

Azure Project 2

Course-End Project Automating Workloads Using ARM Template

The Rand Enterprises Corporation wants to test the ARM template to bring infrastructure as code into practice. Create an entire networking architecture using the ARM template for an operations team. Create storage account and virtual machine with an internal network of Azure to deliver Image-based content. The communication from the application in the VM to the Azure Storage account must take place via the internal network of Azure.

The expectation of the operation team is to create a reusable template that can be used for automation. So, rather than deploying resources in Azure independently, they should leverage Azure ARM templates to deploy and provision all resources in template format. As a security measure, you need to ensure that the operation team can only deploy the resources mentioned in the requirement below and adhere to principle of least privilege.

Expected Deliverables:

- Define access using RBAC for operation team
- Define the network
- Extend that with Compute & Storage
- Create the Storage account container for Images & configure service endpoints

Step 1: Define access using RBAC for operation team

Role-Based Access Control provides fine-grained access management of resources in Azure. This is built in Azure Resource Manager that segregates duties within a team and grants access for what the users need.

Create a role-based access control to define various roles for the operation team. In this case, we will do a simple example with a single resource group with two users to add for developer and security analysis.

1.1 Resource Group

In the Create a resource group page under Basics tab, create a Resource group named “RandEnt” and select the appropriate Region (in this case, (US) East US).

The screenshot shows the Microsoft Azure Resource groups page. At the top, there's a search bar and a Copilot button. Below the header, it says "Home > Resource groups". A message indicates "Simplilearn HOL 29 (simplilearnhol29.onmicrosoft.com)". There are buttons for "+ Create", "Manage view", "Refresh", "Export to CSV", and "Group by none". A note says "Create a new resource group. Version of Browse experience. Some features may be missing. Click here to access the old experience." Below this, there are filter options: "Filter for any field...", "Subscription equals all", "Location equals all", and "+ Add filter". A list of resource groups is shown with checkboxes:

- Name **Cloudlabs-ACI-1523814-VM-1523814-cs513e3f**
- NetworkWatcherRG
- ODL-azure-1523814

The screenshot shows the "Create a resource group" wizard. The title is "Create a resource group". Below it, there are tabs: "Basics" (which is selected), "Tags", and "Review + create". A note explains what a Resource group is: "A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. Learn more".

Project details

Subscription *

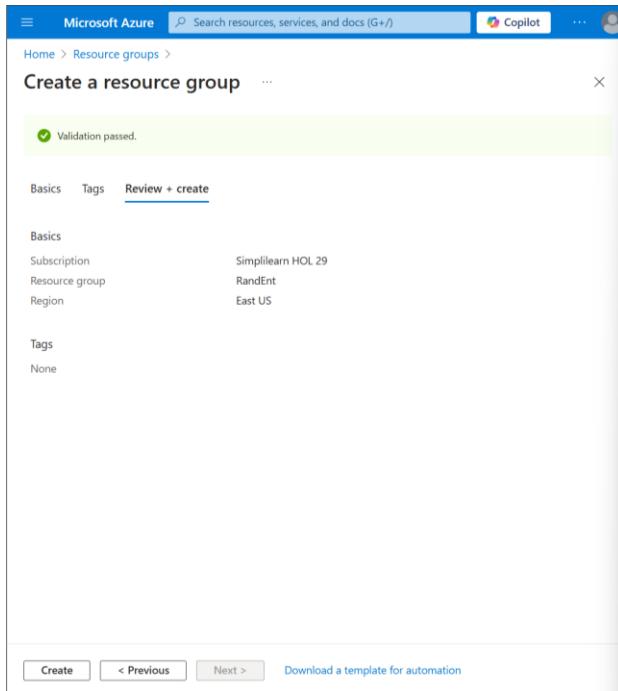
Resource group *

Resource details

Region *

At the bottom, there are buttons: "Review + create", "< Previous", and "Next : Tags >".

Then, click on Review + create.



Click create.

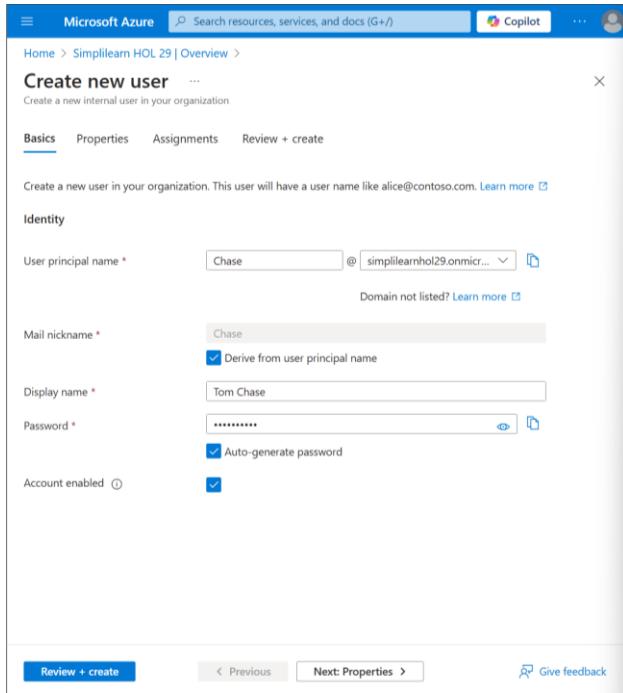
1.2 Add Users

For User, we will create two users with one being the Developer and the second being the Security Analyst.

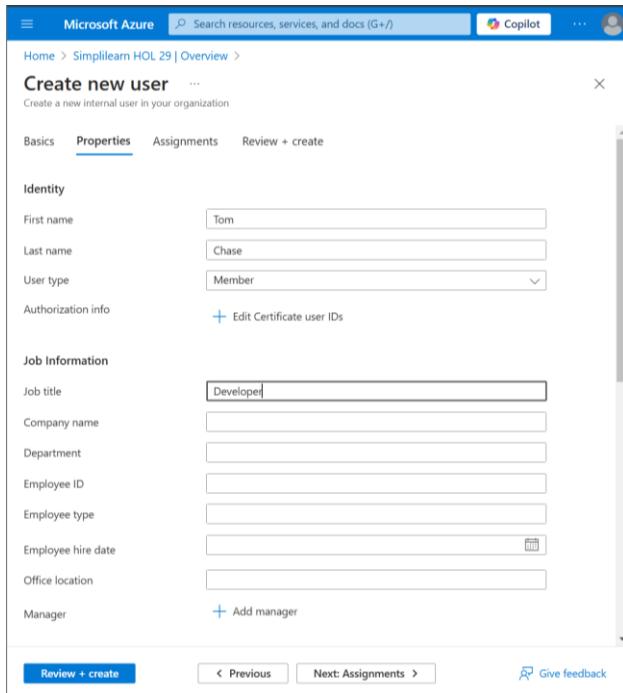
Go to Microsoft Entra ID. In the Overview page, click on Add, select User, and from the drop-out right menu click on Create new user.

A screenshot of the Microsoft Entra ID Overview page for the tenant 'Simplilearn HOL 29'. The left sidebar has sections for Overview, Preview features, Diagnose and solve problems, Manage, Monitoring, and Troubleshooting + Support. The main area has a 'User' dropdown menu open, showing options like 'Create new user', 'Manage tenants', 'What's new', 'Preview features', and 'Got feedback?'. The 'Create new user' option is highlighted. Below the menu, there's a 'Basic information' section with fields for Name (Simplilearn HOL 29), Tenant ID (e2edce3b-5259-4679-9335-940f37afa5e4), Primary domain (simplilearnhol29.onmicrosoft.com), and License (Microsoft Entra ID Free). To the right, there are summary counts: Users (3), Groups (0), Applications (1), and Devices (7).

In the Create new user page, under the Basics tab enter the information of the user. In this case, we will call them Tom Chase.



Click on Properties tab and enter Job title as Developer. Then, click on Review + create



In the Review + create tab, copy the auto-generated password provided in the Password box. This password is given to the user to sign in for the first time. Once the details are entered, click on Create.

The screenshot shows the 'Create new user' wizard in the Microsoft Azure portal. The current step is 'Review + create'. The 'Basics' tab is selected, showing the following user information:

User principal name	Chase@simplilearnhol29.onmicrosoft.com
Display name	Tom Chase
Mail nickname	Chase
Password	*****
Account enabled	Yes

Below the basics section, there are tabs for 'Properties' and 'Assignments'. Under 'Properties', the following details are listed:

First name	Tom
Last name	Chase
User type	Member
Job title	Developer

Under 'Assignments', there are sections for 'Administrative units', 'Groups', and 'Roles', each with a dropdown menu.

At the bottom of the screen, there are buttons for 'Create' (highlighted in blue), '< Previous', 'Next >', and 'Give feedback'.

Repeat the same process for a second user, we will call them Scott Dale.

This one will be Security Analyst.

The screenshot shows the 'Create new user' wizard in the Microsoft Azure portal. The current step is 'Review + create'. The 'Properties' tab is selected, showing the following user information:

First name	Scott
Last name	Dale
User type	Member

Below the properties section, there are tabs for 'Assignments' and 'Review + create'. Under 'Assignments', there are sections for 'Authorization info', 'Job Information', and 'Manager', each with input fields and dropdown menus.

At the bottom of the screen, there are buttons for 'Review + create' (highlighted in blue), '< Previous', 'Next: Properties >', and 'Give feedback'.

User principal name: Dale@simplilearnhol29.onmicrosoft.com

Display name: Scott Dale

Mail nickname: Dale

Password: *****

Account enabled: Yes

First name: Scott

Last name: Dale

User type: Member

Job title: Security Analyst

Two users are created. Check by clicking on Users, under Mange.

Display name	User principal name	User type	On-premises sync	Identities	Company name	Creation type
AM	admin@simplilearnhol29...	Member	No	simplilearnhol29.onmicrosoft.com		
ODL	odl_user_1523814@simpli...	Member	No	simplilearnhol29.onmicrosoft.com		
SJ	Sanjeeb@simplilearnhol2...	Member	No	simplilearnhol29.onmicrosoft.com		
SD	Dale@simplilearnhol29.o...	Member	No	simplilearnhol29.onmicrosoft.com		
TC	Chase@simplilearnhol29...	Member	No	simplilearnhol29.onmicrosoft.com		

Your users on under User in Microsoft Entra ID.

2.3 Access Control (IAM)

Grant access for the developer and security analyst through Access Control (IAM) in your resource group.

Go to Resources Group and Select “RandEnt”.

Click on Access Control (IAM) in Settings. Then click on +Add and select Add role assignment.

In Add role assignment pane, click on the Privileged administrator roles and select Contributor from the list.

Name	Description	Type	Category	Details
Owner	Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.	BuiltinRole	General	View
Contributor	Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, manage assignments i...	BuiltinRole	General	View
Access Review Operator Service Role	Lets you grant Access Review System app permissions to discover and revoke access as needed by the access review pr...	BuiltinRole	None	View
Role Based Access Control Administrator	Manage access to Azure resources by assigning roles using Azure RBAC. This role does not allow you to manage access...	BuiltinRole	None	View
Spektra Custom RBAC Role I20529 S1	Spektra Custom Role.	CustomRole	None	View
Spektra Custom RBAC Role I37619 S1	Spektra Custom Role.	CustomRole	None	View
Spektra Custom RBAC Role I37620 S1	Spektra Custom Role.	CustomRole	None	View
User Access Administrator	Lets you manage user access to Azure resources.	BuiltinRole	General	View

Click on Next.

The screenshot shows the Microsoft Azure 'Add role assignment' interface. In the main pane, the 'Members' tab is selected, showing a 'Contributor' role assigned to 'User, group, or service principal'. A search bar at the top right of the main pane says 'Search resources, services, and docs (G+)'. Below the search bar are icons for Copilot, AI, and others. The top right corner shows the user's email: odl_user_1523814@sim... and the group: SIMPLETEARN HOL 29 (SIMPLE...). The 'Select members' modal is open on the right, displaying a list of users: Amit Malik (admin@simplilearnhol29.onmicrosoft.com), ODL_User_1523814 (odl_user_1523814@simplilearnhol29.onmicrosoft.com), Sanjeeb (Sanjeeb@simplilearnhol29.onmicrosoft.com), Scott Dale (Scott Dale@simplilearnhol29.onmicrosoft.com), Dale (Dale@simplilearnhol29.onmicrosoft.com), Tom Chase (Tom Chase@simplilearnhol29.onmicrosoft.com), and Chase (Chase@simplilearnhol29.onmicrosoft.com). A search bar in the modal says 'Search by name or email address'. At the bottom of the modal, there are 'Selected members:' (Tom Chase) and 'Select' and 'Close' buttons.

In the Members tab, click on +Select members. In the Select members pane, search for and select the developer user “Tom Chase” and click on Select. Then click on Review + Assign.

The screenshot shows the Microsoft Azure 'Add role assignment' interface with the 'Review + assign' tab selected. The assignment details are as follows:

Role	Contributor
Scope	/subscriptions/4bdb238c-14b9-4485-b7e9-52e890fe3321/resourceGroups/RandEnt
Members	Name: Tom Chase, Object ID: 21ee0216-339c-493f-860e-ec903c063f85, Type: User
Description	No description
Assignment type	Eligible
Permanent	No
Start date and time	11/22/2024, 2:03:13 PM
End date and time	11/22/2025, 2:03:13 PM

A note at the bottom left says: "Users with eligible and/or time-bound assignments must have a valid license. [Learn more](#)". At the bottom right, there is a 'Feedback' button.

Click on Review + Assign again.

Click on Role Assignments.

You will see your developer user under Contributor.

For the second user, go to IAM and click on “Add role assignment” again.

Add a second role assignment, under Job Functions, select Security Assessment Contributor.

Name	Description	Type	Category	Details
Azure Container Registry secure supply chain ...	Grants Microsoft Defender for Cloud access to Azure Container Registry for security assessment of container images	BuiltinRole	None	View
Defender Kubernetes Agent Operator	Grants Microsoft Defender for Cloud permissions to provision the Kubernetes defender security agent	BuiltinRole	None	View
Elastic SAN Owner	Allows for full access to all resources under Azure Elastic SAN including changing network security policies to unblock d...	BuiltinRole	None	View
Elastic SAN Volume Group Owner	Allows for full access to a volume group in Azure Elastic SAN including changing network security policies to unblock d...	BuiltinRole	None	View
HDInsight Domain Services Contributor	Can Read, Create, Modify and Delete Domain Services related operations needed for HDInsight Enterprise Security Pack...	BuiltinRole	Analytics	View
Security Admin	Security Admin Role	BuiltinRole	Security	View
Security Assessment Contributor	Lets you push assessments to Security Center	BuiltinRole	Security	View
Security Detonation Chamber Publisher	Allowed to publish and modify platforms, workflows and toolsets to Security Detonation Chamber	BuiltinRole	Security	View
Security Detonation Chamber Reader	Allowed to query submission info and files from Security Detonation Chamber	BuiltinRole	Security	View
Security Detonation Chamber Submission Man...	Allowed to create and manage submissions to Security Detonation Chamber	BuiltinRole	Security	View
Security Detonation Chamber Submitter	Allowed to create submissions to Security Detonation Chamber	BuiltinRole	Security	View
Security Manager (Legacy)	This is a legacy role. Please use Security Administrator instead	BuiltinRole	Security	View

Click Next.

Microsoft Azure

Home > Resource groups > RandEnt-Network | Access control (IAM) >

Add role assignment ...

Role **Members*** **Conditions** **Assignment type (Preview)** **Review + assign**

Selected role Security Assessment Contributor

Assign access to User, group, or service principal Managed identity

Members [+ Select members](#)

Name	Object ID	Type
No members selected		

Description

[Review + assign](#) [Previous](#) [Next](#) [Select](#) [Close](#)

For Select Members, select your use security analyst.

Microsoft Azure

Home > Resource groups > RandEnt | Access control (IAM) >

Add role assignment ...

Role **Members** **Conditions** **Assignment type** **Review + assign**

Role Security Assessment Contributor

Scope /subscriptions/4bdb238c-14b9-4485-b7e9-52e890fe3321/resourceGroups/RandEnt

Members

Name	Object ID	Type
Scott Dale	40171ddd-2945-4958-95f7-2b46bece6ddb	User

Description No description

Assignment type Eligible

Permanent No

Start date and time 11/22/2024, 2:07:53 PM

End date and time 11/22/2025, 2:07:53 PM

Users with eligible and/or time-bound assignments must have a valid license. [Learn more](#)

[Review + assign](#) [Previous](#) [Next](#) [Feedback](#)

Click on Review + Assign and click on it again.

You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.

Resource groups

RandEnt | Access control (IAM)

Name	Type	Role	Identity	Status	Notes
StorageAccountAccess	Managed identity	EventGrid Contributor	Subscription (Inherent)	Active permanent	None
ContainerServiceAccess	Managed identity	Kubernetes Agent Operator	Subscription (Inherent)	Active permanent	None
CloudPostureAccess	Managed identity	Kubernetes Agentless Operator	Subscription (Inherent)	Active permanent	None
ContainerServiceAccess	Managed identity	Kubernetes Agentless Operator	Subscription (Inherent)	Active permanent	None
Scott Dale	User	Security Assessment Contributor	This resource	Future eligible time-based	None
Unknown	Unknown	Spektra Custom RBAC Role	Subscription (Inherent)	Loading...	None
Unknown	Unknown	Spektra Custom RBAC Role	Subscription (Inherent)	Loading...	None
Unknown	Unknown	Spektra Custom RBAC Role	Subscription (Inherent)	Loading...	None
Unknown	Unknown	Spektra Custom RBAC Role	Subscription (Inherent)	Loading...	None
Unknown	Unknown	Spektra Custom RBAC Role	Subscription (Inherent)	Loading...	None
Unknown	Unknown	Spektra Custom RBAC Role	Subscription (Inherent)	Loading...	None
Unknown	Unknown	Spektra Custom RBAC Role	Subscription (Inherent)	Loading...	None
Unknown	Unknown	Spektra Custom RBAC Role	Subscription (Inherent)	Loading...	None

Under Role Assignments, you will see Scott Dale as your Security Assessment Contributor.

Your RBAC is created as appropriate roles are assigned to each group for the operation team.

Step 2: Define the network

Set up a Virtual Network to connect all resources securely for your ARM template.

2.1 Create Virtual Network

In the Azure Portal, go to Virtual networks.

Click “+ Create*” to create your Virtual Network.

Virtual networks

Name	Resource group	Location	Subscription
vnet	ODL-azure-1523814	East US 2	Simplilearn HOL 29

In “Create virtual network”:

Select your resource group “RandEnt” and create a Virtual Network name “RandEnt-VirtNet”. Under region as (US) East Us 2 (East US would be fine but we are using the second version due to policy error).

The screenshot shows the 'Create virtual network' wizard in the Microsoft Azure portal. The current step is 'Basics'. At the top, there's a search bar and a Copilot button. On the right, the user's name 'odl.user.1523814@sim...' and profile picture are visible. Below the header, the breadcrumb navigation shows 'Home > Virtual networks > Create virtual network'. The main content area has tabs for 'Basics', 'Security', 'IP addresses', 'Tags', and 'Review + create'. Under 'Basics', a note explains that VNet is the fundamental building block for private networks in Azure, enabling secure communication between VMs, the internet, and on-premises networks. It also mentions benefits like scale, availability, and isolation. A 'Learn more' link is provided. The 'Project details' section asks to select a subscription and resource group. The 'Subscription' dropdown is set to 'Simplilearn HOL 29' and the 'Resource group' dropdown is set to 'RandEnt'. A 'Create new' link is available. The 'Instance details' section asks for a 'Virtual network name' ('RandEnt-VirtNet') and a 'Region' ('(US) East US 2'). A 'Deploy to an Azure Extended Zone' link is present. At the bottom, there are 'Previous', 'Next', and 'Review + create' buttons, along with a 'Give feedback' link.

Go to IP addresses tab. Have Default address space at “10.0.0.0/16”.

The screenshot shows the 'Create virtual network' wizard in the Microsoft Azure portal, specifically the 'IP addresses' step. The breadcrumb navigation shows 'Home > Virtual networks > Create virtual network'. The 'IP addresses' tab is selected. A note says to configure the virtual network address space with IPv4 and IPv6 ranges and subnets. It also notes that the address space overlaps with another network ('vnet'). A 'Delete address space' link is provided. The main area shows an 'Add a subnet' button. Below it, a table lists a single subnet: 'default' with IP range '10.0.0.0 - 10.0.0.255', size '/24 (256 addresses)', and NAT gateway set to '-'. An 'Edit' icon is next to the subnet row. At the bottom, there's a 'Add IPv4 address space' button and navigation buttons for 'Previous', 'Next', and 'Review + create'.

Click on “Add a subnet”.

Add a subnet

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. [Learn more](#)

Subnet purpose	Default
Name *	Subnet-VM
IPv4	
Include an IPv4 address space	<input checked="" type="checkbox"/>
IPv4 address range *	10.0.0.0/16 10.0.0.0 - 10.0.255.255
Starting address *	10.0.1.0
Size	/24 (256 addresses)
Subnet address range	10.0.1.0 - 10.0.1.255
IPv6	
Include an IPv6 address space	<input type="checkbox"/> This virtual network has no IPv6 address ranges.
Private subnet	
Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. Learn more	
Enable private subnet (no default outbound access)	<input type="checkbox"/>
Security	
Add	Cancel
Give feedback	

Under “Subnets*”, create two subnets as “Subnet-VM” and “Subnet-Storage” for virtual machine and storage account:

Have subnet address range a `10.0.1.0/24` for VM.

Click on Add.

Next create a second subnet for your storage account.

Add a subnet

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. [Learn more](#)

Subnet purpose	Default
Name *	Subnet-Storage
IPv4	
Include an IPv4 address space	<input checked="" type="checkbox"/>
IPv4 address range *	10.0.0.0/16 10.0.0.0 - 10.0.255.255
Starting address *	10.0.2.0
Size	/24 (256 addresses)
Subnet address range	10.0.2.0 - 10.0.2.255
IPv6	
Include an IPv6 address space	<input type="checkbox"/> This virtual network has no IPv6 address ranges.
Private subnet	
Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. Learn more	
Enable private subnet (no default outbound access)	<input type="checkbox"/>
Security	
Add	Cancel
Give feedback	

For storage, have subnet at “10.0.2.0/24”. Click on Add.

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

odl.user.1523814@sim...
SIMPLILEARN HOL 29 (SIMPLI...)

Home > Virtual networks >

Create virtual network

Basics Security IP addresses Tags Review + create

Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet. [Learn more](#)

+ Add a subnet

10.0.0/16 Delete address space
This address prefix overlaps with virtual network 'vnet'. If you intend to peer these virtual networks, change the address space. [Learn more](#)

Subnets	IP address range	Size	NAT gateway
default	10.0.0.0 - 10.0.0.255	/24 (256 addresses)	-
Subnet-Storage	10.0.2.0 - 10.0.2.255	/24 (256 addresses)	-
Subnet-VM	10.0.1.0 - 10.0.1.255	/24 (256 addresses)	-

Previous Next Review + create Give feedback

Go to “Review+create”.

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

odl.user.1523814@sim...
SIMPLILEARN HOL 29 (SIMPLI...)

Home > Virtual networks >

Create virtual network

Basics Security IP addresses Tags Review + create

[View automation template](#)

Basics

Subscription	Simplilearn HOL 29
Resource Group	RandEnt
Name	RandEnt-VirtNet
Region	East US 2

Security

Azure Bastion	Disabled
Azure Firewall	Disabled
Azure DDoS Network Protection	Disabled

IP addresses

Address space	10.0.0/16 (65,536 addresses)
Subnet	default (10.0.0/24) (256 addresses)
Subnet	Subnet-Storage (10.0.2/24) (256 addresses)
Subnet	Subnet-VM (10.0.1/24) (256 addresses)

Tags

Previous Next Create Give feedback

Click “Create”.

The screenshot shows the Microsoft Azure Deployment Overview page for a completed deployment named "RandEnt-VirtNet-1732314978598". The deployment status is marked as "Your deployment is complete". Key details include:

- Deployment name: RandEnt-VirtNet-1732314978598
- Subscription: Simplilearn HOL 29
- Resource group: RandEnt
- Start time: 11/22/2024, 2:36:50 PM
- Correlation ID: 348db7e2-89e9-4136-a514-d0f2c3555689

The page also includes sections for "Deployment details", "Next steps", and a "Go to resource" button. A feedback section at the bottom encourages users to share their experience with deployment.

Your Virtual Network is created.

The screenshot shows the Microsoft Azure Virtual Network Overview page for a virtual network named "RandEnt-VirtNet". The page displays basic information such as the resource group (RandEnt), location (East US 2), subscription (Simplilearn HOL 29), and other properties like address space (10.0.0.0/16) and DNS servers (Azure provided DNS service). The "Capabilities" tab is selected, showing five options: DDoS protection, Azure Firewall, Peerings, Private endpoints, and Microsoft Defender for Cloud. All these features are currently set to "Not configured".

2.2 Create Virtual Machine

Create Virtual Machines (VMs) to host your application. These VMs will connect to the storage account through a private endpoint.

In the Azure Portal, go to Virtual Machines.

In the VM page, click “+ Create” and select “Azure virtual machine”.

The screenshot shows the Microsoft Azure Virtual Machines dashboard. A single virtual machine, "ODL-user-1523814", is listed in the table. The table columns include Type, Resource group, Location, Status, Operating system, Size, Public IP address, and Disks. The VM details are as follows:

Type	Resource group	Location	Status	Operating system	Size	Public IP address	Disks
Azure virtual machine	ODL-azure-1523814	East US 2	Running	Windows	Standard_B4ms	40.75.112.124	1

In “Create a virtual machine”:

Provide a name for your VM, example “VM1” and be sure the Region is the same as your virtual network (US East 2).

Set availability options as “No infrastructure redundancy required”.

Security type as “Standard” and in Image select your operating system as “Windows Server 2022 Datacenter: Azure Edition – x64 Gen2”.

The screenshot shows the "Create a virtual machine" wizard on the "Basics" step. The form includes fields for Project details, Instance details, and Image selection.

Project details:

- Subscription: Simplilearn HOL 29
- Resource group: RandEnt (selected)

Instance details:

- Virtual machine name: VM1
- Region: (US) East US 2
- Availability options: No infrastructure redundancy required
- Security type: Standard
- Image: Windows Server 2022 Datacenter: Azure Edition - x64 Gen2

Note: This image is compatible with additional security features. [Click here to swap to the Trusted launch security type.](#)

Buttons at the bottom: < Previous, Next : Disks >, Review + create, Give feedback.

For Size, select “Standard_DS1_v2” or the appropriate size for your VM.

Home > Virtual machines >

Create a virtual machine

Help me create a low cost VM Help me create a VM optimized for high availability Help me choose the right VM size for my workload

VM architecture Arm64 x64
⚠️ Arm64 is not supported with the selected image.

Run with Azure Spot discount

Size * Standard_DS1_v2 - 1 vcpu, 3.5 GB memory (\$85.41/month)
 See all sizes
⚠️ Item(s) availability based on policy assignment(s) for the selected scope.
[azurerm670-1523814-PolicyDefinitions \(Policy details\)](#)

Enable Hibernation
⚠️ Hibernation is not supported by the size that you have selected. Choose a size that is compatible with Hibernation to enable this feature. [Learn more ↗](#)

Administrator account
 Username *
 Password *
 Confirm password *

Inbound port rules
 Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Inbound port rules
 Public inbound ports * None Allow selected ports
 Select inbound ports * HTTP (80), RDP (3389)
⚠️ All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

Licensing
 Save up to 49% with a license you already own using Azure Hybrid Benefit. [Learn more ↗](#)
 Would you like to use an existing Windows Server license?

< Previous Next : Disks > Review + create

For Administrator account, create a username and password to access your VM.

Inbound port rules, have “Allow selected ports” selected and set them to HTTP and RDP.

For Disks, leave it at default setting.

Home > Virtual machines >

Create a virtual machine

Help me create a low cost VM Help me create a VM optimized for high availability Help me choose the right VM size for my workload

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more ↗](#)

VM disk encryption
 Azure disk storage encryption automatically encrypts your data stored on Azure managed disks (OS and data disks) at rest by default when persisting it to the cloud.

Encryption at host
⚠️ Encryption at host is not registered for the selected subscription. [Learn more ↗](#)

OS disk
 OS disk size image default (127 GB)
 OS disk type * Premium SSD (locally-redundant storage)
 Delete with VM
 Key management Platform-managed key
 Enable Ultra Disk compatibility
⚠️ Ultra disk is not supported for the selected VM size Standard_DS1_v2 in East US 2.

Data disks for VM1
 You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching	Delete with VM
					<input type="checkbox"/>

Create and attach a new disk [Attach an existing disk](#)

< Previous Next : Networking > Review + create

Next click on Networking.

Choose your virtual network you created, (RandEnt-VirNet).

Under Subnet, select the subnet you created for VM, “Subnet-VM”.

Home > Virtual machines >

Create a virtual machine

...

Help me create a low cost VM Help me create a VM optimized for high availability Help me choose the right VM size for my workload

Basics Disks **Networking** Management Monitoring Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.
[Learn more](#)

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network *

Subnet *

Public IP

NIC network security group None Basic Advanced

Public inbound ports * None Allow selected ports

Select inbound ports *

⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

< Previous Next : Management > **Review + create**

Select inbound ports *

⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Delete public IP and NIC when VM is deleted

Enable accelerated networking

Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Load balancing options None Azure load balancer Supports all TCP/UDP network traffic, port-forwarding, and outbound flows. Application gateway Web traffic load balancer for HTTP/HTTPS with URL-based routing, SSL termination, session persistence, and web application firewall.

< Previous Next : Management > **Review + create**

Next in Monitoring.

Home > Virtual machines >

Create a virtual machine

Help me create a low cost VM Help me create a VM optimized for high availability Help me choose the right VM size for my workload

Basics Disks Networking Management **Monitoring** Advanced Tags Review + create

Configure monitoring options for your VM.

Alerts
Enable recommended alert rules

Diagnostics
Boot diagnostics Enable with managed storage account (recommended)
 Enable with custom storage account
 Disable

Enable OS guest diagnostics

Health
Enable application health monitoring

< Previous Next : Advanced > **Review + create**

Set Boot Diagnostics to “Enable with managed storage account”.

Click on “Review + Create”.

Home > Virtual machines >

Create a virtual machine

Validation passed

Help me create a low cost VM Help me create a VM optimized for high availability Help me choose the right VM size for my workload

Basics Disks Networking Management Monitoring Advanced Tags **Review + create**

Price
1 X Standard DS1 v2 by Microsoft Subscription credits apply
0.1170 USD/hr Terms of use | Privacy policy Pricing for other VM sizes

TERMS
By clicking “Create”, I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

⚠ You have set RDP port(s) open to the internet. This is only recommended for testing. If you want to change this setting, go back to Basics tab.

Basics
Subscription Simplilearn HOL 29
Resource group RandEnt

< Previous Next > **Create** Download a template for automation Give feedback

Click “Create”.

Your Virtual Machine and Virtual Network are ready.

Step 3: Compute & Storage

Create a storage account to store your image-based content for ARM template.

3.1 Create Standard Storage Account

Go to “Storage Accounts”.

In Storage Accounts, click on “+ Create”.



No storage accounts to display

Create a storage account to store up to 500TB of data in the cloud. Use a general-purpose storage account to store object data, use a NoSQL data store, define and use queues for message processing, and set up file shares in the cloud. Use the Blob storage account and the hot or cool access tiers to optimize your costs based on how frequently your object data is accessed.

[Create storage account](#)

[Learn more](#)

Under Create the Storage Account:

Select your subscription and your resource group.

In “Storage Account Name”: Create a unique name. For this demo, it will be called `randentstore` .

Select the same region as your virtual network and VM. “East US 2”

For Performance, choose “Standard”, and for Redundancy choose “Locally redundant storage (LRS)”.

The screenshot shows the 'Create a storage account' wizard in the Microsoft Azure portal. The current step is 'Project details'. It includes fields for 'Subscription' (set to 'Simplilearn HOL 29'), 'Resource group' (set to 'RandEnt'), and 'Storage account name' (set to 'randentstore'). Below these, there are dropdowns for 'Region' (set to '(US) East US 2') and 'Primary service' (set to 'Azure Blob Storage or Azure Data Lake Storage Gen 2'). Under 'Performance', the 'Standard' option is selected. Under 'Redundancy', 'Locally-redundant storage (LRS)' is chosen. At the bottom, there are 'Previous', 'Next', and 'Review + create' buttons, with 'Review + create' being the active button.

Click “Review + Create”.

The screenshot shows the 'Create a storage account' wizard in the Microsoft Azure portal, with the 'Review + create' step selected. It displays a summary of the configuration settings:

Setting	Value
Subscription	Simplilearn HOL 29
Resource group	RandEnt
Location	East US 2
Storage account name	randentstore
Primary service	Azure Blob Storage or Azure Data Lake Storage Gen 2
Performance	Standard
Replication	Locally-redundant storage (LRS)

Below the summary, there are sections for 'Advanced' and 'Security' settings, which are currently empty. At the bottom, there are 'Previous', 'Next', and 'Create' buttons, with 'Create' being the active button.

Click “Create”.

Your Storage Account is created.

3.2: Set Up Service Endpoint for Storage

Ensure that the storage account can only be accessed through an internal network of Azure and avoid storage account access to public internet, create a private network by configuring service endpoints.

Select your created storage account.

Properties	
Blob service	Hierarchical namespace Default access tier Blob anonymous access Blob soft delete Container soft delete Versioning Change feed
Security	Require secure transfer for REST API operations Storage account key access Minimum TLS version Infrastructure encryption
Networking	Allow access from All networks

In settings, under “Security + networking”, click and select “Networking”.

Under the tab “Firewalls and virtual networks”, select “Enabled from selected virtual networks and IP addresses” under Public network access.

The screenshot shows the Microsoft Azure Storage accounts page. On the left, there's a sidebar with various options like Overview, Activity log, Tags, Diagnose and solve problems, Access Control (IAM), Data migration, Events, Storage browser, Storage Mover, Partner solutions, Data storage, Security + networking, Networking, Front Door and CDN, Access keys, Shared access signature, Encryption, Microsoft Defender for Cloud, Data management, and Storage tasks (preview). The Networking section is currently selected. The main pane shows the 'Networking' tab for the 'randonstore' storage account. It includes sections for Firewall settings, Virtual networks, Firewall, and Resource instances. A message at the top states: "Firewall settings restricting access to storage services will remain in effect for up to a minute after saving updated settings allowing access." Below this, under "Virtual networks", there are buttons for "+ Add existing virtual network" and "+ Add new virtual network". A table lists "Virtual Network", "Subnet", "Address range", "Endpoint Status", "Resource Group", and "Subscription". Under "Firewall", there are options for "Add IP ranges to allow access from the internet or your on-premises networks" and "Address range". Under "Resource instances", it says "Specify resource instances that will have access to your storage account based on their system-assigned managed identity".

In Firewalls and Virtual Networks tab:

Under “Virtual Networks”, click “+ Add existing virtual network”.

The screenshot shows the "Add networks" dialog box overlaid on the Azure Storage account page. The dialog has fields for "Subscription" (set to "Simplilearn HOL 29"), "Virtual networks" (set to "RandEnt-VirtNet"), and "Subnets" (set to "Subnet-Storage (Service endpoint required)"). A note below states: "The following networks don't have service endpoints enabled for 'Microsoft.Storage'. Enabling access will take up to 15 minutes to complete. After starting this operation, it is safe to leave and return later if you do not wish to wait." At the bottom, there's a table for "Virtual network" and "Service endpoint status" with one entry: "RandEnt-VirtNet" and "Subnet-Stora..." with "Not enabled". There's also an "Enable" button.

In Add networks, select your virtual network (`RandEntVNet`) and storage subnet (`storageSubnet`) to allow the storage account to be accessed from.

Click on Enable to access to storage account.

Click on Add. Then click on Save.

Step 4: Create the Storage account container for Images & configure service endpoints

4.1: Create Private Endpoint

Configure a private endpoint to securely access the storage account from the VM over the internal network.

Go to Private endpoints page, then click “+ Create”.

Name ↑↓	Private IP ↑↓	Resource ↑↓	Target sub-resource ↑↓	Subnet ↑↓	Connection State ↑↓
Showing 0 to 0 of 0 records.					

No private endpoints to display
Try changing or clearing your filters.
[Learn more](#)

In Create the Private Endpoint:

Enter a name, such as `StoragePrivateEnd'. Name for Network Interface Name will be automatically created.

Region is East US 2 as storage account.

The screenshot shows the 'Create a private endpoint' wizard in the Microsoft Azure portal. The current step is 'Basics'. The 'Subscription' dropdown is set to 'Simplilearn HOL 29'. The 'Resource group' dropdown is set to 'RandEnt'. Under 'Instance details', the 'Name' field is 'StoragePrivateEnd', the 'Network Interface Name' field is 'StoragePrivateEnd-nic', and the 'Region' is 'East US 2'. At the bottom, there are 'Next : Resource >' and '< Previous' buttons.

Click on Next: Resource.

The screenshot shows the 'Create a private endpoint' wizard in the Microsoft Azure portal. The current step is 'Resource'. The 'Subscription' dropdown is set to 'Simplilearn HOL 29'. The 'Resource type' dropdown is open, showing a list of options including 'Microsoft.Relay/namespaces', 'Microsoft.Search/searchServices', 'Microsoft.ServiceBus/namespaces', 'Microsoft.SignalRService/SignalR', 'Microsoft.SignalRService/webPubSub', 'Microsoft.Sql/managedInstances', 'Microsoft.Sql/servers', 'Microsoft.Storage/storageAccounts', 'Microsoft.StorageSync/storageSyncServices', 'Microsoft.Synapse/privateLinkHubs', 'Microsoft.Synapse/workspaces', and 'Microsoft.TimeSeriesInsights/environments'. The 'Connect to an Azure resource in my directory' radio button is selected. At the bottom, there are 'Next : Virtual Network >' and '< Previous' buttons.

For Resource type, select “Microsoft.Storage/storageAccounts”.

Home > Private Link Center | Private endpoints >
Create a private endpoint ...

✓ Basics **Resource** ③ Virtual Network ④ DNS ⑤ Tags ⑥ Review + create

Private Link offers options to create private endpoints for different Azure resources, like your private link service, a SQL server, or an Azure storage account. Select which resource you would like to connect to using this private endpoint. [Learn more](#)

Connection method Connect to an Azure resource in my directory.
 Connect to an Azure resource by resource ID or alias.

Subscription * Simplilearn HOL 29

Resource type * Microsoft.Storage/storageAccounts

Resource * randomstore

Target sub-resource * blob

< Previous Next : Virtual Network >

Select your created storage account in Resource and then select “blob” as your target sub-resource.

Next under Virtual Network.

Home > Private Link Center | Private endpoints >
Create a private endpoint ...

✓ Basics ✓ Resource **Virtual Network** ④ DNS ⑤ Tags ⑥ Review + create

Networking

To deploy the private endpoint, select a virtual network subnet. [Learn more](#)

Virtual network RandEnt-VirtNet (RandEnt)

Subnet * Subnet-Storage

Network policy for private endpoints Disabled (edit)

Private IP configuration

Dynamically allocate IP address
 Statically allocate IP address

Application security group

Configure network security as a natural extension of an application's structure. ASG allows you to group virtual machines and define network security policies based on those groups. You can specify an application security group as the source or destination in an NSG security rule. [Learn more](#)

+ Create

Application security group

< Previous Next : DNS >

For Subnet, choose the your storage account subnet “storageSubnet”.

✓ Basics ✓ Resource ✓ Virtual Network **DNS** Tags Review + create

Private DNS integration

To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint with a private DNS zone. You can also utilize your own DNS servers or create DNS records using the host files on your virtual machines. [Learn more ↗](#)

Integrate with private DNS zone Yes No

Configuration name	Subscription	Resource group	Private DNS zone
privatelink-blob-core-win...	Simplilearn HOL 29	RandEnt	(new) privatelink.blob.cor...

< Previous Next : Tags >

Under DNS. Keep the default setting for your subscription and resource group.

Click “Review + Create”.

Microsoft Azure

Home > Private Link Center | Private endpoints >
Create a private endpoint ...

Validation passed

✓ Basics ✓ Resource ✓ Virtual Network ✓ DNS ✓ Tags **Review + create**

Basics

Subscription	Simplilearn HOL 29
Resource group	RandEnt
Region	East US 2
Name	StoragePrivateEnd
Network Interface Name	StoragePrivateEnd-nic

Resource

Subscription ID	4bdb238c-14b9-4485-b7e9-52e890fe3321 (Simplilearn HOL 29)
Link type	Microsoft.Storage/storageAccounts
Resource group	RandEnt
Resource	randonstore
Target sub-resource	blob

Virtual Network

Virtual network resource group	RandEnt
Virtual network	RandEnt-VirtNet
Subnet	Subnet-Storage (10.0.2.0/24)
Network Policies	Disabled
Application security groups	None

Create < Previous Next > Download a template for automation

Click Create.

The screenshot shows the Microsoft Azure Private Endpoint Overview page. The deployment name is "Microsoft.PrivateEndpoint-20241122153245". The status is "Your deployment is complete". Deployment details include a start time of 11/22/2024, 3:48:06 PM, and a correlation ID of dcdba314-7a8a-4524-8285-32a5ec00365a. Resource group is RandEnt. There are sections for Deployment details and Next steps, with a "Go to resource" button. On the right, there are promotional cards for Cost management, Microsoft Defender for Cloud, Free Microsoft tutorials, Work with an expert, and Find an Azure expert.

Private Endpoint is created.

4.2: Configure Storage Container for Images

Create a container to hold image-based content in the storage account..

Go to Storage Account and click on your storage account.

In settings under Data Storage, click on Containers.

The screenshot shows the Microsoft Azure Storage Account Containers page for "randentstore". A single container named "\$logs" is listed. The table columns are Name, Last modified, Anonymous access level, and Lease state. The container was last modified on 11/22/2024, 3:21:43 PM, has private anonymous access, and is available lease state. The left sidebar shows various storage account management options like Overview, Activity log, Tags, and Data storage.

Name	Last modified	Anonymous access level	Lease state
\$logs	11/22/2024, 3:21:43 PM	Private	Available

Click "+ Container".

New container

Name *

Anonymous access level

The access level is set to private because anonymous access is disabled on this storage account.

Advanced

Encryption scope

Use this encryption scope for all blobs in the container

Enable version-level immutability support In order to enable version-level immutability support, your storage account must have versioning turned on.

Create Give feedback

Under New container, provide a name for the container (`image1`). The anonymous access level will be set to “Private (no anonymous access)”.

Then click Create.

Overview of setup in Resource Group “RandEnt”.

Name	Type	Location	Actions
privatelink.blob.core.windows.net	Private DNS zone	Global	...
RandEnt-VirtNet	Virtual network	East US 2	...
randentstore	Storage account	East US 2	...
StoragePrivateEnd	Private endpoint	East US 2	...
StoragePrivateEnd-nic	Network Interface	East US 2	...
VM1	Virtual machine	East US 2	...
VM1-ip	Public IP address	East US 2	...
VM1-nsg	Network security group	East US 2	...

By doing this, the creation of a network, compute, and storage solution aligns with the project requirements. By setting RBAC, control access is given to the operations team (Developer and Security Analysis) and configured private endpoints and service endpoints for secure and private connectivity.

The End