

Secure the Juice

Identity and Access Management

1. Design authentication and authorization controls that manage access, role assignments, and identity

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

- Screenshot(s) that clearly display all Azure AD roles and Azure AD Assignments for all required users.

Home > Udacity 1069 > Groups > Executive

Executive | Assigned roles

Overview | Diagnose and solve problems | Manage | Properties | Members | Owners | Roles and administrators | Administrative units | Group memberships | Assigned roles | Applications

Eligible assignments | Active assignments | Expired assignments

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

Home > Udacity 1069 > Groups > Executive

Executive | Members

Group

Overview

Diagnose and solve problems

Manage

Properties

Members

Owners

Roles and administrators

«

+ Add members

✕ Remove

↺ Refresh

📄 Bulk operations

☰ Columns

Direct members

All members

🔍 Search by name

+ Add filters

	Name	↑↓	Type	Email	User type
<input type="checkbox"/>	CH Chris		User		Member
<input type="checkbox"/>	KA Karl		User		Member

Home > Udacity 1069 > Groups > IT

IT | Members

Group

Overview

Diagnose and solve problems

Manage

Properties

Members

Owners

Roles and administrators

Administrative units

Group memberships

Assigned roles

Applications

Licenses

«

+ Add members

✕ Remove

↺ Refresh

📄 Bulk operations

☰ Columns

...

Direct members

All members

🔍 Search by name

+ Add filters

	Name	↑↓	Type	Email	User type
<input type="checkbox"/>	AN Andrew		User		Member
<input type="checkbox"/>	NE Neelima		User		Member
<input type="checkbox"/>	NE Neha		User		Member
<input type="checkbox"/>	SE Seth		User		Member
<input type="checkbox"/>	SR Srinadh		User		Member
<input type="checkbox"/>	TO Tom		User		Member
<input type="checkbox"/>	WI Winifred		User		Member

Home > Udacity 1069 > Groups > HR

HR | Members

Group

Overview

Diagnose and solve problems

Manage

Properties

Members

Owners

«

+ Add members

✕ Remove

↺ Refresh

📄 Bulk operations

☰ Columns

🗨 Got feedback?

Direct members

All members

🔍 Search by name

+ Add filters

	Name	↑↓	Type	Email	User type
<input type="checkbox"/>	LO Lora		User		Member

Home > Udacity 1069 > 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

+ Add assignments

Refresh

Got feedback?

Eligible assignments

Active assignments

Expired assignments

Search by role

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

Home > Udacity 1069 > Groups > Support Desk

Support Desk | Members

Group

Overview

Diagnose and solve problems

Manage

Properties

Members

Owners

Roles and administrators

+ Add members

Remove

Refresh

Bulk operations

Columns

Got feedback?

Direct members

All members

Search by name

Add filters

Name	Type	Email	User type
<input type="checkbox"/> Winifred	User		Member

Home > Udacity 1069 > 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

+ Add assignments

Refresh

Got feedback?

Eligible assignments

Active assignments

Expired assignments

Search by role

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

Home > Udacity 1069 > Users > Karl

Karl | Assigned roles

User

Overview

Audit logs

Sign-in logs

Diagnose and solve problems

Manage

Custom security attributes (preview)

Assigned roles

Administrative units

Remote

+ Add assignments

Refresh

Got feedback?

Eligible assignments

Active assignments

Expired assignments

Search by role

Role	Principal name	Scope	Membership	State	Start time	End time	Action
Message Center Reader	Karl@c4udacity1069.onmicro...	Directory	Group	Active	5/24/2022, 5:03:29 PM	Permanent	Remove Update
Billing Administrator	Karl@c4udacity1069.onmicro...	Directory	Direct	Active	7/28/2022, 7:36:36 PM	Permanent	Remove Update

Home > Udacity 1069 > Users > Karl

Karl | Assigned roles

User

Overview

Audit logs

Sign-in logs

Diagnose and solve problems

Manage

Custom security attributes (preview)

Assigned roles

Administrative units

+ Add assignments

Refresh

Got feedback?

Eligible assignments

Active assignments

Expired assignments

Search by role

Role	Principal name	Scope	Membership	State	Start time	End time	Action
Message Center Reader	Karl@c4udacity1069.onmicro...	Directory	Group	Active	5/24/2022, 5:03:29 PM	Permanent	Remove Update
Billing Administrator	Karl@c4udacity1069.onmicro...	Directory	Direct	Active	7/28/2022, 7:36:36 PM	Permanent	Remove Update

Home > Udacity 1069 > Users > Seth

Seth | Assigned roles

Overview Audit logs Sign-in logs Diagnose and solve problems Manage Custom security attributes (preview) Assigned roles

Search (Ctrl+F) + Add assignments Refresh Got feedback?

Eligible assignments Active assignments Expired assignments

Search by role

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

- Screenshot(s) that clearly displays Global Admin PIM screen showing duration, eligibility, and expiration.

rg-devdata | Access control (IAM)

Resource group

Search (Ctrl+F) + Add Download role assignments Edit columns Refresh Remove Got feedback?

Check access Role assignments Roles Deny assignments Classic administrators

Number of role assignments for this subscription 23 2000

Search by name or email Type: All Role: All Scope: All scopes Group by: Role

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...	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

Added Role assignment: 2 Role assignments were added to devdata.

rg-data | Access control (IAM)

Resource group

Search (Ctrl+F) + Add Download role assignments Edit columns Refresh Remove Got feedback?

Check access Role assignments Roles Deny assignments Classic administrators

Number of role assignments for this subscription 23 2000

Search by name or email Type: All Role: All Scope: All scopes Group by: Role

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

Added Role assignment: Srinadh was added as Owner

sql-devdata-202442 | Access control (IAM) ...

Search (Ctrl+/) Add Download role assignments Edit columns Refresh Remove Got feedback?

Check access **Role assignments** Roles Deny assignments Classic administrators

Number of role assignments for this subscription 29 2000

Search by name or email Type: All Role: All Scope: All scopes Group by: Role

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 Syst...	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@cl4udacity1069.onmicro...	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

sql-proddata-202442 | Access control (IAM) ...

Search (Ctrl+/) Add Download role assignments Edit columns Refresh Remove Got feedback?

Check access **Role assignments** Roles Deny assignments Classic administrators

Number of role assignments for this subscription 29 2000

Search by name or email Type: All Role: All Scope: All scopes Group by: Role

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 Syst...	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

rg-operations | Access control (IAM)

Resource group

Search (Ctrl+/)

Overview

Activity log

Access control (IAM)

Tags

Resource visualizer

Events

Settings

Deployments

Security

Policies

Properties

Locks

Cost Management

Cost analysis

Cost alerts (preview)

+ Add Download role assignments Edit columns Refresh Remove Got feedback?

Check access Role assignments Roles Deny assignments Classic administrators

Number of role assignments for this subscription

24 2000

Search by name or email

Type: All

Role: All

Scope: All scopes

Group by: Role

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

<input type="checkbox"/>	Name	Type	Role	Scope	Condition
CloudDevOps Custom RBAC I1359 S1					
<input type="checkbox"/>	Identity not found. Unable to find identity.	Unknown	CloudDevOps Custom RBAC I1359 S1	Subscription (Inherited)	None
<input type="checkbox"/>	Identity not found. Unable to find identity.	Unknown	CloudDevOps Custom RBAC I1359 S1	Subscription (Inherited)	None
Contributor					
<input type="checkbox"/>	Andrew Andrew@cl4udacity1069...	User	Contributor	This resource	None
<input type="checkbox"/>	ODL_User 202442 odl_user_202442@cl4ud...	User	Contributor	Subscription (Inherited)	None

Added Role assignment
Andrew was added as Contributor f

rg-dev | Access control (IAM)

Resource group

Search (Ctrl+/)

Overview

Activity log

Access control (IAM)

Tags

Resource visualizer

Events

Settings

Deployments

Security

Policies

Properties

Locks

Cost Management

Cost analysis

Cost alerts (preview)

+ Add Download role assignments Edit columns Refresh Remove Got feedback?

Check access Role assignments Roles Deny assignments Classic administrators

Number of role assignments for this subscription

25 2000

Search by name or email

Type: All

Role: All

Scope: All scopes

Group by: Role

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

<input type="checkbox"/>	Name	Type	Role	Scope	Condition
CloudDevOps Custom RBAC I1359 S1					
<input type="checkbox"/>	Identity not found. Unable to find identity.	Unknown	CloudDevOps Custom RBAC I1359 S1	Subscription (Inherited)	None
<input type="checkbox"/>	Identity not found. Unable to find identity.	Unknown	CloudDevOps Custom RBAC I1359 S1	Subscription (Inherited)	None
Contributor					
<input type="checkbox"/>	Neelima Neelima@cl4udacity106...	User	Contributor	This resource	None
<input type="checkbox"/>	ODL_User 202442 odl_user_202442@cl4ud...	User	Contributor	Subscription (Inherited)	None

Proof of Global Administrator setting with duration, eligibility, expiration

Home > Privileged Identity Management > Udacity 1069 > Global Administrator

Global Administrator | Role settings

Privileged Identity Management | Azure AD roles

« Edit

Manage

- Assignments
- Description
- Role settings

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

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

2. Configure MFA and Conditional Access policies to require MFA for all users.

- Screenshots of Conditional Access policy that clearly demonstrates that MFA has been configured for all users.

Resubmitted –

Home > Conditional Access >

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. Please

Exclude current user, odi_user_202442@d4udacity1069.onmicrosoft.com, from this policy.

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

Save

Grant

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

Screenshots of Multi-Factor authentication configuration pages that clearly demonstrate the stated requirements here:

- MFA tokens should expire every 14 days.
- The Charlotte office is considered a trusted site
- MFA should not be required in the Charlotte Office.
- The Charlotte office has an IP address range of 143.52.0.0/24

Resubmitted --

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. Configure Azure Bastion to allow secure connectivity from the Azure Portal to the Azure Virtual machines.

Screenshot of the Bastion Overview page should indicate the virtual network/subnet. Placed correctly, only one Bastion will be needed.

The screenshot shows the Azure Bastion Overview page for a resource named 'Microsoft.BastionHost-20220728203550'. 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, and Logs. The main content area is divided into 'Essentials' and 'Sessions' sections. The 'Essentials' section displays the following details:

- 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

The 'Sessions' section shows a table with columns: SessionId, StartTime (UTC), TargetSubscriptionId, ResourceType, TargetHostName, TargetResourceGroup, Username, TargetIpAddress, and Protocol. The table currently contains no results.

The screenshot shows the Azure Virtual Machine Overview page for a resource named 'vm-ws16devapp'. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, and Networking. The main content area is divided into 'Essentials' and 'JSON View' sections. The 'Essentials' section displays the following details:

- 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: -

The screenshot shows the Azure Virtual Machine Overview page for a resource named 'VM-WS16OpWeb'. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, and Networking. The main content area is divided into 'Essentials' and 'JSON View' sections. The 'Essentials' section displays the following details:

- 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: -

VM-WS19HRL-App

Virtual machine

Search (Ctrl+/)

ConnectStartRestartStopCaptureDeleteRefreshOpen in mobileCLI / PSFeedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Networking

Essentials

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 : -

VM-WS19OpApp

Virtual machine

Search (Ctrl+/)

ConnectStartRestartStopCaptureDeleteRefreshOpen in mobileCLI / PSFeedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Networking

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 : -

VM-WS19HRL-Web

Virtual machine

Search (Ctrl+/)

ConnectStartRestartStopCaptureDeleteRefreshOpen in mobileCLI / PSFeedback

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Networking

Essentials

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 : -

2. Reduce attack footprint by removing public IP addresses.

The screenshot clearly shows public IP address is blank for each VM

The screenshot displays the Azure portal interface for a virtual machine named **VM-WS16DevWeb**. The left sidebar contains navigation options such as Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Networking, Connect, Windows Admin Center (preview), Disks, Size, Microsoft Defender for Cloud, Advisor recommendations, Extensions + applications, and Continuous delivery. The main content area is divided into two sections: **Essentials** and **Properties**.

Essentials section:

- 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 : -

Properties section:

- 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. Protect data at rest by encrypting data disks using a customer-managed key

Screenshots should show the disk encryption type for each VM.

The screenshot displays the Azure portal interface for managing disk encryption. It is divided into two main sections, each showing the configuration for a specific virtual machine's disk.

Top Section: des-disk | Resources

This section shows a list of resources under the 'des-disk' Disk Encryption Set. The table below summarizes the data shown:

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

Bottom Section: vm-ws16devapp-osdisk | Encryption

This section shows the encryption configuration for the 'vm-ws16devapp-osdisk' disk. The 'Encryption type' is set to 'Encryption at-rest with a customer-managed key' and the 'Disk encryption set' is 'des-disk'. A similar configuration is shown for the 'VM-WS16DevWeb-osdisk' disk in the section below.

Bottom Section: VM-WS16DevWeb-osdisk | Encryption

This section shows the encryption configuration for the 'VM-WS16DevWeb-osdisk' disk. The 'Encryption type' is set to 'Encryption at-rest with a customer-managed key' and the 'Disk encryption set' is 'des-disk'.

Home > VM-WS16OpWeb | Disks > VM-WS16OpWeb-osdisk

VM-WS16OpWeb-osdisk | Encryption

Disk

Search (Ctrl+ /)

Save Discard Refresh

Overview

Activity log

Access control (IAM)

Tags

Settings

Configuration

Size + performance

Encryption

Networking

Disk Export

Recovery

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

Home > Virtual machines > VM-WS19HRL-App | Disks > VM-WS19HRL-App-osdisk

VM-WS19HRL-App-osdisk | Encryption

Disk

Search (Ctrl+ /)

Save Discard Refresh

Overview

Activity log

Access control (IAM)

Tags

Settings

Configuration

Size + performance

Encryption

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

Home > Virtual machines > VM-WS19HRL-Web | Disks > VM-WS19HRL-Web-osdisk

VM-WS19HRL-Web-osdisk | Encryption

Disk

Search (Ctrl+ /)

Save Discard Refresh

Overview

Activity log

Access control (IAM)

Tags

Settings

Configuration

Size + performance

Encryption

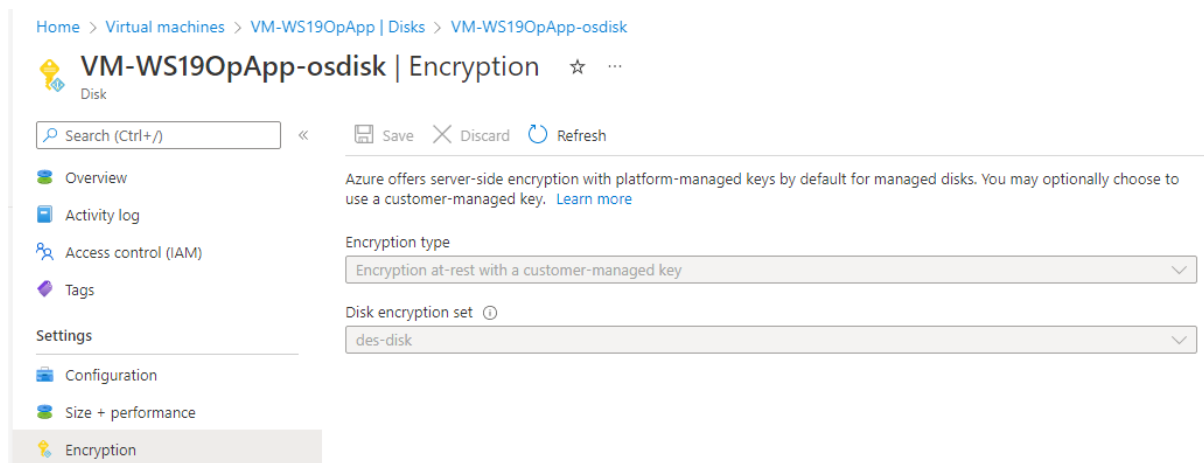
Azure offers server-side encryption with platform-managed keys by default for managed disks. You may optionally choose to use a customer-managed key. [Learn more](#)

Encryption type

Encryption at-rest with a customer-managed key

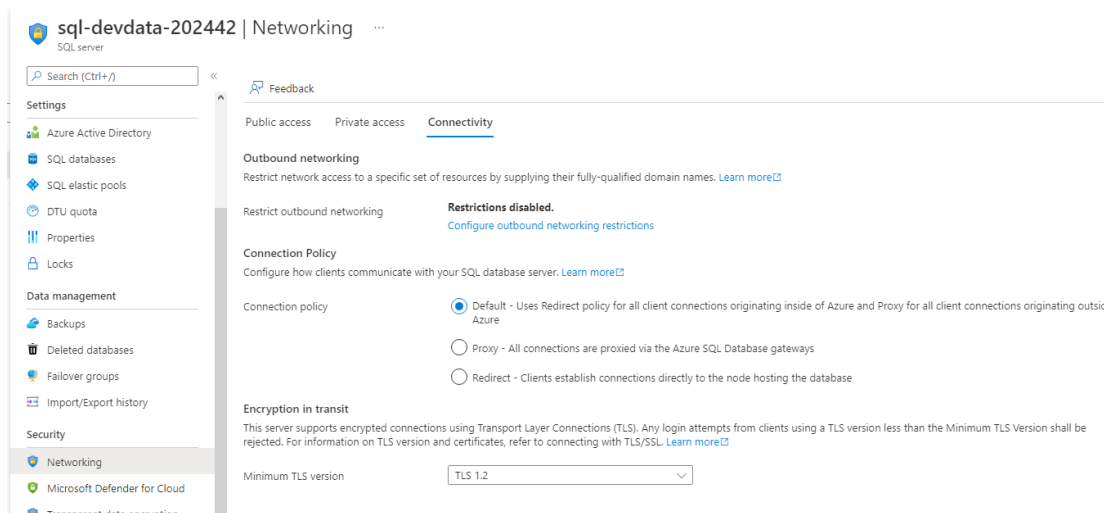
Disk encryption set ⓘ

des-disk



2. Secure traffic to SQL servers and databases by limiting public network access, enforcing TLS minimum requirements, and setting allowed IPs or network requirements

A screenshot of the Firewalls and Virtual networks page for SQL servers that clearly shows the required configuration for no public access and TLS



Home > sql-proddata-202442

sql-proddata-202442 | Networking

SQL server

Search (Ctrl+/)

Feedback

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

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

Data management
Backups
Deleted databases
Failover groups

Public access

Private access

Connectivity

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	hrlLegal	default	10.0.0.0/24	Enabled	rg-hlegal	0d904d18-8d...	Ready

Firewall rules

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

sql-devdata-202442 | Networking

SQL server

Search (Ctrl+/)

Feedback

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

Data management
Backups
Deleted databases
Failover groups
Import/Export history

Security
Networking
Microsoft Defender for Cloud

Public access

Private access

Connectivity

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

Home > sql-proddata-202442

sql-proddata-202442 | Networking

SQL server

Search (Ctrl+/)

Feedback

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

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

Data management
Backups

Public access

Private access

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 connecting with TLS/SSL [Learn more](#)

Minimum TLS version

TLS 1.2

3. Protect SQL data by enabling Azure Defender for SQL.

Screenshot that shows Azure Defender for SQL is enabled.

The image displays two screenshots of the Azure portal interface, specifically the Microsoft Defender for Cloud page for an SQL server resource.

Top Screenshot (sql-devdata-202442):

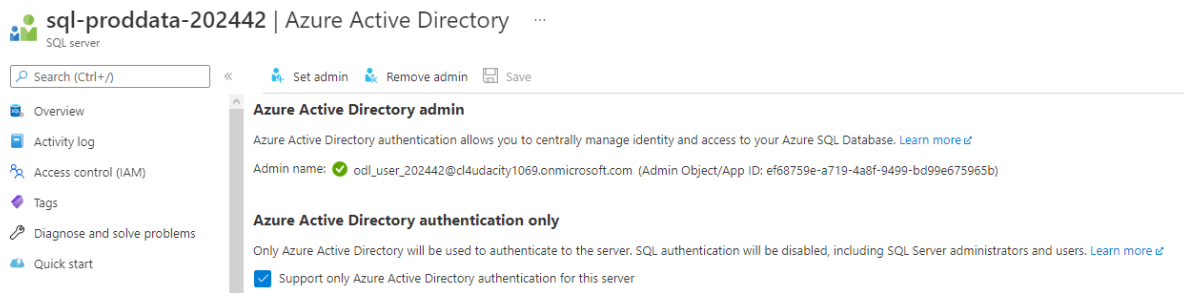
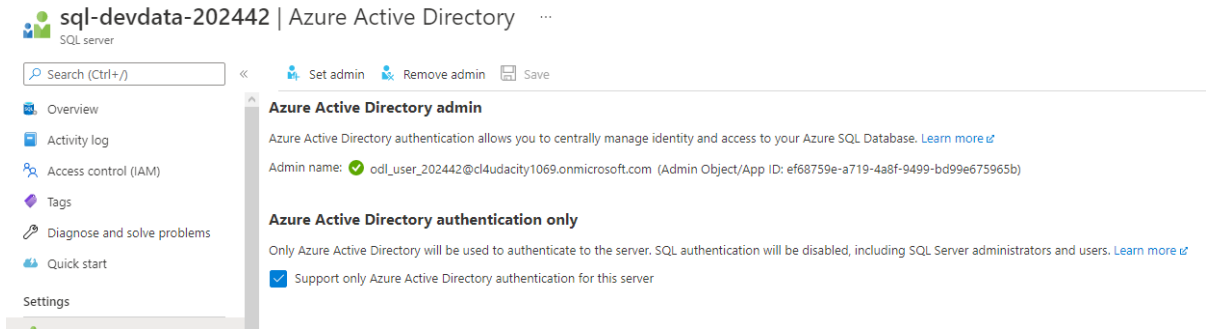
- Header:** sql-devdata-202442 | Microsoft Defender for Cloud
- Left Navigation Panel:** Includes sections for Settings (Azure Active Directory, SQL databases, SQL elastic pools, DTU quota, Properties, Locks), Data management (Backups, Deleted databases, Failover groups, Import/Export history), and Security (Networking, Microsoft Defender for Cloud, Transparent data encryption, Identity, Auditing).
- Main Content Area:**
 - Recommendations:** Shows 0 recommendations. Text: "Defender for Cloud continuously monitors the configuration of your SQL Servers to identify potential security vulnerabilities and recommends actions to mitigate them." Below this, it states "No recommendations to display" and "There are no security recommendations for this resource." A button "View all recommendations in Defender for Cloud" is present.
 - Security incidents and alerts:** Shows 0 alerts. Text: "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."

Bottom Screenshot (sql-proddata-202442):

- Header:** sql-proddata-202442 | Microsoft Defender for Cloud
- Left Navigation Panel:** Includes sections for Overview (Activity log, Access control (IAM), Tags, Diagnose and solve problems, Quick start), Settings (Azure Active Directory, SQL databases, SQL elastic pools, DTU quota, Properties, Locks), Data management (Backups, Deleted databases, Failover groups, Import/Export history), and Security (Networking, Microsoft Defender for Cloud, Transparent data encryption).
- Main Content Area:**
 - Recommendations:** Shows 0 recommendations. Text: "Defender for Cloud continuously monitors the configuration of your SQL Servers to identify potential security vulnerabilities and recommends actions to mitigate them." Below this, it states "No recommendations to display" and "There are no security recommendations for this resource." A button "View all recommendations in Defender for Cloud" is present.
 - Security incidents and alerts:** Shows 1 alert. Text: "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." Below this, a link "Check for alerts on this resource in Microsoft Defender for Cloud" is shown.
 - Vulnerability assessment findings:** This section is visible at the bottom of the screenshot.

4. Secure Azure SQL by enforcing Azure AD authentication over the weaker SQL authentication methods.

Show screenshot of Azure AD authentication for SQL enabled



Protection

1. Protect virtual machines from malware by using available extensions.

Screenshot of the extensions tab for all VM shows anti-malware is enabled

The following screenshots show the 'Extensions' tab for three different virtual machines in the Azure portal, all of which have the 'IaaSAntimalware' extension installed and enabled.

VM-WS16devapp/IaaSAntimalware

Resource group: rg-dev
Subscription: Udacity_1069
Subscription ID: 0d904d18-8db0-4da9-ac30-cbd31a3a16e5
Tags: Click here to add tags

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

Resource group: rg-operations
Subscription: Udacity_1069
Subscription ID: 0d904d18-8db0-4da9-ac30-cbd31a3a16e5
Tags: Click here to add tags

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

Resource group: rg-hrlegal
Subscription: Udacity_1069
Subscription ID: 0d904d18-8db0-4da9-ac30-cbd31a3a16e5
Tags: Click here to add tags

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/laaSAntimalware

microsoft.compute/virtualmachines/extensions

Search (Ctrl+/) <

Refresh Delete

Overview

Activity log

Access control (IAM)

Settings

Locks

Automation

Tasks (preview)

Export template

Support + troubleshooting

New Support Request

Essentials

Resource group (move) : rg-hrlegal

Subscription (move) : Udacity_1062

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

JSON View

Properties

Force update tag	---
Publisher	Microsoft.Azure.Security
Type	laaSAntimalware
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/laaSAntimalware

microsoft.compute/virtualmachines/extensions

Search (Ctrl+/) <

Refresh Delete

Overview

Activity log

Access control (IAM)

Settings

Locks

Automation

Tasks (preview)

Export template

Support + troubleshooting

New Support Request

Essentials

Resource group (move) : rg-operations

Subscription (move) : Udacity_1062

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

JSON View

Properties

Force update tag	---
Publisher	Microsoft.Azure.Security
Type	laaSAntimalware
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-WS16DevWeb/laaSAntimalware

microsoft.compute/virtualmachines/extensions

Search (Ctrl+/) <

Refresh Delete

Overview

Activity log

Access control (IAM)

Settings

Locks

Automation

Tasks (preview)

Export template

Support + troubleshooting

New Support Request

Essentials

Resource group (move) : rg-dev

Subscription (move) : Udacity_1062

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/M...

Type : Microsoft.Compute/virtualMachines/extensions

JSON View

Properties

Force update tag	---
Publisher	Microsoft.Azure.Security
Type	laaSAntimalware
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. Track and remediate vulnerabilities against Azure Security Center (ASC) Default policy

A list of at least 3 recommendations with the justification to remediate vulnerabilities (text file)

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

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

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

User accounts requiring MFA

Enable MFA for the following user accounts:

Ramesh Bamidipati

✓ 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	■■■■■■■

Recommendation in Text with the justification to remediate vulnerabilities

1. "Enable MFA" currently has a score of 0/10. So, it has the biggest impact on security if we fix it. MFA is not set up for user account Ramesh Bamidipati, so we should setup for him
2. The other 2 top remediations are "Apply system updates" and "Remediate vulnerabilities". Both of them have a score of 0/6. So, that can be done also.
3. We should install the log analytics agent on all of our VMs.
4. And we should install vulnerability assessment tools on our VMs.

Resubmitted –

Monitoring

1. Configure Azure Sentinel Connectors.

Provide screenshot of Azure Sentinel Data Connectors Page.

The screenshot displays the Azure Sentinel 'Auditing' configuration page for a specific SQL server. The interface includes a left-hand navigation pane with categories like Data management, Security, Intelligent Performance, Monitoring, Automation, and Support + troubleshooting. The 'Auditing' option is selected. The main content area is titled 'Azure SQL Auditing' and provides instructions on tracking database events. It features a toggle to 'Enable Azure SQL Auditing' (which is turned on) and a section for 'Audit log destination' with checkboxes for 'Storage' and 'Log Analytics' (the latter is checked). Below this, dropdown menus are used to select a 'Subscription' (Udacity 1069) and 'Log Analytics' (law-udacity(eastus)). A second section, 'Auditing of Microsoft support operations', includes a description of tracking support engineers' actions and a toggle to 'Enable Auditing of Microsoft support operations' (which is turned off). At the bottom of this section, there is a checkbox for 'Use different audit log destinations'.

sql-devdata-202442 | Auditing ...

SQL server

Search (Ctrl+/) << Save Discard Feedback

Azure SQL Auditing

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

Enable Azure SQL Auditing ☒ ?

Audit log destination (choose at least one):

☐ Storage

☒ 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 ☐ ?







At least Azure Active Directory and Azure Active Directory Identity Protection connectors should be selected

[Home](#) > [sql-proddata-202442](#)





 **sql-proddata-202442 | Auditing** ...
SQL server

 Save  Discard  Feedback






Settings

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


Data management

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

Security



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

Intelligent Performance

-  Automatic tuning

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 *



Log Analytics *

☐ 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. Monitor and Protect SQL databases by configuring auditing.

Provide screenshot showing SQL Auditing is enabled with Log Analytics Workspace

The screenshot displays the Microsoft Sentinel interface for the 'law-udacity' workspace. The left sidebar contains navigation links for General, Threat management, and Content management. The main area shows the 'Data connectors' page with a summary of 123 connectors and 5 connected ones. A table lists the connectors, with 'Azure SQL Databases' highlighted as connected.

Home > Microsoft Sentinel

Microsoft Sentinel | Data connectors

Selected workspace: 'law-udacity'

Search (Ctrl+/) Refresh Guides & Feedback

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

123 Connectors 5 Connected More content at Content hub

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

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

Compliance

1. Enable monitoring of established industry and regulatory standards

Screenshot proof of added NIST SP 800-53 rev4 policy

Home > Microsoft Defender for Cloud >

Environment settings

+ Add environment

SQL Information Protection

Refresh

Guides & Feedback

Azure subscriptions 1

AWS accounts 0

GCP projects 0

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

Search by name

Environments == All

Standards == All

Coverage == All

Collapse 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		...