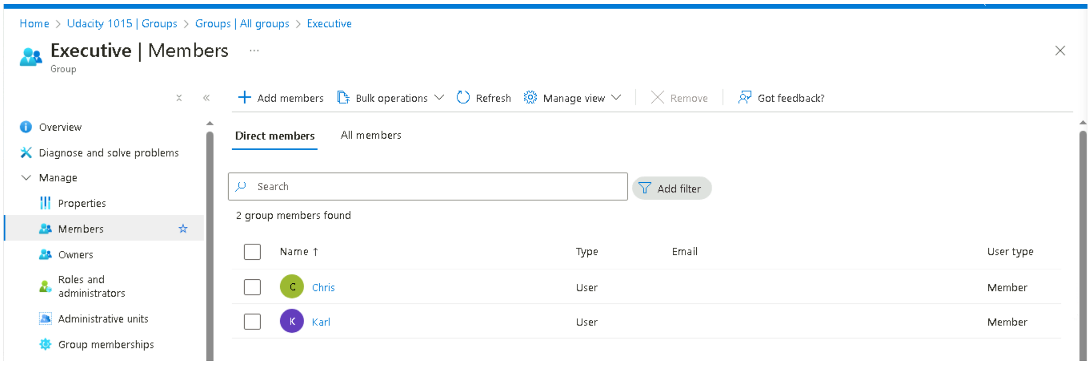
Cloud Security - Building a Robust Azure Infra with Real-World Techniques

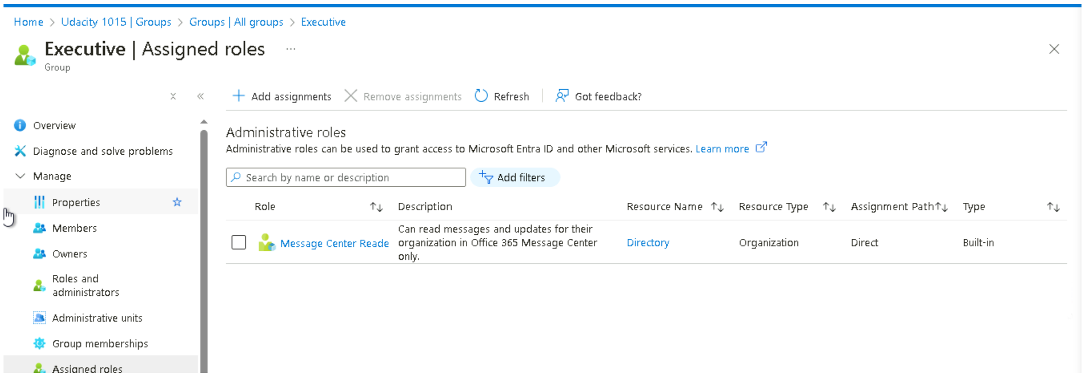
Identity and Access Management

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



2 group members found

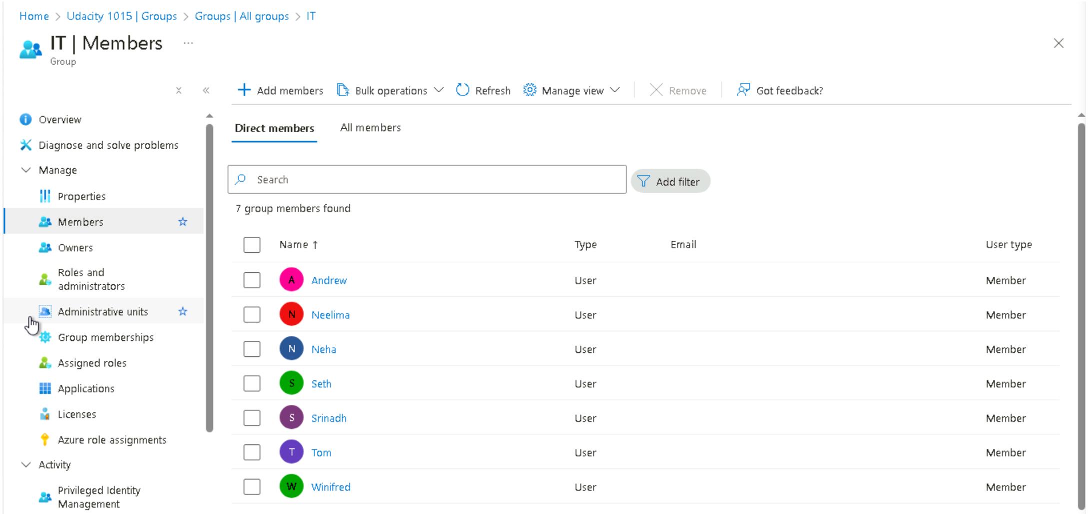
Name ↑	Type	Email	User type
Chris	User		Member
Karl	User		Member



Administrative roles

Administrative roles can be used to grant access to Microsoft Entra ID and other Microsoft services. Learn more

Role	Description	Resource Name	Resource Type	Assignment Path	Type
Message Center Reade	Can read messages and updates for their organization in Office 365 Message Center only.	Directory	Organization	Direct	Built-in

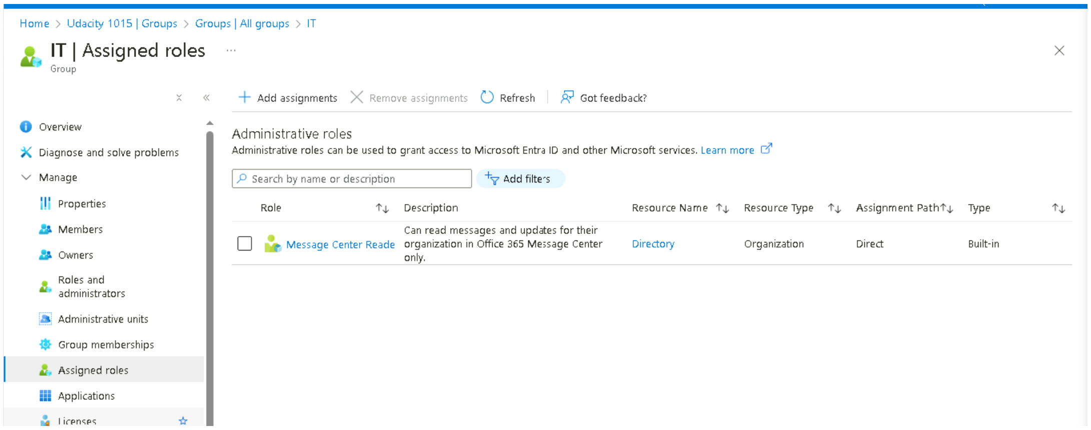


IT | Members

Group

7 group members found

□	Name ↑	Type	Email	User type
□	A Andrew	User		Member
□	N Neelima	User		Member
□	N Neha	User		Member
□	S Seth	User		Member
□	S Srinadh	User		Member
□	T Tom	User		Member
□	W Winifred	User		Member



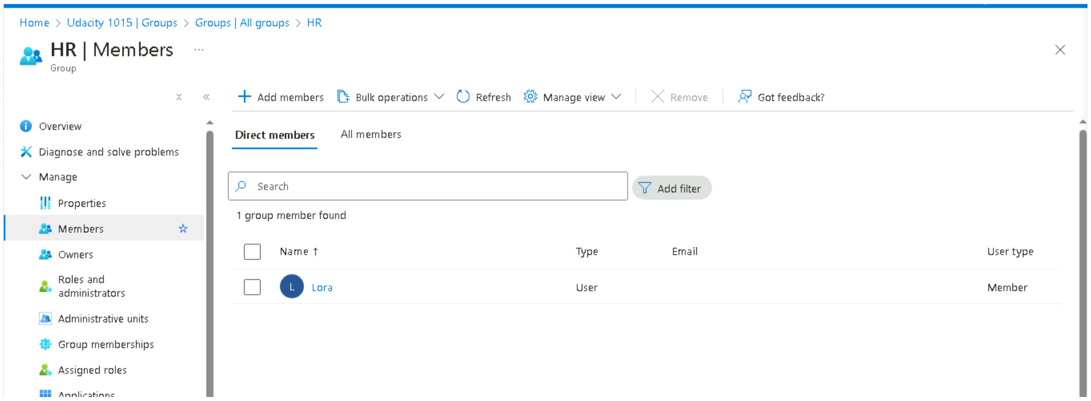
IT | Assigned roles

Group

Administrative roles

Administrative roles can be used to grant access to Microsoft Entra ID and other Microsoft services. Learn more

□	Role	Description	Resource Name	Resource Type	Assignment Path	Type
□	Message Center Reade	Can read messages and updates for their organization in Office 365 Message Center only.	Directory	Organization	Direct	Built-in

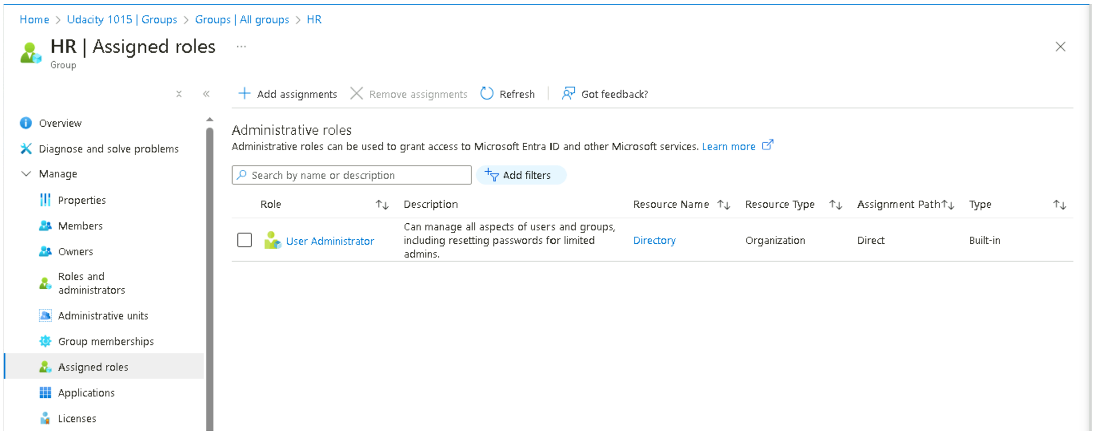


HR | Members

Group

1 group member found

□	Name ↑	Type	Email	User type
□	L Lora	User		Member

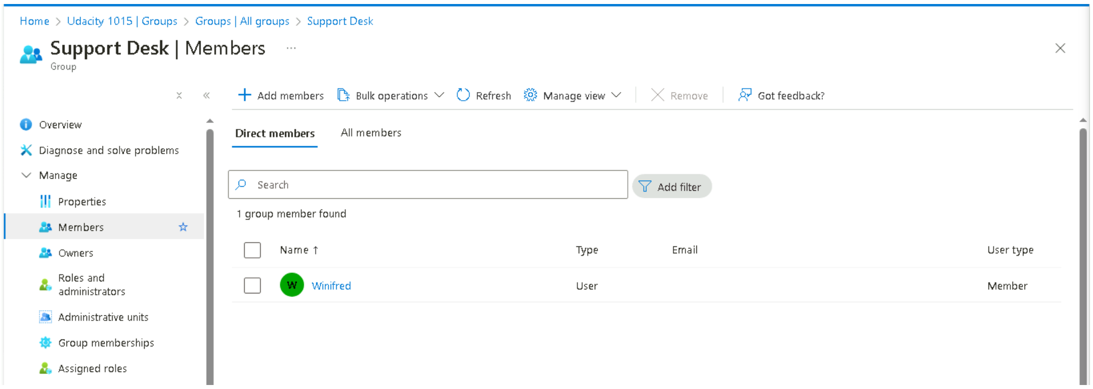


HR | Assigned roles

Administrative roles

Administrative roles can be used to grant access to Microsoft Entra ID and other Microsoft services. Learn more

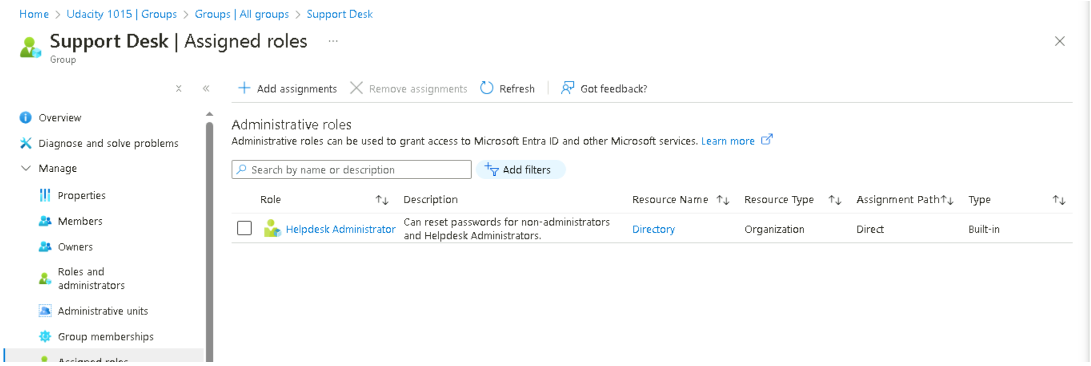
Role	Description	Resource Name	Resource Type	Assignment Path	Type
User Administrator	Can manage all aspects of users and groups, including resetting passwords for limited admins.	Directory	Organization	Direct	Built-in



Support Desk | Members

1 group member found

Name ↑	Type	Email	User type
W Winifred	User		Member

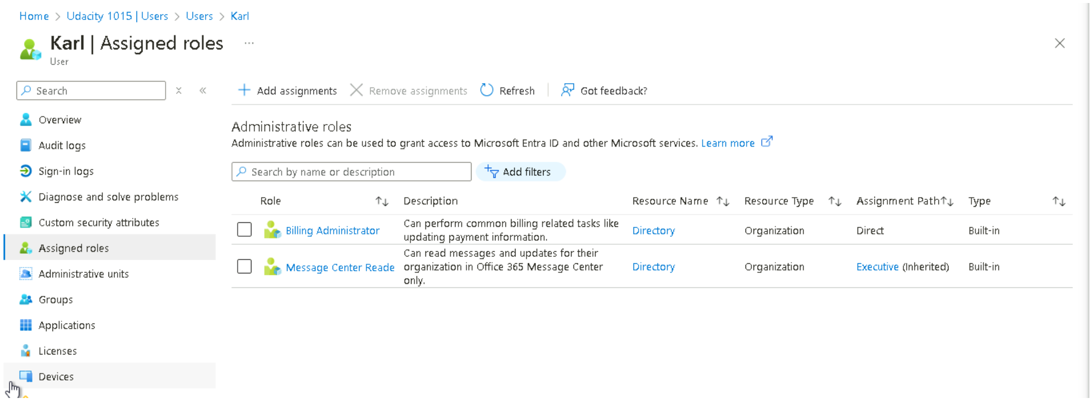


Support Desk | Assigned roles

Administrative roles

Administrative roles can be used to grant access to Microsoft Entra ID and other Microsoft services. Learn more

Role	Description	Resource Name	Resource Type	Assignment Path	Type
Helpdesk Administrator	Can reset passwords for non-administrators and Helpdesk Administrators.	Directory	Organization	Direct	Built-in



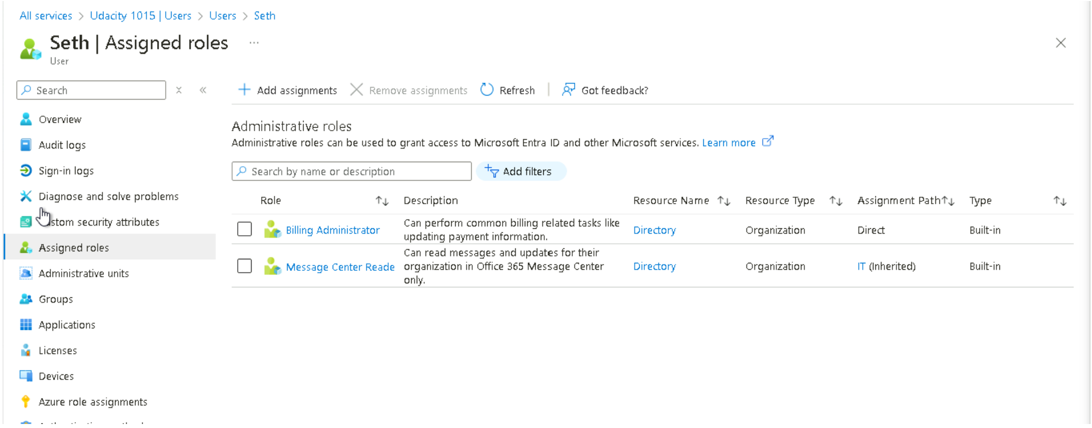
Karl | Assigned roles

User

Administrative roles

Administrative roles can be used to grant access to Microsoft Entra ID and other Microsoft services. Learn more

	Role	Description	Resource Name	Resource Type	Assignment Path	Type
□	Billing Administrator	Can perform common billing related tasks like updating payment information.	Directory	Organization	Direct	Built-in
□	Message Center Reade	Can read messages and updates for their organization in Office 365 Message Center only.	Directory	Organization	Executive (Inherited)	Built-in



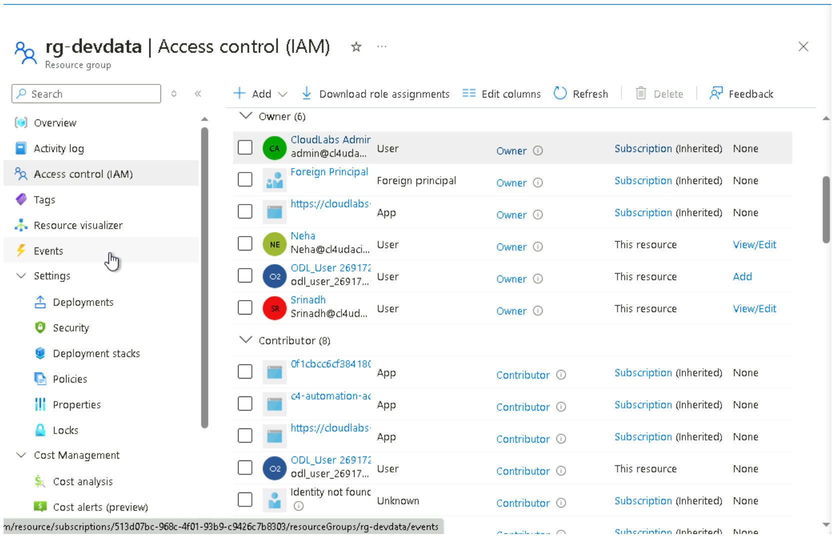
Seth | Assigned roles

User

Administrative roles

Administrative roles can be used to grant access to Microsoft Entra ID and other Microsoft services. Learn more

	Role	Description	Resource Name	Resource Type	Assignment Path	Type
□	Billing Administrator	Can perform common billing related tasks like updating payment information.	Directory	Organization	Direct	Built-in
□	Message Center Reade	Can read messages and updates for their organization in Office 365 Message Center only.	Directory	Organization	IT (Inherited)	Built-in



rg-devdata | Access control (IAM)

Resource group

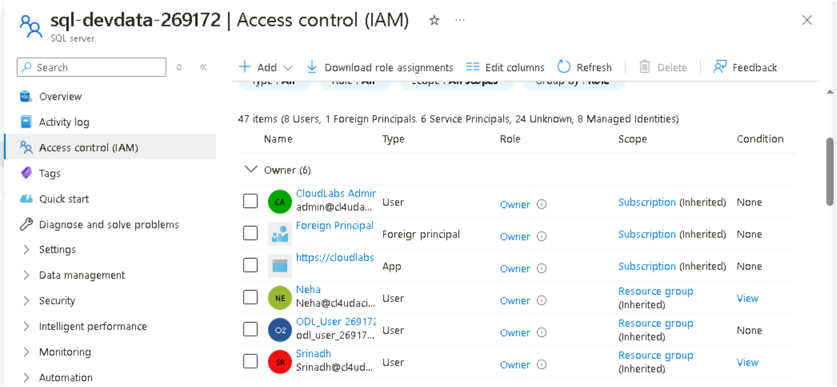
Owner (6)

□	CA	CloudLabs Admir admin@cl4uda...	User	Owner ⓘ	Subscription (Inherited)	None
□		Foreign Principal	Foreign principal	Owner ⓘ	Subscription (Inherited)	None
□		https://cloudlabs-	App	Owner ⓘ	Subscription (Inherited)	None
□	NE	Neha Neha@cl4udaci...	User	Owner ⓘ	This resource	View/Edit
□	O2	ODL_User 269172 odl_user_26917...	User	Owner ⓘ	This resource	Add
□	SR	Srinadh Srinadh@cl4ud...	User	Owner ⓘ	This resource	View/Edit

Contributor (8)

□		0f1cbcc6cf38418(	App	Contributor ⓘ	Subscription (Inherited)	None
□		c4-automation-ac	App	Contributor ⓘ	Subscription (Inherited)	None
□		https://cloudlabs-	App	Contributor ⓘ	Subscription (Inherited)	None
□	O2	ODL_User 269172 odl_user_26917...	User	Contributor ⓘ	This resource	None
□		Identity not founc ⓘ	Unknown	Contributor ⓘ	Subscription (Inherited)	None

m/resource/subscriptions/513d07bc-968c-4f01-93b9-c9426c7b8303/resourceGroups/rg-devdata/events

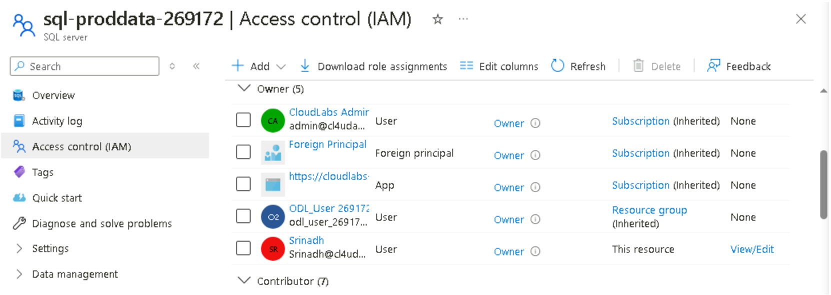


sql-devdata-269172 | Access control (IAM)

SQL server

47 items (8 Users, 1 Foreign Principals. 6 Service Principals, 24 Unknown, 8 Managed Identities)

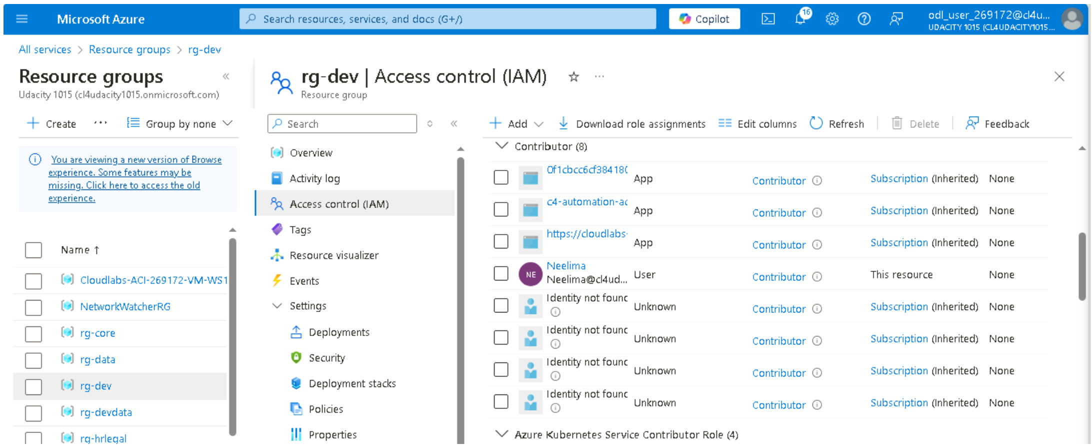
Name	Type	Role	Scope	Condition
Owner (6)				
CloudLabs Admir admin@cl4uda...	User	Owner	Subscription (Inherited)	None
Foreign Principal	Foreigr principal	Owner	Subscription (Inherited)	None
https://cloudlabs-	App	Owner	Subscription (Inherited)	None
Neha Neha@cl4udaci...	User	Owner	Resource group (Inherited)	View
ODL_User 26917: odl_user_26917...	User	Owner	Resource group (Inherited)	None
Srinadh Srinadh@cl4ud...	User	Owner	Resource group (Inherited)	View



sql-proddata-269172 | Access control (IAM)

SQL server

Owner (5)				
CloudLabs Admir admin@cl4uda...	User	Owner	Subscription (Inherited)	None
Foreign Principal	Foreign principal	Owner	Subscription (Inherited)	None
https://cloudlabs-	App	Owner	Subscription (Inherited)	None
ODL_User 26917: odl_user_26917...	User	Owner	Resource group (Inherited)	None
Srinadh Srinadh@cl4ud...	User	Owner	This resource	View/Edit
Contributor (7)				



Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
odl_user_269172@cl4u...
UDACITY 1015 (CL4UDACITY1015...
All services > Resource groups > rg-dev

Resource groups

Udacity 1015 (cl4udacity1015.onmicrosoft.com)

You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.

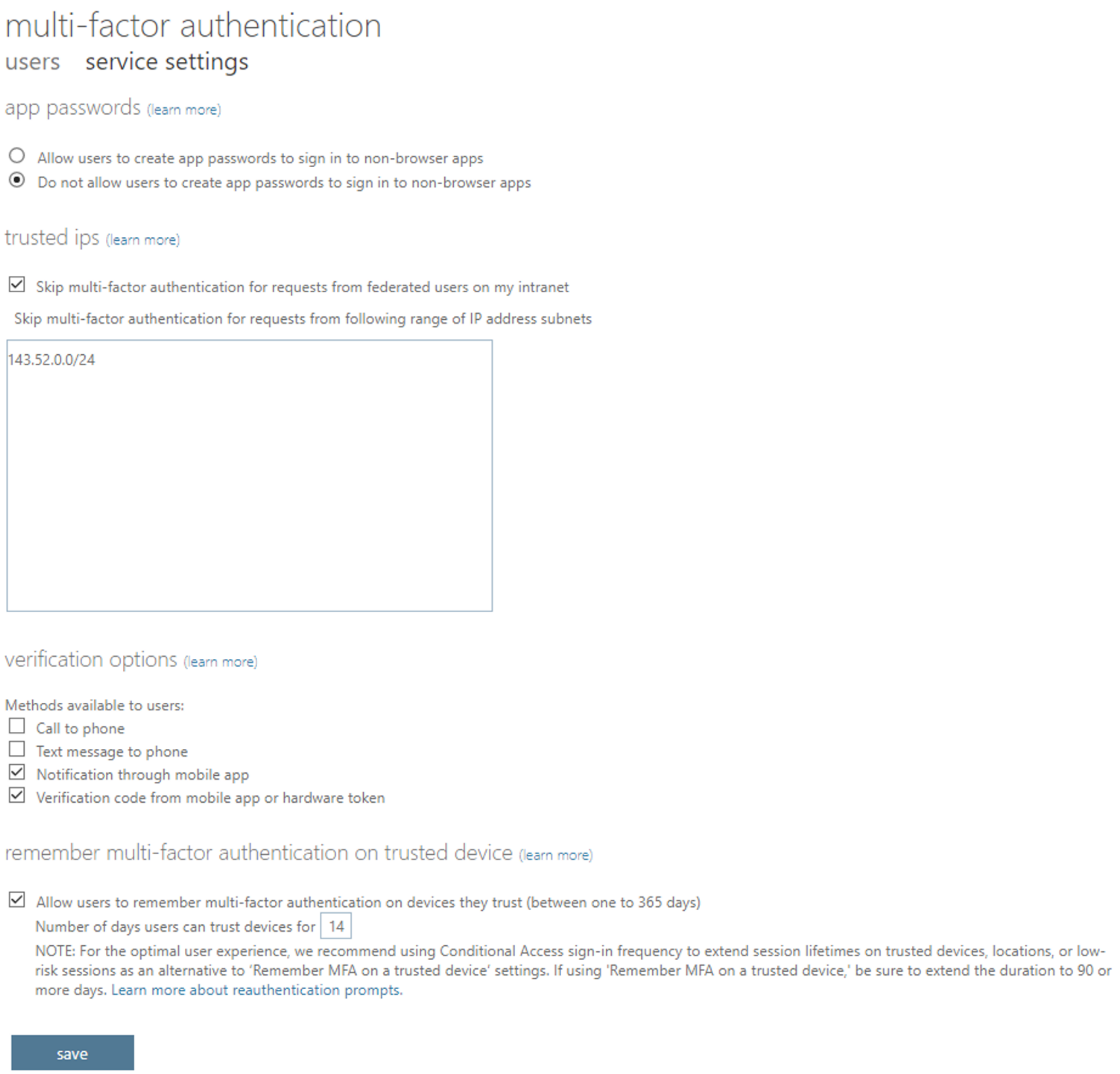
Name ↑
Cloudlabs-ACI-269172-VM-WS1
NetworkWatcherRG
rg-core
rg-data
rg-dev
rg-devdata
rg-hrlegal

rg-dev | Access control (IAM)

Resource group

Contributor (8)				
0f1cbcc6cf38418(	App	Contributor	Subscription (Inherited)	None
c4-automation-ac	App	Contributor	Subscription (Inherited)	None
https://cloudlabs-	App	Contributor	Subscription (Inherited)	None
Neelima Neelima@cl4ud...	User	Contributor	This resource	None
Identity not founc	Unknown	Contributor	Subscription (Inherited)	None
Identity not founc	Unknown	Contributor	Subscription (Inherited)	None
Identity not founc	Unknown	Contributor	Subscription (Inherited)	None
Identity not founc	Unknown	Contributor	Subscription (Inherited)	None
Azure Kubernetes Service Contributor Role (4)				

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



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

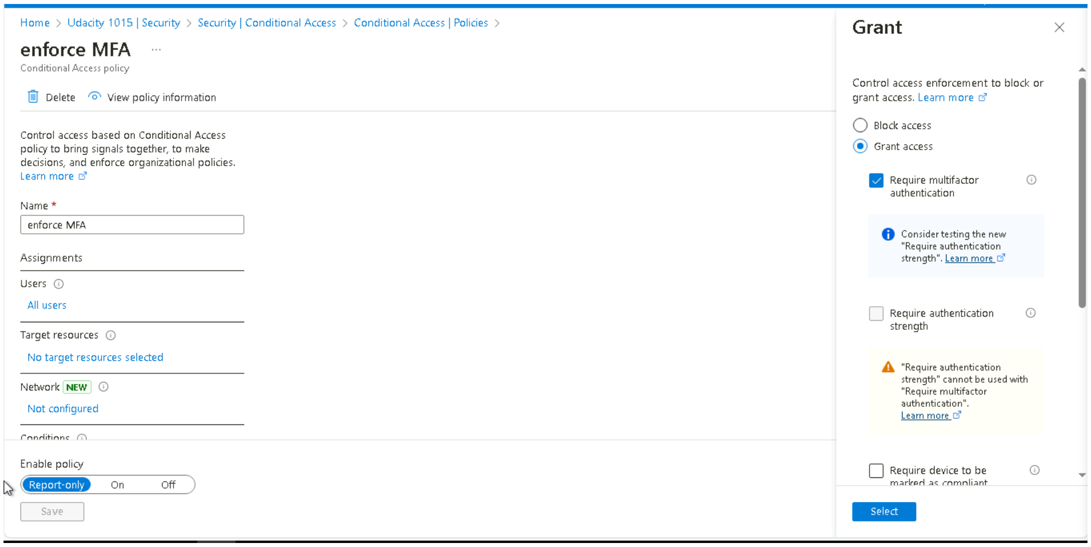
remember multi-factor authentication on trusted device (learn more)

☑ 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.

3. Proof of Conditional Access policy all users



Home > Udacity 1015 | Security > Security | Conditional Access > Conditional Access | Policies >

enforce MFA ···

Conditional Access policy

Delete | View policy information

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

enforce MFA

Assignments

Users: All users

Target resources: No target resources selected

Network NEW: Not configured

Conditions

Enable policy: [✓ Report-only] On Off

Save

Grant

Control access enforcement to block or grant access. Learn more

○ Block access

● Grant access

☑ Require multifactor authentication

Consider testing the new "Require authentication strength". Learn more

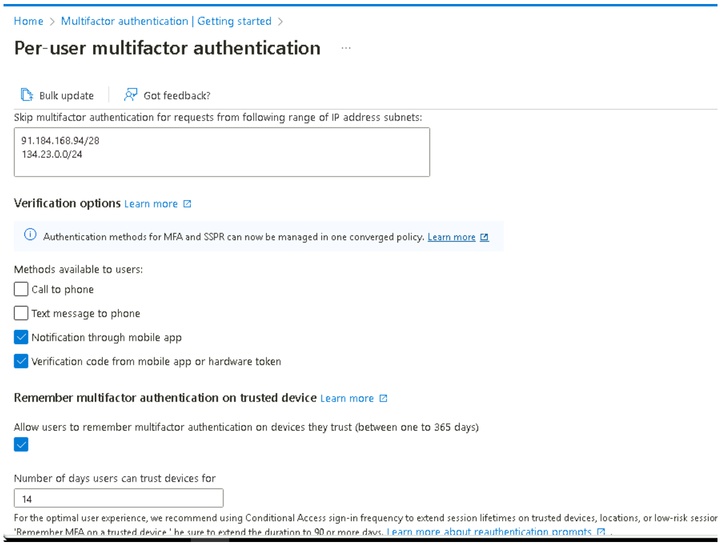
□ Require authentication strength

"Require authentication strength" cannot be used with "Require multifactor authentication". Learn more

□ Require device to be marked as compliant

Select

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



Home > Multifactor authentication | Getting started >

Per-user multifactor authentication ···

Bulk update | Got feedback?

Skip multifactor authentication for requests from following range of IP address subnets:

```
91.184.168.94/28
134.23.0.0/24
```

Verification options Learn more

Authentication methods for MFA and SSPR can now be managed in one converged policy. 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 multifactor authentication on trusted device Learn more

Allow users to remember multifactor authentication on devices they trust (between one to 365 days)

☑

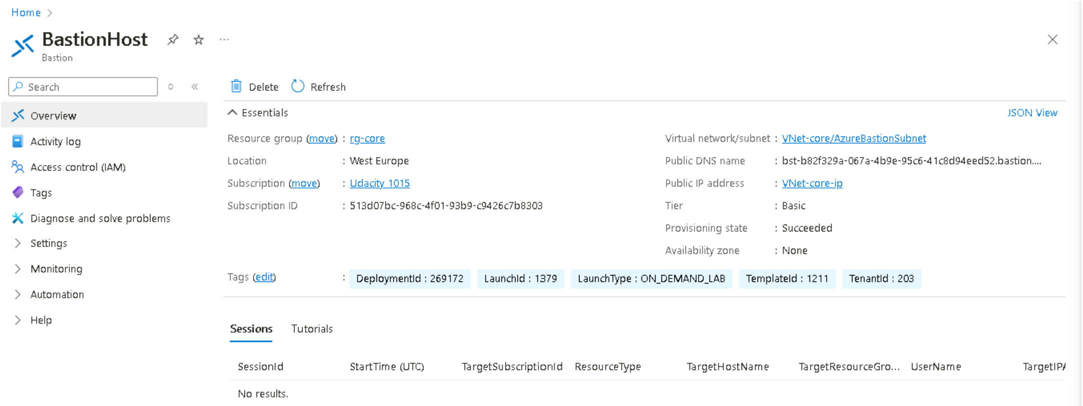
Number of days users can trust devices for

14

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

Network Security

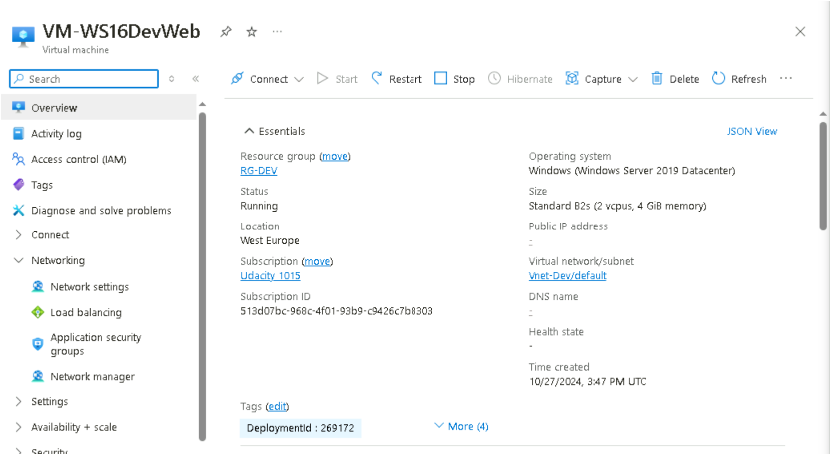
1. Bastion overview



Resource group (move) : rg-core
Location : West Europe
Subscription (move) : Udacity 1015
Subscription ID : 513d07bc-968c-4f01-93b9-c9426c7b8303
Virtual network/subnet : VNet-core/AzureBastionSubnet
Public DNS name : bst-b82f329a-067a-4b9e-95c6-41c8d94eed52.bastion....
Public IP address : VNet-core-ip
Tier : Basic
Provisioning state : Succeeded
Availability zone : None
Tags (edit) : DeploymentId : 269172 | LaunchId : 1379 | LaunchType : ON_DEMAND_LAB | TemplateId : 1211 | TenantId : 203

SessionId	StartTime (UTC)	TargetSubscriptionId	ResourceType	TargetHostName	TargetResourceGro...	UserName	TargetIP/
No results.							

2. Proof of public IP addresses removed



Resource group (move)
RG-DEV

Status
Running

Location
West Europe

Subscription (move)
Udacity 1015

Subscription ID
513d07bc-968c-4f01-93b9-c9426c7b8303

Operating system
Windows (Windows Server 2019 Datacenter)

Size
Standard B2s (2 vcpus, 4 GiB memory)

Public IP address
-

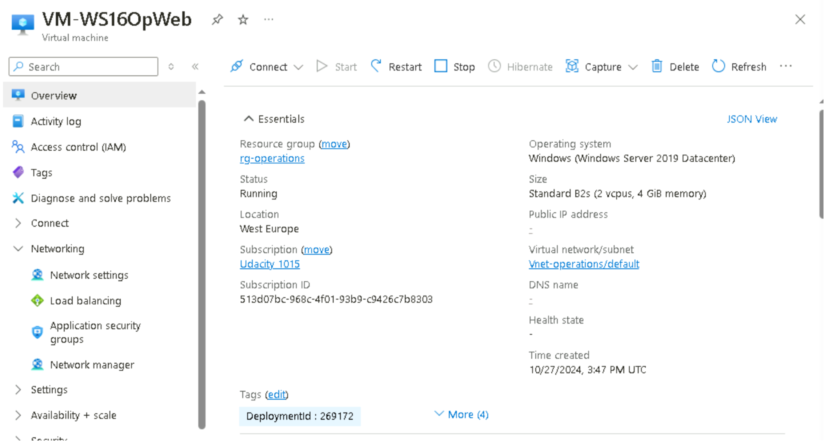
Virtual network/subnet
Vnet-Dev/default

DNS name
-

Health state
-

Time created
10/27/2024, 3:47 PM UTC

Tags (edit)
DeploymentId : 269172



Resource group (move)
rg-operations

Status
Running

Location
West Europe

Subscription (move)
Udacity 1015

Subscription ID
513d07bc-968c-4f01-93b9-c9426c7b8303

Operating system
Windows (Windows Server 2019 Datacenter)

Size
Standard B2s (2 vcpus, 4 GiB memory)

Public IP address
-

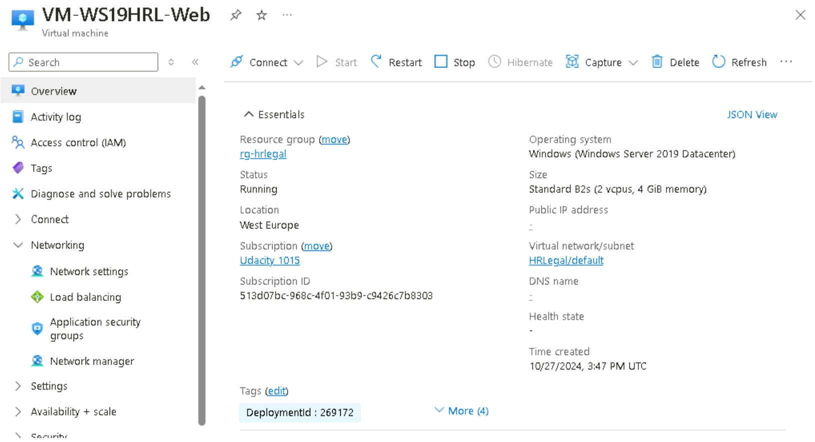
Virtual network/subnet
Vnet-operations/default

DNS name
-

Health state
-

Time created
10/27/2024, 3:47 PM UTC

Tags (edit)
DeploymentId : 269172



VM-WS19HRL-Web

Virtual machine

Essentials

Resource group (move)
rg-hrlegal

Status
Running

Location
West Europe

Subscription (move)
Udacity 1015

Subscription ID
513d07bc-968c-4f01-93b9-c9426c7b8303

Operating system
Windows (Windows Server 2019 Datacenter)

Size
Standard B2s (2 vcpus, 4 GiB memory)

Public IP address
-

Virtual network/subnet
HRLegal/default

DNS name
-

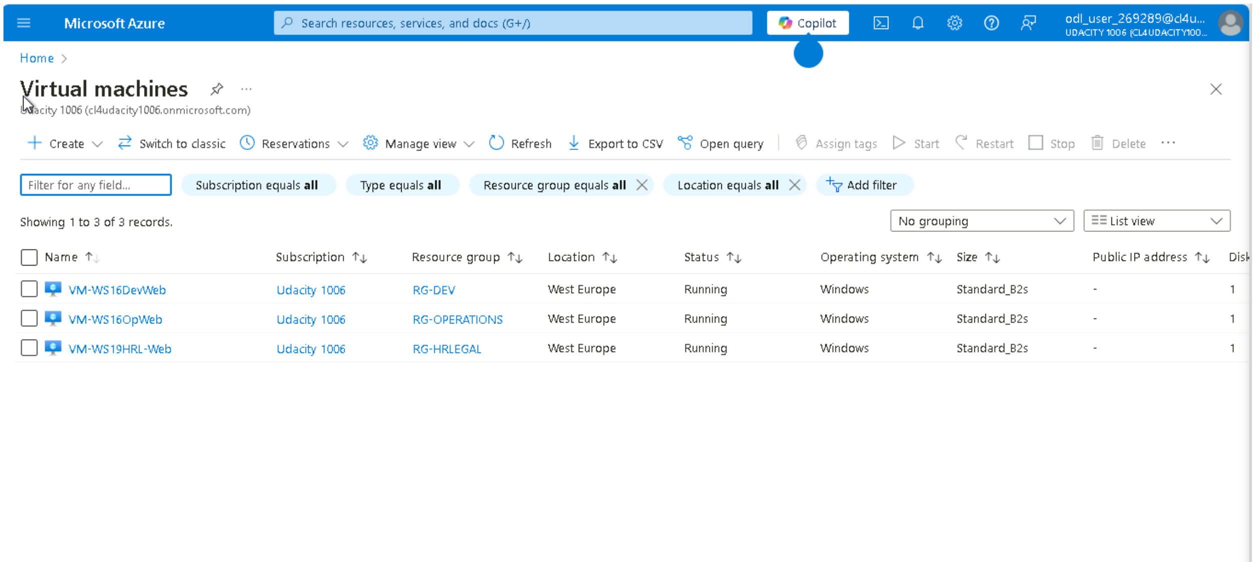
Health state
-

Time created
10/27/2024, 3:47 PM UTC

Tags (edit)
DeploymentId : 269172

Data and Encryption

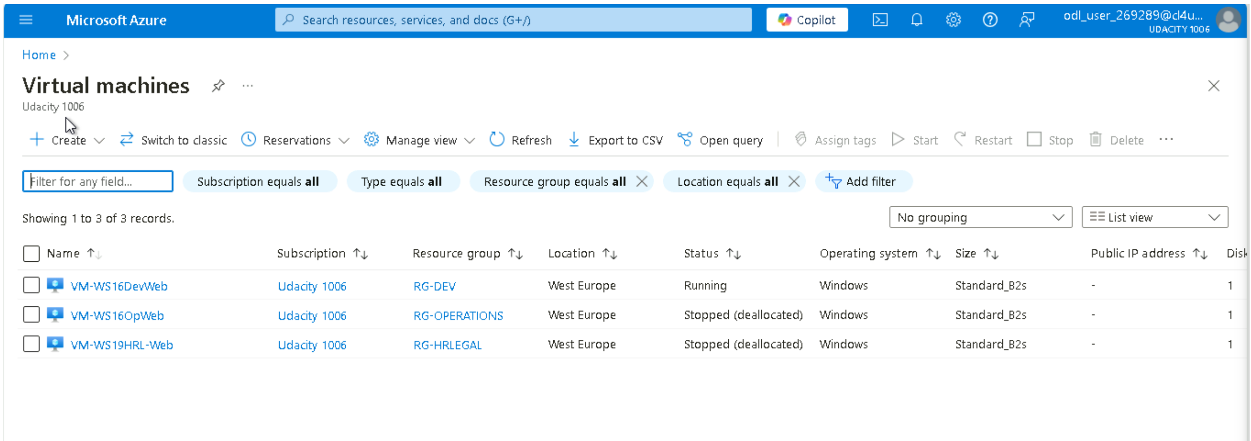
1. Proof of Encryption types for VM (devapp,OpWeb,HRL-App,OPApp, HRL-Web)



Showing 1 to 3 of 3 records.

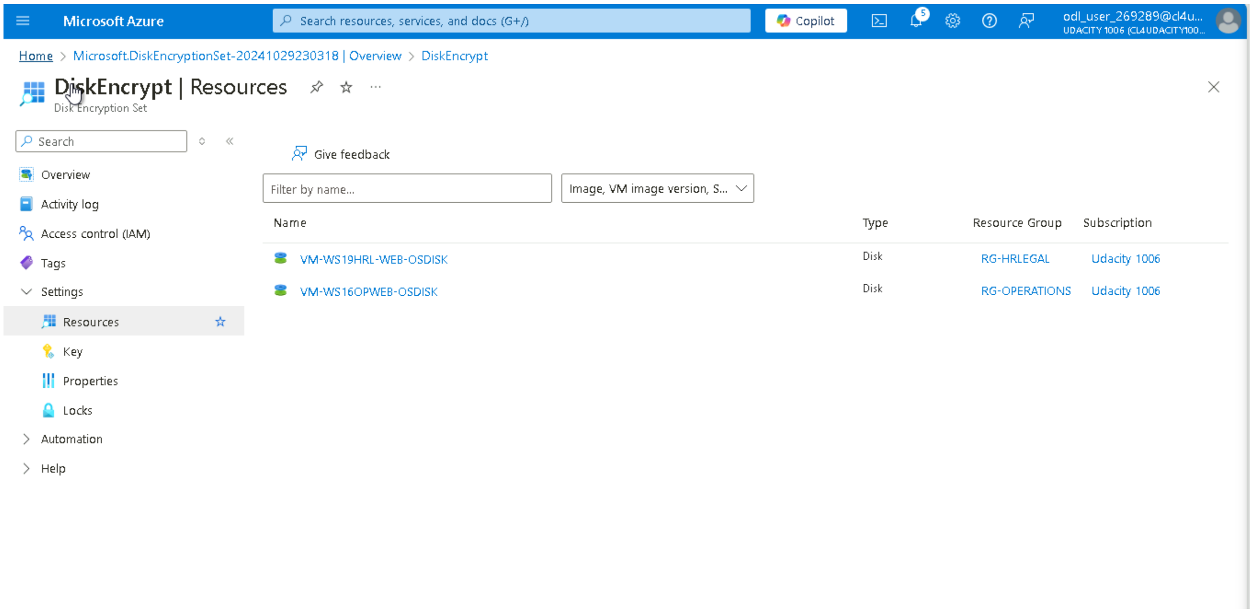
Name	Subscription	Resource group	Location	Status	Operating system	Size	Public IP address	Disk
VM-WS16DevWeb	Udacity 1006	RG-DEV	West Europe	Running	Windows	Standard_B2s	-	1
VM-WS16OpWeb	Udacity 1006	RG-OPERATIONS	West Europe	Running	Windows	Standard_B2s	-	1
VM-WS19HRL-Web	Udacity 1006	RG-HRLEGAL	West Europe	Running	Windows	Standard_B2s	-	1

To enable encryption over the available VMs , we must stop them first. I can stop only two of the above VMs (OpWeb and HRL-Web) here. If I stopped the VM DevWeb, the offered Azure Environment Box will auto restart and get freeze.



Showing 1 to 3 of 3 records.

Name	Subscription	Resource group	Location	Status	Operating system	Size	Public IP address	Disk
VM-WS16DevWeb	Udacity 1006	RG-DEV	West Europe	Running	Windows	Standard_B2s	-	1
VM-WS16OpWeb	Udacity 1006	RG-OPERATIONS	West Europe	Stopped (deallocated)	Windows	Standard_B2s	-	1
VM-WS19HRL-Web	Udacity 1006	RG-HRLEGAL	West Europe	Stopped (deallocated)	Windows	Standard_B2s	-	1



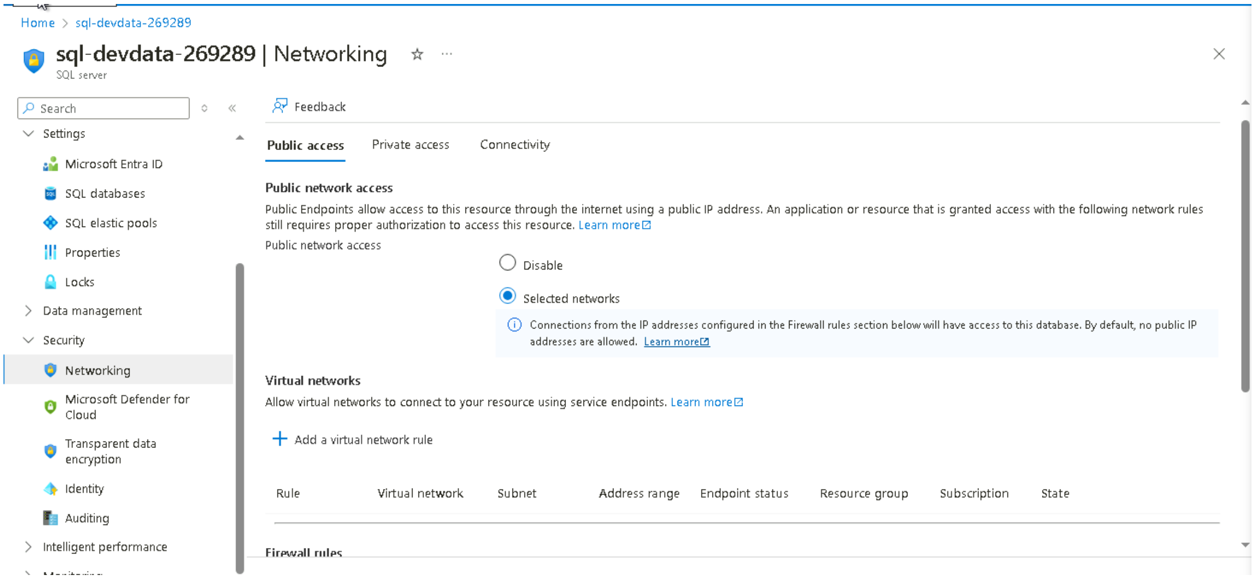
Home > Microsoft.DiskEncryptionSet-20241029230318 | Overview > DiskEncrypt

DiskEncrypt | Resources

Disk Encryption Set

Name	Type	Resource Group	Subscription
VM-WS19HRL-WEB-OSDISK	Disk	RG-HRLEGAL	Udacity 1006
VM-WS16OPWEB-OSDISK	Disk	RG-OPERATIONS	Udacity 1006

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



Home > sql-devdata-269289

sql-devdata-269289 | Networking

SQL server

Public network access

Public Endpoints allow access to this resource through the internet using a public IP address. An application or resource that is granted access with the following network rules still requires proper authorization to access this resource. Learn more

Public network access

○ Disable

● Selected networks

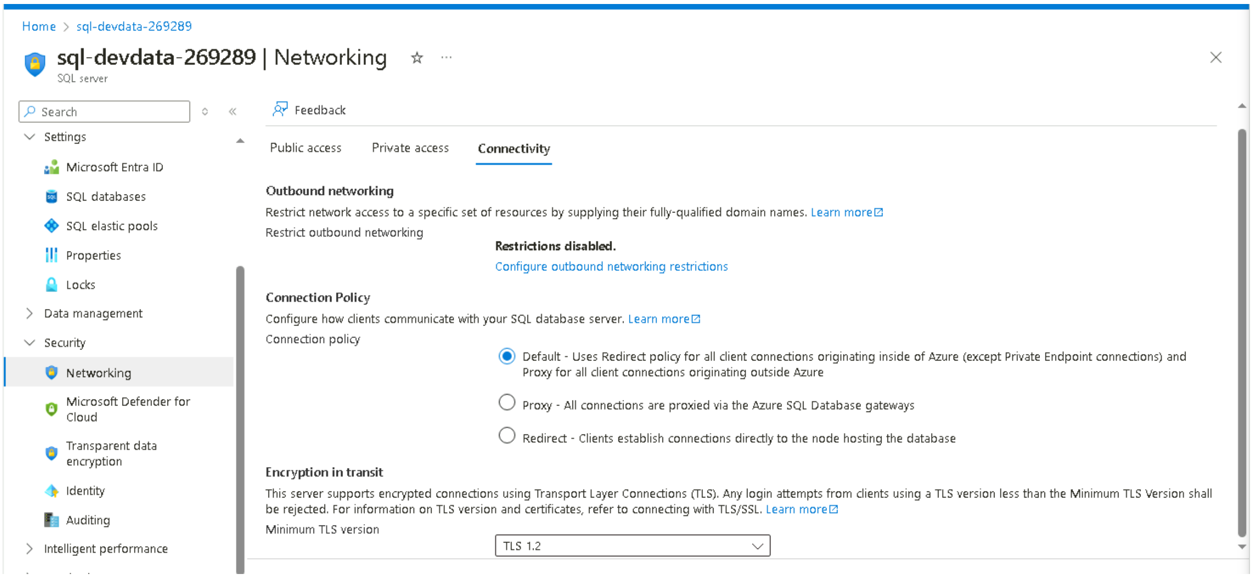
Connections from the IP addresses configured in the Firewall rules section below will have access to this database. By default, no public IP addresses are allowed. Learn more

Virtual networks

Allow virtual networks to connect to your resource using service endpoints. Learn more

Rule	Virtual network	Subnet	Address range	Endpoint status	Resource group	Subscription	State

Firewall rules



Home > sql-devdata-269289

sql-devdata-269289 | Networking

SQL server

Outbound networking

Restrict network access to a specific set of resources by supplying their fully-qualified domain names. Learn more

Restrict outbound networking

Restrictions disabled.

Configure outbound networking restrictions

Connection Policy

Configure how clients communicate with your SQL database server. Learn more

Connection policy

● Default - Uses Redirect policy for all client connections originating inside of Azure (except Private Endpoint connections) and Proxy for all client connections originating outside Azure

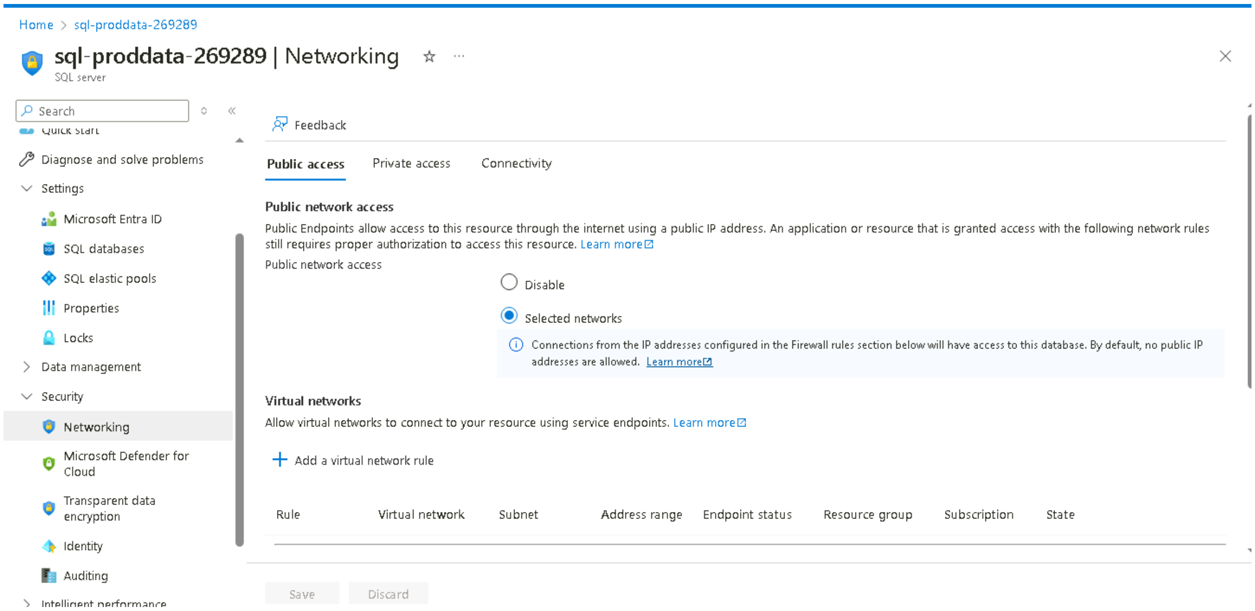
○ Proxy - All connections are proxied via the Azure SQL Database gateways

○ Redirect - Clients establish connections directly to the node hosting the database

Encryption in transit

This server supports encrypted connections using Transport Layer Connections (TLS). Any login attempts from clients using a TLS version less than the Minimum TLS Version shall be rejected. For information on TLS version and certificates, refer to connecting with TLS/SSL. Learn more

Minimum TLS version: TLS 1.2



Home > sql-proddata-269289

sql-proddata-269289 | Networking

SQL server

Public network access

Public Endpoints allow access to this resource through the internet using a public IP address. An application or resource that is granted access with the following network rules still requires proper authorization to access this resource. Learn more

Public network access

○ Disable

● Selected networks

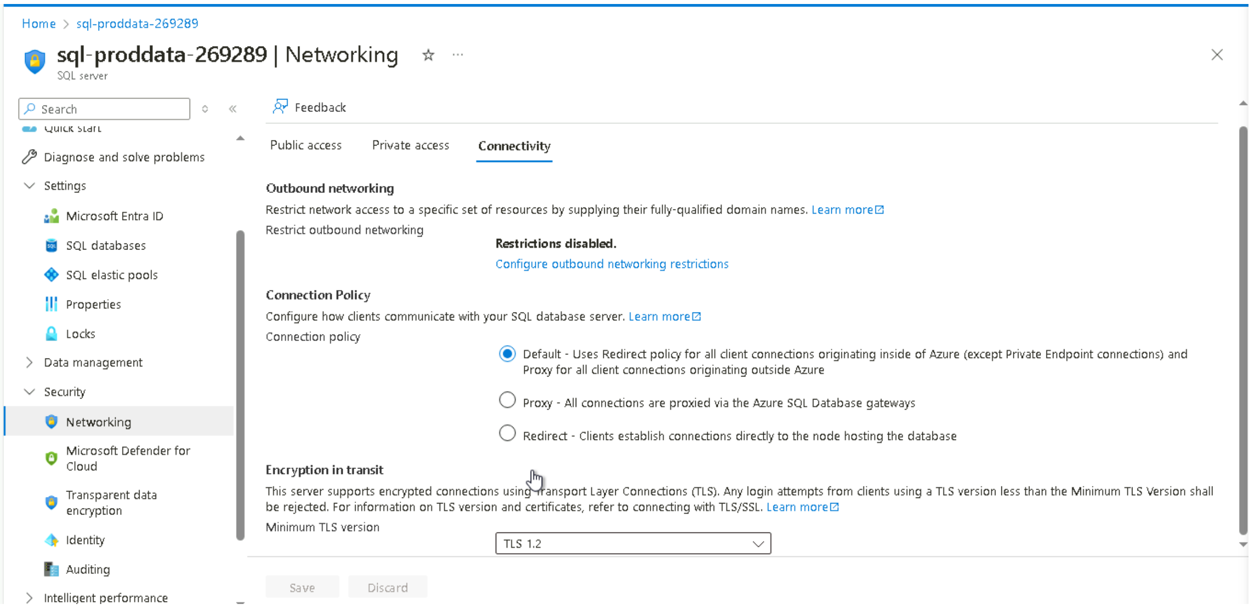
Connections from the IP addresses configured in the Firewall rules section below will have access to this database. By default, no public IP addresses are allowed. Learn more

Virtual networks

Allow virtual networks to connect to your resource using service endpoints. Learn more

+ Add a virtual network rule

Rule	Virtual network	Subnet	Address range	Endpoint status	Resource group	Subscription	State



sql-proddata-269289 | Networking

SQL server

Outbound networking

Restrict network access to a specific set of resources by supplying their fully-qualified domain names. Learn more

Restrict outbound networking

Restrictions disabled.

Configure outbound networking restrictions

Connection Policy

Configure how clients communicate with your SQL database server. Learn more

Connection policy

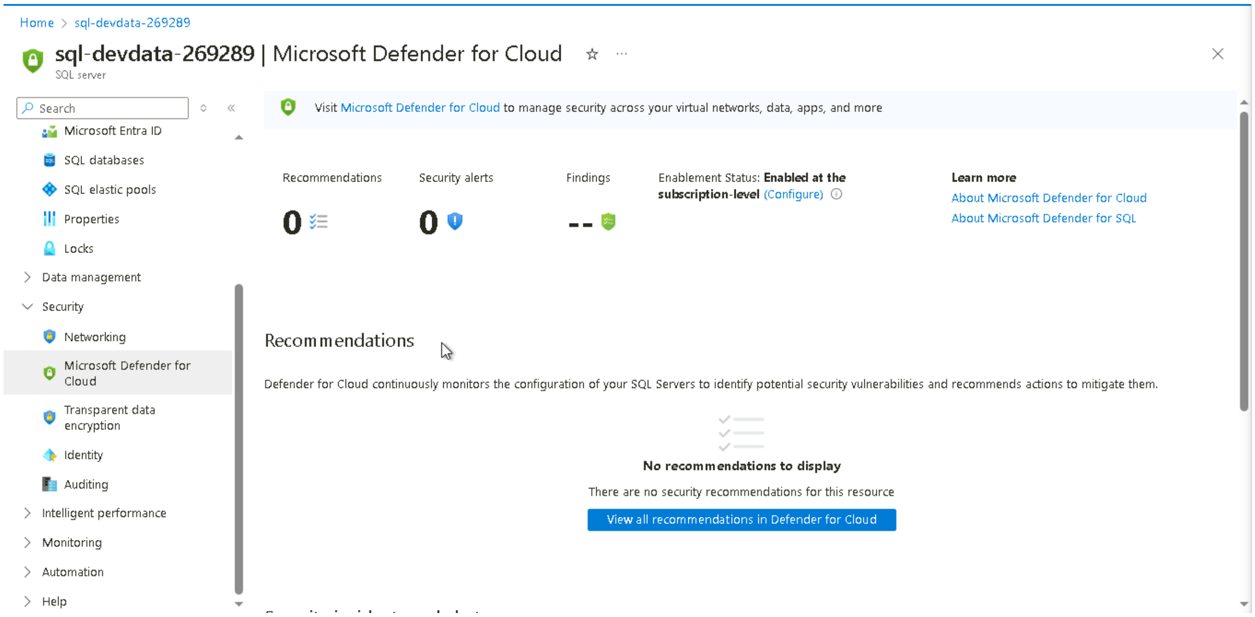
- ● Default - Uses Redirect policy for all client connections originating inside of Azure (except Private Endpoint connections) and Proxy for all client connections originating outside Azure
- ○ Proxy - All connections are proxied via the Azure SQL Database gateways
- ○ Redirect - Clients establish connections directly to the node hosting the database

Encryption in transit

This server supports encrypted connections using Transport Layer Connections (TLS). Any login attempts from clients using a TLS version less than the Minimum TLS Version shall be rejected. For information on TLS version and certificates, refer to connecting with TLS/SSL. Learn more

Minimum TLS version: TLS 1.2

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



sql-devdata-269289 | Microsoft Defender for Cloud

SQL server

Visit Microsoft Defender for Cloud to manage security across your virtual networks, data, apps, and more

Recommendations	Security alerts	Findings	Enablement Status: **Enabled at the subscription-level** (Configure)
0	0	--	

Learn more

About Microsoft Defender for Cloud

About Microsoft Defender for SQL

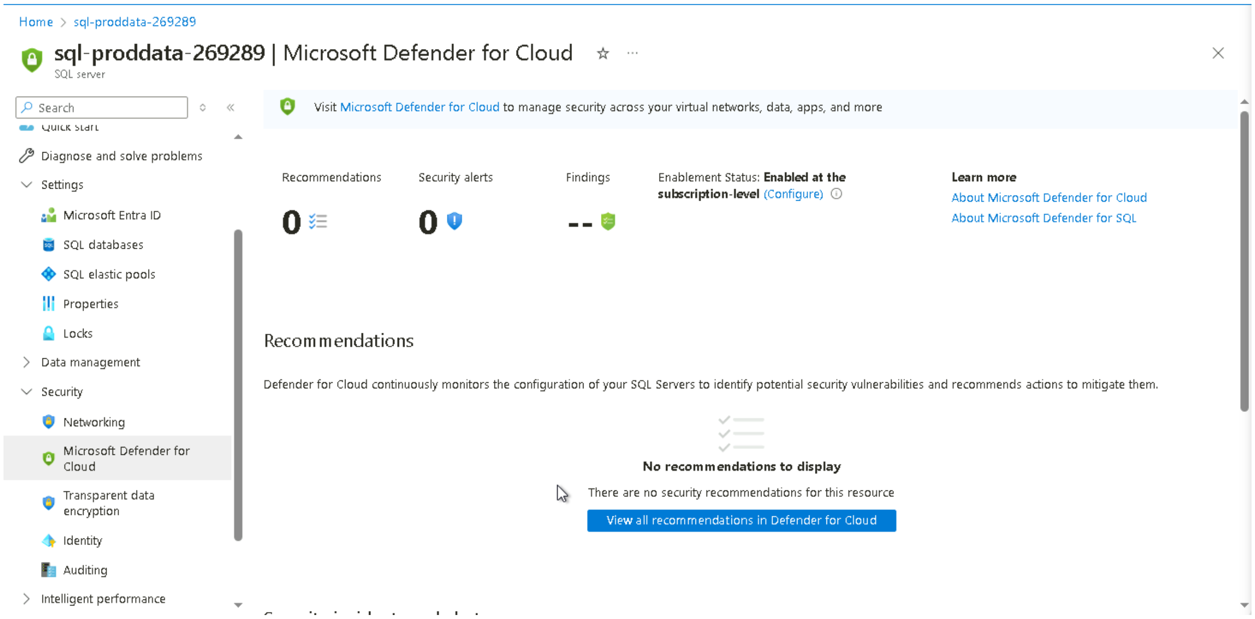
Recommendations

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



Visit Microsoft Defender for Cloud to manage security across your virtual networks, data, apps, and more

Recommendations	Security alerts	Findings	Enablement Status: **Enabled at the subscription-level** (Configure)
0	0	--	

Learn more
About Microsoft Defender for Cloud
About Microsoft Defender for SQL

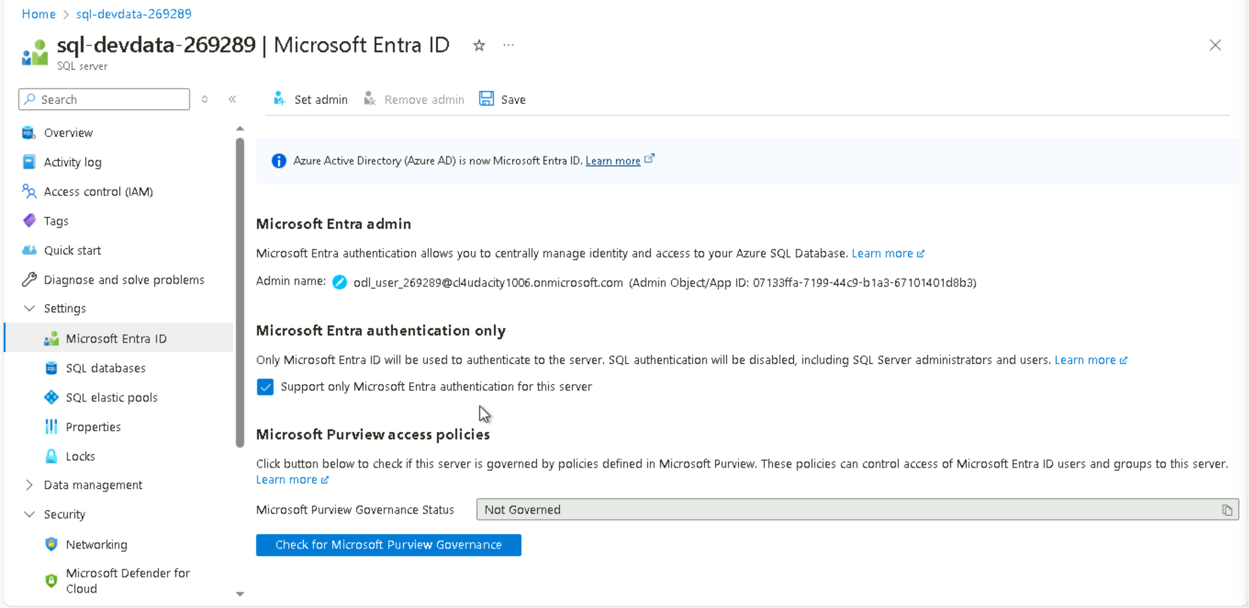
Recommendations

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

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



Azure Active Directory (Azure AD) is now Microsoft Entra ID. Learn more

Microsoft Entra admin

Microsoft Entra authentication allows you to centrally manage identity and access to your Azure SQL Database. Learn more

Admin name: odl_user_269289@cl4udacity1006.onmicrosoft.com (Admin Object/App ID: 07133ffa-7199-44c9-b1a3-67101401d8b3)

Microsoft Entra authentication only

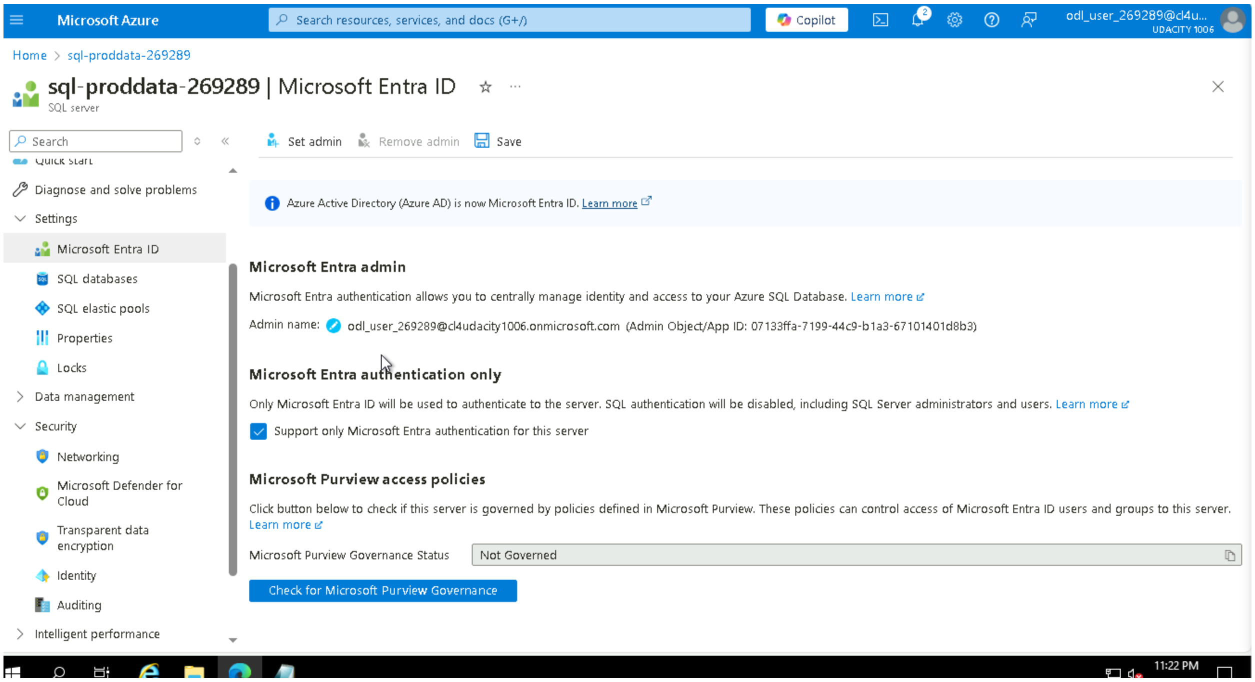
Only Microsoft Entra ID will be used to authenticate to the server. SQL authentication will be disabled, including SQL Server administrators and users. Learn more

☑ Support only Microsoft Entra authentication for this server

Microsoft Purview access policies

Click button below to check if this server is governed by policies defined in Microsoft Purview. These policies can control access of Microsoft Entra ID users and groups to this server. Learn more

Microsoft Purview Governance Status: Not Governed


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
odl_user_269289@cl4u...
UDACITY 1006
Home > sql-proddata-269289

sql-proddata-269289 | Microsoft Entra ID

SQL server

Azure Active Directory (Azure AD) is now Microsoft Entra ID. Learn more

Microsoft Entra admin

Microsoft Entra authentication allows you to centrally manage identity and access to your Azure SQL Database. Learn more

Admin name: odl_user_269289@cl4udacity1006.onmicrosoft.com (Admin Object/App ID: 07133ffa-7199-44c9-b1a3-67101401d8b3)

Microsoft Entra authentication only

Only Microsoft Entra ID will be used to authenticate to the server. SQL authentication will be disabled, including SQL Server administrators and users. Learn more

☑ Support only Microsoft Entra authentication for this server

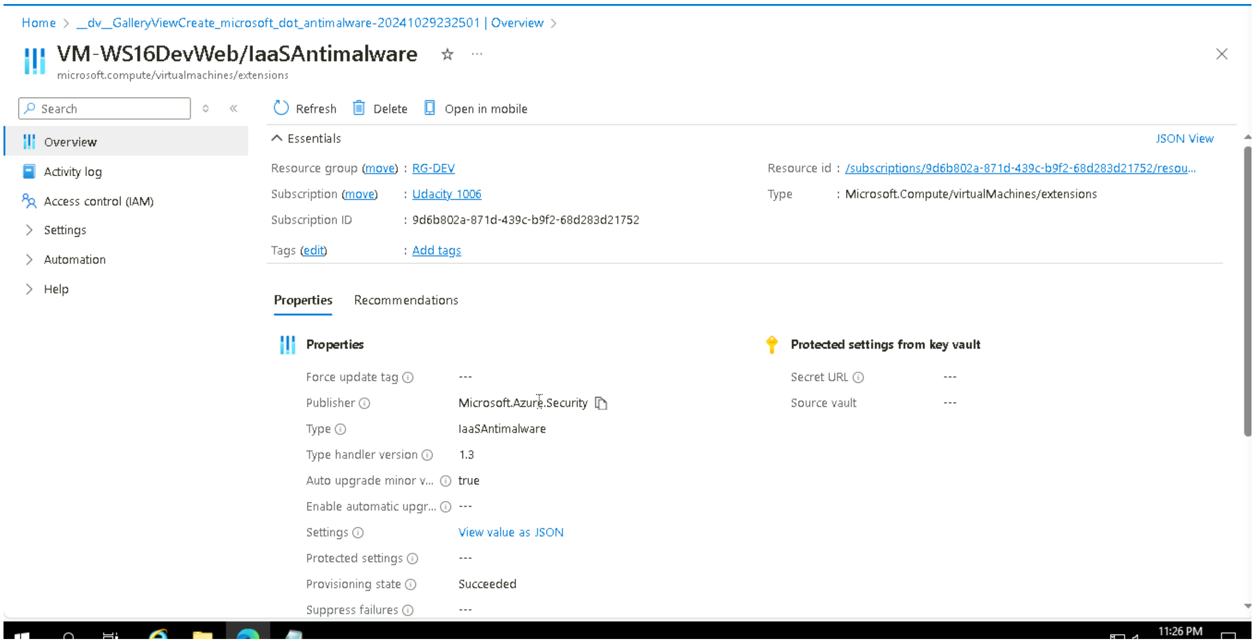
Microsoft Purview access policies

Click button below to check if this server is governed by policies defined in Microsoft Purview. These policies can control access of Microsoft Entra ID users and groups to this server. Learn more

Microsoft Purview Governance Status: Not Governed

Cloud Protection

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


Home > __dv__GalleryViewCreate_microsoft_dot_antimalware-20241029232501 | Overview >

VM-WS16DevWeb/IaaSAntimalware

microsoft.compute/virtualmachines/extensions

Resource group (move) : RG-DEV

Subscription (move) : Udacity 1006

Subscription ID : 9d6b802a-871d-439c-b9f2-68d283d21752

Tags (edit) : Add tags

Resource id : /subscriptions/9d6b802a-871d-439c-b9f2-68d283d21752/resou...

Type : Microsoft.Compute/virtualMachines/extensions

Properties

Force update tag ---

Publisher Microsoft.Azure.Security

Type IaaSAntimalware

Type handler version 1.3

Auto upgrade minor v... true

Enable automatic upgr... ---

Settings View value as JSON

Protected settings ---

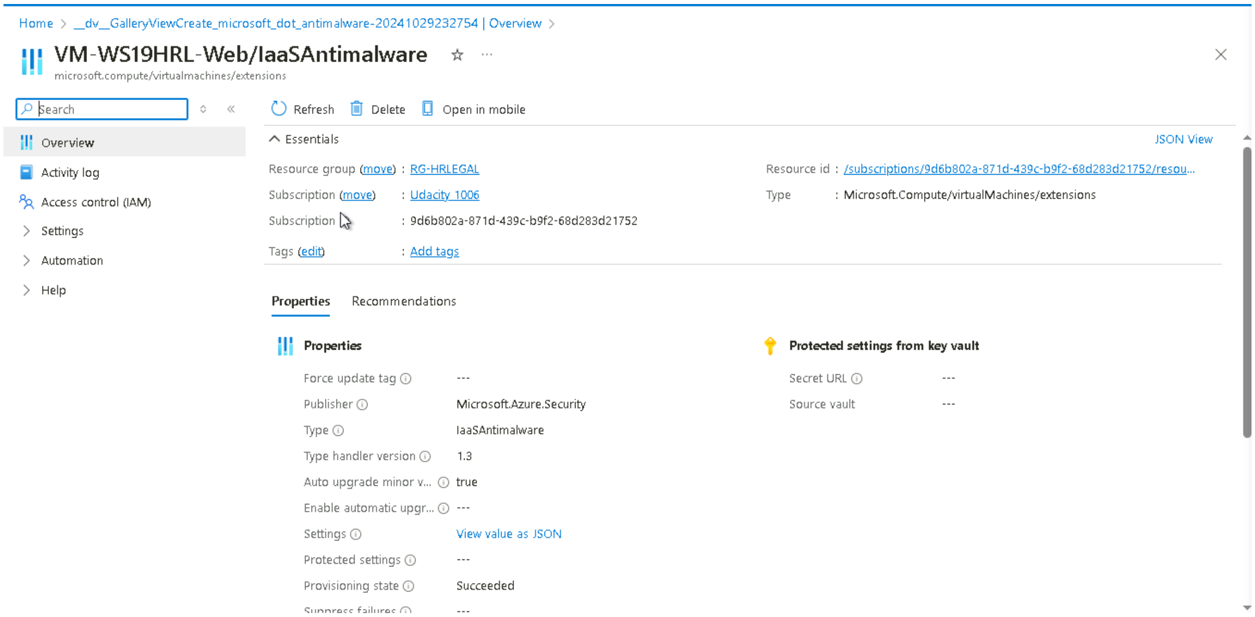
Provisioning state Succeeded

Suppress failures ---

Protected settings from key vault

Secret URL ---

Source vault ---


Home > __dv__GalleryViewCreate_microsoft_dot_antimalware-20241029232754 | Overview >

VM-WS19HRL-Web/IaaSAntimalware

microsoft.compute/virtualmachines/extensions

Resource group (move) : RG-HRLEGAL

Subscription (move) : Udacity 1006

Subscription : 9d6b802a-871d-439c-b9f2-68d283d21752

Tags (edit) : Add tags

Resource id : /subscriptions/9d6b802a-871d-439c-b9f2-68d283d21752/resou...

Type : Microsoft.Compute/virtualMachines/extensions

Properties

Force update tag ---

Publisher Microsoft.Azure.Security

Type IaaSAntimalware

Type handler version 1.3

Auto upgrade minor v... true

Enable automatic upgr... ---

Settings View value as JSON

Protected settings ---

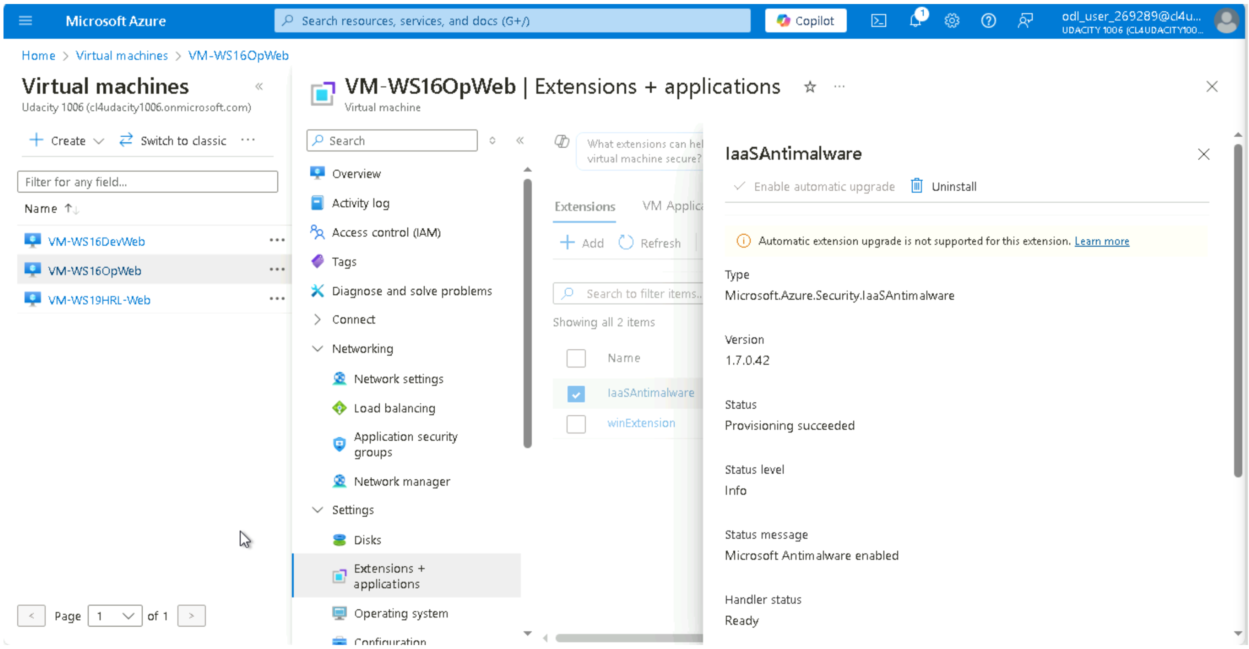
Provisioning state Succeeded

Suppress failures ---

Protected settings from key vault

Secret URL ---

Source vault ---



IaaSAntimalware

Automatic extension upgrade is not supported for this extension. Learn more

Type
Microsoft.Azure.Security.IaaSAntimalware

Version
1.7.0.42

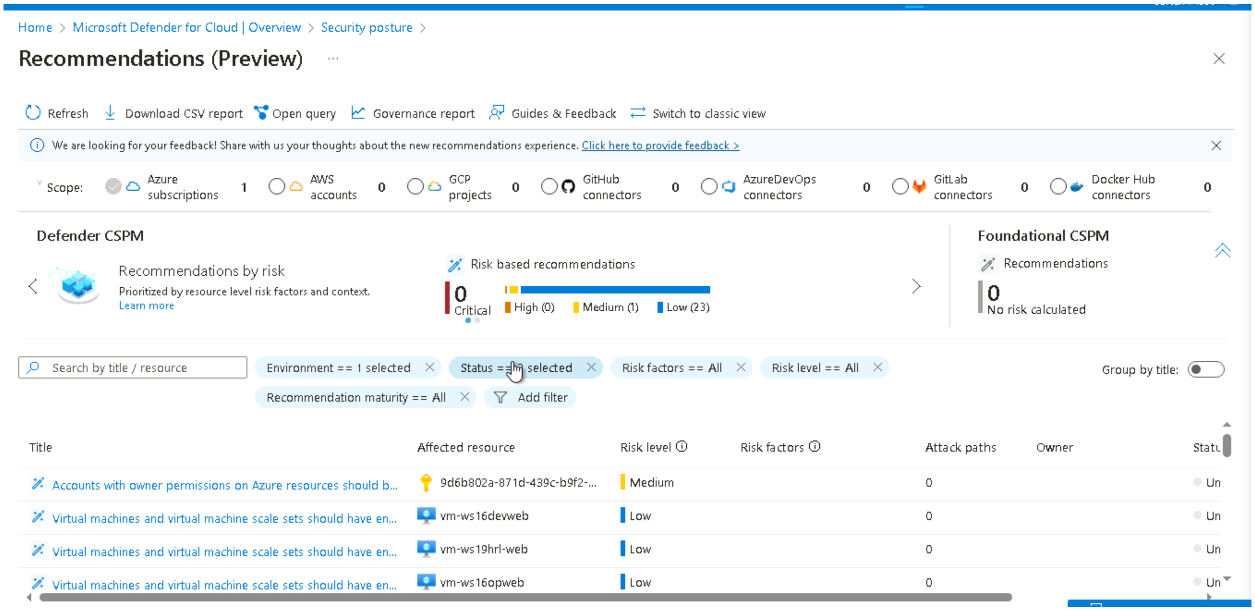
Status
Provisioning succeeded

Status level
Info

Status message
Microsoft Antimalware enabled

Handler status
Ready

2. Recommendations



Recommendations (Preview)

We are looking for your feedback! Share with us your thoughts about the new recommendations experience. Click here to provide feedback >

Scope: Azure subscriptions 1 | AWS accounts 0 | GCP projects 0 | GitHub connectors 0 | AzureDevOps connectors 0 | GitLab connectors 0 | Docker Hub connectors 0

Defender CSPM

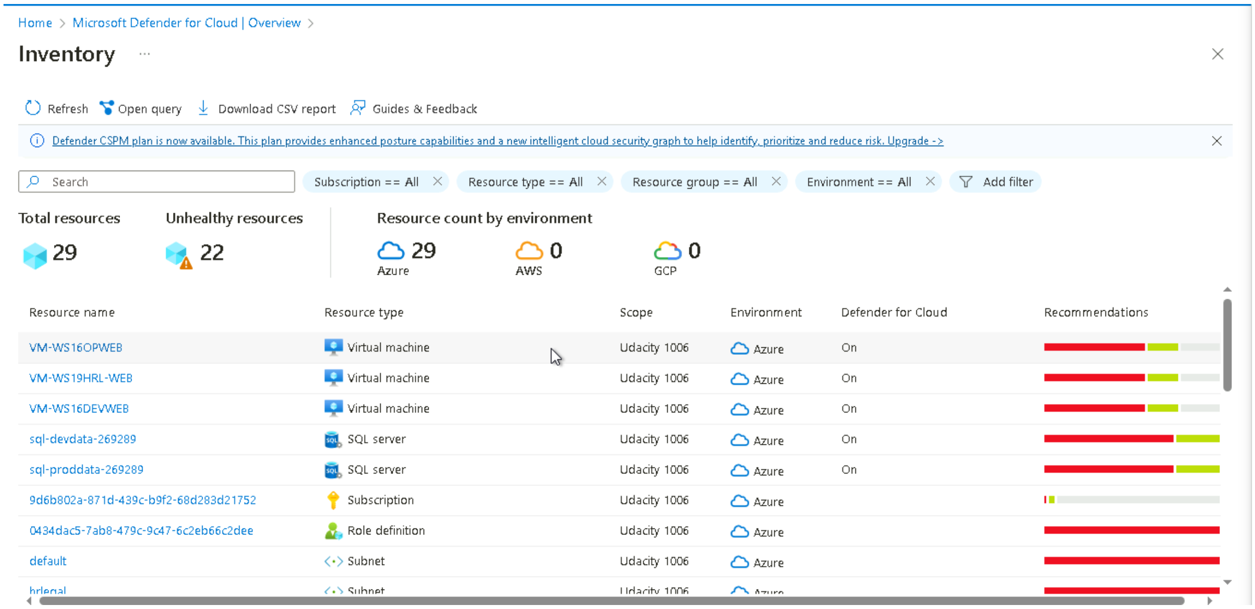
Recommendations by risk
Prioritized by resource level risk factors and context.
Learn more

Risk based recommendations
0 Critical
High (0) Medium (1) Low (23)

Foundational CSPM
Recommendations
0
No risk calculated

Environment == 1 selected | Status == 1 selected | Risk factors == All | Risk level == All | Recommendation maturity == All

Title	Affected resource	Risk level	Risk factors	Attack paths	Owner	Statu
Accounts with owner permissions on Azure resources should b...	9d6b802a-871d-439c-b9f2-...	Medium		0		Un
Virtual machines and virtual machine scale sets should have en...	vm-ws16devweb	Low		0		Un
Virtual machines and virtual machine scale sets should have en...	vm-ws19hrl-web	Low		0		Un
Virtual machines and virtual machine scale sets should have en...	vm-ws16opweb	Low		0		Un



Home > Microsoft Defender for Cloud | Overview >

Inventory ...

Defender CSPM plan is now available. This plan provides enhanced posture capabilities and a new intelligent cloud security graph to help identify, prioritize and reduce risk. Upgrade ->

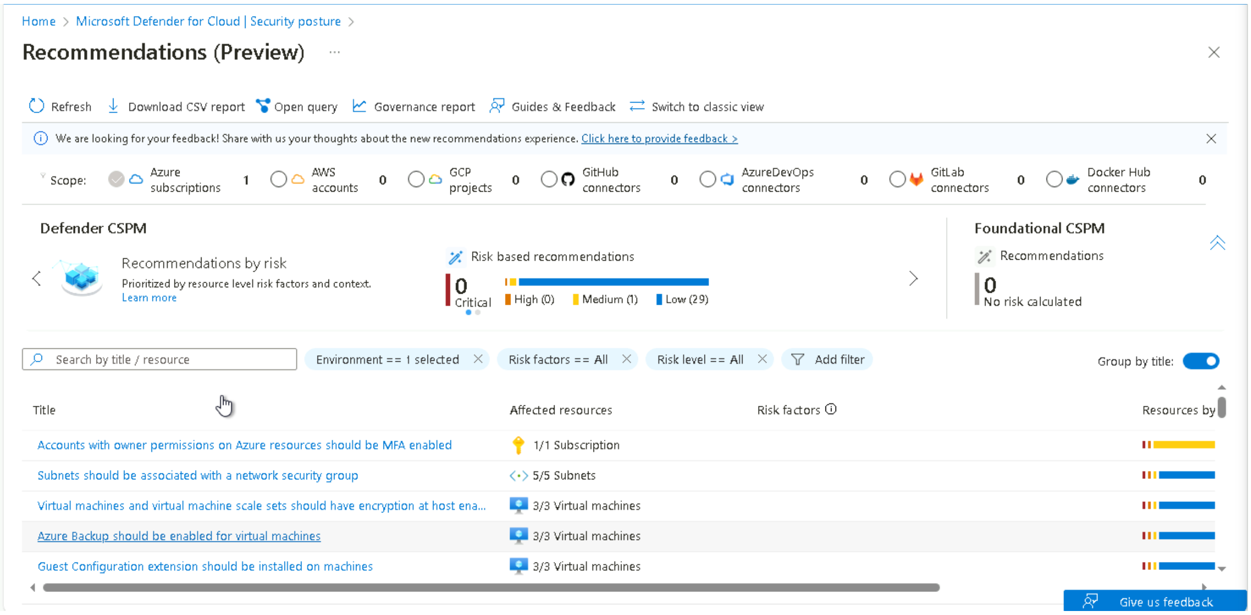
Subscription == All ✕ Resource type == All ✕ Resource group == All ✕ Environment == All ✕ Add filter

Total resources: 29

Unhealthy resources: 22

Resource count by environment: 29 Azure, 0 AWS, 0 GCP

Resource name	Resource type	Scope	Environment	Defender for Cloud	Recommendations
VM-WS16OPWEB	Virtual machine	Udacity 1006	Azure	On	
VM-WS19HRL-WEB	Virtual machine	Udacity 1006	Azure	On	
VM-WS16DEVWEB	Virtual machine	Udacity 1006	Azure	On	
sql-devdata-269289	SQL server	Udacity 1006	Azure	On	
sql-proddata-269289	SQL server	Udacity 1006	Azure	On	
9d6b802a-871d-439c-b9f2-68d283d21752	Subscription	Udacity 1006	Azure		
0434dac5-7ab8-479c-9c47-6c2eb66c2dee	Role definition	Udacity 1006	Azure		
default	Subnet	Udacity 1006	Azure		
hrlegal	Subnet	Udacity 1006	Azure		



Home > Microsoft Defender for Cloud | Security posture >

Recommendations (Preview) ...

We are looking for your feedback! Share with us your thoughts about the new recommendations experience. Click here to provide feedback >

Scope: ● Azure subscriptions 1 ○ AWS accounts 0 ○ GCP projects 0 ○ GitHub connectors 0 ○ AzureDevOps connectors 0 ○ GitLab connectors 0 ○ Docker Hub connectors 0

Defender CSPM

Recommendations by risk

Prioritized by resource level risk factors and context.
Learn more

Risk based recommendations

0 Critical | High (0) | Medium (1) | Low (29)

Foundational CSPM

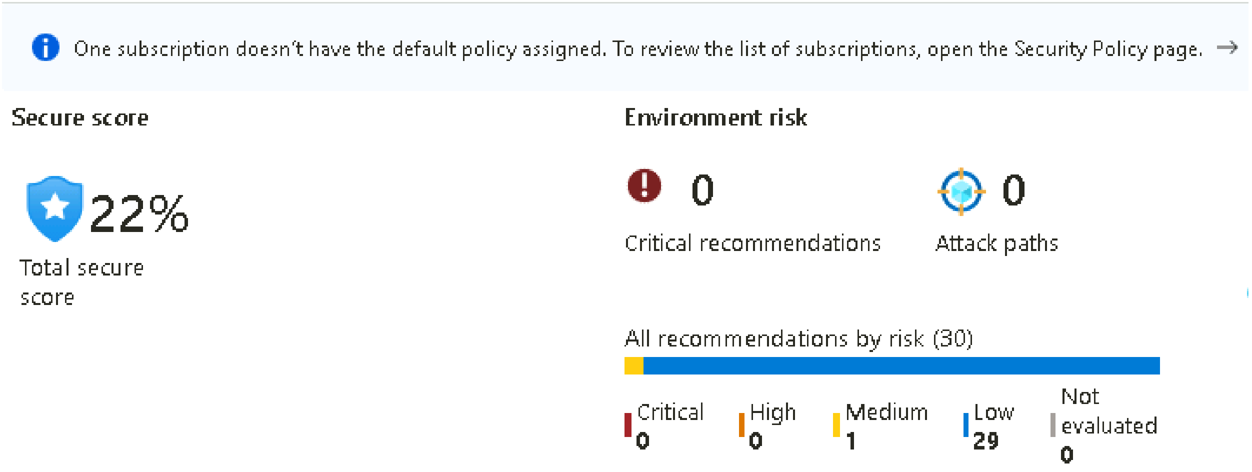
Recommendations

0 No risk calculated

Environment == 1 selected ✕ Risk factors == All ✕ Risk level == All ✕ Add filter

Group by title: ●

Title	Affected resources	Risk factors	Resources by
Accounts with owner permissions on Azure resources should be MFA enabled	1/1 Subscription		
Subnets should be associated with a network security group	5/5 Subnets		
Virtual machines and virtual machine scale sets should have encryption at host ena...	3/3 Virtual machines		
Azure Backup should be enabled for virtual machines	3/3 Virtual machines		
Guest Configuration extension should be installed on machines	3/3 Virtual machines		



One subscription doesn't have the default policy assigned. To review the list of subscriptions, open the Security Policy page. →

Secure score

22%
Total secure score

Environment risk

0
Critical recommendations

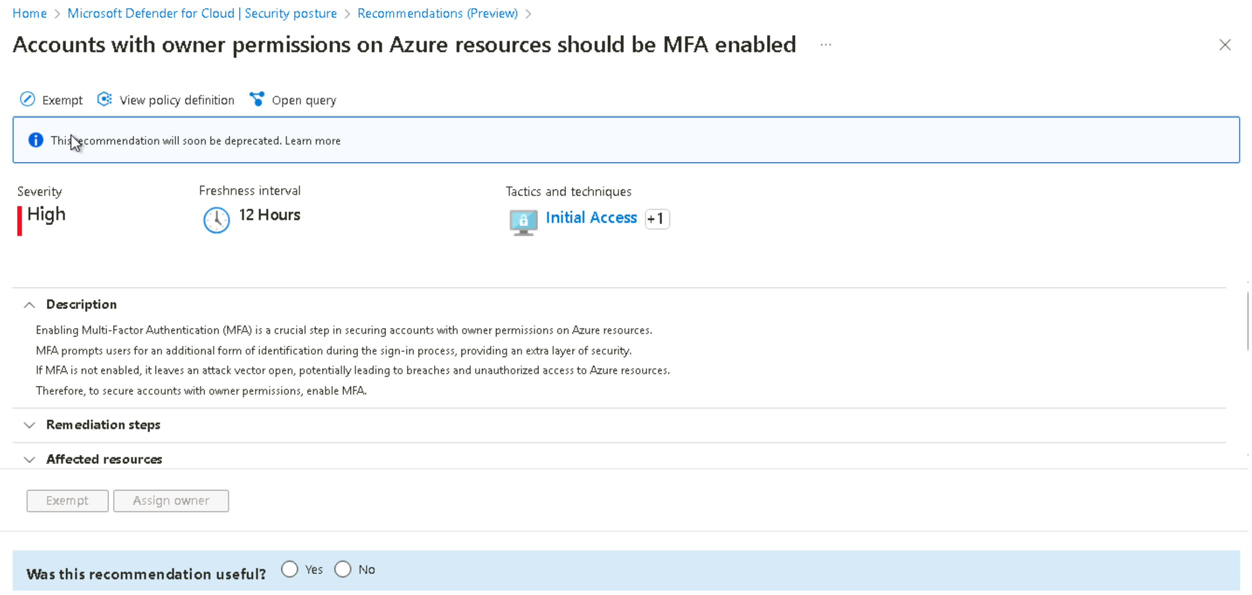
0
Attack paths

All recommendations by risk (30)

Critical	High	Medium	Low	Not evaluated
0	0	1	29	0

1 medium risk and other 29 are Low.

First risk to be address is related to MFA



Home > Microsoft Defender for Cloud | Security posture > Recommendations (Preview) >

Accounts with owner permissions on Azure resources should be MFA enabled ···

This recommendation will soon be deprecated. Learn more

Severity	Freshness interval	Tactics and techniques
High	12 Hours	Initial Access +1

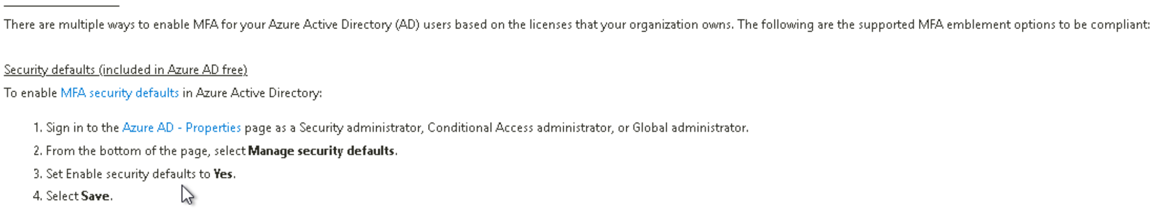
Description

Enabling Multi-Factor Authentication (MFA) is a crucial step in securing accounts with owner permissions on Azure resources.
MFA prompts users for an additional form of identification during the sign-in process, providing an extra layer of security.
If MFA is not enabled, it leaves an attack vector open, potentially leading to breaches and unauthorized access to Azure resources.
Therefore, to secure accounts with owner permissions, enable MFA.

Remediation steps

Affected resources

Was this recommendation useful? ○ Yes ○ No

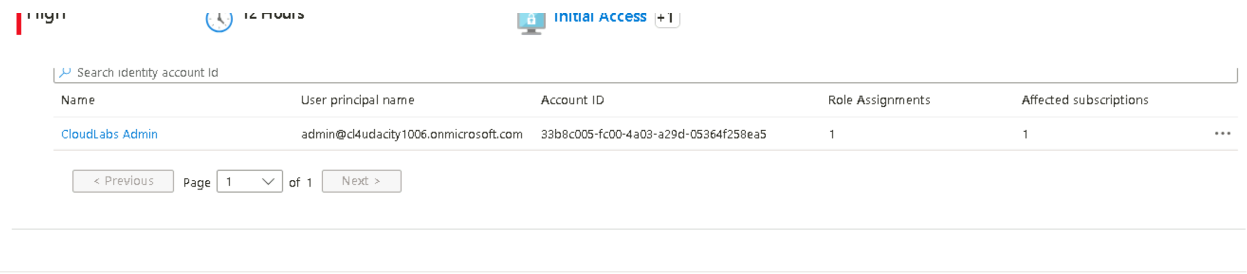


There are multiple ways to enable MFA for your Azure Active Directory (AD) users based on the licenses that your organization owns. The following are the supported MFA emblement options to be compliant:

Security defaults (included in Azure AD free)

To enable MFA security defaults in Azure Active Directory:

1. Sign in to the Azure AD - Properties page as a Security administrator, Conditional Access administrator, or Global administrator.
2. From the bottom of the page, select **Manage security defaults**.
3. Set Enable security defaults to **Yes**.
4. Select **Save**.



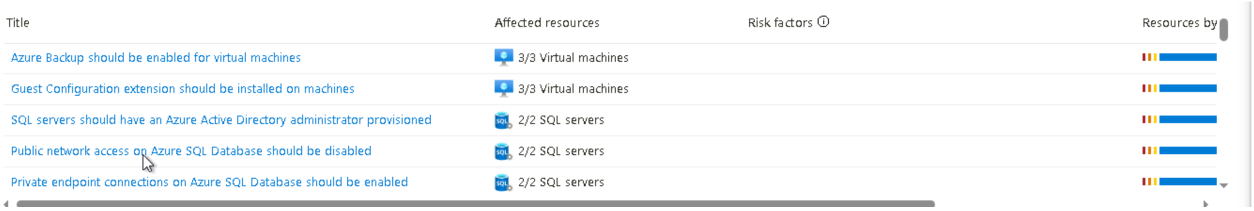
Name	User principal name	Account ID	Role Assignments	Affected subscriptions
CloudLabs Admin	admin@cl4udacity1006.onmicrosoft.com	33b8c005-fc00-4a03-a29d-05364f258ea5	1	1

Recommendation 1 :

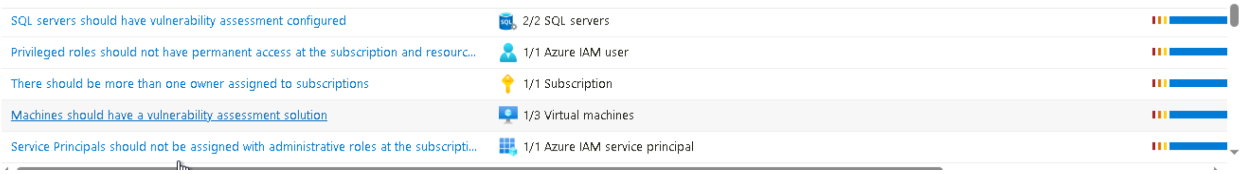
MFA is not set to CloudLab Admin. We should set that in priority to improve the secure score.

Enable MFA for Owner Accounts: Multi-Factor Authentication (MFA) is crucial for owner accounts, as it adds an extra layer of security against unauthorized access to resources with high privileges, reducing the risk of breaches.

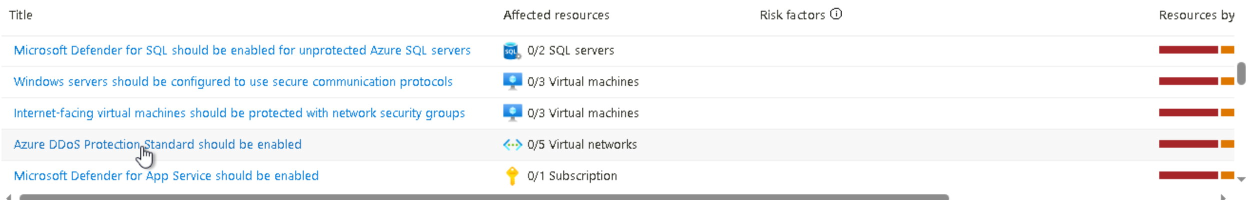
Other Low Risk Level recommendations are



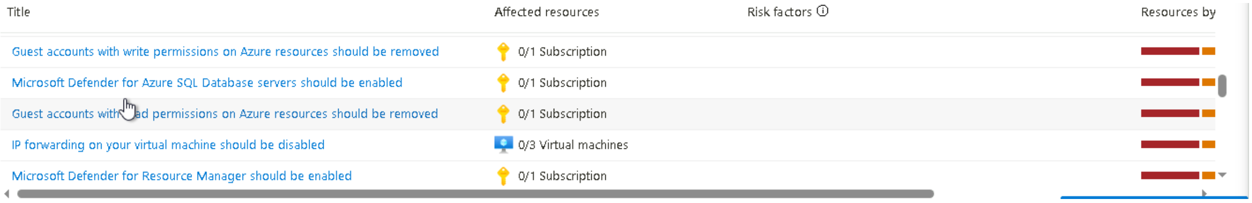
Title	Affected resources	Risk factors	Resources by
Azure Backup should be enabled for virtual machines	3/3 Virtual machines		
Guest Configuration extension should be installed on machines	3/3 Virtual machines		
SQL servers should have an Azure Active Directory administrator provisioned	2/2 SQL servers		
Public network access on Azure SQL Database should be disabled	2/2 SQL servers		
Private endpoint connections on Azure SQL Database should be enabled	2/2 SQL servers		



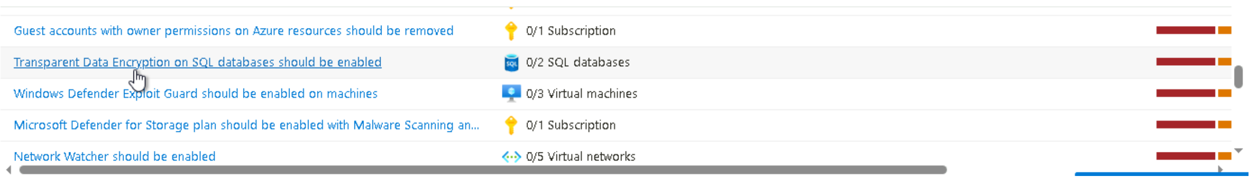
SQL servers should have vulnerability assessment configured	2/2 SQL servers	
Privileged roles should not have permanent access at the subscription and resourc...	1/1 Azure IAM user	
There should be more than one owner assigned to subscriptions	1/1 Subscription	
Machines should have a vulnerability assessment solution	1/3 Virtual machines	
Service Principals should not be assigned with administrative roles at the subscripti...	1/1 Azure IAM service principal	



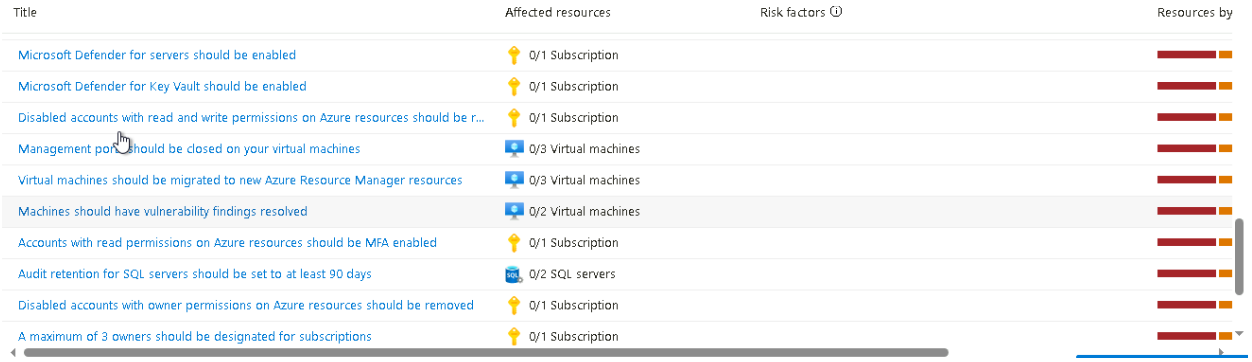
Title	Affected resources	Risk factors	Resources by
Microsoft Defender for SQL should be enabled for unprotected Azure SQL servers	0/2 SQL servers		
Windows servers should be configured to use secure communication protocols	0/3 Virtual machines		
Internet-facing virtual machines should be protected with network security groups	0/3 Virtual machines		
Azure DDoS Protection Standard should be enabled	0/5 Virtual networks		
Microsoft Defender for App Service should be enabled	0/1 Subscription		



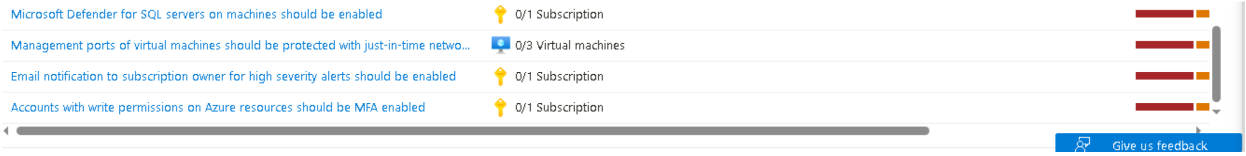
Title	Affected resources	Risk factors ⓘ	Resources by
Guest accounts with write permissions on Azure resources should be removed	0/1 Subscription		
Microsoft Defender for Azure SQL Database servers should be enabled	0/1 Subscription		
Guest accounts with read permissions on Azure resources should be removed	0/1 Subscription		
IP forwarding on your virtual machine should be disabled	0/3 Virtual machines		
Microsoft Defender for Resource Manager should be enabled	0/1 Subscription		



Guest accounts with owner permissions on Azure resources should be removed	0/1 Subscription		
Transparent Data Encryption on SQL databases should be enabled	0/2 SQL databases		
Windows Defender Exploit Guard should be enabled on machines	0/3 Virtual machines		
Microsoft Defender for Storage plan should be enabled with Malware Scanning an...	0/1 Subscription		
Network Watcher should be enabled	0/5 Virtual networks		



Title	Affected resources	Risk factors ⓘ	Resources by
Microsoft Defender for servers should be enabled	0/1 Subscription		
Microsoft Defender for Key Vault should be enabled	0/1 Subscription		
Disabled accounts with read and write permissions on Azure resources should be r...	0/1 Subscription		
Management ports should be closed on your virtual machines	0/3 Virtual machines		
Virtual machines should be migrated to new Azure Resource Manager resources	0/3 Virtual machines		
Machines should have vulnerability findings resolved	0/2 Virtual machines		
Accounts with read permissions on Azure resources should be MFA enabled	0/1 Subscription		
Audit retention for SQL servers should be set to at least 90 days	0/2 SQL servers		
Disabled accounts with owner permissions on Azure resources should be removed	0/1 Subscription		
A maximum of 3 owners should be designated for subscriptions	0/1 Subscription		



Microsoft Defender for SQL servers on machines should be enabled	0/1 Subscription		
Management ports of virtual machines should be protected with just-in-time netwo...	0/3 Virtual machines		
Email notification to subscription owner for high severity alerts should be enabled	0/1 Subscription		
Accounts with write permissions on Azure resources should be MFA enabled	0/1 Subscription		

Recommendation 2 :

Enable Azure Backup for VMs: Regular backups safeguard virtual machines from data loss due to accidental deletion, ransomware, or other disruptions, ensuring business continuity and data recovery.

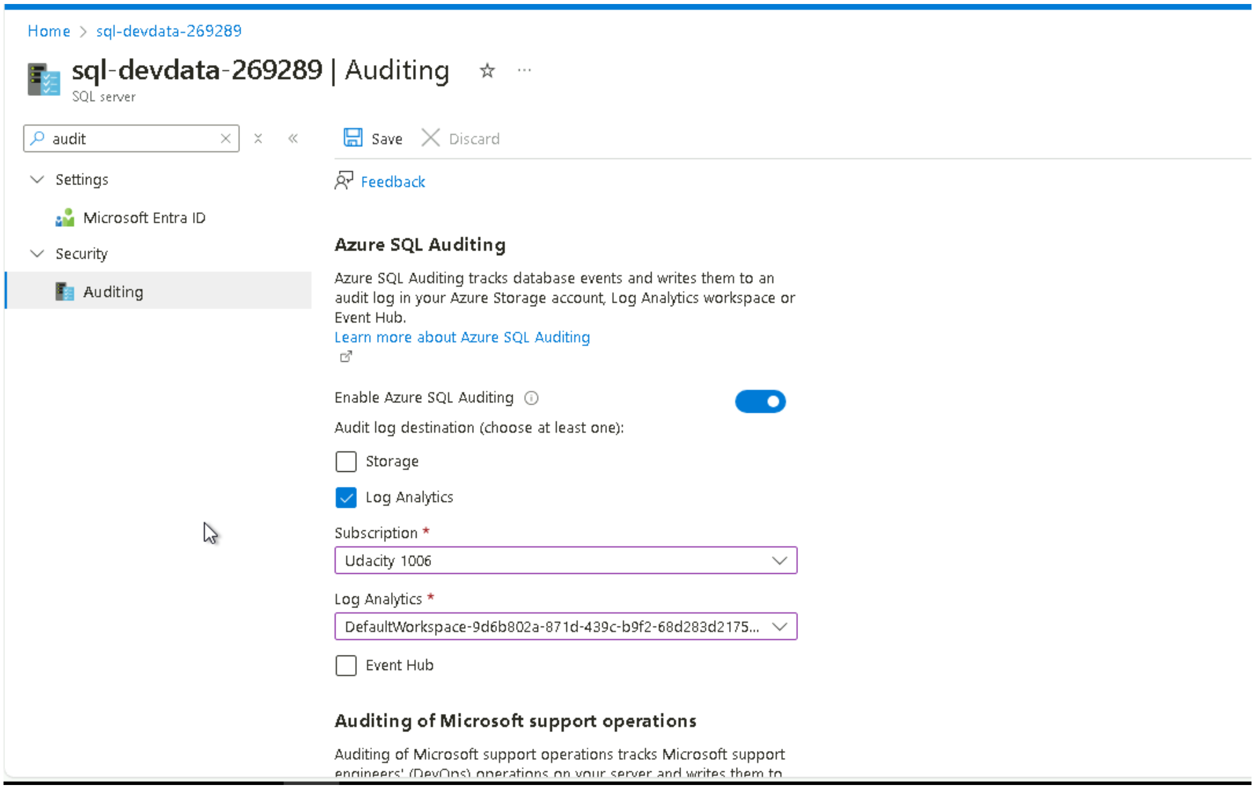
Recommendation 3 :

Implement SQL Server Vulnerability Assessment: A vulnerability assessment detects and addresses security flaws in SQL servers, minimizing the risk of data breaches and compliance violations by identifying misconfigurations and potential attack vectors.

We can always click on each of the risk to know the affected resources details and remediation steps.

Monitoring

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



sql-devdata-269289 | Auditing

SQL server

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 ● (on)

Audit log destination (choose at least one):

□ Storage

☑ Log Analytics

Subscription *

Udacity 1006

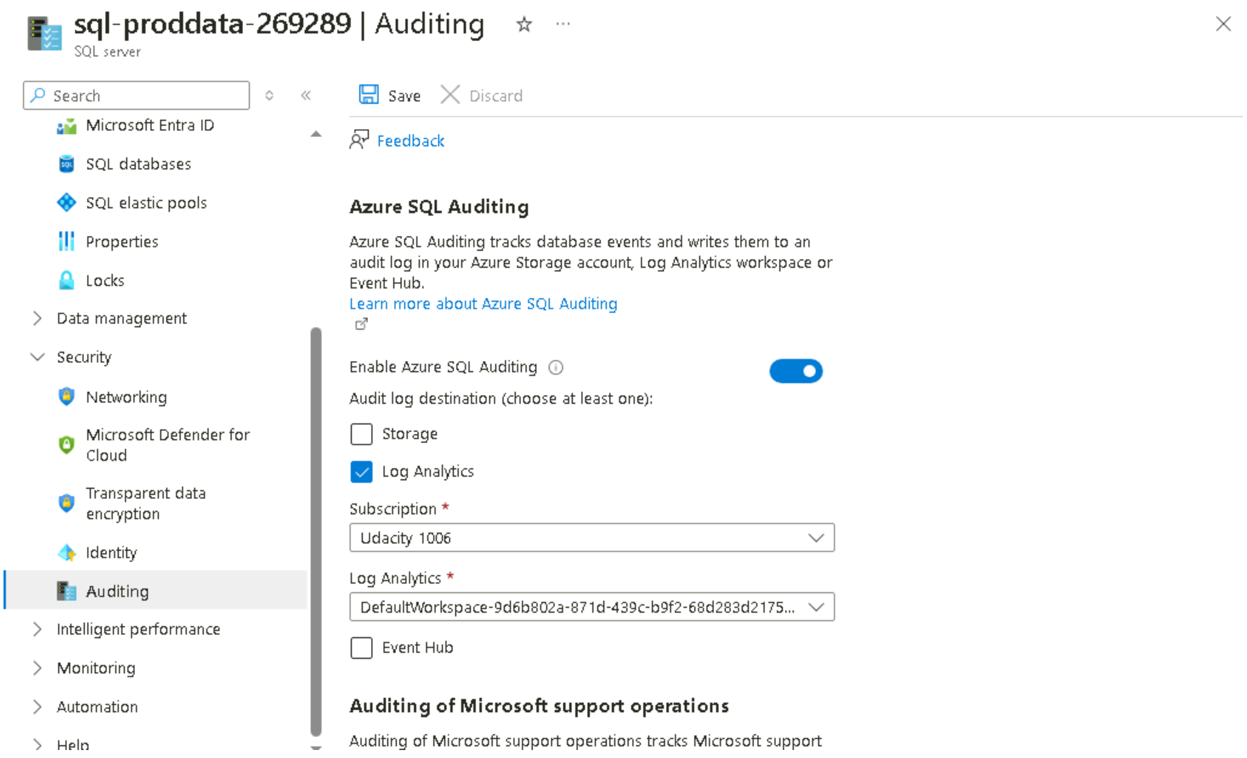
Log Analytics *

DefaultWorkspace-9d6b802a-871d-439c-b9f2-68d283d2175...

□ 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



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

☑ Log Analytics

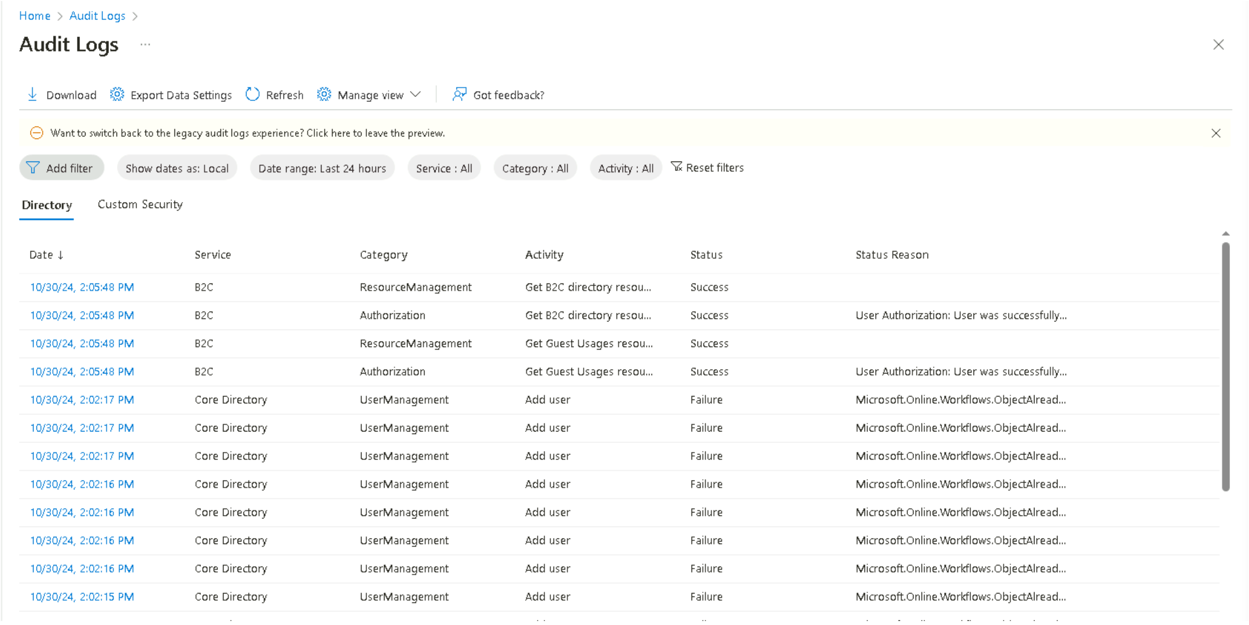
Subscription *
Udacity 1006

Log Analytics *
DefaultWorkspace-9d6b802a-871d-439c-b9f2-68d283d2175...

□ Event Hub

Auditing of Microsoft support operations

Auditing of Microsoft support operations tracks Microsoft support



Want to switch back to the legacy audit logs experience? Click here to leave the preview.

Add filter | Show dates as: Local | Date range: Last 24 hours | Service : All | Category : All | Activity : All | Reset filters

Directory | Custom Security

Date ↓	Service	Category	Activity	Status	Status Reason
10/30/24, 2:05:48 PM	B2C	ResourceManagement	Get B2C directory resou...	Success	
10/30/24, 2:05:48 PM	B2C	Authorization	Get B2C directory resou...	Success	User Authorization: User was successfully...
10/30/24, 2:05:48 PM	B2C	ResourceManagement	Get Guest Usages resou...	Success	
10/30/24, 2:05:48 PM	B2C	Authorization	Get Guest Usages resou...	Success	User Authorization: User was successfully...
10/30/24, 2:02:17 PM	Core Directory	UserManagement	Add user	Failure	Microsoft.Online.Workflows.ObjectAlread...
10/30/24, 2:02:17 PM	Core Directory	UserManagement	Add user	Failure	Microsoft.Online.Workflows.ObjectAlread...
10/30/24, 2:02:17 PM	Core Directory	UserManagement	Add user	Failure	Microsoft.Online.Workflows.ObjectAlread...
10/30/24, 2:02:16 PM	Core Directory	UserManagement	Add user	Failure	Microsoft.Online.Workflows.ObjectAlread...
10/30/24, 2:02:16 PM	Core Directory	UserManagement	Add user	Failure	Microsoft.Online.Workflows.ObjectAlread...
10/30/24, 2:02:16 PM	Core Directory	UserManagement	Add user	Failure	Microsoft.Online.Workflows.ObjectAlread...
10/30/24, 2:02:16 PM	Core Directory	UserManagement	Add user	Failure	Microsoft.Online.Workflows.ObjectAlread...
10/30/24, 2:02:15 PM	Core Directory	UserManagement	Add user	Failure	Microsoft.Online.Workflows.ObjectAlread...

1. B2C Service Successfully Retrieved Directory Resources

This log indicates that an action related to getting resources from the B2C directory service was successful.

Date and Time: 10/30/24, 2:05:48 PM

Service: B2C

Category: Resource Management

Activity: Get B2C directory resources

Status: Success

Status Reason: Not provided (Success indicates the operation was successful)

2. B2C Service Successfully Authorized User

This log shows that the B2C service successfully authorized a user.

Date and Time: 10/30/24, 2:05:48 PM

Service: B2C

Category: Authorization

Activity: Get B2C directory resources

Status: Success

Status Reason: User Authorization: User was successfully authorized

3. Core Directory Failed to Add User - User Already Exists

This log entry highlights that adding a user to the Core Directory failed because the user already exists.

Date and Time: 10/30/24, 2:02:17 PM

Service: Core Directory

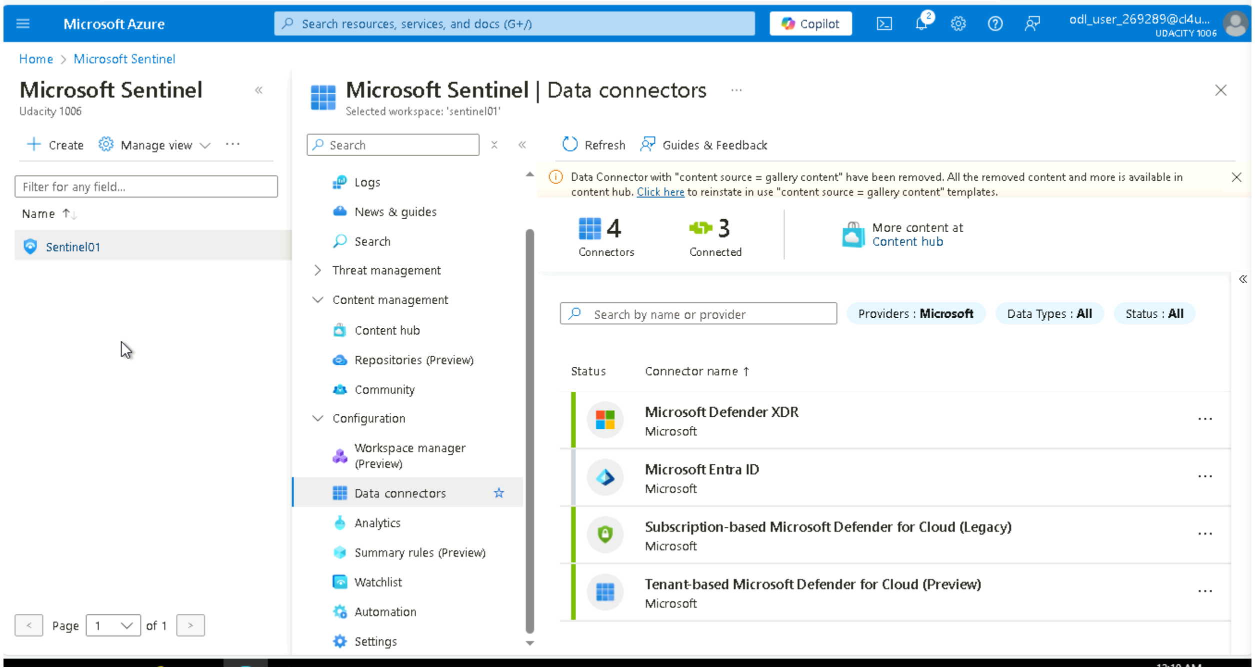
Category: User Management

Activity: Add user

Status: Failure

Status Reason: Microsoft Online Workflows.ObjectAlreadyExist

2. Proof of Sentinel connectors (2+)



Microsoft Sentinel | Data connectors

Selected workspace: 'sentinel01'

Data Connector with "content source = gallery content" have been removed. All the removed content and more is available in content hub. Click here to reinstate in use "content source = gallery content" templates.

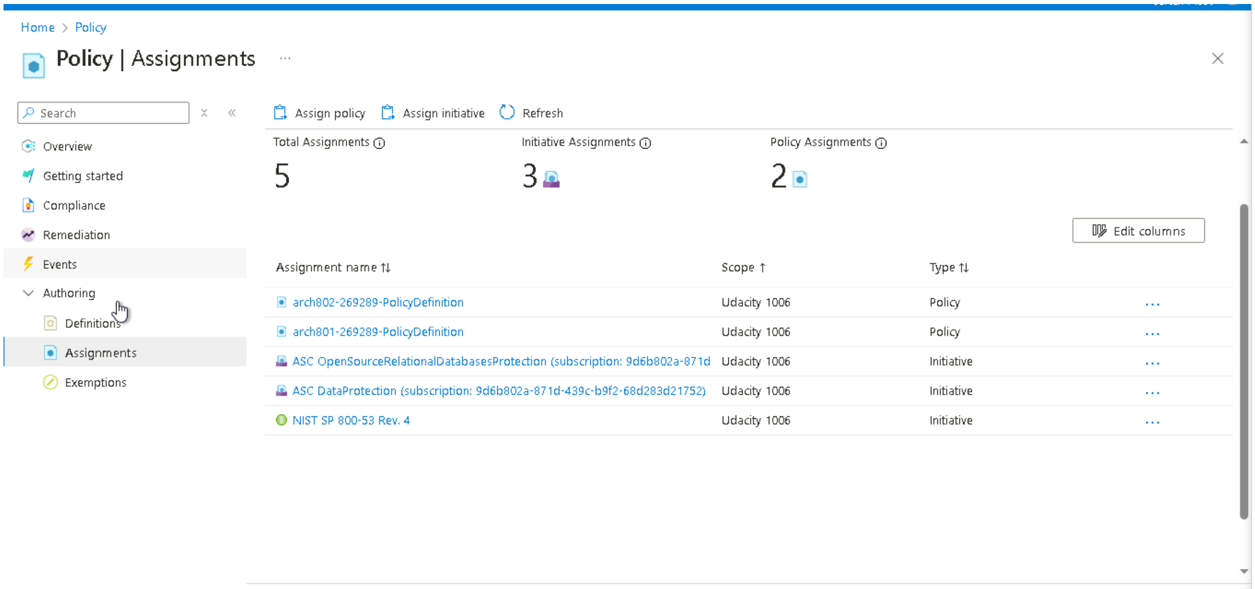
4 Connectors

3 Connected

Status	Connector name ↑
	Microsoft Defender XDR Microsoft
	Microsoft Entra ID Microsoft
	Subscription-based Microsoft Defender for Cloud (Legacy) Microsoft
	Tenant-based Microsoft Defender for Cloud (Preview) Microsoft

Compliance

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



Total Assignments ⓘ 5

Initiative Assignments ⓘ 3

Policy Assignments ⓘ 2

Assignment name ⇅	Scope ↑	Type ⇅
arch802-269289-PolicyDefinition	Udacity 1006	Policy
arch801-269289-PolicyDefinition	Udacity 1006	Policy
ASC OpenSourceRelationalDatabasesProtection (subscription: 9d6b802a-871d	Udacity 1006	Initiative
ASC DataProtection (subscription: 9d6b802a-871d-439c-b9f2-68d283d21752)	Udacity 1006	Initiative
NIST SP 800-53 Rev. 4	Udacity 1006	Initiative