Installing vThunder ADC using PowerShell Templates

Version 1.1.0

February, 2023

© 2023 A10 Networks, Inc. All rights reserved.

Information in this document is subject to change without notice.

PATENT PROTECTION

A10 Networks, Inc. products are protected by patents in the U.S. and elsewhere. The following website is provided to satisfy the virtual patent marking provisions of various jurisdictions including the virtual patent marking provisions of the America Invents Act. A10 Networks, Inc. products, including all Thunder Series products, are protected by one or more of U.S. patents and patents pending listed at: a10-virtual-patent-marking.

TRADEMARKS

A10 Networks, Inc. trademarks are listed at: a10-trademarks

CONFIDENTIALITY

This document contains confidential materials proprietary to A10 Networks, Inc. This document and information and ideas herein may not be disclosed, copied, reproduced or distributed to anyone outside A10 Networks, Inc. without prior written consent of A10 Networks, Inc.

DISCLAIMER

This document does not create any express or implied warranty about A10 Networks, Inc. or about its products or services, including but not limited to fitness for a particular use and non-infringement. A10 Networks, Inc. has made reasonable efforts to verify that the information contained herein is accurate, but A10 Networks, Inc. assumes no responsibility for its use. All information is provided "as-is." The product specifications and features described in this publication are based on the latest information available; however, specifications are subject to change without notice, and certain features may not be available upon initial product release. Contact A10 Networks, Inc. for current information regarding its products or services. A10 Networks, Inc. products and services are subject to A10 Networks, Inc. standard terms and conditions.

ENVIRONMENTAL CONSIDERATIONS

Some electronic components may possibly contain dangerous substances. For information on specific component types, please contact the manufacturer of that component. Always consult local authorities for regulations regarding proper disposal of electronic components in your area.

FURTHER INFORMATION

For additional information about A10 products, terms and conditions of delivery, and pricing, contact your nearest A10 Networks, Inc. location, which can be found by visiting www.a10networks.com.

Table of Contents

Introduction **9**

Azure Cloud Terminology 13

Prerequisites 14

Image Repository 15

Get Started 16

PowerShell Templates 17

Deploy PowerShell A10-vThunder_ADC-2NIC-1VM **18**

System Requirements 19

Supported VM Sizes 21

Create vThunder Instance 22

Initial Setup 22

Deploy vThunder 25

Configure Server and Client Machine 26

Create a Server Machine 26

Create a Client Machine 36

Configure vThunder as an SLB 43

Initial Setup 44

Change Password 47

Deploy vThunder as an SLB 48

Access vThunder using CLI or GUI 49

Access vThunder using CLI 49

Access vThunder using GUI 50

Verify Deployment 50

Verify Traffic Flow 52

Deploy PowerShell A10-vThunder_ADC-2NIC-1VM-GLM **53**

System Requirements 54

Supported VM Sizes 56

Create vThunder Instance 57

Initial Setup 57
Deploy vThunder 60
Configure Server and Client Machine 61
Create a Server Machine 61
Create a Client Machine 71
Configure vThunder as an SLB 78
Initial Setup 79
Change Password 82
Deploy vThunder as an SLB 83
Configure vThunder GLM 84
Initial Setup 84
Apply GLM License 85
Access vThunder using CLI or GUI 85
Access vThunder using CLI 86
Access vThunder using GUI 86
Verify Deployment 87
Verify Traffic Flow 89
Deploy PowerShell A10-vThunder_ADC-3NIC-2VM-HA 91
System Requirements 92
Create vThunder Instances 95
Initial Setup 96
Deploy vThunder 99
Configure Server and Client Machine 100
Create a Server Machine 100
Create a Client Machine 110
Configure vThunder as an SLB 117
Initial Setup 118
Change Password 122
Deploy vThunder as an SLB 123
Configure High Availability 124

Configure High Availability for vThunder 124
Initial Setup 125
Create High Availability for vThunder 127
Access vThunder using CLI or GUI 127
Access vThunder using CLI 127
Access vThunder using GUI 128
Verify Deployment 129
Verify Traffic Flow 131
Deploy PowerShell A10-vThunder_ADC-3NIC-2VM-HA-GLM-PVTVIP 133
System Requirements 134
Supported VM Sizes 137
Create vThunder Instances 138
Initial Setup 138
Deploy vThunder 141
Configure Server and Client Machine 142
Create a Server Machine 142
Create a Client Machine 152
Configure vThunder as an SLB 159
Initial Setup 160
Change Password 164
Deploy vThunder as an SLB 165
Configure High Availability 166
Configure High Availability for vThunder 166
Initial Setup 166
Create High Availability for vThunder 169
Configure vThunder using GLM 169
Initial Setup 169
Apply GLM License 170
Access vThunder using Console/CLI 171
Access vThunder using CLI 171

Access vThunder using GUI 171
Verify Deployment 172
Verify Traffic Flow 176
Deploy PowerShell A10-vThunder_ADC-3NIC-2VM-HA-GLM-PUBVIP-BACKAUTO 178
System Requirements 179
Supported VM Sizes 183
Create vThunder Instances 184
Initial Setup 184
Deploy vThunder 187
Configure Server VMSS 188
Create a Server Machine 189
Verify the Server VMSS Creation 196
Configure Client Machine 197
Create a Client Machine 197
Configure Automation Account 204
Create Automation Account 205
Initial Setup 205
Create an Automation Account 207
Verify the Automation Account creation 207
Change Password 208
Create Runbook 209
Create Automation Account Webhook 211
Initial Setup 211
Create a Webhook 211
Verify the Runbook Job creation 212
Configure vThunder as an SLB 213
Initial Setup 214
Deploy vThunder as an SLB 217
Configure High Availability for vThunder 218
Initial Setup 218

Create High Availability for vThunder 220
Configure vThunder using GLM 221
Initial Setup 221
Apply GLM License 222
Access vThunder using CLI or GUI 222
Access vThunder using CLI 223
Access vThunder using GUI 223
Verify Deployment 224
Verify Traffic Flow 227
Deploy PowerShell A10-vThunder_ADC-3NIC-VMSS 230
System Requirements 231
Supported VM Sizes 235
Create vThunder Instances 236
Initial Setup 236
Deploy vThunder 240
Verify Resource Creation 240
Configure Server VMSS 244
Create a Server Machine 245
Verify the Server VMSS Creation 252
Configure Automation Account 253
Create Automation Account 253
Initial Setup 253
Create an Automation Account 259
Verify the Automation Account Creation 260
Create Automation Account Webhook 261
Initial Setup 261
Create a Webhook 261
Verify the AutoScale Resource Variable creation 262
Verify the SSL File availability 264
Verify the Runbook Jobs creation 265

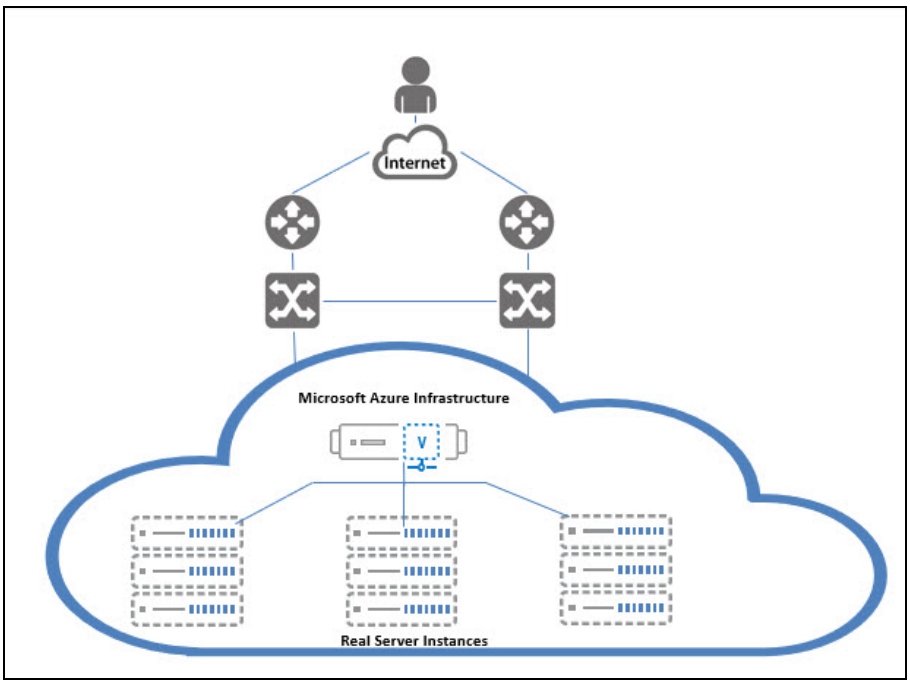
Enable Autoscaling 267
Autoscaling Options 268
Configure Autoscaling and Log Monitoring using Agent Setup 268
Configure Autoscaling using Azure Functions Setup 293
On-demand Password Change 298
Access vThunder using CLI or GUI 300
Access vThunder using CLI 300
Access vThunder using GUI 300
Verify Deployment 301
Verify Traffic Flow 304
Troubleshooting 306
Common Errors 306
Appendix 310
List of Custom Role Permissions 310
Azure Service Application Access Key 316
Use an existing Access Key 316
Create a new Access Key 317
Create a Role 317
Register a Service Application 321
Associate Service Application with a Role 323
Create Certificate and Secrets 324
Collect Azure Access Key 326
Import Azure Access Key 328
Default Password Policy 329

Introduction

vThunder is a fully operational, software-based Application Delivery Controller (ADC) solution that can run on Microsoft Azure cloud. vThunder provides a robust, flexible, and easy-to-deploy application delivery and server load balancing service.

Figure 1 shows how vThunder can be deployed on Microsoft Azure infrastructure.

Figure 1 : vThunder for Microsoft Azure



ACOS uses the PowerShell templates to quickly deploy the vThunder instance on the Azure cloud. Table 1 lists the available PowerShell templates for deploying vThunder ADC on Azure cloud:

Table 1 : Available PowerShell Templates

Template	Description	Configuration
A10-vThunder_ ADC-2NIC-1VM	• Creates one vThunder instance with two Network Interface Cards (NICs). • Deploys a Certificate	• 2 NICs (1 Management + 1 Data) • BYOL (Bring Your Own License)

Template	Description	Configuration
	Authority SSL Certificate and Server Load Balancer (SLB).	• 1 VM (vThunder Virtual Instance) • SLB (vThunder Server Load Balancer) • SSL (Apply SSL Certificate)
A10-vThunder_ ADC-2NIC-1VM-GLM	• Creates one vThunder instance with two Network Interface Cards and A10 Global License Manager (GLM) integration. • Deploys a Certificate Authority SSL Certificate and Server Load Balancer.	• 2 NICs (1 Management + 1 Data) • BYOL (Bring Your Own License) • 1 VM (vThunder Virtual Instance) • SLB (vThunder Server Load Balancer) • SSL (Apply SSL Certificate) • GLM (Auto apply A10 license)
A10-vThunder_ ADC-3NIC-2VM-HA	• Creates two vThunder instances with High Availability (HA) setup, each vThunder contains three Network Interface Cards. • Deploys a Certificate Authority SSL Certificate and Server Load Balancer.	• 3 NICs (1 Management + 2 Data) • BYOL (Bring Your Own License) • 2 VMs (vThunder Virtual Instances) • SLB (vThunder Server Load Balancer) • SSL (Apply SSL Certificate) • HA (High Availability with auto switchover with next available vThunder VM using VRRP)
A10-vThunder_	• Creates two vThunder	• 3 NICs (1 Management + 2

Template	Description	Configuration
ADC-3NIC-2VM-HA-GLM-PVTVIP	instances with High Availability setup and an A10 Global License Manager integration, each vThunder has three Network Interface Cards. • Deploys a Certificate Authority SSL Certificate, and a Server Load Balancer.	Data) • BYOL (Bring Your Own License) • 2 VMs (vThunder Virtual Instances) • SLB (vThunder Server Load Balancer) • SSL (Apply SSL Certificate) • GLM (Auto apply A10 license) • HA (High Availability with auto switchover with available VM using VRRP) • VIP (Private Interface)
A10-vThunder_ ADC-3NIC-2VM-HA-GLM-PUBVIP-BACKAUTO	• Creates two vThunder instances with High Availability (HA) setup and GLM integration, each vThunder contains three Network Interface Cards. • Deploys a Certificate Authority SSL Certificate, Server Load Balancer, and backend server autoscaling support.	• 3 NICs (1 Management + 2 Data) • BYOL (Bring Your Own License) • 2 VMs (vThunder Virtual Instances) • SLB (vThunder Server Load Balancer) • SSL (Apply SSL Certificate) • GLM (Auto apply A10 license) • HA (High Availability with auto switchover for the available VM using VRRP) • VIP (Public Interface) • BACKAUTO (Webhook URL

Template	Description	Configuration
		to apply SLB config into vThunder for newly added/deleted web/app servers via server VMSS)
A10-vThunder_ ADC-3NIC-VMSS	• Creates multiple vThunder instances in a Virtual Machine scale set using CPU Matrix-based autoscaling with GLM integration. Each vThunder contains three Network Interface Cards. • Deploys a Certificate Authority SSL Certificate, Server Load Balancer, Log Analysis using Azure Log Analytics integration, and Azure Application Insight integration.	• 3 NICs (1 Management + 2 Data) • BYOL (Bring Your Own License) • Multiple VMs (vThunder Virtual Instances) • SLB (vThunder Server Load Balancer) • SSL (Apply SSL Certificate) • GLM (Auto apply for A10 license) • VMSS (vThunder virtual machine auto-scale set. Autoscaling on data CPU threshold.) • MONITOR (Azure monitor services for vThunder Syslog and data CPU metric monitoring)

This documentation helps you to deploy vThunder instance on Azure cloud after downloading the required template from GitHub on your local machine, configuring the vThunder installation parameters in the template and executing Azure CLI commands in Windows PowerShell.

Azure Cloud Terminology

- **Azure account** — The Azure account created has different support plans for different regions. For more information on different Azure regions and availability of types of virtual machines in these regions, see https://docs.microsoft.com/en-us/azure/virtual-machines/linux/overview.
- **Resource group** — A resource group is a logical group of all the resources related to an Azure solution. Azure offers flexibility in the allocation of resources to resource groups. For more information, see https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-overview.
- **Availability set** — An availability set is a logical grouping of Azure VM resources so that each VM resource is isolated from other resources when deployed. This hardware isolation ensures that a minimum number of VMs are impacted during a failure. For more information, see https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-overview.
- **Virtual network** — The Microsoft Azure Virtual Network service enables resources to securely communicate with other resources in an Azure network in the cloud. A virtual network is hence logical isolation of the Azure cloud for an Azure account. You can connect different virtual networks and to on-premises networks. For more information, see https://docs.microsoft.com/en-us/azure/virtual-machines/windows/tutorial-availability-sets.
- **Network security group (NSG)** — A network security group (NSG) contains a list of security rules that allow or deny network traffic to resources connected to Azure virtual networks (VNet). The NSGs can be associated with subnets or individual NICs attached to the VMs. When an NSG is associated with a subnet, the rules apply to all the resources connected to the subnet.
- **Azure PowerShell Template** — A JavaScript Object Notation (JSON) file used to specify the resources and its properties which are deployed on the Azure cloud.
- **Virtual Machine Scale Set (VMSS)** — A virtual machine scale set is used to manage and deploy multiple identical virtual machine instances.
- **Azure Automation** — Azure automation is a cloud-based solution to automate recurring and manual tasks. For more information, see https://learn.microsoft.com/en-us/azure/automation/

- **Azure Automation Account** — An automation account is a logical group of all the resources related to Azure automation within a resource group.
- **Azure Service Application Access Key** — An access key is used to automate scale set creation and configuration.
- **Azure Runbook** — A runbook is a PowerShell script used to start the automation jobs in Azure.
- **Azure Automation Webhook** — A webhook is a custom URL that is sent to Azure automation with a runbook-specific data payload.
- **Azure Log Analytics Workspace** — A log analytics workspace is a custom workspace to collect system logs from virtual machine instances.
- **Azure Application Insights** — The application insights are custom metrics used to analyze CPU utilization and configure alerts.
- **Azure Load Balancer Rule** — A load balancer rule is used to define the distribution method of the incoming traffic to all the virtual machine instances within the backend pool.
- **Backend Pool** — A backend pool is used to define the group of resources that serves traffic for a given load-balancing rule.
- **Health Probe** — A health probe is used to determine the health status of the virtual machine instances in the backend pool.

Prerequisites

To deploy vThunder on Azure cloud using any of the supported PowerShell template, you must ensure the following prerequisites are met:

- Azure account and a valid subscription (Required)
  - Download the following Azure tools to create and manage resources:
    - Azure Portal — A web console to create and monitor Azure resources.
    - Azure CLI [2.39.0] — An interface that can be launched using a browser or installed on a system to start a local CLI session.
    - Azure PowerShell — A set of lightweight PowerShell commands called cmdlets used to manage Azure resources from the command line.

- Azure User
  - A user with Contributor Role permission.

- Windows PowerShell [7.0.6 LTS or 7.1.3, 7.2.2 (recommended) or any higher version] — A task automation solution used to install the Az module.

```
PowerShell 7.2.2
Copyright (c) Microsoft Corporation.
https://aka.ms/powershell
Type 'help' to get help.
PS C:\Users\TestUser>
```

- Valid SSL certificate to apply on vThunder (Optional).
- Text editor (Notepad++, Notepad or any other text editor application).
- A10 GLM account access and valid licenses.
  This access is required for the templates using GLM. For more information, see Global License Manager User Guide.
- PowerShell Templates
  Go to GitHub [Branch: release/v1.0.0] and download the required PowerShell template folder to your local machine. The template folder contains the json parameter files and PowerShell scripts for the deployment of the respective template. For example, the downloaded folder path is C:\Users\TestUser\Templates.
- A10 vThunder default user credentials
  Send a request to A10 Networks Support for A10 vThunder login default user credentials.

Image Repository

PowerShell templates support the following Azure Marketplace A10 vThunder images:

- A10 vThunder ADC 520 BYOL for Microsoft Azure - Microsoft Azure
  Tested with 64-bit Advanced Core OS (ACOS) version 5.2.0, build 155 (Aug-10-2020,14:34)
- A10 vThunder ADC 521 BYOL for Microsoft Azure - Microsoft Azure
  Tested with 64-bit Advanced Core OS (ACOS) version 5.2.1-P6, build 74 (Oct -09-

2022,09:24)

- Tested with 64-bit Advanced Core OS (ACOS) version 6.0.0, build 419

Get Started

After the recommended version of PowerShell application is installed, perform the following steps using it:

1. Start a CLI session.

```
PS C:\Users\TestUser> az login
```

Once the authorization is complete and you can access the Azure Portal, the session details appear in the PowerShell prompt.

```
A web browser has been opened at
https://login.microsoftonline.com/organizations/oauth2/v2.0/authorize.
Please continue the login in the web browser. If no web browser is
available or if the web browser fails to open, use device code flow
with `az login --use-device-code`.
[
  {
    "cloudName": "AzureCloud",
    "homeTenantId": "xxxxxxxx-xxx-xxxx-xxxx-xxxxxxxxxxxx",
    "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "isDefault": true,
    "managedByTenants": [],
    "name": "Eng Azure",
    "state": "Enabled",
    "tenantId": "xxxxxxxx-xxx-xxxx-xxxx-xxxxxxxxxxxx",
    "user": {
      "name": "TUser@a10networks.com",
      "type": "user"
    }
  }
]
PS C:\Users\TestUser>
```

2. Install Az Module.

```
PS C:\Users\TestUser> Install-Module Az
```

3. Navigate to the downloaded PowerShell template folder and set the execution policy for this folder.

```
PS C:\Users\TestUser\Templates> Set-ExecutionPolicy -Scope Process -
ExecutionPolicy Bypass
```

PowerShell Templates

To implement infrastructure as a code for your Azure solutions, use PowerShell templates. The template is a json native file that defines the infrastructure and configuration for your project. The template uses declarative syntax to specify the resources that are to be deployed and the properties for those resources without having to write the sequence of programming commands to create it.

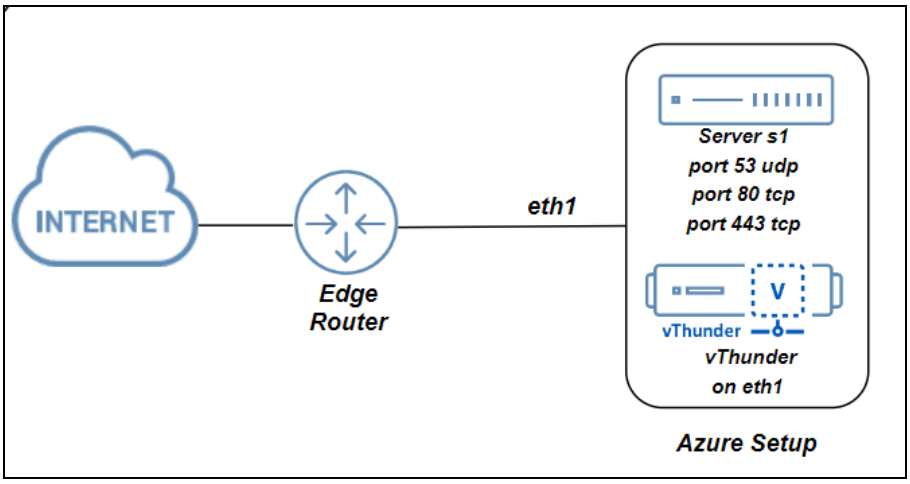
The following templates are available:

- Deploy PowerShell A10-vThunder_ADC-2NIC-1VM
- Deploy PowerShell A10-vThunder_ADC-2NIC-1VM-GLM
- Deploy PowerShell A10-vThunder_ADC-3NIC-2VM-HA
- Deploy PowerShell A10-vThunder_ADC-3NIC-2VM-HA-GLM-PUBVIP-BACKAUTO
- Deploy PowerShell A10-vThunder_ADC-3NIC-2VM-HA-GLM-PVTVIP
- Deploy PowerShell A10-vThunder_ADC-3NIC-VMSS

Deploy PowerShell A10-vThunder_ADC-2NIC-1VM

Figure 2 shows the 2NIC-1VM deployment topology. Using the PowerShell template, one vThunder instance containing one management interface and one data interface can be deployed.

Figure 2 : 2NIC-1VM Topology



The following topics are covered:

System Requirements 19
Supported VM Sizes 21
Create vThunder Instance 22
Configure Server and Client Machine 26
Configure vThunder as an SLB 43
Access vThunder using CLI or GUI 49
Verify Deployment 50
Verify Traffic Flow 52

System Requirements

The PowerShell template will display the default values when you download and save the files on your local machine. You can modify the default values as required for your deployment.

You need the following to deploy vThunder on the Azure cloud:

Table 2 : System Requirements

Resource Name	Description	Default Value
Azure Resource Group	A resource group with the specified name and location is created if it doesn't exist. All the resources required for this template is created under the resource group.	Here, the Azure resource group name used is `vth-rg1`.
Azure Storage Account	A storage account is created inside the resource group if it doesn't exist. If the storage name already exists, the following error is displayed "The storage account named vthunderstorage already exists under the subscription". **Performance**: Standard **Replication**: Read-access geo-redundant storage (RA-GRS) **Account kind**: Storagev2 (general purpose v2)	`vthunderstorage`
Virtual Machine (VM) Instance	A virtual machine instance is created for vThunder. **Product**: A10 vThunder	`vth-inst1`

Resource Name	Description	Default Value
	Operating system: Linux **Default Size**: Standard_DS2v2 (4 vCPUs, 16 GiB Memory) **NOTE:** Before selecting any VM size, it is highly recommended to do an assessment of your projected traffic. Table 3 lists the supported VM sizes.	
Virtual Cloud Network [VCN]	A virtual network is assigned to the virtual machine instance.	`vth-vnet` Address prefix for virtual network: 10.0.0.0/16

Subnet	Two subnets are created with an address prefix each.	Subnet1:
		`10.0.1.0/24`
		Subnet2:
		`10.0.2.0/24`

Network Interface Card [NIC]	Two types of interfaces are created for each vThunder instance: • Management Interface with public IP • Data Interface with primary private IP [Ethernet 1]	`vth-inst1-mgmt-nic1` `10.0.1.5` `vth-inst1-data-nic2` `10.0.2.5 [Primary IP]`
Network Security Group [NSG]	A security group is created for all the associated default interfaces.	`vth-nsg1`

Supported VM Sizes

Table 3 : Supported VM sizes

Series	Size	Qualified Name
A series	Standard A2 Standard A2v2 Standard A2mv2 Standard A4v2 Standard A4mv2 Standard A3 Standard A4 Standard A8v2	Standard_A2 Standard_A2_v2 Standard_A2m_v2 Standard_A4_v2 Standard_A4m_v2 Standard_A3 Standard_A4 Standard_A8_v2
B series	Standard B2s Standard B2ms Standard B4ms	Standard_B2_s Standard_B2ms Standard_B4ms
D series	Standard D2v2 Standard DS2v2 Standard D4v3 Standard D4sv3 Standard D3v2 Standard Ds3v2 Standard D5v2	Standard_D2_v2 Standard_DS2_v2 Standard_D4_v3 Standard_D4s_v3 Standard_D3_v2 Standard_Ds3_v2 Standard_D5_v2
F series	Standard F4s Standard F8 Standard F16s	Standard_F4s Standard_F8 Standard_F16s

Azure is going to retire a few of the above listed VM sizes soon. For the latest updates, see Virtual Machine series | Microsoft Azure.

For more information on Windows and Linux VM sizes, see

https://docs.microsoft.com/en-us/azure/virtual-machines/sizes-general

https://docs.microsoft.com/en-us/azure/virtual-machines/linux/sizes.

Create vThunder Instance

The following topics are covered:

- Initial Setup
- Deploy vThunder

Initial Setup

Before deploying vThunder on Azure cloud, configure the corresponding parameters in the PowerShell template.

To configure the parameters, perform the following steps:

1. Navigate to the folder where you have downloaded the PowerShell template, and open the PS_TMPL_2NIC_1VM_PARAM.json with a text editor.

   NOTE: Each parameter has a default value mentioned in the parameter file.

2. Provision the vThunder instance by entering the default admin credentials as follows:

```
"adminUsername": {
  "value": "vth-user"
},
"adminPassword": {
  "value": "vth-Password"
},
```

NOTE: This is a mandatory step during VM creation. Once the device is provisioned, vThunder auto-deletes all users except the default user.

3. Configure a virtual network.

```
"virtual_network": {
  "value": "vth-vnet"
},
```

4. Configure a DNS label prefix.

```
"dnsLabelPrefix": {
  "value": "vth-inst1"
},
```

5. Configure a VM name.

```
"vmName": {
  "value": "vth-inst1"
},
```

6. Set a VM Size for vThunder.

```
"vmSize": {
  "value": "Standard_DS2_v2"
},
```

Use a suitable VM size that supports at least 2 NICs. For VM sizes, see Supported VM Sizes section.

7. Copy the desired vThunder Image Name and Product Name from the Azure Marketplace for A10 vThunder and update the details in the parameter file as follows:

```
"vThunderImage": {
  "value":"vthunder_520_byol"
},
"publisherName": {
  "value": "a10networks"
},
"productName": {
  "value": "a10-vthunder-adc-520-for-microsoft-azure"
},
```

NOTE: Do not change the publisher name.

8. Configure two network interface cards.

```
"nic1Name": {
  "value": "vth-inst1-mgmt-nic1"
},
"nic2Name": {
  "value": "vth-inst1-data-nic2"
},
```

9. Configure an address prefix and subnet values for each management interface and data interface.

```
"addressPrefixValue": {
  "value": "10.0.0.0/16"
},
"mgmtIntfPrivatePrefix": {
  "value": "10.0.1.0/24"
},
"mgmtIntfPrivateAddress": {
  "value": "10.0.1.5"
},
"eth1PrivatePrefix": {
  "value": "10.0.2.0/24"
},
"eth1PrivateAddress": {
  "value": "10.0.2.4"
},
```

10. Configure a public IP address.

```
"publicIPAddressName": {
  "value": "vth-vm-ip"
},
```

11. Configure a Network Security Group.

```
"networkSecurityGroupName": {
  "value": "vth-nsg1"
},
```

12. Verify if all the configurations in the PS_TMPL_2NIC_1VM_PARAM.json file are correct and then save the changes.

Deploy vThunder

To deploy vThunder on Azure cloud, perform the following steps:

1. From Start menu, open PowerShell and navigate to the folder where you have downloaded the PowerShell template.
2. Run the following command to create a deployment group in Azure and provide a unique storage account name when prompted.

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_2NIC_1VM_1.ps1 -resourceGroup
<resource_group_name> -location "<location_name>"
```

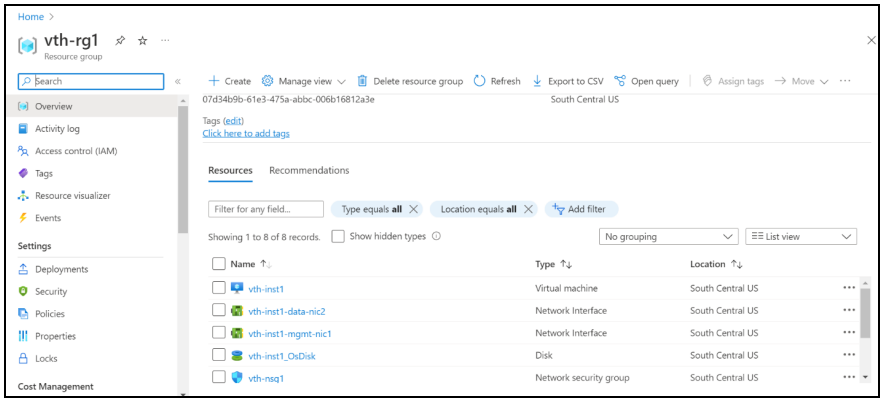
Example:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_2NIC_1VM_1.ps1 -resourceGroup
vth-rg1 -location "south central us"

cmdlet PS_TMPL_2NIC_1VM_1.ps1 at command pipeline position 1
Supply values for the following parameters:
storageaccount: vthunderstorage
vth-rg1
vthunderstorage
South Central US
```

Here, **`vth-rg1`** resource group is created.

3. Verify if all the above listed resources are created in the **Home** > **Azure Services** > **Resource Group** > <resource_group_name>.

Figure 3 : Resource listing in the resource group



Configure Server and Client Machine

The following topics are covered:

- Create a Server Machine
- Create a Client Machine

Create a Server Machine

To create a Server machine, perform the following steps:

1. From **Home**, navigate to **Azure Services** > **Create a resource** > **Virtual machine** and click **Create**.
   The **Create a virtual machine** window is displayed.
2. Select or enter the following mandatory information in the **Basics** tab:

   Project details

   - Subscription
   - Resource group

   Instance details

   - Virtual machine name - Server machine
   - Region

- Image
- Size

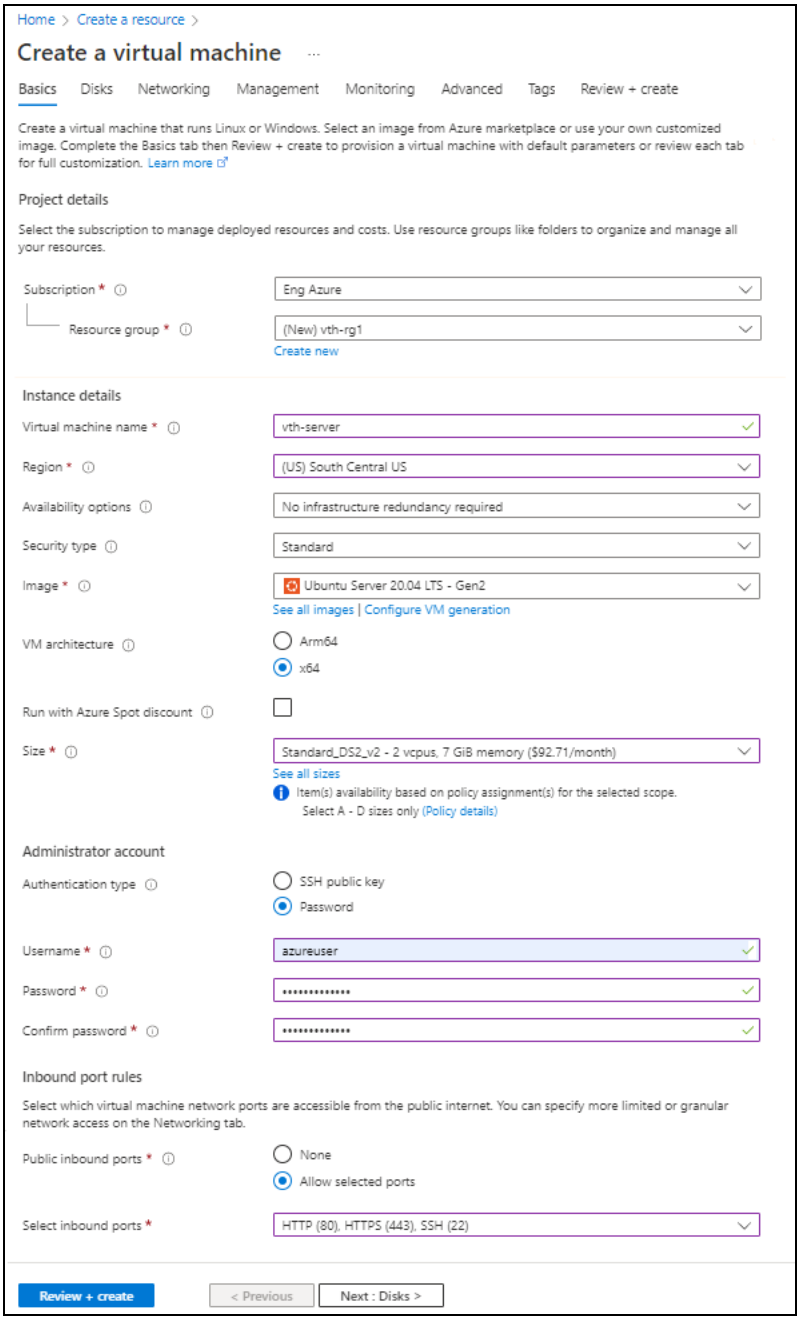
Administrator account

- Depending upon the Authentication type selected, provide the information.

Inbound port rules

- Public inbound ports
- Select inbound ports

Figure 4 : Create a virtual machine window - Basics tab



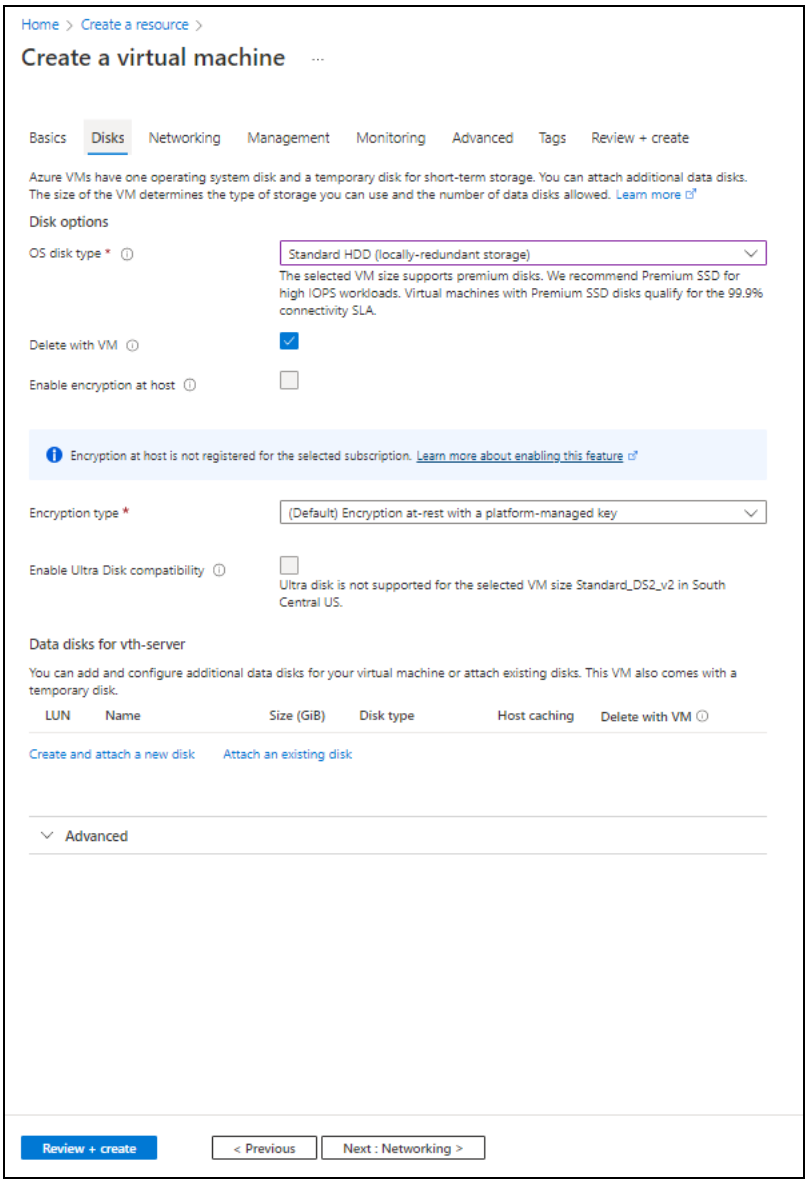
3. Leave the remaining fields as is and click **Next : Disks** at the bottom of the window.

4. Select or enter the following mandatory information in the **Disks** tab:

   Disk options

   - OS disk type
   - Encryption type

   Figure 5 : Create a virtual machine window - Disks tab



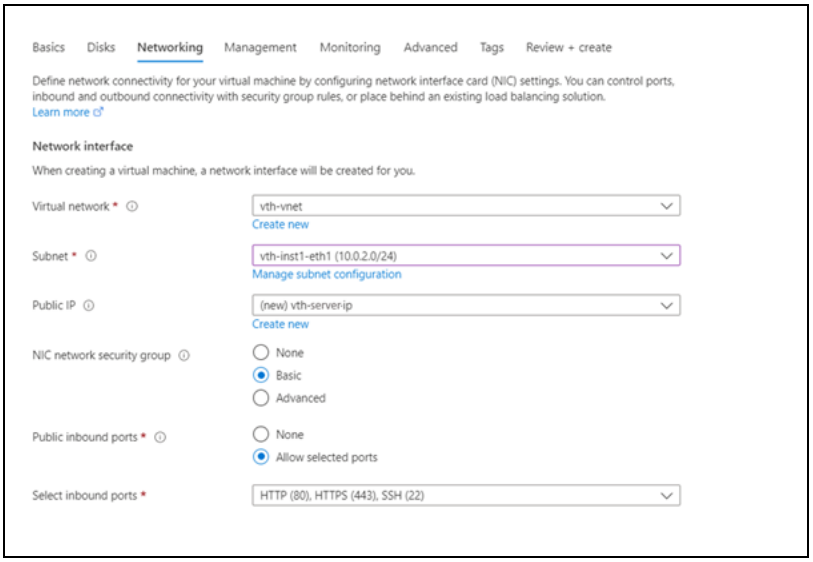
5. Leave the remaining fields as is and click **Next : Networking** at the bottom of the window.

6. Select or enter the following mandatory information in the **Networking** tab:

   Network interface

   - Virtual network
   - Subnet: Data subnet (Ethernet 1)
   - Select inbound ports

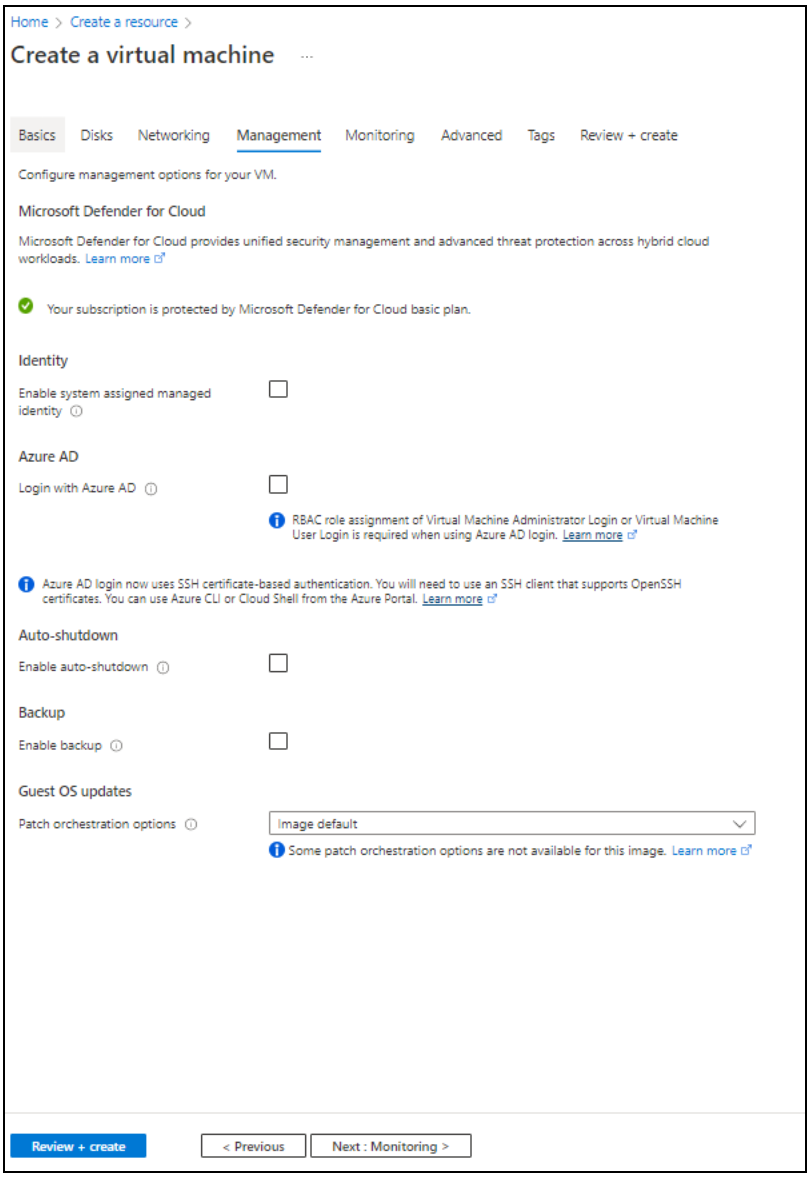
   Figure 6 : Create a virtual machine window - Networking tab



7. Leave the remaining fields as is and click **Next : Management** at the bottom of the window.

8. Select or enter the information in the **Management** tab as needed.

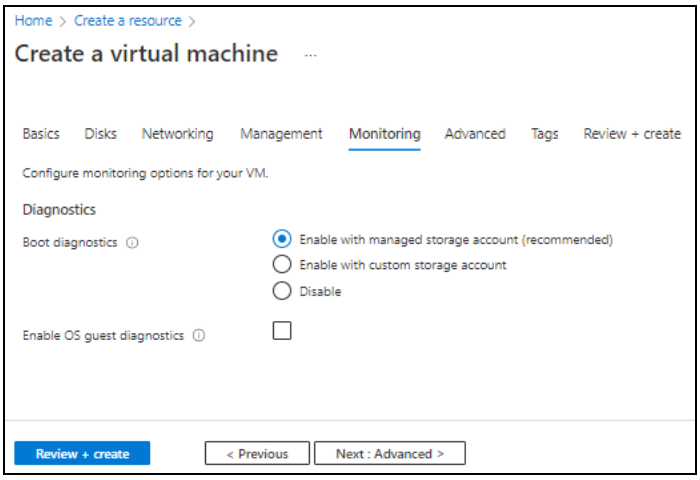
Figure 7 : Create a virtual machine window - Management tab



9. Click **Next : Monitoring** at the bottom of the window.

10. Select the monitoring options in the **Monitoring** tab as needed.

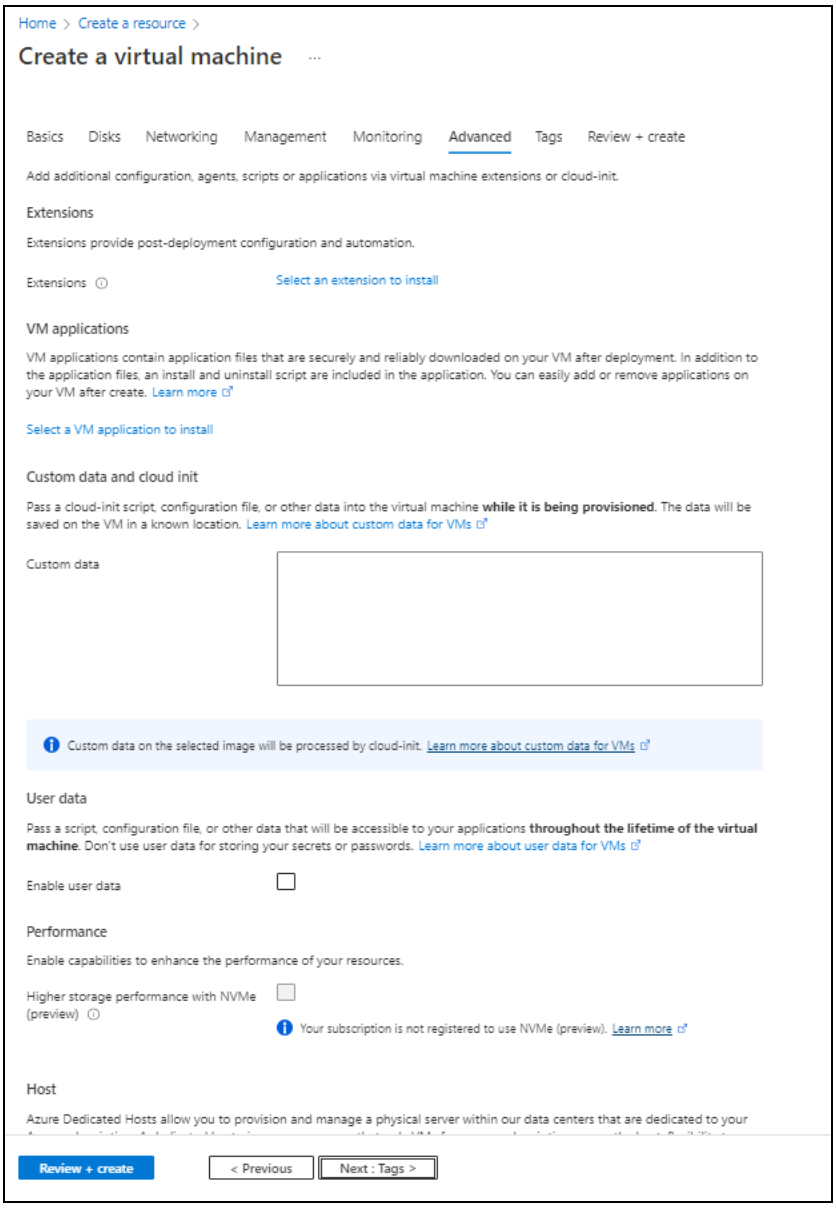
Figure 8 : Create a virtual machine window - Monitoring tab



11. Click **Next : Advanced** at the bottom of the window.

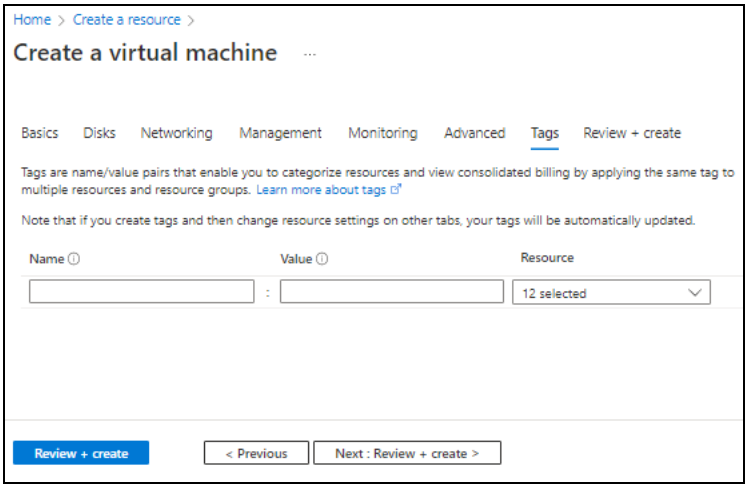
12. Select or enter the additional configuration in the **Advanced** tab as needed.

Figure 9 : Create a virtual machine window - Advanced tab



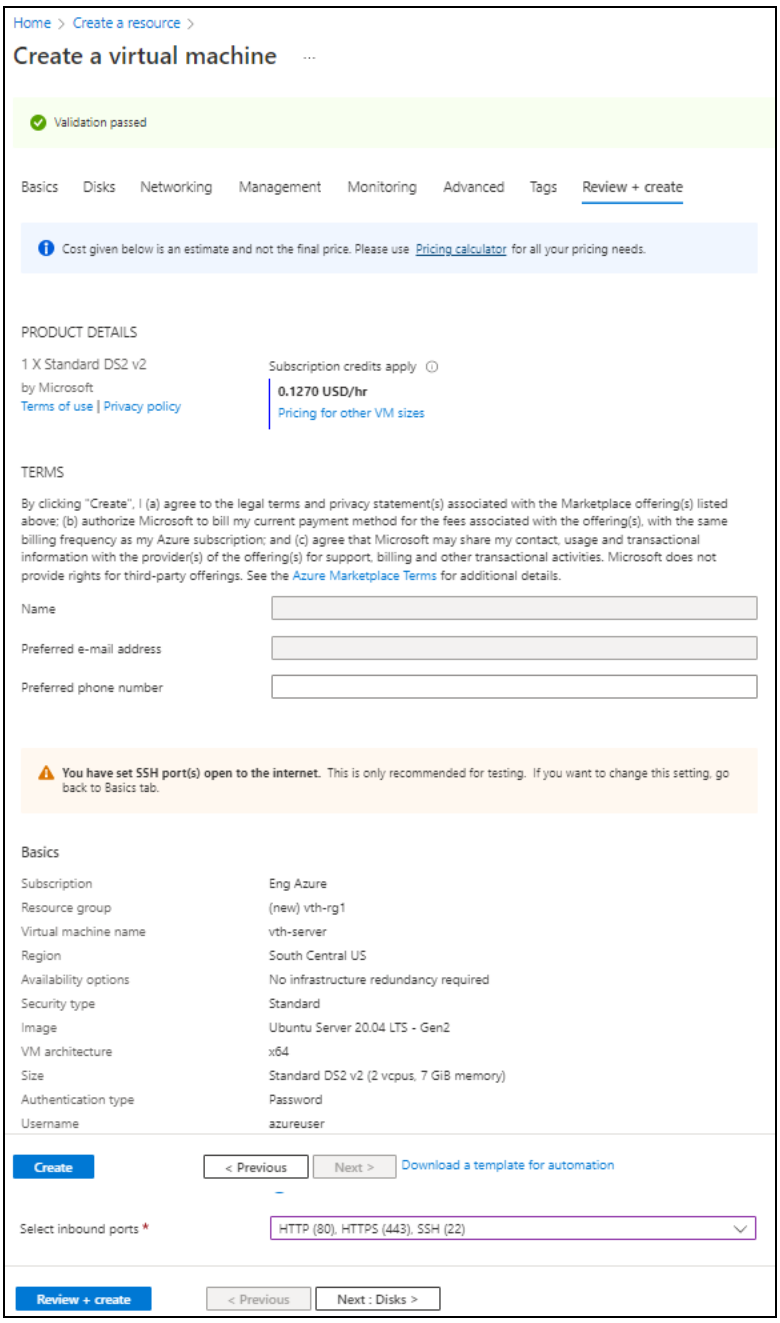
13. Click **Next : Tags** at the bottom of the window.
14. Select or enter the information to categorized resources in the **Tags** tab as needed.

Figure 10 : Create a virtual machine window - Tags tab



15. Click **Next : Review + create** at the bottom of the window.
    The fields **Name** and **Preferred e-mail address** are auto-populated as per the Azure account.

Figure 11 : Create a virtual machine window - Review + create tab



16. Click **Create** at the bottom of the window.
    The Server virtual machine gets created and listed in the **Home** > **Azure Services** > **Virtual machine** window.

17. SSH the Server virtual machine and run the following command to install Apache:
    ```
    sudo apt install apache2
    ```
    While the Apache server is getting installed, you get a prompt to continue further. Enter 'Y' to continue. After the installation is complete, a newline prompt is displayed.

Create a Client Machine

To create a Client machine, perform the following steps:

1. From Home, navigate to **Azure Services** > **Create a resource** > **Virtual machine** and click **Create**.
   The **Create a virtual machine** window is displayed.
2. Select or enter the following mandatory information in the **Basics** tab:

   Project details

   - Subscription
   - Resource group

   Instance details

   - Virtual machine name - Client machine
   - Region
   - Image
   - Size

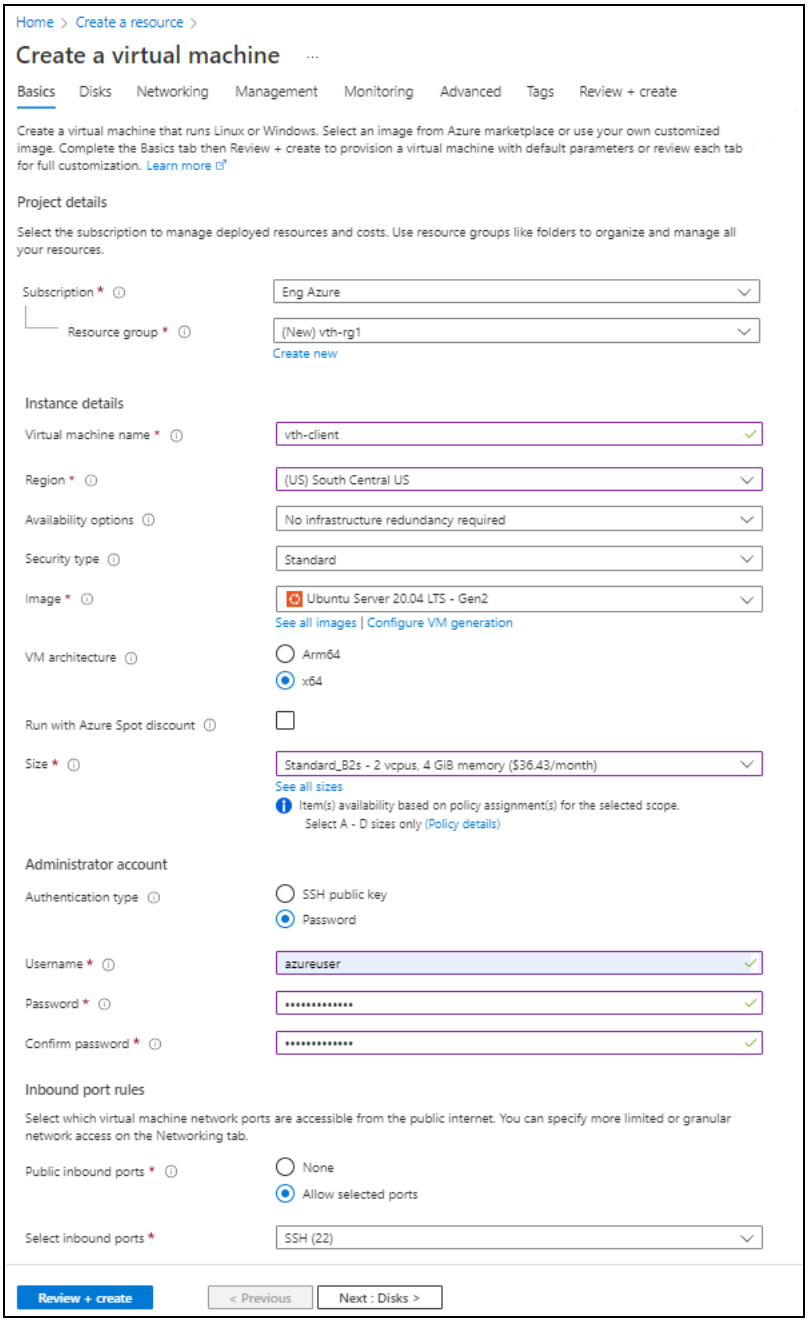
   Administrator account

   - Depending upon the Authentication type selected, provide the information.

   Inbound port rules

   - Public inbound ports
   - Select inbound ports

Figure 12 : Create a virtual machine window - Basics tab



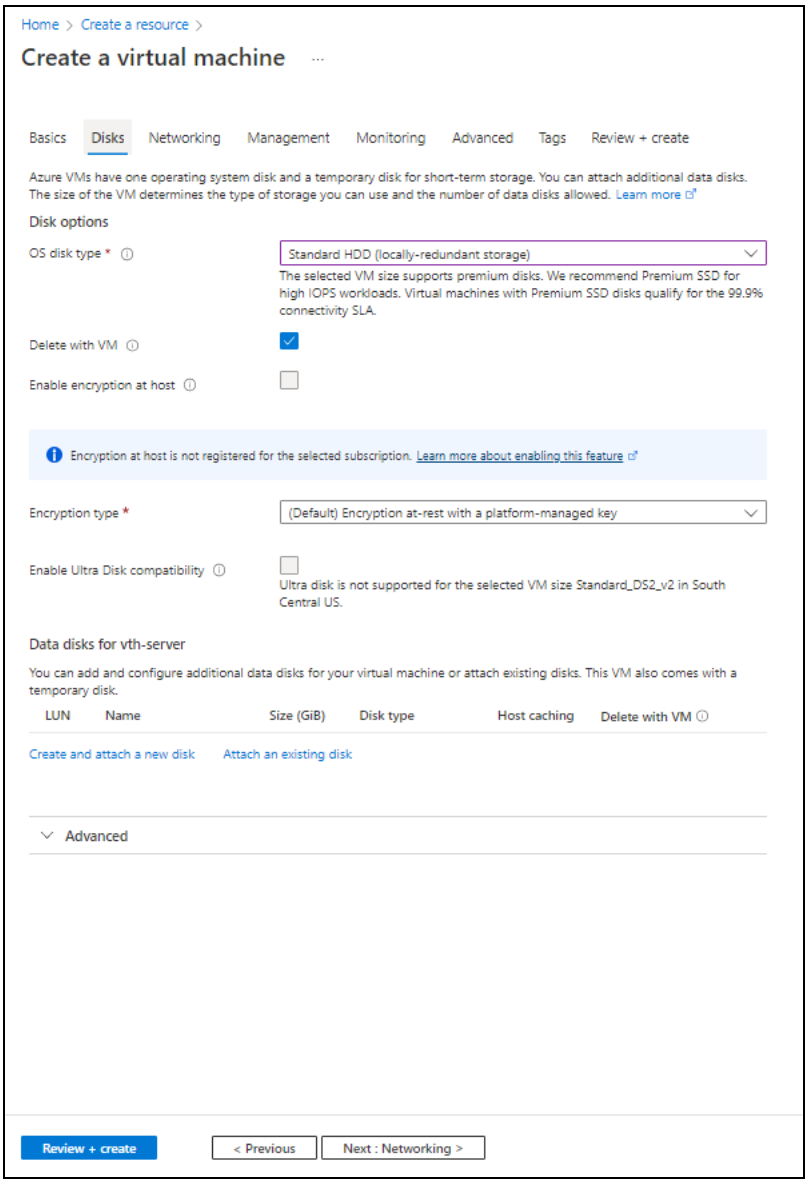
3. Leave the remaining fields as is and click **Next : Disks** at the bottom of the window.

4. Select or enter the following mandatory information in the **Disks** tab:

   Disk options

   - OS disk type
   - Encryption type

   Figure 13 : Create a virtual machine window - Disks tab



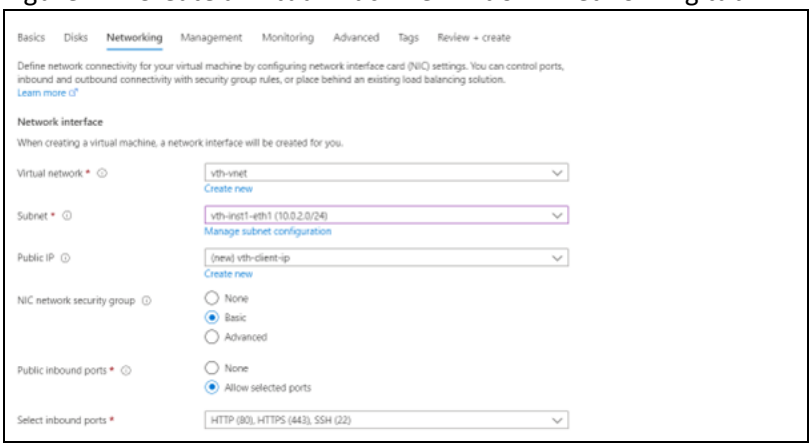
5. Leave the remaining fields as is and click **Next : Networking** at the bottom of the window.

6. Select or enter the following mandatory information in the **Networking** tab:

   Network interface

   - Virtual network
   - Subnet: Data subnet (Ethernet 1)
   - Select inbound ports

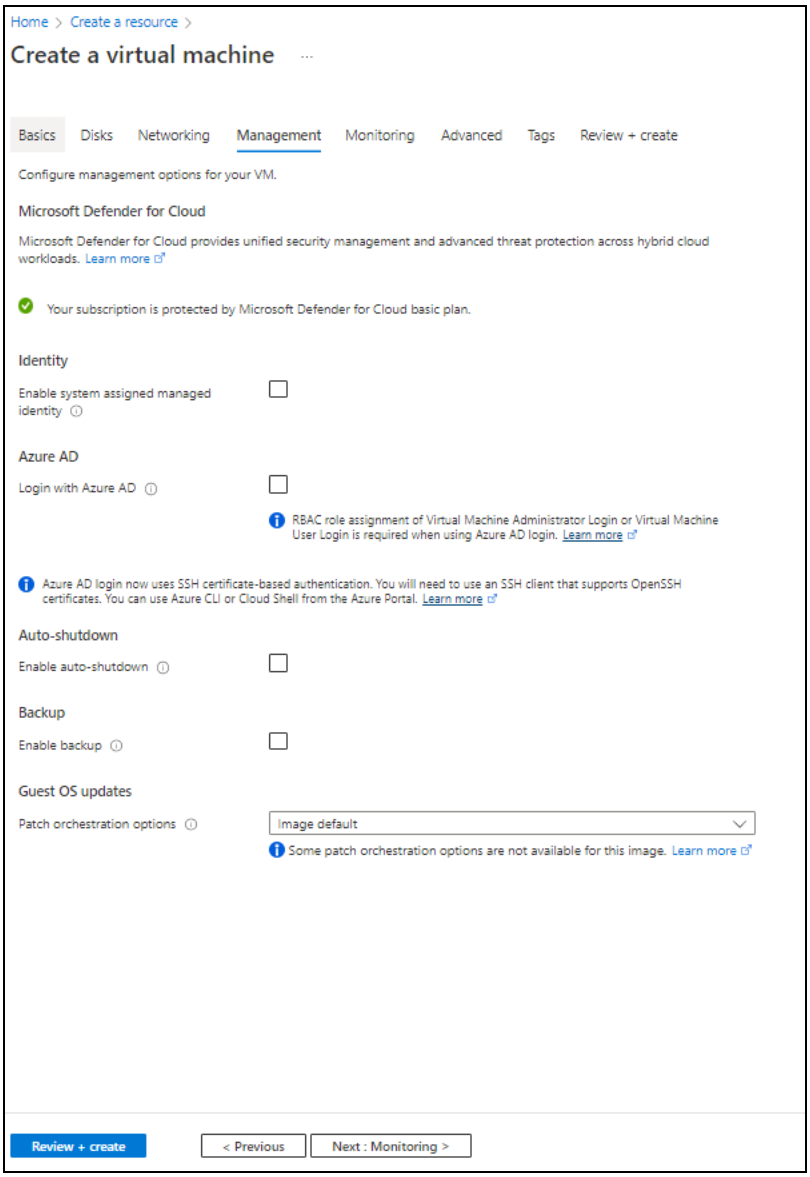
Figure 14 : Create a virtual machine window - Networking tab



7. Leave the remaining fields as is and click **Next : Management** at the bottom of the window.

8. Select or enter the information in the **Management** tab as needed.

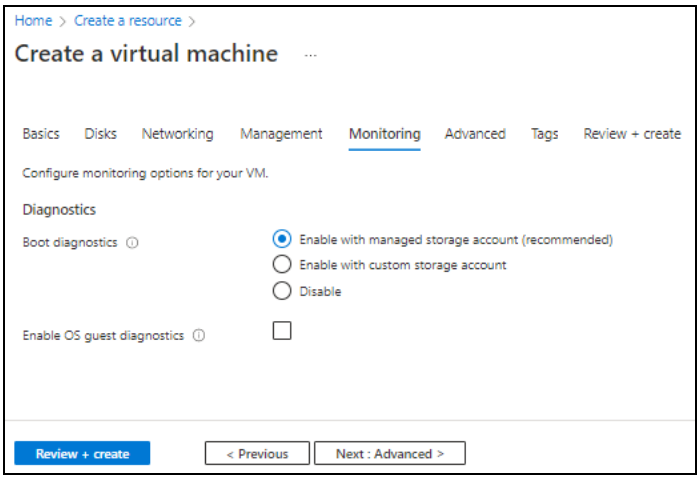
Figure 15 : Create a virtual machine window - Management tab



9. Click **Next : Monitoring** at the bottom of the window.

10. Select the monitoring options in the **Monitoring** tab as needed.

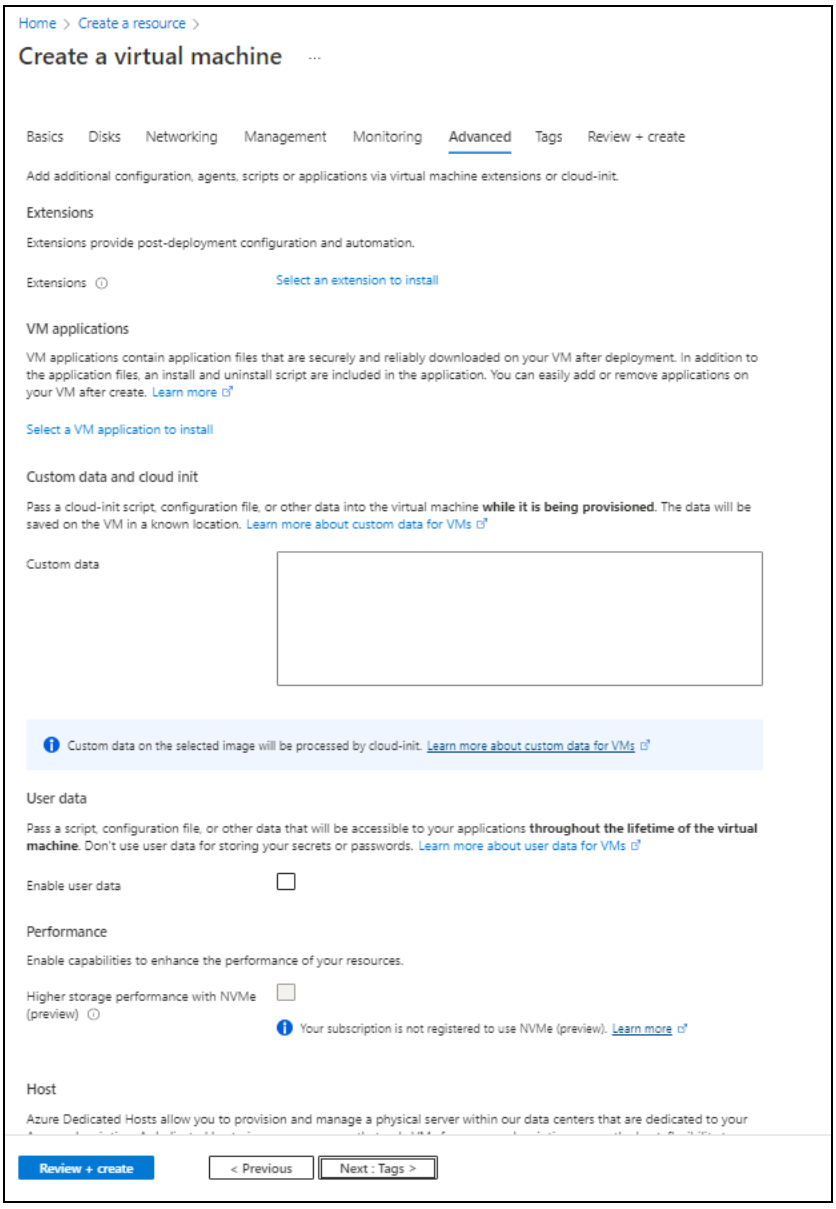
Figure 16 : Create a virtual machine window - Monitoring tab



11. Click **Next : Advanced** at the bottom of the window.

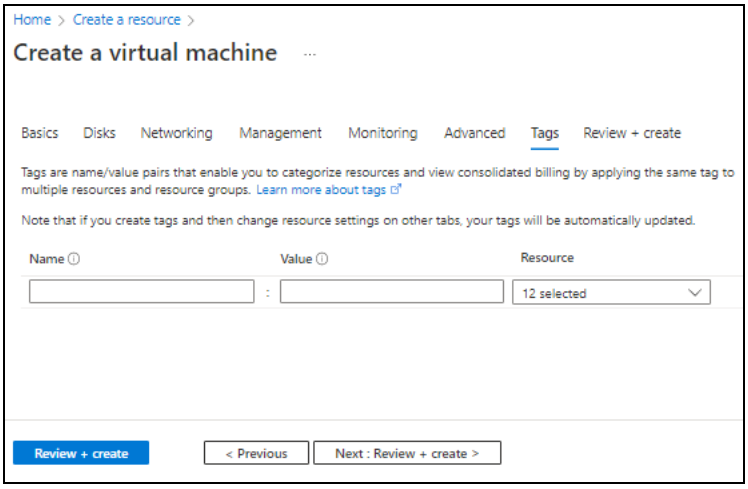
12. Select or enter the additional configuration in the **Advanced** tab as needed.

Figure 17 : Create a virtual machine window - Advanced tab



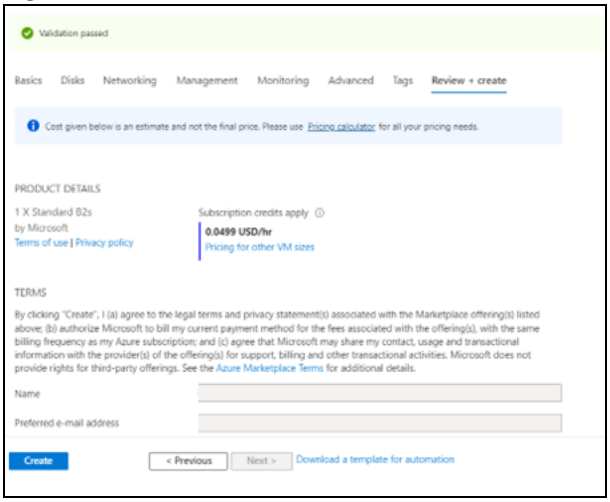
13. Click **Next : Tags** at the bottom of the window.
14. Select or enter the information to categorized resources in the **Tags** tab as needed.

Figure 18 : Create a virtual machine window - Tags tab



15. Click **Next : Review + create** at the bottom of the window.
The fields **Name** and **Preferred e-mail address** are auto-populated as per the Azure account.

Figure 19 : Create a virtual machine window - Review + create tab



16. Click **Create** at the bottom of the window.
The Client machine gets created and listed in the **Home** > **Azure Services** > **Virtual machine** window.

Configure vThunder as an SLB

The following topics are covered:

- Initial Setup
- Change Password
- Deploy vThunder as an SLB

Initial Setup

Before deploying vThunder on Azure cloud as an SLB, configure the corresponding parameters in the PowerShell template.

To configure the parameters, perform the following steps:

1. Open the PS_TMPL_2NIC_1VM_SLB_CONFIG_PARAM.json with a text editor.

   NOTE: Each parameter has a default value mentioned in the parameter file.

2. Configure a SLB server host or domain.
   The SLB server host value is the data NIC's private IP address instance acting as the server.
   Instead of a host, you can also use a domain name. To do so, replace the key 'host' with 'fqdn-name' and provide a domain name instead of the IP address.

```
      "slbServerHostOrDomain": {
        "server-name": "s1",
        "host": "10.0.2.8",
        "metadata": {
          "description": "SLB server host/fqdn-name. To use domain name
replace host with fqdn-name and ip address with domain name"
        }
      },
```

3. Configure SLB server ports.

```
      "slbServerPortList": {
        "value": [
          {
            "port-number": 53,
            "protocol": "udp"
          },
          {
            "port-number": 80,
```

```
            "protocol": "tcp"
          },
          {
            "port-number": 443,
            "protocol": "tcp"
          }
        ]
      },
```

4. Configure Service Group List ports.

```
      "serviceGroupList": {
        "value": [
            {
              "name":"sg443",
              "protocol":"tcp",
              "member-list": [
                {
                  "name":"s1",
                  "port":443
                }
              ]
            },
            {
              "name":"sg53",
              "protocol":"udp",
              "member-list": [
                {
                  "name":"s1",
                  "port":53
                }
              ]
            },
              {
              "name":"sg80",
              "protocol":"tcp",
              "member-list": [
                {
                  "name":"s1",
```

```
                    "port":80
                  }
                ]
              }
            ]
        },
```

5. Configure a Virtual Server.
   The virtual server default name is “vs1”.

```
      "virtualServerList": {
        "virtual-server-name": "vs1",
        "metadata": {
          "description": "virtual server is using ethernet 1 ip
address"
        },
        "value": [
          {
            "port-number":53,
            "protocol":"udp",
            "auto":1,
            "service-group":"sg53"
          },
          {
            "port-number":80,
            "protocol":"http",
            "auto":1,
            "service-group":"sg80"
          },
          {
            "port-number":443,
            "protocol":"https",
            "auto":1,
            "service-group":"sg443"
          }
        ]
       },
```

6. Configure SSL.

```
"sslConfig": {
    "requestTimeOut": 40,
    "Path": <absolute path of the ssl certificate file>",
    "File": "<certificate-name>",
    "CertificationType": "pem"
  }
```

NOTE: By default, SSL configuration is disabled i.e. no SSL configuration is applied.

Example The sample values for the SSL certificate are as shown below:

```
"sslConfig": {
    "requestTimeOut": 40,
    "Path": "C://Users//..//..//..//server.pem" or
"C:\Users\..\..\..\certs\server.pem",
    "File": "server",
    "CertificationType": "pem"
                }
```

7. Provide the resource group name.

```
"resourceGroupName: "vth-rg1"
"vThUsername": "admin"
```

NOTE: Do not change the vThunder instance username.

8. Verify if all the configurations in the PS_TMPL_2NIC_1VM_SLB_CONFIG_PARAM.json file are correct and save the changes.

Change Password

To change the password, perform the following steps:

1. Run the following command to change password:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_2NIC_1VM_CHANGE_PASSWORD_
2.ps1
```

NOTE: It is highly recommended to change the default password provided by the A10 Networks Support when you log in the vThunder instance for the first time.

2. Provide the default and new password when prompted:

```
Enter Default Password:***
Enter New Password:***
Confirm New Password:***
```

The default password is provided by the A10 Networks Support. The new password should follow the Default password policy. For more information, see Default Password Policy.

Deploy vThunder as an SLB

To deploy vThunder on Azure cloud as an SLB, perform the following steps:

1. From PowerShell, navigate to the folder where you have downloaded the PowerShell template.
2. Run the following command to create vThunder SLB instance using the same resource group:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_2NIC_1VM_SLB_CONFIG_3.ps1 -
resourceGroup <resource_group_name>
```

Example:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_2NIC_1VM_SLB_CONFIG_3.ps1 -
resourceGroup vth-rg1
```

A message is prompted to upload the SSL certificate.

```
SSL Certificate
Do you want to upload ssl certificate ?
[Y] Yes  [No] No [?] Help (default is "N"): Y
Public IP Name: vth-inst1-mgmt-nic1-ip
Ethernet-1 Private IP: 10.0.2.47
SLB Server Host IP: 10.0.2.8
Virtual Server Name: vs1
Resource Group Name: vth-rg1
Instance Public IP: 20.165.38.180
```

```
configured ethernet 1 ip
Configured server
Configured service group
0
Configured virtual server
SSL Configured.
Configurations are saved on partition: shared
```

If you want to upload SSL certificate, enter 'Y'. The certificate available in the sslConfig path is uploaded.

3. If the SSL Certificate upload is successful, a message 'SSL Configured' is displayed.

Access vThunder using CLI or GUI

vThunder can be accessed using any of the following ways:

- Access vThunder using CLI
- Access vThunder using GUI

Access vThunder using CLI

To access vThunder using CLI, perform the following steps:

1. Open PuTTY.
2. Enter or select the following basic information in the PuTTy Configuration window:
   - Hostname: Public IP of Virtual Machine Instance
     Here, Public IP of **`vth-inst1`**.
   - Connection Type: SSH
3. Click **Open**.
4. In the active PuTTY session, login with the recently changed password:

```
login as: xxxx <---Enter username provided by A10 Networks Support--->
Using keyboard-interactive authentication.
Password: xxxx <---Enter your password--->
```

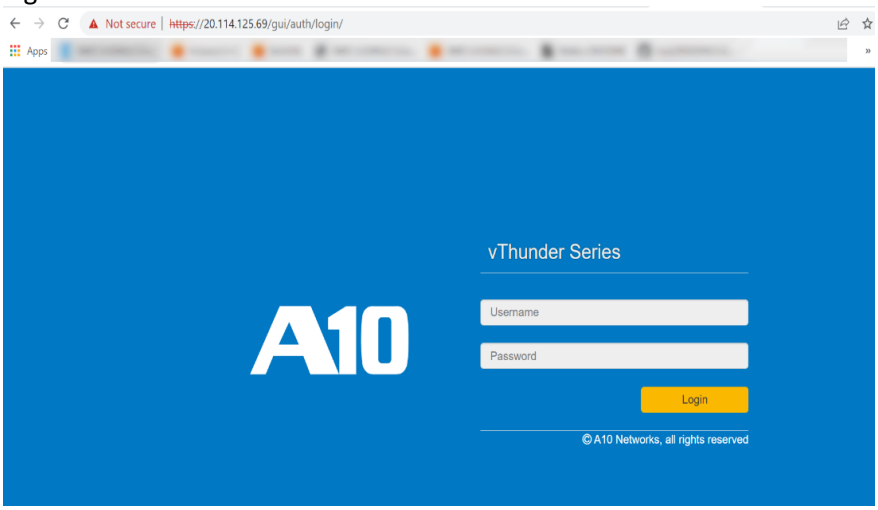
```
Last login: Day MM DD HH:MM:SS from a.b.c.d

System is ready now.

[type ? for help]

vThunder> enable <---Execute command--->
Password:<---just press Enter key--->
vThunder#config <---Configuration mode--->
```

Access vThunder using GUI

To access vThunder using GUI, perform the following steps:

1. Open any browser.
2. Enter *https://<vthunder_public_IP>/gui/auth/login/* in the address bar.

Figure 20 : vThunder GUI



3. Enter the recently configured user credentials.
   The home page gets displayed.

Verify Deployment

To verify vThunder SLB deployment using the PowerShell template, perform the following steps:

1. Run the following command on vThunder:

```
vThunder(config)#show running-config
```

If the deployment is successful, the following slb configuration is displayed:

```
interface management
  ip address dhcp
!
interface ethernet 1
  enable
  ip address 10.0.2.47 255.255.255.0
!
!
slb server s1 10.0.2.8
  port 53 udp
  port 80 tcp
  port 443 tcp
!
slb service-group sg443 tcp
  member s1 443
!
slb service-group sg53 udp
  member s1 53
!
slb service-group sg80 tcp
  member s1 80
!
slb virtual-server vs1 use-if-ip ethernet 1
  port 53 udp
    source-nat auto
    service-group sg53
  port 80 http
    source-nat auto
    service-group sg80
  port 443 https
    source-nat auto
    service-group sg443
!
```

```
!
end
```

2. Run the following command on vThunder:

```
vThunder(config)#show pki cert
```

If the deployment is successful, the following SSL configuration is displayed:

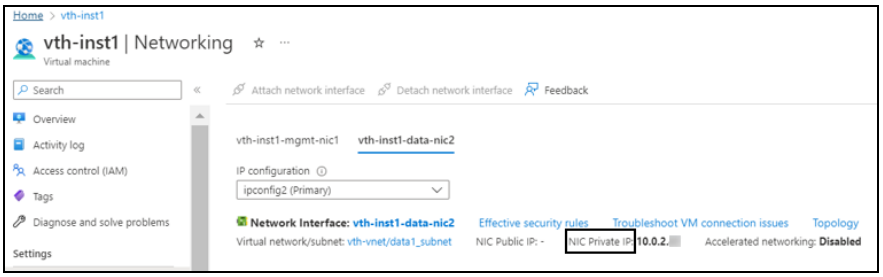
```
Name    Type                        Expiration  Status
-----------------------------------------------------------------
server certificate Jan 28 12:00:00 2028 GMT [Unexpired, Bound]
```

Verify Traffic Flow

To verify the traffic flow from client machine to server machine via vThunder, perform the following:

1. From **Azure Portal** > **Azure Services** > **Resource Group** > <resource_group_name> > <virtual_machine_instance> > **Settings** > **Networking**.
   Here, **`vth-inst1`** is the vThunder instance name.
2. Copy the Private IP address of the data subnet.

   Figure 21 : vThunder instance Data Subnet Private IP



3. Select your client instance from the **Virtual machine** list.
   Here, **`vth-client`** is the client instance name.
4. SSH your client machine and run the following command to verify the traffic flow:

```
curl <vThunder_instance_data_private_IPv4_Address>
```

Example

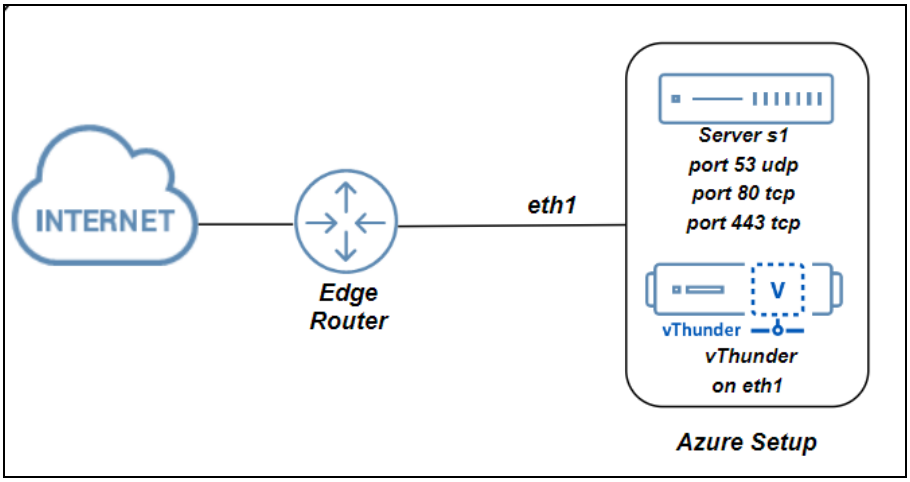
```
curl 10.0.2.4
```

Verify if a response is received.

Deploy PowerShell A10-vThunder_ADC-2NIC-1VM-GLM

Figure 22 shows the 2NIC-1VM-GLM deployment topology. Using the PowerShell template, one vThunder instance containing one management interface and one data interface with GLM integration can be deployed.

Figure 22 : 2NIC-1VM-GLM Topology



The following topics are covered:

System Requirements 54
Create vThunder Instance 57
Configure Server and Client Machine 61
Configure vThunder as an SLB 78
Configure vThunder GLM 84
Access vThunder using CLI or GUI 85
Verify Deployment 87
Verify Traffic Flow 89

System Requirements

The PowerShell template will display the default values when you download and save the files on your local machine. You can modify the default values as required for your deployment.

You need the following to deploy vThunder on the Azure cloud:

Table 4 : System Requirements

Resource Name	Description	Default Value
Azure Resource Group	A resource group with the specified name and location is created, if it doesn't exist. All the resources required for this template is created under the resource group.	Here, the Azure resource group name used is `vth-rg1`.
Azure Storage Account	A storage account is created inside the resource group, if it doesn't exist. If the storage name already exists, the following error is displayed “The storage account named vthunderstorage already exists under the subscription". **Performance**: Standard **Replication**: Read-access geo-redundant storage (RA-GRS) **Account kind**: Storagev2 (general purpose v2)	`vthunderstorage`
Virtual Machine (VM) Instance	A virtual machine instance is created for vThunder. **Product**: A10 vThunder	`vth-inst1`

Resource Name	Description	Default Value
	Operating system: Linux **Default Size**: Standard_DS2v2 (4 vCPUs, 16 GiB Memory) **NOTE:** Before selecting any VM size, it is highly recommended to do an assessment of your projected traffic. Table 5 lists the supported VM sizes.	
Virtual Cloud Network [VCN]	A virtual network is assigned to the virtual machine instance.	`vth-vnet` Address prefix for virtual network: 10.0.0.0/16

Subnet	Two subnets are created with an address prefix each.	Subnet1:
		`10.0.1.0/24`
		Subnet2:
		`10.0.2.0/24`

Network Interface Card [NIC]	Two types of interfaces are created for each vThunder instance: • Management Interface with public IP • Data Interface with primary private IP [Ethernet 1]	`vth-inst1-mgmt-nic1` `10.0.1.5` `vth-inst1-data-nic2` `10.0.2.5 [Primary IP]`
Network Security Group	A security group is created for all the associated default interfaces.	`vth-nsg`

Resource Name	Description	Default Value
[NSG]		

Supported VM Sizes

Table 5 : Supported VM sizes

Series	Size	Qualified Name
A series	Standard A2 Standard A2v2 Standard A2mv2 Standard A4v2 Standard A4mv2 Standard A3 Standard A4 Standard A8v2	Standard_A2 Standard_A2_v2 Standard_A2m_v2 Standard_A4_v2 Standard_A4m_v2 Standard_A3 Standard_A4 Standard_A8_v2
B series	Standard B2s Standard B2ms Standard B4ms	Standard_B2_s Standard_B2ms Standard_B4ms
D series	Standard D2v2 Standard DS2v2 Standard D4v3 Standard D4sv3 Standard D3v2	Standard_D2_v2 Standard_DS2_v2 Standard_D4_v3 Standard_D4s_v3 Standard_D3_v2

Series	Size	Qualified Name
	Standard Ds3v2 Standard D5v2	Standard_Ds3_v2 Standard_D5_v2
F series	Standard F4s Standard F8 Standard F16s	Standard_F4s Standard_F8 Standard_F16s

Azure is going to retire a few of the above listed VM sizes soon. For the latest updates, see Virtual Machine series | Microsoft Azure.

For more information on Windows and Linux VM sizes, see

https://docs.microsoft.com/en-us/azure/virtual-machines/sizes-general

https://docs.microsoft.com/en-us/azure/virtual-machines/linux/sizes.

Create vThunder Instance

The following topics are covered:

- Initial Setup
- Deploy vThunder

Initial Setup

Before deploying vThunder on Azure cloud, configure the corresponding parameters in the PowerShell template.

To configure the parameters, perform the following steps:

1. Navigate to the folder where you have downloaded the PowerShell template, and open the PS_TMPL_2NIC_1VM_PARAM.json with a text editor.

NOTE: Each parameter has a default value mentioned in the parameter file.

2. Provision the vThunder instance by entering the default admin credentials as follows:

```
"adminUsername": {
  "value": "vth-user"
},
"adminPassword": {
  "value": "vth-Password"
},
```

NOTE: This is a mandatory step during VM creation. Once the device is provisioned, vThunder auto-deletes all users except the default user.

3. Configure a virtual network.

```
"virtual_network": {
  "value": "vth-vnet"
},
```

4. Configure a DNS label prefix.

```
"dnsLabelPrefix": {
  "value": "vth-inst1"
},
```

5. Configure a VM name.

```
"vmName": {
  "value": "vth-inst1"
},
```

6. Set a VM Size for vThunder.

```
"vmSize": {
  "value": "Standard_DS2_v2"
},
```

Use a suitable VM size that supports at least 2 NICs. For VM sizes, see Supported VM Sizes section.

7. Copy the desired vThunder Image Name and Product Name from the Azure Marketplace for A10 vThunder and update the details in the parameter file as follows:

```
"vThunderImage": {
  "value":"vthunder_520_byol"
```

```
},
"publisherName": {
  "value": "a10networks"
},
"productName": {
  "value": "a10-vthunder-adc-520-for-microsoft-azure"
},
```

NOTE: Do not change the publisher name.

8. Configure two network interface cards.

```
"nic1Name": {
  "value": "vth-inst1-mgmt-nic1"
},
"nic2Name": {
  "value": "vth-inst1-data-nic2"
},
```

9. Configure an address prefix and subnet values for each management interface and data interface.

```
"addressPrefixValue": {
  "value": "10.0.0.0/16"
},
"mgmtIntfPrivatePrefix": {
  "value": "10.0.1.0/24"
},
"mgmtIntfPrivateAddress": {
  "value": "10.0.1.5"
},
"eth1PrivatePrefix": {
  "value": "10.0.2.0/24"
},
"eth1PrivateAddress": {
  "value": "10.0.2.4"
},
```

10. Configure a public IP address.

```
  "publicIPAddressName": {
    "value": "vth-vm-ip"
  },
```

11. Configure a Network Security Group.

```
  "networkSecurityGroupName": {
    "value": "vth-nsg1"
  },
```

12. Verify if all the configurations in the PS_TMPL_2NIC_1VM_PARAM.json file are correct and then save the changes.

Deploy vThunder

To deploy vThunder on Azure cloud, perform the following steps:

1. From Start menu, open PowerShell and navigate to the folder where you have downloaded the PowerShell template.
2. Run the following command to create a deployment group in Azure and provide a unique storage account name when prompted.

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_2NIC_1VM_1.ps1 -resourceGroup
<resource_group_name> -location "<location_name>"
```

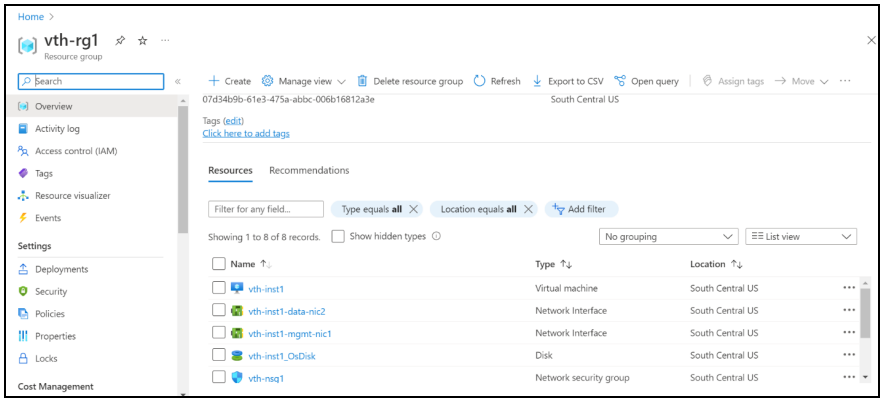
Example:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_2NIC_1VM_1.ps1 -resourceGroup
vth-rg1 -location "south central us"

cmdlet PS_TMPL_2NIC_1VM_1.ps1 at command pipeline position 1
Supply values for the following parameters:
storageaccount: vthunderstorage
vth-rg1
vthunderstorage
South Central US
```

Here, **`vth-rg1`** resource group is created.

3. Verify if all the above listed resources are created in the **Home** > **Azure Services** > **Resource Group** > <resource_group_name>.

Figure 23 : Resource listing in the resource group



Configure Server and Client Machine

The following topics are covered:

- Create a Server Machine
- Create a Client Machine

Create a Server Machine

To create a Server machine, perform the following steps:

1. From **Home**, navigate to **Azure Services** > **Create a resource** > **Virtual machine** and click **Create**.
   The **Create a virtual machine** window is displayed.
2. Select or enter the following mandatory information in the **Basics** tab:

   Project details

   - Subscription
   - Resource group

   Instance details

   - Virtual machine name - Server machine
   - Region

- Image
- Size

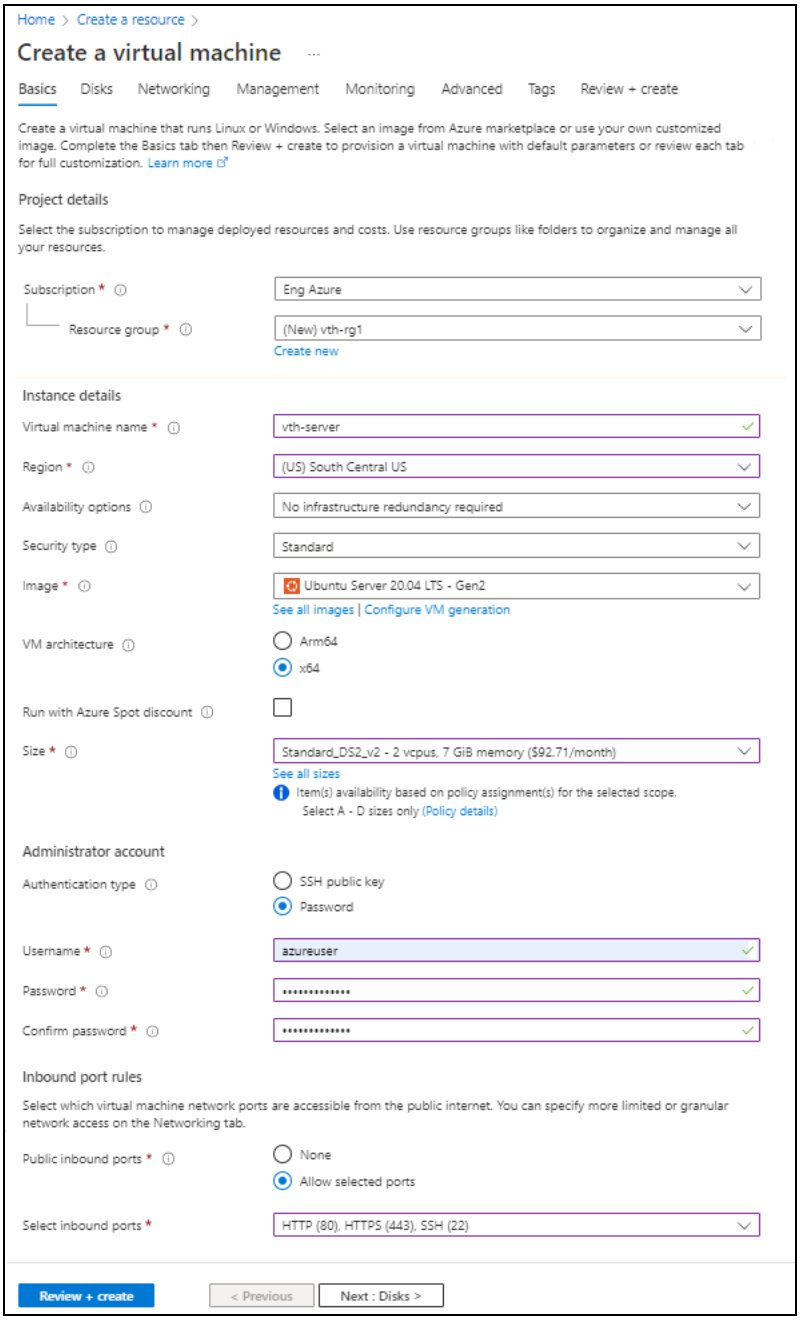
Administrator account

- Depending upon the Authentication type selected, provide the information.

Inbound port rules

- Public inbound ports
- Select inbound ports

Figure 24 : Create a virtual machine window - Basics tab



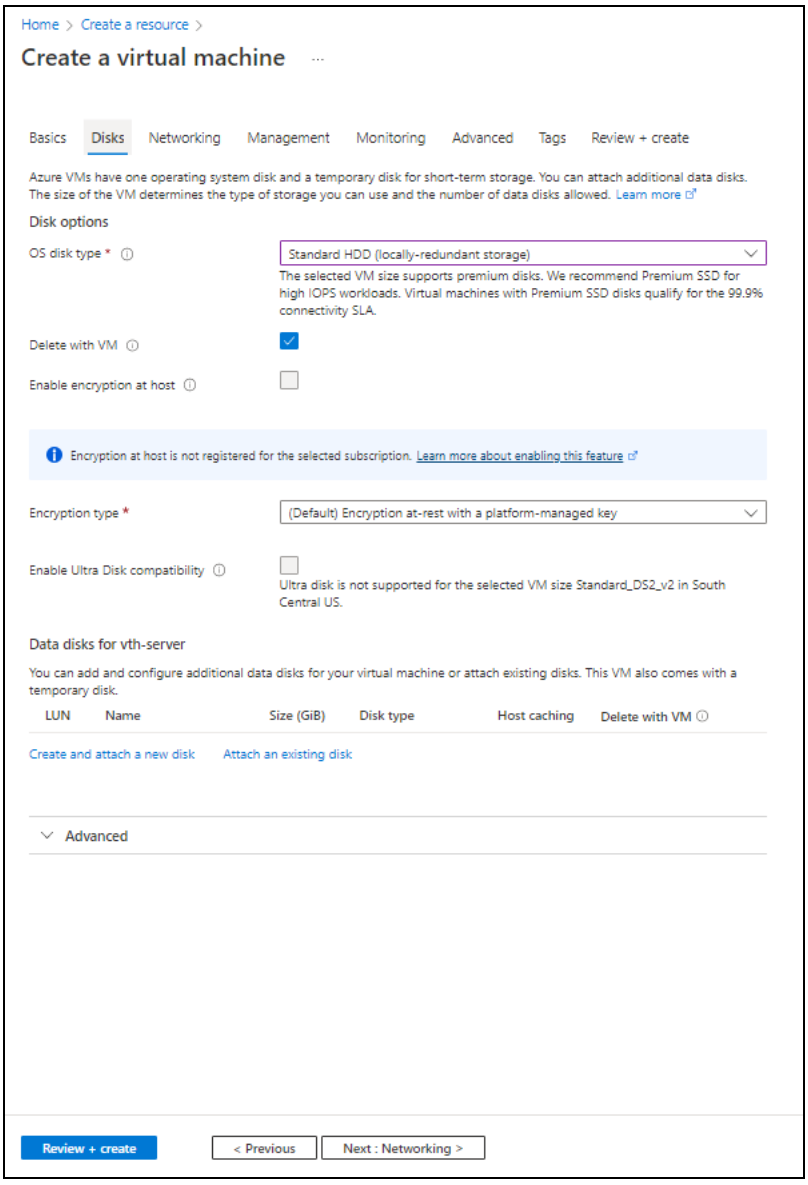
3. Leave the remaining fields as is and click **Next : Disks** at the bottom of the window.

4. Select or enter the following mandatory information in the **Disks** tab:

   Disk options

   - OS disk type
   - Encryption type

   Figure 25 : Create a virtual machine window - Disks tab



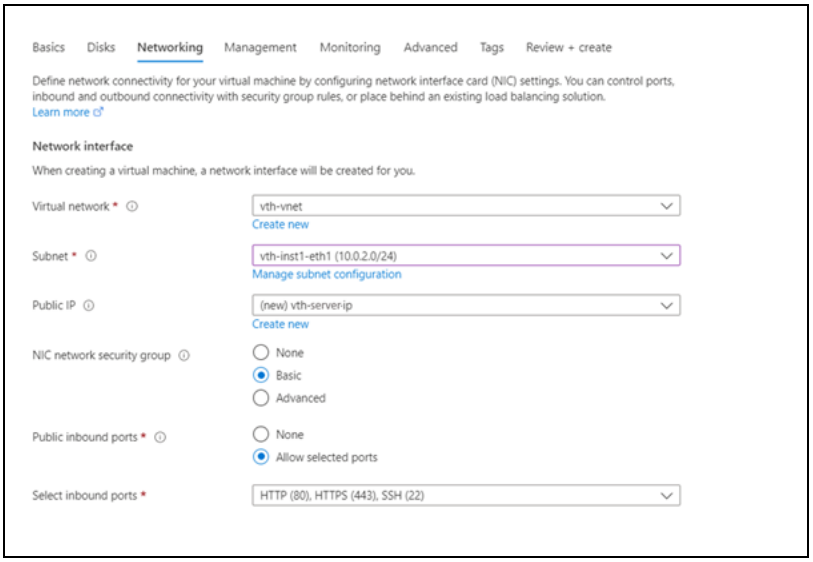
5. Leave the remaining fields as is and click **Next : Networking** at the bottom of the window.

6. Select or enter the following mandatory information in the **Networking** tab:

   Network interface

   - Virtual network
   - Subnet: Data subnet (Ethernet 1)
   - Select inbound ports

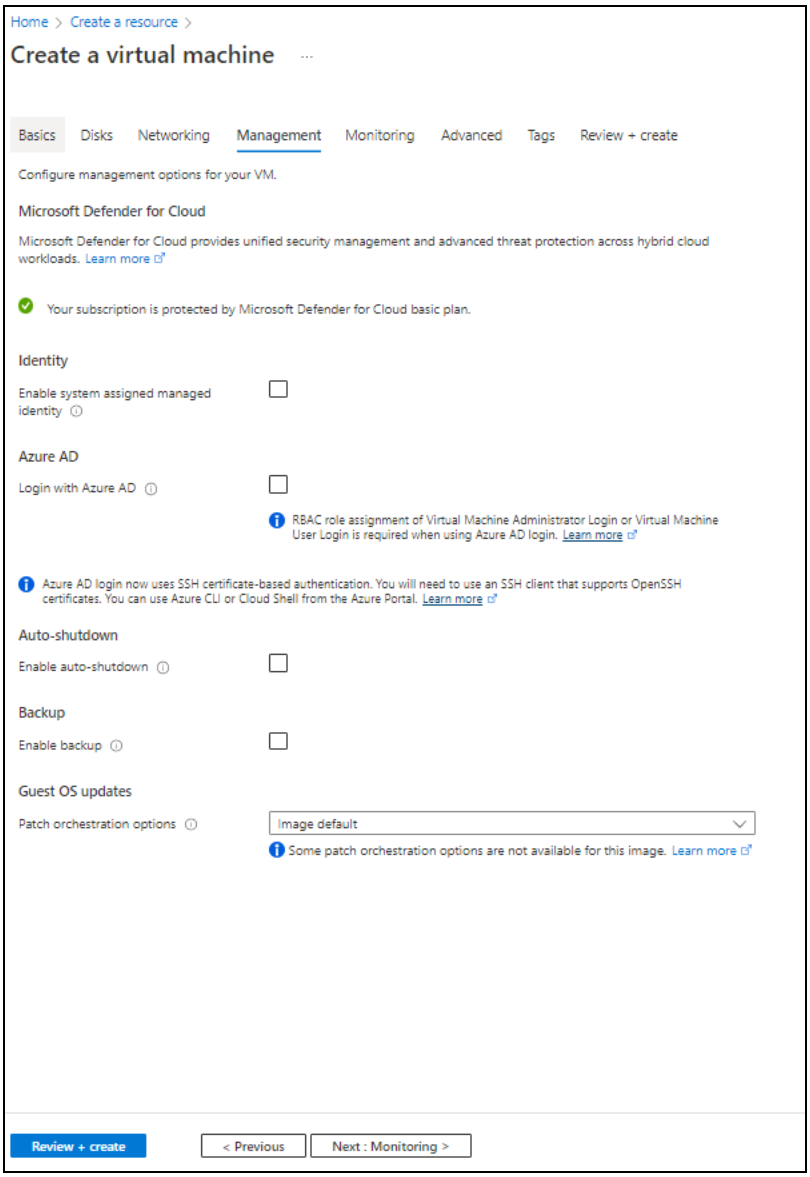
   Figure 26 : Create a virtual machine window - Networking tab



7. Leave the remaining fields as is and click **Next : Management** at the bottom of the window.

8. Select or enter the information in the **Management** tab as needed.

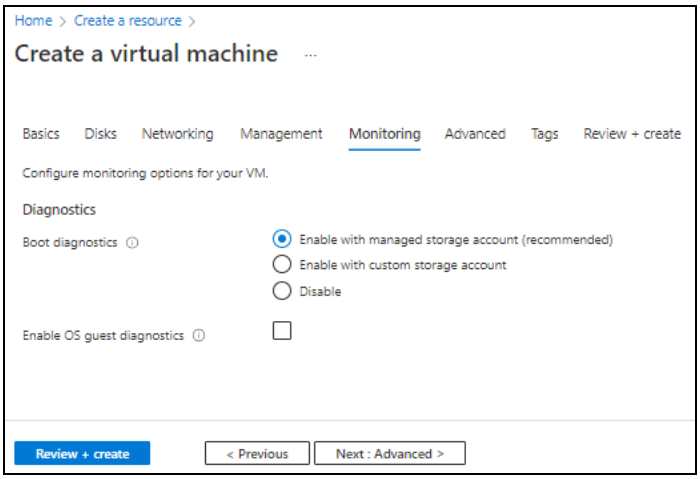
Figure 27 : Create a virtual machine window - Management tab



9. Click **Next : Monitoring** at the bottom of the window.

10. Select the monitoring options in the **Monitoring** tab as needed.

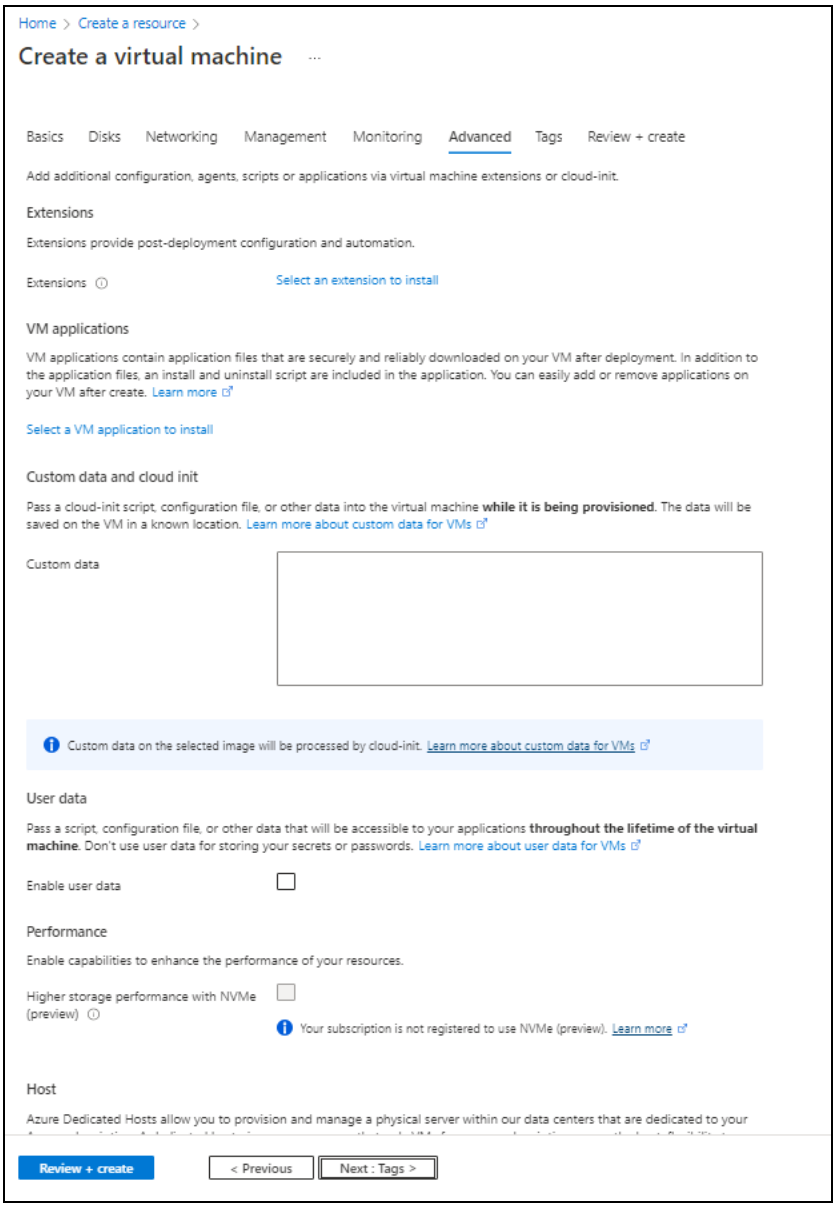
Figure 28 : Create a virtual machine window - Monitoring tab



11. Click **Next : Advanced** at the bottom of the window.

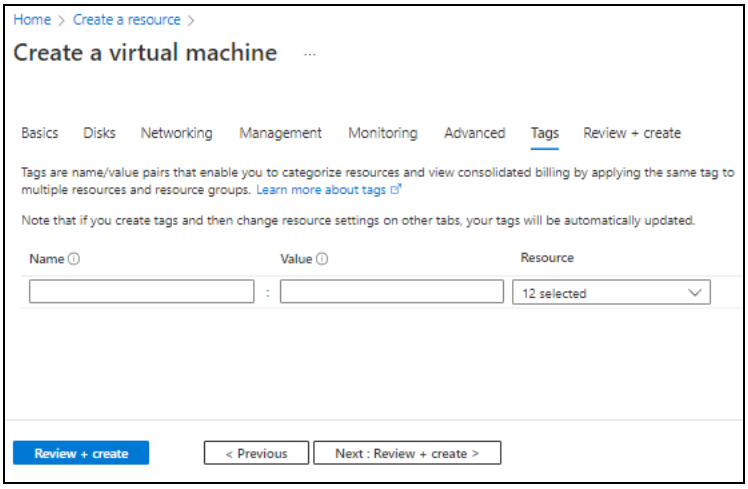
12. Select or enter the additional configuration in the **Advanced** tab as needed.

Figure 29 : Create a virtual machine window - Advanced tab



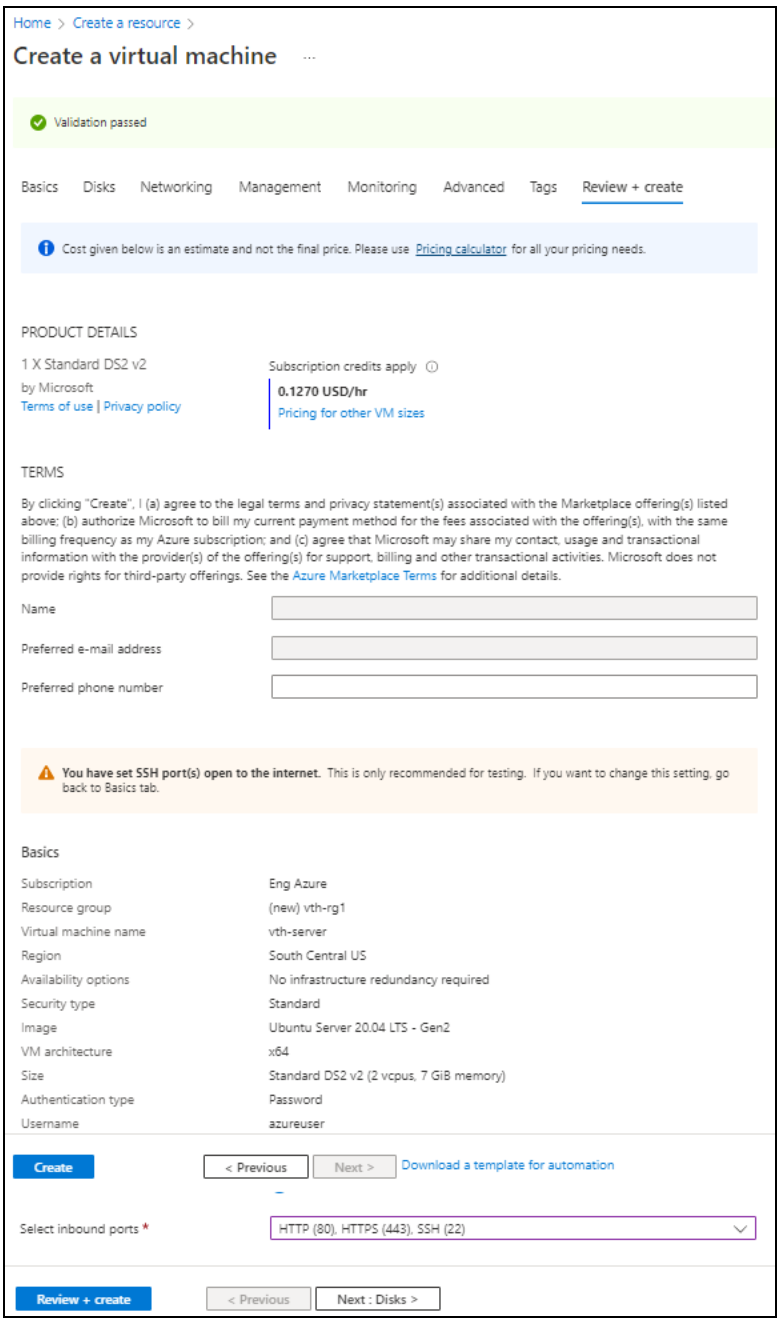
13. Click **Next : Tags** at the bottom of the window.
14. Select or enter the information to categorized resources in the **Tags** tab as needed.

Figure 30 : Create a virtual machine window - Tags tab



15. Click **Next : Review + create** at the bottom of the window.
    The fields **Name** and **Preferred e-mail address** are auto-populated as per the Azure account.

Figure 31 : Create a virtual machine window - Review + create tab



16. Click **Create** at the bottom of the window.
    The Server virtual machine gets created and listed in the **Home** > **Azure Services** > **Virtual machine** window.

17. SSH the Server virtual machine and run the following command to install Apache:
```
sudo apt install apache2
```
While the Apache server is getting installed, you get a prompt to continue further. Enter 'Y' to continue. After the installation is complete, a newline prompt is displayed.

Create a Client Machine

To create a Client machine, perform the following steps:

1. From Home, navigate to **Azure Services** > **Create a resource** > **Virtual machine** and click **Create**.
The **Create a virtual machine** window is displayed.
2. Select or enter the following mandatory information in the **Basics** tab:

Project details

- Subscription
- Resource group

Instance details

- Virtual machine name - Client machine
- Region
- Image
- Size

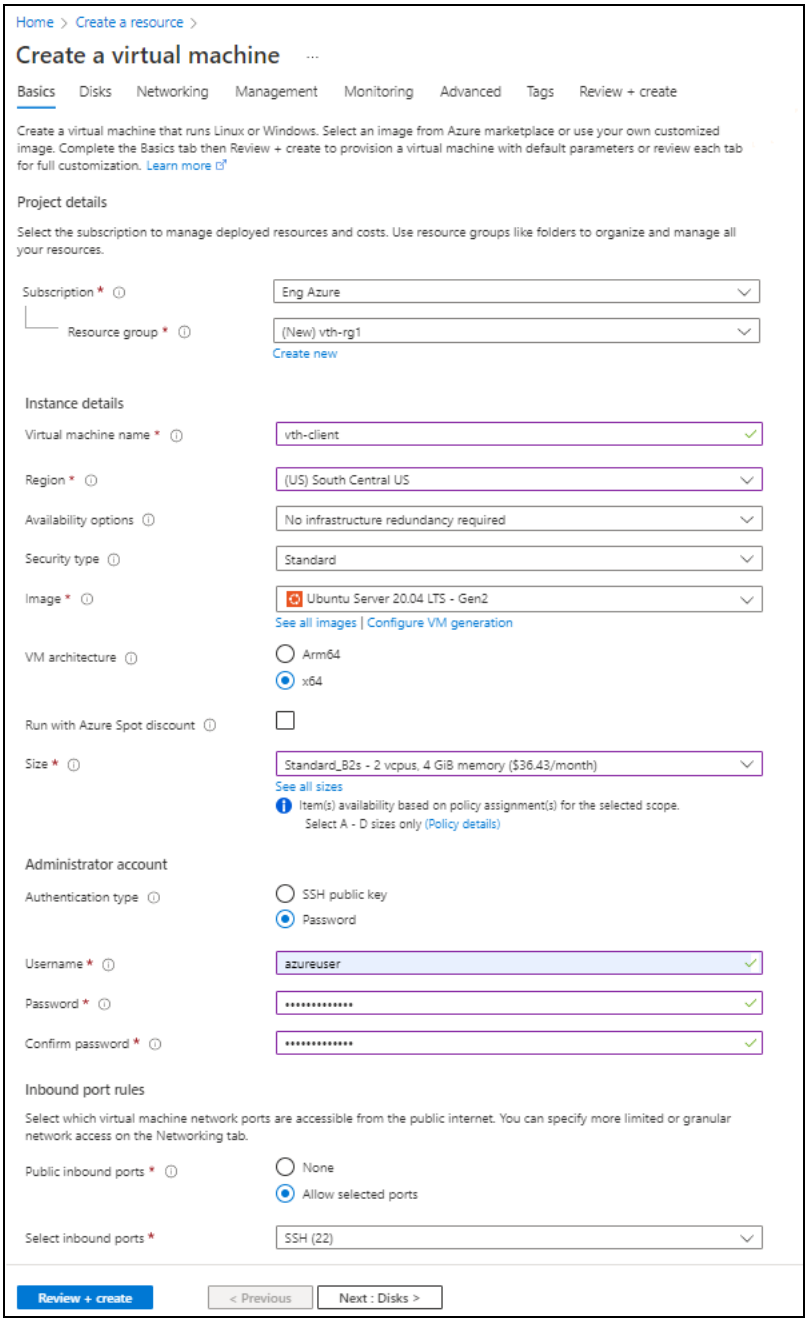
Administrator account

- Depending upon the Authentication type selected, provide the information.

Inbound port rules

- Public inbound ports
- Select inbound ports

Figure 32 : Create a virtual machine window - Basics tab



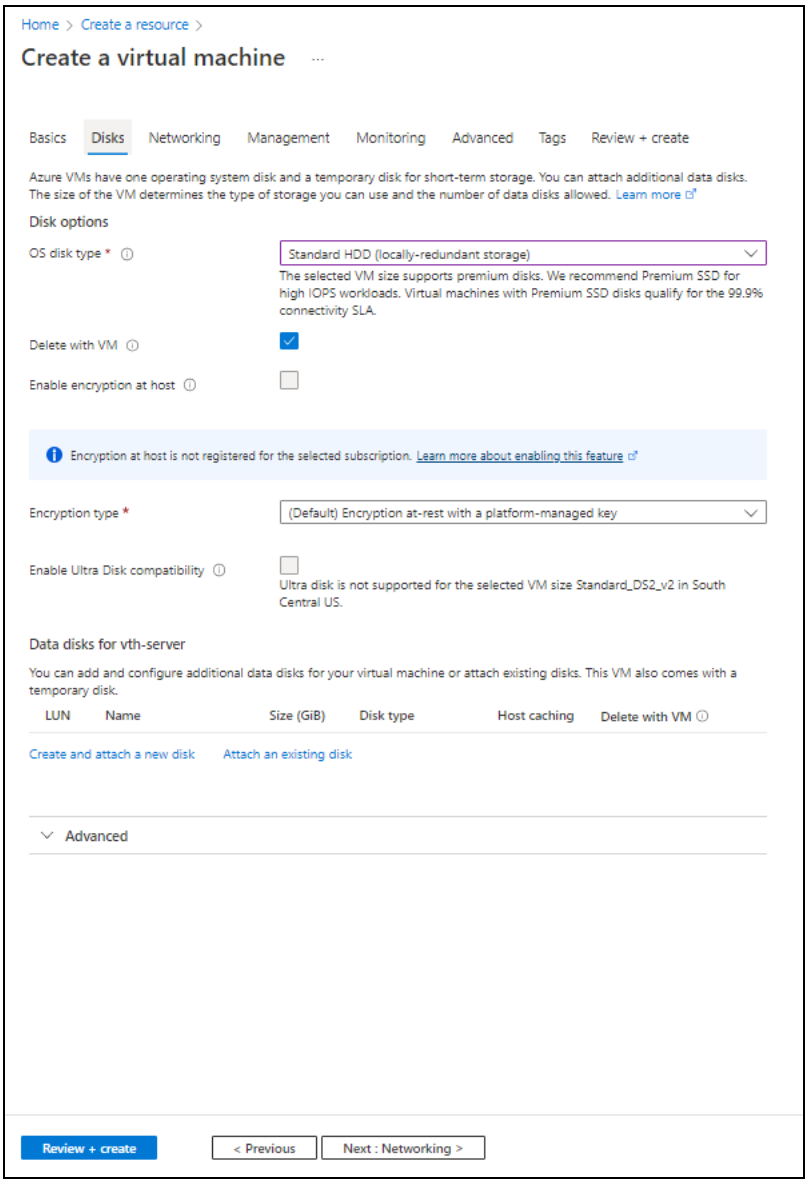
3. Leave the remaining fields as is and click **Next : Disks** at the bottom of the window.

4. Select or enter the following mandatory information in the **Disks** tab:

   Disk options

   - OS disk type
   - Encryption type

   Figure 33 : Create a virtual machine window - Disks tab



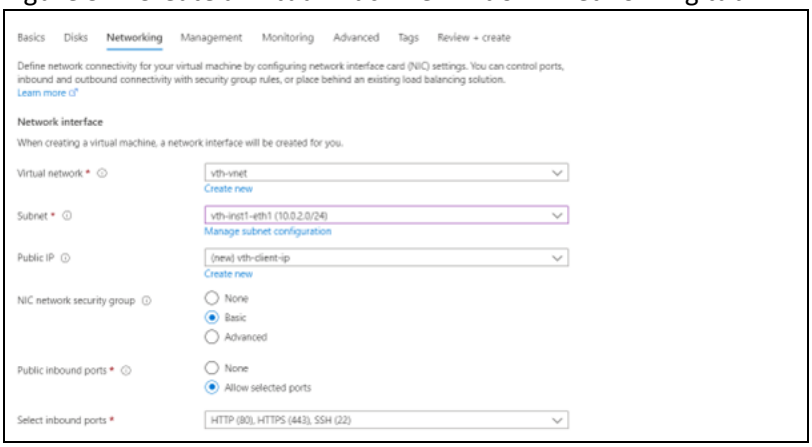
5. Leave the remaining fields as is and click **Next : Networking** at the bottom of the window.

6. Select or enter the following mandatory information in the **Networking** tab:

   Network interface

   - Virtual network
   - Subnet: Data subnet (Ethernet 1)
   - Select inbound ports

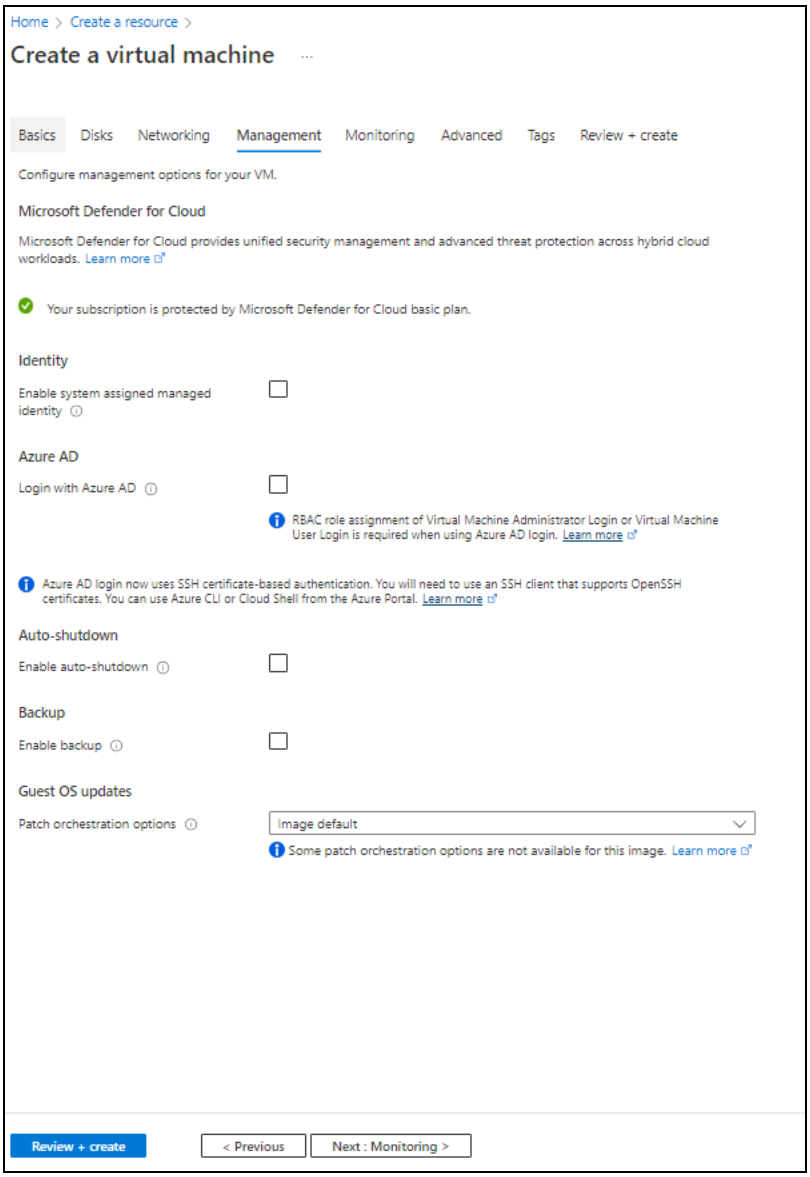
   Figure 34 : Create a virtual machine window - Networking tab



7. Leave the remaining fields as is and click **Next : Management** at the bottom of the window.

8. Select or enter the information in the **Management** tab as needed.

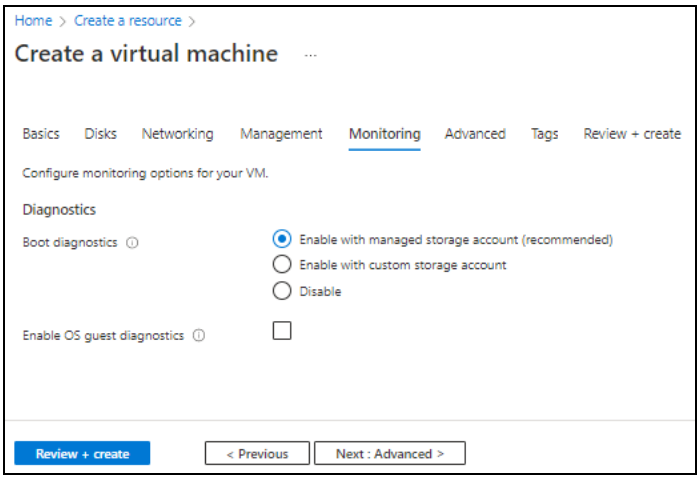
Figure 35 : Create a virtual machine window - Management tab



9. Click **Next : Monitoring** at the bottom of the window.

10. Select the monitoring options in the **Monitoring** tab as needed.

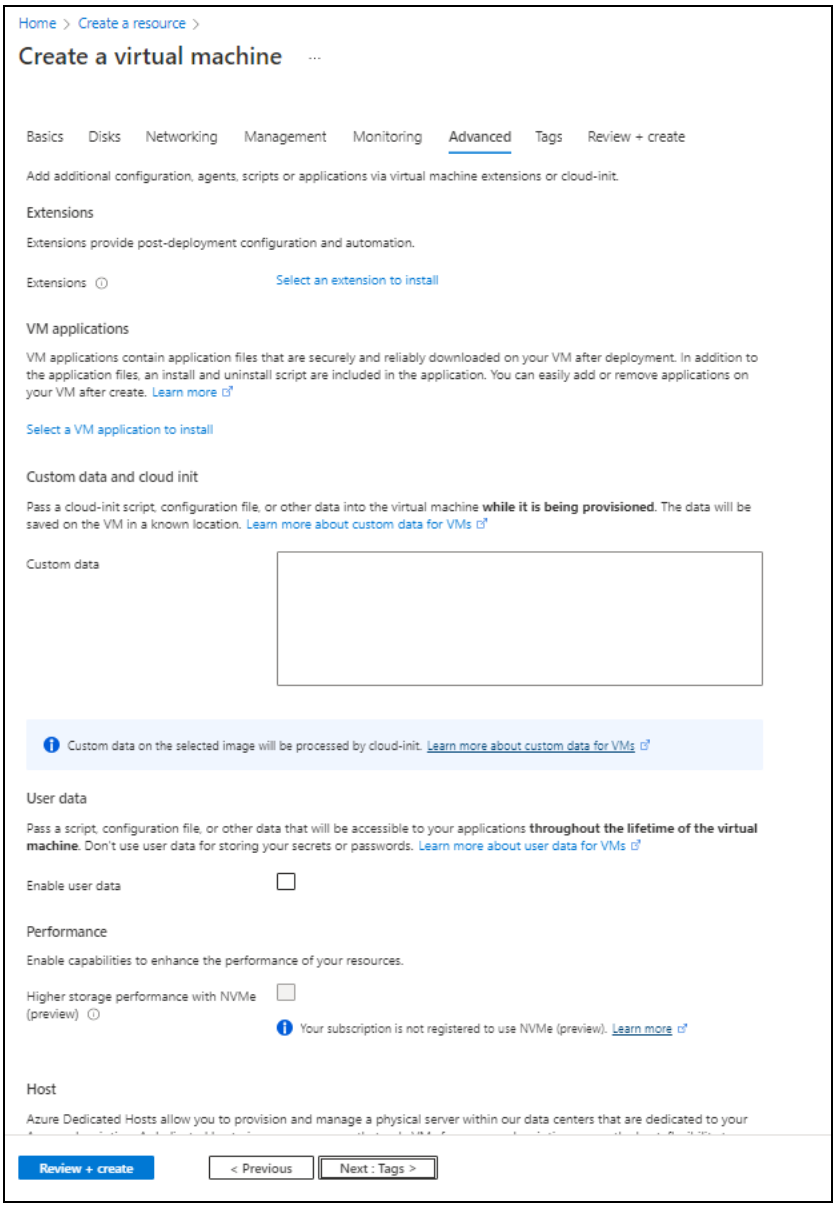
Figure 36 : Create a virtual machine window - Monitoring tab



11. Click **Next : Advanced** at the bottom of the window.

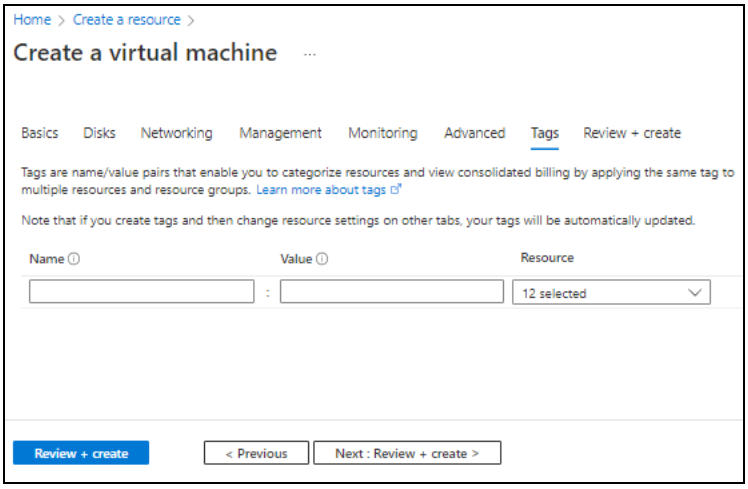
12. Select or enter the additional configuration in the **Advanced** tab as needed.

Figure 37 : Create a virtual machine window - Advanced tab



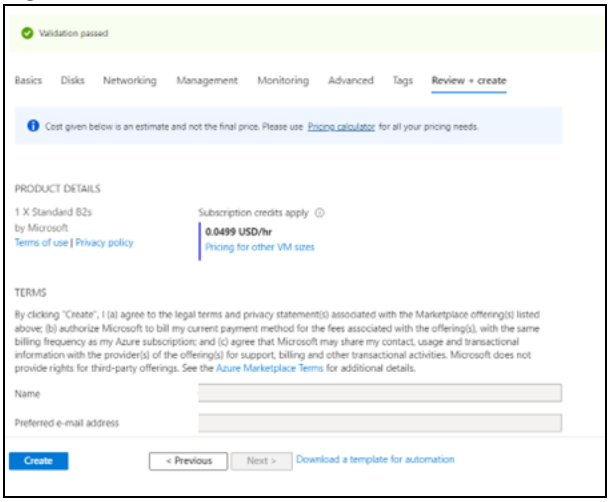
13. Click **Next : Tags** at the bottom of the window.
14. Select or enter the information to categorized resources in the **Tags** tab as needed.

Figure 38 : Create a virtual machine window - Tags tab



15. Click **Next : Review + create** at the bottom of the window.
The fields **Name** and **Preferred e-mail address** are auto-populated as per the Azure account.

Figure 39 : Create a virtual machine window - Review + create tab



16. Click **Create** at the bottom of the window.
The Client machine gets created and listed in the **Home** > **Azure Services** > **Virtual machine** window.

Configure vThunder as an SLB

The following topics are covered:

- Initial Setup
- Change Password
- Deploy vThunder as an SLB

Initial Setup

Before deploying vThunder on Azure cloud as an SLB, configure the corresponding parameters in the PowerShell template.

To configure the parameters, perform the following steps:

1. Open the PS_TMPL_2NIC_1VM_SLB_CONFIG_PARAM.json with a text editor.

   NOTE: Each parameter has a default value mentioned in the parameter file.

2. Configure a SLB server host or domain.
   The SLB server host value is the data NIC's private IP address instance acting as the server.
   Instead of a host, you can also use a domain name. To do so, replace the key 'host' with 'fqdn-name' and provide a domain name instead of the IP address.

```
      "slbServerHostOrDomain": {
        "server-name": "s1",
        "host": "10.0.2.8",
        "metadata": {
          "description": "SLB server host/fqdn-name. To use domain name
replace host with fqdn-name and ip address with domain name"
        }
      },
```

3. Configure SLB server ports.

```
      "slbServerPortList": {
        "value": [
          {
            "port-number": 53,
            "protocol": "udp"
          },
          {
            "port-number": 80,
```

```
            "protocol": "tcp"
          },
          {
            "port-number": 443,
            "protocol": "tcp"
          }
        ]
      },
```

4. Configure service group list ports.

```
      "serviceGroupList": {
        "value": [
            {
              "name":"sg443",
              "protocol":"tcp",
              "member-list": [
                {
                  "name":"s1",
                  "port":443
                }
              ]
            },
            {
              "name":"sg53",
              "protocol":"udp",
              "member-list": [
                {
                  "name":"s1",
                  "port":53
                }
              ]
            },
              {
              "name":"sg80",
              "protocol":"tcp",
              "member-list": [
                {
                  "name":"s1",
```

```
                    "port":80
                  }
                ]
              }
            ]
      },
```

5. Configure a virtual server.
   The virtual server default name is “vs1”.

```
      "virtualServerList": {
        "virtual-server-name": "vs1",
        "metadata": {
          "description": "virtual server is using ethernet 1 ip
address"
        },
        "value": [
          {
            "port-number":53,
            "protocol":"udp",
            "auto":1,
            "service-group":"sg53"
          },
          {
            "port-number":80,
            "protocol":"http",
            "auto":1,
            "service-group":"sg80"
          },
          {
            "port-number":443,
            "protocol":"https",
            "auto":1,
            "service-group":"sg443"
          }
        ]
       },
```

6. Configure SSL.

```
"sslConfig": {
    "requestTimeOut": 40,
    "Path": "<absolute path of the ssl certificate file>",
    "File": "<certificate-name>",
    "CertificationType": "pem"
  }
```

NOTE: By default, SSL configuration is disabled i.e. no SSL configuration is applied.

Example The sample values for the SSL certificate are as shown below:

```
"sslConfig": {
    "requestTimeOut": 40,
    "Path": "C://Users//..//..//..//server.pem” or
“C:\Users\..\..\..\certs\server.pem",
    "File": "server",
    "CertificationType": "pem"
                }
```

7. Provide the resource group name.

```
"resourceGroupName: "vth-rg1"
"vThUsername": "admin"
```

NOTE: Do not change the vThunder instance username.

8. Verify if all the configurations in the PS_TMPL_2NIC_1VM_SLB_CONFIG_PARAM.json file are correct and then save the changes.

Change Password

To change the password, perform the following steps:

1. Run the following command to change password:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_2NIC_1VM_GLM_CHANGE_PASSWORD_
2.ps1
```

NOTE: It is highly recommended to change the default password provided by the A10 Networks Support when you log in the vThunder instance for the first time.

2. Provide the default and new password when prompted:

```
Enter Default Password:***
Enter New Password:***
Confirm New Password:***
```

The default password is provided by the A10 Networks Support. The new password should follow the Default password policy. For more information, see Default Password Policy.

Deploy vThunder as an SLB

To deploy vThunder on Azure cloud as an SLB, perform the following steps:

1. From PowerShell, navigate to the folder where you have downloaded the PowerShell template.
2. Run the following command to create vThunder SLB instance using the same resource group:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_2NIC_1VM_SLB_CONFIG_3.ps1 -
resourceGroup <resource_group_name>
```

Example:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_2NIC_1VM_SLB_CONFIG_3.ps1 -
resourceGroup vth-rg1
```

A message is prompted to upload the SSL certificate.

```
SSL Certificate
Do you want to upload ssl certificate ?
[Y] Yes  [No] No [?] Help (default is "N"): Y
Public IP Name: vth-inst1-mgmt-nic1-ip
Ethernet-1 Private IP: 10.0.2.47
SLB Server Host IP: 10.0.2.8
Virtual Server Name: vs1
Resource Group Name: vth-rg1
Instance Public IP: 20.165.38.180
```

```
configured ethernet 1 ip
Configured server
Configured service group
0
Configured virtual server
SSL Configured.
Configurations are saved on partition: shared
```

If you want to upload SSL certificate, enter 'Y'. The certificate available in the sslConfig path is uploaded.

3. If the SSL Certificate upload is successful, a message 'SSL Configured' is displayed.

Configure vThunder GLM

The following topics are covered:

- Initial Setup
- Apply GLM License

Initial Setup

To configure vThunder GLM using the PowerShell template, perform the following steps:

1. Open the PS_TMPL_2NIC_1VM_GLM_CONFIG_PARAM.json with a text editor.
2. Configure GLM account details.

```
{
  "parameters": {
    "user_name": {
      "value": "<user_email_address>"
    },
    "user_password": {
      "value": "<user_password>"
    },
    "entitlement_token": {
      "value": "<license_entitlement_token>"
```

```
    }
  }
}
```

3. Verify if the configurations in the PS_TMPL_2NIC_1VM_GLM_CONFIG_PARAM.json file are correct and then save the changes.

Apply GLM License

To apply GLM license, perform the following steps:

1. From PowerShell, navigate to the folder where you have downloaded the PowerShell template.
2. Run the following command to apply GLM on vThunder:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_2NIC_1VM_GLM_CONFIG_4.ps1
```

3. If the GLM license is applied successfully, a message is displayed.

```
ConfigureGlm
{
  "response": {
       "status": "OK",
       "msg": "BASE License successfully updated, please log out and log back
in to access license featurebA1070459ec380000\n"
  }
}
GlmRequestSend
Configurations are saved on partition: shared
WriteMemory
```

Access vThunder using CLI or GUI

vThunder can be accessed using any of the following ways:

- Access vThunder using CLI
- Access vThunder using GUI

Access vThunder using CLI

To access vThunder using CLI, perform the following steps:

1. Open PuTTY.
2. Enter or select the following basic information in the PuTTy Configuration window:
   - Hostname: Public IP of Virtual Machine Instance
     Here, Public IP of **`vth-inst1`**.
   - Connection Type: SSH
3. Click **Open**.
4. In the active PuTTY session, login with the recently changed password:

```
login as: xxxx <---Enter username provided by A10 Networks Support--->
Using keyboard-interactive authentication.
Password: xxxx <---Enter your password--->
Last login: Day MM DD HH:MM:SS from a.b.c.d

System is ready now.

[type ? for help]

vThunder> enable <---Execute command--->
Password:<---just press Enter key--->
vThunder#config <---Configuration mode--->
```

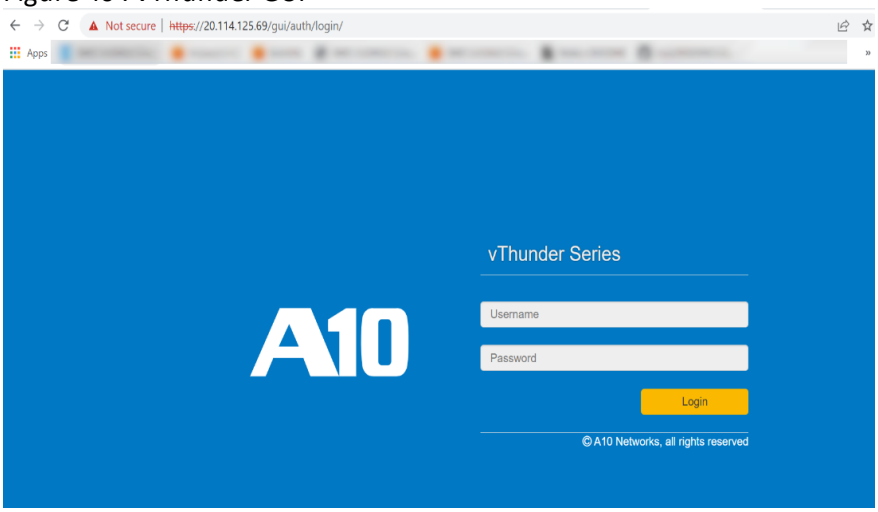
Access vThunder using GUI

To access vThunder using GUI, perform the following steps:

1. Open any browser.

2. Enter *https://<vthunder_public_IP>/gui/auth/login/* in the address bar.

Figure 40 : vThunder GUI



3. Enter the recently configured user credentials.
The home page gets displayed.

Verify Deployment

To verify vThunder SLB deployment using the PowerShell template, perform the following steps:

1. Run the following command on vThunder:

```
vThunder(config)#show running-config
```

If the deployment is successful, the following SLB configuration is displayed:

```
interface management
  ip address dhcp
!
interface ethernet 1
  enable
  ip address 10.0.2.47 255.255.255.0
!
!
slb server s1 10.0.2.8
  port 53 udp
```

```
  port 80 tcp
  port 443 tcp
!
slb service-group sg443 tcp
  member s1 443
!
slb service-group sg53 udp
  member s1 53
!
slb service-group sg80 tcp
  member s1 80
!
slb virtual-server vs1 use-if-ip ethernet 1
  port 53 udp
    source-nat auto
    service-group sg53
  port 80 http
    source-nat auto
    service-group sg80
  port 443 https
    source-nat auto
    service-group sg443
!
!
end
```

2. Run the following command on vThunder:

```
vThunder(config)#show license-info
```

If the GLM is successfully applied on vThunder, the following GLM configuration is displayed:

```
Host ID         : 5DCB01EC264BECCCFECB3C2ED42E02384EE8C527
USB ID          : Not Available
Billing Serials: A10f771cecbe0000
Token           : A10f771cecbe
Product         : ADC
Platform        : vThunder
Burst           : Disabled
```

```
GLM Ping Interval In Hours : 24
------------------------------------------------------------
Enabled Licenses Expiry Date              Notes
------------------------------------------------------------
SLB              None
CGN              None
GSLB             None
RC               None
DAF              None
WAF              None
AAM              None
FP               None
WEBROOT          N/A         Requires an additional Webroot license.
THREATSTOP       N/A         Requires an additional ThreatSTOP license.
QOSMOS           N/A         Requires an additional QOSMOS license.
WEBROOT_TI       N/A         Requires an additional Webroot Threat Intel
license.
CYLANCE          N/A         Requires an additional Cylance license.
IPSEC_VPN        N/A         Requires an additional IPsec VPN license.
25 Mbps Bandwidth 21-December-2022
```

3. Run the following command on vThunder:

```
vThunder(config)#show pki cert
```

If the deployment is successful, the following SSL configuration is displayed:

```
Name    Type                        Expiration  Status
------------------------------------------------------------
server certificate Jan 28 12:00:00 2028 GMT [Unexpired, Bound]
```

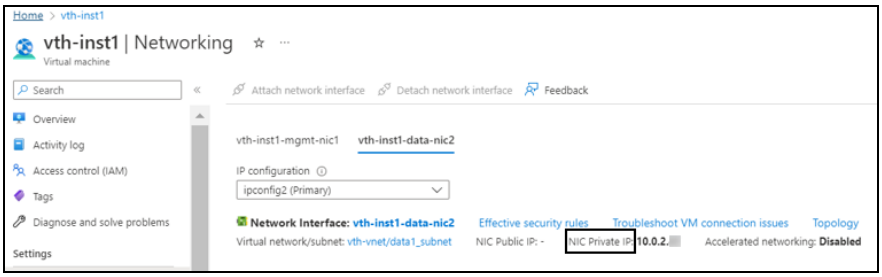
Verify Traffic Flow

To verify the traffic flow from client machine to server machine via vThunder, perform the following:

1. From **Azure Portal** > **Azure Services** > **Resource Group** > <resource_group_name> > <virtual_machine_instance> > **Settings** > **Networking**.
   Here, **`vth-inst1`** is the vThunder instance name.

2. Copy the Private IP address of the data subnet.

Figure 41 : vThunder instance Data Subnet Private IP



3. Select your client instance from the **Virtual machine** list.
   Here, **`vth-client`** is the client instance name.
4. SSH your client machine and run the following command to verify the traffic flow:

```
curl <vThunder_instance_data_private_IPv4_Address>
```

Example

```
curl 10.0.2.4
```

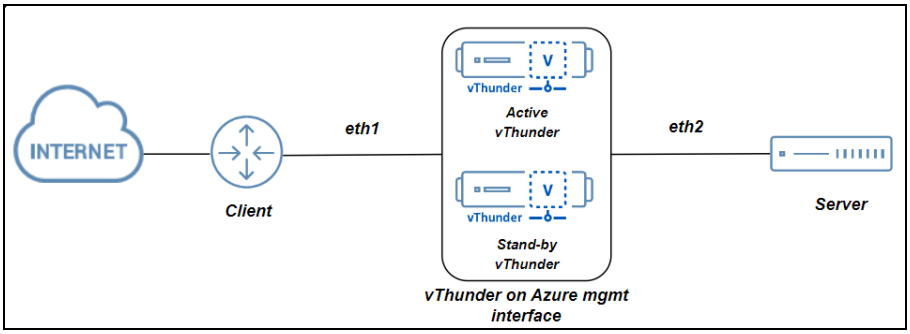
Verify if a response is received.

Deploy PowerShell A10-vThunder_ADC-3NIC-2VM-HA

Figure 42 shows the 3NIC-2VM-HA deployment topology. Using this template, two vThunder instances can be deployed containing:

- One management interface and two data interfaces each
- HA support
- GLM integration

Figure 42 : 3NIC-2VM-HA Topology



The following topics are covered:

System Requirements 92
Create vThunder Instances 95
Configure Server and Client Machine 100
Configure vThunder as an SLB 117
Configure High Availability 124
Access vThunder using CLI or GUI 127
Verify Deployment 129
Verify Traffic Flow 131

System Requirements

The PowerShell template will display the default values when you download and save the files on your local machine. You can modify the default values as required for your deployment.

You need the following resources to deploy vThunder on the Azure cloud:

Table 6 : System Requirements

Resource Name	Description	Default Value
Azure Resource Group	A resource group with the specified name and location is created, if it doesn't exist. All the resources required for this template is created under the resource group.	Here, the Azure resource group name used is **`vth-rg1`**.
Azure Storage Account	A storage account is created inside the resource group, if it doesn't exist. If the storage name already exists, the following error is displayed “The storage account named vthunderstorage already exists under the subscription". **Performance**: Standard **Replication**: Read-access geo-redundant storage (RA-GRS) **Account kind**: Storagev2 (general purpose v2)	**`vthunderstorage`**
Virtual Machine (VM)	Two virtual machine instances are created for vThunder.	**`vth-inst1`** **`vth-inst2`**

Resource Name	Description	Default Value
Instance	**Product**: A10 vThunder **Operating system**: Linux **Default Size**: Standard_B4ms (4 vCPUs, 16 GiB Memory) **NOTE:** Before selecting any VM size, it is highly recommended to do an assessment of your projected traffic. Table 7 lists the supported VM sizes.	
Virtual Cloud Network [VCN]	A virtual network is assigned to the virtual machine instance.	`vth-vnet` Address prefix for virtual network: 10.0.0.0/16
Subnet	Three subnets are created with an address prefix each.	Subnet1: `10.0.1.0/24` Subnet2: `10.0.2.0/24` Subnet3: `10.0.3.0/24`

Network Interface Card [NIC]	Two types of interfaces are created for each vThunder instance:
	• Management Interface with public IP
	• Data Interface with primary
		`vth-inst1-mgmt-nic1` `10.0.1.4`
		`vth-inst1-data-nic2` `10.0.2.4 [Primary IP]`
		`10.0.2.X [Secondary`

Resource Name	Description	Default Value
	private IP [Ethernet 1, Ethernet 2] **NOTE:** The secondary IP of data interface is taken from DHCP server.	IP] vth-inst1-data-nic3: 10.0.3.4 [Primary IP] 10.0.3.X [Secondary IP] vth-inst2-mgmt-nic1: 10.0.1.6 vth-inst2-data-nic2: 10.0.2.6 [Primary IP] 10.0.2.X [Secondary IP] vth-inst2-data-nic3: 10.0.3.6 [Primary IP] 10.0.3.X [Secondary IP]
Network Security Group [NSG]	A security group is created for all the associated default interfaces.	vth-inst1-nsg vth-inst2-nsg
Azure Service Application Access Key	An existing key can be used or a new key can be created. For more information, refer Azure Service Application Access Key.	

Supported VM Sizes

Table 7 : Supported VM sizes

Series	Size	Qualified Name
A series	Standard A4v2	Standard_A4_v2

Series	Size	Qualified Name
	Standard A4mv2	Standard_A4m_v2
	Standard/Basic A4	Standard_A4
	Standard A8v2	Standard_A8_v2
B series	Standard B2s	Standard_B2_s
	Standard B2ms	Standard_B2ms
	Standard B4ms	Standard_B4ms
D series	Standard D3v2	Standard_D3_v2
	Standard DS3v2	Standard_DS3_v2
	Standard D5v2	Standard_D5_v2
F series	Standard F4s	Standard_F4s
	Standard F8	Standard_F8
	Standard F16s	Standard_F16s

Azure is going to retire few of the above listed VM sizes soon, see Virtual Machine series | Microsoft Azure.

For more information on Windows and Linux VM sizes, see

https://docs.microsoft.com/en-us/azure/virtual-machines/sizes-general

https://docs.microsoft.com/en-us/azure/virtual-machines/linux/sizes.

Create vThunder Instances

The following topics are covered:

- Initial Setup
- Deploy vThunder

Initial Setup

Before deploying vThunder on Azure cloud, configure the corresponding parameters in the PowerShell template.

To configure the parameters, perform the following steps:

1. Navigate to the folder where you have downloaded the PowerShell template, and open the PS_TMPL_3NIC_2VM_HA_PARAM.json with a text editor.

   NOTE: Each parameter has a default value mentioned in the parameter file.

2. Provision the vThunder instance by entering the default admin credentials as follows:

```
"adminUsername": {
  "value": "vth-user"
},
"adminPassword": {
  "value": "vth-Password"
},
```

   NOTE: This is a mandatory step during VM creation. Once the device is provisioned, vThunder auto-deletes all users except the default user.

3. Configure a storage account name.

```
"storageAccountName": {
  "value": "vthunderstorage"
},
```

   If the storage account already exists, the following error is displayed, “The storage account named is already taken”.

4. Configure a virtual network.

```
"virtual_network": {
  "value": "vth-vnet"
},
```

5. Configure a vThunder instance names.

```
"vmName_vthunder1": {
  "value": "vth-inst1"
},
"vmName_vthunder2": {
  "value": "vth-inst2"
},
```

6. Set VM size for vThunder.

```
"vmSize": {
  "value": "Standard_B4ms"
},
```

Use a suitable VM size that supports at least 3 NICs. For VM sizes, see System Requirements section.

7. Copy the desired vThunder Image Name and Product Name from the Azure Marketplace for A10 vThunder and update the details in the parameter file as follows:

```
"vThunderImage": {
  "value":"vthunder_520_byol"
},
"publisherName": {
  "value": "a10networks"
},
"productName": {
  "value": "a10-vthunder-adc-520-for-microsoft-azure"
},
```

NOTE: Do not change the publisher name.

8. Configure three network interface cards for two vThunder instances.

```
"nic1Name_vm1": {
  "value": "vth-inst1-mgmt-nic1"
},
"nic2Name_vm1": {
  "value": "vth-inst1-data-nic2"
},
"nic3Name_vm1": {
```

```
    "value": "vth-inst1-data-nic3"
  },
  "nic1Name_vm2": {
    "value": "vth-inst2-mgmt-nic1"
  },
  "nic2Name_vm2": {
    "value": "vth-inst2-data-nic2"
  },
  "nic3Name_vm2": {
    "value": "vth-inst2-data-nic3"
  },
```

9. Configure an address prefix and subnet values for one management interface and two data interface.

```
  "vm1MgmtIntfName": {
    "value": "vth-inst1-mgmt-int"
  },
  "addressPrefix": {
    "value": "10.0.0.0/16"
  },
  "mgmtIntfPrivatePrefix": {
    "value": "10.0.1.0/24"
  },
  "vm1Eth1Name": {
    "value": "vth-inst1-eth1"
  },
  "eth1PrivatePrefix": {
    "value": "10.0.2.0/24"
  },
  "vm1Eth2Name": {
    "value": "vth-inst1-eth2"
  },
  "eth2PrivatePrefix": {
    "value": "10.0.3.0/24"
  },
  "vm2MgmtIntfName": {
    "value": "vth-inst2-mgmt-int"
  },
```

```
    "vm2Eth1Name": {
      "value": "vth-inst2-eth1"
    },
    "vm2Eth2Name": {
      "value": "vth-inst2-eth2"
    },
```

10. Configure network security group for two vThunder instances.

```
    "networkSecurityGroupName_vm1": {
      "value": "vth-inst1-nsg"
    },
    "networkSecurityGroupName_vm2": {
      "value": "vth-inst2-nsg"
    }
```

11. Verify if all the configurations in the PS_TMPL_3NIC_2VM_HA_PARAM.json file are correct and then save the changes.

Deploy vThunder

To deploy vThunder on Azure cloud, perform the following steps:

1. From Start menu, open PowerShell and navigate to the folder where you have downloaded the PowerShell template.
2. Run the following command to create a deployment group in Azure.

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_HA_1.ps1 -
resourceGroup <resource_group_name> -location "<location_name>"
```

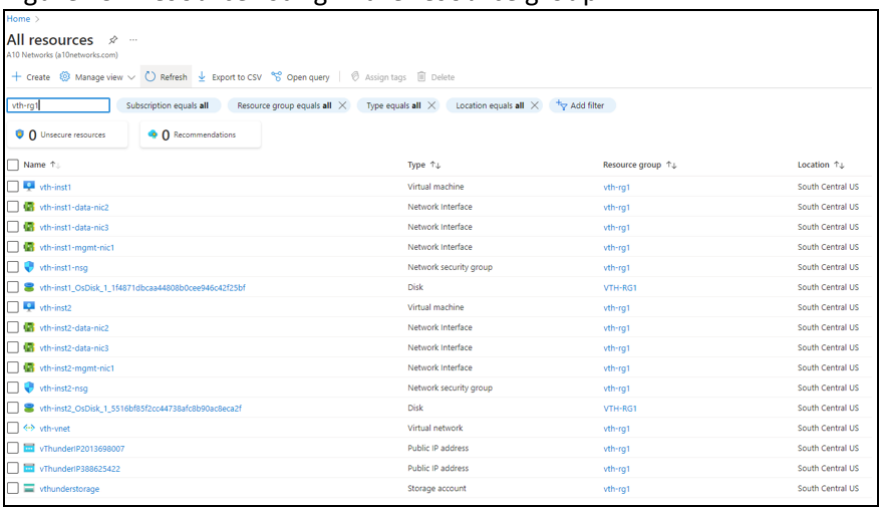
Example:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_HA_1.ps1 -
resourceGroup vth-rg1 -location "south central us"
```

Here, **`vth-rg1`** resource group is created.

3. Verify if all the above listed resources are created in the **Home** > **Azure Services** > **Resource Group** > <resource_group_name>.

Figure 43 : Resource listing in the resource group



Configure Server and Client Machine

The following topics are covered:

- Create a Server Machine
- Create a Client Machine

Create a Server Machine

To create a Server machine, perform the following steps:

1. From **Home**, navigate to **Azure Services** > **Create a resource** > **Virtual machine** and click **Create**.
   The **Create a virtual machine** window is displayed.
2. Select or enter the following mandatory information in the **Basics** tab:

   Project details

   - Subscription
   - Resource group

   Instance details

- Virtual machine name - Server machine
- Region
- Image
- Size

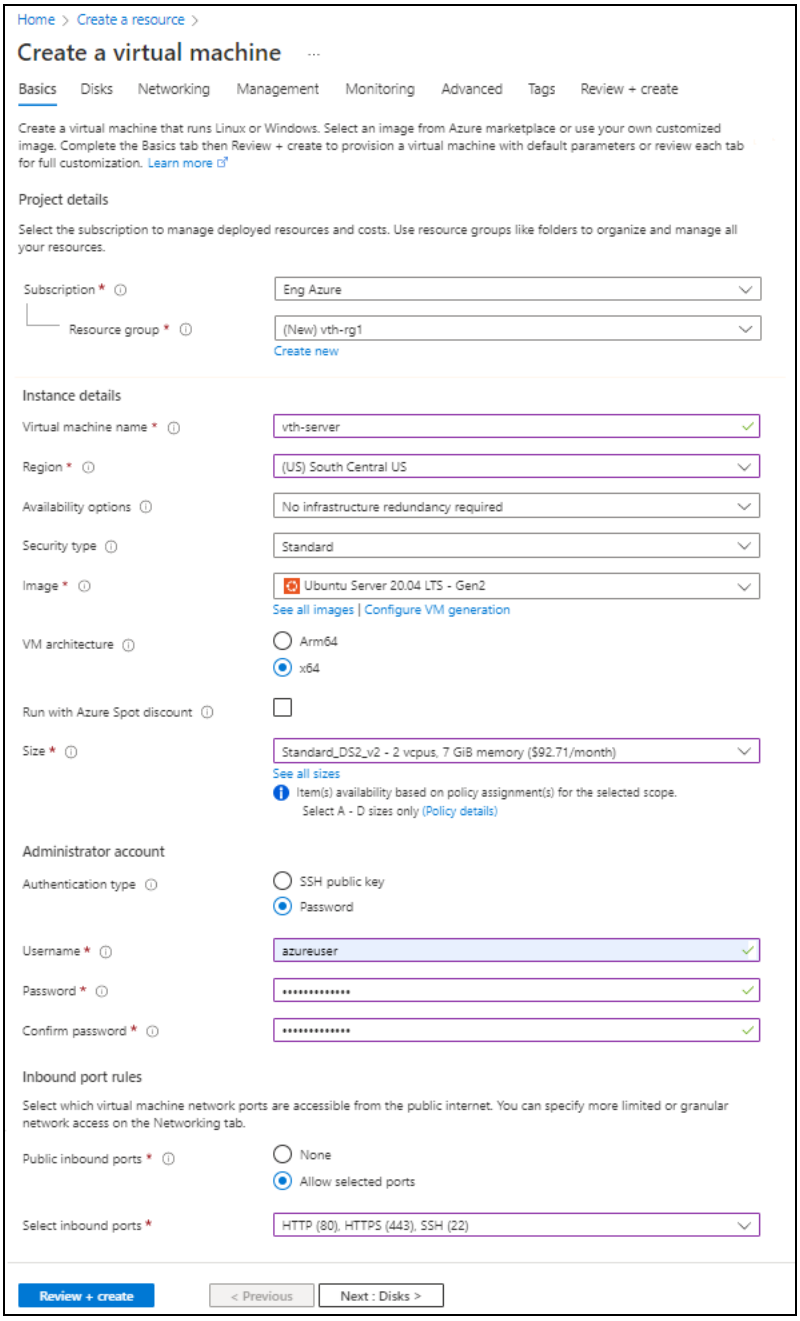
Administrator account

- Depending upon the Authentication type selected, provide the information.

Inbound port rules

- Public inbound ports
- Select inbound ports

Figure 44 : Create a virtual machine window - Basics tab



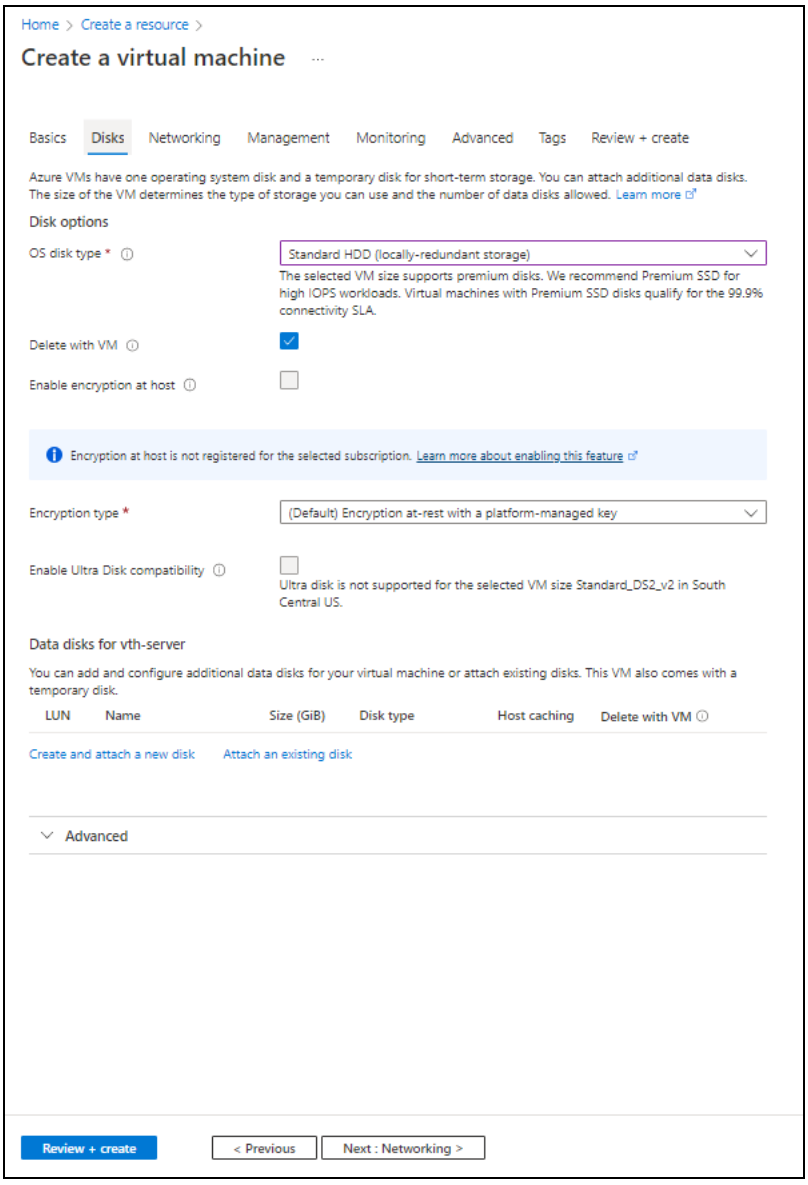
3. Leave the remaining fields as is and click **Next : Disks** at the bottom of the window.

4. Select or enter the following mandatory information in the **Disks** tab:

   Disk options

   - OS disk type
   - Encryption type

   Figure 45 : Create a virtual machine window - Disks tab



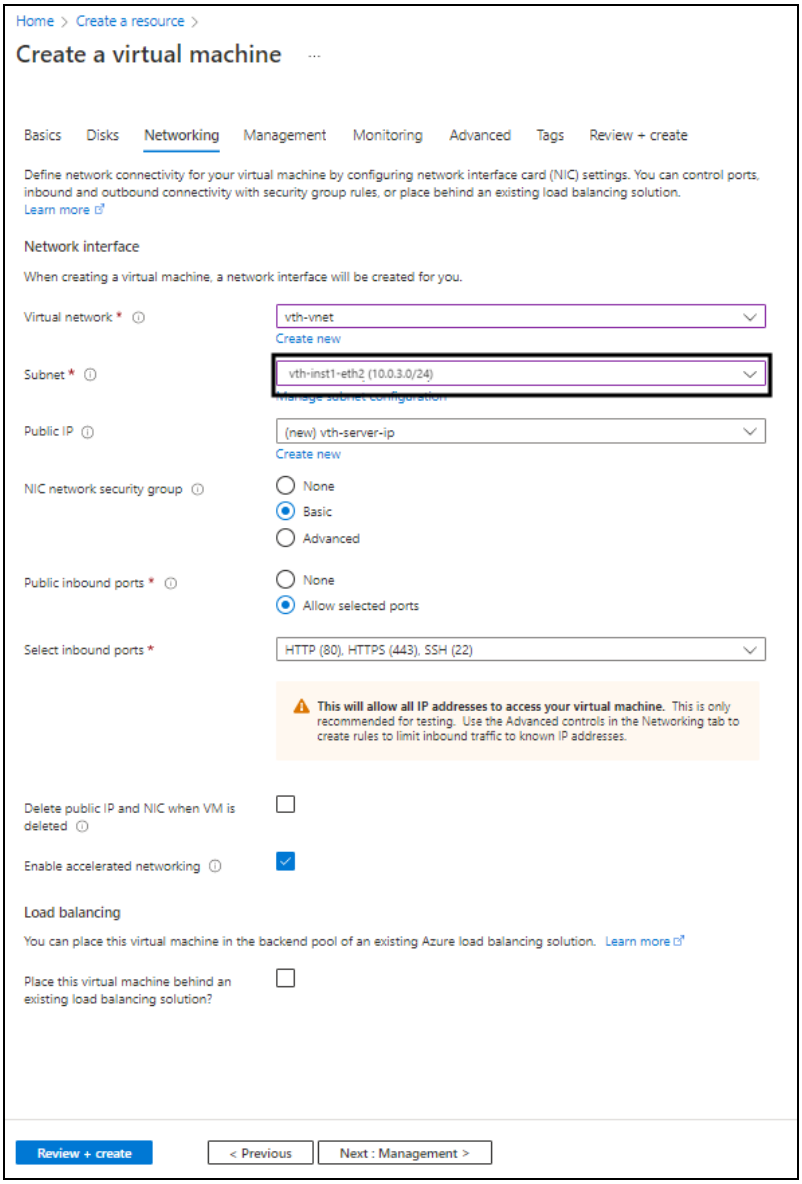
5. Leave the remaining fields as is and click **Next : Networking** at the bottom of the window.

6. Select or enter the following mandatory information in the **Networking** tab:

   Network interface

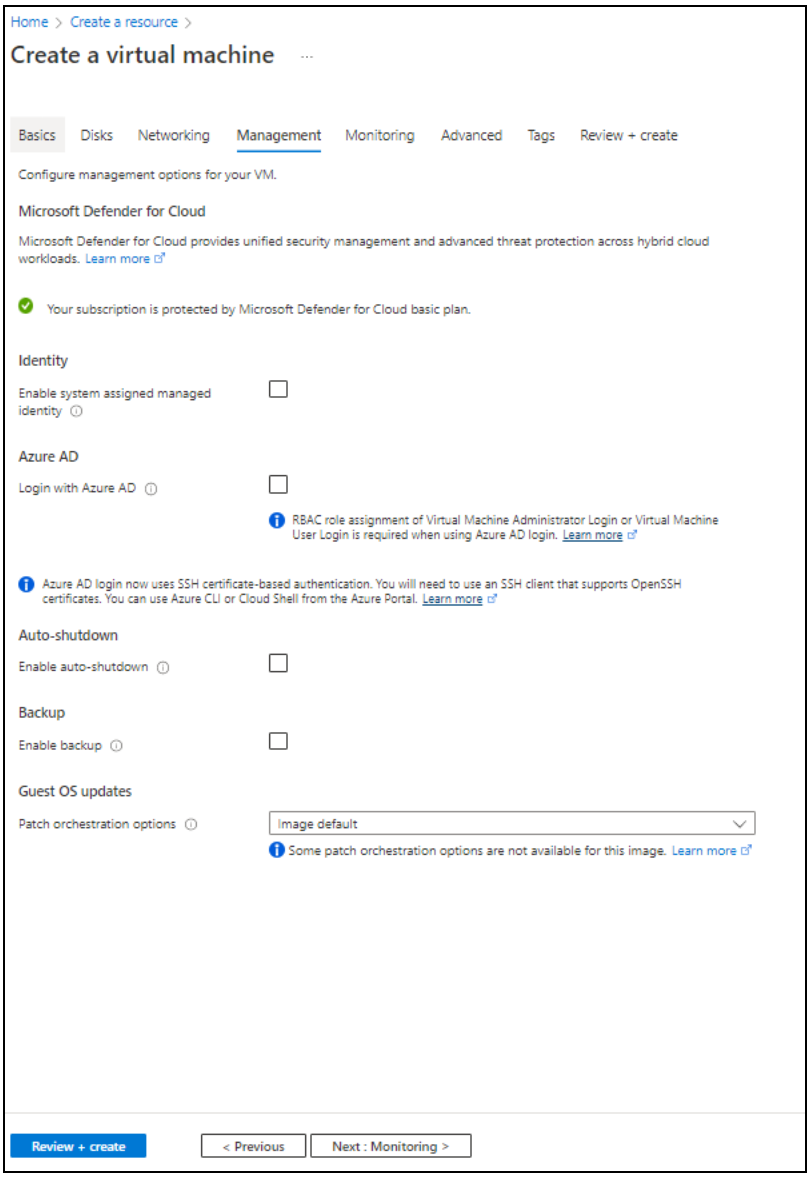
   - Virtual network
   - Subnet: Data subnet 2 (Ethernet 2)
   - Select inbound ports

Figure 46 : Create a virtual machine window - Networking tab



7. Leave the remaining fields as is and click **Next : Management** at the bottom of the window.
8. Select or enter the information in the **Management** tab as needed.

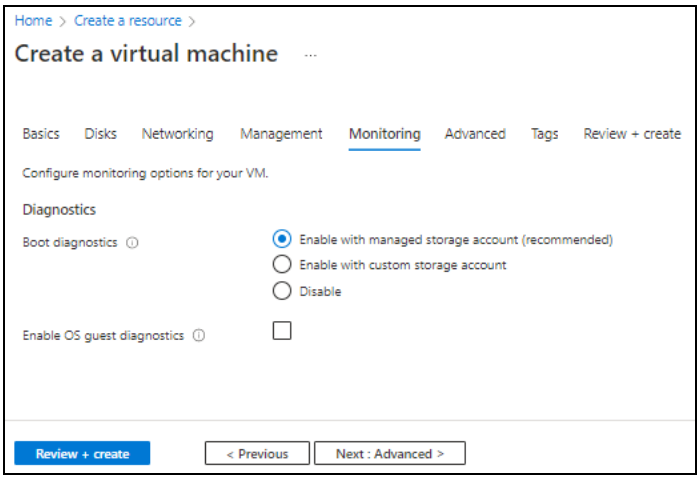
Figure 47 : Create a virtual machine window - Management tab



9. Click **Next : Monitoring** at the bottom of the window.

10. Select the monitoring options in the **Monitoring** tab as needed.

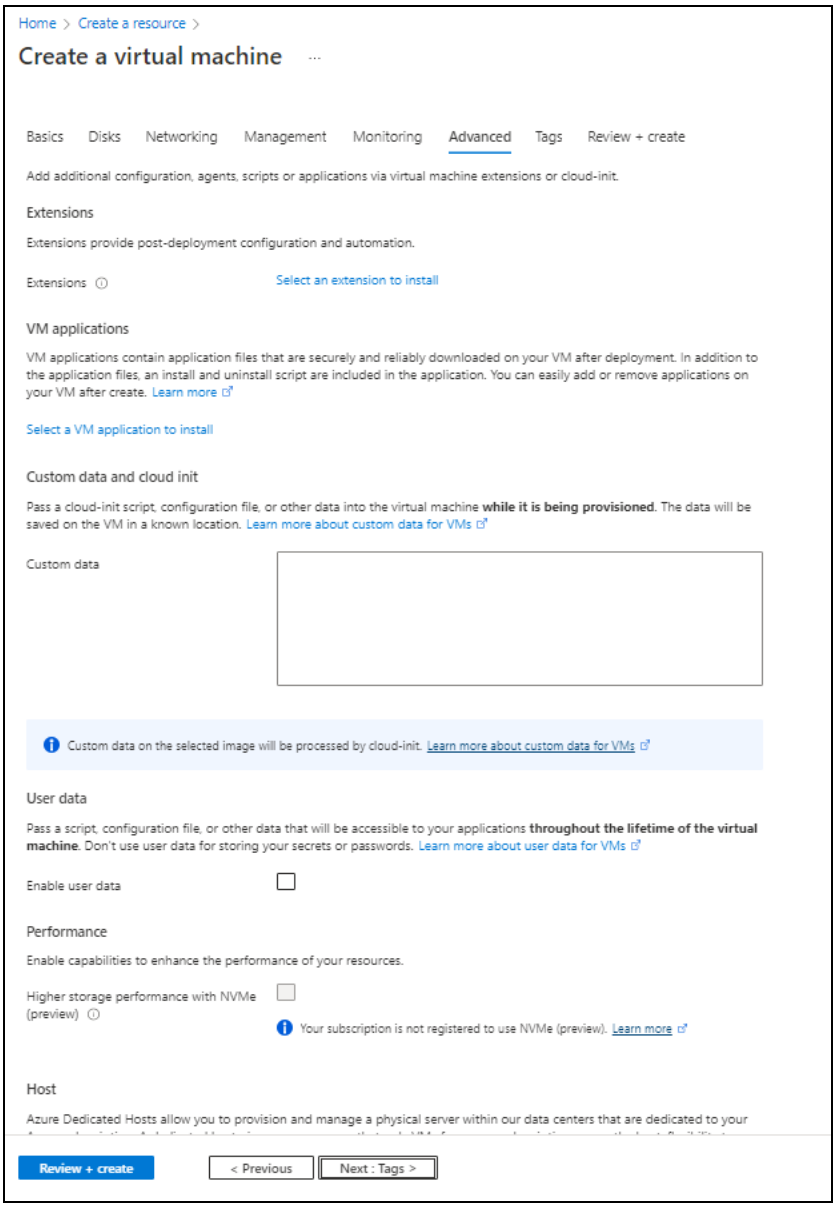
Figure 48 : Create a virtual machine window - Monitoring tab



11. Click **Next : Advanced** at the bottom of the window.

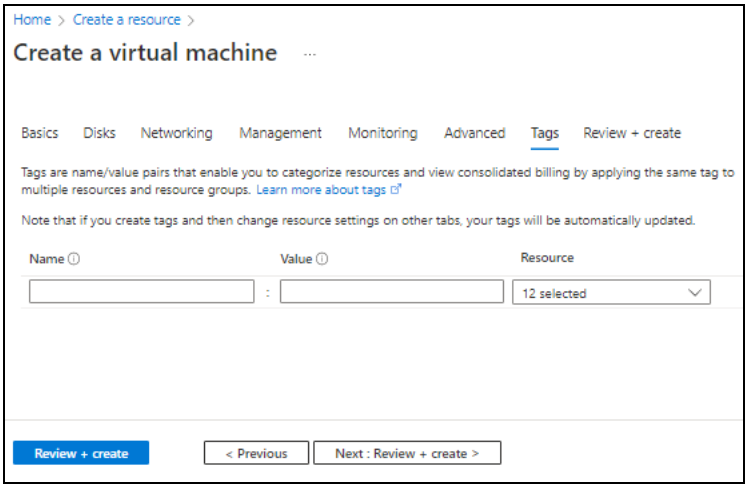
12. Select or enter the additional configuration in the **Advanced** tab as needed.

Figure 49 : Create a virtual machine window - Advanced tab



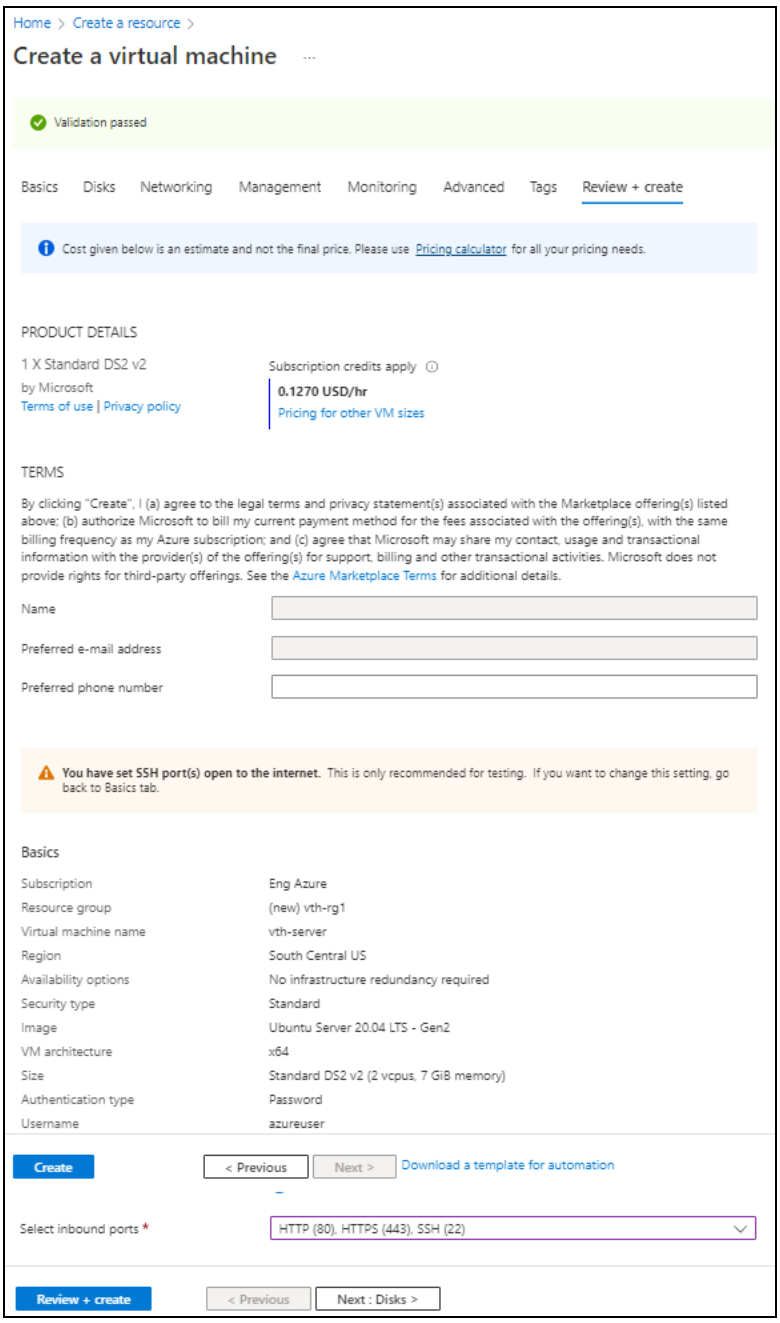
13. Click **Next : Tags** at the bottom of the window.
14. Select or enter the information to categorized resources in the **Tags** tab as needed.

Figure 50 : Create a virtual machine window - Tags tab



15. Click **Next : Review + create** at the bottom of the window.
    The fields **Name** and **Preferred e-mail address** are auto-populated as per the Azure account.

Figure 51 : Create a virtual machine window - Review + create tab



16. Click **Create** at the bottom of the window.
    The Server virtual machine gets created and listed in the **Home** > **Azure Services** > **Virtual machine** window.

17. SSH the Server virtual machine and run the following command to install Apache:
    ```
    sudo apt install apache2
    ```
    While the Apache server is getting installed, you get a prompt to continue further. Enter 'Y' to continue. After the installation is complete, a newline prompt is displayed.

Create a Client Machine

To create a Client machine, perform the following steps:

1. From Home, navigate to **Azure Services** > **Create a resource** > **Virtual machine** and click **Create**.
   The **Create a virtual machine** window is displayed.
2. Select or enter the following mandatory information in the **Basics** tab:

   Project details

   - Subscription
   - Resource group

   Instance details

   - Virtual machine name - Client machine
   - Region
   - Image
   - Size

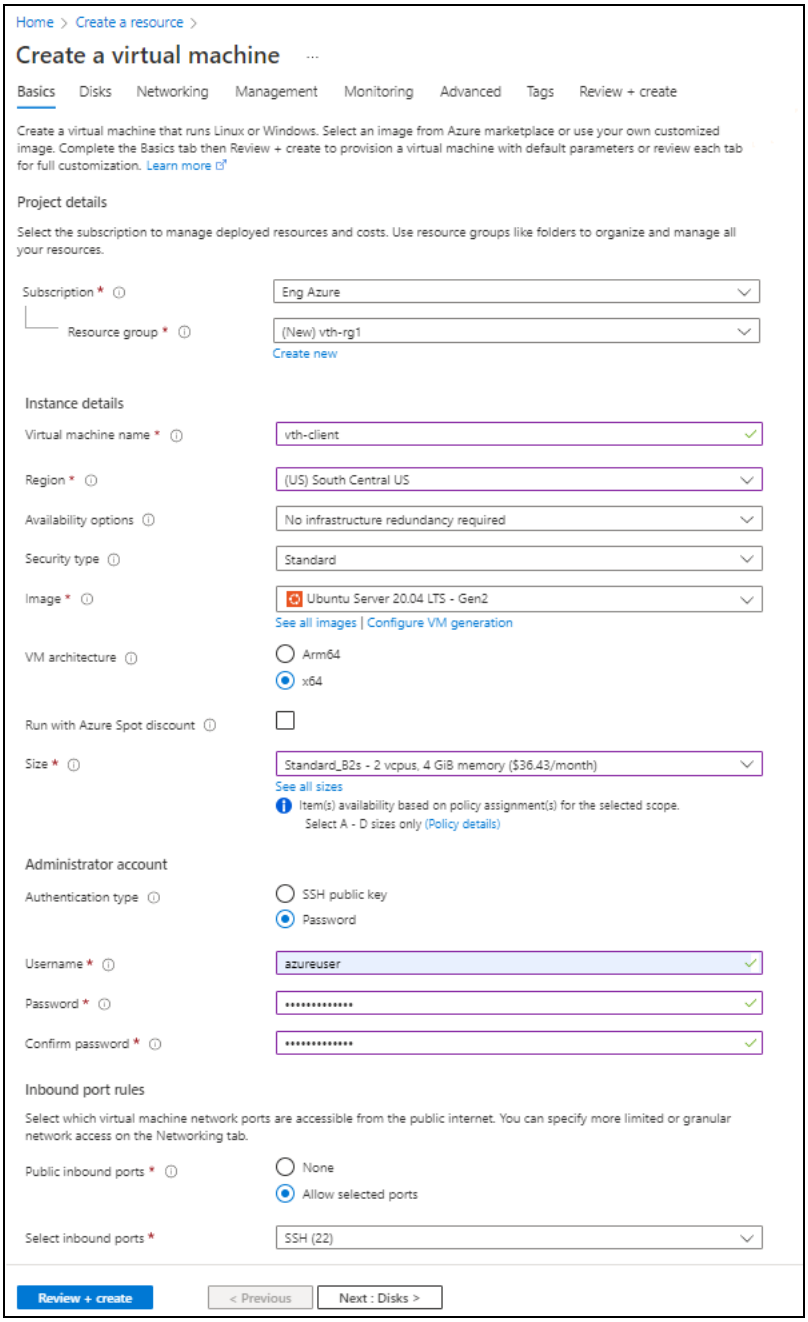
   Administrator account

   - Depending upon the Authentication type selected, provide the information.

   Inbound port rules

   - Public inbound ports
   - Select inbound ports

Figure 52 : Create a virtual machine window - Basics tab



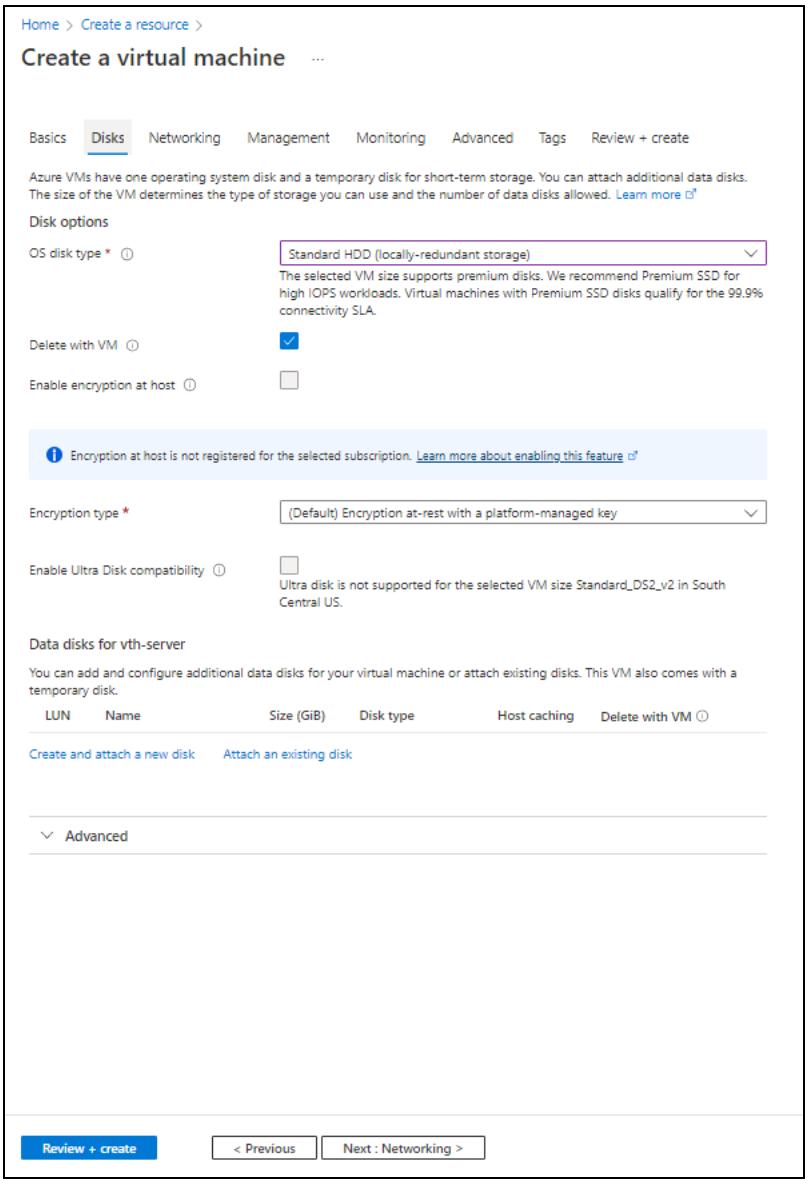
3. Leave the remaining fields as is and click **Next : Disks** at the bottom of the window.

4. Select or enter the following mandatory information in the **Disks** tab:

   Disk options

   - OS disk type
   - Encryption type

   Figure 53 : Create a virtual machine window - Disks tab



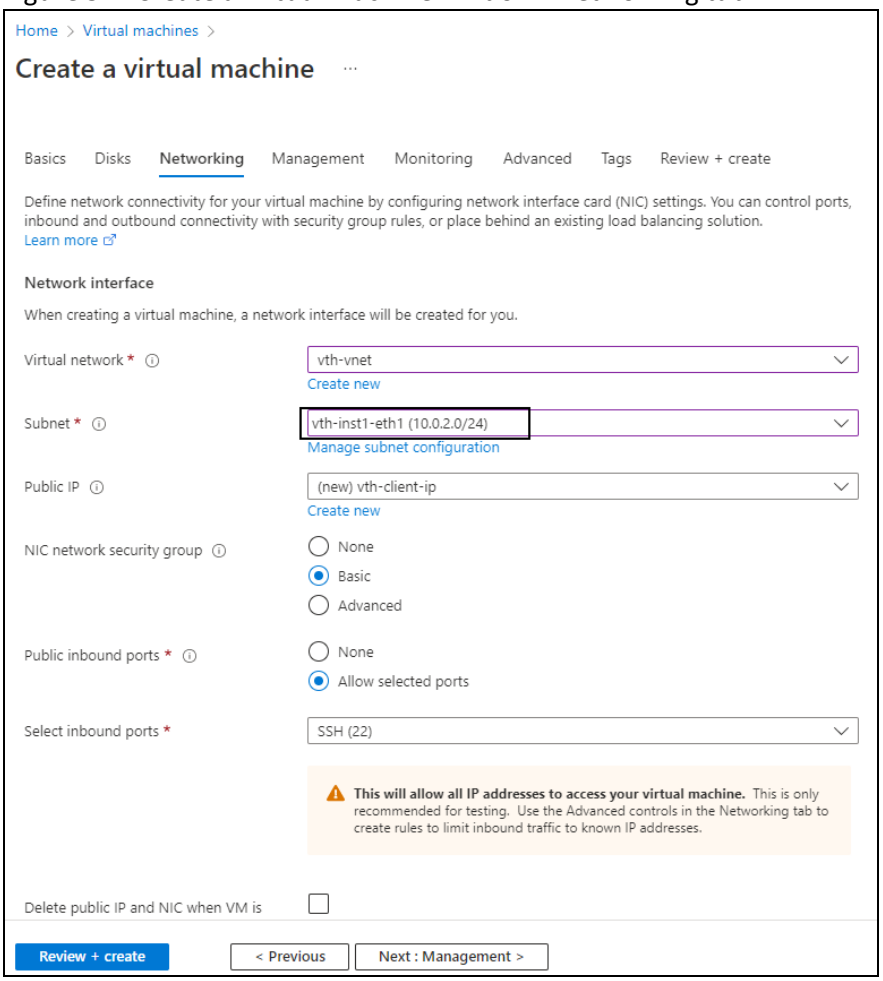
5. Leave the remaining fields as is and click **Next : Networking** at the bottom of the window.

6. Select or enter the following mandatory information in the **Networking** tab:

   Network interface

   - Virtual network
   - Subnet: Data subnet 1 (Ethernet 1)
   - Select inbound ports

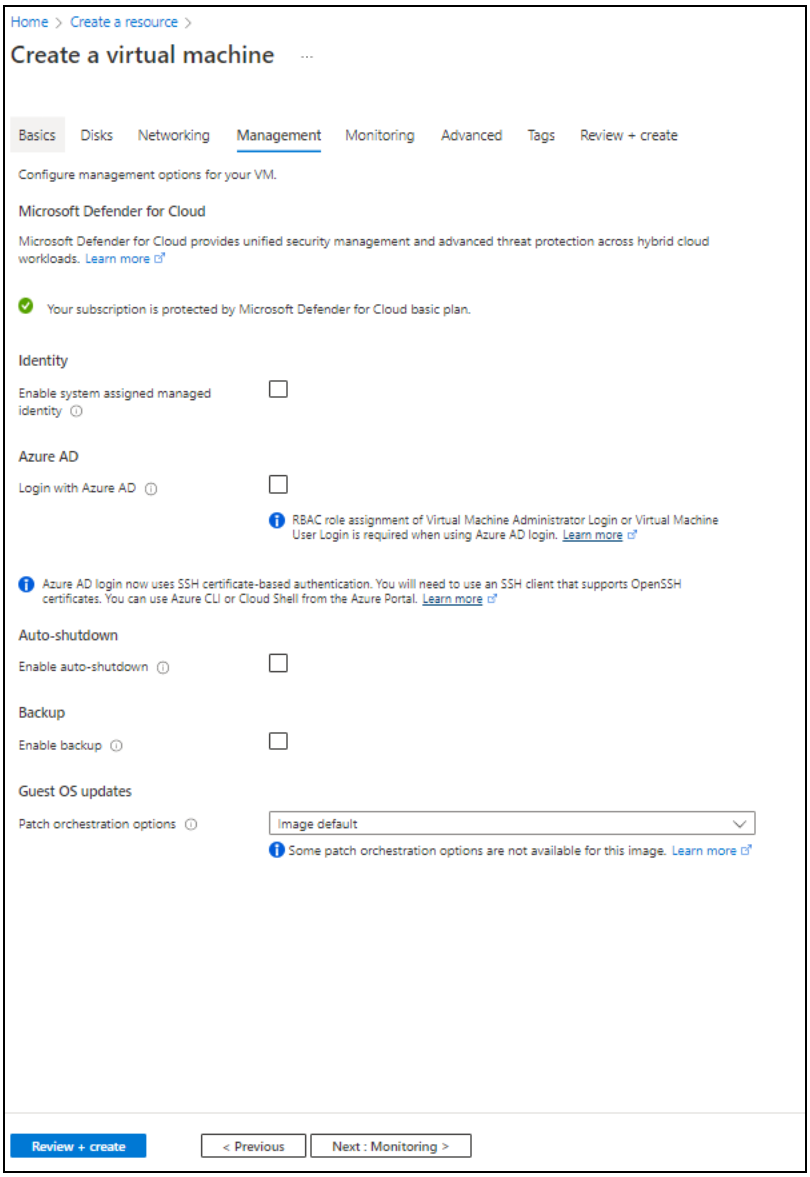
Figure 54 : Create a virtual machine window - Networking tab



7. Leave the remaining fields as is and click **Next : Management** at the bottom of the window.

8. Select or enter the information in the **Management** tab as needed.

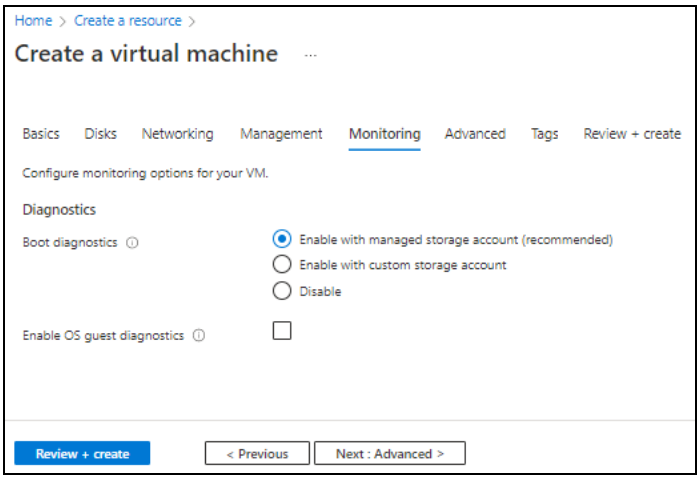
Figure 55 : Create a virtual machine window - Management tab



9. Click **Next : Monitoring** at the bottom of the window.

10. Select the monitoring options in the **Monitoring** tab as needed.

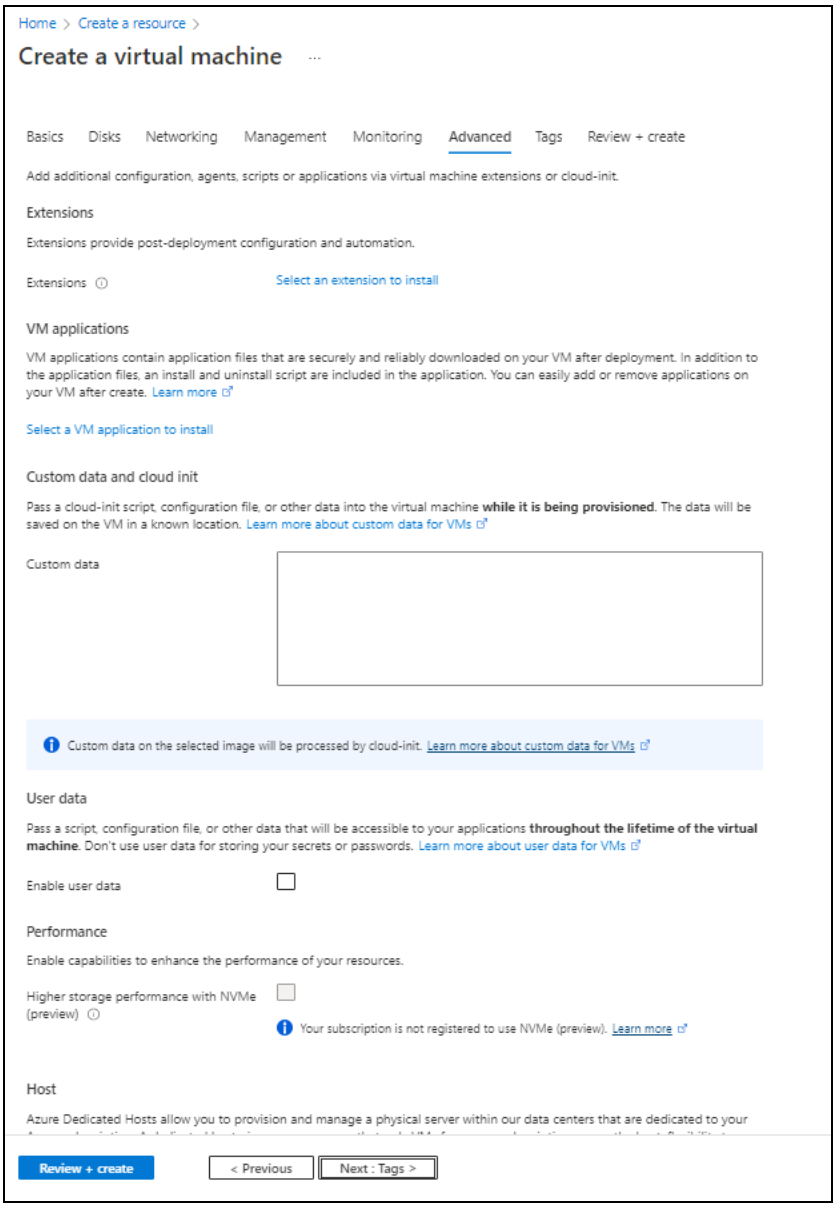
Figure 56 : Create a virtual machine window - Monitoring tab



11. Click **Next : Advanced** at the bottom of the window.

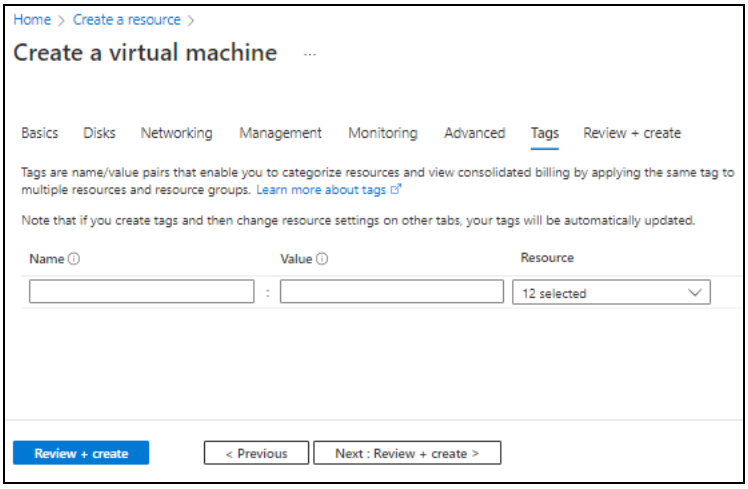
12. Select or enter the additional configuration in the **Advanced** tab as needed.

Figure 57 : Create a virtual machine window - Advanced tab



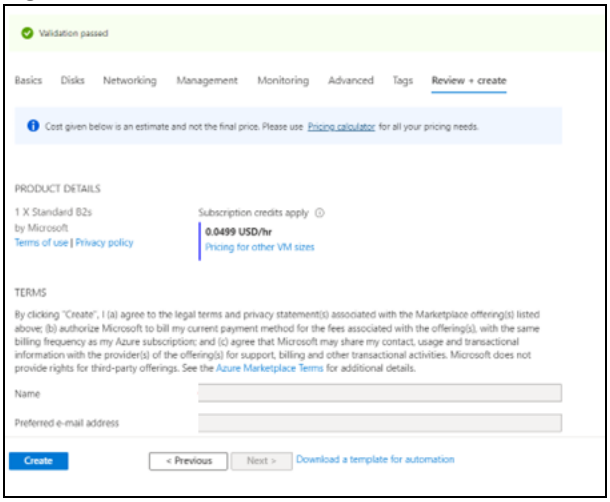
13. Click **Next : Tags** at the bottom of the window.
14. Select or enter the information to categorized resources in the **Tags** tab as needed.

Figure 58 : Create a virtual machine window - Tags tab



15. Click **Next : Review + create** at the bottom of the window.
The fields **Name** and **Preferred e-mail address** are auto-populated as per the Azure account.

Figure 59 : Create a virtual machine window - Review + create tab



16. Click **Create** at the bottom of the window.
The Client machine gets created and listed in the **Home** > **Azure Services** > **Virtual machine** window.

Configure vThunder as an SLB

The following topics are covered:

- Initial Setup
- Change Password
- Deploy vThunder as an SLB

Initial Setup

Before deploying vThunder on Azure cloud as an SLB, configure the corresponding parameters in the PowerShell template.

To configure the parameters, perform the following steps:

1. Open the PS_TMPL_3NIC_2VM_HA_SLB_CONFIG_PARAM.json with a text editor.

   NOTE: Each parameter has a default value mentioned in the parameter file.

2. Configure a SLB server host or domain.
   The SLB server host value is the data NIC's private IP address instance acting as the server.
   Instead of a host, you can also use a domain name. To do so, replace the key 'host' with 'fqdn-name' and provide a domain name instead of the IP address.

```
      "slbServerHostOrDomain": {
        "server-name": "s1",
        "host": "10.0.3.7",
        "metadata": {
          "description": "SLB server host/fqdn-name. To use domain name
replace host with fqdn-name and ip address with domain name"
        }
      },
```

3. Configure SLB server ports.

```
      "slbServerPortList": {
        "value": [
          {
            "port-number": 53,
            "protocol": "udp",
           "health-check-disable":1
          },
          {
```

```
            "port-number": 80,
            "protocol": "tcp",
           "health-check-disable":1
          },
          {
            "port-number": 443,
            "protocol": "tcp",
           "health-check-disable":1
          }
        ]
      },
```

4. Configure service group list ports.

```
      "serviceGroupList": {
        "value": [
            {
              "name":"sg443",
              "protocol":"tcp",
             "health-check-disable":1
              "member-list": [
                {
                  "name":"s1",
                  "port":443
                }
              ]
            },
            {
              "name":"sg53",
              "protocol":"udp",
             "health-check-disable":1
              "member-list": [
                {
                  "name":"s1",
                  "port":53
                }
              ]
            },
              {
```

```
            "name":"sg80",
            "protocol":"tcp",
          "health-check-disable":1
            "member-list": [
              {
                "name":"s1",
                "port":80
              }
            ]
          }
        ]
    },
```

5. Configure a virtual server.
   The virtual server default name is “vip”. The vip address is generated dynamically after deploying the PowerShell template. Therefore, its default value under **`virtualServerList`** should be replaced. To get the vip address, perform the following steps:

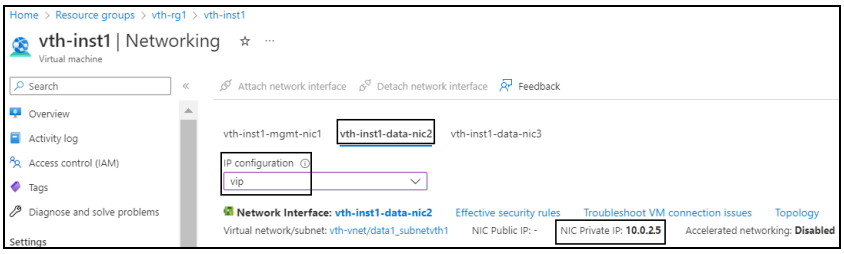
   a. From **Home**, navigate to **Azure Services** > **Resource Group** > <resource_group_name>.

   b. Go to the first virtual machine instance. Here, first virtual machine instance is **`vth-inst1`**.

   c. Select **Networking** from the left **Settings** panel.

   d. Select the Data NIC 2 tab > **IP configuration** > **`vip`**. Here, Data NIC 2 is **`vth-inst1-data-nic2`**.

   Figure 60 : Virtual machine - Networking window - Data NIC 2 tab



   e. Select the **NIC Private IP**.

f. Replace the **ip-address** value under **virtualServerList** with this **vip**.

```
        "virtualServerList": {
          "virtual-server-name": "vip",
          "ip-address": "10.0.2.5",
          "metadata": {
            "description": "virtual server is using VIP from
ethernet 1 subnet"
          },
          "value": [
            {
              "port-number":53,
              "protocol":"udp",
              "ha-conn-mirror":1,
              "auto":1,
              "service-group":"sg53"
            },
            {
              "port-number":80,
              "protocol":"http",
              "auto":1,
              "service-group":"sg80"
            },
            {
              "port-number":443,
              "protocol":"https",
              "auto":1,
              "service-group":"sg443"
            }
          ]
      },
```

CAUTION: Do not configure **ha-conn-mirror** with port 80 and port 443 as it does not work with these ports.

6. Configure SSL.

```
      "sslConfig": {
          "requestTimeOut": 40,
```

```
            "Path": "<absolute path of the ssl certificate file>",
            "File": "<certificate-name>",
            "CertificationType": "pem"
        }
```

NOTE: By default, SSL configuration is disabled i.e. no SSL configuration is applied.

Example The sample values for the SSL certificate are as shown below:

```
      "sslConfig": {
          "requestTimeOut": 40,
          "Path": "C://Users//..//..//..//server.pem” or
“C:\Users\..\..\..\certs\server.pem",
          "File": "server",
          "CertificationType": "pem"
                      }
```

7. Provide the resource group name.

```
     "resourceGroupName: "vth-rg1"
     "vThUsername": "admin"
```

NOTE: Do not change the vThunder instance username.

8. Verify if the vip address and all other configurations in the PS_TMPL_3NIC_2VM_HA_SLB_CONFIG_PARAM.json file are correct and then save the changes.

Change Password

To change the password, perform the following steps:

1. Run the following command to change password:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_HA_CHANGE_PASSWORD_
2.ps1
```

NOTE: It is highly recommended to change the default password provided by the A10 Networks Support when you log in the vThunder instance for the first time.

2. Provide the default and new password when prompted:

```
Enter Default Password:***
Enter New Password:***
Confirm New Password:***
```

The default password is provided by the A10 Networks Support. The new password should follow the Default password policy. For more information, see Default Password Policy.

Deploy vThunder as an SLB

To deploy vThunder on Azure cloud as an SLB, perform the following steps:

1. From PowerShell, navigate to the folder where you have downloaded the PowerShell template.
2. Run the following command to create vThunder SLB instance using the same resource group:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_HA_SLB_CONFIG_3.ps1
-resourceGroup <resource_group_name>
```

Example:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_HA_SLB_CONFIG_3.ps1
-resourceGroup vth-rg1
```

A message is prompted to upload the SSL certificate.

```
SSL Certificate
Do you want to upload ssl certificate ?
[Y] Yes  [No] No [?] Help (default is "N"): Y
SLB Server Host IP: 10.0.3.7
Virtual Server Name: vip
Resource Group Name: vth-rg1
vThunder1 Public IP: 13.85.81.137
vThunder2 Public IP: 13.85.81.113
Configuring vm: vth-inst1
configured ethernet- 1 ip
```

```
configured ethernet- 2 ip
Configured server
Configured service group
0
Configured virtual server
SSL Configured.
Configurations are saved on partition: shared
Configured vThunder Instance 1
Configuring vm: vth-inst2
configured ethernet- 1 ip
configured ethernet- 2 ip
Configured server
Configured service group
0
Configured virtual server
SSL Configured.
Configurations are saved on partition: shared
Configured vThunder Instance 2
```

3. If the SSL Certificate upload is successful, a message 'SSL Configured' is displayed.

Configure High Availability

The following topics are covered:

- Configure Azure Access Key
- Configure High Availability for vThunder

Configure High Availability for vThunder

The following topics are covered:

- Initial Setup
- Create High Availability for vThunder

Initial Setup

Before configuring high availability for vThunder, configure the corresponding parameters in the PowerShell template.

To configure the parameters, perform the following steps:

1. Open the PS_TMPL_3NIC_2VM_HA_CONFIG_PARAM.json with a text editor.

   NOTE: Each parameter has a default value mentioned in the parameter file.

2. Configure DNS.

```
"dns": {
    "value": "8.8.8.8"
},
```

3. Configure a Network Gateway IP.
   The default value of network gateway IP address is 10.0.1.1 as this is the first IP address of the data subnet 1 configuration.

```
"rib-list": [
    {
    "ip-dest-addr":"0.0.0.0",
    "ip-mask":"/0",
    "ip-nexthop-ipv4": [
        {
        "ip-next-hop":"10.0.2.1"
        }
    ]
    }
],
```

4. Set VRRP-A.

```
"vrrp-a": {
    "set-id":1
},
```

5. Set a Terminal Idle Timeout.

```
"terminal": {
    "idle-timeout":0
},
```

6. Configure the VRID details.
   The default value of vrid is 0. The default priority for vThunder-1 is 100, and for vThunder-2 is 99 (100-1). The floating ip address value is generated dynamically after deploying the PowerShell template. Therefore, its default value under **`vrid-list`** should be replaced. To get the fip address, perform the following steps:

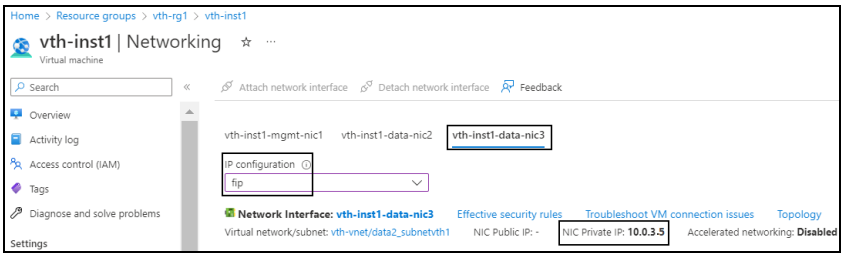
   a. From the **Home**, navigate to **Azure Services** > **Resource Group** > <resource_group_name>.

   b. Go to the first virtual machine instance. Here, first virtual machine instance is **`vth-inst1`**.

   c. Select **Networking** from the left **Settings** panel.

   d. Select the Data NIC 3 tab > **IP configuration**. Here, **`vth-inst1-data-nic3`**.

   Figure 61 : Virtual machine - Networking window - Data NIC 3 tab



   e. Select the **NIC Private IP**.

   f. Replace the **`ip-address`** value under **`vrid-list`** with this **`fip`**.

```
"vrid-list": [
            {
            "vrid-val":0,
            "blade-parameters": {
                "priority": 100
            },
            "floating-ip": {
                "ip-address-cfg": [
                    {
                      "ip-address":"10.0.3.5"
                    }
                ]
            }
```

```
            }
        ]
```

7. Verify if all the configurations in the PS_TMPL_3NIC_2VM_HA_CONFIG_PARAM.json file are correct and then save the changes.

Create High Availability for vThunder

To create High Availability for vThunder, perform the following steps:

1. Import Azure access key on both the vThunder instances. For more information, refer Import Azure Access Key.
2. Run the following command to configure both VM in HA mode.

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_HA_CONFIG_4.ps1 -resourceGroup <resource_group_name>
```

Example:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_HA_CONFIG_4.ps1 -resourceGroup vth-rg1
```

Access vThunder using CLI or GUI

vThunder can be accessed using any of the following ways:

- Access vThunder using CLI
- Access vThunder using GUI

Access vThunder using CLI

To access the vThunder instance using CLI, perform the following steps:

1. Open PuTTY.
2. Enter or select the following basic information in the PuTTy Configuration window:
   - Hostname: Public IP of Virtual Machine Instance
     Here, Public IP of **vth-inst1**, **vth-inst2**

- Connection Type: SSH

3. Click **Open**.
4. In the active PuTTY session, login with the recently changed password:

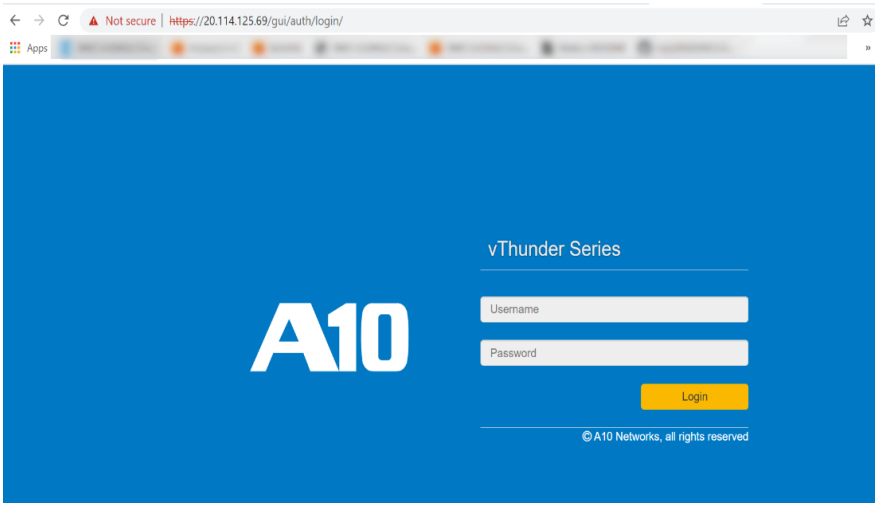
```
login as: xxxx <---Enter username provided by A10 Networks Support--->
Using keyboard-interactive authentication.
Password: xxxx <---Enter your password-->
Last login: Day MM DD HH:MM:SS from a.b.c.d

System is ready now.

[type ? for help]

vThunder> enable <---Execute command--->
Password:<---just press Enter key--->
vThunder#config <---Configuration mode--->
```

Access vThunder using GUI

To access the vThunder instance using GUI, perform the following steps:

1. Open any browser.
2. Enter *https://<vthunder_public_IP>/gui/auth/login/* in the address bar.

Figure 62 : vThunder GUI



3. Enter the recently configured user credentials.
   The home page gets displayed.

Verify Deployment

To verify vThunder SLB deployment using the PowerShell template, perform the following steps:

1. Run the following command on vThunder:

```
vThunder(config)#show running-config slb
```

   If the deployment is successful, the following SLB configuration is displayed on vThunder:

```
!Section configuration: 602 bytes
!
slb server s1 10.0.3.7
  port 53 udp
       health-check-disable
  port 80 tcp
       health-check-disable
  port 443 tcp
       health-check-disable
!
slb service-group sg443 tcp
  health-check-disable
  member s1 443
!
slb service-group sg53 udp
  health-check-disable
  member s1 53
!
slb service-group sg80 tcp
  health-check-disable
  member s1 80
!
slb virtual-server vip 10.0.2.5
  port 53 udp
```

```
    ha-conn-mirror
    source-nat auto
    service-group sg53
  port 80 http
    source-nat auto
    service-group sg80
  port 443 https
    source-nat auto
    service-group sg443
!
```

2. Run the following command on vThunder to verify the SSL Certificate configuration:

```
vThunder(config)#show pki cert
```

If the deployment is successful, the following SSL configuration is displayed:

```
Name    Type                        Expiration  Status
-----------------------------------------------------------------
server certificate Jan 28 12:00:00 2028 GMT [Unexpired, Bound]
```

3. Run the following command on vThunder to verify HA:

```
vThunder(config)#show running-config
```

If the deployment is successful, the following configuration is displayed:

```
!Current configuration: 291 bytes
!Configuration last updated at 17:36:35 IST Mon Sep 5 14 2022
!Configuration last saved at 17:35:40 IST Wed Sep 5 14 2022
!64-bit Advanced Core OS (ACOS) version 5.2.0, build 155 (Aug-10-
2020,14:34)

!
vrrp-a common
  device-id 1
  set-id 1
  enable
!
terminal idle-timeout 0
!
```

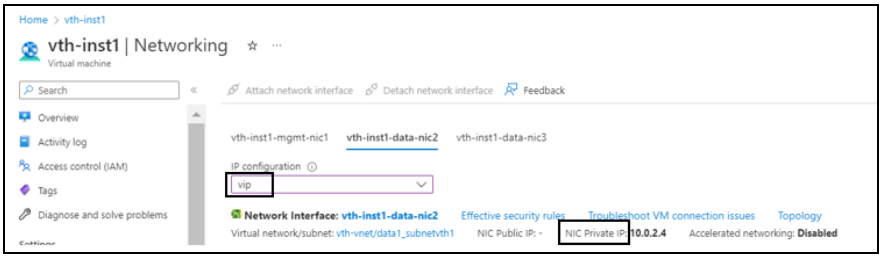
```
ip dns primary 8.8.8.8
!
!
interface management
  ip address dhcp
!
interface ethernet 1
  enable
  ip address dhcp
!
interface ethernet 2
  enable
  ip address dhcp
!
vrrp-a vrid 0
  floating-ip 10.0.3.5
  floating-ip 10.0.2.5
  blade-parameters
       priority 100
!
vrrp-a peer-group
  peer 10.0.2.4
  peer 10.0.2.6
!
ip route 0.0.0.0 /0 10.0.1.1
!
```

Verify Traffic Flow

To verify the traffic flow from client machine to server machine via vThunder, perform the following:

1. From **Azure Portal** > **Azure Services** > **Resource Group** > <resource_group_name> > <active_virtual_machine_instance> > **Settings** > **Networking**.
   Here, **`vth-inst1`** is the active vThunder instance name.
2. Copy the VIP address of the active vThunder instance.

Figure 63 : Active vThunder instance 1 VIP



3. Select your client instance from the **Virtual machine** list.
   Here, **`vth-client`** is the client instance name.
4. SSH your client machine and run the following command to verify the traffic flow:

```
curl <VIP>
```

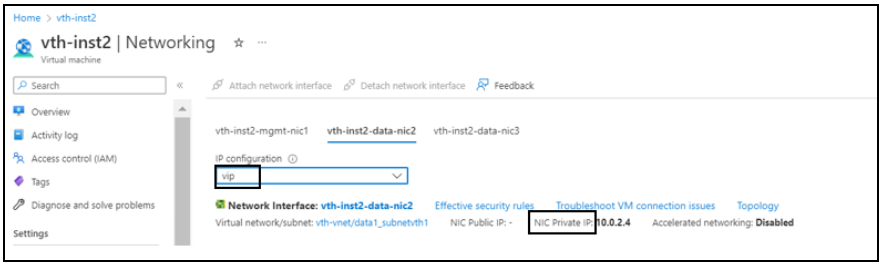
Example

```
curl 10.0.2.4
```

Verify if a response is received.

5. After the switchover, vThunder instance 2 is active, so copy the VIP address of the vThunder instance 2.

Figure 64 : Active vThunder instance 2 VIP



6. SSH your client machine and run the following command to verify the traffic flow:

```
curl <VIP>
```

Example

```
curl 10.0.2.4
```

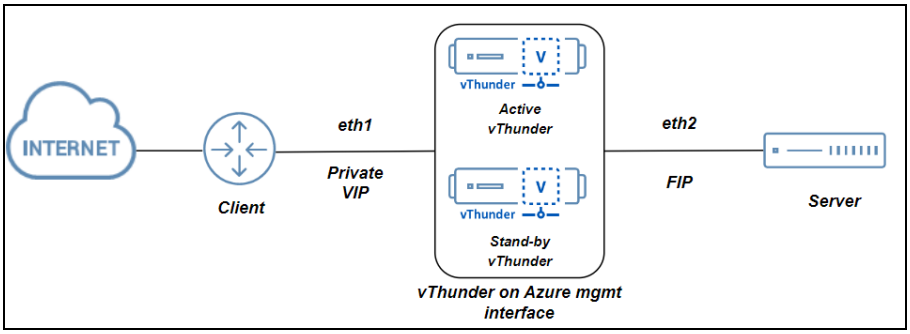
Verify if a response is received.

Deploy PowerShell A10-vThunder_ADC-3NIC-2VM-HA-GLM-PVTVIP

Figure 65 shows the 3NIC-2VM-HA-GLM-PVTVIP deployment topology. Using this template, two vThunder instances can be deployed containing:

- One management interface and two data interfaces each
- HA support
- GLM integration

Figure 65 : 3NIC-2VM-HA-GLM-PVTVIP Topology



The following topics are covered:

System Requirements 134
Create vThunder Instances 138
Configure Server and Client Machine 142
Configure vThunder as an SLB 159
Configure High Availability 166
Configure vThunder using GLM 169
Verify Deployment 172
Verify Traffic Flow 176

System Requirements

The PowerShell template will display the default values when you download and save the files on your local machine. You can modify the default values as required for your deployment.

You need the following resources to deploy vThunder on the Azure cloud:

Table 8 : System Requirements

Resource Name	Description	Default Value
Azure Resource Group	A resource group with the specified name and location is created, if it doesn't exist. All the resources required for this template is created under the resource group.	Here, the Azure resource group name used is **`vth-rg1`**.
Azure Storage Account	A storage account is created inside the resource group, if it doesn't exist. If the storage name already exists, the following error is displayed “The storage account named vthunderstorage already exists under the subscription". **Performance**: Standard **Replication**: Read-	**`vthunderstorage`**

Resource Name	Description	Default Value
	access geo-redundant storage (RA-GRS) **Account kind**: Storagev2 (general purpose v2)	
Virtual Machine (VM) Instance	Two virtual machine instances are created for vThunder. **Product**: A10 vThunder **Operating system**: Linux **Default Size**: Standard_B4ms (4 vCPUs, 16 GiB Memory) **NOTE:** Before selecting any VM size, it is highly recommended to do an assessment of your projected traffic. Table 9 lists the supported VM sizes.	`vth-inst1` `vth-inst2`
Virtual Cloud Net-	A virtual network is assigned to the virtual	`vth-vnet`

Resource Name	Description	Default Value
work [VCN]	machine instance.	Address prefix for virtual network: `10.0.0.0/16`
Subnet	Three subnets are created with an address prefix each.	Subnet1: `vth-vnet1-mgmt-sub1 10.0.1.0/24` Subnet2: `vth-vnet1-data-sub2 10.0.2.0/24` Subnet3: `vth-vnet1-data-sub3 10.0.3.0/24`

Network Interface Card [NIC]	Two types of interfaces are created for each vThunder instance:
	• Management Interface with public IP
	• Data Interface with primary private IP [Ethernet 1, Ethernet 2]
	NOTE: The secondary IP of data interface is taken from DHCP server.
		`vth-inst1-mgmt-nic1` `10.0.1.4`
		`vth-inst1-data-nic2` `10.0.2.4 [Primary IP]`
		`10.0.2.X [Secondary IP]`
		`vth-inst1-data-nic3` `10.0.3.4 [Primary IP]`
		`10.0.3.X [Secondary IP]`
		`vth-inst2-mgmt-nic1` `10.0.1.6`
		`vth-inst2-data-nic2` `10.0.2.6 [Primary IP]`
		`10.0.2.X [Secondary IP]`
		`vth-inst2-data-nic3` `10.0.3.6 [Primary IP]`
		`10.0.3.X [Secondary IP]`

Network Security	A security group is created for all the asso-	`vth-inst1-nsg`

Resource Name	Description	Default Value
Group [NSG]	ciated default inter-faces.	`vth-inst2-nsg`
Azure Ser-vice Applic-ation Access Key	An existing key can be used or a new key can be created. For more information, refer Azure Service Applic-ation Access Key.	

Supported VM Sizes

Table 9 : Supported VM sizes

Series	Size	Qualified Name
A series	Standard A4v2	Standard_A4_v2
	Standard A4mv2	Standard_A4m_v2
	Standard/Basic A4	Standard_A4
	Standard A8v2	Standard_A8_v2
B series	Standard B2s	Standard_B2_s
	Standard B2ms	Standard_B2ms
	Standard B4ms	Standard_B4ms
D series	Standard D3v2	Standard_D3_v2
	Standard DS3v2	Standard_DS3_v2
	Standard D5v2	Standard_D5_v2
F series	Standard F4s	Standard_F4s
	Standard F8	Standard_F8
	Standard F16s	Standard_F16s

Azure is going to retire few of the above listed VM sizes soon, see Virtual Machine series | Microsoft Azure.

For more information on Windows and Linux VM sizes, see

https://docs.microsoft.com/en-us/azure/virtual-machines/sizes-general

https://docs.microsoft.com/en-us/azure/virtual-machines/linux/sizes.

Create vThunder Instances

The following topics are covered:

- Initial Setup
- Deploy vThunder

Initial Setup

Before deploying vThunder on Azure cloud, configure the corresponding parameters in the PowerShell template.

To configure the parameters, perform the following steps:

1. Navigate to the folder where you have downloaded the PowerShell template and open the PS_TMPL_3M_HA_GLM_PVTVIP_PARAM.json with a text editor.

   NOTE: Each parameter has a default value mentioned in the parameter file.

2. Provision the vThunder instance by entering the default admin credentials as follows:

```
"adminUsername": {
  "value": "vth-user"
},
"adminPassword": {
  "value": "vth-Password"
},
```

NOTE: This is a mandatory step during VM creation. Once the device is provisioned, vThunder auto-deletes all users except the default user.

3. Configure a virtual network.

```
"virtual_network": {
  "value": "vth-vnet"
},
```

4. Configure vThunder instance names.

```
"vmName_vthunder1": {
  "value": "vth-inst1"
},
"vmName_vthunder2": {
  "value": "vth-inst2"
},
```

5. Set VM size for vThunder.

```
"vmSize": {
  "value": "Standard_B4ms"
},
```

Use a suitable VM size that supports at least 3 NICs. For VM sizes, see System Requirements section.

6. Copy the desired vThunder Image Name and Product Name from the Azure Marketplace for A10 vThunder and update the details in the parameter file as follows:

```
"vThunderImage": {
  "value":"vthunder_520_byol"
},
"publisherName": {
  "value": "a10networks"
},
"productName": {
  "value": "a10-vthunder-adc-520-for-microsoft-azure"
},
```

NOTE: Do not change the publisher name.

7. Configure three network interface cards for two vThunder instances.

```
"nic1Name_vm1": {
  "value": "vth-inst1-mgmt-nic1"
},
"nic2Name_vm1": {
  "value": "vth-inst1-data-nic2"
},
"nic3Name_vm1": {
  "value": "vth-inst1-data-nic3"
},
"nic1Name_vm2": {
  "value": "vth-inst2-mgmt-nic1"
},
"nic2Name_vm2": {
  "value": "vth-inst2-data-nic2"
},
"nic3Name_vm2": {
  "value": "vth-inst2-data-nic3"
},
```

8. Configure an address prefix and subnet values for one management interface and two data interface.

```
"vm1MgmtIntfName": {
  "value": "vth-inst1-mgmt-int"
},
"addressPrefix": {
  "value": "10.0.0.0/16"
},
"mgmtIntfPrivatePrefix": {
  "value": "10.0.1.0/24"
},
"vm1Eth1Name": {
  "value": "vth-inst1-eth1"
},
"eth1PrivatePrefix": {
  "value": "10.0.2.0/24"
},
"vm1Eth2Name": {
```

```
      "value": "vth-inst1-eth2"
    },
    "eth2PrivatePrefix": {
      "value": "10.0.3.0/24"
    },
    "vm2MgmtIntfName": {
      "value": "vth-inst2-mgmt-int"
    },
    "vm2Eth1Name": {
      "value": "vth-inst2-eth1"
    },
    "vm2Eth2Name": {
      "value": "vth-inst2-eth2"
    },
```

9. Configure network security group for two vThunder instances.

```
    "networkSecurityGroupName_vm1": {
      "value": "vth-inst1-nsg"
    },
    "networkSecurityGroupName_vm2": {
      "value": "vth-inst2-nsg"
    }
```

10. Verify if all the configurations in the PS_TMPL_3NIC_2VM_HA_GLM_PVTVIP_PARAM.json file are correct and then save the changes.

Deploy vThunder

To deploy vThunder on Azure cloud, perform the following steps:

1. From Start menu, open PowerShell and navigate to the folder where you have downloaded the PowerShell template.
2. Run the following command to create a deployment group in Azure.

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_HA_GLM_PVTVIP_1.ps1
-resourceGroup <resource_group_name> -location "<location_name>"
```

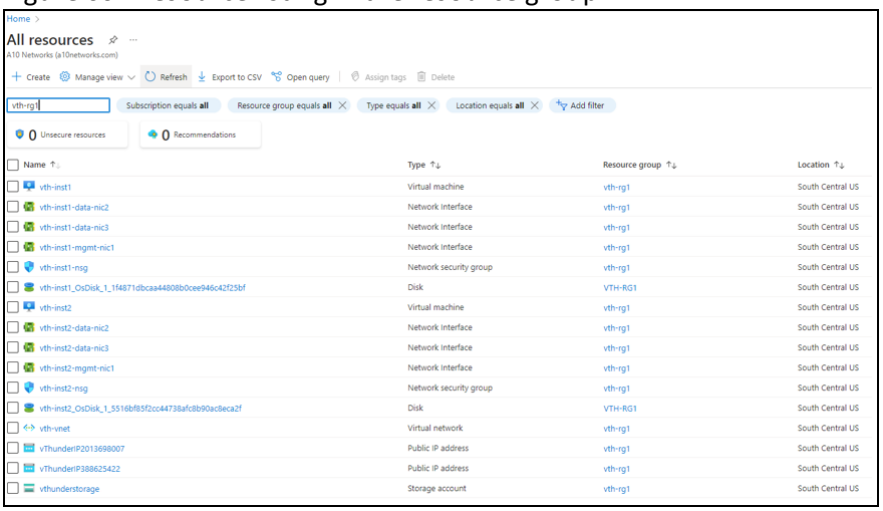
Example:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_HA_GLM_PVTVIP_1.ps1
-resourceGroup vth-rg1 -location "south central us"

cmdlet PS_TMPL_3NIC_2VM_HA_GLM_PVTVIP_1 at command pipeline position 1
Supply values for the following parameters:
storageaccount: vthunderstorage
vth-rg1
vthunderstorage
South Central US
```

Here, **`vth-rg1`** resource group is created.

3. Verify if all the above listed resources are created in the **Home** > **Azure Services > Resource Group >** <resource_group_name>.

Figure 66 : Resource listing in the resource group



Configure Server and Client Machine

The following topics are covered:

- Create a Server Machine
- Create a Client Machine

Create a Server Machine

To create a Server machine, perform the following steps:

1. From Home, navigate to **Azure Services** > **Create a resource** > **Virtual machine** and click **Create**.
   The **Create a virtual machine** window is displayed.
2. Select or enter the following mandatory information in the **Basics** tab:

   Project details

   - Subscription
   - Resource group

   Instance details

   - Virtual machine name - Server machine
   - Region
   - Image
   - Size

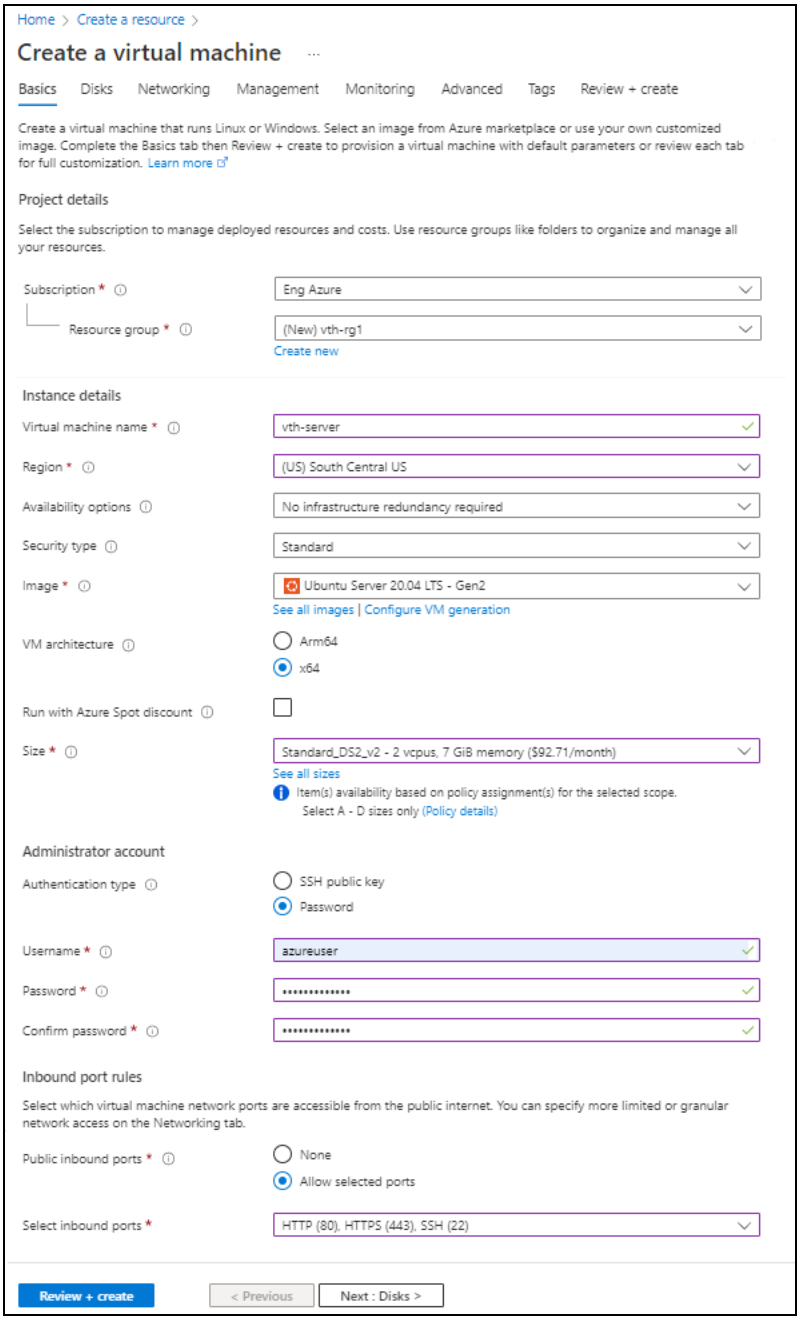
   Administrator account

   - Depending upon the Authentication type, provide the information.

   Inbound port rules

   - Public inbound ports
   - Select inbound ports

Figure 67 : Create a virtual machine window - Basics tab



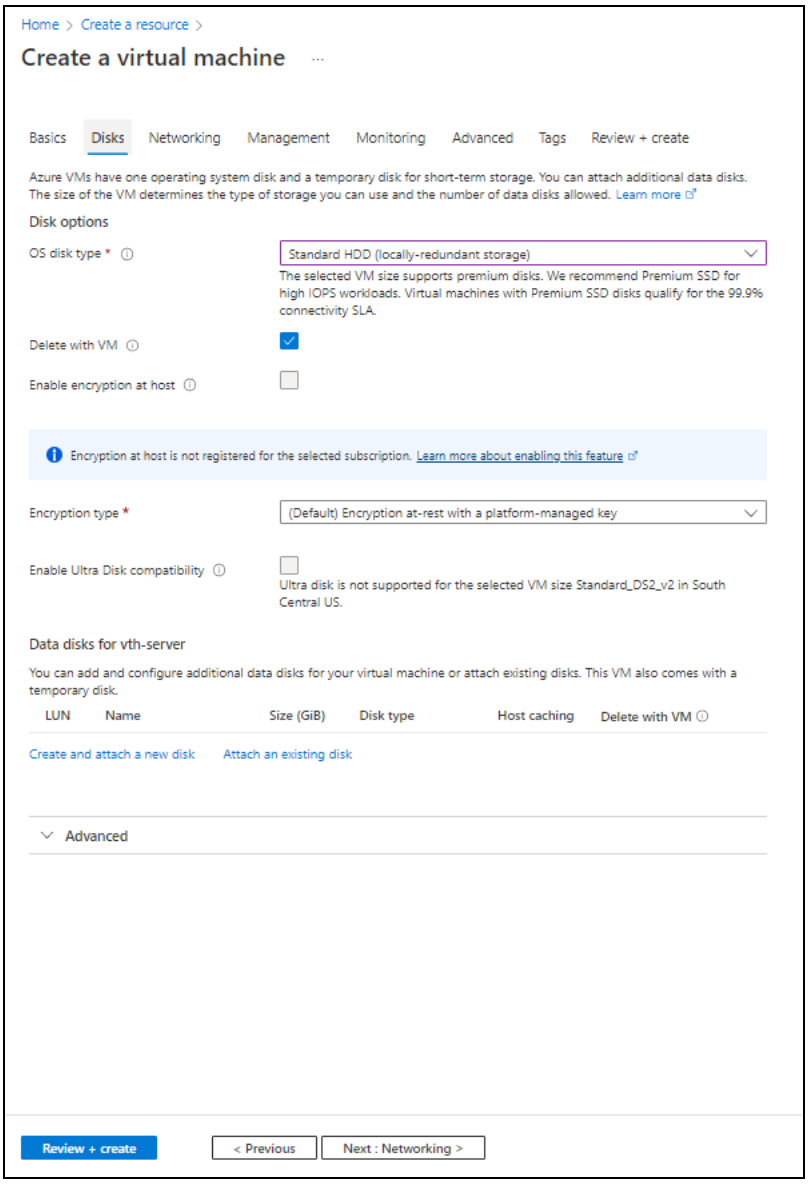
3. Leave the remaining fields as is and click **Next : Disks** at the bottom of the window.

4. Select or enter the following mandatory information in the **Disks** tab:

   Disk options

   - OS disk type
   - Encryption type

   Figure 68 : Create a virtual machine window - Disks tab



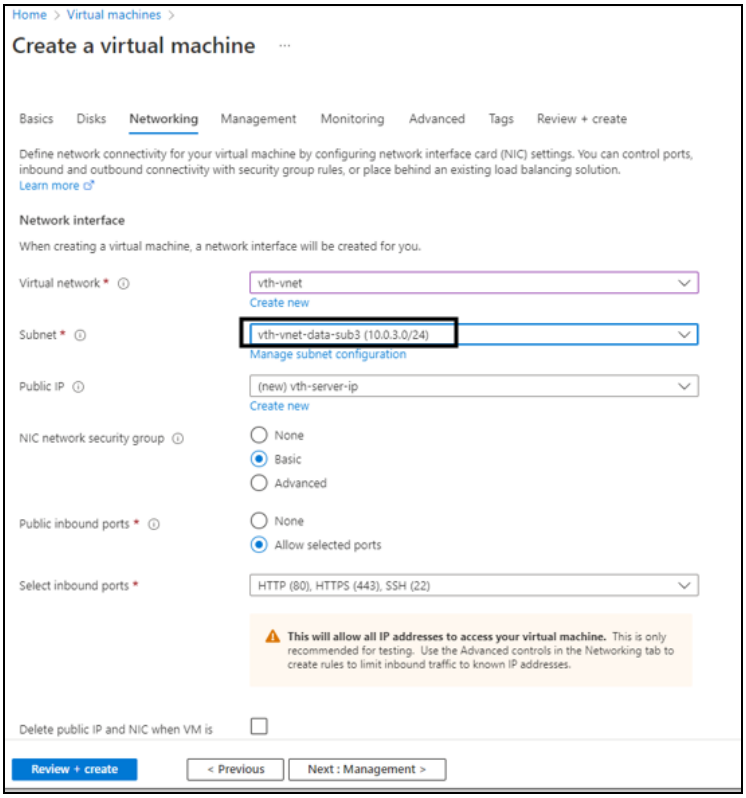
5. Leave the remaining fields as is and click **Next : Networking** at the bottom of the window.

6. Select or enter the following mandatory information in the **Networking** tab:

   Network interface

   - Virtual network
   - Subnet: Data subnet 2 (Ethernet 2)
   - Select inbound ports

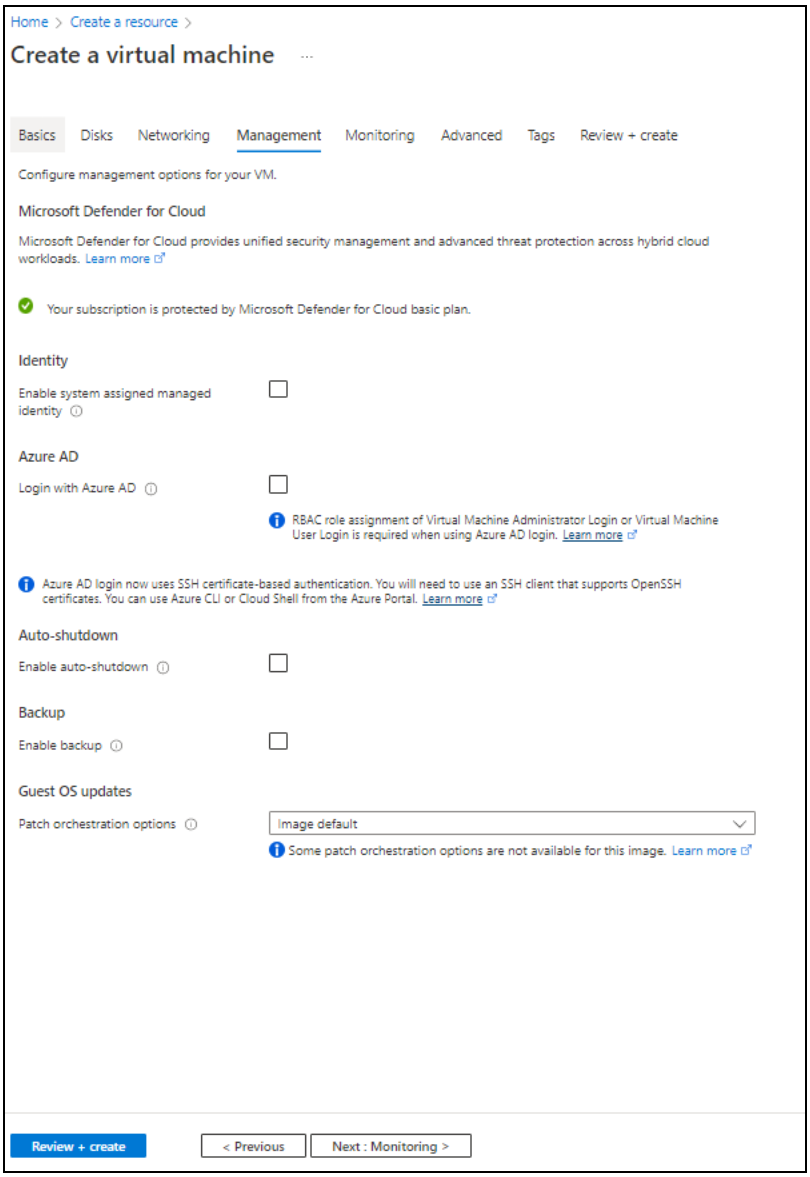
   Figure 69 : Create a virtual machine window - Networking tab



7. Leave the remaining fields as is and click **Next : Management** at the bottom of the window.

8. Select or enter the information in the **Management** tab as needed.

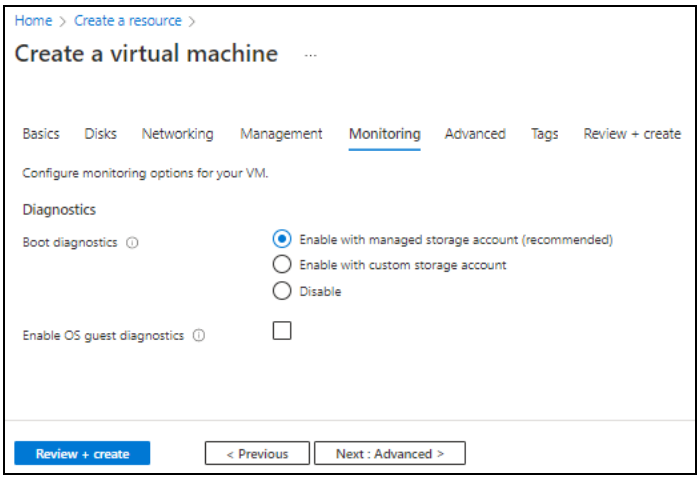
Figure 70 : Create a virtual machine window - Management tab



9. Click **Next : Monitoring** at the bottom of the window.

10. Select or enter the information in the **Monitoring** tab as needed.

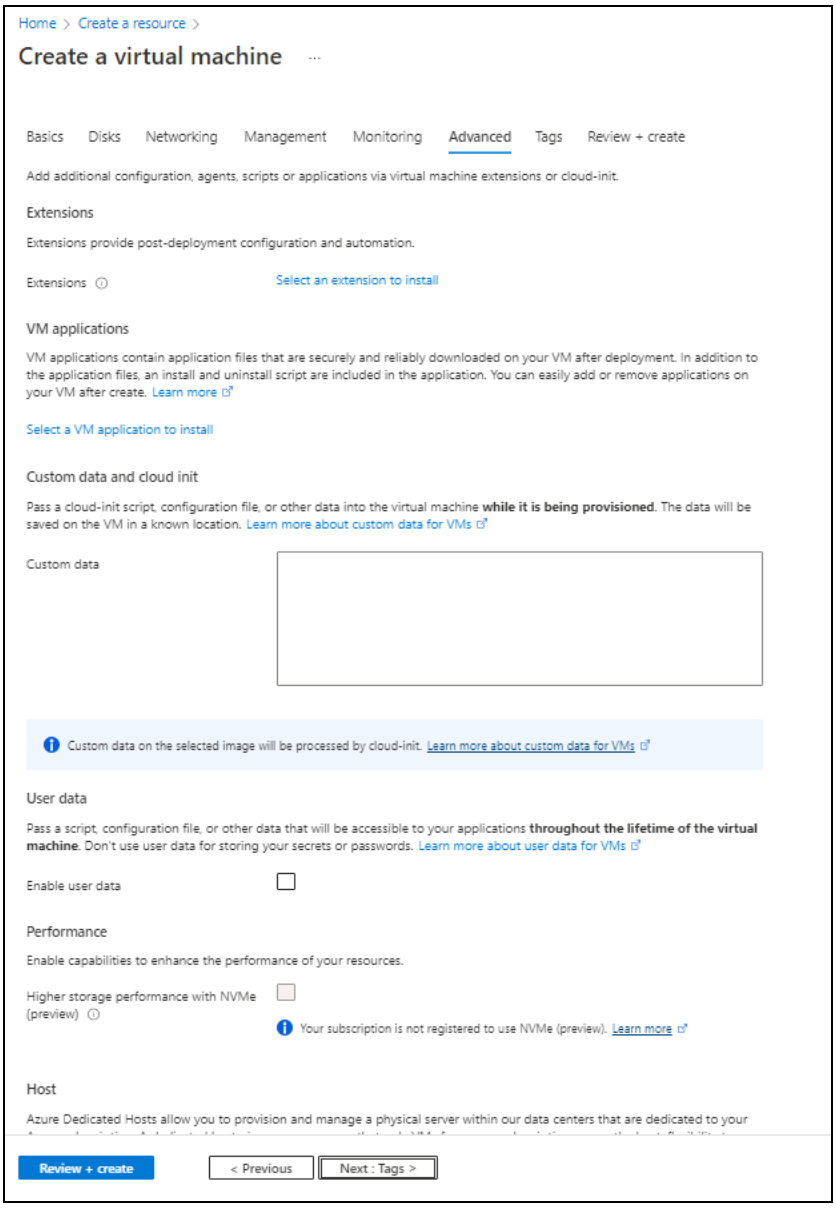
Figure 71 : Create a virtual machine window - Monitoring tab



11. Click **Next : Advanced** at the bottom of the window.

12. Select or enter the information in the **Advanced** tab as needed.

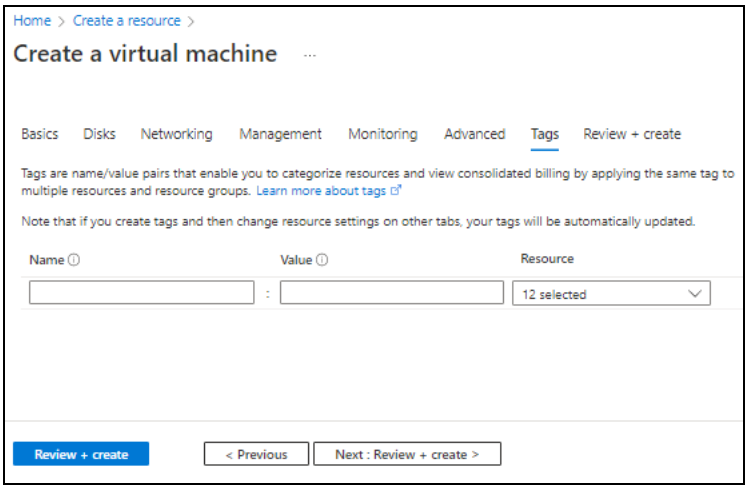
Figure 72 : Create a virtual machine window - Advanced tab



13. Click **Next : Tags** at the bottom of the window.

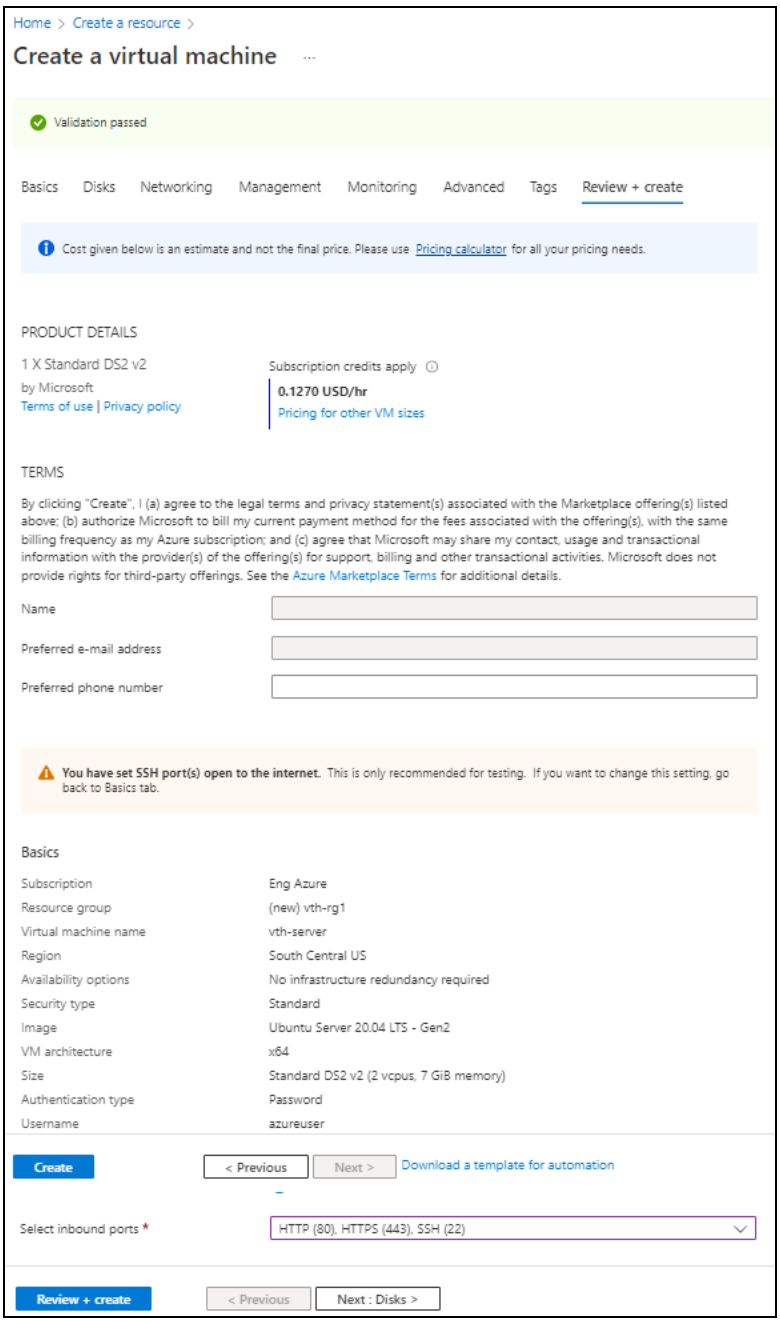
14. Select or enter the information in the **Tags** tab as needed.

Figure 73 : Create a virtual machine window - Tags tab



15. Click **Next : Review + create** at the bottom of the window.
The fields **Name** and **Preferred e-mail address** are auto-populated as per the Azure account.

Figure 74 : Create a virtual machine window - Review + create tab



16. Click **Create** at the bottom of the window.
    The Server machine gets created.
17. SSH the Server virtual machine and run the following command to install Apache:

```
sudo apt install apache2
```

While the Apache server is getting installed, you get a prompt to continue further. Enter 'Y' to continue. After the installation is complete, a newline prompt is displayed.

Create a Client Machine

To create a Client machine, perform the following steps:

1. From Home, navigate to **Azure Services** > **Create a resource** > **Virtual machine** and click **Create**.
   The **Create a virtual machine** window is displayed.
2. Select or enter the following mandatory information in the **Basics** tab:

   Project details

   - Subscription
   - Resource group

   Instance details

   - Virtual machine name - Client machine
   - Region
   - Image
   - Size

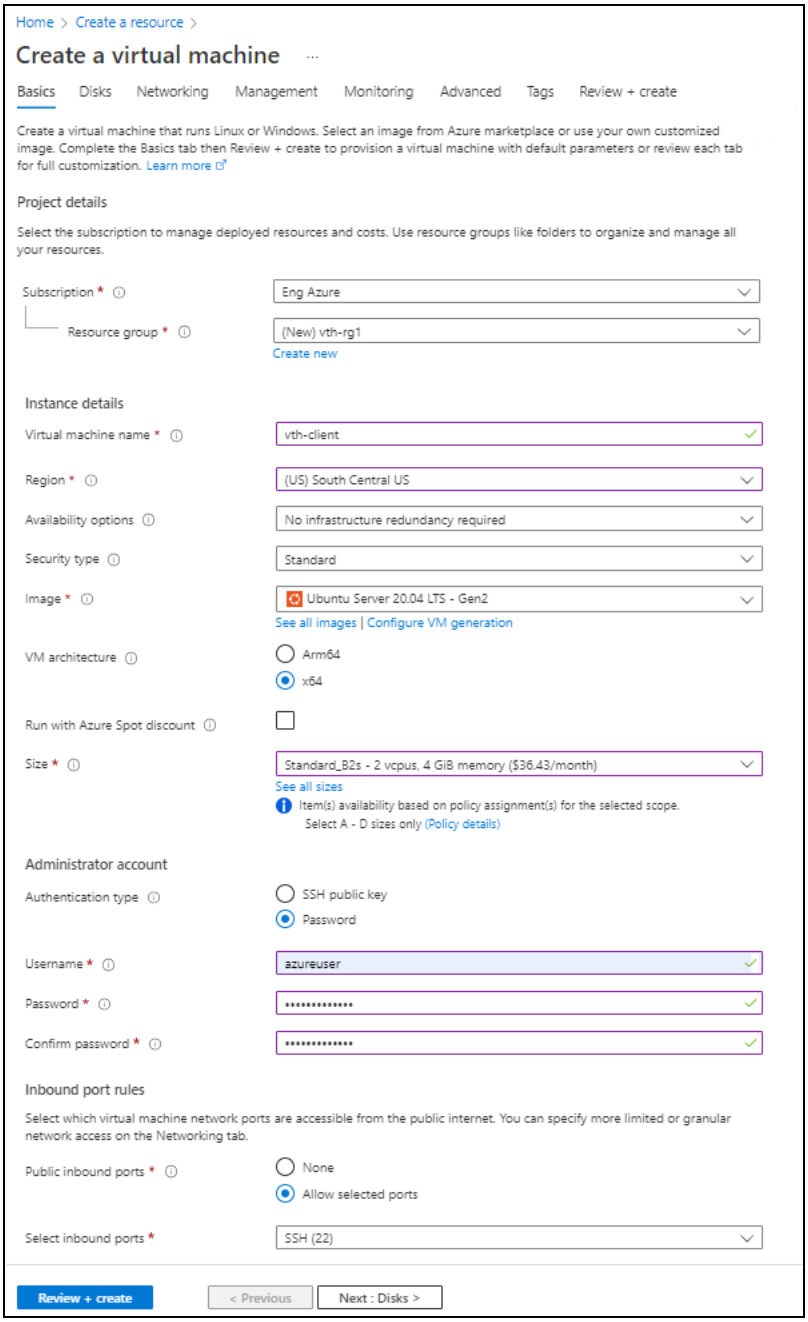
   Administrator account

   - Depending upon the Authentication type, provide the information.

   Inbound port rules

   - Public inbound ports
   - Select inbound ports

Figure 75 : Create a virtual machine window - Basics tab



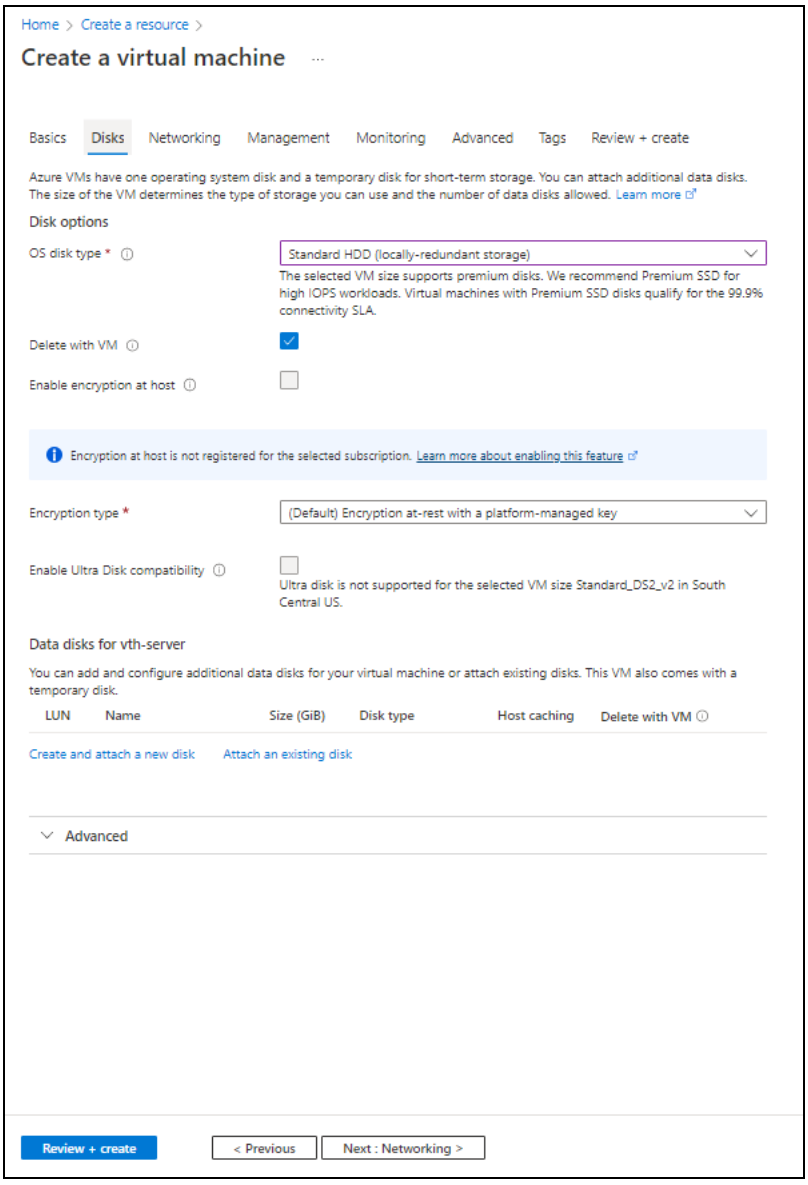
3. Leave the remaining fields as is and click **Next : Disks** at the bottom of the window.

4. Select or enter the following mandatory information in the **Disks** tab:

   Disk options

   - OS disk type
   - Encryption type

   Figure 76 : Create a virtual machine window - Disks tab



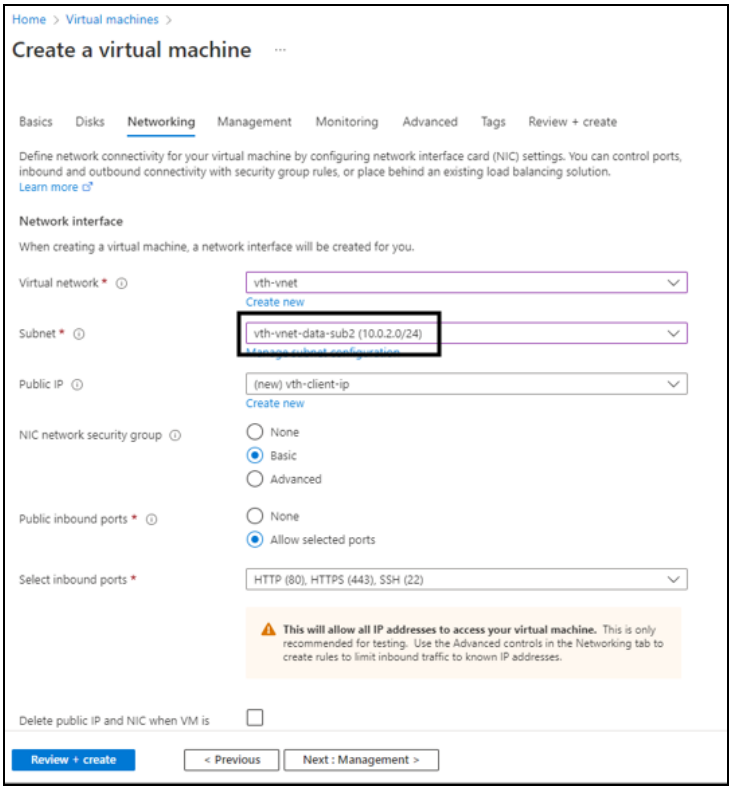
5. Leave the remaining fields as is and click **Next : Networking** at the bottom of the window.

6. Select or enter the following mandatory information in the **Networking** tab:

   Network interface

   - Virtual network
   - Subnet: Data subnet 1 (Ethernet 1)
   - Select inbound ports

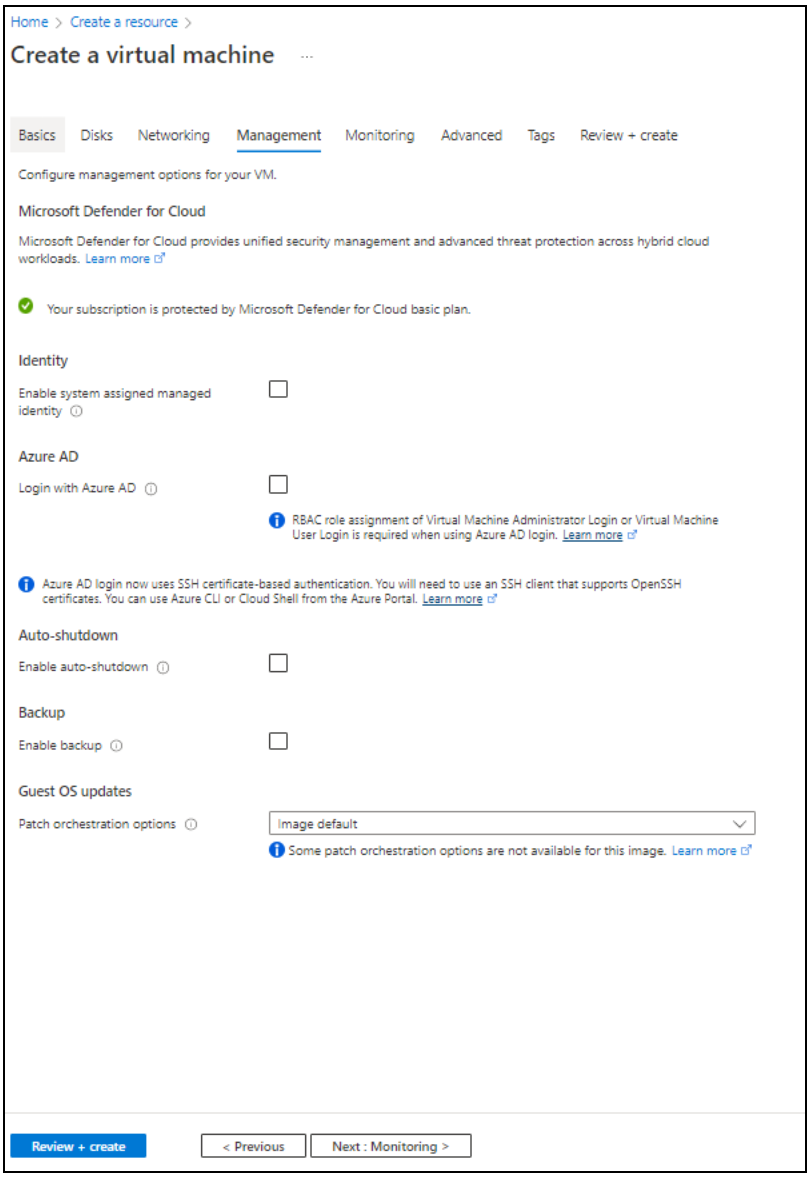
   Figure 77 : Create a virtual machine window - Networking tab



7. Leave the remaining fields as is and click **Next : Management** at the bottom of the window.

8. Select or enter the information in the **Management** tab as needed.

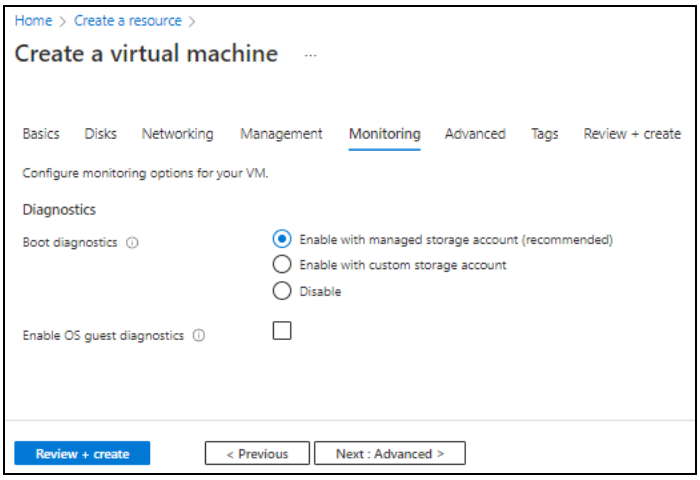
Figure 78 : Create a virtual machine window - Management tab



9. Click **Next : Monitoring** at the bottom of the window.

10. Select or enter the information in the **Monitoring** tab as needed.

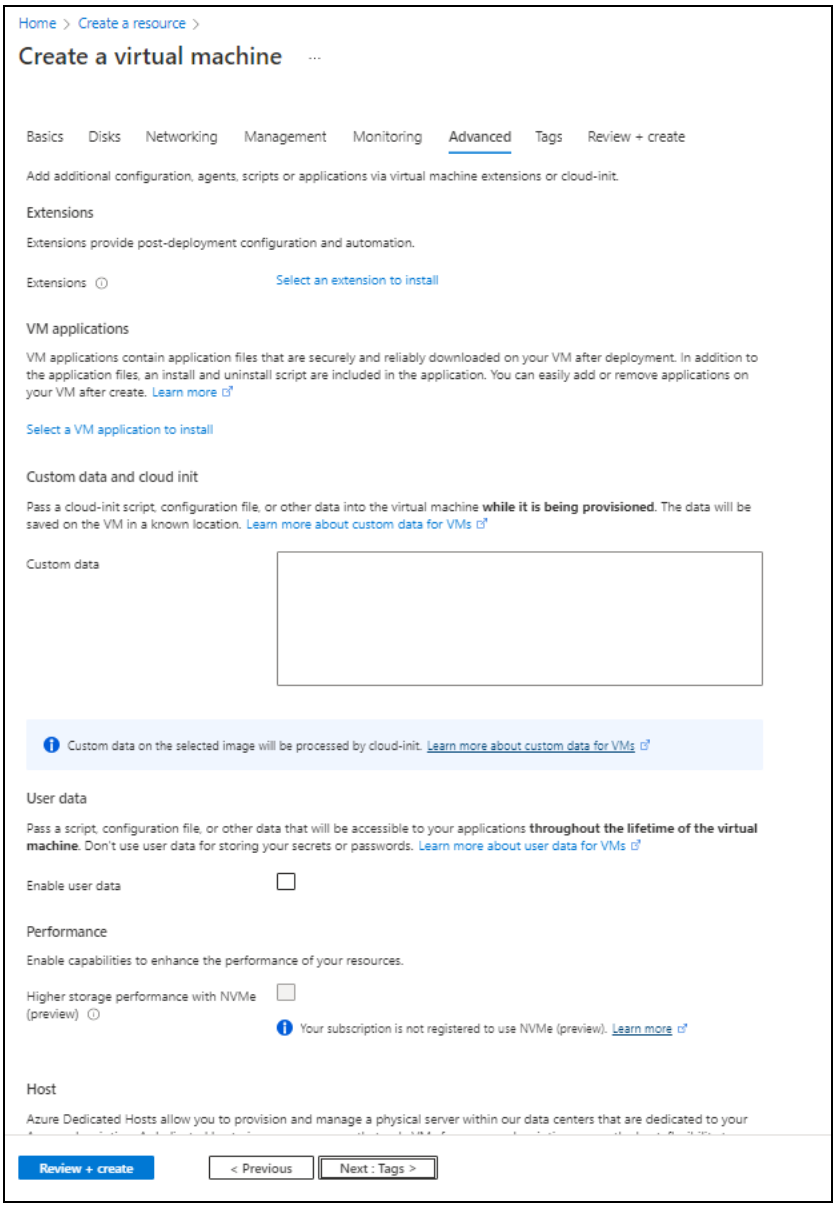
Figure 79 : Create a virtual machine window - Monitoring tab



11. Click **Next : Advanced** at the bottom of the window.

12. Select or enter the information in the **Advanced** tab as needed.

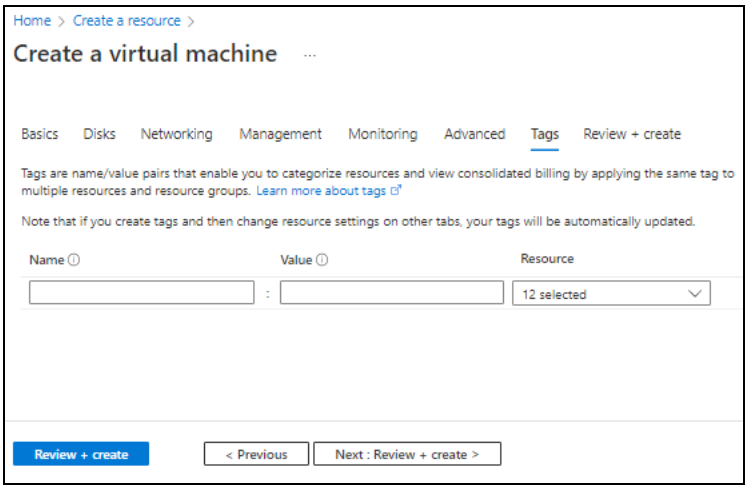
Figure 80 : Create a virtual machine window - Advanced tab



13. Click **Next : Tags** at the bottom of the window.

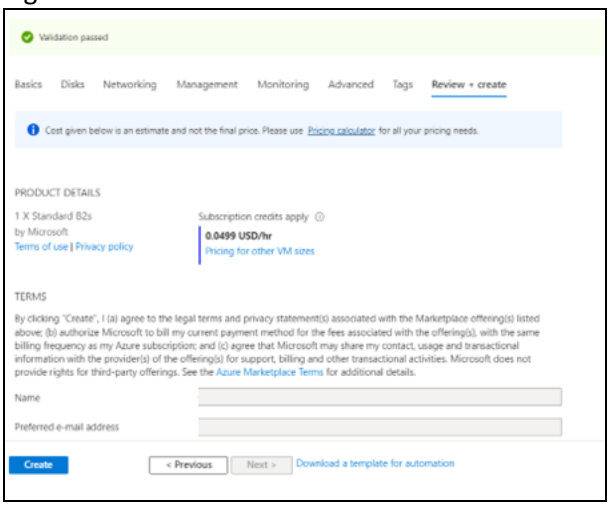
14. Select or enter the information in the **Tags** tab as needed.

Figure 81 : Create a virtual machine window - Tags tab



15. Click **Next : Review + create** at the bottom of the window.
The fields **Name** and **Preferred e-mail address** are auto-populated as per the Azure account.

Figure 82 : Create a virtual machine window - Review + create tab



16. Click **Create** at the bottom of the window.
The Client machine gets created.

Configure vThunder as an SLB

The following topics are covered:

- Initial Setup
- Change Password
- Deploy vThunder as an SLB

Initial Setup

Before deploying vThunder on Azure cloud as an SLB, configure the corresponding parameters in the PowerShell template.

To configure the parameters, perform the following steps:

1. Open the PS_TMPL_3NIC_2VM_SLB_CONFIG_PARAM.json with a text editor.

   NOTE: Each parameter has a default value mentioned in the parameter file.

2. Configure SLB server host or domain.
   The SLB server host value is the data NIC's private IP address instance acting as the server.
   Instead of a host, you can also use a domain name. To do so, replace the key 'host' with 'fqdn-name' and provide a domain name instead of the IP address.

```
      "slbServerHostOrDomain": {
        "server-name": "s1",
        "host": "10.0.3.7",
        "metadata": {
          "description": "SLB server host/fqdn-name. To use domain name
replace host with fqdn-name and ip address with domain name"
        }
      },
```

3. Configure SLB server ports.

```
      "slbServerPortList": {
        "value": [
          {
            "port-number": 53,
            "protocol": "udp",
           "health-check-disable":1
          },
          {
```

```
            "port-number": 80,
            "protocol": "tcp",
           "health-check-disable":1
          },
          {
            "port-number": 443,
            "protocol": "tcp",
           "health-check-disable":1
          }
        ]
      },
```

4. Configure service group list ports.

```
      "serviceGroupList": {
        "value": [
            {
              "name":"sg443",
              "protocol":"tcp",
             "health-check-disable":1
              "member-list": [
                {
                  "name":"s1",
                  "port":443
                }
              ]
            },
            {
              "name":"sg53",
              "protocol":"udp",
             "health-check-disable":1
              "member-list": [
                {
                  "name":"s1",
                  "port":53
                }
              ]
            },
              {
```

```
            "name":"sg80",
            "protocol":"tcp",
          "health-check-disable":1
            "member-list": [
              {
                "name":"s1",
                "port":80
              }
            ]
          }
        ]
    },
```

5. Configure virtual server.
   The virtual server default name is “vip”. The vip address is generated dynamically after deploying the PowerShell template. Therefore, its default value under **`virtualServerList`** should be replaced. To get the vip address, perform the following steps:

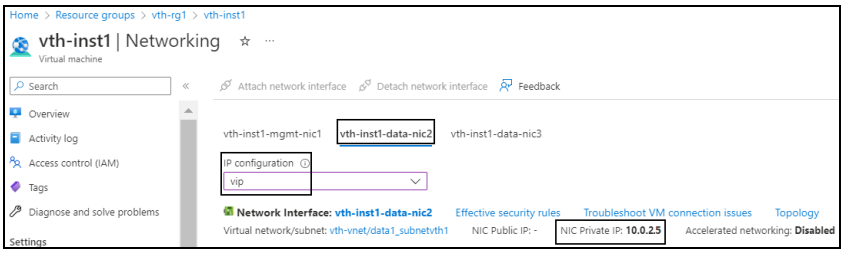
   a. From **Home**, navigate to **Azure Services > Resource Group >** <resource_group_name>.

   b. Go to the first virtual machine instance. Here, first virtual machine instance is **`vth-inst1`**.

   c. Select **Networking** from the left **Settings** panel.

   d. Select the Data NIC 2 tab > **IP configuration** > **`vip`**. Here, Data NIC 2 is **`vth-inst1-data-nic2`**.

   Figure 83 : Virtual machine - Networking window - Data NIC 2 tab



   e. Select the **NIC Private IP**.

f. Replace the **ip-address** value under **virtualServerList** with this **vip**.

```
        "virtualServerList": {
          "virtual-server-name": "vip",
          "ip-address": "10.0.2.5",
          "metadata": {
            "description": "virtual server is using VIP from
ethernet 1 subnet"
          },
          "value": [
            {
              "port-number":53,
              "protocol":"udp",
              "ha-conn-mirror":1,
              "auto":1,
              "service-group":"sg53"
            },
            {
              "port-number":80,
              "protocol":"http",
              "auto":1,
              "service-group":"sg80"
            },
            {
              "port-number":443,
              "protocol":"https",
              "auto":1,
              "service-group":"sg443"
            }
          ]
      },
```

NOTE: **ha-conn-mirror** does not work on port 80 and 443.

6. Configure SSL.

```
    "sslConfig": {
        "requestTimeOut": 40,
        "Path": "<absolute path of the ssl certificate file>",
```

```
            "File": "<certificate-name>",
            "CertificationType": "pem"
        }
```

NOTE: By default, SSL configuration is disabled i.e. no SSL configuration is applied.

Example The sample values for the SSL certificate are as shown below:

```
      "sslConfig": {
          "requestTimeOut": 40,
          "Path": "C://Users//..//..//..//server.pem" or
"C:\Users\..\..\..\certs\server.pem",
          "File": "server",
          "CertificationType": "pem"
                      }
```

7. Provide the resource group name.

```
     "resourceGroupName: "vth-rg1"
     "vThUsername": "admin"
```

NOTE: Do not change the vThunder instance username.

8. Verify if the vip address and all other configurations in the PS_TMPL_3NIC_2VM_SLB_CONFIG_PARAM.json file are correct and then save the changes.

Change Password

To change the password, perform the following steps:

1. Run the following command to change password:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_HA_GLM_CHANGE_
PASSWORD_2.ps1
```

NOTE: It is highly recommended to change the default password provided by the A10 Networks Support when you log in the vThunder instance for the first time.

2. Provide the default and new password when prompted:

```
Enter Default Password:***
Enter New Password:***
Confirm New Password:***
```

The default password is provided by the A10 Networks Support. The new password should follow the Default password policy. For more information, see Default Password Policy.

Deploy vThunder as an SLB

To deploy vThunder on Azure cloud as an SLB, perform the following steps:

1. From PowerShell, navigate to the folder where you have downloaded the PowerShell template.
2. Run the following command to create vThunder SLB instance using the same resource group:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_SLB_CONFIG_3.ps1 -
resourceGroup <resource_group_name>
```

Example:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_SLB_CONFIG_3.ps1 -
resourceGroup vth-rg1
```

A message is prompted to upload the SSL certificate.

```
SSL Certificate
Do you want to upload ssl certificate ?
[Y] Yes  [No] No [?] Help (default is "N"): Y
SLB Server Host IP: 10.0.3.7
Virtual Server Name: vip
Resource Group Name: vth-rg1
vThunder1 Public IP: 13.85.81.137
vThunder2 Public IP: 13.85.81.113
Configuring vm: vth-inst1
configured ethernet- 1 ip
configured ethernet- 2 ip
Configured server
Configured service group
```

```
0
Configured virtual server
SSL Configured.
Configurations are saved on partition: shared
Configured vThunder Instance 1
Configuring vm: vth-inst2
configured ethernet- 1 ip
configured ethernet- 2 ip
Configured server
Configured service group
0
Configured virtual server
SSL Configured.
Configurations are saved on partition: shared
Configured vThunder Instance 2
```

3. If the SSL Certificate upload is successful, a message 'SSL Configured' is displayed.

Configure High Availability

The following topics are covered:

- Configure Azure Access Key
- Configure High Availability for vThunder

Configure High Availability for vThunder

The following topics are covered:

- Initial Setup
- Create High Availability for vThunder

Initial Setup

Before configuring high availability for vThunder, configure the corresponding parameters in the PowerShell template.

To configure the parameters, perform the following steps:

1. Open the PS_TMPL_3NIC_2VM_HA_CONFIG_PARAM.json with a text editor.

   NOTE: Each parameter has a default value mentioned in the parameter file.

2. Configure DNS.

```
"dns": {
    "value": "8.8.8.8"
},
```

3. Configure a Network Gateway IP.
   The default value of network gateway IP address is 10.0.1.1 as this is the first IP address of the data subnet 1 configuration.

```
"rib-list": [
    {
    "ip-dest-addr":"0.0.0.0",
    "ip-mask":"/0",
    "ip-nexthop-ipv4": [
        {
        "ip-next-hop":"10.0.2.1"
        }
    ]
    }
],
```

4. Set VRRP-A.

```
"vrrp-a": {
    "set-id":1
},
```

5. Set a Terminal Idle Timeout.

```
"terminal": {
    "idle-timeout":0
},
```

6. Configure the VRID details.
   The default value of vrid is 0. The default priority for vThunder-1 is 100, and for vThunder-2 is 99 (100-1). The floating ip address value is generated dynamically after deploying the PowerShell template. Therefore, its default value under **`vrid-list`** should be replaced. To get the fip address, perform the following steps:

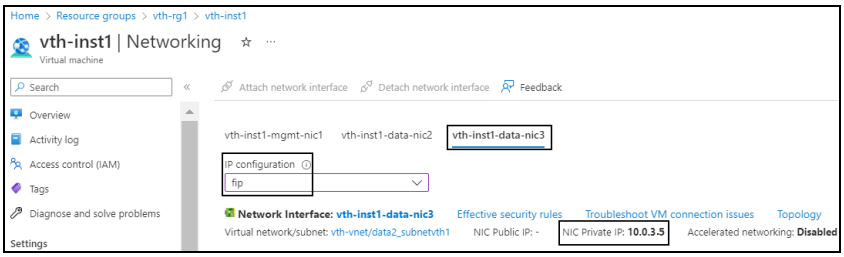
a. From the **Home**, navigate to **Azure Services** > **Resource Group** > <resource_group_name>.

b. Go to the first virtual machine instance. Here, first virtual machine instance is **`vth-inst1`**.

c. Select **Networking** from the left **Settings** panel.

d. Select the Data NIC 3 tab > **IP configuration**. Here, **`vth-inst1-data-nic3`**.

Figure 84 : Virtual machine - Networking window - Data NIC 3 tab



e. Select the **NIC Private IP**.

f. Replace the **`ip-address`** value under **`vrid-list`** with this **`fip`**.

```
"vrid-list": [
            {
            "vrid-val":0,
            "blade-parameters": {
                "priority": 100
            },
            "floating-ip": {
                "ip-address-cfg": [
                    {
                      "ip-address":"10.0.3.5"
                    }
                  ]
                }
            }
        ]
```

7. Verify if all the configurations in the PS_TMPL_3NIC_2VM_HA_CONFIG_PARAM.json file are correct and then save the changes.

Create High Availability for vThunder

To create High Availability for vThunder, perform the following steps:

1. Import Azure access key on both the vThunder instances. For more information, refer Import Azure Access Key.
2. Run the following command to configure both VM in HA mode.

```
S C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_HA_CONFIG_4.ps1 -
resourceGroup <resource_group_name>
```

Example:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_HA_CONFIG_4.ps1 -
resourceGroup vth-rg1
```

Configure vThunder using GLM

The following topics are covered:

- Initial Setup
- Apply GLM License

Initial Setup

Before configuring vThunder with GLM, configure the corresponding parameters in the PowerShell template.

To configure the parameters, perform the following steps:

1. Open the PS_TMPL_3NIC_2VM_GLM_CONFIG_PARAM.json with a text editor.
2. Configure GLM account details.

```
{
  "parameters": {
    "user_name": {
      "value": "user_name"
    },
    "user_password": {
      "value": "user_password"
```

```
    },
    "entitlement_token": {
      "value": "token"
    }
  }
}
```

3. Verify if the configurations in the PS_TMPL_3NIC_2VM_GLM_CONFIG_PARAM.json file are correct and then save the changes.

Apply GLM License

To apply GLM License, perform the following steps:

1. From PowerShell, navigate to the folder where you have downloaded the PowerShell template.
2. Run the following command to apply SLB on vThunder:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_GLM_CONFIG_5.ps1 -
resourceGroupName <resource_group_name>
```

Example:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_GLM_CONFIG_5.ps1 -
resourceGroup vth-rg1
```

3. If the GLM License is applied successfully, a message is displayed.

```
ConfigureGlm
{
  "response": {
       "status": "OK",
       "msg": "BASE License successfully updated, please log out and
log back in to access license featurebA1070459ec380000\n"
  }
}
GlmRequestSend
Configurations are saved on partition: shared
WriteMemory
```

Access vThunder using Console/CLI

vThunder can be accessed using any of the following ways:

- Access vThunder using CLI
- Access vThunder using GUI

Access vThunder using CLI

To access vThunder using CLI, perform the following steps:

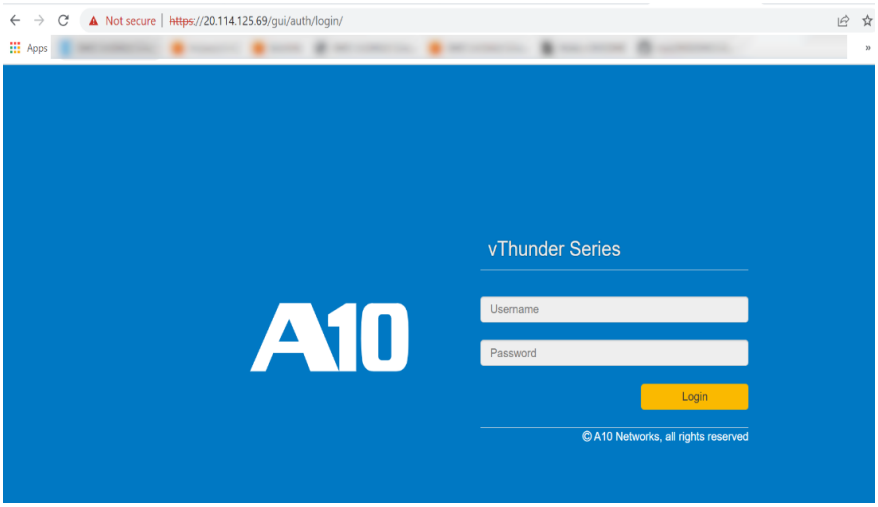
1. Open PuTTY.
2. Enter or select the following basic information in the PuTTy Configuration window:
   - Hostname: Public IP of Virtual Machine Instance 1
     Here, Public IP of **`vth-inst1`**.
   - Connection Type: SSH
3. Click **Open**.
4. In the active PuTTY session, login with the recently changed password:

```
login as: xxxx <---Enter username provided by A10 Networks Support--->
Using keyboard-interactive authentication.
Password: xxxx <---Enter your password--->
Last login: Day MM DD HH:MM:SS from a.b.c.d

System is ready now.

[type ? for help]

vThunder> enable <---Execute command--->
Password:<---just press Enter key--->
vThunder#config <---Configuration mode--->
```

Access vThunder using GUI

To access vThunder using GUI, perform the following steps:

1. Open any browser.
2. Enter *https://<vthunder_public_IP>/gui/auth/login/* in the address bar.



3. Enter the recently configured user credentials.
   The home page gets displayed.

Verify Deployment

To verify vThunder SLB deployment using the PowerShell template, perform the following steps:

1. Run the following command on vThunder:

```
vThunder(config)#show running-config slb
```

   If the deployment is successful, the following slb configuration is displayed:

```
!Section configuration: 602 bytes
!
slb server s1 10.0.3.7
  port 53 udp
       health-check-disable
  port 80 tcp
       health-check-disable
  port 443 tcp
       health-check-disable
!
```

```
slb service-group sg443 tcp
  health-check-disable
  member s1 443
!
slb service-group sg53 udp
  health-check-disable
  member s1 53
!
slb service-group sg80 tcp
  health-check-disable
  member s1 80
!
slb virtual-server vip 10.0.2.5
  port 53 udp
    ha-conn-mirror
    source-nat auto
    service-group sg53
  port 80 http
    source-nat auto
    service-group sg80
  port 443 https
    source-nat auto
    service-group sg443
!
```

2. Run the following command to verify the SSL Certificate configuration:

```
vThunder(config)#show pki cert
```

If the deployment is successful, the following SSL configuration is displayed:

```
Name    Type                        Expiration  Status
-----------------------------------------------------------------
server certificate Jan 28 12:00:00 2028 GMT [Unexpired, Bound]
```

3. Run the following command to verify HA:

```
vThunder(config)#show running-config
```

If the deployment is successful, the following SSL configuration is displayed:

```
!Current configuration: 291 bytes
!Configuration last updated at 17:36:35 IST Mon Sep 5 14 2022
!Configuration last saved at 17:35:40 IST Wed Sep 5 14 2022
!64-bit Advanced Core OS (ACOS) version 5.2.0, build 155 (Aug-10-
2020,14:34)

!
vrrp-a common
  device-id 1
  set-id 1
  enable
!
terminal idle-timeout 0
!
ip dns primary 8.8.8.8
!
!
glm use-mgmt-port
glm enable-requests
glm token A10f771cecbe
!
interface management
  ip address dhcp
!
interface ethernet 1
  enable
  ip address dhcp
!
interface ethernet 2
  enable
  ip address dhcp
!
vrrp-a vrid 0
  floating-ip 10.0.3.5
  floating-ip 10.0.2.5
  blade-parameters
       priority 100
```

```
!
vrrp-a peer-group
  peer 10.0.2.4
  peer 10.0.2.6
!
ip route 0.0.0.0 /0 10.0.1.1
!
```

4. Run the following command to verify the GLM License Provision configuration:

```
vThunder(config)#show license-info
```

If the GLM is successfully applied on vThunder, the following GLM configuration is displayed:

```
Host ID         : 5DCB01EC264BECCCFECB3C2ED42E02384EE8C527
USB ID          : Not Available
Billing Serials: A10f771cecbe0000
Token           : A10f771cecbe
Product         : ADC
Platform        : vThunder
Burst           : Disabled
GLM Ping Interval In Hours : 24
-----------------------------------------------------------------
Enabled Licenses Expiry Date              Notes
-----------------------------------------------------------------
SLB              None
CGN              None
GSLB             None
RC               None
DAF              None
WAF              None
AAM              None
FP               None
WEBROOT          N/A         Requires an additional Webroot license.
THREATSTOP       N/A         Requires an additional ThreatSTOP license.
QOSMOS           N/A         Requires an additional QOSMOS license.
WEBROOT_TI       N/A         Requires an additional Webroot Threat Intel
license.
CYLANCE          N/A         Requires an additional Cylance license.
```

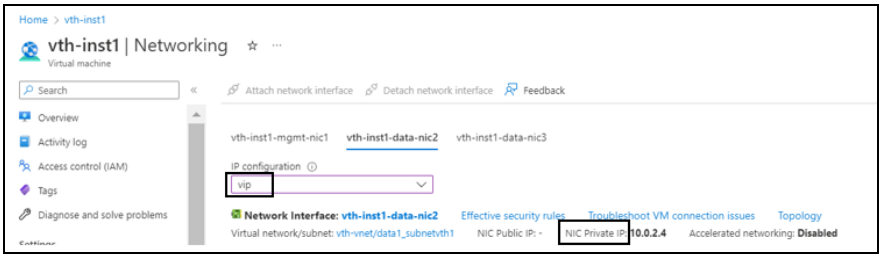
```
IPSEC_VPN          N/A          Requires an additional IPsec VPN license.
25 Mbps Bandwidth 21-December-2022
```

Verify Traffic Flow

To verify the traffic flow from client machine to server machine via vThunder, perform the following:

1. From **Azure Portal** > **Azure Services** > **Resource Group** > <resource_group_name> > <active_virtual_machine_instance> > **Settings** > **Networking**.
   Here, **`vth-inst1`** is the active vThunder instance name.
2. Copy the VIP address of the active vThunder instance.

   Figure 85 : Active vThunder instance 1 VIP



3. Select your client instance from the **Virtual machine** list.
   Here, **`vth-client`** is the client instance name.
4. SSH your client machine and run the following command to verify the traffic flow:

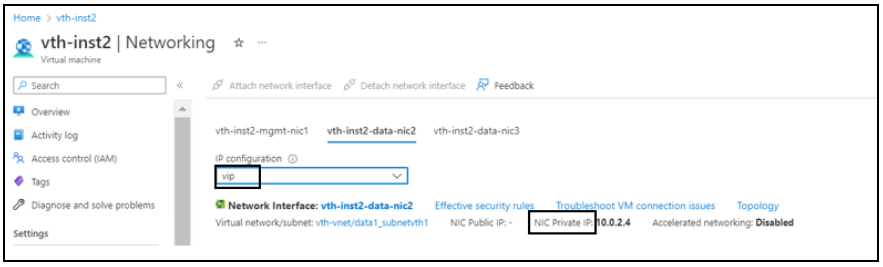
   ```
   curl <VIP>
   ```

   Example

   ```
   curl 10.0.2.4
   ```

   Verify if a response is received.
5. After the switchover, vThunder instance 2 is active, so copy the VIP address of the vThunder instance 2.

Figure 86 : Active vThunder instance 2 VIP



6. SSH your client machine and run the following command to verify the traffic flow:

```
curl <VIP>
```

Example

```
curl 10.0.2.4
```

Verify if a response is received.

Deploy PowerShell A10-vThunder_ADC-3NIC-2VM-HA-GLM-PUBVIP-BACKAUTO

Figure 87 shows the 3NIC-2VM-HA-GLM-PUBVIP-BACKAUTO deployment topology. Using this template, two vThunder instances can be deployed containing:

- One management interface and two data interfaces each
- HA support
- GLM integration
- Backend server autoscaling support.

Figure 87 : 3NIC-2VM-HA-GLM-PUBVIP-BACKAUTO Topology

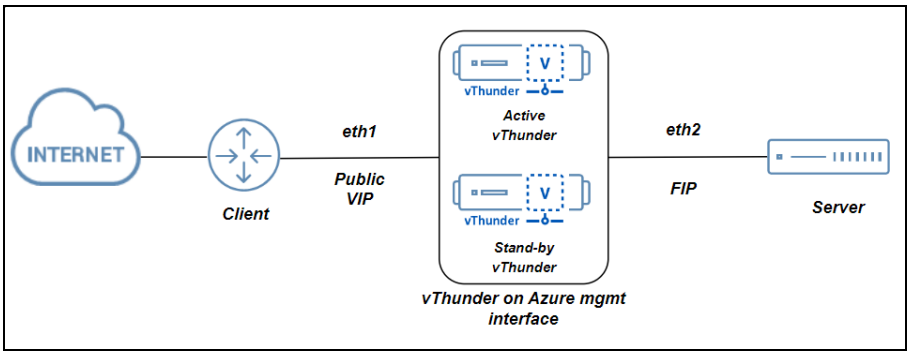
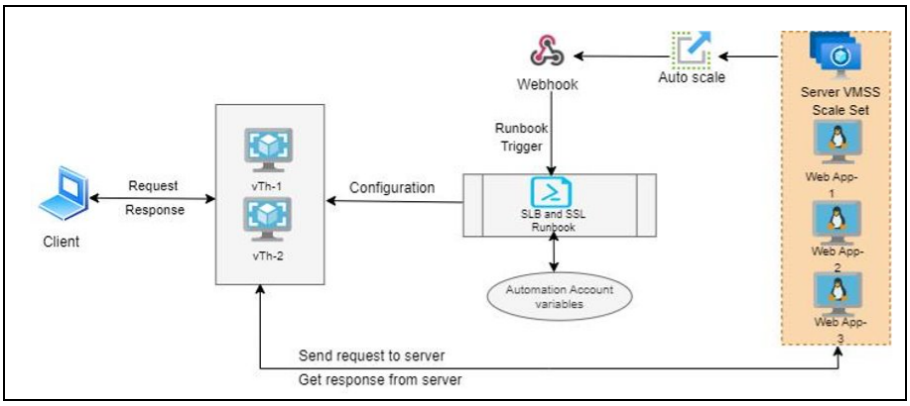


Figure 88 shows the process flow when different Azure resources and system components are connected to each other in the 3NIC-2VM-HA-GLM-PUBVIP-BACKAUTO topology.

Figure 88 : 3NIC-2VM-HA-GLM-PUBVIP-BACKAUTO Process Flow



The following topics are covered:

System Requirements 179
Create vThunder Instances 184
Configure Server VMSS 188
Configure Client Machine 197
Configure Automation Account 204
Configure vThunder as an SLB 213
Configure High Availability for vThunder 218
Configure vThunder using GLM 221
Access vThunder using CLI or GUI 222
Verify Deployment 224
Verify Traffic Flow 227

System Requirements

The PowerShell template will display the default values when you download and save the files on your local machine. You can modify the default values as required for your deployment.

You need the following resources to deploy vThunder on the Azure cloud:

Table 10 : System Requirements

Resource Name	Description	Default Value
Azure Resource Group	A resource group with the specified name and location is created, if it doesn't exist. All the resources required for this template is created under the resource group.	Here, the Azure resource group name used is **`vth-rg1`**.

Resource Name	Description	Default Value
Azure Storage Account	A storage account is created inside the resource group, if it doesn't exist. If the storage name already exists, the following error is displayed “The storage account named vthunderstorage already exists under the subscription". **Performance**: Standard **Replication**: Read-access geo-redundant storage (RA-GRS) **Account kind**: Storagev2 (general purpose v2)	`vthunderstorage`
Virtual Machine (VM) Instance	Two virtual machine instances are created for vThunder. **Product**: A10 vThunder **Operating system**: Linux **Default Size**: Standard_B4ms (4 vCPUs, 16 GiB Memory)	`vth-inst1` `vth-inst2`

Resource Name	Description	Default Value
	NOTE: Before selecting any VM size, it is highly recommended to do an assessment of your projected traffic. Table 11 lists the supported VM sizes.	
Azure Automation Account	An automation account is created under the resource group.	**vth-amt-acc**
Azure Runbook with Webhook	A custom runbook is created under the automation account: SLB-Config A webhook is created for SLB.	
Virtual Machine Scale Set [VMSS]	A virtual machine scale set is created.	**vth-server-vmss**
Virtual Cloud Network [VCN]	A virtual network is assigned to the virtual machine instance.	**vth-vmss-vnet** Address prefix for virtual network:

Resource Name	Description	Default Value
		10.0.0.0/16
Subnet	Three subnets are created with an address prefix each.	Subnet1: vth-vnet1-mgmt-sub1 10.0.1.0/24 Subnet2: vth-vnet1-data-sub2 10.0.2.0/24 Subnet3: vth-vnet1-data-sub3 10.0.3.0/24
Network Interface Card [NIC]	Two types of interfaces are created for each vThunder instance: • Management Interface with public IP • Data Interface with primary private IP [Ethernet 1, Ethernet 2] **NOTE:** The secondary IP of data interface is taken from DHCP server.	vth-inst1-mgmt-nic1: 10.0.1.4 vth-inst1-data-nic2: 10.0.2.4 [Primary IP] 10.0.2.X [Secondary IP] vth-inst1-data-nic3: 10.0.3.4 [Primary IP] 10.0.3.X [Secondary IP] vth-inst2-mgmt-nic1: 10.0.1.6 vth-inst2-data-nic2: 10.0.2.6 [Primary IP] 10.0.2.X [Secondary IP] vth-inst2-data-nic3: 10.0.3.6 [Primary IP] 10.0.3.X [Secondary IP]
Network Security	A security group is created for all the asso-	vth-nsg1

Resource Name	Description	Default Value
Group [NSG]	ciated default inter-faces.	`vth-nsg2`
Azure Ser-vice Applic-ation Access Key	An existing key can be used or a new key can be created. For more information, refer Azure Service Applic-ation Access Key.	

Supported VM Sizes

Table 11 : Supported VM sizes

Series	Size	Qualified Name
A series	Standard A4v2	Standard_A4_v2
	Standard A4mv2	Standard_A4m_v2
	Standard/Basic A4	Standard_A4
	Standard A8v2	Standard_A8_v2
B series	Standard B2s	Standard_B2_s
	Standard B2ms	Standard_B2ms
	Standard B4ms	Standard_B4ms
D series	Standard D3v2	Standard_D3_v2
	Standard DS3v2	Standard_DS3_v2
	Standard D5v2	Standard_D5_v2
F series	Standard F4s	Standard_F4s
	Standard F8	Standard_F8
	Standard F16s	Standard_F16s

Azure is going to retire few of the above listed VM sizes soon, see Virtual Machine series | Microsoft Azure.

For more information on Windows and Linux VM sizes, see

https://docs.microsoft.com/en-us/azure/virtual-machines/sizes-general

https://docs.microsoft.com/en-us/azure/virtual-machines/linux/sizes.

Create vThunder Instances

The following topics are covered:

- Initial Setup
- Deploy vThunder

Initial Setup

Before deploying vThunder on Azure cloud, configure the corresponding parameters in the PowerShell template.

To configure the parameters, perform the following steps:

1. Navigate to the folder where you have downloaded the PowerShell template, and open the PS_TMPL_3NIC_2VM_PARAM.json with a text editor.

   NOTE: Each parameter has a default value mentioned in the parameter file.

2. Provision the vThunder instance by entering the default admin credentials as follows:

```
"adminUsername": {
  "value": "vth-user"
},
"adminPassword": {
  "value": "vth-Password"
},
```

NOTE: This is a mandatory step during VM creation. Once the device is provisioned, vThunder auto-deletes all users except the default user.

3. Configure a virtual network.

```
"virtual_network": {
  "value": "vth-vmss-vnet"
},
```

4. Configure vThunder instance names.

```
"vmName_vthunder1": {
  "value": "vth-inst1"
},
"vmName_vthunder2": {
  "value": "vth-inst2"
},
```

5. Set VM size for vThunder.

```
"vmSize": {
  "value": "Standard_B4ms"
},
```

Use a suitable VM size that supports at least 3 NICs. For VM sizes, see Supported VM Sizes section.

6. Copy the desired vThunder Image Name and Product Name from the Azure Marketplace for A10 vThunder and update the details in the parameter file as follows:

```
"vThunderImage": {
  "value":"vthunder_520_byol"
},
"publisherName": {
  "value": "a10networks"
},
"productName": {
  "value": "a10-vthunder-adc-520-for-microsoft-azure"
},
```

NOTE: Do not change the publisher name.

7. Configure three network interface cards for two vThunder instances.

```
"nic1Name_vm1": {
  "value": "vth-inst1-mgmt-nic1"
},
"nic2Name_vm1": {
  "value": "vth-inst1-data-nic2"
},
"nic3Name_vm1": {
  "value": "vth-inst1-data-nic3"
},
"nic1Name_vm2": {
  "value": "vth-inst2-mgmt-nic1"
},
"nic2Name_vm2": {
  "value": "vth-inst2-data-nic2"
},
"nic3Name_vm2": {
  "value": "vth-inst2-data-nic3"
},
```

8. Configure an address prefix and subnet values for one management interface and two data interface.

```
"vm1MgmtIntfName": {
  "value": "vth-inst1-mgmt"
},
"addressPrefix": {
  "value": "10.0.0.0/16"
},
"mgmtIntfPrivatePrefix": {
  "value": "10.0.1.0/24"
},
"vm1Eth1Name": {
  "value": "vth-inst1-data1"
},
"eth1PrivatePrefix": {
  "value": "10.0.2.0/24"
},
"vm1Eth2Name": {
```

```
      "value": "vth-inst1-data2"
    },
    "eth2PrivatePrefix": {
      "value": "10.0.3.0/24"
    },
    "vm2MgmtIntfName": {
      "value": "vth-inst2-mgmt"
    },
    "vm2Eth1Name": {
      "value": "vth-inst2-data1"
    },
    "vm2Eth2Name": {
      "value": "vth-inst2-data2"
    },
```

9. Configure network security group for two vThunder instances.

```
    "networkSecurityGroupName_vm1": {
      "value": "vth-nsg1"
    },
    "networkSecurityGroupName_vm2": {
      "value": "vth-nsg2"
    }
  }
```

10. Verify if all the configurations in the PS_TMPL_3NIC_2VM_PARAM.json file are correct and then save the changes.

Deploy vThunder

To deploy vThunder on Azure cloud, perform the following steps:

1. From Start menu, open PowerShell and navigate to the folder where you have downloaded the PowerShell template.
2. Run the following command to create a deployment group in Azure and provide a unique storage account name when prompted.

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_1.ps1 -resourceGroup
<resource_group_name> -location "<location_name>"
```

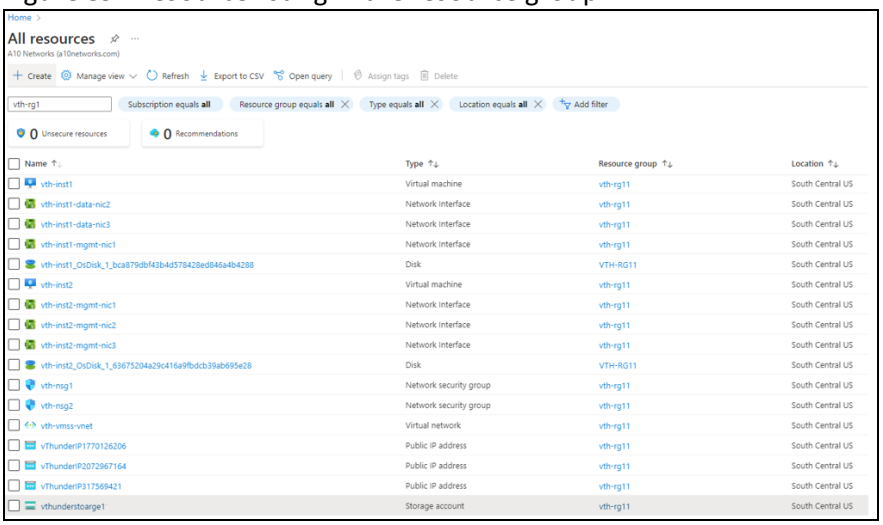
Example:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_1.ps1 -resourceGroup
vth-rg1 -location "south central us"

cmdlet .\PS_TMPL_3NIC_2VM_1.ps1 at command pipeline position 1
Supply values for the following parameters:
storageaccount: vthunderstorage
vth-rg1
vthunderstorage
South Central US
```

Here, **`vth-rg1`** resource group is created.

3. Verify if all the above listed resources are created in the **Home** > **Azure Services > Resource Group >** <resource_group_name>.

Figure 89 : Resource listing in the resource group



Configure Server VMSS

The following topics are covered:

- Create a Server Machine
- Verify the Server VMSS Creation

Create a Server Machine

To create a Server machine, perform the following steps:

1. From Home, navigate to **Azure Services** > **Virtual machine scale sets** and click **Create**.
   The **Create a virtual machine** window is displayed.
2. Select or enter the following mandatory information in the **Basics** tab:

   Project details

   - Subscription
   - Resource group

   Scale set details

   - Virtual machine scale set name - Server machine
   - Region

   Orchestration

   - Orchestration mode

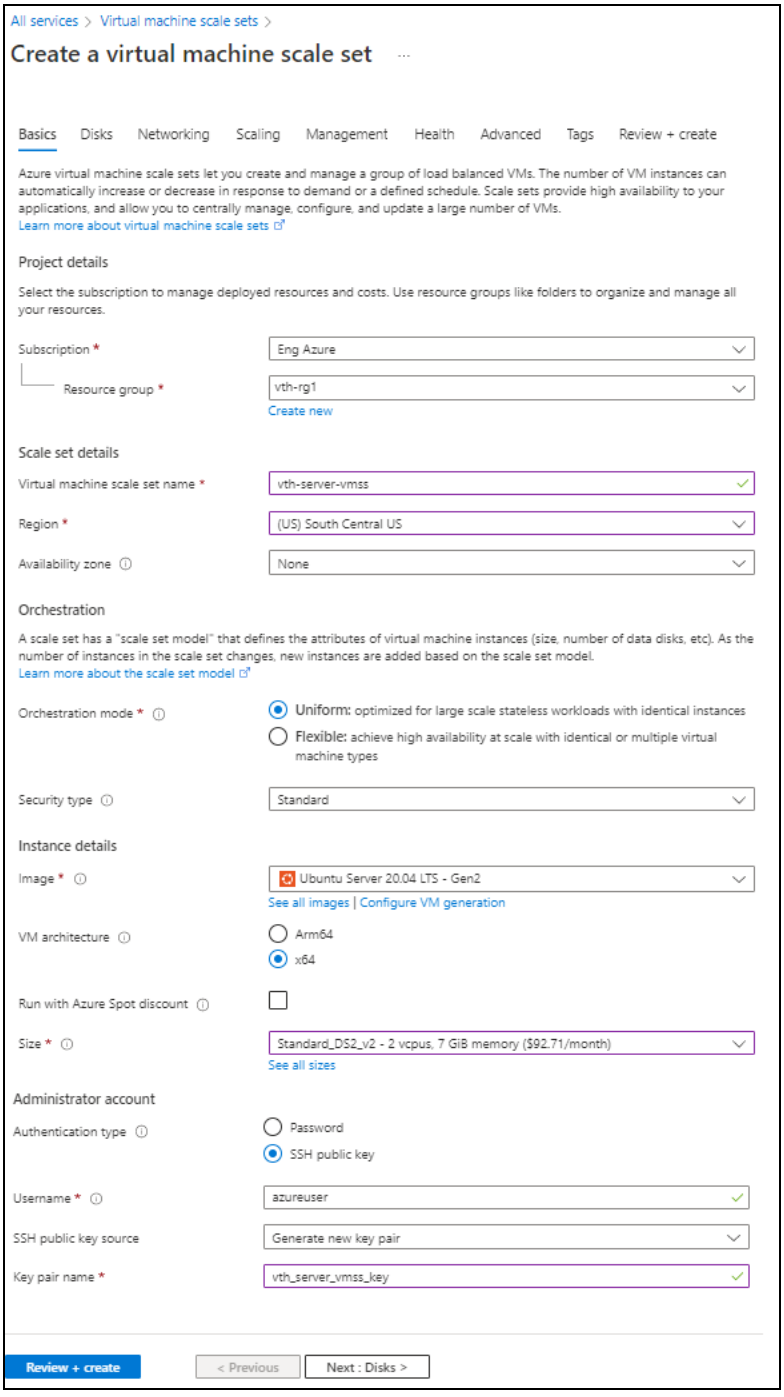
   Instance details

   - Image
   - Size

   Administrator account

   - Depending upon the Authentication type, provide the information.

Figure 90 : Create a virtual machine scale set window - Basics tab



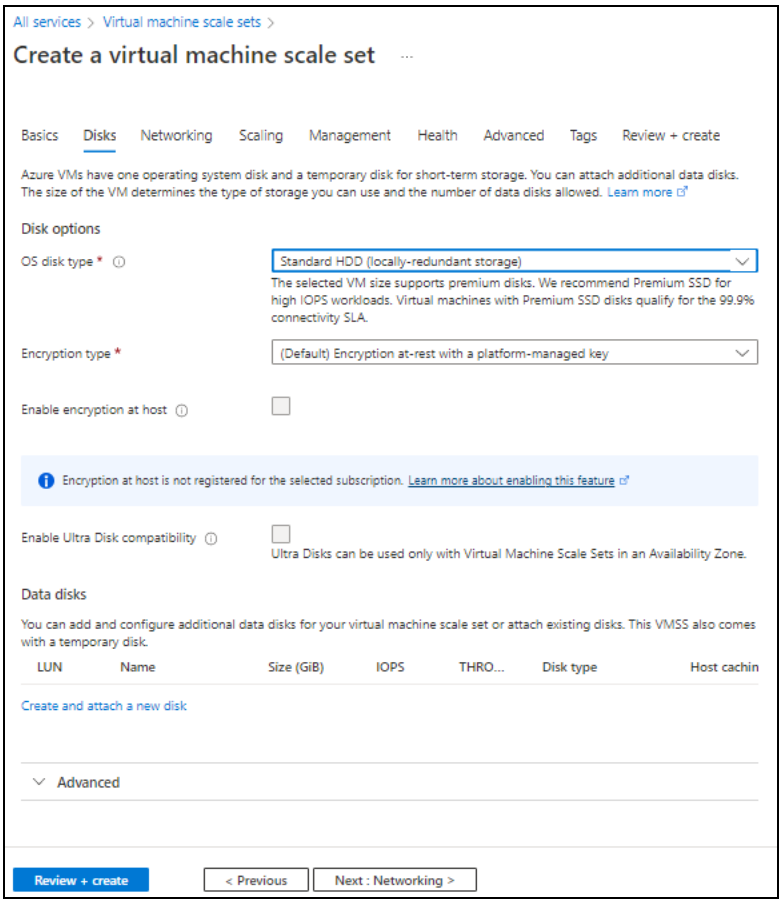
3. Leave the remaining fields as is and click **Next : Disks** at the bottom of the window.

4. Select or enter the following mandatory information in the **Disks** tab:

   Disk options

   - OS disk type
   - Encryption type

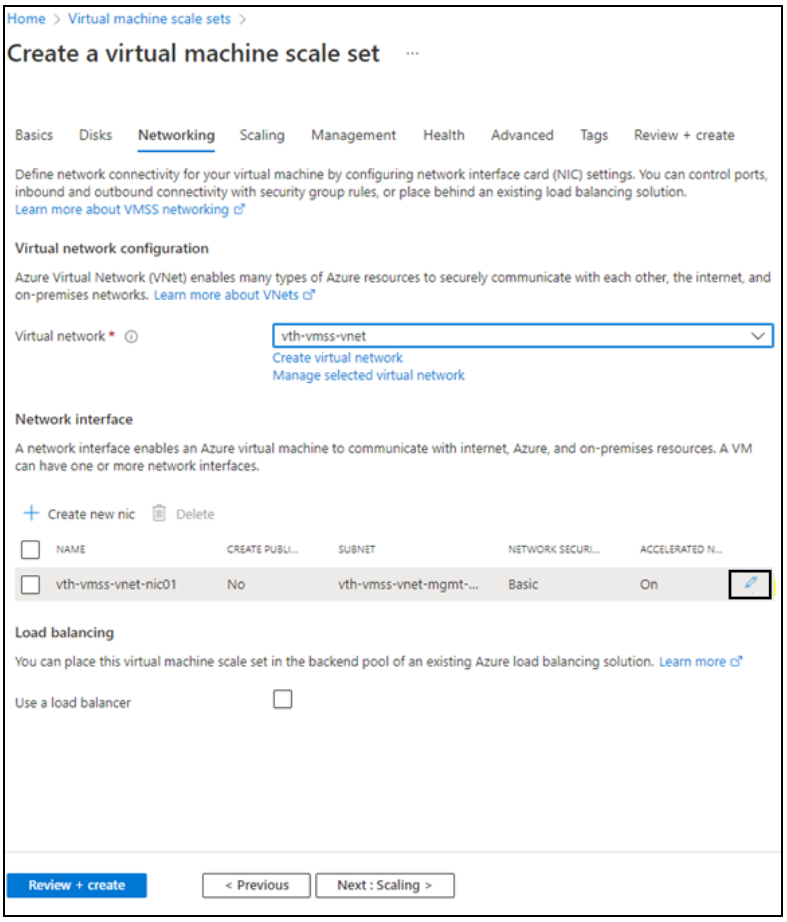
   Figure 91 : Create a virtual machine scale set window - Disks tab



5. Leave the remaining fields as is and click **Next : Networking** at the bottom of the window.

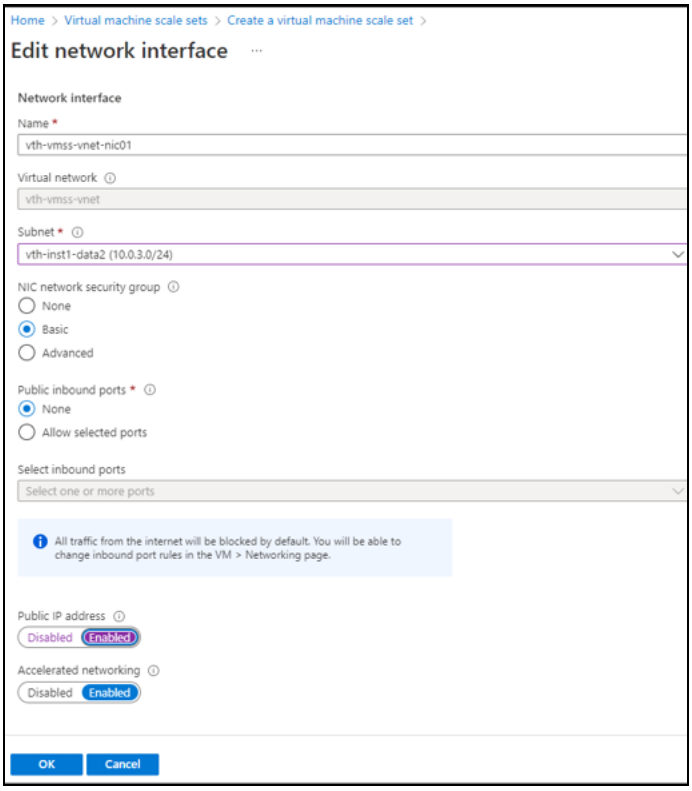
6. Select the Virtual network in the **Networking** tab.

Figure 92 : Create a virtual machine scale set window - Networking tab



7. If Data subnet 2 (Ethernet 2) value is not assigned to management NIC 1, click the edit button corresponding to it.
   The **Edit Network Interface** window appears.
8. Select Data subnet 2 value in the **Subnet** field and then click **OK**. Here, the Subnet 3 value is `10.0.3.0/24`.

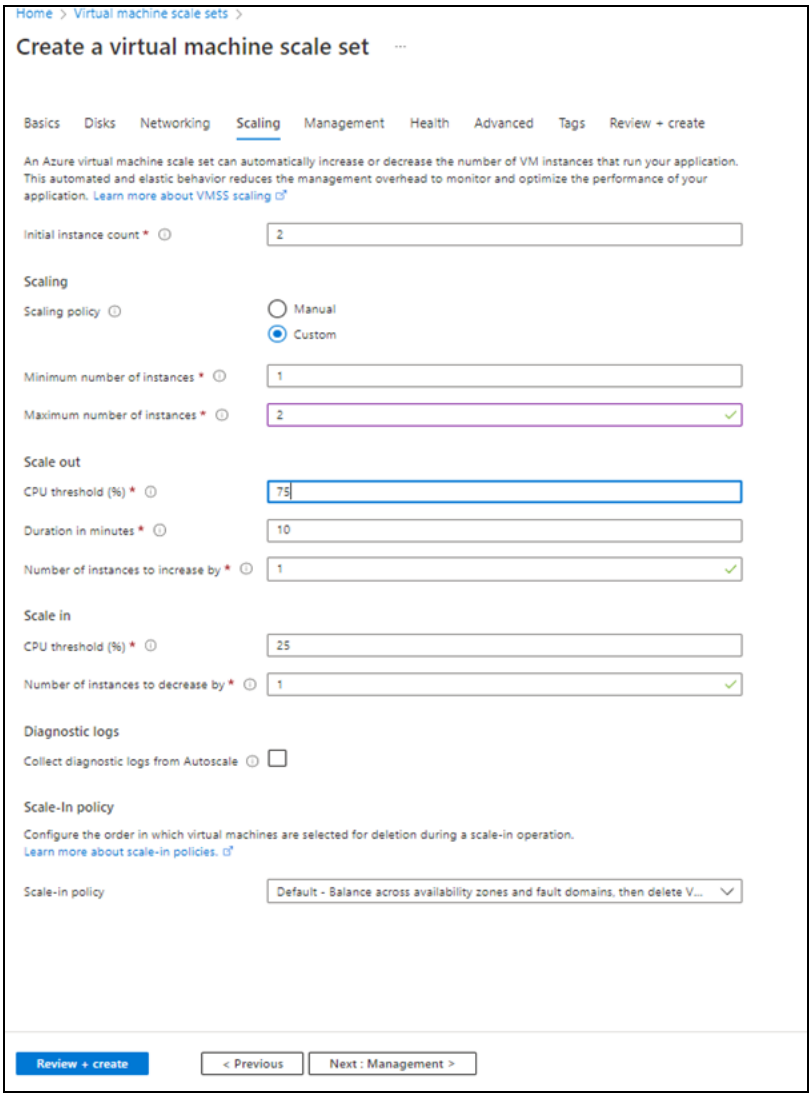
Figure 93 : Edit network interface window



9. Leave the remaining fields as is in the **Networking** tab and click **Next : Scaling** at the bottom of the window.

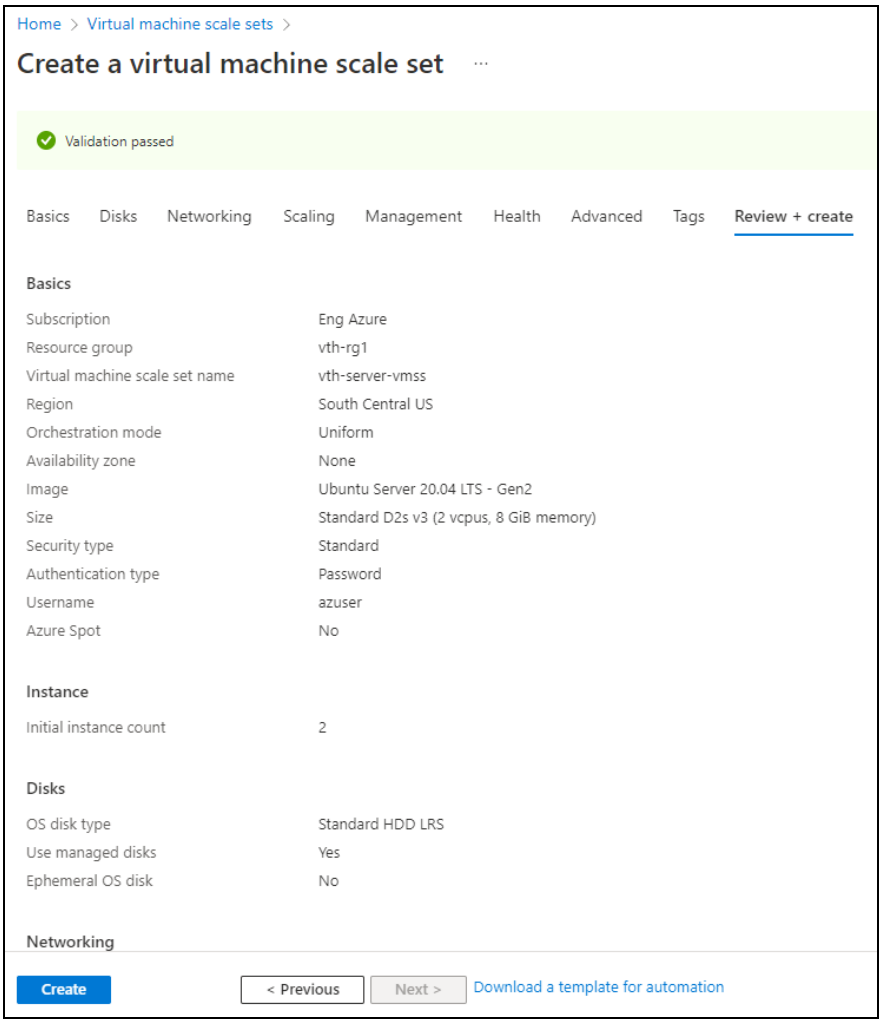
10. Select or enter the information in the **Scaling** tab as shown below.

Figure 94 : Create a virtual machine scale set window - Scaling tab



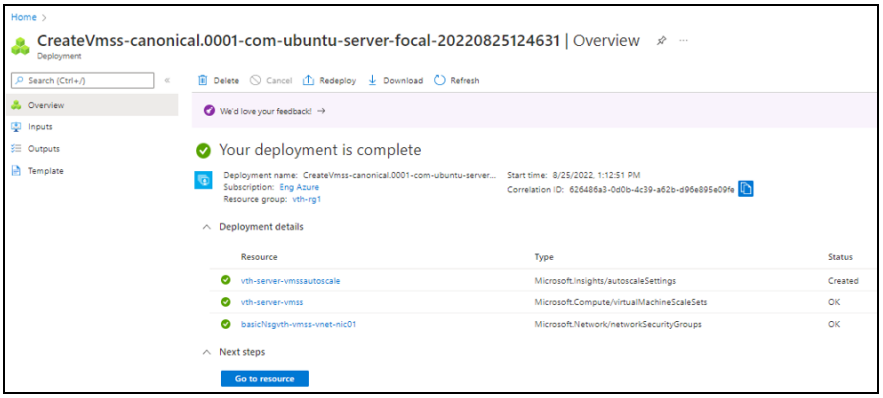
11. Click **Review + create** at the bottom of the window to skip the other tabs.

Figure 95 : Create a virtual machine scale set window - Review + create tab



12. Click **Create** at the bottom of the window.
When the VMSS is created, a message "Your deployment is complete" is displayed in the Create VMSS window.

Figure 96 : Create VMSS window



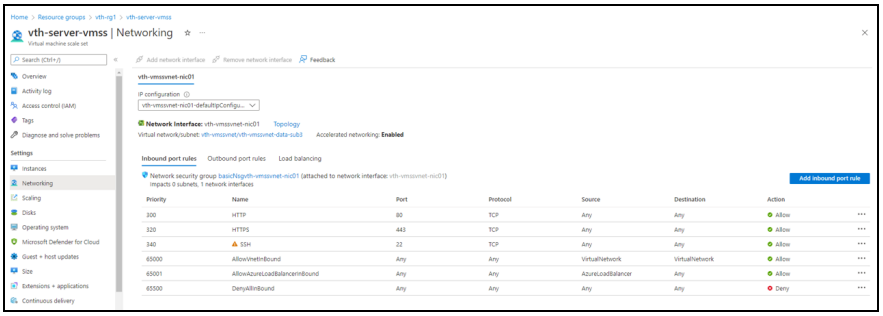
NOTE: It may take the system several minutes to display your resources.

Verify the Server VMSS Creation

To verify the creation of server VMSS, perform the following steps:

1. In the Create VMSS > **Deployment details** section, click the server VMSS resource. Here, the VMSS resource is **`vth-server-vmss`**.
   The VMSS resource details window is displayed.
2. Select **Networking** from the left **Settings** panel.
   VMSS has only one interface. The ports 80 and 443 are available in the **Inbound port rules** tab.

   Figure 97 : VMSS > Inbound port rules



3. SSH the Server virtual machine and run the following command to install Apache:

```
sudo apt install apache2
```

While the Apache server is getting installed, you get a prompt to continue further. Enter 'Y' to continue. After the installation is complete, a newline prompt is displayed.

Configure Client Machine

The following topics are covered:

- Create a Client Machine

Create a Client Machine

To create a Client machine, perform the following steps:

1. From Home, navigate to **Azure Services** > **Create a resource** > **Virtual machine** and click **Create**.
   The **Create a virtual machine** window is displayed.
2. Select or enter the following mandatory information in the **Basics** tab:

   Project details

   - Subscription
   - Resource group

   Instance details

   - Virtual machine name - Client machine
   - Region
   - Image
   - Size

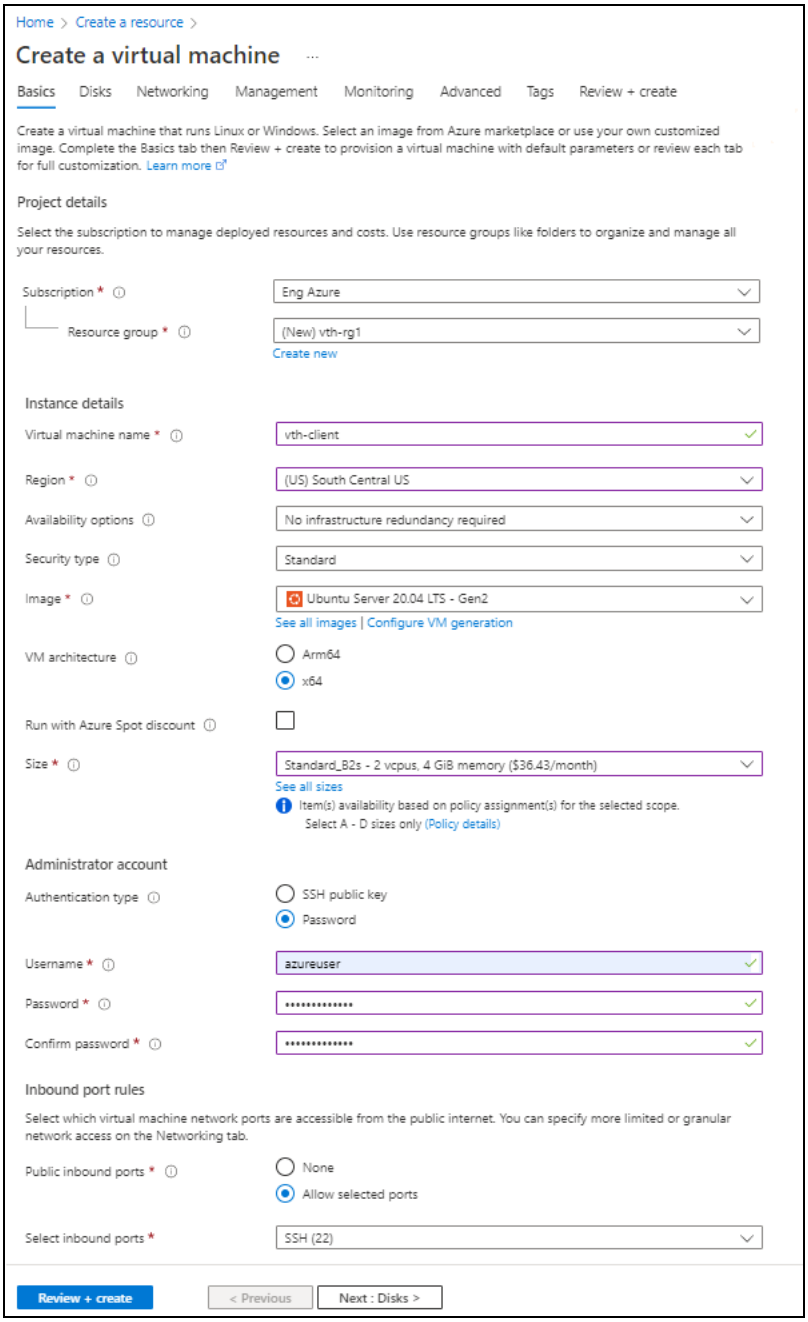
   Administrator account

   - Depending upon the Authentication type, provide the information.

   Inbound port rules

- Public inbound ports
- Select inbound ports

Figure 98 : Create a virtual machine window - Basics tab

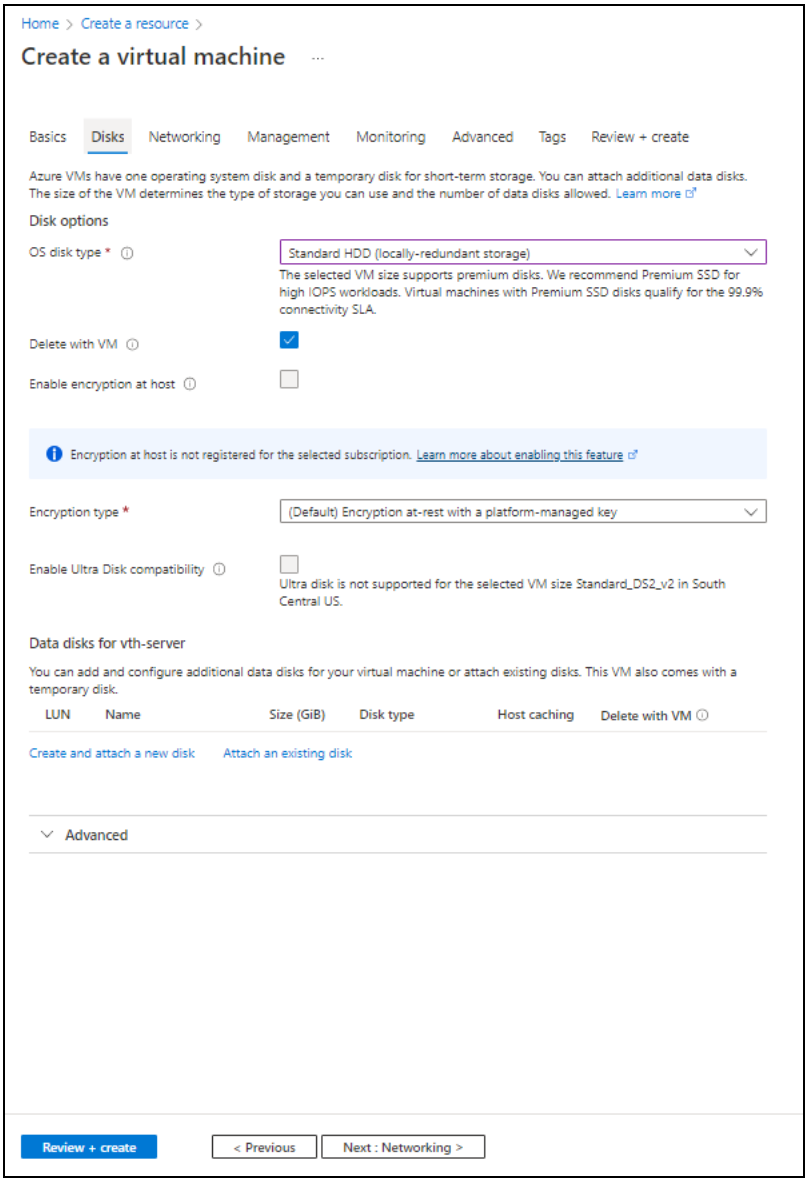


3. Leave the remaining fields as is and click **Next : Disks** at the bottom of the window.
4. Select or enter the following mandatory information in the **Disks** tab:

   Disk options

   - OS disk type
   - Encryption type

Figure 99 : Create a virtual machine window - Disks tab

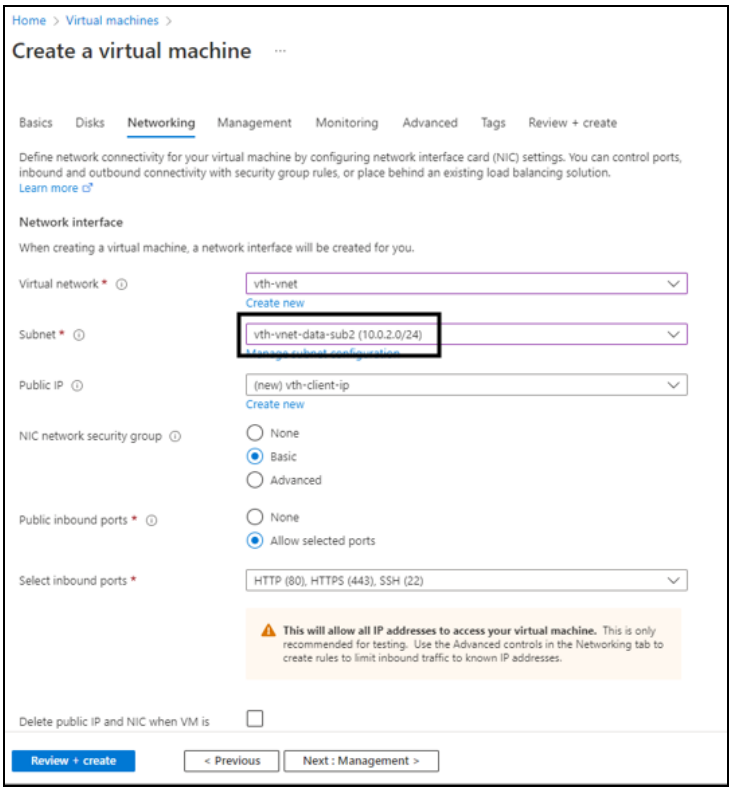


5. Leave the remaining fields as is and click **Next : Networking** at the bottom of the window.
6. Select or enter the following mandatory information in the **Networking** tab:

   Network interface

   - Virtual network
   - Subnet: Data subnet 1 (Ethernet 1)
   - Select inbound ports

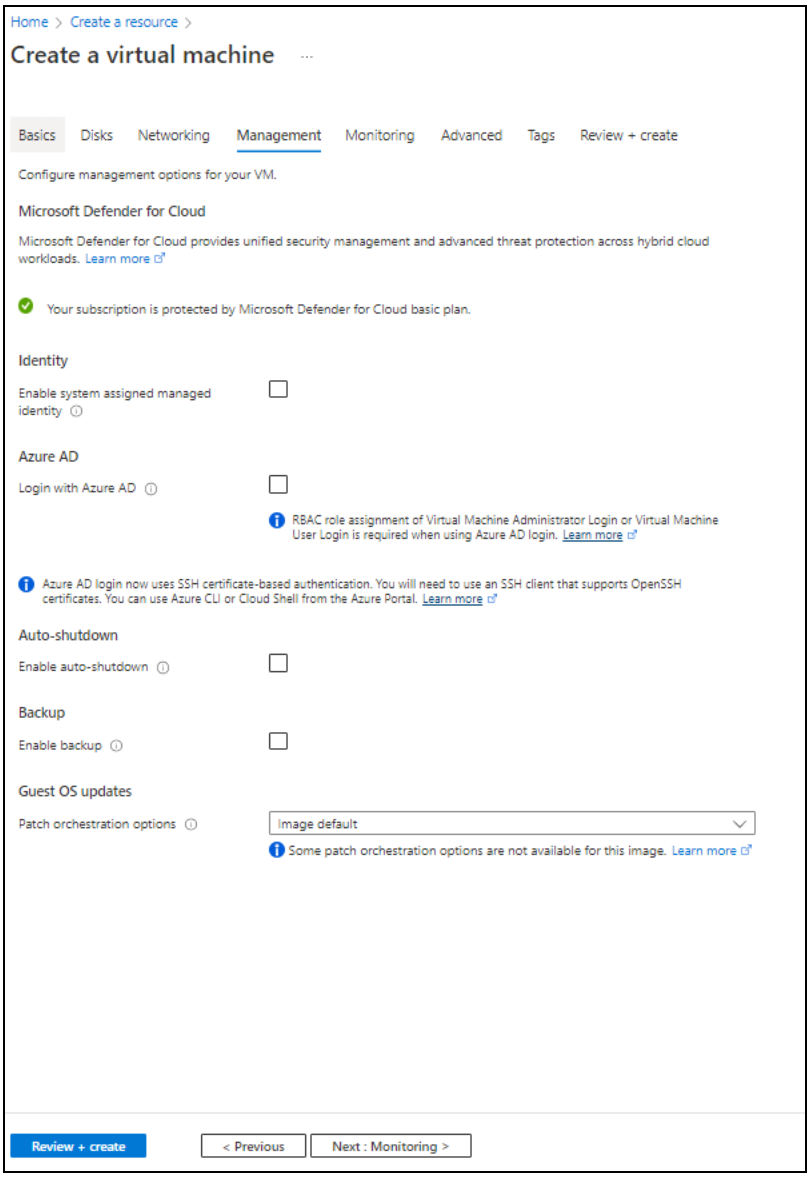
   Figure 100 : Create a virtual machine window - Networking tab



7. Leave the remaining fields as is and click **Next : Management** at the bottom of the window.

8. Select or enter the information in the **Management** tab as needed.

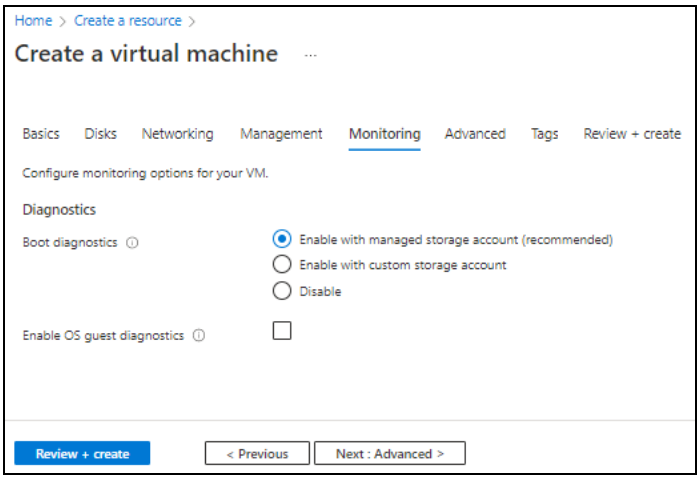
Figure 101 : Create a virtual machine window - Management tab



9. Click **Next : Monitoring** at the bottom of the window.

10. Select or enter the information in the **Monitoring** tab as needed.

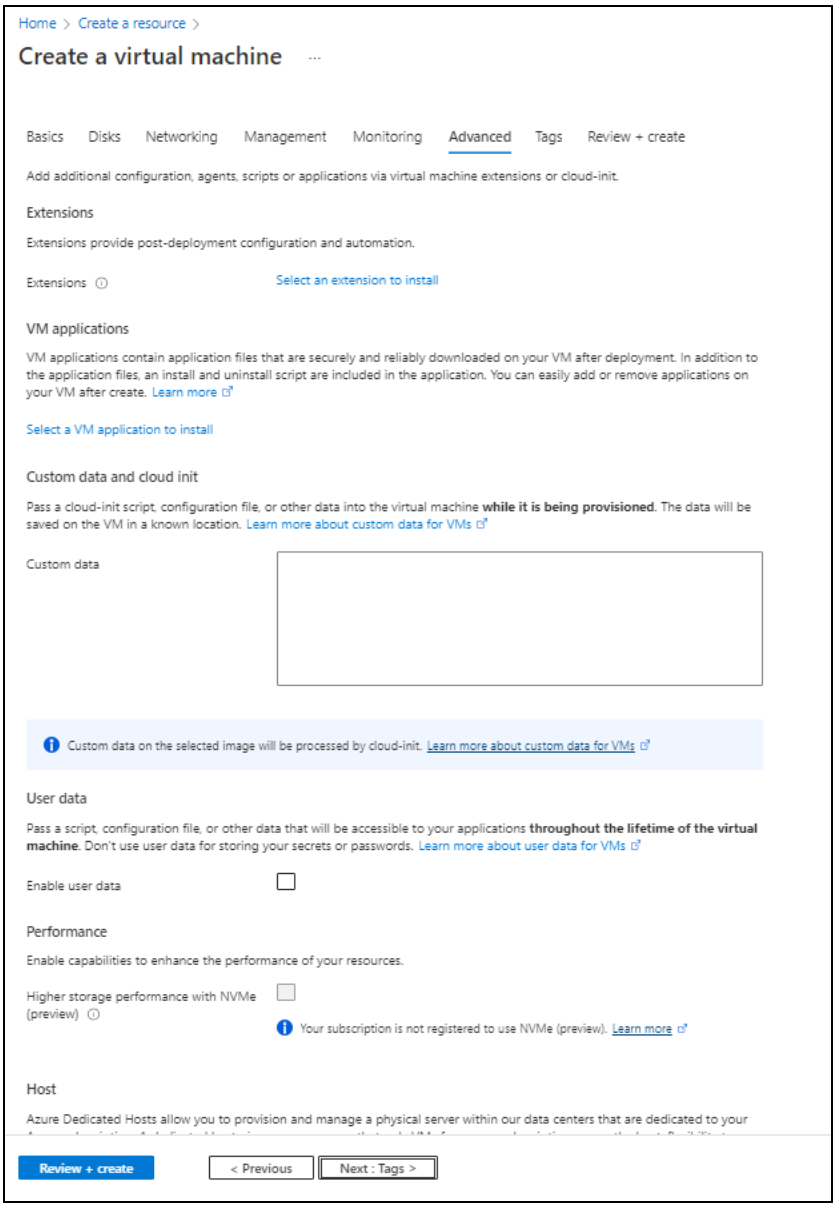
Figure 102 : Create a virtual machine window - Monitoring tab



11. Click **Next : Advanced** at the bottom of the window.

12. Select or enter the information in the **Advanced** tab as needed.

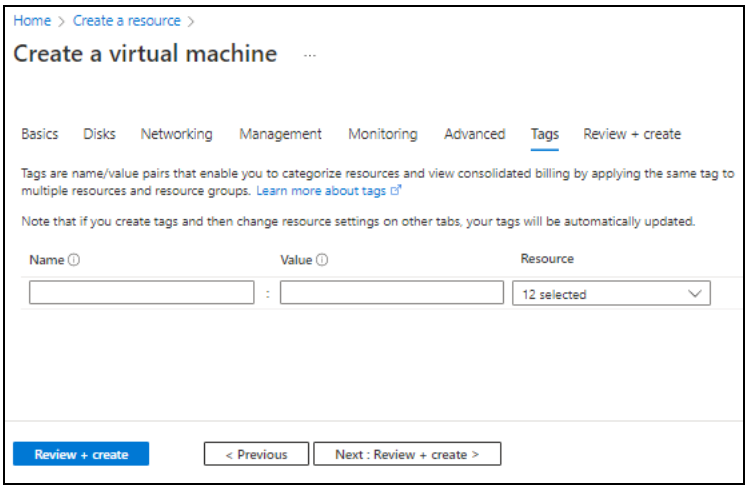
Figure 103 : Create a virtual machine window - Advanced tab



13. Click **Next : Tags** at the bottom of the window.

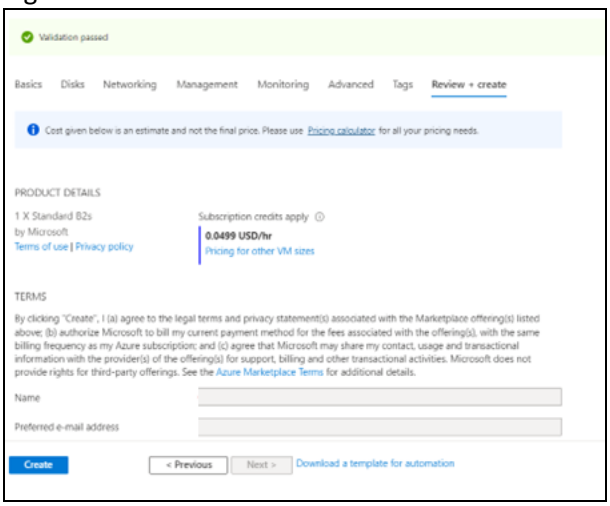
14. Select or enter the information in the **Tags** tab as needed.

Figure 104 : Create a virtual machine window - Tags tab



15. Click **Next : Review + create** at the bottom of the window.
The fields **Name** and **Preferred e-mail address** are auto-populated as per the Azure account.

Figure 105 : Create a virtual machine window - Review + create tab



16. Click **Create** at the bottom of the window.
The Client machine gets created.

Configure Automation Account

The following topics are covered:

- Configure Azure Access Key
- Create Automation Account
- Create Runbook
- Create Automation Account Webhook

Create Automation Account

The following topics are covered:

- Initial Setup
- Create an Automation Account
- Verify the Automation Account creation
- Change Password

Initial Setup

Before creating an automation account, configure the corresponding parameters in the PowerShell template.

To configure the parameters, perform the following steps:

1. Open the PS_TMPL_3NIC_2VM_AUTOMATION_ACCOUNT_PARAM.json with a text editor.
2. Configure Automation Account.
   If the automation account does not exist, then a new automation account gets created inside resource group. If automation account already exists, then template gets auto-updated.

   If the automation account variable does not exist, then a new automation account variable gets created inside the automation account. If an automation account variable already exists, an error "The variable already exists" is prompted.

   ```
   "automationAccountName": "vth-amt-acc",
   ```

3. Configure location.

   ```
   "location": "South Central US",
   ```

4. Provide the client secret ID, application ID, and tenant ID from **Home** > **Azure Services** > **Azure Active Directory** > **App Registration** > **Owned applications** > <application_name>.

```
"clientSecret": "<service-app-client-secret>",
"appId": "<service-app-client-id>",
"tenantId": "<service-app-tenant-id>",
```

5. Configure VMSS.

```
"vmssName": "vth-server-vmss",
```

6. Configure network interface cards.

```
"mgmtInterface1": "vth-inst1-mgmt-nic1",
"mgmtInterface2": "vth-inst2-mgmt-nic1",
```

7. Configure resource group name. It is the resource group where virtual machine scale set having vThunder servers and resources created by the PowerShell template are available.

```
"resourceGroupName": "vth-rg1",
```

8. Provide the vThunder instance username.

```
 "vThUsername": "admin",
```

NOTE: Do not change the vThunder instance username.

9. Configure ports.

```
"portList":{
  "value": [
    {
      "port-number": 53,
      "protocol": "udp",
      "health-check-disable":1
    },
    {
    "port-number": 80,
    "protocol": "tcp",
    "health-check-disable":1
    },
```

```
        {
        "port-number": 443,
        "protocol": "tcp",
        "health-check-disable":1
        }
    ]
}
```

10. Verify if all the configurations in the PS_TMPL_3NIC_2VM_AUTOMATION_ACCOUNT_PARAM.json file are correct and then save the changes.

Create an Automation Account

To create an automation account, run the following command:

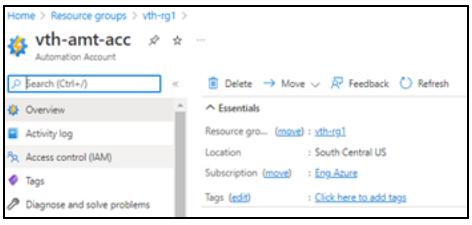
```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_AUTOMATION_ACCOUNT_
2.ps1
```

Verify the Automation Account creation

To verify the creation of an automation account, perform the following steps:

1. From **Home**, navigate to **Azure Services** > **Resource Group** > <resource_group_name>.
   The selected resource group - Overview window is displayed.
2. Under **Resources** tab, group the resources based on the resource type.
3. Verify if the recently created automation account is listed under **Automation Accounts** type.
4. Select the recently created automation account.
   The selected automation account - Overview window is displayed.

   Figure 106 : Selected automation account - Overview window



5. Click **Variables** from the left **Shared Resources** panel.
   The selected automation account - Variables window is displayed.

Figure 107 : Selected automation account - Variables window

6. Verify if all the variables associated with the automation account are listed.

Change Password

To change the vThunder instance password for the first-time, perform the following steps:

1. Run the following command to change password:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_HA_GLM_CHANGE_
PASSWORD_3.ps1
```

NOTE: It is highly recommended to change the default password provided by the A10 Networks Support when you log in the vThunder instance for the first time.

2. Provide the default and new password when prompted:

```
Enter Default Password:***
Enter New Password:***
Confirm New Password:***
```

The default password is provided by the A10 Networks Support. The new password should follow the Default password policy. For more information, see Default Password Policy.

Figure 108 : Updated Variables window

To change the password subsequently, perform the following steps:

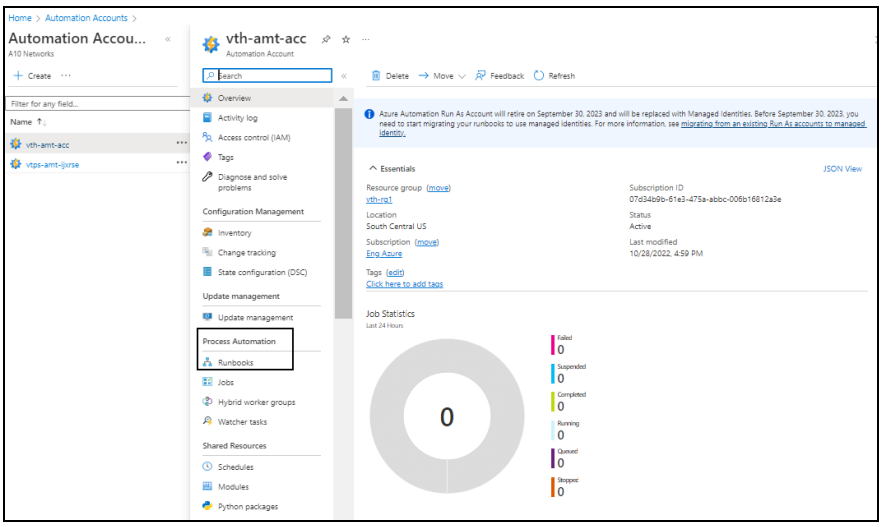
1. Change the password in vThunder instance.
2. Update the same password in the **Azure Services** > **Resource Group** > <resource_group_name> > <automation_account > **Variables** > **vThPassword** variable manually.

Create Runbook

To create the SLB-Config runbook, perform the following steps:

1. From **Home**, navigate to **Azure Services** > **Automation Accounts** > <automation_account_name>.
   The selected automation account window is displayed.

   Figure 109 : Selected automation account window

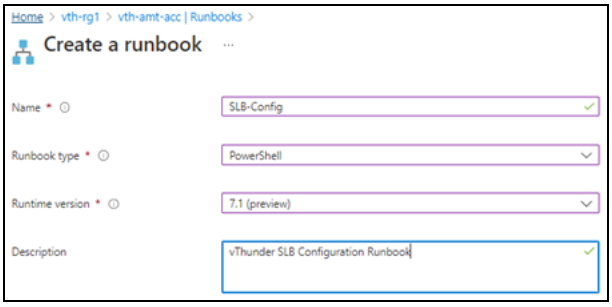


2. Select **Runbooks** from left **Process Automation** panel.
   The <automation_account_name> - Runbooks window is displayed.

Figure 110 : Selected automation account - Runbooks window

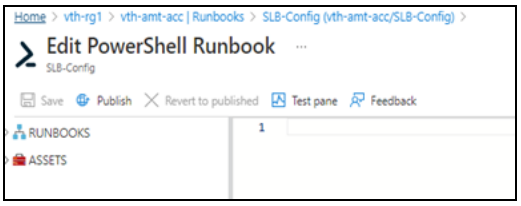
3. Click **Create a runbook**.
   The **Create a runbook** window is displayed.

   Figure 111 : Create a runbook window



4. Select or enter the following information:
   - Name: SLB-Config
   - Runbook type: PowerShell
   - Runtime version: 7.1
   - Description
5. Click **Create**.
   The **Edit PowerShell Runbook** is displayed.

   Figure 112 : Edit PowerShell Runbook window



NOTE: It may take the system a few minutes to display the edit window.

6. From the downloaded template folder, open **PS_TMPL_3NIC_2VM_SLB_SERVER_RUNBOOK.ps1** with a text editor and copy the entire content of the runbook.

7. Paste this content in the right panel of the **Edit PowerShell Runbook** window.
8. Click **Save** and then click **Publish**.
   The runbook gets created for the selected automation account.

Create Automation Account Webhook

The following topics are covered:

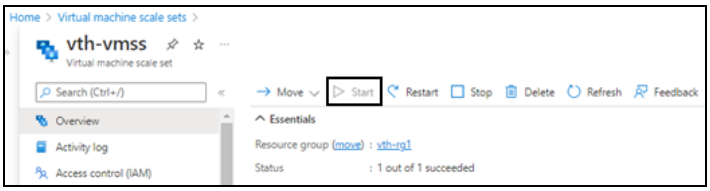
- Initial Setup
- Create a Webhook
- Verify the Runbook Job creation

Initial Setup

To verify that the virtual machine instances are running, perform the following steps:

1. From **Home**, navigate to **Azure Services** > **Resource Group** > <resource_group_ name>.
   The selected resource group - Overview window is displayed.
2. Under **Resources** tab, group the resources based on the resource type.
3. Select the virtual machine scale set instance under **Virtual machine scale set** type and verify that the instance is in **Start** mode.

   Figure 113 : VMSS window



Create a Webhook

To create a webhook, perform the following steps:

1. From Start menu, open PowerShell and navigate to the folder where you have downloaded the PowerShell template.

2. Run the following command to create the webhook:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_WEBHOOK_4.ps1 -
runBookName "<runbook_name>"
```

Example:

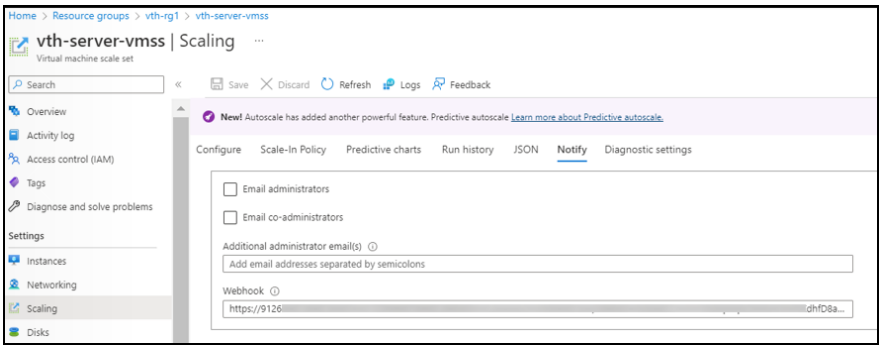
```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_WEBHOOK_4.ps1 -
runBookName "SLB-Config"
```

After the webhook installation is complete, the webhook url is displayed.

```
Save this URL :
https://fa72c8e5-xxxx-xxxx-9dc5-b4a71eec0a95.webhook.scus.azure-
automation.net/webhooks?token=Q*****pG4UEOScfqdEGEAkqJPgdK%2bOpusoUAWk
*****%3d
```

3. Save this webhook url for future purpose.
4. From **Home**, navigate to **Azure Services** > **Virtual machine scale set** > <vmss_ name>.
   The selected VMSS - Overview window is displayed. Here, the VMSS name is **`vth-server-vmss`**.
5. Click **Scaling** from the left **Settings** panel.
   The selected VMSS - Scaling window is displayed.

   Figure 114 : VMSS-Scaling - Notify tab



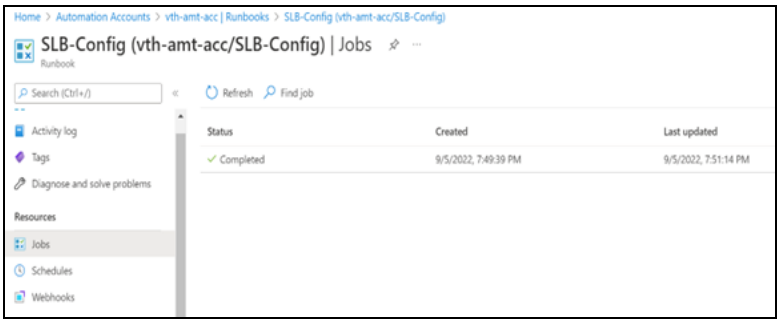
6. Select **Notify** tab.
7. Copy the saved webhook url and paste it in the **Webhook** field.
8. Click **Save** to save the changes.

Verify the Runbook Job creation

To verify the creation of runbook job, perform the following steps:

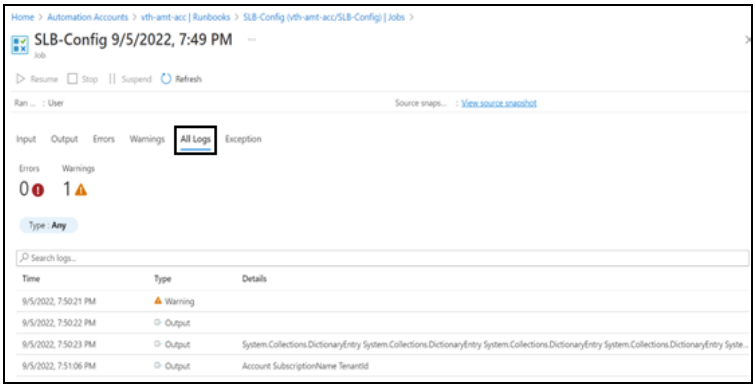
1. From **Home**, navigate to **Azure Services** > **Automation Accounts** > <automation_account_name>.
   The selected automation account - Overview window is displayed.
2. Click **Jobs** from the left **Process Automation** panel.
   The selected automation account - Jobs window is displayed. Here, the job is **`SLB-Config`**.

   Figure 115 : Selected automation account - Jobs window



3. Verify if the runbook job has completed status.
4. Select the runbook job > **All Logs** tab to verify the logs.
   The selected automation account - selected job - Jobs window is displayed.

   Figure 116 : Selected runbook job window



Configure vThunder as an SLB

The following topics are covered:

- Initial Setup
- Deploy vThunder as an SLB

Initial Setup

Before deploying vThunder on Azure cloud as an SLB, configure the corresponding parameters in the PowerShell template.

To configure the parameters, perform the following steps:

1. Open the PS_TMPL_3NIC_2VM_SLB_CONFIG_PARAM.json with a text editor.

   NOTE: Each parameter has a default value mentioned in the parameter file.

2. Configure service group list ports.

```
"serviceGroupList": {
        "value": [
            {
              "name":"sg443",
              "protocol":"tcp",
              "health-check-disable":1
            },
            {
              "name":"sg53",
              "protocol":"udp",
              "health-check-disable":1
            },
              {
              "name":"sg80",
              "protocol":"tcp",
              "health-check-disable":1
            }
          ]
      },
```

3. Configure virtual server.
   The virtual server default name is “vip”. The vip address is generated dynamically after deploying the PowerShell template. Therefore, its default value under

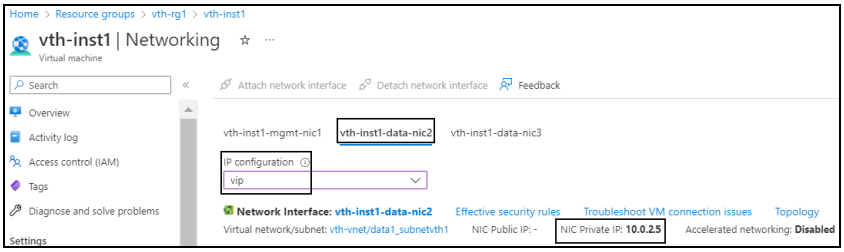
virtualServerList should be replaced. To get the vip address, perform the following steps:

a. From **Home**, navigate to **Azure Services > Resource Group >** <resource_group_name>.

b. Go to the first virtual machine instance. Here, first virtual machine instance is **vth-inst1**.

c. Select the Data NIC 2 tab > **IP configuration** > **vip**. Here, Data NIC 2 is **vth-inst1-data-nic2**.

Figure 117 : Virtual machine - Networking window - Data NIC 2 tab



d. Select **Networking** from the left **Settings** panel.

e. Select the **NIC Private IP**.

f. Replace **ip-address** value under **virtualServerList** with this **vip**.

```
        "virtualServerList": {
          "virtual-server-name": "vip",
          "ip-address": "10.0.2.5",
          "metadata": {
            "description": "virtual server is using VIP from
ethernet 1 subnet"
          },
          "value": [
            {
              "port-number":53,
              "protocol":"udp",
              "ha-conn-mirror":1,
              "auto":1,
              "service-group":"sg53"
            },
            {
```

```
            "port-number":80,
            "protocol":"http",
            "auto":1,
            "service-group":"sg80"
          },
          {
            "port-number":443,
            "protocol":"https",
            "auto":1,
            "service-group":"sg443"
          }
        ]
    },
```

NOTE: **`ha-conn-mirror`** does not work on port 80 and 443.

4. Configure SSL.

```
    "sslConfig": {
        "requestTimeOut": 40,
        "Path": "<absolute path of the ssl certificate file>",
        "File": "<certificate-name>",
        "CertificationType": "pem"
      }
```

NOTE: By default, SSL configuration is disabled i.e. no SSL configuration is applied.

Example The sample values for the SSL certificate are as shown below:

```
    "sslConfig": {
        "requestTimeOut": 40,
        "Path": "C://Users//..//..//..//server.pem” or
"C:\Users\..\..\..\certs\server.pem",
        "File": "server",
        "CertificationType": "pem"
                    }
```

5. Verify if the vip address and all other configurations in the PS_TMPL_3NIC_2VM_SLB_CONFIG_PARAM.json file are correct and then save the changes.

Deploy vThunder as an SLB

To deploy vThunder on Azure cloud as an SLB, perform the following steps:

1. From PowerShell, navigate to the folder where you have downloaded the PowerShell template.
2. Run the following command to deploy vThunder as an SLB instance using the same resource group:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_SLB_CONFIG_5.ps1 -
resourceGroup <resource_group_name>
```

Example:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_SLB_CONFIG_5.ps1 -
resourceGroup vth-rg1
```

A message is prompted to upload the SSL certificate.

```
SSL Certificate
Do you want to upload ssl certificate ?
[Y] Yes  [No] No [?] Help (default is "N"): Y
SLB Server Host IP: 10.0.3.7
Virtual Server Name: vip
Resource Group Name: vth-rg1
vThunder1 Public IP: 13.85.81.137
vThunder2 Public IP: 13.85.81.113
Configuring vm: vth-inst1
configured ethernet- 1 ip
configured ethernet- 2 ip
Configured server
Configured service group
0
Configured virtual server
SSL Configured.
Configurations are saved on partition: shared
Configured vThunder Instance 1
Configuring vm: vth-inst2
configured ethernet- 1 ip
configured ethernet- 2 ip
```

```
Configured server
Configured service group
0
Configured virtual server
SSL Configured.
Configurations are saved on partition: shared
Configured vThunder Instance 2
```

3. If the SSL Certificate upload is successful, a message 'SSL Configured' is displayed.

Configure High Availability for vThunder

The following topics are covered:

- Initial Setup
- Create High Availability for vThunder

Initial Setup

Before configuring high availability for vThunder, configure the corresponding parameters in the PowerShell template.

To configure the parameters, perform the following steps:

1. Navigate to the folder where you have downloaded the PowerShell template and open the PS_TMPL_3NIC_2VM_HA_CONFIG_PARAM.json with a text editor.
2. Configure DNS.

```
        "dns": {
            "value": "8.8.8.8"
        },
```

3. Configure a Network Gateway IP.
   The default value of network gateway IP address is the first IP address of data subnet 1 configuration.

```
        "rib-list": [
            {
            "ip-dest-addr":"0.0.0.0",
            "ip-mask":"/0",
```

```
            "ip-nexthop-ipv4": [
                {
                "ip-next-hop":"10.0.2.1"
                }
            ]
            }
        ],
```

4. Set a VRRP-A.

```
        "vrrp-a": {
            "set-id":1
        },
```

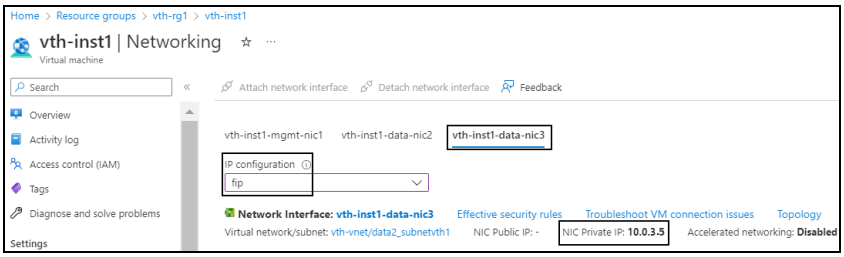
5. Set a Terminal Idle Timeout.

```
        "terminal": {
            "idle-timeout":0
        },
```

6. Configure VRID details.
   The default value of vrid is 0. The default priority for vThunder-1 is 100, and for vThunder-2 is 99 (100-1). The floating ip (fip) address value is generated dynamically after deploying the PowerShell template. Therefore, its default value under **`vrid-list`** should be replaced. To get the fip address, perform the following steps:
   a. From **Home**, navigate to **Azure Services** > **Resource Group** > <resource_group_name>.
   b. Go to the first virtual machine instance. Here, first virtual machine instance is **`vth-inst1`**.
   c. Select **Networking** from the left **Settings** panel.

d. Select the Data NIC 3 tab > **IP configuration**. Here, **`vth-inst1-data-nic3`**.

Figure 118 : Virtual machine - Networking tab - Data NIC 3 tab



e. Select the **NIC Private IP**.

f. Replace the **`ip-address`** value under **`vrid-list`** with this **`fip`**.

```
"vrid-list": [
            {
            "vrid-val":0,
            "blade-parameters": {
                "priority": 100
            },
            "floating-ip": {
                "ip-address-cfg": [
                    {
                      "ip-address":"10.0.3.5"
                    }
                  ]
                }
            }
        ]
```

7. Verify if all the configurations in the PS_TMPL_3NIC_2VM_HA_CONFIG_ PARAM.json file are correct and then save the changes.

Create High Availability for vThunder

To create High Availability for vThunder, perform the following steps:

1. Import Azure access key on both the vThunder instances. For more information, refer Import Azure Access Key.

2. Run the following command to configure both vThunder instances in HA mode.

```
S C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_HA_CONFIG_6.ps1 -
resourceGroup <resource_group_name>
```

Example:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_HA_CONFIG_6.ps1 -
resourceGroup vth-rg1
```

Configure vThunder using GLM

The following topics are covered:

- Initial Setup
- Apply GLM License

Initial Setup

Before configuring vThunder with GLM, configure the corresponding parameters in the PowerShell template.

To configure the parameters, perform the following steps:

1. From the downloaded PowerShell template folder, open the PS_TMPL_3NIC_2VM_GLM_CONFIG_PARAM.json with a text editor.
2. Configure GLM account details.

```
{
  "parameters": {
    "user_name": {
      "value": "user_name"
    },
    "user_password": {
      "value": "user_password"
    },
    "entitlement_token": {
      "value": "token"
    }
```

```
  }
}
```

3. Verify if the configurations in the PS_TMPL_3NIC_2VM_GLM_CONFIG_PARAM.json file are correct and then save the changes.

Apply GLM License

To apply GLM License, perform the following steps:

1. From PowerShell, navigate to the folder where you have downloaded the PowerShell template.
2. Run the following command to apply SLB on vThunder:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_GLM_CONFIG_7.ps1 -
resourceGroupName <resource_group_name>
```

Example:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_GLM_CONFIG_7.ps1 -
resourceGroup vth-rg1
```

3. If the GLM License is applied successfully, a message is displayed.

```
ConfigureGlm
{
  "response": {
       "status": "OK",
       "msg": "BASE License successfully updated, please log out and log back
in to access license featurebA1070459ec380000\n"
  }
}
GlmRequestSend
Configurations are saved on partition: shared
WriteMemory
```

Access vThunder using CLI or GUI

vThunder can be accessed using any of the following ways:

- Access vThunder using CLI
- Access vThunder using GUI

Access vThunder using CLI

To access the two vThunder instances using CLI, perform the following steps:

1. Open PuTTY.
2. Enter or select the following basic information in the PuTTy Configuration window:
   - Hostname: Public IP of Virtual Machine Instance
     Here, Public IP of **vth-inst1**, **vth-inst2**
   - Connection Type: SSH
3. Click **Open**.
4. In the active PuTTY session, login with the recently changed password:

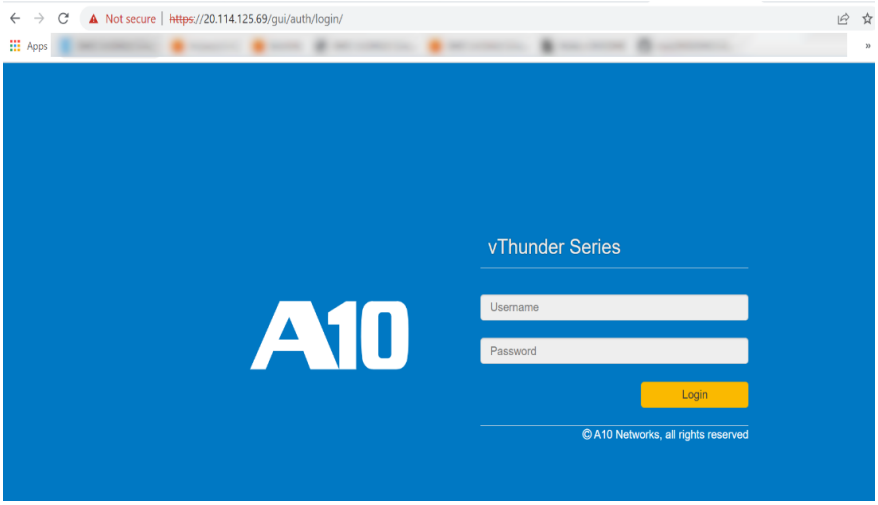
```
login as: xxxx <---Enter username provided by A10 Networks Support--->
Using keyboard-interactive authentication.
Password: xxxx <---Enter password provided by A10 Networks Support-->
Last login: Day MM DD HH:MM:SS from a.b.c.d

System is ready now.

[type ? for help]

vThunder> enable <---Execute command--->
Password:<---just press Enter key--->
vThunder#config <---Configuration mode--->
```

Access vThunder using GUI

To access the two vThunder instances using GUI, perform the following steps:

1. Open any browser.
2. Enter *https://<vthunder_public_IP>/gui/auth/login/* in the address bar.

   Figure 119 : vThunder GUI



3. Enter the recently configured user credentials.
   The home page gets displayed.

Verify Deployment

To verify deployment using the PowerShell template, perform the following steps:

1. Run the following command on vThunder:

```
vThunder-Active(config)#show running-config slb
```

   If the deployment is successful, the following SLB configuration is displayed:

```
slb service-group sg443 tcp
  health-check-disable
!
slb service-group sg53 udp
  health-check-disable
!
slb service-group sg80 tcp
  health-check-disable
!
```

```
slb virtual-server vip 10.0.2.5
  port 53 udp
    ha-conn-mirror
    source-nat auto
    service-group sg53
  port 80 http
    source-nat auto
    service-group sg80
  port 443 https
    source-nat auto
    service-group sg443
!
```

2. Run the following command to verify HA:

```
vThunder-Active(config)#show running-config
```

If the deployment is successful, the following configuration is displayed:

```
!Current configuration: 536 bytes
!Configuration last updated at 17:36:35 IST Mon Sep 5 14 2022
!Configuration last saved at 17:35:40 IST Wed Sep 5 14 2022
!64-bit Advanced Core OS (ACOS) version 5.2.0, build 155 (Aug-10-
2020,14:34)

!
vrrp-a common
  device-id 1
  set-id 1
  enable
!
multi-config enable
!
terminal idle-timeout 0
!
ip dns primary 8.8.8.8
!
!
glm use-mgmt-port
```

```
glm enable-requests
glm token vTh11e089e10
!
interface management
  ip address dhcp
!
interface ethernet 1
  enable
  ip address dhcp
!
interface ethernet 2
  enable
  ip address dhcp
!
vrrp-a vrid 0
  floating-ip 10.0.3.5
  floating-ip 10.0.2.5
  blade-parameters
       priority 100
!
vrrp-a peer-group
  peer 10.0.2.4
  peer 10.0.2.6
!
ip route 0.0.0.0 /0 10.0.2.1
!
```

3. Run the following command to verify the SSL Certificate configuration:

```
vThunder-Active(config)#show pki cert
```

If the deployment is successful, the following SSL configuration is displayed:

```
Name    Type                        Expiration  Status
-----------------------------------------------------------------
server certificate Jan 28 12:00:00 2028 GMT [Unexpired, Bound]
```

4. Run the following command to force stop the active vThunder and make standby vThunder as active device:

```
vThunder-Active(config)#vrrp-a force-self-standby enable
```

```
vThunder-ForcedStandby(config)#
```

5. Run the following command to disable the active standby vThunder:

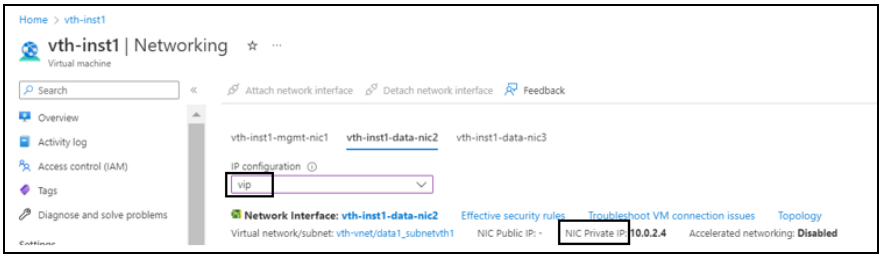
```
vThunder-ForcedStandby(config)#vrrp-a force-self-standby disable
vThunder-Active(config)#
```

Verify Traffic Flow

To verify the traffic flow from client machine to server machine via vThunder, perform the following:

1. From **Azure Portal** > **Azure Services** > **Resource Group** > <resource_group_name> > <active_virtual_machine_instance> > **Settings** > **Networking**.
   Here, **`vth-inst1`** is the active vThunder instance name.
2. Copy the VIP address of the active vThunder instance.

   Figure 120 : Active vThunder instance 1 VIP



3. Select your client instance from the **Virtual machine** list.
   Here, **`vth-client`** is the client instance name.
4. SSH your client machine and run the following command to verify the traffic flow:

```
curl <VIP>
```

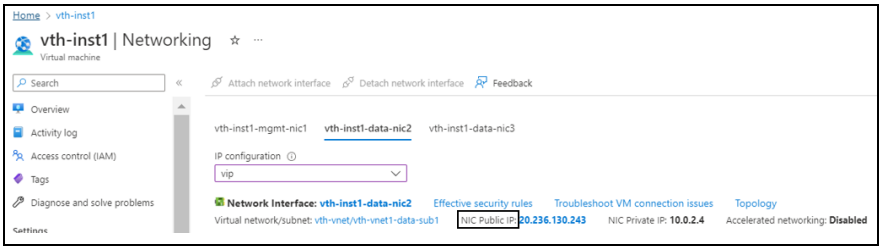
   Example

```
curl 10.0.2.4
```

   Verify if a response is received.

5. Copy the Public IP address of the active vThunder instance 1 data subnet 1.

Figure 121 : Active vThunder instance 1 Public IP address



6. Run the following command from the client machine to verify the traffic flow:

```
curl <public_ip_of_data_nic2>
```

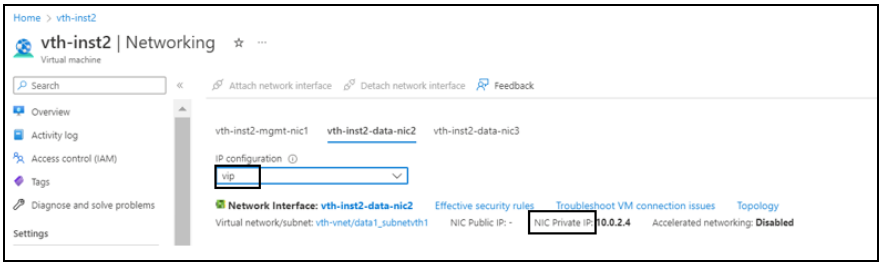
Example

```
curl 20.236.130.243
```

Verify if a response is received.

7. After the switchover, vThunder instance 2 is active, so copy the VIP address of the vThunder instance 2.

Figure 122 : Active vThunder instance 2 VIP



8. SSH your client machine and run the following command to verify the traffic flow:

```
curl <VIP>
```

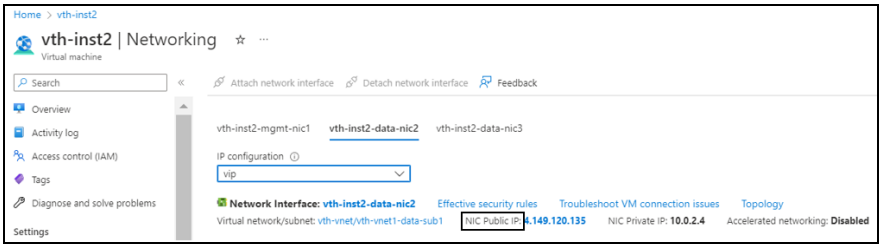
Example

```
curl 10.0.2.4
```

Verify if a response is received.

9. Copy the Public IP address of the active vThunder instance 2 data subnet 1.

Figure 123 : Active vThunder instance 2 Public IP address



1. Run the following command from the client machine to verify the traffic flow:

```
curl <public_ip_of_data_nic2>
```

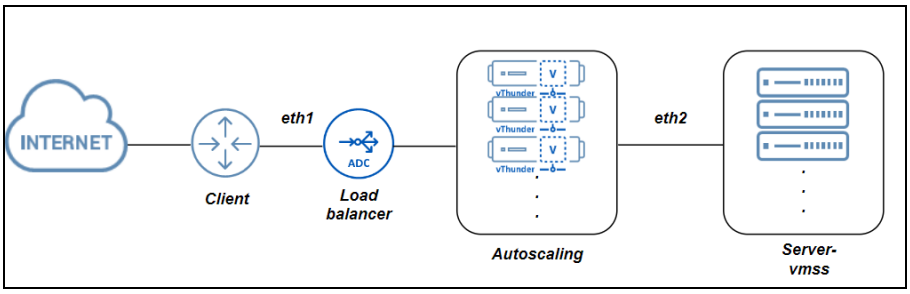
Verify if a response is received.

Deploy PowerShell A10-vThunder_ADC-3NIC-VMSS

Figure 124 shows the 3NIC-NVM-VMSS deployment topology. Using this template, multiple vThunder instances in a Virtual Machine scale set using CPU Matrix-based autoscaling can be deployed containing:

- One management interface and two data interfaces each
- GLM integration
- SSL Certificate support
- Server Load Balancer
- Log Analysis using Azure Log Analytics integration
- Azure Application Insight integration

Figure 124 : 3NIC-NVM-VMSS Topology



The following topics are covered:

System Requirements 231
Create vThunder Instances 236
Configure Server VMSS 244
Configure Automation Account 253
Enable Autoscaling 267
On-demand Password Change 298
Access vThunder using CLI or GUI 300
Verify Deployment 301

Verify Traffic Flow 304

System Requirements

The PowerShell template will display the default values when you download and save the files on your local machine. You can modify the default values as required for your deployment.

You need the following resources to deploy vThunder on the Azure cloud:

Table 12 : System Requirements

Resource Name	Description	Default Value
Azure Resource Group	A resource group with the specified name and location is created if it doesn't exist. All the resources required for this template is created under the resource group.	Here, the Azure resource group name used is **`vth-rg1`**.
Azure Storage Account	A storage account is created inside the resource group, if it doesn't exist. If the storage name already exists, the following error is displayed “The storge account named vthunderstorage already exists under the subscription". **Performance**: Standard **Replication**: Read-access geo-redundant storage (RA-GRS) **Account kind**: Storagev2 (general purpose v2)	Azure Storage Account: **`vthunderstorage`** SSL Container: **`ssl`** Log Agent Container: **`vth-agent-cont`**
Virtual Machine	Two virtual machine instances are created, vThunder and	A10 vThunder instance: **`vth-vmss_0`**

Resource Name	Description	Default Value
(VM) Instance	monitoring agent. **Product**: A10 vThunder **Operating system**: Linux **Default Size**: Standard_B4ms (4 vCPUs, 16 GiB Memory) **Product**: A10 Monitoring Agent **Operating system**: Linux **Default Size**: Standard DS2_V2 (2 vCPUs, 7 GiB Memory) **NOTE:** Before selecting any VM size, it is highly recommended to do an assessment of your projected traffic. Table 13 lists the supported VM sizes.	A10 Monitoring Agent: `vth-agent-ins1`
Azure Automation Account	An automation account is created under the resource group.	`vth-amt-acc`
Azure Runbook with Webhook	Multiple custom runbooks are created under the automation account: • Change-Password-Config	

Resource Name	Description	Default Value
	• Event-Config • GLM-Config • GLM-Revoke-Config • Master-Runbook • SLB-Config • SSL-Config A webhook is created under the Master-Runbook.	
Azure Log Analytics Workspace	A log analytics workspace is created. A custom agent, fluentbit, sends all logs to log analytics.	`vth-vmss-log-workspace`
Azure Application Insights	The custom metrics are created. Depending upon the configured threshold values, it is considered for autoscaling.	Default application insight name: `vth-vmss-app-insights` Default custom metrics name: `vth-cpu-metrics` Default threshold for autoscale-in is **25**%. Default threshold for autoscale-out is **80**%.
Azure Load Balancer [LB]	A load balancer with an interface is created under the automation account if it does not exist. The creation of LB is optional, and it can be skipped during the execution. One backend pool is created, and it gets attached to the Network Interface Card 2 (NIC2).	Azure Load Balancer: `vth-lb1` Backend Pool: `vth-lb1-bck-pool1` Three default rules are created: • rulePort80 • rulePort443 • rulePort53

Resource Name	Description	Default Value
	Three default LB rules are created. Three default health probes are created.	Three default probes are created: • HealthProbe80 • HealthProbe443 • HealthProbe53
Virtual Machine Scale Set [VMSS]	A virtual machine scale set is created.	**vth-vmss**
Virtual Cloud Network [VCN]	A virtual network is assigned to the virtual machine instance.	**vth-vmss-vnet** Address prefix for virtual network: 10.0.0.0/16
Subnet	Three subnets are created with an address prefix each.	Subnet1: **10.0.1.0/24** Subnet2: **10.0.2.0/24** Subnet3: **10.0.3.0/24**
Public and Private IP address	Single frontend static public IP is created and attached to LB interface.	Public IP address: **vth-lb1-ip** Private IP address: **vth-lb1-frnt-ip**
Network Interface Card [NIC]	Two types of interfaces are created for each vThunder instance: • Management Interface with public IP • Data Interface with primary private IP [Ethernet 1, Ethernet	**vth-inst1-mgmt-nic1** **vth-inst1-data-nic2** **vth-inst1-data-nic3**

Resource Name	Description	Default Value
	2] **NOTE:** The secondary IP of data interface is taken from DHCP server.	
Network Security Group [NSG]	A security group is created for all the associated default interfaces.	`vth-nsg1`
Azure Service Application Access Key	An existing key can be used or a new key can be created. For more information, refer Azure Service Application Access Key.	

Supported VM Sizes

Table 13 : Supported VM sizes

Series	Size	Qualified Name
A series	Standard A4_v2 Standard A4m_v2 Standard/Basic A4 Standard A8_v2	Standard_A4_v2 Standard_A4m_v2 Standard_A4 Standard_A8_v2
B series	Standard B2s Standard B2ms Standard B4ms	Standard_B2_s Standard_B2ms Standard_B4ms
D series	Standard D3_v2 Standard DS3_v2	Standard_D3_v2 Standard_DS3_v2

Series	Size	Qualified Name
	Standard D5_v2	Standard_D5_v2
F series	Standard F4s Standard F8 Standard F16s	Standard_F4s Standard_F8 Standard_F16s

Azure is going to retire few of the above listed VM sizes soon, see Virtual Machine series | Microsoft Azure.

For more information on Windows and Linux VM sizes, see

https://docs.microsoft.com/en-us/azure/virtual-machines/sizes-general

https://docs.microsoft.com/en-us/azure/virtual-machines/linux/sizes

Create vThunder Instances

The following topics are covered:

- Initial Setup
- Deploy vThunder
- Verify Resource Creation

Initial Setup

Before deploying vThunder instances on Azure cloud, configure the corresponding parameters in the PowerShell template.

To configure the parameters, perform the following steps:

1. Navigate to the folder where you have downloaded the PowerShell template, and open the PS_TMPL_3NIC_NVM_VMSS_PARAM.json with a text editor.

NOTE: Each parameter has a default value mentioned in the parameter file.

2. Provision the vThunder instance by entering the default admin credentials as follows:

```
"adminUsername": {
  "value": "vth-user"
},
"adminPassword": {
  "value": "vth-Password"
},
```

NOTE: This is a mandatory step during VM creation. Once the device is provisioned, vThunder auto-deletes all users except the default user.

3. Configure DNS label prefix for vThunder host name.

```
"dnsLabelPrefix": {
    "value": "vth-inst1"
 },
```

4. Configure a virtual network scale set.

```
"vmssName":{
    "value":"vth-vmss"
 },
```

5. Set a VMSS size for vThunder.

```
"vmssSku":{
    "value":"Standard_B4ms"
 },
```

6. Set a VM size for Agent.

```
"vmSku":{
    "value":"Standard_B4ms"
 },
```

Use a suitable VM size that supports at least 3 NICs. For VM sizes, see System Requirements section.

7. Set an instance count.

```
"instanceCount":{
    "value":1
},
```

NOTE: The instance count cannot be less than 1.

8. Copy the desired vThunder Image Name and Product Name from the Azure Marketplace for A10 vThunder and update the details in the parameter file as follows:

```
"vThunderImage":{
   "value":"vthunder_520_byol"
},
"publisherName":{
   "value":"a10networks"
},
"productName":{
   "value":"a10-vthunder-adc-520-for-microsoft-azure"
},
```

NOTE: Do not change the publisher name.

9. Configure an address prefix and subnet values for each vThunder instances' management interface and data interfaces.

```
"mgmtIntfPrivatePrefix":{
   "value":"10.0.1.0/24"
},
"eth1PrivatePrefix":{
   "value":"10.0.2.0/24"
},
"eth2PrivatePrefix":{
   "value":"10.0.3.0/24"
},
```

10. Configure network interface cards for each vThunder instances.

```
"nic1Name":{
   "value":"vth-inst1-mgmt-nic1"
},
```

```
    "nic2Name":{
       "value":"vth-inst1-data-nic2"
    },
    "nic3Name":{
       "value":"vth-inst1-data-nic3"
    },
```

11. Configure NIC1 public IP name for vThunder.

```
    "nic1PublicIPName":{
       "value":"vth-inst1-mgmt-nic1-ip"
    },
```

12. Configure a network security group.

```
    "networkSecurityGroupName":{
       "value":"vth-nsg1"
    },
```

13. Configure a storage account name.

```
    "storageAccountName": {
       "value": "vthunderstorage"
    },
```

If the storage account already exists, the following error is displayed, “The storage account named is already taken”.

14. Configure SSL container name.

```
   "sslContainerName": {
      "value": "ssl"
   },
```

NOTE: Do not change the SSL container name.

15. Configure load balancer name, public IP name, backend IP name, and frontend pool name.

```
    "lbPubIPName": {
       "value": "vth-lb1-ip"
    },
    "lbName": {
       "value": "vth-lb1"
    },
```

```
        "lbBackEndPoolName": {
            "value": "vth-lb1-bck-pool1"
        },
        "lbFrontEndName": {
            "value": "vth-lb1-frnt-ip"
        },
```

16. Configure vThunder monitoring VM name.

```
        "vmName": {
            "value": "vth-agent-ins1"
        },
```

17. Configure log agent container name.

```
        "logAgentContainerName": {
            "value": "vth-agent-cont"
        }
```

18. Verify if all the configurations in the PS_TMPL_3NIC_NVM_VMSS_PARAM.json file are correct and then save the changes.

Deploy vThunder

To deploy vThunder on Azure cloud, perform the following steps:

1. From Start menu, open PowerShell and navigate to the folder where you have downloaded the PowerShell template.
2. Run the following command to create a deployment group in Azure.

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_NVM_VMSS_1.ps1 -
resourceGroup <resource_group_name> -location "<location_name>"
```

Example:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_NVM_VMSS_1.ps1 -
resourceGroup vth-rg1 -location "south central us"
```

Here, **`vth-rg1`** resource group is created.

Verify Resource Creation

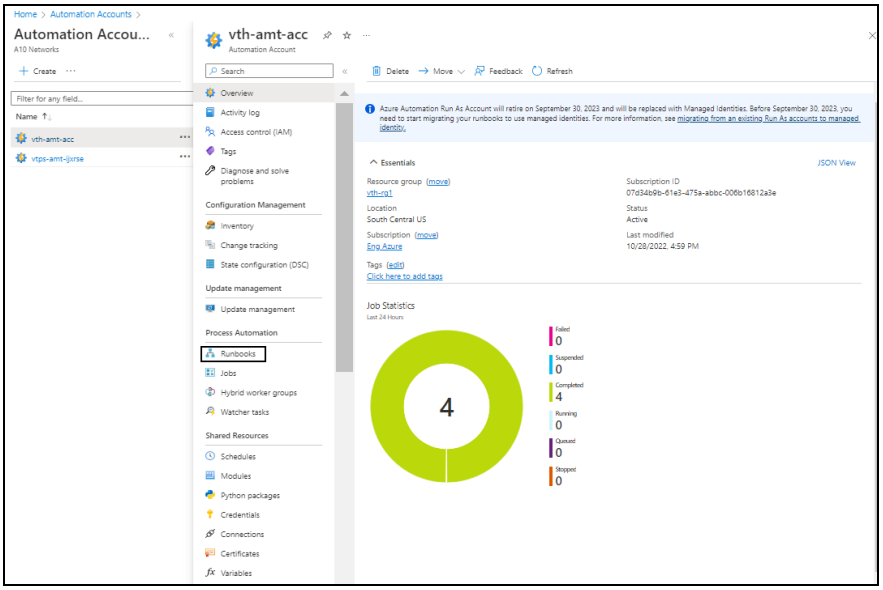
Runbook

To verify the creation of runbooks, perform the following steps:

1. From **Home**, navigate to **Azure Services** > **Automation Accounts** > <automation_account_name>.

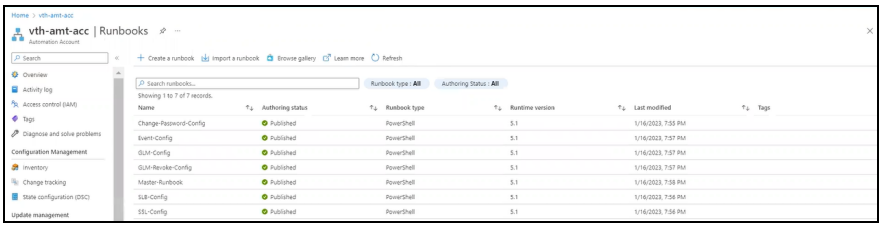
   The selected automation account - Overview window is displayed.

   Figure 125 : Selected automation account - Overview window



2. Click **Runbooks** from the left **Process Automation** panel.
   The selected automation account - Jobs window is displayed.

   Figure 126 : Selected automation account - Runbooks window



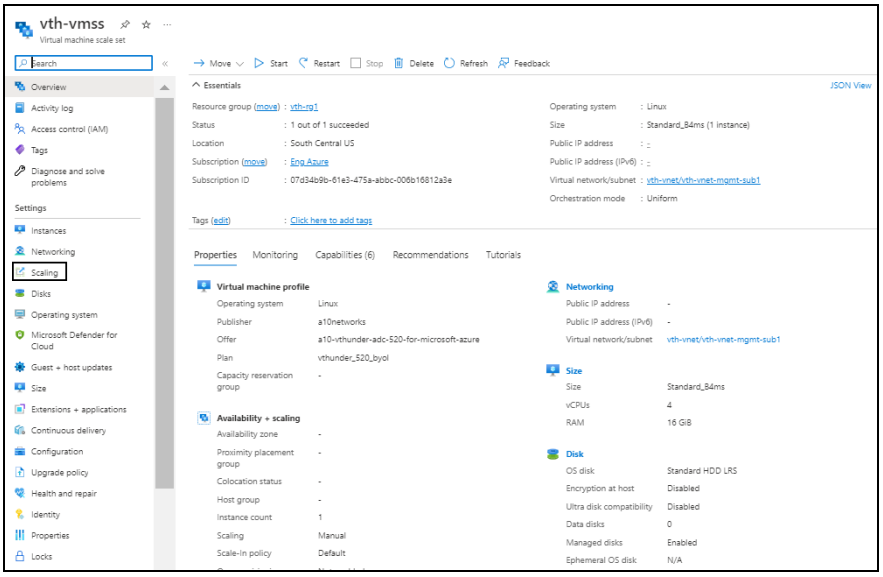
Instance Count

To verify the instance count, perform the following steps:

1. From **Home**, navigate to **Azure Services** > **Virtual machine scale set** > <vmss_name>.

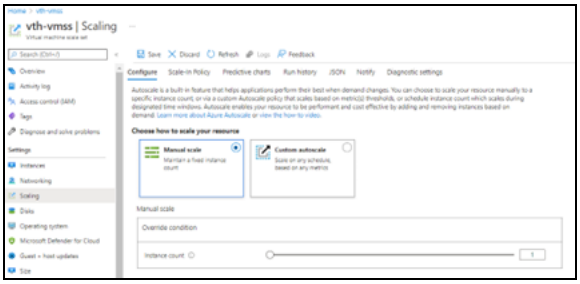
The selected VMSS - Overview window is displayed. Here, the VMSS name is **`vth-vmss`**.

Figure 127 : Virtual machine scale set - Overview window



2. Click **Scaling** from the left **Settings** panel.
   The selected VMSS - Scaling window is displayed.

   Figure 128 : Virtual machine scale set - Scaling window - Configure tab



3. Verify the configured instance count.
   If the instance gets deleted either manually or automatically, VMSS creates a new instance.

LB creation

To verify LB resource creation, perform the following steps:

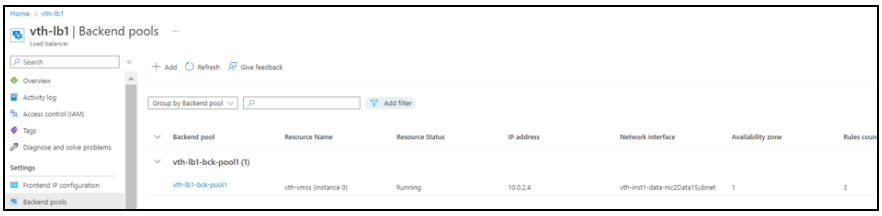
a. From **Home**, navigate to **Azure Services** > **Load balancer** > <lb_name>.
   The selected LB - Overview window is displayed. Here, the LB name is **`vth-lb1`**.

b. Click **Frontend IP configuration** from the left **Settings** panel to verify if the LB frontend IP is created.

Figure 129 : Selected Frontend IP configuration window

c. Click **Backend pools** from the left **Settings** panel to verify if the backend pools are created.

Figure 130 : Selected Backend pools window

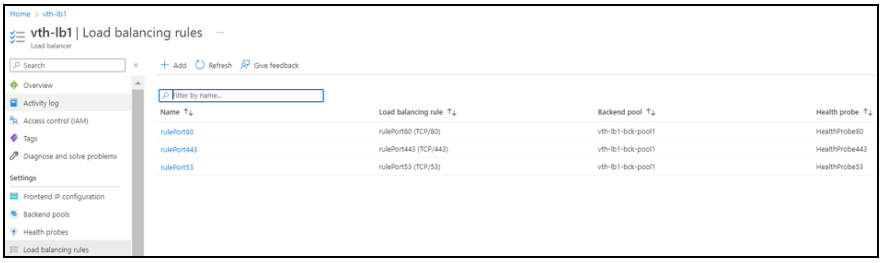


d. Click **Health probes** from the left **Settings** panel to verify if the health probes are created.

Figure 131 : Selected Health Probes window

e. Click **Load balancing rules** from the left **Settings** panel to verify if the load balancing rules are created.

Figure 132 : Selected load balancing rules window



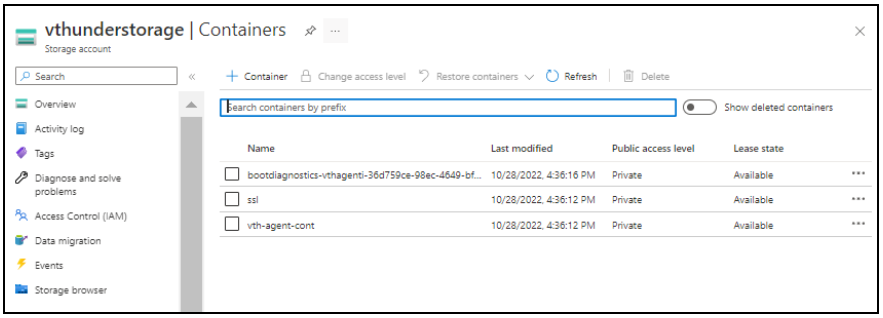
Storage Account Container

To verify storage account container, perform the following steps:

a. From **Home**, navigate to **Azure Services** > **Storage account** > <storage_account_ name>.
The selected storage account - Overview window is displayed. Here, the storage account name is **`vthunderstorage`**.

b. Click **Containers** from the left **Data storage** panel.
The selected storage account - Containers window is displayed.

Figure 133 : Selected storage account - Containers window



Configure Server VMSS

The following topics are covered:

- Create a Server Machine
- Verify the Server VMSS Creation

Create a Server Machine

To create a Server machine, perform the following steps:

1. From Home, navigate to **Azure Services** > **Virtual machine scale sets** and click **Create**.
   The **Create a virtual machine** window is displayed.
2. Select or enter the following mandatory information in the **Basics** tab:

   Project details

   - Subscription
   - Resource group

   Scale set details

   - Virtual machine scale set name - Server machine
   - Region

   Orchestration

   - Orchestration mode

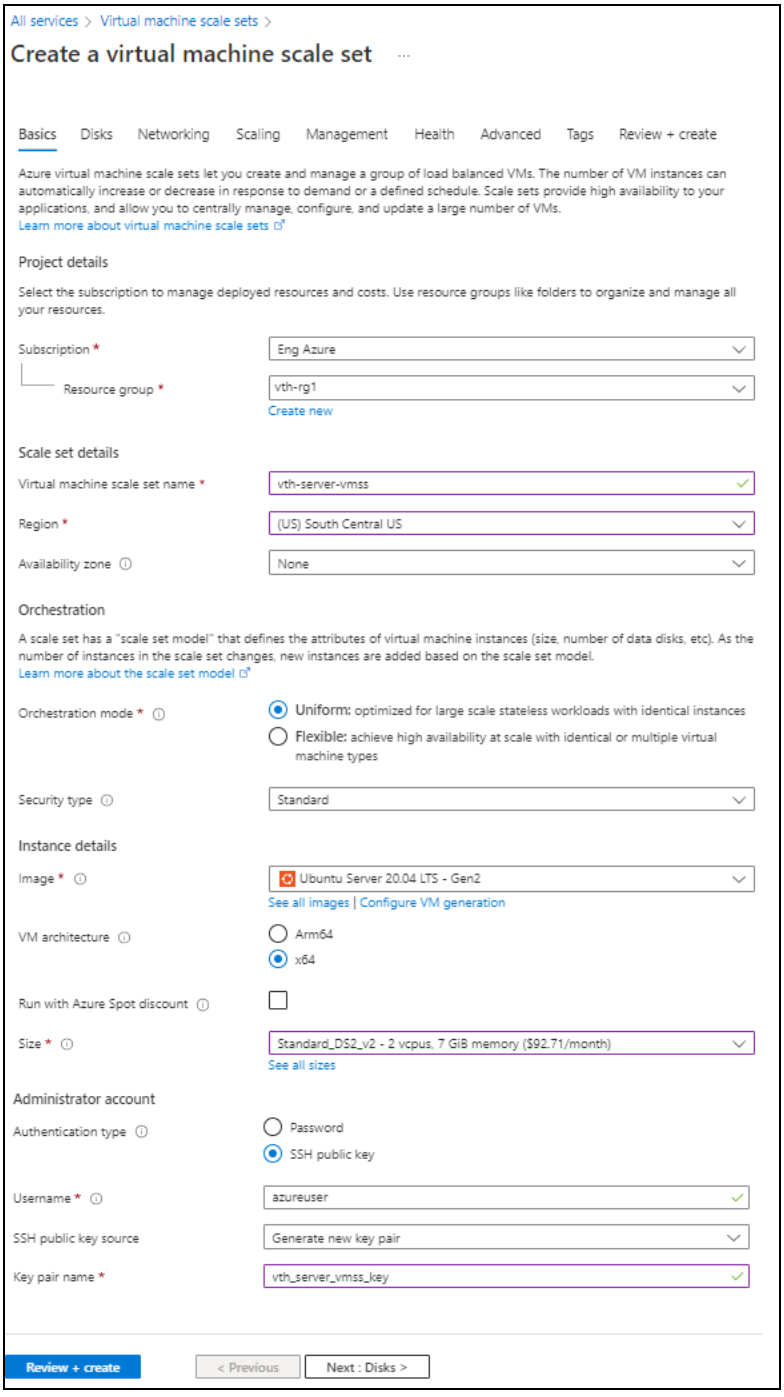
   Instance details

   - Image
   - Size

   Administrator account

   - Depending upon the Authentication type, provide the information.

Figure 134 : Create a virtual machine scale set window - Basics tab



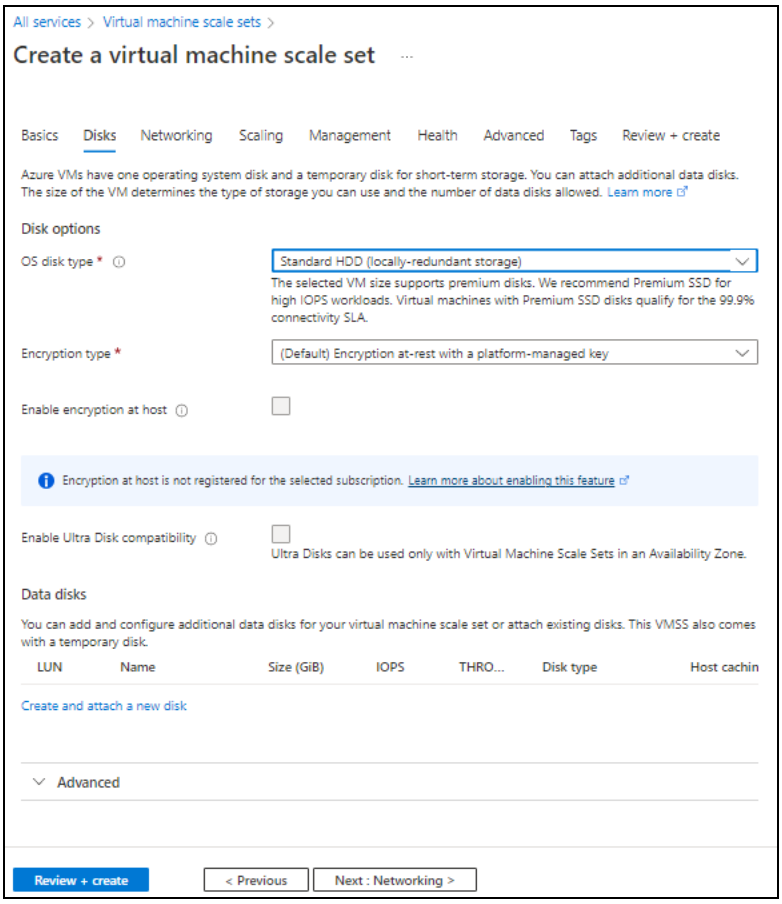
3. Leave the remaining fields as is and click **Next : Disks** at the bottom of the window.

4. Select or enter the following mandatory information in the **Disks** tab:

   Disk options

   - OS disk type
   - Encryption type

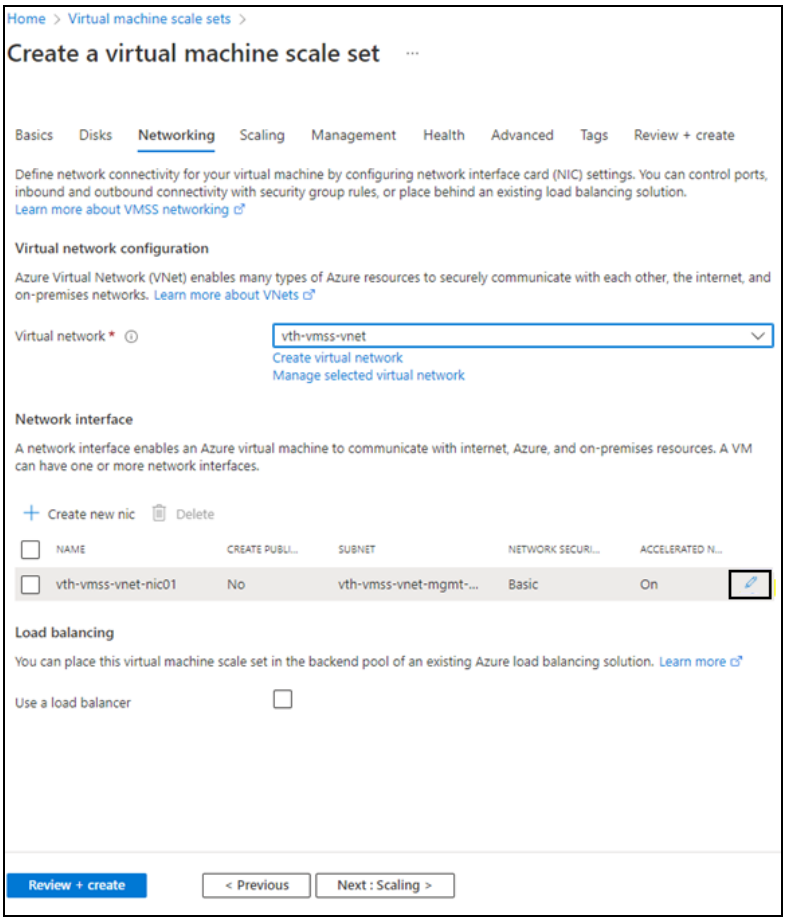
   Figure 135 : Create a virtual machine scale set window - Disks tab



5. Leave the remaining fields as is and click **Next : Networking** at the bottom of the window.

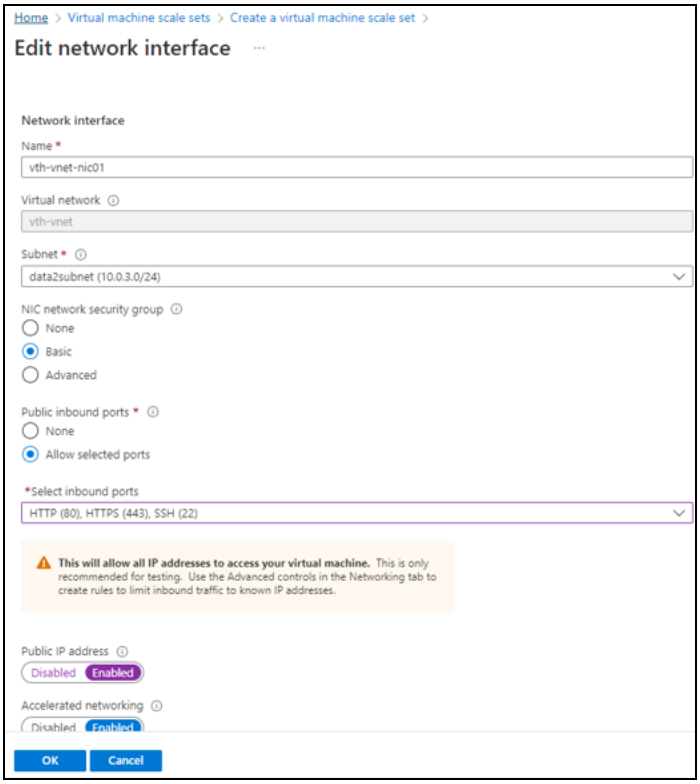
6. Select the Virtual network in the **Networking** tab.

Figure 136 : Create a virtual machine scale set window - Networking tab



7. If Data subnet 2 value is not assigned to management NIC 1, click the edit button corresponding to it.
   The **Edit Network Interface** window appears.
8. Select Data subnet 2 value in the **Subnet** field and then click **OK**. Here, the Subnet 2 value is `10.0.3.0/24`.

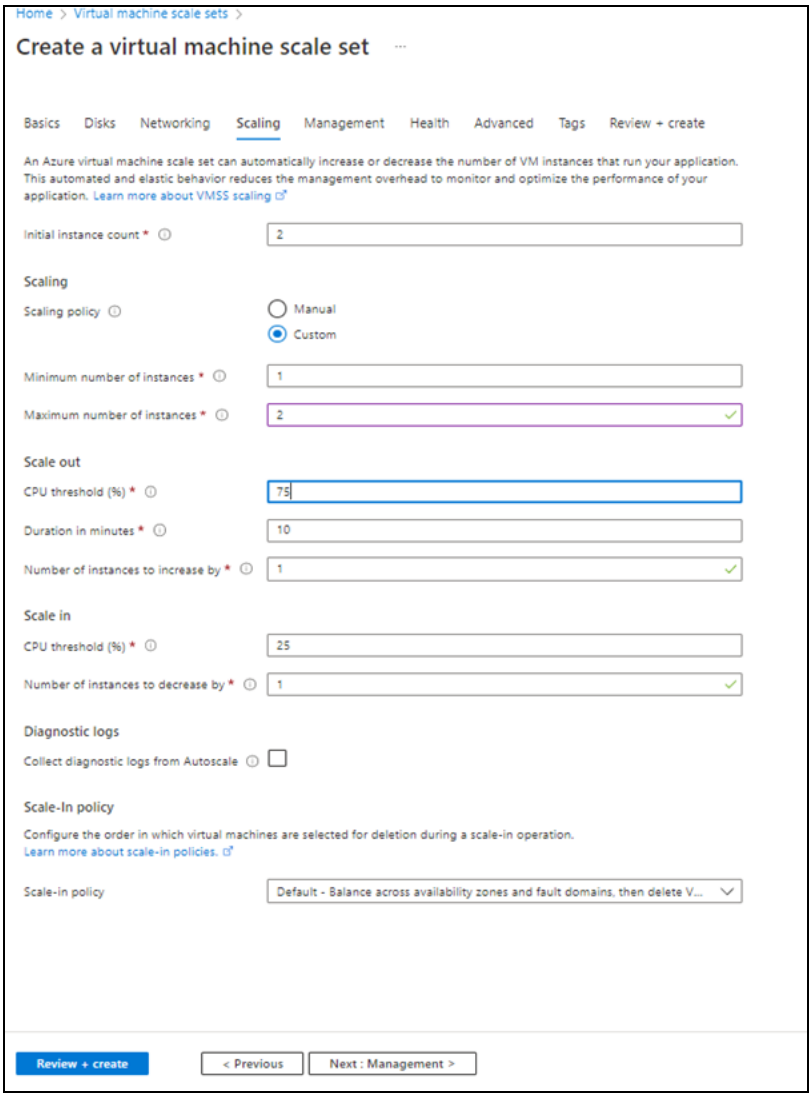
Figure 137 : Edit network interface window



9. Leave the remaining fields as is in the **Networking** tab and click **Next : Scaling** at the bottom of the window

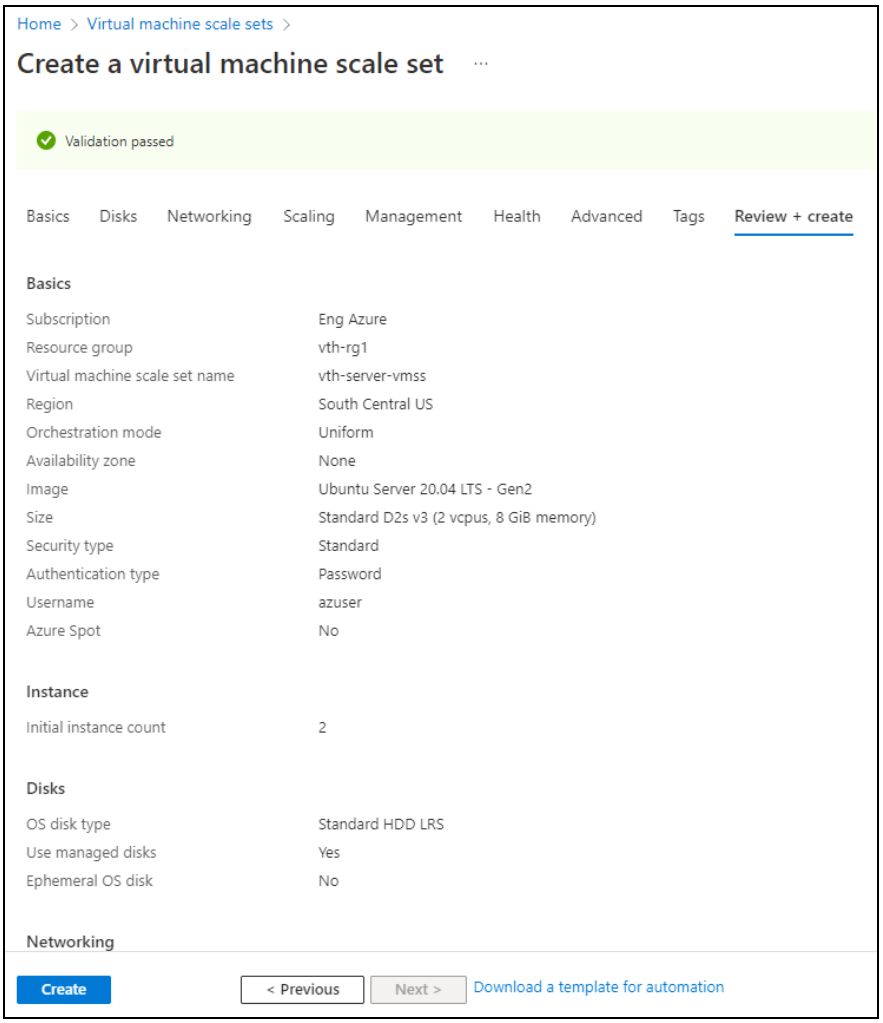
10. Select or enter the information in the **Scaling** tab as shown below.

Figure 138 : Create a virtual machine scale set window - Scaling tab



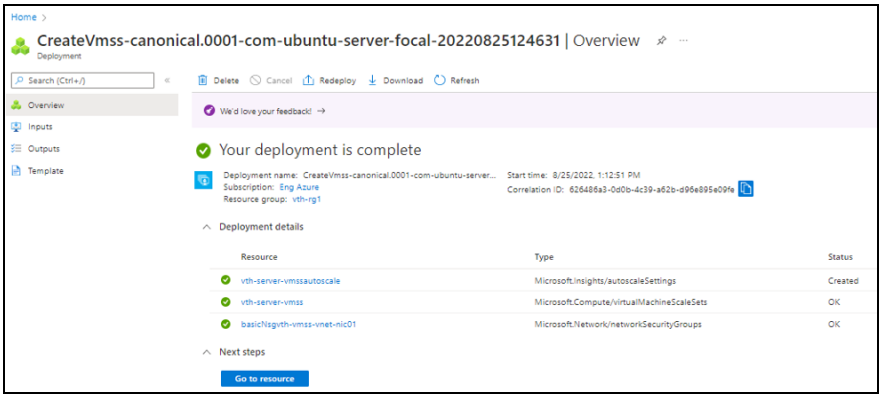
11. Click **Review + create** at the bottom of the window to skip the other tabs.

Figure 139 : Create a virtual machine scale set window - Review + create tab



12. Click **Create** at the bottom of the window.
When the VMSS is created, a message "Your deployment is complete" is displayed in the Create VMSS window.

Figure 140 : Create VMSS window



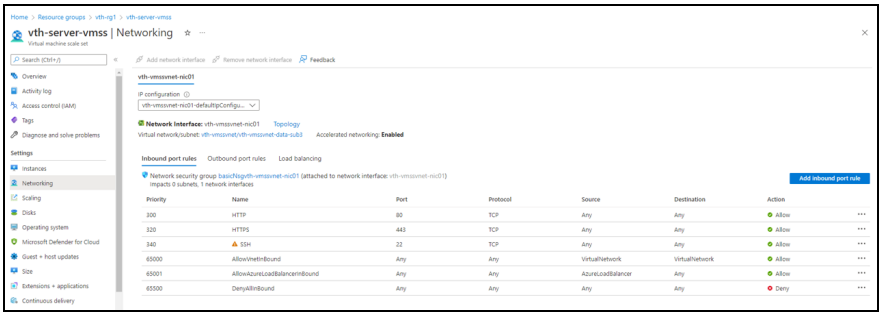
NOTE: It may take the system several minutes to display your resources.

Verify the Server VMSS Creation

To verify the creation of server VMSS, perform the following steps:

1. In the Create VMSS > **Deployment details** section, click the server VMSS resource. Here, the VMSS resource is **`vth-server-vmss`**.
   The VMSS resource details window is displayed.
2. Select **Networking** from the left panel.
   VMSS has only one interface. The ports 80 and 443 are available in the **Inbound port rules** tab.

   Figure 141 : VMSS > Inbound port rules



3. SSH the Server virtual machine and run the following command to install Apache:

```
sudo apt install apache2
```

While the Apache server is getting installed, you get a prompt to continue further. Enter 'Y' to continue. After the installation is complete, a newline prompt is displayed.

Configure Automation Account

The following topics are covered:

- Configure Azure Access Key
- Create Automation Account
- Create Automation Account Webhook

Create Automation Account

The following topics are covered:

- Initial Setup
- Create an Automation Account
- Verify the Automation Account Creation

Initial Setup

Before creating an automation account, configure the corresponding parameters in the PowerShell template.

To configure the parameters, perform the following steps:

1. Open the PS_TMPL_3NIC_NVM_VMSS_RUNBOOK_VARIABLES.json with a text editor.
2. Configure the Azure autoscale resources.

   If the automation account does not exist, then a new automation account gets created inside resource group. If automation account already exists, then template gets auto-updated.
   If the automation account variable does not exist, then a new automation

account variable gets created inside the automation account. If an automation account variable already exists, an error is displayed "The variable already exists".

Provide the application/client ID and tenant ID saved in the Collect Azure Access Key step or you can get these values from **Home** > **Azure Services** > **Azure Active Directory** > **App Registration** > **Owned applications** > <application_name>.

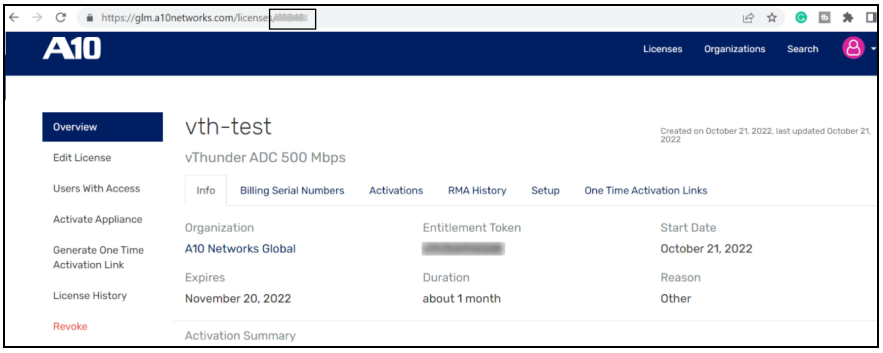
```
"azureAutoScaleResources": {
  "resourceGroupName": "vth-rg1",
  "automationAccountName": "vth-amt-acc",
  "vThunderScaleSetName": "vth-vmss",
  "serverScaleSetName": "vth-server-vmss",
  "storageAccountName": "vthunderstorage",
  "appId": "xxxxxxxx-xxx-xxxx-xxxx-xxxxxxxxxxxx",
  "tenantId": "xxxxxxxx-xxx-xxxx-xxxx-xxxxxxxxxxxx",
  "masterWebhookUrl": "<master-runbook-webhook-url>",
  "location": "South Central US"
},
```

NOTE: Do not change the **Master Webhook url**. It gets updated automatically.

3. Configure the GLM parameters.

```
"glmParam": {
  "userName": "youremail@a10networks.com",
  "userPassword": "your_password",
  "entitlementToken": "A10xxa2fxxxx",
  "licenseId": "59xxx"
},
```

You can get the license ID from GLM Portal. Select your license and go to the URL. The license ID is at the end of the URL. For example, glm.a10networks.com/license/**12345**



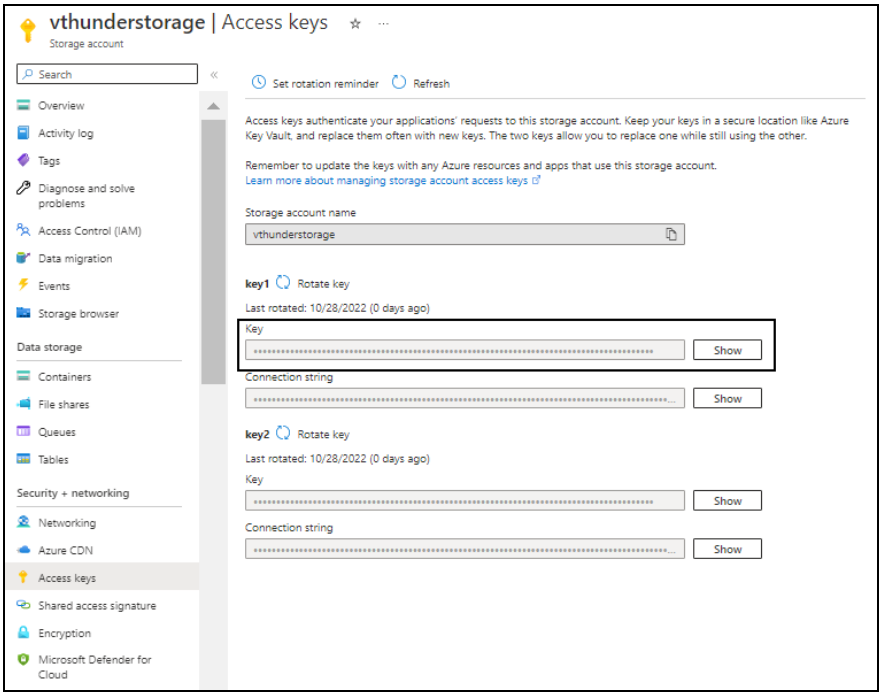
4. Configure SSL parameters.

```
  "sslParam": {
    "requestTimeout": 40,
    "path": "server.pem",
    "file": "server",
    "certificationType": "pem",
    "containerName": "ssl",

"storageAccountKey":"LX6z8xxxxxxehXx0xxxv7xxxx/xxxOfzxxxxxROxxx5gXzxxx
xfhxcx0gxxxxx9rxxASxxxsx=="
  },
```

NOTE: The **`server.pem`** file should be placed in the same downloaded folder from which your are executing the scripts. For example, the server.pem should be placed in 'C:\Users\TestUser\Templates\' folder.

You can get the storage account key from **Azure Portal** > **Azure Services** > **Storage accounts** > <storage_account_name> > **Access Keys** > **Key1** > **Key**.

Figure 142 : Selected storage account - Access keys window



5. Configure SLB parameters.

```
"slbParam":{
  "slb_port":{
    "value":[
      {
        "port-number": 53,
        "protocol": "udp",
        "health-check-disable":1
      },
      {
        "port-number": 80,
        "protocol": "tcp",
        "health-check-disable":1
      },
      {
        "port-number": 443,
        "protocol": "tcp",
        "health-check-disable":1
```

```
        }
      ]
    },
    "vip_port":{
      "value": [
        {
          "port-number":53,
          "protocol":"udp",
          "ha-conn-mirror":1,
          "auto":1,
          "service-group":"sg53"
        },
        {
          "port-number":80,
          "protocol":"http",
          "auto":1,
          "service-group":"sg80"
        },
        {
          "port-number":443,
          "protocol":"https",
          "auto":1,
          "service-group":"sg443"
        }
      ]
    },
    "rib_list": [
      {
      "ip-dest-addr":"0.0.0.0",
      "ip-mask":"/0",
      "ip-nexthop-ipv4": [
          {
          "ip-next-hop":"10.0.2.1"
          }
      ]
      }
    ]
```

```
},
```

6. Configure AutoScale parameters.

```
"autoScaleParam": {
  "maxScaleOutLimit": 10,
  "minScaleInLimit": 1,
  "scaleInThreshold": 25,
  "scaleOutThreshold": 80
},
```

NOTE: These parameters are applied only for the function-based autoscaling. Skip these parameters for Agent-based autoscaling.

7. Provide the client secret ID from **Azure Portal** > **Azure Services** > **Azure Active Directory** > **App Registration** > **Owned applications** > <application_name> > **Certificates & secrets**.

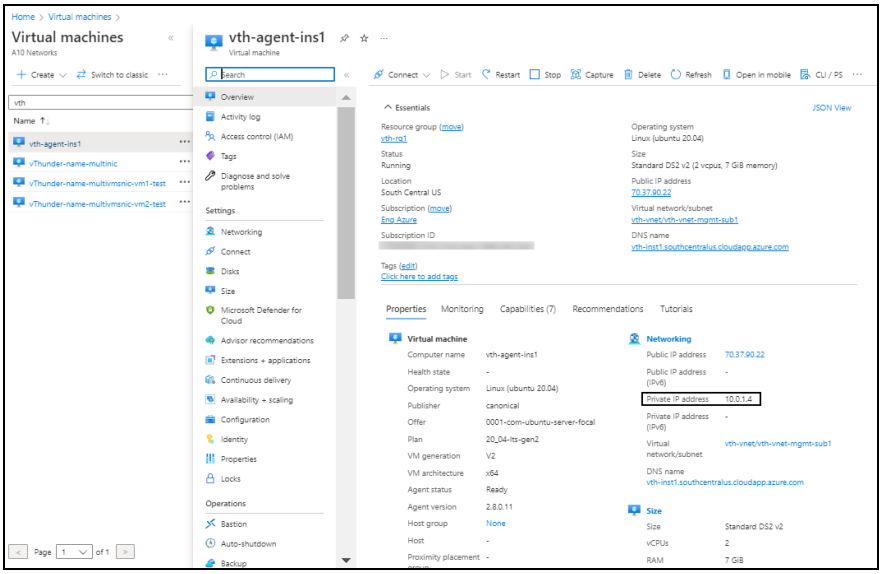
```
"clientSecret": "9-xxx~jIxxxEVyxxxxHNxxxOwv_xxxxZLxxxTM",
```

8. Configure private IP of agent VM.

```
"agentPrivateIP": "10.0.1.4"
```

You get this value from **Azure Portal** > **Azure Services** > **Virtual machine** > <virtual_machine> > **Overview** > **Properties** > **Private IP address**.

Figure 143 : Selected virtual machine - Overview window



9. Verify the vThunder instance username.

```
"vThUsername": "admin"
```

NOTE: Do not change the vThunder instance username.

10. Retain the vThunder new password application flag initially as 'False'.

```
"vThNewPassApplyFlag": "False"
```

11. Verify if all the configurations in the PS_TMPL_3NIC_NVM_VMSS_RUNBOOK_VARIABLES.json file are correct and then save the changes.

Create an Automation Account

To create an automation account, perform the following steps:

1. Run the following command:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_NVM_VMSS_AUTOMATION_ACCOUNT_2.ps1
```

2. Provide the default and new password when prompted:

```
Enter Default Password:***
Enter New Password:***
Confirm New Password:***
```

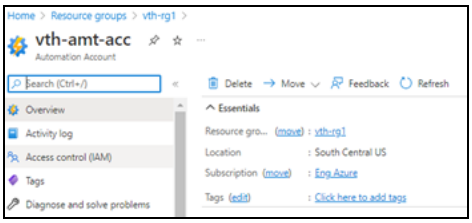
The default password is provided by the A10 Networks Support. The new password should follow the Default password policy. For more information, see Default Password Policy.

Verify the Automation Account Creation

To verify the creation of an automation account, perform the following steps:

1. From the **Home**, navigate to **Azure Services** > **Resource Group** > <resource_group_name>.
   The selected resource group - Overview window is displayed.
2. Under **Resources** tab, group the resources based on the resource type.
3. Verify if the recently created automation account is listed under **Automation Accounts** type.
4. Select the required automation account.
   The selected automation account - Overview window is displayed.

   Figure 144 : Selected automation account - Overview window



5. Click **Variables** from the left **Shared Resources** panel.
   The selected automation account - Variables window is displayed

   Figure 145 : Selected automation account - Variables window

6. Verify if all the variables associated with the automation account are listed.

Create Automation Account Webhook

The following topics are covered:

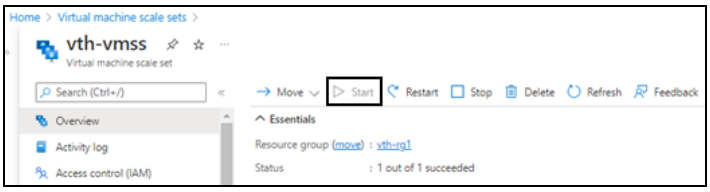
- Initial Setup
- Create a Webhook
- Verify the AutoScale Resource Variable creation
- Verify the SSL File availability
- Verify the Runbook Jobs creation

Initial Setup

To verify that the virtual machine scale set resources are running, perform the following steps:

1. From **Home**, navigate to **Azure Services** > **Resource Group** > <resource_group_name>.
   The selected resource group - Overview window is displayed.

   Figure 146 : VMSS window

2. Under **Resources** tab, group the resources based on the resource type.
3. Select the virtual machine scale set instance under **Virtual machine scale set** type and verify that the instance is in **Start** mode.

Create a Webhook

To create a webhook, perform the following steps:

1. From Start menu, open PowerShell and navigate to the folder where you have downloaded the PowerShell template.
2. Run the following command to create the webhook:

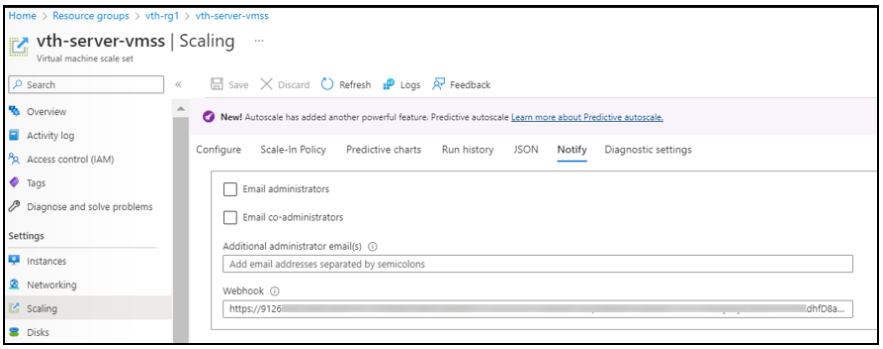
```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_NVM_VMSS_WEBHOOK_3.ps1
```

3. After the webhook installation is complete, the webhook url is displayed.

```
Save this URL :
https://fa72c8e5-xxxx-xxxx-9dc5-b4a71eec0a95.webhook.scus.azure-
automation.net/webhooks?token=Q*****pG4UEOScfqdEGEAkqJPgdK%2bOpusoUAWk
*****%3d
```

4. Save this webhook url for future purpose.
5. From **Home**, navigate to **Azure Services** > **Virtual machine scale set** > <vmss_ name>.
   The selected VMSS - Overview window is displayed. Here, the VMSS name is **`vth-server-vmss`**.
6. Click **Scaling** from the left **Settings** panel.
   The selected VMSS - Scaling window is displayed.

   Figure 147 : VMSS-Scaling - Notify tab



7. Select **Notify** tab.
8. Copy the saved webhook url and paste it in the **Webhook** field.
9. Click **Save** to save the changes.

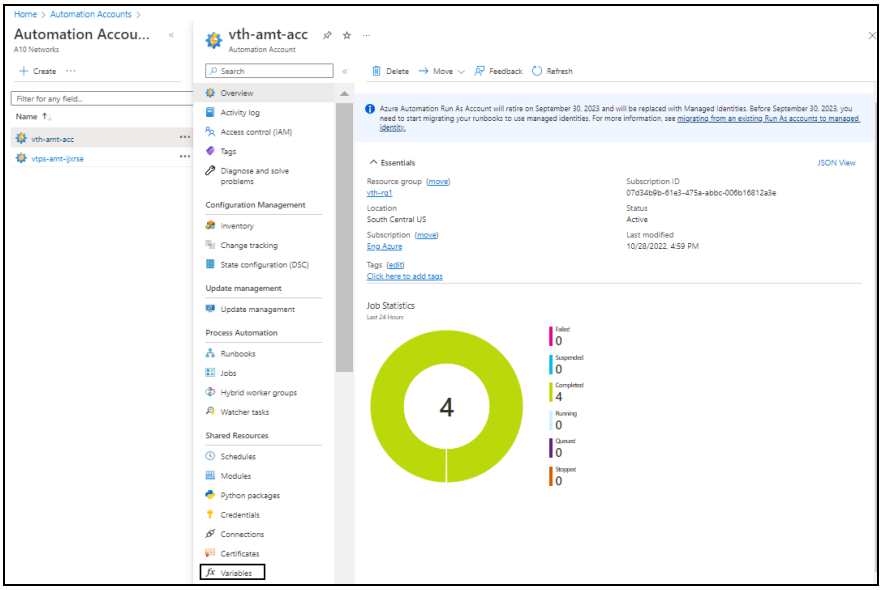
Verify the AutoScale Resource Variable creation

To verify the creation of an autoscale resource variable, perform the following steps:

1. From **Home**, navigate to **Azure Services** > **Automation Accounts** > <automation_ account_name>.

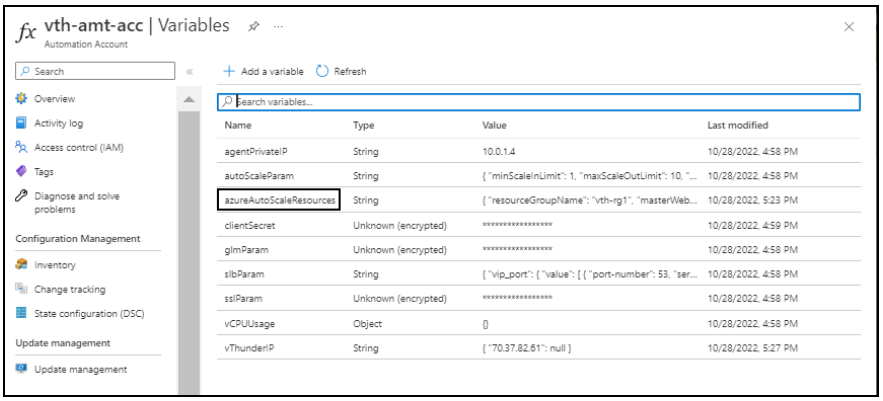
   The selected automation account - Overview window is displayed.

Figure 148 : Selected automation account - Overview window



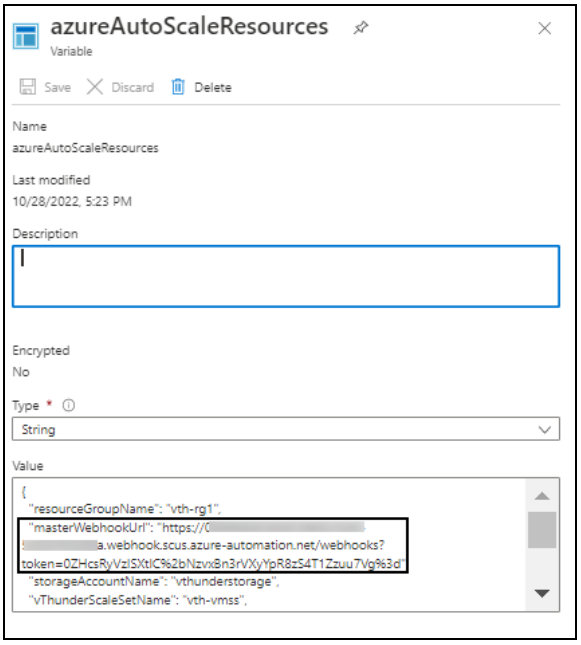
2. Click **Variables** from the left **Shared Resources** panel.
   The selected automation account - Variables window is displayed.

Figure 149 : Selected automation account - Variables window



3. Select the **azureAutoScaleResources** variable.
   The azureAutoScaleResources variable window is displayed.

Figure 150 : AzureAutoScaleResources variable window



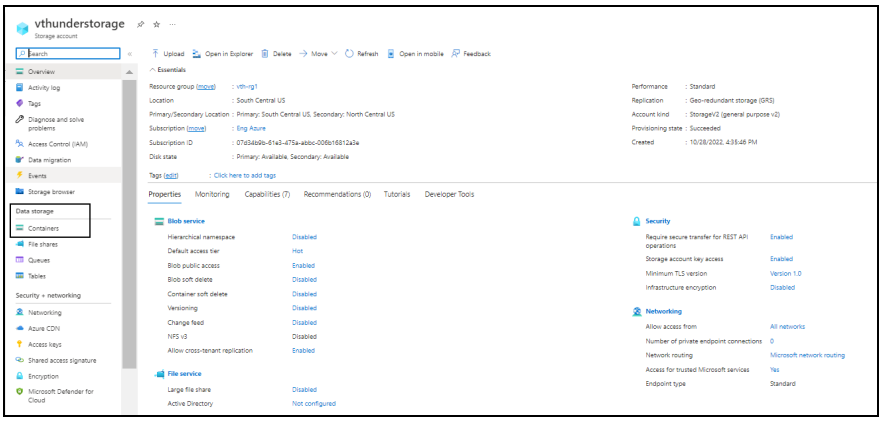
4. Verify the master webhook URL in the **Value** field.

Verify the SSL File availability

To verify the availability of SSL file, perform the following steps:

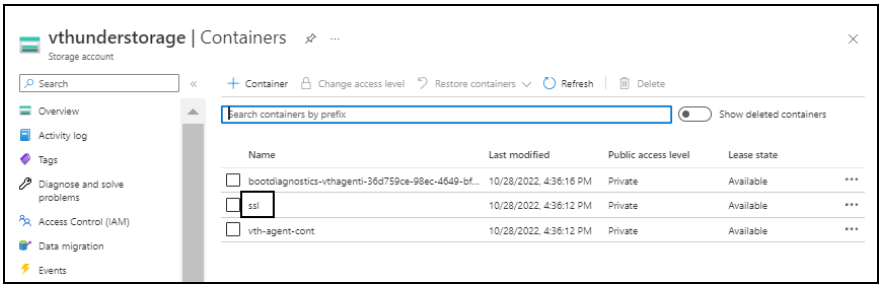
1. From **Home**, navigate to **Azure Services** > **Storage Accounts** > <storage_account_name>.
   The selected storage account - Overview window is displayed.

   Figure 151 : Selected storage account - Overview window



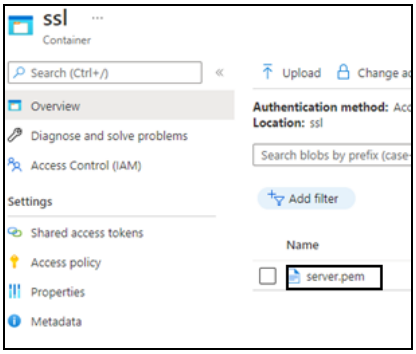
2. Click **Containers** from the left **Data Storage** panel.
   The selected storage account - Containers window is displayed.

   Figure 152 : Selected storage account - Containers window



3. Select the SSL container.
   The SSL container window is displayed.

   Figure 153 : SSL Container window



4. Verify if the SSL config file is listed. Here, the SSL config file is **`server.pem`**.

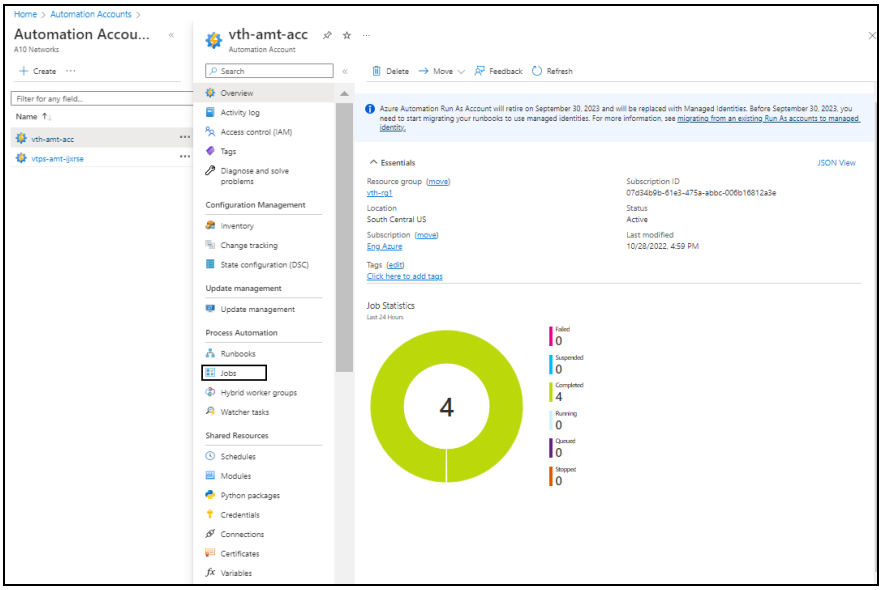
Verify the Runbook Jobs creation

To verify the creation of runbook jobs, perform the following steps:

1. From **Home**, navigate to **Azure Services** > **Automation Accounts** > <automation_account_name>.

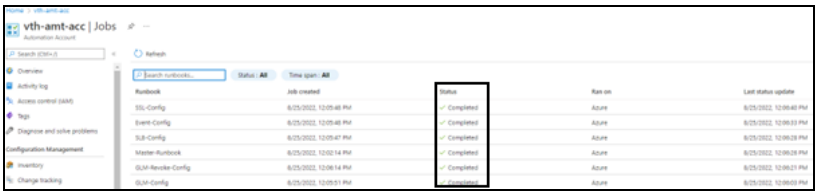
   The selected automation account - Overview window is displayed.

Figure 154 : Selected automation account - Overview window



2. Click **Jobs** from the left **Process Automation** panel.
   The selected automation account - Jobs window is displayed.

   Figure 155 : Selected automation account - Jobs window



3. Verify if all the runbook jobs have completed status.

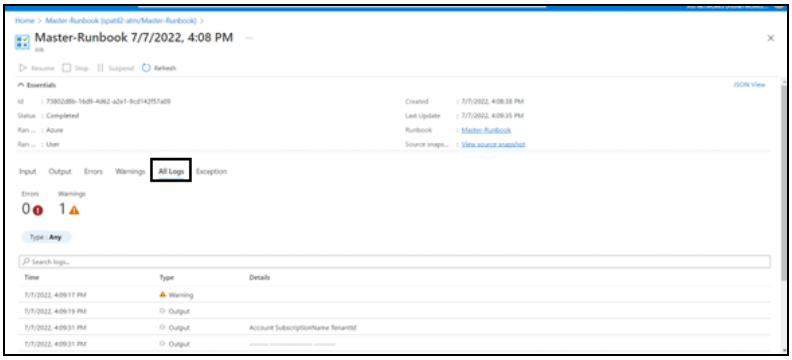
   The master runbook automatically triggers all the jobs one-by-one.

   NOTE: It may take the system a few minutes to display the completed status.

   If any job has failed or if it is not working, refer Common Errors.

4. Select each runbook job > **All Logs** tab to verify the logs.
   The selected automation account - selected job - Jobs window is displayed.

Figure 156 : Selected runbook job window



Enable Autoscaling

An Azure virtual machine scale set can automatically increase or decrease the number of vThunder VM instances to meet the changing demand.

To enable autoscaling, use any of the following two options:

1. AutoScaling and Log Monitoring using Agent Setup
   Using this option:
   - Custom metrics of vThunder can be collected and published into Azure application insight service and same metrics can be used along with vmss rule for autoscaling.
   - CPU utilization alerts can be scheduled using vmss alert rule.
   - CPU utilization of vThunder can be viewed in Azure application insight console.
   - vThunder logs can be viewed in Azure log analytics workspace.

NOTE: ACOS supports and recommends **AutoScaling and Log Monitoring using Agent Setup** option.

2. AutoScaling using Azure Function Setup
   Using this option:
   - CPU utilization metrics can be collected by the Custom Azure functions. The function periodically maintains vThunder CPU Utilization.

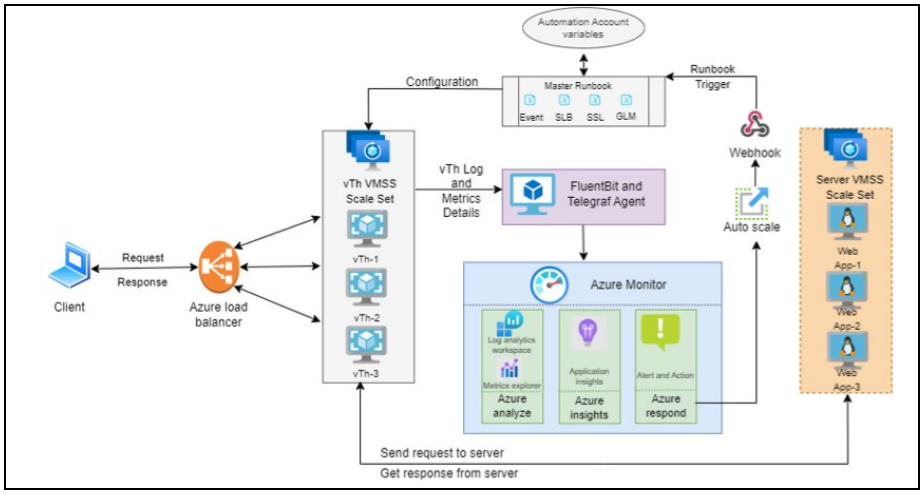
- AutoScaling can be done as per the automation account threshold configuration with variable name **ThresholdForScaleOut** and **ThresholdForScaleIn** for Scale Out and Scale In respectively.
- vThunder logs cannot be viewed in Azure log analytics workspace. For more information, see Azure Log Function.
- CPU utilization of vThunder cannot be viewed in Azure application insight console.

Autoscaling Options

Configure Autoscaling and Log Monitoring using Agent Setup

Figure 157 shows the process flow when different Azure resources and system components are connected to each other in the 3NIC-NVM-VMSS Autoscaling and Log Monitoring using Agent Setup.

Figure 157 : 3NIC-NVM-VMSS Autoscaling and Log Monitoring using Agent Setup Process Flow



The following topics are covered:

- Initial Setup
- Create Fluentbit and Telegraf Agent
- Verify Log Agent file upload
- Access vThunder Agent using CLI

- Create Autoscale Rule
- Create Autoscale Alert
- Verify Logs in Log Analytics Workspace
- Verify Metrics in Application Insights

Initial Setup

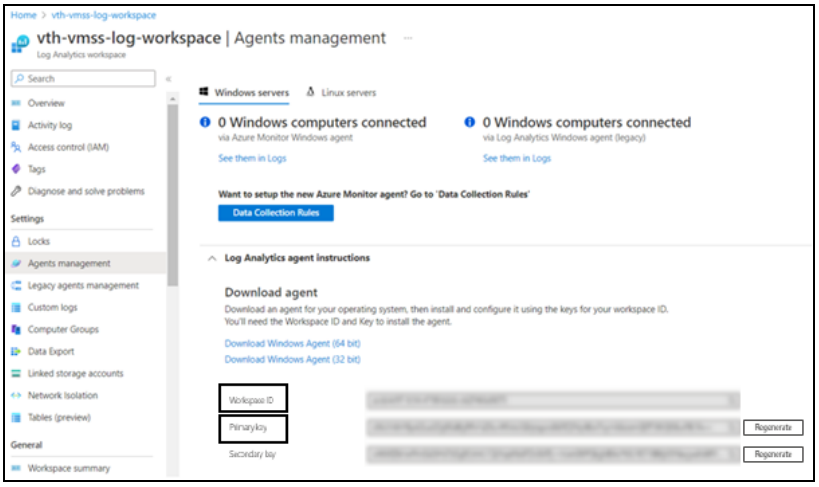
To configure autoscaling and log monitoring using the PowerShell template, perform the following steps:

1. Navigate to the folder where you have downloaded the PowerShell template and open PS_TMPL_3NIC_NVM_VMSS_LOG_AGENT_SHELL_SCRIPT.sh with a text editor.
2. Update the customer ID with the workspace ID and shared key with primary key.

```
# azure log workspace id
customer_id="d1c8985b-xxxx-xxxx-xxxx-12868ad9d740"
# azure log Primary Key
shared_key="tewPsyMYkdGOThRjEyl***********F8CzJ49ZRgw=="
```

   You can get these values from **Home** > **Azure Services** > **Log Analytics workspaces** > <log_analytics_workspace> **Settings** > **Agents management**.

   Figure 158 : Agents management window



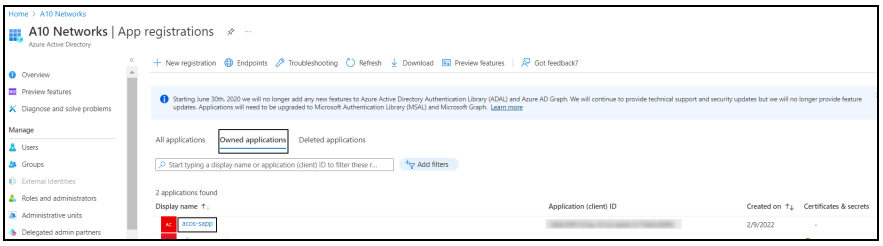
3. Update client ID, tenant ID, and client secret.

```
(cat /etc/environment; echo "AZURE_CLIENT_ID=10724xxx-xxxx-xxxx-xxxx-
xxxxxc14726d"; echo "AZURE_TENANT_ID=91d27xxx-xxxx-xxxx-xxxx-
```

```
xxxbf81fcb2f"; echo "AZURE_CLIENT_SECRET=9-xxx~jxxOREVyxxxxxHNxxxOwv_
xxxxxZLIYxxx"
```

You can get these values from **Home** > **Azure Services** > **Azure Active Directory** > **App Registration** > **Owned applications** > <application_name>.

Figure 159 : Azure active directory - App registrations window



4. Update app insights key with instrumentation key.

```
app_insights_Key="37b1aea5-xxxx-xxxx-xxxx-f2c012bccd93"
```

You can get this value from **Home** > **Azure Services** > **Application Insights** > <application_insight> > **Overview**.

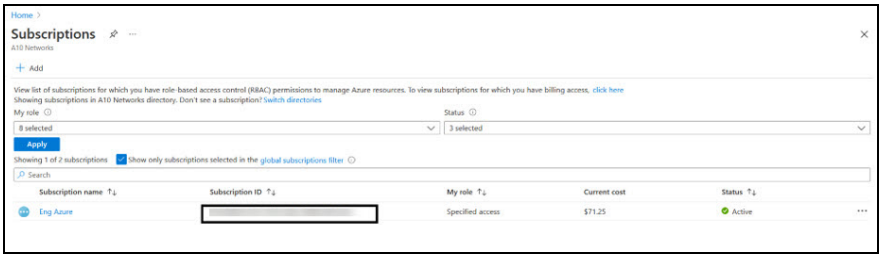
Figure 160 : Selected application insight - Overview window

5. Navigate to the folder where you have downloaded the PowerShell template > plugins > telegraf > plugins > inputs > customplugin and open **get_cpu_param.json** file with a text editor to configure the CPU parameters.

```
{
  "Subscription_Id": "07d3xxxx-xxxx-xxxx-xxxx-xxxxx6812a3e",
  "ResourceGroupName": "vth-rg1",
  "VmssName": "vth-vmss"
}
```

You can get the Subscription ID value from **Home** > **Azure Services** > **Subscriptions** > <subscription_name>.

Figure 161 : Subscriptions window



6. Verify if all the configurations in the PS_TMPL_3NIC_NVM_VMSS_LOG_AGENT_SHELL_SCRIPT.sh file are correct and then save the changes.

Create Fluentbit and Telegraf Agent

To create fluentbit and telegraf agent in virtual machine, perform the following steps:

1. From Start menu, open PowerShell and navigate to the folder where you have downloaded the PowerShell template.
2. Run the following command to create fluentbit and telegraf agents in VM:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_NVM_VMSS_LOG_AGENT_VM_5.ps1
```

NOTE: It may take the system a few minutes to display the resources.

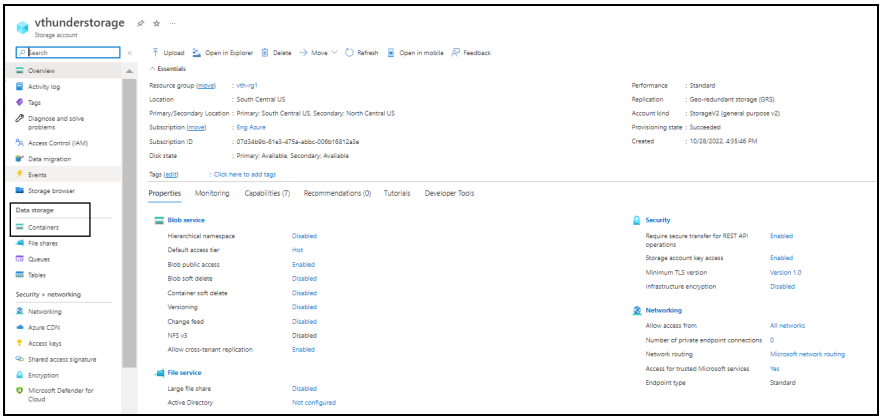
The fluentbit [2.0.3] and telegraf [1.23.4] agents are created.

Verify Log Agent file upload

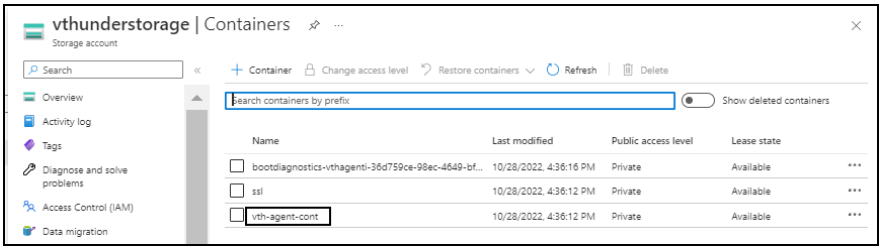
To verify if the log agent file is uploaded, perform the following steps:

1. From **Home**, navigate to **Azure Services** > **Storage Accounts** > <storage_account_name>.
   The selected storage account - Overview window is displayed.

Figure 162 : Selected storage account - Overview window

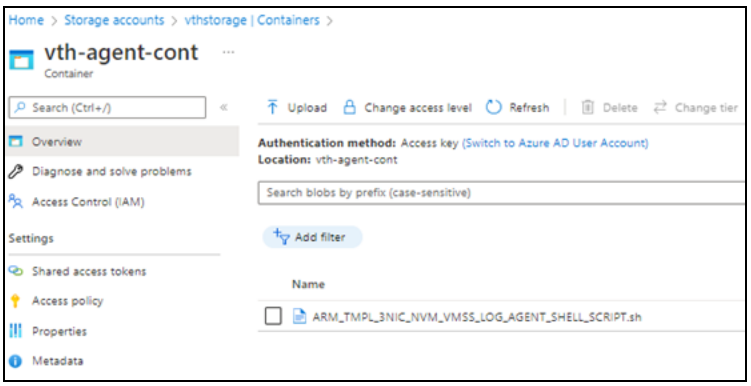


2. Click **Containers** from the left **Data Storage** panel.
   The selected storage account - Containers window is displayed.



3. Select the agent container.
   The agent container window is displayed.

Figure 163 : Agent container window



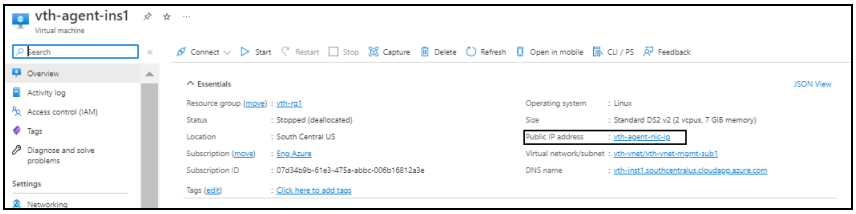
4. Verify if PS_TMPL_3NIC_NVM_VMSS_LOG_AGENT_SHELL_SCRIPT.sh file is uploaded.

Access vThunder Agent using CLI

To access the vThunder agent instance using CLI, perform the following steps:

1. Open PuTTY.
2. Enter or select the following basic information in the PuTTy Configuration window:
   - Hostname: Public IP of the agent virtual machine instance
   - Connection Type: SSH

   Figure 164 : Virtual machine - Agent instance window



3. Click **Open**.
4. In the active PuTTY session, enter the following:

```
login as: vth-user <---adminUsername value configured in PS_TMPL_3NIC_
NVM_VMSS_PARAM.json--->
Using keyboard-interactive authentication.
Password: vth-Password <---adminPassword value configured in PS_TMPL_
3NIC_NVM_VMSS_PARAM.json--->
Last login: Day MM DD HH:MM:SS from a.b.c.d

System is ready now.

[type ? for help]

vth-agent-inst> enable <---Execute command--->
Password:<---just press Enter key--->
vth-agent-inst#config <---Configuration mode--->
vth-agent-inst(config)#
```

5. Run the following command to check the status of the agent service.

```
vth-agent-inst(config)# systemctl status telegraf.service
```

The following output is displayed.

```
● telegraf.service - The plugin-driven server agent for reporting
metrics into InfluxDB
   Loaded: loaded (/lib/systemd/system/telegraf.service; enabled;
vendor preset: enabled)
   Active: active (running) since Thu 2022-08-25 10:24:26 UTC; 18min
ago
     Docs: https://github.com/influxdata/telegraf
 Main PID: 17855 (telegraf)
    Tasks: 9 (limit: 8321)
   Memory: 43.6M
   CGroup: /system.slice/telegraf.service
           └17855 /usr/bin/telegraf - config /etc/telegraf/telegraf.conf
-config-directory /etc/telegraf/telegraf.d

Aug 25 10:42:16 vth-agent-ins1 telegraf[17855]: 2022-08-25T10:42:162Z
E! [outputs.influxdb] When writing to [http://localhost:8086] : failed
doing req: Post ">
Aug 25 10:42:16 vth-agent-ins1 telegraf[17855]: 2022-08-25T10:42:162Z
E! [agent] Error writing to outputs.influxdb: could not write any
address
Aug 25 10:42:26 vth-agent-ins1 telegraf[17855]: 2022-08-25T10:42:162Z
E! [outputs.influxdb] When writing to [http://localhost:8086] : failed
doing req: Post ">
Aug 25 10:42:26 vth-agent-ins1 telegraf[17855]: 2022-08-25T10:42:162Z
E! [agent] Error writing to outputs.influxdb: could not write any
address
Aug 25 10:42:36 vth-agent-ins1 telegraf[17855]: 2022-08-25T10:42:162Z
E! [outputs.influxdb] When writing to [http://localhost:8086] : failed
doing req: Post ">
Aug 25 10:42:36 vth-agent-ins1 telegraf[17855]: 2022-08-25T10:42:162Z
E! [agent] Error writing to outputs.influxdb: could not write any
address
Aug 25 10:42:46 vth-agent-ins1 telegraf[17855]: 2022-08-25T10:42:162Z
E! [outputs.influxdb] When writing to [http://localhost:8086] : failed
doing req: Post ">
Aug 25 10:42:46 vth-agent-ins1 telegraf[17855]: 2022-08-25T10:42:162Z
E! [agent] Error writing to outputs.influxdb: could not write any
```

```
address
Aug 25 10:42:56 vth-agent-ins1 telegraf[17855]: 2022-08-25T10:42:162Z
E! [outputs.influxdb] When writing to [http://localhost:8086] : failed
doing req: Post ">
Aug 25 10:42:56 vth-agent-ins1 telegraf[17855]: 2022-08-25T10:42:162Z
E! [agent] Error writing to outputs.influxdb: could not write any
address
```

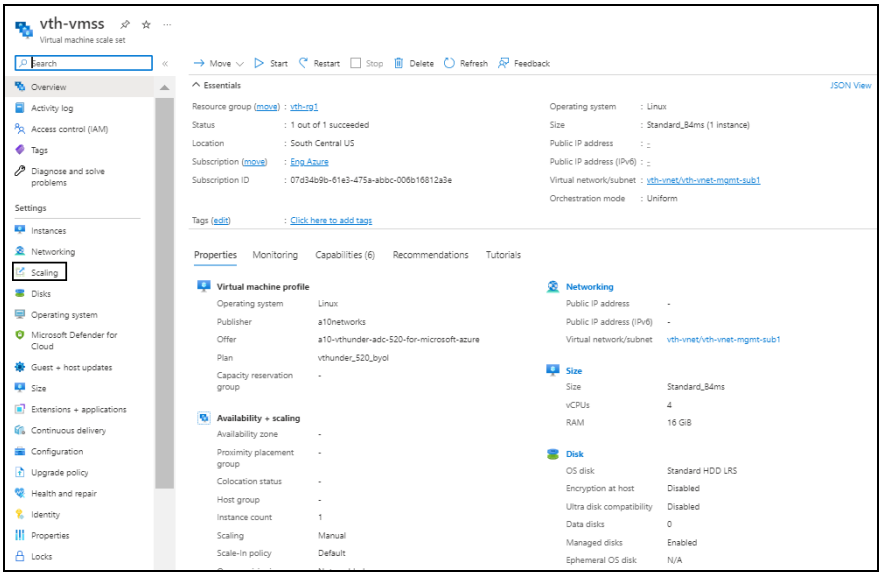
There is a possibility that the command might return few errors. The errors displayed in the above output can be ignored.

Create Autoscale Rule

To create autoscale rule, perform the following steps:

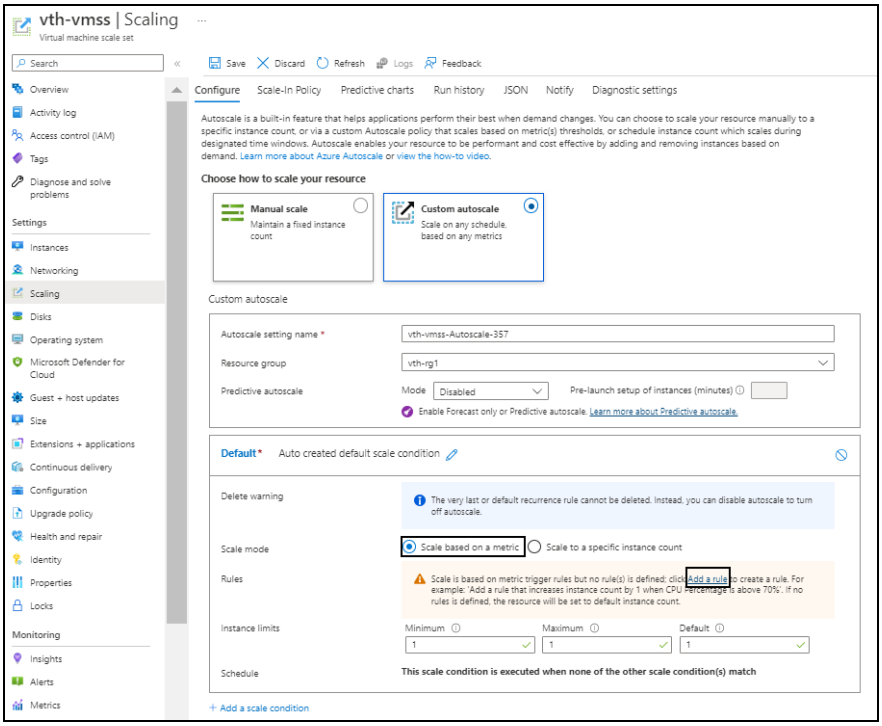
1. From **Home**, navigate to **Azure Services** > **Virtual machine scale set** > <vmss_ name>.
   The selected vmss - Overview window is displayed.

   Figure 165 : Selected VMSS - Overview window



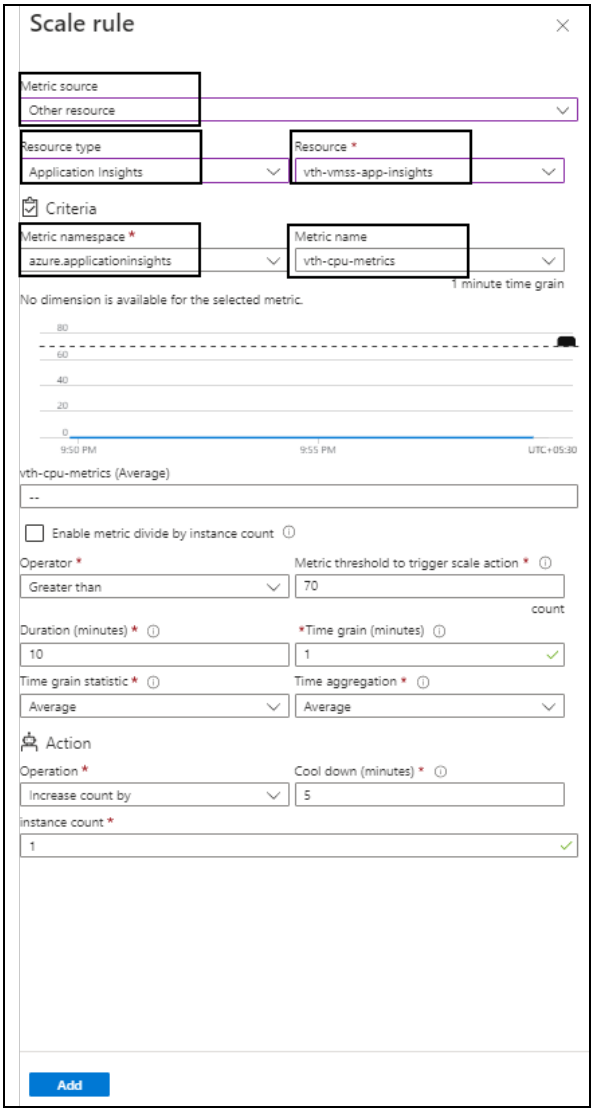
2. Click **Scaling** from the left **Settings** panel.
   The selected vmss - Scaling window is displayed.

Figure 166 : Selected VMSS - Scaling window



3. Under **Configure** tab, select **Custom autoscale** option.
   The fields relevant to this option are displayed.
4. Select the **Scale mode** as **Scale based on a metric**.
5. Click **Add a rule**.
   The **Scale rule** window is displayed.

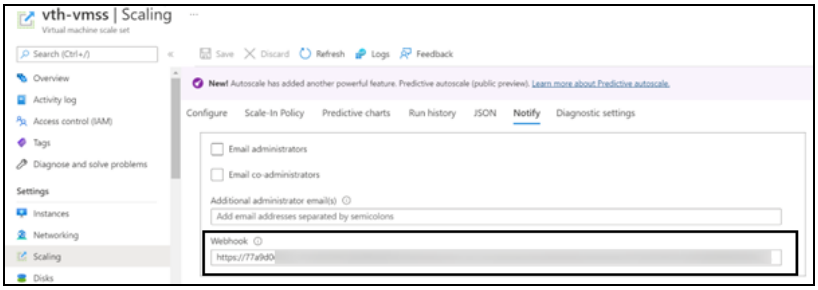
Figure 167 : Scale rule window



6. Select or enter the information in the following fields:
   - Metric source: Other resource
   - Resource type: Application Insights
   - Resource
   - Time aggregation
   - Metric namespace
   - Metric name

7. Click **Add** to add the scale rule.
   The selected vmss - Scaling window is displayed.
8. Click **Save** in the **Configure** tab to save the changes.
9. Select **Notify** tab, enter the webhook url saved in the Create Automation Account Webhook step or you can get the url from **Home** > **Azure Services** > **Automation Accounts** > <automation_account_name> > **Shared Resources** > **Variables** > **azureAutoScaleResources** > **Value** > **masterWebhook_url**.

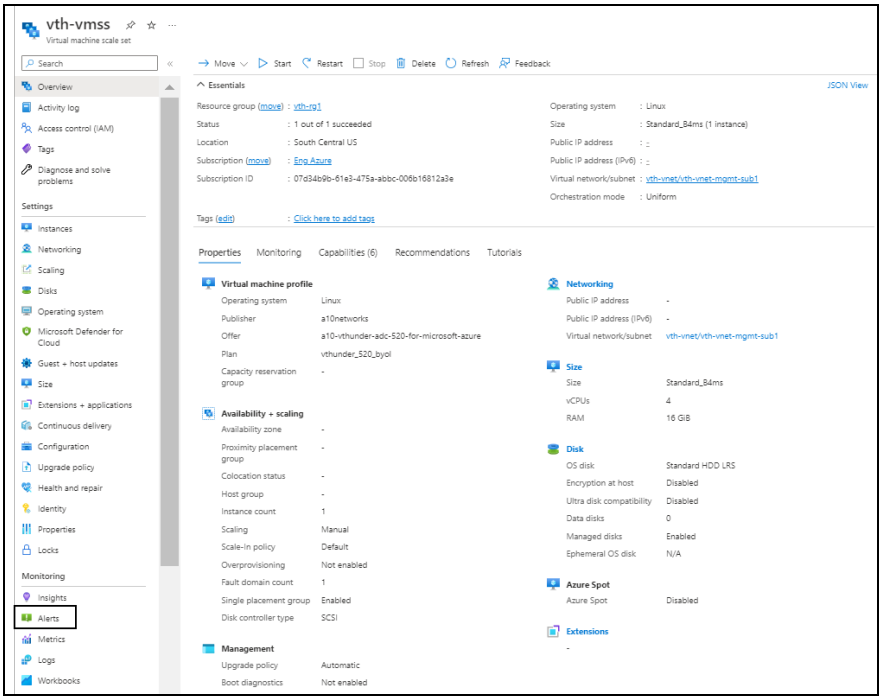
   Figure 168 : Selected VMSS - Scaling window - Notify tab



Create Autoscale Alert

1. From **Home**, navigate to **Azure Services** > **Virtual machine scale set** > <vmss_name>.
   The selected vmss - Overview window is displayed.

Figure 169 : Selected VMSS - Overview window

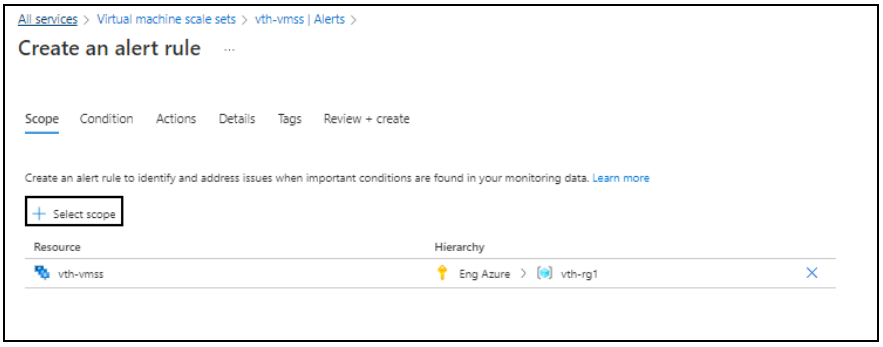


2. Click **Alerts** from the left **Monitoring** panel.
   The selected vmss - Alerts window is displayed.

Figure 170 : Selected VMSS - Alerts window

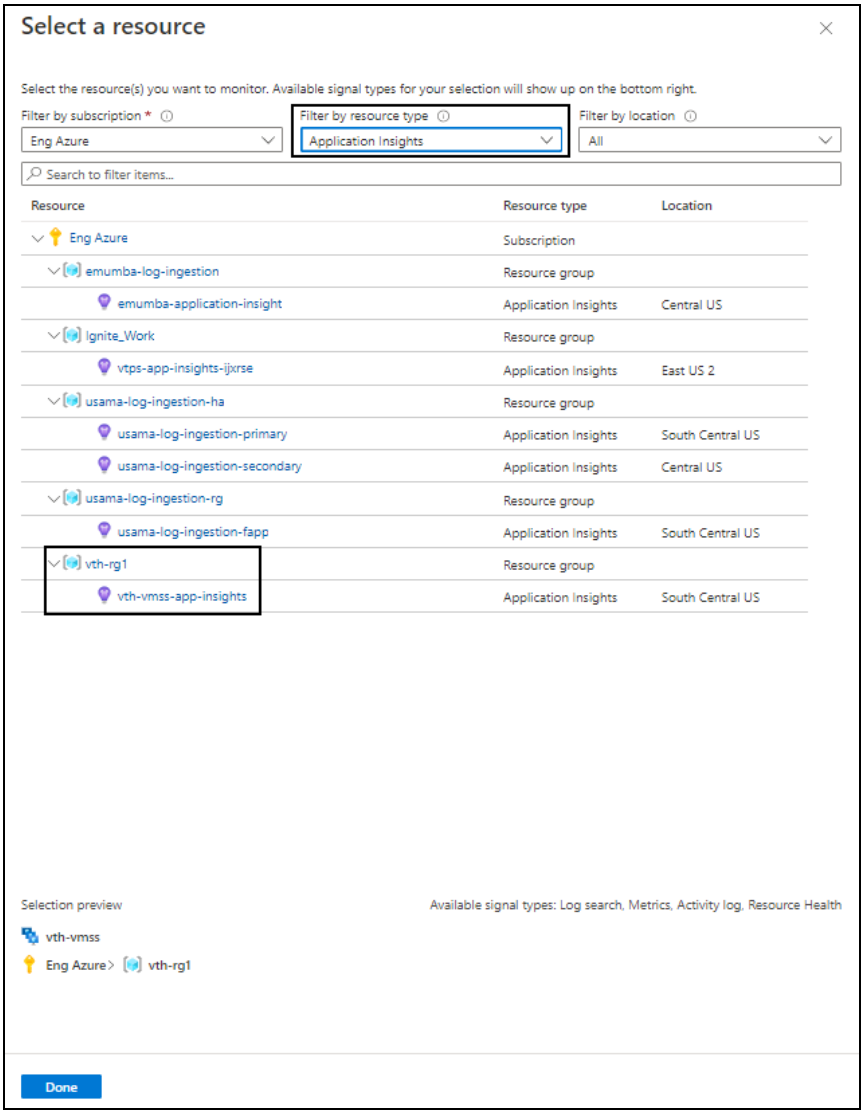
3. Click **Create** > **Alert rule**.
   The Create an alert rule - Scope window is displayed.

Figure 171 : Create an alert rule window - Scope tab



4. Click **Select scope** in the **Scope** tab.
   The **Select a resource** window is displayed.

Figure 172 : Select a resource window

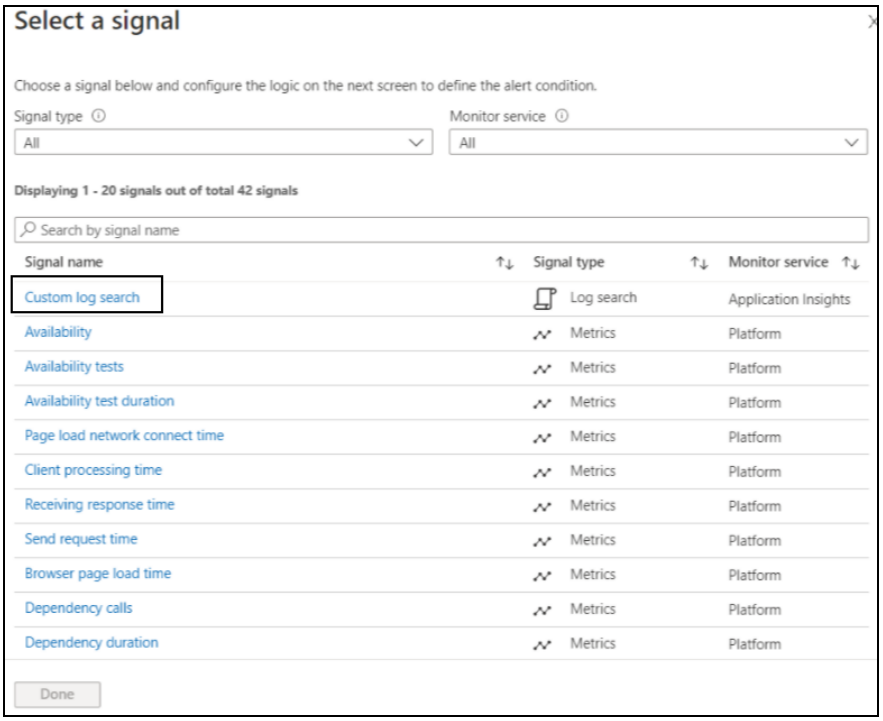


5. From **Filter by resource type**, select **Application Insights**.
   The resource group having application insight resources are displayed.
6. Select the required application insight resource and click **Done**.
   The selected application insight resource is listed under the alert rule scope.
7. Click **Next : Condition** at the bottom of the window.
   The **Create an alert rule** - **Condition** tab window is displayed.

Figure 173 : Create an alert rule window - Condition tab

8. Click **Add condition** in the **Condition** tab.
   The **Select a signal** window is displayed.

   Figure 174 : Select a signal window

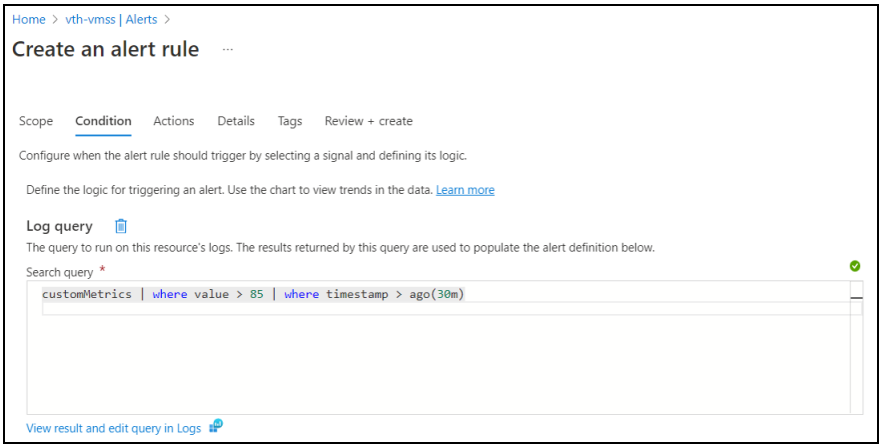


9. Select **Custom log search** as the signal.
   The window to define the signal's logic is displayed in the alert rule condition.
10. Enter any of the following query to fetch the data in the **Search query** field:

```
customMetrics | where value > 85 | where timestamp > ago(30m)
customMetrics | where value > 85 | where timestamp > ago(24h)
customMetrics | where value > 85 | where timestamp > ago(7d)
```

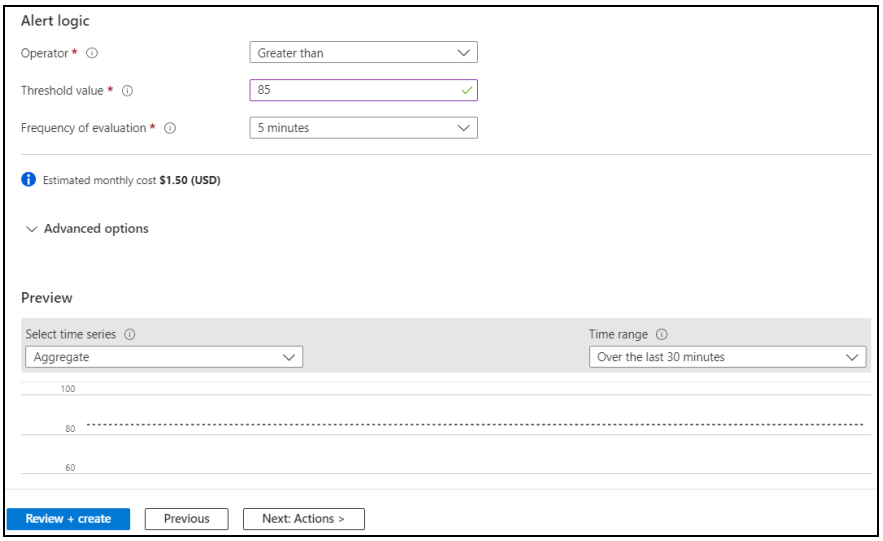
    The above query specifies the frequency for alert data.

Figure 175 : Create an alert rule window - Condition tab



11. Configure alert logic in the **Alert logic** section.

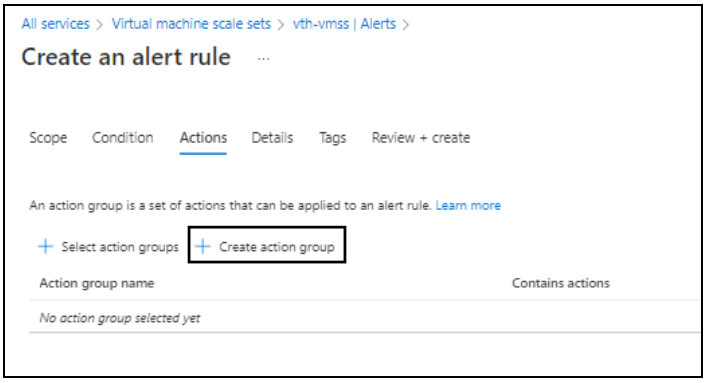
Figure 176 : Alert logic section



Depending upon the signal logic configuration, the monthly cost for the alert is displayed.

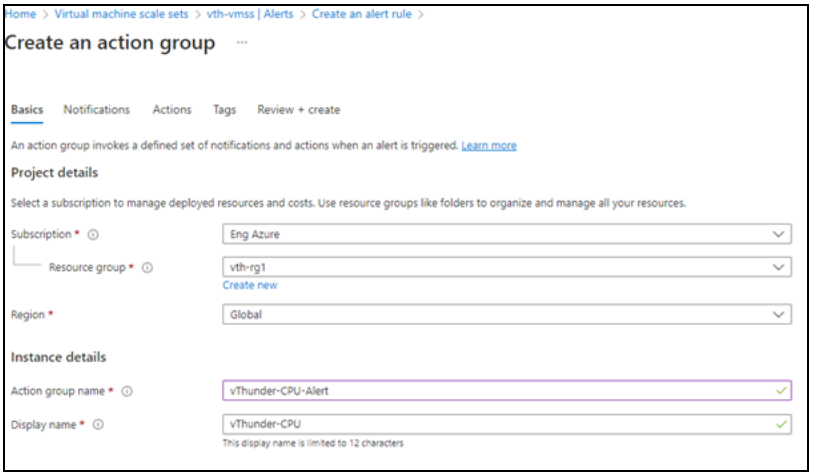
12. Click **Next : Actions** at the bottom of the window.
The **Create an alert rule** - **Actions** window is displayed.

Figure 177 : Create an alert rule window - Actions tab



13. Click **Create action group**.
    The **Create an action group** - **Basics** window is displayed.

Figure 178 : Create an action group window - Basics tab



a. Select or enter the following mandatory information in the **Basics** tab:

   Project details

   - Subscription
   - Resource group
   - Region

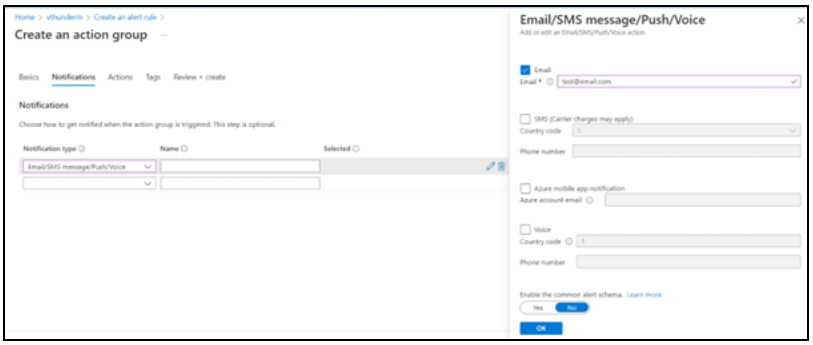
   Instance details

- Action group name
- Display name

b. Click **Next : Notifications** at the bottom of the window.
The **Create an action group** - **Notifications** window is displayed.

c. Select the **Notification type**.
The corresponding window to configure the notification type is displayed.

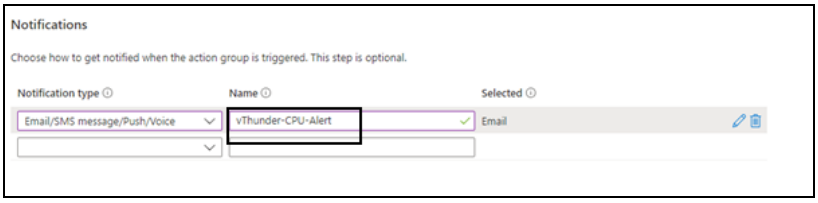
Figure 179 : Create an action group window - Notifications tab - Type



d. Select the **Email** option and provide the correct email ID in the **Email** field and then click **OK**.

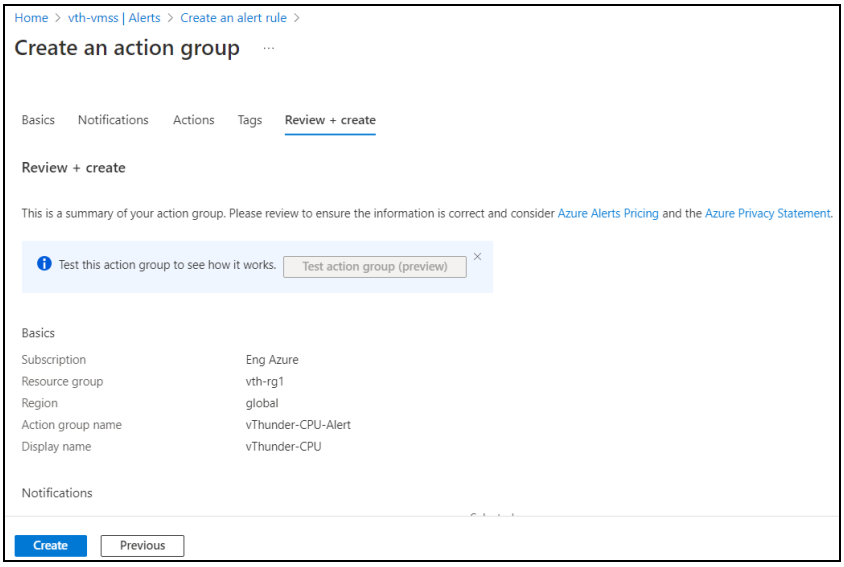
e. Enter a unique name for the notification in the **Name** field.

Figure 180 : Create an action group window - Notifications tab



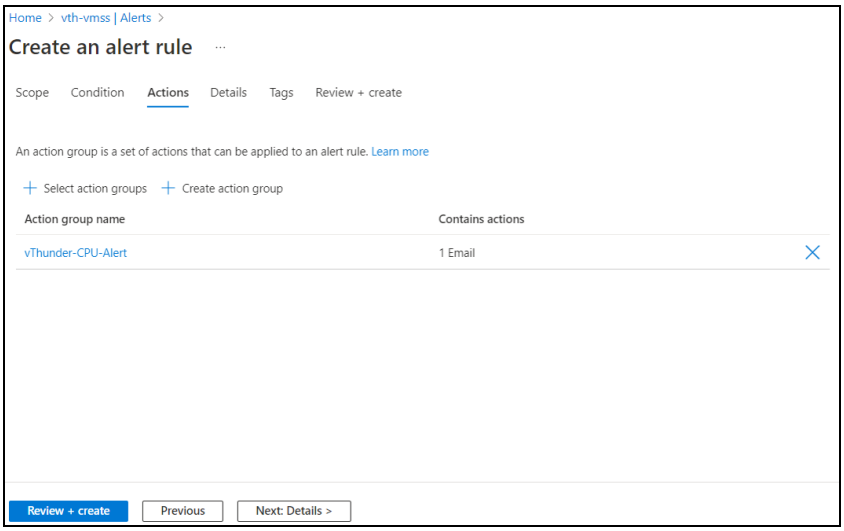
f. Skip the other tabs and click **Review + create** at the bottom of the window.
The **Create an action group** - **Review + create** window is displayed.

Figure 181 : Create an action group window - Review + create tab



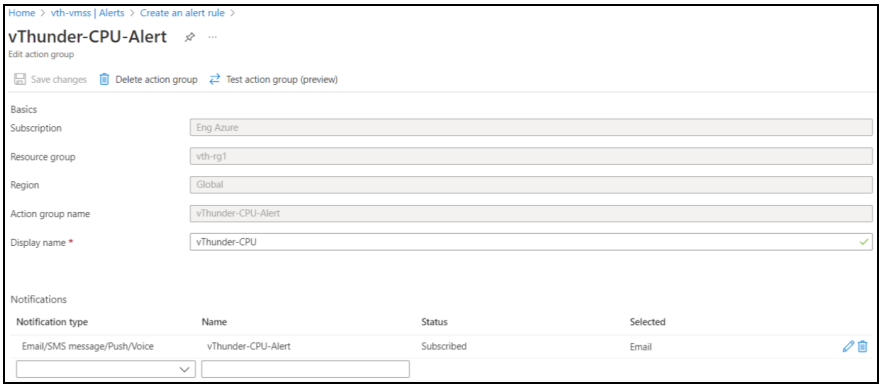
g. Click **Create**.
The action group is listed under **Actions** tab.

Figure 182 : Create an alert rule window - Actions tab



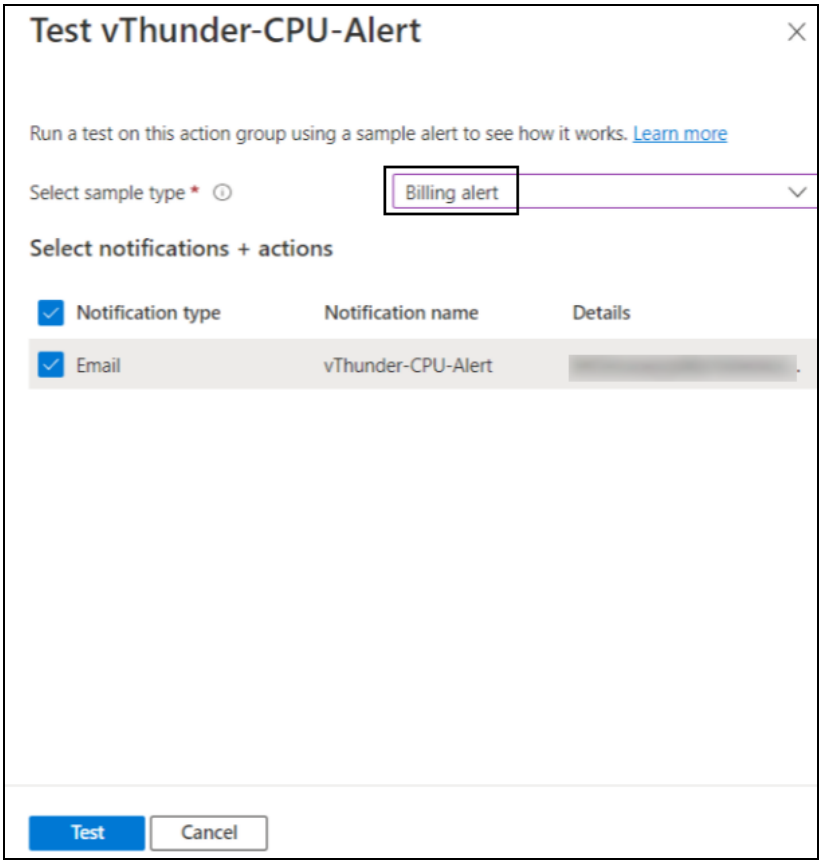
14. Select the recently created action group.
The selected action group is displayed.

Figure 183 : Selected action group



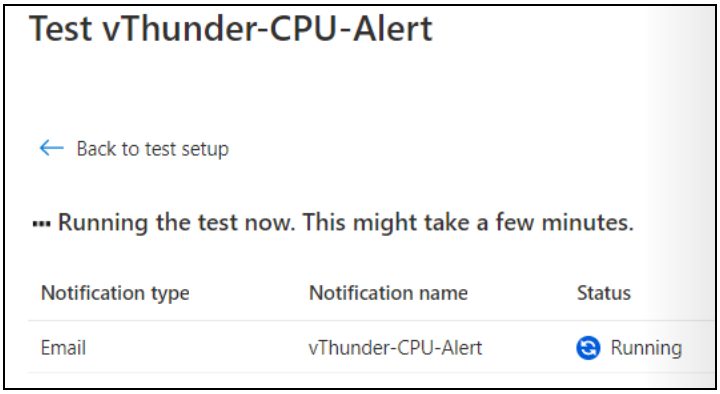
15. Click **Test action group (preview)**.
The Test <action_group_name>-alert window is displayed.

Figure 184 : Test <action_group_name>-alert window



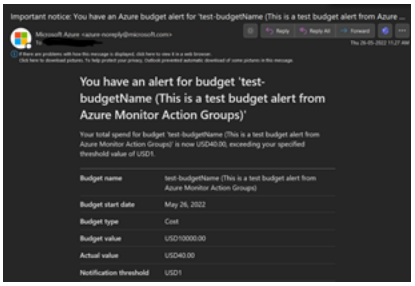
16. Select **Billing alert** as the Sample type and click **Test**.
The running status for the test rule is displayed.

Figure 185 : Test <action_group_name>-alert window - Running status



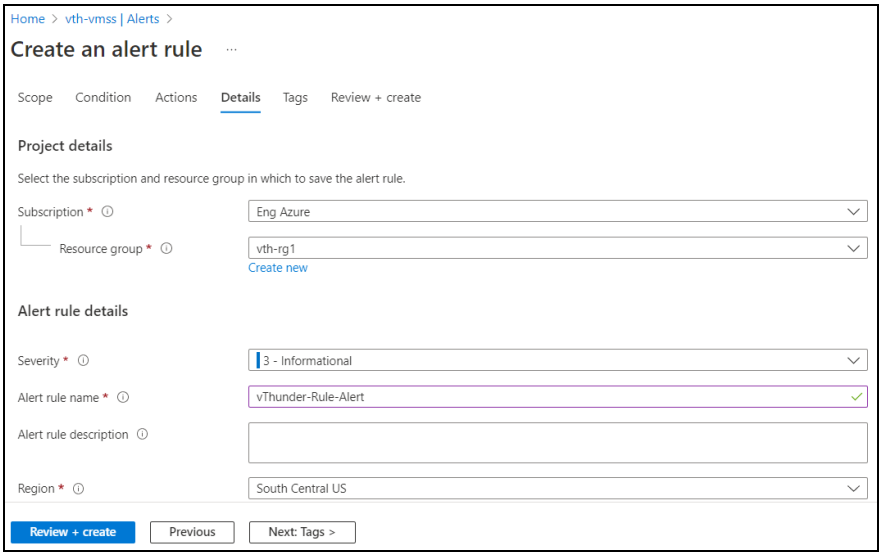
When the success status is displayed, an email notification is triggered to the email ID provided in the Email Notification step.

Figure 186 : Email Notification



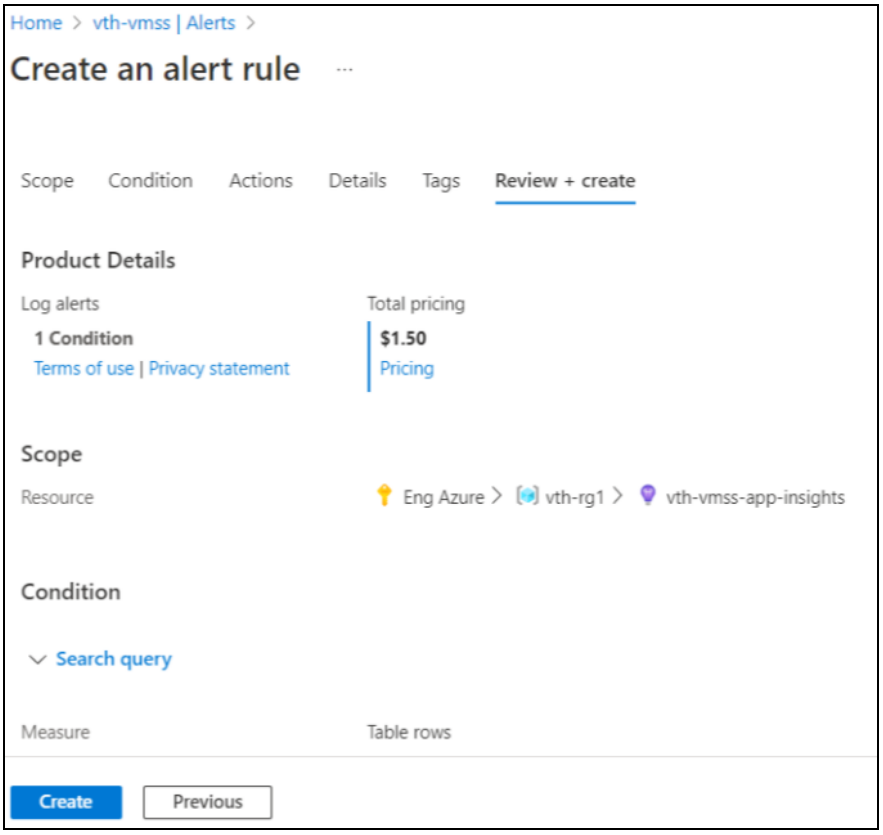
17. Click **Done** on Test <action_group_name>-alert window.
    The selected action group is displayed.
18. Close the selected action group window.
    The Create an alert rule - Actions window is displayed.
19. Click **Next : Details** at the bottom of the window.
    The **Create an alert rule** - **Details** window is displayed.

Figure 187 : Create an alert rule window - Details tab



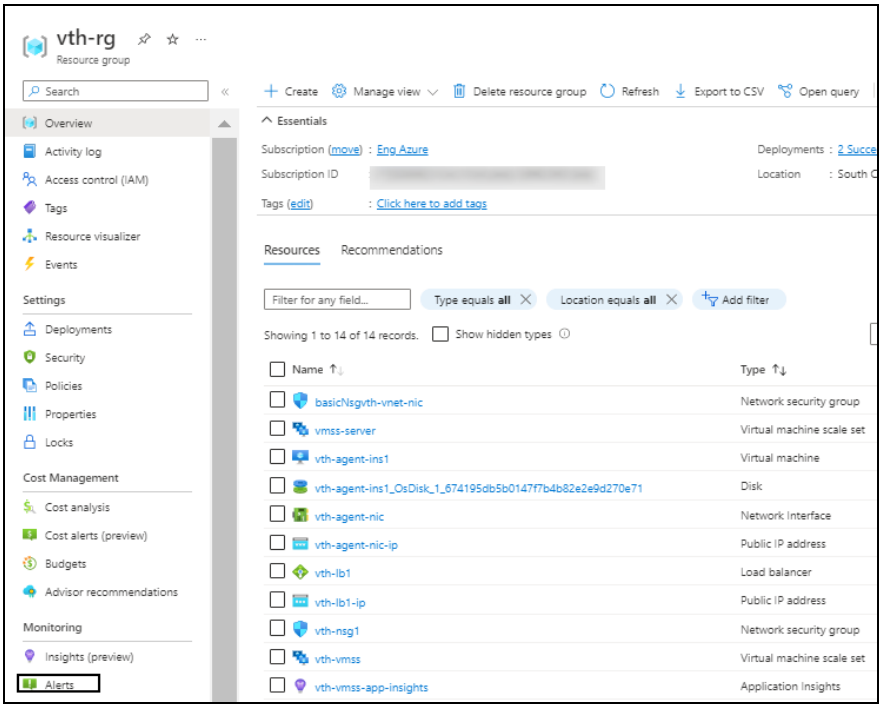
20. Enter the Alert rule name and provide the other mandatory details.
21. Skip the other tabs and click **Review + create** at the bottom of the window. The **Create an alert rule** - **Review + create** window is displayed.

Figure 188 : Create an alert rule window - Review + create tab



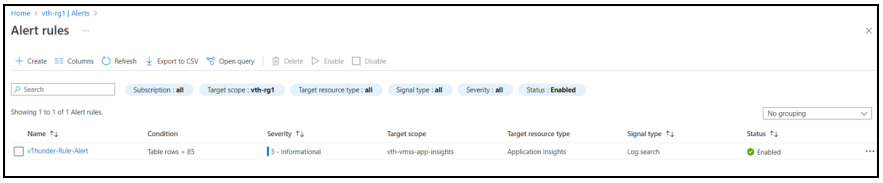
22. Click **Create**.
    The alert rule is created.
23. From **Home**, navigate to **Azure Services** > **Resource groups** > <resource_group_name>.
    The selected resource group - Overview window is displayed.

Figure 189 : Selected resource group - Overview window



24. Click **Alerts** from the left **Monitoring** panel.
    The selected alert window is displayed.
25. Click **Alert rules**.
    The alert rules for the selected resource group is displayed.

Figure 190 : Selected resource group - Alert rules window

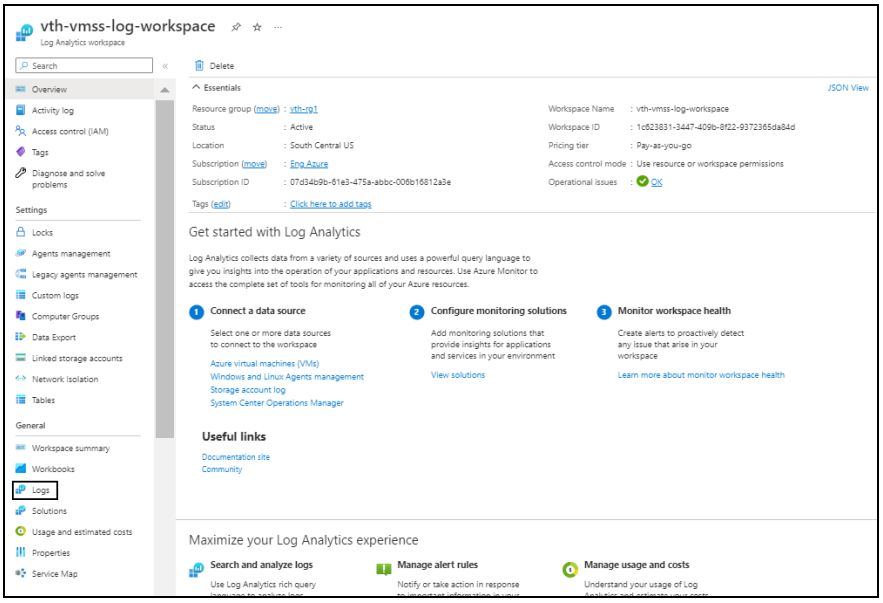


Verify Logs in Log Analytics Workspace

To verify the logs in log analytics workspace, perform the following steps:

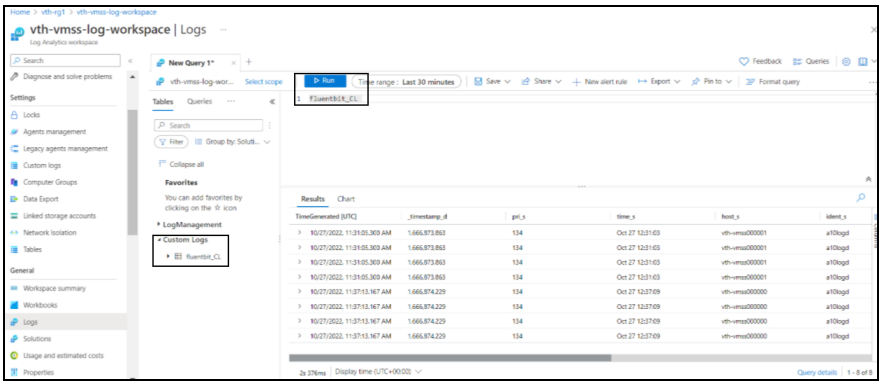
a. From **Home**, navigate to **Azure Services** > **Log Analytics workspaces** > <log_ workspace_name>.
   The selected log workspace - Overview window is displayed.

Figure 191 : Selected log workspace - Overview window



b. Click **Logs** from the left **General** panel.
The selected log window is displayed.

Figure 192 : Selected log analytics workspace - Logs window



c. Expand **Custom Logs** in the left **Tables** tab panel.

d. Double-click **fluentbit_CL**.
The fluentbi_CL query window is displayed.

e. Click **Run**.
All logs are displayed in tabular format with expandable details.

Verify Metrics in Application Insights

To verify if the metrics in application insights, perform the following steps:

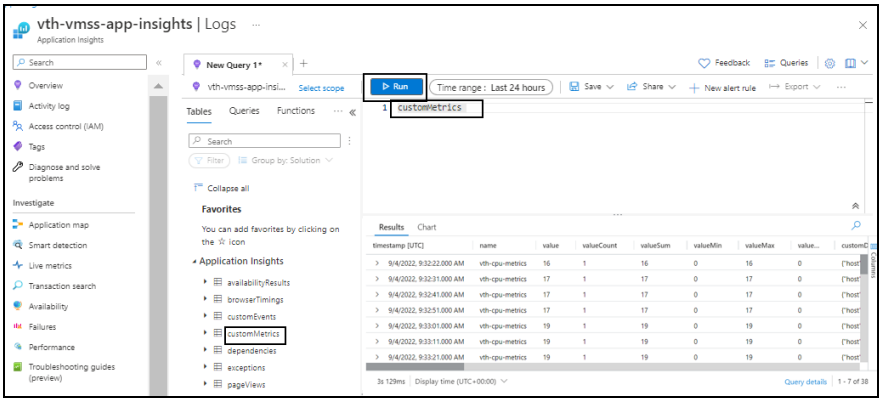
a. From **Home**, navigate to **Azure Services** > **Application Insights** > <application_ insight_name>.
The selected application insight - Overview window is displayed.

b. Click **Logs** from the left **Monitoring** panel.
The selected log query window is displayed.

c. Expand **Application Insights** in the left **Tables** tab panel.

d. Double-click **customMetrics**.
The customMetrics query window is displayed.

Figure 193 : Selected application insight - Logs window

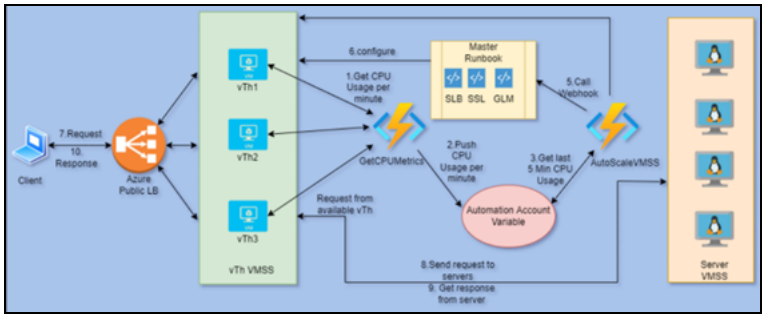


e. Click **Run**.
All logs are displayed in tabular format with expandable details. Each record is aggregated value for all vThunder instances. The **Value** field displays the data-CPU utilization percentage. Default interval is 60 seconds. This value is configured in telegraf agent of the agent instance.

Configure Autoscaling using Azure Functions Setup

Figure 194 shows the process flow when different Azure resources and system components are connected to each other in the 3NIC-NVM-VMSS Autoscaling using Azure Functions Setup.

Figure 194 : 3NIC-NVM-VMSS Autoscaling using Azure Functions Setup Process Flow



The following topics are covered:

- Initial Setup
- Create Autoscale Function
- Verify Autoscale Function Creation
- AutoScale Function On-demand Password Change

Initial Setup

To configure autoscaling using Azure functions setup, perform the following steps:

1. Navigate to the folder where you have downloaded the PowerShell template and open the PS_TMPL_3NIC_NVM_VMSS_FUNCTION_APP_PARAM.json with a text editor.
2. Configure function application name, application insight name, and subscription ID.

```
{
    "functionAppName": "vth-auto-func-app",
    "applicationInsightsName": "vth-vmss-app-insights",
    "subscriptionId": "07d3xxxx-xxxx-xxxx-xxxx-xxxxx6812a3e",
    "filePath": "AZURE_FUNCTIONS\\GetMetrics.zip",
    "vThUserName": "admin"
}
```

NOTE: Do not change the vThunder instance username.

You can get the application insight name from **Home** > **Azure Services** > **Application Insights**.

You can get subscription ID value from **Home** > **Azure Services** > **Subscriptions** > **Subscription name**.

Provide the absolute file path of the folder where you have downloaded the PowerShell template > **AZURE_FUNCTIONS** > **GetMetrics.zip**.

3. Verify if all the configurations in the PS_TMPL_3NIC_NVM_VMSS_FUNCTION_APP_PARAM.json file are correct and then save the changes.

Create Autoscale Function

To create autoscale function using CLI, perform the following steps:

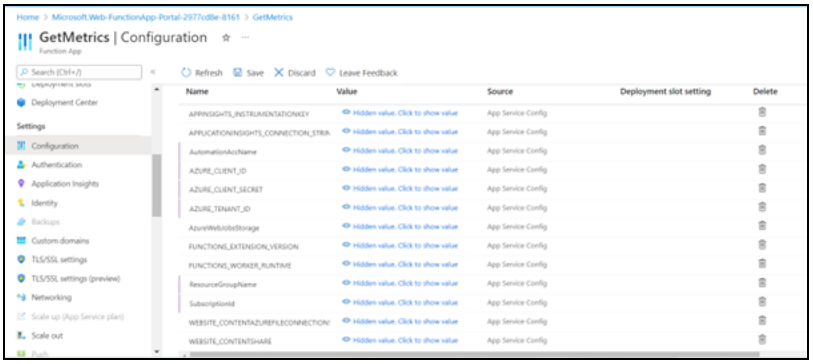
1. From Start menu, open PowerShell and navigate to the folder where you have downloaded the PowerShell template.
2. Run the following command to create autoscale function:
```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_NVM_VMSS_FUNCTION_APP_4.ps1
```
3. Provide the updated password of existing vThunder instances and then confirm the same password when prompted.

Verify Autoscale Function Creation

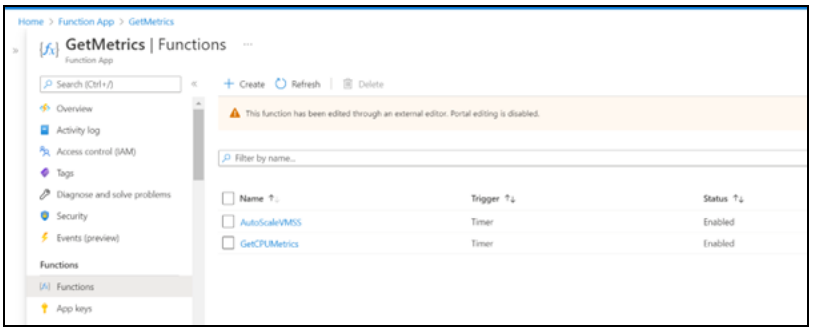
To verify autoscale function creation, perform the following steps:

1. From **Home**, navigate to **Azure Services** > **Function App**.
The Function App window is displayed.
2. Select GetMetrics function from the list.
The GetMetrics function - Overview window is displayed.
3. Click **Configuration** from the left **Settings** panel.
The GetMetrics function - Configuration window is displayed.

Figure 195 : GetMetrics function - Configuration window



4. Verify if all the function configurations are listed under Application settings.
5. Select **Functions** from left **Functions** panel.
   The GetMetrics function - Functions window is displayed.



6. Verify if **AutoScaleVMSS** and **GetCPUMetrics** functions are listed.
7. Click **GetCPUMetrics**.
   The GetCPUMetrics function - Overview window is displayed.
8. Click **Monitor** from the left **Developer** panel.
   The GetCPUMetrics function - Monitor window is displayed.

Figure 196 : GetCPUMetrics function - Monitor window

9. Verify if the logs are generated by the functions.

AutoScale Function On-demand Password Change

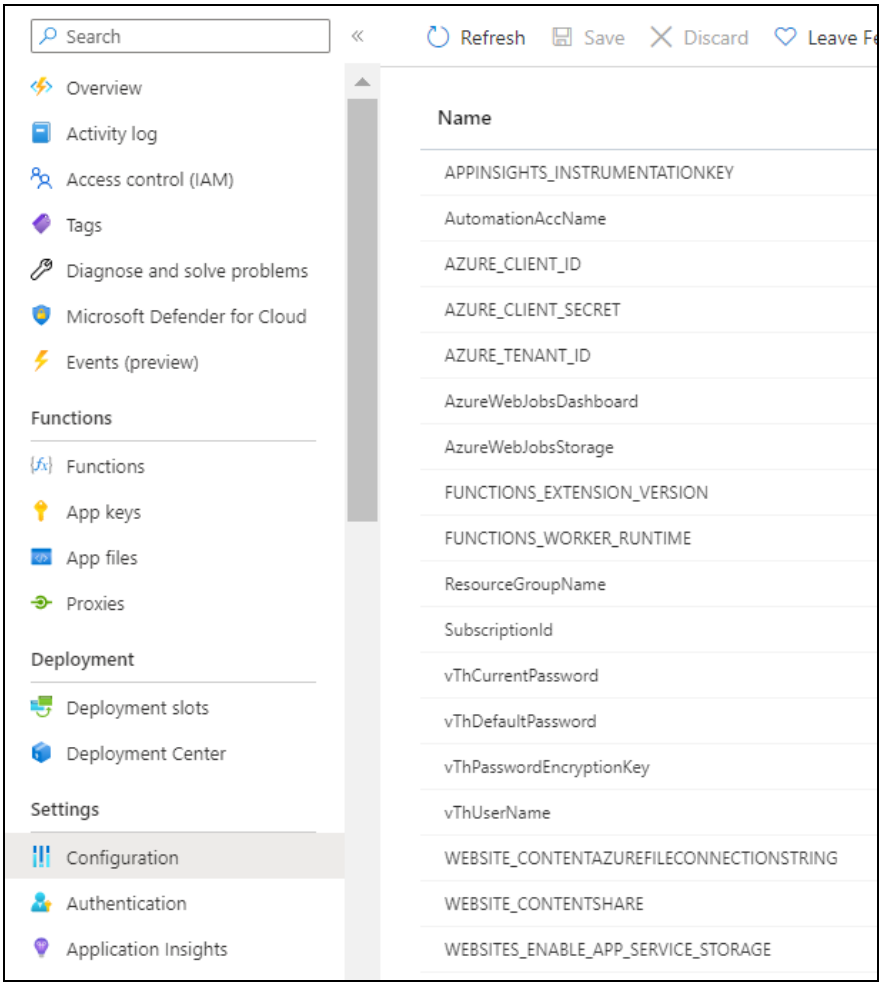
If you are changing the vThunder instance password using On-demand Password Change, perform the following steps else skip them:

1. Run the following script to get the encryption key and encrypted password:
```
PS C:\Users\TestUser\Templates> python .\utils\Encrypt_Password.py
```
2. Provide the recently updated password of existing vThunder instances and then confirm the same password when prompted:
```
Password:
Confirm Password:
<encrypted_key> <encrypted_password>
```
Figure 197 : Encrypted Key and Encrypted Password

The encrypted key and encrypted password are displayed.

3. From **Home**, navigate to **Azure Services** > **Function App** > **Settings** > **Configuration** and enter the encrypted key in the **vThPasswordEncryptionKey** field and encrypted password in the **vThCurrentPassword** value field.
The function starts using the password provided in the **vThCurrentPassword** field to get the metric data from VMSS vThunder instances.

Figure 198 : Configuration window



On-demand Password Change

The on-demand password change allows you to change the password for all the existing vThunder instances in the VMSS at one go.

To change the on-demand password, perform the following steps:

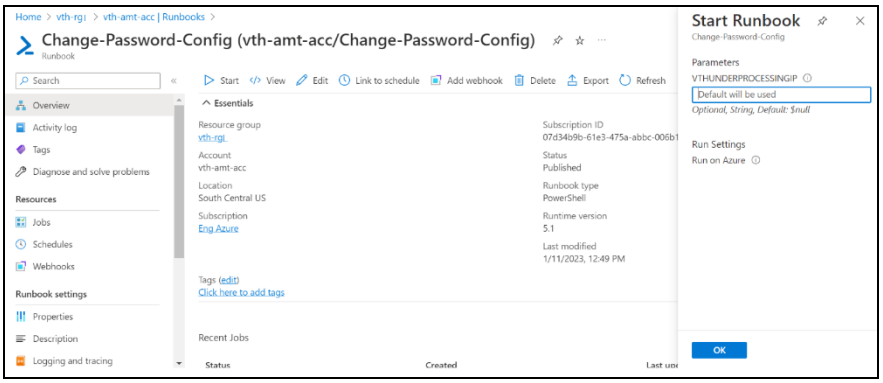
1. From **Home**, navigate to **Azure Services** > **Automation Accounts** > **Variables**.

   Figure 199 : On-demand Password Change Variables

vThNewPassApplyFlag	String	True
vThNewPassword	Unknown (encrypted)	**********

2. Set **vThNewPassApplyFlag** to **True**.
3. Update **vThNewPassword** with the new password.
4. Navigate to **Azure Services** > **Automation Accounts** > <automation_account_name> > **Runbooks**.
5. Select the **Change-Password-Config** runbook and click **Start**.
6. Leave the **vTHUNDERPROCESSINGIP** parameter empty so that it takes the default value.

   Figure 200 : Change-Password-Config runbook



7. Navigate to **Azure Services** > **Automation Accounts** > <automation_account_name> > **Jobs**.
8. Verify if the **Change-Password-Config** runbook job has completed status.
9. Navigate to **Azure Services** > **Automation Accounts** > **Variables**, verify if the **vThNewPassApplyFlag** flag is set to **False** after the execution of the Change-Password-Config runbook is successful. The **vThNewPassApplyFlag** flag should be set to false after the password is updated for all vThunder instances in VMSS.

If you are autoscaling using Azure Function setup, you need to also change the password in the autoscale function. For more information, see AutoScale Function On-demand Password Change.

Access vThunder using CLI or GUI

vThunder can be accessed using any of the following ways:

- Access vThunder using CLI
- Access vThunder using GUI

Access vThunder using CLI

To access the vThunder instances using CLI, perform the following steps:

1. Open PuTTY.
2. Enter or select the following basic information in the PuTTy Configuration window:
   - Hostname: Public IP of Virtual Machine Instance under the VMSS
     Here, Public IP of **`vth-vmss`**
   - Connection Type: SSH
3. Click **Open**.
4. In the active PuTTY session, login with the recently changed password:

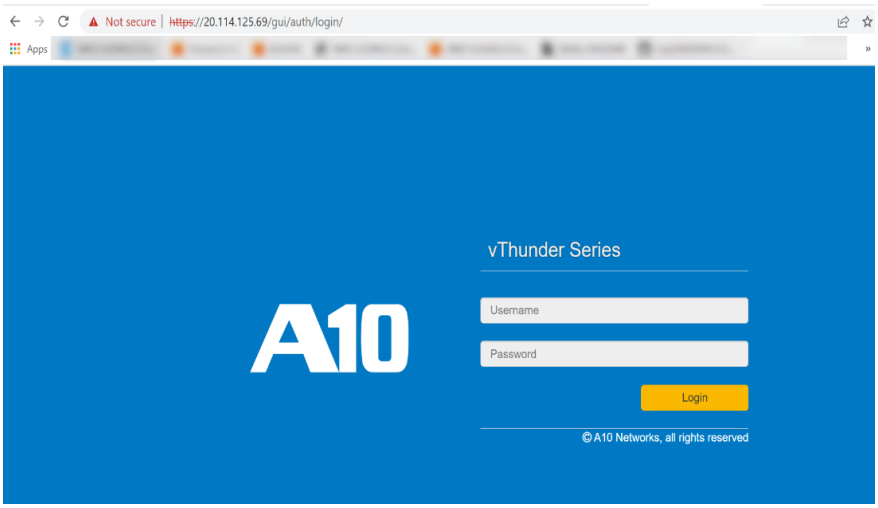
```
login as: xxxx <---Enter username provided by A10 Networks Support--->
Using keyboard-interactive authentication.
Password: xxxx <---Enter your password>
Last login: Day MM DD HH:MM:SS from a.b.c.d

System is ready now.

[type ? for help]

vThunder> enable <---Execute command--->
Password:<---just press Enter key--->
vThunder#config <---Configuration mode--->
```

Access vThunder using GUI

To access the vThunder instances using GUI, perform the following steps:

1. Open any browser.
2. Enter *https://<vthunder_public_IP>/gui/auth/login/* in the address bar.

   Figure 201 : vThunder GUI



3. Enter the username provided by A10 Networks Support and recently changed password.
   The home page gets displayed.

Verify Deployment

To verify deployment using the PowerShell template, perform the following steps:

1. Run the following command on vThunder:

```
vThunder(config)#show running-config slb
```

   If the deployment is successful, the following configuration is displayed:

```
!Section configuration: 711 bytes
!
slb server vth-server-vmss_0 10.0.3.5
  port 53 udp
       health-check-disable
  port 80 tcp
       health-check-disable
  port 443 tcp
```

```
       health-check-disable
!
slb service-group sg443 tcp
  health-check-disable
  member vth-server-vmss_0 443
!
slb service-group sg53 udp
  health-check-disable
  member vth-server-vmss_0 53
!
slb service-group sg80 tcp
  health-check-disable
  member vth-server-vmss_0 80
!
slb virtual-server vip use-if-ip ethernet 1
  port 53 udp
    ha-conn-mirror
    source-nat auto
    service-group sg53
  port 80 http
    source-nat auto
    service-group sg80
  port 443 https
    source-nat auto
    service-group sg443
!
slb virtual-server vip2 10.0.2.10
!
```

2. Run the following command on vThunder to verify the GLM License Provision configuration:

```
vThunder(config)#show license-info
```

If the master webhook is executed successfully, the following GLM configuration is displayed:

```
Host ID        : 5DCB01EC264BECCCFECB3C2ED42E02384EE8C527
USB ID         : Not Available
Billing Serials: A10f771cecbe0000
```

```
Token           : A10f771cecbe
Product         : ADC
Platform        : vThunder
Burst           : Disabled
GLM Ping Interval In Hours : 24
-----------------------------------------------------------------
Enabled Licenses Expiry Date (UTC)            Notes
-----------------------------------------------------------------
SLB              None
CGN              None
GSLB             None
RC               None
DAF              None
WAF              None
AAM              None
FP               None
WEBROOT          N/A         Requires an additional Webroot license.
THREATSTOP       N/A         Requires an additional ThreatSTOP license.
QOSMOS           N/A         Requires an additional QOSMOS license.
WEBROOT_TI       N/A         Requires an additional Webroot Threat Intel
license.
CYLANCE          N/A         Requires an additional Cylance license.
IPSEC_VPN        N/A         Requires an additional IPsec VPN license.
500 Mbps Bandwidth 14-November-2022
```

3. From vThunder Console, navigate to **Home** > **License History** to verify your license:

Figure 202 : License History

4. Run the following command on vThunder to verify the SSL Certificate configuration:

```
vThunder(config)#show pki cert
```

If the SSL Certificate configuration is correct and applied successfully, the following SSL configuration is displayed:

```
Name    Type                          Expiration  Status
-----------------------------------------------------------------
server certificate Jan 28 12:00:00 2028 GMT [Unexpired, Bound]
```

5. Run the following command to verify vThunder logs sync-up configuration:

```
vThunder(config)#show running-config acos-events
```

If the vThunder logs sync-up configuration is correct, the following configuration is displayed:

```
!Section configuration: 467 bytes
!
acos-events message-selector vThunderLog
  rule 1
    severity equal-and-higher debugging
!
acos-events log server fluentBitLogAgent 10.0.1.4
  health-check-disable
  port 514 udp
    health-check-disable
!
acos-events collector-group vThunderSyslog udp
  log-server fluentBitLogAgent 514
!
acos-events template fluentBitRemoteServer
  message-selector vThunderLog
    collector-group vThunderSyslog
!
acos-events active-template fluentBitRemoteServer
!
```

Verify Traffic Flow

To verify the traffic flow from client machine to server machine via vThunder, perform the following:

1. From **Azure Portal** > **Azure Services** > **Resource Group** > <resource_group_name> > <load_balancer> > **Settings** > **Frontend IP configuration**.
   Here, **`vth-lb1`** is the load balancer.

2. Copy the frontend IP address.

   Figure 203 : Load balancer frontend IP address

3. Select your client instance from the **Virtual machine** list.
   Here, **`vth-client`** is the client instance name.

4. SSH your client machine and run the following command to verify the traffic flow:

```
curl <vth-lb1-font-ip>
```

   Example

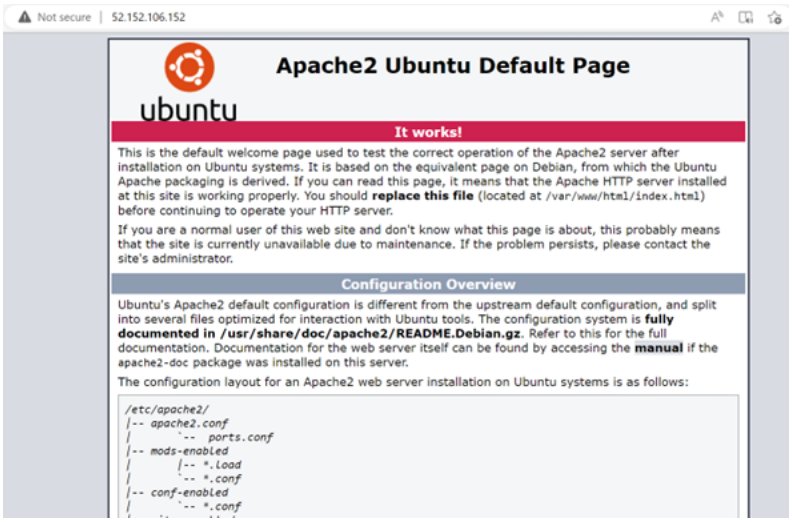
```
curl 52.152.106.152
```

   Verify if a response is received.

   or

   Copy the load balancer frontend IP address in the browser.

   Figure 204 : API response



   Verify if the API response is received.

Troubleshooting

Common Errors

While deploying the templates, you might encounter some errors or issues. The common errors and issues are listed below:

Unauthorized

This error is encountered when your credentials are incorrect or missing. Provide the correct credentials in the respective powershell script.

Given below is an example of the error:

```
Line |
149 |  … $response = Invoke-RestMethod -SkipCertificateCheck -Uri $Url -
Method …
     |
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
     | {   "response": {     "status": "fail",     "err": {
"code": 1208008960,       "from": "HTTP",       "msg": "Unauthorized"
 }   } }
```

The storage account named vthunderstorage already exists under the subscription.

This error is encountered if the storage account name is already in use. Provide a unique storage account name in the parameter json file.

Given below is an example of the error:

```
{"status":"Failed","error":{"code":"DeploymentFailed","message":"At
least one resource deployment operation failed. Please list deployment
operations for details. Please see https://aka.ms/DeployOperations for
usage details.","details":[{"code":"BadRequest","message":"{\r\n
\"error\": {\r\n    \"code\": \"DnsRecordInUse\",\r\n    \"message\":
\"DNS record vth-inst1.southcentralus.cloudapp.azure.com is already used
by another public IP.\",\r\n    \"details\": []\r\n  }\r\n}"},
{"code":"Conflict","message":"{\r\n  \"error\": {\r\n    \"code\":
```

```
\"StorageAccountAlreadyExists\",\r\n    \"message\": \"The storage
account named vthunderstorage already exists under the
subscription.\"\r\n  }\r\n}"}]}}
```

Cannot bind argument to parameter 'Container' because it is null

This error is encountered if the 'server.pem' is not available at the mentioned path or if the path format is incorrect. Provide a correct path of the 'server.pem' in the parameter json file.

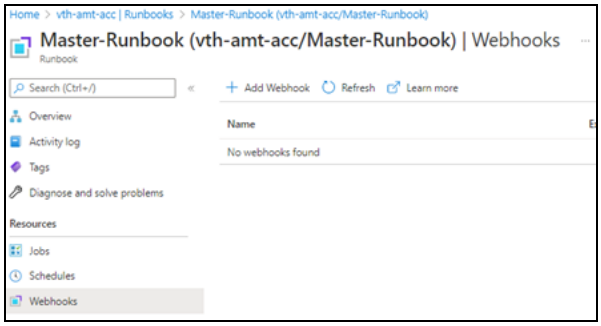
Given below is an example of the error:

```
Set -AzStorageBlobContent @blobSSL
Cannot bind argument to parameter 'Container' because it is null.
```

Cannot validate argument on parameter 'Uri'

This error is encountered if webhook URL is not configured or it already exists. Delete 'master-webhook' from **Azure Portal** > **Automation Account** > **Runbooks** and ensure it is empty before the running webhook script.

Figure 205 : Master Runbook



Given below is an example of the error:

```
... -Invoke-WebRequest -Method POst -Uri $webHookURL.WebhookURI -UseBas
...
Cannot validate argument on parameter 'Uri'. The argument is null or
empty. Provide an argument that is not null or empty, and then try the
command again.
```

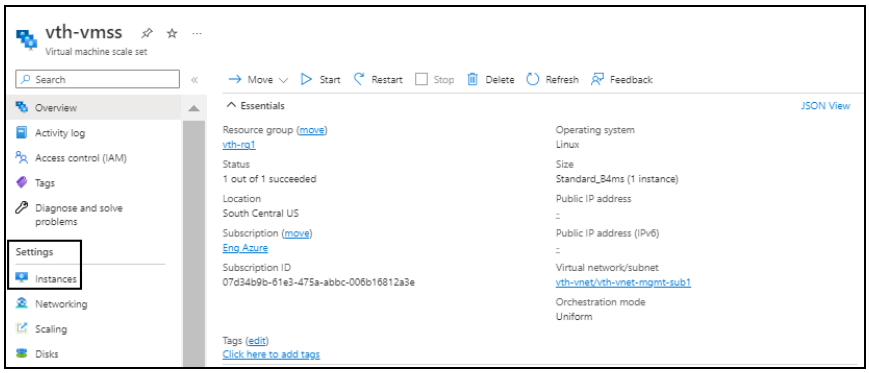
Runbook Job failed or not working

If the Runbook job has failed or is not working, re-run the master runbook.

To re-run the master runbook, perform the following steps:

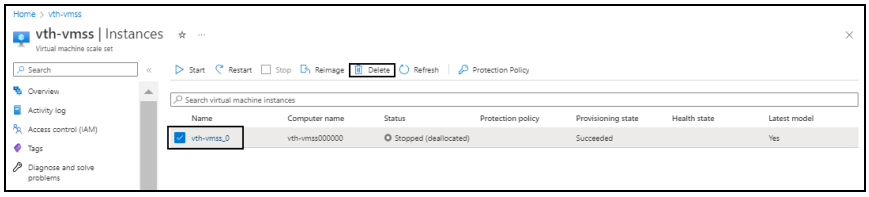
1. From **Azure Portal**, navigate to **Azure Services** > **Virtual machine scale sets** > <vmss_name>.
   The selected vmss - Overview window is displayed.

   Figure 206 : Selected vmss - Overview window



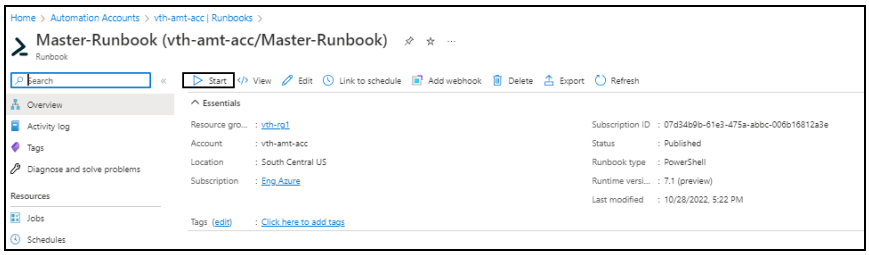
2. Click **Instances** from the left **Settings** panel.
   The selected vmss - Instances window is displayed.

   Figure 207 : Selected vmss - Instances window



3. Click **Delete** to delete all the vmss instances.
4. From the Master-Runbook Job window, click **Start** to re-run the master runbook.

   Figure 208 : Master-Runbook Job window



NOTE: It may take the system a few minutes to display the completed status.

5. Verify if all the runbook jobs have completed status.

Appendix

List of Custom Role Permissions

The following is the list of custom role permissions:

```
"Microsoft.Automation/automationAccounts/variables/read",
"Microsoft.Automation/automationAccounts/variables/write",
"Microsoft.Automation/automationAccounts/variables/delete",
"Microsoft.Automation/automationAccounts/runbooks/read",
"Microsoft.Automation/automationAccounts/runbooks/content/read",
"Microsoft.Automation/automationAccounts/jobs/write",
"Microsoft.Automation/automationAccounts/jobSchedules/write",
"Microsoft.Automation/automationAccounts/jobs/read",
"Microsoft.Automation/automationAccounts/jobs/output/read",
"Microsoft.Automation/automationAccounts/runbooks/operationResults/read",
"Microsoft.Automation/automationAccounts/jobs/streams/read",
"Microsoft.Automation/automationAccounts/jobSchedules/read",
"Microsoft.OperationalInsights/workspaces/sharedKeys/action",
"Microsoft.OperationalInsights/workspaces/read"

"Microsoft.Compute/virtualMachineScaleSets/read",
"Microsoft.Compute/virtualMachineScaleSets/write",
"Microsoft.Compute/virtualMachineScaleSets/delete",
"Microsoft.Compute/virtualMachineScaleSets/delete/action",
"Microsoft.Compute/virtualMachineScaleSets/start/action",
"Microsoft.Compute/virtualMachineScaleSets/powerOff/action",
"Microsoft.Compute/virtualMachineScaleSets/restart/action",
"Microsoft.Compute/virtualMachineScaleSets/deallocate/action",
"Microsoft.Compute/virtualMachineScaleSets/scale/action",
"Microsoft.Compute/virtualMachineScaleSets/networkInterfaces/read",
"Microsoft.Compute/virtualMachineScaleSets/publicIPAddresses/read",

"Microsoft.Compute/virtualMachineScaleSets/providers/Microsoft.Insights/l
ogDefinitions/read",
```

```
"Microsoft.Compute/virtualMachineScaleSets/providers/Microsoft.Insights/diagnosticSettings/read",

"Microsoft.Compute/virtualMachineScaleSets/providers/Microsoft.Insights/diagnosticSettings/write",
"Microsoft.Compute/virtualMachineScaleSets/instanceView/read",
"Microsoft.Compute/virtualMachineScaleSets/skus/read",


"Microsoft.Compute/virtualMachineScaleSets/providers/Microsoft.Insights/metricDefinitions/read",
"Microsoft.Compute/virtualMachineScaleSets/vmSizes/read",
"Microsoft.Compute/virtualMachineScaleSets/virtualMachines/read",
"Microsoft.Compute/virtualMachineScaleSets/virtualMachines/write",
"Microsoft.Compute/virtualMachineScaleSets/virtualMachines/delete",
"Microsoft.Compute/virtualMachineScaleSets/virtualMachines/start/action",

"Microsoft.Compute/virtualMachineScaleSets/virtualMachines/powerOff/action",

"Microsoft.Compute/virtualMachineScaleSets/virtualMachines/restart/action",

"Microsoft.Compute/virtualMachineScaleSets/virtualMachines/deallocate/action",

"Microsoft.Compute/virtualMachineScaleSets/virtualMachines/instanceView/read",

"Microsoft.Compute/virtualMachineScaleSets/virtualMachines/networkInterfaces/read",

"Microsoft.Compute/virtualMachineScaleSets/virtualMachines/networkInterfaces/ipConfigurations/read",

"Microsoft.Compute/virtualMachineScaleSets/virtualMachines/networkInterfaces/ipConfigurations/publicIPAddresses/read",
```

```
"Microsoft.Compute/virtualMachineScaleSets/virtualMachines/providers/Micro
soft.Insights/metricDefinitions/read",

"Microsoft.Compute/locations/vmSizes/read",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/powerOff/action",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/restart/action",

"Microsoft.Compute/virtualMachines/providers/Microsoft.Insights/logDefinit
ions/read",

"Microsoft.Compute/virtualMachines/providers/Microsoft.Insights/diagnostic
Settings/read",

"Microsoft.Compute/virtualMachines/providers/Microsoft.Insights/diagnostic
Settings/write",
"Microsoft.Compute/virtualMachines/instanceView/read",

"Microsoft.Compute/virtualMachines/providers/Microsoft.Insights/metricDefi
nitions/read",
"Microsoft.Compute/virtualMachines/vmSizes/read",

"Microsoft.Network/operations/read",

"Microsoft.Network/loadBalancers/read",
"Microsoft.Network/loadBalancers/write",
"Microsoft.Network/loadBalancers/delete",
"Microsoft.Network/loadBalancers/backendAddressPools/read",
"Microsoft.Network/loadBalancers/backendAddressPools/write",
"Microsoft.Network/loadBalancers/backendAddressPools/delete",
"Microsoft.Network/loadBalancers/backendAddressPools/join/action",

"Microsoft.Network/loadBalancers/backendAddressPools/backendPoolAddresses/
read",
```

```
"Microsoft.Network/loadBalancers/providers/Microsoft.Insights/diagnosticSettings/read",

"Microsoft.Network/loadBalancers/providers/Microsoft.Insights/diagnosticSettings/write",
"Microsoft.Network/loadBalancers/frontendIPConfigurations/read",
"Microsoft.Network/loadBalancers/frontendIPConfigurations/join/action",

"Microsoft.Network/loadBalancers/frontendIPConfigurations/loadBalancerPools/read",

"Microsoft.Network/loadBalancers/frontendIPConfigurations/loadBalancerPools/write",

"Microsoft.Network/loadBalancers/frontendIPConfigurations/loadBalancerPools/delete",

"Microsoft.Network/loadBalancers/frontendIPConfigurations/loadBalancerPools/join/action",
"Microsoft.Network/loadBalancers/inboundNatPools/read",
"Microsoft.Network/loadBalancers/inboundNatPools/join/action",
"Microsoft.Network/loadBalancers/inboundNatRules/read",
"Microsoft.Network/loadBalancers/inboundNatRules/write",
"Microsoft.Network/loadBalancers/inboundNatRules/delete",
"Microsoft.Network/loadBalancers/inboundNatRules/join/action",
"Microsoft.Network/loadBalancers/loadBalancingRules/read",

"Microsoft.Network/loadBalancers/providers/Microsoft.Insights/logDefinitions/read",
"Microsoft.Network/loadBalancers/networkInterfaces/read",
"Microsoft.Network/loadBalancers/outboundRules/read",
"Microsoft.Network/loadBalancers/probes/read",
"Microsoft.Network/loadBalancers/probes/join/action",
"Microsoft.Network/loadBalancers/virtualMachines/read",

"Microsoft.Network/loadBalancers/providers/Microsoft.Insights/metricDefinitions/read",
```

```
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/defaultSecurityRules/read",
"Microsoft.Network/networkSecurityGroups/securityRules/read",
"Microsoft.Network/networkSecurityGroups/securityRules/write",
"Microsoft.Network/networkSecurityGroups/securityRules/delete",

"Microsoft.Network/publicIPAddresses/read",
"Microsoft.Network/publicIPAddresses/write",
"Microsoft.Network/publicIPAddresses/delete",

"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/write",
"Microsoft.Network/virtualNetworks/delete",

"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.Network/virtualNetworks/subnets/delete",

"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
"Microsoft.Network/virtualNetworks/virtualMachines/read",

"Microsoft.Network/virtualNetworkGateways/read",
"Microsoft.Network/virtualNetworkGateways/write",
"Microsoft.Network/virtualNetworkGateways/delete",
"microsoft.network/virtualNetworkGateways/natRules/read",
"microsoft.network/virtualNetworkGateways/natRules/write",
"microsoft.network/virtualNetworkGateways/natRules/delete",

"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkInterfaces/delete",

"Microsoft.Network/networkProfiles/read",
"Microsoft.Network/networkProfiles/write",
"Microsoft.Network/networkProfiles/delete",
```

```
"Microsoft.Network/networkInterfaces/ipconfigurations/read",


"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/networkInterfaces/ipconfigurations/join/action",
"Microsoft.Network/publicIPAddresses/join/action",
"Microsoft.Network/virtualNetworks/join/action",
```

Azure Service Application Access Key

The Azure service application access key is required to access the Azure resources.

The following topics are covered:

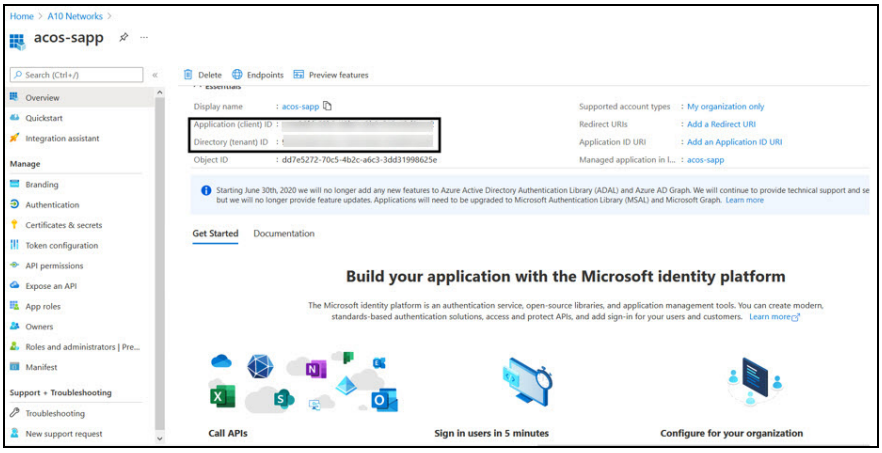
- Use an existing Access Key
- Create a new Access Key

Use an existing Access Key

To use an existing Azure service application access key, perform the following steps:

1. From **Azure Portal**, navigate to **Azure Services** > **Azure Active Directory** > **App Registration**.
   The list of service applications are displayed under **Owned applications** tab.
2. If you are the owner of the required service application, the required service application would be listed under the **Owned applications** tab. If not, perform the below steps with Administrator privileges:
   a. Select **Owners** from the left **Manage** panel.
      The Owners window appears.
   b. Select **Add** to get a list of user accounts.
   c. Search and select your user account.
   d. Click **Select** to add the user account to your owned application.
3. Select your service application from the list of applications.
   The selected service application window is displayed.

Figure 209 : Selected Service application window



4. Copy and save the Client ID, Tenant ID from the service application window.

```
client_id= 'cc4c86xx-65b3-48xx-a3xx-610cxxxxxxxx'
tenant_id= '91d27axx-8cxx-41xx-82xx-3d1bxxxxxxxx'
```

Create a new Access Key

To create a new Azure service application access key, perform the following steps with Administrator privileges:

1. Create a Role
2. Register a Service Application
3. Associate Service Application with a Role
4. Create Certificate and Secrets
5. Collect Azure Access Key
6. Import Azure Access Key

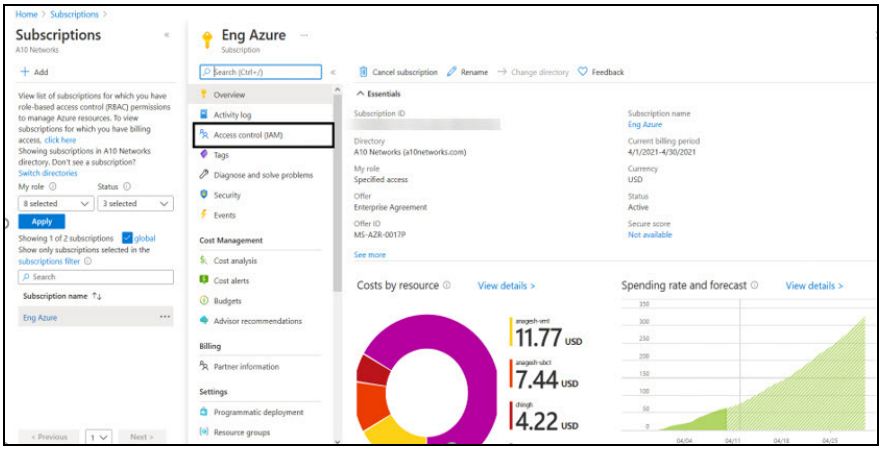
Create a Role

To create a custom role, perform the following steps:

1. From **Home**, navigate to **Azure Services** > **Subscriptions** > <subscription_name>. The selected Subscription - Overview window is displayed. Here, the subscription

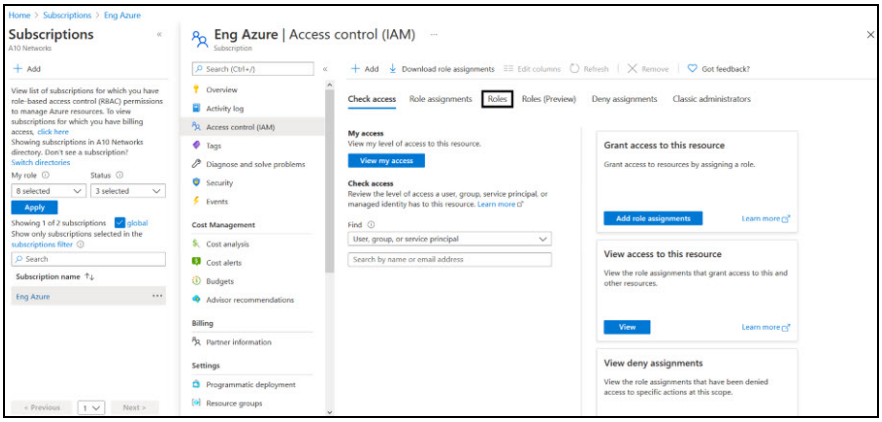
is Eng Azure.

Figure 210 : Subscriptions - Overview window



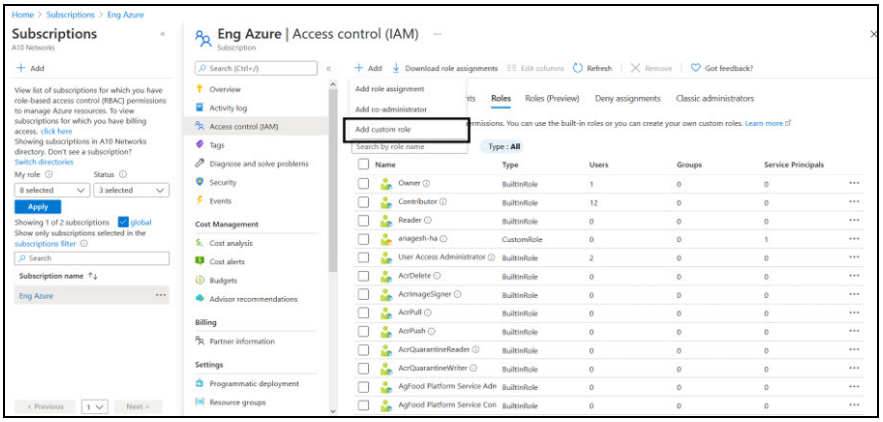
2. Click **Access control (IAM)** from left panel.
   The selected Subscription - Access control (IAM) window is displayed.
3. Select the **Roles** tab.
   The Roles window is displayed.

Figure 211 : Access Control - Role Window



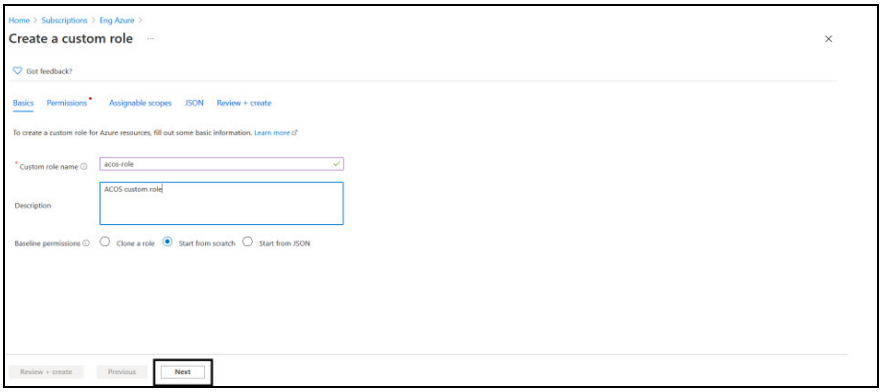
4. Click **Add** to select **Add custom role** option.
   The Create a custom role window is displayed.

Figure 212 : Add custom role window



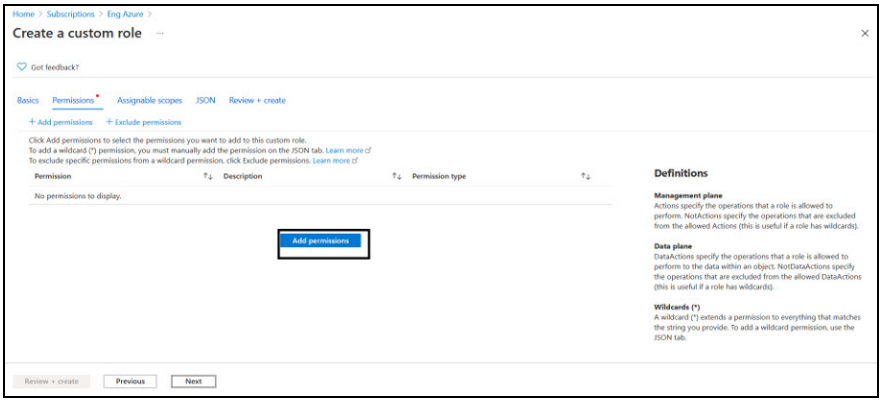
5. Enter **Customer role name** and **Description** (optional) in the **Basics** tab.

Figure 213 : Create a custom role window



6. Click **Next** at the bottom of the window.
The Permissions window is displayed.

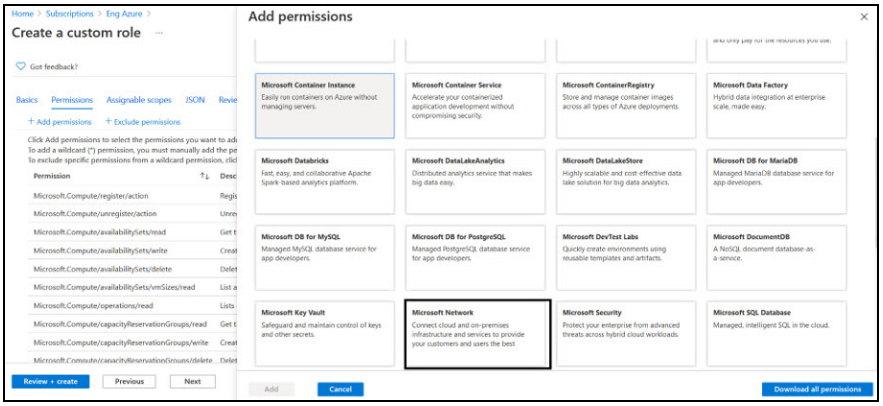
Figure 214 : Permission window



7. Click **Add Permissions** to add permissions to the custom role.

   The Add Permissions window is displayed.

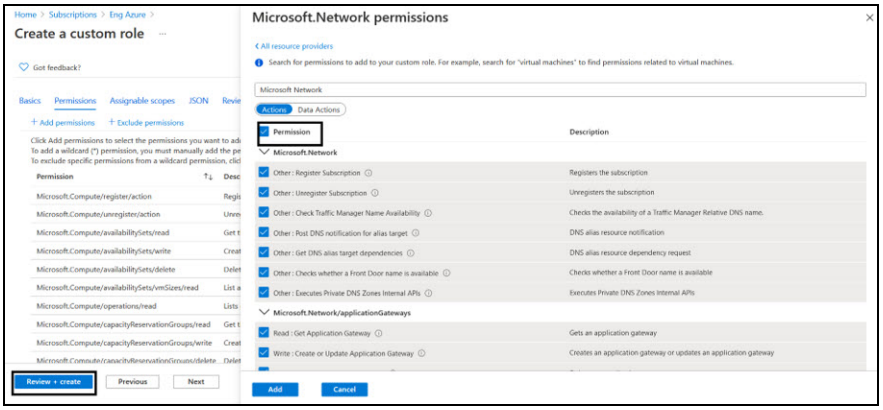
   Figure 215 : Add permissions window



6. Search the following permission groups from the Add Permissions window and select the corresponding permissions listed in the List of Custom Role Permissions:

   - Microsoft Automation
   - Microsoft Operational Insights
   - Microsoft Compute
   - Microsoft Network

Figure 216 : Microsoft Network permissions window



The selected permissions are listed under **Create a custom role** > **Permissions** tab.

8. Click **Review + create** at the bottom of the window to skip the other tabs.
   The **Create a custom role** confirmation window is displayed.

9. Click **OK** to successfully create the custom role with permissions.

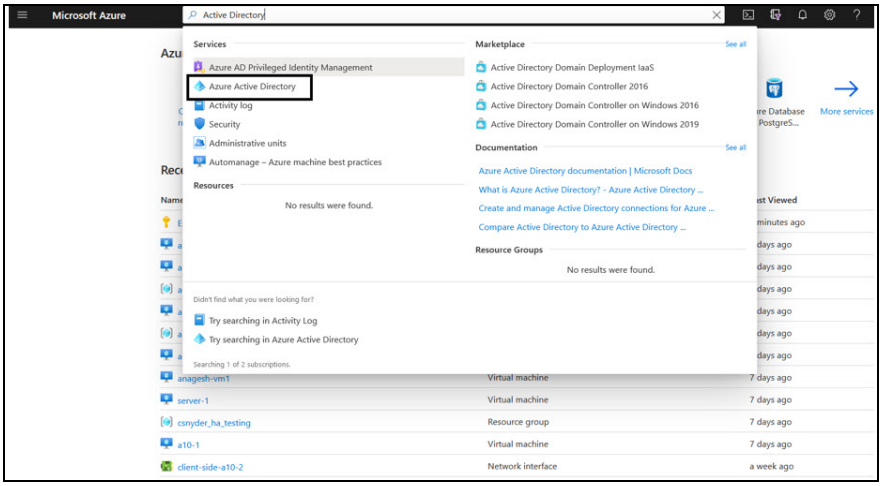
NOTE: It may take the system a few minutes to display your role everywhere.

Register a Service Application

To register a service application, perform the following steps:

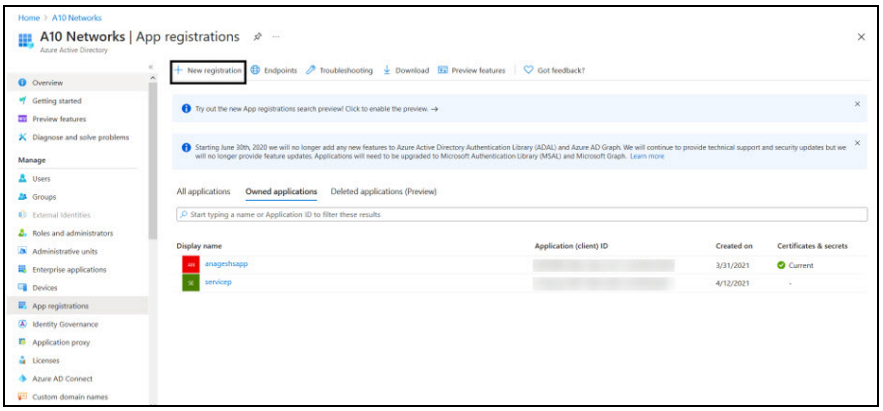
1. From **Home**, navigate to **Azure Services** > **Azure Active Directory** option.

   Figure 217 : Azure Active Directory window



2. On the Azure Active Directory window, click **App registrations** menu option from the left **Manage** panel.
   The App registration window to register an application is displayed.

   Figure 218 : App registrations window



3. Click **New Registration**.
   The Register an application window is displayed.

Figure 219 : Register an application window

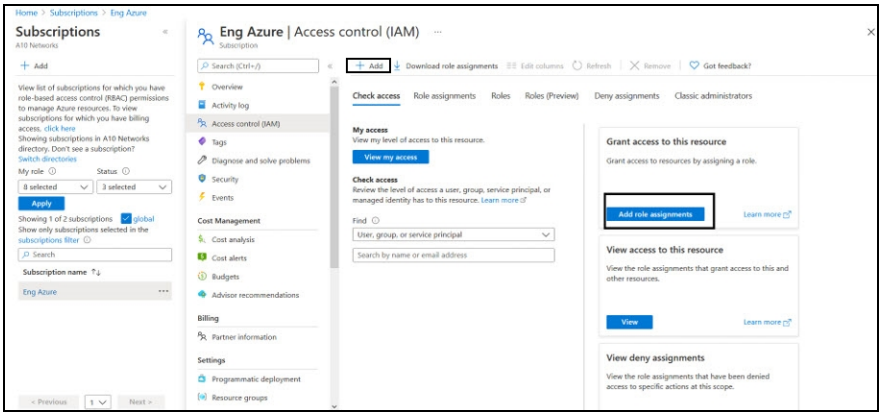
4. Enter the **Name** of the application. For example, acos-sapp.
5. Click **Register** to register the application. The application gets listed under Azure Active Directory - Apps registrations window.

Associate Service Application with a Role

To associate service application with a role, perform the following steps:

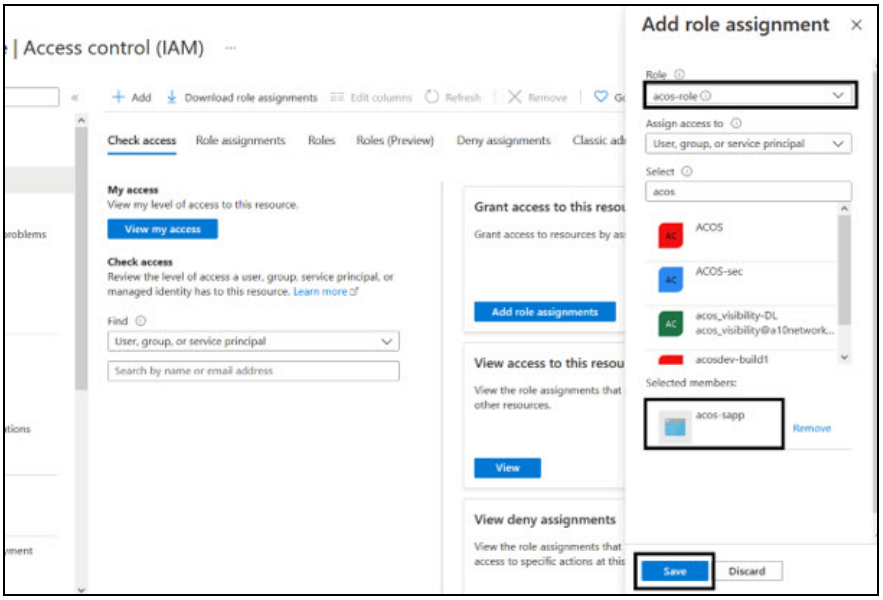
1. From **Home**, navigate to **Azure Services** > **Subscriptions** > <subscription_name>. The selected Subscription - Overview window is displayed. Here, the subscription is Eng Azure.
2. Click **Access control (IAM)** from left panel.
   The selected Subscription - Access control (IAM) window is displayed.

Figure 220 : Subscription - Access control (IAM) window



3. To assign a role to the above scope, click **Add** from the main menu options. The Add role assignment window is displayed.

Figure 221 : Add a role assignment -1



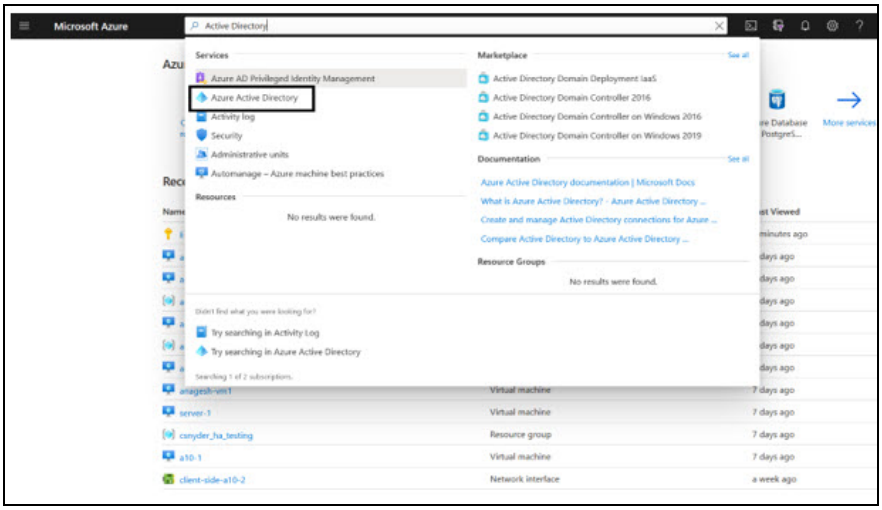
4. Select a **Role** from the drop-down list. For example, acos-role.
5. Select the required **Assign Access to** option from the drop-down list.
6. Enter a string to search and select for a name or email address. For example, acos.
7. Click the **Save** button to save the configuration.

Create Certificate and Secrets

To create certificate and secrets for the assigned role, perform the following steps:

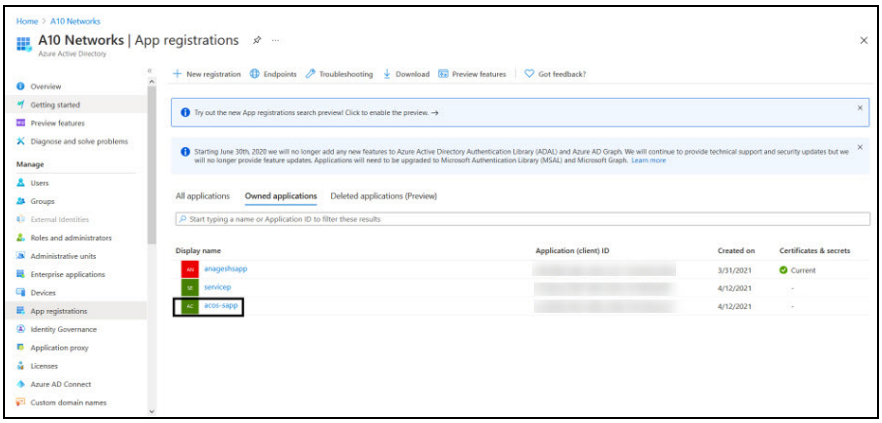
1. From **Home**, navigate to **Azure Services** > **Azure Active Directory** option.

   Figure 222 : Azure Active Directory - Overview window



2. On the Azure Active Directory - Overview window, click **App registrations** menu option from the left panel.
   The App registration window with a registered application(s) is displayed.

   Figure 223 : App registrations - Overall applications window



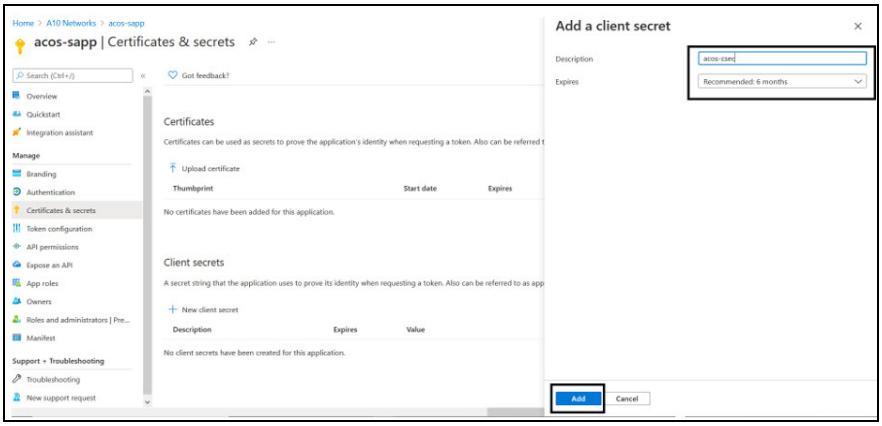
3. Select a service application from list of applications.
   The selected service application window is displayed.

4. Select the **Certificates & secrets** option from the left Manage navigation pane.
   The acos sapp - Certificates & secrets window is displayed.

5. Browse and upload certificates.

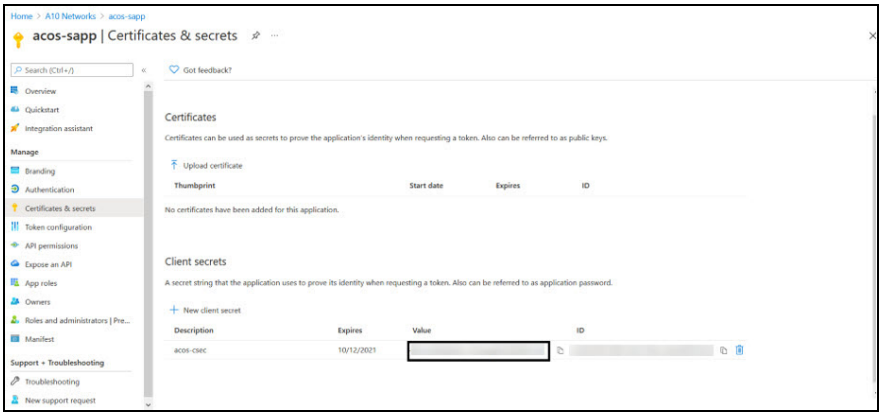
6. Select the **Start date** and **Expires** date from the date picker or click the **New client secret** button.
   The Add a client secret window is displayed.

   Figure 224 : Add a client secret window



7. Enter the New client secret **Description**, **Expires** value.
   The entered value is displayed on the acos-Certificates & secrets window.

   Figure 225 : acos-sapp Certificates & secrets window



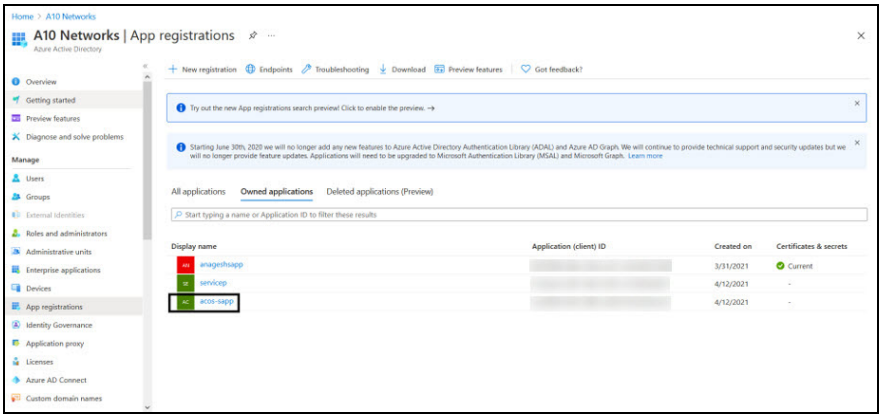
NOTE: Save the new client secret value in a text file, as it is not visible once the window is refreshed.

Collect Azure Access Key

To collect Azure access keys, perform the following steps:

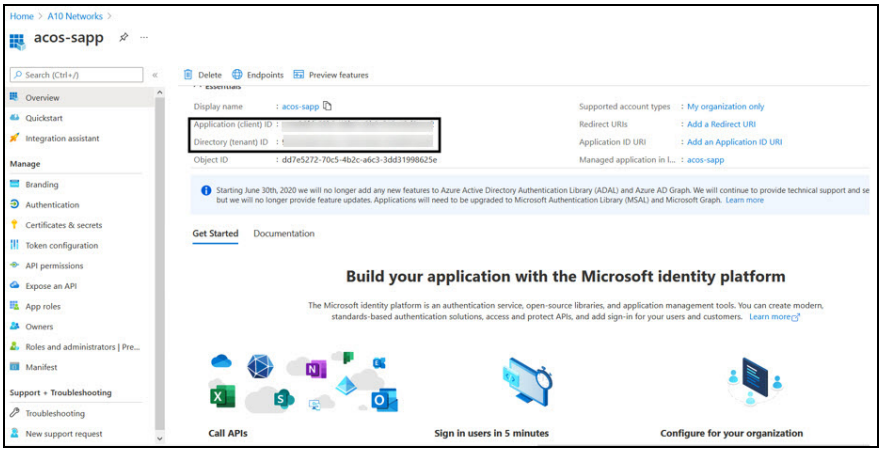
1. From **Home**, navigate to **Azure Services** > **Azure Active Directory** > **App registrations**.

Figure 226 : Azure Active Directory - App registrations window



2. From the **Owned applications** tab, select service application from the list of applications.
The selected service application window is displayed.

Figure 227 : Selected Service application window

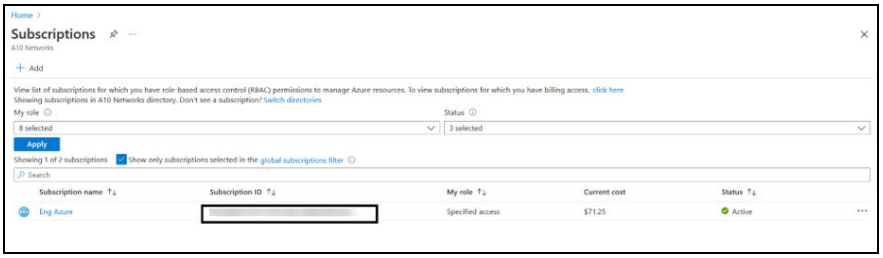


3. Copy the Client ID, Tenant ID from the service application window.

```
client_id= 'cc4c86xx-65b3-48xx-a3xx-610cxxxxxxxx'
tenant_id= '91d27axx-8cxx-41xx-82xx-3d1bxxxxxxxx'
```

4. Navigate to the **Home** > **Subscriptions** > **Registered Subscription Name**, and copy subscription ID value.

Figure 228 : Subscriptions window



5. Create a text file having subscription, client_id, client_secret, and tenant_id information as shown below:

```
subscription='07d34bxx-61xx-47xx-abxx-006bxxxxxxxx'
client_id='cc4c86xx-65xx-48xx-a3xx-610cxxxxxxxx'
client_secret='G0x_hVDzZxxxx-o1Vsw.xxxx.Zxxxx-xx'
tenant_id='91d2xxxx-8xxe-41xx-82xx-3d1bxxxxxxxx'
```

Import Azure Access Key

Each vThunder instance requires a copy of the Azure Access key and so it should be imported using the file transfer protocol methods.

To import the Azure access key, perform the following steps:

1. Log in to the vThunder instance.
2. Go to the config mode.

```
vThunder> enable
Password:
vThunder# config
```

3. Go to the admin mode.

```
vThunder(config)#admin ?
  admin
  NAME<length:1-31>  System admin user name
vThunder(config)#admin admin
```

4. Import the Azure Access key by using any of the file transfer methods recommended.

```
vThunder(config-admin:admin)#azure-cred import ?
  use-mgmt-port  Use management port as source port
```

```
  tftp:          Remote file path of tftp: file system(Format:
tftp://host/file)
  ftp:           Remote file path of ftp: file system(Format:
                 ftp://[user@]host[:port]/file)
  scp:           Remote file path of scp: file system(Format:
                 scp://[user@]host/file)
  sftp:          Remote file path of sftp: file system(Format:
                 sftp://[user@]host/file)
```

To delete the key, use the following command:

```
vThunder-Active(config-admin:admin)(NOLICENSE)#azure-cred delete 0
```

To verify the imported Azure Access keys, use the following commands:

```
vThunder-Active(config)(NOLICENSE)#admin ad
vThunder-Active(config)(NOLICENSE)#admin admin
vThunder-Active(config-admin:admin)(NOLICENSE)#azure-cred import
scp://username@<ip-addr>:/<file-path>/cred.txt
vThunder-Active(config-admin:admin)(NOLICENSE)#azure-cred sh
vThunder-Active(config-admin:admin)(NOLICENSE)#azure-cred show
SUB_ID = 'dfe16a52-xxxx-xxxx-a168-91767a54c0Ce'
client_id = 'b8d52c6f-xxxx-xxxx-bafd-e03cc942aa66'
secret = '****_XGEd9u0Or+M2Css=********-0b'
tenant = '1e94d773-****-****-b25d-3b3e1b64948d'
vThunder-Active(config-admin:admin)(NOLICENSE)#
```

Default Password Policy

The default password policy has the following criteria:

- The password should be at least nine characters in length.
- The password should contain at least one number, an uppercase letter (English), a lowercase letter (English), and a special character.
- The password should have at least one letter or number different from the previous password.
- The password should not contain its corresponding username with the same capitalization of letters.

- The password should not contain repeated characters of the same letter or number with the same capitalization of letters.
- The password should not contain the sequential row keyboard input of four letters or numbers with the same capitalization of letters.

Contact Us

©2023 A10 Networks, Inc. All rights reserved. A10 Networks, the A10 Networks logo, ACOS, A10 Thunder, Thunder TPS, A10 Harmony, SSLi and SSL Insight are trademarks or registered trademarks of A10 Networks, Inc. in the United States and other countries. All other trademarks are property of their respective owners. A10 Networks assumes no responsibility for any inaccuracies in this document. A10 Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. For the full list of trademarks, visit: www.a10networks.com/company/legal/trademarks/.