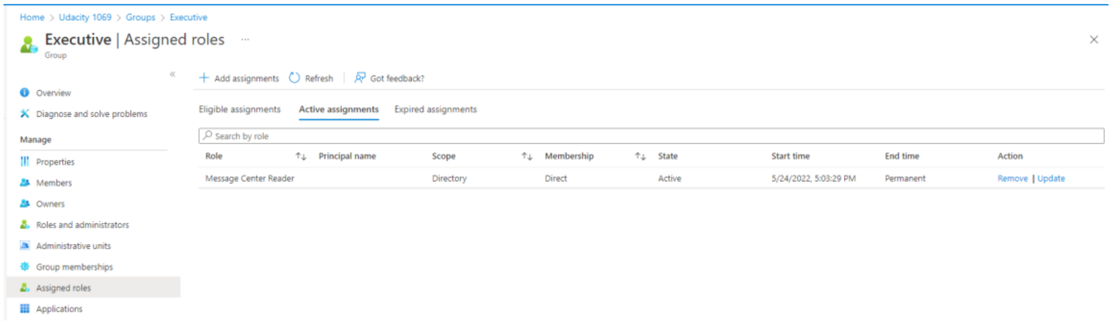
Attention students:

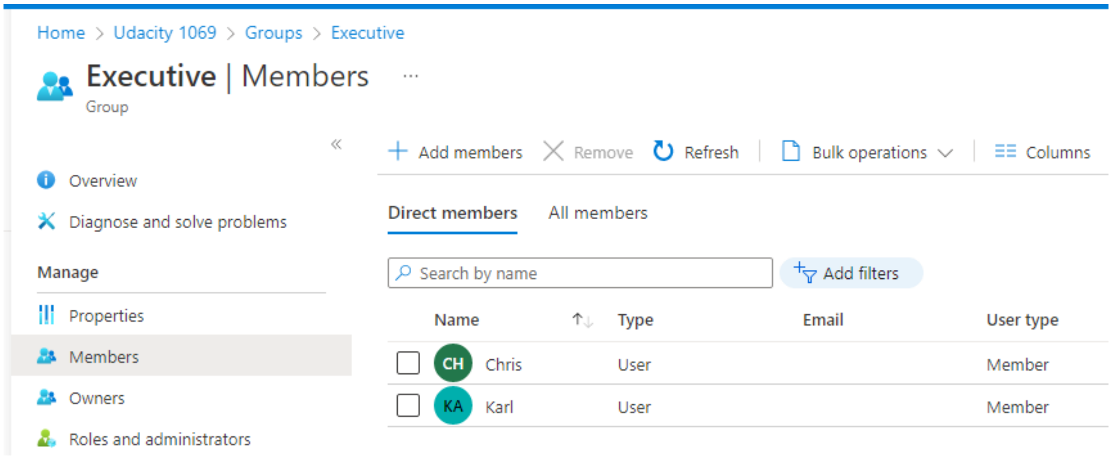
In order to demonstrate successful completion of all components in the project, please use screenshot(s) to show each <u>completed</u> action step as specified on the instructions page.

Identity and Access Management

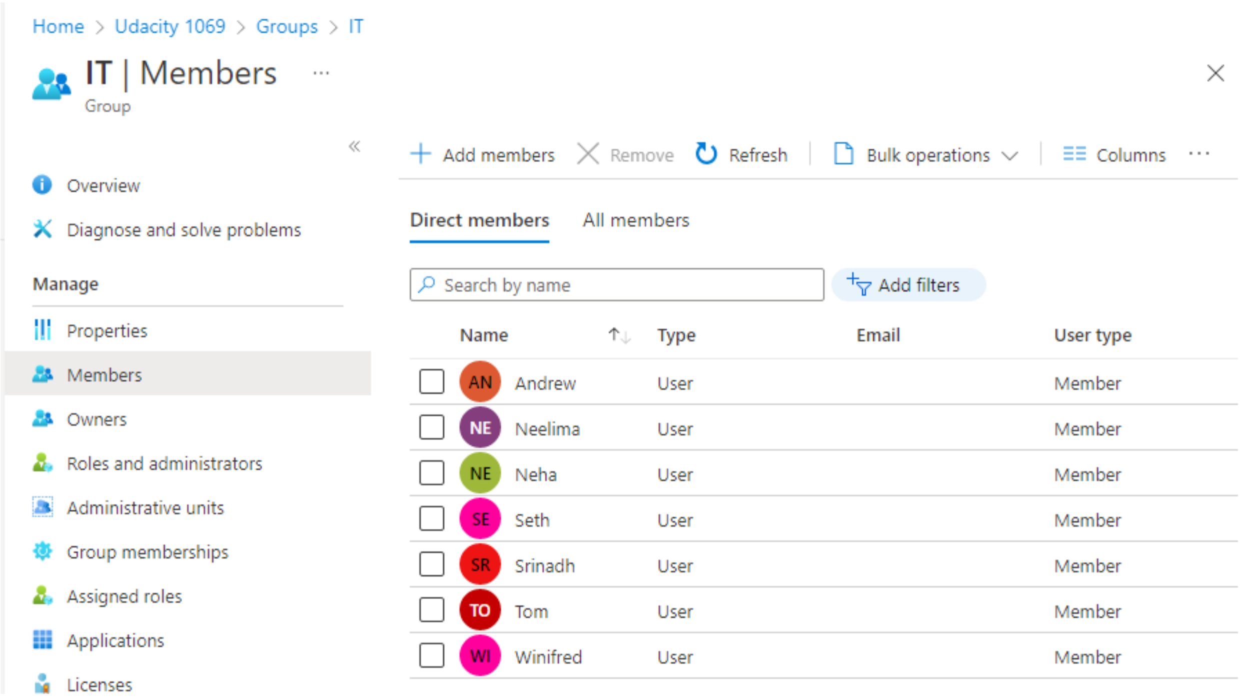
1. Proof of Assigned roles and AD assignments
    a. Andrew
    b. Chris
    c. Karl
    d. Lora
    e. Neelima
    f. Neha
    g. Seth
    h. Srinadh
    i. Tom
    j. Winifred



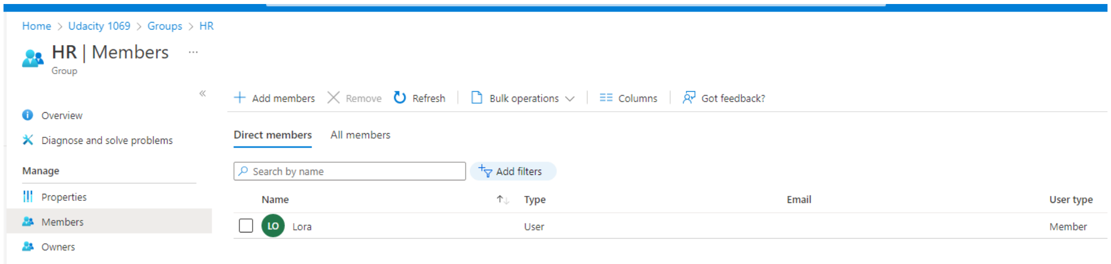
Role	Principal name	Scope	Membership	State	Start time	End time	Action
Message Center Reader		Directory	Direct	Active	5/24/2022, 5:03:29 PM	Permanent	Remove | Update



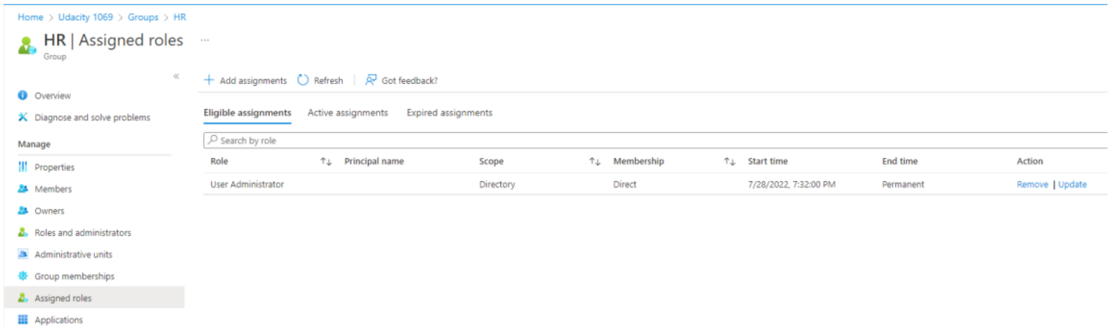
	Name	Type	Email	User type
□	CH Chris	User		Member
□	KA Karl	User		Member



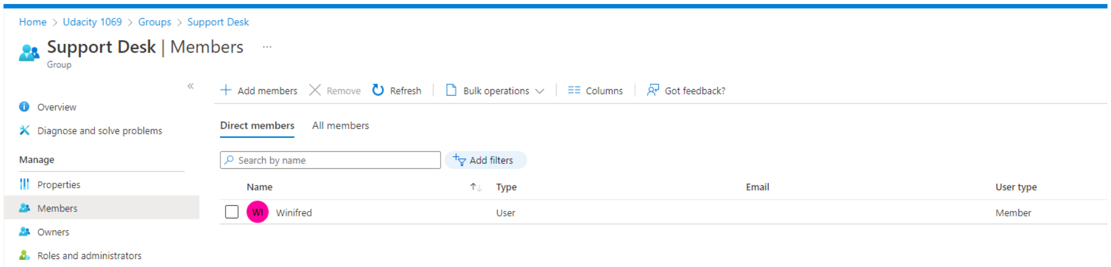
	Name	Type	Email	User type
□	AN Andrew	User		Member
□	NE Neelima	User		Member
□	NE Neha	User		Member
□	SE Seth	User		Member
□	SR Srinadh	User		Member
□	TO Tom	User		Member
□	WI Winifred	User		Member



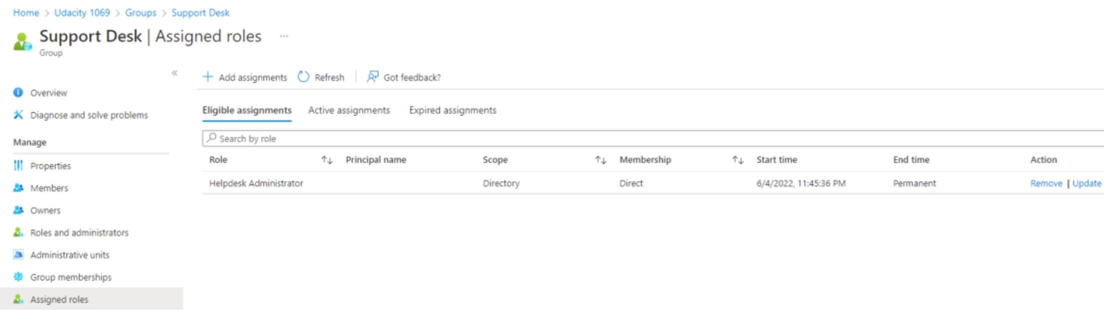
	Name	Type	Email	User type
□	LO Lora	User		Member



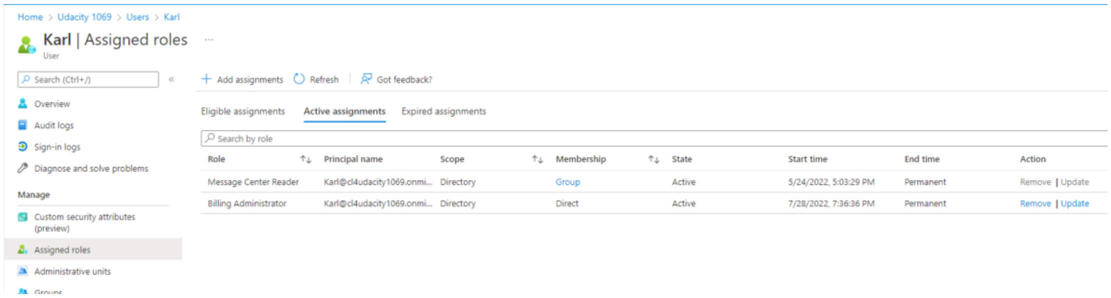
Role	Principal name	Scope	Membership	Start time	End time	Action
User Administrator		Directory	Direct	7/28/2022, 7:32:00 PM	Permanent	Remove | Update



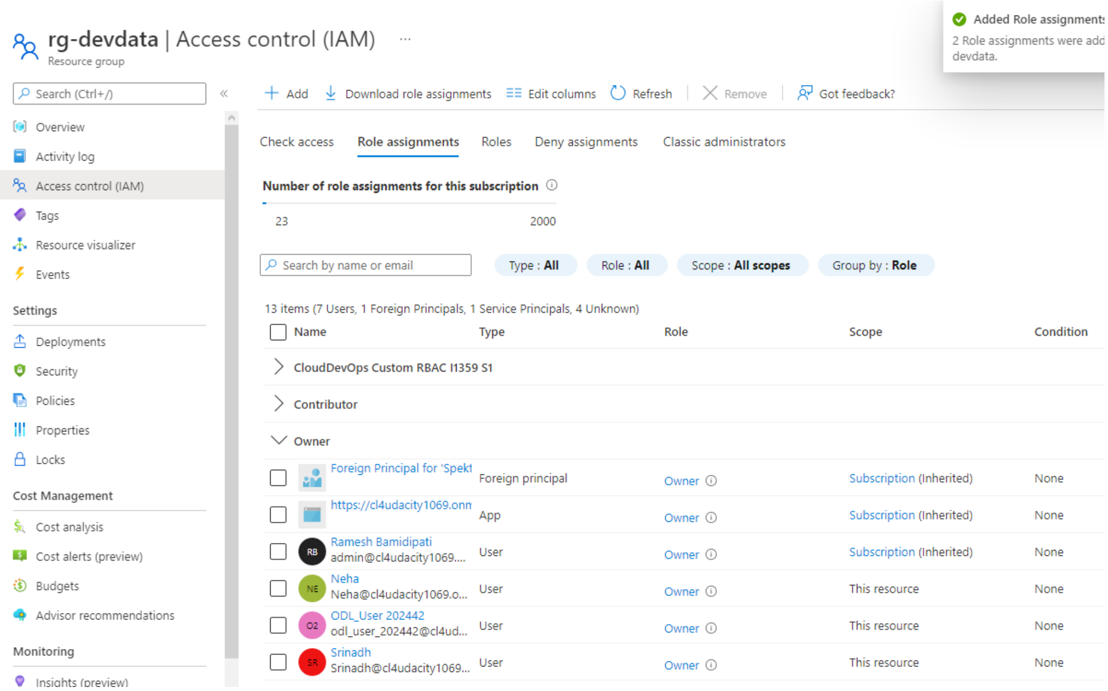
	Name	Type	Email	User type
□	WI Winifred	User		Member



Role	Principal name	Scope	Membership	Start time	End time	Action
Helpdesk Administrator		Directory	Direct	6/4/2022, 11:45:36 PM	Permanent	Remove | Update



Role	Principal name	Scope	Membership	State	Start time	End time	Action
Message Center Reader	Karl@cl4udacity1069.onmi...	Directory	Group	Active	5/24/2022, 5:03:29 PM	Permanent	Remove | Update
Billing Administrator	Karl@cl4udacity1069.onmi...	Directory	Direct	Active	7/28/2022, 7:36:36 PM	Permanent	Remove | Update



rg-devdata | Access control (IAM)

Resource group

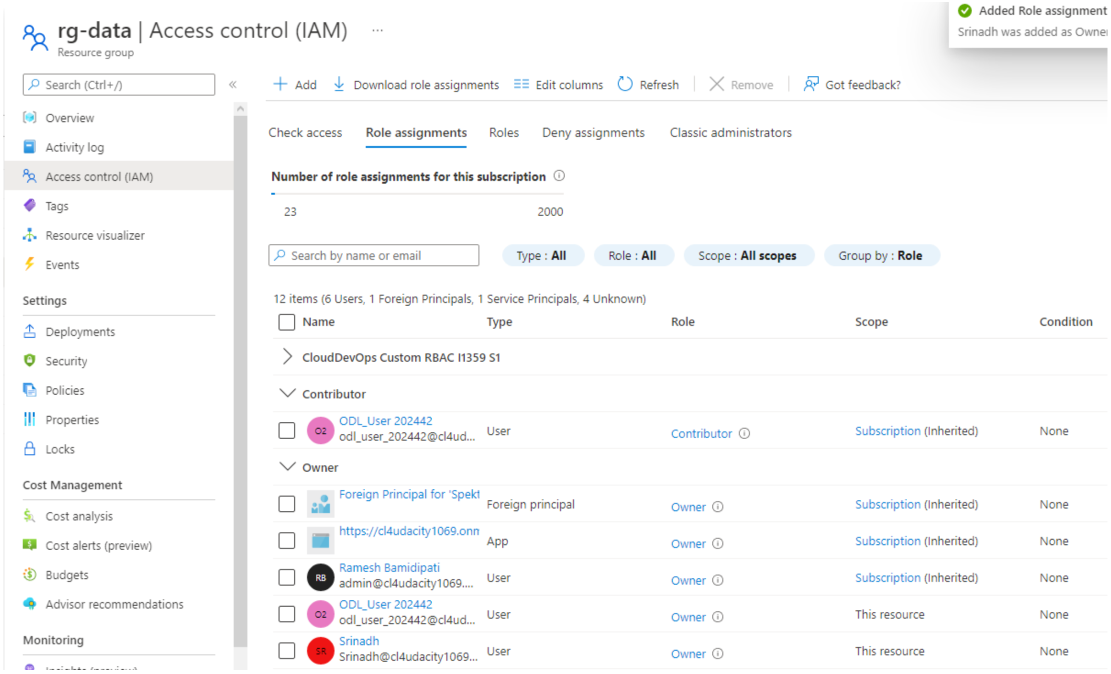
Added Role assignment
2 Role assignments were add
devdata.

Number of role assignments for this subscription

23 2000

13 items (7 Users, 1 Foreign Principals, 1 Service Principals, 4 Unknown)

Name	Type	Role	Scope	Condition
CloudDevOps Custom RBAC I1359 S1				
Contributor				
Owner				
Foreign Principal for 'Spekt	Foreign principal	Owner	Subscription (Inherited)	None
https://cl4udacity1069.onn	App	Owner	Subscription (Inherited)	None
Ramesh Bamidipati admin@cl4udacity1069....	User	Owner	Subscription (Inherited)	None
Neha Neha@cl4udacity1069.o...	User	Owner	This resource	None
ODL_User 202442 odl_user_202442@cl4ud...	User	Owner	This resource	None
Srinadh Srinadh@cl4udacity1069...	User	Owner	This resource	None



rg-data | Access control (IAM)

Resource group

Added Role assignment
Srinadh was added as Owne

Number of role assignments for this subscription

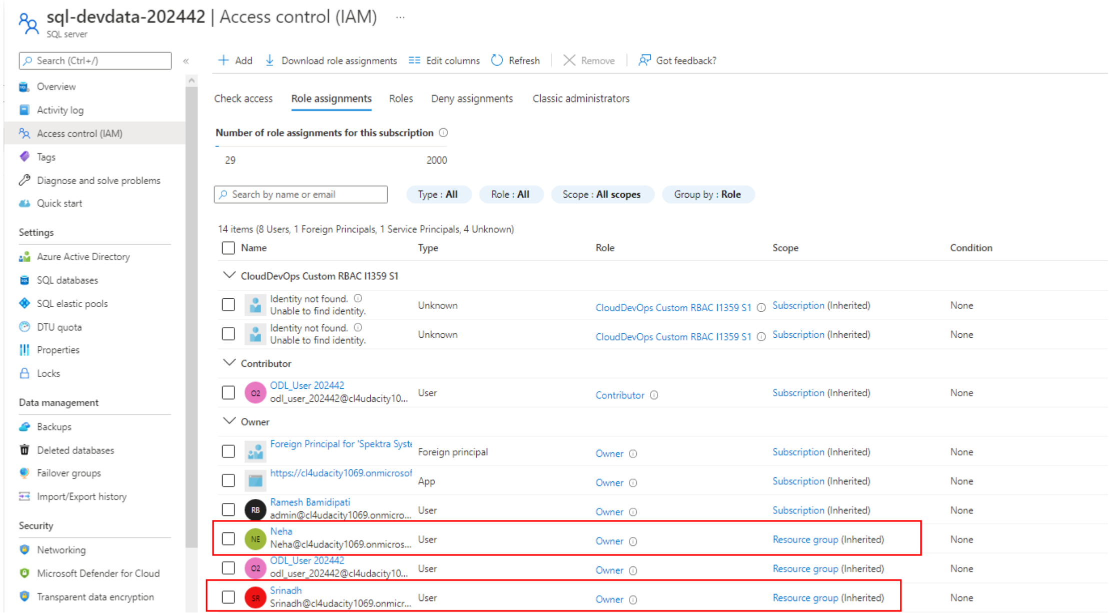
23 2000

12 items (6 Users, 1 Foreign Principals, 1 Service Principals, 4 Unknown)

Name	Type	Role	Scope	Condition
CloudDevOps Custom RBAC I1359 S1				
Contributor				
ODL_User 202442 odl_user_202442@cl4ud...	User	Contributor	Subscription (Inherited)	None
Owner				
Foreign Principal for 'Spekt	Foreign principal	Owner	Subscription (Inherited)	None
https://cl4udacity1069.onn	App	Owner	Subscription (Inherited)	None
Ramesh Bamidipati admin@cl4udacity1069....	User	Owner	Subscription (Inherited)	None
ODL_User 202442 odl_user_202442@cl4ud...	User	Owner	This resource	None
Srinadh Srinadh@cl4udacity1069...	User	Owner	This resource	None

V2:

Owner’s Access to Development and Production SQL Servers:

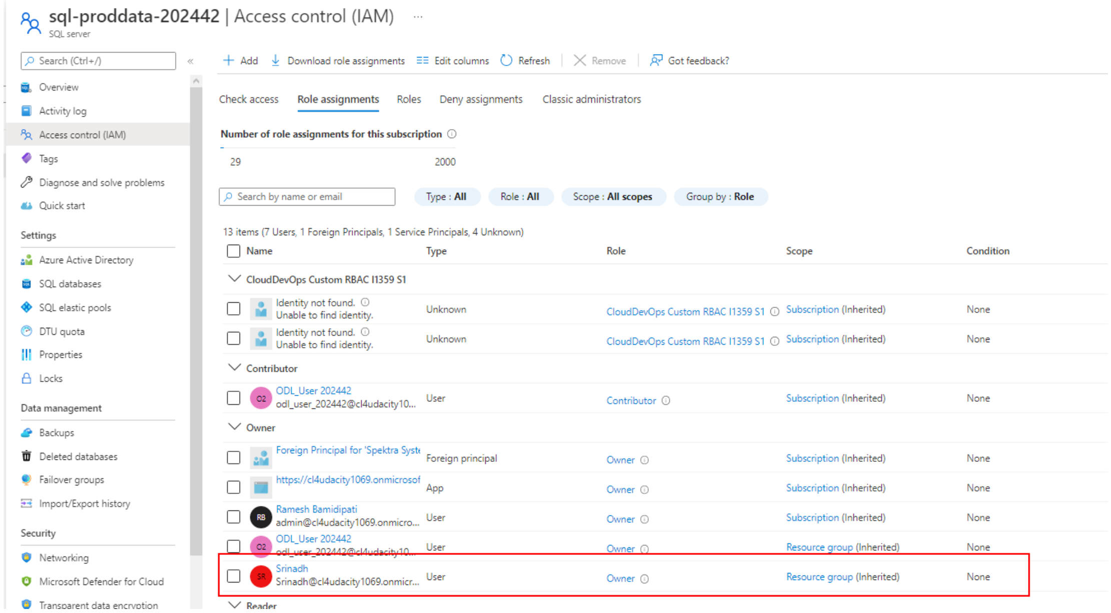


Number of role assignments for this subscription

29 2000

14 items (8 Users, 1 Foreign Principals, 1 Service Principals, 4 Unknown)

Name	Type	Role	Scope	Condition
CloudDevOps Custom RBAC I1359 S1				
Identity not found. Unable to find identity.	Unknown	CloudDevOps Custom RBAC I1359 S1	Subscription (Inherited)	None
Identity not found. Unable to find identity.	Unknown	CloudDevOps Custom RBAC I1359 S1	Subscription (Inherited)	None
Contributor				
ODL_User 202442 odl_user_202442@cl4udacity10...	User	Contributor	Subscription (Inherited)	None
Owner				
Foreign Principal for 'Spektra Syste	Foreign principal	Owner	Subscription (Inherited)	None
https://cl4udacity1069.onmicrosof	App	Owner	Subscription (Inherited)	None
Ramesh Bamidipati admin@cl4udacity1069.onmicro...	User	Owner	Subscription (Inherited)	None
Neha Neha@cl4udacity1069.onmicros...	User	Owner	Resource group (Inherited)	None
ODL_User 202442 odl_user_202442@cl4udacity10...	User	Owner	Resource group (Inherited)	None
Srinadh Srinadh@cl4udacity1069.onmicr...	User	Owner	Resource group (Inherited)	None

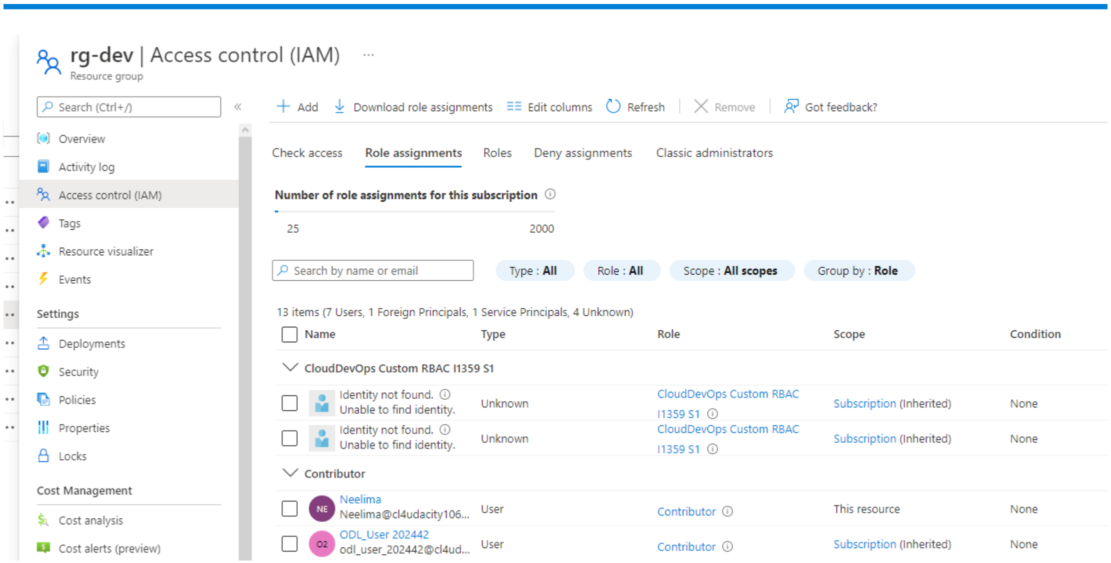


Number of role assignments for this subscription

29 2000

13 items (7 Users, 1 Foreign Principals, 1 Service Principals, 4 Unknown)

Name	Type	Role	Scope	Condition
CloudDevOps Custom RBAC I1359 S1				
Identity not found. Unable to find identity.	Unknown	CloudDevOps Custom RBAC I1359 S1	Subscription (Inherited)	None
Identity not found. Unable to find identity.	Unknown	CloudDevOps Custom RBAC I1359 S1	Subscription (Inherited)	None
Contributor				
ODL_User 202442 odl_user_202442@cl4udacity10...	User	Contributor	Subscription (Inherited)	None
Owner				
Foreign Principal for 'Spektra Syste	Foreign principal	Owner	Subscription (Inherited)	None
https://cl4udacity1069.onmicrosof	App	Owner	Subscription (Inherited)	None
Ramesh Bamidipati admin@cl4udacity1069.onmicro...	User	Owner	Subscription (Inherited)	None
ODL_User 202442 odl_user_202442@cl4udacity10...	User	Owner	Resource group (Inherited)	None
Srinadh Srinadh@cl4udacity1069.onmicr...	User	Owner	Resource group (Inherited)	None
Reader				

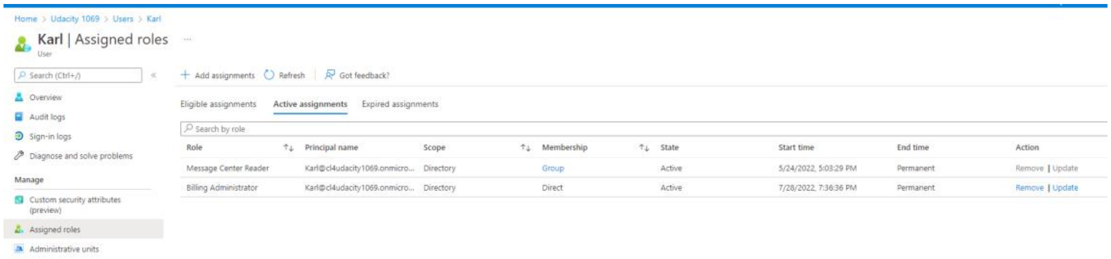


Number of role assignments for this subscription ⓘ

25 2000

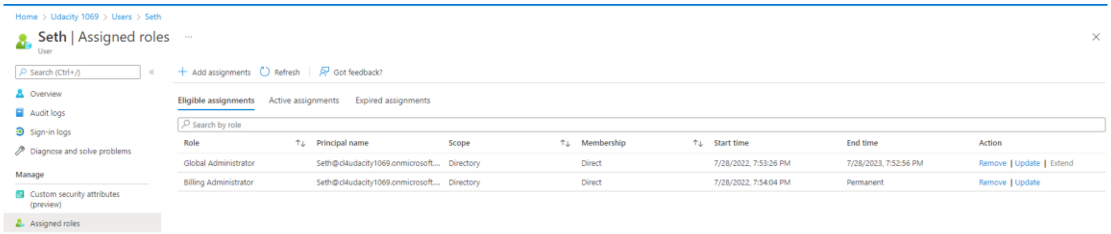
13 items (7 Users, 1 Foreign Principals, 1 Service Principals, 4 Unknown)

□ Name	Type	Role	Scope	Condition
CloudDevOps Custom RBAC I1359 S1				
□ Identity not found. ⓘ Unable to find identity.	Unknown	CloudDevOps Custom RBAC I1359 S1 ⓘ	Subscription (Inherited)	None
□ Identity not found. ⓘ Unable to find identity.	Unknown	CloudDevOps Custom RBAC I1359 S1 ⓘ	Subscription (Inherited)	None
Contributor				
□ NE Neelima Neelima@cl4udacity106...	User	Contributor ⓘ	This resource	None
□ O2 ODL_User 202442 odl_user_202442@cl4ud...	User	Contributor ⓘ	Subscription (Inherited)	None



Karl | Assigned roles

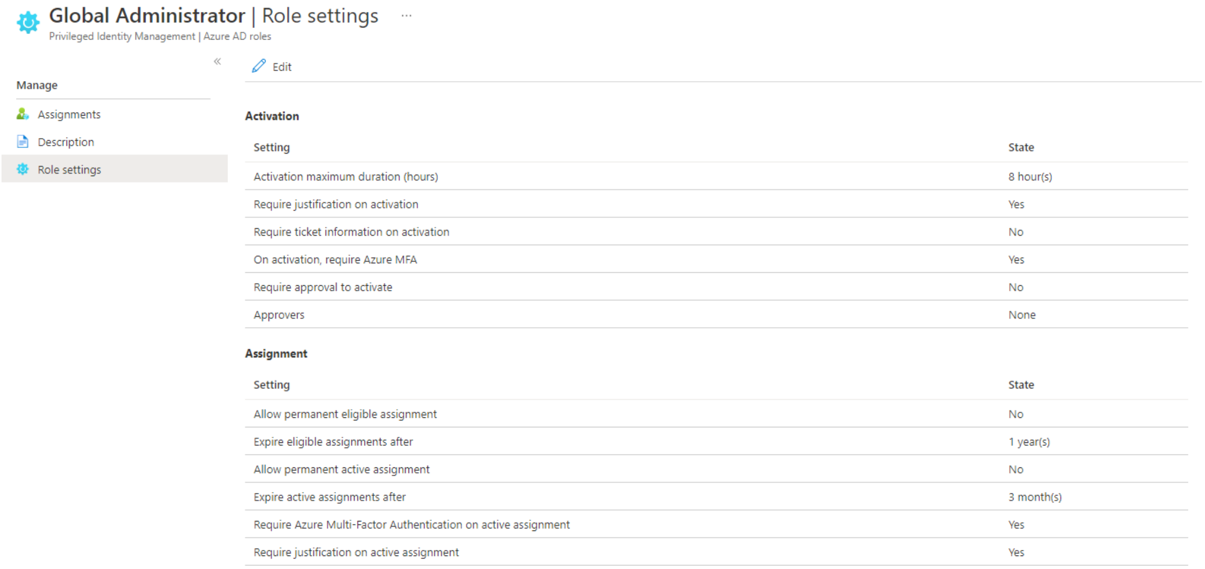
Role	Principal name	Scope	Membership	State	Start time	End time	Action
Message Center Reader	Karl@cl4udacity1069.onmicro...	Directory	Group	Active	5/24/2022, 5:03:29 PM	Permanent	Remove | Update
Billing Administrator	Karl@cl4udacity1069.onmicro...	Directory	Direct	Active	7/28/2022, 7:36:36 PM	Permanent	Remove | Update



Seth | Assigned roles

Role	Principal name	Scope	Membership	Start time	End time	Action
Global Administrator	Seth@cl4udacity1069.onmicrosoft....	Directory	Direct	7/28/2022, 7:53:26 PM	7/28/2023, 7:52:56 PM	Remove | Update | Extend
Billing Administrator	Seth@cl4udacity1069.onmicrosoft....	Directory	Direct	7/28/2022, 7:54:04 PM	Permanent	Remove | Update

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



Global Administrator | Role settings

Privileged Identity Management | Azure AD roles

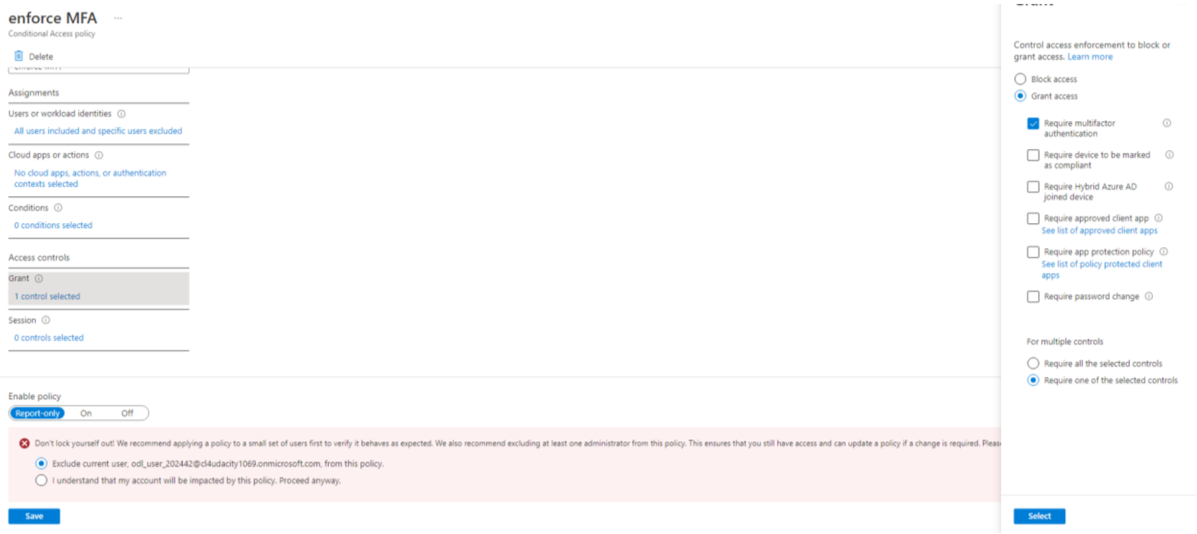
Activation

Setting	State
Activation maximum duration (hours)	8 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	No
Approvers	None

Assignment

Setting	State
Allow permanent eligible assignment	No
Expire eligible assignments after	1 year(s)
Allow permanent active assignment	No
Expire active assignments after	3 month(s)
Require Azure Multi-Factor Authentication on active assignment	Yes
Require justification on active assignment	Yes

3. Proof of Conditional Access policy all users



enforce MFA ···

Conditional Access policy

Delete

Assignments

Users or workload identities ⓘ

All users included and specific users excluded

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ

0 controls selected

Enable policy

[✓ Report-only] On Off

Don't lock yourself out! We recommend applying a policy to a small set of users first to verify it behaves as expected. We also recommend excluding at least one administrator from this policy. This ensures that you still have access and can update a policy if a change is required. Pleas

● Exclude current user, odl_user_202442@cl4udacity1069.onmicrosoft.com, from this policy.

○ I understand that my account will be impacted by this policy. Proceed anyway.

Save

Control access enforcement to block or grant access. Learn more

○ Block access

● Grant access

☑ Require multifactor authentication ⓘ

☐ Require device to be marked as compliant ⓘ

☐ Require Hybrid Azure AD joined device ⓘ

☐ Require approved client app ⓘ
See list of approved client apps

☐ Require app protection policy ⓘ
See list of policy protected client apps

☐ Require password change ⓘ

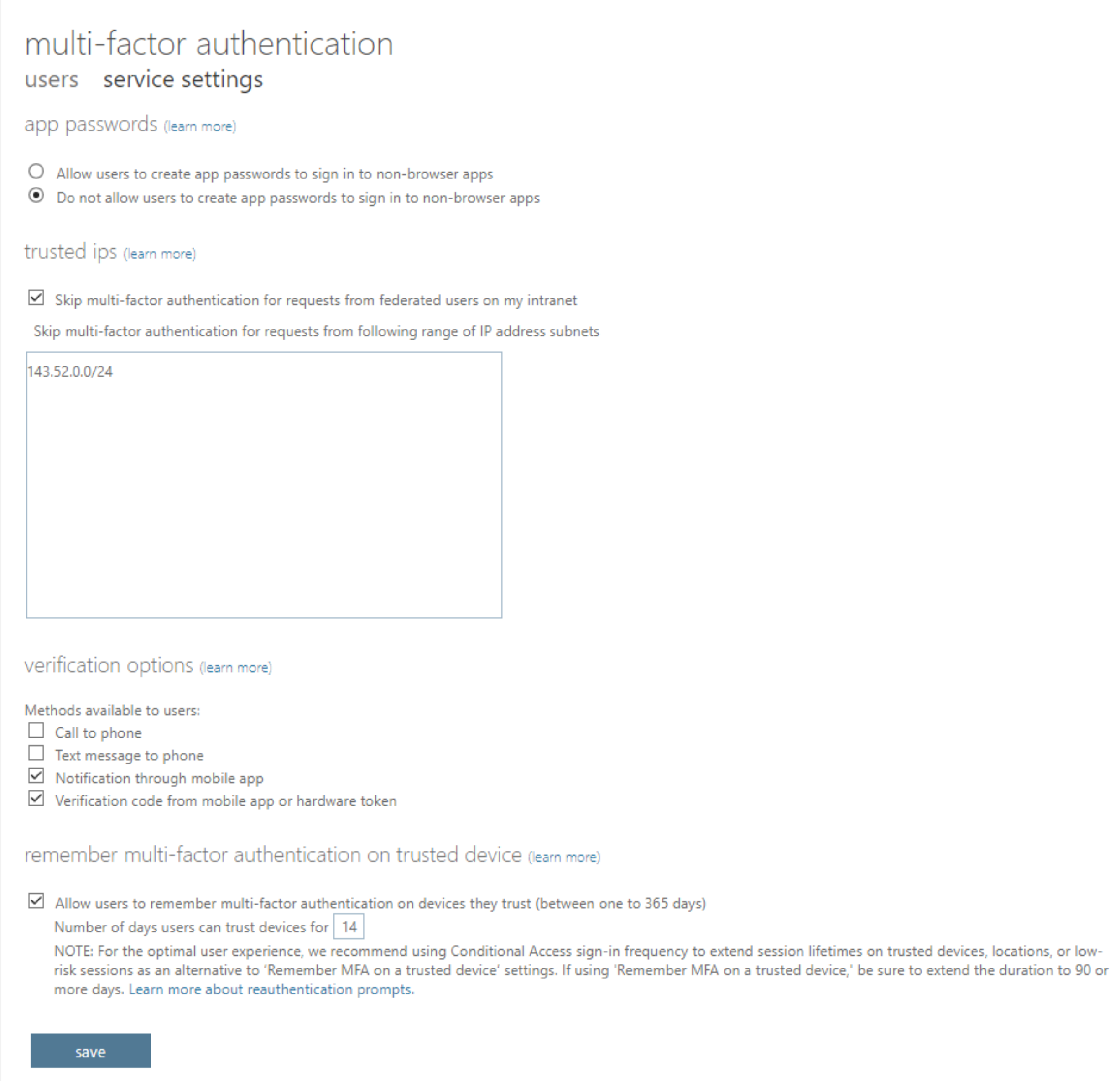
For multiple controls

○ Require all the selected controls

● Require one of the selected controls

Select

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



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)

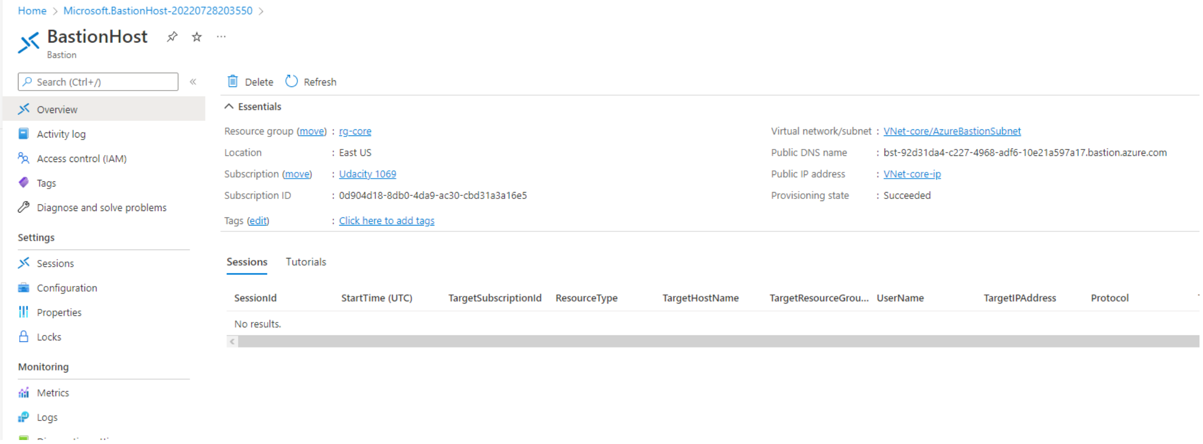
☑ Allow users to remember multi-factor authentication on devices they trust (between one to 365 days)

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.

Network Security

1. Bastion overview



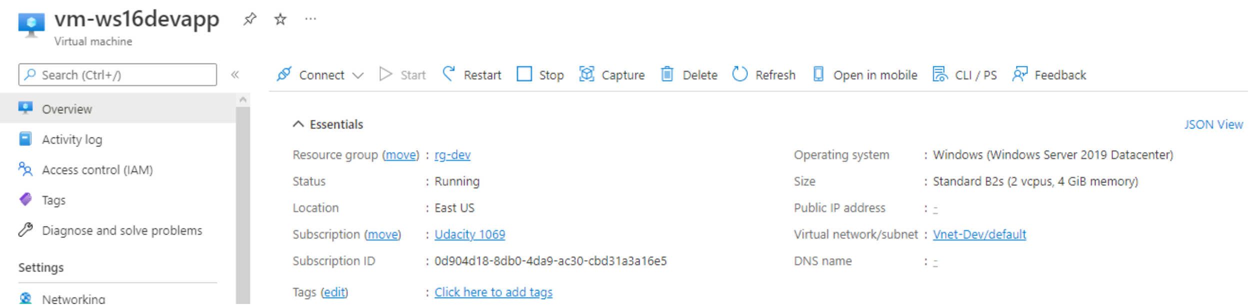
Essentials

Resource group (move) : rg-core
Location : East US
Subscription (move) : Udacity 1069
Subscription ID : 0d904d18-8db0-4da9-ac30-cbd31a3a16e5
Tags (edit) : Click here to add tags

Virtual network/subnet : VNet-core/AzureBastionSubnet
Public DNS name : bst-92d31da4-c227-4968-adf6-10e21a597a17.bastion.azure.com
Public IP address : VNet-core-ip
Provisioning state : Succeeded

SessionId	StartTime (UTC)	TargetSubscriptionId	ResourceType	TargetHostName	TargetResourceGrou...	UserName	TargetIPAddress	Protocol
No results.								

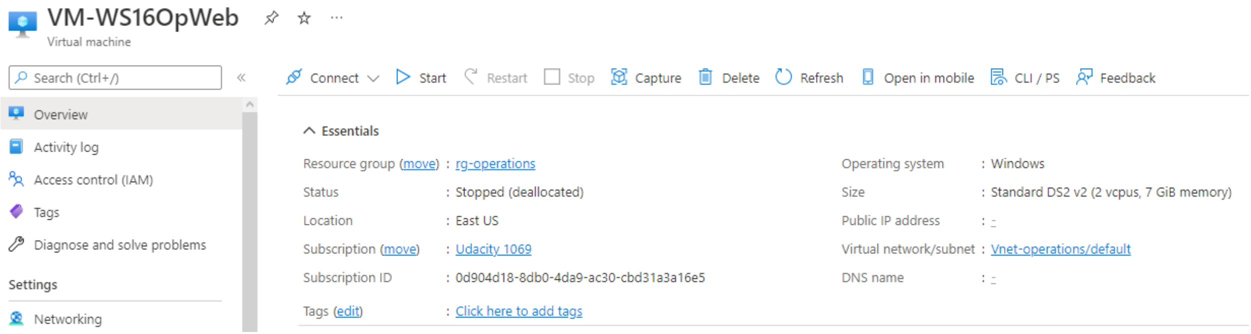
2. Proof of public IP addresses removed



Essentials

Resource group (move) : rg-dev
Status : Running
Location : East US
Subscription (move) : Udacity 1069
Subscription ID : 0d904d18-8db0-4da9-ac30-cbd31a3a16e5
Tags (edit) : Click here to add tags

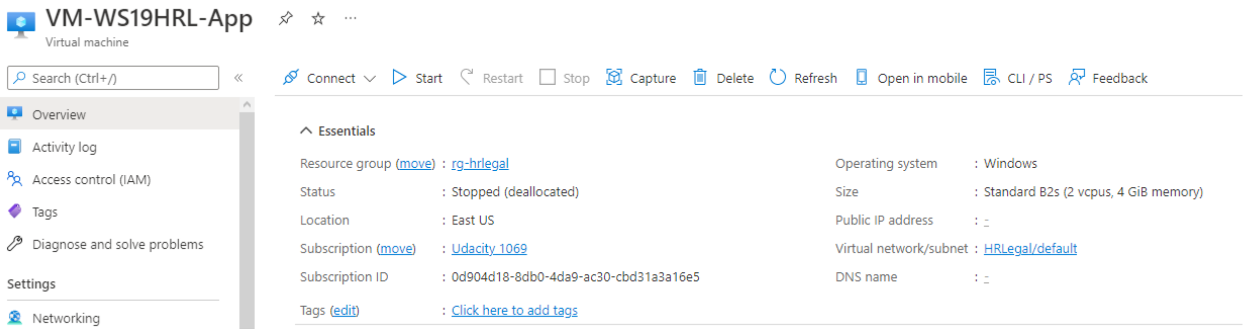
Operating system : Windows (Windows Server 2019 Datacenter)
Size : Standard B2s (2 vcpus, 4 GiB memory)
Public IP address : -
Virtual network/subnet : Vnet-Dev/default
DNS name : -



Essentials

Resource group (move) : rg-operations
Status : Stopped (deallocated)
Location : East US
Subscription (move) : Udacity 1069
Subscription ID : 0d904d18-8db0-4da9-ac30-cbd31a3a16e5
Tags (edit) : Click here to add tags

Operating system : Windows
Size : Standard DS2 v2 (2 vcpus, 7 GiB memory)
Public IP address : -
Virtual network/subnet : Vnet-operations/default
DNS name : -



Resource group (move) : rg-hrlegal

Status : Stopped (deallocated)

Location : East US

Subscription (move) : Udacity 1069

Subscription ID : 0d904d18-8db0-4da9-ac30-cbd31a3a16e5

Tags (edit) : Click here to add tags

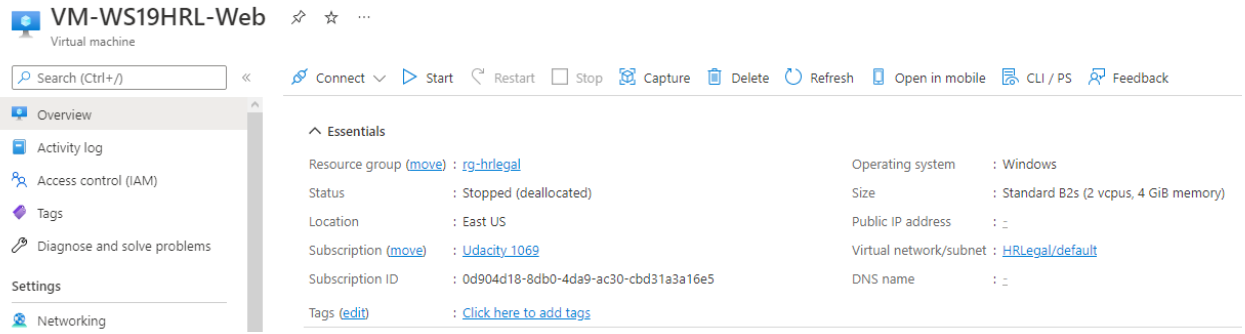
Operating system : Windows

Size : Standard B2s (2 vcpus, 4 GiB memory)

Public IP address : -

Virtual network/subnet : HRLegal/default

DNS name : -



Resource group (move) : rg-hrlegal

Status : Stopped (deallocated)

Location : East US

Subscription (move) : Udacity 1069

Subscription ID : 0d904d18-8db0-4da9-ac30-cbd31a3a16e5

Tags (edit) : Click here to add tags

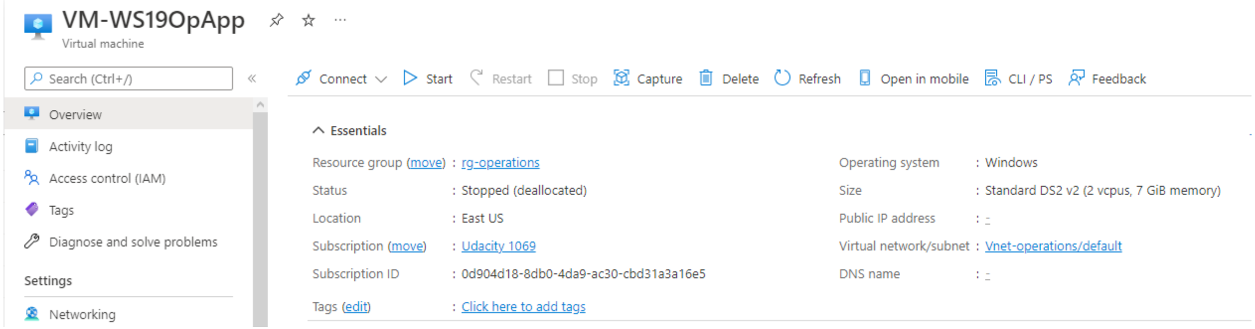
Operating system : Windows

Size : Standard B2s (2 vcpus, 4 GiB memory)

Public IP address : -

Virtual network/subnet : HRLegal/default

DNS name : -



Resource group (move) : rg-operations

Status : Stopped (deallocated)

Location : East US

Subscription (move) : Udacity 1069

Subscription ID : 0d904d18-8db0-4da9-ac30-cbd31a3a16e5

Tags (edit) : Click here to add tags

Operating system : Windows

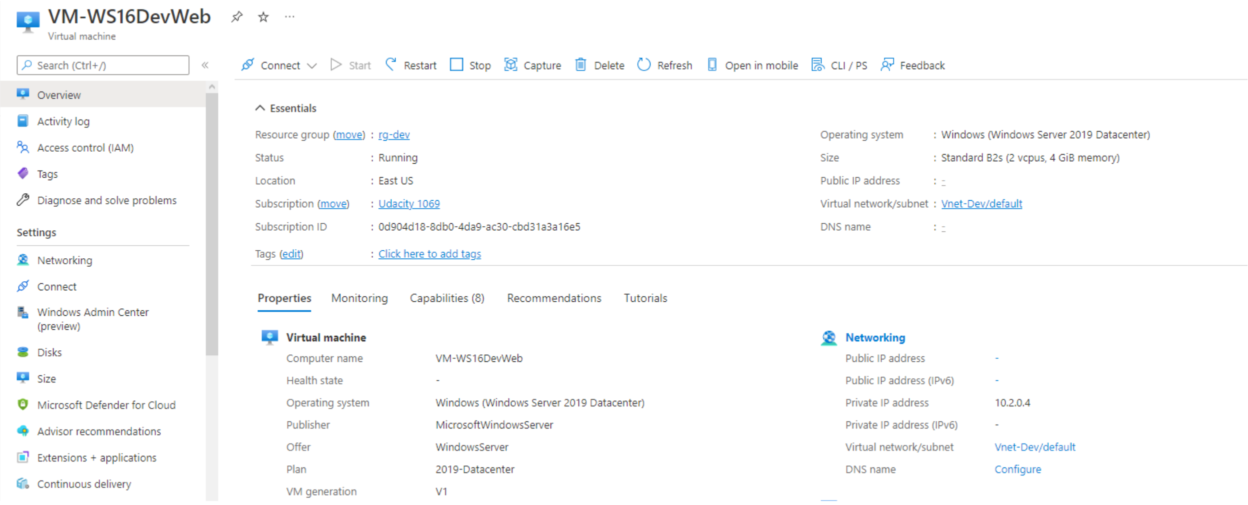
Size : Standard DS2 v2 (2 vcpus, 7 GiB memory)

Public IP address : -

Virtual network/subnet : Vnet-operations/default

DNS name : -

Removed public IP Address from VM-WS16DevWeb



Essentials

Resource group (move) : rg-dev
Status : Running
Location : East US
Subscription (move) : Udacity 1069
Subscription ID : 0d904d18-8db0-4da9-ac30-cbd31a3a16e5
Tags (edit) : Click here to add tags

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 : -

Virtual machine

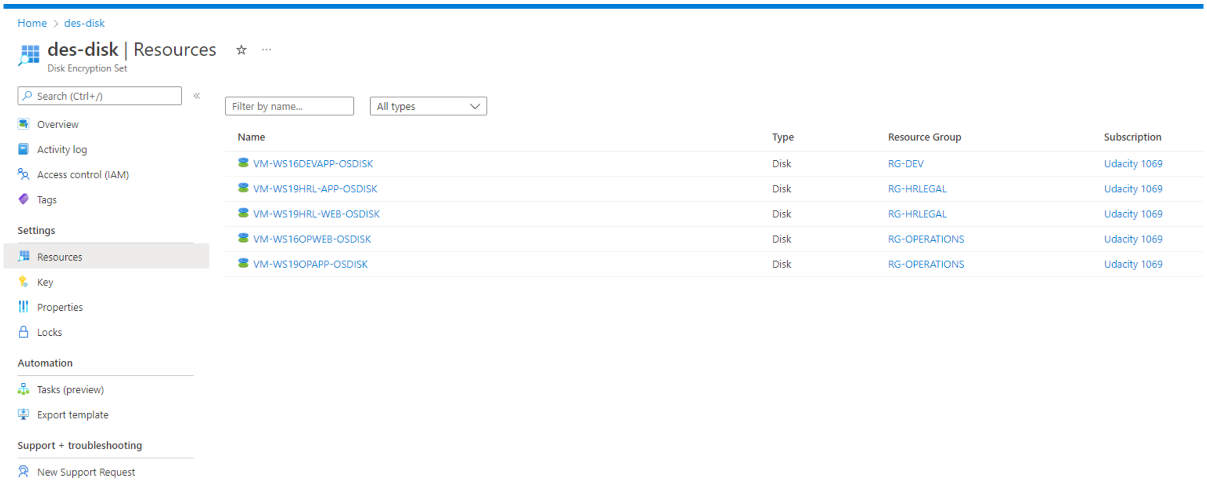
Computer name	VM-WS16DevWeb
Health state	-
Operating system	Windows (Windows Server 2019 Datacenter)
Publisher	MicrosoftWindowsServer
Offer	WindowsServer
Plan	2019-Datacenter
VM generation	V1

Networking

Public IP address	-
Public IP address (IPv6)	-
Private IP address	10.2.0.4
Private IP address (IPv6)	-
Virtual network/subnet	Vnet-Dev/default
DNS name	Configure

Data and Encryption

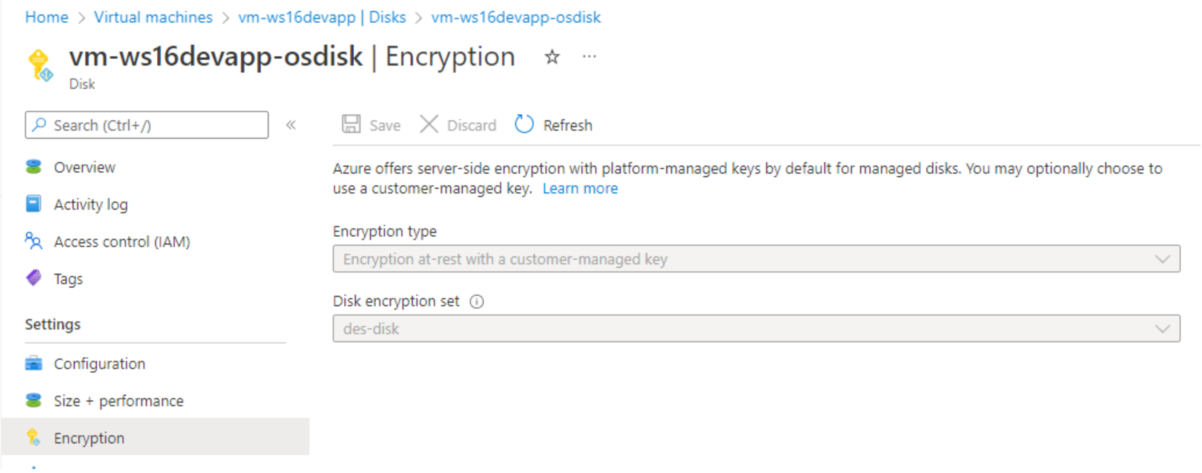
1. Proof of Encryption types for VM (devapp,DevWeb,OpWeb,HRL-App,OPApp, HRL-Web)



des-disk | Resources

Disk Encryption Set

Name	Type	Resource Group	Subscription
VM-WS16DEVAPP-OSDISK	Disk	RG-DEV	Udacity 1069
VM-WS19HRL-APP-OSDISK	Disk	RG-HRLEGAL	Udacity 1069
VM-WS19HRL-WEB-OSDISK	Disk	RG-HRLEGAL	Udacity 1069
VM-WS16OPWEB-OSDISK	Disk	RG-OPERATIONS	Udacity 1069
VM-WS19OPAPP-OSDISK	Disk	RG-OPERATIONS	Udacity 1069



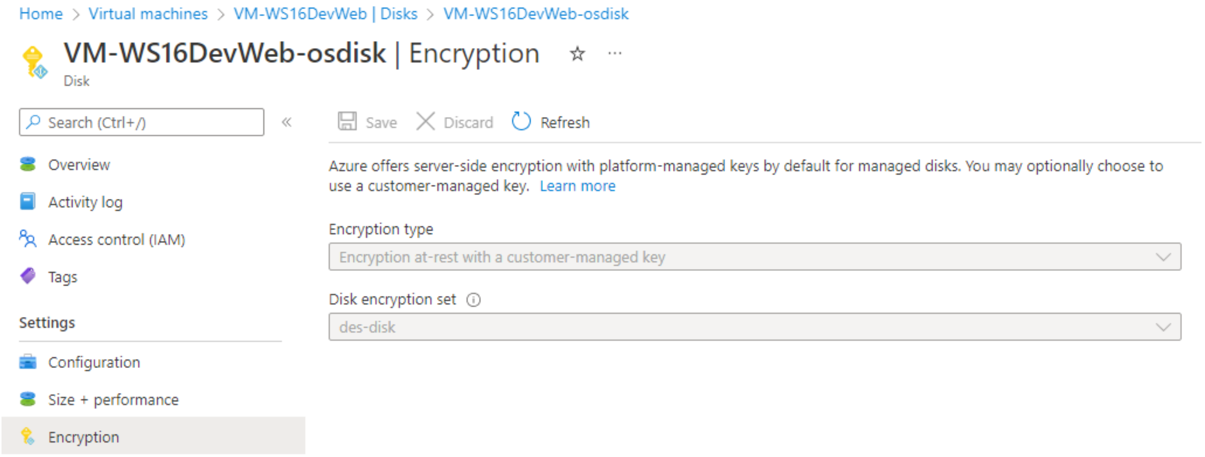
vm-ws16devapp-osdisk | Encryption

Disk

Azure offers server-side encryption with platform-managed keys by default for managed disks. You may optionally choose to use a customer-managed key. Learn more

Encryption type: Encryption at-rest with a customer-managed key

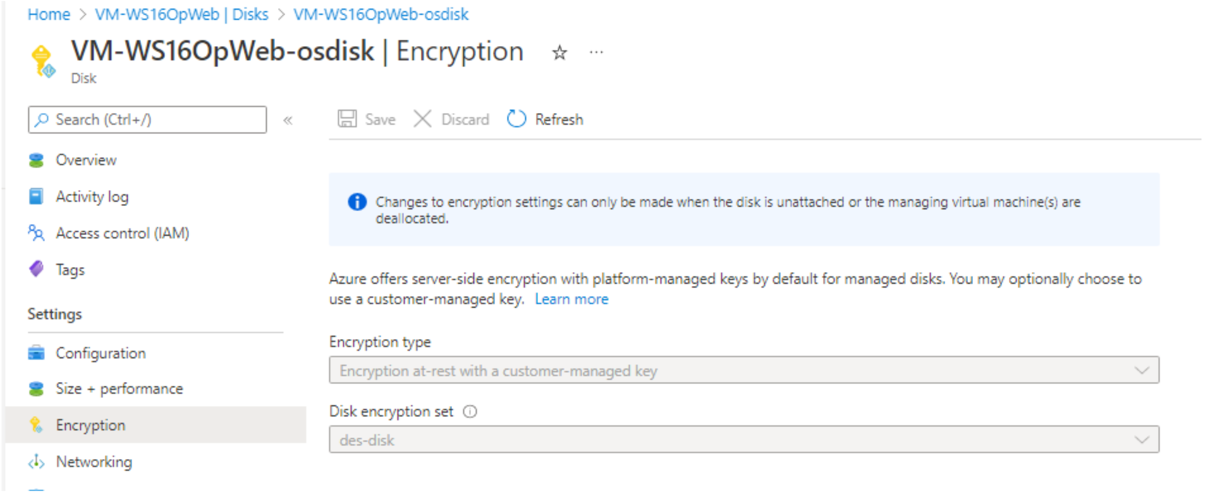
Disk encryption set: des-disk



Azure offers server-side encryption with platform-managed keys by default for managed disks. You may optionally choose to use a customer-managed key. Learn more

Encryption type: Encryption at-rest with a customer-managed key

Disk encryption set: des-disk

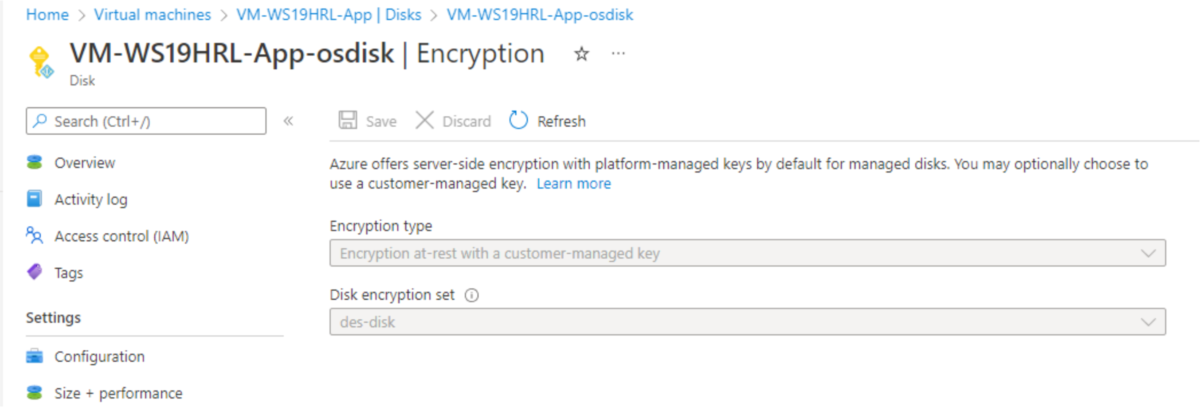


Changes to encryption settings can only be made when the disk is unattached or the managing virtual machine(s) are deallocated.

Azure offers server-side encryption with platform-managed keys by default for managed disks. You may optionally choose to use a customer-managed key. Learn more

Encryption type: Encryption at-rest with a customer-managed key

Disk encryption set: des-disk



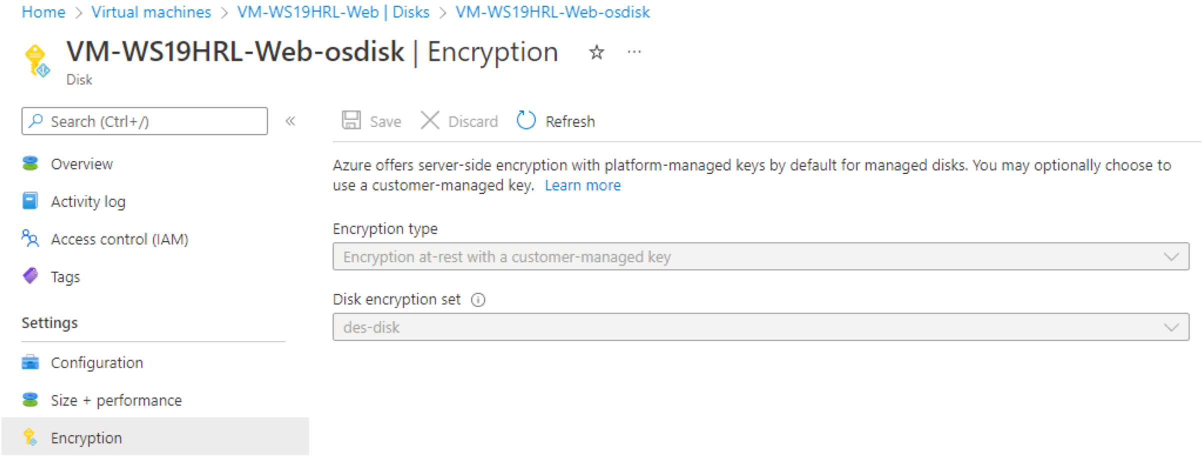
VM-WS19HRL-App-osdisk | Encryption

Disk

Azure offers server-side encryption with platform-managed keys by default for managed disks. You may optionally choose to use a customer-managed key. Learn more

Encryption type: Encryption at-rest with a customer-managed key

Disk encryption set: des-disk



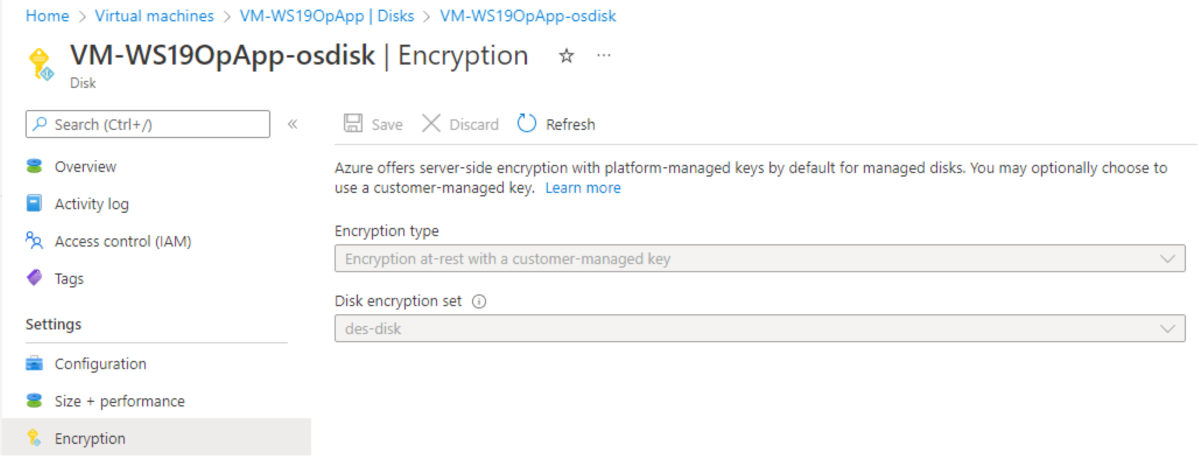
VM-WS19HRL-Web-osdisk | Encryption

Disk

Azure offers server-side encryption with platform-managed keys by default for managed disks. You may optionally choose to use a customer-managed key. Learn more

Encryption type: Encryption at-rest with a customer-managed key

Disk encryption set: des-disk



VM-WS19OpApp-osdisk | Encryption

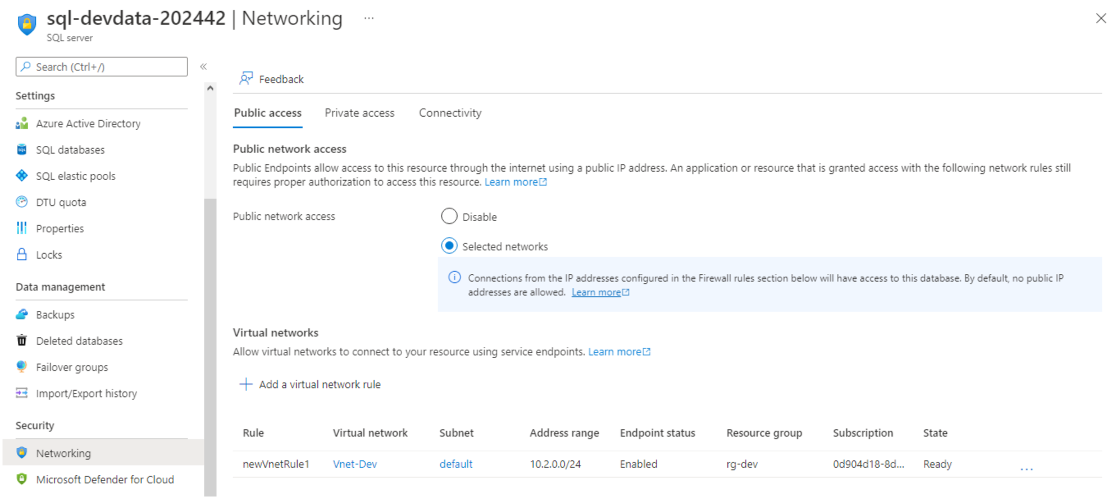
Disk

Azure offers server-side encryption with platform-managed keys by default for managed disks. You may optionally choose to use a customer-managed key. Learn more

Encryption type: Encryption at-rest with a customer-managed key

Disk encryption set: des-disk

2. Firewall and virtual networks page
    a. Proof of No Public access, TLS for SQL servers (prod, dev)



sql-devdata-202442 | 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

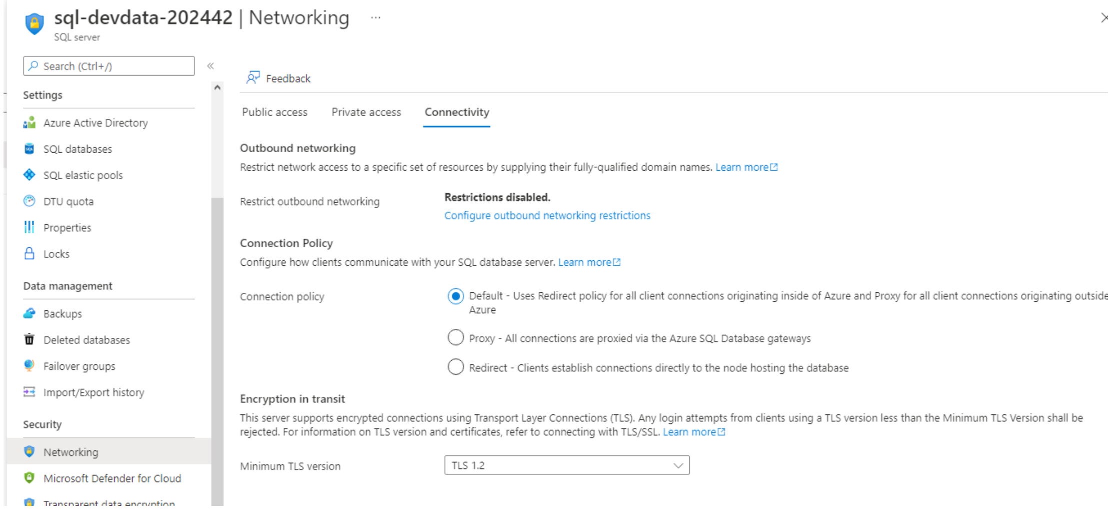
Connections from the IP addresses configured in the Firewall rules section below will have access to this database. By default, no public IP addresses are allowed. Learn more

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
newVnetRule1	Vnet-Dev	default	10.2.0.0/24	Enabled	rg-dev	0d904d18-8d...	Ready



sql-devdata-202442 | 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 and Proxy for all client connections originating outside Azure

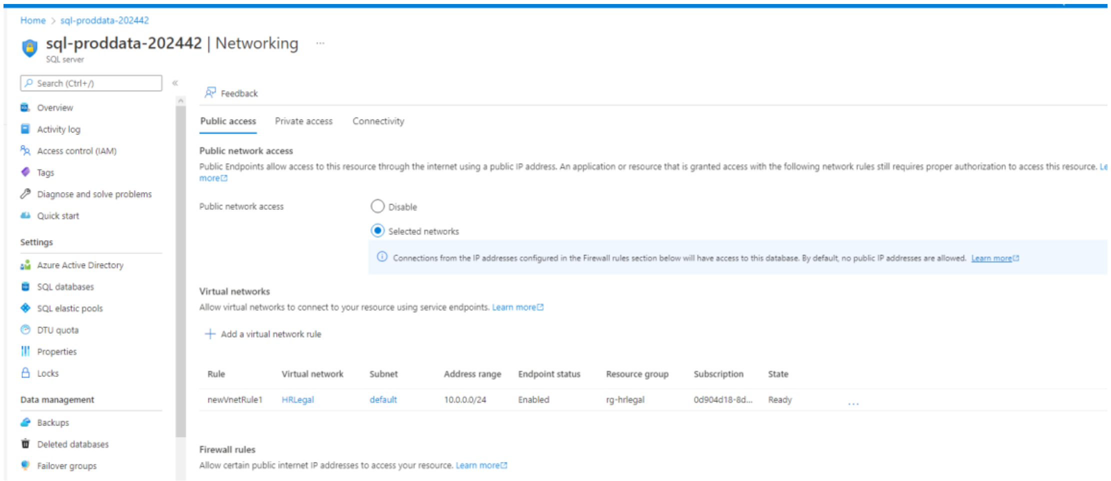
○ Proxy - All connections are proxied via the Azure SQL Database gateways

○ 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



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. Le 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

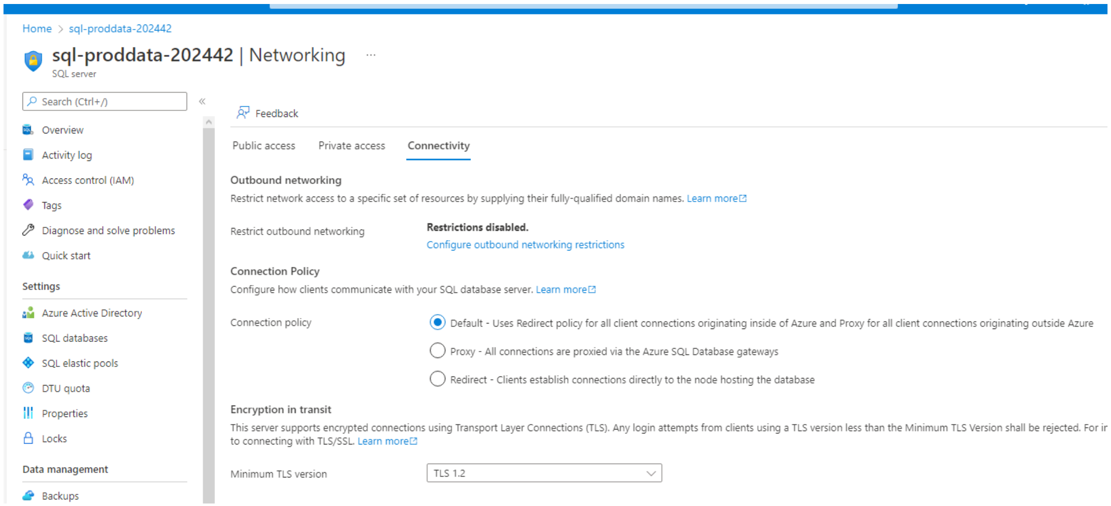
Allow virtual networks to connect to your resource using service endpoints. Learn more

+ Add a virtual network rule

Rule	Virtual network	Subnet	Address range	Endpoint status	Resource group	Subscription	State	
newVnetRule1	HRLegal	default	10.0.0.0/24	Enabled	rg-hrlegal	0d904d18-8d...	Ready	...

Firewall rules

Allow certain public internet IP addresses to access your resource. Learn more



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 and Proxy for all client connections originating outside Azure

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

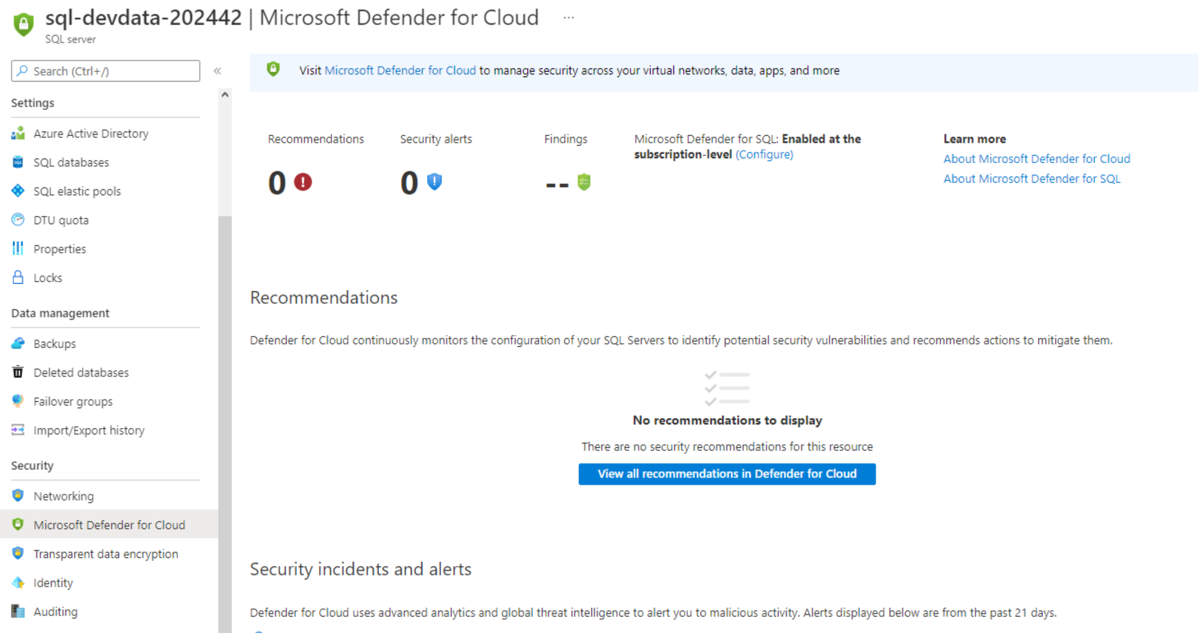
○ Redirect - Clients establish connections directly to the node hosting the database

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 ir to connecting with TLS/SSL. Learn more

Minimum TLS version TLS 1.2

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



sql-devdata-202442 | Microsoft Defender for Cloud

SQL server

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

Recommendations 0

Security alerts 0

Findings --

Microsoft Defender for SQL: **Enabled at the subscription-level** (Configure)

Learn more

About Microsoft Defender for Cloud

About Microsoft Defender for SQL

Recommendations

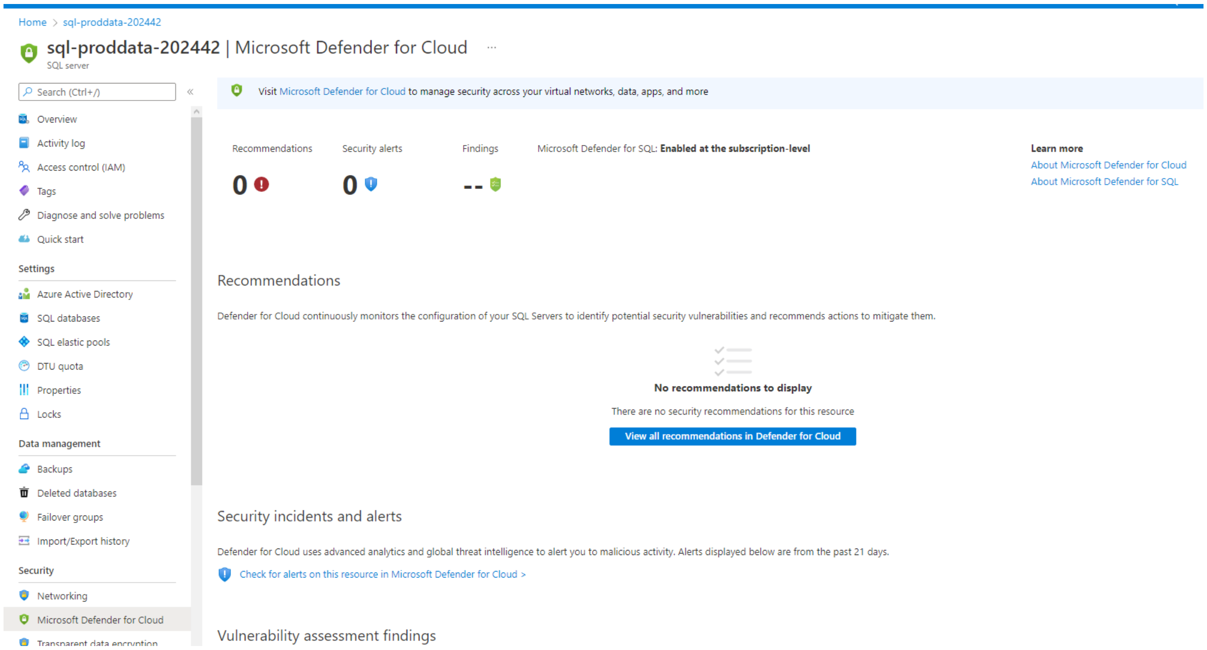
Defender for Cloud continuously monitors the configuration of your SQL Servers to identify potential security vulnerabilities and recommends actions to mitigate them.

No recommendations to display

There are no security recommendations for this resource

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.



sql-proddata-202442 | Microsoft Defender for Cloud

SQL server

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

Recommendations 0

Security alerts 0

Findings --

Microsoft Defender for SQL: **Enabled at the subscription-level**

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

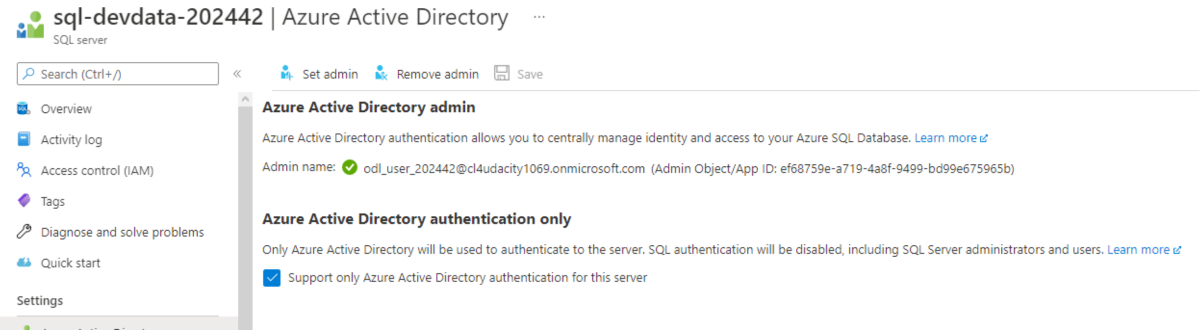
Security incidents and alerts

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

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



Azure Active Directory admin

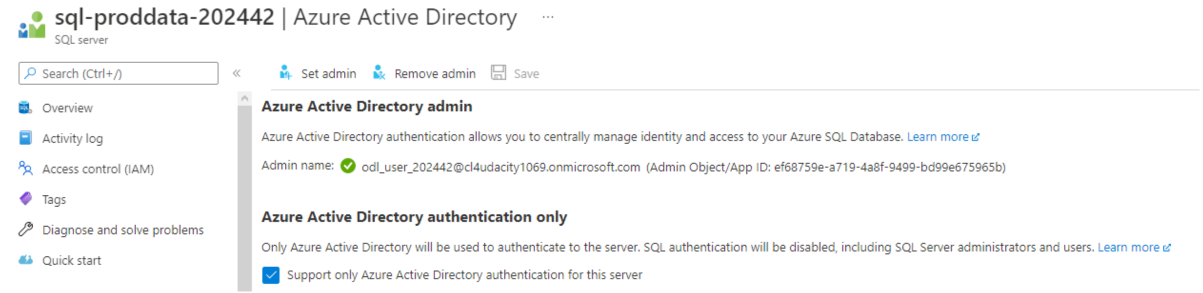
Azure Active Directory authentication allows you to centrally manage identity and access to your Azure SQL Database. Learn more

Admin name: ✓ odl_user_202442@cl4udacity1069.onmicrosoft.com (Admin Object/App ID: ef68759e-a719-4a8f-9499-bd99e675965b)

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



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_202442@cl4udacity1069.onmicrosoft.com (Admin Object/App ID: ef68759e-a719-4a8f-9499-bd99e675965b)

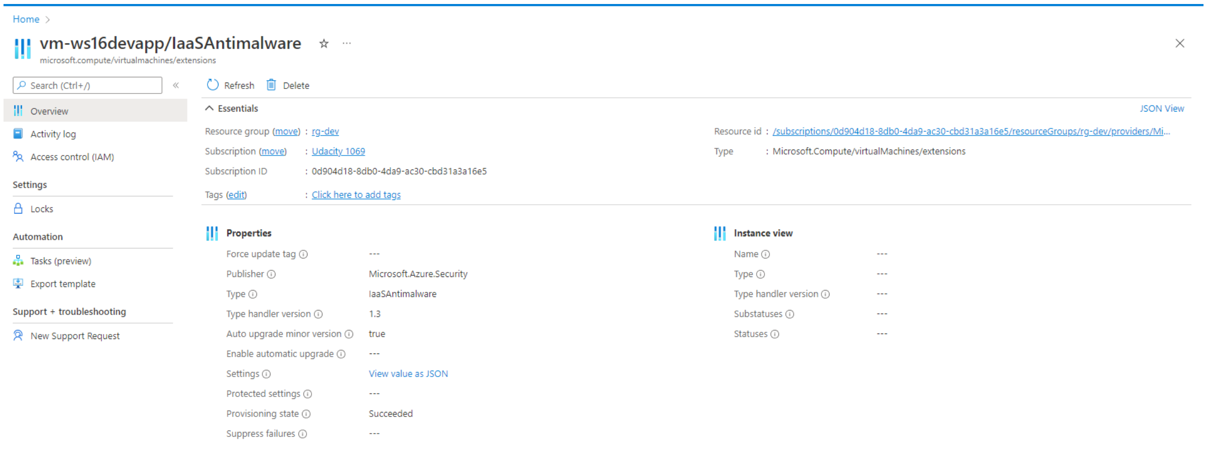
Azure Active Directory authentication only

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,DevWeb,OpApp,HRL-Web, HRL-App,OpWeb)



vm-ws16devapp/IaaSAntimalware

microsoft.compute/virtualmachines/extensions

Essentials

Resource group (move) : rg-dev

Subscription (move) : Udacity 1069

Subscription ID : 0d904d18-8db0-4da9-ac30-cbd31a3a16e5

Tags (edit) : Click here to add tags

Resource id : /subscriptions/0d904d18-8db0-4da9-ac30-cbd31a3a16e5/resourceGroups/rg-dev/providers/Mi...

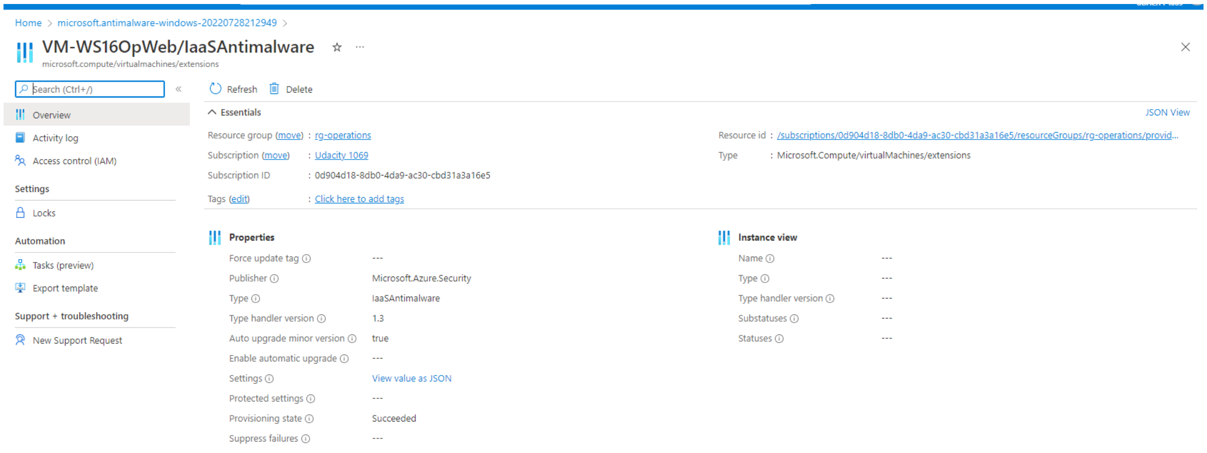
Type : Microsoft.Compute/virtualMachines/extensions

Properties

Force update tag	---
Publisher	Microsoft.Azure.Security
Type	IaaSAntimalware
Type handler version	1.3
Auto upgrade minor version	true
Enable automatic upgrade	---
Settings	View value as JSON
Protected settings	---
Provisioning state	Succeeded
Suppress failures	---

Instance view

Name	---
Type	---
Type handler version	---
Substatuses	---
Statuses	---



VM-WS16OpWeb/IaaSAntimalware

microsoft.compute/virtualmachines/extensions

Essentials

Resource group (move) : rg-operations

Subscription (move) : Udacity 1069

Subscription ID : 0d904d18-8db0-4da9-ac30-cbd31a3a16e5

Tags (edit) : Click here to add tags

Resource id : /subscriptions/0d904d18-8db0-4da9-ac30-cbd31a3a16e5/resourceGroups/rg-operations/provid...

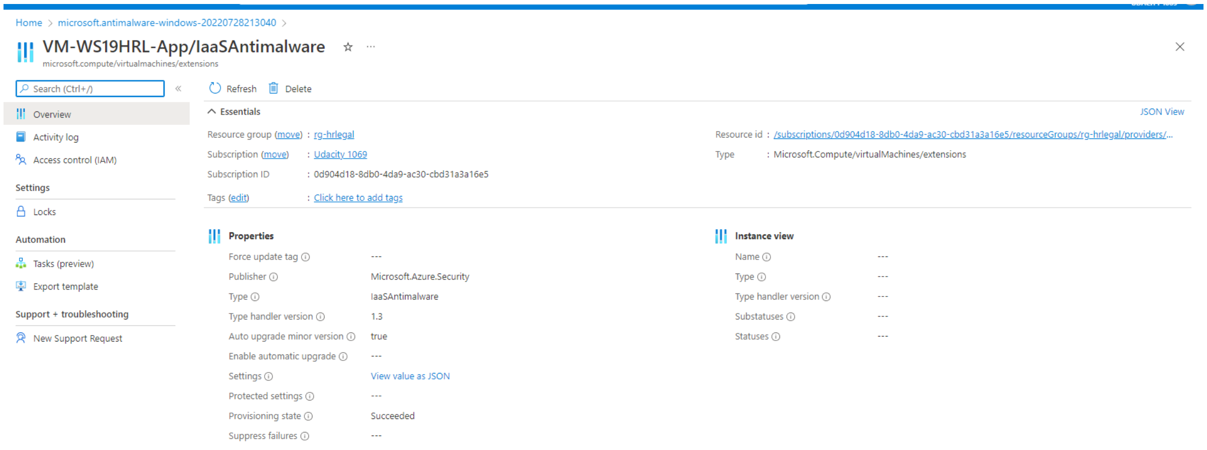
Type : Microsoft.Compute/virtualMachines/extensions

Properties

Force update tag	---
Publisher	Microsoft.Azure.Security
Type	IaaSAntimalware
Type handler version	1.3
Auto upgrade minor version	true
Enable automatic upgrade	---
Settings	View value as JSON
Protected settings	---
Provisioning state	Succeeded
Suppress failures	---

Instance view

Name	---
Type	---
Type handler version	---
Substatuses	---
Statuses	---



VM-WS19HRL-App/IaaSAntimalware

microsoft.compute/virtualmachines/extensions

Essentials

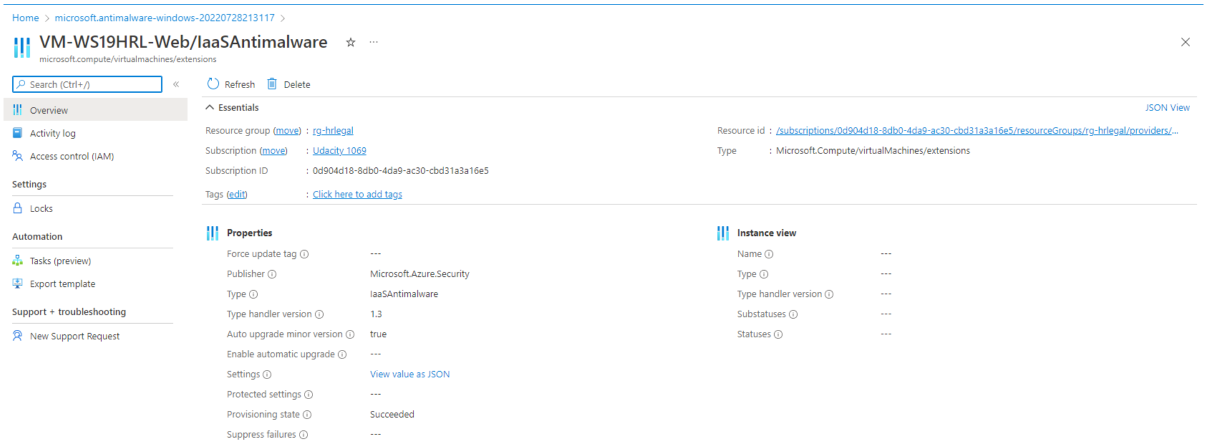
Resource group (move) : rg-hrlegal
Subscription (move) : Udacity 1069
Subscription ID : 0d904d18-8db0-4da9-ac30-cbd31a3a16e5
Tags (edit) : Click here to add tags
Resource id : /subscriptions/0d904d18-8db0-4da9-ac30-cbd31a3a16e5/resourceGroups/rg-hrlegal/providers/...
Type : Microsoft.Compute/virtualMachines/extensions

Properties

Force update tag	---
Publisher	Microsoft.Azure.Security
Type	IaaSAntimalware
Type handler version	1.3
Auto upgrade minor version	true
Enable automatic upgrade	---
Settings	View value as JSON
Protected settings	---
Provisioning state	Succeeded
Suppress failures	---

Instance view

Name	---
Type	---
Type handler version	---
Substatuses	---
Statuses	---



VM-WS19HRL-Web/IaaSAntimalware

microsoft.compute/virtualmachines/extensions

Essentials

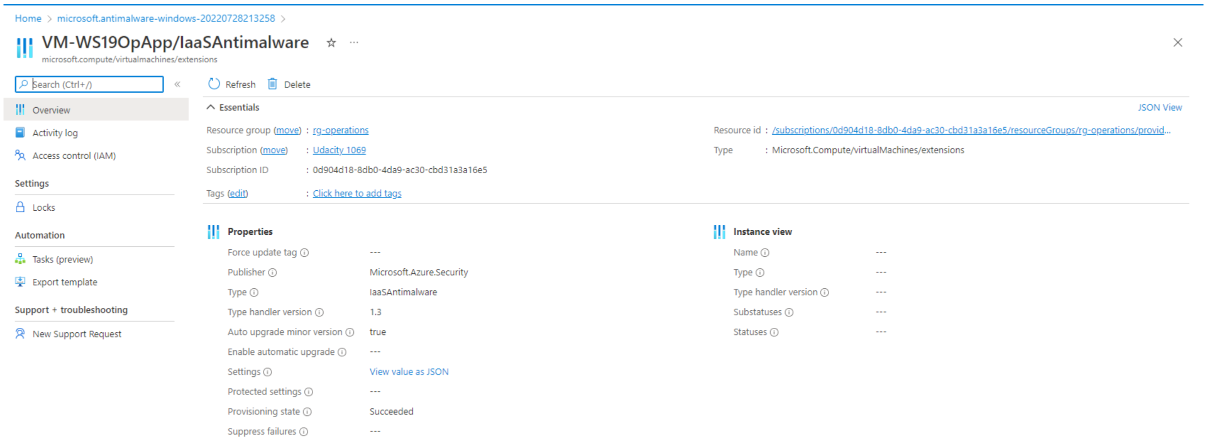
Resource group (move) : rg-hrlegal
Subscription (move) : Udacity 1069
Subscription ID : 0d904d18-8db0-4da9-ac30-cbd31a3a16e5
Tags (edit) : Click here to add tags
Resource id : /subscriptions/0d904d18-8db0-4da9-ac30-cbd31a3a16e5/resourceGroups/rg-hrlegal/providers/...
Type : Microsoft.Compute/virtualMachines/extensions

Properties

Force update tag	---
Publisher	Microsoft.Azure.Security
Type	IaaSAntimalware
Type handler version	1.3
Auto upgrade minor version	true
Enable automatic upgrade	---
Settings	View value as JSON
Protected settings	---
Provisioning state	Succeeded
Suppress failures	---

Instance view

Name	---
Type	---
Type handler version	---
Substatuses	---
Statuses	---



VM-WS19OpApp/IaaSAntimalware

microsoft.compute/virtualmachines/extensions

Essentials

Resource group (move) : rg-operations
Subscription (move) : Udacity 1069
Subscription ID : 0d904d18-8db0-4da9-ac30-cbd31a3a16e5
Tags (edit) : Click here to add tags
Resource id : /subscriptions/0d904d18-8db0-4da9-ac30-cbd31a3a16e5/resourceGroups/rg-operations/provid...
Type : Microsoft.Compute/virtualMachines/extensions

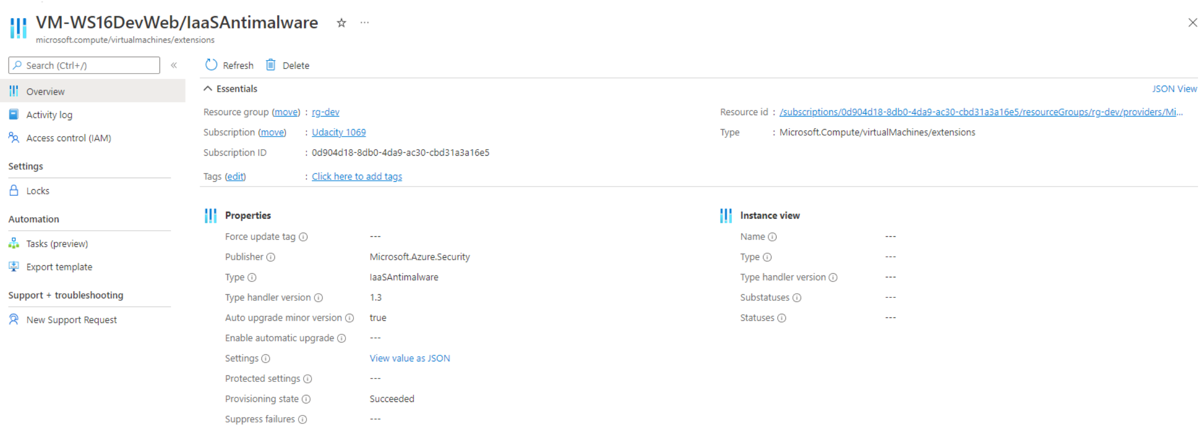
Properties

Force update tag	---
Publisher	Microsoft.Azure.Security
Type	IaaSAntimalware
Type handler version	1.3
Auto upgrade minor version	true
Enable automatic upgrade	---
Settings	View value as JSON
Protected settings	---
Provisioning state	Succeeded
Suppress failures	---

Instance view

Name	---
Type	---
Type handler version	---
Substatuses	---
Statuses	---

Antimalware on VM-WS16DevWeb:



VM-WS16DevWeb/IaaSAntimalware

microsoft.compute/virtualmachines/extensions

Resource group (move)	: rg-dev
Subscription (move)	: Udacity 1069
Subscription ID	: 0d904d18-8db0-4da9-ac30-cbd31a3a16e5
Tags (edit)	: Click here to add tags
Resource id	: /subscriptions/0d904d18-8db0-4da9-ac30-cbd31a3a16e5/resourceGroups/rg-dev/providers/Mi...
Type	: Microsoft.Compute/virtualMachines/extensions

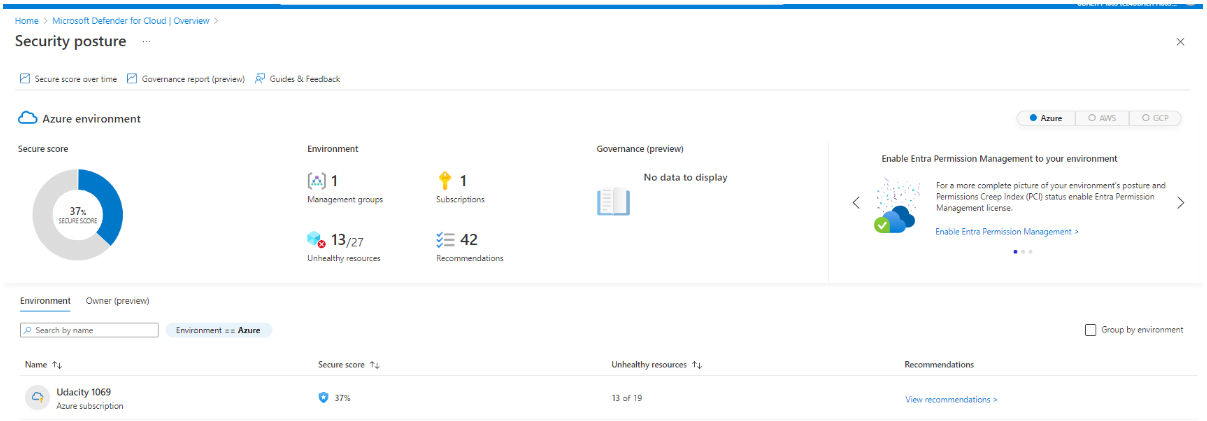
Properties

Force update tag ⓘ	---
Publisher ⓘ	Microsoft.Azure.Security
Type ⓘ	IaaSAntimalware
Type handler version ⓘ	1.3
Auto upgrade minor version ⓘ	true
Enable automatic upgrade ⓘ	---
Settings ⓘ	View value as JSON
Protected settings ⓘ	---
Provisioning state ⓘ	Succeeded
Suppress failures ⓘ	---

Instance view

Name ⓘ	---
Type ⓘ	---
Type handler version ⓘ	---
Substatuses ⓘ	---
Statuses ⓘ	---

2. Recommendations



Home > Microsoft Defender for Cloud | Overview >

Security posture

Secure score over time | Governance report (preview) | Guides & Feedback

Azure environment

● Azure ○ AWS ○ GCP

Secure score: 37% SECURE SCORE

Environment: 1 Management groups; 1 Subscriptions; 13/27 Unhealthy resources; 42 Recommendations

Governance (preview): No data to display

Enable Entra Permission Management to your environment

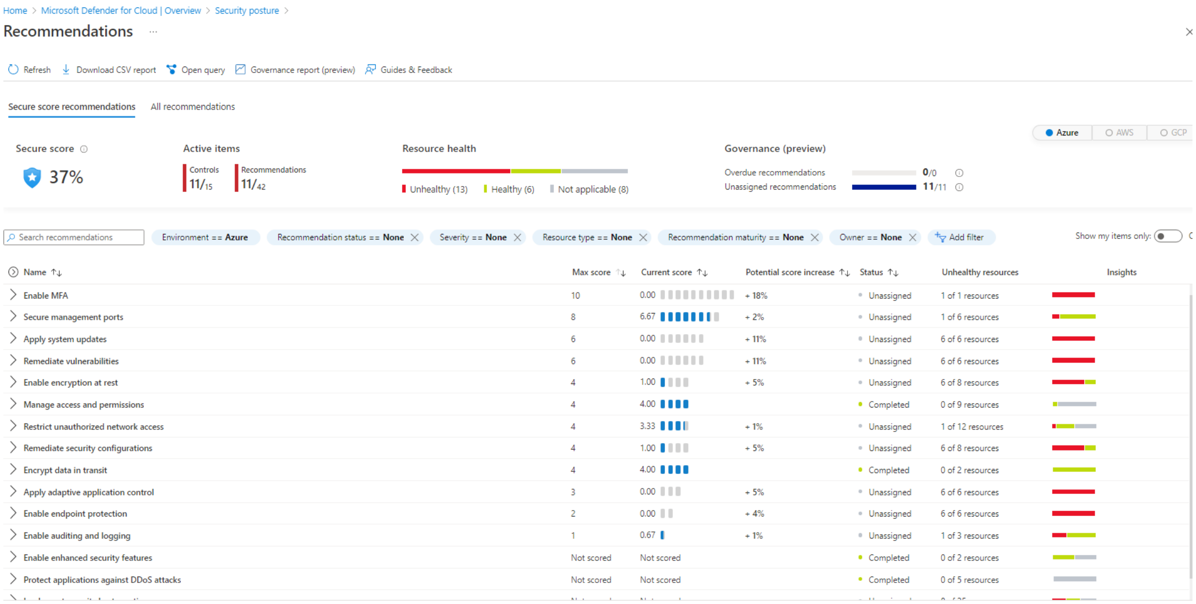
For a more complete picture of your environment's posture and Permissions Creep Index (PCI) status enable Entra Permission Management license.

Enable Entra Permission Management >

Environment | Owner (preview)

Search by name | Environment == Azure | □ Group by environment

Name ↑↓	Secure score ↑↓	Unhealthy resources ↑↓	Recommendations
Udacity 1069 Azure subscription	37%	13 of 19	View recommendations >



Home > Microsoft Defender for Cloud | Overview > Security posture >

Recommendations

Refresh | Download CSV report | Open query | Governance report (preview) | Guides & Feedback

Secure score recommendations | All recommendations

● Azure ○ AWS ○ GCP

Secure score: 37%

Active items: Controls 11/15; Recommendations 11/42

Resource health: Unhealthy (13) | Healthy (6) | Not applicable (8)

Governance (preview): Overdue recommendations 0/0; Unassigned recommendations 11/11

Search recommendations | Environment == Azure | Recommendation status == None | Severity == None | Resource type == None | Recommendation maturity == None | Owner == None | Add filter | Show my items only:

Name ↑↓	Max score ↑↓	Current score ↑↓	Potential score increase ↑↓	Status ↑↓	Unhealthy resources	Insights
Enable MFA	10	0.00	+ 18%	Unassigned	1 of 1 resources	
Secure management ports	8	6.67	+ 2%	Unassigned	1 of 6 resources	
Apply system updates	6	0.00	+ 11%	Unassigned	6 of 6 resources	
Remediate vulnerabilities	6	0.00	+ 11%	Unassigned	6 of 6 resources	
Enable encryption at rest	4	1.00	+ 5%	Unassigned	6 of 8 resources	
Manage access and permissions	4	4.00		Completed	0 of 9 resources	
Restrict unauthorized network access	4	3.33	+ 1%	Unassigned	1 of 12 resources	
Remediate security configurations	4	1.00	+ 5%	Unassigned	6 of 8 resources	
Encrypt data in transit	4	4.00		Completed	0 of 2 resources	
Apply adaptive application control	3	0.00	+ 5%	Unassigned	6 of 6 resources	
Enable endpoint protection	2	0.00	+ 4%	Unassigned	6 of 6 resources	
Enable auditing and logging	1	0.67	+ 1%	Unassigned	1 of 3 resources	
Enable enhanced security features	Not scored	Not scored		Completed	0 of 2 resources	
Protect applications against DDoS attacks	Not scored	Not scored		Completed	0 of 5 resources	

“Enable MFA” currently has a score of 0/10. This will have the biggest impact on security if we will fix it.

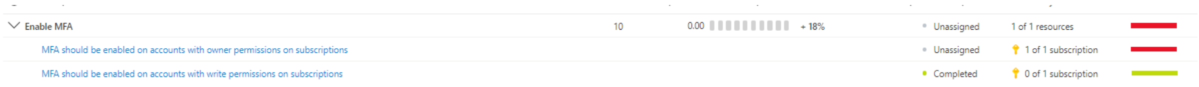
Multi-Factor Authentication (MFA) is a method used to authenticate our identity. It is often stated as a combination of two or more forms of

- What you know,
- What you have, or

- What you are

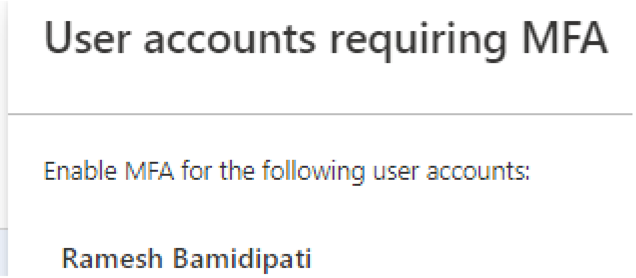
Multi-Factor Authentication has become commonplace in everyday life for most of us. It is so common we often use it without even realizing it. Banking is the most common use. When you use an ATM, you often use a card and a PIN. Your credit cards now have a chip that confirms the number on the card belongs to that chip and hasn't been duplicated onto a false card.

MFA must be used to ensure or verify that the individual logging in is actually himself not someone spoofing his identity. If someone else spoofs his identity by guessing/brute forcing into his account, this will lead to breach. MFA is very crucial in terms of security.



Enable MFA	10	0.00	+ 18%	Unassigned	1 of 1 resources	🟥
MFA should be enabled on accounts with owner permissions on subscriptions				Unassigned	1 of 1 subscription	🟥
MFA should be enabled on accounts with write permissions on subscriptions				Completed	0 of 1 subscription	🟩

Multi Factor Authentication is not set up for user account Ramesh Bamidipati.



User accounts requiring MFA

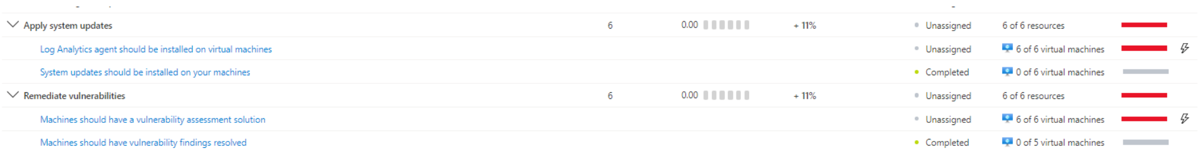
Enable MFA for the following user accounts:

Ramesh Bamidipati

Other 2 top remediations are “Apply system updates” and “Remediate vulnerabilities”. Both of them have a score of 0/6.

System Updates are crucial as hackers are constantly searching for their way in by any means. Systems sometimes have older versions installed for which many vulnerabilities are already known giving advantage to a hacker, in case one gets access to say a Windows XP machine, vulnerabilities and ways working best for this system are available on MITRE ATT&CK, hackers can use this to their advantage to Inject a malware into the system hence leading to other problems and eventually breach.

Security patches are constantly released for systems so keeping them up to date ensures that one cannot use that as an advantage to gain access to something. For example, the log4j vulnerability was found, very soon a system security patch was released fixing it. Which is basically the remedy for the vulnerability.



Apply system updates	6	0.00	+ 11%	Unassigned	6 of 6 resources
Log Analytics agent should be installed on virtual machines				Unassigned	6 of 6 virtual machines
System updates should be installed on your machines				Completed	0 of 6 virtual machines
Remediate vulnerabilities	6	0.00	+ 11%	Unassigned	6 of 6 resources
Machines should have a vulnerability assessment solution				Unassigned	6 of 6 virtual machines
Machines should have vulnerability findings resolved				Completed	0 of 5 virtual machines

We should install the log analytics agent on all of our VMs.

Log analytics also clarify patterns that relate to performance. Reviewing logs from data sources helps determine trends, allows for greater understanding of user behavior, and improves search functionality of application issues.

When something off is detected or an anomaly is detected logs help us search and know what happened due to what and decide on how to fix it. Security wise logs play an important role, the SoC team utilizes this a lot. Hence logs for ingress and egress for eg, are stored showing which packet came In from where containing what data, etc. Hence logs are very useful

Log Analytics Agent:

- Collect logs and performance data from Azure virtual machines or hybrid machines hosted outside of Azure.
- Send data to a Log Analytics workspace to take advantage of features supported by Azure Monitor Logs, such as log queries.
- Use VM insights, which allows you to monitor your machines at scale and monitor their processes and dependencies on other resources and external processes.
- Manage the security of your machines by using Microsoft Defender for Cloud or Microsoft Sentinel.
- Use Azure Automation Update Management, Azure Automation State Configuration, or Azure Automation Change Tracking and Inventory to deliver comprehensive management of your Azure and non-Azure machines.
- Use different solutions to monitor a particular service or application.

And we should install vulnerability assessment tools on our VMs.

Vulnerability scanning or vulnerability assessment is a systematic process of finding security loopholes in any system addressing the potential vulnerabilities.

The purpose of vulnerability assessments is to prevent the possibility of unauthorized access to systems. Vulnerability testing preserves the confidentiality, integrity, and availability of the system. The system refers to any computers, networks, network devices, software, web application, cloud computing, etc.

Types of Vulnerability Scanners

Vulnerability scanners have their ways of doing jobs. We can classify the vulnerability scanners into four types based on how they operate.

Cloud-Based Vulnerability Scanners

Used to find vulnerabilities within cloud-based systems such as web applications, WordPress, and Joomla.

Host-Based Vulnerability Scanners

Used to find vulnerabilities on a single host or system such as an individual computer or a network device like a switch or core-router.

Network-Based Vulnerability Scanners

Used to find vulnerabilities in an internal network by scanning for open ports. Services running on open ports determined whether vulnerabilities exist or not with the help of the tool.

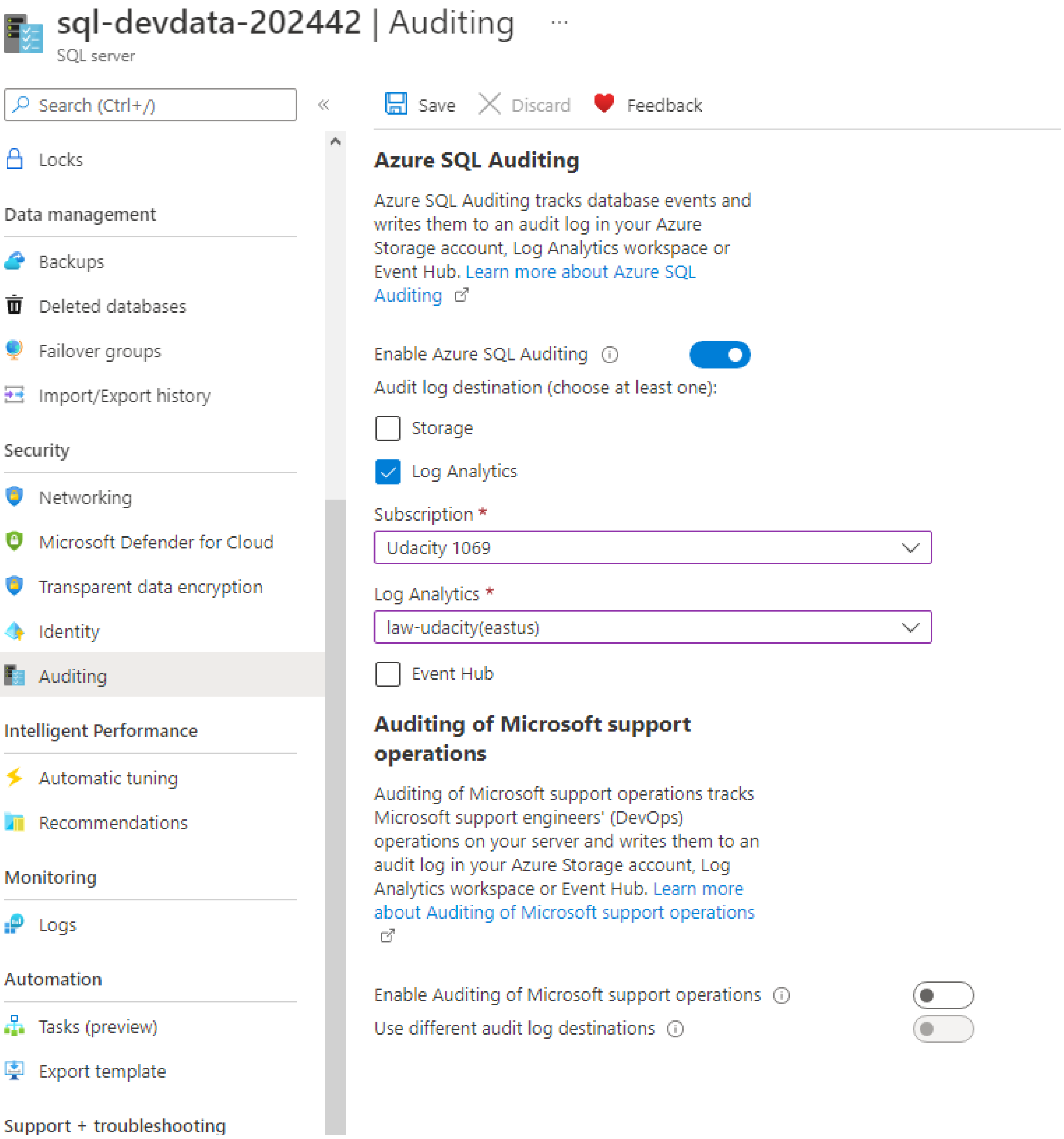
Database-Based Vulnerability Scanners

Used to find vulnerabilities in database management systems. Databases are the backbone of any system storing sensitive information. Vulnerability scanning is performed on database systems to prevent attacks like SQL Injection.

Eg: Microsoft Baseline Security Analyzer (MBSA), Nmap, Nessus, Nikto2 etc.

Monitoring

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



sql-devdata-202442 | 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 ⓘ ●

Audit log destination (choose at least one):

☐ Storage

☑ Log Analytics

Subscription *

Udacity 1069

Log Analytics *

law-udacity(eastus)

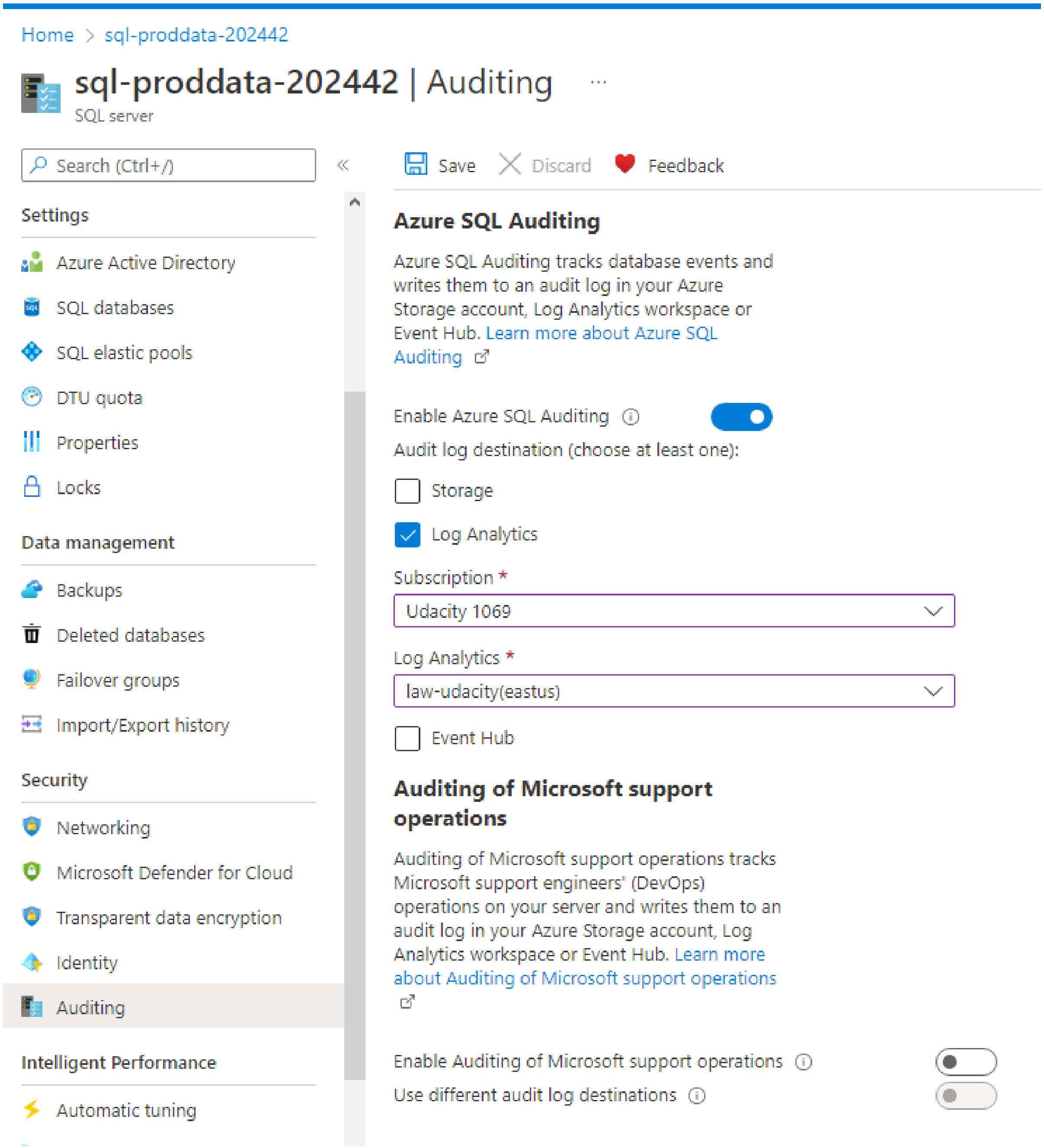
☐ Event Hub

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 ⓘ ○



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 1069

Log Analytics *: law-udacity(eastus)

□ Event Hub

Auditing of Microsoft support operations

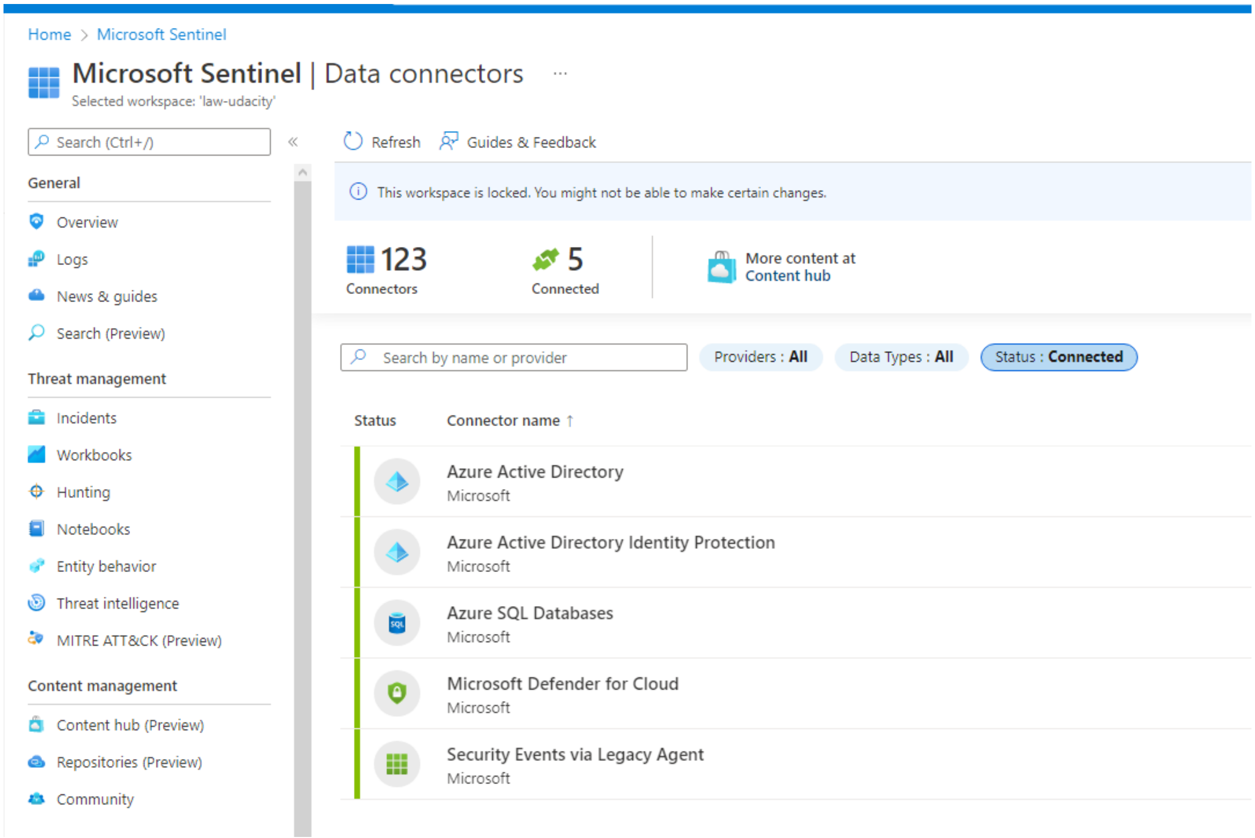
Auditing of Microsoft support operations tracks Microsoft support engineers' (DevOps) operations on your server and writes them to an audit log in your Azure Storage account, Log Analytics workspace or Event Hub. Learn more about Auditing of Microsoft support operations

Enable Auditing of Microsoft support operations ⓘ ○

Use different audit log destinations ⓘ ○

2. Proof of Sentinel connectors (2+)

Adding Azure AD Connector to Sentinel:

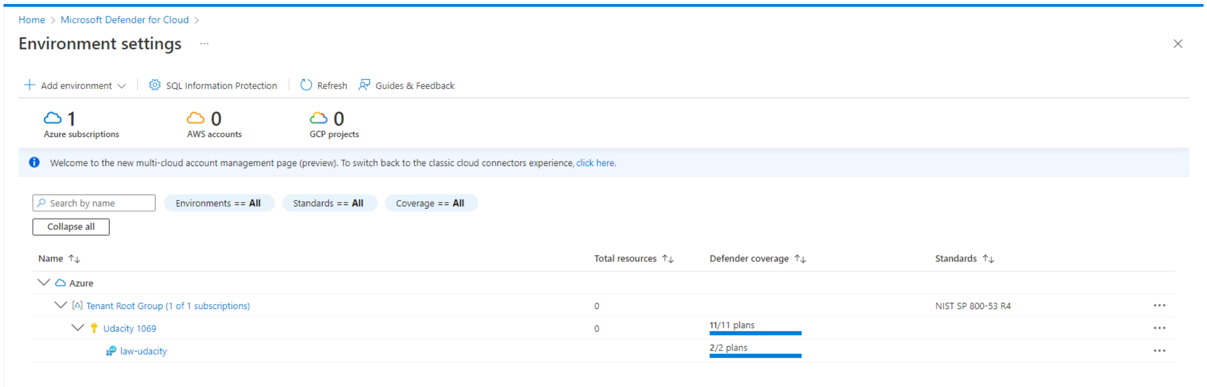


This workspace is locked. You might not be able to make certain changes.

Status	Connector name ↑
Connected	Azure Active Directory Microsoft
Connected	Azure Active Directory Identity Protection Microsoft
Connected	Azure SQL Databases Microsoft
Connected	Microsoft Defender for Cloud Microsoft
Connected	Security Events via Legacy Agent Microsoft

Compliance

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



Environment settings

1 Azure subscriptions

0 AWS accounts

0 GCP projects

Welcome to the new multi-cloud account management page (preview). To switch back to the classic cloud connectors experience, click here.

Environments == **All** | Standards == **All** | Coverage == **All**

Name ↑↓	Total resources ↑↓	Defender coverage ↑↓	Standards ↑↓	
Azure				
Tenant Root Group (1 of 1 subscriptions)	0		NIST SP 800-53 R4	...
Udacity 1069	0	11/11 plans		...
law-udacity		2/2 plans		...