Secure the Juice

Identity and Access Management

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

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

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

Home > Udacity 1069 > Groups > Executive

Executive | Members
Group

Manage

- Overview
- Diagnose and solve problems
- Properties
- Members
- Owners
- Roles and administrators

+ Add members ✕ Remove ⟳ Refresh ▯ Bulk operations ∨ ☷ Columns

Direct members | All members

🔍 Search by name   ⊹ Add filters

	Name	↑↓	Type	Email	User type
☐	CH Chris		User		Member
☐	KA Karl		User		Member

Home > Udacity 1069 > Groups > IT

IT | Members
Group

Manage

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

✕

+ Add members ✕ Remove ⟳ Refresh ▯ Bulk operations ∨ ☷ Columns ⋯

Direct members | All members

🔍 Search by name   ⊹ Add filters

	Name	↑↓	Type	Email	User type
☐	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 > Udacity 1069 > Groups > HR

HR | Members
Group

Manage

- Overview
- Diagnose and solve problems
- Properties
- Members
- Owners

+ Add members ✕ Remove ⟳ Refresh ▯ Bulk operations ☷ Columns Got feedback?

Direct members | All members

🔍 Search by name   ⊹ Add filters

	Name	↑↓	Type	Email	User type
☐	LO Lora		User		Member

HR | Assigned roles
Group

+ Add assignments   ↻ Refresh | 🗫 Got feedback?

Eligible assignments   Active assignments   Expired assignments

🔍 Search by role

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

Left navigation:
- ⓘ Overview
- ✕ Diagnose and solve problems
- **Manage**
- Ⅲ Properties
- 👥 Members
- 👥 Owners
- 👥 Roles and administrators
- ▣ Administrative units
- ⊕ Group memberships
- 👥 Assigned roles
- ▦ Applications

Support Desk | Members
Group

+ Add members   ✕ Remove   ↻ Refresh | 📄 Bulk operations ⌄ | ≡≡ Columns   🗫 Got feedback?

Direct members   All members

🔍 Search by name   ⊕ Add filters

Name		Type	Email	User type
☐ 🟣WI Winifred		User		Member

Left navigation:
- ⓘ Overview
- ✕ Diagnose and solve problems
- **Manage**
- Ⅲ Properties
- 👥 Members
- 👥 Owners
- 👥 Roles and administrators

Support Desk | Assigned roles
Group

+ Add assignments   ↻ Refresh | 🗫 Got feedback?

Eligible assignments   Active assignments   Expired assignments

🔍 Search by role

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

Left navigation:
- ⓘ Overview
- ✕ Diagnose and solve problems
- **Manage**
- Ⅲ Properties
- 👥 Members
- 👥 Owners
- 👥 Roles and administrators
- ▣ Administrative units
- ⊕ Group memberships
- 👥 Assigned roles

Karl | Assigned roles
User

🔍 Search (Ctrl+/)

+ Add assignments   ↻ Refresh | 🗫 Got feedback?

Eligible assignments   **Active assignments**   Expired assignments

🔍 Search by role

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

Left navigation:
- 👥 Overview
- 🗒 Audit logs
- ⊙ Sign-in logs
- ✎ Diagnose and solve problems
- **Manage**
- ▣ Custom security attributes (preview)
- 👥 Assigned roles
- ▣ Administrative units
- 👥 Groups

Karl | Assigned roles
User

🔍 Search (Ctrl+/)

+ Add assignments   ↻ Refresh | 🗫 Got feedback?

Eligible assignments   **Active assignments**   Expired assignments

🔍 Search by role

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

Left navigation:
- 👥 Overview
- 🗒 Audit logs
- ⊙ Sign-in logs
- ✎ Diagnose and solve problems
- **Manage**
- ▣ Custom security attributes (preview)
- 👥 Assigned roles
- ▣ Administrative units

Seth | Assigned roles
User

⊕ Add assignments   ↻ Refresh | ▱ Got feedback?

Eligible assignments   Active assignments   Expired assignments

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

Overview
Audit logs
Sign-in logs
Diagnose and solve problems

Manage
Custom security attributes (preview)
Assigned roles

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

rg-devdata | Access control (IAM)
Resource group

⊕ Add   ↓ Download role assignments   ≣ Edit columns   ↻ Refresh   ✕ Remove   ▱ Got feedback?

Check access   Role assignments   Roles   Deny assignments   Classic administrators

Number of role assignments for this subscription ⓘ

23   2000

| Type : All | Role : All | Scope : All scopes | Group by : Role |

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

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

Added Role assignments
2 Role assignments were add
devdata.

rg-data | Access control (IAM)
Resource group

⊕ Add   ↓ Download role assignments   ≣ Edit columns   ↻ Refresh   ✕ Remove   ▱ Got feedback?

Check access   Role assignments   Roles   Deny assignments   Classic administrators

Number of role assignments for this subscription ⓘ

23   2000

| Type : All | Role : All | Scope : All scopes | Group by : Role |

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

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

Added Role assignment
Srinadh was added as Owner

sql-devdata-202442 | Access control (IAM)
SQL server

Search (Ctrl+/)

+ Add   ↓ Download role assignments   ≣ Edit columns   ↻ Refresh   ✕ Remove   ⊠ Got 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

Check access   Role assignments   Roles   Deny assignments   Classic administrators

Number of role assignments for this subscription ⓘ

29   2000

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

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

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

sql-proddata-202442 | Access control (IAM)
SQL server

Search (Ctrl+/)

+ Add   ↓ Download role assignments   ≣ Edit columns   ↻ Refresh   ✕ Remove   ⊠ Got 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

Check access   Role assignments   Roles   Deny assignments   Classic administrators

Number of role assignments for this subscription ⓘ

29   2000

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

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

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

rg-operations | Access control (IAM)
Resource group

Added Role assignment
Andrew was added as Contributor fo

Search (Ctrl+/)

+ 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)

Check access   Role assignments   Roles   Deny assignments   Classic administrators

Number of role assignments for this subscription ⓘ

24   2000

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

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

Name	Type	Role	Scope	Condition
CloudDevOps Custom RBAC I1359 S1				
Identity not found. ⓘ Unable to find identity.	Unknown	CloudDevOps Custom RBAC I1359 S1 ⓘ	Subscription (Inherited)	None
Identity not found. ⓘ Unable to find identity.	Unknown	CloudDevOps Custom RBAC I1359 S1 ⓘ	Subscription (Inherited)	None
Contributor				
Andrew Andrew@cl4udacity1069...	User	Contributor ⓘ	This resource	None
ODL_User 202442 odl_user_202442@cl4ud...	User	Contributor ⓘ	Subscription (Inherited)	None

---

rg-dev | Access control (IAM)
Resource group

Search (Ctrl+/)

+ 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)

Check access   Role assignments   Roles   Deny assignments   Classic administrators

Number of role assignments for this subscription ⓘ

25   2000

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

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

Name	Type	Role	Scope	Condition
CloudDevOps Custom RBAC I1359 S1				
Identity not found. ⓘ Unable to find identity.	Unknown	CloudDevOps Custom RBAC I1359 S1 ⓘ	Subscription (Inherited)	None
Identity not found. ⓘ Unable to find identity.	Unknown	CloudDevOps Custom RBAC I1359 S1 ⓘ	Subscription (Inherited)	None
Contributor				
Neelima Neelima@cl4udacity106...	User	Contributor ⓘ	This resource	None
ODL_User 202442 odl_user202442@cl4ud...	User	Contributor ⓘ	Subscription (Inherited)	None

Proof of Global Administrator setting with duration, eligibility, expiration

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

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

Resubmitted –

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

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

Resubmitted --

multi-factor authentication
users   service settings

app passwords (learn more)

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

trusted ips (learn more)

☑ Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

143.52.0.0/24

verification options (learn more)

Methods available to users:
☐ Call to phone
☐ Text message to phone
☑ Notification through mobile app
☑ Verification code from mobile app or hardware token

remember multi-factor authentication on trusted device (learn more)

☑ Allow users to remember multi-factor authentication on devices they trust (between one to 365 days)
Number of days users can trust devices for 14
NOTE: For the optimal user experience, we recommend using Conditional Access sign-in frequency to extend session lifetimes on trusted devices, locations, or low-risk sessions as an alternative to 'Remember MFA on a trusted device' settings. If using 'Remember MFA on a trusted device,' be sure to extend the duration to 90 or more days. Learn more about reauthentication prompts.

save

Network Security

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

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

VM-WS19HRL-App
Virtual machine

Connect ∨ ▷ Start ⟳ Restart ☐ Stop ⊠ Capture 🗑 Delete ⟳ Refresh 📱 Open in mobile CLI / PS Feedback

Search (Ctrl+/) «

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

Settings
- Networking

∧ 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 1069	Virtual network/subnet	: HRLegal/default
Subscription ID	: 0d904d18-8db0-4da9-ac30-cbd31a3a16e5	DNS name	: -
Tags (edit)	: Click here to add tags		

VM-WS19OpApp
Virtual machine

Connect ∨ ▷ Start ⟳ Restart ☐ Stop ⊠ Capture 🗑 Delete ⟳ Refresh 📱 Open in mobile CLI / PS Feedback

Search (Ctrl+/) «

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

Settings
- Networking

∧ 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 1069	Virtual network/subnet	: Vnet-operations/default
Subscription ID	: 0d904d18-8db0-4da9-ac30-cbd31a3a16e5	DNS name	: -
Tags (edit)	: Click here to add tags		

VM-WS19HRL-Web
Virtual machine

Connect ∨ ▷ Start ⟳ Restart ☐ Stop ⊠ Capture 🗑 Delete ⟳ Refresh 📱 Open in mobile CLI / PS Feedback

Search (Ctrl+/) «

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

Settings
- Networking

∧ 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 1069	Virtual network/subnet	: HRLegal/default
Subscription ID	: 0d904d18-8db0-4da9-ac30-cbd31a3a16e5	DNS name	: -
Tags (edit)	: Click here to add tags		

2. Reduce attack footprint by removing public IP addresses.

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

Data and Encryption

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

   Screenshots should show the disk encryption type for each VM.

des-disk | Resources ☆ ⋯
Disk Encryption Set

🔍 Search (Ctrl+/)   «

Filter by name...   All types ⌄

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

Overview
Activity log
Access control (IAM)
Tags

Settings
Resources
Key
Properties
Locks

Automation
Tasks (preview)
Export template

Support + troubleshooting
New Support Request

---

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

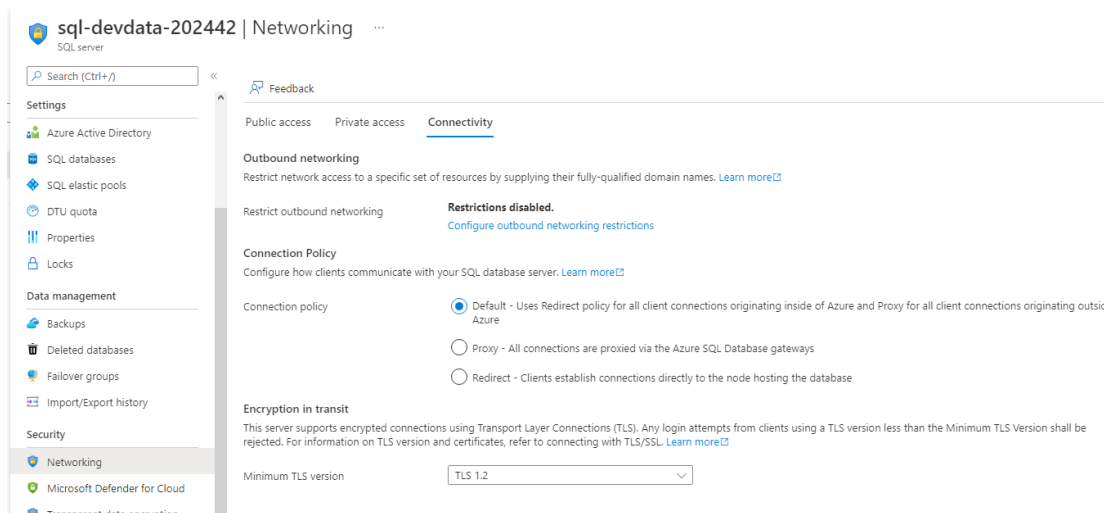Encryption type
Encryption at-rest with a customer-managed key   ⌄

Disk encryption set ⓘ
des-disk   ⌄

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   ⌄

🔑 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

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

Encryption type

Encryption at-rest with a customer-managed key ⌄

Disk encryption set ⓘ

des-disk ⌄

🔑 VM-WS19HRL-App-osdisk | Encryption ☆ ⋯
Disk

🔍 Search (Ctrl+/) «

💾 Save   ✕ Discard   ↻ Refresh

- 🟢 Overview
- 📃 Activity log
- 🔑 Access control (IAM)
- 🏷 Tags

Settings

- 🧳 Configuration
- 🟢 Size + performance
- 🔑 Encryption

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

Encryption type

Encryption at-rest with a customer-managed key ⌄

Disk encryption set ⓘ

des-disk ⌄

🔑 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 ⌄

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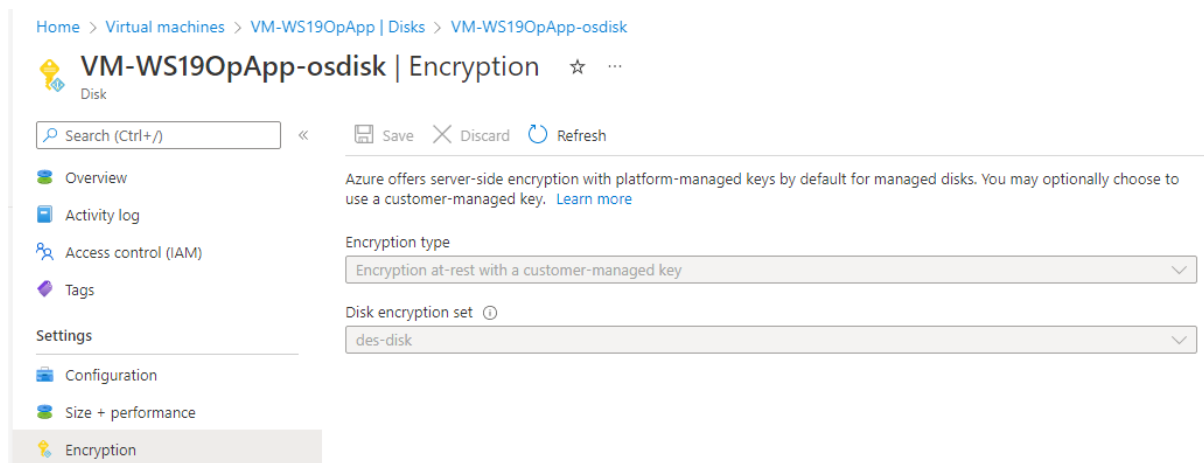
2. **Secure traffic to SQL servers and databases by limiting public network access, enforcing TLS minimum requirements, and setting allowed IPs or network requirements**

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

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 | ⌄ |

Screenshot 1: sql-proddata-202442 | Networking

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	0d904d18-8d...	Ready	...

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

---

Screenshot 2: sql-devdata-202442 | Networking

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

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

Screenshot 3: sql-proddata-202442 | Networking

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 in to connecting with TLS/SSL. Learn more

Minimum TLS version
TLS 1.2

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

Screenshot that shows Azure Defender for SQL is enabled.

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

Show screenshot of Azure AD authentication for SQL enabled
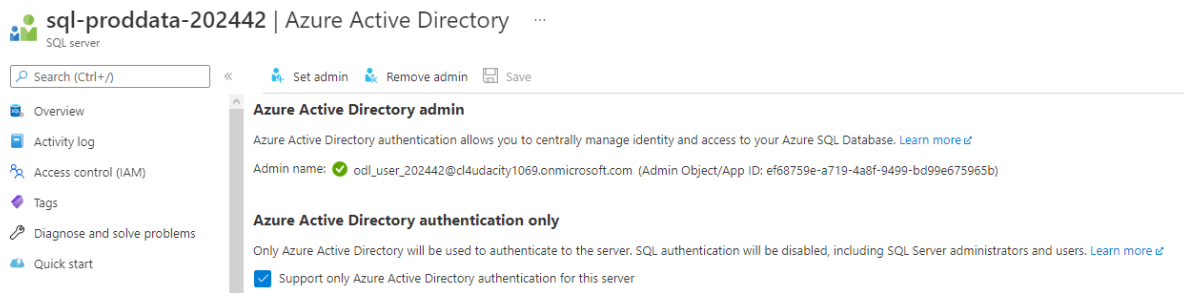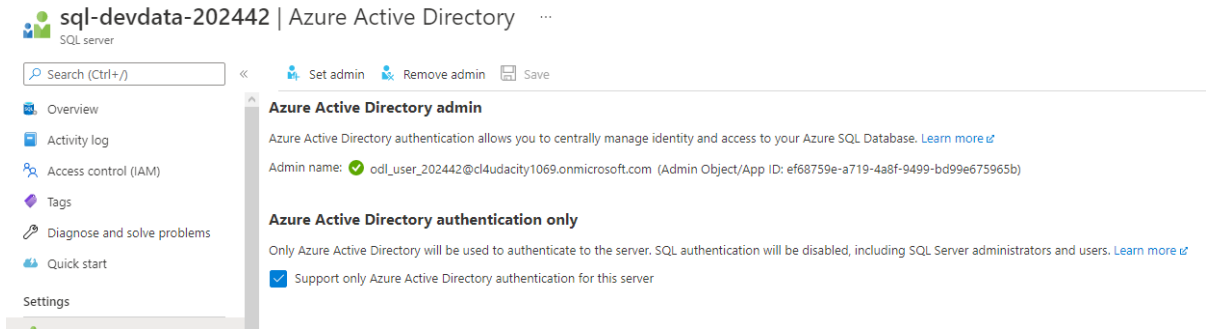
Protection

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

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

VM-WS19HRL-Web/IaaSAntimalware ☆ ···
microsoft.compute/virtualmachines/extensions

🔍 Search (Ctrl+/) «   ↻ Refresh   🗑 Delete   ×

||| Overview

Activity log

Access control (IAM)

Settings

🔒 Locks

Automation

Tasks (preview)

Export template

Support + troubleshooting

New Support Request

⌃ Essentials   JSON View

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

||| Properties ||| Instance view

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

VM-WS19OpApp/IaaSAntimalware ☆ ···
microsoft.compute/virtualmachines/extensions

🔍 Search (Ctrl+/) «   ↻ Refresh   🗑 Delete   ×

||| Overview

Activity log

Access control (IAM)

Settings

🔒 Locks

Automation

Tasks (preview)

Export template

Support + troubleshooting

New Support Request

⌃ Essentials   JSON View

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

||| Properties ||| Instance view

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

VM-WS16DevWeb/IaaSAntimalware ☆ ···
microsoft.compute/virtualmachines/extensions

🔍 Search (Ctrl+/) «   ↻ Refresh   🗑 Delete   ×

||| Overview

Activity log

Access control (IAM)

Settings

🔒 Locks

Automation

Tasks (preview)

Export template

Support + troubleshooting

New Support Request

⌃ Essentials   JSON View

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

||| Properties ||| Instance view

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

2. Track and remediate vulnerabilities against Azure Security Center (ASC) Default policy

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

User accounts requiring MFA

Enable MFA for the following user accounts:

Ramesh Bamidipati

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

==Recommendation in Text with the justification to remediate vulnerabilities==

1. =="Enable MFA" currently has a score of 0/10. So, it has the biggest impact on security if we fix it. MFA is not set up for user account Ramesh Bamidipati, so we should setup for him==

2. ==The other 2 top remediations are "Apply system updates" and "Remediate vulnerabilities". Both of them have a score of 0/6. So, that can be done also.==

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

4. ==And we should install vulnerability assessment tools on our VMs.==

   Resubmitted –

Monitoring

1. **Configure Azure Sentinel Connectors.**

   Provide screenshot of Azure Sentinel Data Connectors Page.

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

Home > sql-proddata-202442

sql-proddata-202442 | Auditing
SQL server

🔍 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. Monitor and Protect SQL databases by configuring auditing.

Provide screenshot showing SQL Auditing is enabled with Log Analytics Workspace

Compliance

1. **Enable monitoring of established industry and regulatory standards**

   Screenshot proof of added NIST SP 800-53 rev4 policy