

Attention students:

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

Identity and Access Management

1. Proof of Assigned roles and AD assignments

- a. Andrew
- b. Chris
- c. Karl
- d. Lora
- e. Neelima
- f. Neha
- g. Seth
- h. Srinadh
- i. Tom
- j. Winifred

The image contains two screenshots of the Microsoft Azure portal, both titled "Executive | Assigned roles" and "Executive | Members".

Executive | Assigned roles (Top Screenshot):

- Overview:** Shows a single assignment: "Message Center Reader" for "Directory" scope, "Direct" membership, and "Active" state, starting on 4/9/2023 at 5:28:19 PM and ending as permanent.
- Manage:** Under "Assigned roles", "Chris" and "Karl" are listed as members.

Role	Principal name	Scope	Membership	State	Start time	End time	Action
Message Center Reader		Directory	Direct	Active	4/9/2023, 5:28:19 PM	Permanent	Remove Update

Executive | Members (Bottom Screenshot):

- Overview:** Shows "Chris" and "Karl" as direct members.
- Manage:** Under "Members", "Chris" and "Karl" are listed as members.

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

Microsoft Azure Search resources, services, and docs (G+)

Home > Groups | All groups > IT

IT | Members

Group

Overview

Diagnose and solve problems

Manage

- Properties
- Members**
- Owners
- Roles and administrators
- Administrative units
- Group memberships
- Applications
- Licenses
- Azure role assignments

Activity

Privileged Identity Management (Preview)

Direct members All members

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

Search by name Add filters

Microsoft Azure Search resources, services, and docs (G+)

Home > Groups | All groups > HR

HR | Members

Group

Overview

Diagnose and solve problems

Manage

- Properties
- Members**
- Owners
- Roles and administrators
- Administrative units
- Group memberships
- Applications
- Licenses
- Azure role assignments

Direct members All members

Name	Type	Email	User type
LO Lora	User		Member

Search by name Add filters

Microsoft Azure Search resources, services, and docs (G+)

Home > Groups | All groups > HR

HR | Assigned roles

Group

Overview

Diagnose and solve problems

Manage

- Properties
- Members
- Owners
- Roles and administrators
- Administrative units
- Group memberships
- Assigned roles**
- Applications
- Licenses
- Azure role assignments

Add assignments Refresh Got feedback?

Eligible assignments Active assignments Expired assignments

User	Role	Principal name	Scope	Membership	Start time	End time	Action
	User Administrator		Directory	Direct	4/9/2023, 5:51:14 PM	Permanent	Remove Update

Microsoft Azure Search resources, services, and docs (G+)

Home > Groups | All groups > Support Desk

Support Desk | Members

Group

[Overview](#) [Diagnose and solve problems](#)

Manage

- [Properties](#)
- [Members](#) **Selected**
- [Owners](#)
- [Roles and administrators](#)
- [Administrative units](#)
- [Group memberships](#)
- [Assigned roles](#)
- [Applications](#)
- [Licenses](#)
- [Azure role assignments](#)

[Activity](#)

[Add members](#) [Remove](#) [Refresh](#) [Bulk operations](#) [Columns](#) [Got feedback?](#)

Direct members All members

Name	Type	Email	User type
Wi Winifred	User		Member

Microsoft Azure Search resources, services, and docs (G+)

Home > Groups | All groups > Support Desk

Support Desk | Assigned roles

Group

[Overview](#) [Diagnose and solve problems](#)

Manage

- [Properties](#)
- [Members](#)
- [Owners](#)
- [Roles and administrators](#)
- [Administrative units](#)
- [Group memberships](#)
- [Assigned roles](#) **Selected**
- [Applications](#)
- [Licenses](#)

[Add assignments](#) [Refresh](#) [Got feedback?](#)

Eligible assignments Active assignments Expired assignments

Role	Principal name	Scope	Membership	Start time	End time	Action
Helpdesk Administrator		Directory	Direct	4/9/2023, 6:35:22 PM	Permanent	Remove Update

Microsoft Azure Search resources, services, and docs (G+)

Home > Karl

Karl | Assigned roles

User

[Diagnose and solve problems](#)

Manage

- [Profile](#)
- [Custom security attributes \(preview\)](#)
- [Assigned roles](#) **Selected**
- [Roles and administrators](#)
- [Administrative units](#)
- [Groups](#)
- [Applications](#)
- [Licenses](#)

[Add assignments](#) [Refresh](#) [Got feedback?](#)

Eligible assignments Active assignments Expired assignments

Role	Principal name	Scope	Membership	State	Start time	End time	Action
Message Center Reader	Karl@cl4udacity1071...	Directory	Group	Active	4/9/2023, 5:28:19 PM	Permanent	Remove Update
Billing Administrator	Karl@cl4udacity1071...	Directory	Direct	Active	4/9/2023, 6:37:54 PM	Permanent	Remove Update

Microsoft Azure Search resources, services, and docs (G+) odl_user_230277@c4ud... UDACITY 1071 (CLAUDACITY1071...)

Home > All resources > rg-devdata

All resources

rg-devdata | Access control (IAM) ...

Resource group

	Name	Type	Role	Subscription	Encryption User
<input type="checkbox"/>	Identity not found.	Unknown	Key Vault Crypto Service	Subscription (Inherited)	None
Kubernetes Extension Contributor					
> Log Analytics Contributor					
Owner					
<input type="checkbox"/>	Foreign Principal for https://c4udacity1071...	Foreign principal	Owner	Subscription (Inherited)	None
<input type="checkbox"/>	App https://c4udacity1071...	App	Owner	Subscription (Inherited)	None
<input type="checkbox"/>	User Ramesh_Bamidipati admin@c4udacity...	User	Owner	Subscription (Inherited)	None
<input type="checkbox"/>	User Neha Neha@c4udacity...	User	Owner	This resource	None
<input type="checkbox"/>	User ODL_User_230277 odl_user_230277...	User	Owner	This resource	None
<input type="checkbox"/>	User Srinadh Srinadh@c4udaci...	User	Owner	This resource	None
Reader					
<input type="checkbox"/>	User ODL_User_230277 odl_user_230277...	User	Reader	Subscription (Inherited)	None
> Security Admin					

Events

Settings

Deployments

Security

Policies

Properties

Locks

Cost Management

Cost analysis

Cost alerts (preview)

Rainbow

Microsoft Azure Search resources, services, and docs (G+) odl_user_230277@c4ud... UDACITY 1071 (CLAUDACITY1071...)

Home > All resources > rg-data

All resources

rg-data | Access control (IAM) ...

Resource group

	Name	Type	Role	Subscription	Encryption User
<input type="checkbox"/>	Defender for Container	App	Log Analytics Contributor	Subscription (Inherited)	None
<input type="checkbox"/>	Defender for Container	App	Log Analytics Contributor	Subscription (Inherited)	None
<input type="checkbox"/>	Defender for Container	App	Log Analytics Contributor	Subscription (Inherited)	None
Owner					
<input type="checkbox"/>	Foreign Principal for https://c4udacity1071...	Foreign principal	Owner	Subscription (Inherited)	None
<input type="checkbox"/>	App https://c4udacity1071...	App	Owner	Subscription (Inherited)	None
<input type="checkbox"/>	User Ramesh_Bamidipati admin@c4udacity...	User	Owner	Subscription (Inherited)	None
<input type="checkbox"/>	User ODL_User_230277 odl_user_230277...	User	Owner	This resource	None
<input type="checkbox"/>	User Srinadh Srinadh@c4udaci...	User	Owner	This resource	None
Reader					
<input type="checkbox"/>	User ODL_User_230277 odl_user_230277...	User	Reader	Subscription (Inherited)	None
> Security Admin					

Events

Settings

Deployments

Security

Policies

Properties

Locks

Cost Management

Cost analysis

Cost alerts (preview)

sql-devdata-230277 | Access control (IAM)

	Role	Principal	Subscription	Notes
<input type="checkbox"/>	App	Defender for Contain	Log Analytics Contributor	Subscription (Inherited) None
<input type="checkbox"/>	App	https://cl4udacity10	Log Analytics Contributor	Subscription (Inherited) None
Owner				
<input type="checkbox"/>	Foreign Principal for	Foreign principal	Owner	Subscription (Inherited) None
<input type="checkbox"/>	App	Owner	Subscription (Inherited) None	Subscription (Inherited) None
<input type="checkbox"/>	User	Ramesh Bamidipati	Owner	Subscription (Inherited) None
<input type="checkbox"/>	User	Neha	Owner	Resource group (Inherited) None
<input type="checkbox"/>	User	ODL_User_230277	Owner	Resource group (Inherited) None
<input type="checkbox"/>	User	Srinadh	Owner	Resource group (Inherited) None
Reader				

sql-proodata-230277 | Access control (IAM)

	Role	Principal	Subscription	Notes
<input type="checkbox"/>	App	Defender for Contain	Log Analytics Contributor	Subscription (Inherited) None
<input type="checkbox"/>	App	https://cl4udacity10	Log Analytics Contributor	Subscription (Inherited) None
Owner				
<input type="checkbox"/>	Foreign Principal for	Foreign principal	Owner	Subscription (Inherited) None
<input type="checkbox"/>	App	Owner	Subscription (Inherited) None	Subscription (Inherited) None
<input type="checkbox"/>	User	Ramesh Bamidipati	Owner	Subscription (Inherited) None
<input type="checkbox"/>	User	ODL_User_230277	Owner	Resource group (Inherited) None
<input type="checkbox"/>	User	Srinadh	Owner	Resource group (Inherited) None
Reader				

rg-dev | Access control (IAM)

Added Role assignment
ODL_User_230277 was added as Contributor for rg-dev.

	Role	Principal	Subscription	Notes
<input type="checkbox"/>	App	Defender for Contain	Contributor Role	Subscription (Inherited) None
<input type="checkbox"/>	App	Defender for Contain	Contributor Role	Subscription (Inherited) None
<input type="checkbox"/>	App	Defender for Contain	Contributor Role	Subscription (Inherited) None
Contributor				
<input type="checkbox"/>	App	8c90677cada14be1b	Contributor	Subscription (Inherited) None
<input type="checkbox"/>	App	Defender for Contain	Contributor	Subscription (Inherited) None
<input type="checkbox"/>	App	Defender for Contain	Contributor	Subscription (Inherited) None
<input type="checkbox"/>	App	Defender for Contain	Contributor	Subscription (Inherited) None
<input type="checkbox"/>	User	Neelima	Contributor	This resource None
<input type="checkbox"/>	User	ODL_User_230277	Contributor	This resource None

Microsoft Azure Search resources, services, and docs (G+) odl_user_230277@cl4ud...
UDACITY 1071 (CL4UDACITY1071...)

Home > Users > Karl

Karl | Assigned roles

User

+ Add assignments Refresh Got feedback?

Overview Audit logs Sign-in logs Diagnose and solve problems

Manage Custom security attributes (preview)

Assigned roles (selected) Administrative units Groups

Eligible assignments Active assignments Expired assignments

Search by role

Role	Principal name	Scope	Membership	State	Start time	End time	Action
Message Center Reader	Karl@cl4udacity1071...	Directory	Group	Active	4/9/2023, 5:28:19 PM	Permanent	Remove Update
Billing Administrator	Karl@cl4udacity1071....	Directory	Direct	Active	4/9/2023, 6:37:54 PM	Permanent	Remove Update

Microsoft Azure Search resources, services, and docs (G+) odl_user_230277@cl4ud...
UDACITY 1071 (CL4UDACITY1071...)

Home > Users > Seth

Seth | Assigned roles

User

+ Add assignments Refresh Got feedback?

Overview Audit logs Sign-in logs Diagnose and solve problems

Manage Custom security attributes (preview)

Assigned roles (selected) Administrative units Groups Applications Licenses

Eligible assignments Active assignments Expired assignments

Search by role

Role	Principal name	Scope	Membership	Start time	End time	Action
Global Administrator	Seth@cl4udacity1071.on...	Directory	Direct	4/9/2023, 7:17:01 PM	Permanent	Remove Update
Billing Administrator	Seth@cl4udacity1071.on...	Directory	Direct	4/9/2023, 7:17:34 PM	Permanent	Remove Update

Vnet-Dev | Access control (IAM)

	Identity	Type	Role	Scope	Access Level
<input type="checkbox"/>	Identity not found.	Unknown	Log Analytics Contributor	Subscription (Inherited)	None
<input type="checkbox"/>	Identity not found.	Unknown	Log Analytics Contributor	Subscription (Inherited)	None
Owner					
<input type="checkbox"/>	Foreign Principal for https://cl4udacity10'	Foreign principal	Owner	Subscription (Inherited)	None
<input type="checkbox"/>	Ramesh Bamidipati admin@cl4udacity...	User	Owner	Subscription (Inherited)	None
<input checked="" type="checkbox"/>	Neha Neha@cl4udacity...	User	Owner	This resource	None
<input type="checkbox"/>	ODL_User 231021 odl_user_231021...	User	Owner	Resource group (Inherited)	None
<input checked="" type="checkbox"/>	Srinadh Srinadh@cl4udaci...	User	Owner	This resource	None
Reader					
<input type="checkbox"/>	ODL_User 231021 odl_user_231021...	User	Reader	Subscription (Inherited)	None
Security Admin					
<input type="checkbox"/>	ODL_User 231021 odl_user_231021...	User	Security Admin	Subscription (Inherited)	None
Spektra Custom RBAC I1379 S1					
<input type="checkbox"/>	ODL_User 231021 odl_user_231021...	User	Spektra Custom RBAC I1379 S1	Subscription (Inherited)	None
<input type="checkbox"/>	ODL_User 231021 odl_user_231021...	User	Spektra Custom RBAC I1379 S1	Resource group (Inherited)	None

VNet-prod | Access control (IAM)

	Identity	Type	Role	Scope	Access Level
<input type="checkbox"/>	Identity not found.	Unknown	Log Analytics Contributor	Subscription (Inherited)	None
<input type="checkbox"/>	Identity not found.	Unknown	Log Analytics Contributor	Subscription (Inherited)	None
Owner					
<input type="checkbox"/>	Foreign Principal for https://cl4udacity10'	Foreign principal	Owner	Subscription (Inherited)	None
<input type="checkbox"/>	Ramesh Bamidipati admin@cl4udacity...	User	Owner	Subscription (Inherited)	None
<input type="checkbox"/>	ODL_User 231021 odl_user_231021...	User	Owner	Resource group (Inherited)	None
<input type="checkbox"/>	Srinadh Srinadh@cl4udaci...	User	Owner	This resource	None
Reader					
<input type="checkbox"/>	ODL_User 231021 odl_user_231021...	User	Reader	Subscription (Inherited)	None
Security Admin					
<input type="checkbox"/>	ODL_User 231021 odl_user_231021...	User	Security Admin	Subscription (Inherited)	None
Spektra Custom RBAC I1379 S1					

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

Global Administrator | Role settings

Activation

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

Assignment

Setting	State
Allow permanent eligible assignment	No
Expire eligible assignments after	6 month(s)
Allow permanent active assignment	No
Expire active assignments after	6 month(s)
Require Azure Multi-Factor Authentication on active assignment	No
Require justification on active assignment	Yes

Send notifications when members are assigned as eligible to this role:

Type	Default recipients	Additional recipients	Critical emails only
Role assignment alert	Admin	None	False

3. Proof of Conditional Access policy all users

Grant

Control access enforcement to block or grant access. [Learn more](#)

Block access

Grant access

Require multifactor authentication

Consider testing the new multi-factor authentication strength public preview. [Learn more](#)

Require authentication strength (Preview)

⚠️ "Require authentication strength" cannot be used with "Require multifactor authentication". [Learn more](#)

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

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

save

Network Security

1. Bastion overview

The screenshot shows the Microsoft Azure portal interface for the 'VNet-core-bastion' resource. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Sessions, Configuration, Properties, Locks), Monitoring (Metrics, Logs, Diagnostics settings, Connection Troubleshoot), and Automation (Tasks). The main content area displays the 'Essentials' section with the following details:

Resource group (move)	rg-core	Virtual network/subnet	VNet-core/AzureBastionSubnet
Location	East US	Public DNS name	bst-613a7841-0b94-4f75-85cf-1029a4b42bcc.bastion.azure.com
Subscription (move)	Udacity_1071	Public IP address	VNet-core-ip
Subscription ID	46c79782-e579-4022-a44c-abfefce2f14c	Tier	Basic
		Provisioning state	Succeeded

Tags (edit): DeploymentId : 230277, LaunchId : 1379, LaunchType : ON_DEMAND_LAB, TemplateId : 1211, TenantId : 203

Below the Essentials section is a table for Sessions and Tutorials, which currently shows 'No results.'

2. Proof of public IP addresses removed

The screenshot shows the Microsoft Azure portal interface for the 'VM-WS16DevWeb' virtual machine. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Networking, Connect, Windows Admin Center, Disks, Size, Microsoft Defender for Cloud, Advisor recommendations, Extensions + applications, Continuous delivery), Properties, Monitoring, Capabilities (8), Recommendations, and Tutorials. The main content area displays the 'Essentials' section with the following details:

Resource group (move)	rg-dev	Operating system	Windows
Status	Stopped (deallocated)	Size	Standard B2s (2 vcpus, 4 GiB memory)
Location	East US	Public IP address	-
Subscription (move)	Udacity_1071	Virtual network/subnet	Vnet-Dev/default
Subscription ID	46c79782-e579-4022-a44c-abfefce2f14c	DNS name	-

Tags (edit): DeploymentId : 230277, LaunchId : 1379, LaunchType : ON_DEMAND_LAB, TemplateId : 1211, TenantId : 203

Below the Essentials section is a table for Properties, Monitoring, Capabilities (8), Recommendations, and Tutorials. The 'Virtual machine' section shows the following details:

Computer name	VM-WS16DevWeb
Health state	-
Operating system	Windows
Publisher	MicrosoftWindowsServer
Offer	WindowsServer
Plan	2019-Datacenter

The 'Networking' section shows the following details:

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	-

Microsoft Azure Search resources, services, and docs (G+) odl_user_230277@cl4ud... UDACITY 1071

Home > VM-WS16OpWeb Virtual machine

VM-WS16OpWeb Overview

Essentials

Resource group (move) : rg-operations	Operating system : Windows
Status : Stopped (deallocated)	Size : Standard B2s (2 vcpus, 4 GiB memory)
Location : East US	Public IP address : -
Subscription (move) : Udacity_1071	Virtual network/subnet : Vnet-operations/default
Subscription ID : 46c79782-e579-4022-a44c-abfefce2f14c	DNS name : -
Tags (edit) : DeploymentId : 230277 LaunchId : 1379 LaunchType : ON_DEMAND_LAB TemplateId : 1211 TenantId : 203	

Properties Monitoring Capabilities (8) Recommendations Tutorials

Virtual machine

Computer name : VM-WS16OpWeb	Networking
Health state : -	Public IP address : -
Operating system : Windows	Public IP address (IPv6) : -
Publisher : MicrosoftWindowsServer	Private IP address : 10.0.0.4
Offer : WindowsServer	Private IP address (IPv6) : -
Plan : 2019-Datacenter	Virtual network/subnet : Vnet-operations/default
VM generation : V1	DNS name : -
VM architecture : x64	Size
Host group : None	Size : Standard B2s
Host : -	vCPUs : 2
Proximity placement group : -	RAM : 4 GiB

Networking

Size

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Networking

Connect

Windows Admin Center

Disk

Size

Microsoft Defender for Cloud

Advisor recommendations

Extensions + applications

Continuous delivery

Availability + scaling

Configuration

Identity

Properties

Locks

Microsoft Azure Search resources, services, and docs (G+) odl_user_230277@cl4ud... UDACITY 1071

Home > VM-WS19HRL-Web Virtual machine

VM-WS19HRL-Web Overview

Essentials

Resource group (move) : rg-hrlegal	Operating system : Windows
Status : Stopped (deallocated)	Size : Standard B2s (2 vcpus, 4 GiB memory)
Location : East US	Public IP address : -
Subscription (move) : Udacity_1071	Virtual network/subnet : HRLegal/default
Subscription ID : 46c79782-e579-4022-a44c-abfefce2f14c	DNS name : -
Tags (edit) : DeploymentId : 230277 LaunchId : 1379 LaunchType : ON_DEMAND_LAB TemplateId : 1211 TenantId : 203	

Properties Monitoring Capabilities (8) Recommendations Tutorials

Virtual machine

Computer name : VM-WS19HRL-Web	Networking
Health state : -	Public IP address : -
Operating system : Windows	Private IP address : 10.0.0.4
Publisher : MicrosoftWindowsServer	Private IP address (IPv6) : -
Offer : WindowsServer	Virtual network/subnet : HRLegal/default
Plan : 2019-Datacenter	DNS name : -
VM generation : V1	Size
VM architecture : x64	Size : Standard B2s
Host group : None	

Networking

Size

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Networking

Connect

Windows Admin Center

Disk

Size

Microsoft Defender for Cloud

Advisor recommendations

Extensions + applications

Continuous delivery

Availability + scaling

Configuration

Identity

Data and Encryption

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

The image contains two side-by-side screenshots of the Microsoft Azure portal, both titled "Encryption".

Screenshot 1: VM-WS16DevWeb-osdisk | Encryption

- Left Panel (Navigation):** Home > All resources > VM-WS16DevWeb | Disks > VM-WS16DevWeb-osdisk
- Right Panel (Main Content):**
 - Encryption Settings:** Key management dropdown shows "Customer-managed key: disk-dec".
 - Information:** "Azure offers server-side encryption with platform-managed keys by default for managed disks. You may optionally choose to use a customer-managed key." with a "Learn more" link.
 - Feedback:** "Give feedback" and "Help improve this page" links.

Screenshot 2: VM-WS16OpWeb-osdisk | Encryption

- Left Panel (Navigation):** Home > All resources > VM-WS16OpWeb | Disks > VM-WS16OpWeb-osdisk
- Right Panel (Main Content):**
 - Encryption Settings:** Key management dropdown shows "Customer-managed key: disk-dec".
 - Information:** "Azure offers server-side encryption with platform-managed keys by default for managed disks. You may optionally choose to use a customer-managed key." with a "Learn more" link.
 - Feedback:** "Give feedback" and "Help improve this page" links.

The image shows two screenshots of the Microsoft Azure portal interface.

Screenshot 1: VM-WS19HRL-Web-osdisk | Encryption

This screenshot shows the Azure portal's navigation bar at the top. Below it, the URL indicates the user is viewing the 'Encryption' section for the 'VM-WS19HRL-Web-osdisk' disk. The left sidebar has 'Encryption' selected under 'Settings'. The main content area displays a note about server-side encryption and key management options, with 'Customer-managed key: disk-dec' selected. There are also 'Give feedback' and 'Help improve this page' links.

Screenshot 2: disk-dec | Resources

This screenshot shows the Azure portal's navigation bar at the top. Below it, the URL indicates the user is viewing the 'Resources' section for the 'disk-dec' disk encryption set. The left sidebar has 'Resources' selected under 'Settings'. The main content area displays a table of resources:

Name	Type	Resource Group	Subscription
VM-WS16DEVWEB-OSDISK	Disk	RG-DEV	Udacity 1071
VM-WS19HRL-WEB-OSDISK	Disk	RG-HRLEGAL	Udacity 1071
VM-WS16OPWEB-OSDISK	Disk	RG-OPERATIONS	Udacity 1071

2. Firewalls and virtual networks page

- Proof of no public access and TLS for SQL servers(prod, dev)

All resources

Udacity 1071 (cl4udacity1071.onmicrosoft.com)

+ Create Manage view ...

Filter for any field...

- Name ↑
 - uevveeu-pip
 - VNet-core-ip
 - web-pip
 - SQL database
 - DB-development-230277 (sql-devdata-2...)
 - DB-operations-230277 (sql-proodata-2...)
 - SQL server
 - sql-devdata-230277
 - sql-proodata-230277
 - Virtual machine
 - VM-WS16DevWeb
 - VM-WS16OpWeb
 - VM-WS19HRL-Web
 - Virtual network
 - HRLegal
 - VNet-core

sql-devdata-230277 | Networking

SQL server

Search Properties Feedback

Locks

Data management

- Backups
- Deleted databases
- Failover groups
- Import/Export history

Security

- Networking
- Microsoft Defender for Cloud
- Transparent data encryption
- Identity
- Auditing

Intelligent Performance

- Automatic tuning
- Recommendations

Monitoring

Public access

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 r...	Endpoint sta...	Resource gro...	Subscripti...	State
newVNetRule1	Vnet-Dev	default	10.2.0.0/24	Enabled	rg-dev	46c79782...	Ready

Firewall rules

Connectivity

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

sql-proddata-230277 | Networking

Public access

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 r...	Endpoint sta...	Resource gro...	Subscripti...	State
newVNetRule1	VNet-prod	Operations	10.1.0.0/24	Succeeded	rg-prod	46c79782...	Ready

Firewall rules

Allow certain public internet IP addresses to access your resource. [Learn more](#)

sql-proddata-230277 | Networking

Connectivity

Outbound networking

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

Restrict outbound networking

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 Security (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)

Microsoft Azure | Search resources, services, and docs (G+)

Home > All resources > sql-devdata-230277

All resources

sql-devdata-230277 | Microsoft Defender for Cloud

SQL server

Backups Deleted databases Recommendations Security alerts Findings Enablement Status: Enabled at the subscription-level (Configure) Learn more

0 0 0

Public IP address: devweb-pip, devweb-pip, VNet-core-ip, web-pip

SQL database: DB-development-230277 (sql-devdata-230277), DB-operations-230277 (sql-proodata-230277)

SQL server: sql-devdata-230277, sql-proodata-230277

Virtual machine: VM-WS16DevWeb, VM-WS16OpWeb, VM-WS19HRL-Web

Virtual network: HRLegal

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

Intelligent Performance: Automatic tuning, Recommendations

Monitoring: Logs

Automation: Tasks (preview), Export template

Help

Microsoft Azure | Search resources, services, and docs (G+)

Home > All resources > sql-proodata-230277

All resources

sql-proodata-230277 | Microsoft Defender for Cloud

SQL server

Backups Deleted databases Recommendations Security alerts Findings Enablement Status: Enabled at the subscription-level (Configure) Learn more

0 0 0

Public IP address: dewweb-pip, devweb-pip, VNet-core-ip, web-pip

SQL database: DB-development-230277 (sql-devdata-230277), DB-operations-230277 (sql-proodata-230277)

SQL server: sql-devdata-230277, sql-proodata-230277

Virtual machine: VM-WS16DevWeb, VM-WS16OpWeb, VM-WS19HRL-Web

Virtual network: HRLegal

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

Intelligent Performance: Automatic tuning, Recommendations

Monitoring: Logs

Automation: Tasks (preview), Export template

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

Microsoft Azure Search resources, services, and docs (G+) odl_user_230277@cl4ud... UDACITY 1071 (CLAUDACITY1071...)

Home > All resources > sql-proodata-230277

All resources

Udacity 1071 (cl4udacity1071.onmicrosoft.com)

+ Create Manage view ...

Filter for any field...

Name ↑

✓ Public IP address

- devweb-pip
- devweb-pip
- VNet-core-ip
- web-pip

SQL database

sql-proodata-230277 | Azure Active Directory ...

SQL server

Set admin Remove admin Save

Tags

Diagnose and solve problems

Quick start

Settings

Azure Active Directory

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

SQL databases

SQL elastic pools

DTU quota

Microsoft Azure Search resources, services, and docs (G+) odl_user_230277@cl4ud... UDACITY 1071 (CLAUDACITY1071...)

Home > All resources > sql-devdata-230277

All resources

Udacity 1071 (cl4udacity1071.onmicrosoft.com)

+ Create Manage view ...

Filter for any field...

Name ↑

✓ Public IP address

- devweb-pip
- devweb-pip
- VNet-core-ip
- web-pip

SQL database

sql-devdata-230277 | Azure Active Directory ...

SQL server

Set admin Remove admin Save

Tags

Diagnose and solve problems

Quick start

Settings

Azure Active Directory

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

SQL databases

SQL elastic pools

DTU quota

Cloud Protection

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

The image displays two side-by-side screenshots of the Microsoft Azure portal showing the 'Overview' page for two different virtual machines. Both machines are configured with IaaS Antimalware.

VM-WS16DevWeb/IaaSAntimalware (Left Screenshot):

- Essentials:**
 - Resource group: rg-dev
 - Subscription: Udacity_1071
 - Subscription ID: 46c79782-e579-4022-a44c-abfefce2f14c
 - Tags: DeploymentId: 230277, LaunchId: 1379, LaunchType: ON_DEMAND_LAB, TemplateId: 1211, TenantId: 203
- Properties:**
 - Force update tag: ---
 - Publisher: Microsoft.Azure.Security
 - Type: IaaSAntimalware
 - Type handler version: 1.3
 - Auto upgrade minor vers...: true
 - Enable automatic upgrade: ---
 - Settings: View value as JSON
 - Protected settings from key vault:
 - Secret URL: ---
 - Source vault: ---
 - Provisioning state: Succeeded
 - Suppress failures: ---
- Instance view:**
 - Name: ---
 - Type: ---
 - Type handler version: ---

VM-WS16OpWeb/IaaSAntimalware (Right Screenshot):

- Essentials:**
 - Resource group: rg-operations
 - Subscription: Uadacty_1071
 - Subscription ID: 46c79782-e579-4022-a44c-abfefce2f14c
 - Tags: DeploymentId: 230277, LaunchId: 1379, LaunchType: ON_DEMAND_LAB, TemplateId: 1211, TenantId: 203
- Properties:**
 - Force update tag: ---
 - Publisher: Microsoft.Azure.Security
 - Type: IaaSAntimalware
 - Type handler version: 1.3
 - Auto upgrade minor vers...: true
 - Enable automatic upgrade: ---
 - Settings: View value as JSON
 - Protected settings from key vault:
 - Secret URL: ---
 - Source vault: ---
 - Provisioning state: Succeeded
 - Suppress failures: ---
- Instance view:**
 - Name: ---
 - Type: ---

Microsoft Azure Search resources, services, and docs (G+)

Home > microsoft.antimalware-windows-20230410001413 | Overview >

VM-WS19HRL-Web/IaaSAntimalware

microsoft.compute/virtualmachines/extensions

Search Refresh Delete

Overview Activity log Access control (IAM) Settings Locks Automation Tasks (preview) Export template Help New Support Request

Essentials

Resource group (move) : rg-hrlegal
Subscription (move) : UDACTY 1071
Subscription ID : 46c79782-e579-4022-a44c-abfece2f14c
Tags (edit) : DeploymentId : 230277 LaunchId : 1379 LaunchType : ON_DEMAND_LAB TemplateId : 1211 TenantId : 203

Resource id : /subscriptions/46c79782-e579-4022-a44c-abfece2f14c/resourceGroups/rg-hrlega...
Type : Microsoft.Compute/virtualMachines/extensions

Properties Recommendations

Properties

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

Protected settings from key vault

Secret URL ---
Source vault ---

Instance view

Name ---
Type ---
Type handler version ---

JSON View

2. Recommendations

Microsoft Azure Search resources, services, and docs (G+)

Home > Microsoft Defender for Cloud | Overview >

Security posture

Secure score over time Governance report Guides & Feedback

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

Azure environment

Azure AWS GCP

Secure score 44% SECURE SCORE

Environment

Management groups 0 Subscriptions 1

Unhealthy resources 0/0 Recommendations 0

Governance

Assign ownership and drive recommendations remediation using governance. To create your first rule, click here.

Environment Owner

Search by name Environment == All Group by environment

Name ↑	Secure score ↑↓	Unhealthy resources ↑↓	Attack paths ↑↓	Recommendations
Udacity 1071 Azure subscription	44%	0 of 0	0	View recommendations >

Microsoft Azure odl user 230277@clAud...
UDACITY 1071 (CLAUDACITY1071...)

Home > Microsoft Defender for Cloud

Microsoft Defender for Cloud | Recommendations

Showing subscription 'Udacity 1071'

Refresh Download CSV report Open query Governance report Guides & Feedback

General

- Overview**
- Getting started
- Recommendations**
- Security alerts
- Inventory
- Cloud Security Explorer
- Workbooks
- Community
- Diagnose and solve problems

Secure score recommendations All recommendations

Azure AWS GCP

Secure score 42% **Active recommendations** 0/0 **Attack path** 0 We didn't find attack paths in your environment. Learn more >

Recommendation status == None Severity == None Add filter More (4) Show my items only: Off

Name ↑	Max score ↓	Current score ↑↓	Potential score increase ↑↓	Status ↑↓	Unhealthy resources	Insights
Enable encryption at rest	4	4.00		Completed	0 of 5 resources	
Remediate security configur...	4	0.00	+ 44%	Unassigned	2 of 5 resources	
Enable auditing and logging	1	0.00	+ 11%	Unassigned	3 of 3 resources	
Remediate vulnerabilities	Not scored	Not scored		Completed	0 of 3 resources	
Enable endpoint protection	Not scored	Not scored		Completed	0 of 3 resources	
Manage access and permissi...	Not scored	Not scored		Completed	0 of 7 resources	
Enable MFA	Not scored	Not scored		Completed	0 of 1 resources	
Enable enhanced security fe...	Not scored	Not scored		Completed	0 of 4 resources	

Monitoring

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

The screenshot shows the Azure portal interface for managing resources. On the left, there's a sidebar with navigation links like Home, All resources, and a search bar. The main content area is titled "sql-devdata-230626 | Auditing".

Azure SQL Auditing: This section is currently active. It includes a toggle switch for "Enable Azure SQL Auditing" (which is turned on) and a dropdown menu for "Audit log destination" where "Log Analytics" is selected. It also shows the "Subscription" set to "Udacity 1074" and the "Log Analytics" workspace set to "loganalytics(eastus)".

Auditing of Microsoft support operations: This section is shown below the audit log settings. It has a toggle switch for "Enable Auditing of Microsoft support operations" (which is turned off). It describes how auditing tracks Microsoft support engineers' (DevOps) operations and writes them to an audit log in your Azure Storage account, Log Analytics workspace or Event Hub.

Navigation: At the bottom left, there are page navigation controls (Page, 1, of 1).

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar titled 'All resources' with a search bar at the top. The main content area is titled 'sql-proodata-230626 | Auditing'. It includes sections for 'Feedback', 'Azure SQL Auditing', 'Data management', 'Security', and 'Intelligent Performance'. Under 'Azure SQL Auditing', the 'Enable Azure SQL Auditing' toggle is turned on. For 'Audit log destination', 'Log Analytics' is selected under 'Subscription' (Udacity 1074) and 'Log Analytics' (loganalytics(eastus)). There's also a section for 'Auditing of Microsoft support operations' with its own toggle.

Audit log:

- Add member to role: This is audit log when the Role Based Access Control needs to be provided for a member to perform and provide necessary and required access only. It contains such as: status, role id..etc
 - Add conditional access policy: This is showing the condition access policy is created by subscription. Log detail contains such as: status, username, etc...
 - Add member to group: This log showing the information when added user to the group. The detail contains such as: Status, role id, user name...etc.
2. Proof of Sentinel connectors (2+)

Microsoft Azure Search resources, services, and docs (G+)

Home > Microsoft Sentinel > Microsoft Sentinel

Microsoft Sentinel | Data connectors

Selected workspace: 'log1'

+ Create Manage view ...

Filter for any field... Name ↑

log1

News & guides Search Threat management 127 Connectors 3 Connected More content at Content hub

127 Connectors 3 Connected

All Data Connectors and additional out-of-the-box (OOTB) content are now centrally available in Content hub. Starting Q2 2023 only in-use Data Connectors will be available in this gallery. Learn more about the [OOTB content centralization changes](#).

Search by name or provider Providers : All Data Types : All Status : All

Status ↑	Connector name
	Azure Active Directory Identity Protection Microsoft
	Azure SQL Databases Microsoft
	Microsoft 365 Defender Microsoft
	Agari Phishing Defense and Brand Protection (Preview) Agari
	AI Analyst Darktrace (Preview) Darktrace
	AI Vectra Detect (Preview) Vectra AI

< Page 1 > of 1

Compliance

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

The screenshot shows the Microsoft Defender for Cloud Regulatory compliance dashboard. On the left, there's a navigation sidebar with sections like General, Cloud Security, and Management. The main area displays a chart titled 'Lowest compliance regulatory standards' comparing 'NIST SP 800 53 R4' against '390/424'. Below the chart, there's a section for 'Audit reports' with a 'Show all 1' button and a blue 'Open' button. At the bottom, there's a survey question: 'Is the regulatory compliance experience clear to you?' with 'Yes' and 'No' options. A note states: 'Recommendations from Microsoft Defender for Cloud - Regulatory Compliance should not be interpreted as a guarantee of compliance. It is up to you to evaluate and validate the effectiveness of customer controls per your regulatory environment. These services are subject to the terms and conditions in the [licensing terms](#). NIST SP 800 53 R4 is applied to the subscription Uadcty 1073'.

Three recommendations for remediation of vulnerabilities in Azure and the justification for each:

- Enable multi-factor authentication (MFA): MFA adds an additional layer of security to your Azure environment. Enabling MFA for all user accounts can significantly reduce the risk of successful attacks that rely on compromised credentials.
- Use network security groups (NSGs) to restrict traffic: Network security groups (NSGs) are a powerful tool for restricting traffic to and from resources in Azure. By creating and applying NSGs to virtual machines and subnets, you can limit access to only the necessary ports and protocols, and block traffic from untrusted sources.
- Regularly apply security updates and patches: Regularly applying security updates and patches is critical to address known vulnerabilities in Azure.