Project 2: 02-Azure Networking and Storage

Overview

This project demonstrates how to configure networking and storage services in Microsoft Azure.

The goal is to create secure, scalable network environments and properly configured storage accounts.

Objectives

- Deploy a Virtual Machine (VM) in Azure.
- Configure SSH key authentication for secure access.
- Open necessary network ports.
- Connect to the VM securely.
- Install and configure basic services (e.g., NGINX).
- Demonstrate best practices in identity and security management.

Project Tasks

🚀 Task 1: Configure a Virtual Network (VNet)

1. **Sign in to the Azure Portal.**
2. **Navigate to Virtual Networks > + Create.**
3. **Select the Subscription and Resource Group.**
4. **Name your VNet (e.g., MyVNet) and select a region.**
5. **Add subnets (e.g., Frontend Subnet, Backend Subnet).**
6. **Review and create the VNet.**

🚀 Step 2: Create a Network Security Group (NSG)

1. **Go to Network Security Groups > + Create.**
2. **Fill in the NSG name and associate it with the appropriate subnet.**
3. **Add inbound/outbound security rules to control traffic.**
4. **Associate the NSG with your VNet's subnet or network interface.**

🚀 Step 3: Set Up Azure Storage Account

1. **Navigate to Storage accounts > + Create.**
2. **Choose the resource group, name your storage account, and select a region.**
3. **Choose the Standard or Premium performance tier.**
4. **Enable Blob, File, Queue, or Table storage based on requirements.**
5. **Review and create the storage account.**

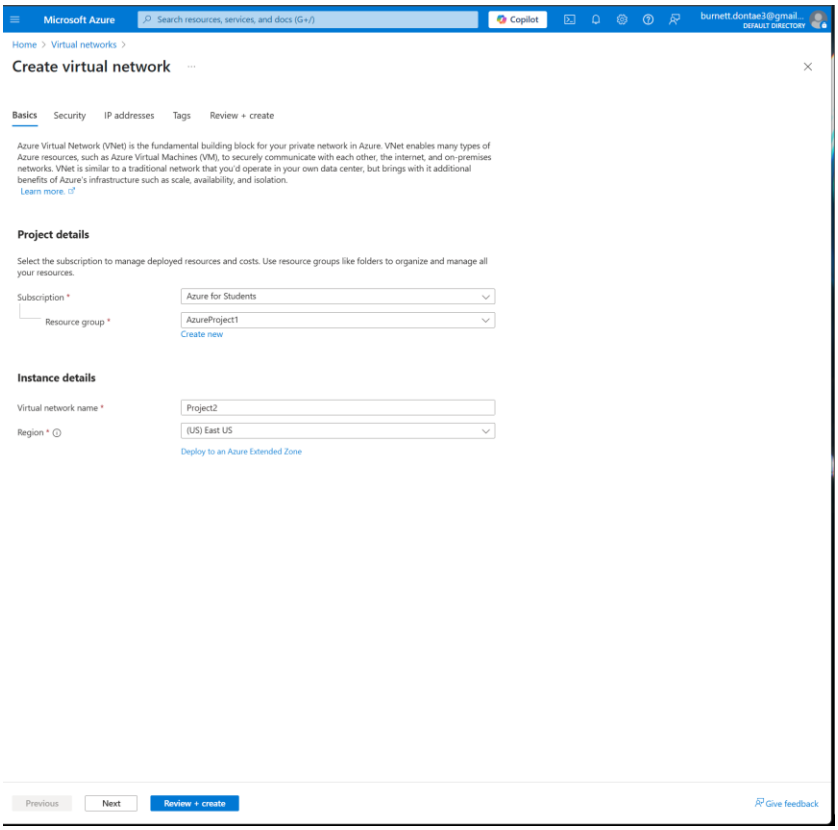
🚀 Step 4: Upload and Access Data

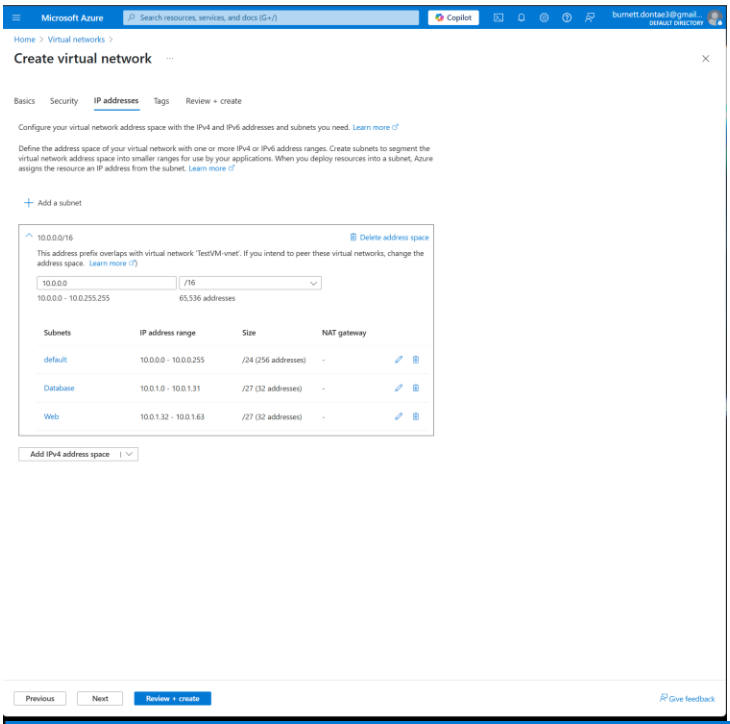
1. **Open the storage account and go to Containers.**
2. **Create a new container (e.g., project2data).**
3. **Upload sample files and test access using Azure Storage Explorer or SAS token.**

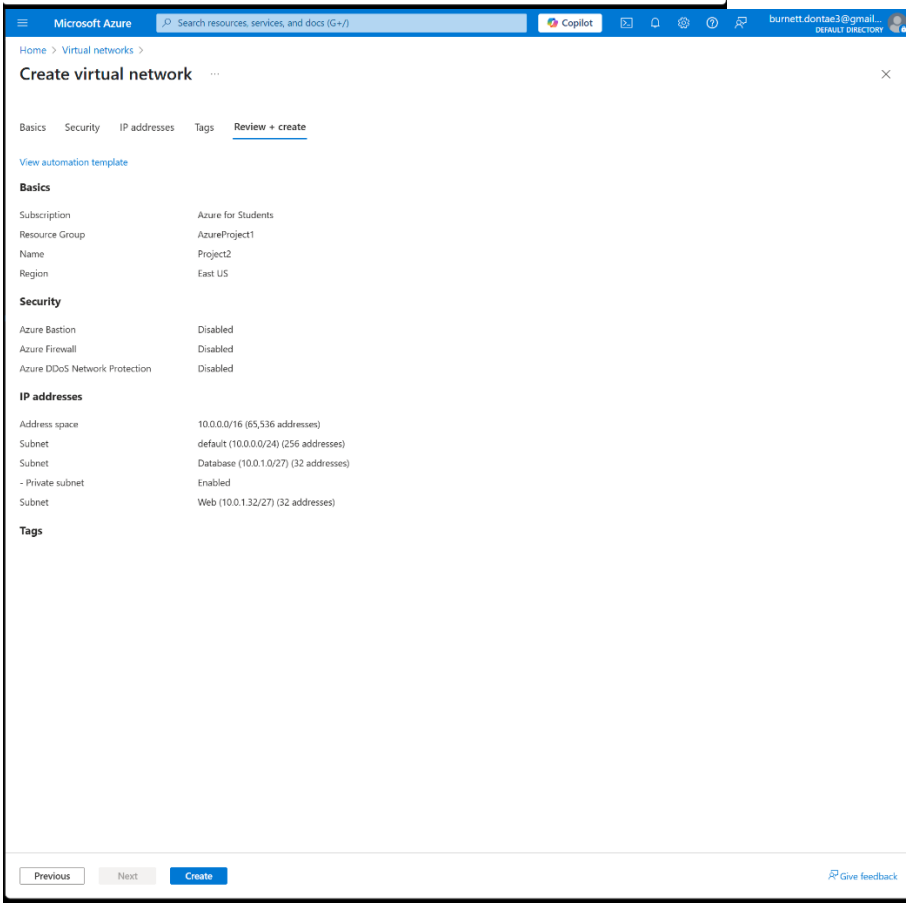
Steps 1 Creating the VNet

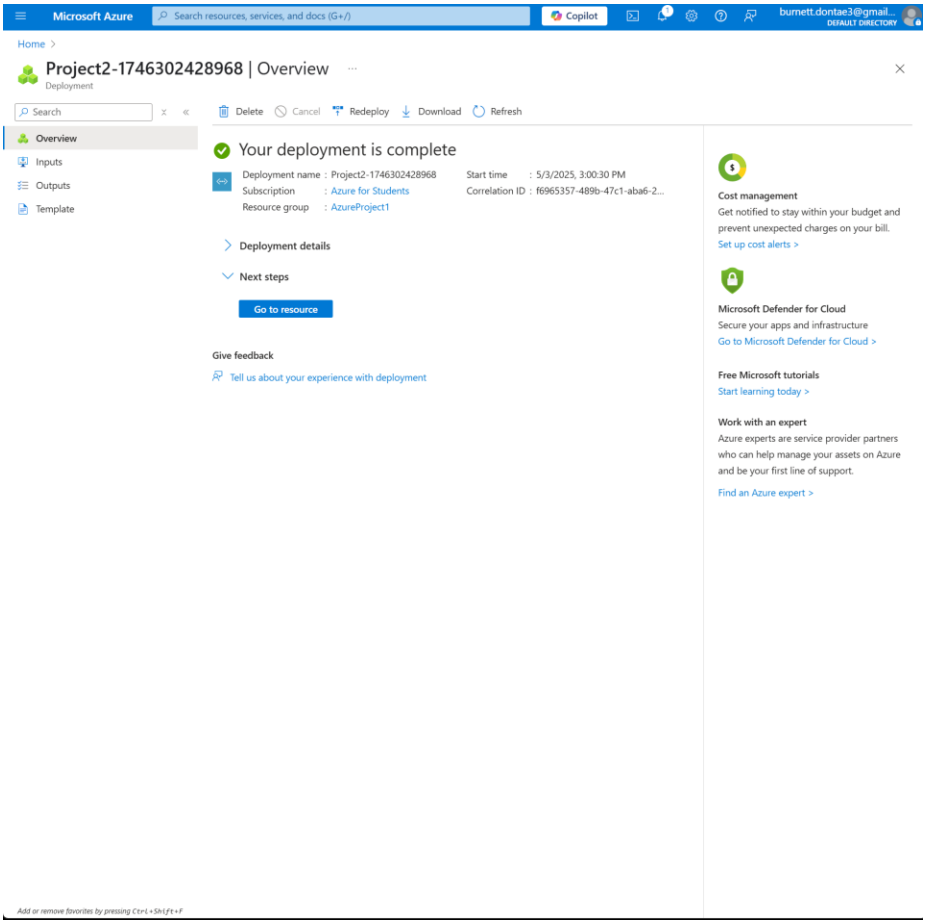
1. Go to Azure Portal > Virtual Networks > Create.
2. **Add two subnets: "Web" and "Database".**
    - Subnet > Name “Database” > IPv4 > 10.0.0.0 > /27 Size > Enable private subnet > Enable Service Endpoints for Microsoft. Storage for secure access.
    - Add a Subnet > Name “Web” > IPv4 > 10.0.1.0 > /27 Size.
    - Review and create.

3. Azure automatically sets up **intra-VNet communication**.
4. Subnets within the same VNet can communicate directly by default.



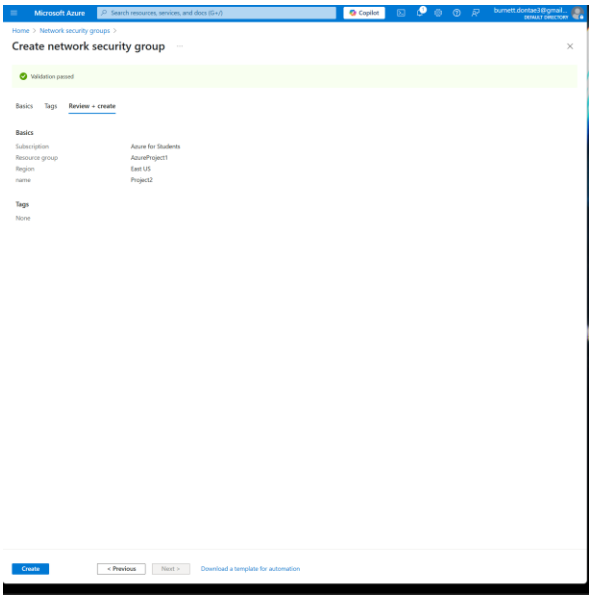

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
burnett.dontae3@gmail...
DEFAULT DIRECTORY
Home > Virtual networks >
Create virtual network
Basics Security IP addresses Tags Review + create
Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. Learn more
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
10.0.0.0/16
Delete address space
This address prefix overlaps with virtual network 'TestVM-vnet'. If you intend to peer these virtual networks, change the address space. Learn more
10.0.0.0
/16
10.0.0.0 - 10.0.255.255
65,536 addresses
Subnets
IP address range
Size
NAT gateway
default
10.0.0.0 - 10.0.0.255
/24 (256 addresses)
-
Database
10.0.1.0 - 10.0.1.31
/27 (32 addresses)
-
Web
10.0.1.32 - 10.0.1.63
/27 (32 addresses)
-
Add IPv4 address space
Previous
Next
Review + create
Give feedback

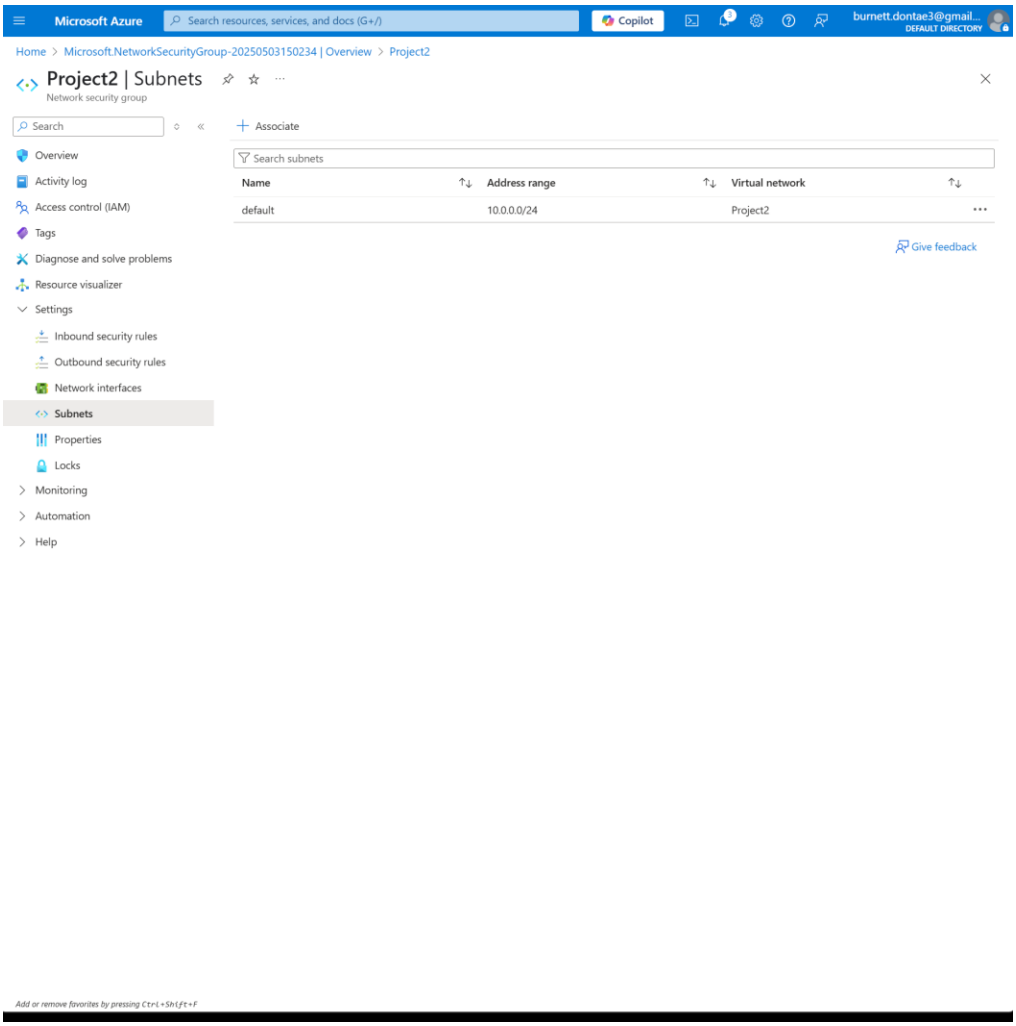

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
burnett.dontae3@gmail...
DEFAULT DIRECTORY
Home > Virtual networks >
Create virtual network
Basics Security IP addresses Tags Review + create
View automation template
Basics
Subscription Azure for Students
Resource Group AzureProject1
Name Project2
Region East US
Security
Azure Bastion Disabled
Azure Firewall Disabled
Azure DDoS Network Protection Disabled
IP addresses
Address space 10.0.0.0/16 (65,536 addresses)
Subnet default (10.0.0.0/24) (256 addresses)
Subnet Database (10.0.1.0/27) (32 addresses)
- Private subnet Enabled
Subnet Web (10.0.1.32/27) (32 addresses)
Tags
Previous
Next
Create
Give feedback



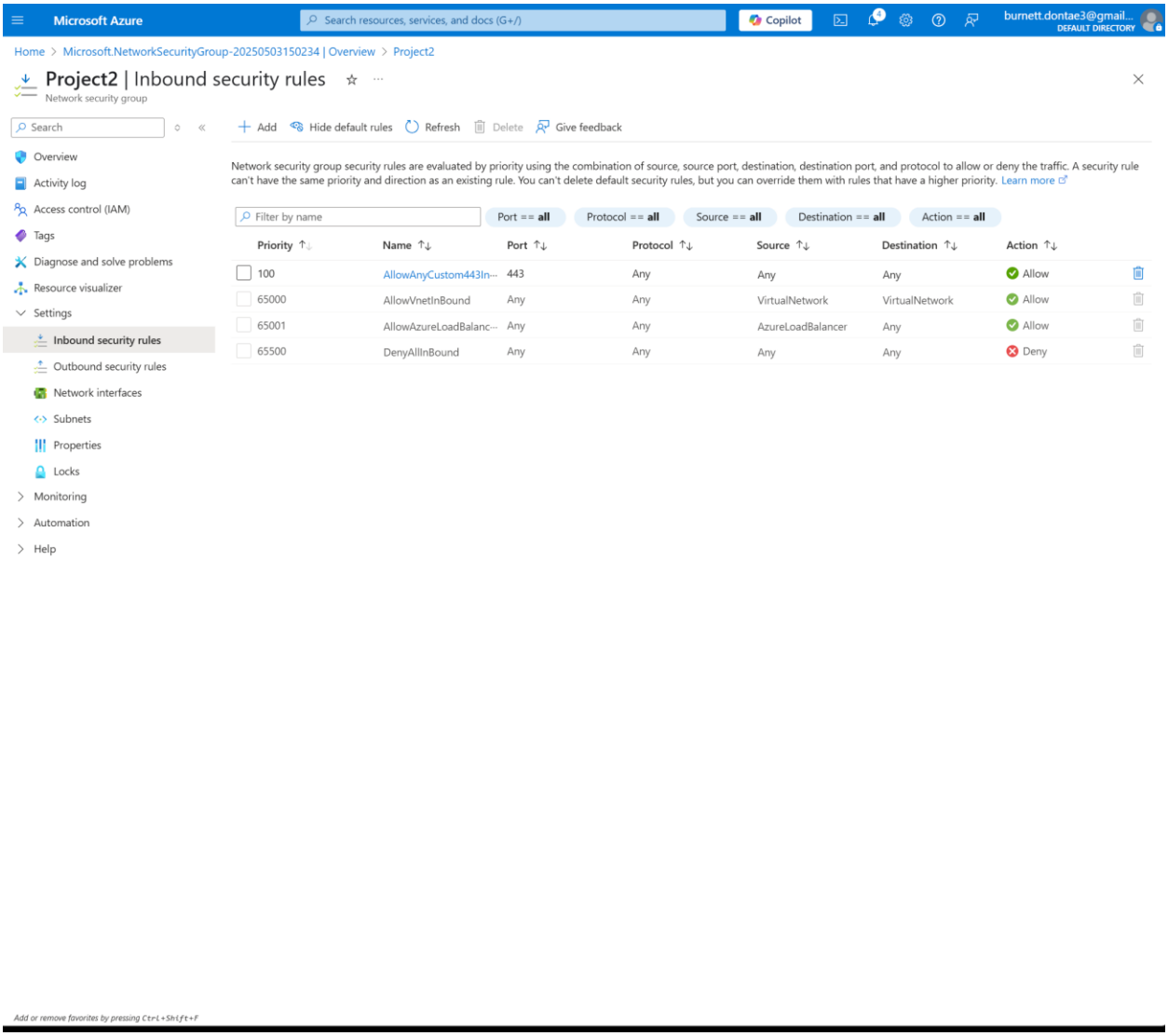
Step 2 Deploy a Network Security Group (NSG)

1. Navigate to Network Security Groups > Create.
2. Associate it with the "Web" subnet.


Microsoft Azure
Copilot
Home > Network security groups >
Create network security group
Validation passed
Basics
Tags
Review + create
Basics
Subscription
Azure for Students
Resource group
AzureProject1
Region
East US
name
Project2
Tags
None
Create
< Previous
Next >
Download a template for automation

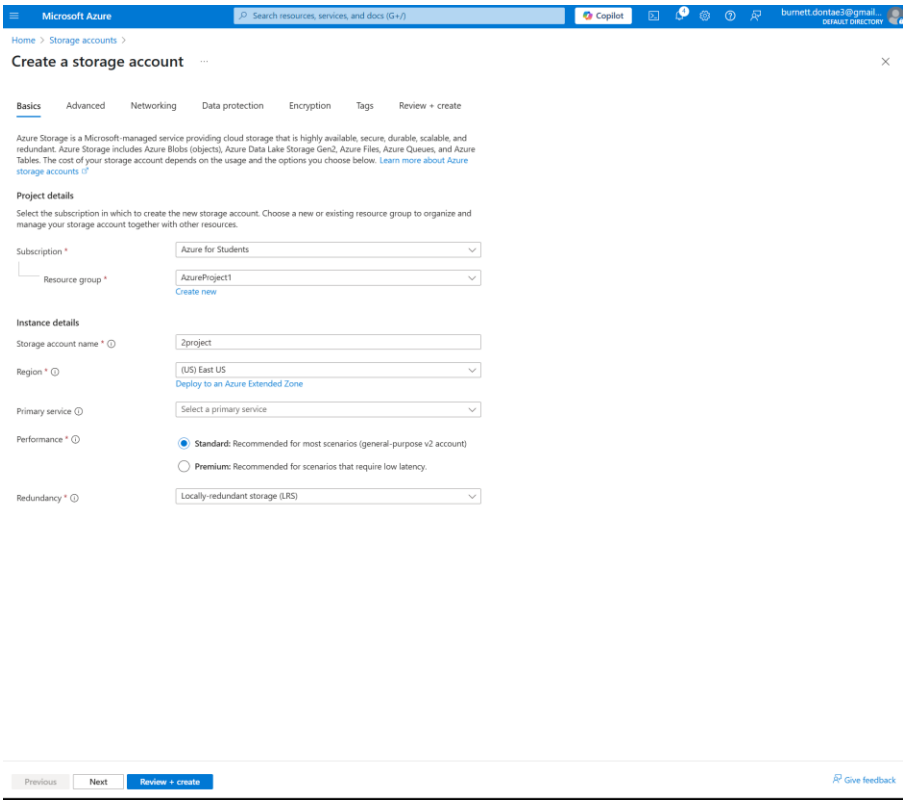

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
burnett.dontae3@gmail...
DEFAULT DIRECTORY
Home > MicrosoftNetworkSecurityGroup-20250503150234 | Overview > Project2
Project2 | Subnets
Network security group
Search
Associate
Search subnets
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Settings
Inbound security rules
Outbound security rules
Network interfaces
Subnets
Properties
Locks
Monitoring
Automation
Help
Name
Address range
Virtual network
default
10.0.0.0/24
Project2
Give feedback
Add or remove favorites by pressing Ctrl+Shift+F

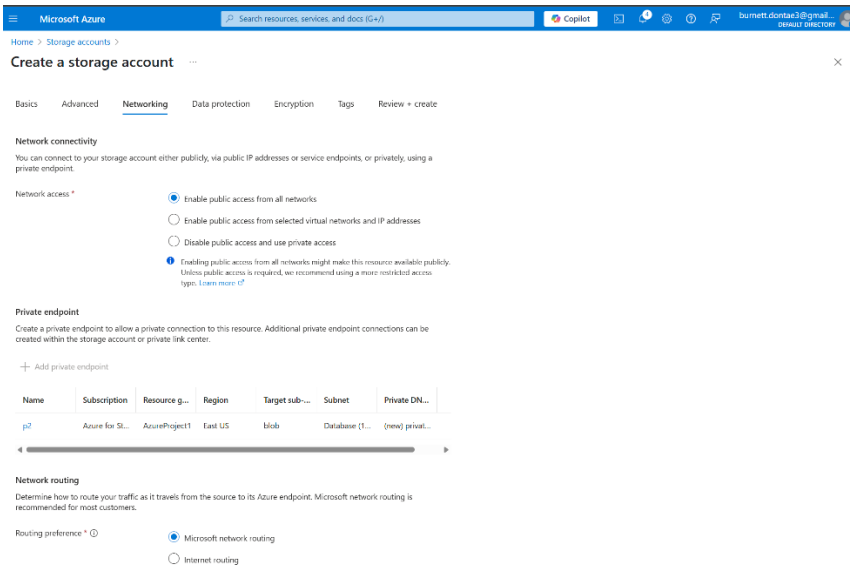
3. **Add inbound rules:**
    - Allow HTTPS (443) traffic from the internet.
        - Now go to Inbound security rules > Add > Destination port 443 / Service HTTPS > Add
    - Block all other inbound internet traffic (except Azure services if needed).
        - Add > Destination port * > Add
        - If you need to allow any specific ports like SSH / RDP then just add them as an increased priority
        - Note that you can't modify the default ones but you can override them with a higher priority; AllowVnetInBound, AllowAzureLoadBalancerInBound, DenyAllInBound

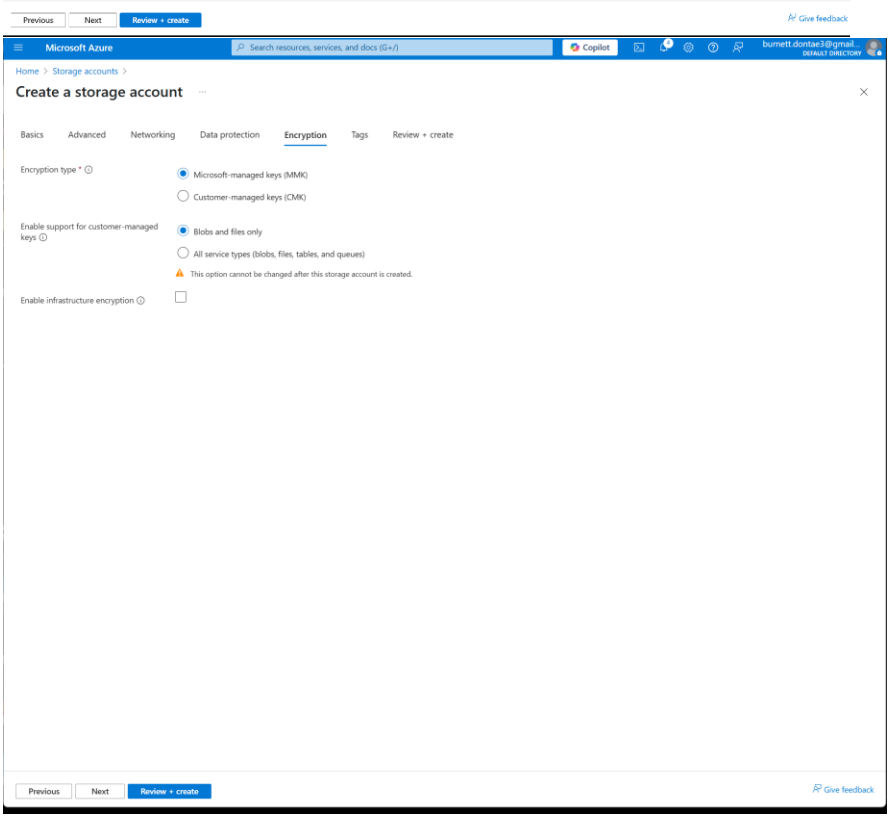


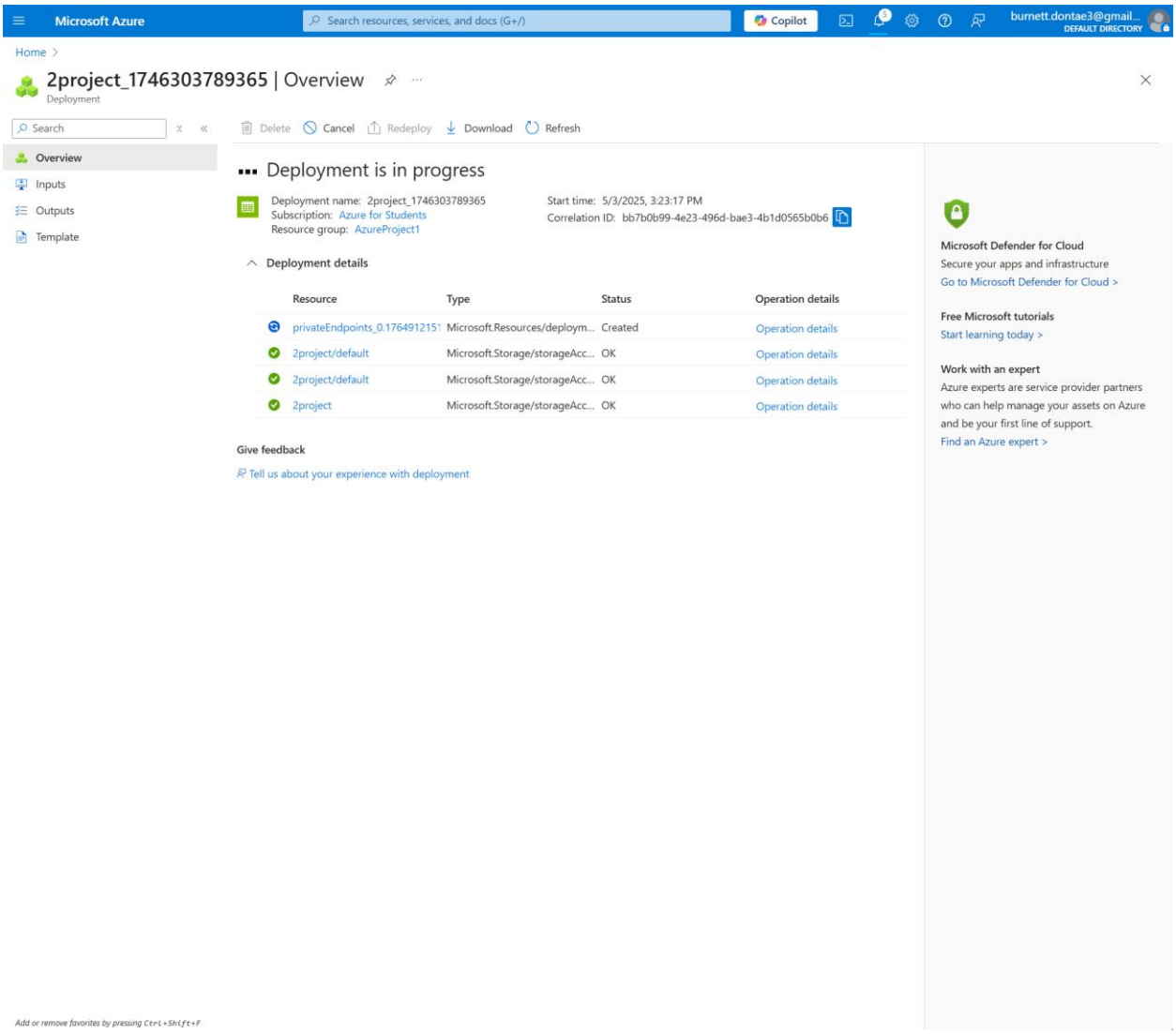
4. Create and Configure a Storage Account

- Navigate to **Storage Accounts** > **Create**.
- Configure:
    - **Replication**: Choose locally redundant storage (LRS) or geo-redundant storage (GRS).
    - **Private Endpoint**: Ensure secure access from the database subnet.
        - Go to Advanced > Permitted scope… From storage accounts that have a private endpoint… > Next
        - Disable public access > Add private endpoint > Select database subnet
    - **Encryption**: Use Microsoft-managed keys.



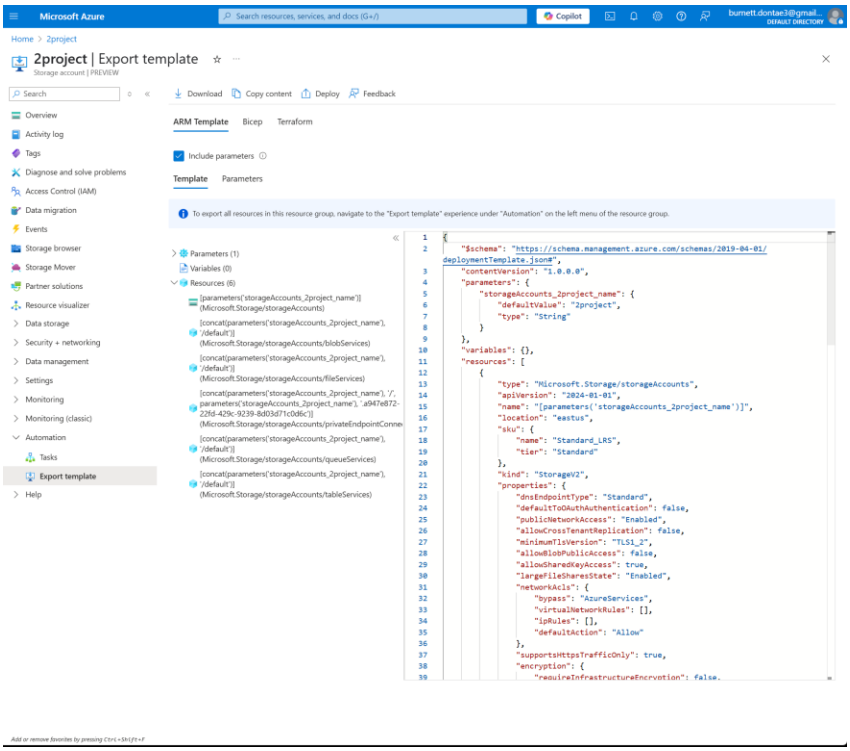

Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
burnett.dontae3@gmail...
DEFAULT DIRECTORY
Home > Storage accounts >
Create a storage account
Basics
Advanced
Networking
Data protection
Encryption
Tags
Review + create
Network connectivity
You can connect to your storage account either publicly, via public IP addresses or service endpoints, or privately, using a private endpoint.
Network access *
Enable public access from all networks
Enable public access from selected virtual networks and IP addresses
Disable public access and use private access
Enabling public access from all networks might make this resource available publicly. Unless public access is required, we recommend using a more restricted access type. Learn more
Private endpoint
Create a private endpoint to allow a private connection to this resource. Additional private endpoint connections can be created within the storage account or private link center.
Add private endpoint
Name
Subscription
Resource g...
Region
Target sub-...
Subnet
Private DN...
p2
Azure for St...
AzureProject1
East US
blob
Database (1...
(new) privat...
Network routing
Determine how to route your traffic as it travels from the source to its Azure endpoint. Microsoft network routing is recommended for most customers.
Routing preference *
Microsoft network routing
Internet routing

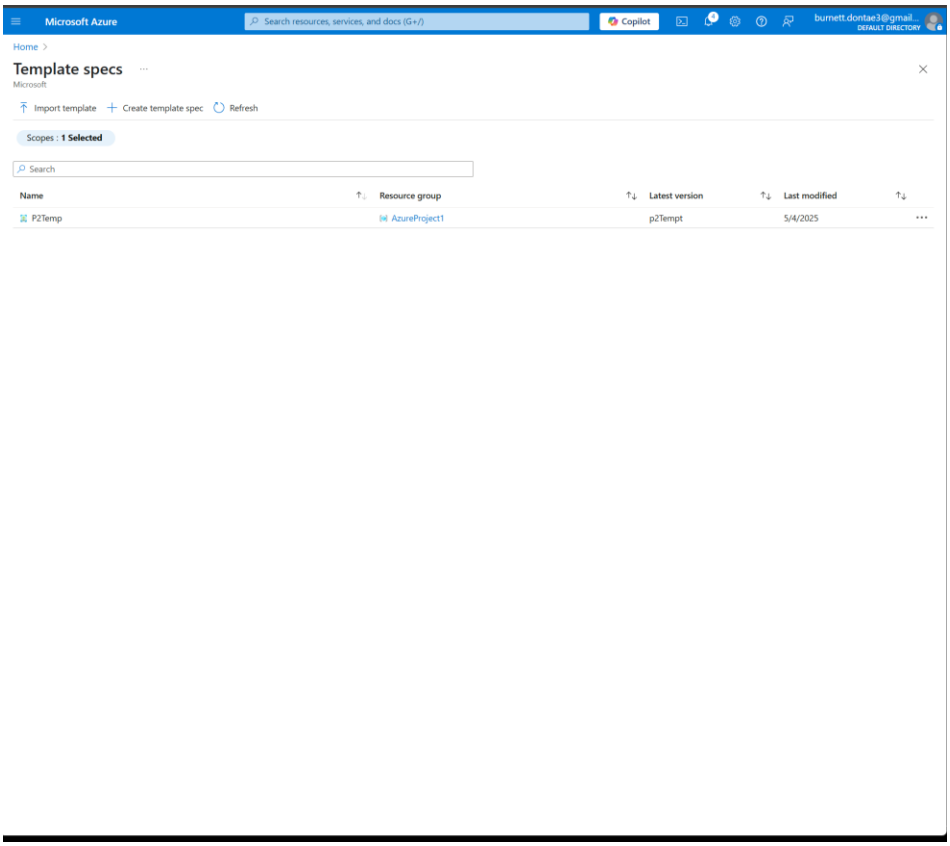

Previous
Next
Review + create
Give feedback
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
burnett.dontae3@gmail...
DEFAULT DIRECTORY
Home > Storage accounts >
Create a storage account
Basics
Advanced
Networking
Data protection
Encryption
Tags
Review + create
Encryption type *
Microsoft-managed keys (MMK)
Customer-managed keys (CMK)
Enable support for customer-managed keys
Blobs and files only
All service types (blobs, files, tables, and queues)
This option cannot be changed after this storage account is created.
Enable infrastructure encryption
Previous
Next
Review + create
Give feedback



5. Deploy the VNet and Storage Account Using ARM Templates

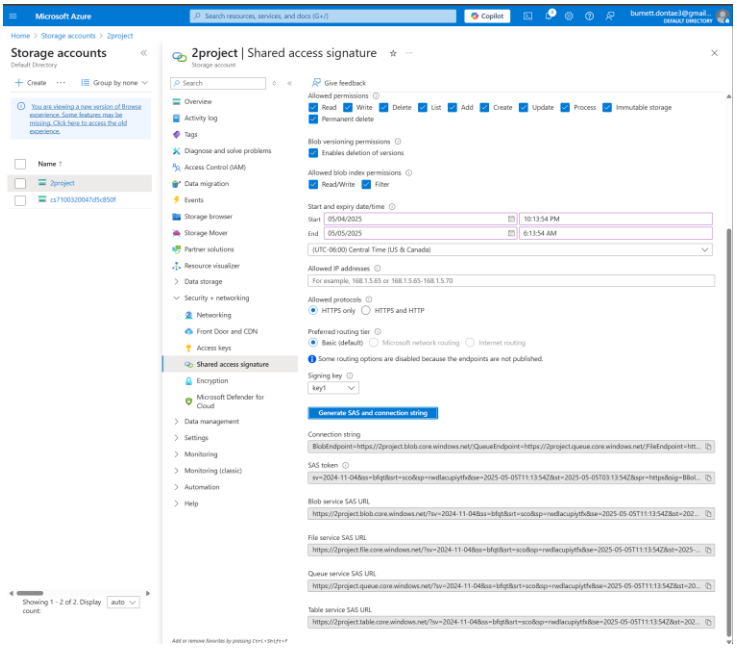
- For both Vnet and Storage Account go to Automation > Export Template > Download
- Navigate to **Templates specs** > Import template > select template file (template.json from the download > Create.
- Then click three dots of your new template in Template specs > Deploy


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
burnett.dontae3@gmail...
DEFAULT DIRECTORY
Home > 2project
2project | Export template
Storage account | PREVIEW
Search
Overview
Activity log
Tags
Diagnose and solve problems
Access Control (IAM)
Data migration
Events
Storage browser
Storage Mover
Partner solutions
Resource visualizer
Data storage
Security + networking
Data management
Settings
Monitoring
Monitoring (classic)
Automation
Tasks
Export template
Help
Download
Copy content
Deploy
Feedback
ARM Template
Bicep
Terraform
Include parameters
Template
Parameters
To export all resources in this resource group, navigate to the "Export template" experience under "Automation" on the left menu of the resource group.
Parameters (1)
Variables (0)
Resources (6)
[parameters('storageAccounts_2project_name')] (Microsoft.Storage/storageAccounts)
[concat(parameters('storageAccounts_2project_name'), /default')] (Microsoft.Storage/storageAccounts/blobServices)
[concat(parameters('storageAccounts_2project_name'), /default')] (Microsoft.Storage/storageAccounts/fileServices)
[concat(parameters('storageAccounts_2project_name'), '/', parameters('storageAccounts_2project_name'), '.a947e872-22fd-429c-9239-8d03d71cd8c')] (Microsoft.Storage/storageAccounts/privateEndpointConne
[concat(parameters('storageAccounts_2project_name'), /default')] (Microsoft.Storage/storageAccounts/queueServices)
[concat(parameters('storageAccounts_2project_name'), /default')] (Microsoft.Storage/storageAccounts/tableServices)
{
"$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
"contentVersion": "1.0.0.0",
"parameters": {
"storageAccounts_2project_name": {
"defaultValue": "2project",
"type": "String"
}
},
"variables": {},
"resources": [
{
"type": "Microsoft.Storage/storageAccounts",
"apiVersion": "2024-01-01",
"name": "[parameters('storageAccounts_2project_name')]",
"location": "eastus",
"sku": {
"name": "Standard_LRS",
"tier": "Standard"
},
"kind": "StorageV2",
"properties": {
"dnsEndpointType": "Standard",
"defaultToOAuthAuthentication": false,
"publicNetworkAccess": "Enabled",
"allowCrossTenantReplication": false,
"minimumTlsVersion": "TLS1_2",
"allowBlobPublicAccess": false,
"allowSharedKeyAccess": true,
"largeFileSharesState": "Enabled",
"networkAcls": {
"bypass": "AzureServices",
"virtualNetworkRules": [],
"ipRules": [],
"defaultAction": "Allow"
},
"supportsHttpsTrafficOnly": true,
"encryption": {
"requireInfrastructureEncryption": false,


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
burnett.dontae3@gmail...
DEFAULT DIRECTORY
Home >
Template specs
Microsoft
Import template
Create template spec
Refresh
Scopes : 1 Selected
Search
Name
Resource group
Latest version
Last modified
P2Temp
AzureProject1
p2Tempt
5/4/2025

6. Test Access and Encryption

- Generate a **Shared Access Signature (SAS)** token to test secure access.
    - Go to Storage accounts > your storage account > Security + networking > Shared access signature > Select all Allowed resource types > Generate SAS



- **Test Blob Service SAS URL**
    - Use Azure Storage Explorer:
        - Download and install Azure Storage Explorer.
        - Go to "Connect to Azure Resources" > Use a shared access signature (SAS) URI.
        - Paste the Connection String
        - Test if you can upload/download files (e.g. create a blob container and upload).
    - Use AzCopy:
        - Install AzCopy: Download AzCopy.
        - Run a test upload/download:

bash
Copy code
azcopy copy "file-to-upload.txt" https://proj2saqwerty.blob.core.windows.net/container-name/file-to-upload.txt?[SAS]

Replace [SAS] with the SAS token.