Soliz, Joseph
Simplilearn – Cloud Computing
Designing Microsoft Azure Infrastructure Solutions AZ:305
11/23/2024

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

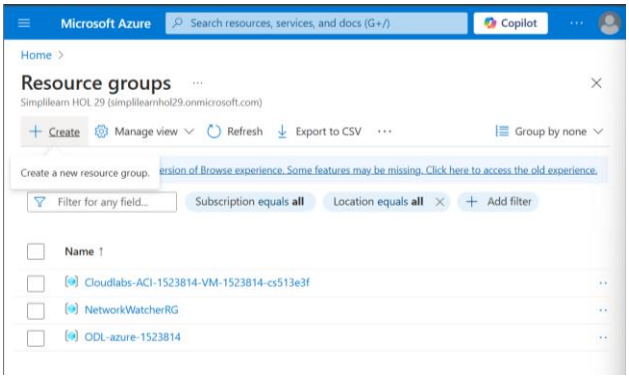
Step 1: Define access using RBAC for operation team

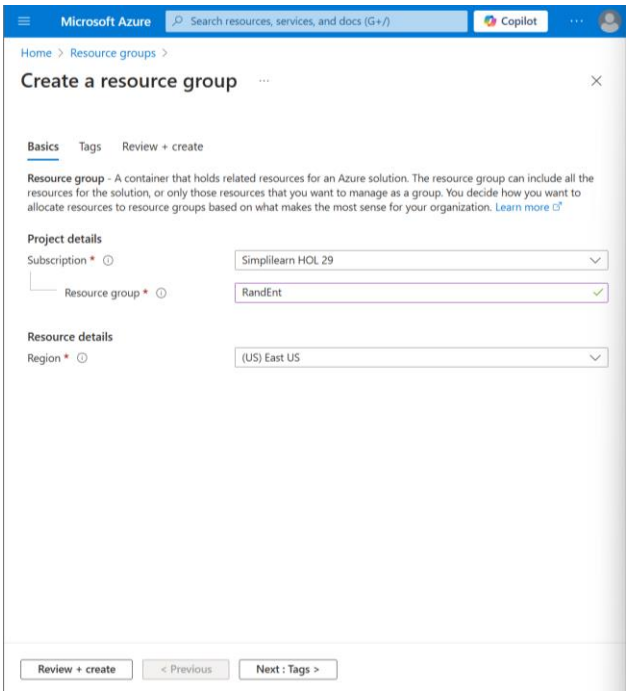
Role-Based Access Control provides fine-grained access management of resources in Azure. This is built in Azure Resource Manager that segregates duties within a team and grants access for what the users need.

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.

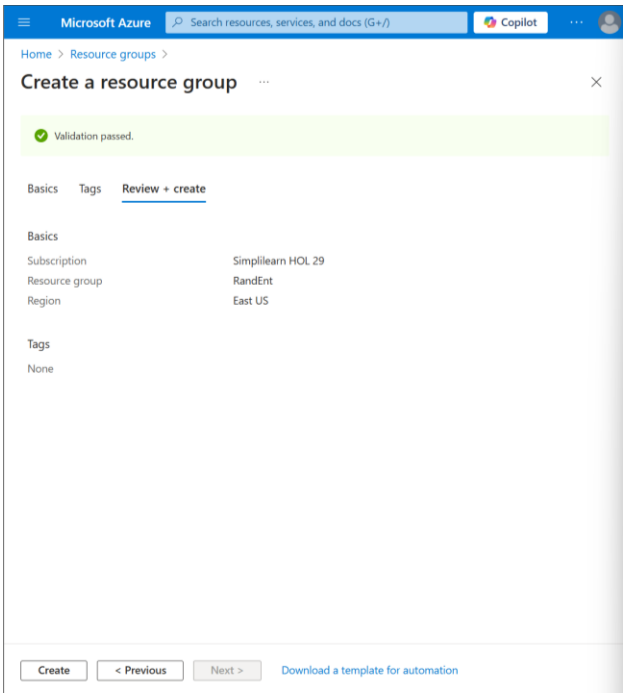
1.1 Resource Group

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).





Then, click on Review + create.

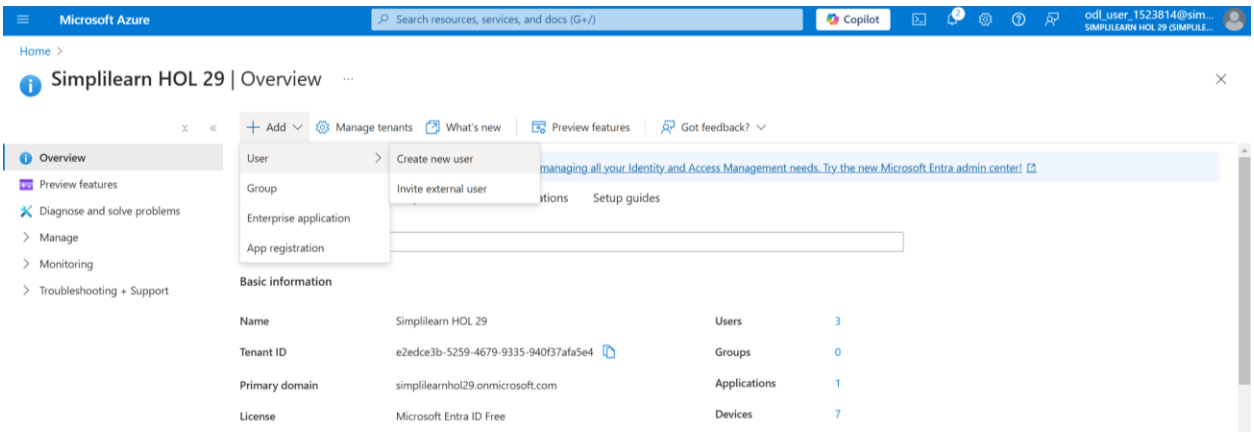


Click create.

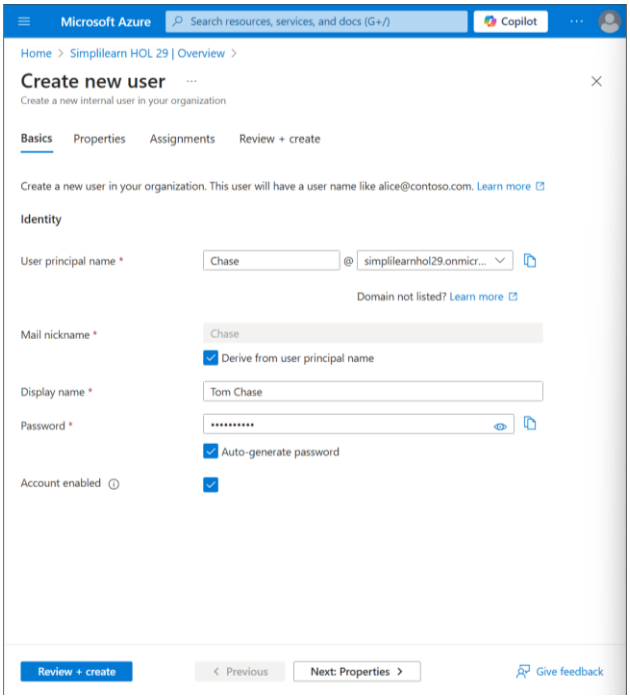
1.2 Add Users

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

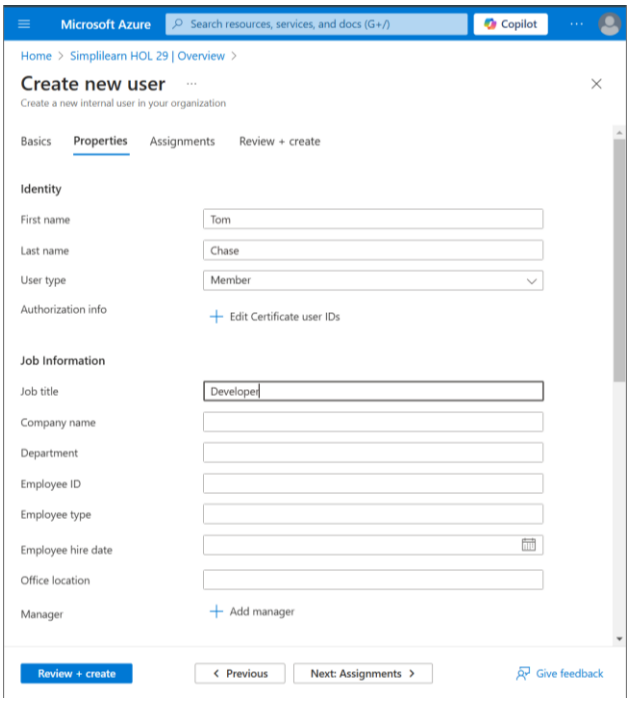
Go to Microsoft Entra ID. In the Overview page, click on Add, select User, and from the drop-out right menu click on Create new user.



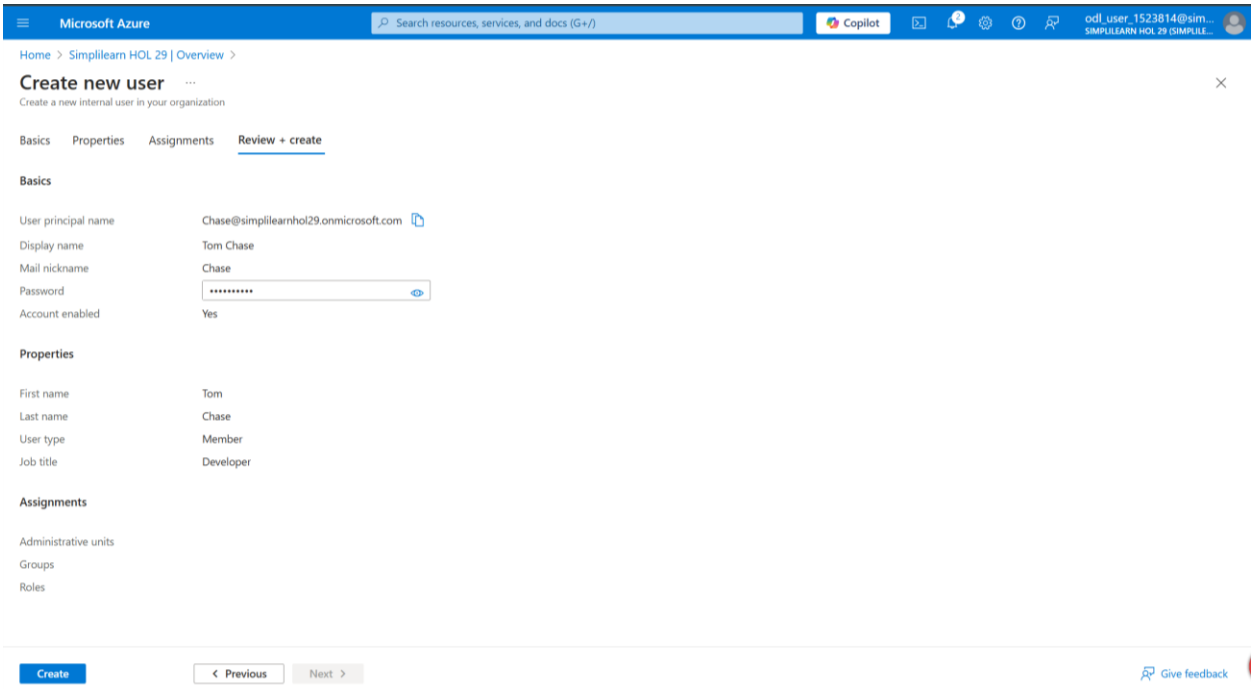
In the Create new user page, under the Basics tab enter the information of the user. In this case, we will call them Tom Chase.



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

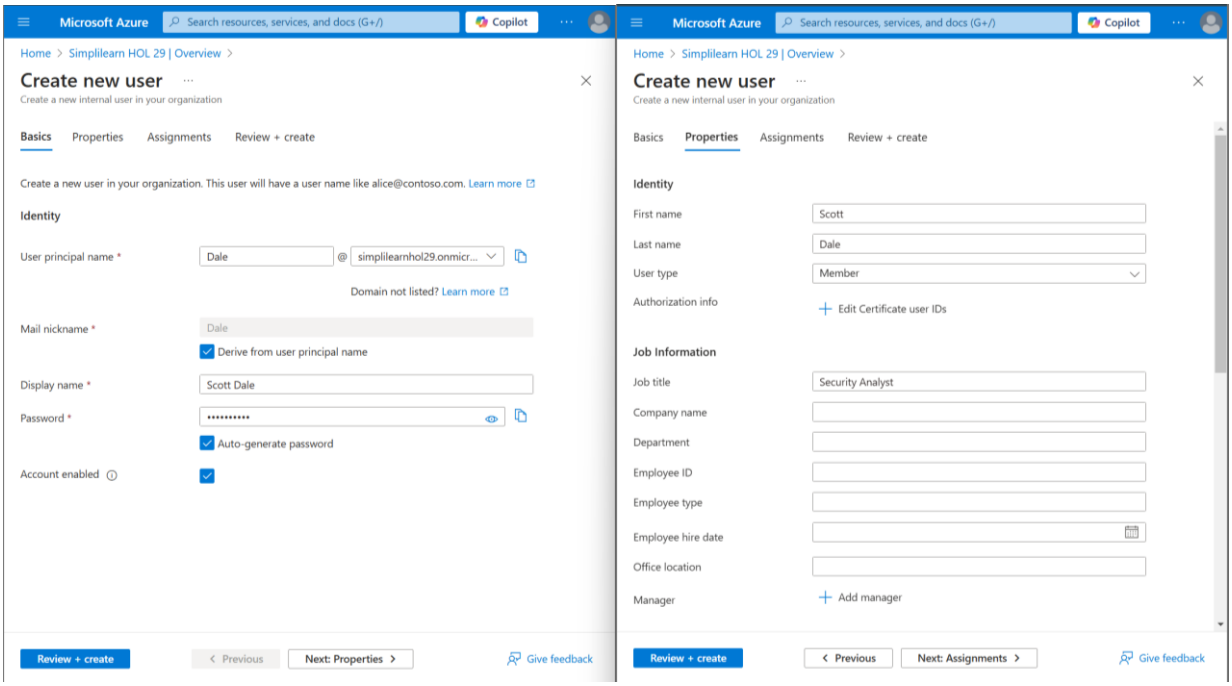


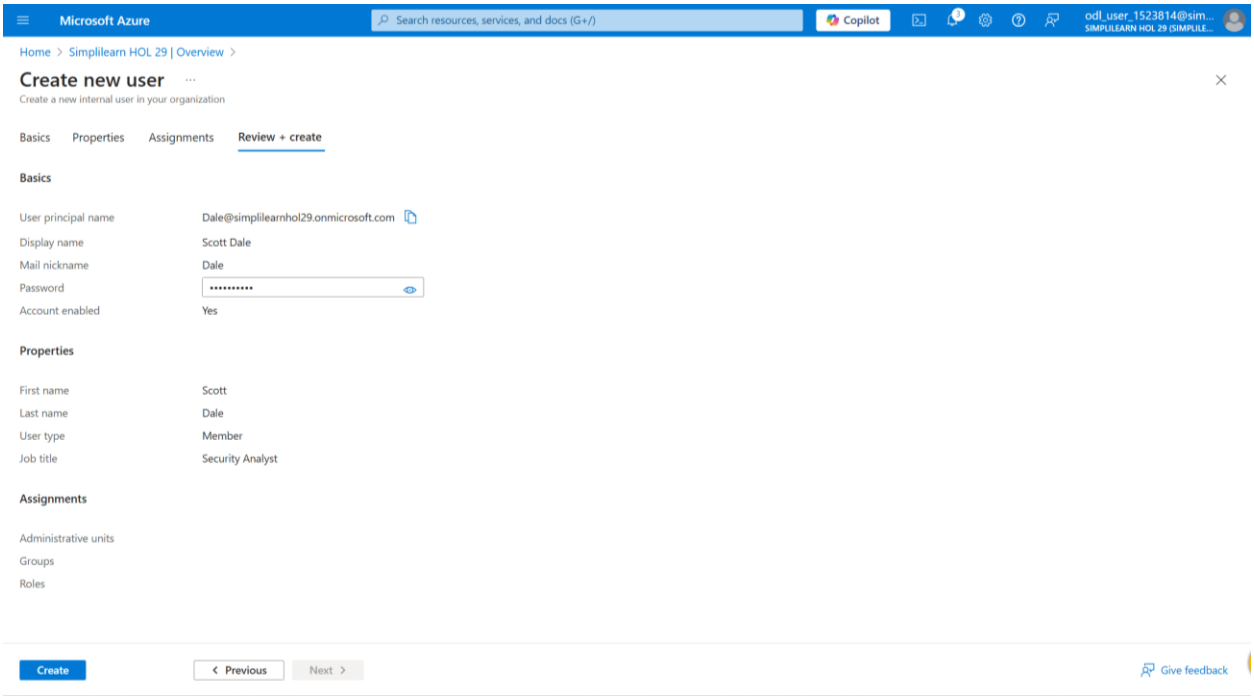
In the Review + create tab, copy the auto-generated password provided in the Password box. This password is given to the user to sign in for the first time. Once the details are entered, click on Create.



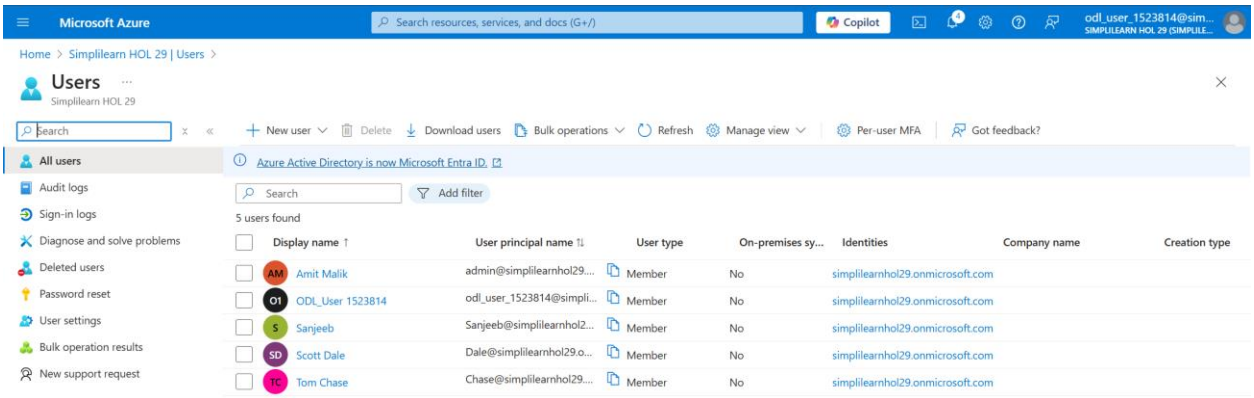
Repeat the same process for a second user, we will call them Scott Dale.

This one will be Security Analyst.





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

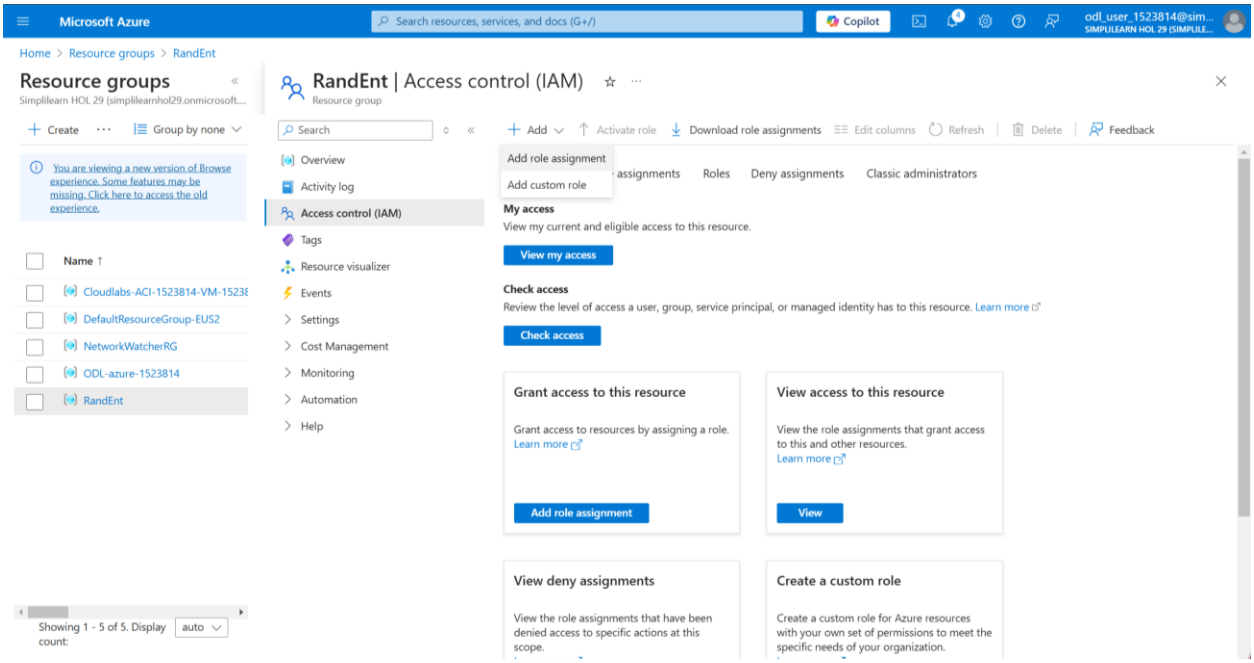


Your users on under User in Microsoft Entra ID.

2.3 Access Control (IAM)

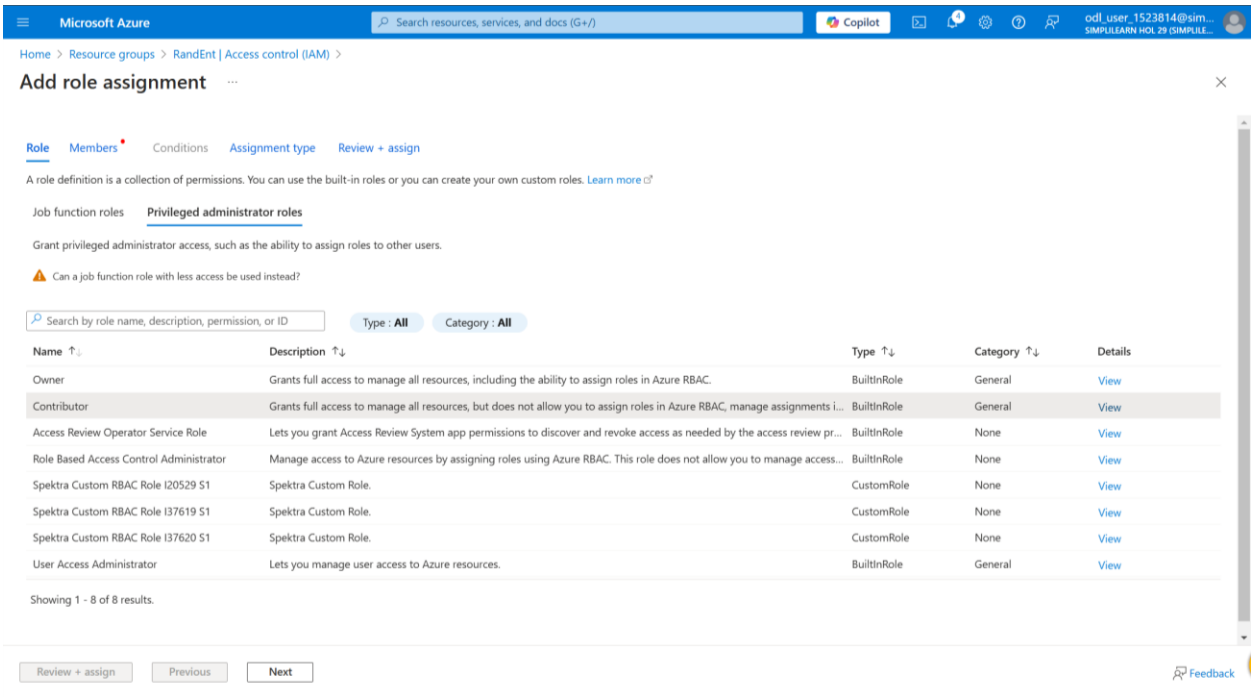
Grant access for the developer and security analysist through Access Control (IAM) in your resource group.

Go to Resources Group and Select “RandEnt”.

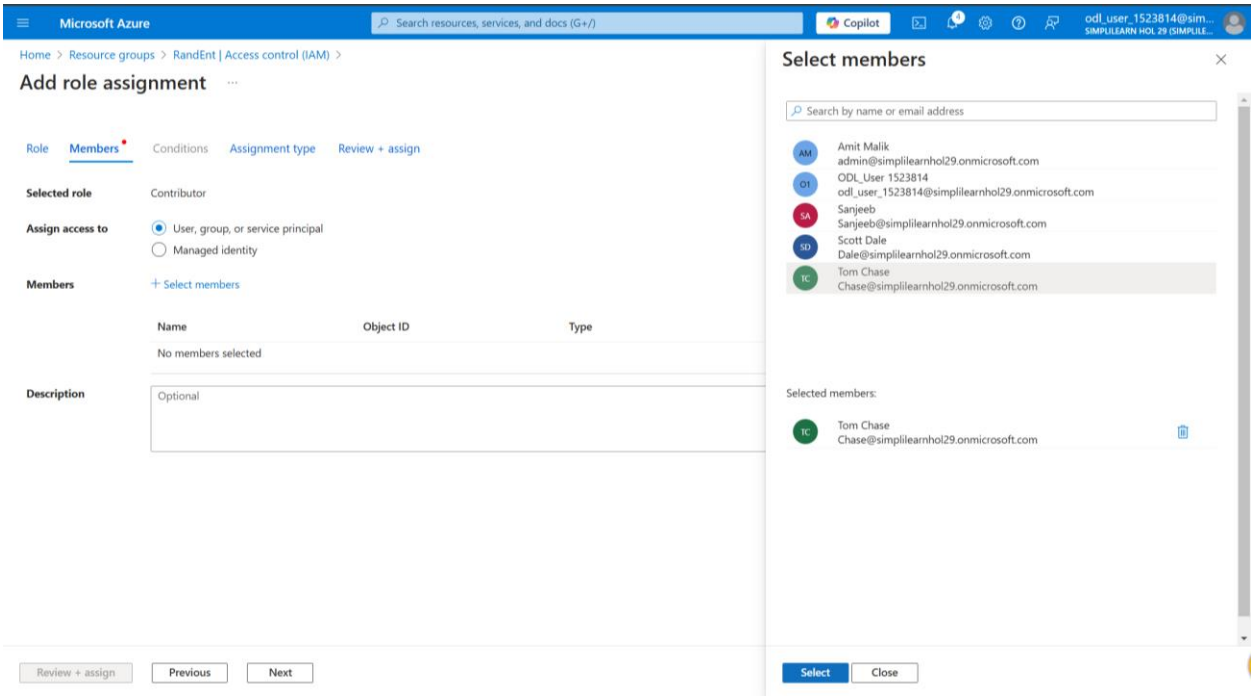


Click on Access Control (IAM) in Settings. Then click on +Add and select Add role assignment.

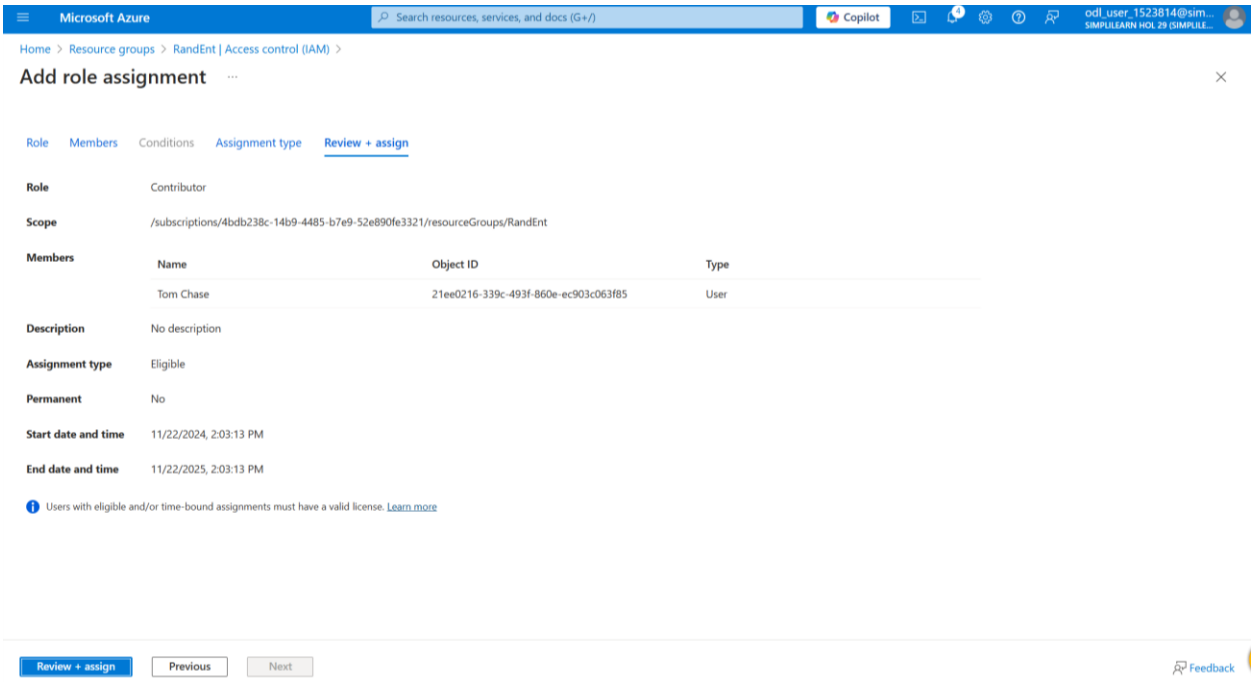
In Add role assignment pane, click on the Privileged administrator roles and select Contributor from the list.



Click on Next.

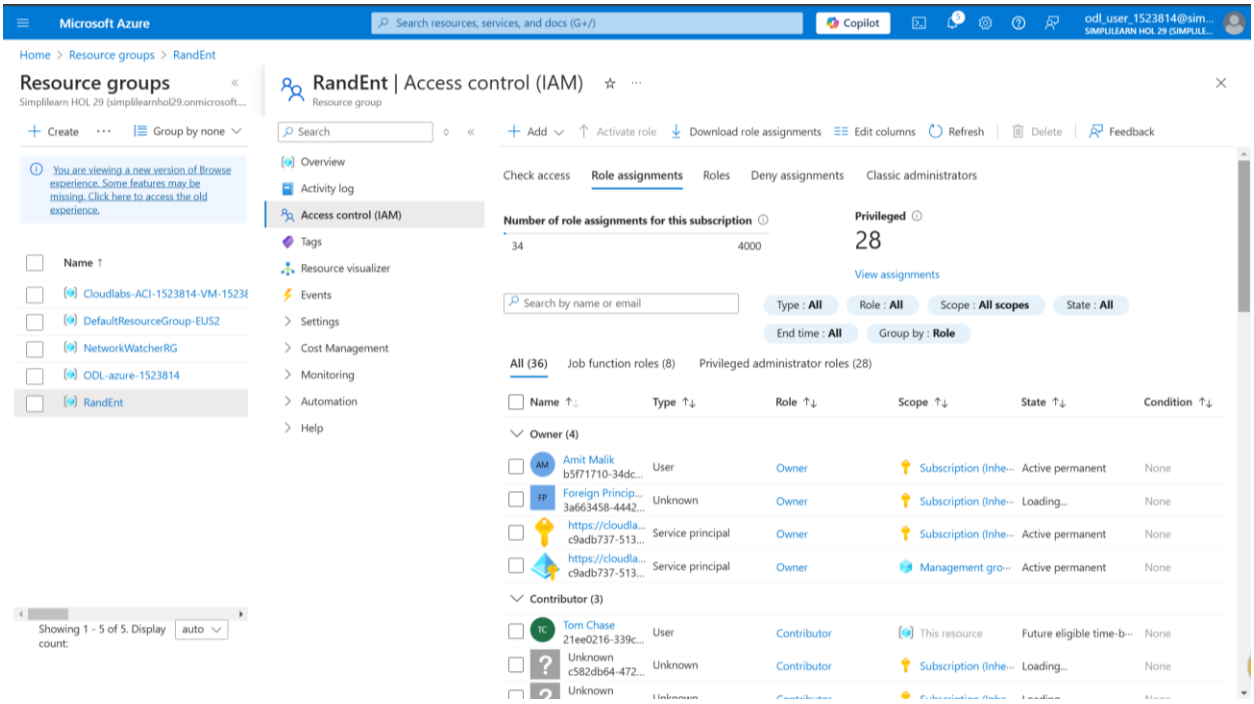


In the Members tab, click on +Select members. In the Select members pane, search for and select the developer user “Tom Chase” and click on Select. The click on Review + Assign.



Click on Review + Assign again.

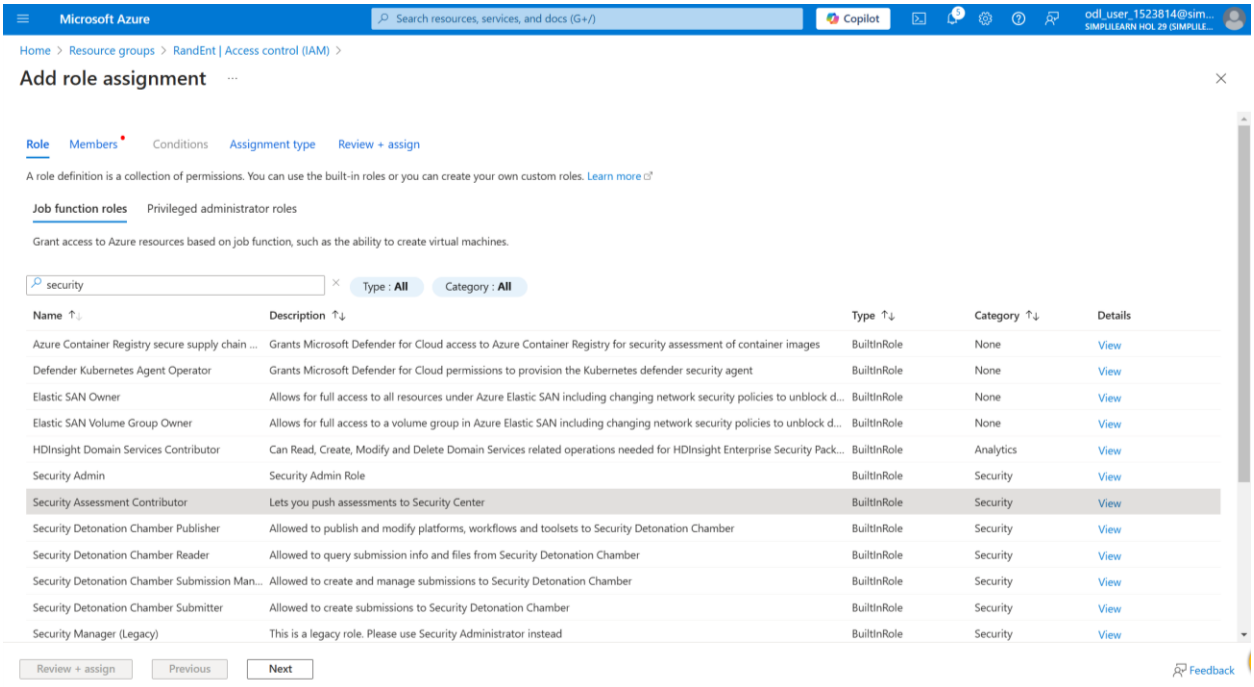
Click on Role Assignments.



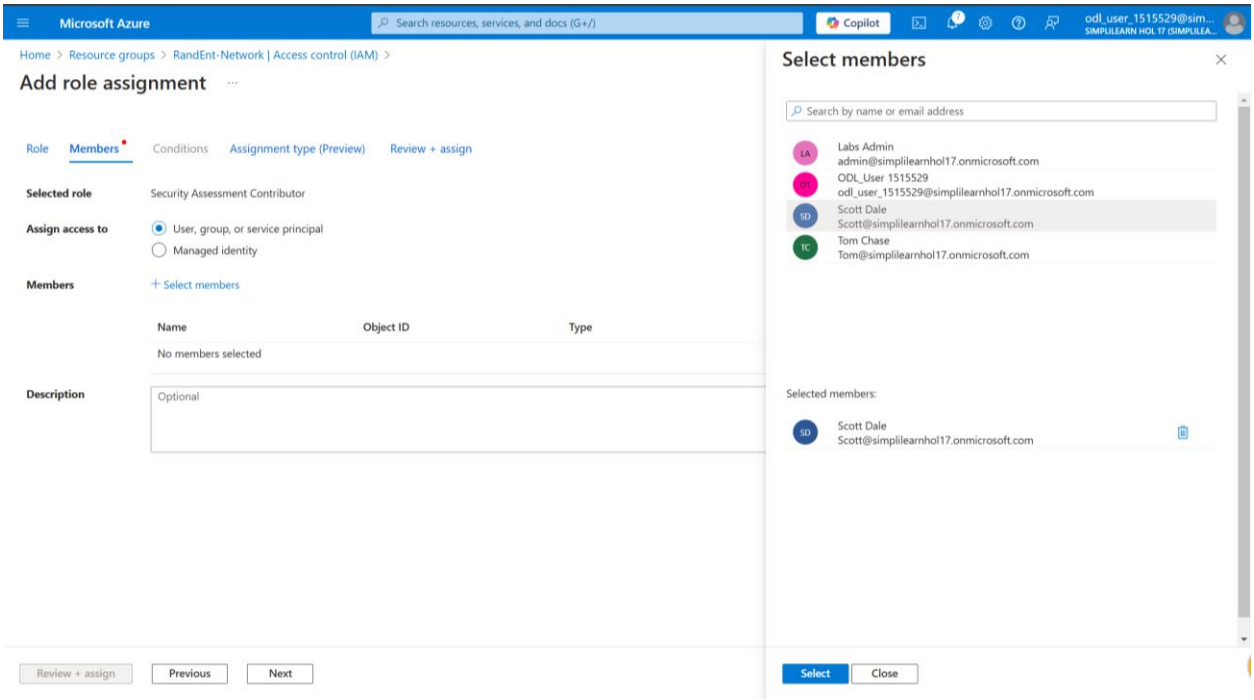
You will see your developer user under Contributor.

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

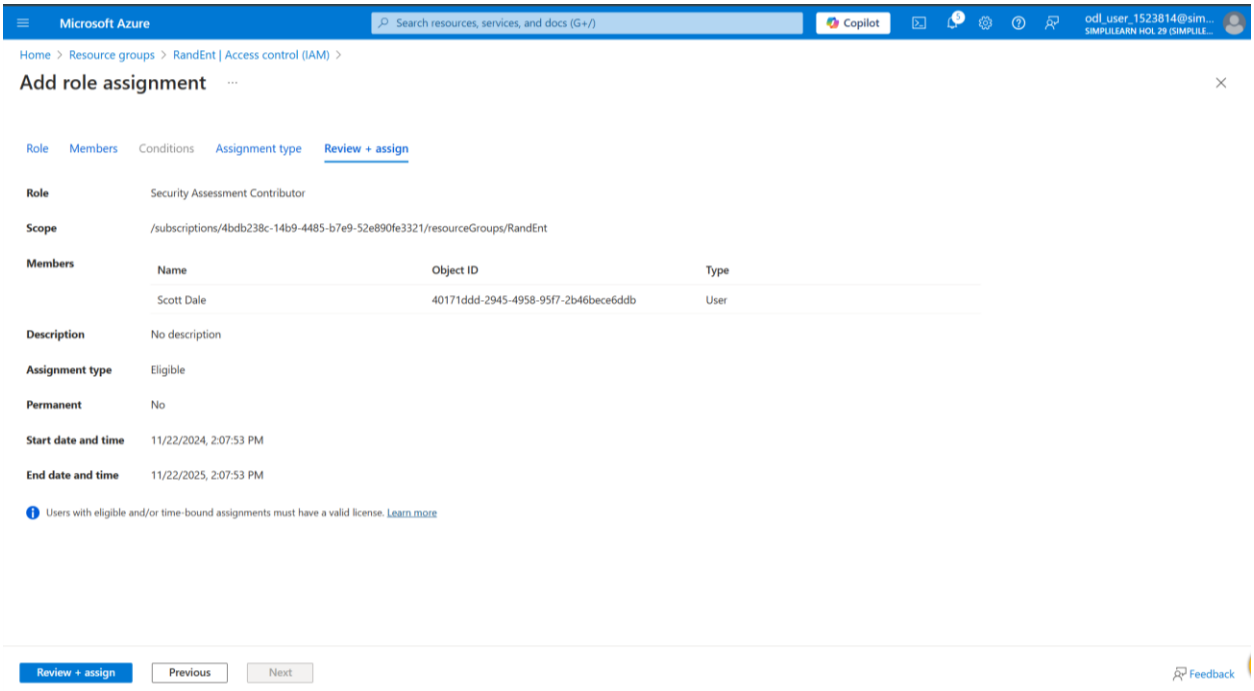
Add a second role assignment, under Job Functions, select Security Assessment Contributor.



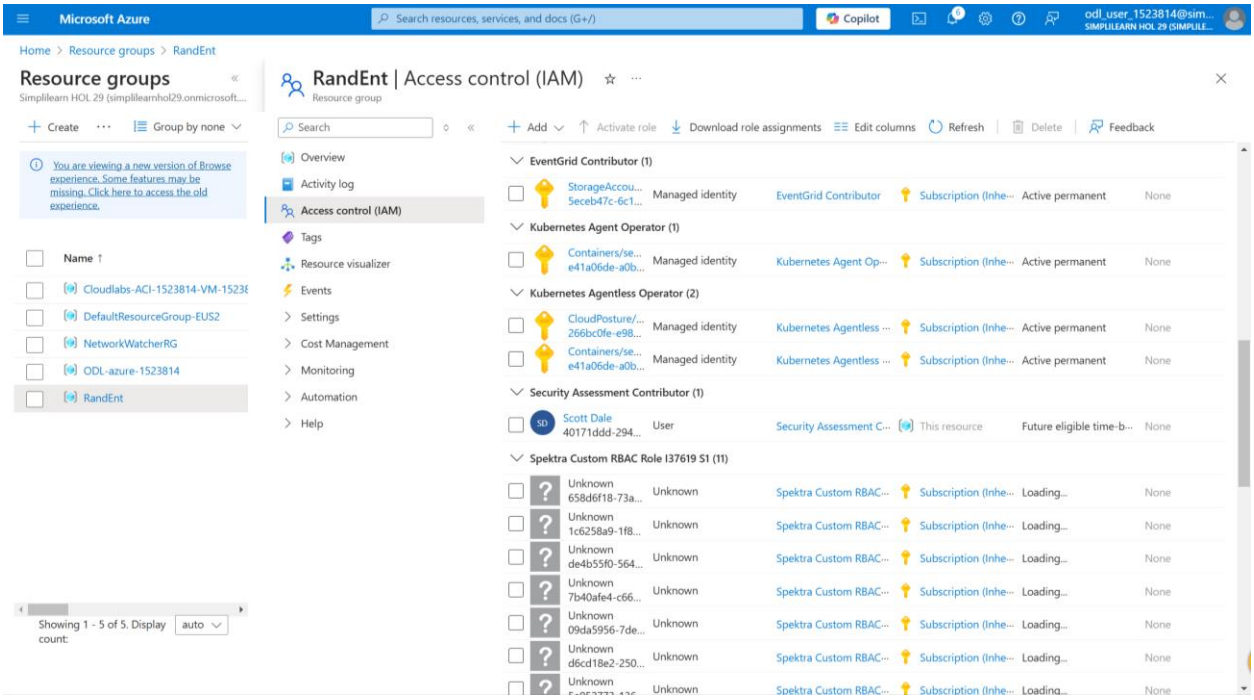
Click Next.



For Select Members, select your use security analyst.



Click on Review + Assign and click on it again.



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.

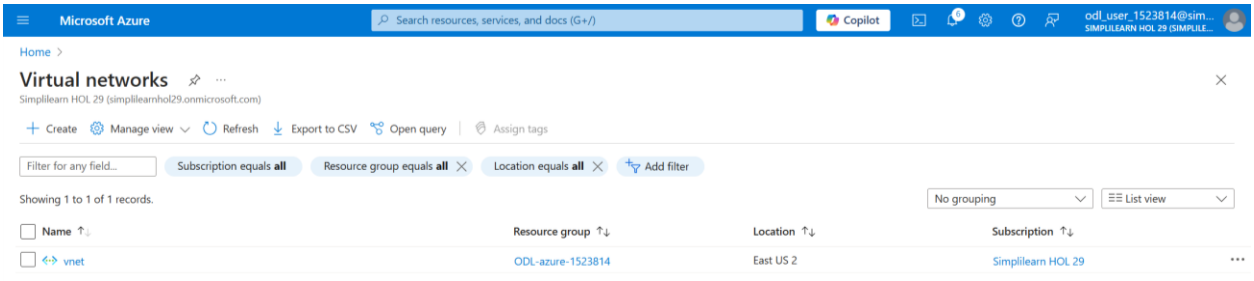
Step 2: Define the network

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

2.1 Create Virtual Network

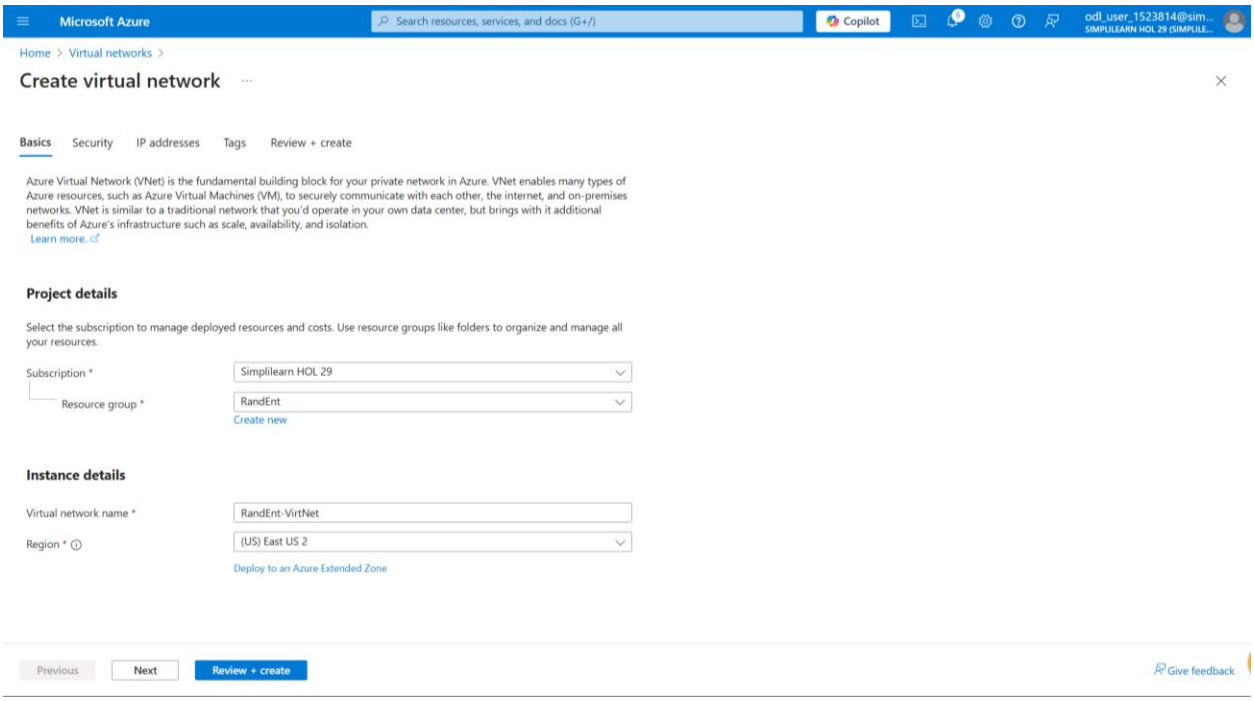
In the Azure Portal, go to Virtual networks.

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

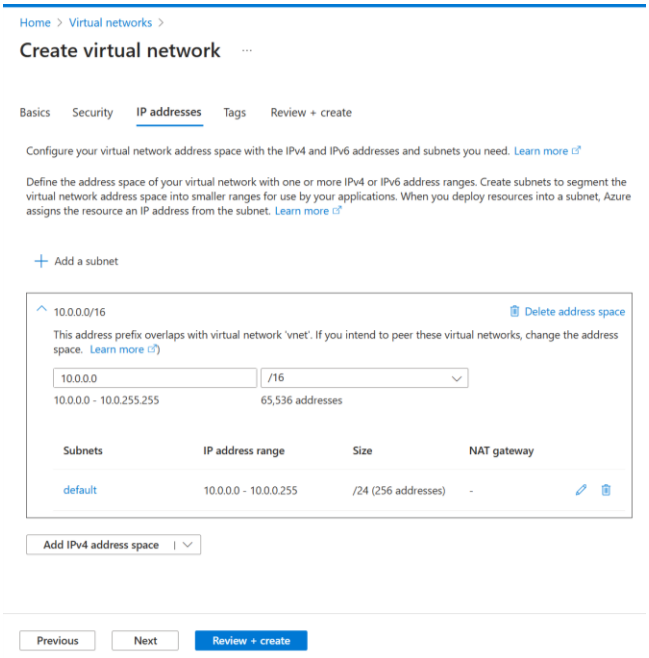


In “Create virtual network”:

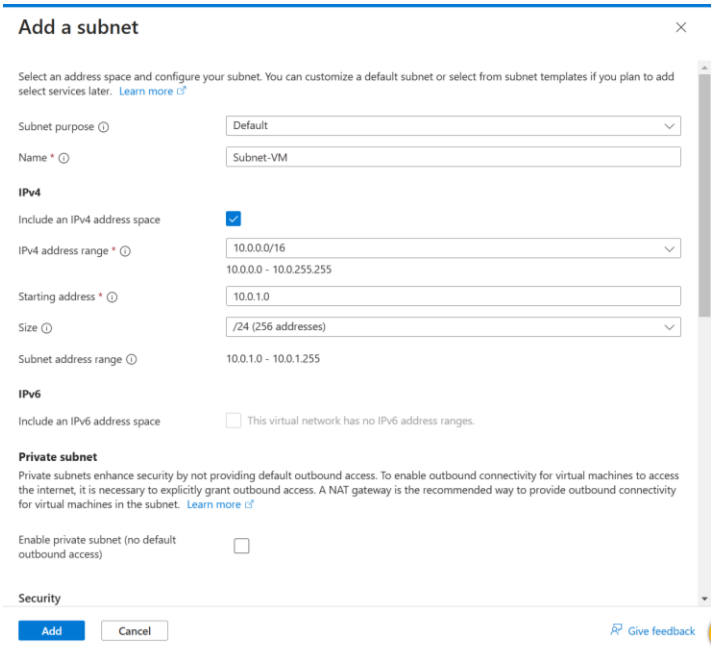
Select your resource group “RandEnt” and create a Virtual Network name “RandEnt-VirtNet”. Under region as (US) East Us 2 (East US would be fine but we are using the second version due to policy error).



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



Click on “Add a subnet”.

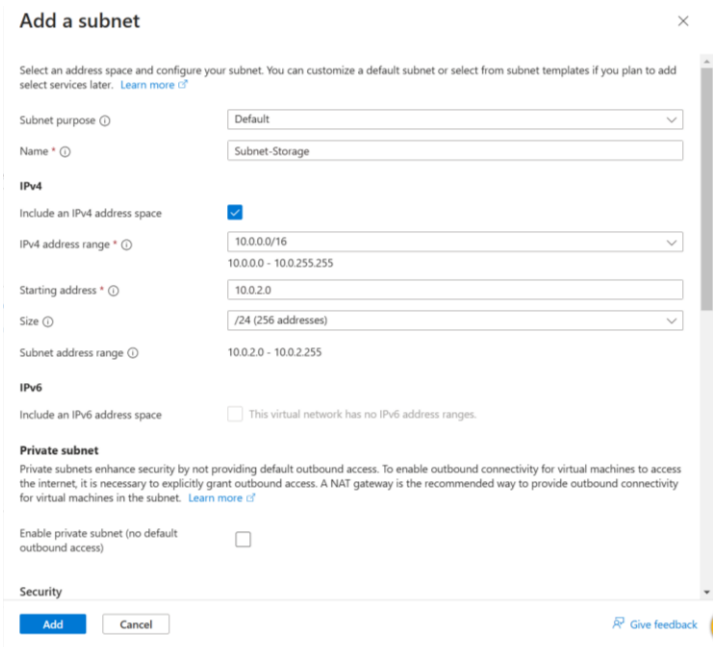


Under “Subnets*”, create two subnets as “Subnet-VM” and “Subnet-Storage” for virtual machine and storage account:

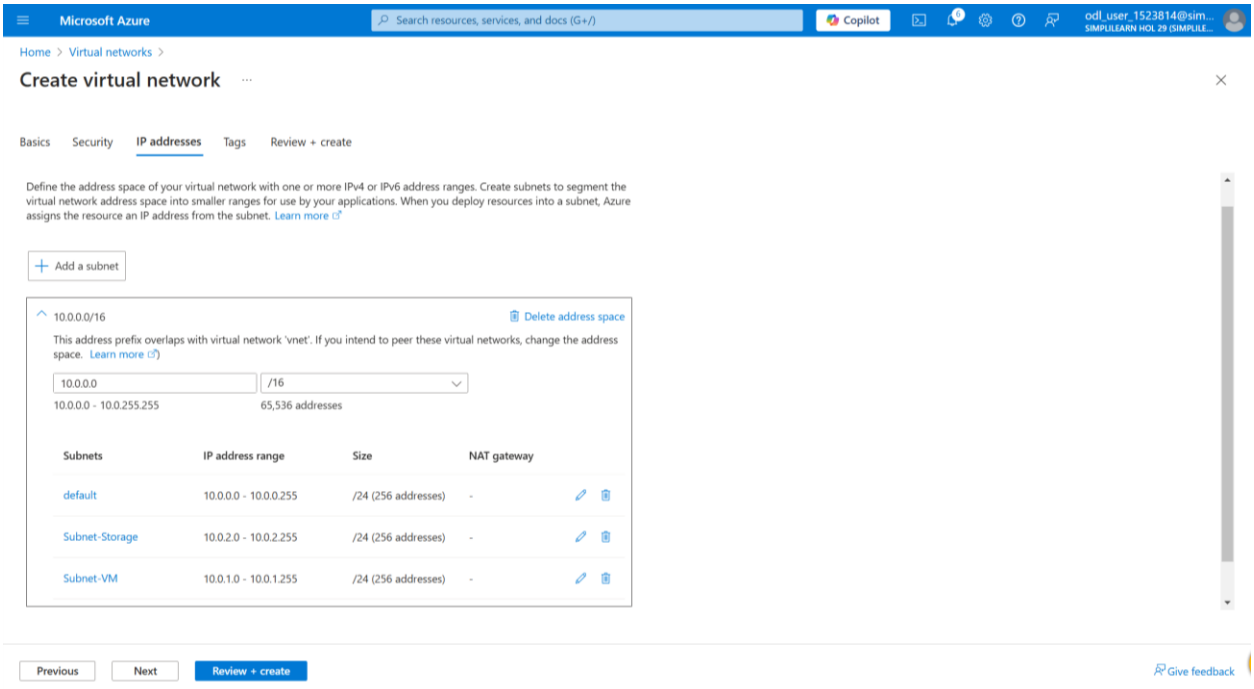
Have subnet address range a `10.0.1.0/24` for VM.

Click on Add.

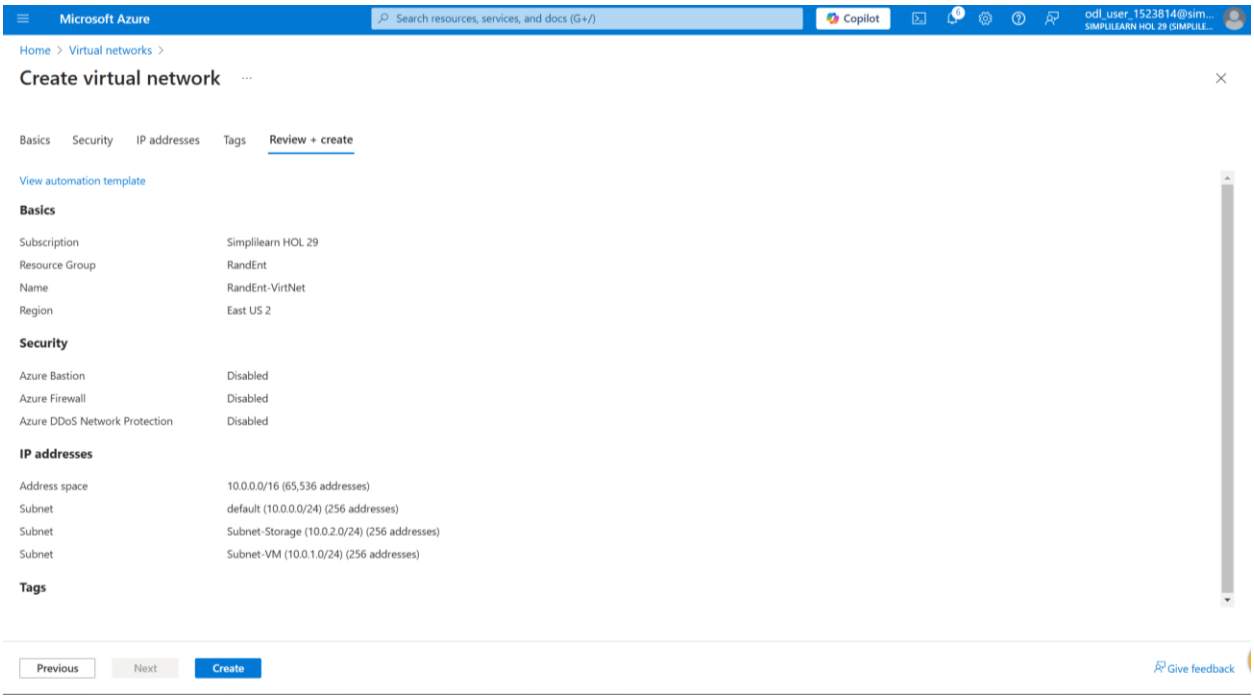
Next create a second subnet for your storage account.



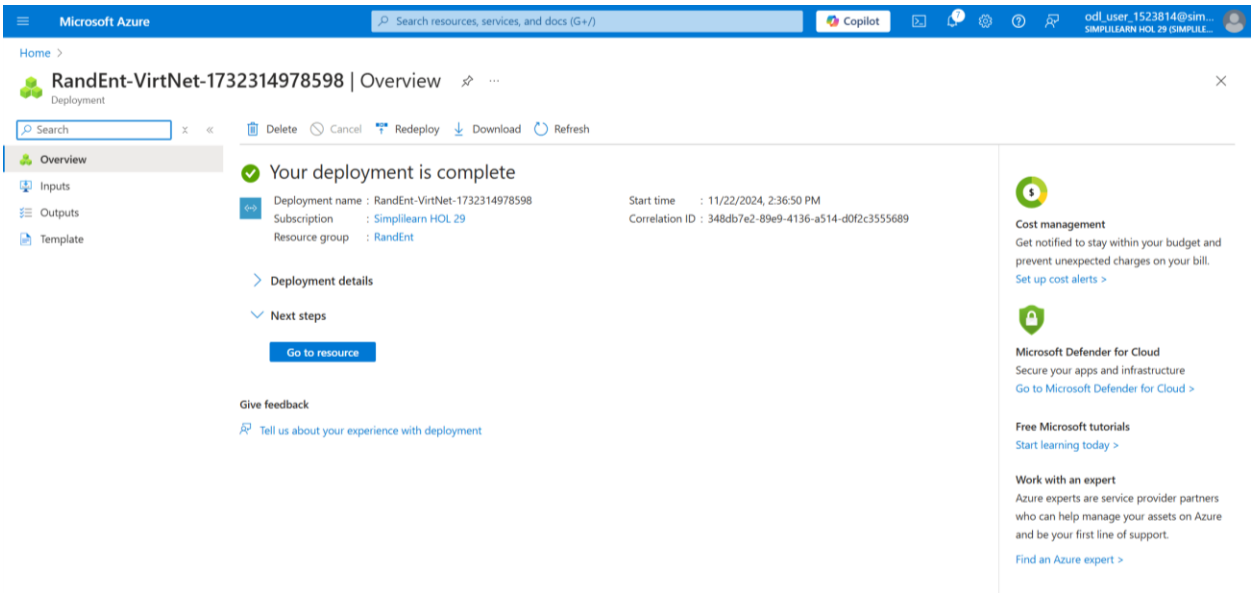
For storage, have subnet at “10.0.2.0/24”. Click on Add.



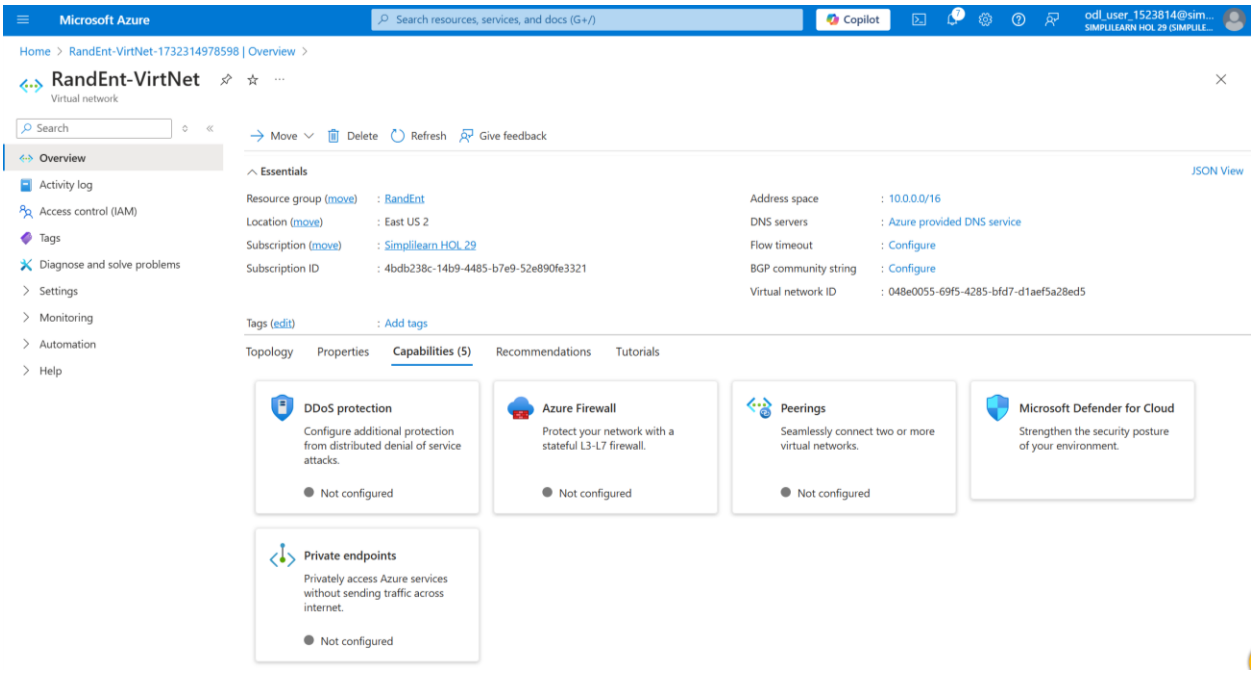
Go to “Review+create”.



Click “Create”.



Your Virtual Network is created.

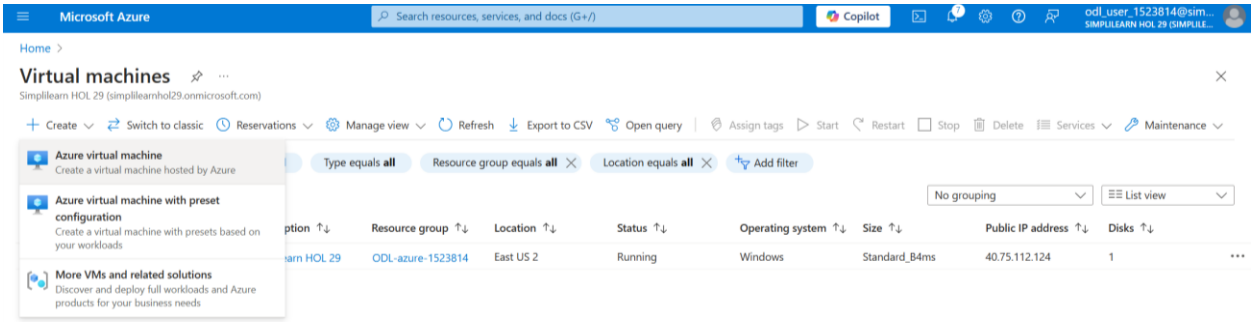


2.2 Create Virtual Machine

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”.

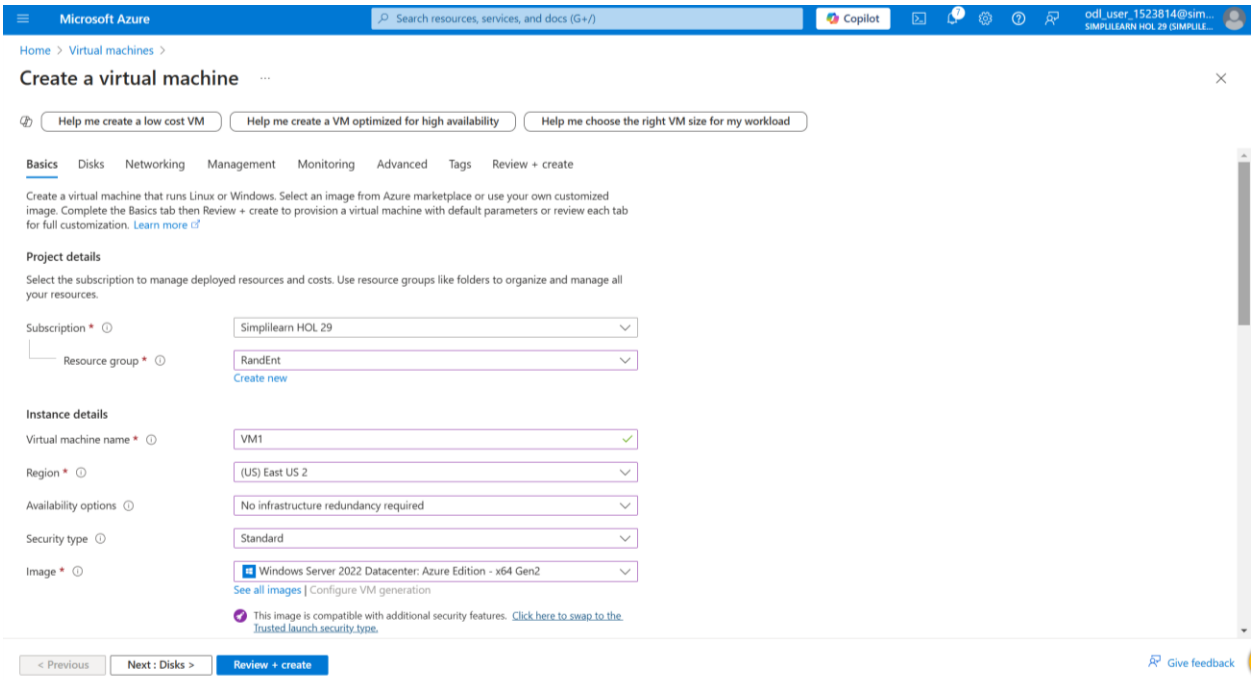


In “Create a virtual machine”:

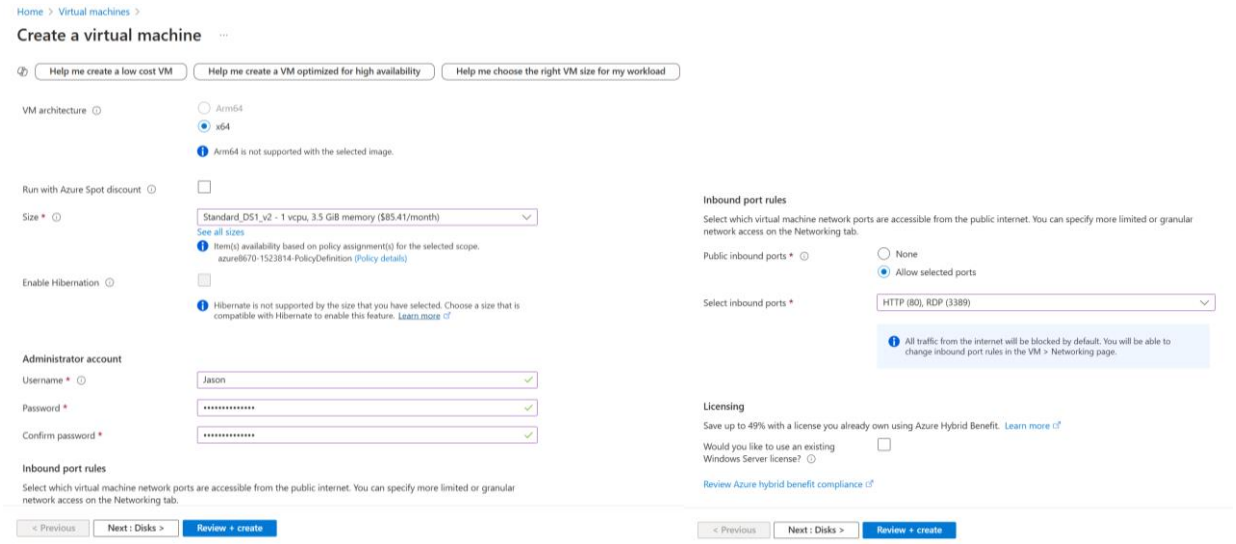
Provide a name for your VM, example “VM1” and be sure the Region is the same as your virtual network (US East 2).

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”.



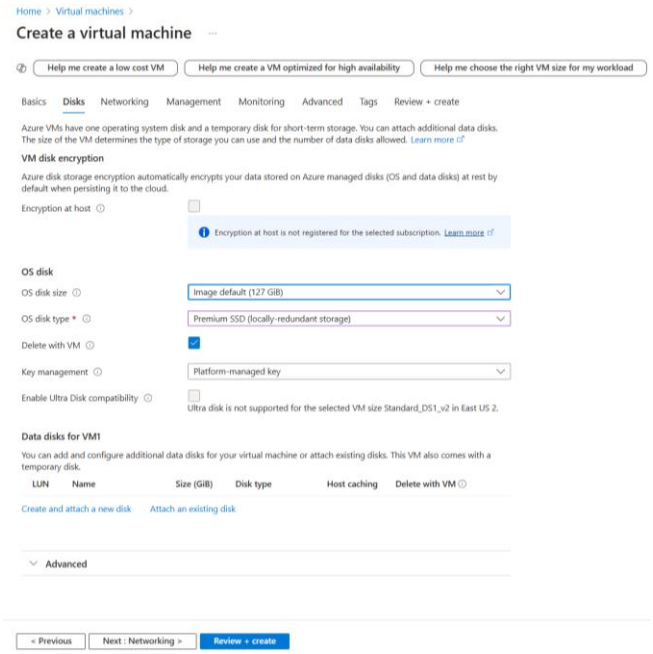
For Size, select “Standard_DS1_v2” or the appropriate size for your VM.



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.

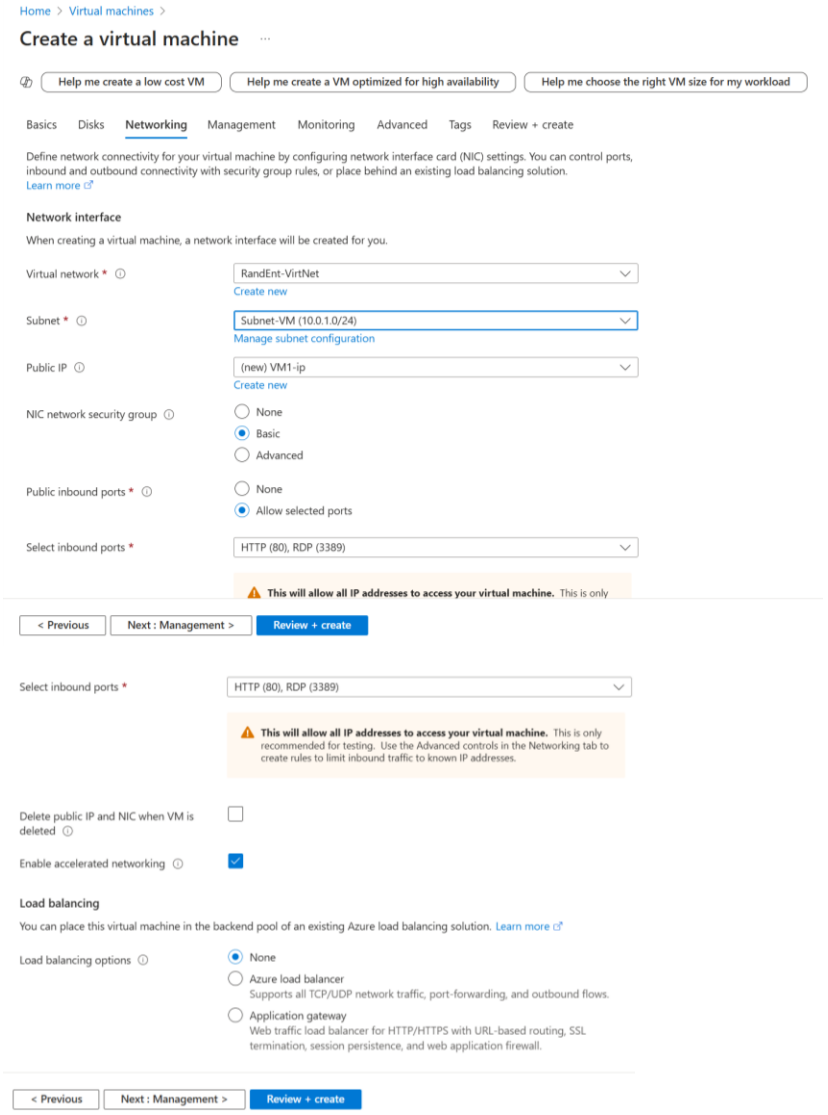
For Disks, leave it at default setting.



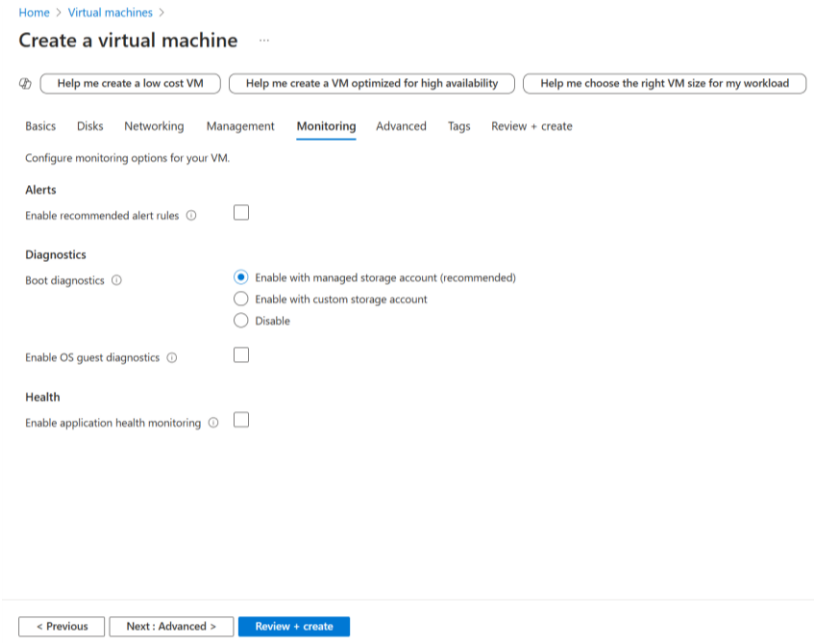
Next click on Networking.

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

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

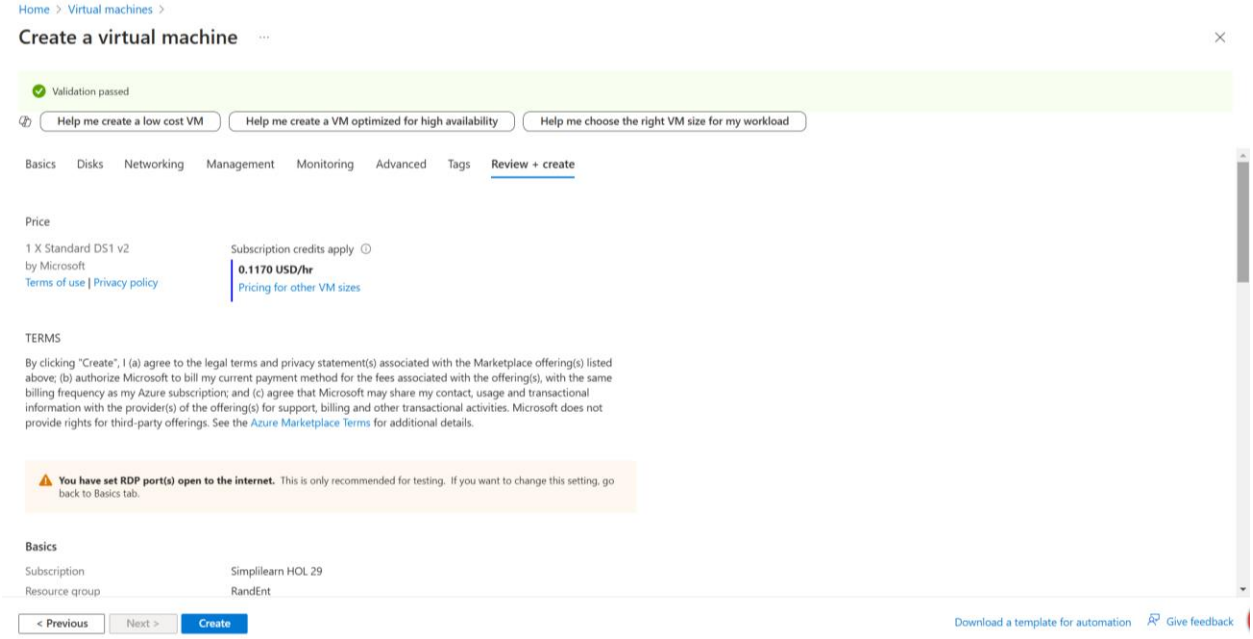


Next in Monitoring.

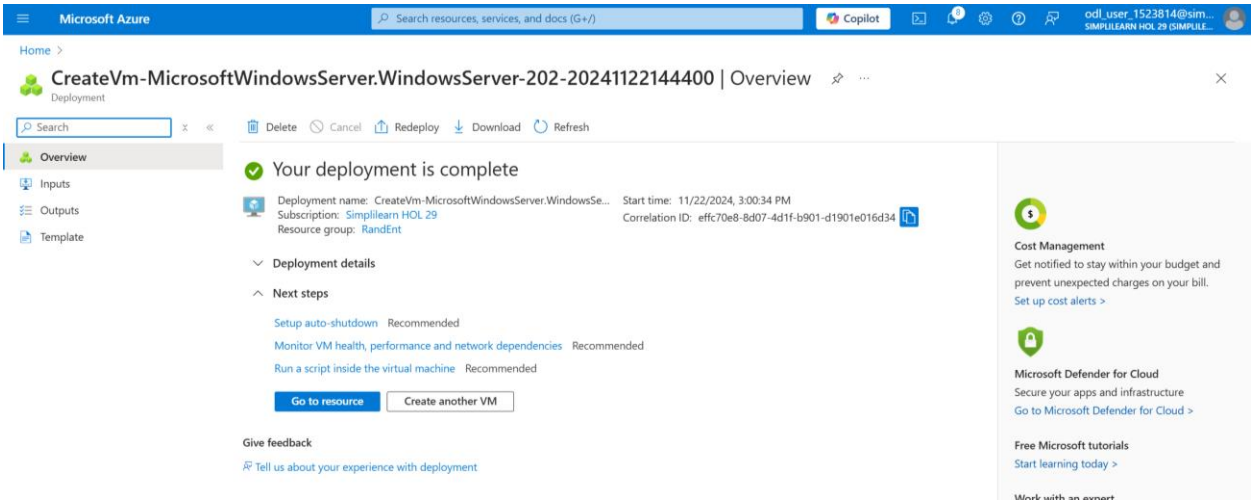


Set Boot Diagnostics to “Enable with managed storage account”.

Click on “Review + Create”.



Click “Create”.



Your Virtual Machine and Virtual Network are ready.

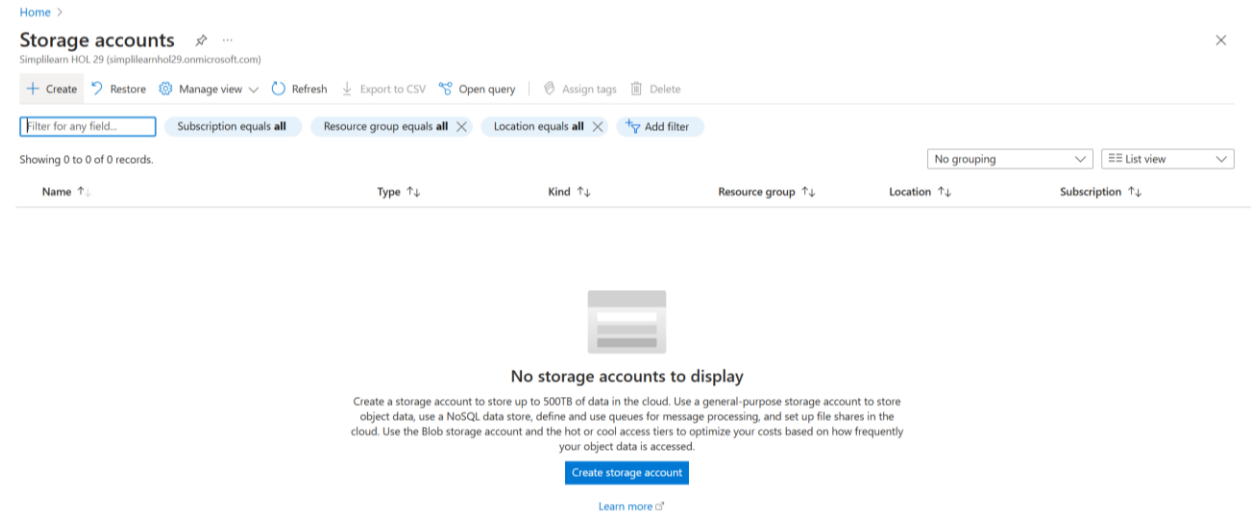
Step 3: Compute & Storage

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”.



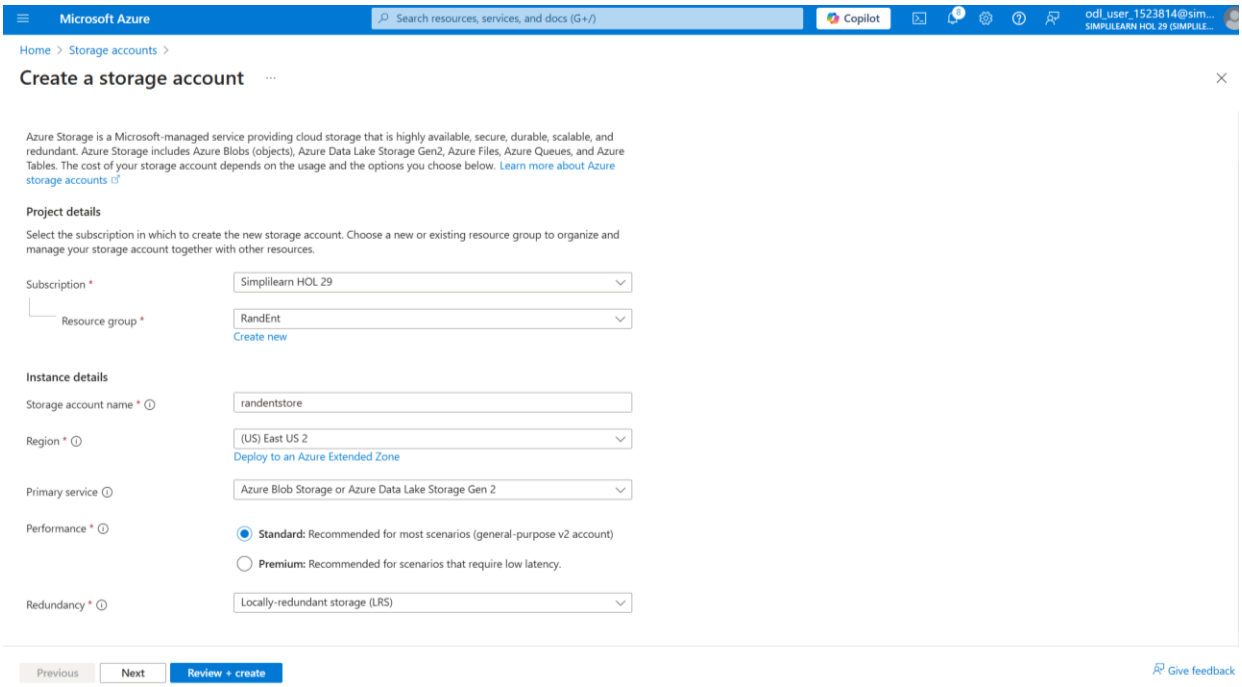
Under Create the Storage Account:

Select your subscription and your resource group.

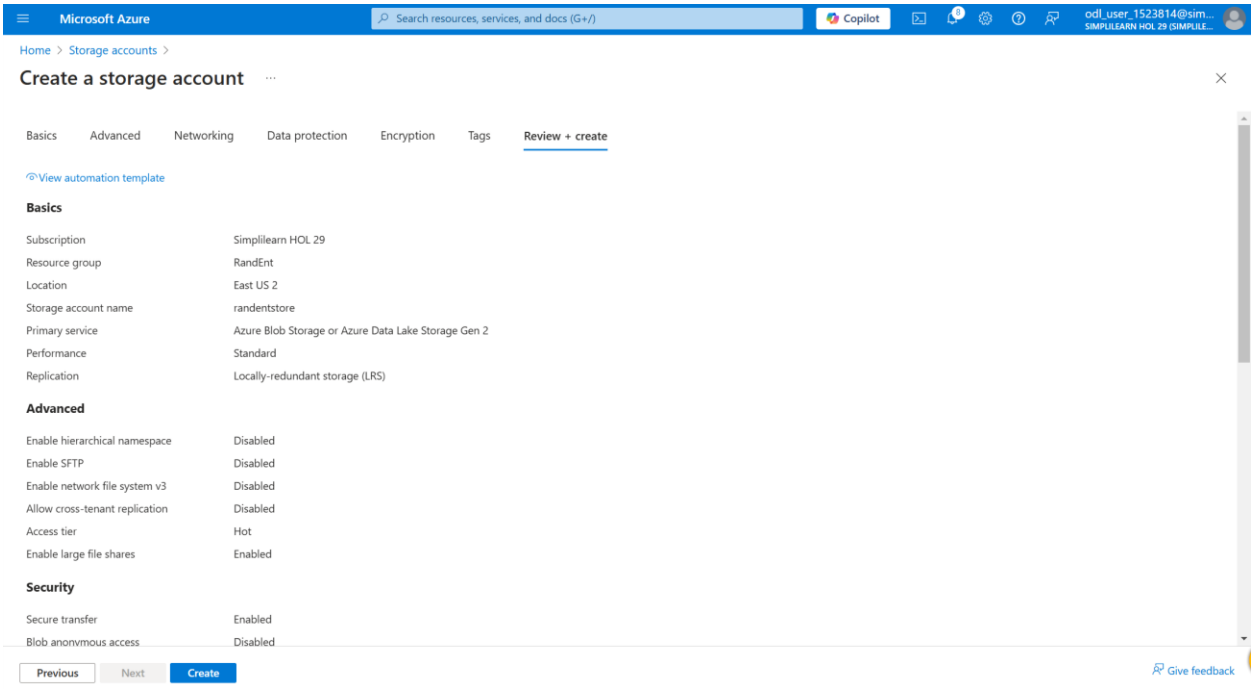
In “Storage Account Name”: Create a unique name. For this demo, it will be called `randentstore`.

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

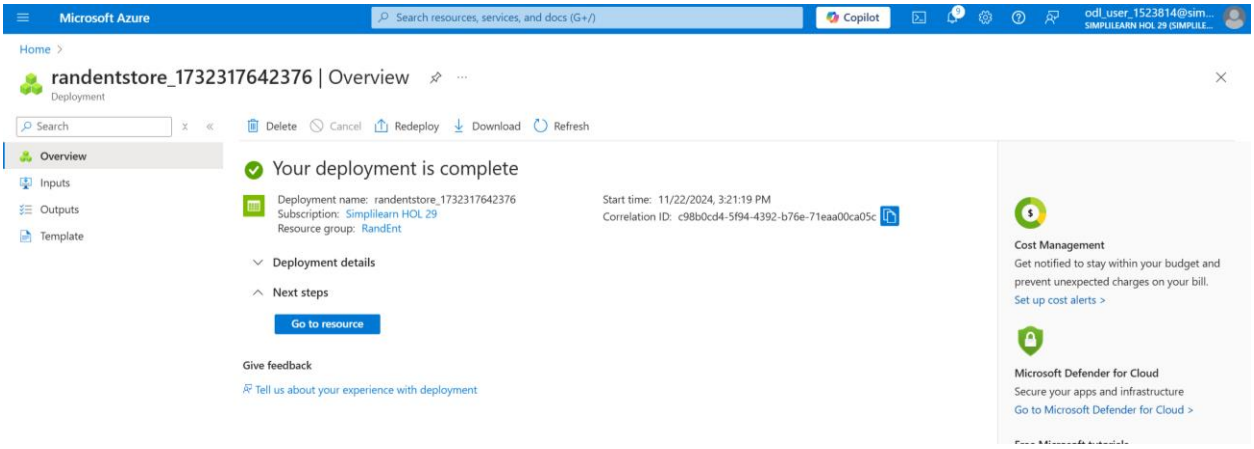
For Performance, choose “Standard”, and for Redundancy choose “Locally redundant storage (LRS)”.



Click “Review + Create”.



Click “Create”.

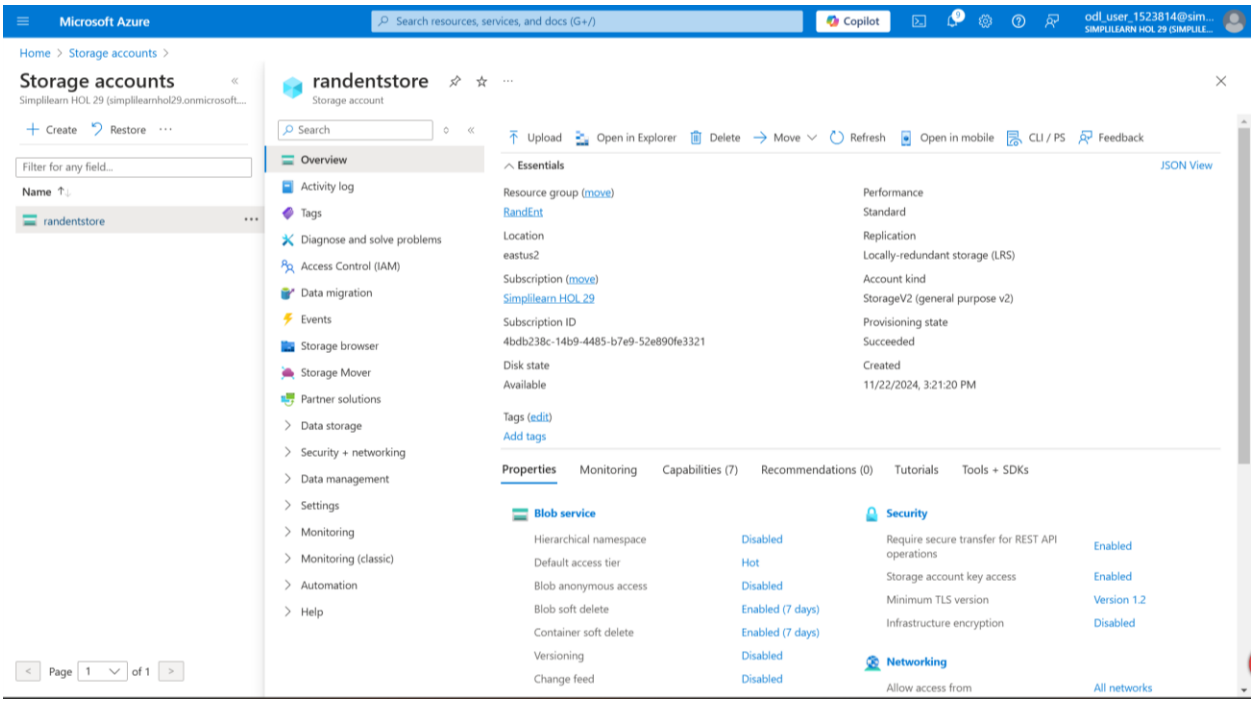


Your Storage Account is created.

3.2: Set Up Service Endpoint for Storage

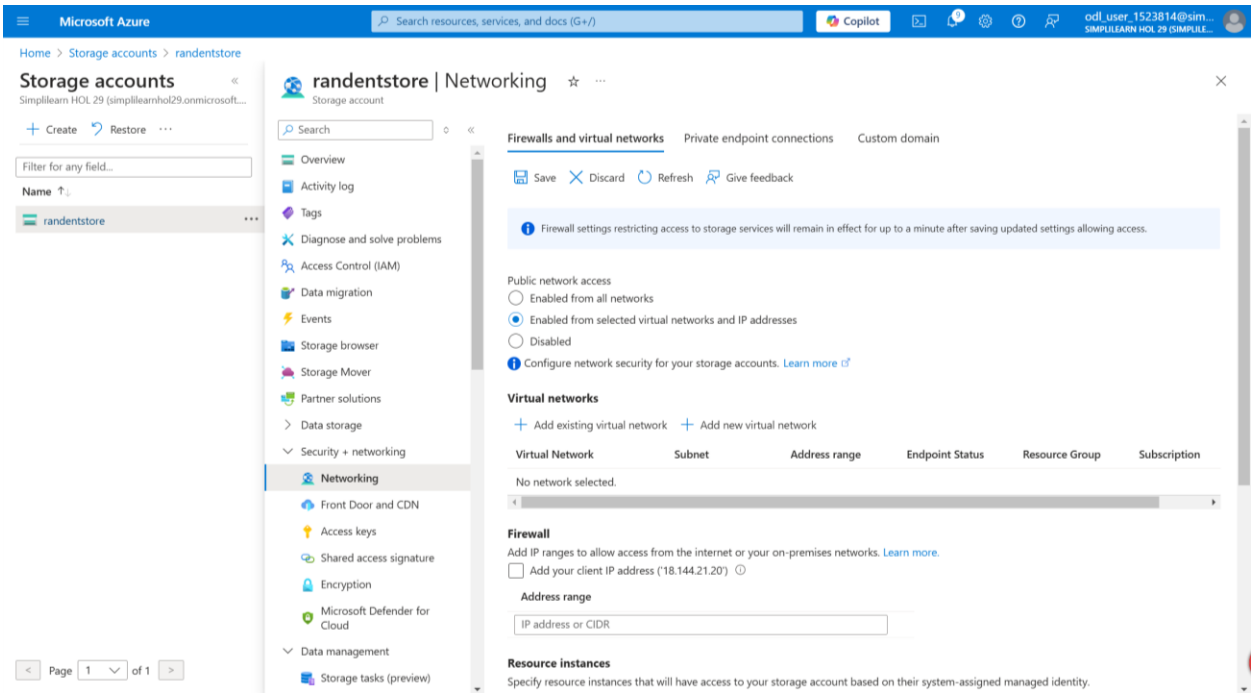
Ensure that the storage account can only be accessed through an internal network of Azure and avoid storage account access to public internet, create a private network by configuring service endpoints.

Select your created storage account.



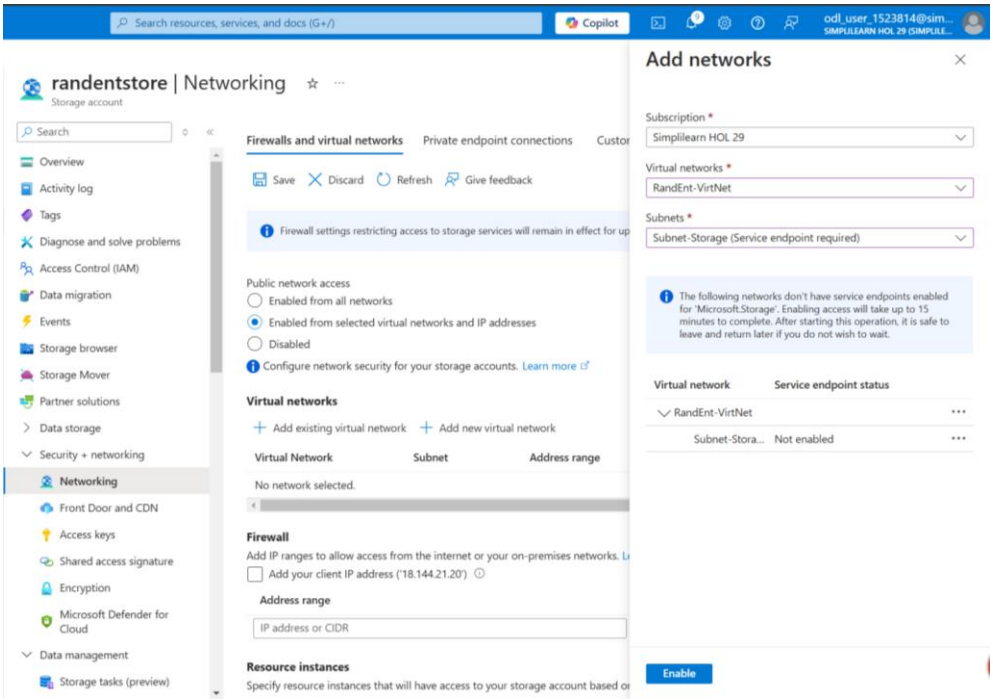
In settings, under “Security + networking”, click and select “Networking”.

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



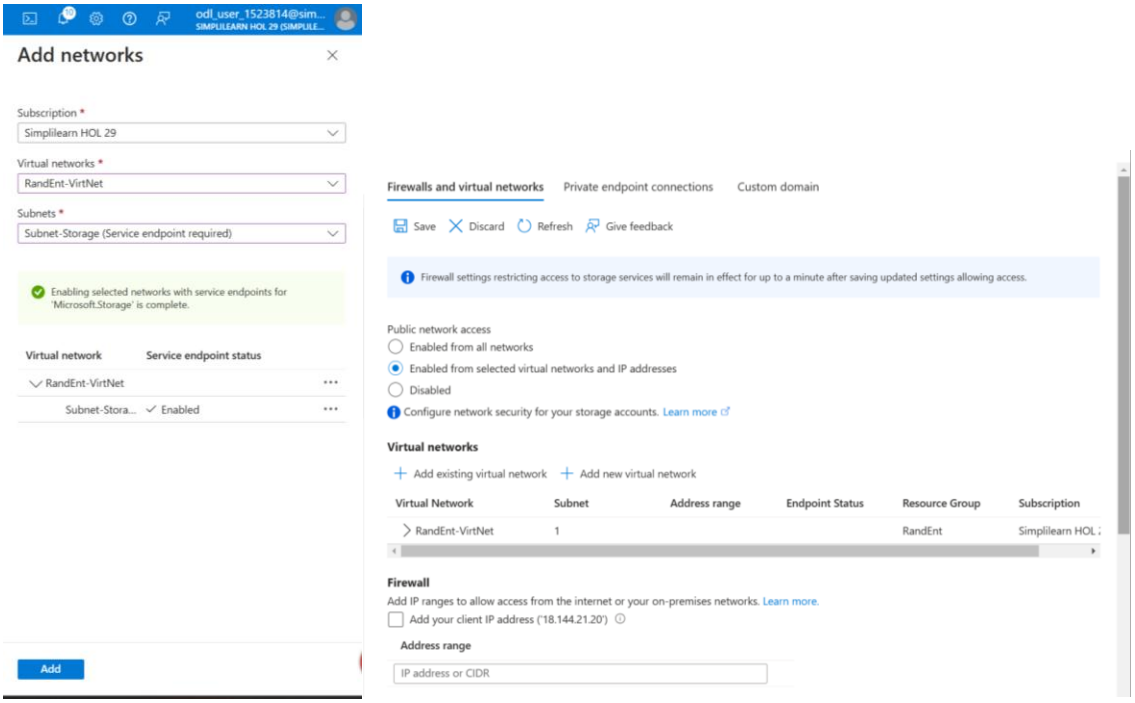
In Firewalls and Virtual Networks tab:

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



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.



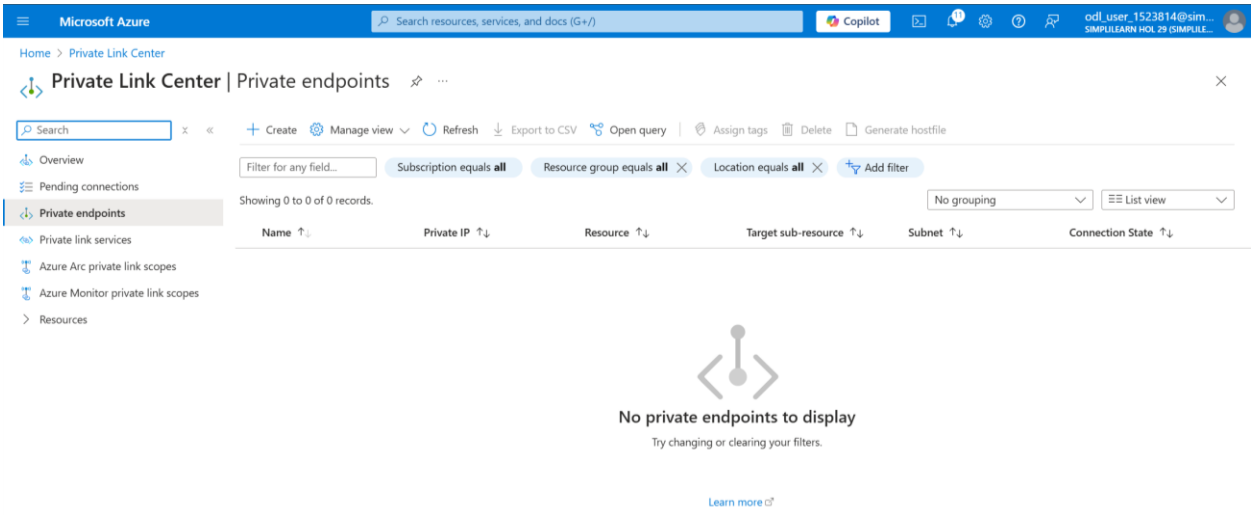
Click on Add. Then click on Save.

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.

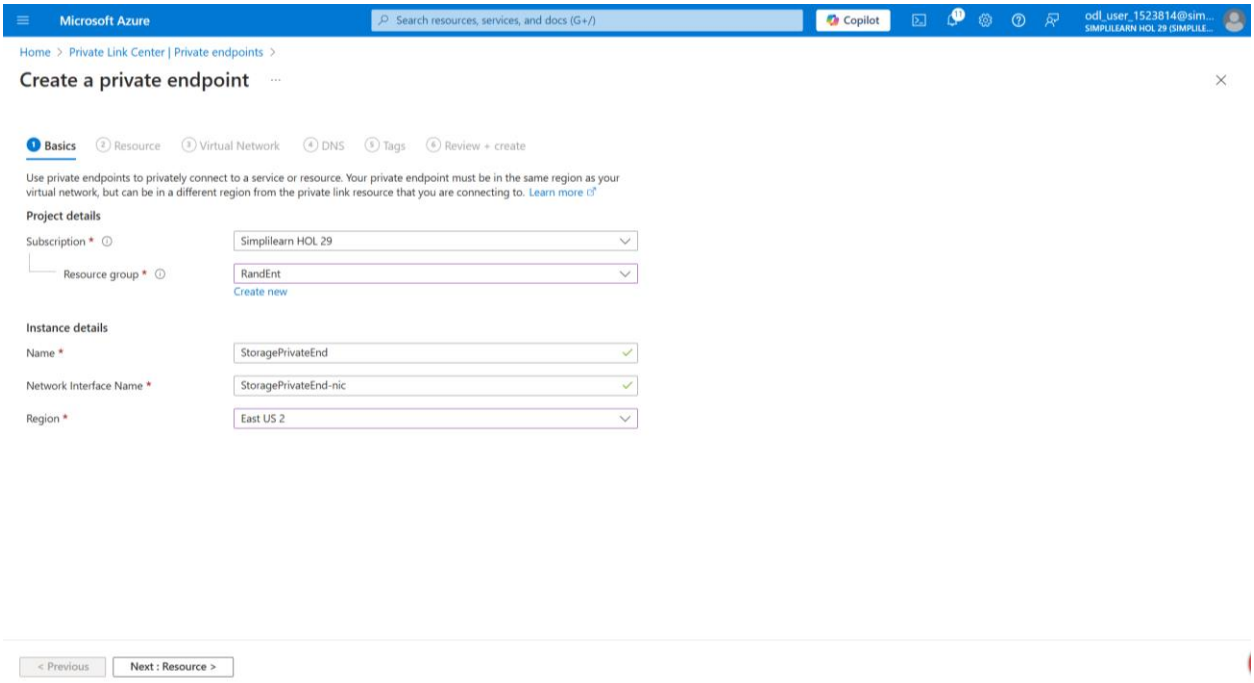
Go to Private endpoints page, then click “+ Create”.



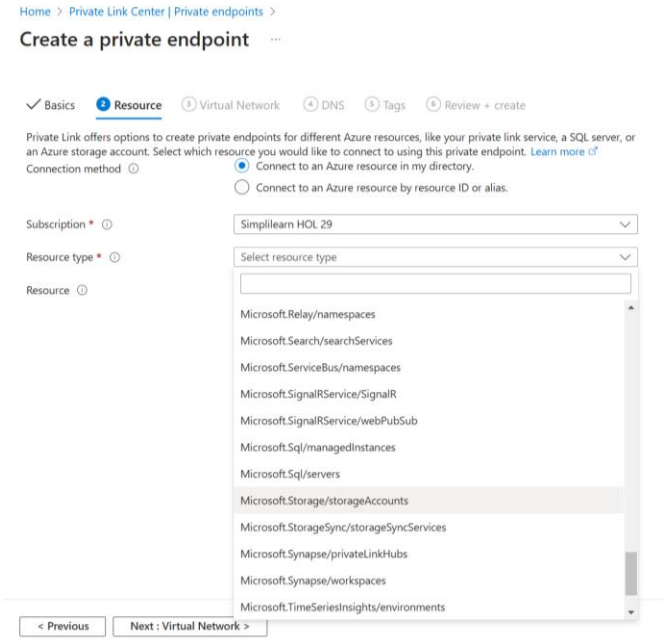
In Create the Private Endpoint:

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

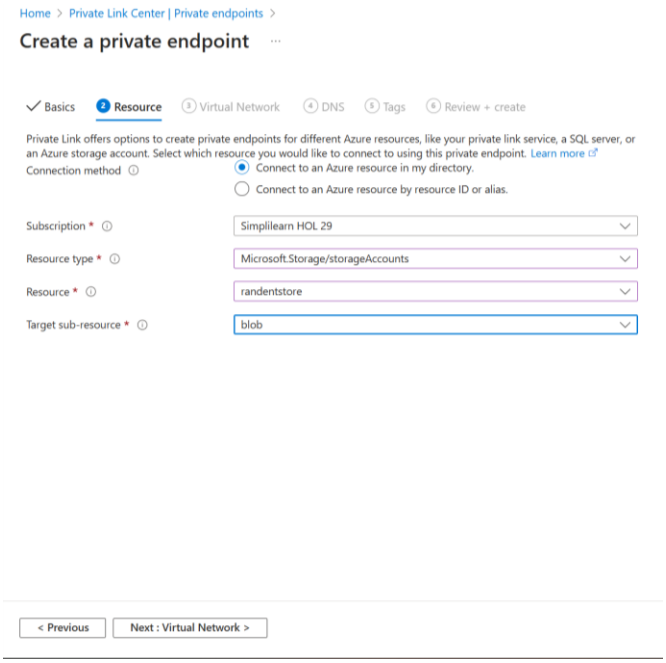
Region is East US 2 as storage account.



Click on Next: Resource.

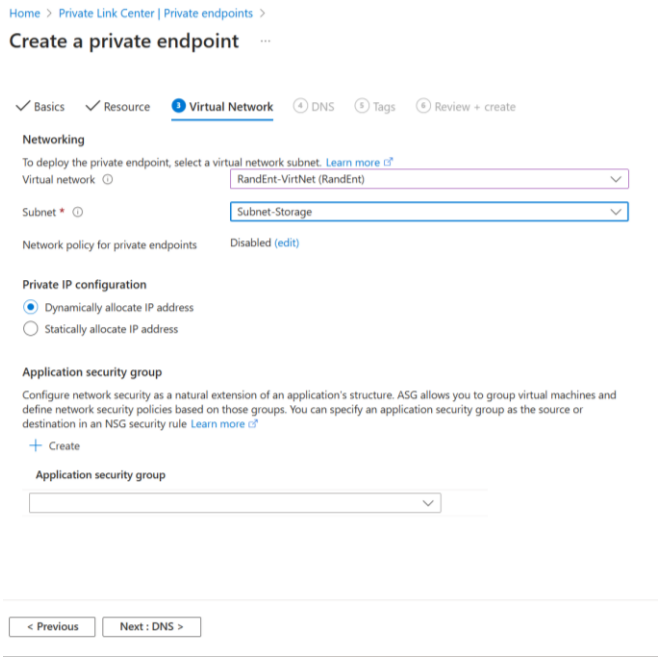


For Resource type, select “Microsoft.Storage/storageAccounts”.

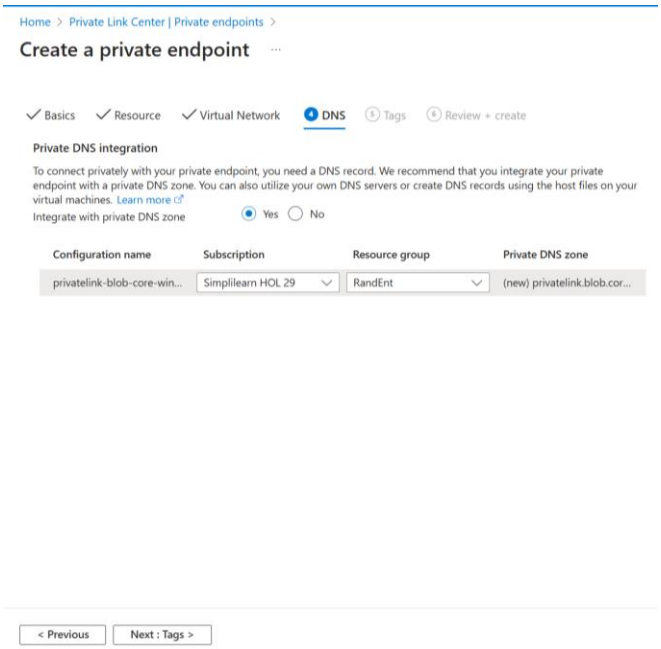


Select your created storage account in Resource and then select “blob” as your target sub-resource.

Next under Virtual Network.

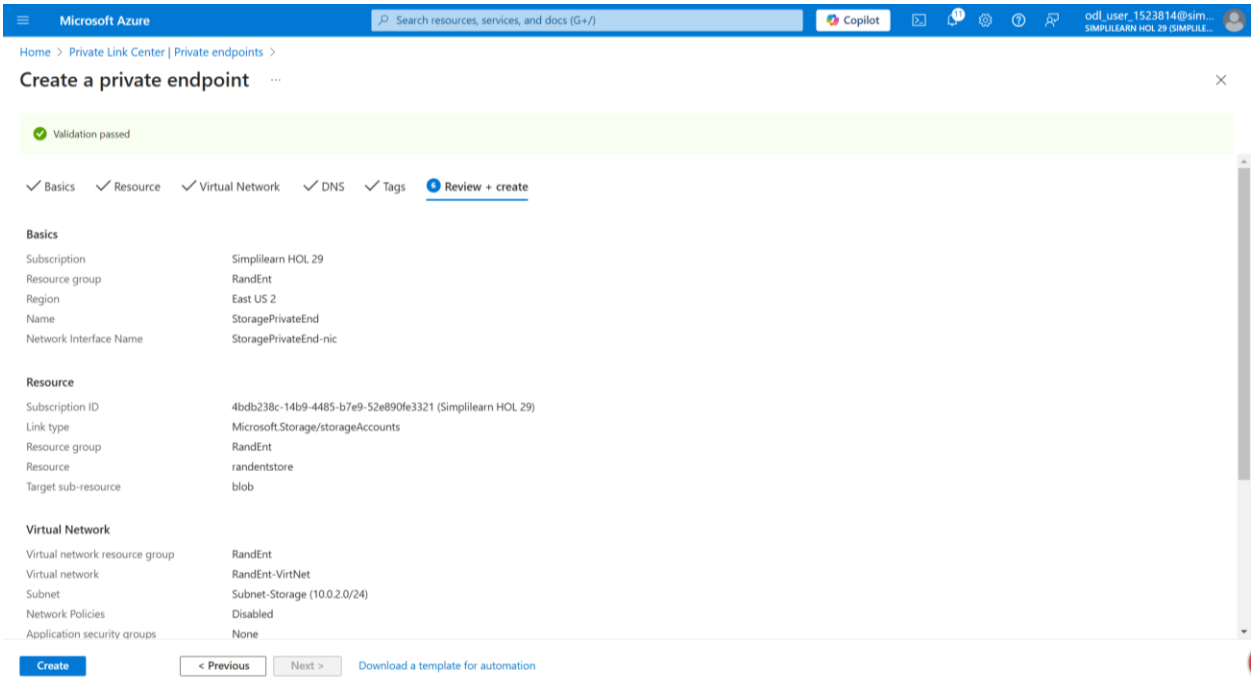


For Subnet, choose the your storage account subnet “storageSubnet”.

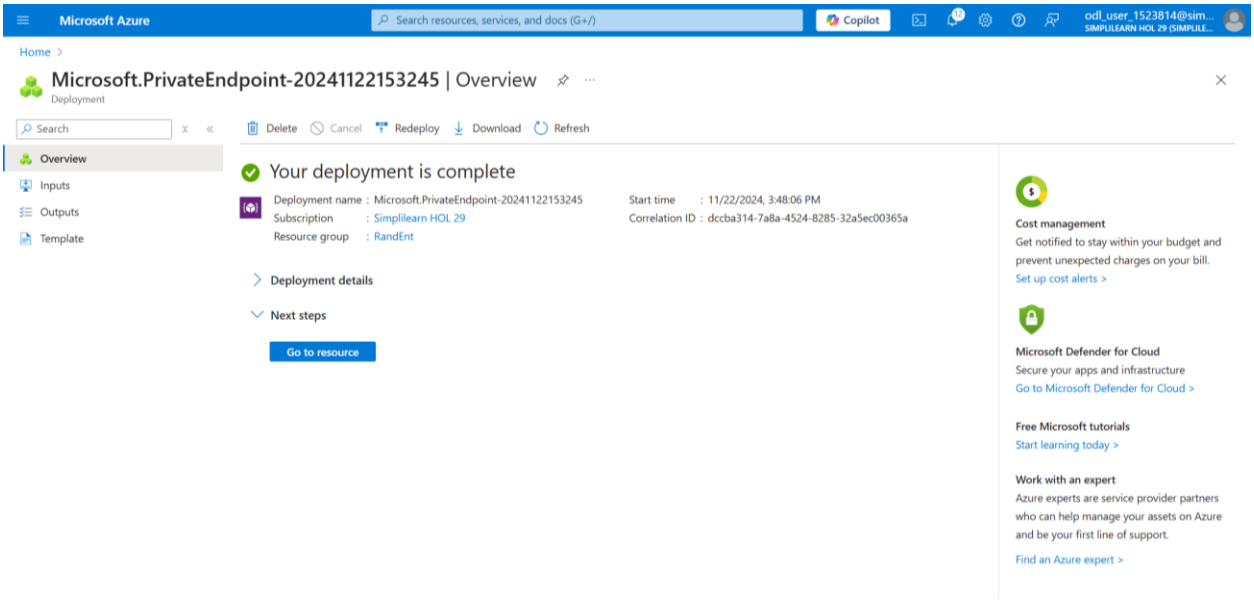


Under DNS. Keep the default setting for your subscription and resource group.

Click “Review + Create”.



Click Create.



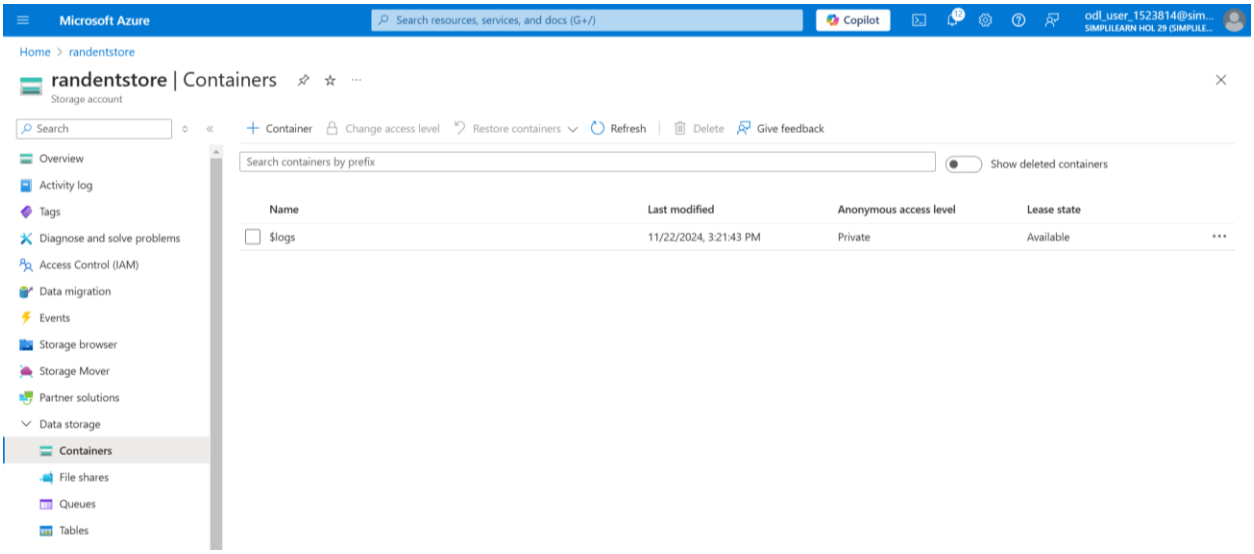
Private Endpoint is created.

4.2: Configure Storage Container for Images

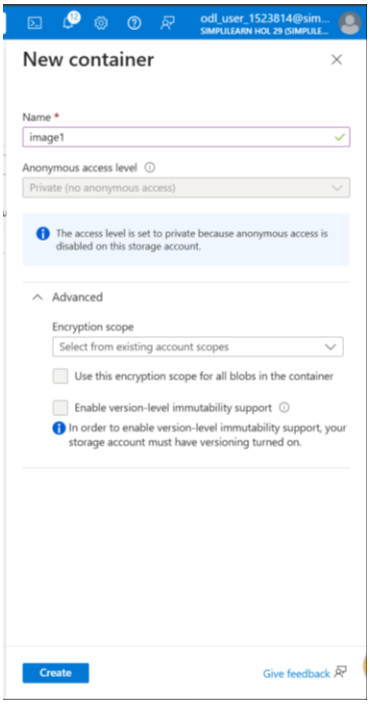
Create a container to hold image-based content in the storage account..

Go to Storage Account and click on your storage account.

In settings under Data Storage, click on Containers.



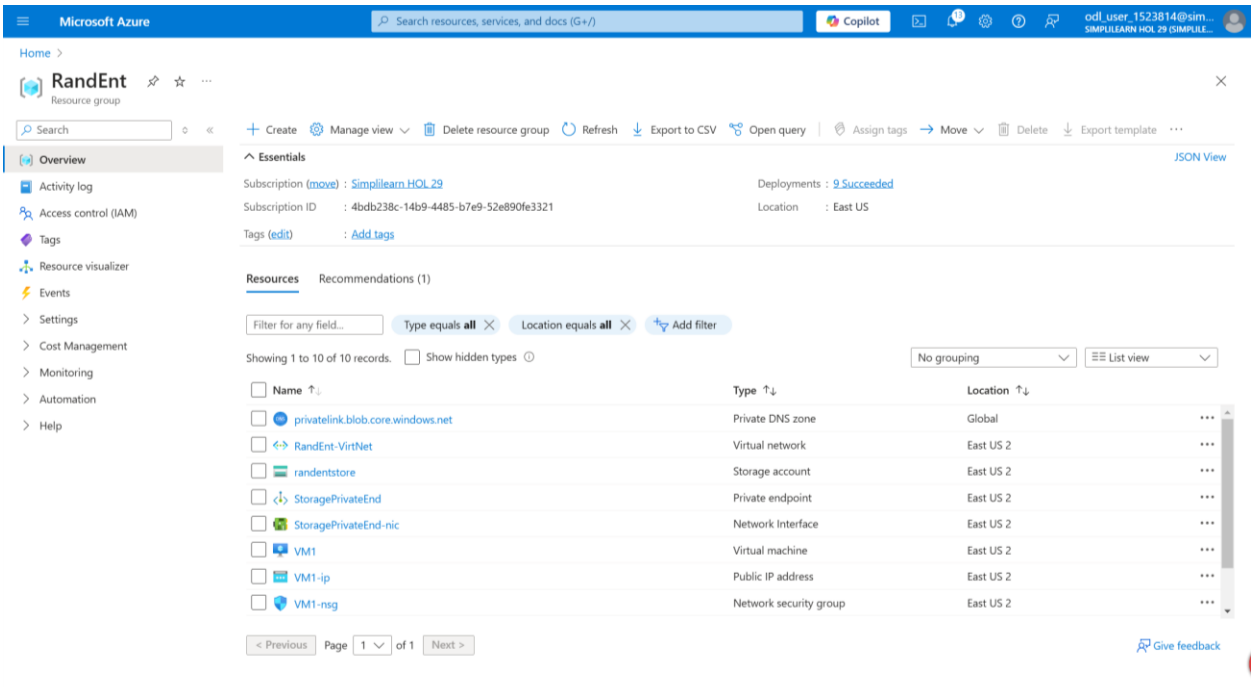
Click “+ Container”.



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”.



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