

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

Home > Groups | All groups > IT

IT | 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

Role	Principal name	Scope	Membership	State	Start time	End time	Action
Message Center Reader		Directory	Direct	Active	-	Permanent	Remove Update

Home > IT

IT | Members

Group

Overview Diagnose and solve problems

Manage

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

Add members Remove Refresh Bulk operations Columns Got feedback?

Direct members All members

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

Home > Groups | All groups > Executive

Executive | 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

Role	Principal name	Scope	Membership	State	Start time	End time	Action
Message Center Reader		Directory	Direct	Active	-	Permanent	Remove Update

Home > Groups | All groups > Executive

Executive | Members

Group

Overview

Diagnose and solve problems

Manage

- Properties
- Members**
- Owners
- Roles and administrators

Direct members All members

Search by name Add filters

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

Home > HR

HR | Assigned roles

Group

Overview

Diagnose and solve problems

Manage

- Properties
- Members
- Owners
- Roles and administrators

Eligible assignments Active assignments Expired assignments

Search by role

Role	Principal name	Scope	Membership	Start time	End time	Action
User Administrator		Directory	Direct	1/3/2023, 5:08:07 AM	Permanent	Remove Update

Home > Groups | All groups > HR

HR | Members

Group

Overview

Diagnose and solve problems

Manage

- Properties
- Members**
- Owners
- Roles and administrators

Direct members All members

Search by name Add filters

Name	Type	Email	User type
LO Lora	User		Member

Home > Groups | All groups > Support Desk

Support Desk | Assigned roles

Group

Overview

Diagnose and solve problems

Manage

- Properties
- Members
- Owners

Eligible assignments **Active assignments** Expired assignments

Search by role

Role	Principal name	Scope	Membership	State	Start time	End time	Action
Helpdesk Administrator		Directory	Direct	Active	-	Permanent	Remove Update

Home > Groups | All groups > Support Desk

Support Desk | Members

Group

Overview

Diagnose and solve problems

Manage

- Properties
- Members
- Owners

Direct members All members

Search by name Add filters

Name	Type	Email	User type
Winfred	User		Member

The COO will have the Billing Admin role active

Karl | Assigned roles

Eligible assignments Active assignments Expired assignments

Role	Principal name	Scope	Membership	State	Start time	End time	Action
Message Center Reader	Karl@cl4udacity1072.onmicrosoft.com	Directory	Group	Active	-	Permanent	Remove Update
Billing Administrator	Karl@cl4udacity1072.onmicrosoft.com	Directory	Direct	Active	1/3/2023, 3:35:18 AM	Permanent	Remove Update

The Azure Architect will be eligible for the Global Admin and Billing admin roles

Seth | Assigned roles

Eligible assignments Active assignments Expired assignments

Role	Principal name	Scope	Membership	State	Start time	End time	Action
Global Administrator	Seth@cl4udacity1072.onmicrosoft.com	Directory	Direct	Active	1/3/2023, 3:42:25 AM	Permanent	Remove Update
Message Center Reader	Seth@cl4udacity1072.onmicrosoft.com	Directory	Group	Active	-	Permanent	Remove Update
Billing Administrator	Seth@cl4udacity1072.onmicrosoft.com	Directory	Direct	Active	1/3/2023, 4:25:45 AM	Permanent	Remove Update

The CIO will not continually work in the environment however, they will need the same Azure AD access should the need arise to step in for the Azure Architect

Chris | Assigned roles

Eligible assignments Active assignments Expired assignments

Role	Principal name	Scope	Membership	State	Start time	End time	Action
Global Administrator	Chris@cl4udacity1072.onmicrosoft.com	Directory	Direct	Active	1/3/2023, 4:33:38 AM	Permanent	Remove Update
Message Center Reader	Chris@cl4udacity1072.onmicrosoft.com	Directory	Group	Active	-	Permanent	Remove Update
Billing Administrator	Chris@cl4udacity1072.onmicrosoft.com	Directory	Direct	Active	1/3/2023, 4:33:07 AM	Permanent	Remove Update

Development DBA will only need to access the Dev Database

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 | Monitoring | Insights (preview) | Alerts | Metrics | Diagnostic settings | Logs | Advisor recommendations | Workbooks | Automation

Access control (IAM)

27 items (7 Users, 1 Foreign Principals, 2 Service Principals, 16 Unknown, 1 Managed identities)

Name	Type	Role	Scope	Condition
Azure Kubernetes Service Contributor Role				
Contributor				
Kubernetes Extension Contributor				
Log Analytics Contributor				
Owner				
Foreign Principal for Spektra Systems L	Foreign principal	Owner	Subscription (Inherited)	None
https://c4udacity1072.onmicrosoft.com	App	Owner	Subscription (Inherited)	None
Ramesh Bamidipati	User	Owner	Subscription (Inherited)	None
NE	User	Owner	This resource	None
ODL_User_221029	User	Owner	This resource	None
O2	User	Owner	This resource	None
Srinadh	User	Owner	This resource	None
Reader				
O2	User	Reader	Subscription (Inherited)	None
Security Admin				
Spektra Custom RBAC I1379 S1				
O2	User	Spektra Custom RBAC I1379 S1	Subscription (Inherited)	None
VM Scanner Operator				
Microsoft Defender for Cloud Servers S	App	VM Scanner Operator	Subscription (Inherited)	None

The lead DBA will need access to all SQL infrastructure and data

rg-data | 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 | Monitoring | Insights (preview) | Alerts | Metrics | Diagnostic settings | Logs | Advisor recommendations | Workbooks | Automation

Access control (IAM)

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

Number of role assignments for this subscription ○

37 4000

Name	Type	Role	Scope	Condition
Azure Kubernetes Service Contributor Role				
Contributor				
Kubernetes Extension Contributor				
Log Analytics Contributor				
Owner				
Foreign Principal for Spektra Systems L	Foreign principal	Owner	Subscription (Inherited)	None
https://c4udacity1072.onmicrosoft.com	App	Owner	Subscription (Inherited)	None
Ramesh Bamidipati	User	Owner	Subscription (Inherited)	None
ODL_User_221029	User	Owner	This resource	None
O2	User	Owner	This resource	None
Srinadh	User	Owner	This resource	Home
Reader				
O2	User	Reader	Subscription (Inherited)	None
Security Admin				
O2	User	Security Admin	Subscription (Inherited)	None
Spektra Custom RBAC I1379 S1				

The IT Engineers will each need access to their assigned environments but will not need to provide this access to others

Name	Type	Role	Scope	Condition
271c5e827def47949e89b146	App	Contributor	Subscription (Inherited)	None
Identity not found.	Unknown	Contributor	Subscription (Inherited)	None
Identity not found.	Unknown	Contributor	Subscription (Inherited)	None
Identity not found.	Unknown	Contributor	Subscription (Inherited)	None
Identity not found.	Unknown	Contributor	Subscription (Inherited)	None
Identity not found.	Unknown	Contributor	Subscription (Inherited)	None
IT	Group	Contributor	This resource	None
Kubernetes Extension Contributor				
Log Analytics Contributor				
Owner				
Reader				
ODL_User_221029	User	Reader	Subscription (Inherited)	None
Security Admin				

Development Lead will each need access to their assigned environments but will not need to provide this access to others

Name	Type	Role	Scope	Condition
271c5e827def47949e89b146	App	Contributor	Subscription (Inherited)	None
Neelima	User	Contributor	This resource	None
Identity not found.	Unknown	Contributor	Subscription (Inherited)	None
Identity not found.	Unknown	Contributor	Subscription (Inherited)	None
Identity not found.	Unknown	Contributor	Subscription (Inherited)	None
Identity not found.	Unknown	Contributor	Subscription (Inherited)	None

rg-prod | Access control (IAM)

Number of role assignments for this subscription

Name	Type	Role	Scope	Condition
27 items (7 Users, 1 Foreign Principals, 2 Service Principals, 16 Unknown, 1 Managed Identities)				
271c5e827def47949e89b146	App	Contributor	Subscription (Inherited)	None
Neelima	User	Contributor	This resource	None
Identity not found.	Unknown	Contributor	Subscription (Inherited)	None
Identity not found.	Unknown	Contributor	Subscription (Inherited)	None
Identity not found.	Unknown	Contributor	Subscription (Inherited)	None
Identity not found.	Unknown	Contributor	Subscription (Inherited)	None
Identity not found.	Unknown	Contributor	Subscription (Inherited)	None

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

Global Administrator | Role settings

Activation

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

Assignment

Setting	State
Allow permanent eligible assignment	No
Expire eligible assignments after	1 year(s)
Allow permanent active assignment	No
Expire active assignments after	6 month(s)
Require Azure Multi-Factor Authentication on active assignment	No
Require justification on active assignment	Yes

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

Type	Default recipients	Additional recipients	Critical emails only
Role assignment alert	Admin	None	False
Notification to the assigned user (assignee)	Assignee	None	False
Request to approve a role assignment renewal/extension	Approver	None	False

3. Proof of Conditional Access policy all users

The screenshot shows the Microsoft Azure Conditional Access policy configuration page for a policy named "CA004: Require multifactor authentication for all users".

Left Panel (Policy Overview):

- Name:** CA004: Require multifactor authentication for all users
- Description:** Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.
- Assignments:**
 - Users:** All users included and specific users excluded
 - Cloud apps or actions:** All cloud apps
 - Conditions:** 0 conditions selected
- Access controls:**
 - Grant:** 1 control selected
 - Session:** 0 controls selected
- Enable policy:** Report-only (selected), On, Off
- Buttons:** Save, Select

Right Panel (Grant Configuration):

Grant

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

Block access
 Grant access

Require multifactor authentication

Consider testing the new "Require authentication strength" public preview. [Learn more](#)

Require authentication strength (Preview)

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

Require device to be marked as compliant

Require Hybrid Azure AD joined device

Require approved client app [See list of approved client apps](#)

Require app protection policy [See list of policy protected client apps](#)

Require password change

For multiple controls

Require all the selected controls
 Require one of the selected

Select

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

multi-factor authentication

users service settings

app passwords [\(learn more\)](#)

- Allow users to create app passwords to sign in to non-browser apps
- Do not allow users to create app passwords to sign in to non-browser apps

trusted ips [\(learn more\)](#)

- Skip multi-factor authentication for requests from federated users on my intranet
- Skip multi-factor authentication for requests from following range of IP address subnets

143.52.0.0/24

verification options [\(learn more\)](#)

Methods available to users:

- Call to phone
- Text message to phone
- Notification through mobile app
- Verification code from mobile app or hardware token

remember multi-factor authentication on trusted device [\(learn more\)](#)

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

Number of days users can trust devices for

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

save

Manage advanced settings and view reports [Go to the portal](#)

Network Security

1. Bastion overview

Home > [Bastions](#) >

Create a Bastion

Validation passed

Basics Tags Advanced [Review + create](#)

Summary

Basics

Name	CoreBastion
Subscription	Udacity 1072
Resource group	rg-core
Region	East US
Virtual network	VNet-core
Subnets	AzureBastionSubnet
Public IP address	VNet-core-ip
Tier	Standard
Instance count	2
Copy and paste	Enabled
IP-based connection	Disabled
Kerberos authentication (Preview)	Disabled
Shareable Link	Disabled
Native client support	Disabled

Home > Microsoft.BastionHost-20230103050309 | Overview >

CoreBastion Bastion

Search Delete Refresh

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

Essentials

Resource group (move)	rg-core	Virtual network/subnet	VNet-core/AzureBastionSubnet
Location	: East US	Public DNS name	: bst-48490811-b2da-43d8-baed-2187aa542b75.bastion.azure.com
Subscription (move)	: Udacity_1072	Public IP address	: VNet-core-ip
Subscription ID	: 95ced28e-73b9-4d38-99e0-ff480a9455a	Tier	: Standard
		Provisioning state	: Succeeded

Tags (edit) : DeploymentId : 221029 LaunchId : 1379 LaunchType : ON_DEMAND_LAB TemplateId : 1211 TenantId : none

Sessions Tutorials

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

Metrics Logs Diagnostics settings Connection Troubleshoot

Tasks (preview) Export template

Resource health New Support Request

2. Proof of public IP addresses removed

Home > VM-WS16DevWeb

VM-WS16DevWeb Virtual machine

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

Overview

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

Settings

Networking Connect Windows Admin Center Disks Size Microsoft Defender for Cloud Advisor recommendations Extensions + applications Continuous delivery Availability + scaling Configuration Identity Properties Locks

Operations

Bastion Auto-shutdown Backup Disaster recovery

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)	: Uadcity_1072	Virtual network/subnet	: Vnet-Dev/default
Subscription ID	: 95ced28e-73b9-4d38-99e0-ffc480a9455a	DNS name	: -
Tags (edit)	: DeploymentId : 221029 LaunchId : 1379 LaunchType : ON_DEMAND_LAB TemplateId : 1211 TenantId : none		

Properties Monitoring Capabilities (8) Recommendations Tutorials

Virtual machine

Computer name	VM-WS16DevWeb	Networking	Public IP address	-
Health state	-	Public IP address (IPv6)	-	
Operating system	Windows	Private IP address	10.2.0.4	
Publisher	MicrosoftWindowsServer	Private IP address (IPv6)	-	
Offer	WindowsServer	Virtual network/subnet	Vnet-Dev/default	
Plan	2019-Datacenter	DNS name	-	
VM generation	V1			
VM architecture	x64			
Host group	None			
Host	-			
Proximity placement group	-			
Colocation status	N/A			
Capacity reservation group	-			

Availability + scaling

Availability zone	-	Size	Size	Standard B2s
Availability set	-	vCPUs	2	
Scale Set	-	RAM	4 GiB	

Disk

OS disk	VM-WS16DevWeb-osdisk
Encryption at host	Disabled
Azure disk encryption	Not enabled
Ephemeral OS disk	N/A
Data disks	0

JSON View

Home > All resources > VM-WS16OpWeb

VM-WS16OpWeb Virtual machine

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

Overview

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

Settings

Networking Connect Windows Admin Center Disks Size Microsoft Defender for Cloud Advisor recommendations Extensions + applications Continuous delivery Availability + scaling Configuration Identity Properties Locks

Operations

Bastion Auto-shutdown Backup Disaster recovery

Invitations

Essentials

Resource group (move)	: rg-operations	Operating system	: Windows
Status	: Stopped (deallocated)	Size	: Standard B2s (2 vcpus, 4 GiB memory)
Location	: East US	Public IP address	: -
Subscription (move)	: Uadcity_1072	Virtual network/subnet	: Vnet-operations/default
Subscription ID	: 95ced28e-73b9-4d38-99e0-ffc480a9455a	DNS name	: -
Tags (edit)	: DeploymentId : 221029 LaunchId : 1379 LaunchType : ON_DEMAND_LAB TemplateId : 1211 TenantId : none		

Properties Monitoring Capabilities (8) Recommendations Tutorials

Virtual machine

Computer name	VM-WS16OpWeb	Networking	Public IP address	-
Health state	-	Public IP address (IPv6)	-	
Operating system	Windows	Private IP address	10.0.0.4	
Publisher	MicrosoftWindowsServer	Private IP address (IPv6)	-	
Offer	WindowsServer	Virtual network/subnet	Vnet-operations/default	
Plan	2019-Datacenter	DNS name	-	
VM generation	V1			
VM architecture	x64			
Host group	None			
Host	-			
Proximity placement group	-			
Colocation status	N/A			
Capacity reservation group	-			

Availability + scaling

Availability zone	-	Size	Size	Standard B2s
Availability set	-	vCPUs	2	
Scale Set	-	RAM	4 GiB	

Disk

OS disk	VM-WS16OpWeb-osdisk
Encryption at host	Disabled
Azure disk encryption	Not enabled
Ephemeral OS disk	N/A
Data disks	0

JSON View

VM-WS19HRL-Web Virtual machine

[Search](#) Connect Start Restart Stop Capture Delete Refresh Open in mobile CLI / PS Feedback

[Overview](#) [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_1072	Virtual network/subnet :	HRLegal/default
Subscription ID :	95ced28e-73b9-4d38-99e0-fc480a9455a	DNS name :	-
Tags (edit) :	DeploymentId : 221029 LaunchId : 1379 LaunchType : ON_DEMAND_LAB TemplateId : 1211 TenantId : none		

Properties [Monitoring](#) [Capabilities \(8\)](#) [Recommendations](#) [Tutorials](#)

Virtual machine

Computer name	VM-WS19HRL-Web
Health state	-
Operating system	Windows
Publisher	MicrosoftWindowsServer
Offer	WindowsServer
Plan	2019-Datacenter
VM generation	V1
VM architecture	x64
Host group	None
Host	-
Proximity placement group	-
Colocation status	N/A
Capacity reservation group	-

Availability + scaling

Availability zone	-
Availability set	-
Scale Set	-

Security type

Auto-shutdown	Auto-shutdown
---------------	-------------------------------

Networking

Public IP address	-
Public IP address (IPv6)	-
Private IP address	10.0.0.4
Private IP address (IPv6)	-
Virtual network/subnet	HRLegal/default
DNS name	-

Size

Size	Standard B2s
vCPUs	2
RAM	4 GiB

Disk

OS disk	VM-WS19HRL-Web-osdisk
Encryption at host	Disabled
Azure disk encryption	Not enabled
Ephemeral OS disk	N/A
Data disks	0

Auto-shutdown

Auto-shutdown	Not enabled
---------------	-----------------------------

Data and Encryption

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

Home > All resources > p2-disk-en-set

p2-disk-en-set | Resources ...

Disk Encryption Set

Search Filter by name... All types

Overview Activity log Access control (IAM) Tags Settings

Name	Type	Resource Group	Subscription
VM-WS16DEVWEB-OSDISK	Disk	RG-DEV	Udacity 1074
VM-WS19HRL-WEB-OSDISK	Disk	RG-HRLEGAL	Udacity 1074
VM-WS16OPWEB-OSDISK	Disk	RG-OPERATIONS	Udacity 1074

Home > VM-WS19HRL-Web-osdisk

VM-WS19HRL-Web-osdisk | Encryption ...

Disk

Search Save Discard Refresh

Overview Activity log Access control (IAM) Tags Settings

Encryption

i 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](#)

Key management i

Customer-managed key: p2-disk-en-set

Home > VM-WS16OpWeb-osdisk

VM-WS16OpWeb-osdisk | Encryption ...

Disk

Search Save Discard Refresh

Overview Activity log Access control (IAM) Tags Settings

Encryption

i 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](#)

Key management i

Customer-managed key: p2-disk-en-set

Home > VM-WS16DevWeb-osdisk

VM-WS16DevWeb-osdisk | Encryption ⋮

Disk

Search Save Discard Refresh

Overview Activity log Access control (IAM) Tags

Settings Configuration Size + performance Encryption

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](#)

Key management ⓘ Customer-managed key: p2-disk-en-set

2. Firewalls and virtual networks page

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

Home > sql-devdata-221096

sql-devdata-221096 | Networking ⋮

SQL server

Search 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 Import/Export history

Security Networking Microsoft Defender for Cloud Transparent data encryption Identity Auditing

Intelligent Performance

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	6e9c6c2a-779...	Ready

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

+ Add your client IPv4 address (58.186.28.50) + Add a firewall rule

Rule name	Start IPv4 address	End IPv4 address

Exceptions Allow Azure services and resources to access this server

Home > sql-devdata-221096

sql-devdata-221096 | Networking

SQL server

Search

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. [Click to go back, hold to see history.](#)

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

Home > sql-proodata-221096

sql-proodata-221096 | Networking

SQL server

Search

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	VNet-prod	Operations	10.1.1.0/24	Enabled	rg-prod	6e9c6c2a-779...	Ready

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

+ Add your client IPv4 address (58.186.28.50) + Add a firewall rule

Home > sql-proodata-221096

sql-proodata-221096 | Networking

SQL server

Search

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

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

sql-devdata-221096 | Microsoft Defender for Cloud

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
- Import/Export history

Security

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

Intelligent Performance

Recommendations

0 1

Security alerts

0 1

Findings

Enable

Enable Status: Enabled at the subscription-level (Configured)

Learn more

About Microsoft Defender for Cloud

About Microsoft Defender for SQL

SQL Vulnerability Assessment is not configured. Click to enable express configuration (preview). Learn more

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

ID	Security Check	Applies to	Severity
No results			

sql-proddata-221096 | Microsoft Defender for Cloud

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
- Import/Export history

Security

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

Intelligent Performance

Recommendations Security alerts Findings

Enablement Status: Enabled at the subscription-level (Configure)

SQL Vulnerability Assessment is not configured. Click to enable express configuration (preview). Learn more

Enable

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

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

ID	Security Check	Applies to	Severity
No results			

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

sql-devdata-221096 | Azure Active Directory

SQL server

Search Set admin Remove admin Save

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

Settings

Azure Active Directory

Azure Active Directory admin

Azure Active Directory authentication allows you to centrally manage identity and access to your Azure SQL Database. [Learn more](#)

Admin name: odl_user_221096@cl4udacity1074.onmicrosoft.com (Admin Object/App ID: 1995a042-0155-4531-82d1-3707c8b5d354)

Azure Active Directory authentication only

Only Azure Active Directory will be used to authenticate to the server. SQL authentication will be disabled, including SQL Server administrators and users. [Learn more](#)

Support only Azure Active Directory authentication for this server

sql-proddata-221096 | Azure Active Directory ... X

Search Set admin Save

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

Settings

Azure Active Directory

Azure Active Directory admin

Azure Active Directory authentication allows you to centrally manage identity and access to your Azure SQL Database. [Learn more ↗](#)

Admin name: odl_user_221096@cl4udacity1074.onmicrosoft.com (Admin Object/App ID: 1995a042-0155-4531-82d1-3707c8b5d354)

Azure Active Directory authentication only

Only Azure Active Directory will be used to authenticate to the server. SQL authentication will be disabled, including SQL Server administrators and users. [Learn more ↗](#)

Support only Azure Active Directory authentication for this server

Cloud Protection

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

Home > microsoft.antimalware-windows-20230103105846 | Overview >

VM-WS19HRL-Web/IaaSAntimalware ...

microsoft.compute/virtualmachines/extensions

Search Refresh Delete

Overview

Essentials

Resource group (move) : rg-hrlegal
Subscription (move) : Udacity_1074
Subscription ID : 6e9c6c2a-779b-442b-a00d-1d0b1236722a
Tags (edit) : DeploymentId : 221096 LaunchId : 1379 LaunchType : ON_DEMAND_LAB TemplateId : 1211 TenantId : none

Resource id : /subscriptions/6e9c6c2a-779b-442b-a00d-1d0b1236722a/resourceGroups/rg-hrlegal/providers/Microsoft.Compute/virtualMachines/extensions
Type : Microsoft.Compute/virtualMachines/extensions

Properties

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

Instance view

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

JSON View

Home > microsoft.antimalware-windows-20230103105615 | Overview >

VM-WS16OpWeb/IaaSAntimalware ...

microsoft.compute/virtualmachines/extensions

Search Refresh Delete

Overview

Essentials

Resource group (move) : rg-operations
Subscription (move) : Udacity_1074
Subscription ID : 6e9c6c2a-779b-442b-a00d-1d0b1236722a
Tags (edit) : DeploymentId : 221096 LaunchId : 1379 LaunchType : ON_DEMAND_LAB TemplateId : 1211 TenantId : none

Resource id : /subscriptions/6e9c6c2a-779b-442b-a00d-1d0b1236722a/resourceGroups/rg-operations/providers/Microsoft.Compute/virtualMachines/extensions
Type : Microsoft.Compute/virtualMachines/extensions

Properties

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

Instance view

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

JSON View

Home > microsoft.antimalware-windows-20230103110509 | Overview >

VM-WS16DevWeb/IaaSAntimalware ...

microsoft.compute/virtualmachines/extensions

Search Refresh Delete

Overview

Essentials

Resource group (move) : rg-dev
Subscription (move) : Udacity_1074
Subscription ID : 6e9c6c2a-779b-442b-a00d-1d0b1236722a
Tags (edit) : DeploymentId : 221096 LaunchId : 1379 LaunchType : ON_DEMAND_LAB TemplateId : 1211 TenantId : none

Resource id : /subscriptions/6e9c6c2a-779b-442b-a00d-1d0b1236722a/resourceGroups/rg-dev/providers/Microsoft.Compute/virtualMachines/extensions
Type : Microsoft.Compute/virtualMachines/extensions

Properties

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

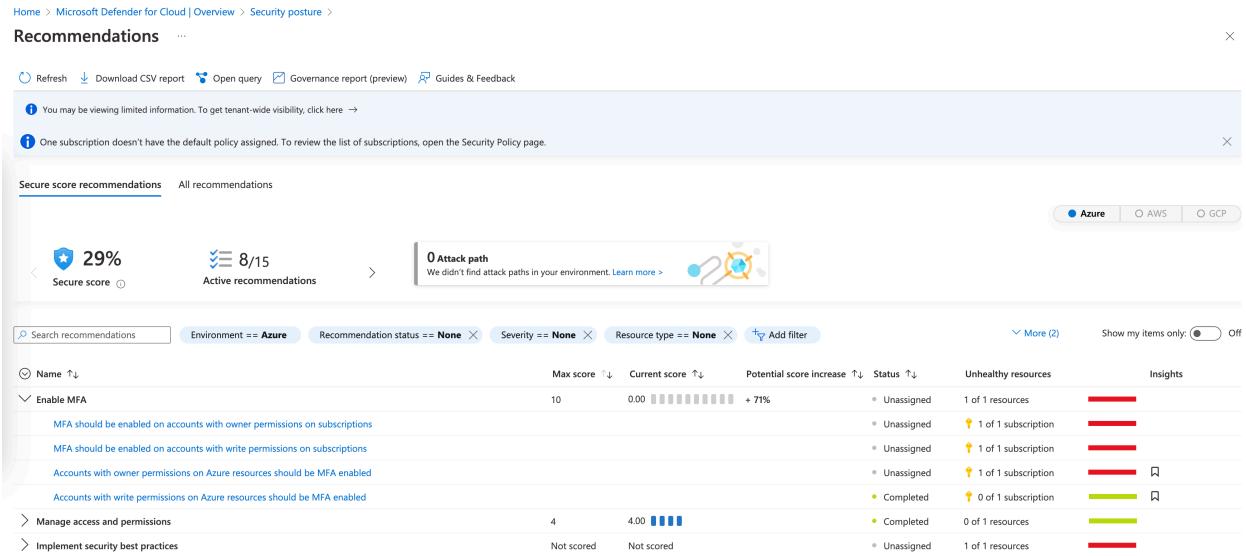
Instance view

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

JSON View

2. Recommendations

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

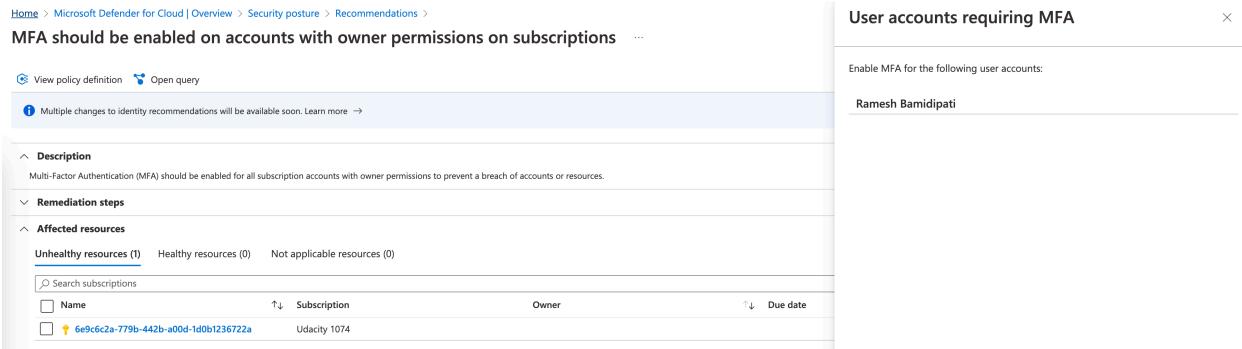


The screenshot shows the Microsoft Defender for Cloud Recommendations page. At the top, it displays a secure score of 29% (29%), 8/15 active recommendations, and 0 attack paths. Below this, there's a search bar and filter options for environment (Azure), recommendation status (None), severity (None), and resource type (None). A table lists recommendations, including "Enable MFA" which has the highest impact (Max score 10) and "Manage access and permissions" (Max score 4). The table includes columns for Max score, Current score, Potential score increase, Status, Unhealthy resources, and Insights.

A. Based on the security score, the “Enable MFA” has the greatest impact on security (0/10 score).

1. MFA should be enabled on accounts with owner permissions on subscriptions
2. MFA should be enabled on accounts with write permissions on
3. Accounts with owner permissions on Azure resources should be MFA enabled
4. Accounts with write permissions on Azure resources should be MFA enabled

Home > Microsoft Defender for Cloud | Overview > Security posture > Recommendations > MFA should be enabled on accounts with owner permissions on subscriptions ...



The screenshot shows a detailed view of the "MFA should be enabled on accounts with owner permissions on subscriptions" recommendation. It includes sections for Description (Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with owner permissions to prevent a breach of accounts or resources), Remediation steps, and Affected resources. The Affected resources section shows one unhealthy resource (Udacity 1074) and lists user accounts requiring MFA. A separate "User accounts requiring MFA" pane shows a list of accounts: Ramesh Bamidipati.

Home > Recommendations >

MFA should be enabled on accounts with write permissions on subscriptions

[View policy definition](#) [Open query](#)

[Multiple changes to identity recommendations will be available soon. Learn more →](#)

[Description](#)
Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with write privileges to prevent a breach of accounts or resources.

[Remediation steps](#)

[Affected resources](#)
Unhealthy resources (1) Healthy resources (0) Not applicable resources (0)

Search subscriptions

Name	Subscription	Owner	Due date
Ge9c6c2a-779b-442b-a00d-1d0b1236722a	Udacity 1074		

User accounts requiring MFA

Enable MFA for the following user accounts:

ODL_User 221096

The MFA is disabled for the account Ramesh Bamidipati which has owner permissions and ODL_User 221096 which has write permissions.

⇒ We should apply a Policy to enforce using MFA for all users (including owner, write role)

B. The “Manage access and permissions” is already solved (4/4 score)

C. Implement security best practices

[Implement security best practices](#)

Not scored	Not scored	Unassigned	1 of 1 resources
Completed	0 of 1 subscription	Completed	0 of 1 subscription
Completed	0 of 1 subscription	Completed	0 of 1 subscription
Completed	0 of 1 subscription	Completed	0 of 1 subscription
Completed	0 of 1 subscription	Completed	0 of 1 subscription
Completed	0 of 1 subscription	Completed	0 of 1 subscription
Completed	0 of 5 Subnets	Unassigned	1 of 1 subscription
Completed	0 of 3 virtual machines	Completed	0 of 1 subscription

MFA should be enabled on accounts with read permissions on subscriptions
Accounts with read permissions on Azure resources should be MFA enabled
Guest accounts with read permissions on Azure resources should be removed
External accounts with read permissions should be removed from subscriptions
A maximum of 3 owners should be designated for subscriptions
Subnets should be associated with a network security group
There should be more than one owner assigned to subscriptions
Non-internet-facing virtual machines should be protected with network security groups

There is 1 unresolve point in the best practices:

Home >

There should be more than one owner assigned to subscriptions

[View policy definition](#) [Open query](#)

Severity: **High** Freshness interval: **24 Hours** Tactics and techniques: **Defense Evasion**

[Description](#)
Designate more than one subscription owner in order to have administrator access redundancy.

[Remediation steps](#)

[Affected resources](#)
Unhealthy resources (1) Healthy resources (0) Not applicable resources (0)

Search subscriptions

Name	Subscription	Owner	Due date	Status
Ge9c6c2a-779b-442b-a00d-1d0b1236722a	Udacity 1074			

This point recommends having at least 2 users with owner role in a subscription. Designate more than one subscription owner in order to have administrator access redundancy so that if one of the owners forget or lost their password, or the account is hacked, etc. we still have at least 1 other owner.

To add assign an user as an owner, we can use the Access Control (IAM)

Monitoring

Identify 3 items from the Audit log and explain what each log shows.

Audit Logs						
1/3/2023, 4:21:39 PM	B2C	Authorization	Get B2C directory resources in a s...	Success	User Authorization: User was gran...	NotSet
1/3/2023, 4:21:15 PM	B2C	ResourceManagement	Get B2C directory resources in a s...	Success		NotSet
1/3/2023, 4:21:15 PM	B2C	ResourceManagement	Get Guest Usages resources in a s...	Success		NotSet
1/3/2023, 4:21:15 PM	B2C	Authorization	Get B2C directory resources in a s...	Success	User Authorization: User was gran...	NotSet
1/3/2023, 4:21:15 PM	B2C	Authorization	Get Guest Usages resources in a s...	Success	User Authorization: User was gran...	NotSet
1/3/2023, 4:07:34 PM	B2C	ResourceManagement	Get Guest Usages resources in a s...	Success		NotSet
1/3/2023, 4:07:34 PM	B2C	Authorization	Get Guest Usages resources in a s...	Success	User Authorization: User was gran...	NotSet
1/3/2023, 4:07:33 PM	B2C	ResourceManagement	Get B2C directory resources in a s...	Success		NotSet
1/3/2023, 4:07:33 PM	B2C	Authorization	Get B2C directory resources in a s...	Success	User Authorization: User was gran...	NotSet
1/3/2023, 4:05:45 PM	B2C	ResourceManagement	Get Guest Usages resources in a s...	Success		NotSet
1/3/2023, 4:05:45 PM	B2C	ResourceManagement	Get B2C directory resources in a s...	Success		NotSet
1/3/2023, 4:05:45 PM	B2C	Authorization	Get Guest Usages resources in a s...	Success	User Authorization: User was gran...	NotSet
1/3/2023, 4:05:45 PM	B2C	Authorization	Get B2C directory resources in a s...	Success	User Authorization: User was gran...	NotSet
1/3/2023, 4:05:41 PM	B2C	ResourceManagement	Get Guest Usages resources in a s...	Success		NotSet
1/3/2023, 4:05:41 PM	B2C	Authorization	Get Guest Usages resources in a s...	Success	User Authorization: User was gran...	NotSet
1/3/2023, 4:05:41 PM	B2C	ResourceManagement	Get B2C directory resources in a s...	Success		NotSet
1/3/2023, 4:05:41 PM	B2C	Authorization	Get B2C directory resources in a s...	Success	User Authorization: User was gran...	NotSet
1/3/2023, 4:02:21 PM	Core Directory	UserManagement	Add user	Failure	Microsoft.Online.Workflows.OBJ...	Michael@cl4udacity1075.onmicrosoft...
1/3/2023, 4:02:21 PM	Core Directory	UserManagement	Add user	Failure	Microsoft.Online.Workflows.OBJ...	Winifred@cl4udacity1075.onmicrosoft...
1/3/2023, 4:02:20 PM	Core Directory	UserManagement	Add user	Failure	Microsoft.Online.Workflows.OBJ...	Seth@cl4udacity1075.onmicrosoft...
1/3/2023, 4:02:20 PM	Core Directory	UserManagement	Add user	Failure	Microsoft.Online.Workflows.OBJ...	Lora@cl4udacity1075.onmicrosoft...
1/3/2023, 4:02:20 PM	Core Directory	UserManagement	Add user	Failure	Microsoft.Online.Workflows.OBJ...	Kaitlyn@cl4udacity1075.onmicrosoft...
1/3/2023, 4:02:20 PM	Core Directory	UserManagement	Add user	Failure	Microsoft.Online.Workflows.OBJ...	Allison@cl4udacity1075.onmicrosoft...
1/3/2023, 4:02:20 PM	Core Directory	UserManagement	Add user	Failure	Microsoft.Online.Workflows.OBJ...	Sherrie@cl4udacity1075.onmicrosoft...
1/3/2023, 4:02:19 PM	Core Directory	UserManagement	Add user	Failure	Microsoft.Online.Workflows.OBJ...	Garett@cl4udacity1075.onmicrosoft...
1/3/2023, 4:02:19 PM	Core Directory	UserManagement	Add user	Failure	Microsoft.Online.Workflows.OBJ...	Karl@cl4udacity1075.onmicrosoft...
1/3/2023, 4:02:19 PM	Core Directory	UserManagement	Add user	Failure	Microsoft.Online.Workflows.OBJ...	Chris@cl4udacity1075.onmicrosoft...

- Audit Log 1: Add User

[Home](#) >

Audit Logs ...

Download	Refresh	Columns	Got feedback?
1/3/2023, 4:21:39 PM	B2C	Authorization	Get B2C directory resources in a ... Su
1/3/2023, 4:21:15 PM	B2C	ResourceManagement	Get B2C directory resources in a ... Su
1/3/2023, 4:21:15 PM	B2C	ResourceManagement	Get Guest Usages resources in a ... Su
1/3/2023, 4:21:15 PM	B2C	Authorization	Get B2C directory resources in a ... Su
1/3/2023, 4:21:15 PM	B2C	Authorization	Get Guest Usages resources in a ... Su
1/3/2023, 4:07:34 PM	B2C	ResourceManagement	Get Guest Usages resources in a ... Su
1/3/2023, 4:07:34 PM	B2C	Authorization	Get Guest Usages resources in a ... Su
1/3/2023, 4:07:33 PM	B2C	ResourceManagement	Get B2C directory resources in a ... Su
1/3/2023, 4:07:33 PM	B2C	Authorization	Get B2C directory resources in a ... Su
1/3/2023, 4:05:45 PM	B2C	ResourceManagement	Get Guest Usages resources in a ... Su
1/3/2023, 4:05:45 PM	B2C	ResourceManagement	Get B2C directory resources in a ... Su
1/3/2023, 4:05:45 PM	B2C	Authorization	Get Guest Usages resources in a ... Su
1/3/2023, 4:05:45 PM	B2C	Authorization	Get B2C directory resources in a ... Su
1/3/2023, 4:05:41 PM	B2C	ResourceManagement	Get Guest Usages resources in a ... Su
1/3/2023, 4:05:41 PM	B2C	Authorization	Get Guest Usages resources in a ... Su
1/3/2023, 4:05:41 PM	B2C	ResourceManagement	Get B2C directory resources in a ... Su
1/3/2023, 4:05:41 PM	B2C	Authorization	Get B2C directory resources in a ... Su
1/3/2023, 4:02:21 PM	Core Directory	UserManagement	Add user Fa
1/3/2023, 4:02:21 PM	Core Directory	UserManagement	Add user Fa
1/3/2023, 4:02:20 PM	Core Directory	UserManagement	Add user Fa
1/3/2023, 4:02:20 PM	Core Directory	UserManagement	Add user Fa
1/3/2023, 4:02:20 PM	Core Directory	UserManagement	Add user Fa
1/3/2023, 4:02:19 PM	Core Directory	UserManagement	Add user Fa
1/3/2023, 4:02:19 PM	Core Directory	UserManagement	Add user Fa
1/3/2023, 4:02:19 PM	Core Directory	UserManagement	Add user Fa

Audit Log Details

Activity	Target(s)	Modified Properties
Activity		
Date	1/3/2023, 4:02 PM	
Activity Type	Add user	
Correlation ID	4365043b-a2ea-423c-9233-8fab2474219	
Category	UserManagement	
Status	failure	
Status reason	Microsoft.Online.Workflows.ObjectAlreadyExistsException	
Initiated by (actor)		
Type	User	
Display Name		
Object ID	3dd42e03-5778-4f7d-82b2-0c609087a755	
IP address	20.127.52.190	
User Principal Name	odl_user_221142@cl4udacity1075.onmicrosoft.com	
Additional Details		
User-Agent	Swagger-Codegen/1.4.0.0/csharp	

Activity	Target(s)	<u>Modified Properties</u>	
Target	Property Name	Old Value	New Value
Michael@...	AccountEnabled	[]	[true]
Michael@...	City	[]	["Detroit"]
Michael@...	Department	[]	["IT"]
Michael@...	DisplayName	[]	["Michael"]
Michael@...	JobTitle	[]	["Support Desk Admin"]
Michael@...	MailNickname	[]	["Michael"]
Michael@...	StsRefreshToke...	[]	["2023-01-03T09:02:21Z"]
Michael@...	UserPrincipalN...	[]	["Michael@cl4udacity1075.onmicrosoft.com"]
Michael@...	UserType	[]	["Member"]
Michael@...	Included Updat...		"AccountEnabled, City, Department, DisplayName, JobTitle, MailNickname, StsRefreshTokensValidFrom, UserPrincipalName, UserType"
Michael@...	MethodExecuti...		"Microsoft.Online.Workflows.ObjectAlreadyExistsException"

⇒ A new user is added to the AAD, we can see the details of the action including datetime, IP address, status of the action,... The logs also shows the details of the event, in this case is the details of the user

- Audit Log 2: Add Member to Role

Home >

Audit Logs ...

Download Refresh Columns Got feedback?

12/30/2022, 12:01:15 AM	Core Directory	UserManagement	Delete user	Su	Activity	Target(s)
12/30/2022, 12:01:14 AM	Core Directory	UserManagement	Delete user	Su	Date	12/29/2022, 11:22 PM
12/30/2022, 12:01:14 AM	Core Directory	UserManagement	Delete user	Su	Activity Type	Add member to role
12/30/2022, 12:01:13 AM	Core Directory	UserManagement	Delete user	Su	Correlation ID	ea0feb27-7704-4ca3-b1c9-c6fe96450405
12/30/2022, 12:01:07 AM	Core Directory	UserManagement	Delete user	Su	Category	RoleManagement
12/29/2022, 11:29:36 PM	Core Directory	UserManagement	Add user	Su	Status	success
12/29/2022, 11:29:35 PM	Core Directory	UserManagement	Add user	Su	Status reason	
12/29/2022, 11:29:33 PM	Core Directory	UserManagement	Add user	Su	User Agent	
12/29/2022, 11:29:32 PM	Core Directory	UserManagement	Add user	Su	Initiated by (actor)	
12/29/2022, 11:29:31 PM	Core Directory	UserManagement	Add user	Su	Type	User
12/29/2022, 11:29:30 PM	Core Directory	UserManagement	Add user	Su	Display Name	
12/29/2022, 11:29:29 PM	Core Directory	UserManagement	Add user	Su	Object ID	00000000-0000-0000-000000000000
12/29/2022, 11:29:27 PM	Core Directory	UserManagement	Add user	Su	IP address	20.190.151.161
12/29/2022, 11:29:26 PM	Core Directory	UserManagement	Add user	Su	User Principal Name	marketplace@spektrsystems.com
12/29/2022, 11:29:25 PM	Core Directory	UserManagement	Add user	Su		
12/29/2022, 11:29:23 PM	Core Directory	UserManagement	Add user	Su		
12/29/2022, 11:29:23 PM	Core Directory	UserManagement	Add user	Su		
12/29/2022, 11:29:21 PM	Core Directory	UserManagement	Add user	Su		
12/29/2022, 11:29:20 PM	Core Directory	UserManagement	Add user	Su		
12/29/2022, 11:29:19 PM	Core Directory	UserManagement	Add user	Su		
12/29/2022, 11:29:19 PM	Core Directory	UserManagement	Add user	Su		
12/29/2022, 11:29:19 PM	Core Directory	UserManagement	Add user	Su		
12/29/2022, 11:22:44 PM	Core Directory	RoleManagement	Add member to role	Su		
12/29/2022, 11:21:37 PM	Core Directory	UserManagement	Add user	Su		

Target	Property Name	Old Value	New Value
odl_user_2...	Role.ObjectID		"0e599a48-f786-4c28-baad-20968d5427aa"
odl_user_2...	Role.DisplayNa...		"Global Administrator"
odl_user_2...	Role.TemplatedId		"62e90394-69f5-4237-9190-012177145e10"
odl_user_2...	Role.WellKnow...		"TenantAdmins"

⇒ Beside the general information, this log shows us there are 2 roles (Global Admin, Tenant Admin) assigned to user odl_user_220700

- Audit Log 2: Add Member to Role

Home >

Audit Logs ...

Download Refresh Columns Got feedback?

12/30/2022, 7:01:42 AM	Core Directory	UserManagement	Hard Delete user	Su	Activity	Target(s)
12/30/2022, 7:01:41 AM	Core Directory	UserManagement	Hard Delete user	Su	Date	Modified Properties
12/30/2022, 7:01:41 AM	Core Directory	UserManagement	Hard Delete user	Su	Activity Type	Hard Delete user
12/30/2022, 7:01:41 AM	Core Directory	UserManagement	Hard Delete user	Su	Correlation ID	d8c750a0-896f-44de-8860-08064e1dcf44
12/30/2022, 7:01:40 AM	Core Directory	UserManagement	Hard Delete user	Su	Category	UserManagement
12/30/2022, 7:01:40 AM	Core Directory	UserManagement	Hard Delete user	Su	Status	success
12/30/2022, 7:01:39 AM	Core Directory	UserManagement	Hard Delete user	Su	Status reason	
12/30/2022, 7:01:39 AM	Core Directory	UserManagement	Hard Delete user	Su	User Agent	
12/30/2022, 7:01:38 AM	Core Directory	UserManagement	Hard Delete user	Su	Initiated by (actor)	
12/30/2022, 7:01:38 AM	Core Directory	UserManagement	Hard Delete user	Su	Type	Application
12/30/2022, 7:01:38 AM	Core Directory	UserManagement	Hard Delete user	Su	Display Name	https://cl4udacity1075.onmicrosoft.com/cloudlabs.ai/
12/30/2022, 12:01:22 AM	Core Directory	UserManagement	Delete user	Su	App ID	
12/30/2022, 12:01:21 AM	Core Directory	UserManagement	Delete user	Fa	Service principal ID	854e7193-1af5-4ff8-b21f-4c2fc1999959
12/30/2022, 12:01:21 AM	Core Directory	UserManagement	Delete user	Su	Service principal name	
12/30/2022, 12:01:20 AM	Core Directory	UserManagement	Delete user	Su		

Target

Type	User
Id	67f5367e-d50f-43fa-827c-2bb38377d177
Display Name	
User Principal Name	67f5367ed50f43fa827c2bb38377d177Chris@cl4udacity1075.onmicrc

⇒ This log shows us the the user with ID 67f5367e-d50f-43fa-827c-2bb38377d177 is hard deleted. The log contains additional info like time, action type, status of the action, category, etc.

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

sql-devdata-221096 | Auditing

SQL server

<

 Save  Discard  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
-  Import/Export history

Security

-  Networking
-  Microsoft Defender for Cloud
-  Transparent data encryption

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 1074

Log Analytics *

p3-log-analytics(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 

sql-prodata-221096 | Auditing ...

SQL server

Search 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 1074

Log Analytics *

p3-log-analytics(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

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

Recommendations

Monitoring

Logs

** Audit logs for SQL

Identify 3 items from the Audit log and explain what each log shows.

The screenshot shows the Azure Log Analytics workspace interface. A query is running in a new query window titled 'New Query 1*'. The query is:

```

1 AzureDiagnostics
2 | where Category == '$SQLSecurityAuditEvents'
3 | and true == true
4 | and true == true
5 | and true == true
6 | and true == true

```

The results table has the following columns:

- ip....
- audit_schema_version_d
- event_time_t [UTC]
- sequence_number_d
- action_id_s
- action_name_s
- succeeded_s
- is_column_permission

The results table displays 23 rows of log data, each with a timestamp between 1/3/2023 and 1/3/2023, and various action names like DBAS, DBAF, BCM, and AUSC.

Above is the screenshot of the created log analytics workspace (configurated for 2 sql servers). There're some logs after I tried to login and executed some queries.

The logs with action name “DATABASE_AUTHENTICATION” shows the history of attempts to login to the server with some other useful info: instance name, time, status, server principal name, etc.

The logs with action name “BATCH_COMPLETED” shows the history of the executed queries in the database, we can find the full statement, object name, database name, etc. in the logs

database_name_s	object_name_s	statement_s
master	master	
DB-development-221142	DB-development-221142	
DB-development-221142	DB-development-221142	
master	master	SELECT ISNULL(SESSIONPROPERTY ('ANSI_NULLS'), 0), ISNULL(SESSIONPROPERTY ('QUOTED_IDENTIFIER'), 1)
DB-development-221142	DB-development-221142	SET NOEXEC OFF SET ROWCOUNT 0 SET TEXTSIZE 2147483647 SET NOCOUNT OFF SET CONCAT_NULL_YIELDS_NULL ON SET ARITHABORT ON SET LOCK_TIMEOUT 5000
DB-development-221142	DB-development-221142	CREATE TABLE Persons (PersonID int, LastName varchar(255), FirstName varchar(255), Address varchar(255), City varchar(255));
master	master	SELECT CONVERT(NVARCHAR(36), CONTEXT_INFO())
master	master	SELECT ISNULL(SESSIONPROPERTY ('ANSI_NULLS'), 0), ISNULL(SESSIONPROPERTY ('QUOTED_IDENTIFIER'), 1)
master	master	SELECT CONVERT(NVARCHAR(36), CONTEXT_INFO())
master	master	set LOCK_TIMEOUT 5000
master	master	SET ANSI_NULLS, ANSI_PADDING, ANSI_WARNINGS, ARITHABORT, CONCAT_NULL_YIELDS_NULL, QUOTED_IDENTIFIER ON; SET NUMERIC_ROUNDABORT OFF;
master	master	SELECT ISNULL(SESSIONPROPERTY ('ANSI_NULLS'), 0), ISNULL(SESSIONPROPERTY ('QUOTED_IDENTIFIER'), 1)
master	master	SELECT name FROM sys.databases WHERE state_desc='ONLINE' ORDER BY name ASC

The AUDIT_SESSION_CHANGE logs are the log of log audit service in the server.

2. Proof of Sentinel connectors (2+)

Home > Microsoft Sentinel

Microsoft Sentinel | Data connectors ...

Selected workspace: 'p3-log-analytics'

Search Refresh Guides & Feedback

General

- Overview
- Logs
- News & guides
- Search

Threat management

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

Content management

125 Connectors 2 Connected More content at Content hub

azure active

Providers : All Data Types : All Status : All

Status	Connector name ↑
	Azure Active Directory Microsoft
	Azure Active Directory Identity Protection Microsoft

Compliance

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

Home > Microsoft Defender for Cloud | Overview >

Environment settings ... X

+ Add environment | Refresh | Guides & Feedback

Governance rules
Assign owners and set expected timeframes for recommendations

Cloud provider	Count	Actions
Azure subscriptions	1	
AWS accounts	0	
GCP projects	0	
GitHub connectors	0	
AzureDevOps connectors	0	

Environments == All Standards == All Coverage == All

Name	Total resources	Defender coverage	Standards
Udacity 1074	4	12/12 plans 2/2 plans	...
p3-log-analytics			...