

Project 1: Active Directory Domain Services

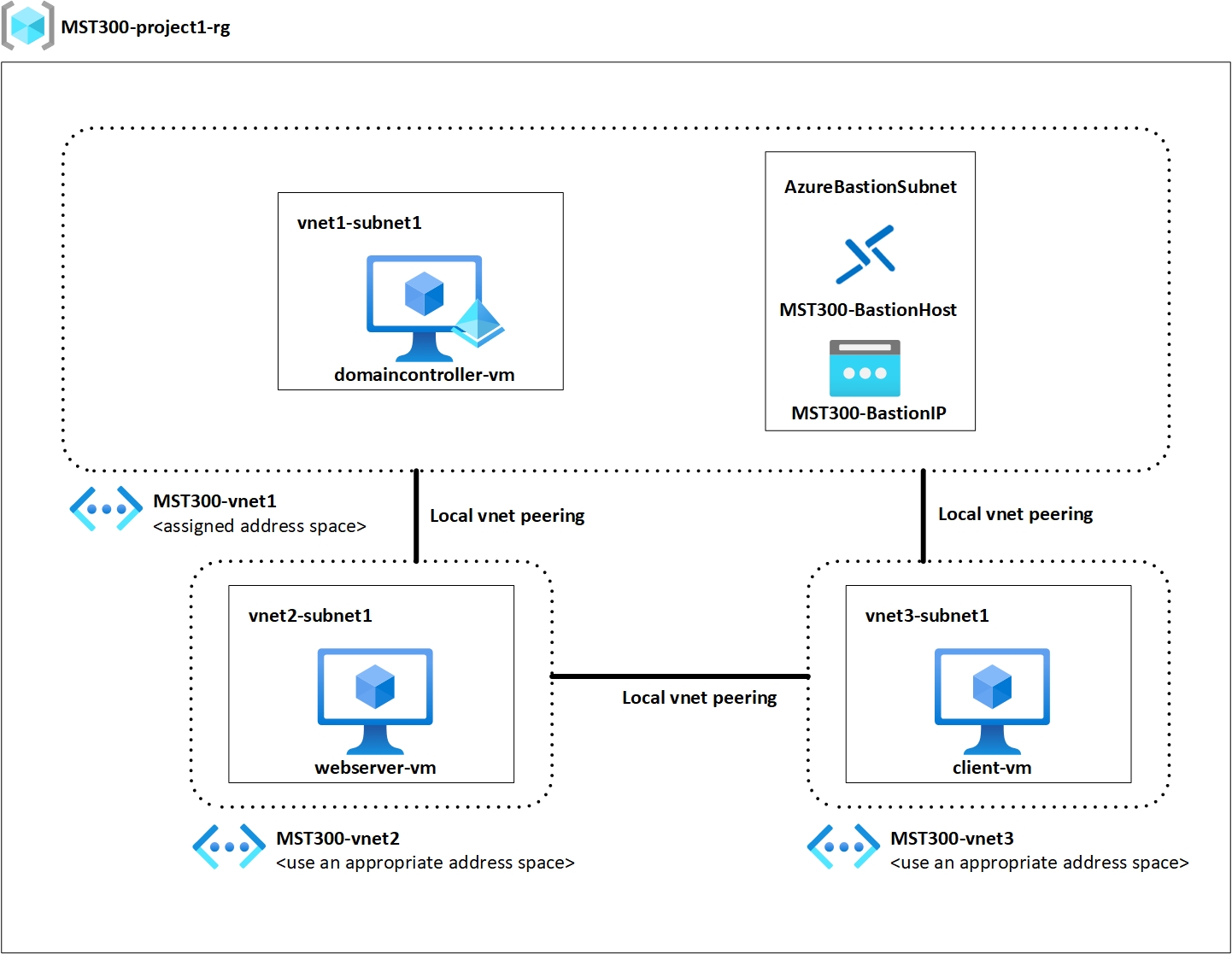
At the end of each session, any resources you created in your account will be preserved. Some Azure resources, such as VM instances, may be automatically shut down, while other resources, such as storage services will be left running. Keep in mind that some Azure features cannot be stopped and can still incur charges (i.e. Azure Bastion). To minimize your costs, delete all resources and recreate them as needed to test your work during a session.

A screenshot of a computer

Description automatically generated with medium confidence

# Lab Objectives

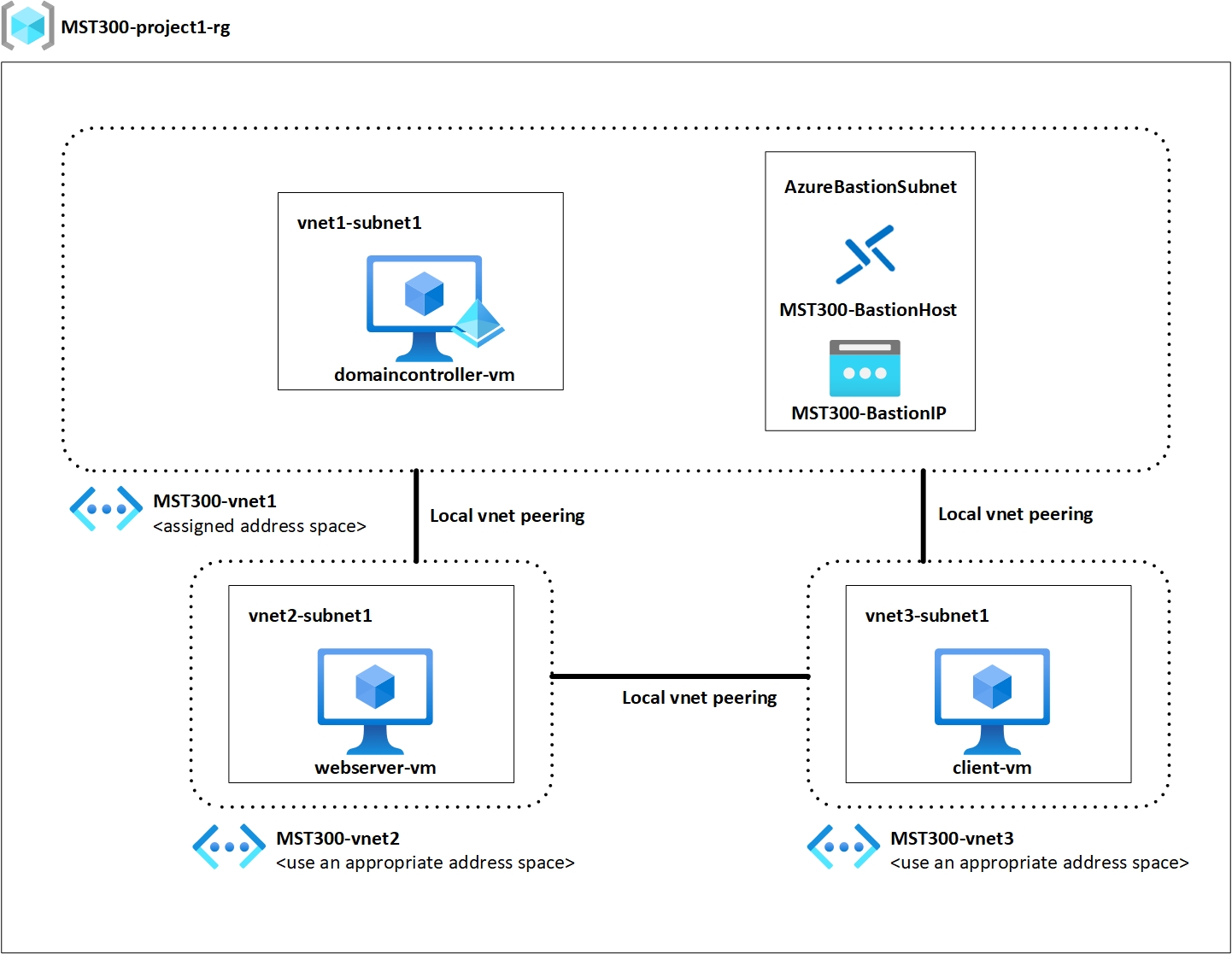
In this project, we will investigate and construct an architecture using the following Azure services:

* [](https://seneca.sharepoint.com/:i:/s/CTYCurriculum/EYGCCzA0lZ1Os3uAtx4xGt8BexgPSmoxV0T_AISRSNPfeA?e=sgDEYy)Azure Bastion
* Azure Virtual Machines
* Azure Virtual Networks
* Azure Virtual Network peering

# Lab Materials

* Azure Bastion
  + [What is Azure Bastion?](https://docs.microsoft.com/en-us/azure/bastion/bastion-overview)
  + [Azure Bastion Tutorial](https://docs.microsoft.com/en-us/azure/bastion/tutorial-create-host-portal)
* Azure Virtual Networks
  + [What is Azure Virtual Network?](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview)
  + [Azure Virtual Network Tutorial](https://docs.microsoft.com/en-us/azure/virtual-network/quick-create-portal)
* Azure Virtual Network Peering
  + [What is Azure Virtual Network Peering?](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview)
  + [Azure Virtual Network Peering Tutorial](https://docs.microsoft.com/en-us/azure/virtual-network/tutorial-connect-virtual-networks-portal)
* Project Topology
  + [Download Topology](https://seneca.sharepoint.com/:i:/s/CTYCurriculum/EYid-XK0BONEmq27roXv3eQBaebpsFrMQmDwQ8ivLPe4OA?e=Ce9pr4)
* Network address space from Seneca Blackboard
  + Use the assigned network address space as indicated in the project

# Project Instructions

[](https://seneca.sharepoint.com/:i:/s/CTYCurriculum/EYGCCzA0lZ1Os3uAtx4xGt8BexgPSmoxV0T_AISRSNPfeA?e=sgDEYy)We will be creating a domain controller which will reside on its own virtual network. A webserver and client will exist on their own virtual networks as well. Both webserver and client will be part of the domain. We will demonstrate on the client VM that we can access the website on the webserver using the FQDN. The project topology outlines the different components and requirements for our project.

The project contains the following components:

1 – Resource Group

1 – Domain Controller VM

1 – Webserver VM

1 – Client VM

3 – Virtual Networks

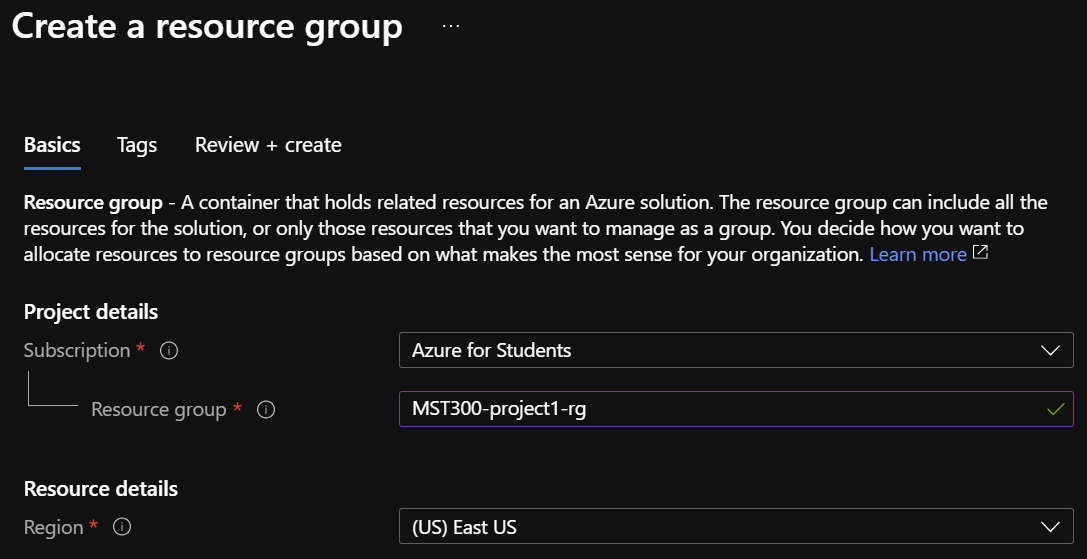
4 – Subnets in total

1 – Azure Bastion Host

# Resource Group Requirements

Create a resource group that will be the logical container that holds all our resources for this project.

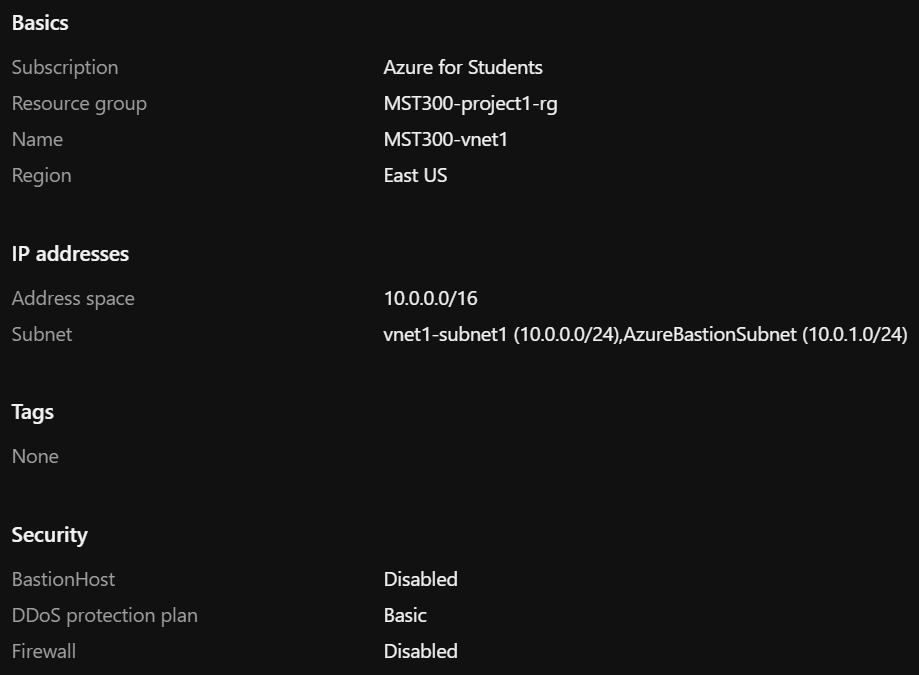
Resource group name: **MST300-project1-rg**

****

# Virtual Network Requirements

Create 3 virtual networks which will be used to connect our resources. A total of 4 subnets will be created [2 subnets in vnet1, 1 subnet in vnet2, 1 subnet in vnet3]. Configure Virtual Network Peering between the virtual networks.

Virtual Network 1

* Use your network address space assigned in Blackboard
* Name: **MST300-vnet1**
* Create 2 subnets within this Virtual Network
  + Subnet Name: **vnet1-subnet1**
  + Subnet Name: **AzureBastionSubnet**
* Assign an appropriate address using your network address

Virtual Network 2

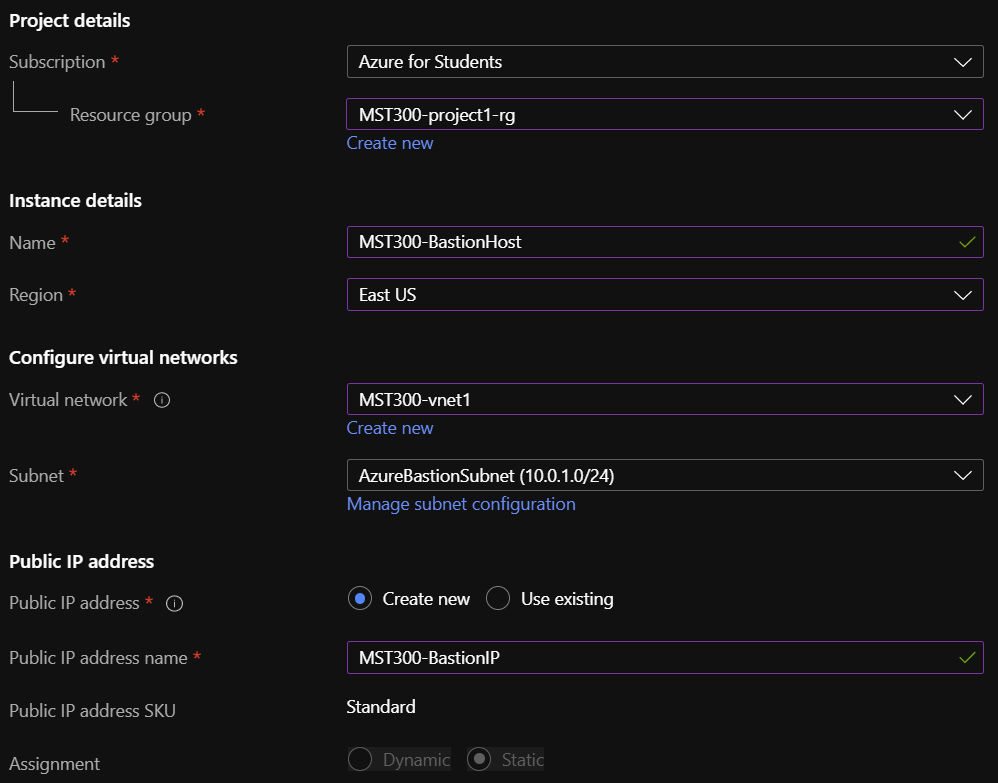
* Name: **MST300-vnet2**
* Create 1 subnet within this Virtual Network
  + Subnet Name: **vnet2-subnet1**
* Assign an appropriate address for this virtual network

Virtual Network 3

* Name: **MST300-vnet3**
* Create 1 subnet within this Virtual Network
  + Subnet Name: **vnet3-subnet1**
* Assign an appropriate address for this virtual network

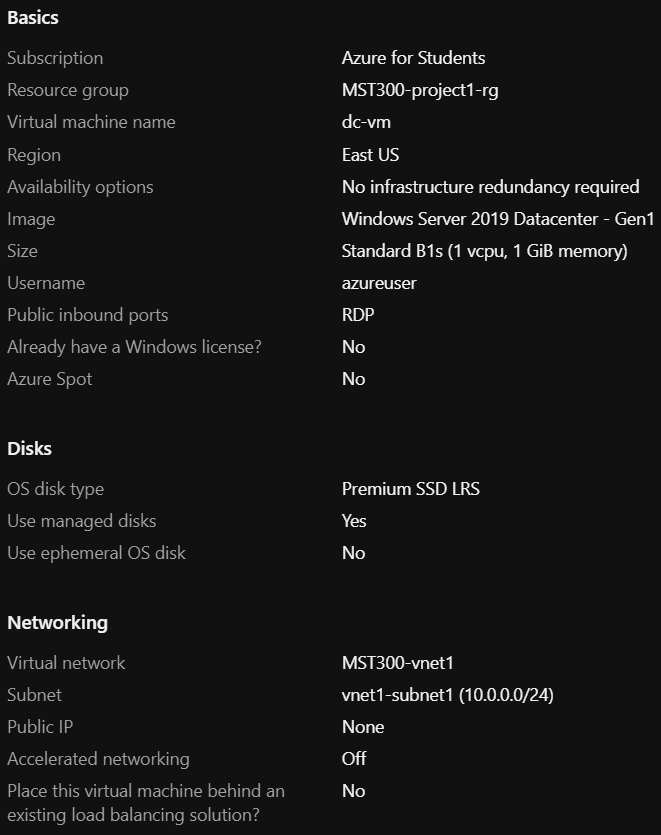
# Azure Bastion Requirements

To access our virtual machines, we will use the Azure Bastion PaaS service. This service allows us to connect to our virtual machines through SSL. By using this service, we do not need a public IP address for our virtual machines.

* ****Name: **MST300-BastionHost**
* Region: **Use the same region as your vnets**
* Virtual network: **MST300-vnet1**
* Subnet: **AzureBastionSubnet**
* Public IP address name: **MST300-BastionIP**

# Domain Controller Requirements

Create 1 virtual machine which will be running ADDS role. This vm will operate in the same virtual network as our Azure Bastion Host.

Domain Controller

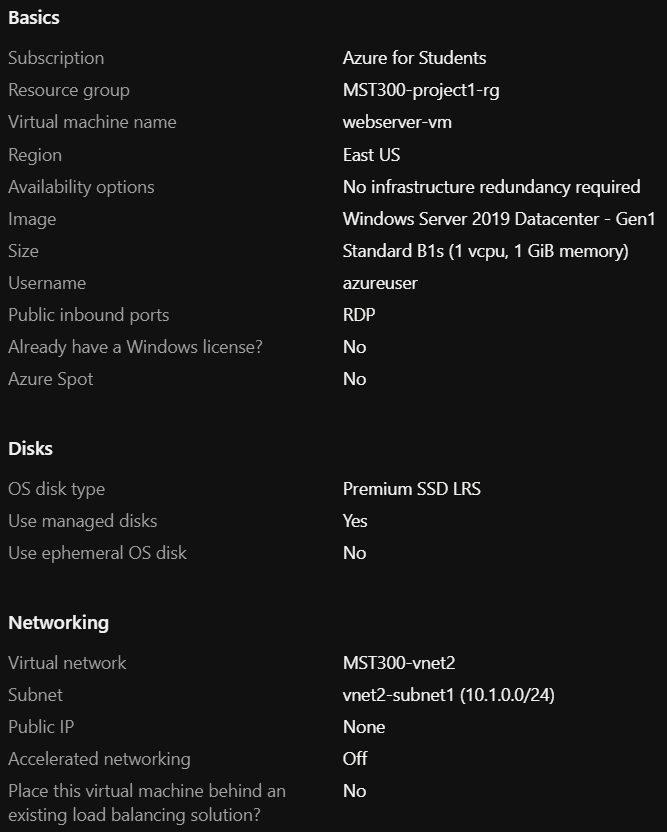
* Name: **dc-vm**
* Image: **Windows Server 2019 Datacenter – Gen1**
* Size: **Standard\_B1s**
* Virtual network: **MST300-vnet1**
* Subnet: **vnet1-subnet1**
* Public IP: **None**

Domain

* Name: **studentID.MST300.com**
* User: **studentID.admin**
  + Member of **Domain Administrators**
* User: **studentID**
  + Member of **Domain** **Users**

# Webserver Requirements

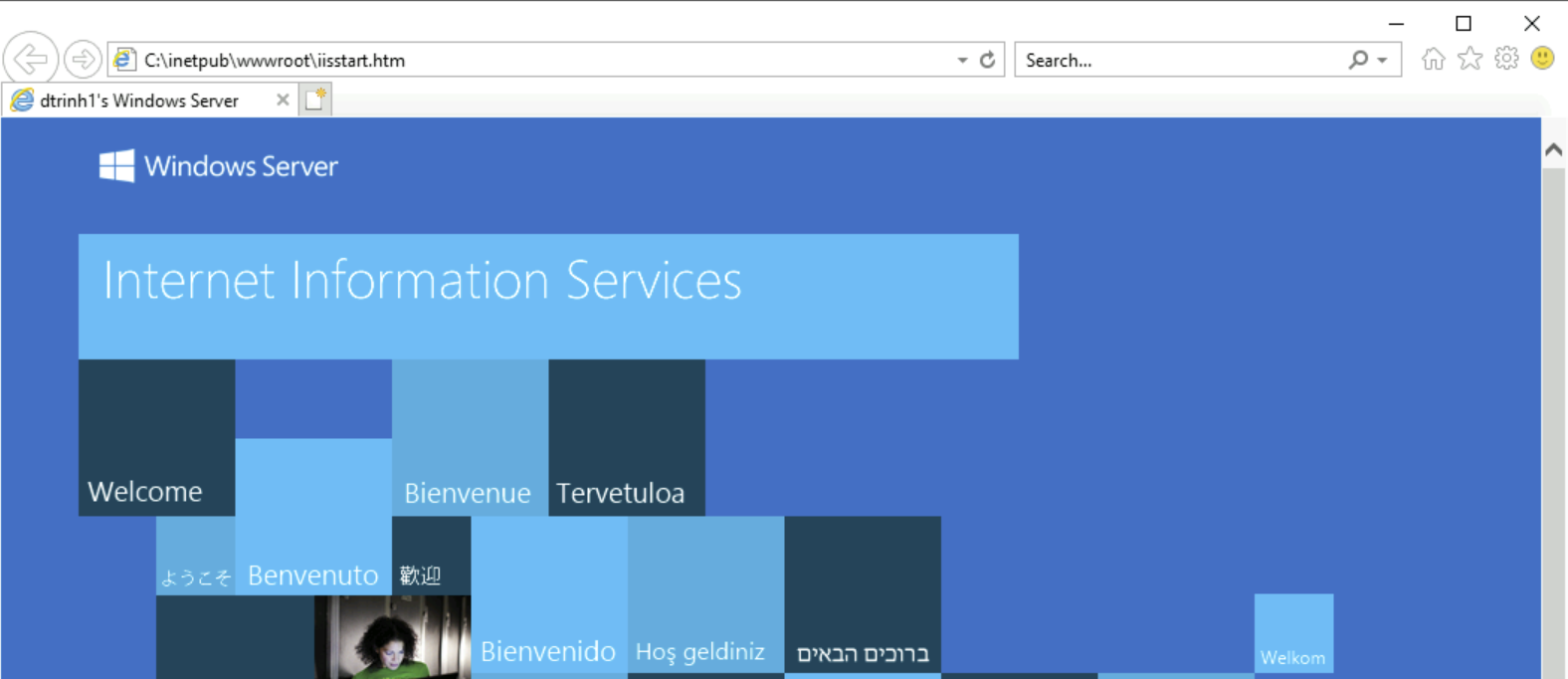
Create 1 virtual machine which will be running IIS role. This vm will operate in its own virtual network. This vm will be part of the domain hosted by the domain controller. The default page will be modified. Remember we will need to configure virtual network peering for us to log into the virtual machine using our Bastion Host.

****Webserver

* Name: **webserver-vm**
* Image: **Windows Server 2019 Datacenter – Gen1**
* Size: **Standard\_B1s**
* Virtual network: **MST300-vnet2**
* Subnet: **vnet2-subnet1**
* Public IP: **None**

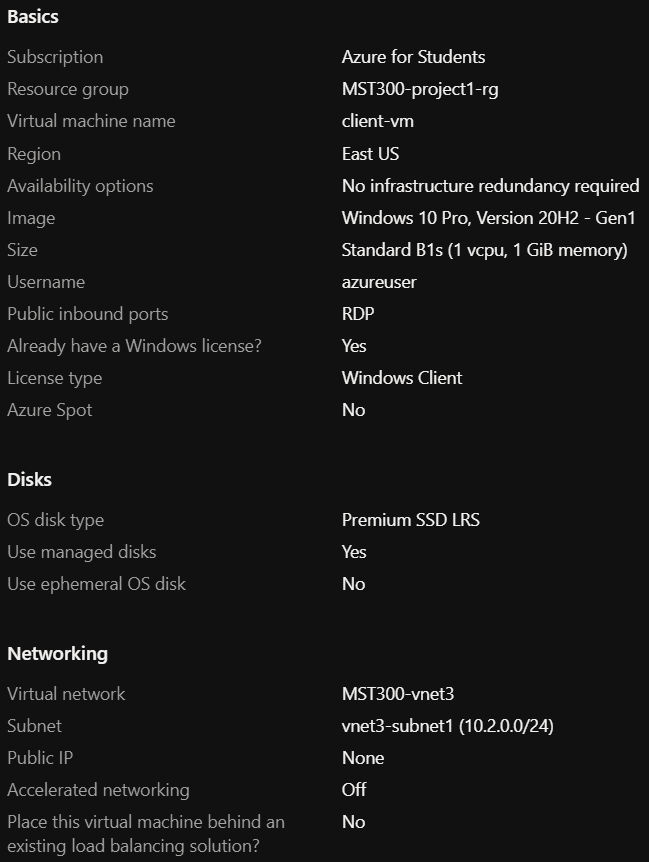
IIS on Webserver

* Webpage Title: **studentID’s Windows Server**

****

# Client VM Requirements

Create 1 virtual machine which will be running Windows 10 operating system. This virtual machine will operate in its own virtual network. This vm will be part of the domain hosted by the domain controller. Remember we will need to configure virtual network peering for us to log into the virtual machine using our Bastion Host.

* ****Name: **client-vm**
* Image: **Windows 10 Pro, Version 20H2 – Gen1**
* Size: **Select an appropriate size based on the OS**
* Virtual network: **MST300-vnet3**
* Subnet: **vnet3-subnet1**
* Public IP: **None**

# Project Rubric

The project will be graded on successful functionality of each of the following components:

1. **Azure Bastion [Yes / No]**
   * Demonstrate connectivity to client-vm using Azure Bastion Host
   * Login should be using AD user account [not AD domain admin or local admin account]
2. **Webservers with modified default pages [Yes / No]**
   * Title modified to show studentID
   * Successful access of website from client-vm using FQDN [ie. webserver.dtrinh1.mst300.com]
3. **Virtual Network Peering [Yes / No]**
   * Demonstrate that all virtual machines are on different virtual networks
4. **Domain Controller [Yes / No]**
   * Demonstrate connectivity to domain controller using Azure Bastion Host
   * Login should be using AD domain admin account [not local admin account]
   * Demonstrate domain controller is <studentID>.MST300.com
   * Demonstrate both webserver and client vms are part of the domain

# Project Submission

1. The project submission will be in a video format uploaded to Microsoft Stream.
2. Use a screen capturing software to demonstrate the different project components as outlined in the project rubric.
3. Submit a link to your video demonstration in Blackboard.

Resources:

* Microsoft Stream: <https://www.microsoft.com/en-us/microsoft-365/microsoft-stream>
* Microsoft Stream screen capture: [Create a screen recording from your desktop](https://docs.microsoft.com/en-us/stream/portal-create-screen-recording#:~:text=To%20record%20your%20screen%2C%20you,use%20your%20camera%20and%20microphone.)
* Video link: [Obtain direct link to video](https://docs.microsoft.com/en-us/stream/portal-share-video)
* Submission Example: [Project Demonstration Sample](https://web.microsoftstream.com/video/5277161e-d3d8-42e3-abf1-21ca3800d199)