

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 screenshot shows the 'Assigned roles' page for the 'Executive' group in the Microsoft Entra ID console. The breadcrumb trail is 'Home > Udacity 1095 | Groups > Groups | All groups > Executive'. The page title is 'Executive | Assigned roles'. The left sidebar contains navigation options: Overview, Diagnose and solve problems, Manage (Properties, Members, Owners, Roles and administrators, Administrative units, Group memberships, Assigned roles, Applications, Licenses, Azure role assignments), and Activity (Privileged access (Preview), Access reviews, Audit logs, Bulk operation results). The main content area has tabs for 'Eligible assignments', 'Active assignments' (selected), and 'Expired assignments'. Below the tabs is a search bar 'Search by role'. A table lists the active role assignments:

Role	Principal name	Scope	Membership	State	Start time	End time	Action
Message Center Reader		Directory	Direct	Active	9/24/2022, 3:24:17 PM	Permanent	Remove Update

Home > Udacity 1095 | Groups > Groups | All groups > Executive

Executive | Members

Group

Overview

Diagnose and solve problems

Manage

Properties

Members

Owners

Roles and administrators

Administrative units

Group memberships

Assigned roles

Applications

Licenses

Azure role assignments

Activity

Privileged access (Preview)

Access reviews

Audit logs

Bulk operation results

+ 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"/>	CH Chris	User		Member
<input type="checkbox"/>	KA Karl	User		Member

Home > Udacity 1095 | Groups > Groups | All 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

Azure role assignments

Activity

Privileged access (Preview)

Access reviews

Audit logs

Bulk operation results

+ 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"/>	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 1095 | Groups > Groups | All groups > HR

HR | Members

Group

Overview

Diagnose and solve problems

Manage

Properties

Members

Owners

Roles and administrators

Administrative units

Group memberships

Assigned roles

Applications

Licenses

Azure role assignments

Activity

Privileged access (Preview)

Access reviews

Audit logs

Bulk operation results

+ 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"/>	 Lora	User		Member

Home > Udacity 1095 | Groups > 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

Activity

Privileged access (Preview)

Access reviews

Audit logs

Bulk operation results

+ 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	9/24/2022, 3:41:55 PM	Permanent	Remove Update

Home > Udacity 1095 | Groups > Groups | All groups > Support Desk

Support Desk | Members

Group

Overview

Diagnose and solve problems

Manage

Properties

Members

Owners

Roles and administrators

Administrative units

Group memberships

Assigned roles

Applications

Licenses

Azure role assignments

Activity

Privileged access (Preview)

Access reviews

Audit logs

Bulk operation results

+ 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 1095 | Groups > 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

Applications

Licenses

Azure role assignments

Activity

Privileged access (Preview)

Access reviews

Audit logs

Bulk operation results

+ 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	9/24/2022, 3:54:02 PM	Permanent	Remove Update

Home > Udacity 1095 | Users > Users > Karl

Karl | Assigned roles

User

Search

«

+ Add assignments

Refresh

Got feedback?

Overview

Audit logs

Sign-in logs

Diagnose and solve problems

Manage

Custom security attributes (preview)

Assigned roles

Administrative units

Groups

Applications

Licenses

Devices

Azure role assignments

Authentication methods

Troubleshooting + Support

New support request

Eligible assignments

Active assignments

Expired assignments

Search by role

Role	Principal name	Scope	Membership	State	Start time	End time	Action
Message Center Reader	Karl@cl4udacity1095...	Directory	Group	Active	9/24/2022, 3:24:17 PM	Permanent	Remove Update
Billing Administrator	Karl@cl4udacity1095...	Directory	Direct	Active	9/24/2022, 3:55:53 PM	Permanent	Remove Update

Home > rg-devdata

rg-devdata | Access control (IAM)

Resource group

Search

«

+ Add

Download role assignments

Edit columns

Refresh

Remove

Got feedback?

Overview

Activity log

Access control (IAM)

Tags

Resource visualizer

Events

Settings

Deployments

Security

Policies

Properties

Locks

Cost Management

Cost analysis

Cost alerts (preview)

Budgets

Advisor recommendations

15 items (7 Users, 1 Foreign Principals, 1 Service Principals, 5 Unknown, 1 Managed Identities)

Name	Type	Role	Scope	Condition
CloudDevOps Custom RBAC I1346 S1				
Identity not found. Unable to find identity.	Unknown	CloudDevOps Custom RBAC I1346 S1	Subscription (Inherited)	None
Identity not found. Unable to find identity.	Unknown	CloudDevOps Custom RBAC I1346 S1	Subscription (Inherited)	None
Contributor				
Key Vault Crypto Service Encryption User				
Owner				
Foreign Principal for 'Spektra S	Foreign principal	Owner	Subscription (Inherited)	None
https://cl4udacity1095.onmicr	App	Owner	Subscription (Inherited)	None
Ramesh Bamidipati admin@cl4udacity1095.onm...	User	Owner	Subscription (Inherited)	None
Neha Neha@cl4udacity1095.onmi...	User	Owner	This resource	None
ODL_User_208585 odl_user_208585@cl4udacit...	User	Owner	This resource	None
Srinadh Srinadh@cl4udacity1095.on...	User	Owner	This resource	None
Reader				

Home > sql-proddata-208585 > rg-data

rg-data | Access control (IAM)

Search

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

CloudDevOps Custom RBAC I1346 S1					
<input type="checkbox"/>	Identity not found. Unable to find identity.	Unknown	CloudDevOps Custom RBAC I1346 S1	Subscription (Inherited)	None
<input type="checkbox"/>	Identity not found. Unable to find identity.	Unknown	CloudDevOps Custom RBAC I1346 S1	Subscription (Inherited)	None
Contributor					
<input type="checkbox"/>	2940bafbb0b24c76b1cce908	App	Contributor	Subscription (Inherited)	None
<input type="checkbox"/>	ODL_User 208585 odl_user_208585@cl4udacit...	User	Contributor	Subscription (Inherited)	None
Key Vault Crypto Service Encryption User					
Owner					
<input type="checkbox"/>	Foreign Principal for 'Spektra S	Foreign principal	Owner	Subscription (Inherited)	None
<input type="checkbox"/>	https://cl4udacity1095.onmicrc	App	Owner	Subscription (Inherited)	None
<input type="checkbox"/>	Ramesh Bamidipati admin@cl4udacity1095.onm...	User	Owner	Subscription (Inherited)	None
<input type="checkbox"/>	ODL_User 208585 odl_user_208585@cl4udacit...	User	Owner	This resource	None
<input type="checkbox"/>	Srinadh Srinadh@cl4udacity1095.on...	User	Owner	This resource	None
Reader					

V2:

Owner Access to Dev and Prod SQL Servers:

Home > sql-devdata-208585

sql-devdata-208585 | Access control (IAM)

Search

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

CloudDevOps Custom RBAC I1346 S1					
<input type="checkbox"/>	Identity not found. Unable to find identity.	Unknown	CloudDevOps Custom RBAC I1346 S1	Subscription (Inherited)	None
<input type="checkbox"/>	Identity not found. Unable to find identity.	Unknown	CloudDevOps Custom RBAC I1346 S1	Subscription (Inherited)	None
Contributor					
Key Vault Crypto Service Encryption User					
<input type="checkbox"/>	Identity not found. Unable to find identity.	Unknown	Key Vault Crypto Service Encryption User	Subscription (Inherited)	None
Owner					
<input type="checkbox"/>	Foreign Principal for 'Spektra S	Foreign principal	Owner	Subscription (Inherited)	None
<input type="checkbox"/>	https://cl4udacity1095.onmicrc	App	Owner	Subscription (Inherited)	None
<input type="checkbox"/>	Ramesh Bamidipati admin@cl4udacity1095.onm...	User	Owner	Subscription (Inherited)	None
<input type="checkbox"/>	Neha Neha@cl4udacity1095.onmi...	User	Owner	Resource group (Inherited)	None
<input type="checkbox"/>	ODL_User 208585 odl_user_208585@cl4udacit...	User	Owner	Resource group (Inherited)	None
<input type="checkbox"/>	Srinadh Srinadh@cl4udacity1095.on...	User	Owner	Resource group (Inherited)	None
Reader					
<input type="checkbox"/>	Identity not found. Unable to find identity.	Unknown			

Home > sql-proddata-208585

sql-proddata-208585 | Access control (IAM)

SQL server

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Quick start

Settings

Azure Active Directory

SQL databases

SQL elastic pools

DTU quota

Properties

Locks

Data management

Backups

Deleted databases

Failover groups

+ Add

Download role assignments

Edit columns

Refresh

Remove

Got feedback?

CloudDevOps Custom RBAC I1346 S1

Identity not found. Unable to find identity.

Unknown

CloudDevOps Custom RBAC I1346 S1

Subscription (Inherited)

None

Identity not found. Unable to find identity.

Unknown

CloudDevOps Custom RBAC I1346 S1

Subscription (Inherited)

None

Contributor

2940bafb0b24c76b1cce908

App

Contributor

Subscription (Inherited)

None

ODL_User_208585 odl_user_208585@cl4udacit...

User

Contributor

Subscription (Inherited)

None

Key Vault Crypto Service Encryption User

Identity not found. Unable to find identity.

Unknown

Key Vault Crypto Service Encryption User

Subscription (Inherited)

None

Owner

Foreign Principal for 'Spektra S

Foreign principal

Owner

Subscription (Inherited)

None

https://cl4udacity1095.onmicrc

App

Owner

Subscription (Inherited)

None

Ramesh Bamjidipti admin@cl4udacity1095.onm...

User

Owner

Subscription (Inherited)

None

ODL_User_208585 odl_user_208585@cl4udacit...

User

Owner

Resource group (Inherited)

None

Srinadh Srinadh@cl4udacity1095.on...

User

Owner

Resource group (Inherited)

None

Home > rg-dev

rg-dev | Access control (IAM)

Resource group

Search

Overview

Activity log

Access control (IAM)

Tags

Resource visualizer

Events

Settings

Deployments

Security

Policies

Properties

Locks

Cost Management

Cost analysis

Cost alerts (preview)

Budgets

Advisor recommendations

+ Add

Download role assignments

Edit columns

Refresh

Remove

Got feedback?

Number of role assignments for this subscription

26

4000

Search by name or email

Type: All

Role: All

Scope: All scopes

Group by: Role

15 items (7 Users, 1 Foreign Principals, 1 Service Principals, 5 Unknown, 1 Managed Identities)

CloudDevOps Custom RBAC I1346 S1

Identity not found. Unable to find identity.

Unknown

CloudDevOps Custom RBAC I1346 S1

Subscription (Inherited)

None

Identity not found. Unable to find identity.

Unknown

CloudDevOps Custom RBAC I1346 S1

Subscription (Inherited)

None

Contributor

2940bafb0b24c76b1cce908

App

Contributor

Subscription (Inherited)

None

Neelima Neelima@cl4udacity1095.on...

User

Contributor

This resource

None

ODL_User_208585 odl_user_208585@cl4udacit...

User

Contributor

Subscription (Inherited)

None

Key Vault Crypto Service Encryption User

Identity not found. Unable to find identity.

Unknown

Key Vault Crypto Service Encryption User

Subscription (Inherited)

None

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

Home > Privileged Identity Management | Azure AD roles > Udacity 1095 | Roles > Global Administrator

Global Administrator | Role settings

Privileged Identity Management | Azure AD roles

Manage

- Assignments
- Description
- Role settings

« Edit

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

Assignment

Setting	State
Allow permanent eligible assignment	No
Expire eligible assignments after	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

3. Proof of Conditional Access policy all users

Home > Conditional Access | Policies >

New

Conditional Access policy

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

Create

aka.ms/capolicygrant

Grant

☐ Block access

☒ Grant access

☒ Require multifactor authentication

☐ Require device to be marked as compliant

☐ Require Hybrid Azure AD joined device

☐ Require approved client app

☐ Require app protection policy

☐ 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)

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 Azure portal interface for a resource named 'VNet-core-bastion'. The left sidebar contains navigation options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Sessions, Configuration, Properties, Locks, Monitoring, Metrics, Logs, Diagnostics settings, Connection Troubleshoot, Automation, and Tasks (preview). The main content area displays the 'Essentials' tab, which includes a search bar, 'Delete' and 'Refresh' buttons, and a 'JSON View' link. Below this, the 'Resource group' is 'rg-core', 'Location' is 'East US', 'Subscription' is 'Udacity_1095', and 'Subscription ID' is 'f48382ed-3e11-4494-af76-2a61b91fabd6'. The 'Virtual network/subnet' is 'VNet-core/AzureBastionSubnet', 'Public DNS name' is 'bst-a1fd191f-4562-406b-a160-3b56fd801a1c.bastion.azure.com', 'Public IP address' is 'VNet-core-ip', 'Tier' is 'Basic', and 'Provisioning state' is 'Succeeded'. The 'Tags' section shows 'DeploymentId : 208585', 'LaunchId : 1365', 'LaunchType : ON_DEMAND_LAB', 'TemplateId : 1145', and 'TenantId : none'. Below the 'Sessions' tab, a table with columns 'SessionId', 'StartTime (UTC)', 'TargetSubscriptionId', 'ResourceType', 'TargetHostName', 'TargetResourceGro...', 'UserName', 'TargetIPAddress', and 'Pr' is shown, with a message 'No results.' and a search bar.

2. Proof of public IP addresses removed

The screenshot shows the Azure portal interface for a virtual machine named 'vm-ws16devapp'. The left sidebar contains navigation options: 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, Continuous delivery, and Availability + scaling. The main content area displays the 'Essentials' tab, which includes a search bar, 'Connect', 'Start', 'Restart', 'Stop', 'Capture', 'Delete', 'Refresh', 'Open in mobile', and 'CLI / PS' buttons. Below this, the 'Resource group' is 'rg-dev', 'Status' is 'Running', 'Location' is 'East US', 'Subscription' is 'Udacity_1095', and 'Subscription ID' is 'f48382ed-3e11-4494-af76-2a61b91fabd6'. The 'Operating system' is 'Windows (Windows Server 2019 Datacenter)', 'Size' is 'Standard B2s (2 vcpus, 4 GiB memory)', 'Public IP address' is '-', 'Virtual network/subnet' is '-', and 'DNS name' is '-'. The 'Tags' section shows 'DeploymentId : 208585', 'LaunchId : 1365', 'LaunchType : ON_DEMAND_LAB', 'TemplateId : 1145', and 'TenantId : none'. Below the 'Properties' tab, a table with columns 'Virtual machine' and 'Networking' is shown. The 'Virtual machine' section includes 'Computer name' (VM-WS16DevWeb), 'Health state' (-), 'Operating system' (Windows (Windows Server 2019 Datacenter)), 'Publisher' (MicrosoftWindowsServer), and 'Offer' (WindowsServer). The 'Networking' section includes 'Public IP address' (-), 'Public IP address (IPv6)' (-), 'Private IP address' (-), and 'Private IP address (IPv6)' (-). At the bottom, a URL is visible: 'portal.azure.com/#@cl4udacity1095.onmicrosoft.com/resource/subscriptions/f48382ed-3e11-4494-af76-2a61b91fabd6/resourceGroups/rg-dev/providers/Microsoft.Compute/virtualMachines/vm-ws16devapp/o...'. A 'Give feedback' link is also present.

Home > Resource groups > rg-operations >

VM-WS16OpWeb

Virtual machine

Search

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

Advisor (1 of 1): Vulnerabilities in security configuration on your Windows machines should be remediated (powered by Guest Configuration) →

JSON View

Essentials

Resource group (move) : [rg-operations](#) Operating system : Windows

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

Location : East US Public IP address : -

Subscription (move) : [Udacity_1095](#) Virtual network/subnet : -

Subscription ID : f48382ed-3e11-4494-af76-2a61b91fabd6 DNS name : -

Tags (edit) : DeploymentId : 208585 LaunchId : 1365 LaunchType : ON_DEMAND_LAB TemplateId : 1145 TenantId : none

Properties Monitoring Capabilities (8) Recommendations (1) Tutorials

Virtual machine

Computer name	VM-WS16OpWeb
Health state	-
Operating system	Windows
Publisher	MicrosoftWindowsServer
Offer	WindowsServer

Networking

Public IP address	-
Public IP address (IPv6)	-
Private IP address	-
Private IP address (IPv6)	-
Virtual network/subnet	-

Give feedback

Home > Resource groups > rg-hrlegal >

VM-WS19HRL-App

Virtual machine

Search

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

Advisor (1 of 1): Vulnerabilities in security configuration on your Windows machines should be remediated (powered by Guest Configuration) →

JSON View

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_1095](#) Virtual network/subnet : -

Subscription ID : f48382ed-3e11-4494-af76-2a61b91fabd6 DNS name : -

Tags (edit) : DeploymentId : 208585 LaunchId : 1365 LaunchType : ON_DEMAND_LAB TemplateId : 1145 TenantId : none

Properties Monitoring Capabilities (8) Recommendations (1) Tutorials

Virtual machine

Computer name	VM-WS19HRL-Web
Health state	-
Operating system	Windows
Publisher	MicrosoftWindowsServer
Offer	WindowsServer

Networking

Public IP address	-
Public IP address (IPv6)	-
Private IP address	-
Private IP address (IPv6)	-
Virtual network/subnet	-

Give feedback

Home > Resource groups > rg-hrlegal >

VM-WS19HRL-Web

Virtual machine

Search

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

Advisor (1 of 1): Vulnerabilities in security configuration on your Windows machines should be remediated (powered by Guest Configuration) →

JSON View

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_1095	Virtual network/subnet	: -
Subscription ID	: f48382ed-3e11-4494-af76-2a61b91fabd6	DNS name	: -
Tags (edit)	DeploymentId : 208585 LaunchId : 1365 LaunchType : ON_DEMAND_LAB TemplateId : 1145 TenantId : none		

Properties

Virtual machine		Networking	
Computer name	VM-WS19HRL-Web	Public IP address	-
Health state	-	Public IP address (IPv6)	-
Operating system	Windows	Private IP address	-
Publisher	MicrosoftWindowsServer	Private IP address (IPv6)	-
Offer	WindowsServer	Virtual network/subnet	-

Give feedback

V2:

Removed public ip address from VM-WS16DevWeb

Home > Resource groups > rg-dev >

VM-WS16DevWeb

Virtual machine

Search

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

Advisor (1 of 1): Vulnerabilities in security configuration on your Windows machines should be remediated (powered by Guest Configuration) →

JSON View

Essentials

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_1095	Virtual network/subnet	: -
Subscription ID	: f48382ed-3e11-4494-af76-2a61b91fabd6	DNS name	: -
Tags (edit)	DeploymentId : 208585 LaunchId : 1365 LaunchType : ON_DEMAND_LAB TemplateId : 1145 TenantId : none		

Properties

Virtual machine		Networking	
Computer name	VM-WS16DevWeb	Public IP address	-
Health state	-	Public IP address (IPv6)	-
Operating system	Windows	Private IP address	-
Publisher	MicrosoftWindowsServer	Private IP address (IPv6)	-
Offer	WindowsServer	Virtual network/subnet	-

Give feedback

Data and Encryption

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

Home > des-disk

des-disk | Resources ☆ ...

Search (Ctrl+N)

Home > Virtual machines > vm-ws16devapp | Disks > vm-ws16devapp-osdisk

vm-ws16devapp-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-WS16DevWeb | Disks > VM-WS16DevWeb-osdisk

VM-WS16DevWeb-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 > 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

Disks

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

Networking

Disk Export

Disks

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-WS19OpApp | Disks > VM-WS19OpApp-osdisk

VM-WS19OpApp-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. Firewalls and virtual networks page

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

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

sql-devdata-202442 | Networking

SQL server

Search (Ctrl+/)

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

Feedback

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 TLS version and certificates, refer to connecting with TLS/SSL. [Learn more](#)

Minimum TLS version TLS 1.2

Home > sql-proddata-202442

sql-proddata-202442 | Networking

SQL server

Search (Ctrl+/)

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

Feedback

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	HRLegal	default	10.0.0.0/24	Enabled	rg-hrlegal	0d904d18-9d...	Ready

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

Home > sql-proddata-202442

sql-proddata-202442 | Networking

SQL server

Search (Ctrl+/)

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

Feedback

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 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)

Search (Ctrl+/)

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

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

Recommendations

0

Security alerts

0

Findings

--

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

Learn more

[About Microsoft Defender for Cloud](#)
[About Microsoft Defender for SQL](#)

Recommendations

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



No recommendations to display

There are no security recommendations for this resource

[View all recommendations in Defender for Cloud](#)

Security incidents and alerts

Defender for Cloud uses advanced analytics and global threat intelligence to alert you to malicious activity. Alerts displayed below are from the past 21 days.

Search (Ctrl+/)

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

Settings

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

Data management

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

Security

- Networking
- Microsoft Defender for Cloud
- Transparent data encryption

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

Recommendations

0

Security alerts

0

Findings

--

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

Learn more

[About Microsoft Defender for Cloud](#)
[About Microsoft Defender for SQL](#)

Recommendations

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



No recommendations to display

There are no security recommendations for this resource

[View all recommendations in Defender for Cloud](#)

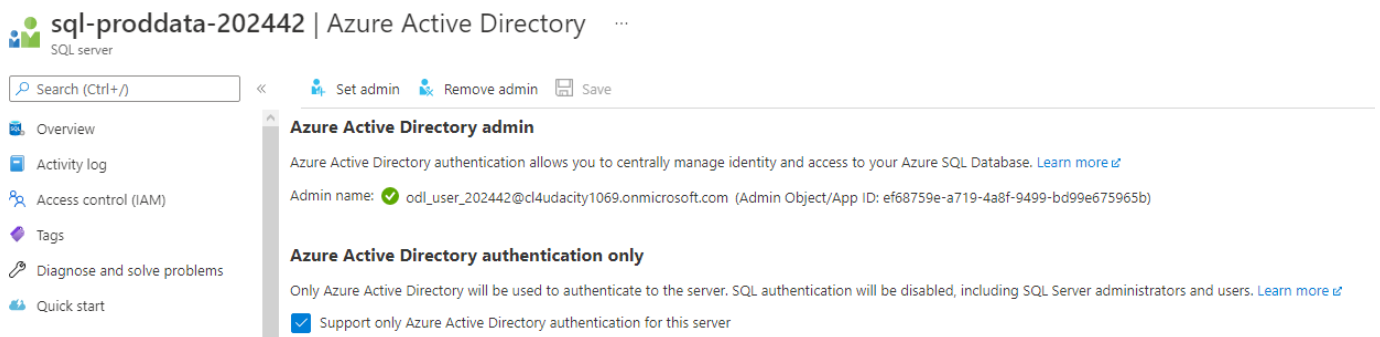
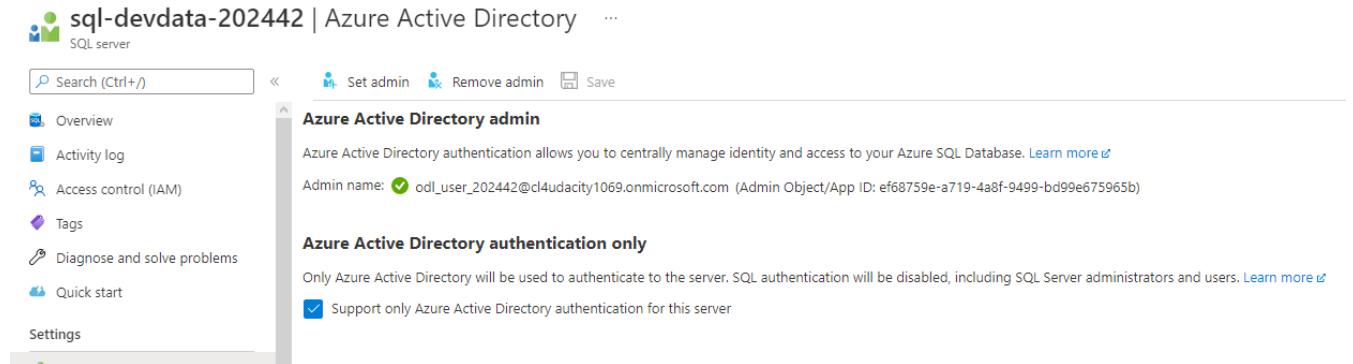
Security incidents and alerts

Defender for Cloud uses advanced analytics and global threat intelligence to alert you to malicious activity. Alerts displayed below are from the past 21 days.

[Check for alerts on this resource in Microsoft Defender for Cloud >](#)

Vulnerability assessment findings

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



Cloud Protection

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

Home >

vm-ws16devapp/laaSAntimalware

microsoft.compute/virtualmachines/extensions

Search (Ctrl+J)

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-1069

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

Tags (edit) : Click here to add tags

Resource id : /subscriptions/0d904d18-8db0-4da9-ac30-cbd31a3a16e5/resourceGroups/rg-dev/providers/Microsoft.Compute/virtualMachines/extensions

Type : Microsoft.Compute/virtualMachines/extensions

JSON View

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 : ---

Home > microsoft.antimalware-windows-20220728212949

VM-WS16OpWeb/laaSAntimalware

microsoft.compute/virtualmachines/extensions

Search (Ctrl+J)

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-1069

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

Tags (edit) : Click here to add tags

Resource id : /subscriptions/0d904d18-8db0-4da9-ac30-cbd31a3a16e5/resourceGroups/rg-operations/providers/Microsoft.Compute/virtualMachines/extensions

Type : Microsoft.Compute/virtualMachines/extensions

JSON View

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 : ---

Home > microsoft.antimalware-windows-20220728213040 >

VM-WS19HRL-App/laaSAntimalware

☆ ...

✕

microsoft.compute/virtualmachines/extensions

Search (Ctrl+J)

<

Refresh

Delete

Overview

Essentials

JSON View

Activity log

Access control (IAM)

Settings

Locks

Automation

Tasks (preview)

Export template

Support + troubleshooting

New Support Request

Resource group (move)

Subscription (move)

Subscription ID

Tags (edit)

rg-hrlegal

usdacity-1062

0d904d18-8db0-4da9-ac30-cbd31a3a16e5

Click here to add tags

Resource id

Type

/subscriptions/0d904d18-8db0-4da9-ac30-cbd31a3a16e5/resourceGroups/rg-hrlegal/providers/...

Microsoft.Compute/virtualMachines/extensions

Properties

Instance view

Force update tag

Publisher

Type

Type handler version

Auto upgrade minor version

Enable automatic upgrade

Settings

Protected settings

Provisioning state

Suppress failures

Microsoft.Azure.Security

laaSAntimalware

1.3

true

View value as JSON

Succeeded

Name

Type

Type handler version

Substatuses

Statuses

Home > microsoft.antimalware-windows-20220728213117 >

VM-WS19HRL-Web/laaSAntimalware

☆ ...

✕

microsoft.compute/virtualmachines/extensions

Search (Ctrl+J)

<

Refresh

Delete

Overview

Essentials

JSON View

Activity log

Access control (IAM)

Settings

Locks

Automation

Tasks (preview)

Export template

Support + troubleshooting

New Support Request

Resource group (move)

Subscription (move)

Subscription ID

Tags (edit)

rg-hrlegal

usdacity-1062

0d904d18-8db0-4da9-ac30-cbd31a3a16e5

Click here to add tags

Resource id

Type

/subscriptions/0d904d18-8db0-4da9-ac30-cbd31a3a16e5/resourceGroups/rg-hrlegal/providers/...

Microsoft.Compute/virtualMachines/extensions

Properties

Instance view

Force update tag

Publisher

Type

Type handler version

Auto upgrade minor version

Enable automatic upgrade

Settings

Protected settings

Provisioning state

Suppress failures

Microsoft.Azure.Security

laaSAntimalware

1.3

true

View value as JSON

Succeeded

Name

Type

Type handler version

Substatuses

Statuses

Home > microsoft.antimalware-windows-20220726213258 >

VM-WS19OpApp/laaSantimalware

microsoft.compute/virtualmachines/extensions

Search (Ctrl+F) 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 1069

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

Tags (edit) : Click here to add tags

Resource id : /subscriptions/0d904d18-8db0-4da9-ac30-cbd31a3a16e5/resourceGroups/rg-operations/providers/Microsoft.Compute/virtualMachines/extensions

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 : ---

V2:

Antimalware on VM-WS16DevWeb:

Home >

VM-WS16DevWeb/laaSantimalware

microsoft.compute/virtualmachines/extensions

Search (Ctrl+F) 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 1069

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

Tags (edit) : Click here to add tags

Resource id : /subscriptions/0d904d18-8db0-4da9-ac30-cbd31a3a16e5/resourceGroups/rg-dev/providers/Microsoft.Compute/virtualMachines/extensions

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. Recommendations

Home > Microsoft Defender for Cloud | Overview >

Security posture

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

Azure environment

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.

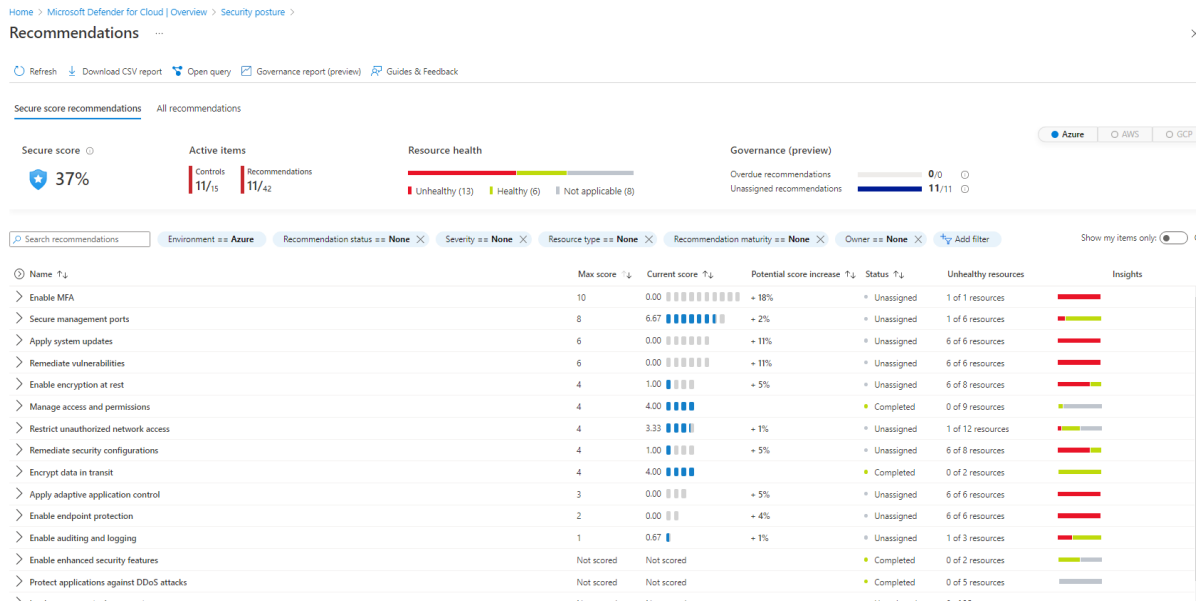
Enable Entra Permission Management >

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 >



→ Multi-Factor Authentication (MFA) is a method used to authenticate our identity.

It is often stated as a combination of two or more forms of

- What you know,
- What you have
- What you are

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

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

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

User accounts requiring MFA

Enable MFA for the following user accounts:

Ramesh Bamidipati

- Other 2 top remediations are “Apply system updates” and “Remediate vulnerabilities”. Both of them have a score of 0/6.
- System Updates are crucial as hackers are constantly searching for their way in by any means.
- Security patches are constantly released for systems so keeping them up to date ensures that one cannot use that as an advantage to gain access to something

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

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

And we should install vulnerability assessment tools on our VMs.

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

Monitoring

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



Save



Discard



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

Logs

Automation

Tasks (preview)

Export template

Support + troubleshooting

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



Home > sql-proddata-202442

sql-proddata-202442 | Auditing

SQL server

Search (Ctrl+/) 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 *

Udacity 1069

Log Analytics *

law-udacity(eastus)

- ☐ Event Hub

Auditing of Microsoft support operations

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

Enable Auditing of Microsoft support operations ☒

Use different audit log destinations ☐

2. Proof of Sentinel connectors (2+)

Adding Azure AD Connector to Sentinel:

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

General

- Overview
- Logs
- News & guides
- Search (Preview)

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence
- MITRE ATT&CK (Preview)

Content management

- Content hub (Preview)
- Repositories (Preview)
- Community

Compliance

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

Home > Microsoft Defender for Cloud >

Environment settings

+ Add environment | SQL Information Protection | Refresh Guides & Feedback

1 Azure subscriptions 0 AWS accounts 0 GCP projects

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

Search by name Environments == All Standards == All Coverage == All

Collapse all

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