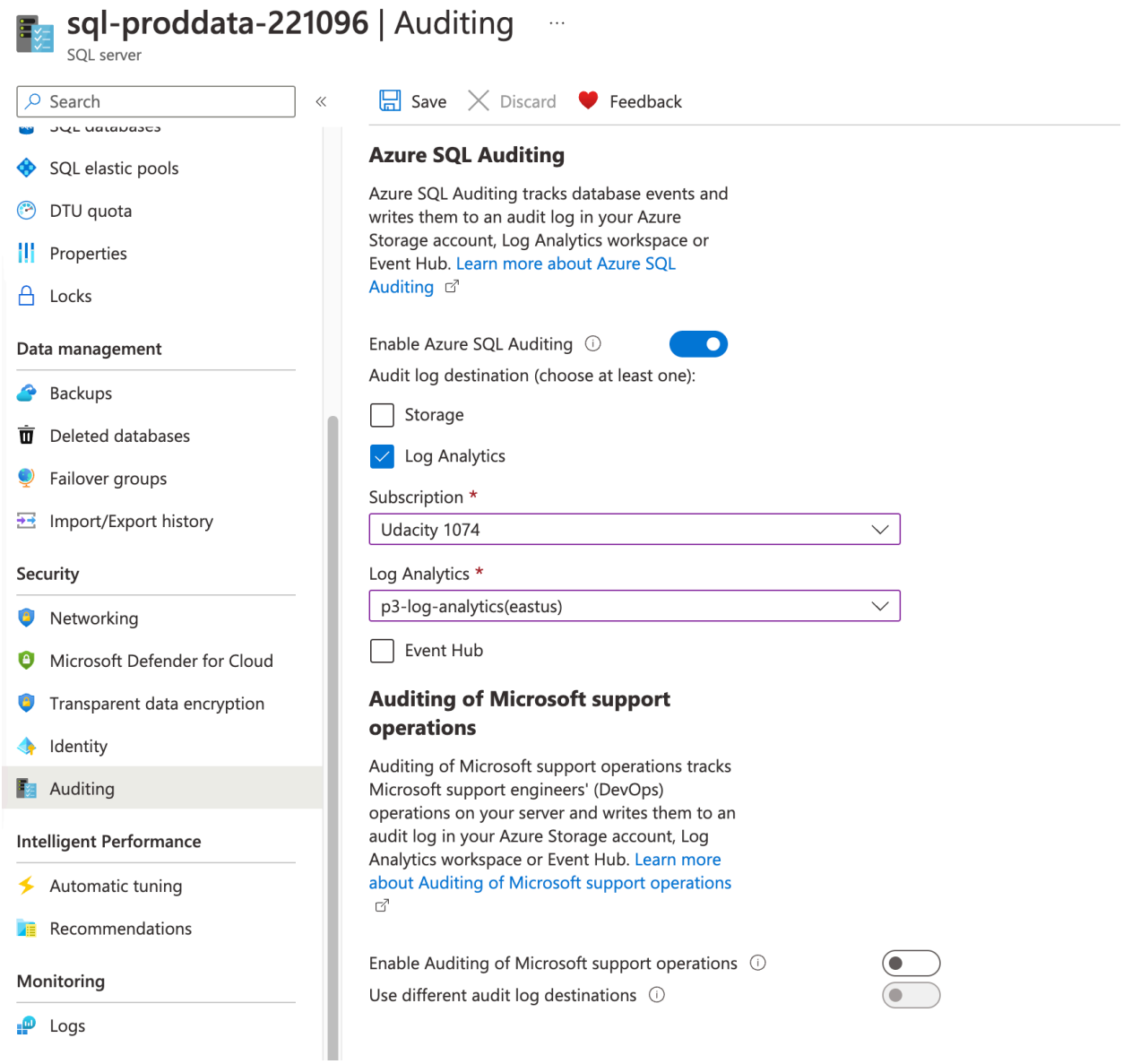
- [ ] Event Hub

Auditing of Microsoft support operations

Auditing of Microsoft support operations tracks Microsoft support engineers' (DevOps) operations on your server and writes them to an audit log in your Azure Storage account, Log Analytics workspace or Event Hub. Learn more about Auditing of Microsoft support operations

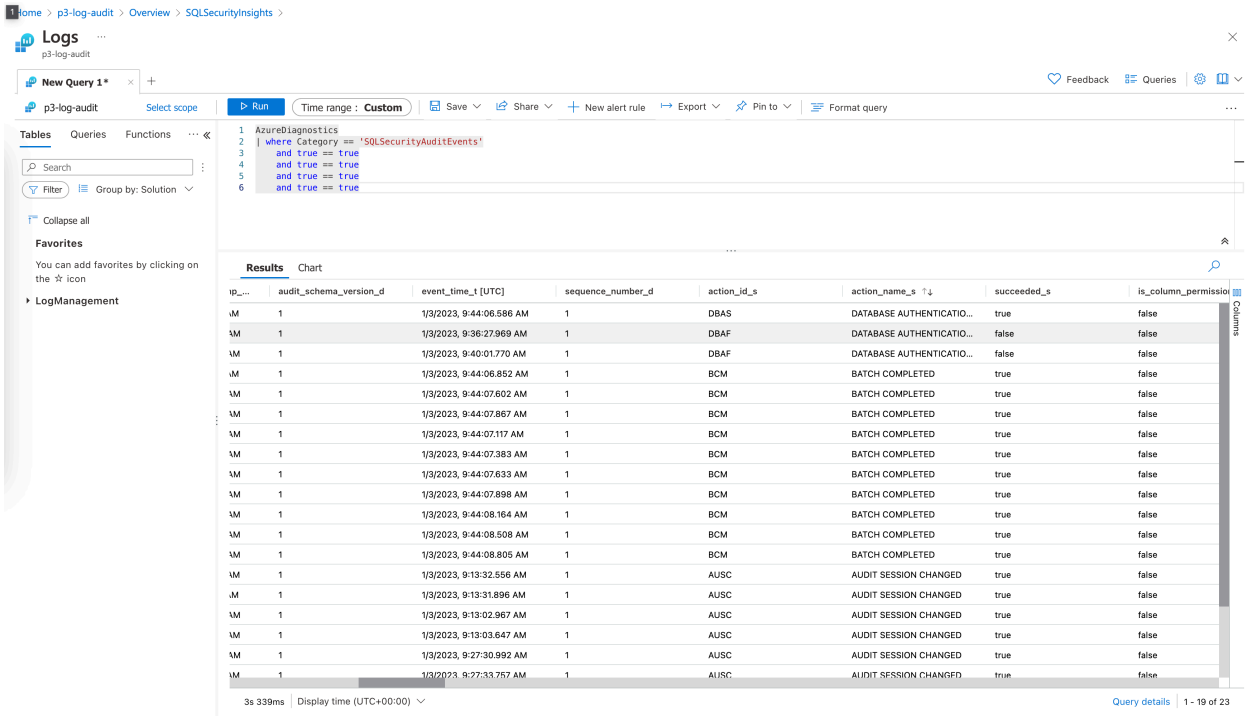
Enable Auditing of Microsoft support operations

Use different audit log destinations



** Audit logs for SQL

Identify 3 items from the Audit log and explain what each log shows.



Above is the screenshot of the created log analytics workspace (configurated for 2 sql servers). There're some logs after I tried to login and executed some queries.

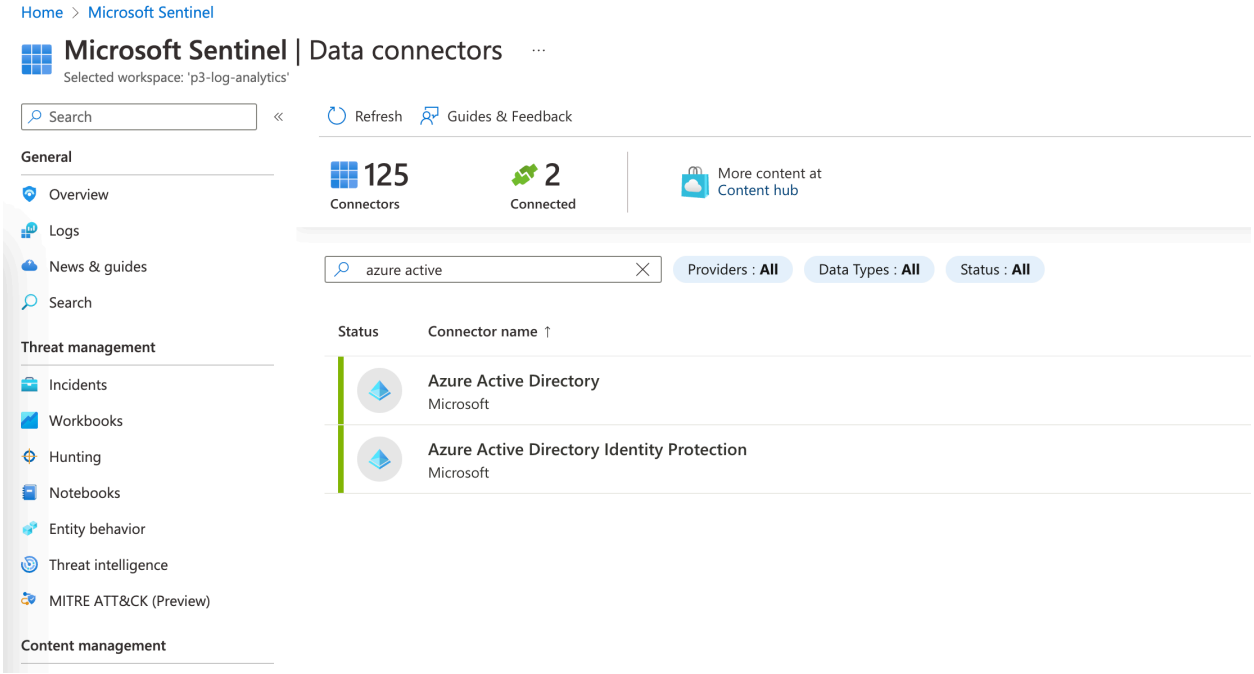
The logs with action name "DATABASE_AUTHENTICATION" shows the history of attempts to login to the server with some other useful info: instance name, time, status, server principal name, etc.

The logs with action name "BATCH_COMPLETED" shows the history of the executed queries in the database, we can find the full statement, object name, database name, etc. in the logs

database_name_s	object_name_s	statement_s
master	master	
DB-development-221142	DB-development-221142	
DB-development-221142	DB-development-221142	
master	master	SELECT ISNULL(SESSIONPROPERTY ('ANSI_NULLS'), 0), ISNULL(SESSIONPROPERTY ('QUOTED_IDENTIFIER'), 1)
DB-development-221142	DB-development-221142	SET NOEXEC OFF SET ROWCOUNT 0 SET TEXTSIZE 2147483647 SET NOCOUNT OFF SET CONCAT_NULL_YIELDS_NULL ON SET ARITHABORT ON SET LOCK_TIMEO
DB-development-221142	DB-development-221142	CREATE TABLE Persons (PersonID int, LastName varchar(255), FirstName varchar(255), Address varchar(255), City varchar(255));
master	master	SELECT CONVERT(NVARCHAR(36), CONTEXT_INFO())
master	master	SELECT ISNULL(SESSIONPROPERTY ('ANSI_NULLS'), 0), ISNULL(SESSIONPROPERTY ('QUOTED_IDENTIFIER'), 1)
master	master	SELECT CONVERT(NVARCHAR(36), CONTEXT_INFO())
master	master	set LOCK_TIMEOUT 5000
master	master	SET ANSI_NULLS, ANSI_PADDING, ANSI_WARNINGS, ARITHABORT, CONCAT_NULL_YIELDS_NULL, QUOTED_IDENTIFIER ON; SET NUMERIC_ROUNDABORT OFF;
master	master	SELECT ISNULL(SESSIONPROPERTY ('ANSI_NULLS'), 0), ISNULL(SESSIONPROPERTY ('QUOTED_IDENTIFIER'), 1)
master	master	SELECT name FROM sys.databases WHERE state_desc='ONLINE' ORDER BY name ASC

The AUDIT_SESSION_CHANGE logs are the log of log audit service in the server.

2. Proof of Sentinel connectors (2+)



Compliance

1. Proof of NIST SP 800-53 rev4 policy added