



Installing vThunder ADC using PowerShell Templates

Version 1.0.0

November, 2022

© 2022 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	12
Prerequisites	14
Image Repository	15
Get Started	16
PowerShell Templates	17
Deploy PowerShell Template 2NIC-1VM	18
System Requirements	18
Supported VM Sizes	21
Create vThunder Instance	22
Initial Setup	22
Deploy vThunder	25
Configure vThunder as an SLB	26
Initial Setup	26
Deploy vThunder as an SLB	30
Access vThunder using CLI or GUI	31
Access vThunder using CLI	31
Access vThunder using GUI	32
Verify Deployment	32
Deploy PowerShell Template 2NIC-1VM-GLM	35
System Requirements	35
Supported VM Sizes	38
Create vThunder Instance	39
Initial Setup	39
Deploy vThunder	42
Configure vThunder as an SLB	43
Initial Setup	43
Deploy vThunder as an SLB	47

Configure vThunder GLM	48
Initial Setup	48
Apply GLM License	48
Access vThunder using CLI or GUI	49
Access vThunder using CLI	49
Access vThunder using GUI	50
Verify Deployment	51
Deploy PowerShell Template 3NIC-2VM-HA	54
System Requirements	54
Create vThunder Instances	58
Initial Setup	58
Deploy vThunder	62
Configure Server and Client Machine	63
Create a Server Machine	63
Create a Client Machine	73
Configure vThunder as an SLB	81
Initial Setup	81
Deploy vThunder as an SLB	85
Configure High Availability	87
Configure High Availability for vThunder	87
Initial Setup	87
Create High Availability for vThunder	89
Access vThunder using CLI or GUI	90
Access vThunder using CLI	90
Access vThunder using GUI	91
Verify Deployment	92
Deploy PowerShell Template 3NIC-2VM-HA-GLM-PUBVIP-BACKAUTO	95
System Requirements	96
Supported VM Sizes	100
Create vThunder Instances	101

Initial Setup	101
Deploy vThunder	104
Configure Server VMSS	106
Create a Server Machine	106
Verify the Server VMSS Creation	113
Configure Automation Account	114
Create Automation Account	114
Initial Setup	114
Create an Automation Account	116
Verify the Automation Account creation	116
Create Runbook	117
Create Automation Account Webhook	119
Initial Setup	119
Create a Webhook	119
Verify the Runbook Job creation	121
Configure vThunder as an SLB	122
Initial Setup	122
Deploy vThunder as an SLB	125
Configure High Availability for vThunder	126
Initial Setup	126
Create High Availability for vThunder	128
Configure vThunder using GLM	129
Initial Setup	129
Apply GLM License	130
Access vThunder using CLI or GUI	130
Access vThunder using CLI	131
Access vThunder using GUI	132
Verify Deployment	132
Deploy PowerShell Template 3NIC-2VM-HA-GLM-PVTVIP	136
System Requirements	137

Supported VM Sizes	140
Create vThunder Instances	141
Initial Setup	141
Deploy vThunder	144
Configure Server and Client Machine	145
Create a Server Machine	146
Create a Client Machine	155
Configure vThunder as an SLB	163
Initial Setup	163
Deploy vThunder as an SLB	167
Configure High Availability	169
Configure High Availability for vThunder	169
Initial Setup	169
Create High Availability for vThunder	171
Configure vThunder using GLM	172
Initial Setup	172
Apply GLM License	173
Access vThunder using Console/CLI	173
Access vThunder using CLI	174
Access vThunder using GUI	174
Verify Deployment	175
Deploy PowerShell Template 3NIC-NVM-VMSS	180
System Requirements	181
Supported VM Sizes	185
Create vThunder Instances	186
Initial Setup	186
Deploy vThunder	190
Verify Resource Creation	190
Configure Server VMSS	193
Create a Server Machine	194

Verify the Server VMSS Creation	201
Configure Automation Account	202
Create Automation Account	202
Initial Setup	202
Create an Automation Account	208
Verify the Automation Account Creation	208
Create Runbooks	209
Create Automation Account Webhook	216
Initial Setup	216
Create a Webhook	217
Verify the AutoScale Resource Variable creation	217
Verify the SSL File availability	219
Verify the Runbook Jobs creation	221
Enable Autoscaling	223
Autoscaling Options	224
Configure Autoscaling and Log Monitoring using Agent Setup	224
Initial Setup	225
Create Fluentbit and Telegraf Agent	227
Verify Log Agent file upload	228
Access vThunder Agent using CLI	229
Create Autoscale Rule	231
Create Autoscale Alert	235
Verify Logs in Log Analytics Workspace	248
Verify Metrics in Application Insights	250
Configure Autoscaling using Azure Functions Setup	251
Initial Setup	251
Create Autoscale Function	252
Verify Autoscale Function Creation	252
Configure Autoscaling and Log Monitoring using Agent Setup	254
Initial Setup	255
Create Fluentbit and Telegraf Agent	257

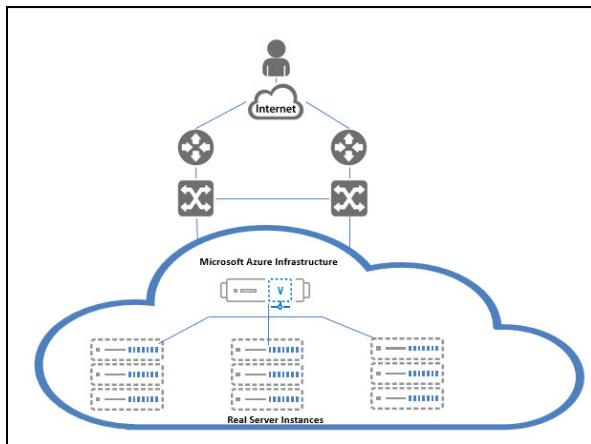
Verify Log Agent file upload	257
Access vThunder Agent using CLI	259
Create Autoscale Rule	261
Create Autoscale Alert	265
Verify Logs in Log Analytics Workspace	278
Verify Metrics in Application Insights	280
Configure Autoscaling using Azure Functions Setup	281
Initial Setup	281
Create Autoscale Function	282
Verify Autoscale Function Creation	282
Access vThunder using CLI or GUI	284
Access vThunder using CLI	284
Access vThunder using GUI	285
Verify Deployment	285
Troubleshooting	290
Common Errors	290
Appendix	294
List of Custom Role Permissions	294
Azure Service Application Access Key	300
Use an existing Access Key	300
Create a new Access Key	301
Create a Role	301
Register a Service Application	306
Associate Service Application with a Role	308
Create Certificate and Secrets	310
Collect Azure Access Key	312
Import Azure Access Key	314

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
POWERSHELL-2NIC-1VM	<ul style="list-style-type: none">Creates 1 vThunder instance with 2 Network Interface Cards (NICs).Deploys a Certificate Authority SSL Certificate and Server Load Balancer (SLB).	<ul style="list-style-type: none">2 NICs (1 Management + 1 Data)BYOL (Bring Your Own License)1 VM (vThunder Virtual Instance)SLB (vThunder Server Load Balancer)

Template	Description	Configuration
		<ul style="list-style-type: none"> SSL (Apply SSL Certificate)
POWERSHELL-2NIC-1VM-GLM	<ul style="list-style-type: none"> Creates 1 vThunder instance with 2 Network Interface Cards and A10 Global License Manager (GLM) integration. Deploys a Certificate Authority SSL Certificate and Server Load Balancer. 	<ul style="list-style-type: none"> 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)
POWERSHELL-3NIC-2VM-HA	<ul style="list-style-type: none"> Creates 2 vThunder instances with High Availability (HA) setup, each vThunder contains 3 Network Interface Cards. Deploys a Certificate Authority SSL Certificate and Server Load Balancer. 	<ul style="list-style-type: none"> 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)
POWERSHELL-3NIC-2VM-HA-GLM-PVTVIP	<ul style="list-style-type: none"> Creates 2 vThunder instances with High Availability setup and an A10 Global License 	<ul style="list-style-type: none"> 3 NICs (1 Management + 2 Data) BYOL (Bring Your Own

Template	Description	Configuration
	<p>Manager integration, each vThunder has 3 Network Interface Cards.</p> <ul style="list-style-type: none"> Deploys a Certificate Authority SSL Certificate, and a Server Load Balancer. 	<ul style="list-style-type: none"> 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)
POWERSHELL-3NIC-2VM-HA-GLM-PUBVIP-BACKAUTO	<ul style="list-style-type: none"> Creates 2 vThunder instances with High Availability (HA) setup and GLM integration, each vThunder contains 3 Network Interface Cards. Deploys a Certificate Authority SSL Certificate, Server Load Balancer, and backend server autoscaling support. 	<ul style="list-style-type: none"> 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 to apply SLB config into vThunder for newly

Template	Description	Configuration
POWERSHELL-3NIC-VMSS	<ul style="list-style-type: none"> • Creates multiple vThunder instances in a Virtual Machine scale set using CPU Matrix-based autoscaling with GLM integration. Each vThunder contains 3 Network Interface Cards. • Deploys a Certificate Authority SSL Certificate, Server Load Balancer, Log Analysis using Azure Log Analytics integration, and Azure Application Insight integration. 	<ul style="list-style-type: none"> • 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-p5, build 114 (Jul-14-2022,05:11)

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.

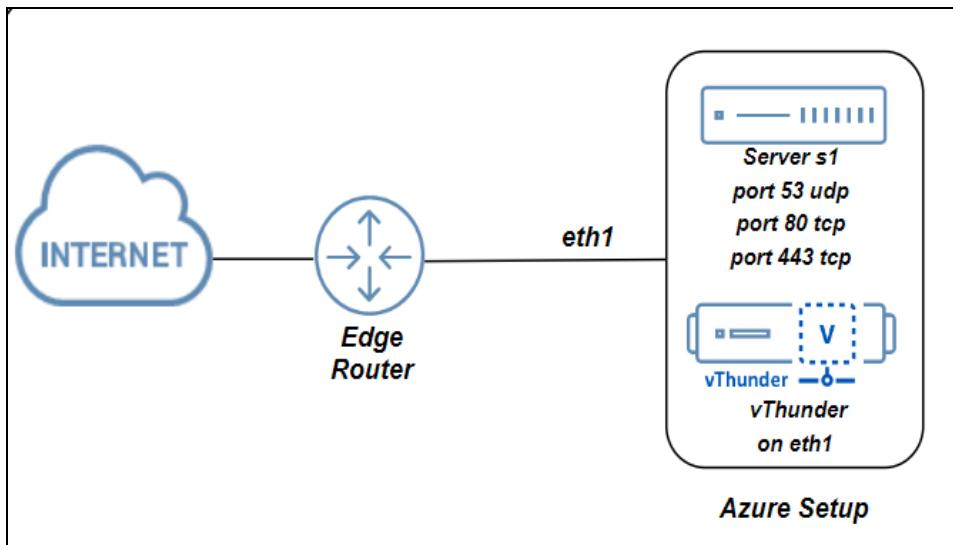
The following templates are available:

- [Deploy PowerShell Template 2NIC-1VM](#)
- [Deploy PowerShell Template 2NIC-1VM-GLM](#)
- [Deploy PowerShell Template 3NIC-2VM-HA](#)
- [Deploy PowerShell Template 3NIC-2VM-HA-GLM-PUBVIP-BACKAUTO](#)
- [Deploy PowerShell Template 3NIC-2VM-HA-GLM-PVTVIP](#)
- [Deploy PowerShell Template 3NIC-NVM-VMSS](#)

Deploy PowerShell Template 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	18
Supported VM Sizes	21
Create vThunder Instance	22
Configure vThunder as an SLB	26
Access vThunder using CLI or GUI	31
Verify Deployment	32

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	<p>A resource group with the specified name and location is created if it doesn't exist.</p> <p>All the resources required for this template is created under the resource group.</p>	Here, the Azure resource group name used is vth-rg1 .
Azure Storage Account	<p>A storage account is created inside the resource group if it doesn't exist.</p> <p>If the storage name already exists, the following error is displayed "The storage account named vthunderstorage already exists under the subscription".</p> <p>Performance: Standard</p> <p>Replication: Read-access geo-redundant storage (RA-GRS)</p> <p>Account kind: Storagev2 (general purpose v2)</p>	vthunderstorage
Virtual Machine (VM) Instance	<p>A virtual machine instance is created for vThunder.</p> <p>Product: A10 vThunder</p> <p>Operating system: Linux</p> <p>Default Size: Standard_DS2v2 (4 vCPUs, 16 GiB Memory)</p>	vth-inst1

Resource Name	Description	Default Value
	<p>NOTE: Before selecting any VM size, it is highly recommended to do an assessment of your projected traffic.</p> <hr/> <p>Table 3 lists the supported VM sizes.</p>	
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: <ul style="list-style-type: none"> Management Interface with public IP Data Interface with primary private IP [Ethernet 1] 	vth-inst1- 10.0.1.5 mgmt-nic1 vth-inst1- 10.0.2.5 data-nic2 [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_A2
	Standard A2v2	Standard_A2_v2
	Standard A2mv2	Standard_A2m_v2
	Standard A4v2	Standard_A4_v2
	Standard A4mv2	Standard_A4m_v2
	Standard A3	Standard_A3
	Standard 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 D2v2	Standard_D2_v2
	Standard DS2v2	Standard_DS2_v2
	Standard D4v3	Standard_D4_v3
	Standard D4sv3	Standard_D4s_v3
	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 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": "10.0.2.5"
},
```

10. Configure a public IP address.

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

11. Configure a Network Security Group.

```
"networkSecurityGroupName": {
    "value": "vth-nsgr1"
},
```

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"

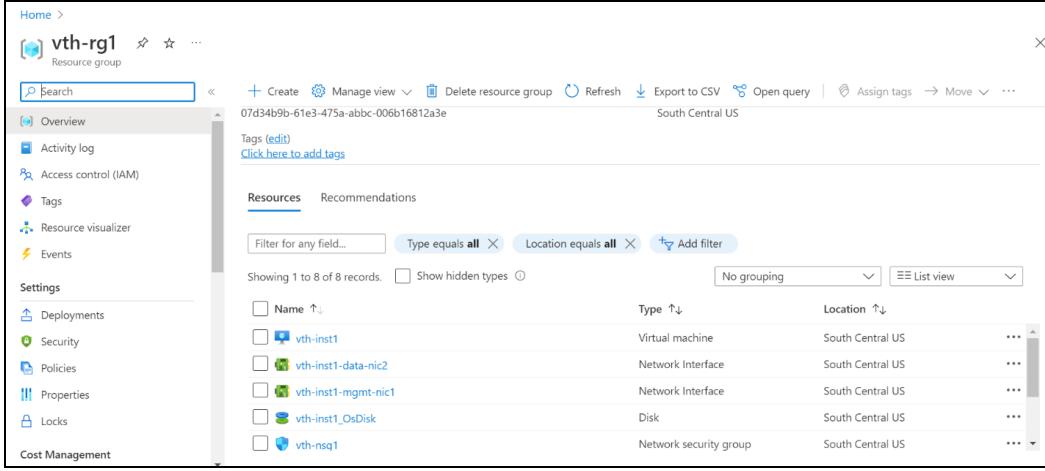
cmdlet PS_TMPL_2NIC_1VM_1.ps1 at command pipeline position 1
Supply values for the following parameters:
storageaccount: vthunderstorage
vth-rg1
vthunderstorage
South Central US
```

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

Deploy PowerShell Template 2NIC-1VM



Name	Type	Location
vth-inst1	Virtual machine	South Central US
vth-inst1-data-nic2	Network Interface	South Central US
vth-inst1-mgmt-nic1	Network Interface	South Central US
vth-inst1_OsDisk	Disk	South Central US
vth-nsq1	Network security group	South Central US

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_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 management 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. Verify if all the configurations in the PS_TMPL_2NIC_1VM_SLB_CONFIG_PARAM.json file are correct and 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 create vThunder SLB instance using the same resource group:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_2NIC_1VM_SLB_CONFIG_2.ps1 -  
resourceGroup <resource_group_name>
```

Example:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_2NIC_1VM_SLB_CONFIG_2.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](#)

NOTE: For A10 vThunder default login credentials, send a request to [A10 Networks Support](#).

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 default login credentials provided by A10 Networks Support and change the default password as soon as you login for the first time:

```
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--->
vThunder(config)#admin <admin_username> password <new_password>
```

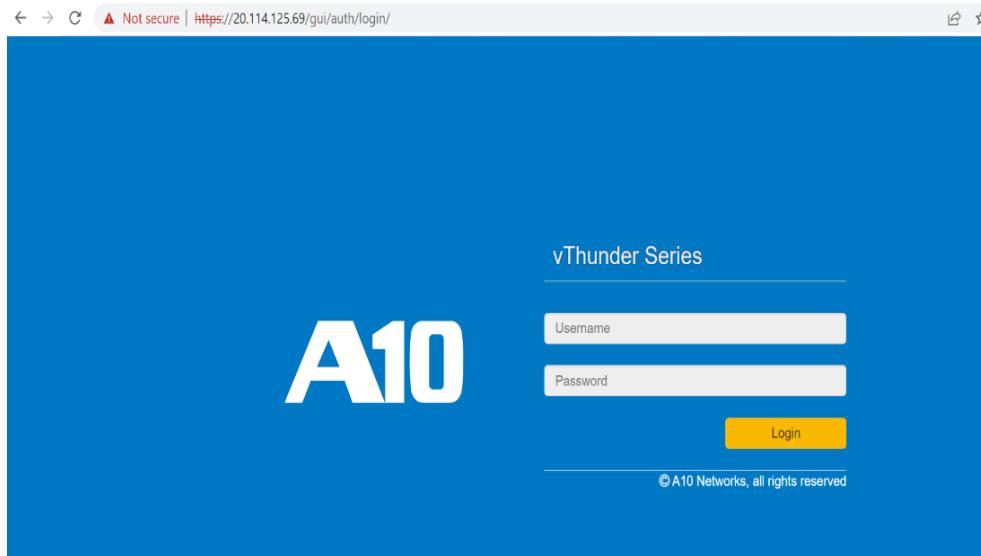
NOTE: It is highly recommended to change the default password when you login for the first time.

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 4 : vThunder GUI



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

Verify Deployment

To verify vThunder SLB deployment thru 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
```

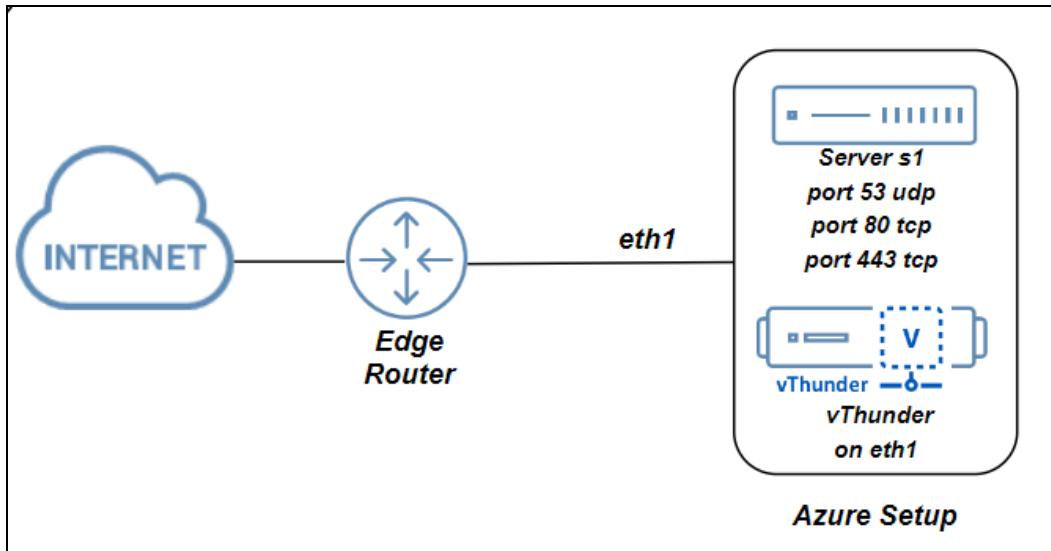
If the deployment is successful, the following SSL configuration is displayed:

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

Deploy PowerShell Template 2NIC-1VM-GLM

[Figure 5](#) 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 5 : 2NIC-1VM-GLM Topology



The following topics are covered:

System Requirements	35
Create vThunder Instance	39
Configure vThunder as an SLB	43
Configure vThunder GLM	48
Access vThunder using CLI or GUI	49
Verify Deployment	51

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	<p>A resource group with the specified name and location is created, if it doesn't exist.</p> <p>All the resources required for this template is created under the resource group.</p>	Here, the Azure resource group name used is <code>vth-rg1</code> .
Azure Storage Account	<p>A storage account is created inside the resource group, if it doesn't exist.</p> <p>If the storage name already exists, the following error is displayed "The storage account named vthunderstorage already exists under the subscription".</p> <p>Performance: Standard</p> <p>Replication: Read-access geo-redundant storage (RA-GRS)</p> <p>Account kind: Storagev2 (general purpose v2)</p>	<code>vthunderstorage</code>
Virtual Machine (VM) Instance	<p>A virtual machine instance is created for vThunder.</p> <p>Product: A10 vThunder</p> <p>Operating system: Linux</p> <p>Default Size: Standard_DS2v2 (4 vCPUs, 16 GiB Memory)</p>	<code>vth-inst1</code>

Resource Name	Description	Default Value
	<p>NOTE: Before selecting any VM size, it is highly recommended to do an assessment of your projected traffic.</p> <hr/> <p>Table 5 lists the supported VM sizes.</p>	
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: <ul style="list-style-type: none"> 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-nsg

Supported VM Sizes

Table 5 : Supported VM sizes

Series	Size	Qualified Name
A series	Standard A2	Standard_A2
	Standard A2v2	Standard_A2_v2
	Standard A2mv2	Standard_A2m_v2
	Standard A4v2	Standard_A4_v2
	Standard A4mv2	Standard_A4m_v2
	Standard A3	Standard_A3
	Standard 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 D2v2	Standard_D2_v2
	Standard DS2v2	Standard_DS2_v2
	Standard D4v3	Standard_D4_v3
	Standard D4sv3	Standard_D4s_v3
	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 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": "10.0.2.5"
},
```

10. Configure a public IP address.

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

11. Configure a Network Security Group.

```
"networkSecurityGroupName": {
    "value": "vth-nsgr1"
},
```

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"

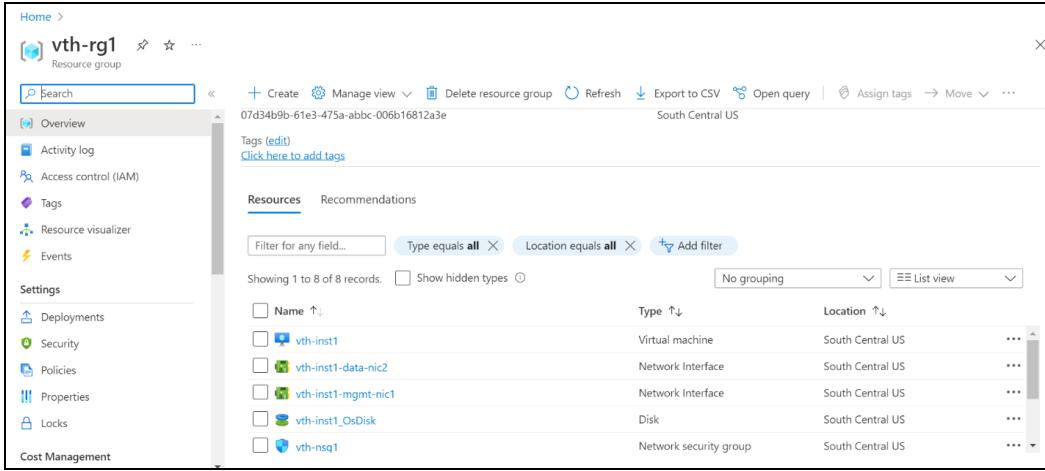
cmdlet PS_TMPL_2NIC_1VM_1.ps1 at command pipeline position 1
Supply values for the following parameters:
storageaccount: vthunderstorage
vth-rg1
vthunderstorage
South Central US
```

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 6 : Resource listing in the resource group

Deploy PowerShell Template 2NIC-1VM-GLM



Name	Type	Location
vth-inst1	Virtual machine	South Central US
vth-inst1-data-nic2	Network Interface	South Central US
vth-inst1-mgmt-nic1	Network Interface	South Central US
vth-inst1_OsDisk	Disk	South Central US
vth-nsq1	Network security group	South Central US

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_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 management 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. Verify if all the configurations in the PS_TMPL_2NIC_1VM_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 create vThunder SLB instance using the same resource group:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_2NIC_1VM_SLB_CONFIG_2.ps1 -  
resourceGroup <resource_group_name>
```

Example:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_2NIC_1VM_SLB_CONFIG_2.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_3.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](#)

NOTE: For A10 vThunder default login credentials, send a request to [A10 Networks Support](#).

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 default login credentials provided by A10 Networks Support and change the default password as soon as you login for the first time:

```
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-->
vThunder(config)#admin <admin_username> password <new_password>
```

NOTE: It is highly recommended to change the default password when you login for the first time.

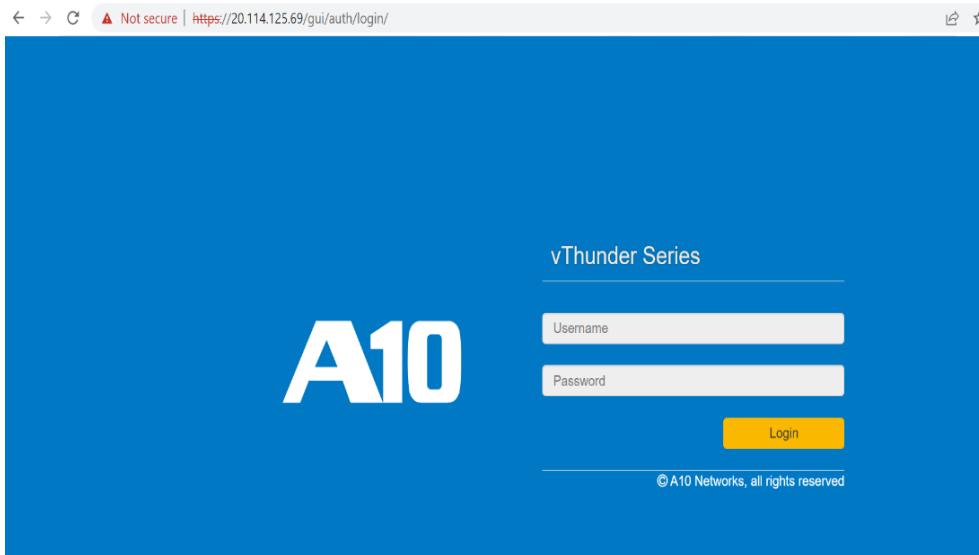
Access vThunder using GUI

To access vThunder using GUI, perform the following steps:

1. Open any browser.

- Enter `https://<vthunder_public_IP>/gui/auth/login/` in the address bar.

Figure 7 : vThunder GUI



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

Verify Deployment

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

- 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
```

[Deploy PowerShell Template 2NIC-1VM-GLM](#)

```

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

[Deploy PowerShell Template 2NIC-1VM-GLM](#)

Burst	:	Disabled
GLM Ping Interval In Hours	:	24
<hr/>		
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:

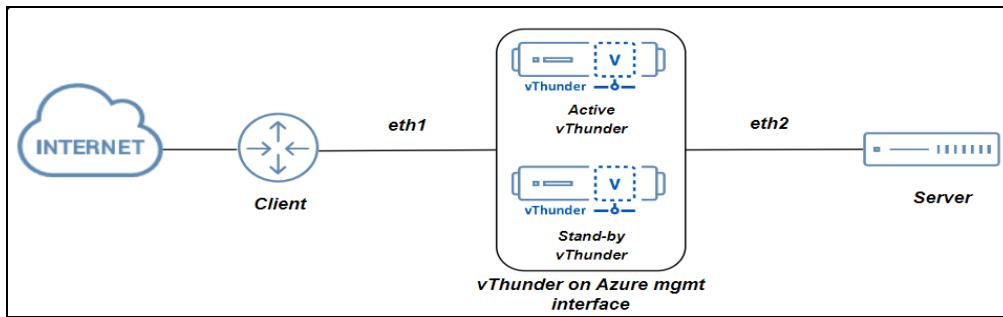
Name	Type	Expiration	Status
<hr/>			
server certificate		Jan 28 12:00:00 2028 GMT	[Unexpired, Bound]

Deploy PowerShell Template 3NIC-2VM-HA

[Figure 8](#) 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 8 : 3NIC-2VM-HA Topology



The following topics are covered:

System Requirements	54
Create vThunder Instances	58
Configure Server and Client Machine	63
Configure vThunder as an SLB	81
Configure High Availability	87
Access vThunder using CLI or GUI	90
Verify Deployment	92

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	<p>A resource group with the specified name and location is created, if it doesn't exist.</p> <p>All the resources required for this template is created under the resource group.</p>	Here, the Azure resource group name used is <code>vth-rg1</code> .
Azure Storage Account	<p>A storage account is created inside the resource group, if it doesn't exist.</p> <p>If the storage name already exists, the following error is displayed "The storage account named vthunderstorage already exists under the subscription".</p> <p>Performance: Standard</p> <p>Replication: Read-access geo-redundant storage (RA-GRS)</p> <p>Account kind: Storagev2 (general purpose v2)</p>	<code>vthunderstorage</code>
Virtual Machine (VM) Instance	<p>Two virtual machine instances are created for vThunder.</p> <p>Product: A10 vThunder</p> <p>Operating system: Linux</p> <p>Default Size: Standard_B4ms (4 vCPUs, 16 GiB Memory)</p>	<code>vth-inst1</code> <code>vth-inst2</code>

Resource Name	Description	Default Value										
	<p>NOTE: Before selecting any VM size, it is highly recommended to do an assessment of your projected traffic.</p> <p>Table 7 lists the supported VM sizes.</p>											
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]	<p>Two types of interfaces are created for each vThunder instance:</p> <ul style="list-style-type: none"> Management Interface with public IP Data Interface with primary private IP [Ethernet 1, Ethernet 2] <p>NOTE: The secondary IP of data interface is taken from DHCP server.</p>	<table border="1"> <tr> <td>vth-inst1-mgmt-nic1</td> <td>10.0.1.4</td> </tr> <tr> <td>vth-inst1-data-nic2</td> <td>10.0.2.4 [Primary IP]</td> </tr> <tr> <td></td> <td>10.0.2.X [Secondary IP]</td> </tr> <tr> <td>vth-inst1-data-nic3</td> <td>10.0.3.4 [Primary IP]</td> </tr> <tr> <td></td> <td>10.0.3.X [Secondary IP]</td> </tr> </table>	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-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]											

Resource Name	Description	Default Value	
		<code>vth-inst2-mgmt-nic1</code>	10.0.1.6
		<code>vth-inst2-data-nic2</code>	10.0.2.6 [Primary IP]
			10.0.2.X [Secondary IP]
		<code>vth-inst2-data-nic3</code>	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.	<code>vth-inst1-nsg</code> <code>vth-inst2-nsg</code>	
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
	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

Series	Size	Qualified Name
	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>"
```

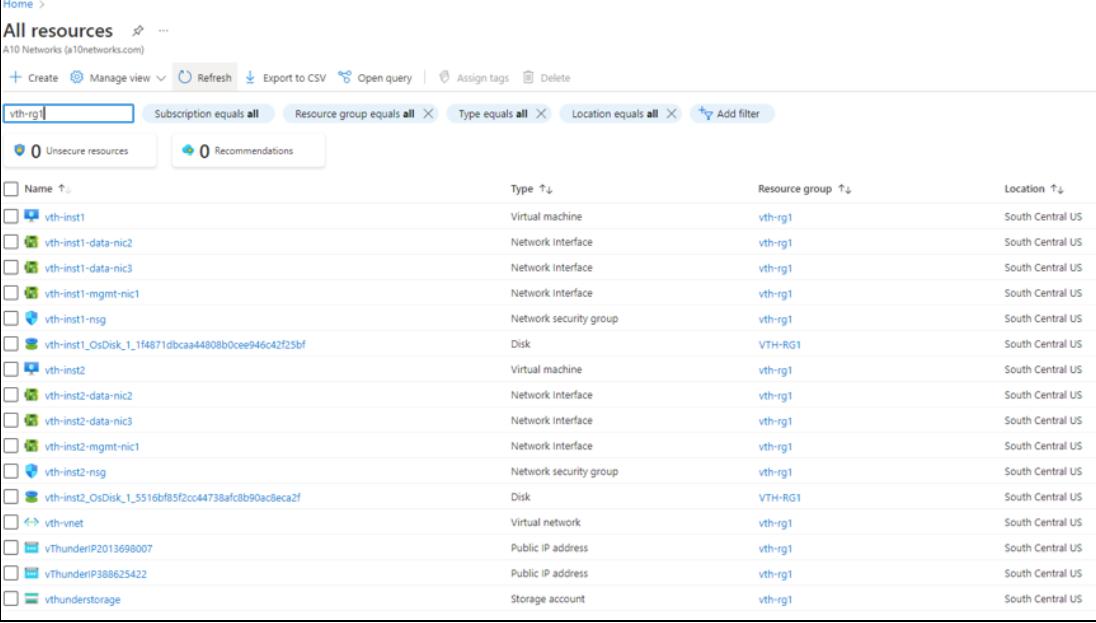
Example:

```
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 9 : Resource listing in the resource group



Name ↑	Type ↑	Resource group ↑↓	Location ↑↓
vth-inst1	Virtual machine	vth-rg1	South Central US
vth-inst1-data-nic2	Network interface	vth-rg1	South Central US
vth-inst1-data-nic3	Network interface	vth-rg1	South Central US
vth-inst1-mgmt-nic1	Network interface	vth-rg1	South Central US
vth-inst1-nsg	Network security group	vth-rg1	South Central US
vth-inst1_OsDisk_1_1f4871dbcaa44800b0cee946c42f25bf	Disk	VTH-RG1	South Central US
vth-inst2	Virtual machine	vth-rg1	South Central US
vth-inst2-data-nic2	Network interface	vth-rg1	South Central US
vth-inst2-data-nic3	Network interface	vth-rg1	South Central US
vth-inst2-mgmt-nic1	Network interface	vth-rg1	South Central US
vth-inst2-nsg	Network security group	vth-rg1	South Central US
vth-inst2_OsDisk_1_5516bf85f2cc44738afc8b90ac8eca2f	Disk	VTH-RG1	South Central US
vth-net	Virtual network	vth-rg1	South Central US
vThunderIP2013698007	Public IP address	vth-rg1	South Central US
vThunderIP388625422	Public IP address	vth-rg1	South Central US
vthunderstorage	Storage account	vth-rg1	South Central US

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 thru **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

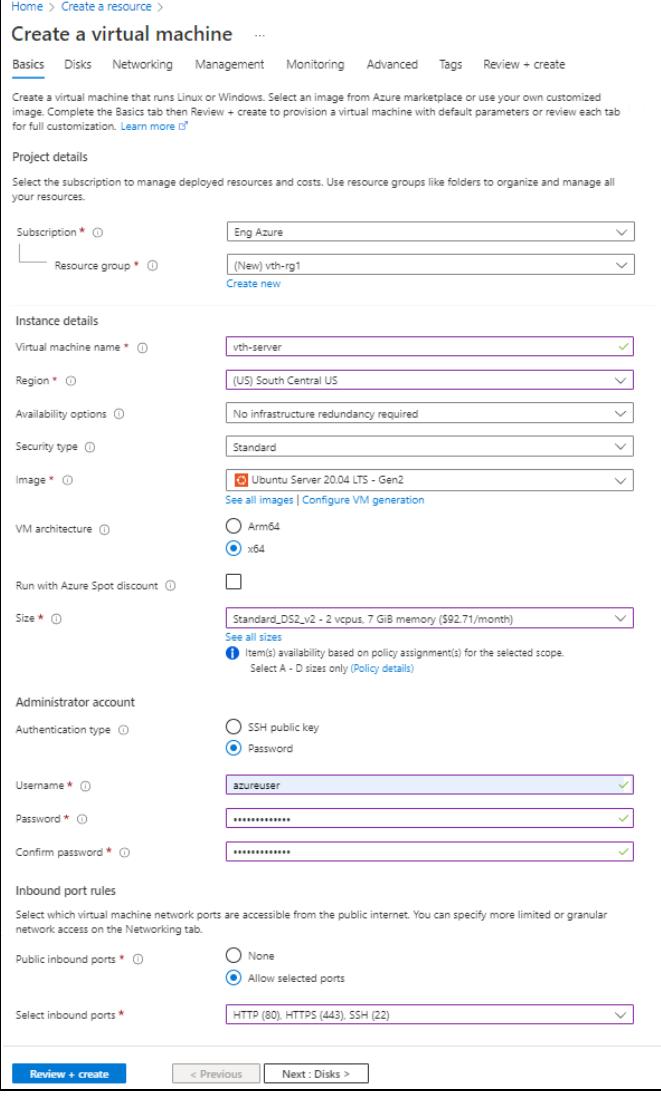
Administrator account

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

Inbound port rules

- Public inbound ports
- Select inbound ports

Figure 10 : Create a virtual machine window - Basics tab



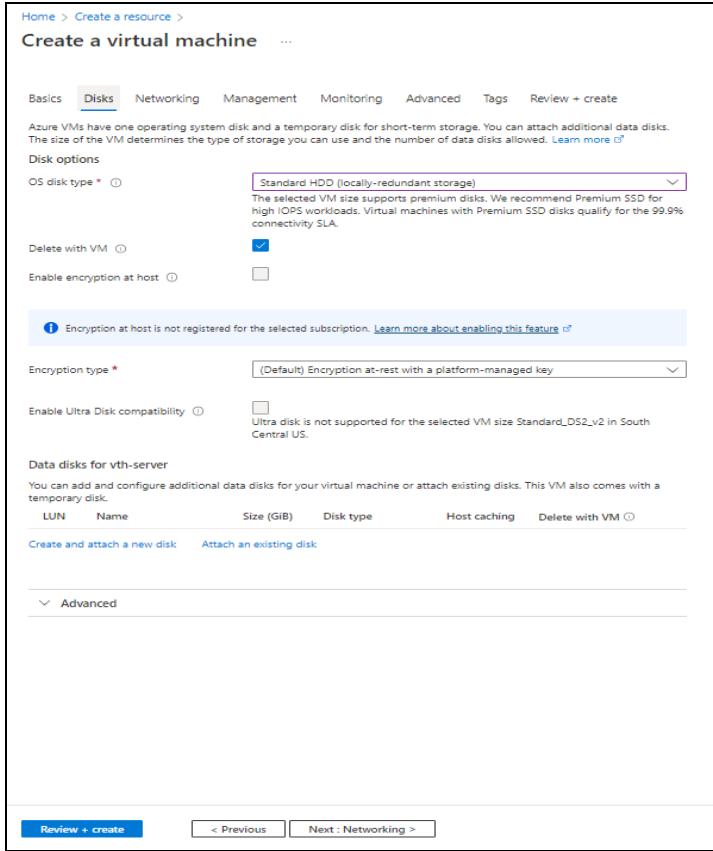
The screenshot shows the 'Create a virtual machine' wizard in the Azure portal, specifically the 'Basics' tab. The window title is 'Create a virtual machine ...'. The 'Basics' tab is selected. The 'Subscription' dropdown is set to 'Eng Azure'. The 'Resource group' dropdown is set to '(New) vth-rg1'. Under 'Instance details', the 'Virtual machine name' is 'vth-server', 'Region' is '(US) South Central US', 'Availability options' is 'No infrastructure redundancy required', 'Security type' is 'Standard', 'Image' is 'Ubuntu Server 20.04 LTS - Gen2', 'VM architecture' is 'x64', and 'Size' is 'Standard_DS2_v2 - 2 vcpus, 7 GiB memory (\$92.71/month)'. Under 'Administrator account', the 'Authentication type' is 'Password', and the 'Username' is 'azureuser'. In the 'Inbound port rules' section, 'Public inbound ports' is set to 'Allow selected ports' and 'Select inbound ports' includes 'HTTP (80), HTTPS (443), SSH (22)'. At the bottom, there are buttons for 'Review + create', '< Previous', and 'Next : Disks >'.

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 11 : Create a virtual machine window - Disks tab

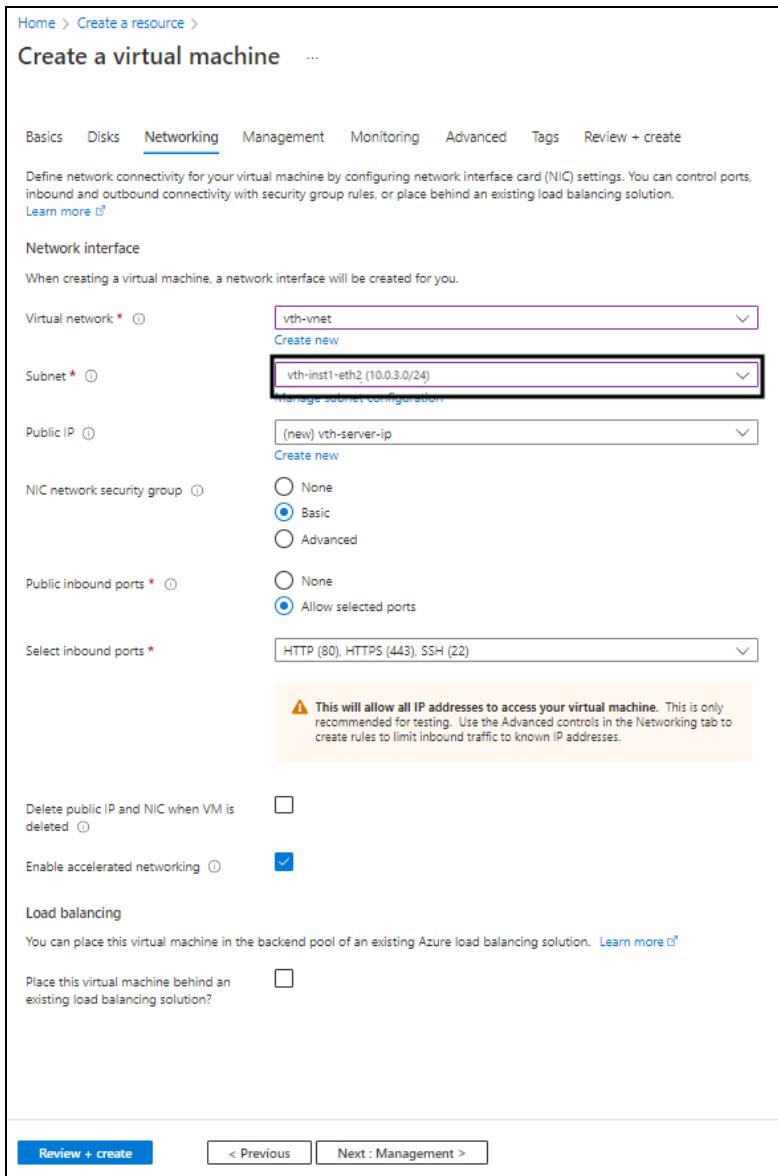


5. Leave the remaining fields as is and click **Next : Networking** at the bottom of the window.
6. Select or enter the following mandatory information in the **Networking** tab:

Network interface

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

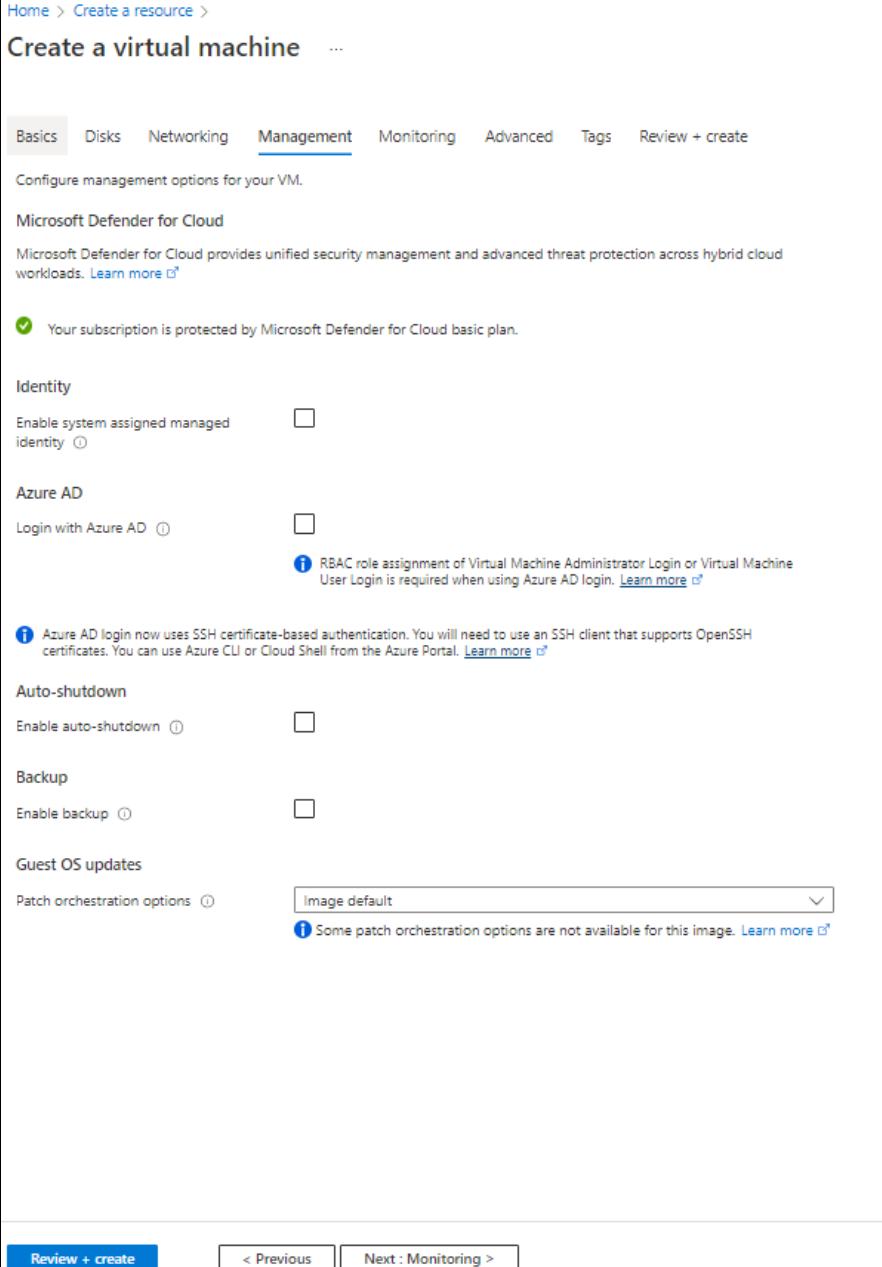
Figure 12 : Create a virtual machine window - Networking tab



- 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 13 : Create a virtual machine window - Management tab



The screenshot shows the 'Create a virtual machine' wizard in the Azure portal, specifically the 'Management' tab. The top navigation bar includes 'Home > Create a resource > Create a virtual machine'. The 'Management' tab is selected, indicated by an underline. Below the tabs are several configuration sections:

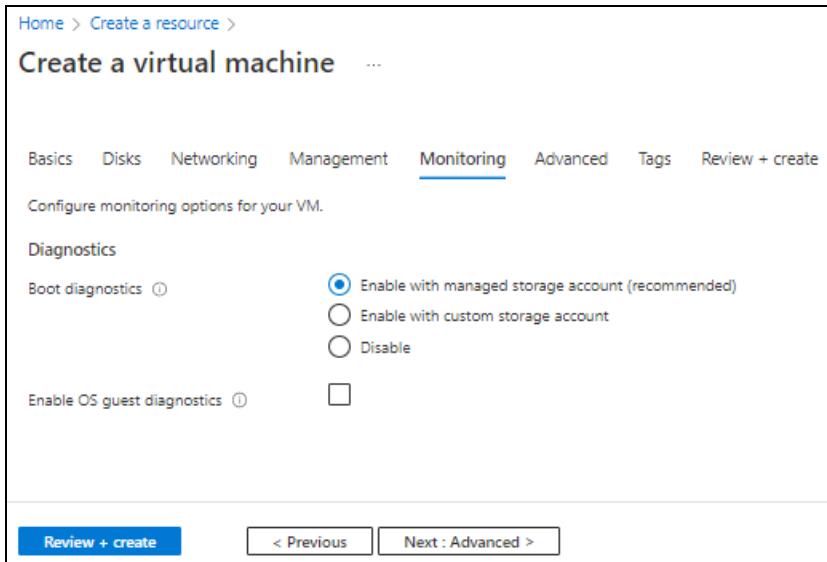
- Microsoft Defender for Cloud**: A note stating "Microsoft Defender for Cloud provides unified security management and advanced threat protection across hybrid cloud workloads." with a "Learn more" link.
- Identity**:
 - Enable system assigned managed identity**: A checkbox is checked.
 - Azure AD**:
 - Login with Azure AD**: A checkbox is checked.
 - A note: "Azure AD login now uses SSH certificate-based authentication. You will need to use an SSH client that supports OpenSSH certificates. You can use Azure CLI or Cloud Shell from the Azure Portal." with a "Learn more" link.
- Auto-shutdown**:
 - Enable auto-shutdown**: A checkbox is checked.
- Backup**:
 - Enable backup**: A checkbox is checked.
- Guest OS updates**:
 - Patch orchestration options**: A dropdown menu is set to "Image default". A note: "Some patch orchestration options are not available for this image." with a "Learn more" link.

At the bottom of the window are three buttons: "Review + create" (highlighted in blue), "< Previous", and "Next : Monitoring >".

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

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

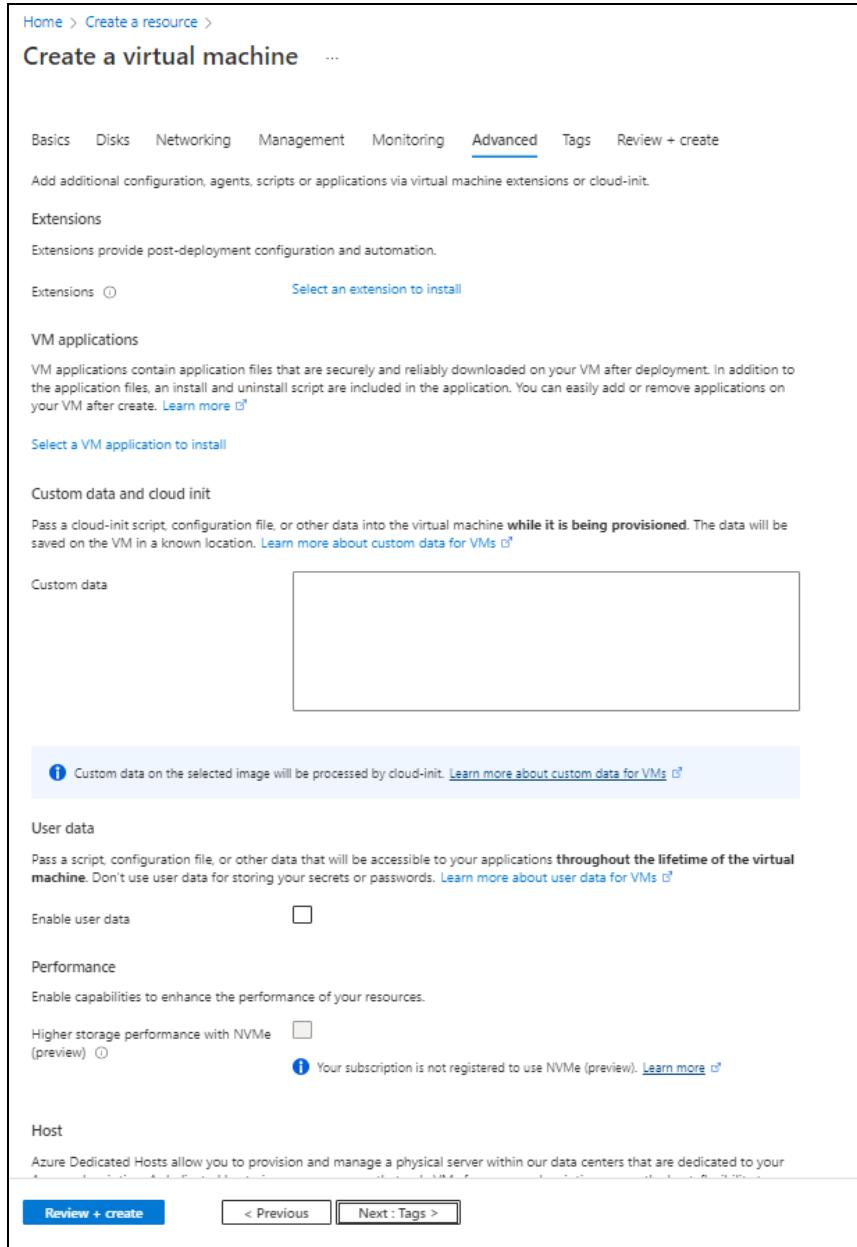
Figure 14 : Create a virtual machine window - Monitoring tab



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

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

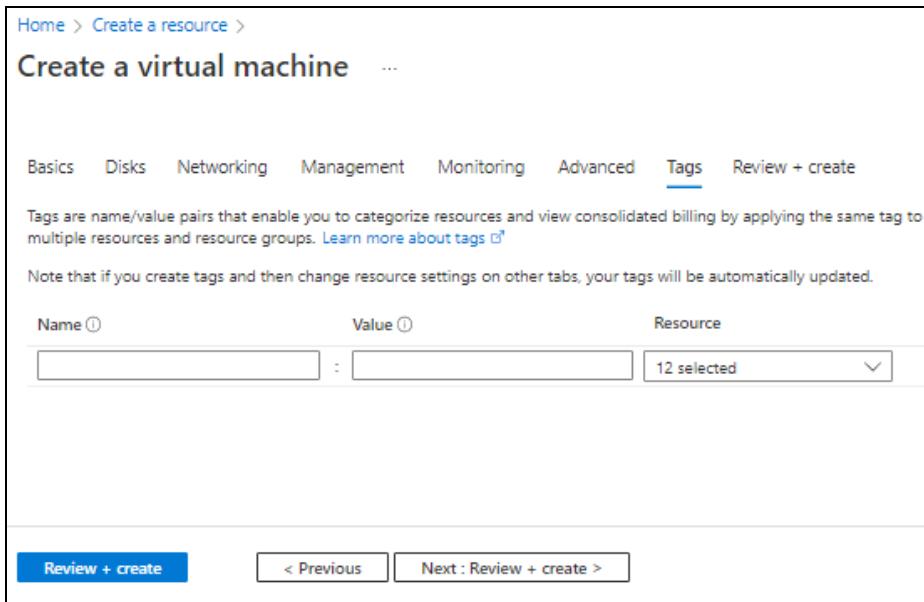
Figure 15 : Create a virtual machine window - Advanced tab



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

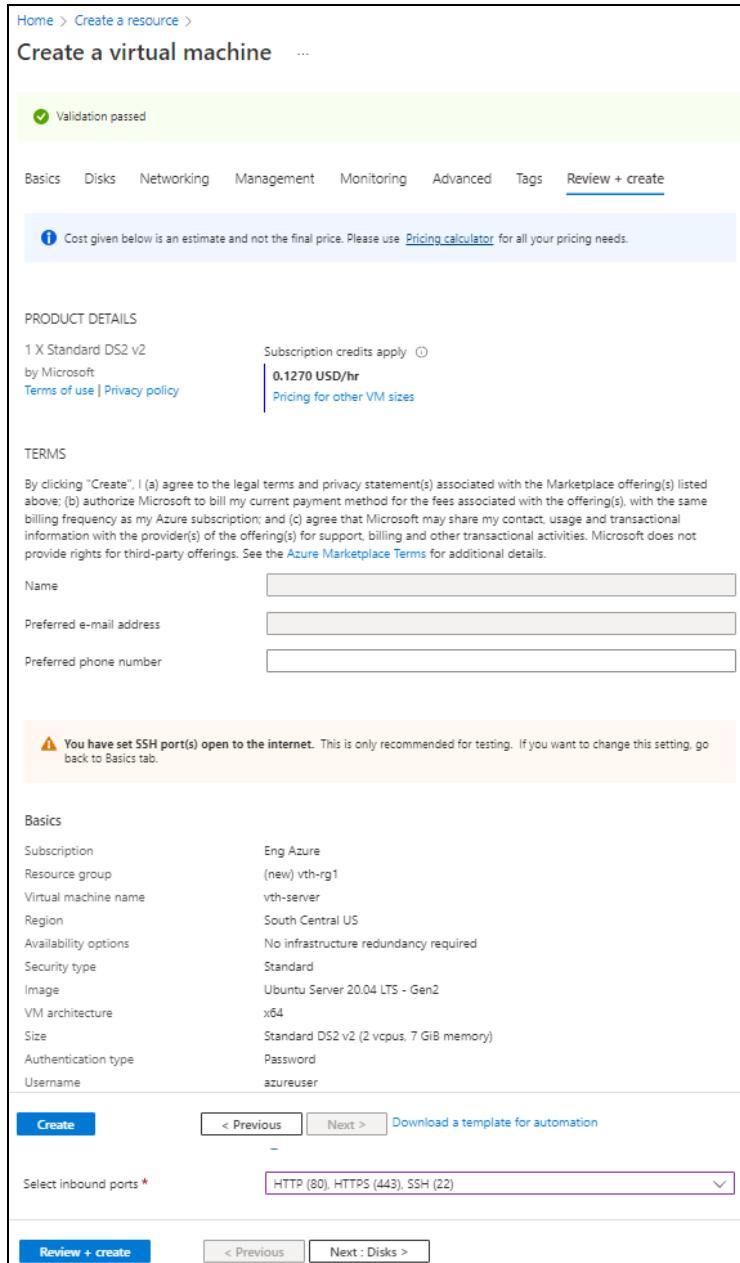
14. Select or enter the information to categorized resources in the **Tags tab as needed.**

Figure 16 : 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 17 : 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.

Create a Client Machine

To create a Client machine, perform the following steps:

1. From Home, navigate thru **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

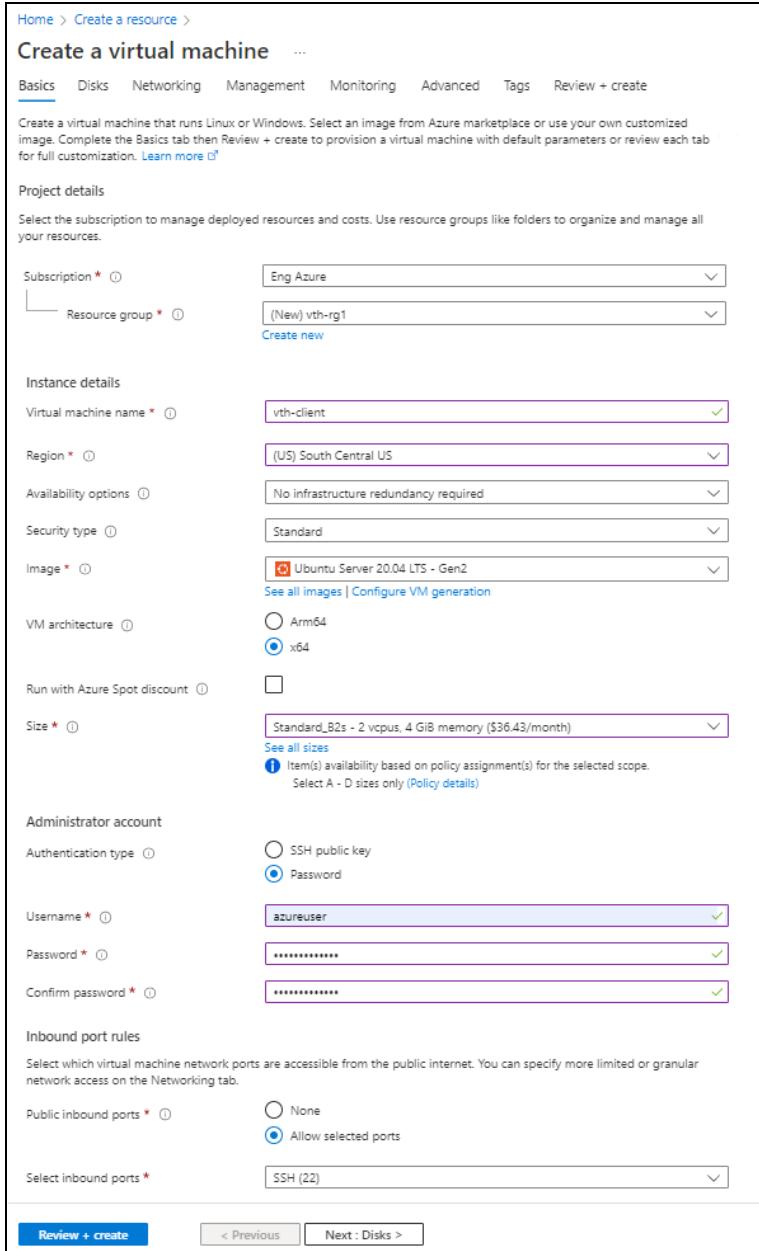
Administrator account

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

Inbound port rules

- Public inbound ports
- Select inbound ports

Figure 18 : Create a virtual machine window - Basics tab



The screenshot shows the 'Create a virtual machine' wizard in the Azure portal, specifically the 'Basics' tab. The window title is 'Create a virtual machine ...'. The tabs at the top are 'Basics', 'Disks', 'Networking', 'Management', 'Monitoring', 'Advanced', 'Tags', and 'Review + create'. The 'Basics' tab is selected.

Project details:

- Subscription: Eng Azure
- Resource group: (New) vth-rg1

Instance details:

- Virtual machine name: vth-client
- Region: (US) South Central US
- Availability options: No infrastructure redundancy required
- Security type: Standard
- Image: Ubuntu Server 20.04 LTS - Gen2
- VM architecture: x64
- Run with Azure Spot discount: Unchecked
- Size: Standard_B2s - 2 vcpus, 4 GiB memory (\$36.43/month)

Administrator account:

- Authentication type: Password
- Username: azureuser
- Password: (redacted)
- Confirm password: (redacted)

Inbound port rules:

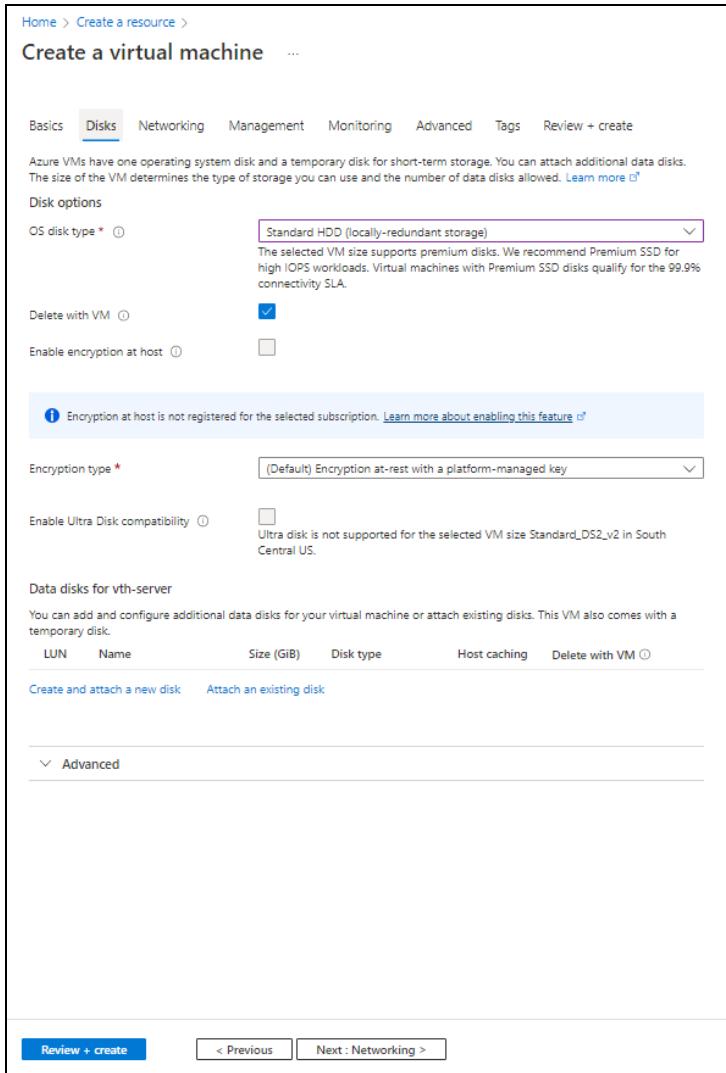
- Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.
- Public inbound ports: Allow selected ports
- Select inbound ports: SSH (22)

At the bottom of the window are buttons for 'Review + create' (highlighted in blue), '< Previous', and 'Next : Disks >'.

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 19 : Create a virtual machine window - Disks tab



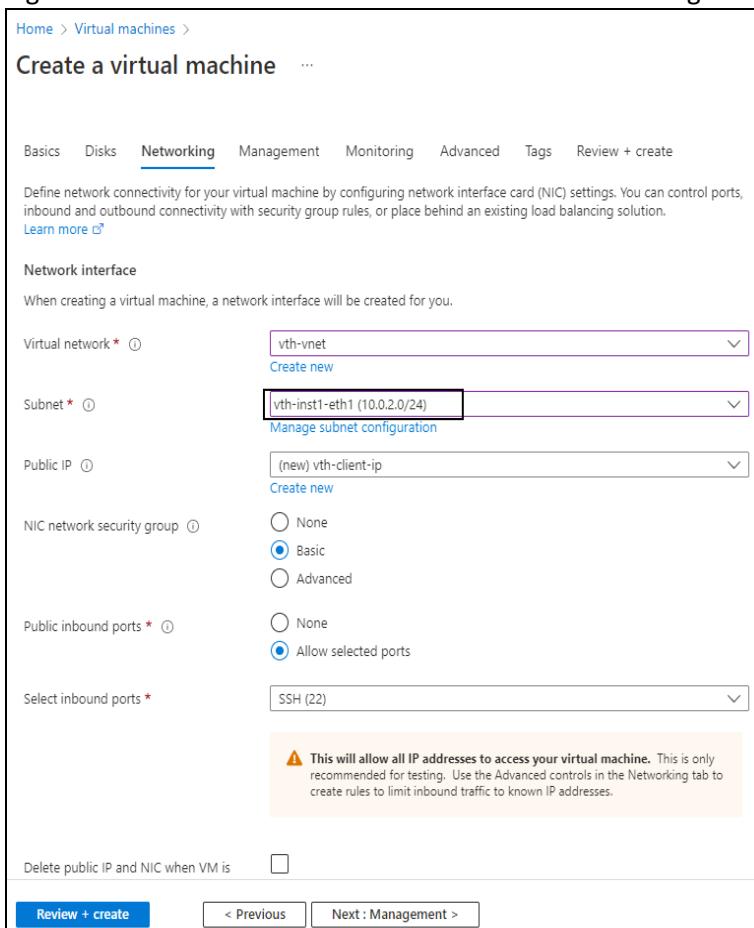
5. Leave the remaining fields as is and click **Next : Networking** at the bottom of the window.
6. Select or enter the following mandatory information in the **Networking** tab:

Network interface

[Deploy PowerShell Template 3NIC-2VM-HA](#)

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

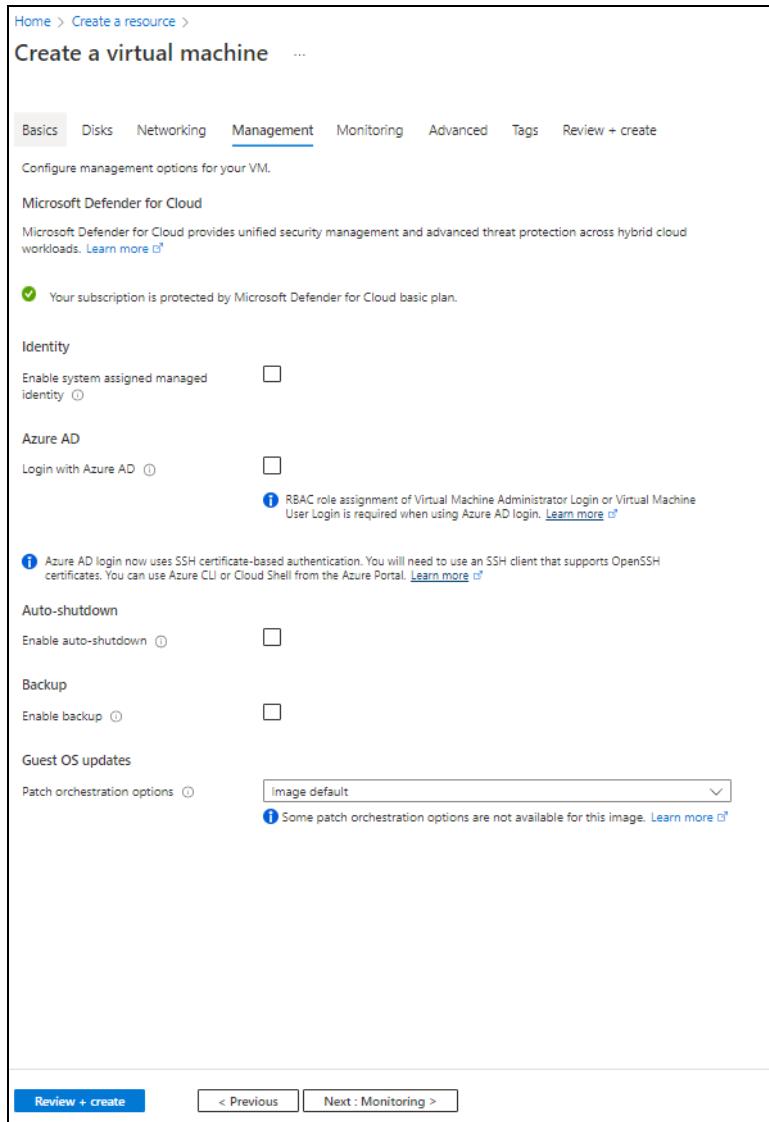
Figure 20 : Create a virtual machine window - Networking tab



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.

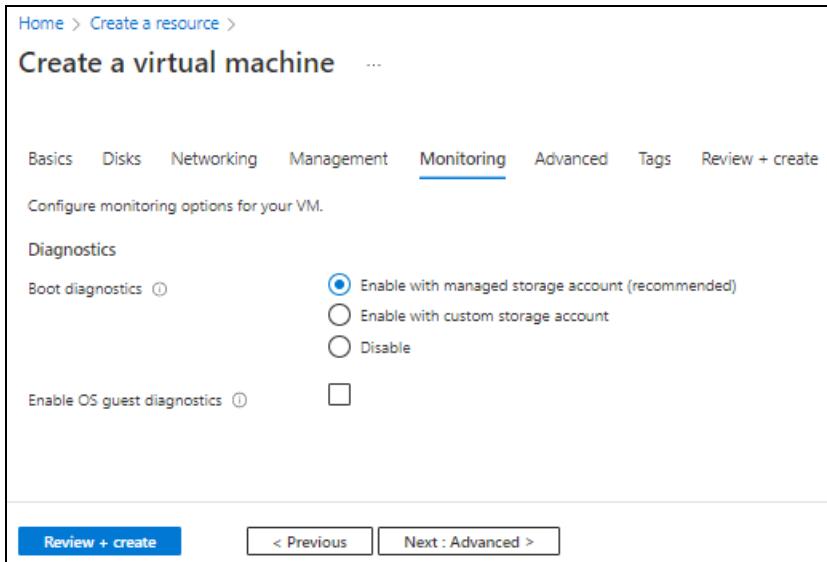
Figure 21 : Create a virtual machine window - Management tab



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

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

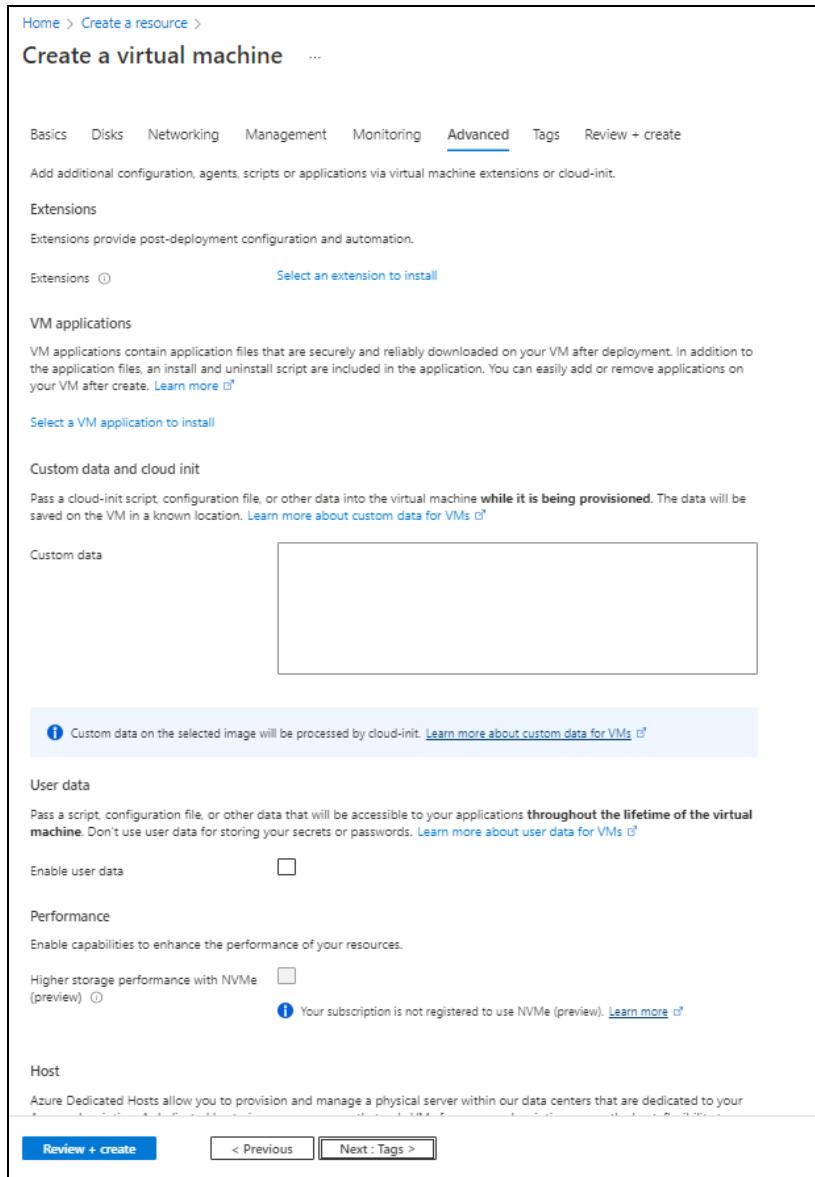
Figure 22 : Create a virtual machine window - Monitoring tab



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

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

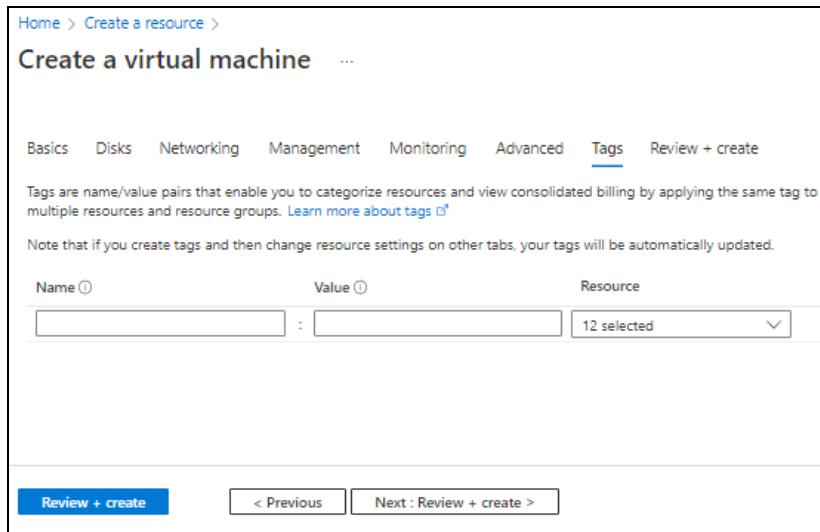
Figure 23 : Create a virtual machine window - Advanced tab



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.**

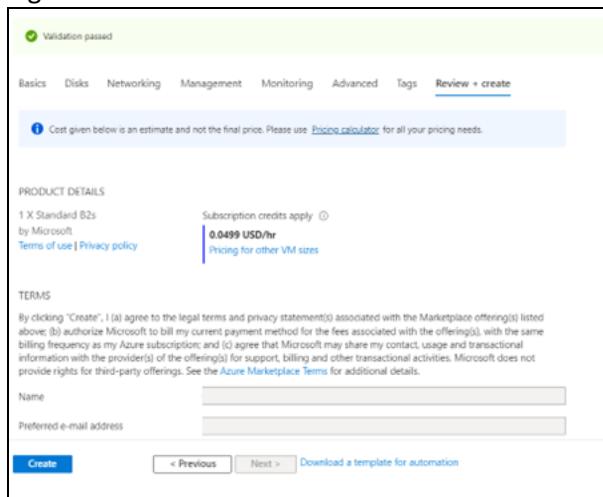
Figure 24 : Create a virtual machine window - Tags tab



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 25 : 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](#)
- [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 management 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
                }
            ]
        }
    ]
},
```

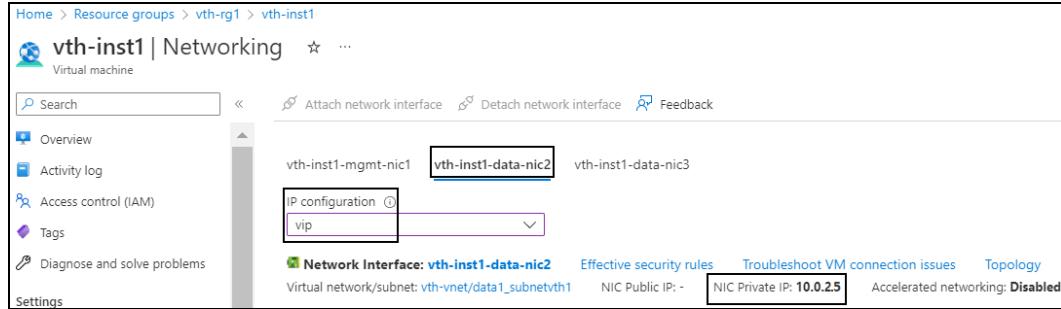
```
        ],
    },
    {
        "name": "sg80",
        "protocol": "tcp",
        "health-check-disable": 1
        "member-list": [
            {
                "name": "s1",
                "port": 80
            }
        ]
    }
],
```

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 thru **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 26 : 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"
        }
    ]
}

```

```

        "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. 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.

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.

- 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_2.ps1  
-resourceGroup <resource_group_name>
```

Example:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_HA_SLB_CONFIG_2.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":"10.0.1.1"
            }
        ]
    ],

```

4. Set VRRP-A.

```

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

```

5. Set a Terminal Idle Timeout.

```

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

```

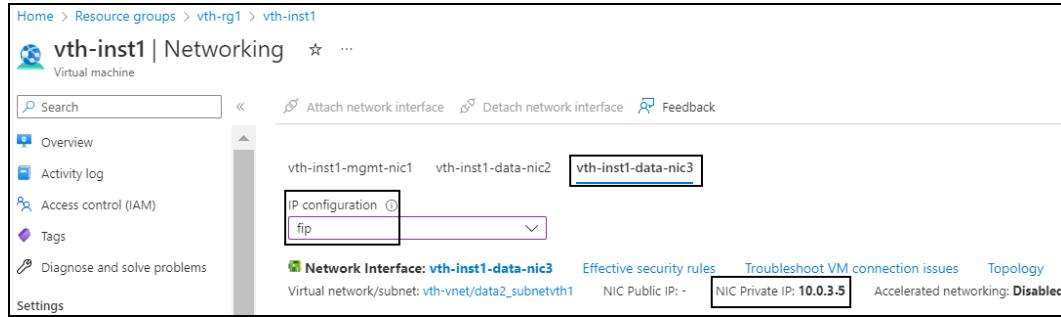
6. Configure the VRID details.

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:

- From the **Home**, navigate thru **Azure Services > Resource Group > <resource_group_name>**.
- Go to the first virtual machine instance. Here, first virtual machine instance is `vth-inst1`.
- Select **Networking** from the left **Settings** panel.

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

Figure 27 : 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_3.ps1 -  
resourceGroup <resource_group_name>
```

Example:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_HA_CONFIG_3.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](#)

NOTE: For A10 vThunder default login credentials, send a request to [A10 Networks Support](#).

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 default login credentials provided by A10 Networks Support and change the default password as soon as you login for the first time:

```
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--->
vThunder(config)#admin <admin_username> password <new_password>

```

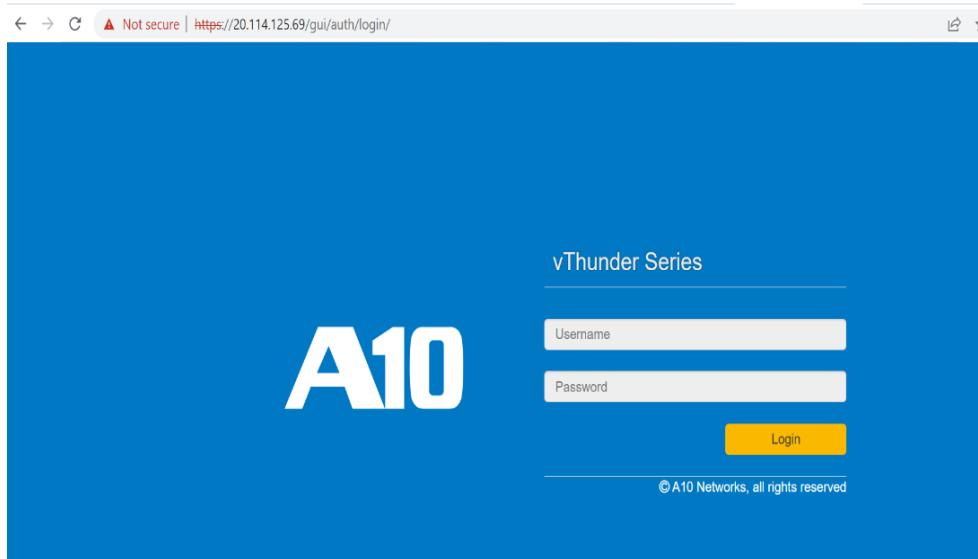
NOTE: It is highly recommended to change the default password when you login for the first time.

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 28 : vThunder GUI



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

Verify Deployment

To verify vThunder SLB deployment thru 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
!
```

- 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
<hr/>			
server certificate		Jan 28 12:00:00 2028 GMT	[Unexpired, Bound]

- 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
!
```

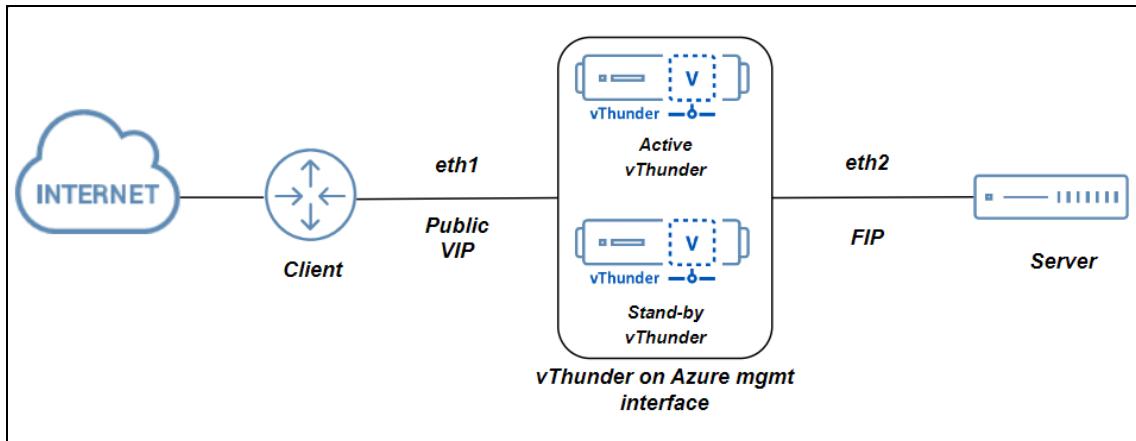
```
ip dns primary 8.8.8.8
!
!
interface management
    ip address dhcp
!
interface ethernet 1
    enable
    ip address dhcp
!
interface ethernet 2
    enable
    ip address dhcp
!
vrrp-a vrid 0
    floating-ip 10.0.3.5
    floating-ip 10.0.2.5
    blade-parameters
        priority 100
!
vrrp-a peer-group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

Deploy PowerShell Template 3NIC-2VM-HA-GLM-PUBVIP-BACKAUTO

[Figure 29](#) shows the 3NIC-2VM-HA-GLM-PUBVIP-BACKAUTO deployment topology. Using this template, two vThunder instances can be deployed containing:

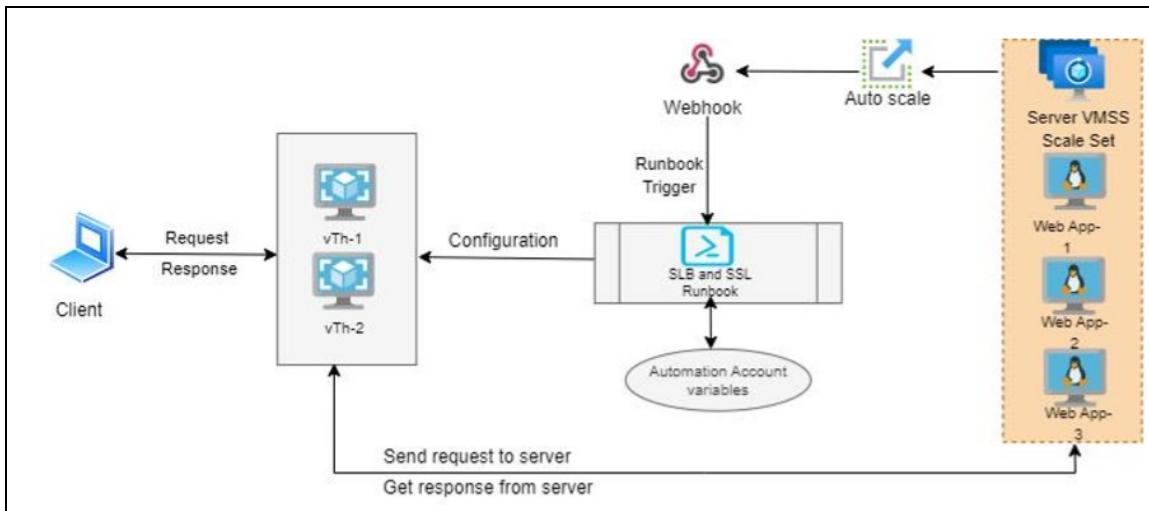
- One management interface and two data interfaces each
- HA support
- GLM integration
- Backend server autoscaling support.

Figure 29 : 3NIC-2VM-HA-GLM-PUBVIP-BACKAUTO Topology



[Figure 30](#) 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 30 : 3NIC-2VM-HA-GLM-PUBVIP-BACKAUTO Process Flow



The following topics are covered:

System Requirements	96
Create vThunder Instances	101
Configure Server VMSS	106
Configure Automation Account	114
Configure vThunder as an SLB	122
Configure High Availability for vThunder	126
Configure vThunder using GLM	129
Access vThunder using CLI or GUI	130
Verify Deployment	132

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

Resource Name	Description	Default Value
Instance	<p>Product: A10 vThunder</p> <p>Operating system: Linux</p> <p>Default Size: Standard_B4ms (4 vCPUs, 16 GiB Memory)</p> <p>NOTE: Before selecting any VM size, it is highly recommended to do an assessment of your projected traffic.</p> <p>Table 9 lists the supported VM sizes.</p>	
Azure Automation Account	An automation account is created under the resource group.	vth-amt-acc
Azure Run-book with Webhook	A custom runbook is created under the automation account: SLB-Config A webhook is created for SLB.	

Resource Name	Description	Default Value																		
Virtual Machine Scale Set [VMSS]	A virtual machine scale set is created.	<code>vth-server-vmss</code>																		
Virtual Cloud Network [VCN]	A virtual network is assigned to the virtual machine instance.	vth-vmss-vnet Address prefix for virtual network: <code>10.0.0.0/16</code>																		
Subnet	Three subnets are created with an address prefix each.	Subnet1: <code>vth-vnet1-mgmt-sub1 10.0.1.0/24</code> Subnet2: <code>vth-vnet1-data-sub2 10.0.2.0/24</code> Subnet3: <code>vth-vnet1-data-sub3 10.0.3.0/24</code>																		
Network Interface Card [NIC]	Two types of interfaces are created for each vThunder instance: <ul style="list-style-type: none"> Management Interface with public IP Data Interface with primary private IP [Ethernet 1, Ethernet 2] <p>NOTE: The secondary IP of data interface is taken from DHCP server.</p>	<table border="1"> <tr> <td><code>vth-inst1-mgmt-nic1</code></td> <td><code>10.0.1.4</code></td> </tr> <tr> <td><code>vth-inst1-data-nic2</code></td> <td><code>10.0.2.4</code> [Primary IP]</td> </tr> <tr> <td></td> <td><code>10.0.2.X</code> [Secondary IP]</td> </tr> <tr> <td><code>vth-inst1-data-nic3</code></td> <td><code>10.0.3.4</code> [Primary IP]</td> </tr> <tr> <td></td> <td><code>10.0.3.X</code> [Secondary IP]</td> </tr> <tr> <td><code>vth-inst2-mgmt-nic1</code></td> <td><code>10.0.1.6</code></td> </tr> <tr> <td><code>vth-inst2-data-nic2</code></td> <td><code>10.0.2.6</code> [Primary IP]</td> </tr> <tr> <td></td> <td><code>10.0.2.X</code> [Secondary IP]</td> </tr> <tr> <td><code>vth-inst2-</code></td> <td><code>10.0.3.6</code></td> </tr> </table>	<code>vth-inst1-mgmt-nic1</code>	<code>10.0.1.4</code>	<code>vth-inst1-data-nic2</code>	<code>10.0.2.4</code> [Primary IP]		<code>10.0.2.X</code> [Secondary IP]	<code>vth-inst1-data-nic3</code>	<code>10.0.3.4</code> [Primary IP]		<code>10.0.3.X</code> [Secondary IP]	<code>vth-inst2-mgmt-nic1</code>	<code>10.0.1.6</code>	<code>vth-inst2-data-nic2</code>	<code>10.0.2.6</code> [Primary IP]		<code>10.0.2.X</code> [Secondary IP]	<code>vth-inst2-</code>	<code>10.0.3.6</code>
<code>vth-inst1-mgmt-nic1</code>	<code>10.0.1.4</code>																			
<code>vth-inst1-data-nic2</code>	<code>10.0.2.4</code> [Primary IP]																			
	<code>10.0.2.X</code> [Secondary IP]																			
<code>vth-inst1-data-nic3</code>	<code>10.0.3.4</code> [Primary IP]																			
	<code>10.0.3.X</code> [Secondary IP]																			
<code>vth-inst2-mgmt-nic1</code>	<code>10.0.1.6</code>																			
<code>vth-inst2-data-nic2</code>	<code>10.0.2.6</code> [Primary IP]																			
	<code>10.0.2.X</code> [Secondary IP]																			
<code>vth-inst2-</code>	<code>10.0.3.6</code>																			

Resource Name	Description	Default Value	
		<code>data-nic3</code>	[Primary IP] <code>10.0.3.x</code> [Secondary IP]
Network Security Group [NSG]	A security group is created for all the associated default interfaces.	<code>vth-nsg1</code>	<code>vth-nsg2</code>
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 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

Series	Size	Qualified Name
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 31 : Resource listing in the resource group

All resources				
Subscription equals all Resource group equals all Type equals all Location equals all Add filter				
	Name	Type	Resource group	Location
<input type="checkbox"/>	vth-inst1	Virtual machine	vth-rg11	South Central US
<input type="checkbox"/>	vth-inst1-data-nic2	Network Interface	vth-rg11	South Central US
<input type="checkbox"/>	vth-inst1-data-nic3	Network Interface	vth-rg11	South Central US
<input type="checkbox"/>	vth-inst1-mgmt-nic1	Network Interface	vth-rg11	South Central US
<input type="checkbox"/>	vth-inst1_OsDisk_1_bca879dbf43b4d578428ed846aa4b4288	Disk	VTH-RG11	South Central US
<input type="checkbox"/>	vth-inst2	Virtual machine	vth-rg11	South Central US
<input type="checkbox"/>	vth-inst2-mgmt-nic1	Network Interface	vth-rg11	South Central US
<input type="checkbox"/>	vth-inst2-mgmt-nic2	Network Interface	vth-rg11	South Central US
<input type="checkbox"/>	vth-inst2-mgmt-nic3	Network Interface	vth-rg11	South Central US
<input type="checkbox"/>	vth-inst2_OsDisk_1_63675204a29c416a9fbdc39ab695e28	Disk	VTH-RG11	South Central US
<input type="checkbox"/>	vth-nsg1	Network security group	vth-rg11	South Central US
<input type="checkbox"/>	vth-nsg2	Network security group	vth-rg11	South Central US
<input type="checkbox"/>	vth-vms2-vnet	Virtual network	vth-rg11	South Central US
<input type="checkbox"/>	vThunderIP1770126206	Public IP address	vth-rg11	South Central US
<input type="checkbox"/>	vThunderIP2072967164	Public IP address	vth-rg11	South Central US
<input type="checkbox"/>	vThunderIP317569421	Public IP address	vth-rg11	South Central US
<input type="checkbox"/>	vthunderstoarge1	Storage account	vth-rg11	South Central US

Configure Server VMSS

The following topics are covered:

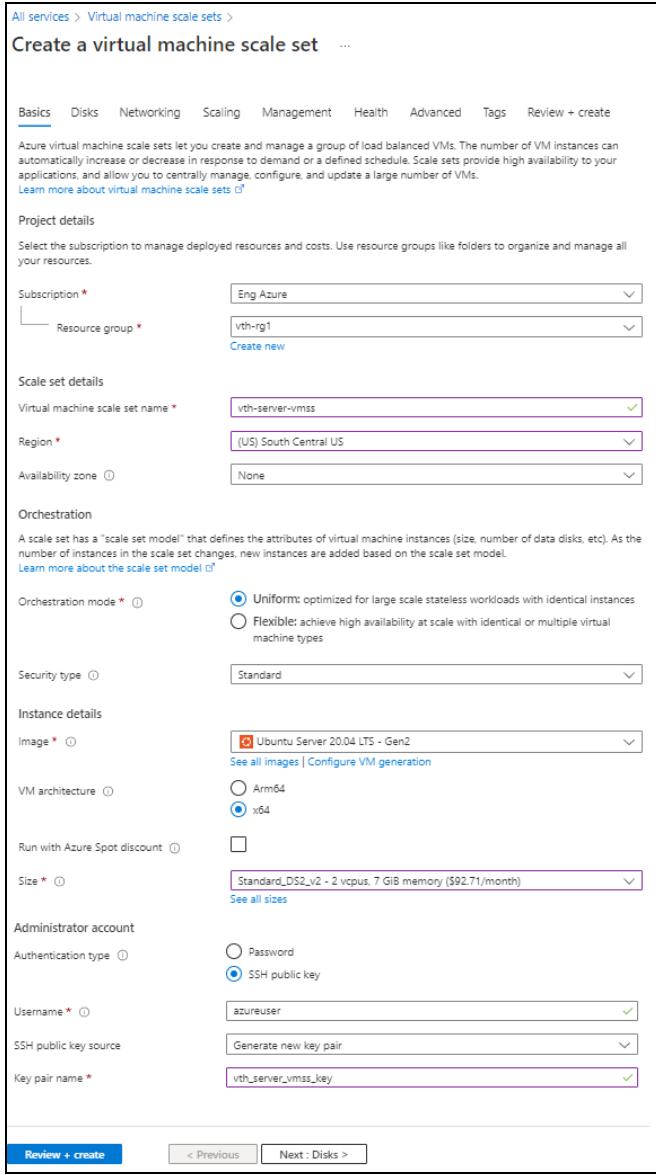
- [Create a Server Machine](#)
- [Verify the Server VMSS Creation](#)

Create a Server Machine

To create a Server machine, perform the following steps:

1. From Home, navigate thru **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 32 : Create a virtual machine scale set window - Basics tab



The screenshot shows the 'Create a virtual machine scale set' window in the Azure portal. The 'Basics' tab is selected. The configuration includes:

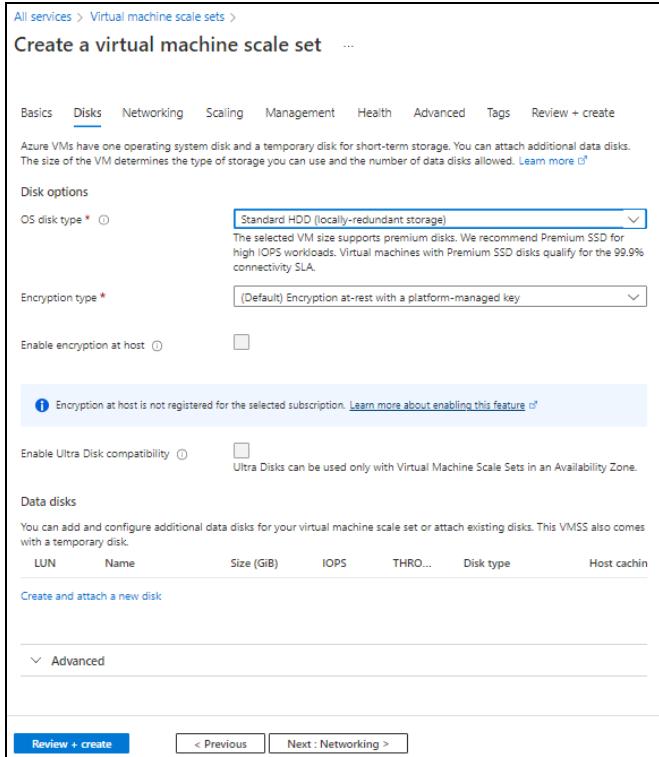
- Subscription:** Eng Azure
- Resource group:** vth-rg1
- Virtual machine scale set name:** vth-server-vmss
- Region:** (US) South Central US
- Availability zone:** None
- Orchestration mode:** Uniform (selected)
- Security type:** Standard
- Image:** Ubuntu Server 20.04 LTS - Gen2
- VM architecture:** x64
- Run with Azure Spot discount:** Unchecked
- Size:** Standard_DS2_v2 - 2 vcpus, 7 GB memory (\$92.71/month)
- Administrator account:**
 - Authentication type: SSH public key (selected)
 - Username: azureuser
 - SSH public key source: Generate new key pair
 - Key pair name: vth_server_vmss_key

At the bottom, there are buttons for **Review + create**, < Previous, and Next : Disks >.

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

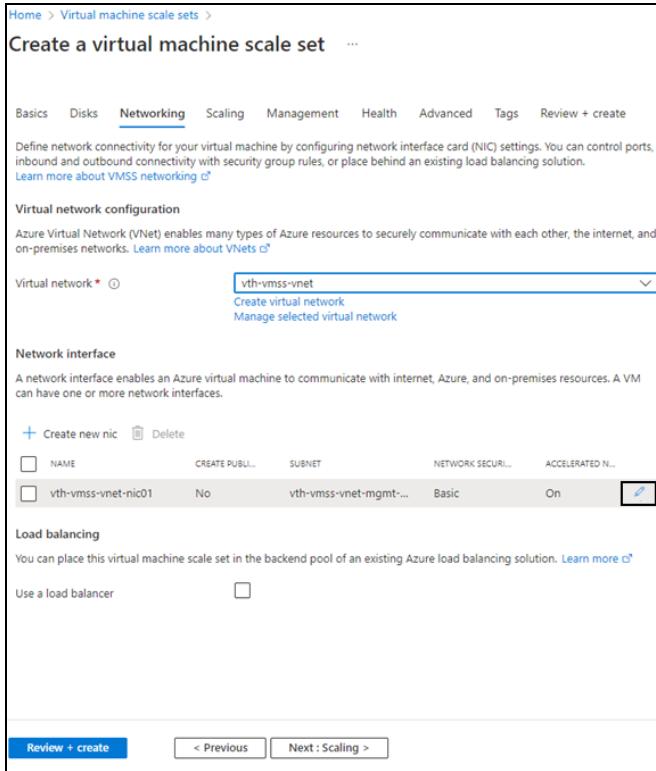
Figure 33 : Create a virtual machine scale set window - Disks tab



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 34 : Create a virtual machine scale set window - Networking tab

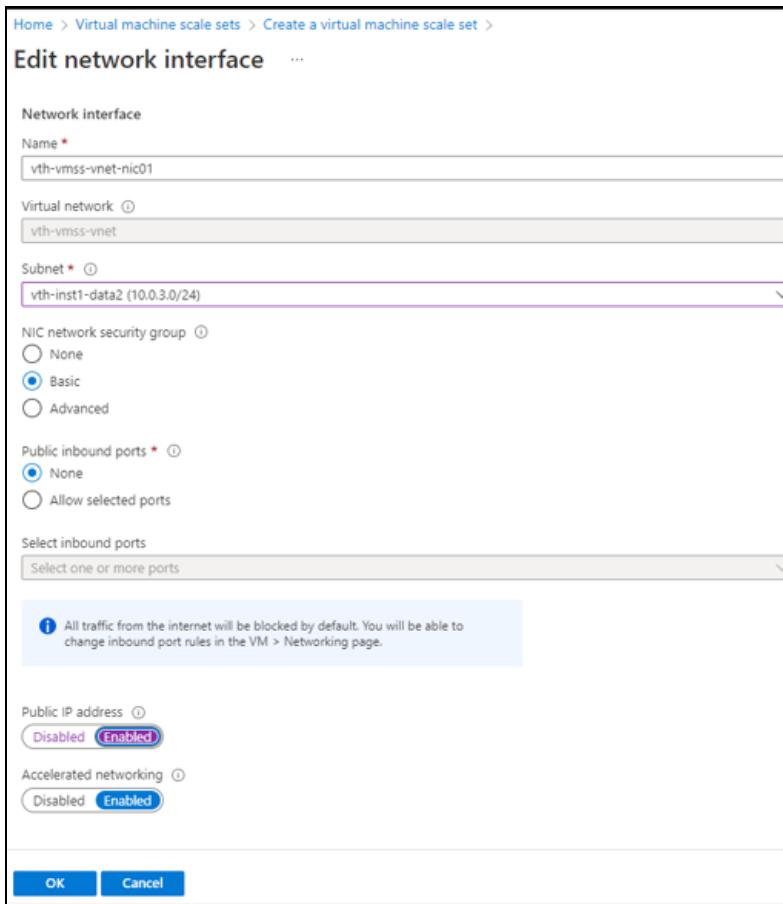


- If Data subnet 2 (Ethernet 2) value is not assigned to management NIC 1, click the edit button corresponding to it.

The **Edit Network Interface** window appears.

- Select Data subnet 2 value in the **Subnet** field and then click **OK**. Here, the Subnet 3 value is **10.0.3.0/24**.

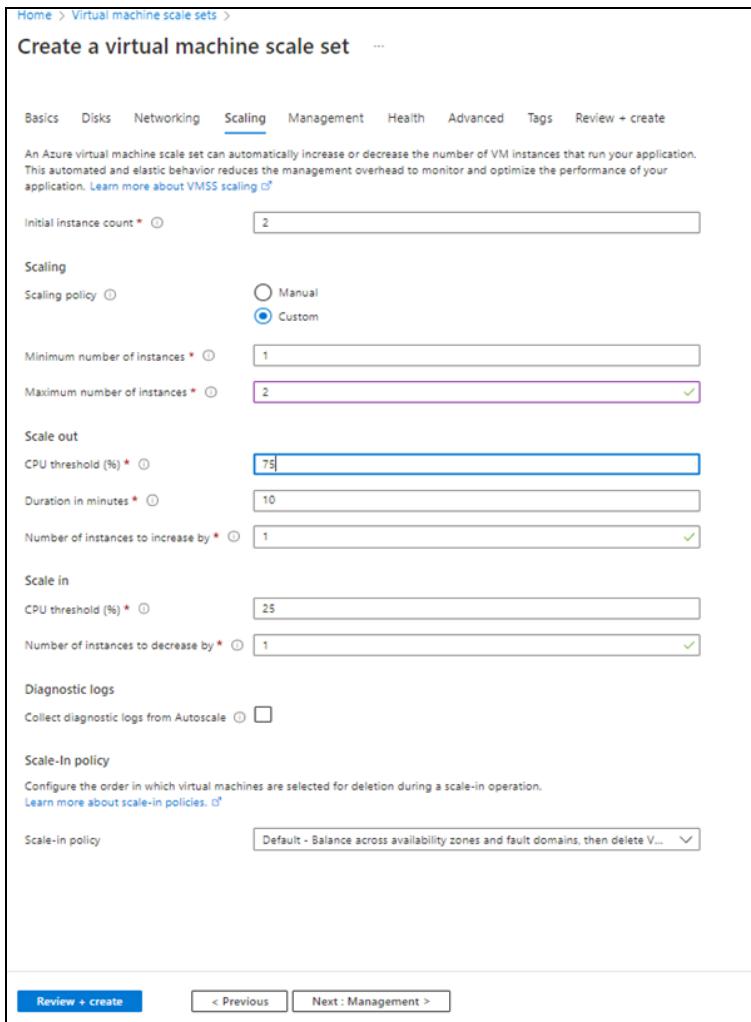
Figure 35 : Edit network interface window



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 36 : Create a virtual machine scale set window - Scaling tab



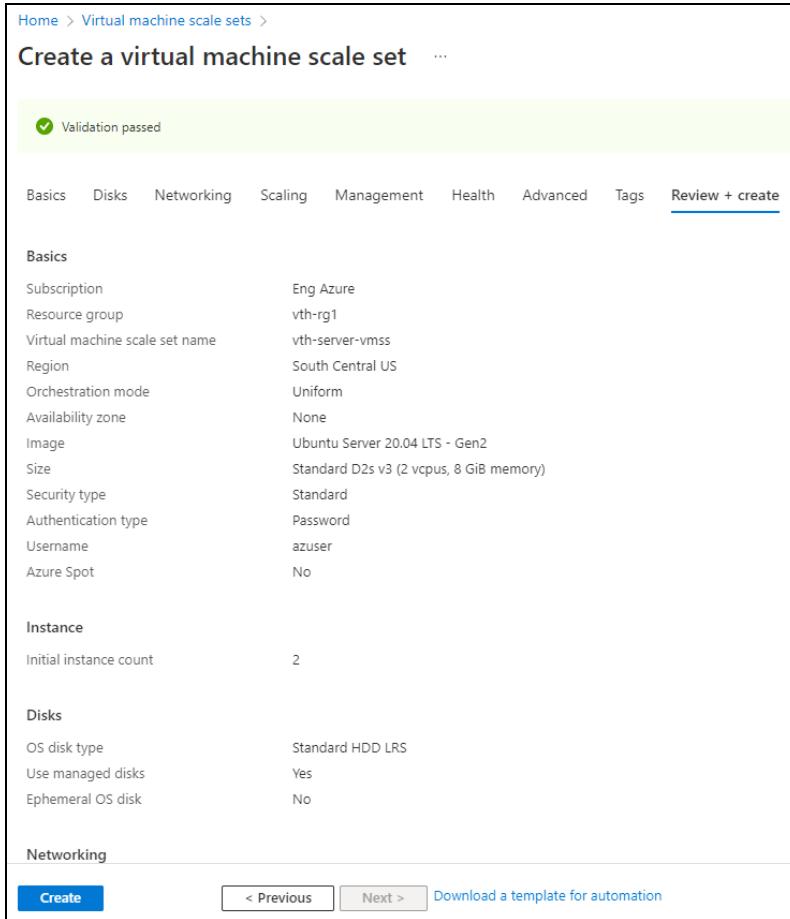
The screenshot shows the 'Create a virtual machine scale set' wizard on the 'Scaling' tab. The 'Scaling' tab is selected in the top navigation bar. The page includes a brief description of VMSS scaling and links to learn more. The configuration fields are as follows:

- Initial instance count:** 2
- Scaling policy:** Custom (selected)
- Minimum number of instances:** 1
- Maximum number of instances:** 2
- Scale out:**
 - CPU threshold (%): 75
 - Duration in minutes: 10
 - Number of instances to increase by: 1
- Scale in:**
 - CPU threshold (%): 25
 - Number of instances to decrease by: 1
- Diagnostic logs:** Collect diagnostic logs from Autoscale (unchecked)
- Scale-in policy:** Configure the order in which virtual machines are selected for deletion during a scale-in operation. A link to learn more about scale-in policies is provided. The current policy is set to "Default - Balance across availability zones and fault domains, then delete V...".

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

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

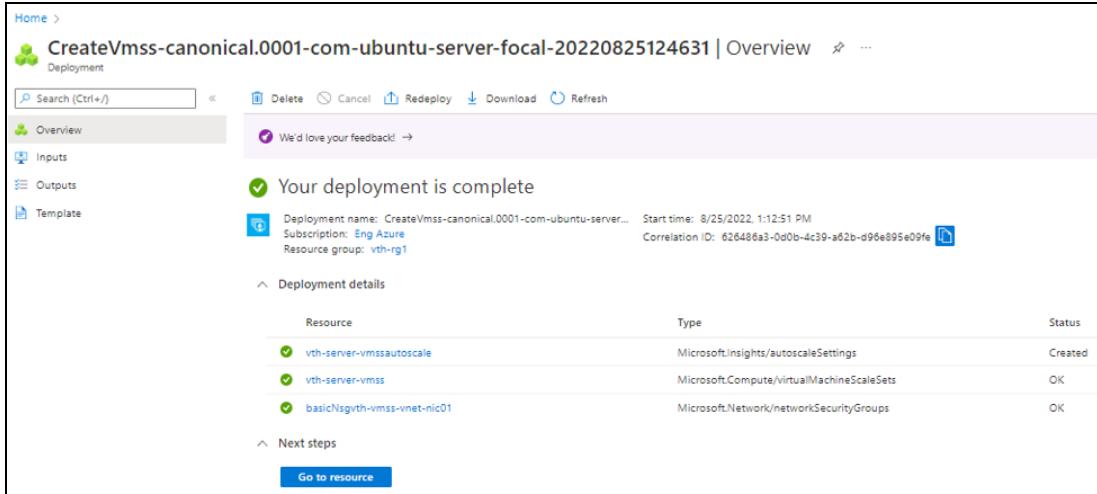
Figure 37 : Create a virtual machine scale set window - Review + create tab



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 38 : Create VMSS window



Resource	Type	Status
vth-server-vmssautoscale	Microsoft.Insights/autoscaleSettings	Created
vth-server-vmss	Microsoft.Compute/virtualMachineScaleSets	OK
basicNsgvth-vmss-vnet-nic01	Microsoft.Network/networkSecurityGroups	OK

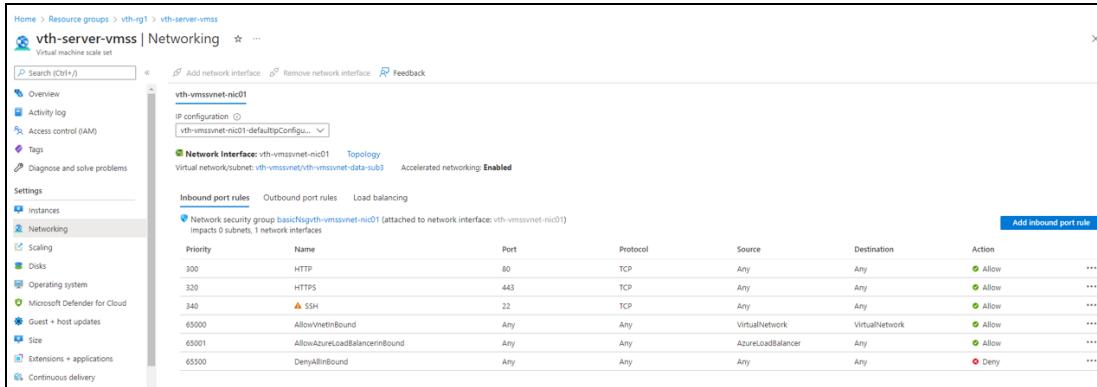
NOTE: It may take the system several minutes to display your resources.

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 39 : VMSS > Inbound port rules



Priority	Name	Port	Protocol	Source	Destination	Action
300	HTTP	80	TCP	Any	Any	Allow
320	HTTPS	443	TCP	Any	Any	Allow
340	SSH	22	TCP	Any	Any	Allow
65000	AllowAllInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65501	AllowAzureLoadBalancerInbound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

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](#)

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 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",
```

6. Configure VMSS.

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

7. Configure network interface cards.

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

8. 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
    }
]
}

```

- 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:

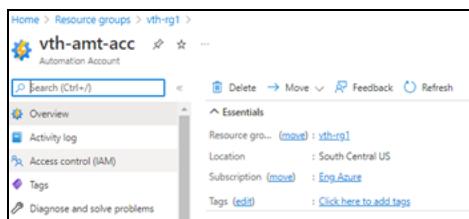
```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_AUTOMATION_ACCOUNT_2.ps1
```

Verify the Automation Account creation

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

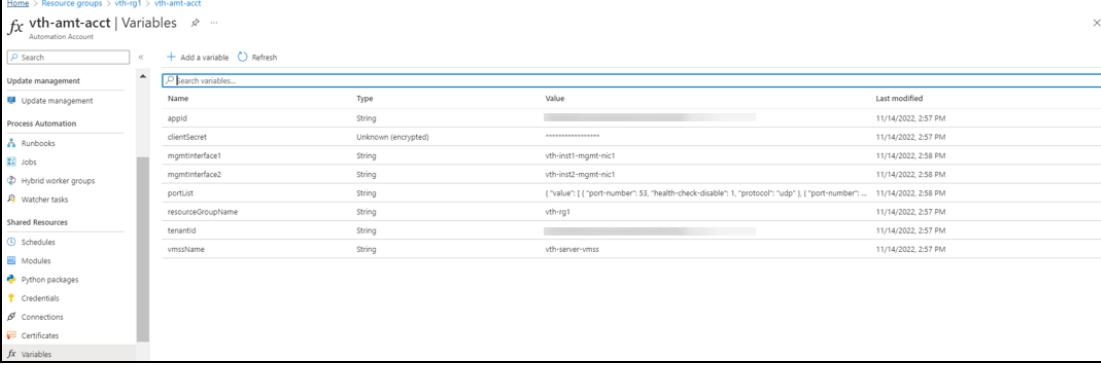
- From **Home**, navigate thru **Azure Services > Resource Group > <resource_group_name>**.
The selected resource group - Overview window is displayed.
- Under **Resources** tab, group the resources based on the resource type.
- Verify if the recently created automation account is listed under **Automation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

Figure 40 : Selected automation account - Overview window



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

Figure 41 : Selected automation account - Variables window



The screenshot shows the 'Variables' section of an Azure Automation Account named 'vth-amt-acc'. The variables listed are:

Name	Type	Value	Last modified
appid	String	[REDACTED]	11/14/2022, 2:57 PM
clientSecret	Unknown (encrypted)	[REDACTED]	11/14/2022, 2:57 PM
mgmtInterface1	String	vth-inst1-mgmt-nic1	11/14/2022, 2:58 PM
mgmtInterface2	String	vth-inst2-mgmt-nic1	11/14/2022, 2:58 PM
portlist	String	{"value": [{"port-number": 53, "health-check-disable": 1, "protocol": "udp"}, {"port-number": ...	11/14/2022, 2:58 PM
resourceGroupName	String	vth-rg1	11/14/2022, 2:57 PM
tenantId	String	[REDACTED]	11/14/2022, 2:57 PM
vmssName	String	vth-server-vmss	11/14/2022, 2:57 PM

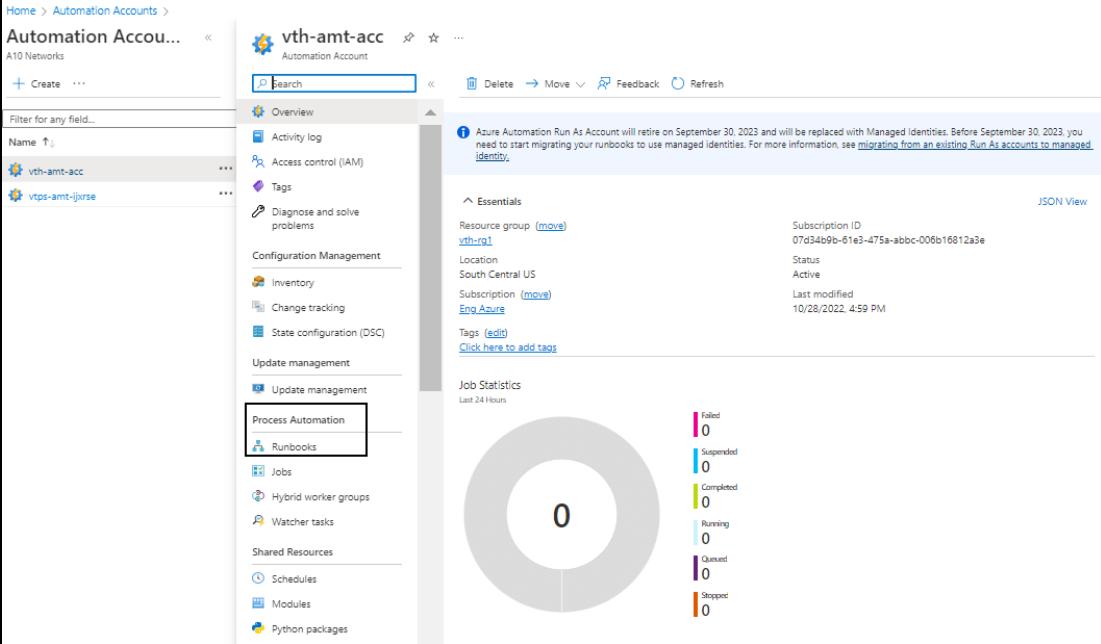
- Verify if all the variables associated with the automation account are listed.

Create Runbook

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

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

Figure 42 : Selected automation account window

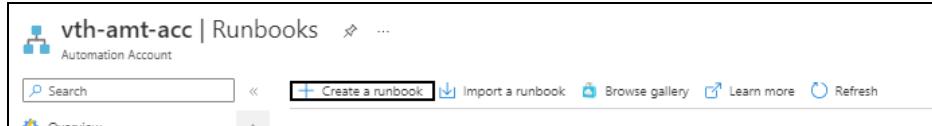


The screenshot shows the 'Overview' page of the Azure Automation Account 'vth-amt-acc'. The account is active and last modified on 10/28/2022, 4:59 PM. It is part of the resource group 'vth-rg1' in South Central US, using the 'Eng_Azure' subscription. The 'Process Automation' section is highlighted. A circular 'Job Statistics' chart indicates 0 failed, 0 suspended, 0 completed, 0 running, 0 queued, and 0 stopped jobs over the last 24 hours.

2. Select **Runbooks from left **Process Automation** panel.**

The <automation_account_name> - Runbooks window is displayed.

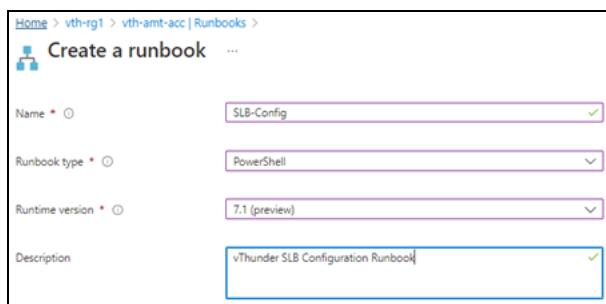
Figure 43 : Selected automation account - Runbooks window



3. Click **Create a runbook.**

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

Figure 44 : Create a runbook window



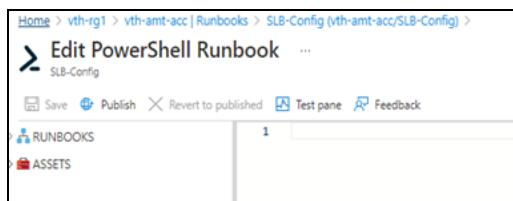
4. Select or enter the following information:

- Name: SLB-Config
- Runbook type: PowerShell
- Runtime version: 7.1
- Description

5. Click **Create.**

The **Edit PowerShell Runbook** is displayed.

Figure 45 : 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:

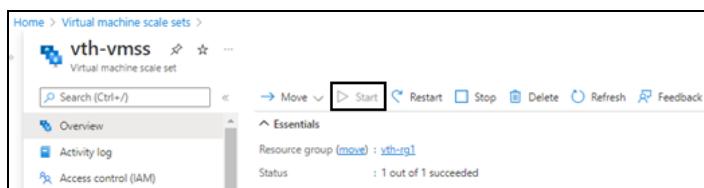
- [Initial Setup](#)
- [Create a Webhook](#)
- [Verify the Runbook Job creation](#)

Initial Setup

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

1. From **Home**, navigate thru **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 46 : 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_3.ps1 -runBookName "<runbook_name>"
```

Example:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_WEBHOOK_3.ps1 -runBookName "SLB-Config"
```

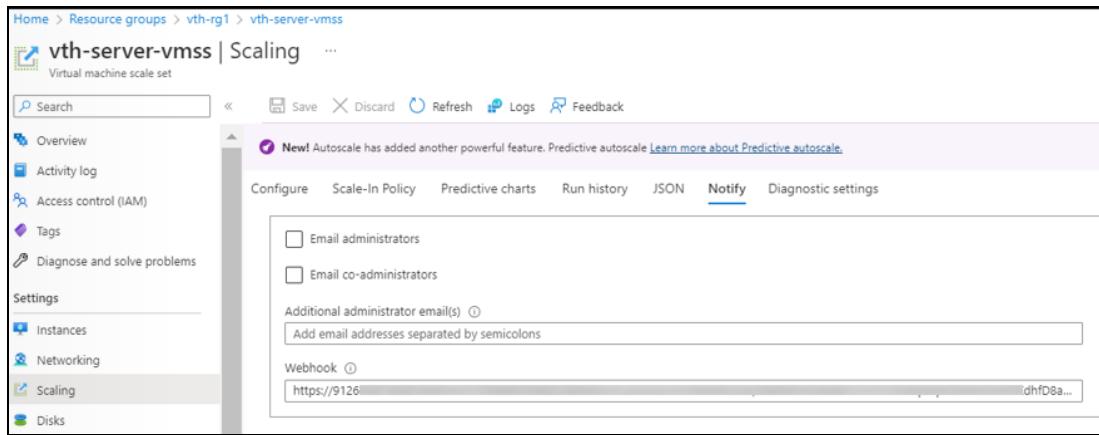
After the webhook installation is complete, the webhook url is displayed.

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 thru **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 47 : 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:

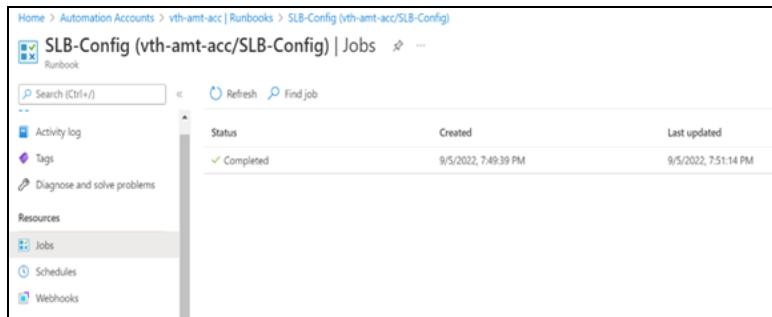
1. From Home, navigate thru Azure Services > Automation Accounts > <automation_account_name>.

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**.

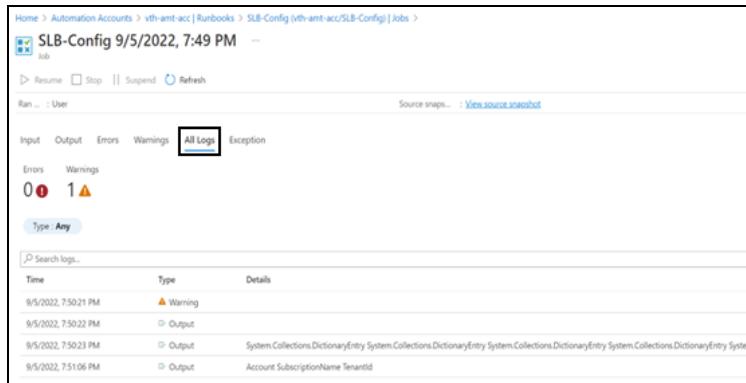
Figure 48 : Selected automation account - Jobs window



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 49 : 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  
        }  
    ]  
}
```

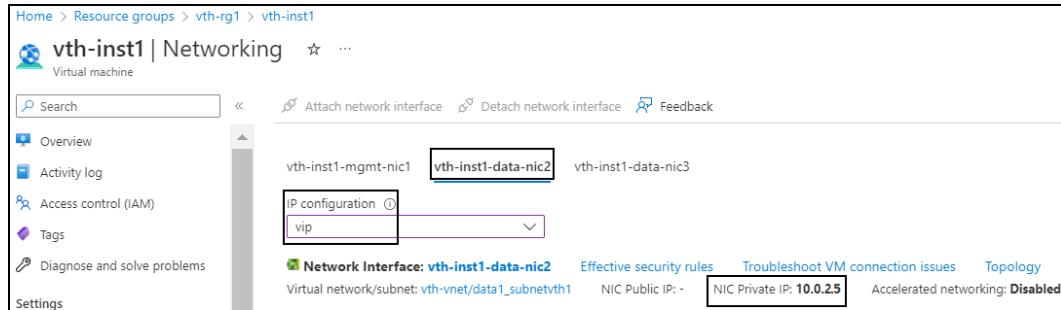
```
        ],
    },
```

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:

- From **Home**, navigate thru **Azure Services > Resource Group > <resource_group_name>**.
- Go to the first virtual machine instance. Here, first virtual machine instance is **vth-inst1**.
- Select the Data NIC 2 tab > **IP configuration** > **vip**. Here, Data NIC 2 is **vth-inst1-data-nic2**.

Figure 50 : Virtual machine - Networking window - Data NIC 2 tab



- Select **Networking** from the left **Settings** panel.
- Select the **NIC Private IP**.
- 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": [
        {
            "ip": "10.0.2.5"
        }
    ]
}
```

```

        "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"
    }
}

```

- 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:

- From PowerShell, navigate to the folder where you have downloaded the PowerShell template.
- 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_4.ps1 -resourceGroup <resource_group_name>
```

Example:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_SLB_CONFIG_4.ps1 -resourceGroup vth-rg1
```

A message is prompted to upload the SSL certificate.

```

SSL Certificate
Do you want to upload ssl certificate ?
[Y] Yes [N] 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
    },

```

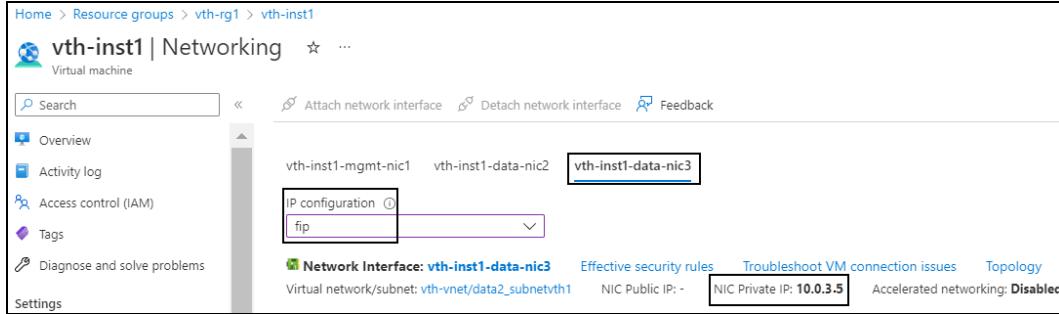
6. Configure VRID details.

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:

- From **Home**, navigate thru **Azure Services > Resource Group > <resource_group_name>**.
- 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 51 : 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_5.ps1 -  
resourceGroup <resource_group_name>
```

Example:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_HA_CONFIG_5.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": "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_6.ps1 -resourceGroupName <resource_group_name>
```

Example:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_GLM_CONFIG_6.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](#)

NOTE: For A10 vThunder default login credentials, send a request to [A10 Networks Support](#).

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 default login credentials provided by A10 Networks Support and change the default password as soon as you login for the first time:

```
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-->
vThunder(config)#admin <admin_username> password <new_password>
```

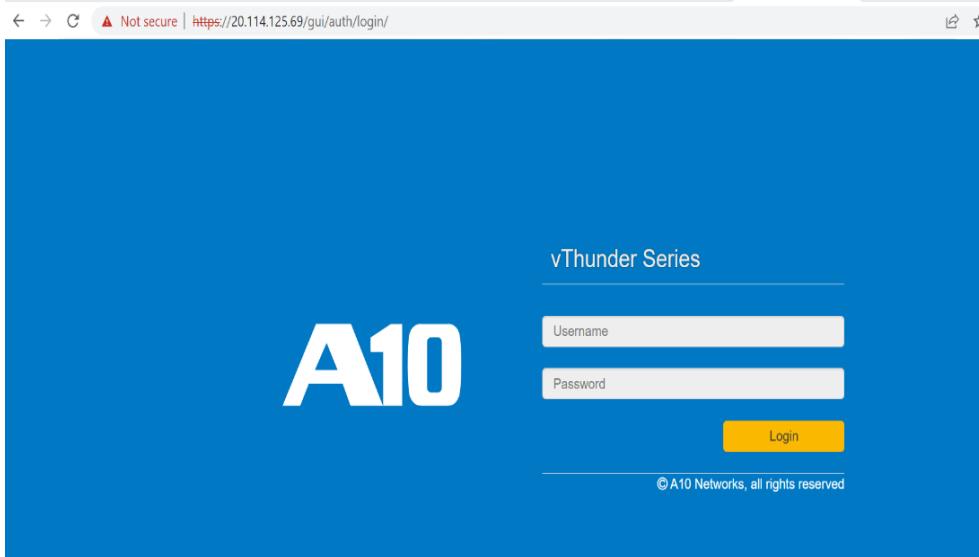
NOTE: It is highly recommended to change the default password when you login for the first time.

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 52 : vThunder GUI



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

Verify Deployment

To verify deployment thru 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
<hr/>			
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:

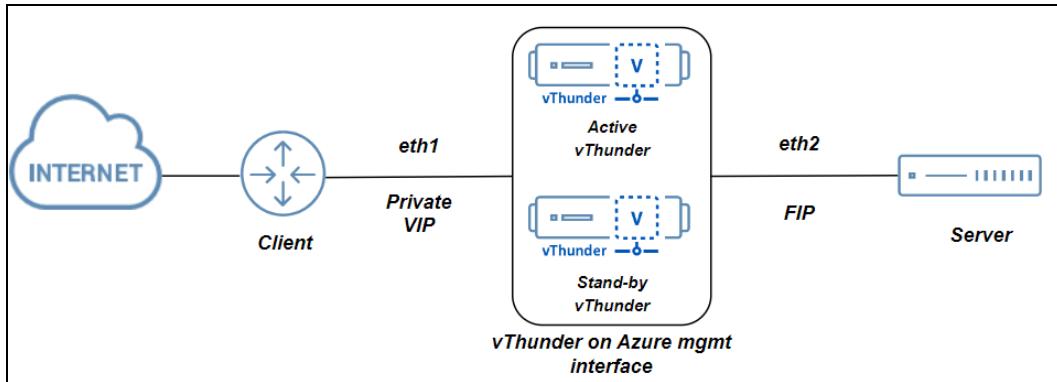
```
vThunder-ForcedStandby(config) #vrrp-a force-self-standby disable  
vThunder-Active(config) #
```

Deploy PowerShell Template 3NIC-2VM-HA-GLM-PVTVIP

[Figure 53](#) 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 53 : 3NIC-2VM-HA-GLM-PVTVIP Topology



The following topics are covered:

System Requirements	137
Create vThunder Instances	141
Configure Server and Client Machine	145
Configure vThunder as an SLB	163
Configure High Availability	169
Configure vThunder using GLM	172
Verify Deployment	175

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 .
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
	<p>access geo-redundant storage (RA-GRS)</p> <p>Account kind: Storagev2 (general purpose v2)</p>	
Virtual Machine (VM) Instance	<p>Two virtual machine instances are created for vThunder.</p> <p>Product: A10 vThunder</p> <p>Operating system: Linux</p> <p>Default Size: Standard_B4ms (4 vCPUs, 16 GiB Memory)</p> <p>NOTE: Before selecting any VM size, it is highly recommended to do an assessment of your projected traffic.</p> <p>Table 11 lists the supported VM sizes.</p>	<p>vth-inst1 vth-inst2</p>
Virtual	A virtual network is	vth-vnet

Resource Name	Description	Default Value																				
Cloud Network [VCN]	assigned to the virtual 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]	<p>Two types of interfaces are created for each vThunder instance:</p> <ul style="list-style-type: none"> Management Interface with public IP Data Interface with primary private IP [Ethernet 1, Ethernet 2] <p>NOTE: The secondary IP of data interface is taken from DHCP server.</p>	<table border="1"> <tbody> <tr> <td>vth-inst1-mgmt-nic1</td><td>10.0.1.4</td></tr> <tr> <td>vth-inst1-data-nic2</td><td>10.0.2.4 [Primary IP]</td></tr> <tr> <td></td><td>10.0.2.X [Secondary IP]</td></tr> <tr> <td>vth-inst1-data-nic3</td><td>10.0.3.4 [Primary IP]</td></tr> <tr> <td></td><td>10.0.3.X [Secondary IP]</td></tr> <tr> <td>vth-inst2-mgmt-nic1</td><td>10.0.1.6</td></tr> <tr> <td>vth-inst2-data-nic2</td><td>10.0.2.6 [Primary IP]</td></tr> <tr> <td></td><td>10.0.2.X [Secondary IP]</td></tr> <tr> <td>vth-inst2-data-nic3</td><td>10.0.3.6 [Primary IP]</td></tr> <tr> <td></td><td>10.0.3.X [Secondary IP]</td></tr> </tbody> </table>	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]
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	A security group is cre-	vth-inst1-nsg																				

Resource Name	Description	Default Value
Security Group [NSG]	ated for all the associated default interfaces.	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 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_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_GL_M_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_GL_M_PVTVIP_1.ps1
-resourceGroup <resource_group_name> -location "<location_name>"
```

Example:

[Deploy PowerShell Template 3NIC-2VM-HA-GLM-PVTVIP](#)

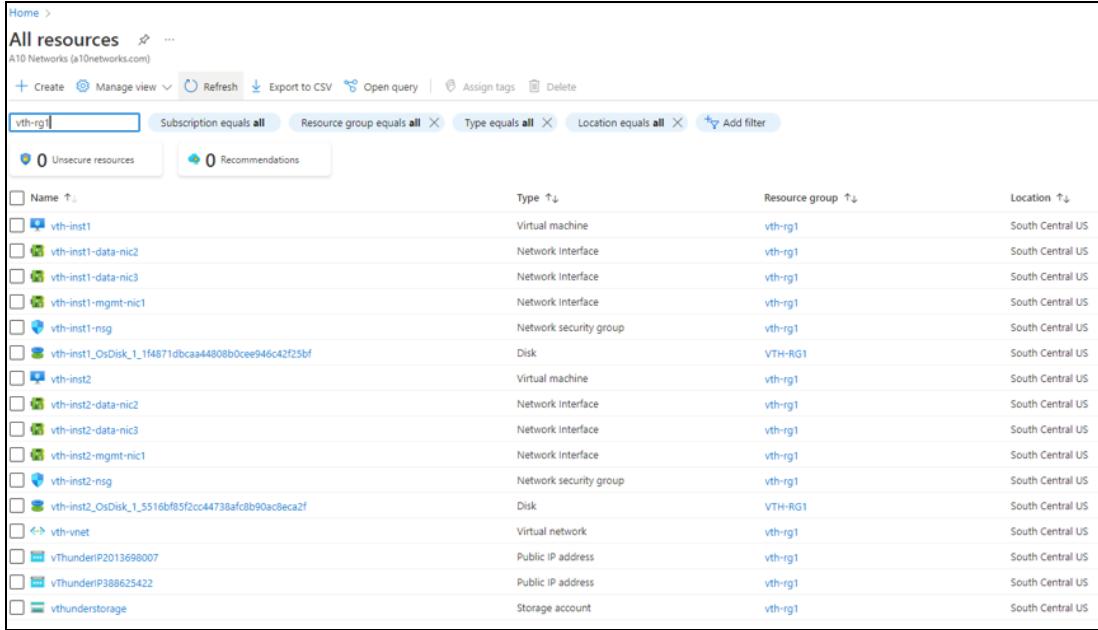
```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_HA_GL_M_PVTVIP_1.ps1
-resourceGroup vth-rg1 -location "south central us"

cmdlet PS_TMPL_3NIC_2VM_HA_GL_M_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.

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

Figure 54 : Resource listing in the resource group



The screenshot shows the Azure portal's 'All resources' view for the 'vth-rg1' resource group. The table lists various resources with their details:

Name	Type	Resource group	Location
vth-inst1	Virtual machine	vth-rg1	South Central US
vth-inst1-data-nic2	Network Interface	vth-rg1	South Central US
vth-inst1-data-nic3	Network Interface	vth-rg1	South Central US
vth-inst1-mgmt-nic1	Network Interface	vth-rg1	South Central US
vth-inst1-nsg	Network security group	vth-rg1	South Central US
vth-inst1_OsDisk_1_f14871dbcaa44808b0cee946c42f25bf	Disk	VTH-RG1	South Central US
vth-inst2	Virtual machine	vth-rg1	South Central US
vth-inst2-data-nic2	Network Interface	vth-rg1	South Central US
vth-inst2-data-nic3	Network Interface	vth-rg1	South Central US
vth-inst2-mgmt-nic1	Network Interface	vth-rg1	South Central US
vth-inst2-nsg	Network security group	vth-rg1	South Central US
vth-inst2_OsDisk_1_5516bf85f2cc44738afc8b90ac8eca2f	Disk	VTH-RG1	South Central US
vth-net	Virtual network	vth-rg1	South Central US
vThunderIP2013698007	Public IP address	vth-rg1	South Central US
vThunderIP388625422	Public IP address	vth-rg1	South Central US
vthunderstorage	Storage account	vth-rg1	South Central US

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 thru **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

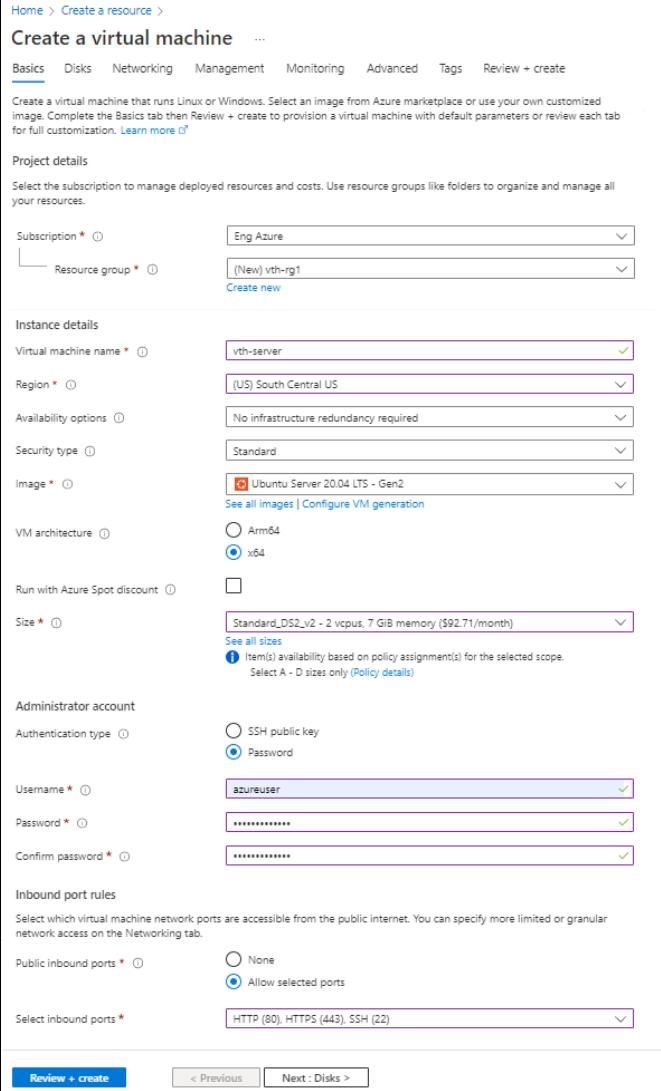
Administrator account

- Depending upon the Authentication type, provide the information.

Inbound port rules

- Public inbound ports
- Select inbound ports

Figure 55 : Create a virtual machine window - Basics tab



Home > Create a resource >

Create a virtual machine

[Basics](#) [Disks](#) [Networking](#) [Management](#) [Monitoring](#) [Advanced](#) [Tags](#) [Review + create](#)

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * [Eng Azure](#) [Resource group *](#) [\(New\) vth-rg1](#) [Create new](#)

Instance details

Virtual machine name * [vth-server](#)

Region * [\(US\) South Central US](#)

Availability options [No infrastructure redundancy required](#)

Security type [Standard](#)

Image * [Ubuntu Server 20.04 LTS - Gen2](#) [See all images](#) [Configure VM generation](#)

VM architecture [x64](#)

Run with Azure Spot discount [\(checkbox\)](#)

Size * [Standard_DS2_v2 - 2 vcpus, 7 GiB memory \(\\$92.71/month\)](#) [See all sizes](#)

Item(s) availability based on policy assignment(s) for the selected scope.
Select A - D sizes only ([Policy details](#))

Administrator account

Authentication type [Password](#)

Username * [azureuser](#)

Password * [*****](#)

Confirm password * [*****](#)

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the [Networking](#) tab.

Public inbound ports * [None](#) [Allow selected ports](#)

Select inbound ports * [HTTP \(80\), HTTPS \(443\), SSH \(22\)](#)

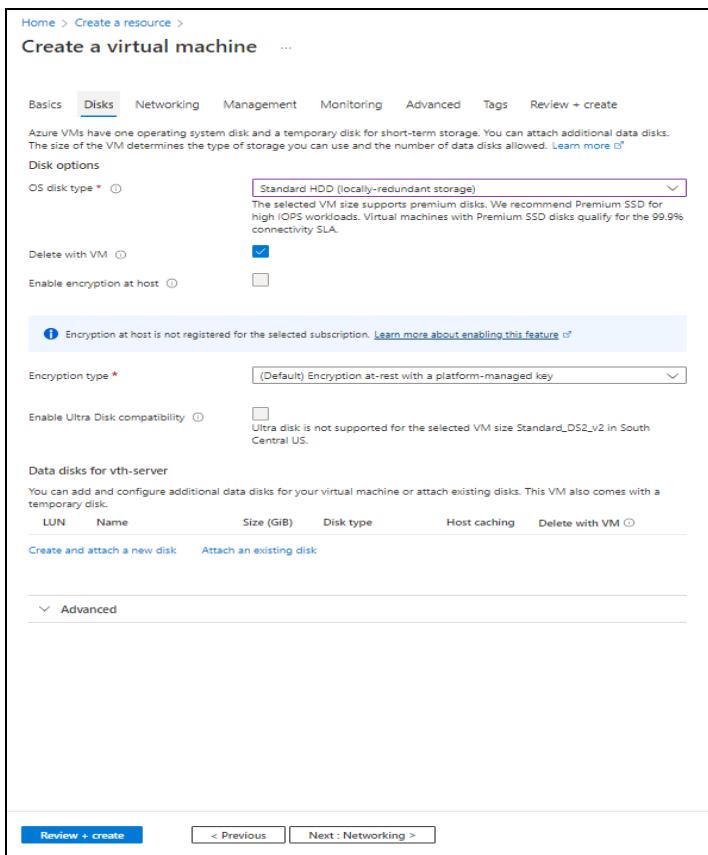
[Review + create](#) [< Previous](#) [Next : Disks >](#)

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 56 : Create a virtual machine window - Disks tab

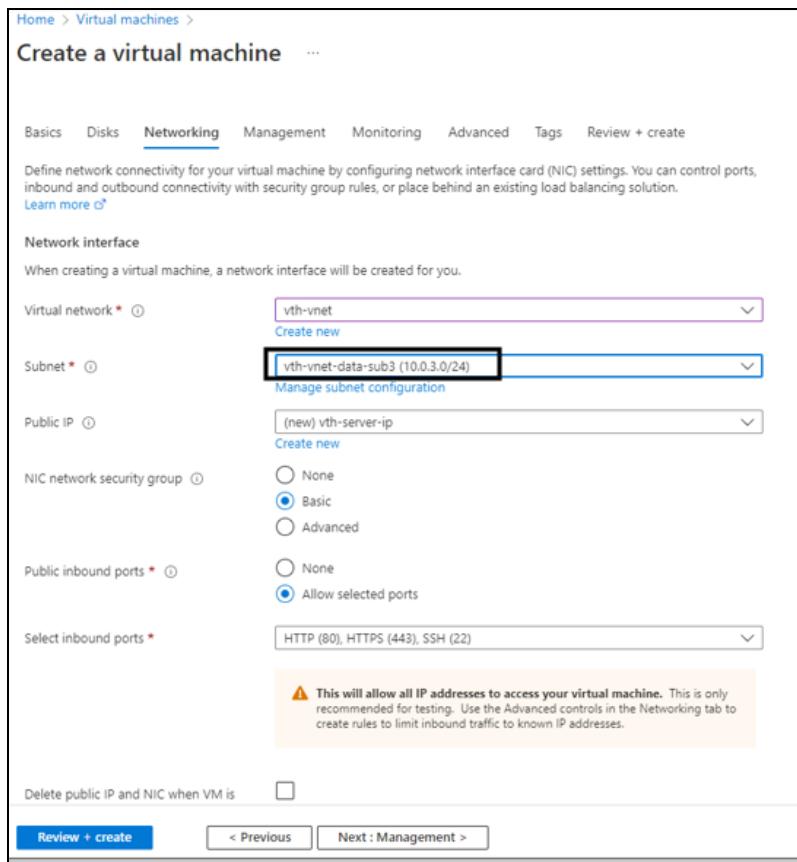


5. Leave the remaining fields as is and click **Next : Networking** at the bottom of the window.
6. Select or enter the following mandatory information in the **Networking** tab:

Network interface

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

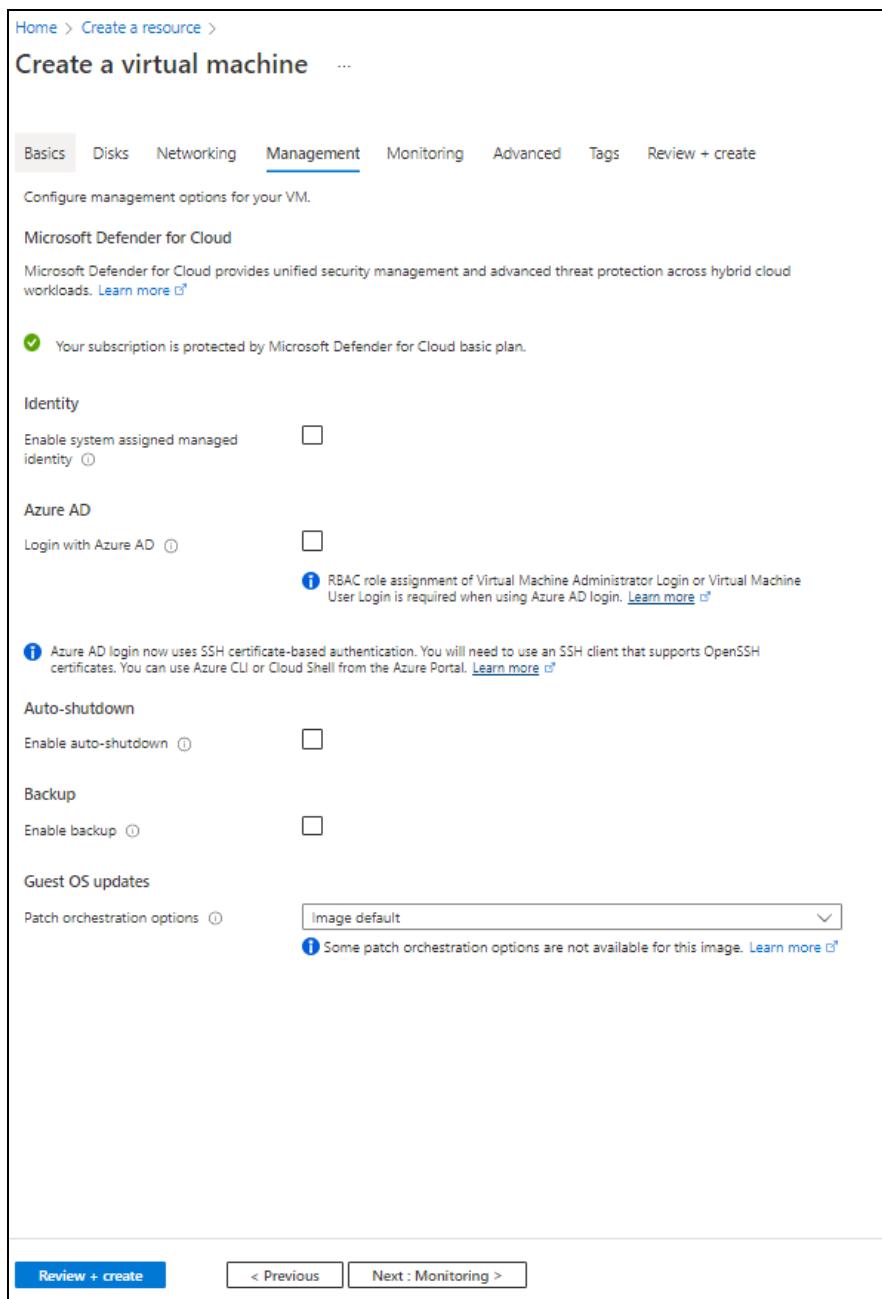
Figure 57 : Create a virtual machine window - Networking tab



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.

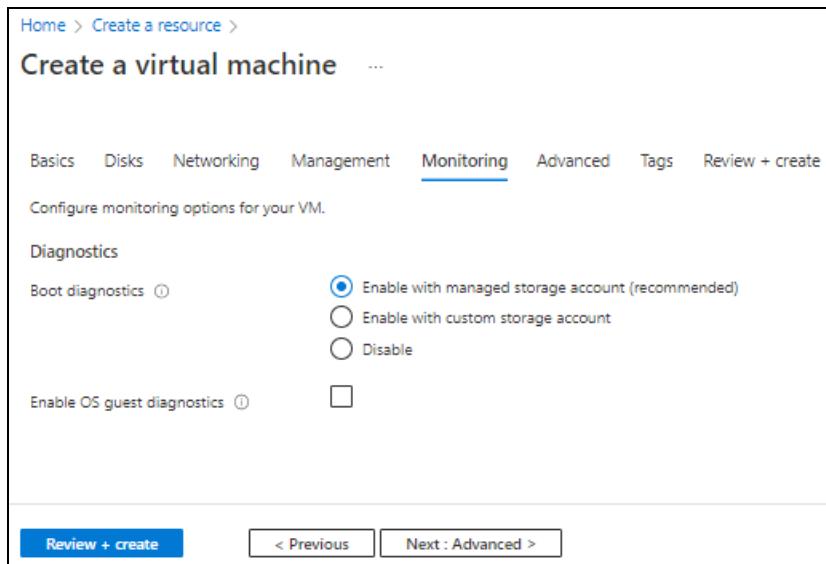
Figure 58 : Create a virtual machine window - Management tab



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

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

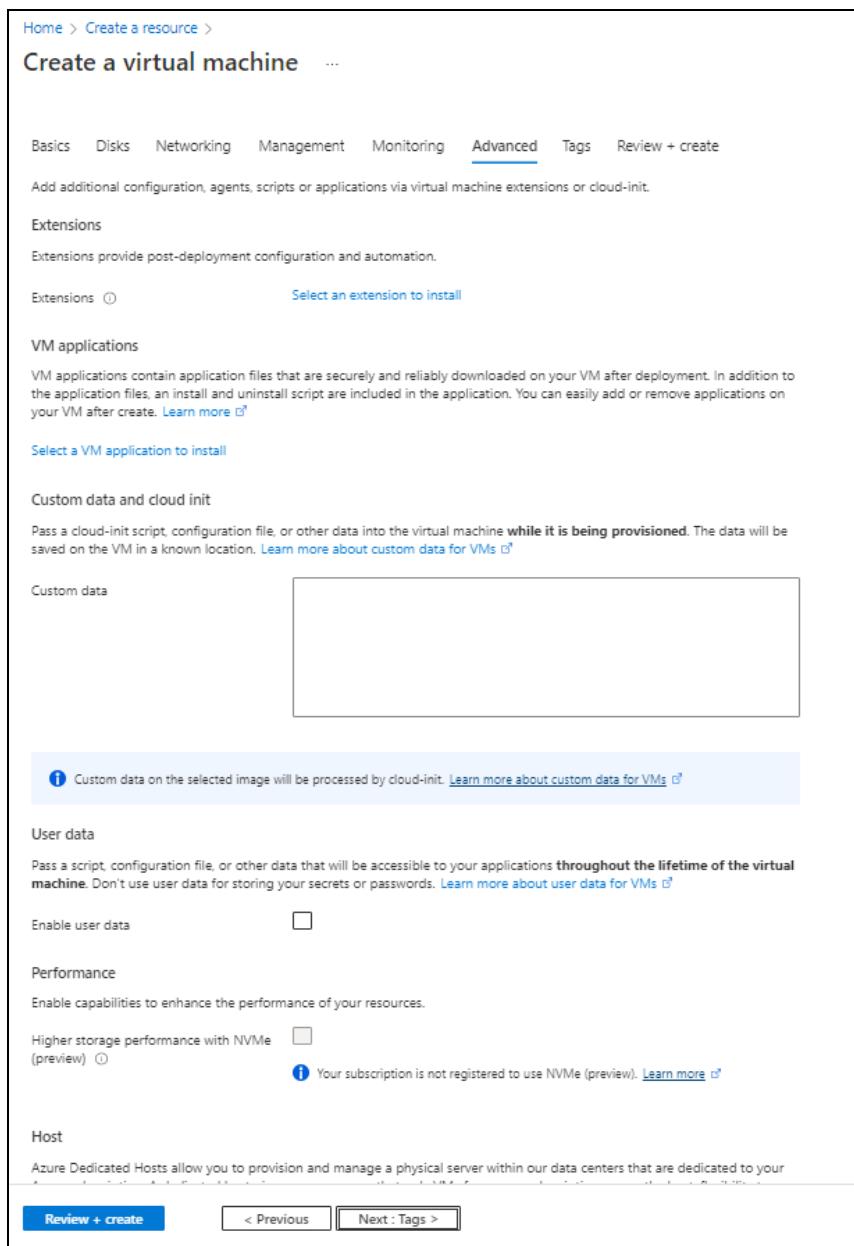
Figure 59 : Create a virtual machine window - Monitoring tab



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

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

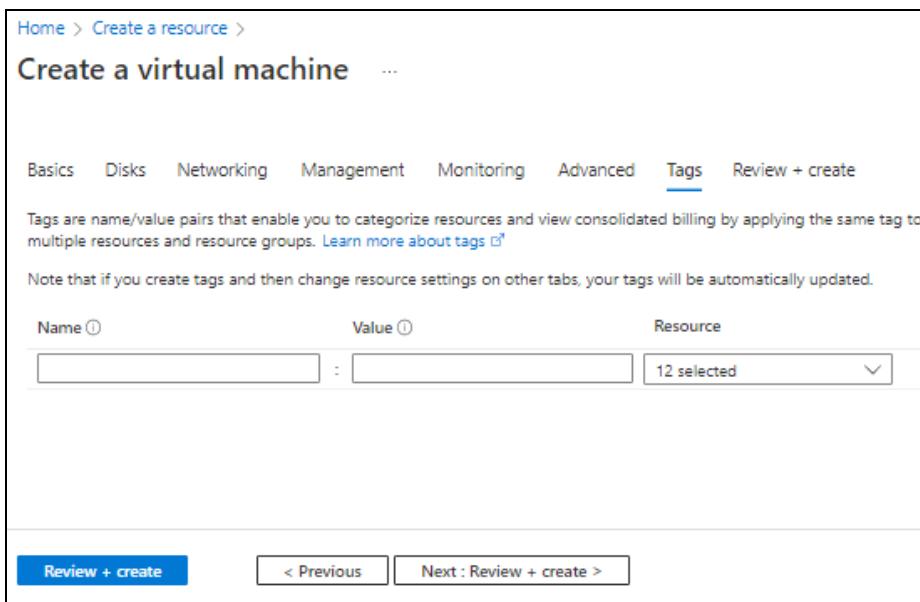
Figure 60 : Create a virtual machine window - Advanced tab



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

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

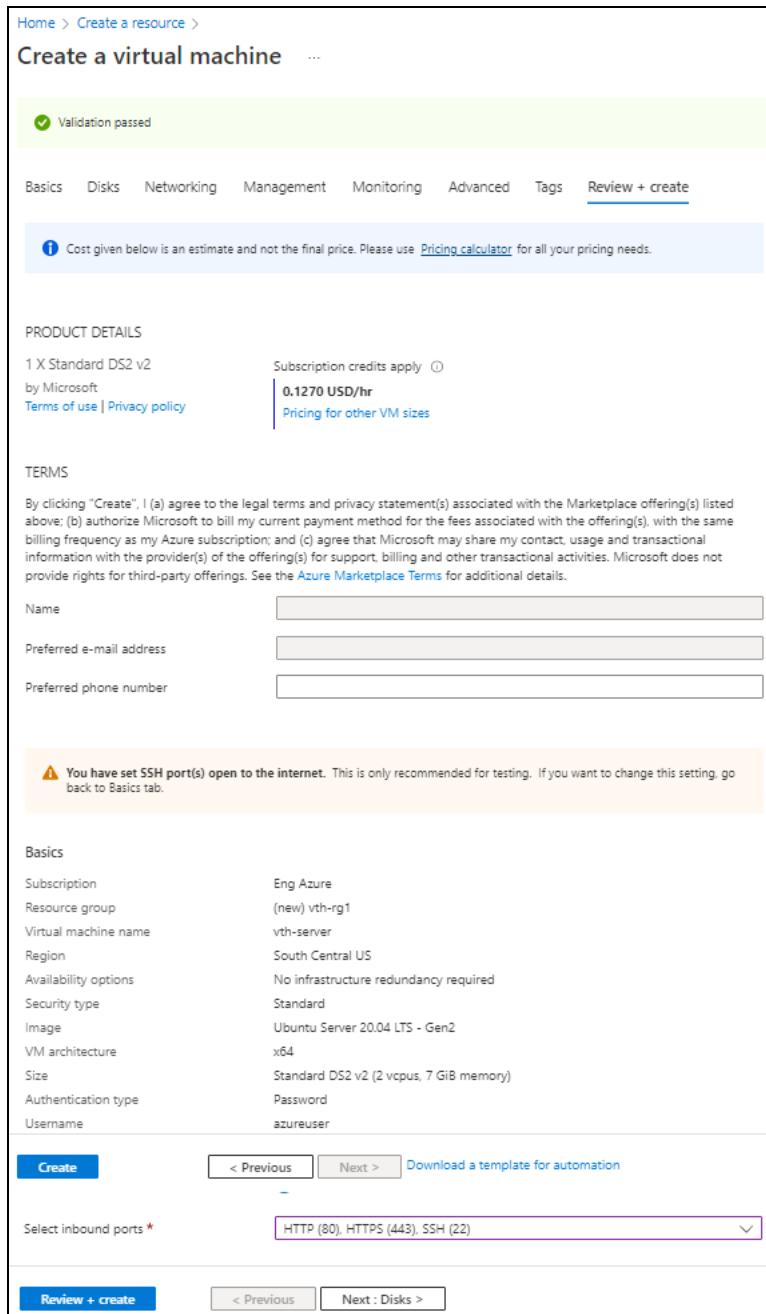
Figure 61 : Create a virtual machine window - Tags tab



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 62 : Create a virtual machine window - Review + create tab



- Click **Create** at the bottom of the window.
The Server machine gets created.

Create a Client Machine

To create a Client machine, perform the following steps:

1. From Home, navigate thru **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

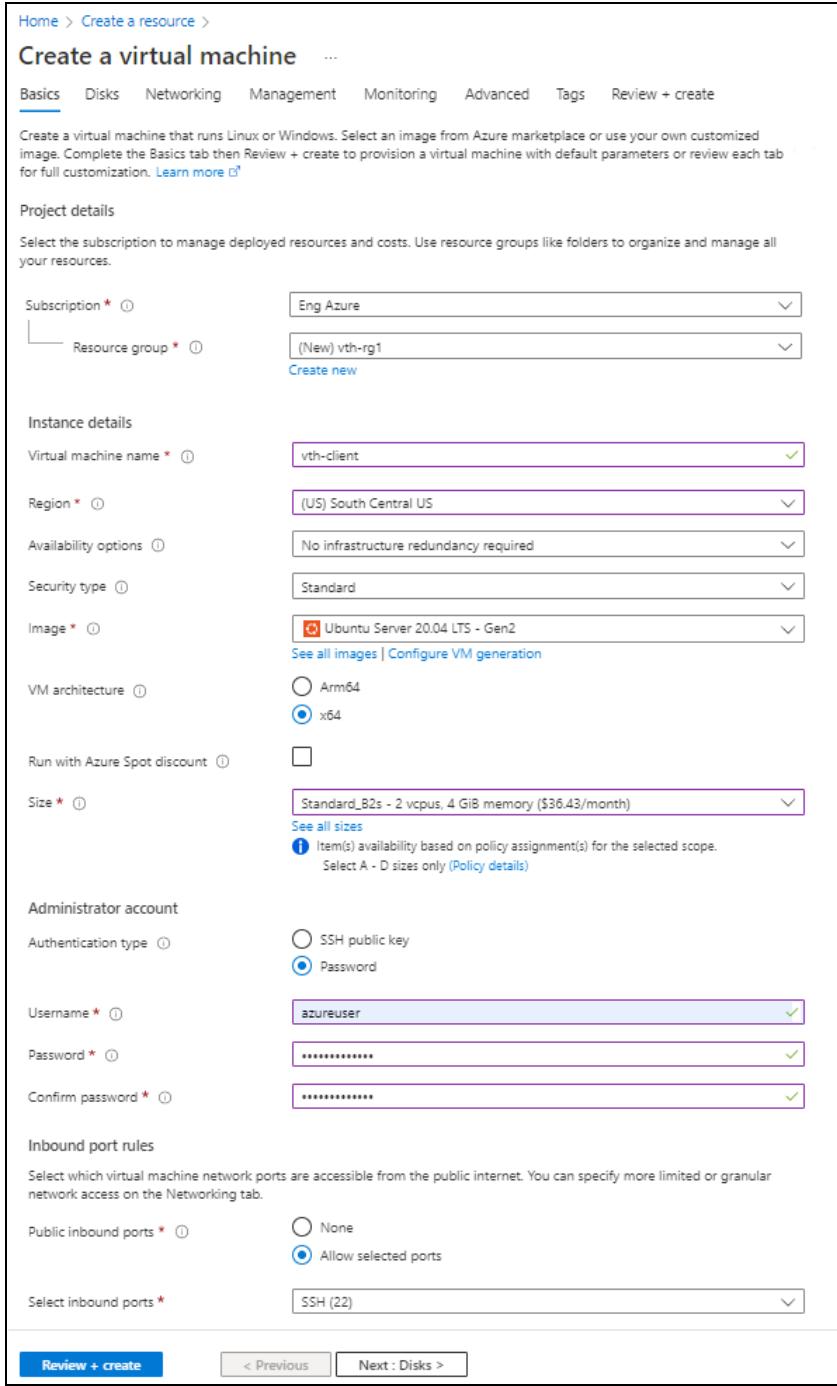
Administrator account

- Depending upon the Authentication type, provide the information.

Inbound port rules

- Public inbound ports
- Select inbound ports

Figure 63 : Create a virtual machine window - Basics tab



The screenshot shows the 'Create a virtual machine' Basics tab configuration window. The 'Subscription' dropdown is set to 'Eng Azure'. The 'Resource group' dropdown shows '(New) vth-rg1' with a 'Create new' link below it. The 'Virtual machine name' is 'vth-client'. The 'Region' is '(US) South Central US'. Under 'Availability options', 'No infrastructure redundancy required' is selected. The 'Security type' is 'Standard'. The 'Image' dropdown shows 'Ubuntu Server 20.04 LTS - Gen2' with a 'See all images | Configure VM generation' link. The 'VM architecture' is 'x64'. The 'Size' dropdown shows 'Standard_B2s - 2 vcpus, 4 GiB memory (\$36.43/month)' with a 'See all sizes' link and a note about policy assignment(s). The 'Administrator account' section shows 'Authentication type' as 'Password' with 'Username' 'azureuser' and 'Confirm password' both set to '*****'. Under 'Inbound port rules', 'Public inbound ports' is set to 'Allow selected ports' with 'Select inbound ports' showing 'SSH (22)'. At the bottom, there are 'Review + create', '< Previous', and 'Next : Disks >' buttons.

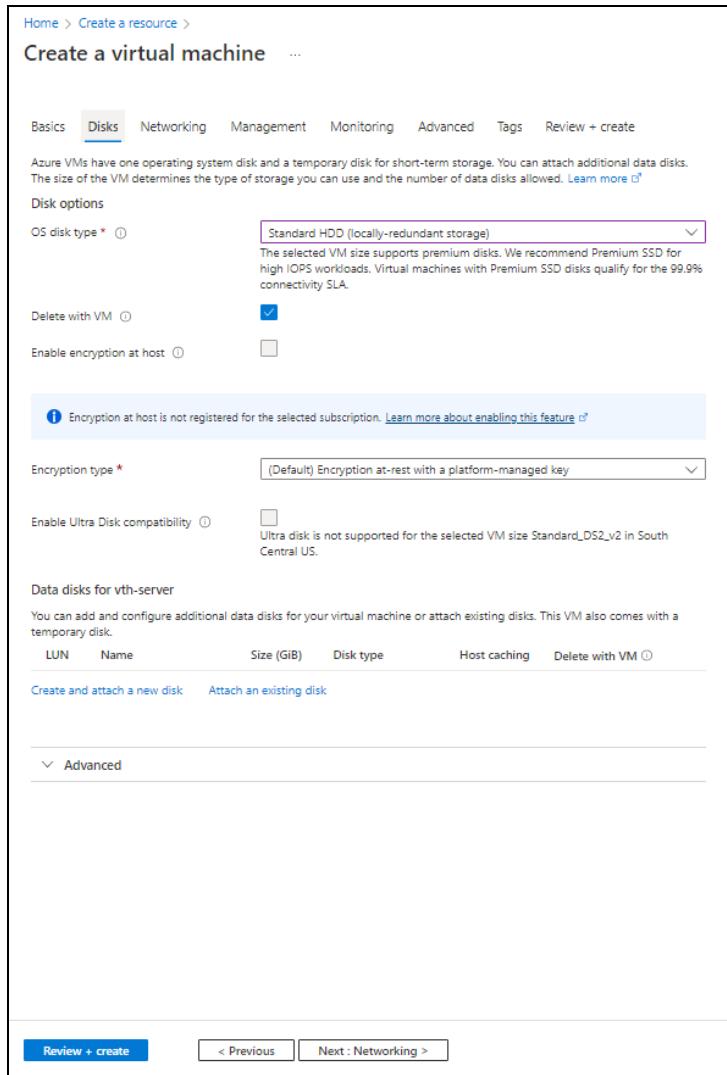
- Leave the remaining fields as is and click **Next : Disks** at the bottom of the window.

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

Disk options

- OS disk type
- Encryption type

Figure 64 : Create a virtual machine window - Disks tab



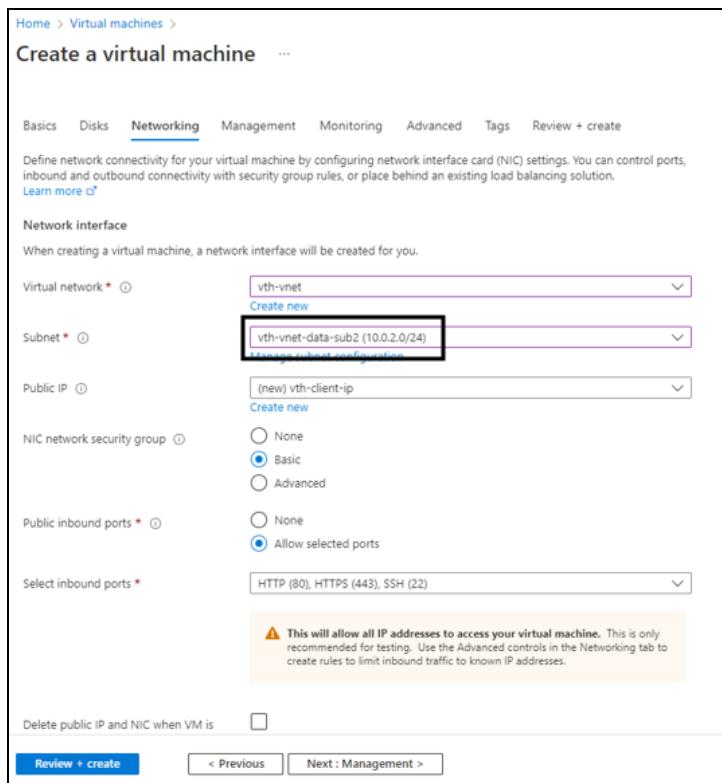
5. Leave the remaining fields as is and click **Next : Networking** at the bottom of the window.

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

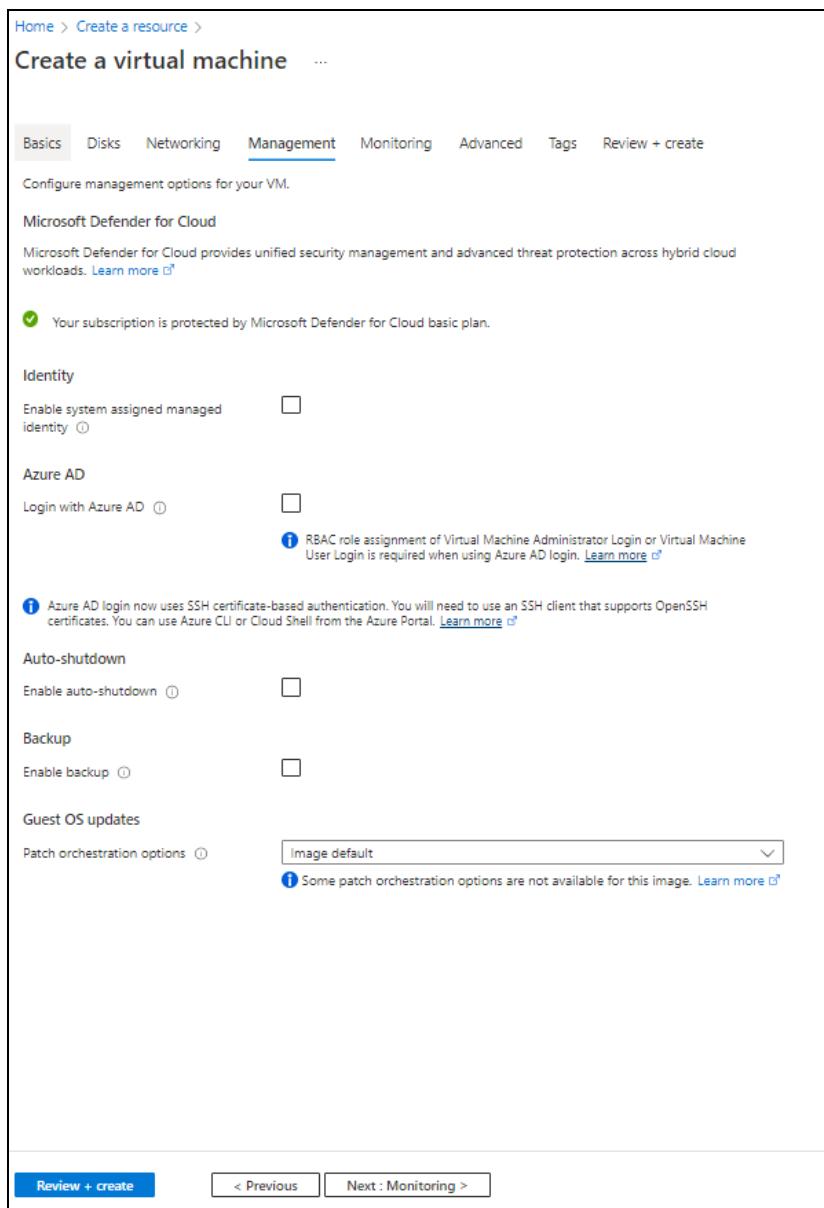
Figure 65 : Create a virtual machine window - Networking tab



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.

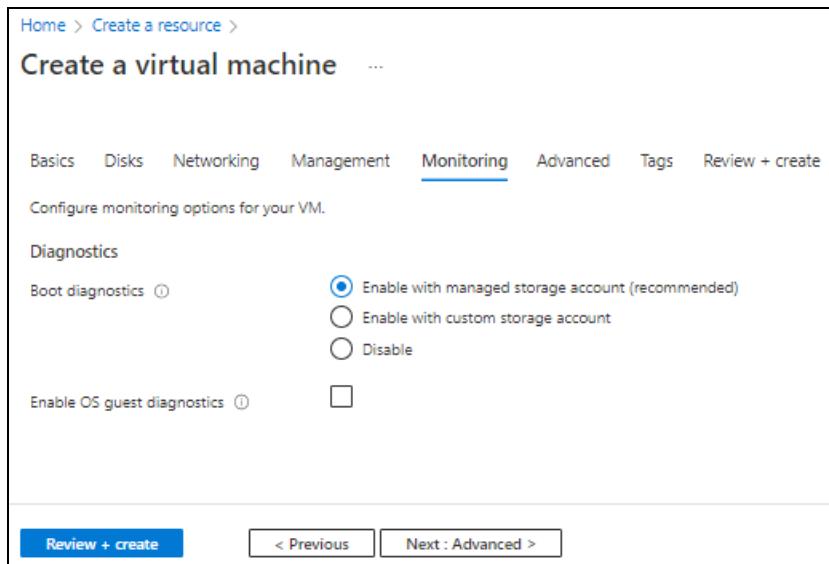
Figure 66 : Create a virtual machine window - Management tab



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

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

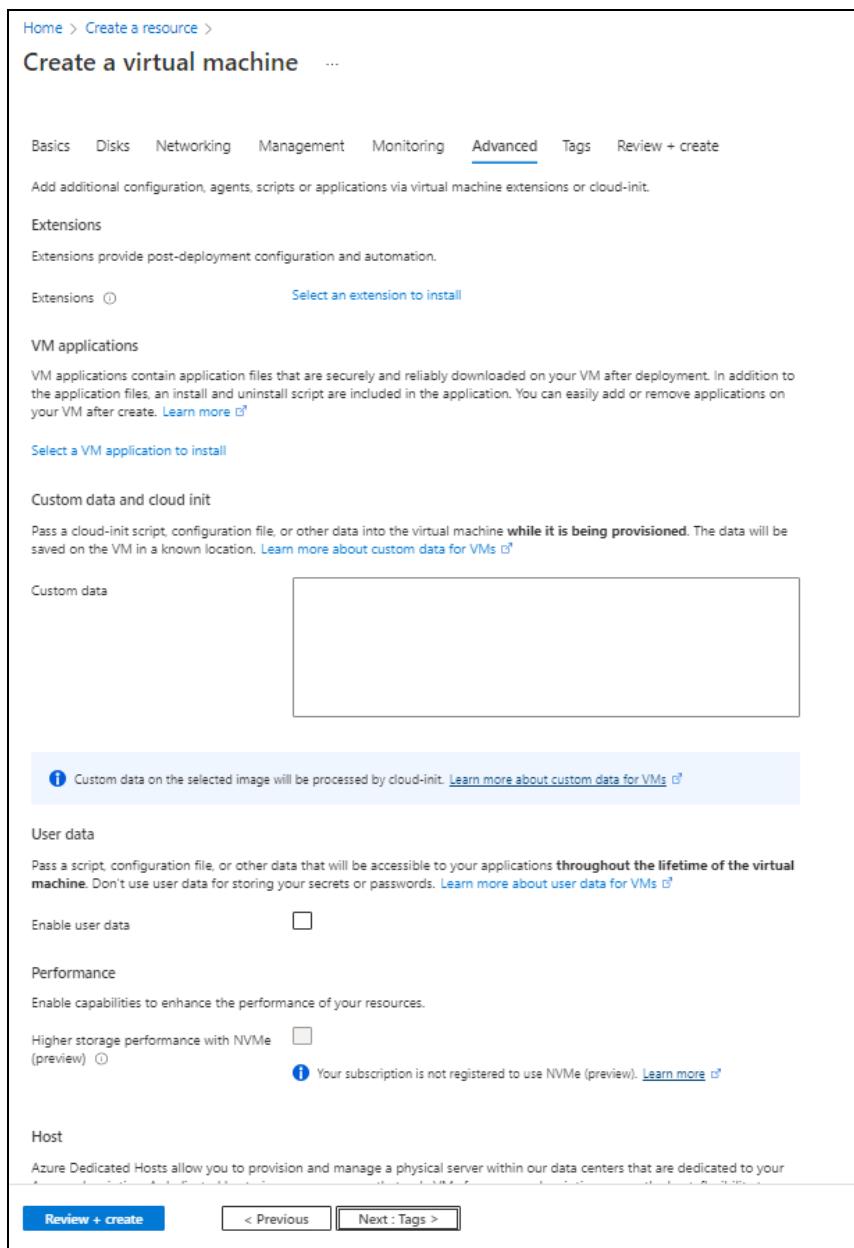
Figure 67 : Create a virtual machine window - Monitoring tab



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

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

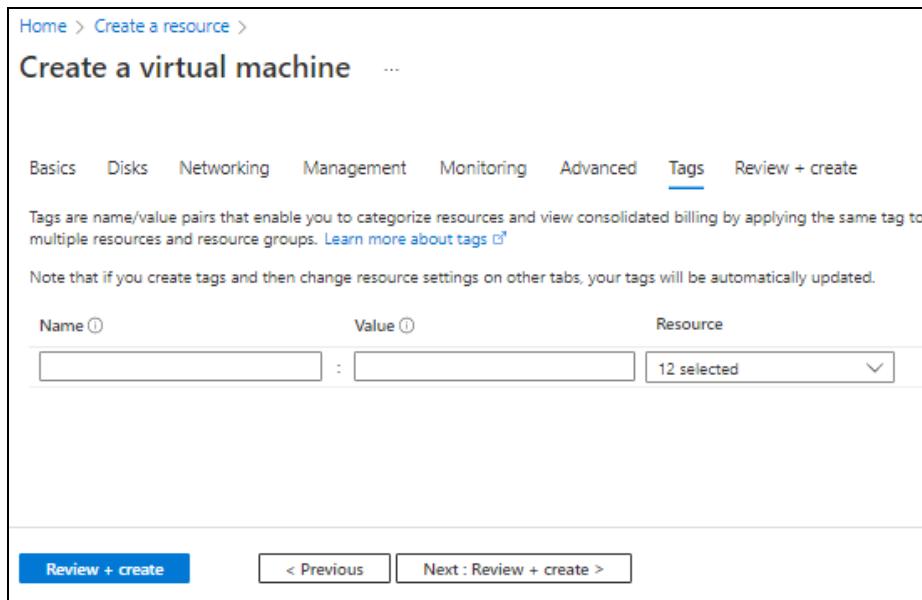
Figure 68 : Create a virtual machine window - Advanced tab



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

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

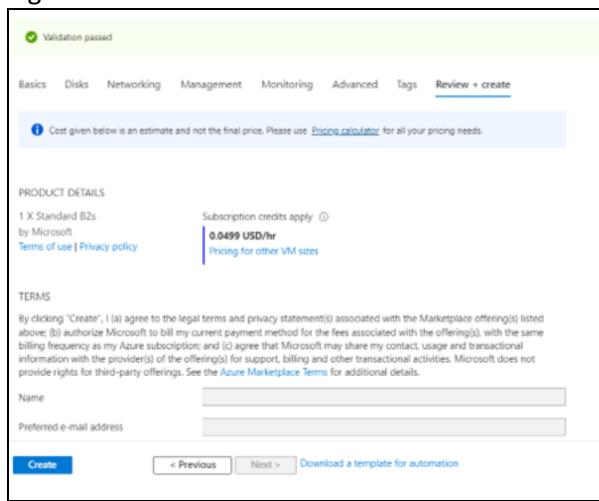
Figure 69 : Create a virtual machine window - Tags tab



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 70 : 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](#)
- [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 management 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",  
            "fqdn-name": "s1",  
            "ip": "10.0.3.7",  
            "port": 53  
        }  
    ]  
},
```

```
        "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
                }
            ]
        }
    ]
},
```

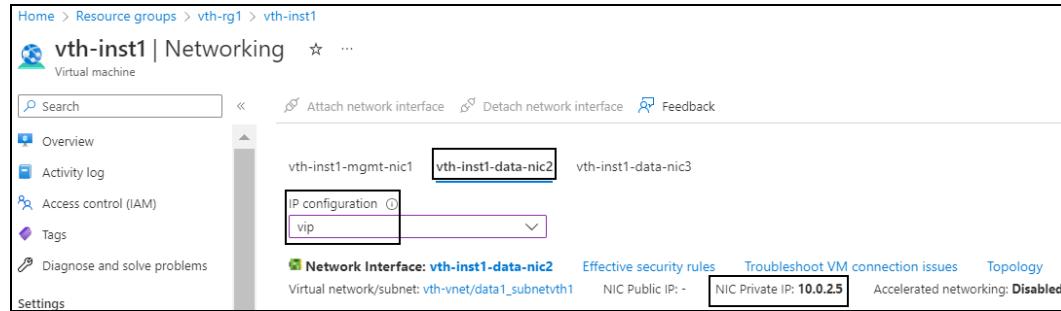
```
        ],
    },
    {
        "name": "sg80",
        "protocol": "tcp",
        "health-check-disable": 1
        "member-list": [
            {
                "name": "s1",
                "port": 80
            }
        ]
    }
],
},
```

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 thru **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 71 : 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. 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.

- 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_2.ps1 -  
resourceGroup <resource_group_name>
```

Example:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_SLB_CONFIG_2.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":"10.0.1.1"
            }
        ]
    ],
]
```

4. Set VRRP-A.

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

5. Set a Terminal Idle Timeout.

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

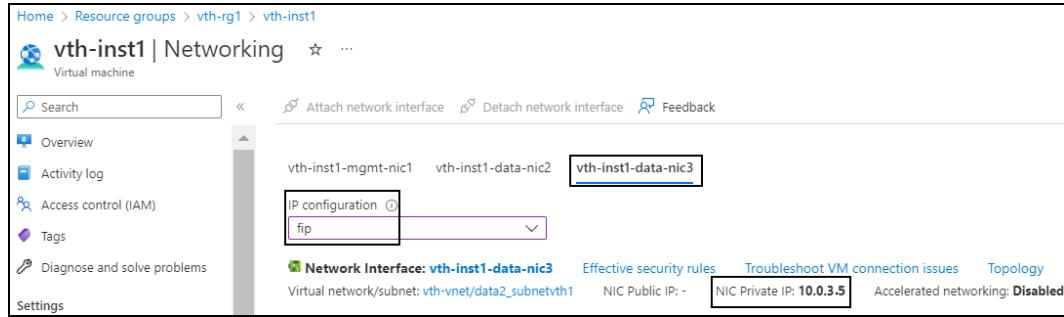
6. Configure the VRID details.

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 thru **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 72 : 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](#).

- Run the following command to configure both VM in HA mode.

```
S C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_HA_CONFIG_3.ps1 -  
resourceGroup <resource_group_name>
```

Example:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_HA_CONFIG_3.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:

- Open the PS_TMPL_3NIC_2VM_GLM_CONFIG_PARAM.json with a text editor.
- 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_4.ps1 -  
resourceGroupName <resource_group_name>
```

Example:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_2VM_GLM_CONFIG_4.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](#)

NOTE: For A10 vThunder default login credentials, send a request to [A10 Networks Support](#).

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 default login credentials provided by A10 Networks Support and change the default password as soon as you login for the first time:

```
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]

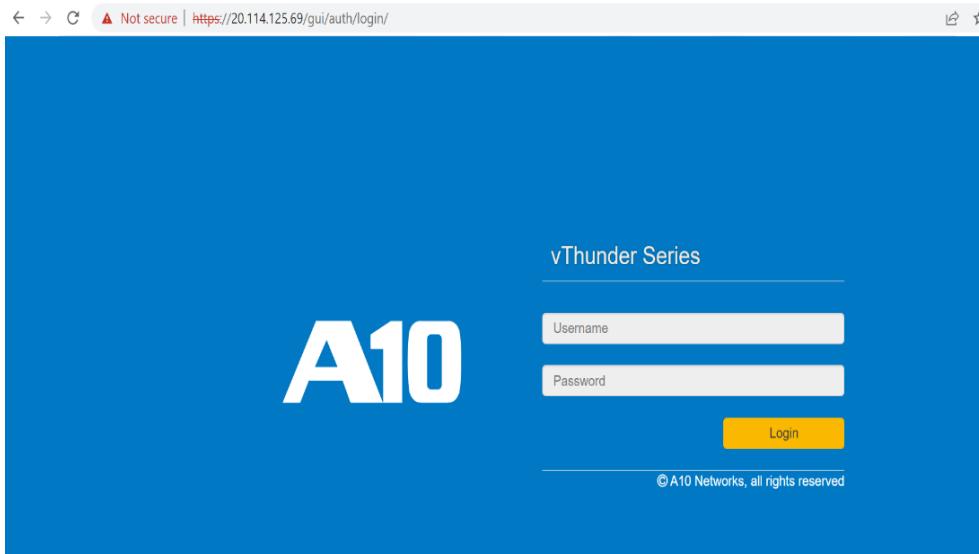
vThunder> enable <--Execute command-->
Password:<--just press Enter key-->
vThunder#config <--Configuration mode-->
vThunder(config)#admin <admin_username> password <new_password>
```

NOTE: It is highly recommended to change the default password when you login for the first time.

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 thru 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
<hr/>			
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.
```

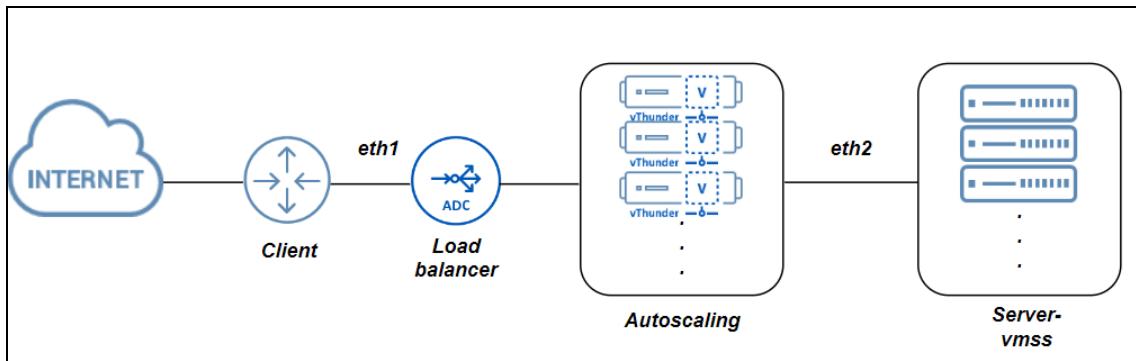
CYLANCE	N/A	Requires an additional Cylance license.
IPSEC_VPN	N/A	Requires an additional IPsec VPN license.
25 Mbps Bandwidth 21-December-2022		

Deploy PowerShell Template 3NIC-NVM-VMSS

[Figure 73](#) 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 73 : 3NIC-NVM-VMSS Topology



The following topics are covered:

System Requirements	181
Create vThunder Instances	186
Configure Server VMSS	193
Configure Automation Account	202
Enable Autoscaling	223
Access vThunder using CLI or GUI	284
Verify Deployment	285

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	<p>A resource group with the specified name and location is created if it doesn't exist.</p> <p>All the resources required for this template is created under the resource group.</p>	Here, the Azure resource group name used is <code>vth-rg1</code> .
Azure Storage Account	<p>A storage account is created inside the resource group, if it doesn't exist.</p> <p>If the storage name already exists, the following error is displayed "The storage account named vthunderstorage already exists under the subscription".</p> <p>Performance: Standard</p> <p>Replication: Read-access geo-redundant storage (RA-GRS)</p> <p>Account kind: Storagev2 (general purpose v2)</p>	<p>Azure Storage Account: <code>vthunderstorage</code></p> <p>SSL Container: <code>ssl</code></p> <p>Log Agent Container: <code>vth-agent-cont</code></p>
Virtual Machine (VM) Instance	Two virtual machine instances are created, vThunder and monitoring agent.	<p>A10 vThunder instance: <code>vth-vmss_0</code></p> <p>A10 Monitoring Agent: <code>vth-</code></p>

Resource Name	Description	Default Value
	<p>Product: A10 vThunder</p> <p>Operating system: Linux</p> <p>Default Size: Standard_B4ms (4 vCPUs, 16 GiB Memory)</p> <p>Product: A10 Monitoring Agent</p> <p>Operating system: Linux</p> <p>Default Size: Standard DS2_V2 (2 vCPUs, 7 GiB Memory)</p> <p>NOTE: Before selecting any VM size, it is highly recommended to do an assessment of your projected traffic.</p> <p>Table 13 lists the supported VM sizes.</p>	agent-ins1
Azure Automation Account	An automation account is created under the resource group.	vth-amt-acc
Azure Runbook with Webhook	<p>Multiple custom runbooks are created under the automation account:</p> <ul style="list-style-type: none"> • Event-Config • GLM-Config 	

Resource Name	Description	Default Value
	<ul style="list-style-type: none"> • GLM-Revoke-Config • Master-Runbook • SLB-Config • SSL-Config <p>A webhook is created under the Master-Runbook.</p>	
Azure Log Analytics Workspace	A log analytics workspace is created. A custom agent, fluentbit, sends all logs to log analytics.	<code>vth-vmss-log-workspace</code>
Azure Application Insights	The custom metrics are created. Depending upon the configured threshold values, it is considered for autoscaling.	<p>Default application insight name: <code>vth-vmss-app-insights</code></p> <p>Default custom metrics name: <code>vth-cpu-metrics</code></p> <p>Default threshold for autoscale-in is 25%.</p> <p>Default threshold for autoscale-out is 80%.</p>
Azure Load Balancer [LB]	<p>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.</p> <p>One backend pool is created, and it gets attached to the Network Interface Card 2 (NIC2).</p> <p>Three default LB rules are created.</p>	<p>Azure Load Balancer: <code>vth-lb1</code></p> <p>Backend Pool: <code>vth-lb1-bck-pool1</code></p> <p>Three default rules are created:</p> <ul style="list-style-type: none"> • rulePort80 • rulePort443 • rulePort53 <p>Three default probes are created:</p>

Resource Name	Description	Default Value
	Three default health probes are created.	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Management Interface with public IP • Data Interface with primary private IP [Ethernet 1, Ethernet 2] 	vth-inst1-mgmt-nic1 vth-inst1-data-nic2 vth-inst1-data-nic3

Resource Name	Description	Default Value
	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.	<code>vth-nsg1</code>
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_A4_v2
	Standard A4m_v2	Standard_A4m_v2
	Standard/Basic A4	Standard_A4
	Standard A8_v2	Standard_A8_v2
B series	Standard B2s	Standard_B2_s
	Standard B2ms	Standard_B2ms
	Standard B4ms	Standard_B4ms
D series	Standard D3_v2	Standard_D3_v2
	Standard DS3_v2	Standard_DS3_v2
	Standard D5_v2	Standard_D5_v2

Series	Size	Qualified Name
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](#)
- [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

To verify the instance count, perform the following steps:

1. From **Home**, navigate thru **Azure Services > Virtual machine scale set > <vmss_name>**.

The selected VMSS - Overview window is displayed. Here, the VMSS name is **vth-vmss**.

Deploy PowerShell Template 3NIC-NVM-VMSS

Figure 74 : Virtual machine scale set - Overview window

2. Click **Scaling** from the left **Settings** panel.

The selected VMSS - Scaling window is displayed.

Figure 75 : 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.

To verify LB resource creation, perform the following steps:

- From **Home**, navigate thru **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.

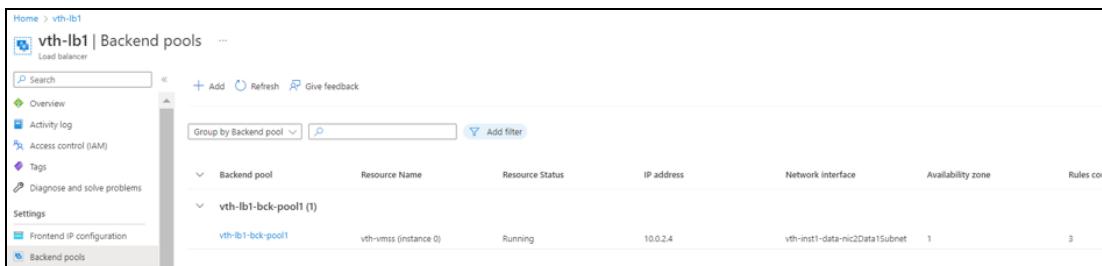
Figure 76 : Selected Frontend IP configuration window



Name	IP address	Rules count
vth-lb1-fmt-ip	20.64.115.110 (vth-lb1-ip)	3

- c. Click **Backend pools** from the left **Settings** panel to verify if the backend pools are created.

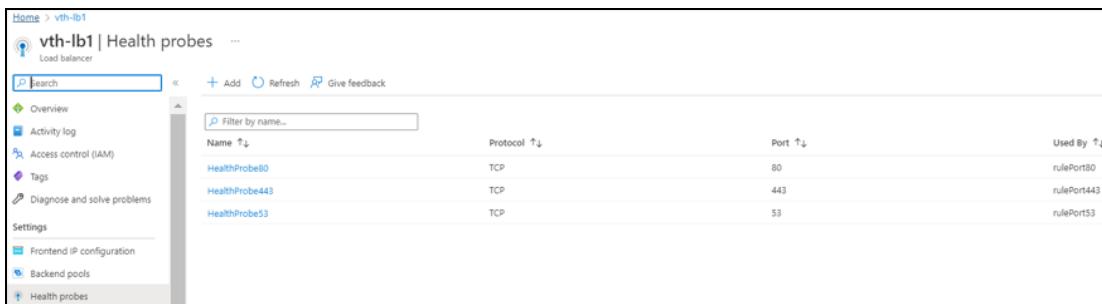
Figure 77 : Selected Backend pools window



Backend pool	Resource Name	Resource Status	IP address	Network interface	Availability zone	Rules count
vth-lb1-bck-pool1 (1)	vth-vmss (instance 0)	Running	10.0.2.4	vth-inst1-data-nic2Data1Subnet	1	3

- d. Click **Health probes** from the left **Settings** panel to verify if the health probes are created.

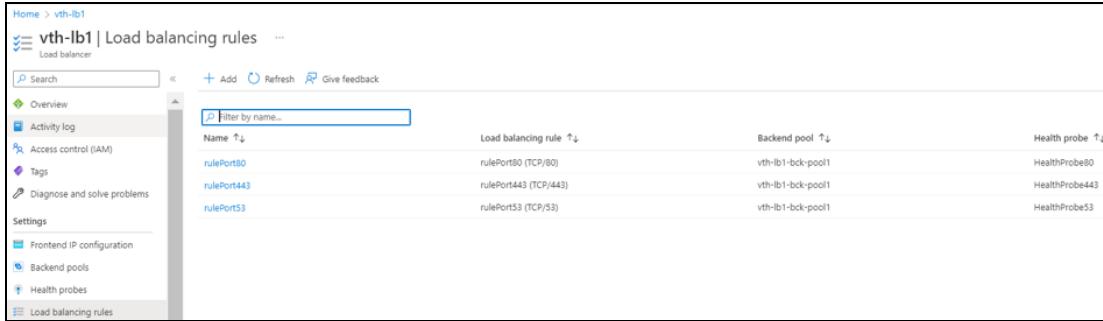
Figure 78 : Selected Health Probes window



Name	Protocol	Port	Used By
HealthProbe80	TCP	80	rulePort80
HealthProbe443	TCP	443	rulePort443
HealthProbe53	TCP	53	rulePort53

- e. Click **Load balancing rules** from the left **Settings** panel to verify if the load balancing rules are created.

Figure 79 : Selected load balancing rules window



Name	Load balancing rule	Backend pool	Health probe
rulePort80	rulePort80 (TCP/80)	vth-lb1-bck-pool1	HealthProbe80
rulePort443	rulePort443 (TCP/443)	vth-lb1-bck-pool1	HealthProbe443
rulePort53	rulePort53 (TCP/53)	vth-lb1-bck-pool1	HealthProbe53

To verify storage account container, perform the following steps:

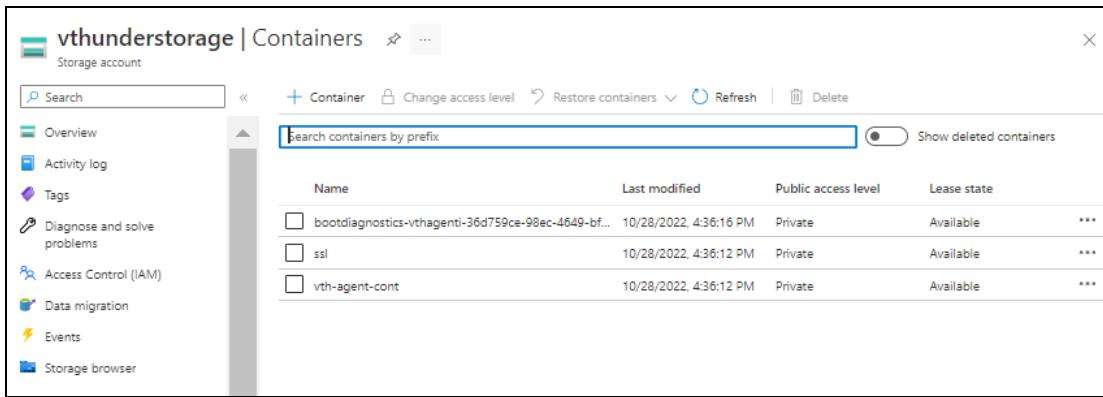
- From **Home**, navigate thru **Azure Services > Storage account > <storage_account_name>**.

The selected storage account - Overview window is displayed. Here, the storage account name is **vthunderstorage**.

- Click **Containers** from the left **Data storage** panel.

The selected storage account - Containers window is displayed.

Figure 80 : Selected storage account - Containers window



Name	Last modified	Public access level	Lease state
bootdiagnostics-vthagenti-36d759ce-98ec-4649-bf...	10/28/2022, 4:36:16 PM	Private	Available
ssl	10/28/2022, 4:36:12 PM	Private	Available
vth-agent-cont	10/28/2022, 4:36:12 PM	Private	Available

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 thru **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

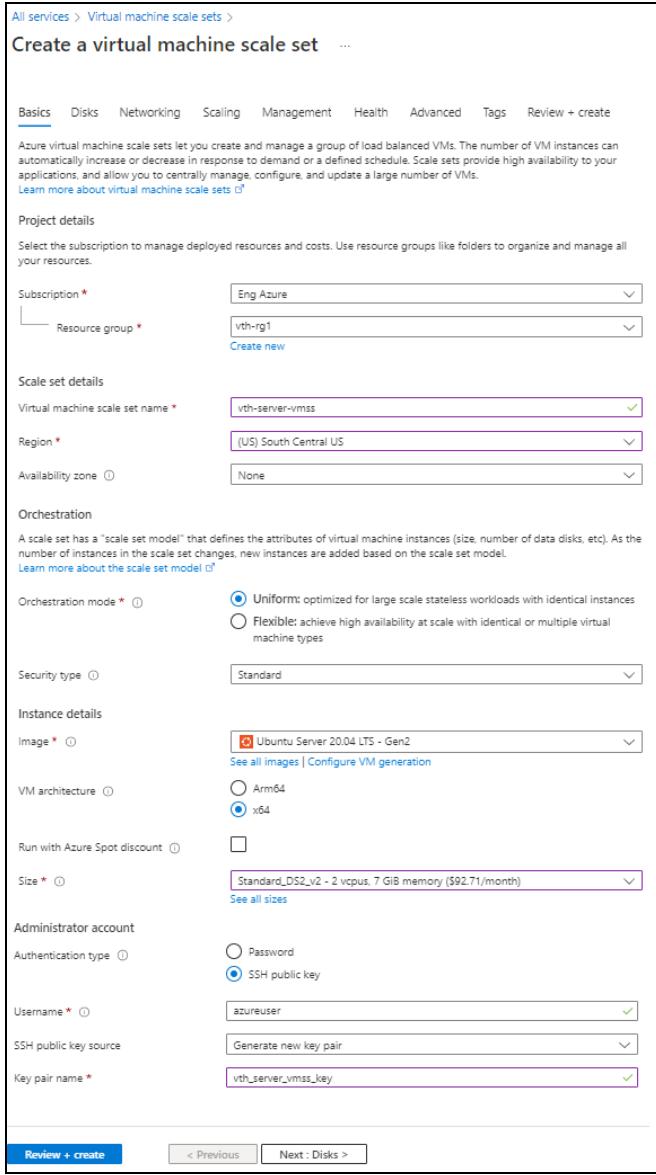
- Image
- Size

Administrator account

- Depending upon the Authentication type, provide the information.

[Deploy PowerShell Template 3NIC-NVM-VMSS](#)

Figure 81 : Create a virtual machine scale set window - Basics tab



The screenshot shows the 'Create a virtual machine scale set' window in the Azure portal. The 'Basics' tab is selected. The configuration includes:

- Subscription:** Eng Azure
- Resource group:** vth-rg1
- Virtual machine scale set name:** vth-server-vmss
- Region:** (US) South Central US
- Availability zone:** None
- Orchestration mode:** Uniform (selected)
- Security type:** Standard
- Image:** Ubuntu Server 20.04 LTS - Gen2
- VM architecture:** x64
- Run with Azure Spot discount:** Unchecked
- Size:** Standard_DS2_v2 - 2 vcpus, 7 GB memory (\$92.71/month)
- Administrator account:**
 - Authentication type: SSH public key (selected)
 - Username: azureuser
 - SSH public key source: Generate new key pair
 - Key pair name: vth_server_vmss_key

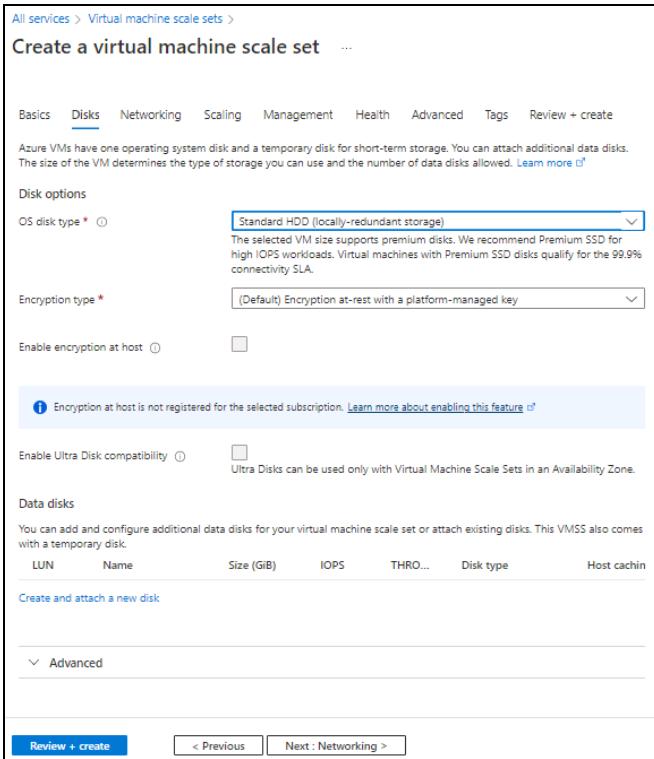
At the bottom, there are buttons for **Review + create**, < Previous, and Next : Disks >.

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

Deploy PowerShell Template 3NIC-NVM-VMSS

- OS disk type
- Encryption type

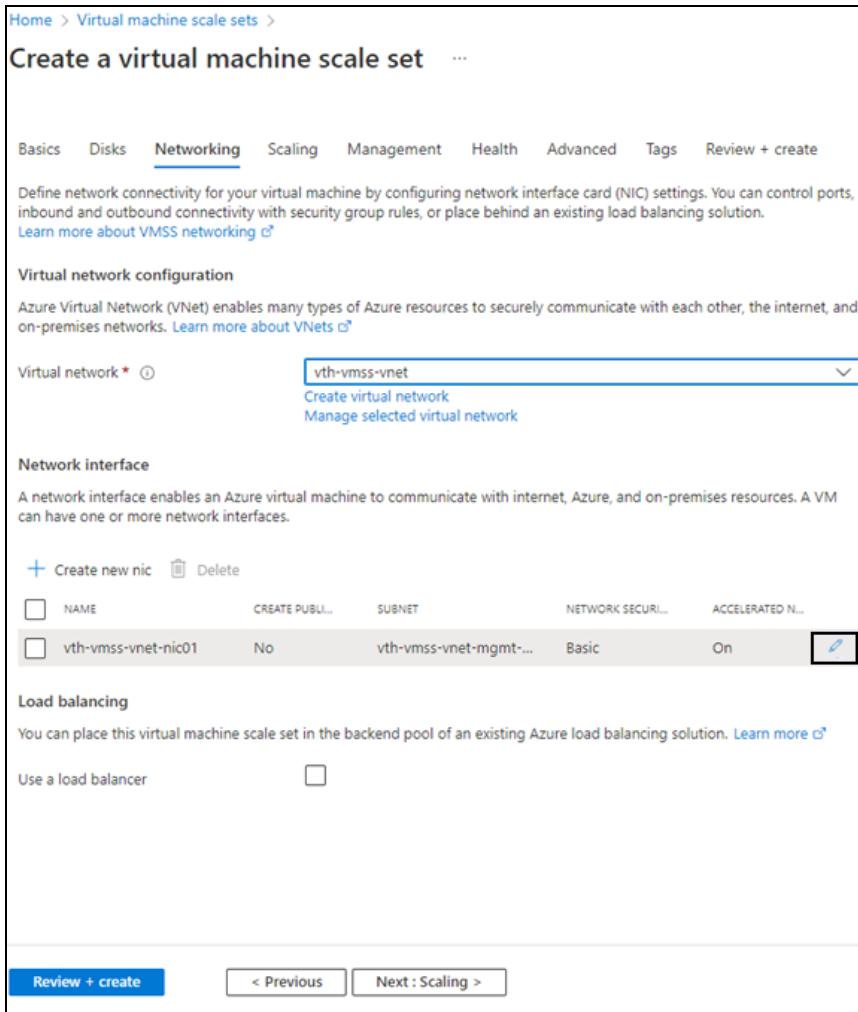
Figure 82 : Create a virtual machine scale set window - Disks tab



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

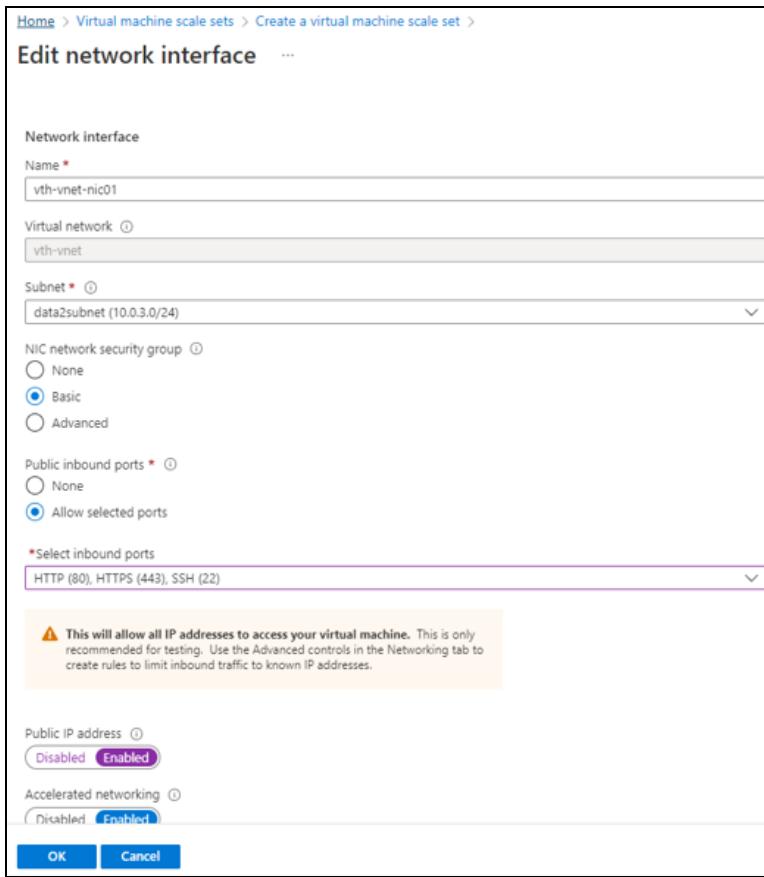
6. Select the Virtual network in the **Networking** tab.

Figure 83 : 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**.

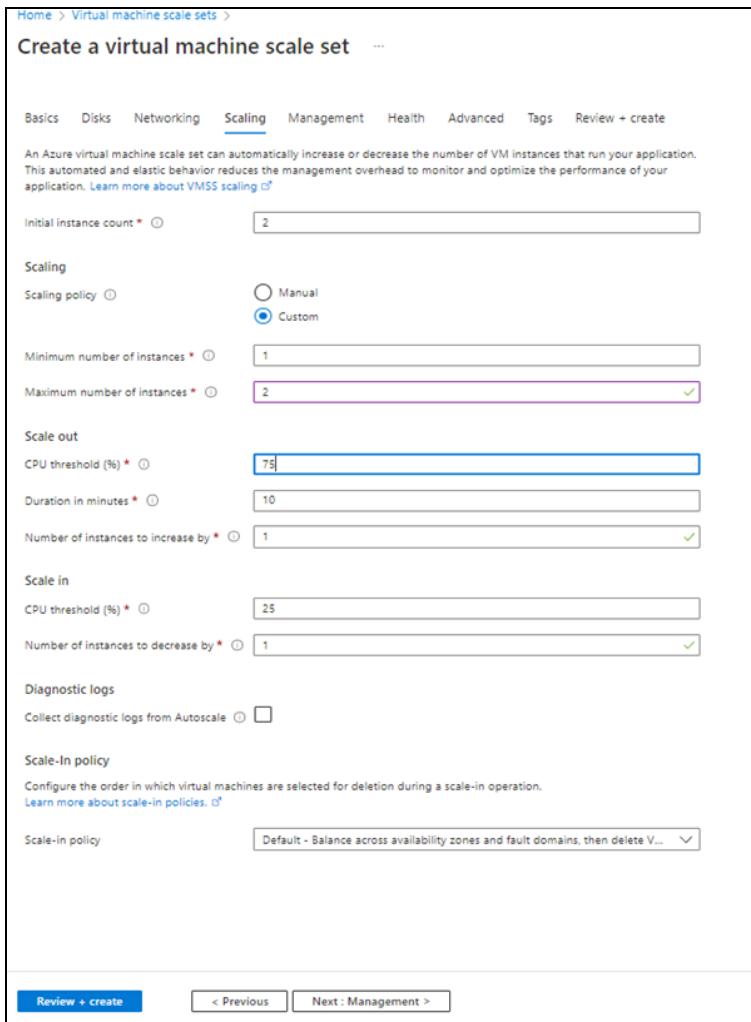
Figure 84 : Edit network interface window



- 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 85 : Create a virtual machine scale set window - Scaling tab

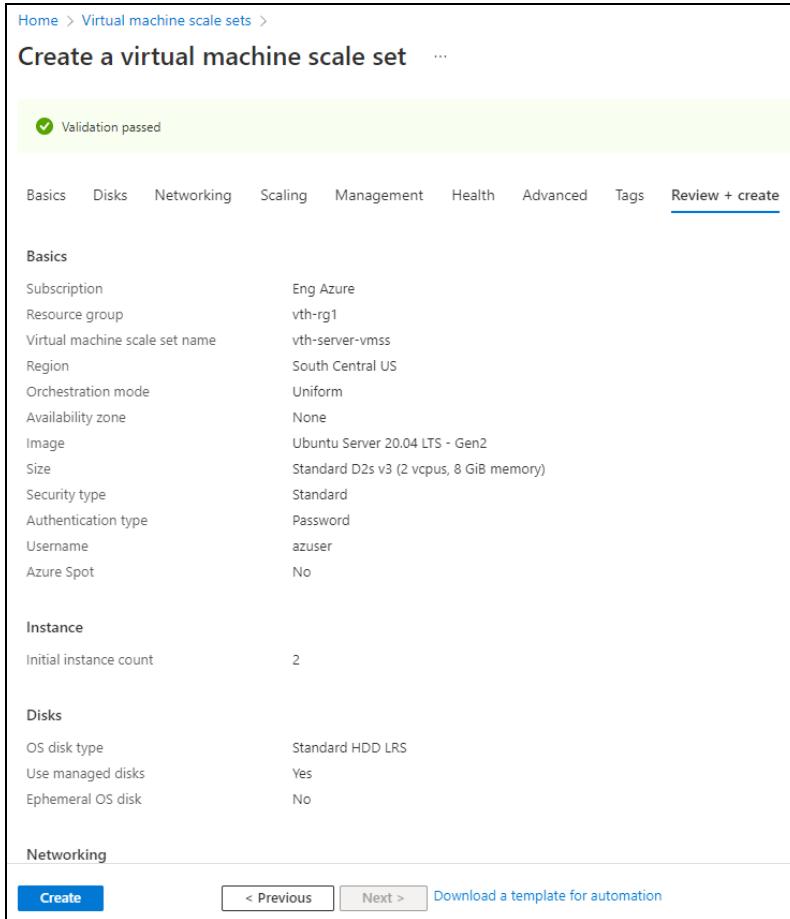


The screenshot shows the 'Create a virtual machine scale set' wizard with the 'Scaling' tab selected. The 'Scaling' tab is highlighted in blue at the top of the navigation bar. Below the tabs, there is a note about VMSS scaling. The main configuration area includes:

- Initial instance count:** Set to 2.
- Scaling policy:** Set to **Custom**.
- Minimum number of instances:** Set to 1.
- Maximum number of instances:** Set to 2.
- Scale out:**
 - CPU threshold (%):** Set to 75.
 - Duration in minutes:** Set to 10.
 - Number of instances to increase by:** Set to 1.
- Scale in:**
 - CPU threshold (%):** Set to 25.
 - Number of instances to decrease by:** Set to 1.
- Diagnostic logs:** A checkbox labeled 'Collect diagnostic logs from Autoscale' is unchecked.
- Scale-in policy:** A note says 'Configure the order in which virtual machines are selected for deletion during a scale-in operation.' Below it is a dropdown menu set to 'Default - Balance across availability zones and fault domains, then delete V...'.
 - Review + create**
 - < Previous**
 - Next : Management >**

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

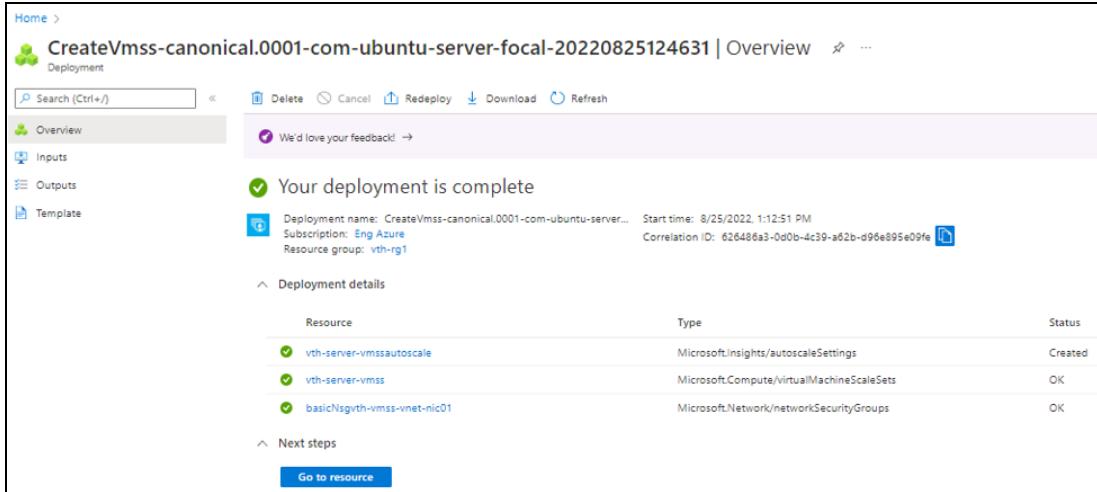
Figure 86 : Create a virtual machine scale set window - Review + create tab



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 87 : Create VMSS window



Resource	Type	Status
vth-server-vmssautoscale	Microsoft.Insights/autoscaleSettings	Created
vth-server-vmss	Microsoft.Compute/virtualMachineScaleSets	OK
basicNsgvth-vmss-vnet-nic01	Microsoft.Network/networkSecurityGroups	OK

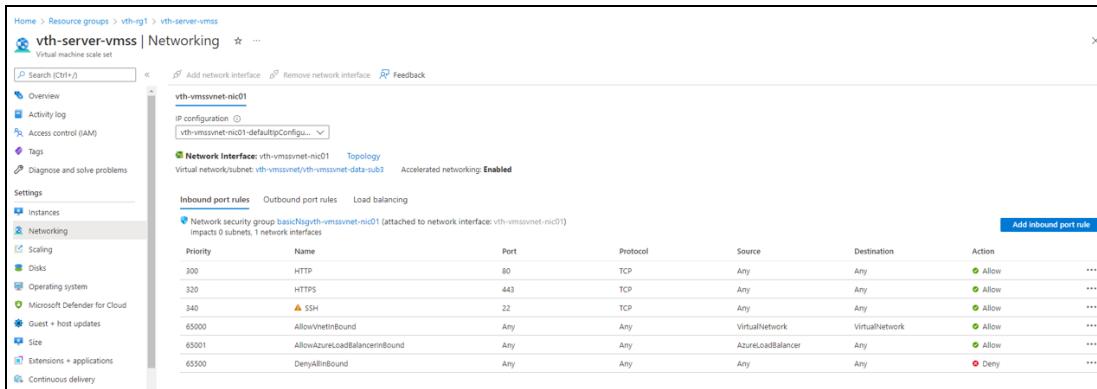
NOTE: It may take the system several minutes to display your resources.

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 88 : VMSS > Inbound port rules



Priority	Name	Port	Protocol	Source	Destination	Action
300	HTTP	80	TCP	Any	Any	Allow, Allow, ...
320	HTTPS	443	TCP	Any	Any	Allow, Allow, ...
340	SSH	22	TCP	Any	Any	Allow, Allow, ...
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow, Allow, ...
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow, Allow, ...
65500	DenyAllInBound	Any	Any	Any	Any	Deny, Deny, ...

Configure Automation Account

The following topics are covered:

- [Configure Azure Access Key](#)
- [Create Automation Account](#)
- [Create Runbooks](#)
- [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 refer 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>**.

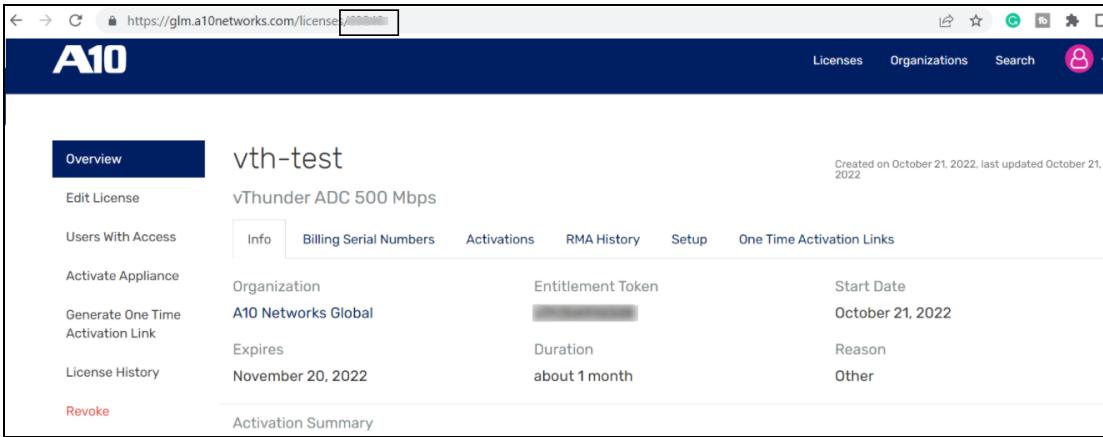
```
"azureAutoScaleResources": {
    "resourceGroupName": "vth-rg1",
    "automationAccountName": "vth-amt-acc",
    "vThunderScaleSetName": "vth-vmss",
    "serverScaleSetName": "vth-server-vmss",
    "storageAccountName": "vthunderstorage",
    "appId": "xxxxxxxx-xxx-xxxx-xxxx-xxxxxxxxxxxx",
    "tenantId": "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",

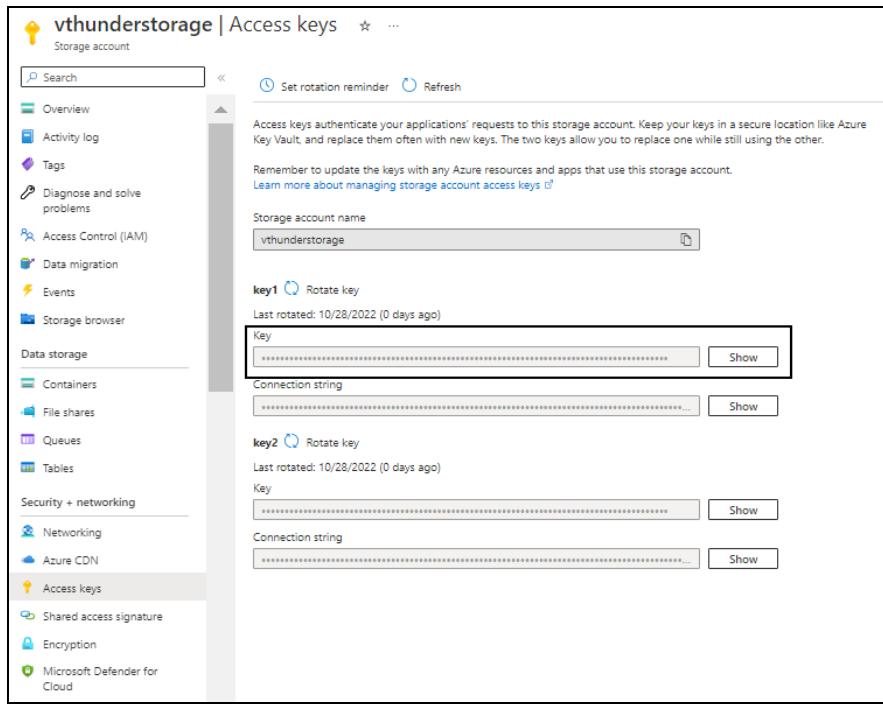
    "storageAccountKey": "LX6z8xxxxxxehXx0xxxv7xxxx/xxxOfxxxxxxxxR0xxx5gXxxxx
xfhxcx0gxxxxx9rxxASxxxx=="
},

```

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 89 : 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
        }
      ]
    }
  ]
}
```

[Deploy PowerShell Template 3NIC-NVM-VMSS](#)

```
        }
    ],
},
"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**.

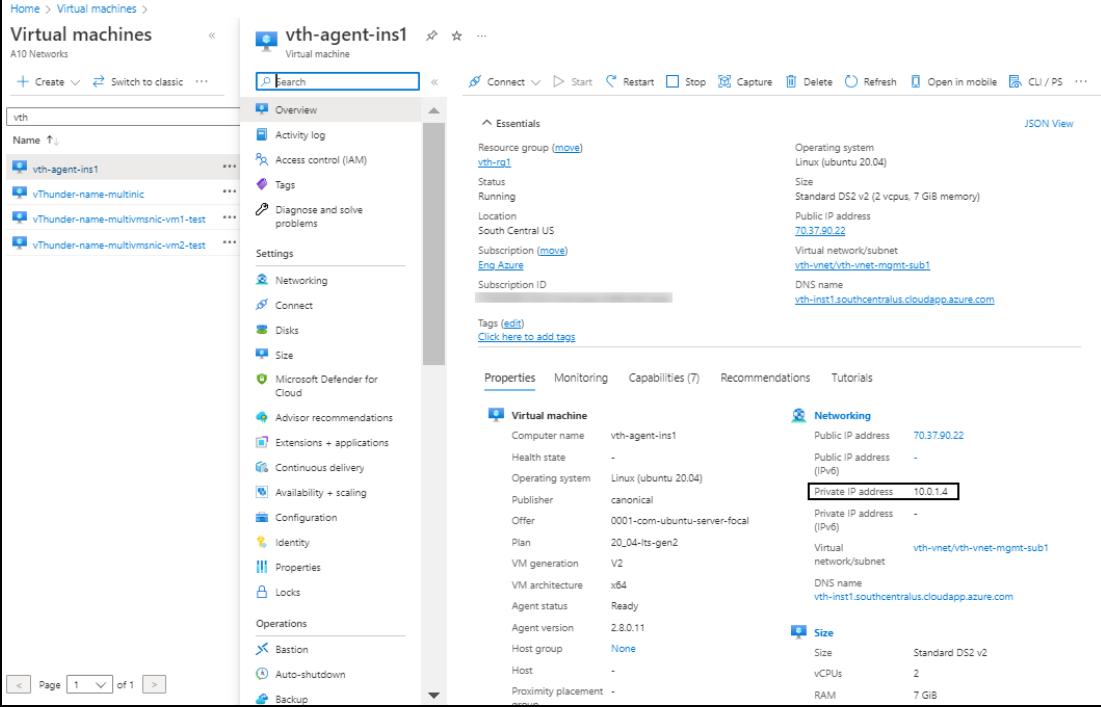
```
"clientSecret": "9-xxxx~jIxxxEVyxxxxHNxxxOwv_xxxxZLxxxTM",
```

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 90 : Selected virtual machine - Overview window



The screenshot shows the Azure portal's Virtual machines blade. A search bar at the top right is set to 'Search' and contains the text 'vth'. Below it, a list of virtual machines includes 'vth-agent-ins1', 'vThunder-name-multinic', 'vThunder-name-multivmsnic-vm1-test', and 'vThunder-name-multivmsnic-vm2-test'. On the left, a navigation menu lists options like Create, Switch to classic, Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Networking, Connect, Disks, Size, Microsoft Defender for Cloud, Advisor recommendations, Extensions + applications, Continuous delivery, Availability + scaling, Configuration, Identity, Properties, Locks, Operations, Bastion, Auto-shutdown, and Backup. The main content area is titled 'vth-agent-ins1' and shows the 'Overview' tab selected. It provides detailed information about the VM, including its resource group, status, location, and subscription. The 'Networking' section is expanded, showing the private IP address (10.0.1.4) and public IP address (70.37.90.22). Other sections visible include 'Essentials', 'Properties', 'Monitoring', 'Capabilities (7)', 'Recommendations', and 'Tutorials'.

- Verify if all the configurations in the refer 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, run the following command:

```
PS C:\Users\TestUser\Templates> .\PS_TMPL_3NIC_NVM_VMSS_AUTOMATION_ACCOUNT_2.ps1
```

Verify the Automation Account Creation

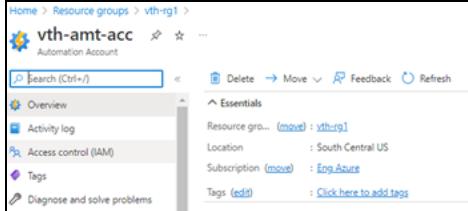
To verify the creation of an automation account, perform the following steps:

- From the **Home**, navigate thru **Azure Services > Resource Group > <resource_group_name>**.
The selected resource group - Overview window is displayed.
- Under **Resources** tab, group the resources based on the resource type.
- 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.

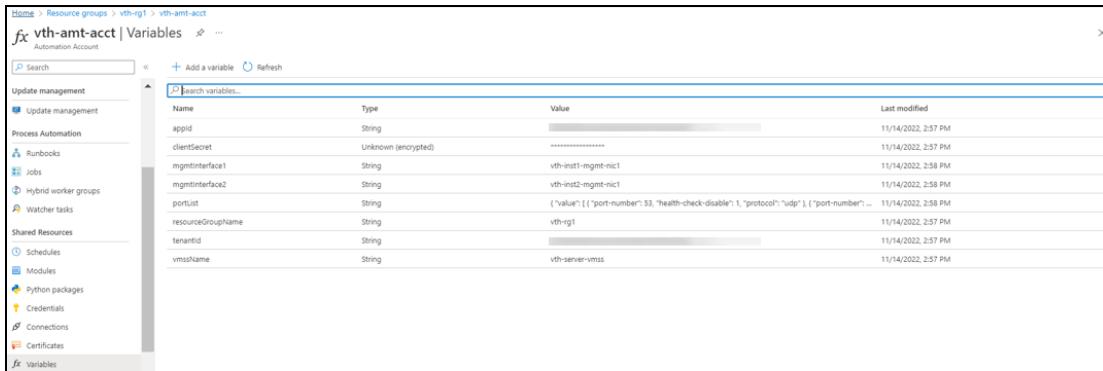
Figure 91 : Selected automation account - Overview window



5. Click **Variables from the left **Shared Resources** panel.**

The selected automation account - Variables window is displayed.

Figure 92 : Selected automation account - Variables window



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

Create Runbooks

Create the following runbooks:

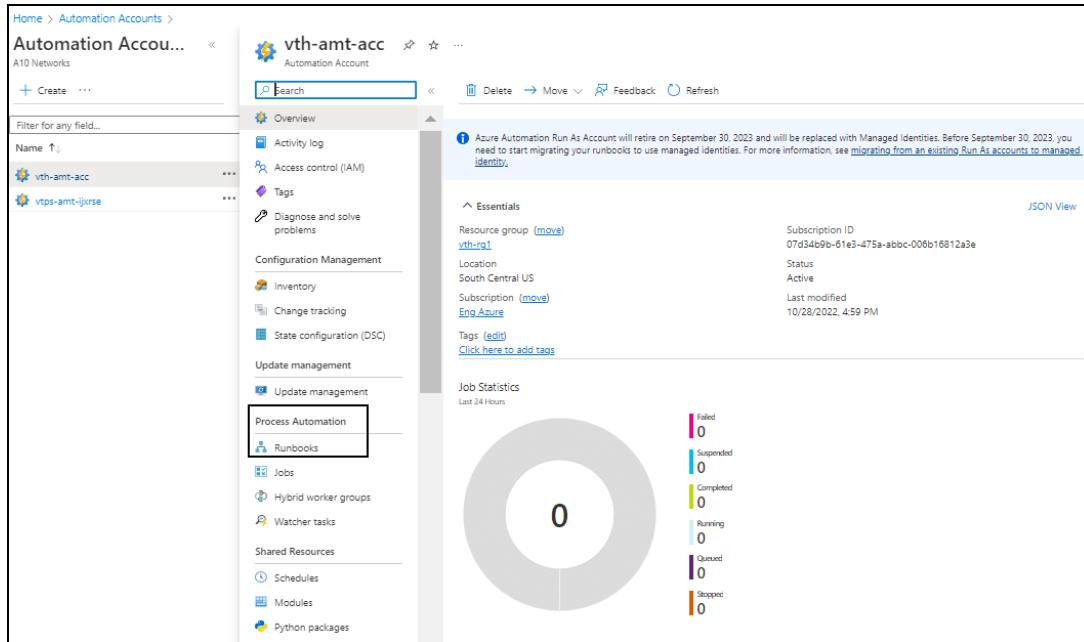
- [SSL-Config Runbook](#)
- [SLB-Config Runbook](#)
- [GLM-Config Runbook](#)
- [GLM-Revoke-Config Runbook](#)
- [Event-Config Runbook](#)
- [Master-Runbook](#)

SSL-Config Runbook

To create a SSL-Config runbook, perform the following steps:

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

Figure 93 : Selected automation account window



- Select **Runbooks** from left **Process Automation** panel.

The <automation_account_name> - Runbooks window is displayed.

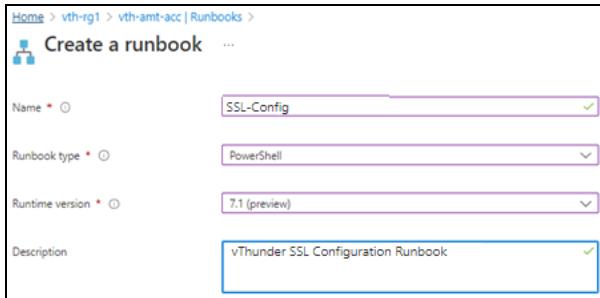
Figure 94 : Selected automation account - Runbooks window



- Click **Create a runbook**.

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

Figure 95 : Create a runbook window



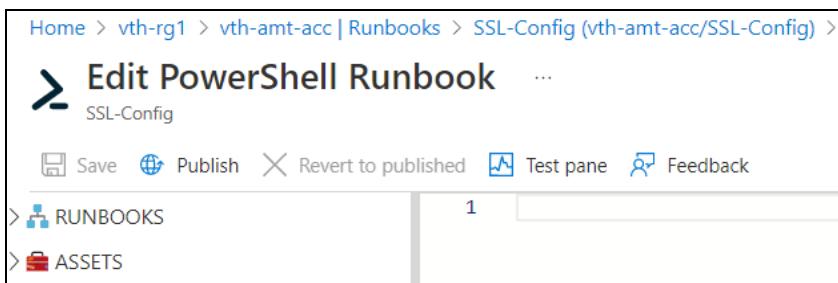
4. Select or enter the following information:

- Name: SSL-Config
- Runbook type: PowerShell
- Runtime version: 7.1
- Description

5. Click **Create**.

The **Edit PowerShell Runbook** is displayed.

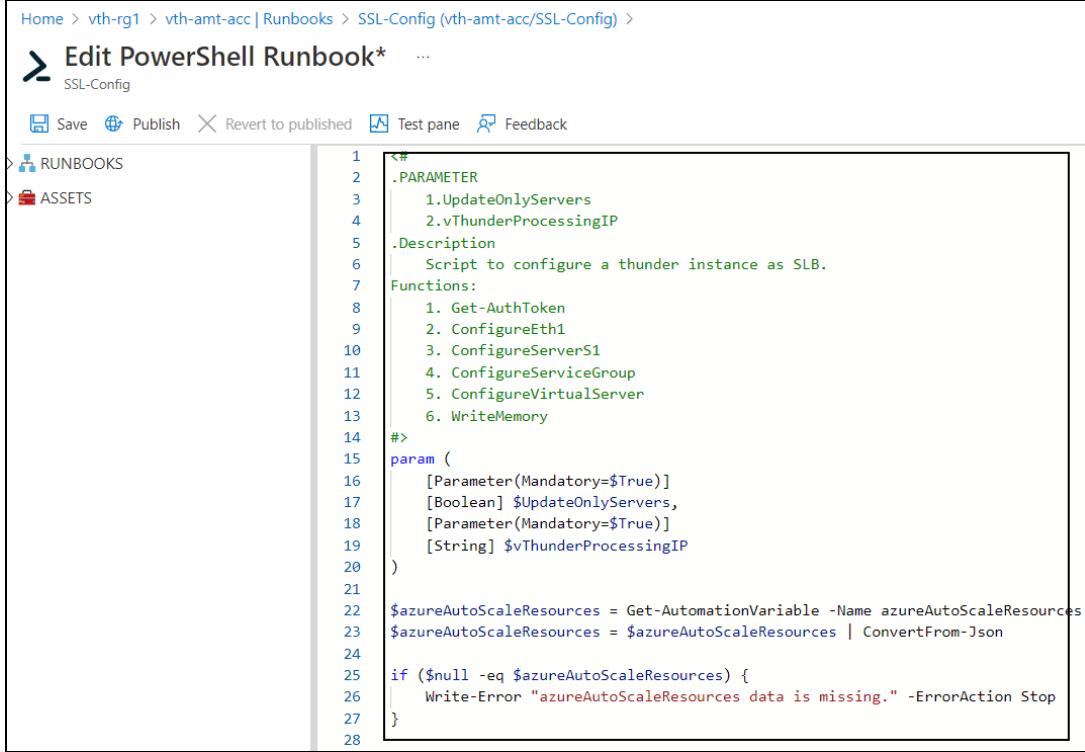
Figure 96 : Edit Runbook window



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

6. From the downloaded template folder, open **PS_TMPL_3NIC_NVM_VMSS_SSL_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.



The screenshot shows the 'Edit PowerShell Runbook' interface. The left sidebar lists 'RUNBOOKS' and 'ASSETS'. The main area contains the PowerShell script for 'SSL-Config'.

```

1<#
2.PARAMETER
3    1.UpdateOnlyServers
4        2.vThunderProcessingIP
5.Description
6    Script to configure a thunder instance as SLB.
7.Functions:
8    1. Get-AuthToken
9        2. ConfigureEth1
10       3. ConfigureServerS1
11       4. ConfigureServiceGroup
12       5. ConfigureVirtualServer
13       6. WriteMemory
14#>
15param (
16    [Parameter(Mandatory=$True)]
17    [Boolean] $UpdateOnlyServers,
18    [Parameter(Mandatory=$True)]
19    [String] $vThunderProcessingIP
20)
21
22$azureAutoScaleResources = Get-AutomationVariable -Name azureAutoScaleResources
23$azureAutoScaleResources = $azureAutoScaleResources | ConvertFrom-Json
24
25if ($null -eq $azureAutoScaleResources) {
26    Write-Error "azureAutoScaleResources data is missing." -ErrorAction Stop
27}

```

8. Click **Save** and then click **Publish**.

The runbook gets created for the selected automation account.

SLB-Config Runbook

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

1. From the **Azure Portal**, navigate thru **Azure Services > Automation Accounts > <automation_account_name>**.
The selected automation account window is displayed.
2. Select **Runbooks** from left **Process Automation** panel.
The <automation_account_name> - Runbooks window is displayed.
3. Click **Create a runbook**.
The **Create a runbook** window is displayed.
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.

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

6. From the downloaded template folder, open **PS_TMPL_3NIC_NVM_VMSS_SLB_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.

GLM-Config Runbook

To create a GLM-Config runbook, perform the following steps:

1. From the **Azure Portal**, navigate thru **Azure Services > Automation Accounts > <automation_account_name>**.
The selected automation account window is displayed.
2. Select **Runbooks** from left **Process Automation** panel.
The <automation_account_name> - Runbooks window is displayed.
3. Click **Create a runbook**.
The **Create a runbook** window is displayed.
4. Select or enter the following information:
 - Name: GLM-Config
 - Runbook type: PowerShell
 - Runtime version: 7.1
 - Description
5. Click **Create**.
The **Edit PowerShell Runbook** is displayed.

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

6. From the downloaded template folder, open **PS_TMPL_3NIC_NVM_VMSS_GLM_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.

GLM-Revoke-Config Runbook

To create a GLM-Revoke-Config runbook, perform the following steps:

1. From the **Azure Portal**, navigate thru **Azure Services > Automation Accounts > <automation_account_name>**.
The selected automation account window is displayed.
2. Select **Runbooks** from left **Process Automation** panel.
The <automation_account_name> - Runbooks window is displayed.
3. Click **Create a runbook**.
The **Create a runbook** window is displayed.
4. Select or enter the following information:
 - Name: GLM-Revoke-Config
 - Runbook type: PowerShell
 - Runtime version: 7.1
 - Description
5. Click **Create**.
The **Edit PowerShell Runbook** is displayed.

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

6. From the downloaded template folder, open **PS_TMPL_3NIC_NVM_VMSS_GLM_REVOKE_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.

Event-Config Runbook

To create a Event-Config runbook, perform the following steps:

1. From the **Azure Portal**, navigate thru **Azure Services > Automation Accounts > <automation_account_name>**.
The selected automation account window is displayed.
2. Select **Runbooks** from left **Process Automation** panel.
The <automation_account_name> - Runbooks window is displayed.
3. Click **Create a runbook**.
The **Create a runbook** window is displayed.
4. Select or enter the following information:
 - Name: Event-Config
 - Runbook type: PowerShell
 - Runtime version: 7.1
 - Description
5. Click **Create**.
The **Edit PowerShell Runbook** is displayed.

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

6. From the downloaded template folder, open **PS_TMPL_3NIC_NVM_VMSS_ACOS_EVENT_CONFIG_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.

Master-Runbook

To create a Master-Runbook, perform the following steps:

1. From the **Azure Portal**, navigate thru **Azure Services > Automation Accounts > <automation_account_name>**.
The selected automation account window is displayed.
2. Select **Runbooks** from left **Process Automation** panel.
The <automation_account_name> - Runbooks window is displayed.

3. Click **Create a runbook**.
The **Create a runbook** window is displayed.
4. Select or enter the following information:
 - Name: Master-Runbook
 - Runbook type: PowerShell
 - Runtime version: 7.1
 - Description
5. Click **Create**.
The **Edit PowerShell Runbook** is displayed.

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

6. From the downloaded template folder, open **PS_TMPL_3NIC_NVM_VMSS_MASTER_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:

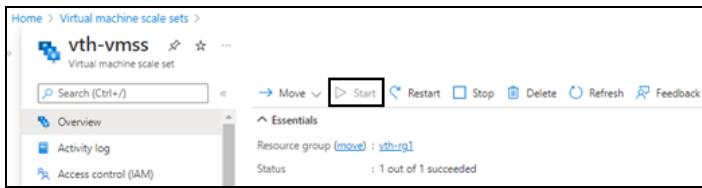
- [Initial Setup](#)
- [Create a Webhook](#)
- [Verify the AutoScale Resource Variable creation](#)
- [Verify the SSL File availability](#)
- [Verify the Runbook Jobs creation](#)

Initial Setup

To verify that the virtual machine scale set resources are running, perform the following steps:

1. From **Home**, navigate thru **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 97 : 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_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.

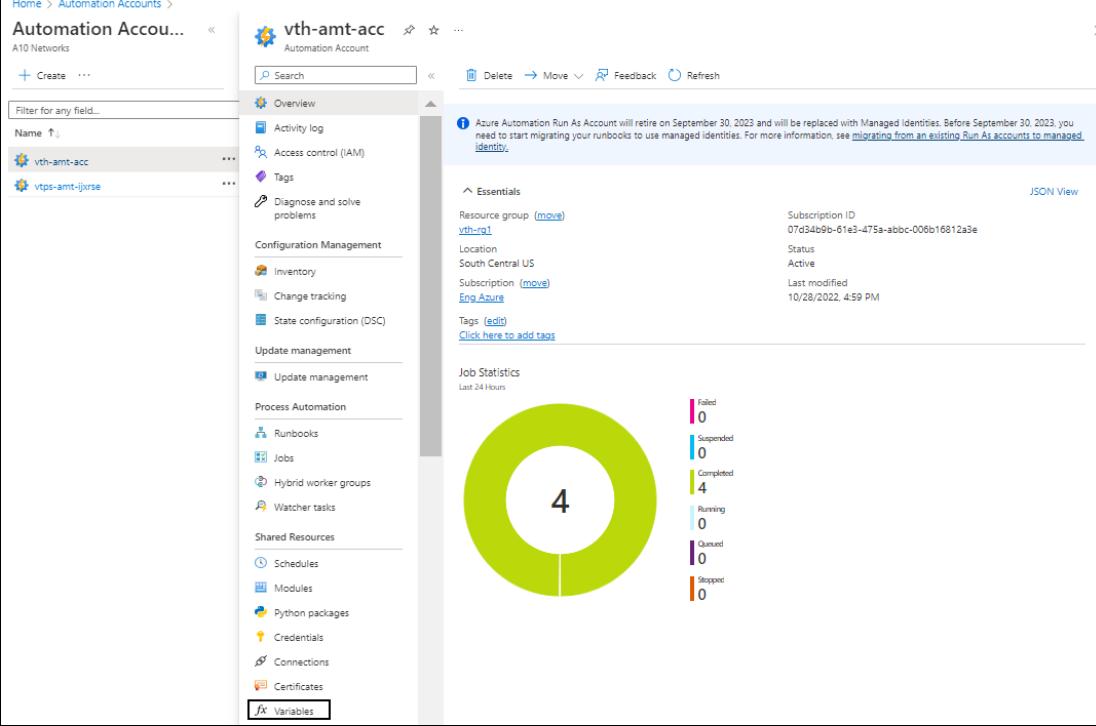
Verify the AutoScale Resource Variable creation

To verify the creation of an autoscale resource variable, perform the following steps:

1. From **Home**, navigate thru **Azure Services > Automation Accounts > <automation_account_name>**.

The selected automation account - Overview window is displayed.

Figure 98 : Selected automation account - Overview window

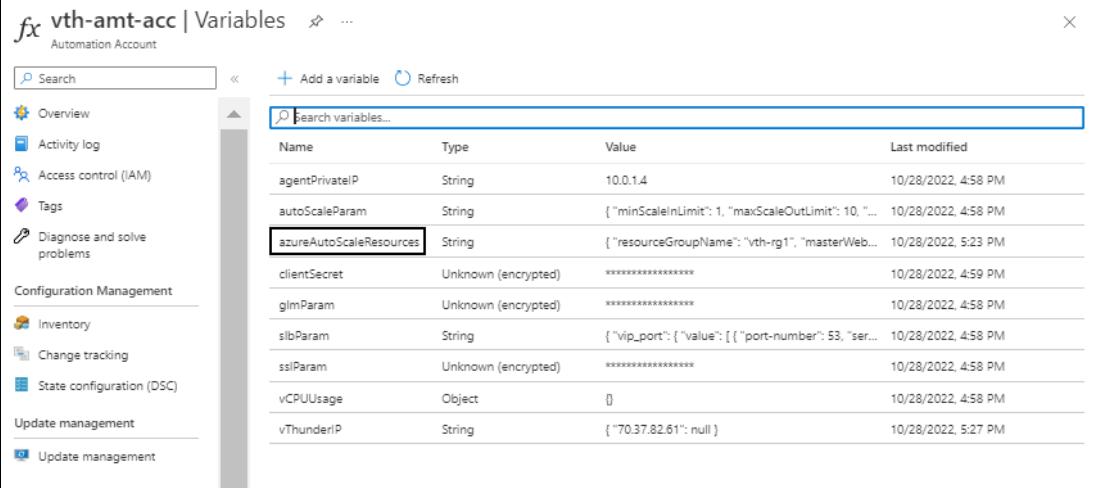


The screenshot shows the Azure portal's Automation Accounts page. On the left, a navigation pane lists various management categories like A10 Networks, Create, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Configuration Management, Inventory, Change tracking, State configuration (DSC), Update management, Process Automation, Runbooks, Jobs, Hybrid worker groups, Watcher tasks, Shared Resources, Schedules, Modules, Python packages, Credentials, Connections, Certificates, and Variables. The 'Variables' item is highlighted with a red box. The main panel displays the details for the 'vth-amt-acc' automation account. It includes sections for Overview, Essentials (Resource group: vth-rg1, Location: South Central US, Subscription: Eng Azure, Status: Active, Last modified: 10/28/2022, 4:59 PM), and Job Statistics (Last 24 Hours: Failed 0, Suspended 0, Completed 4, Running 0, Queued 0, Stopped 0). A large green donut chart in the center indicates 4 completed jobs.

2. Click **Variables** from the left **Shared Resources** panel.

The selected automation account - Variables window is displayed.

Figure 99 : Selected automation account - Variables window



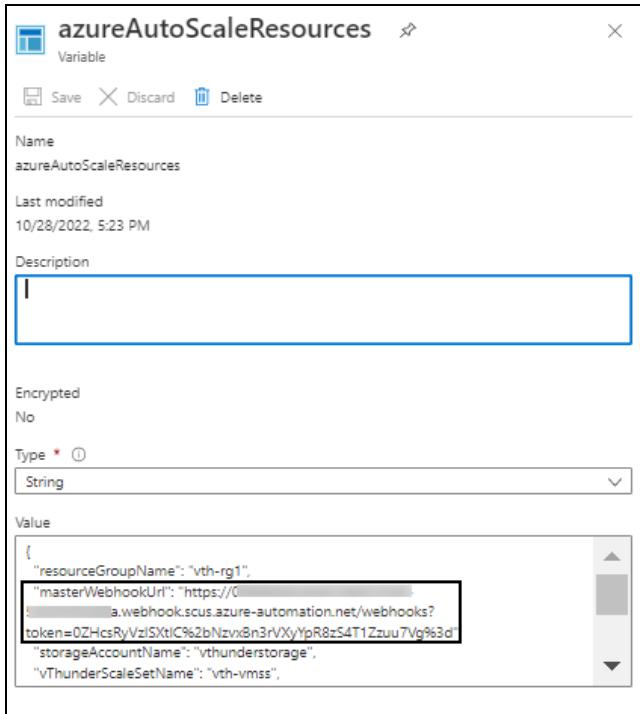
The screenshot shows the 'Variables' window for the 'vth-amt-acc' automation account. The left sidebar lists the same navigation categories as Figure 98. The main area shows a table of variables:

Name	Type	Value	Last modified
agentPrivateIP	String	10.0.1.4	10/28/2022, 4:58 PM
autoScaleParam	String	{"minScaleInLimit": 1, "maxScaleOutLimit": 10, ...}	10/28/2022, 4:58 PM
azureAutoScaleResources	String	{"resourceGroupName": "vth-rg1", "masterWeb..."}	10/28/2022, 5:23 PM
clientSecret	Unknown (encrypted)	*****	10/28/2022, 4:59 PM
glmParam	Unknown (encrypted)	*****	10/28/2022, 4:58 PM
slbParam	String	{"vip_port": {"value": [{"port-number": 53, "ser..."}]}	10/28/2022, 4:58 PM
sslParam	Unknown (encrypted)	*****	10/28/2022, 4:58 PM
vCPUUsage	Object	{}	10/28/2022, 4:58 PM
vThunderIP	String	{"70.37.82.61": null}	10/28/2022, 5:27 PM

3. Select the **azureAutoScaleResources** variable.

The **azureAutoScaleResources** variable window is displayed.

Figure 100 : AzureAutoScaleResources variable window



- Verify the master webhook URL in the **Value** field.

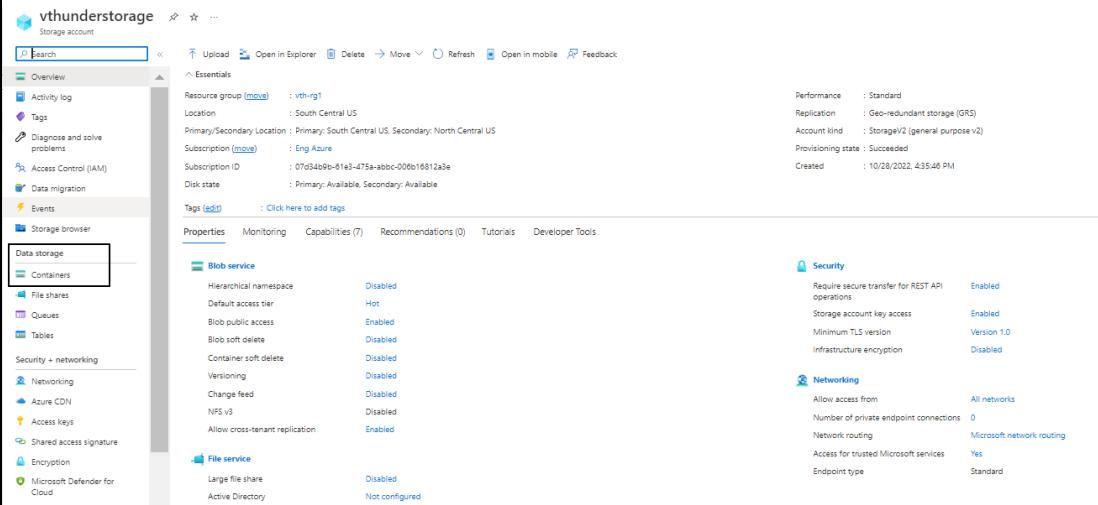
Verify the SSL File availability

To verify the availability of SSL file, perform the following steps:

- From **Home**, navigate thru **Azure Services > Storage Accounts > <storage_account_name>**.
The selected storage account - Overview window is displayed.

Deploy PowerShell Template 3NIC-NVM-VMSS

Figure 101 : Selected storage account - Overview window



Storage account

Overview

Essentials

Resource group (move)	vth-vrg1
Location	South Central US
Primary/Secondary Location	Primary: South Central US; Secondary: North Central US
Subscription (move)	Eng Azure
Subscription ID	07d34b9b-81e3-475a-abb0-00b616812a3e
Disk state	Primary: Available, Secondary: Available
Tags (edit)	Click here to add tags

Properties **Monitoring** **Capabilities (7)** **Recommendations (0)** **Tutorials** **Developer Tools**

Blob service

Hierarchical namespace	Disabled
Default access tier	Hot
Blob public access	Enabled
Blob soft delete	Disabled
Container soft delete	Disabled
Versioning	Disabled
Change feed	Disabled
NFS v3	Disabled
Allow cross-tenant replication	Enabled

File service

Large file share	Disabled
Active Directory	Not configured

Security

Require secure transfer for REST API operations	Enabled
Storage account key access	Enabled
Minimum TLS version	Version 1.0
Infrastructure encryption	Disabled

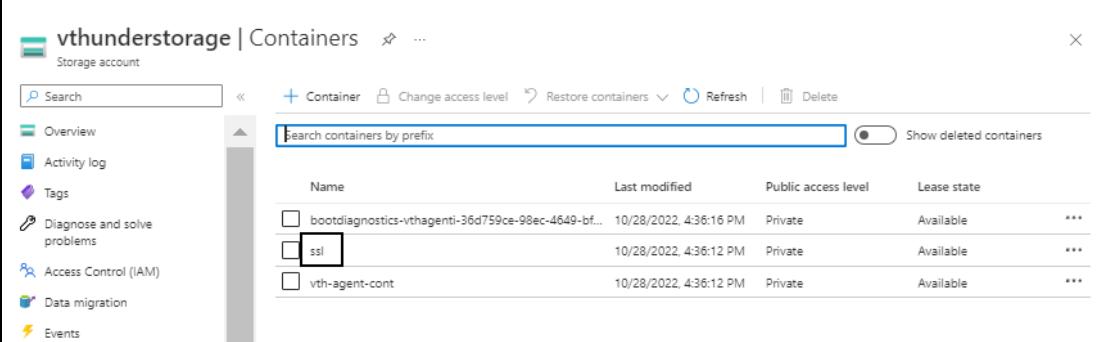
Networking

Allow access from	All networks
Number of private endpoint connections	0
Network routing	Microsoft network routing
Access for trusted Microsoft services	Yes
Endpoint type	Standard

2. Click **Containers** from the left **Data Storage** panel.

The selected storage account - Containers window is displayed.

Figure 102 : Selected storage account - Containers window



vthunderstorage | Containers

Search

Container **Change access level** **Restore containers** **Refresh** **Delete**

Search containers by prefix

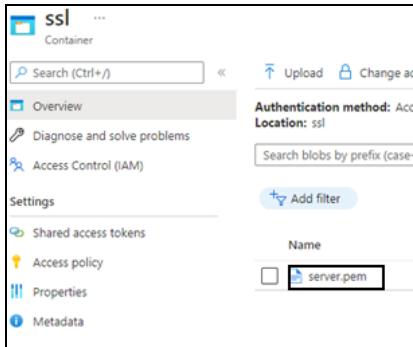
Show deleted containers

Name	Last modified	Public access level	Lease state
bootdiagnostics-vthagenti-36d759ce-98ec-4649-bf...	10/28/2022, 4:36:16 PM	Private	Available ***
ssl	10/28/2022, 4:36:12 PM	Private	Available ***
vth-agent-cont	10/28/2022, 4:36:12 PM	Private	Available ***

3. Select the SSL container.

The SSL container window is displayed.

Figure 103 : SSL Container window



4. Verify if the SSL config file is listed. Here, the SSL config file is **server.pem**.

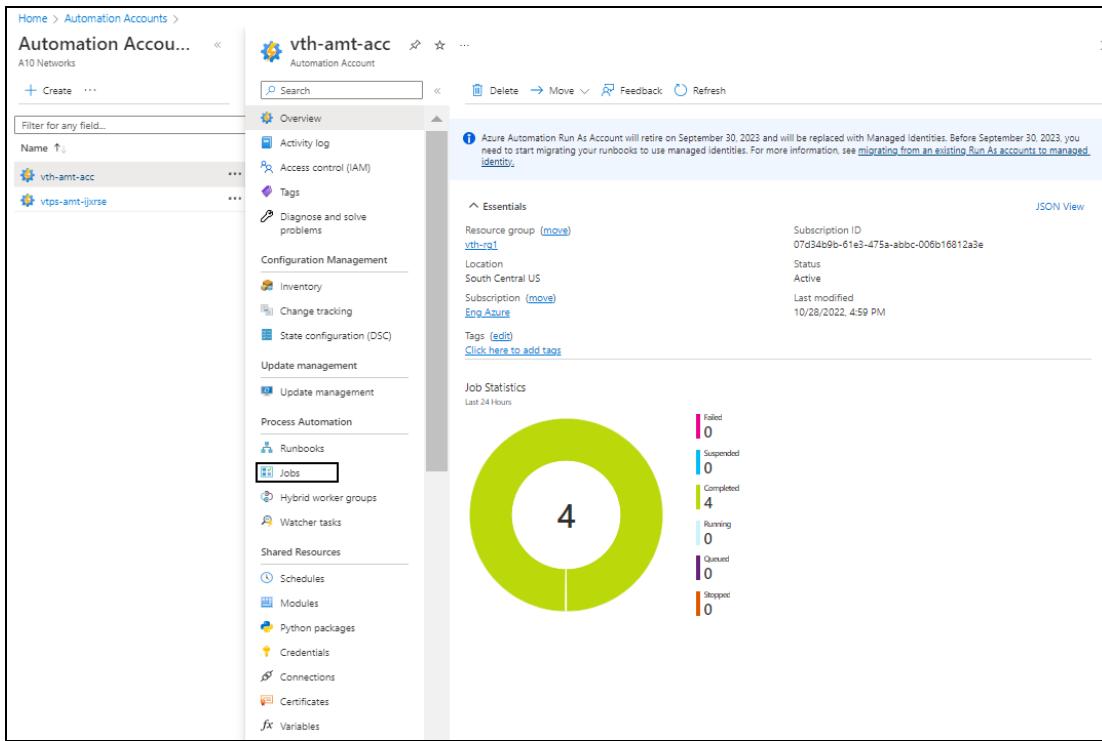
Verify the Runbook Jobs creation

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

1. From **Home**, navigate thru **Azure Services > Automation Accounts > <automation_account_name>**.

The selected automation account - Overview window is displayed.

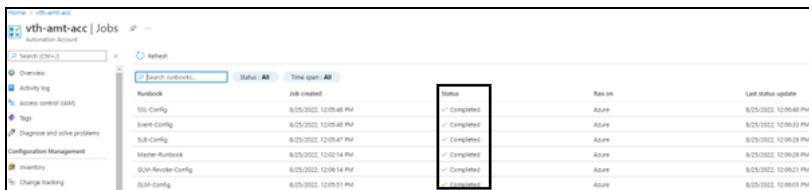
Figure 104 : Selected automation account - Overview window



2. Click **Jobs** from the left **Process Automation** panel.

The selected automation account - Jobs window is displayed.

Figure 105 : Selected automation account - Jobs window



Job name	Status	Job created	Run on	Last status update
Runbook	Completed	8/25/2022, 12:05:48 PM	Azure	8/25/2022, 12:06:40 PM
SSL-Config	Completed	8/25/2022, 12:05:49 PM	Azure	8/25/2022, 12:06:33 PM
Event-Config	Completed	8/25/2022, 12:05:49 PM	Azure	8/25/2022, 12:06:29 PM
SLB-Config	Completed	8/25/2022, 12:05:49 PM	Azure	8/25/2022, 12:06:29 PM
Master-Runbook	Completed	8/25/2022, 12:05:49 PM	Azure	8/25/2022, 12:06:29 PM
QoS-Reader Config	Completed	8/25/2022, 12:06:14 PM	Azure	8/25/2022, 12:06:21 PM
QoS-Config	Completed	8/25/2022, 12:05:51 PM	Azure	8/25/2022, 12:06:09 PM

3. Verify if all the runbook jobs have completed status.

The master runbook automatically triggers all the jobs one by one.

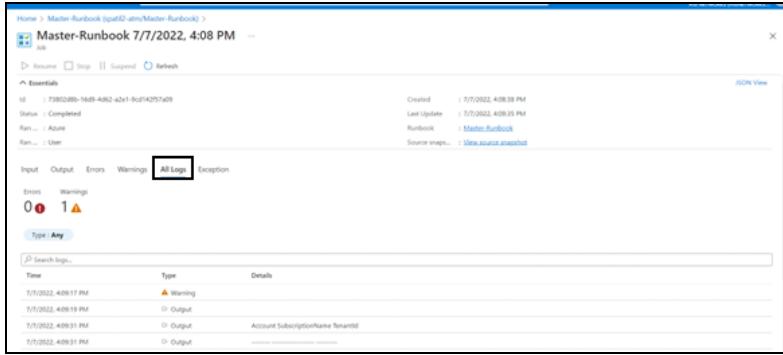
NOTE: It may take the system a few minutes to display the completed status.

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 106 : 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.

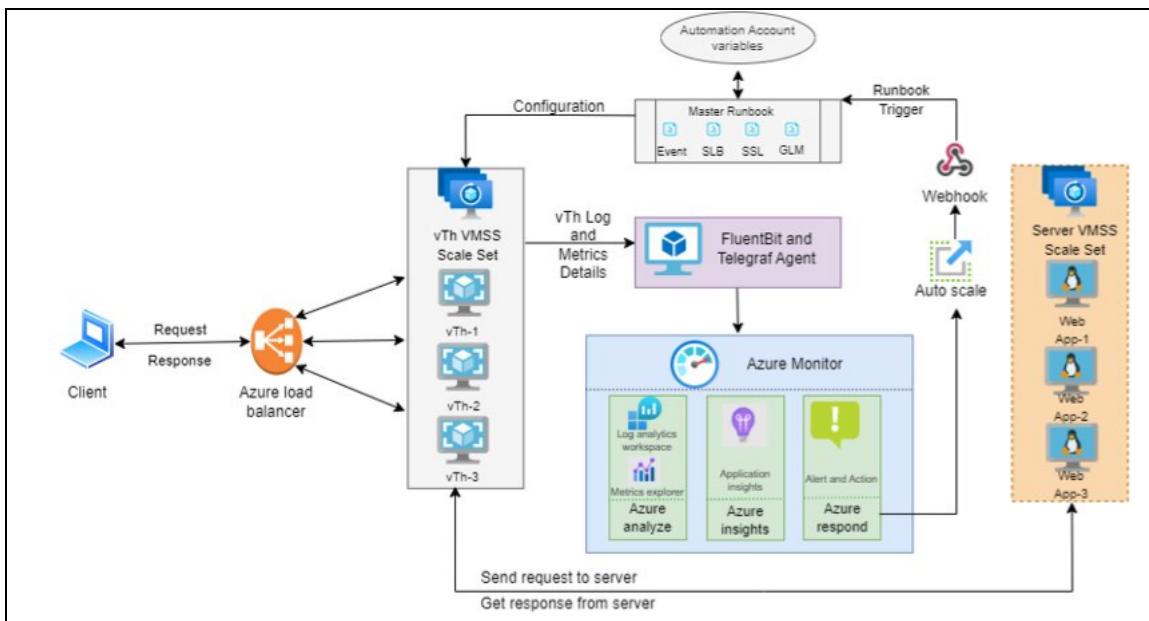
- AutoScaling can be done as per the automation account threshold configuration with variable name **ThresholdForScaleOut** and **ThresholdForScaleIn** for Scale Out and Scale In respectively.
- vThunder logs cannot be viewed in Azure log analytics workspace. For more information, see [Azure Log Function](#).
- CPU utilization of vThunder cannot be viewed in Azure application insight console.

Autoscaling Options

Configure Autoscaling and Log Monitoring using Agent Setup

[Figure 107](#) 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 107 : 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

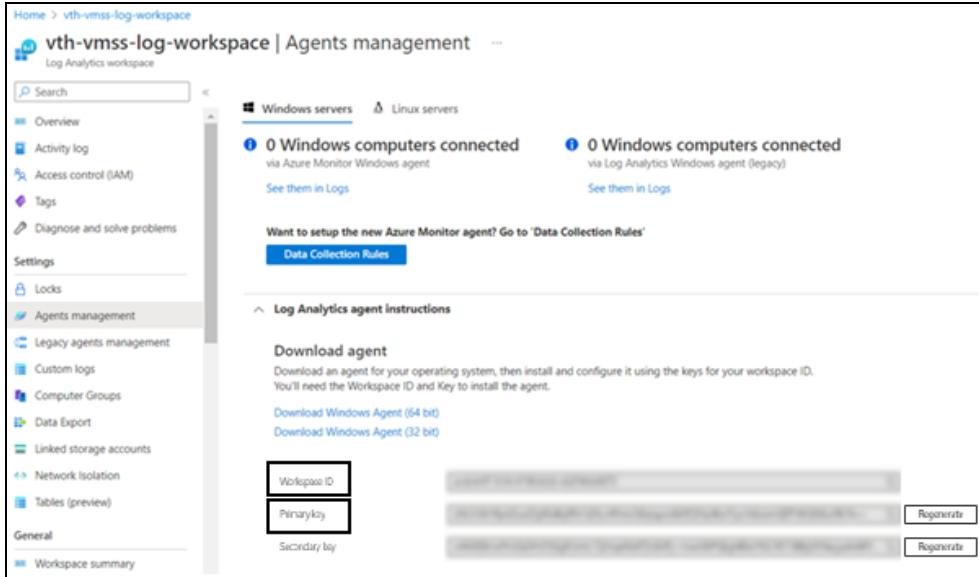
To configure autoscaling and log monitoring using the PowerShell template, perform the following steps:

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 108 : Agents management window



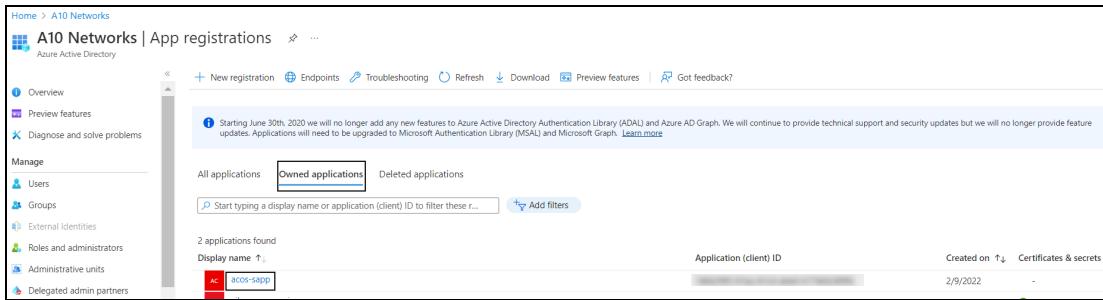
The screenshot shows the 'Agents management' section of the Azure Log Analytics workspace. It displays two sections: 'Windows servers' and 'Linux servers', both showing 0 connected computers. Below these are sections for 'Data Collection Rules' and 'Log Analytics agent instructions'. Under 'Download agent', there are links for 'Download Windows Agent (64 bit)' and 'Download Windows Agent (32 bit)'. A key pair for the workspace is shown, with 'Workspace ID' and 'Primary key' fields, each having a 'Regenerate' button.

3. Update client ID, tenant ID, and client secret.

```
(cat /etc/environment; echo "AZURE_CLIENT_ID=10724xxx-xxxx-xxxx-xxxx-xxxxc14726d"; echo "AZURE_TENANT_ID=91d27xxx-xxxx-xxxx-xxxx-xxxxbf81fc82f"; 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 109 : Azure active directory - App registrations window



The screenshot shows the 'App registrations' page for the 'A10 Networks' tenant. The 'Owned applications' tab is selected. A message at the top states: 'Starting June 30th, 2020 we will no longer add new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph.' Below this, a table lists the registered application 'a10c-sapp' with details like Application (client) ID, Created on (2/9/2022), and Certificates & secrets.

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 110 : Selected application insight - Overview window

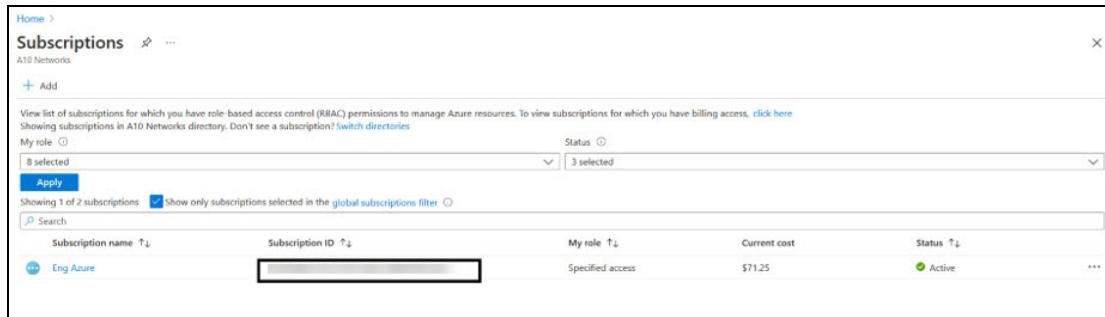


- Navigate to the folder where you have downloaded the PowerShell template > plugins > telegraf > plugins > inputs > customplugin and open **get_cpu_param.json** file with a text editor to configure the CPU parameters.

```
{
  "Subscription_Id": "07d3xxxx-xxxx-xxxx-xxxx-xxxxxx6812a3e",
  "ResourceGroupName": "vth-rg1",
  "VmssName": "vth-vmss"
}
```

You can get the Subscription ID value from **Home > Azure Services > Subscriptions > <subscription_name>**.

Figure 111 : Subscriptions window



- 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:

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

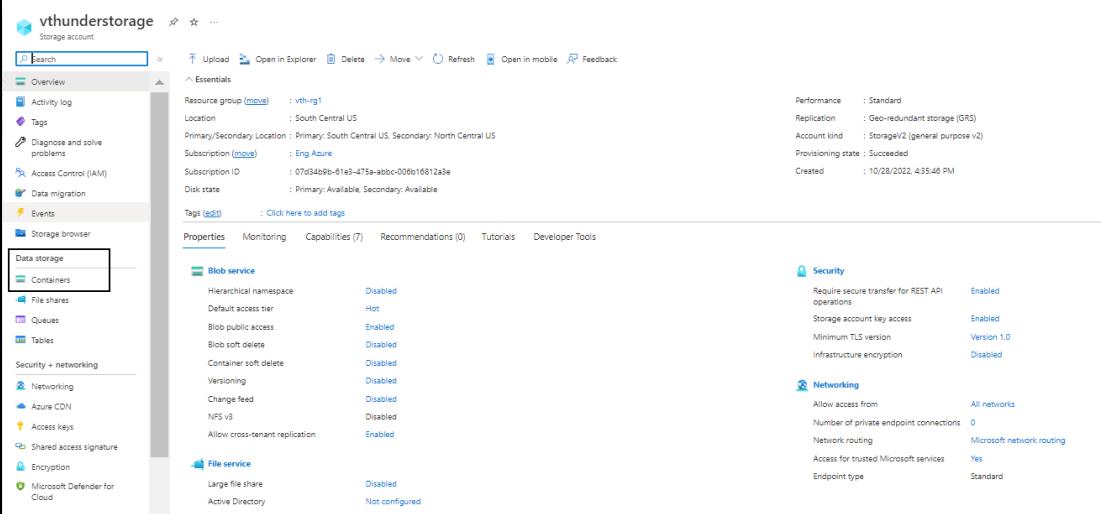
Verify Log Agent file upload

To verify if the log agent file is uploaded, perform the following steps:

- From **Home**, navigate thru **Azure Services > Storage Accounts > <storage_account_name>**.

The selected storage account - Overview window is displayed.

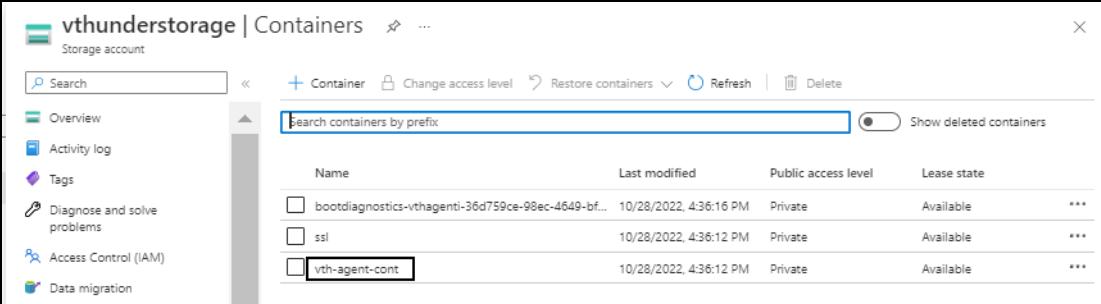
Figure 112 : Selected storage account - Overview window



Properties		Monitoring		Capabilities (7)		Recommendations (0)		Tutorials		Developer Tools	

- Click **Containers** from the left Data Storage panel.

The selected storage account - Containers window is displayed.

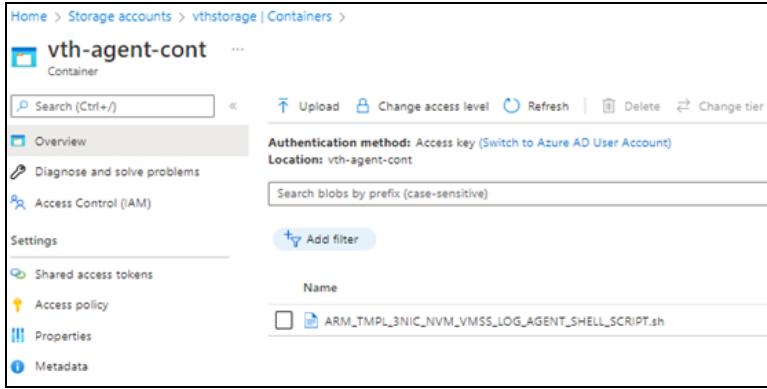


Name	Last modified	Public access level	Lease state
bootdiagnostics-vthagenti-36d759ce-90ec-4649-bf...	10/28/2022, 4:36:16 PM	Private	Available
ssl	10/28/2022, 4:36:12 PM	Private	Available
vth-agent-cont	10/28/2022, 4:36:12 PM	Private	Available

- Select the agent container.

The agent container window is displayed.

Figure 113 : Agent container window



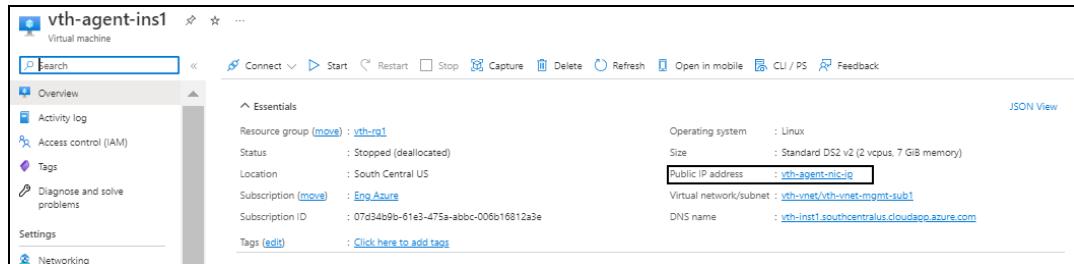
- Verify if PS_TMPL_3NIC_NVM_VMSS_LOG_AGENT_SHELL_SCRIPT.sh file is uploaded.

Access vThunder Agent using CLI

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

- Open PuTTY.
- 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 114 : Virtual machine - Agent instance window



- Click Open.
- 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]: 2022-08-25T10:42:16Z
E! [outputs.influxdb] When writing to [http://localhost:8086] : failed
doing req: Post ">
Aug 25 10:42:16 vth-agent-ins1 telegraf[17855]: 2022-08-25T10:42:16Z
E! [agent] Error writing to outputs.influxdb: could not write any
address
Aug 25 10:42:26 vth-agent-ins1 telegraf[17855]: 2022-08-25T10:42:16Z
E! [outputs.influxdb] When writing to [http://localhost:8086] : failed

```

```
doing req: Post ">
Aug 25 10:42:26 vth-agent-ins1 telegraf[17855]: 2022-08-25T10:42:16Z
E! [agent] Error writing to outputs.influxdb: could not write any
address
Aug 25 10:42:36 vth-agent-ins1 telegraf[17855]: 2022-08-25T10:42:16Z
E! [outputs.influxdb] When writing to [http://localhost:8086] : failed
doing req: Post ">
Aug 25 10:42:36 vth-agent-ins1 telegraf[17855]: 2022-08-25T10:42:16Z
E! [agent] Error writing to outputs.influxdb: could not write any
address
Aug 25 10:42:46 vth-agent-ins1 telegraf[17855]: 2022-08-25T10:42:16Z
E! [outputs.influxdb] When writing to [http://localhost:8086] : failed
doing req: Post ">
Aug 25 10:42:46 vth-agent-ins1 telegraf[17855]: 2022-08-25T10:42:16Z
E! [agent] Error writing to outputs.influxdb: could not write any
address
Aug 25 10:42:56 vth-agent-ins1 telegraf[17855]: 2022-08-25T10:42:16Z
E! [outputs.influxdb] When writing to [http://localhost:8086] : failed
doing req: Post ">
Aug 25 10:42:56 vth-agent-ins1 telegraf[17855]: 2022-08-25T10:42:16Z
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

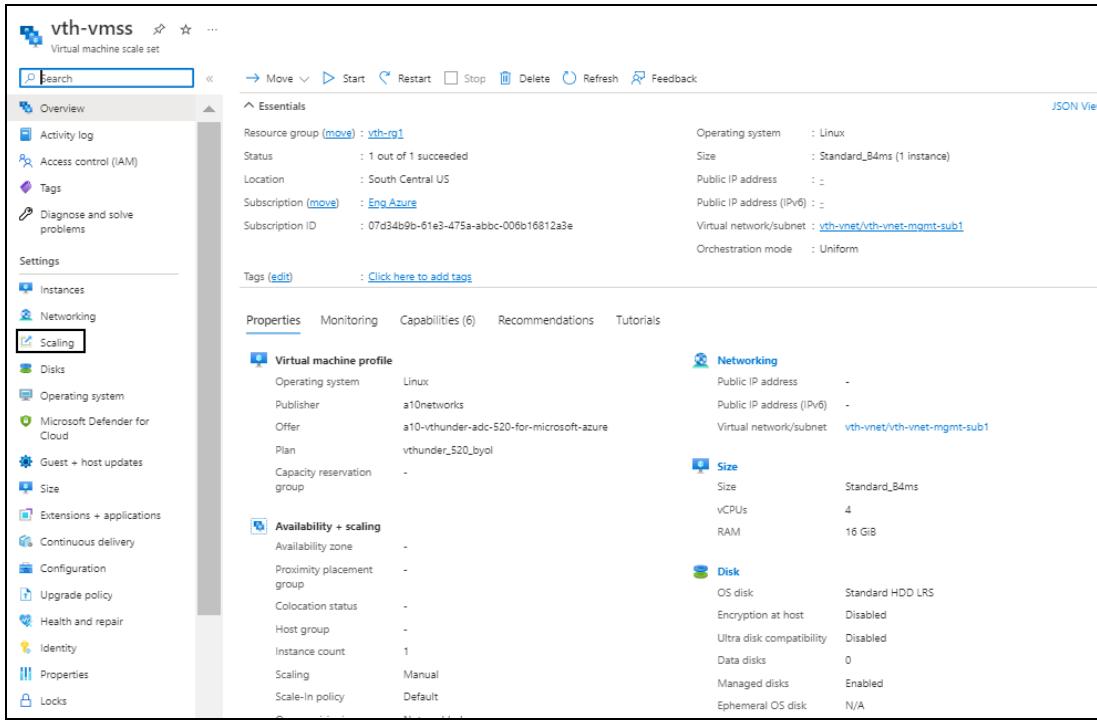
To create autoscale rule, perform the following steps:

1. From **Home**, navigate thru **Azure Services > Virtual machine scale set > <vmss_name>**.

The selected vmss - Overview window is displayed.

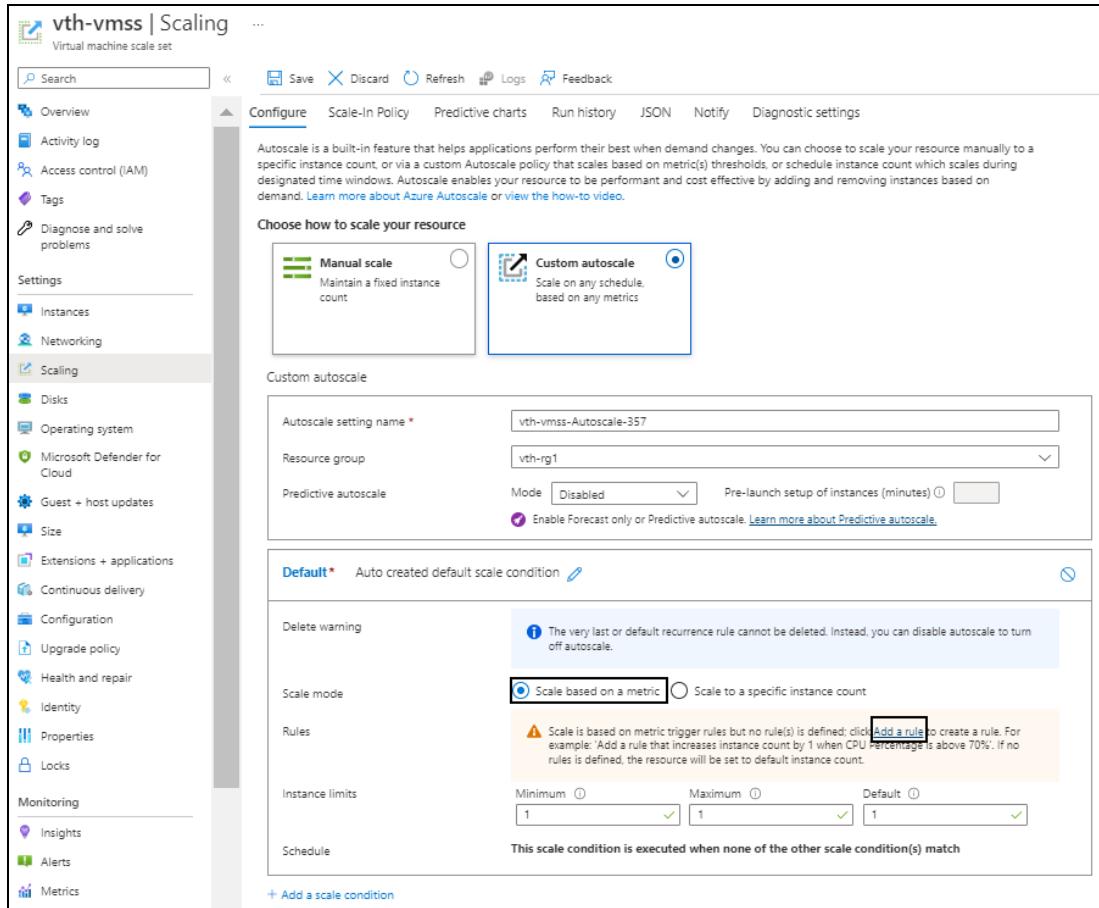
[Deploy PowerShell Template 3NIC-NVM-VMSS](#)

Figure 115 : Selected VMSS - Overview window



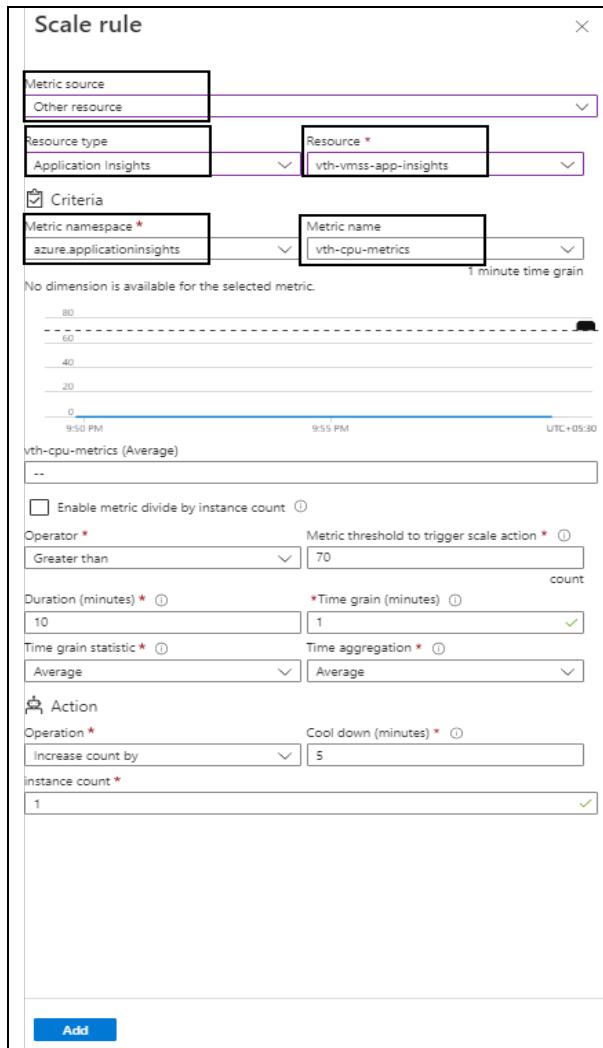
2. Click **Scaling** from the left **Settings** panel.
The selected vmss - Scaling window is displayed.

Figure 116 : 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 117 : Scale rule window



6. Select or enter the information in the following fields:

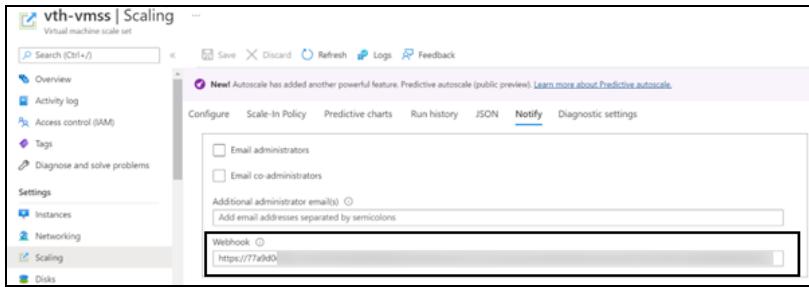
- Metric source: Other resource
- Resource type: Application Insights
- Resource
- Time aggregation
- Metric namespace
- Metric name

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 118 : Selected VMSS - Scaling window - Notify tab



Create Autoscale Alert

1. From **Home**, navigate thru **Azure Services > Virtual machine scale set > <vmss_name>**.
The selected vmss - Overview window is displayed.

[Deploy PowerShell Template 3NIC-NVM-VMSS](#)

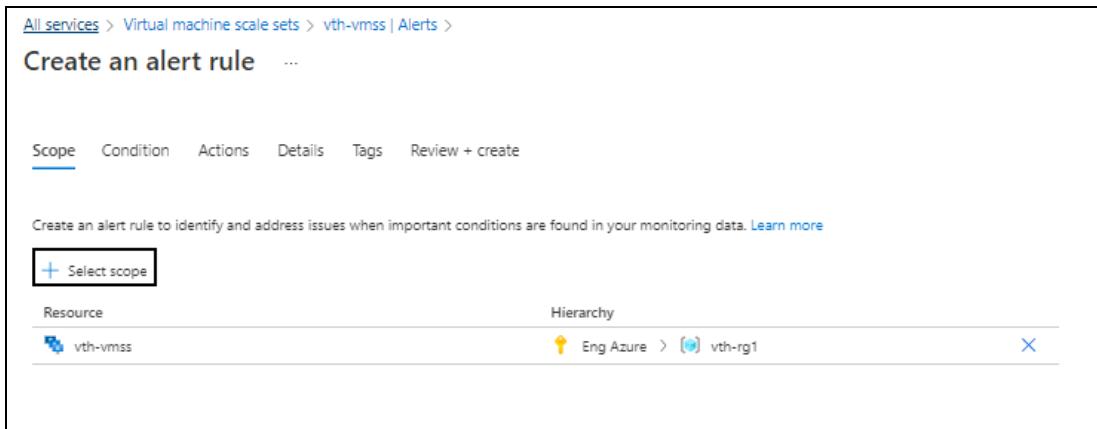
Figure 119 : Selected VMSS - Overview window

- Click **Alerts** from the left **Monitoring** panel.
- The selected vmss - Alerts window is displayed.

Figure 120 : Selected VMSS - Alerts window

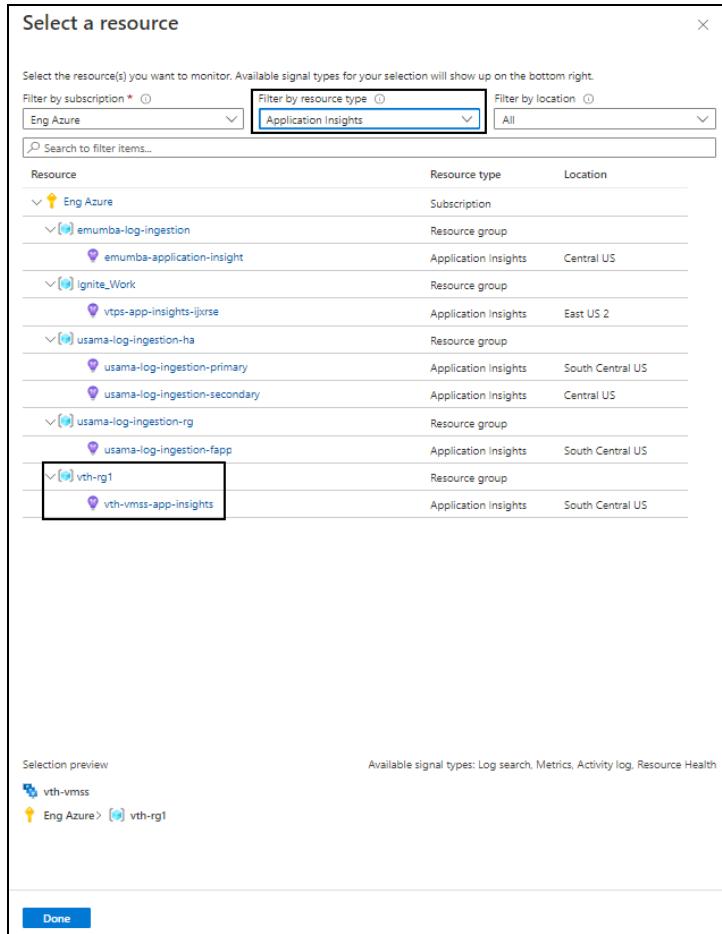
- Click **Create > Alert rule**.
- The Create an alert rule - Scope window is displayed.

Figure 121 : Create an alert rule window - Scope tab



4. Click **Select scope** in the **Scope** tab.
The **Select a resource** window is displayed.

Figure 122 : Select a resource window



5. From Filter by resource type, select Application Insights.

The resource group having application insight resources are displayed.

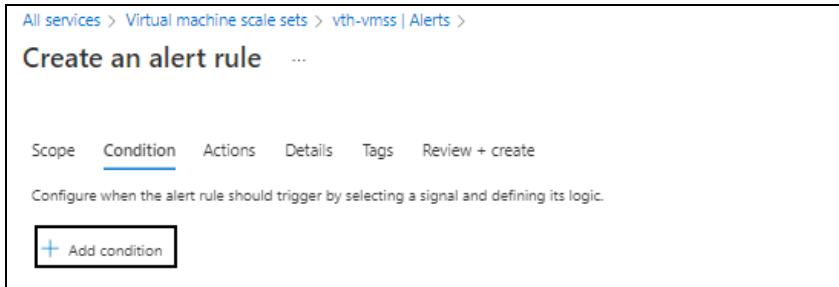
6. Select the required application insight resource and click Done.

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.

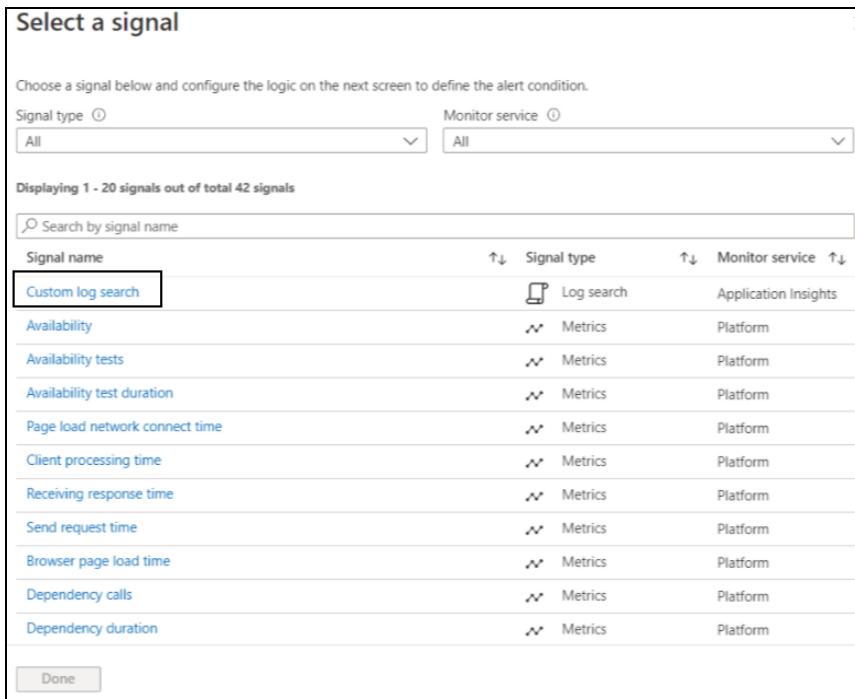
Figure 123 : Create an alert rule window - Condition tab



- Click **Add condition** in the **Condition** tab.

The **Select a signal** window is displayed.

Figure 124 : Select a signal window



- Select **Custom log search** as the signal.

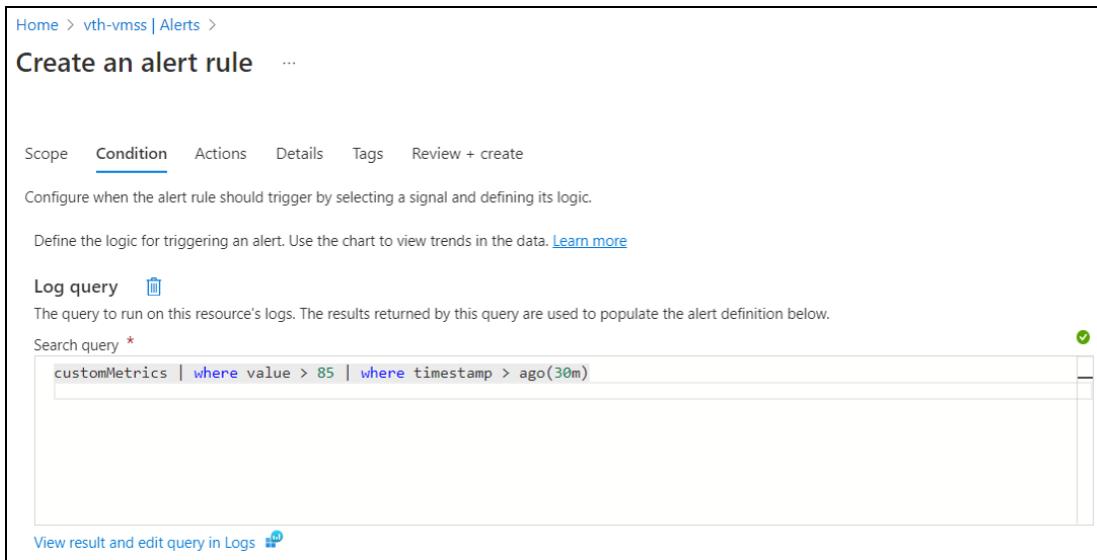
The window to define the signal's logic is displayed in the alert rule condition.

- 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.

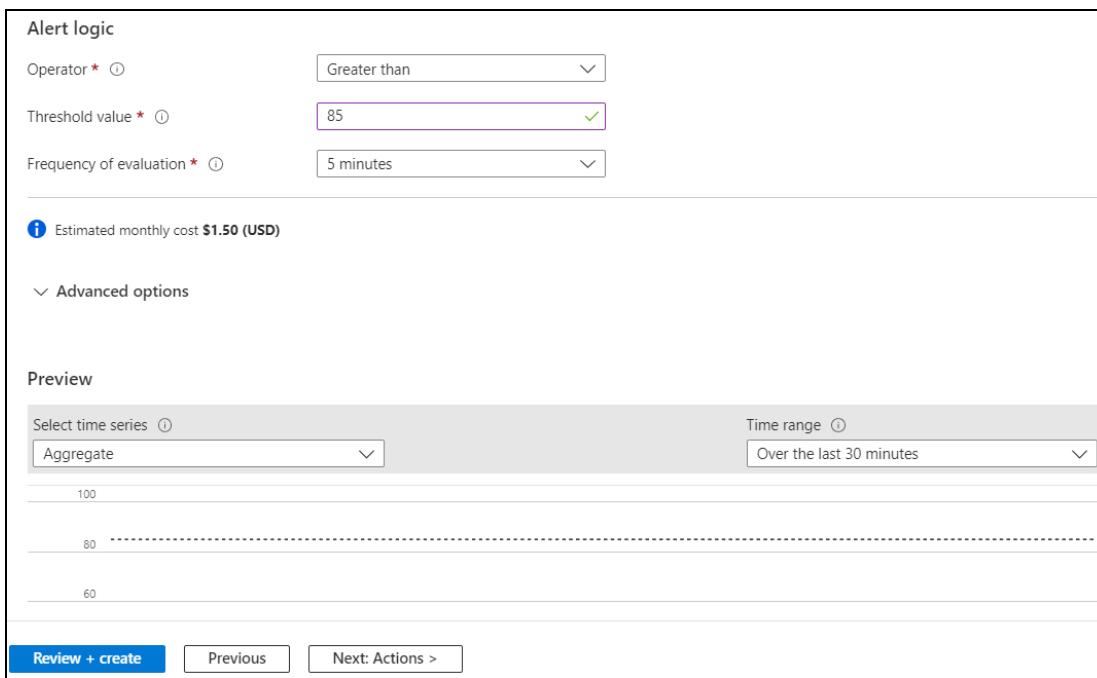
Figure 125 : Create an alert rule window - Condition tab



The screenshot shows the 'Create an alert rule' window with the 'Condition' tab selected. At the top, there are tabs for Scope, Condition, Actions, Details, Tags, and Review + create. Below the tabs, a note says: 'Configure when the alert rule should trigger by selecting a signal and defining its logic.' A link 'Learn more' is provided. Under 'Log query', it says: 'The query to run on this resource's logs. The results returned by this query are used to populate the alert definition below.' A search bar contains the query: 'customMetrics | where value > 85 | where timestamp > ago(30m)'. A green checkmark is next to the search bar. At the bottom, a link 'View result and edit query in Logs' is shown.

11. Configure alert logic in the Alert logic section.

Figure 126 : Alert logic section

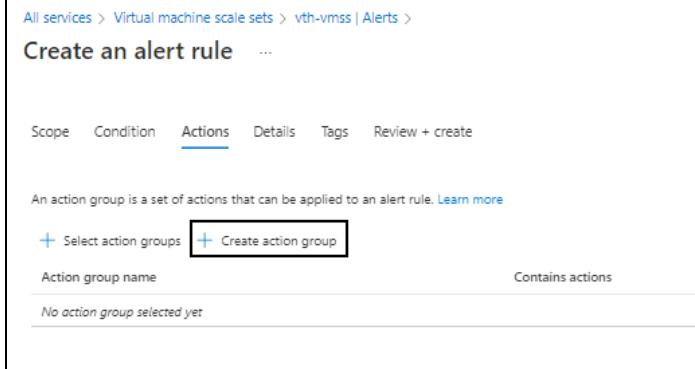


The screenshot shows the 'Alert logic' configuration section. It includes fields for Operator (set to 'Greater than'), Threshold value (set to '85'), and Frequency of evaluation (set to '5 minutes'). A note below states: 'Estimated monthly cost \$1.50 (USD)'. The 'Advanced options' section is collapsed. The 'Preview' section shows a line chart with data points at 100, 80, and 60, spanning a time range of 'Over the last 30 minutes'. Navigation buttons at the bottom include 'Review + create', 'Previous', and 'Next: Actions >'.

Depending upon the signal logic configuration, the monthly cost for the alert is displayed.

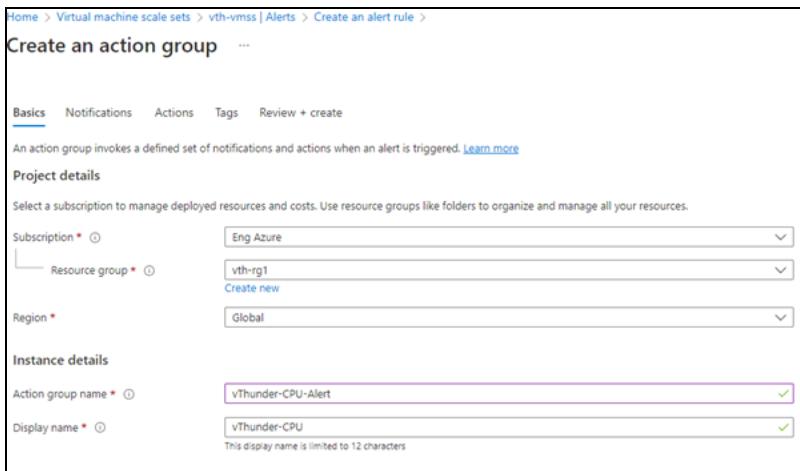
12. Click **Next : Actions** at the bottom of the window.
The **Create an alert rule - Actions** window is displayed.

Figure 127 : Create an alert rule window - Actions tab



13. Click **Create action group**.
The **Create an action group - Basics** window is displayed.

Figure 128 : Create an action group window - Basics tab



- a. Select or enter the following mandatory information in the **Basics** tab:

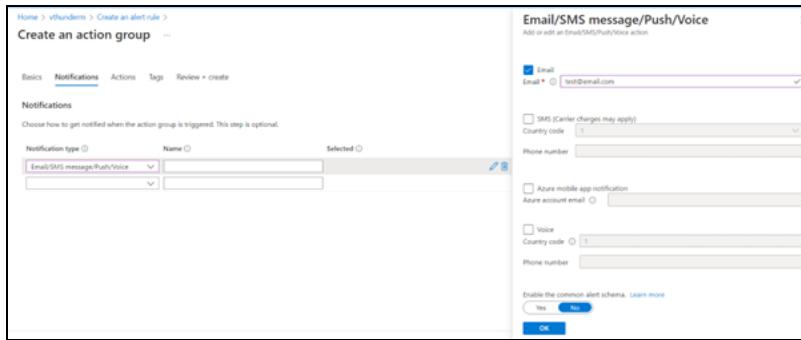
Project details

- Subscription
- Resource group
- Region

Instance details

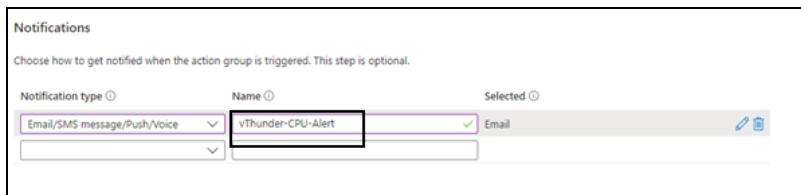
- Action group name
 - Display name
- b. Click **Next : Notifications** at the bottom of the window.
The **Create an action group - Notifications** window is displayed.
- c. Select the **Notification type**.
The corresponding window to configure the notification type is displayed.

Figure 129 : Create an action group window - Notifications tab - Type



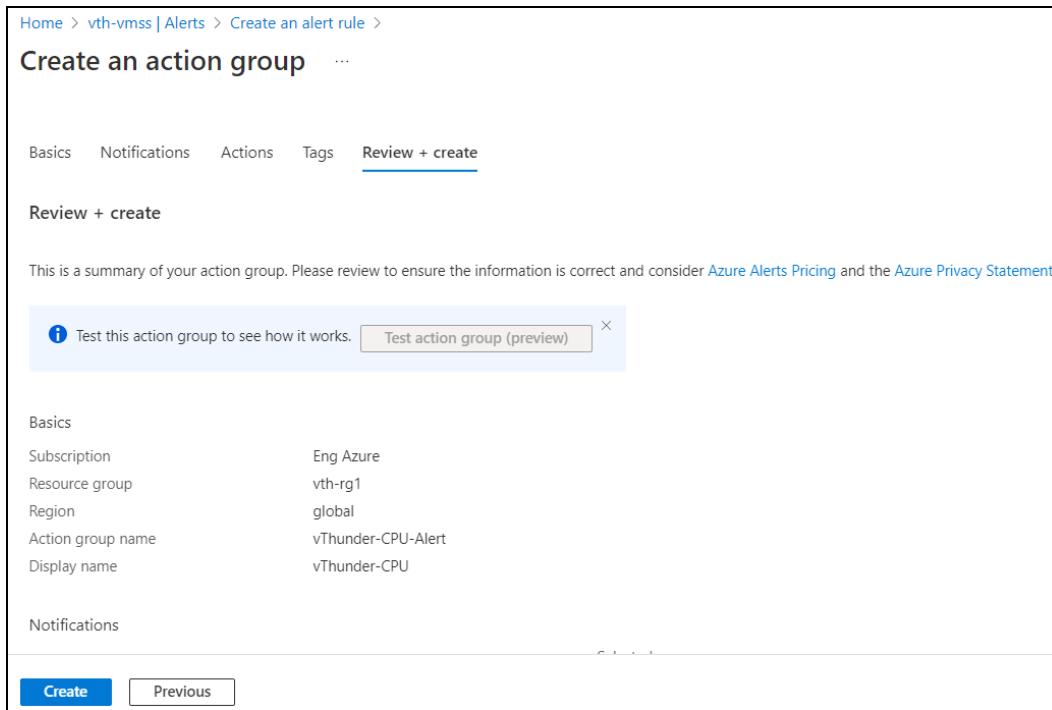
- d. Select the **Email** option and provide the correct email ID in the **Email** field and then click **OK**.
- e. Enter a unique name for the notification in the **Name** field.

Figure 130 : 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.

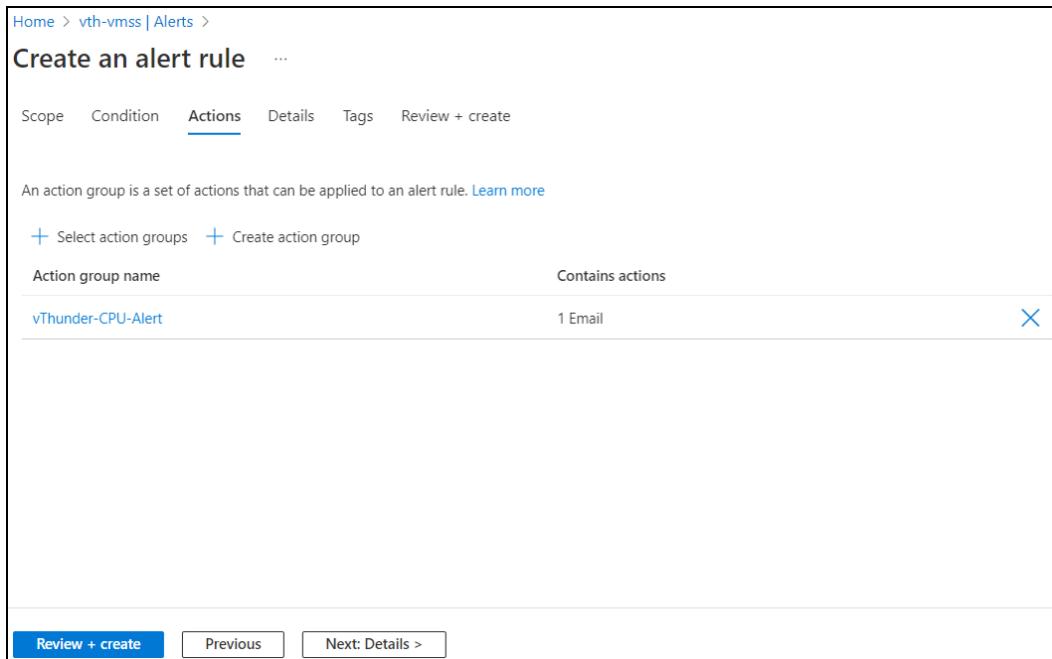
Figure 131 : Create an action group window - Review + create tab



g. Click **Create**.

The action group is listed under **Actions** tab.

Figure 132 : Create an alert rule window - Actions tab

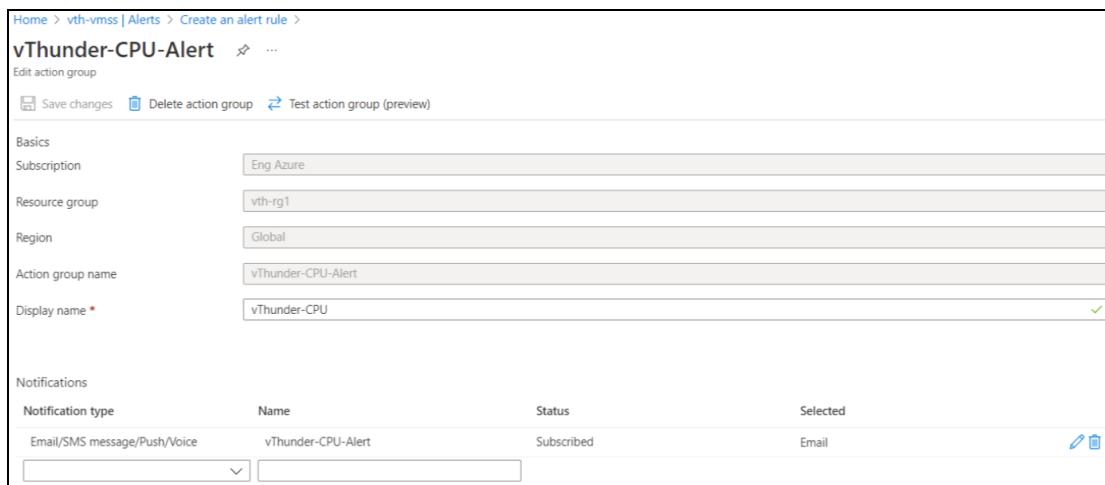


The screenshot shows the 'Create an alert rule' window with the 'Actions' tab selected. At the top, there are tabs for Scope, Condition, Actions (which is underlined), Details, Tags, and Review + create. Below the tabs, a message states: 'An action group is a set of actions that can be applied to an alert rule.' with a 'Learn more' link. There are two buttons: '+ Select action groups' and '+ Create action group'. A table lists an action group named 'vThunder-CPU-Alert' which 'Contains actions' (1 Email). A blue 'X' button is next to the table row. At the bottom, there are buttons for 'Review + create', 'Previous', and 'Next: Details >'

14. Select the recently created action group.

The selected action group is displayed.

Figure 133 : Selected action group

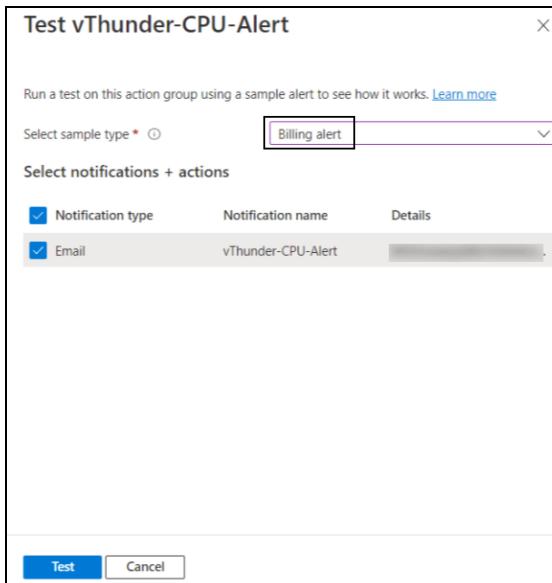


The screenshot shows the 'Edit action group' window for 'vThunder-CPU-Alert'. It has sections for Basics (Subscription: Eng Azure, Resource group: vth-rg1, Region: Global, Action group name: vThunder-CPU-Alert, Display name: vThunder-CPU) and Notifications (Email/SMS message/Push/Voice: vThunder-CPU-Alert, Status: Subscribed, Selected: Email). Buttons at the top include Save changes, Delete action group, and Test action group (preview).

15. Click **Test action group (preview)**.

The Test <action_group_name>-alert window is displayed.

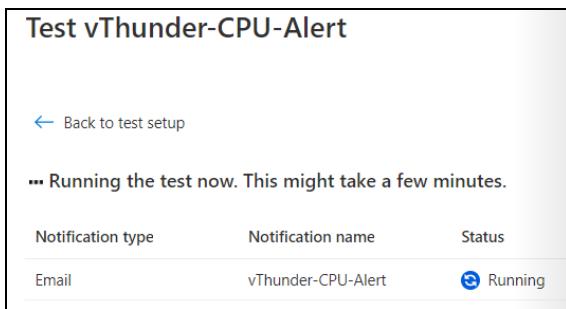
Figure 134 : Test <action_group_name>-alert window



16. Select **Billing alert** as the Sample type and click **Test**.

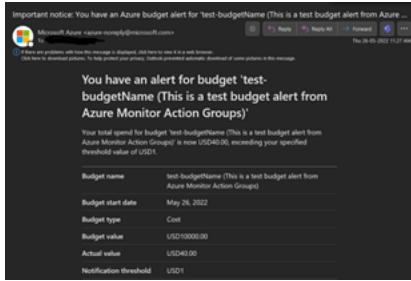
The running status for the test rule is displayed.

Figure 135 : Test <action_group_name>-alert window - Running status



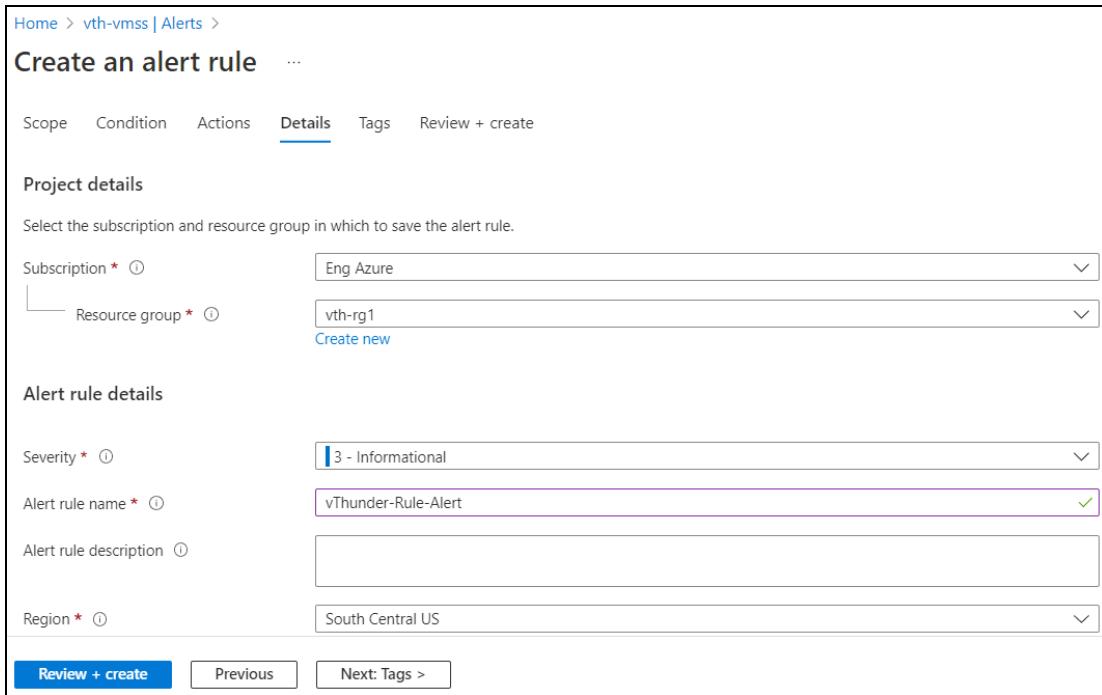
When the success status is displayed, an email notification is triggered to the email ID provided in the [Email Notification](#) step.

Figure 136 : 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 137 : Create an alert rule window - Details tab



The screenshot shows the 'Create an alert rule - Details' window in the Azure portal. The window has a header 'Home > vth-vmss | Alerts > Create an alert rule ...'. Below the header, there are tabs: Scope, Condition, Actions, **Details**, Tags, and Review + create. The **Details** tab is selected.

Project details

Select the subscription and resource group in which to save the alert rule.

Subscription *: Eng Azure

Resource group *: vth-rg1

Alert rule details

Severity *: 3 - Informational

Alert rule name *: vThunder-Rule-Alert

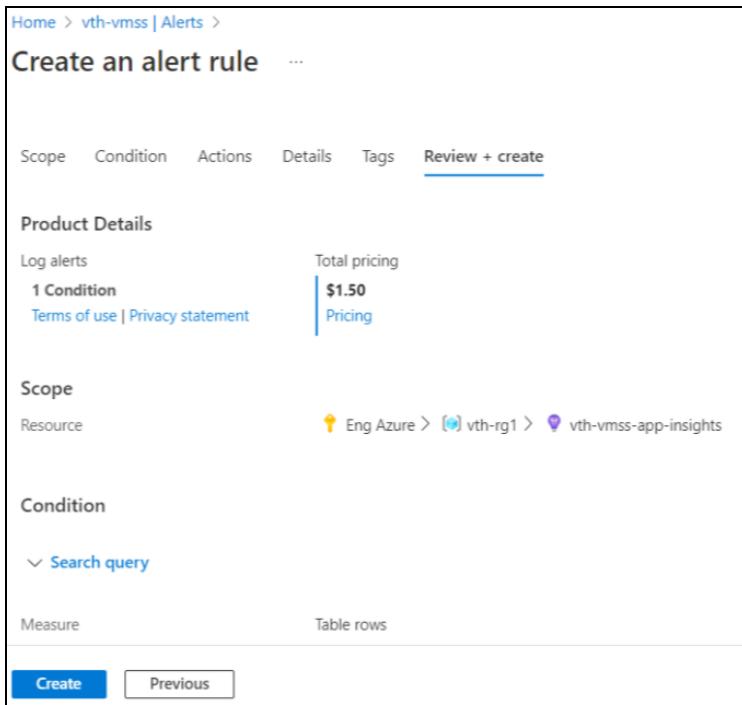
Alert rule description: (empty text area)

Region *: South Central US

At the bottom of the window are buttons: **Review + create** (highlighted in blue), **Previous**, and **Next: Tags >**.

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.

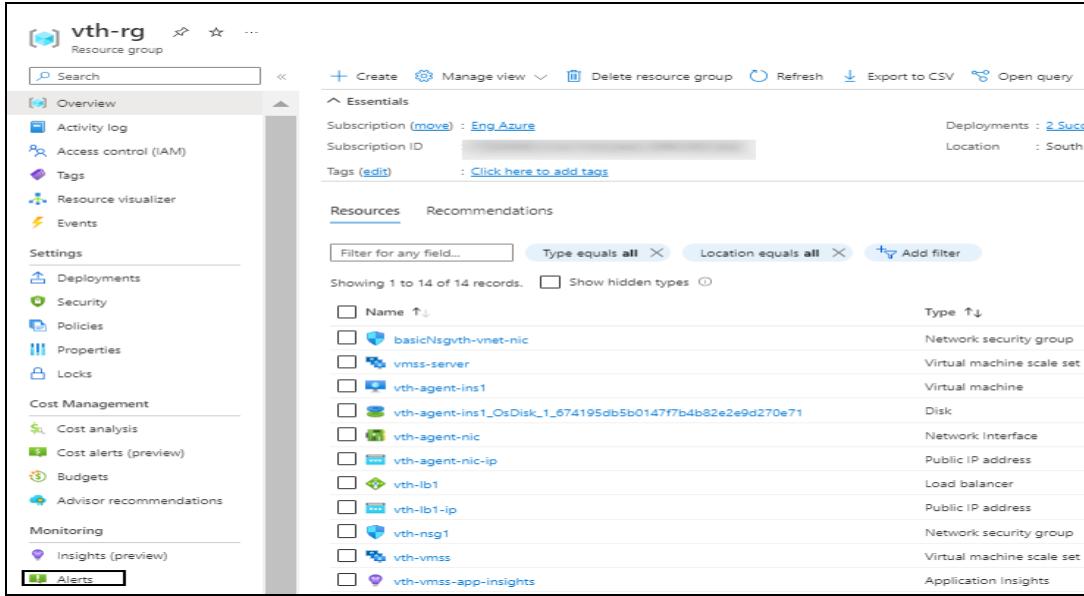
Figure 138 : Create an alert rule window - Review + create tab



22. Click **Create**.
The alert rule is created.
23. From **Home**, navigate thru **Azure Services > Resource groups > <resource_group_name>**.
The selected resource group - Overview window is displayed.

[Deploy PowerShell Template 3NIC-NVM-VMSS](#)

Figure 139 : Selected resource group - Overview window



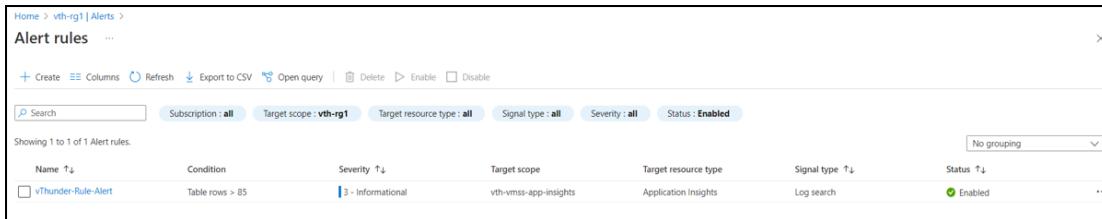
24. Click **Alerts** from the left **Monitoring** panel.

The selected alert window is displayed.

25. Click **Alert rules**.

The alert rules for the selected resource group is displayed.

Figure 140 : Selected resource group - Alert rules window



Verify Logs in Log Analytics Workspace

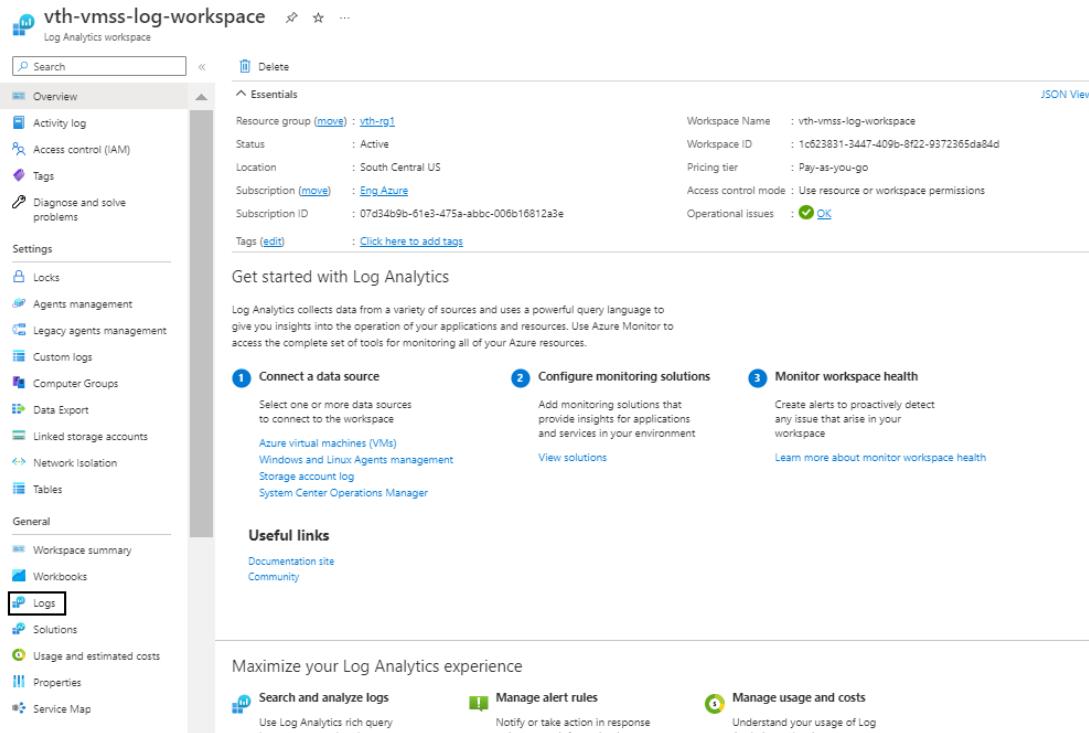
To verify the logs in log analytics workspace, perform the following steps:

- From **Home**, navigate thru **Azure Services > Log Analytics workspaces > <log_workspace_name>**.

The selected log workspace - Overview window is displayed.

Deploy PowerShell Template 3NIC-NVM-VMSS

Figure 141 : Selected log workspace - Overview window



Essentials

- Resource group ([move](#)) : [vth-rg1](#)
- Status : Active
- Location : South Central US
- Subscription ([move](#)) : [Eng_Azure](#)
- Subscription ID : 07a34b9b-61e3-475a-abbc-006b16812a3e
- Tags ([edit](#)) : [Click here to add tags](#)

Workspace Name : vth-vmss-log-workspace
Workspace ID : 1c623831-3447-409b-8f22-9372365da84d
Pricing tier : Pay-as-you-go
Access control mode : Use resource or workspace permissions
Operational issues : [OK](#)

Get started with Log Analytics

Log Analytics collects data from a variety of sources and uses a powerful query language to give you insights into the operation of your applications and resources. Use Azure Monitor to access the complete set of tools for monitoring all of your Azure resources.

1 Connect a data source
Select one or more data sources to connect to the workspace

- Azure virtual machines (VMs)
- Windows and Linux Agents management
- Storage account log
- System Center Operations Manager

2 Configure monitoring solutions
Add monitoring solutions that provide insights for applications and services in your environment

3 Monitor workspace health
Create alerts to proactively detect any issue that arise in your workspace

[View solutions](#) [Learn more about monitor workspace health](#)

Useful links

- [Documentation site](#)
- [Community](#)

Maximize your Log Analytics experience

Search and analyze logs
Use Log Analytics rich query [Learn more about rich queries](#)

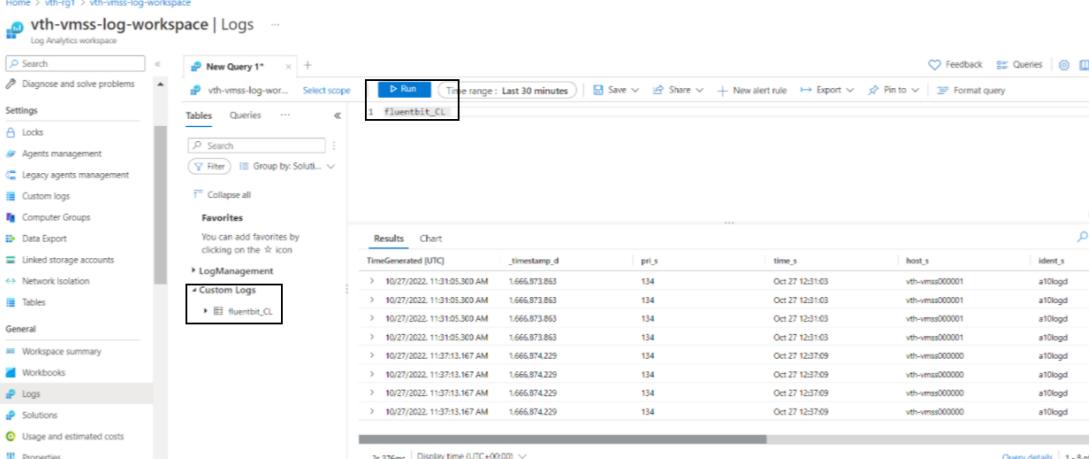
Manage alert rules
Notify or take action in response to important information in your logs [Learn more about alert rules](#)

Manage usage and costs
Understand your usage of Log Analytics and optimize your costs [Learn more about usage and costs](#)

b. Click **Logs** from the left **General** panel.

The selected log window is displayed.

Figure 142 : Selected log analytics workspace - Logs window



TimeGenerated (UTC)	_timestamp_d	pri_s	time_s	host_s	ident_s
> 10/27/2022 11:31:05.300 AM	1666873863	134	Oct 27 12:31:03	vth-vmss000001	a10logd
> 10/27/2022 11:31:05.300 AM	1666873863	134	Oct 27 12:31:03	vth-vmss000001	a10logd
> 10/27/2022 11:31:05.300 AM	1666873863	134	Oct 27 12:31:03	vth-vmss000001	a10logd
> 10/27/2022 11:31:05.300 AM	1666873863	134	Oct 27 12:31:03	vth-vmss000001	a10logd
> 10/27/2022 11:31:13.167 AM	1666874229	134	Oct 27 12:37:09	vth-vmss000000	a10logd
> 10/27/2022 11:31:13.167 AM	1666874229	134	Oct 27 12:37:09	vth-vmss000000	a10logd
> 10/27/2022 11:31:13.167 AM	1666874229	134	Oct 27 12:37:09	vth-vmss000000	a10logd
> 10/27/2022 11:31:13.167 AM	1666874229	134	Oct 27 12:37:09	vth-vmss000000	a10logd

c. Expand **Custom Logs** in the left **Tables** tab panel.

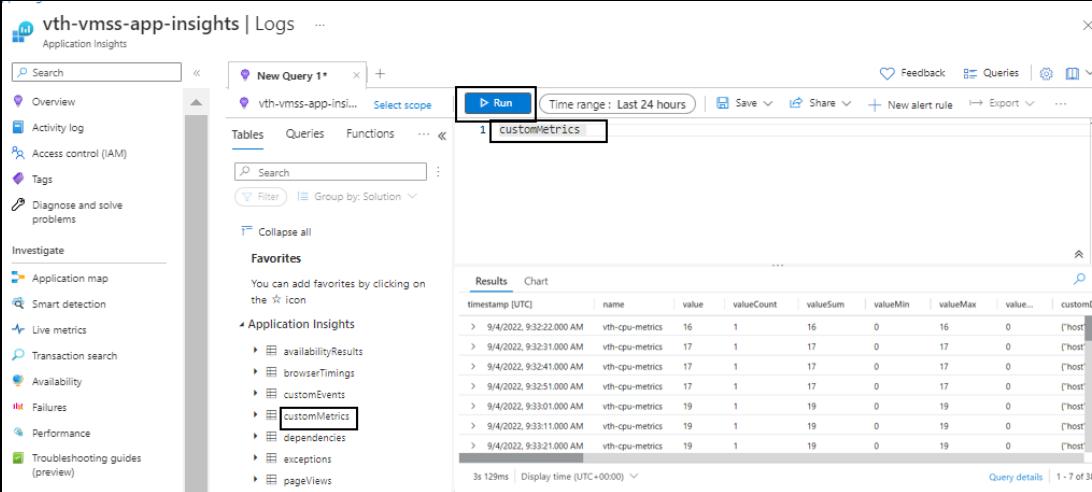
- d. Double-click **fluentbit_CL**.
The fluentbi_CL query window is displayed.
- e. Click **Run**.
All logs are displayed in tabular format with expandable details.

Verify Metrics in Application Insights

To verify if the metrics in application insights, perform the following steps:

- a. From **Home**, navigate thru **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 143 : Selected application insight - Logs window



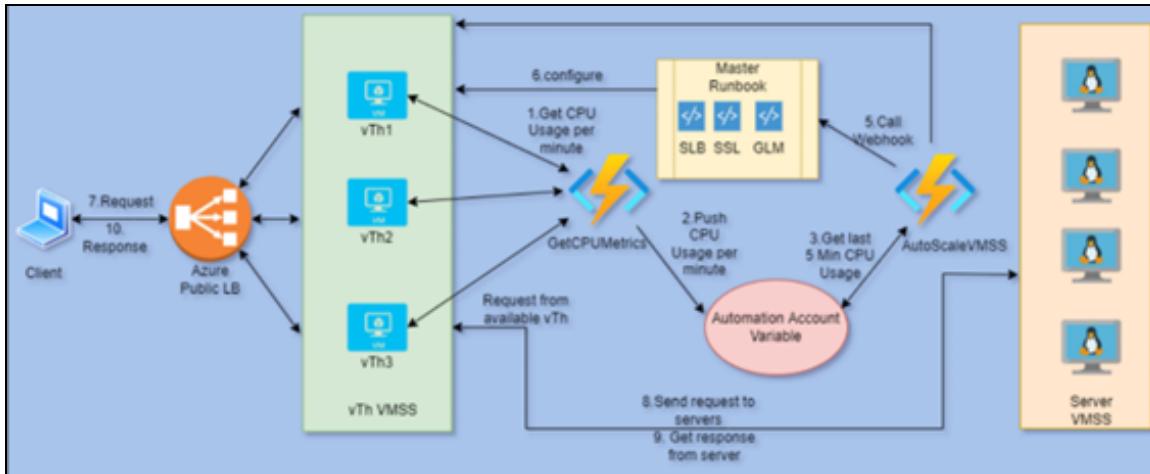
The screenshot shows the Azure Application Insights Logs interface. On the left, there's a navigation sidebar with links like Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. Under Investigate, there are sections for Application map, Smart detection, Live metrics, Transaction search, Availability, Failures, Performance, and Troubleshooting guides (preview). The main area has a search bar at the top, followed by a 'New Query 1' section with a 'Run' button and a time range of 'Last 24 hours'. Below this, there are tabs for Tables, Queries, Functions, and more. A search bar and filter options are also present. The 'Tables' tab is selected, showing a table titled 'customMetrics'. The table has columns: timestamp (UTC), name, value, valueCount, valueSum, valueMin, valueMax, value... (truncated), and customC... (truncated). The data shows multiple entries for 'vth-cpu-metrics' at different times, with values ranging from 16 to 19. At the bottom, it says '3s 129ms | Display time (UTC+0:00)' and 'Query details | 1 - 7 of 38'.

- 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 144](#) 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 144 : 3NIC-NVM-VMSS Autoscaling using Azure Functions Setup Process Flow



The following topics are covered:

- [Initial Setup](#)
- [Create Autoscale Function](#)
- [Verify Autoscale Function Creation](#)

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"
}

```

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 refer 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
```

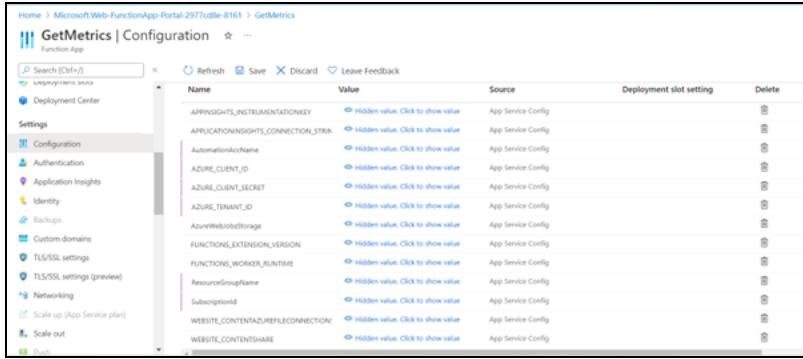
Verify Autoscale Function Creation

To verify autoscale function creation, perform the following steps:

1. From **Home**, navigate thru **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.

[Deploy PowerShell Template 3NIC-NVM-VMSS](#)

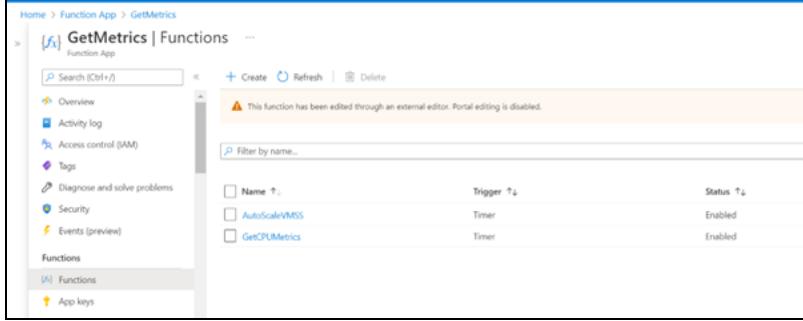
Figure 145 : GetMetrics function - Configuration window



The screenshot shows the 'Configuration' tab for the 'GetMetrics' function. It lists various application settings with their values and sources:

Name	Value	Source	Deployment slot setting	Delete
APPLICATIONINSIGHTS_INSTRUMENTATIONKEY	Hidden value. Click to show value	App Service Config		
APPLICATIONINSIGHTS_CONNECTION_STRING	Hidden value. Click to show value	App Service Config		
AutomationAccountName	Hidden value. Click to show value	App Service Config		
AZURE_CLIENT_ID	Hidden value. Click to show value	App Service Config		
AZURE_CLIENT_SECRET	Hidden value. Click to show value	App Service Config		
AZURE_TENANT_ID	Hidden value. Click to show value	App Service Config		
AzureWebJobsStorage	Hidden value. Click to show value	App Service Config		
FUNCTIONS_EXTENSION_VERSION	Hidden value. Click to show value	App Service Config		
FUNCTIONS_WORKER_RUNTIME	Hidden value. Click to show value	App Service Config		
ResourceGroupName	Hidden value. Click to show value	App Service Config		
SubscriptionId	Hidden value. Click to show value	App Service Config		
WEBSITE_CONTENTAZUREFILECONNECTIONSTRING	Hidden value. Click to show value	App Service Config		
WEBSITE_CONTENTSHARE	Hidden value. Click to show value	App Service Config		

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.

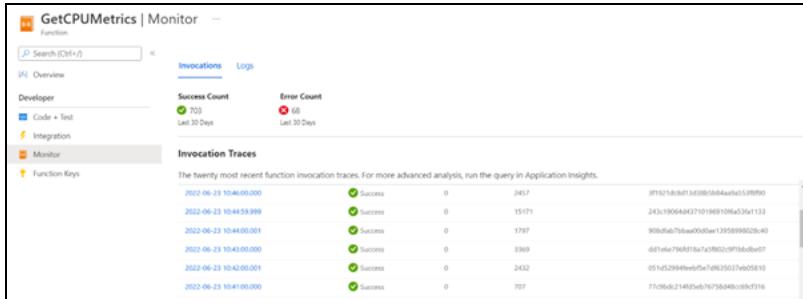


The screenshot shows the 'Functions' tab for the 'GetMetrics' function. It lists two functions:

Name	Trigger	Status
AutoScaleVMSS	Timer	Enabled
GetCPUMetrics	Timer	Enabled

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 146 : GetCPUMetrics function - Monitor window



The screenshot shows the 'Monitor' tab for the 'GetCPUMetrics' function. It displays invocation traces:

Success Count	Error Count
703	68

Invocation Traces:

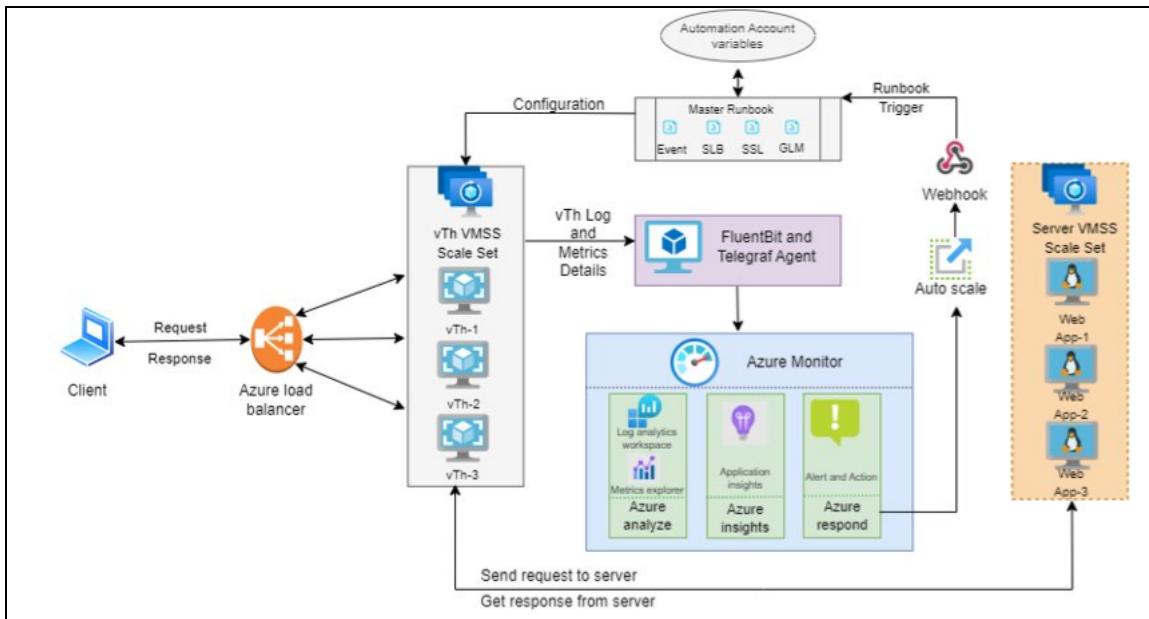
Date	Status	Count	Trace ID
2022-06-23 10:40:00.000	Success	0	3f9521dcb013433809844a65539ff0
2022-06-23 10:44:39.999	Success	0	243c190644371019610fa33fa1123
2022-06-23 10:44:00.001	Success	0	908fbaf7b6e00001e1359998002e40
2022-06-23 10:43:00.000	Success	0	d01ee79f81f61a7a1c980cc0f3bd8e87
2022-06-23 10:42:00.001	Success	0	051fd2894bed5ef7d832927e905810
2022-06-23 10:41:00.000	Success	0	77096d2140f5ebf7c75b348cc0fe9316

9. Verify if the logs generated by functions are created.

Configure Autoscaling and Log Monitoring using Agent Setup

[Figure 147](#) 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 147 : 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

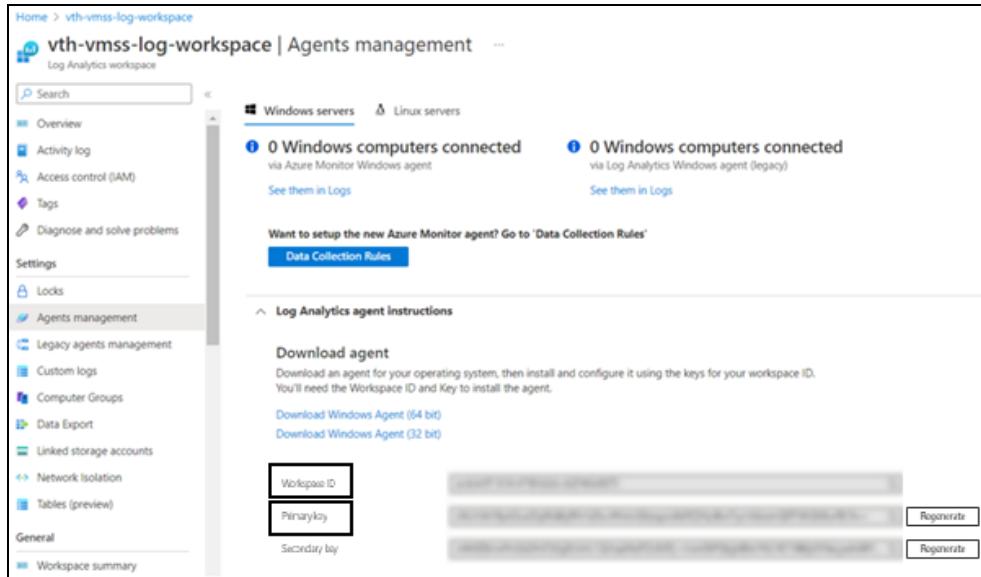
To configure autoscaling and log monitoring using the PowerShell template, perform the following steps:

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 148 : Agents management window

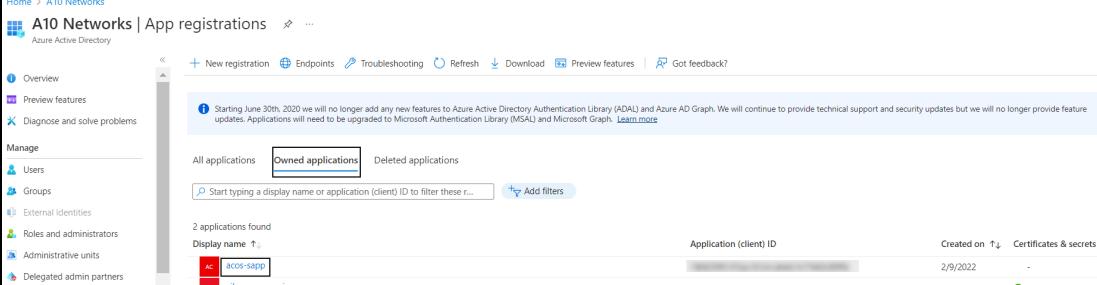


3. Update client ID, tenant ID, and client secret.

```
(cat /etc/environment; echo "AZURE_CLIENT_ID=10724xxx-xxxx-xxxx-xxxx-
xxxxxc14726d"; echo "AZURE_TENANT_ID=91d27xxx-xxxx-xxxx-xxxx-
xxxbf81fc2f"; 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 149 : Azure active directory - App registrations window



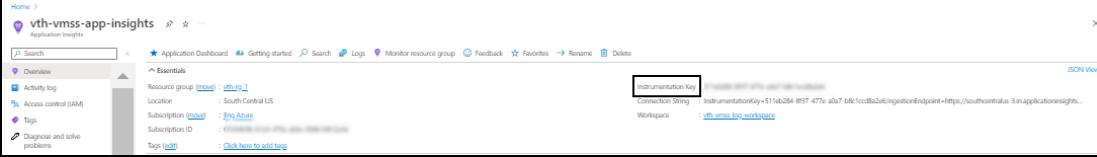
The screenshot shows the 'App registrations' page in the Azure portal. The left sidebar includes 'Overview', 'Preview features', 'Diagnose and solve problems', 'Manage' (with options like 'Users', 'Groups', 'External identities', 'Roles and administrators', 'Administrative units', and 'Delegated admin partners'), and a 'Search' bar. The main area has tabs for 'All applications', 'Owned applications' (which is selected), and 'Deleted applications'. A search bar says 'Start typing a display name or application (client) ID to filter these results...' and a 'Add filters' button. Below, it says '2 applications found'. A table lists the application 'vtho-sapp' with columns for 'Display name', 'Application (client) ID', 'Created on', and 'Certificates & secrets'. The 'Application (client) ID' column shows a long GUID.

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 150 : Selected application insight - Overview window



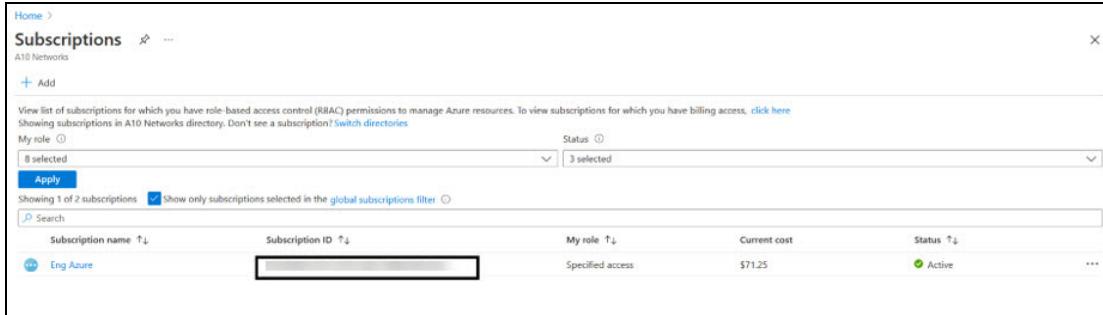
The screenshot shows the 'Overview' page for the application insight 'vth-vmss-app-insights'. The left sidebar has 'Search' and 'Essentials' sections with items like 'Activity log', 'Logs', 'Metrics', and 'Logs'. The main area has tabs for 'Application Dashboard', 'Getting started', 'Search', 'Logs', 'Monitor resource group', 'Feedback', 'Favorites', 'Rename', and 'Delete'. On the right, there's a 'Instrumentation Key' section with the value '37b1aea5-xxxx-xxxx-xxxx-f2c012bccd93'. Below it are 'Connection string' and 'Workspace' details. A 'JSON View' link is also present.

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-xxxx6812a3e",
    "ResourceGroupName": "vth-rg1",
    "VmssName": "vth-vmss"
}
```

You can get the Subscription ID value from **Home > Azure Services > Subscriptions > <subscription_name>**.

Figure 151 : Subscriptions window



The screenshot shows the 'Subscriptions' page in the Azure portal. It displays a single subscription named 'Eng Azure'. The table includes columns for Subscription name, Subscription ID, My role, Current cost, and Status. The status is listed as 'Active'.

Subscription name ↑↓	Subscription ID ↑↓	My role ↑↓	Current cost	Status ↑↓
Eng Azure	[Redacted]	Specified access	\$71.25	Active

- 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:

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

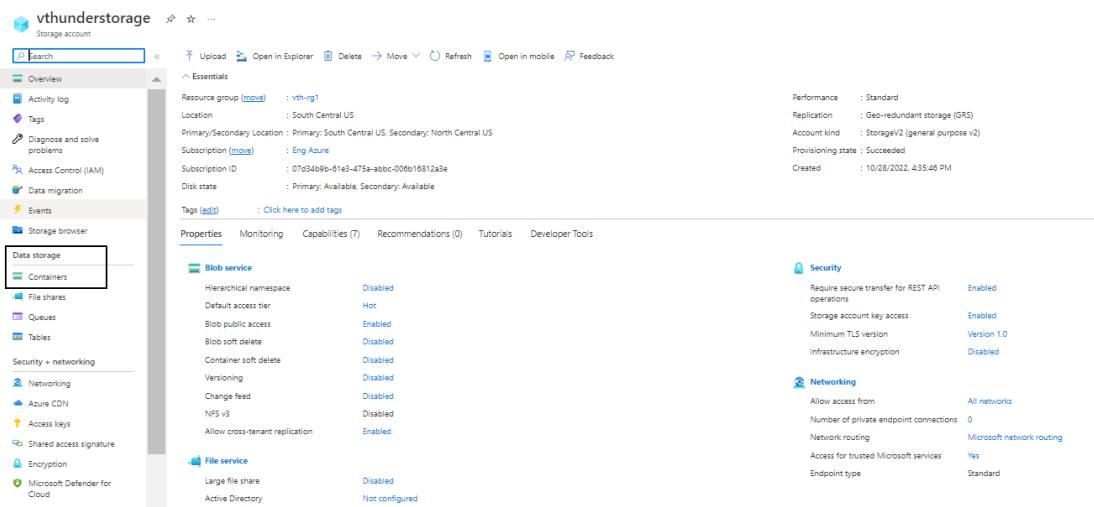
Verify Log Agent file upload

To verify if the log agent file is uploaded, perform the following steps:

- From Home, navigate thru **Azure Services > Storage Accounts > <storage_account_name>**.
The selected storage account - Overview window is displayed.

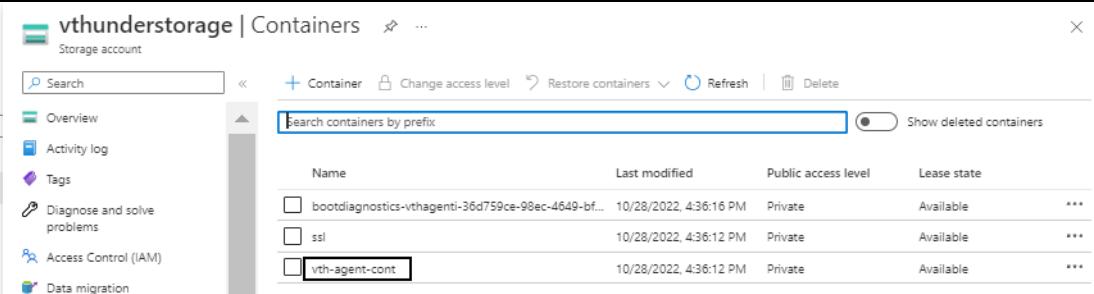
Deploy PowerShell Template 3NIC-NVM-VMSS

Figure 152 : Selected storage account - Overview window



2. Click **Containers** from the left Data Storage panel.

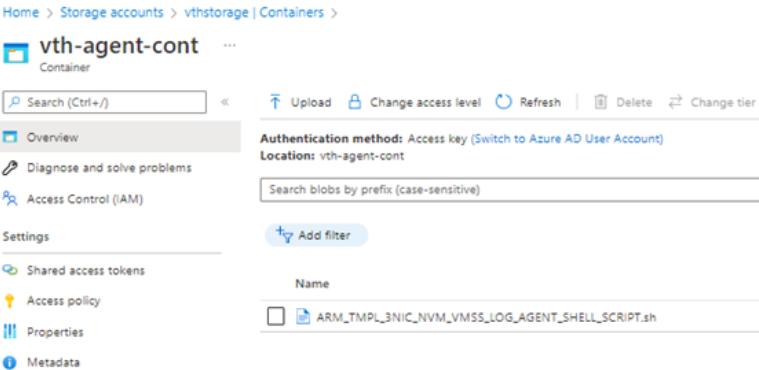
The selected storage account - Containers window is displayed.



3. Select the agent container.

The agent container window is displayed.

Figure 153 : Agent container window



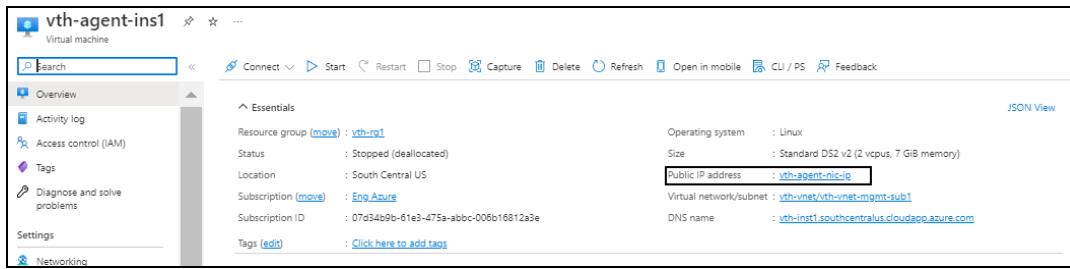
4. Verify if PS_TMPL_3NIC_NVM_VMSS_LOG_AGENT_SHELL_SCRIPT.sh file is uploaded.

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 154 : 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]: 2022-08-25T10:42:16Z
E! [outputs.influxdb] When writing to [http://localhost:8086] : failed
doing req: Post ">
Aug 25 10:42:16 vth-agent-ins1 telegraf[17855]: 2022-08-25T10:42:16Z
E! [agent] Error writing to outputs.influxdb: could not write any
address
Aug 25 10:42:26 vth-agent-ins1 telegraf[17855]: 2022-08-25T10:42:16Z
E! [outputs.influxdb] When writing to [http://localhost:8086] : failed
doing req: Post ">
Aug 25 10:42:26 vth-agent-ins1 telegraf[17855]: 2022-08-25T10:42:16Z
E! [agent] Error writing to outputs.influxdb: could not write any
address
Aug 25 10:42:36 vth-agent-ins1 telegraf[17855]: 2022-08-25T10:42:16Z
E! [outputs.influxdb] When writing to [http://localhost:8086] : failed
doing req: Post ">
Aug 25 10:42:36 vth-agent-ins1 telegraf[17855]: 2022-08-25T10:42:16Z
E! [agent] Error writing to outputs.influxdb: could not write any
address
Aug 25 10:42:46 vth-agent-ins1 telegraf[17855]: 2022-08-25T10:42:16Z
```

```
E! [outputs.influxdb] When writing to [http://localhost:8086] : failed  
doing req: Post ">  
Aug 25 10:42:46 vth-agent-ins1 telegraf[17855]: 2022-08-25T10:42:16Z  
E! [agent] Error writing to outputs.influxdb: could not write any  
address  
Aug 25 10:42:56 vth-agent-ins1 telegraf[17855]: 2022-08-25T10:42:16Z  
E! [outputs.influxdb] When writing to [http://localhost:8086] : failed  
doing req: Post ">  
Aug 25 10:42:56 vth-agent-ins1 telegraf[17855]: 2022-08-25T10:42:16Z  
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.

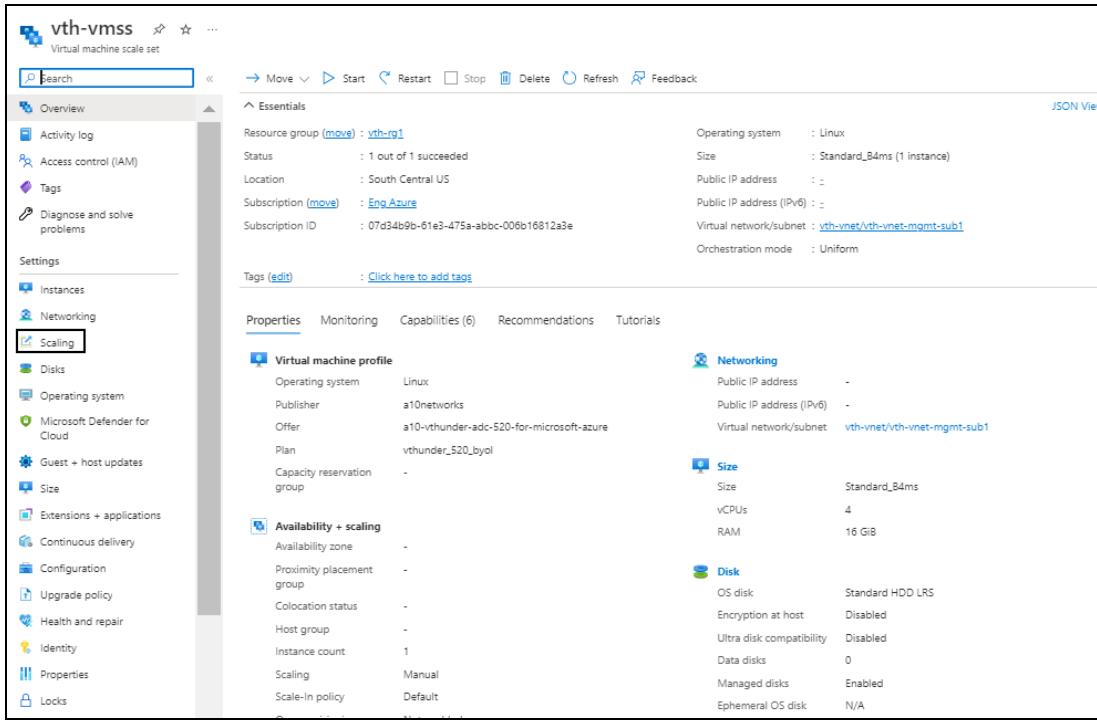
Create Autoscale Rule

To create autoscale rule, perform the following steps:

1. From **Home**, navigate thru **Azure Services > Virtual machine scale set > <vmss_name>**.
The selected vmss - Overview window is displayed.

[Deploy PowerShell Template 3NIC-NVM-VMSS](#)

Figure 155 : Selected VMSS - Overview window



vth-vmss Virtual machine scale set

Overview

Activity log Access control (IAM) Tags Diagnose and solve problems

Instances Networking **Scaling** Disks Operating system Microsoft Defender for Cloud Guest + host updates Size Extensions + applications Continuous delivery Configuration Upgrade policy Health and repair Identity Properties Locks

Resource group ([move](#)) : [vth-rg1](#) Status : 1 out of 1 succeeded Location : South Central US Subscription ([move](#)) : [Eng_Azure](#) Subscription ID : 07a34b9b-61e3-475a-abbc-006b16812a3e Tags ([edit](#)) : [Click here to add tags](#)

Operating system : Linux Size : Standard_B4ms (1 instance) Public IP address : - Public IP address (IPv6) : - Virtual network/subnet : [vth-vnet/vth-vnet-mgmt-sub1](#) Orchestration mode : Uniform

Tags ([edit](#)) : [Click here to add tags](#)

Properties Monitoring Capabilities (6) Recommendations Tutorials

Virtual machine profile

Operating system	Linux
Publisher	a10networks
Offer	a10-vthunder-adc-520-for-microsoft-azure
Plan	vthunder_520_byol
Capacity reservation group	-

Availability + scaling

Availability zone	-
Proximity placement group	-
Colocation status	-
Host group	-
Instance count	1
Scaling	Manual
Scale-In policy	Default

Networking

Public IP address	-
Public IP address (IPv6)	-
Virtual network/subnet	vth-vnet/vth-vnet-mgmt-sub1

Size

Size	Standard_B4ms
vCPUs	4
RAM	16 GiB

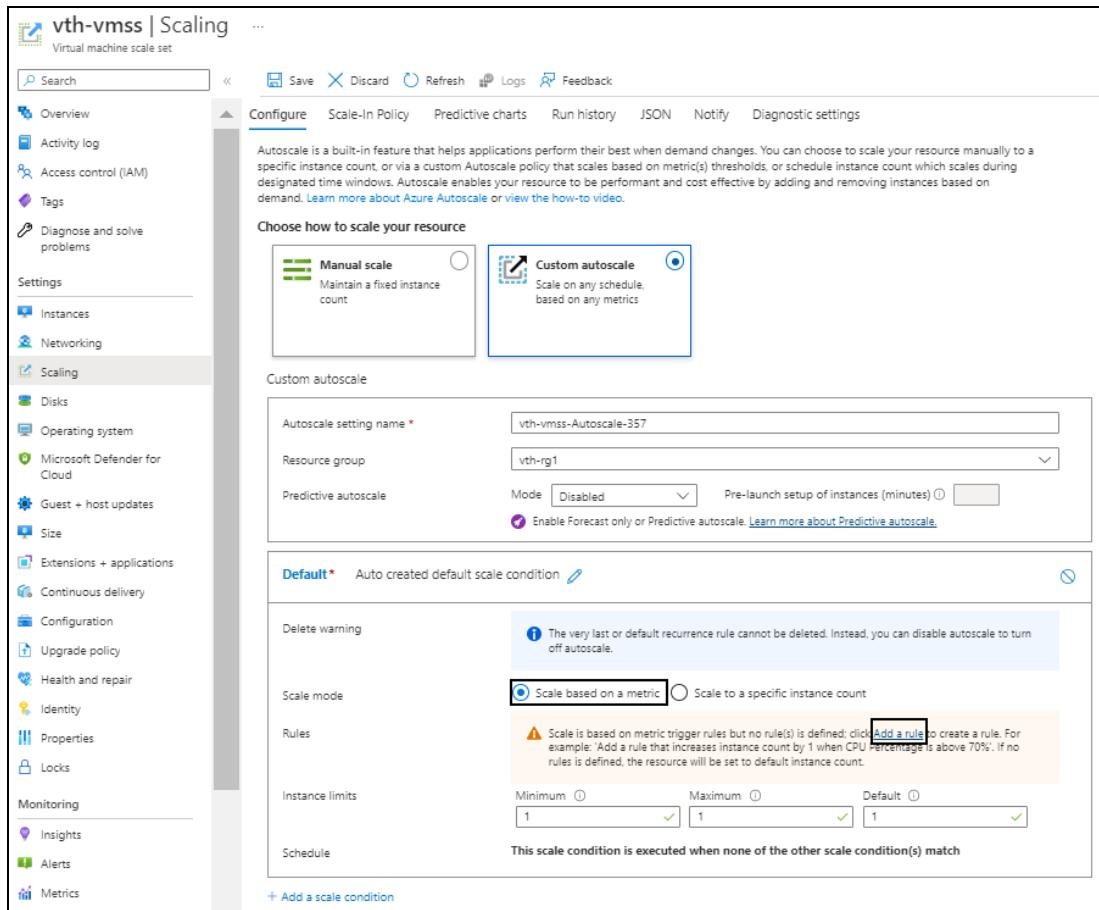
Disk

OS disk	Standard HDD LRS
Encryption at host	Disabled
Ultra disk compatibility	Disabled
Data disks	0
Managed disks	Enabled
Ephemeral OS disk	N/A

- Click **Scaling** from the left **Settings** panel.
- The selected vmss - Scaling window is displayed.

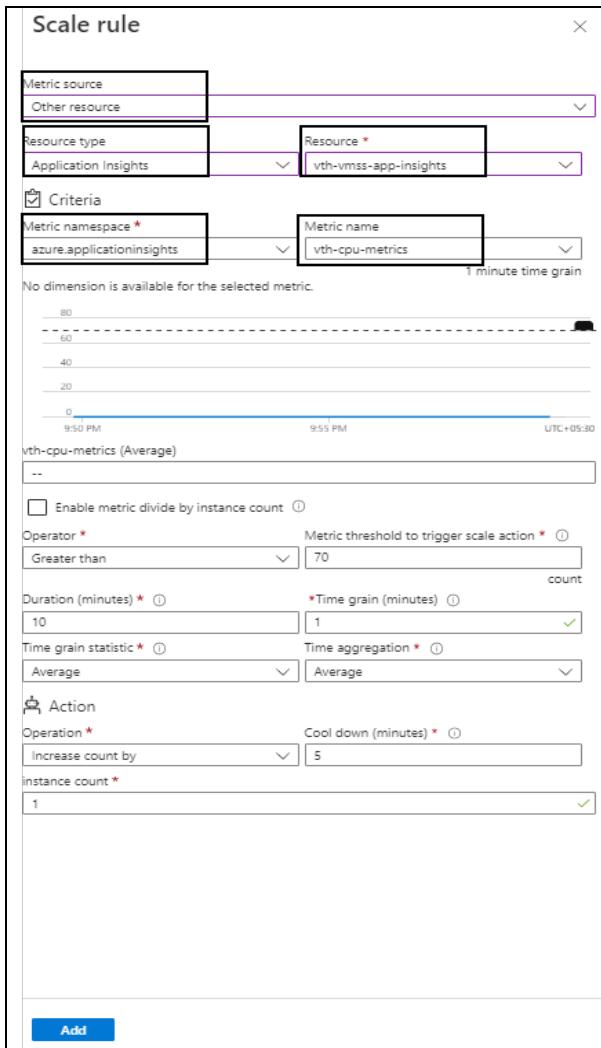
[Deploy PowerShell Template 3NIC-NVM-VMSS](#)

Figure 156 : 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 157 : Scale rule window



6. Select or enter the information in the following fields:

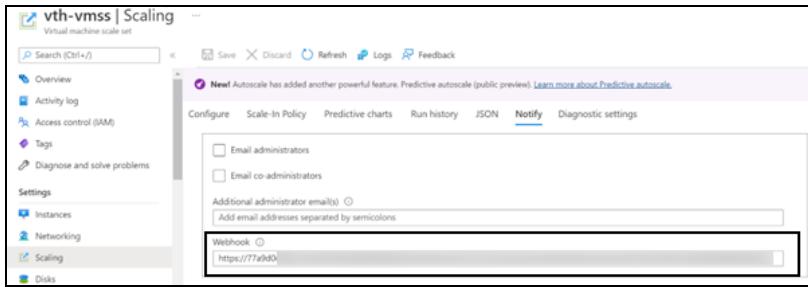
- Metric source: Other resource
- Resource type: Application Insights
- Resource
- Time aggregation
- Metric namespace
- Metric name

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 158 : Selected VMSS - Scaling window - Notify tab



Create Autoscale Alert

1. From **Home**, navigate thru **Azure Services > Virtual machine scale set > <vmss_name>**.
The selected vmss - Overview window is displayed.

[Deploy PowerShell Template 3NIC-NVM-VMSS](#)

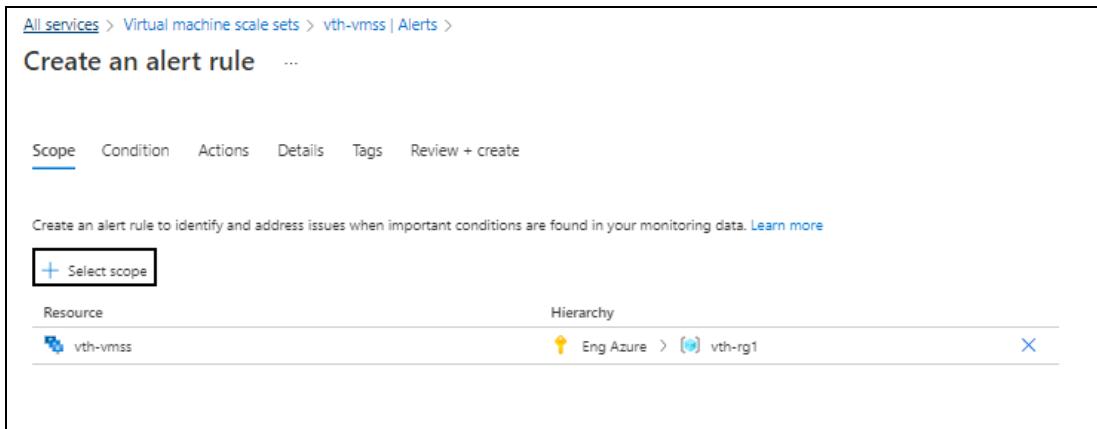
Figure 159 : Selected VMSS - Overview window

- Click **Alerts** from the left **Monitoring** panel.
- The selected vmss - Alerts window is displayed.

Figure 160 : Selected VMSS - Alerts window

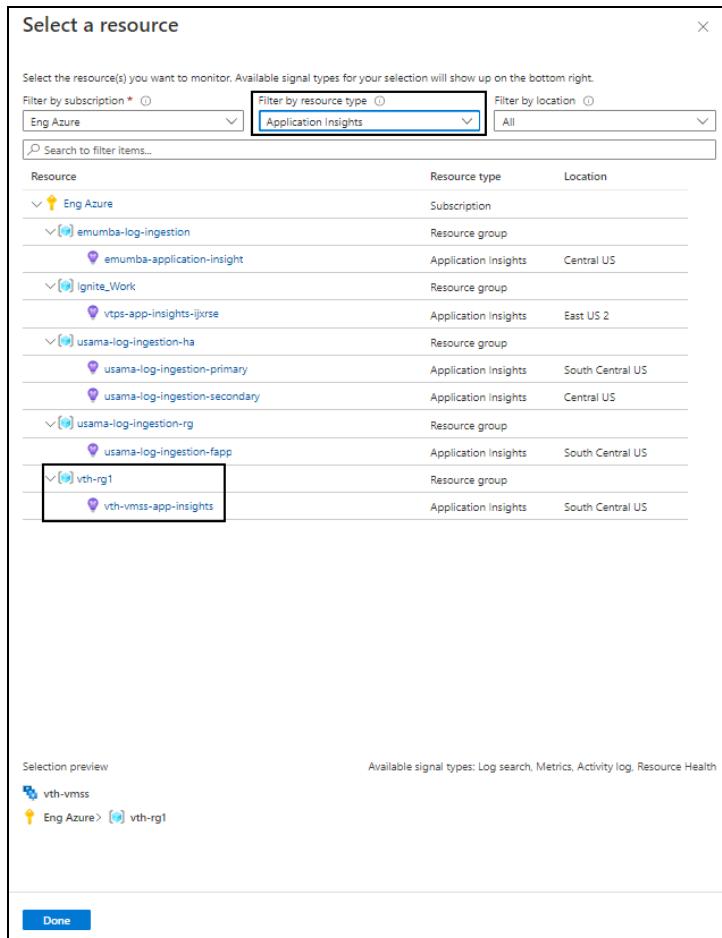
- Click **Create > Alert rule**.
- The Create an alert rule - Scope window is displayed.

Figure 161 : Create an alert rule window - Scope tab



4. Click **Select scope** in the **Scope** tab.
The **Select a resource** window is displayed.

Figure 162 : Select a resource window



5. From Filter by resource type, select Application Insights.

The resource group having application insight resources are displayed.

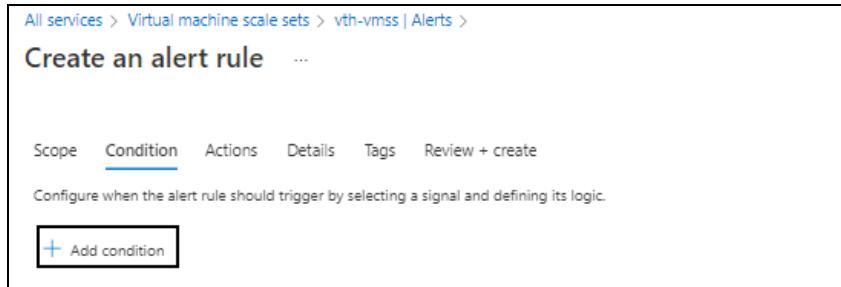
6. Select the required application insight resource and click Done.

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.

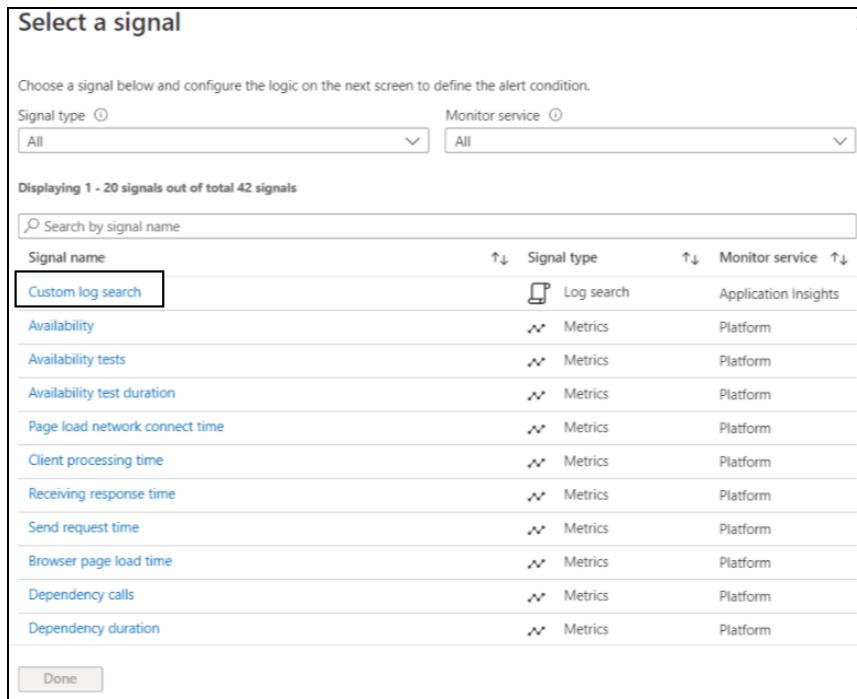
Figure 163 : Create an alert rule window - Condition tab



8. Click **Add condition** in the **Condition** tab.

The **Select a signal** window is displayed.

Figure 164 : Select a signal window



9. Select **Custom log search** as the signal.

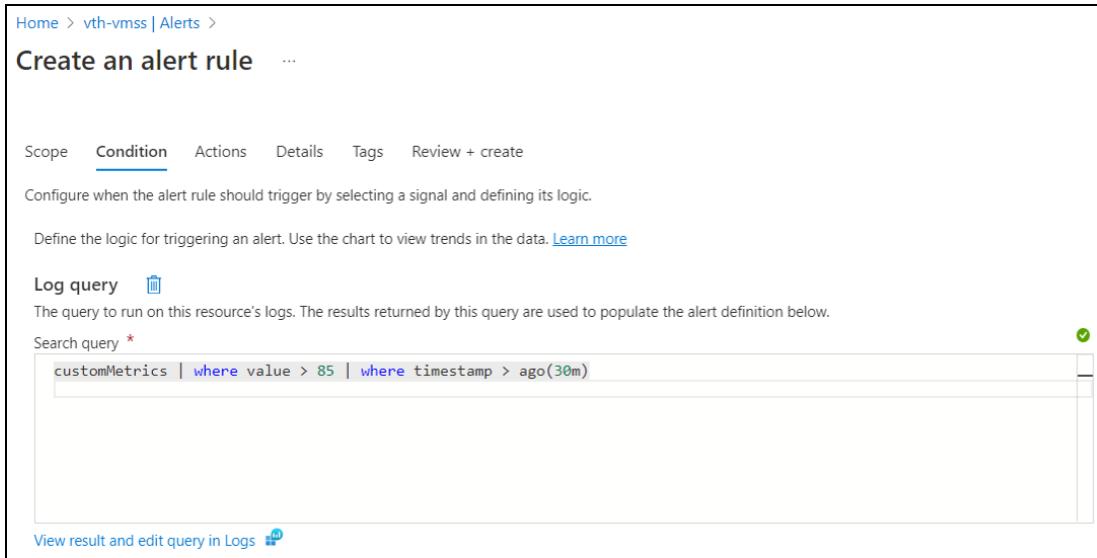
The window to define the signal's logic is displayed in the alert rule condition.

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.

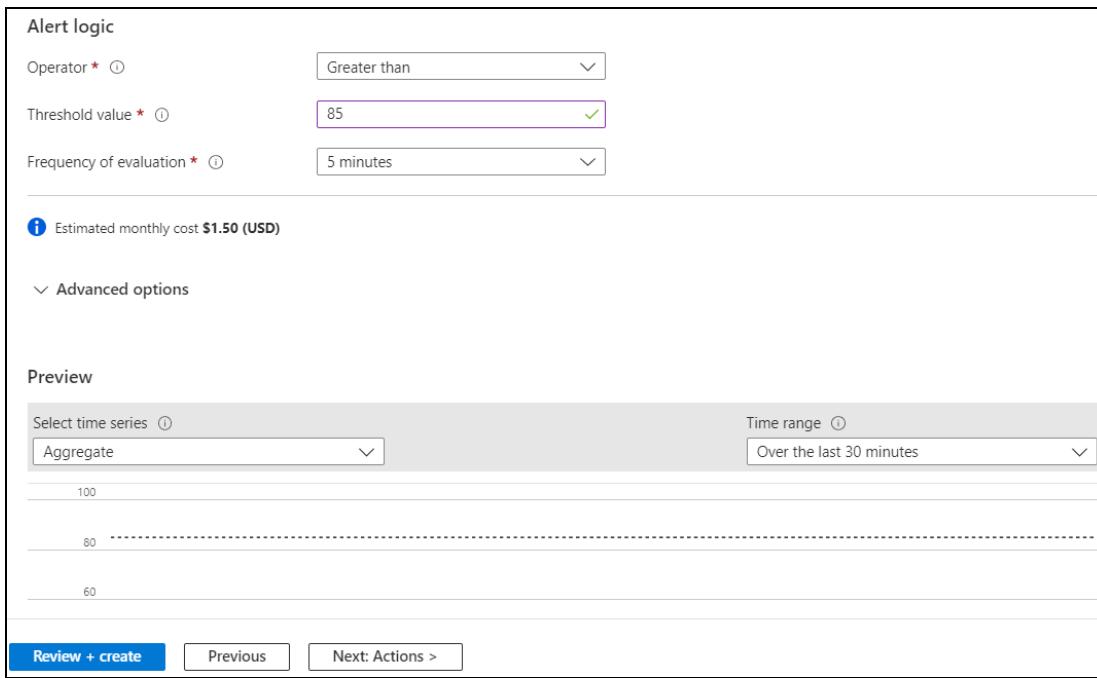
Figure 165 : Create an alert rule window - Condition tab



The screenshot shows the 'Create an alert rule' window with the 'Condition' tab selected. At the top, there are tabs for Scope, Condition, Actions, Details, Tags, and Review + create. Below the tabs, a note says: 'Configure when the alert rule should trigger by selecting a signal and defining its logic.' A link 'Learn more' is provided. Under 'Log query', it says: 'The query to run on this resource's logs. The results returned by this query are used to populate the alert definition below.' A search bar contains the query: 'customMetrics | where value > 85 | where timestamp > ago(30m)'. A green checkmark is next to the search bar. At the bottom, a link 'View result and edit query in Logs' is shown.

11. Configure alert logic in the Alert logic section.

Figure 166 : Alert logic section

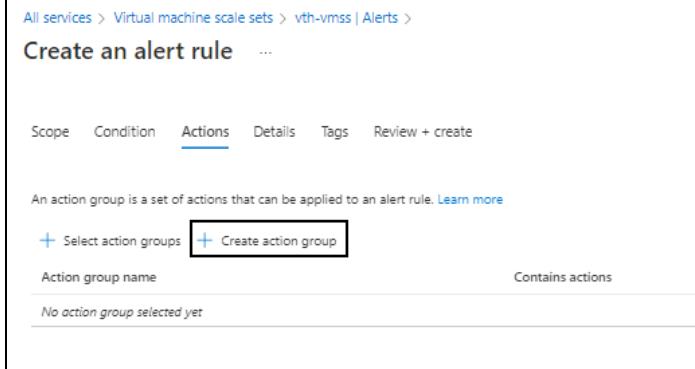


The screenshot shows the 'Alert logic' configuration section. It includes fields for Operator (set to 'Greater than'), Threshold value (set to '85'), and Frequency of evaluation (set to '5 minutes'). A note below states: 'Estimated monthly cost \$1.50 (USD)'. The 'Preview' section displays a line chart showing data over the last 30 minutes, with values ranging from 60 to 100. Navigation buttons at the bottom include 'Review + create', 'Previous', and 'Next: Actions >'.

Depending upon the signal logic configuration, the monthly cost for the alert is displayed.

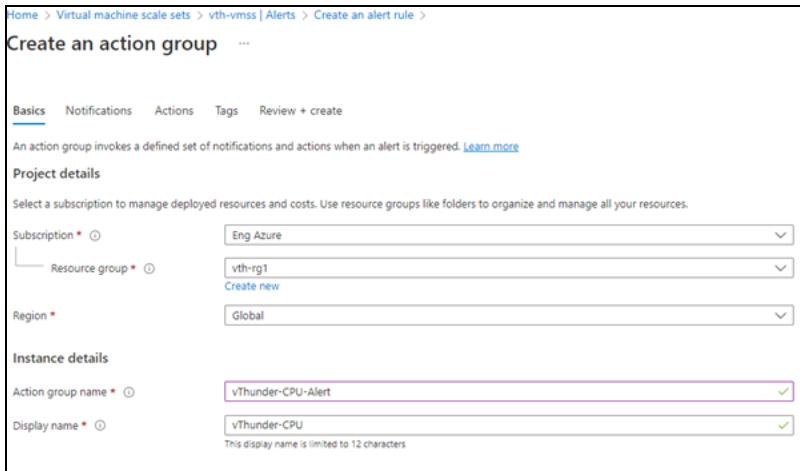
12. Click **Next : Actions** at the bottom of the window.
 The **Create an alert rule - Actions** window is displayed.

Figure 167 : Create an alert rule window - Actions tab



13. Click **Create action group**.
 The **Create an action group - Basics** window is displayed.

Figure 168 : Create an action group window - Basics tab



- a. Select or enter the following mandatory information in the **Basics** tab:

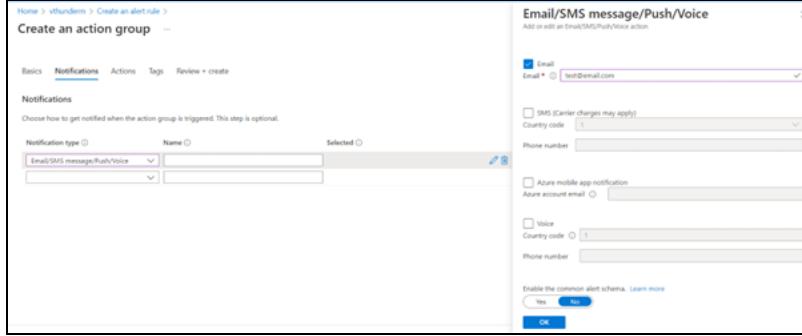
Project details

- Subscription
- Resource group
- Region

Instance details

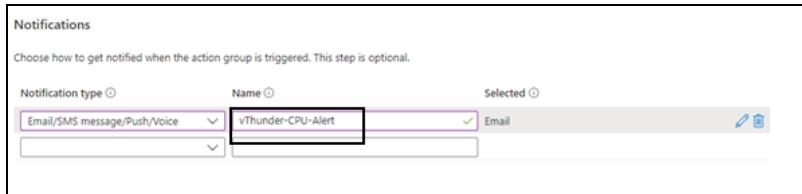
- Action group name
 - Display name
- b. Click **Next : Notifications** at the bottom of the window.
The **Create an action group - Notifications** window is displayed.
- c. Select the **Notification type**.
The corresponding window to configure the notification type is displayed.

Figure 169 : Create an action group window - Notifications tab - Type



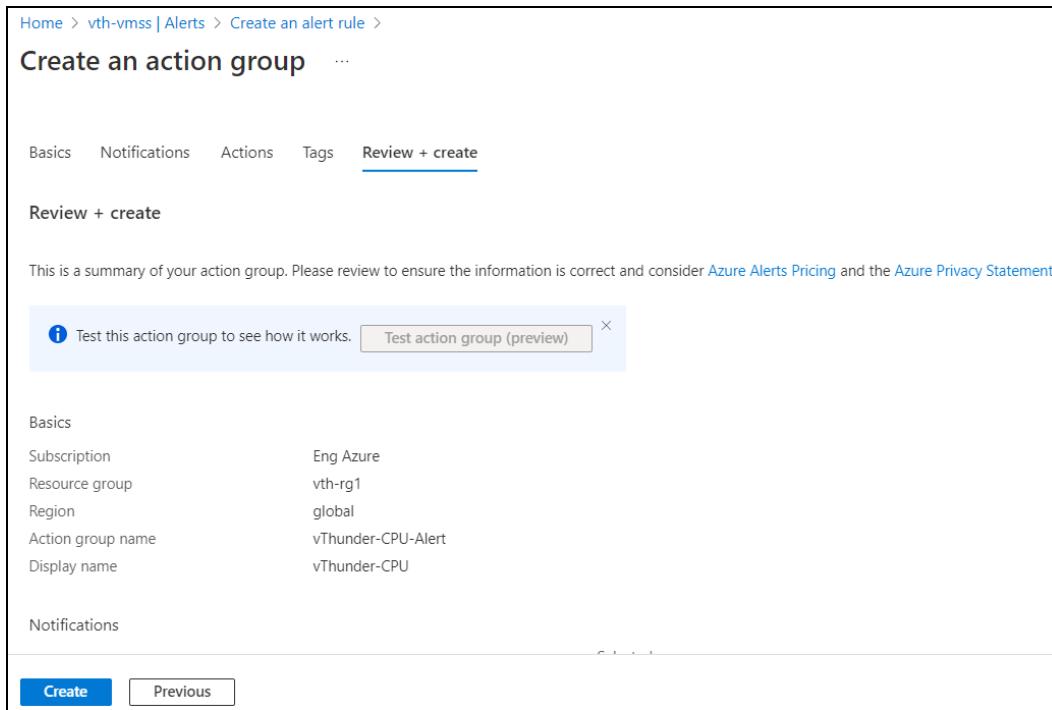
- d. Select the **Email** option and provide the correct email ID in the **Email** field and then click **OK**.
- e. Enter a unique name for the notification in the **Name** field.

Figure 170 : 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.

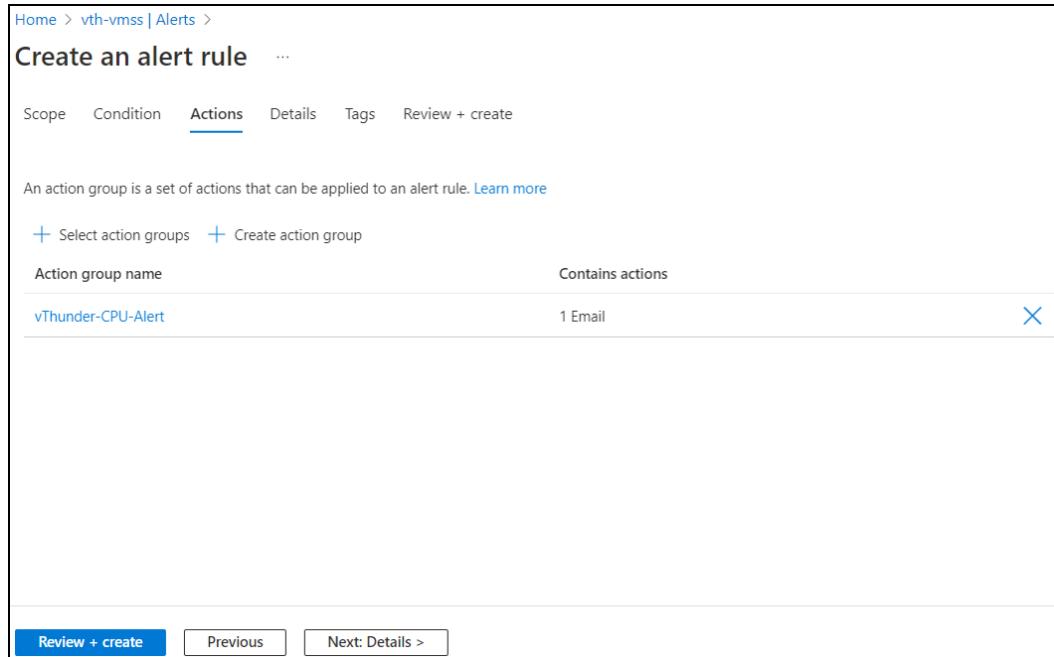
Figure 171 : Create an action group window - Review + create tab



g. Click **Create**.

The action group is listed under **Actions** tab.

Figure 172 : Create an alert rule window - Actions tab

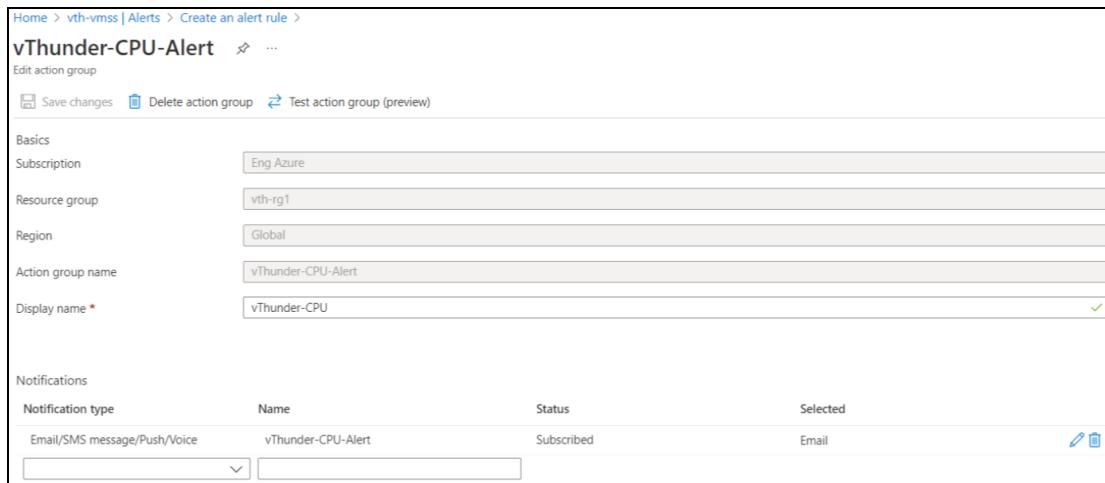


The screenshot shows the 'Create an alert rule' window with the 'Actions' tab selected. At the top, there are tabs for Scope, Condition, Actions (which is underlined), Details, Tags, and Review + create. Below the tabs, a note says 'An action group is a set of actions that can be applied to an alert rule.' with a 'Learn more' link. There are two buttons: '+ Select action groups' and '+ Create action group'. A table lists an action group named 'vThunder-CPU-Alert' under 'Contains actions', which is described as '1 Email'. At the bottom, there are buttons for 'Review + create', 'Previous', and 'Next: Details >'.

14. Select the recently created action group.

The selected action group is displayed.

Figure 173 : Selected action group

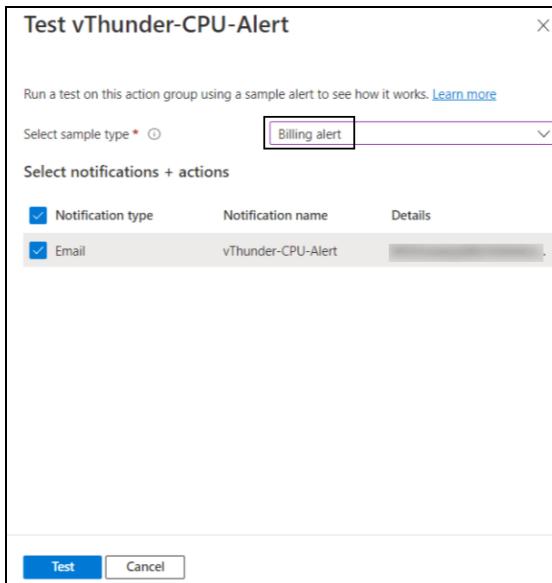


The screenshot shows the 'Edit action group' window for 'vThunder-CPU-Alert'. It has sections for Basics (Subscription: Eng Azure, Resource group: vth-rg1, Region: Global, Action group name: vThunder-CPU-Alert, Display name: vThunder-CPU) and Notifications (Email/SMS message/Push/Voice: vThunder-CPU-Alert, Status: Subscribed, Selected: Email). Buttons at the top include Save changes, Delete action group, and Test action group (preview).

15. Click **Test action group (preview)**.

The Test <action_group_name>-alert window is displayed.

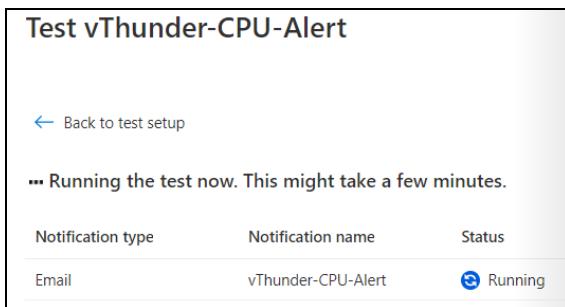
Figure 174 : Test <action_group_name>-alert window



16. Select **Billing alert** as the Sample type and click **Test**.

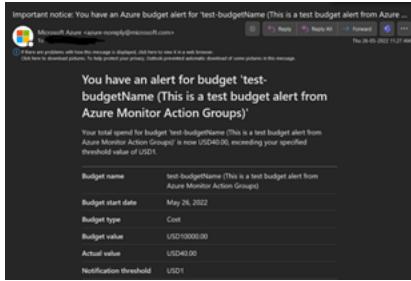
The running status for the test rule is displayed.

Figure 175 : Test <action_group_name>-alert window - Running status



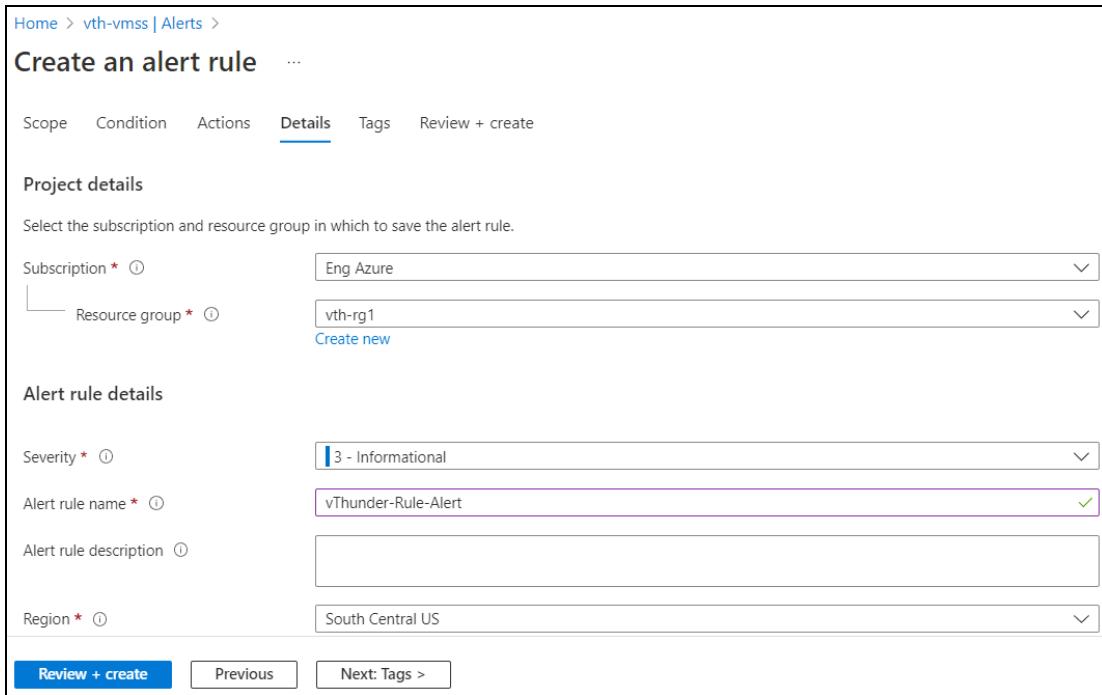
When the success status is displayed, an email notification is triggered to the email ID provided in the [Email Notification](#) step.

Figure 176 : 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 177 : Create an alert rule window - Details tab

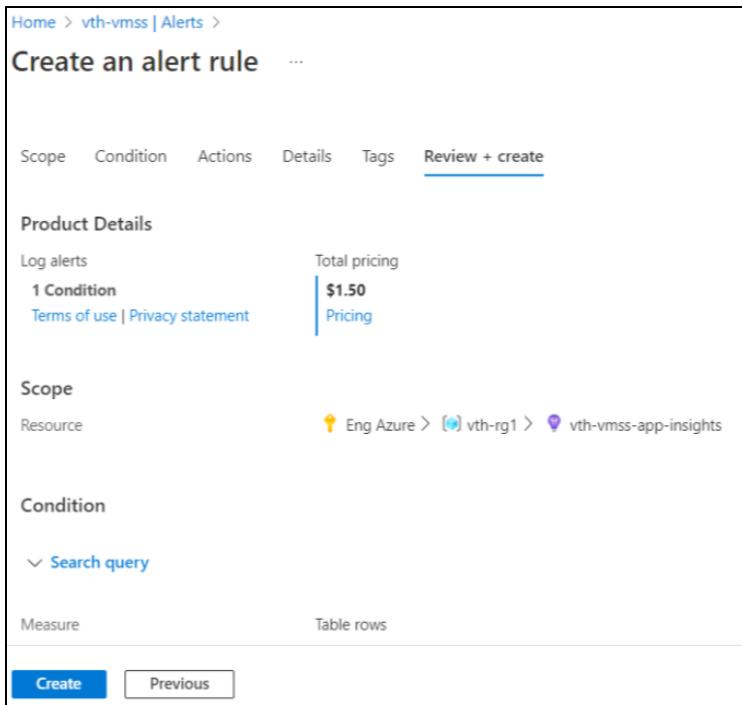


The screenshot shows the 'Create an alert rule - Details' window in the Azure portal. The 'Details' tab is selected. The window is divided into several sections:

- Project details:** Selects the subscription ('Eng Azure') and resource group ('vth-rg1').
- Alert rule details:** Sets the severity to '3 - Informational', names the alert rule as 'vThunder-Rule-Alert', and provides a description. The region is set to 'South Central US'.
- Buttons at the bottom:** 'Review + create' (highlighted in blue), 'Previous', and 'Next: Tags >'.

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.

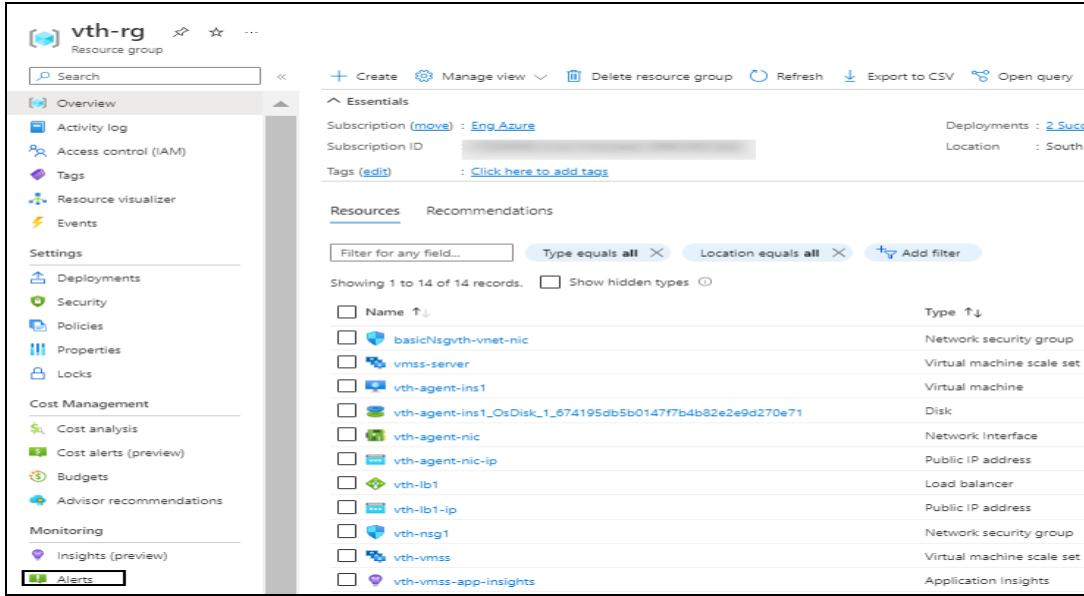
Figure 178 : Create an alert rule window - Review + create tab



22. Click **Create**.
The alert rule is created.
23. From **Home**, navigate thru **Azure Services > Resource groups > <resource_group_name>**.
The selected resource group - Overview window is displayed.

Deploy PowerShell Template 3NIC-NVM-VMSS

Figure 179 : Selected resource group - Overview window



Name	Type
basicNsgvth-vnet-nic	Network security group
vmss-server	Virtual machine scale set
vth-agent-inst1	Virtual machine
vth-agent-inst1_OsDisk_1_674195db5b0147f7b4b82e2e9d270e71	Disk
vth-agent-nic	Network interface
vth-agent-nic-ip	Public IP address
vth-lb1	Load balancer
vth-lb1-ip	Public IP address
vth-nsg1	Network security group
vth-vmss	Virtual machine scale set
vth-vmss-app-insights	Application Insights

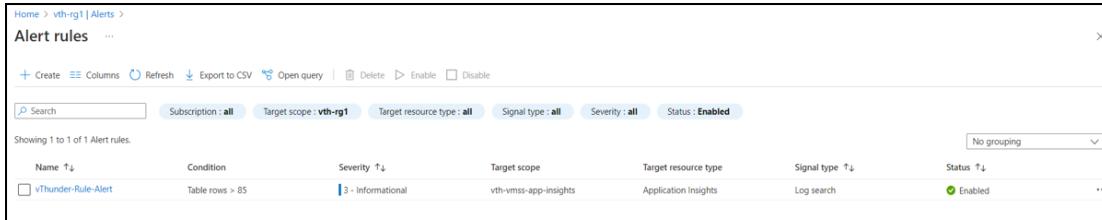
24. Click **Alerts** from the left **Monitoring** panel.

The selected alert window is displayed.

25. Click **Alert rules**.

The alert rules for the selected resource group is displayed.

Figure 180 : Selected resource group - Alert rules window



Name	Condition	Severity	Target scope	Target resource type	Signal type	Status
vThunder-Rule-Alert	Table rows > 85	Informational	vth-vmss-app-insights	Application Insights	Log search	Enabled

Verify Logs in Log Analytics Workspace

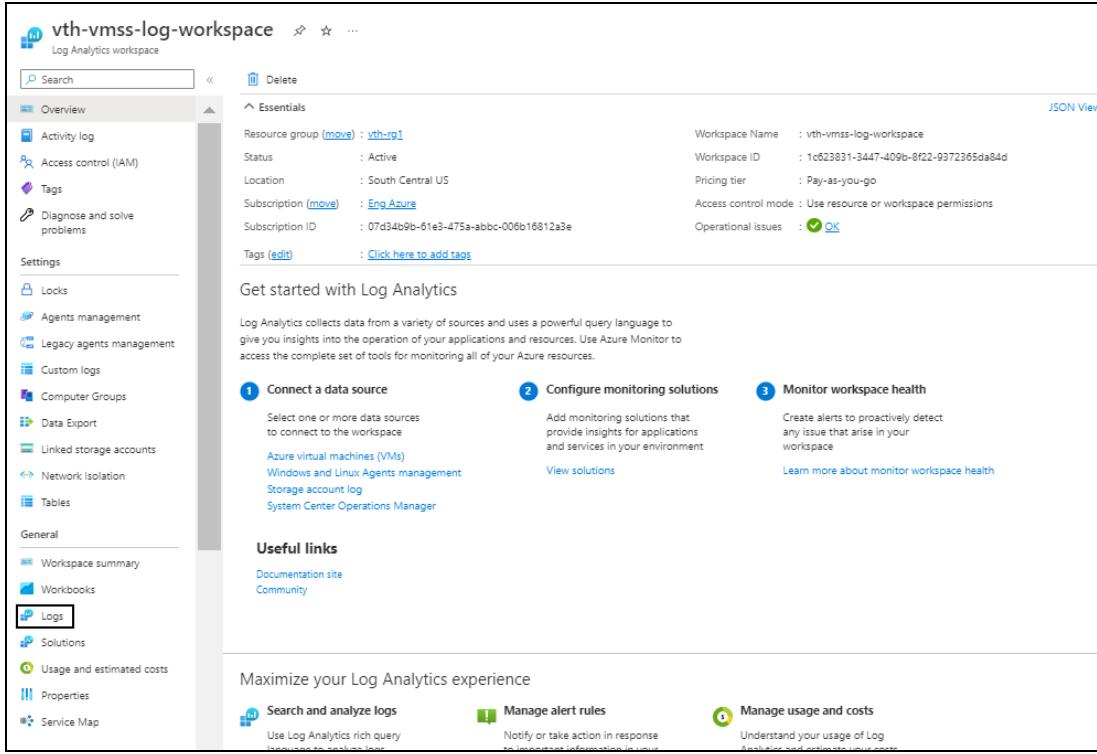
To verify the logs in log analytics workspace, perform the following steps:

a. From **Home**, navigate thru **Azure Services > Log Analytics workspaces > <log_workspace_name>**.

The selected log workspace - Overview window is displayed.

Deploy PowerShell Template 3NIC-NVM-VMSS

Figure 181 : Selected log workspace - Overview window



Essentials

- Resource group ([move](#)) : [vth-rg1](#)
- Status : Active
- Location : South Central US
- Subscription ([move](#)) : [Eng_Azure](#)
- Subscription ID : 07a34b9b-61e3-475a-abbc-006b16812a3e
- Tags ([edit](#)) : [Click here to add tags](#)

Workspace Name : vth-vmss-log-workspace
Workspace ID : 1c623831-3447-409b-8f22-9372365da84d
Pricing tier : Pay-as-you-go
Access control mode : Use resource or workspace permissions
Operational issues : [OK](#)

Get started with Log Analytics

Log Analytics collects data from a variety of sources and uses a powerful query language to give you insights into the operation of your applications and resources. Use Azure Monitor to access the complete set of tools for monitoring all of your Azure resources.

1 Connect a data source
Select one or more data sources to connect to the workspace

- Azure virtual machines (VMs)
- Windows and Linux Agents management
- Storage account log
- System Center Operations Manager

2 Configure monitoring solutions
Add monitoring solutions that provide insights for applications and services in your environment

3 Monitor workspace health
Create alerts to proactively detect any issue that arise in your workspace

[View solutions](#) [Learn more about monitor workspace health](#)

Useful links

- [Documentation site](#)
- [Community](#)

Maximize your Log Analytics experience

Search and analyze logs
Use Log Analytics rich query [Learn more about rich query](#)

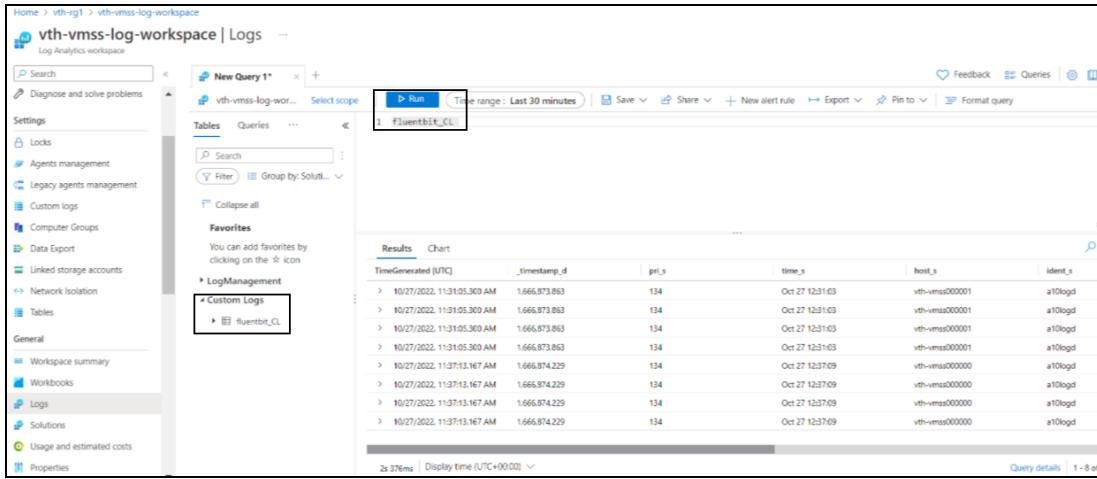
Manage alert rules
Notify or take action in response to important information in your logs [Learn more about alert rules](#)

Manage usage and costs
Understand your usage of Log Analytics and optimize your costs [Learn more about usage and costs](#)

b. Click **Logs** from the left **General** panel.

The selected log window is displayed.

Figure 182 : Selected log analytics workspace - Logs window



TimeGenerated (UTC)	_timestamp_d	pri_s	time_s	host_s	ident_s
> 10/27/2022, 11:31:05.300 AM	1666873863	134	Oct 27 12:31:03	vth-vmss000001	a10logd
> 10/27/2022, 11:31:05.300 AM	1666873863	134	Oct 27 12:31:03	vth-vmss000001	a10logd
> 10/27/2022, 11:31:05.300 AM	1666873863	134	Oct 27 12:31:03	vth-vmss000001	a10logd
> 10/27/2022, 11:31:05.300 AM	1666873863	134	Oct 27 12:31:03	vth-vmss000001	a10logd
> 10/27/2022, 11:37:13.167 AM	1666874229	134	Oct 27 12:37:09	vth-vmss000000	a10logd
> 10/27/2022, 11:37:13.167 AM	1666874229	134	Oct 27 12:37:09	vth-vmss000000	a10logd
> 10/27/2022, 11:37:13.167 AM	1666874229	134	Oct 27 12:37:09	vth-vmss000000	a10logd

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 thru **Azure Services > Application Insights > <application_insight_name>**.

The selected application insight - Overview window is displayed.

- b. Click **Logs** from the left **Monitoring** panel.

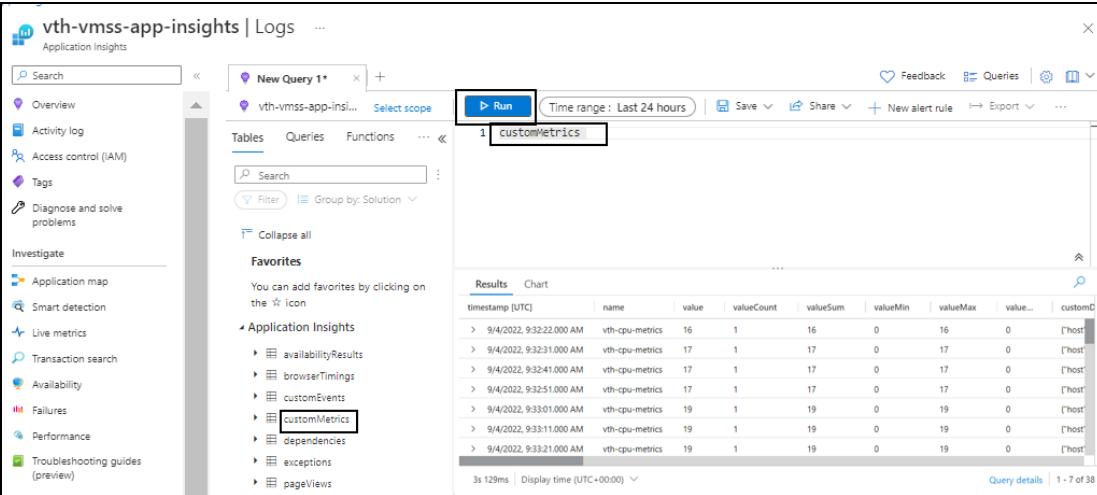
The selected log query window is displayed.

- c. Expand **Application Insights** in the left **Tables** tab panel.

- d. Double-click **customMetrics**.

The customMetrics query window is displayed.

Figure 183 : Selected application insight - Logs window



The screenshot shows the Azure Application Insights Logs interface. On the left, the navigation pane includes sections like Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. Under Investigate, there are links for Application map, Smart detection, Live metrics, Transaction search, Availability, Failures, Performance, and Troubleshooting guides (preview). The main area shows a query editor with a search bar, a scope dropdown set to 'vth-vmss-app-insights', and a 'Run' button. Below the search bar are tabs for Tables, Queries, Functions, and more. A search bar and filter options are also present. The 'Tables' tab is selected, showing a table named 'customMetrics'. The table has columns: timestamp (UTC), name, value, valueCount, valueSum, valueMin, valueMax, value... (partial), and customC... (partial). The data shows multiple entries for 'vth-cpu-metrics' at different times, with values ranging from 16 to 19. At the bottom, it says '3s 129ms | Display time (UTC+0:00)' and 'Query details | 1 - 7 of 38'.

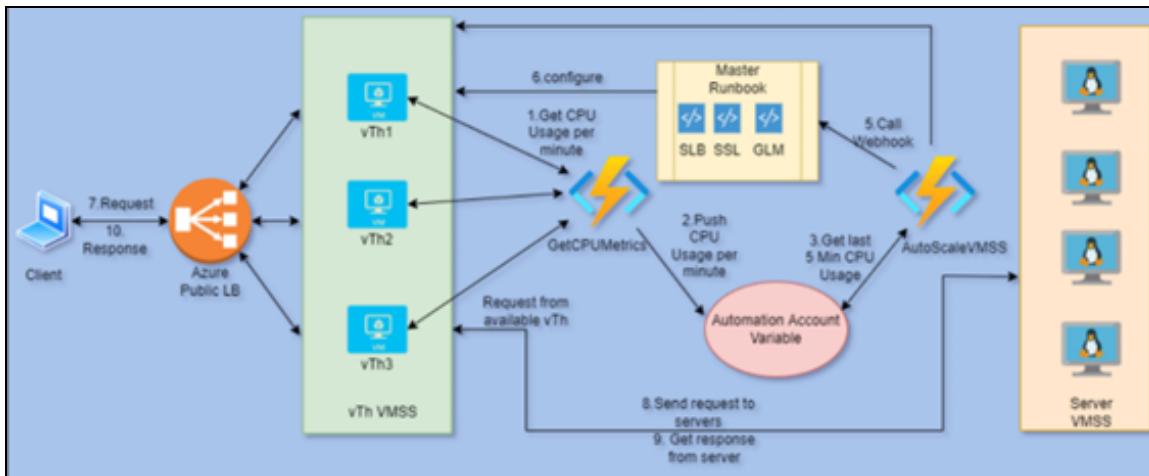
- e. Click **Run**.

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 184](#) 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 184 : 3NIC-NVM-VMSS Autoscaling using Azure Functions Setup Process Flow



The following topics are covered:

- [Initial Setup](#)
- [Create Autoscale Function](#)
- [Verify Autoscale Function Creation](#)

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"
}

```

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 refer 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
```

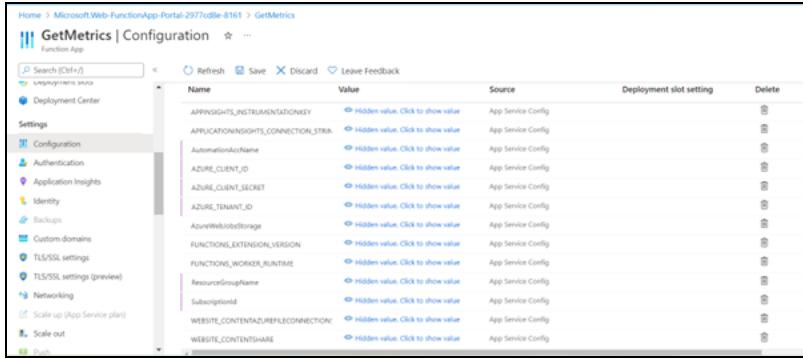
Verify Autoscale Function Creation

To verify autoscale function creation, perform the following steps:

1. From **Home**, navigate thru **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.

[Deploy PowerShell Template 3NIC-NVM-VMSS](#)

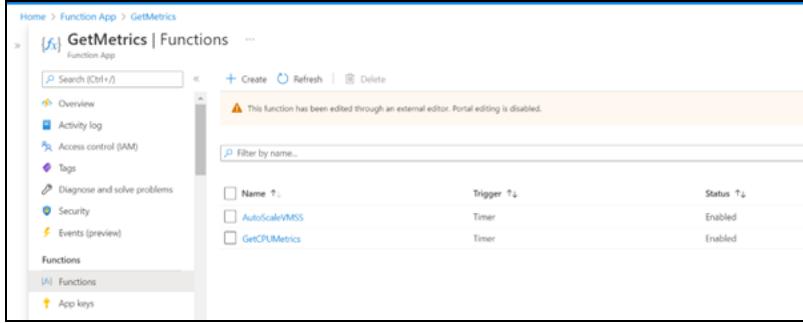
Figure 185 : GetMetrics function - Configuration window



The screenshot shows the 'Configuration' tab for the 'GetMetrics' function. The left sidebar lists various settings like Deployment Center, Configuration, Authentication, Application Insights, Identity, Backups, Custom domains, TLS/SSL settings, Networking, Scale up (App Service plan), Scale out, and Path. The main pane displays a table of application settings:

Name	Value	Source	Deployment slot setting	Delete
APPLICATIONINSIGHTS_INSTRUMENTATIONKEY	Hidden value. Click to show value	App Service Config		
APPLICATIONINSIGHTS_CONNECTION_STRING	Hidden value. Click to show value	App Service Config		
AUTOMATIONACCOUNTNAME	Hidden value. Click to show value	App Service Config		
AZURE_CLIENT_ID	Hidden value. Click to show value	App Service Config		
AZURE_CLIENT_SECRET	Hidden value. Click to show value	App Service Config		
AZURE_TENANT_ID	Hidden value. Click to show value	App Service Config		
AzureWebJobsStorage	Hidden value. Click to show value	App Service Config		
FUNCTIONS_EXTENSION_VERSION	Hidden value. Click to show value	App Service Config		
FUNCTIONS_WORKER_RUNTIME	Hidden value. Click to show value	App Service Config		
ResourceGroupName	Hidden value. Click to show value	App Service Config		
SubscriptionId	Hidden value. Click to show value	App Service Config		
WEBSITE_CONTENTAZUREFILECONNECTION	Hidden value. Click to show value	App Service Config		
WEBSITE_CONTENTSHARE	Hidden value. Click to show value	App Service Config		

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.



The screenshot shows the 'Functions' tab for the 'GetMetrics' function. The left sidebar lists Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Security, Events (preview), Functions, Functions, and App keys. The main pane displays a table of functions:

Name	Trigger	Status
AutoScaleVMSS	Timer	Enabled
GetCPUMetrics	Timer	Enabled

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 186 : GetCPUMetrics function - Monitor window



The screenshot shows the 'Monitor' tab for the 'GetCPUMetrics' function. The left sidebar lists Overview, Developer (Code + Test, Integration, Monitor), and Function Keys. The main pane displays the 'Invocation Traces' section, which shows the twenty most recent function invocation traces. The table includes columns for Success Count, Error Count, and Trace ID.

Success Count	Error Count	Trace ID
703	68	3f1521dcb013438819844a65539f90
2022-06-23 10:44:59.999	Success	243c19064443710196010fa33fa1123
2022-06-23 10:44:00.001	Success	90d0fb170e00001e1359998002e40
2022-06-23 10:43:00.000	Success	d01ee79ff1f1a7a1c980cc0f3bdbe8e7
2022-06-23 10:42:00.001	Success	051d52994bed5ef7d832927e905810
2022-06-23 10:41:00.000	Success	77096d2140f5ebf7c75b348cc0fe9316

9. Verify if the logs generated by functions are created.

Access vThunder using CLI or GUI

vThunder can be accessed using any of the following ways:

- [Access vThunder using CLI](#)
- [Access vThunder using GUI](#)

NOTE: For A10 vThunder default login credentials, send a request to [A10 Networks Support](#).

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 under the VMSS
Here, Public IP of **vth-vmss**
 - Connection Type: SSH
3. Click **Open**.
4. In the active PuTTY session, login with the default login credentials provided by A10 Networks Support and change the default password as soon as you login for the first time:

```

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-->
vThunder(config)#admin <admin_username> password <new_password>
```

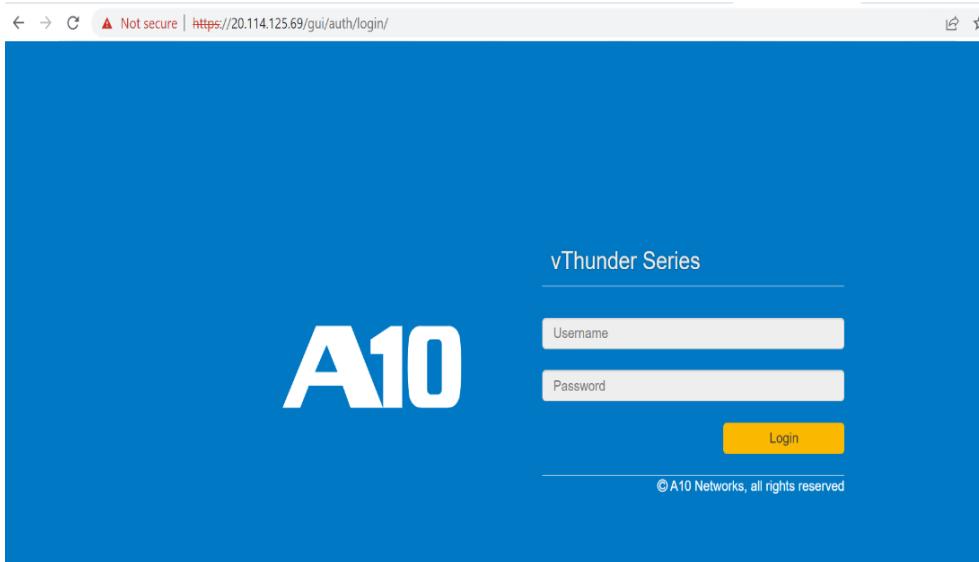
NOTE: It is highly recommended to change the default password when you login for the first time.

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 187 : vThunder GUI



3. Enter the user credentials provided by A10 Networks Support.
The home page gets displayed.

Verify Deployment

To verify deployment thru 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 10.0.0.3.5
    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
!
```

- 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
```

- From vThunder Console, navigate thru **Home > License History** to verify your

license:

Figure 188 : License History



- 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
<hr/>			
server certificate		Jan 28 12:00:00 2028 GMT	[Unexpired, Bound]

- Run the following command to verify vThunder logs sync-up configuration:

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

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:

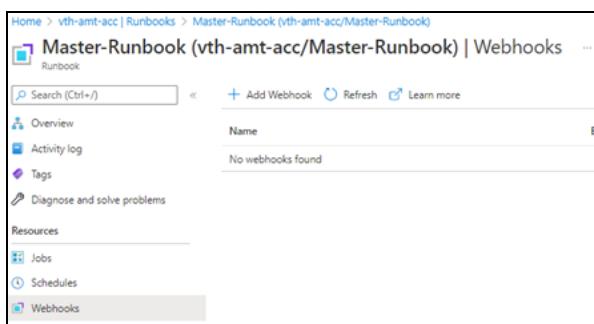
```
Set -AzStorageBlobContent @blobSSL
Cannot bind argument to parameter 'Container' because it is null.
```

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 189 : 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

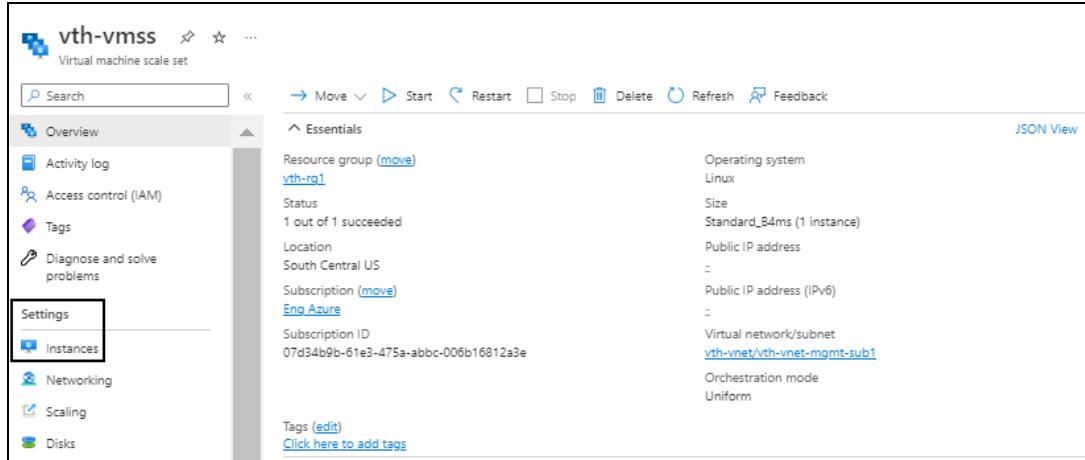
If the Runbook job has failed or is not working, re-run the master runbook.

To re-run the master runbook, perform the following steps:

- From **Azure Portal**, navigate thru **Azure Services > Virtual machine scale sets > <vmss_name>**.

The selected vmss - Overview window is displayed.

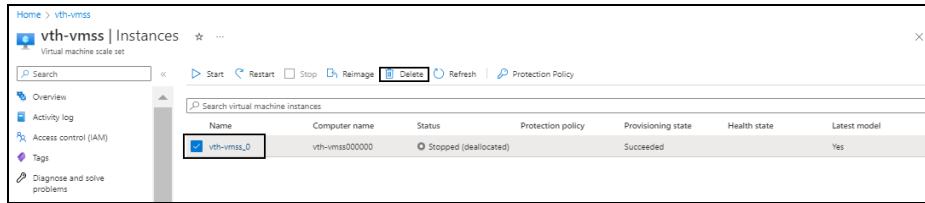
Figure 190 : Selected vmss - Overview window



- Click **Instances** from the left **Settings** panel.

The selected vmss - Instances window is displayed.

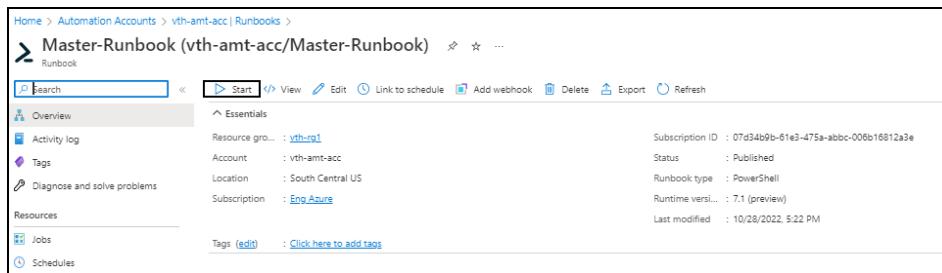
Figure 191 : Selected vmss - Instances window



- Click **Delete** to delete all the vmss instances.

- From the Master-Runbook Job window, click **Start** to re-run the master runbook.

Figure 192 : 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

```
"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/logDefinitions/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/Microsoft.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/logDefinitions/read",

"Microsoft.Compute/virtualMachines/providers/Microsoft.Insights/diagnosticSettings/read",

"Microsoft.Compute/virtualMachines/providers/Microsoft.Insights/diagnosticSettings/write",
"Microsoft.Compute/virtualMachines/instanceView/read",

"Microsoft.Compute/virtualMachines/providers/Microsoft.Insights/metricDefinitions/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

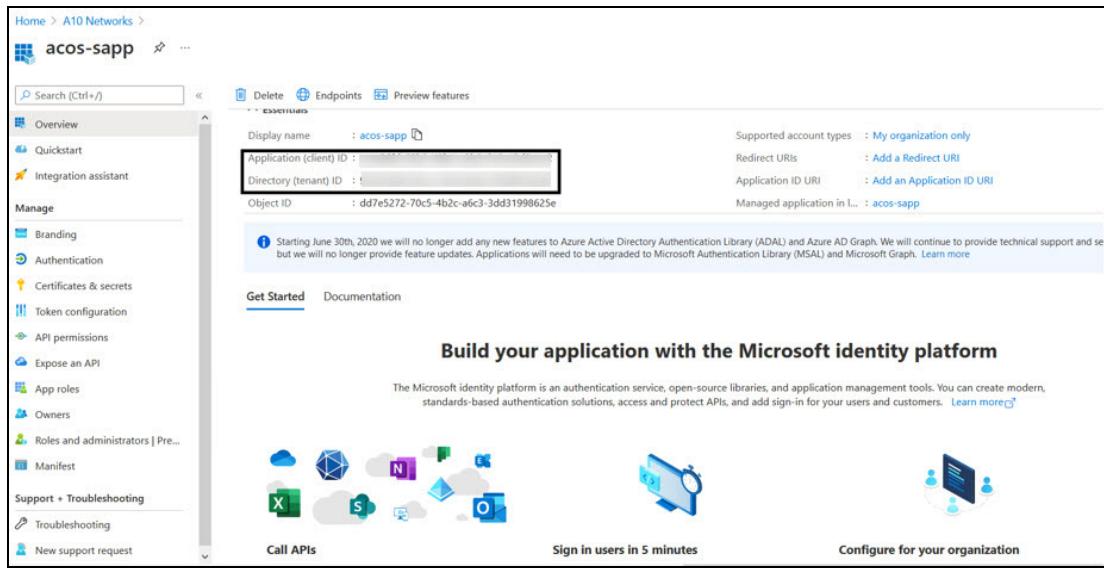
The Azure service application access key is required to access the Azure resources.

Use an existing Access Key

To use an existing Azure service application access key, perform the following steps:

1. From **Azure Portal**, navigate thru **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 193 : 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:

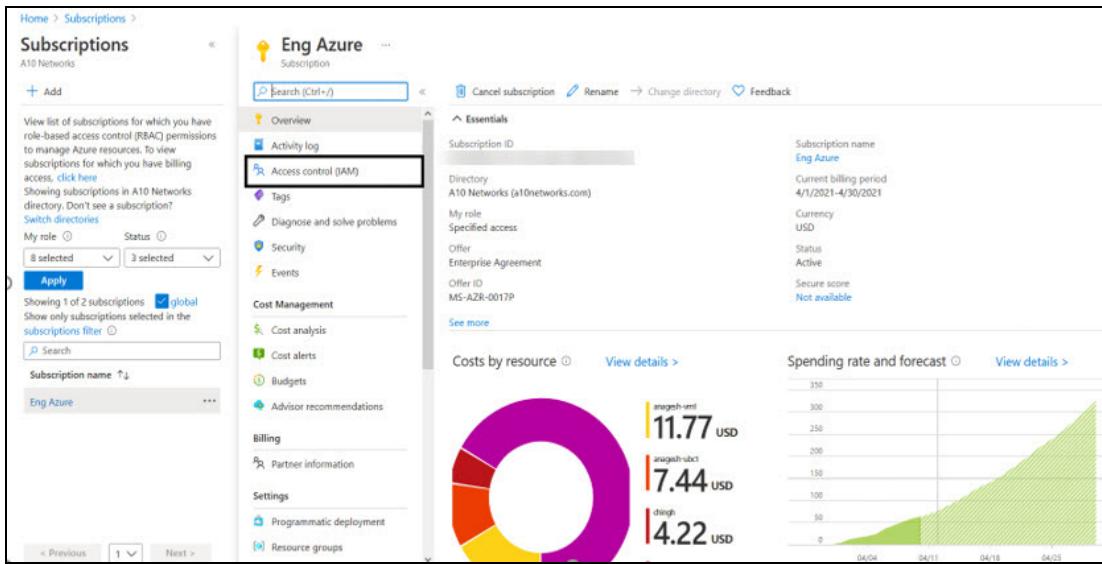
1. [Create a Role](#)
2. [Register a Service Application](#)
3. [Associate Service Application with a Role](#)
4. [Create Certificate and Secrets](#)
5. [Collect Azure Access Key](#)
6. [Import Azure Access Key](#)

Create a Role

To create a custom role, perform the following steps:

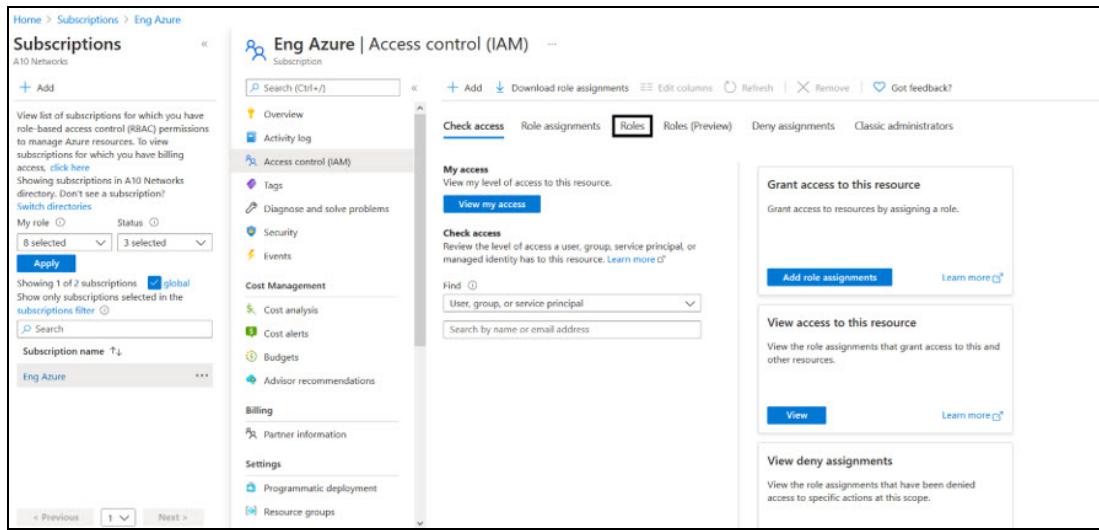
- From **Home**, navigate thru **Azure Services > Subscriptions > <subscription_name>**.
The selected Subscription - Overview window is displayed. Here, the subscription is Eng Azure.

Figure 194 : Subscriptions - Overview window



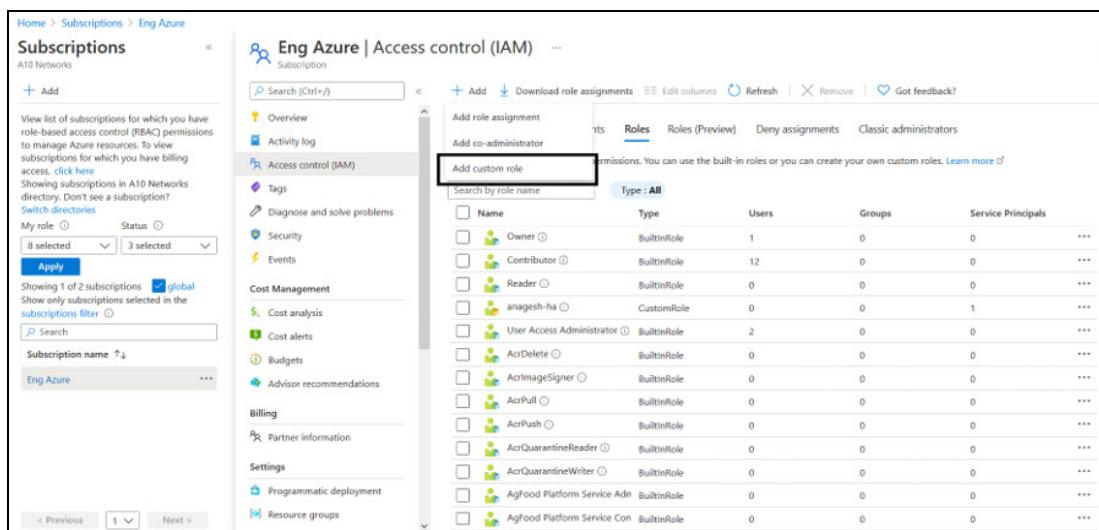
- Click **Access control (IAM)** from left panel.
The selected Subscription - Access control (IAM) window is displayed.
- Select the **Roles** tab.
The Roles window is displayed.

Figure 195 : Access Control - Role Window



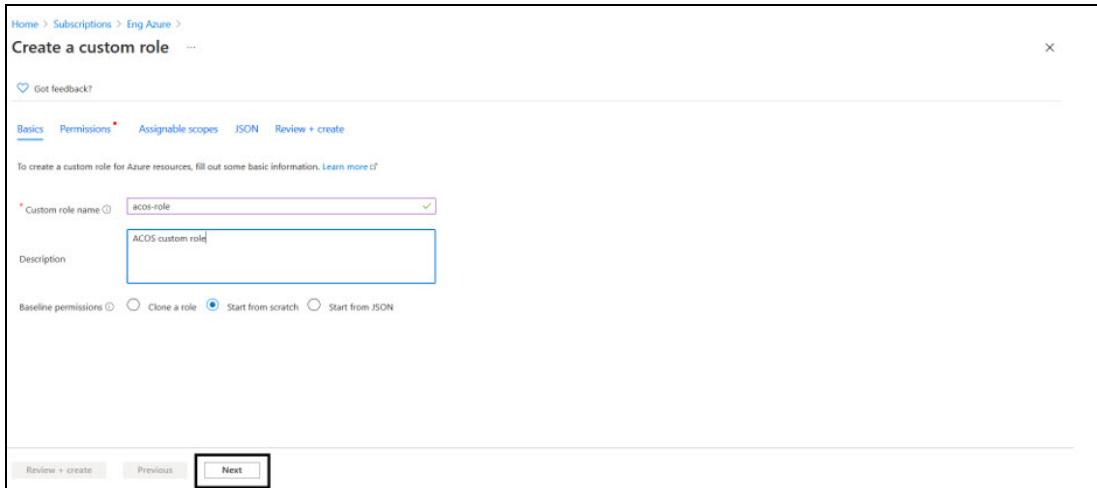
4. Click **Add** to select **Add custom role** option.
The Create a custom role window is displayed.

Figure 196 : Add custom role window



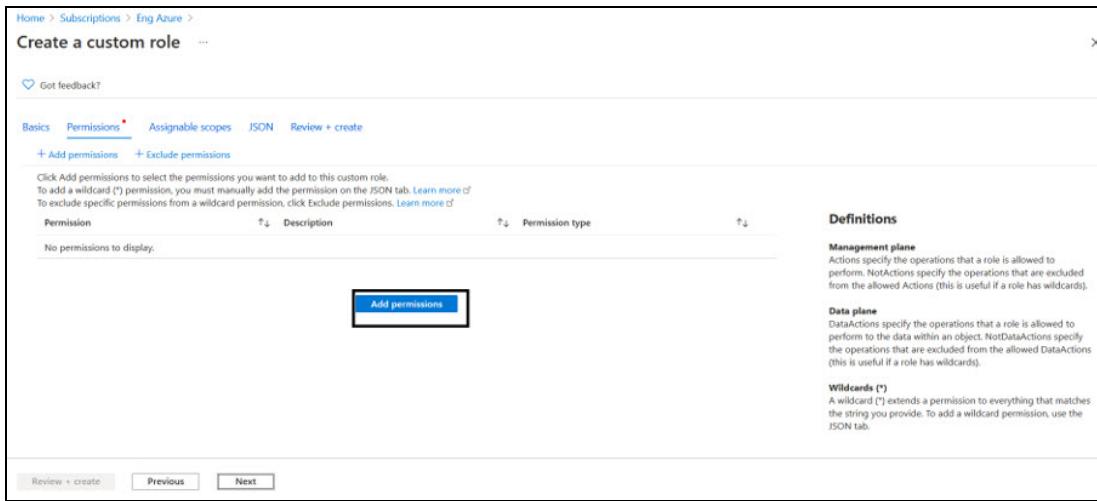
5. Enter **Customer role name** and **Description** (optional) in the **Basics** tab.

Figure 197 : Create a custom role window



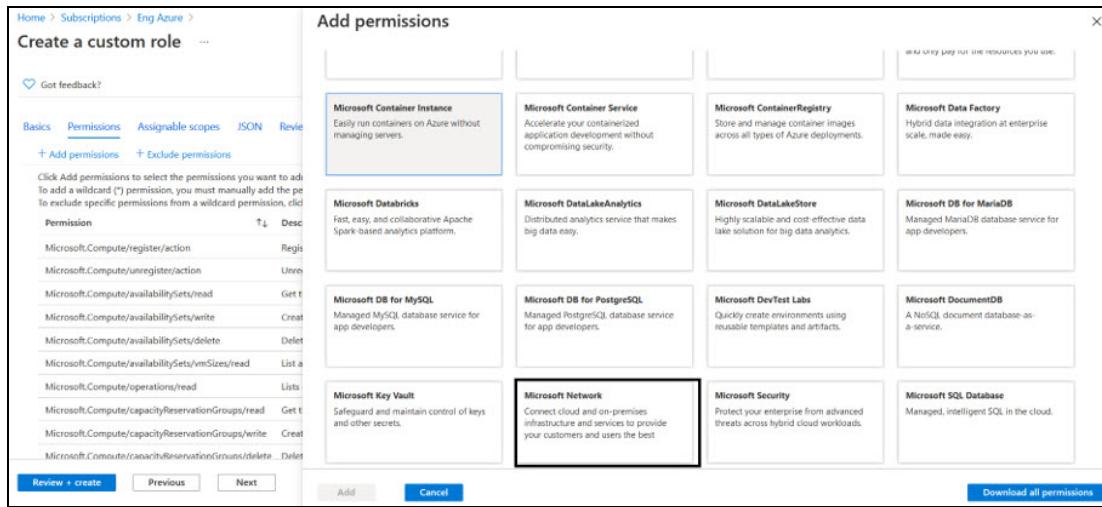
6. Click **Next** at the bottom of the window.
The Permissions window is displayed.

Figure 198 : Permission window



7. Click **Add Permissions** to add permissions to the custom role.
The Add Permissions window is displayed.

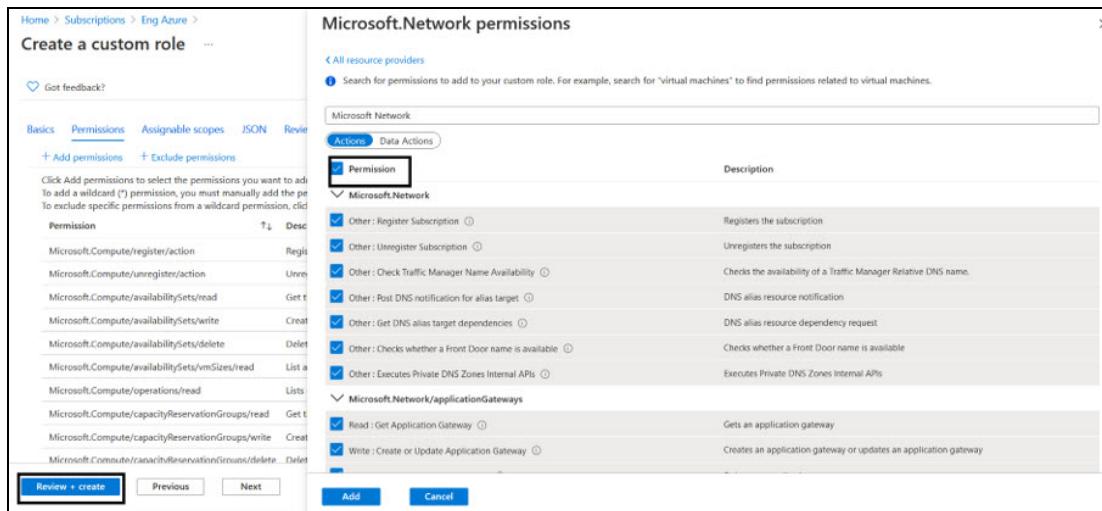
Figure 199 : Add permissions window



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 200 : 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.

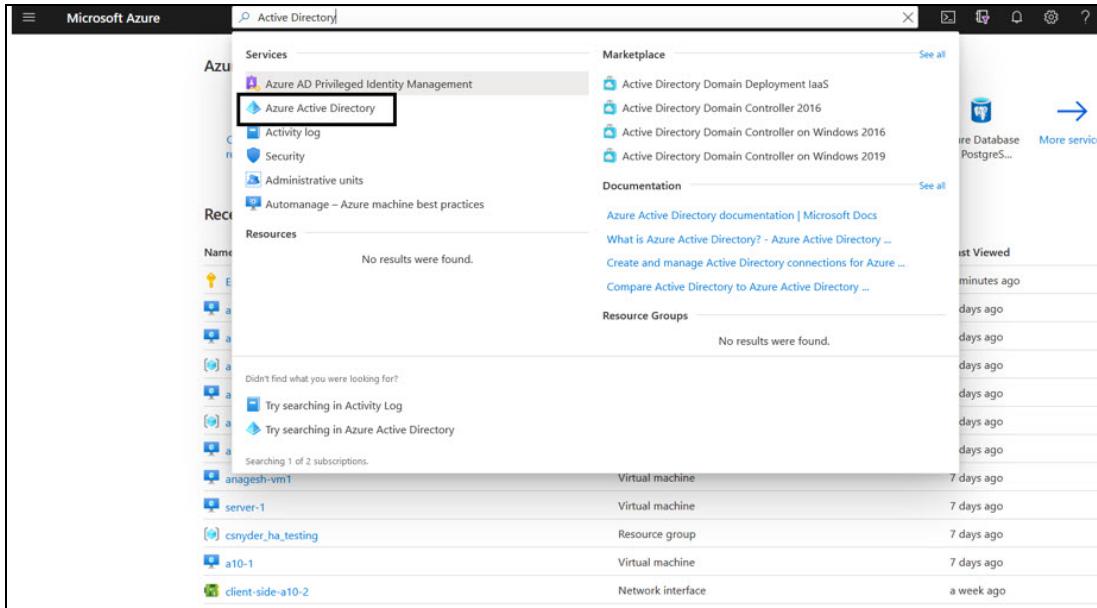
NOTE: It may take the system a few minutes to display your role everywhere.

Register a Service Application

To register a service application, perform the following steps:

1. From Home, navigate thru Azure Services > Azure Active Directory option.

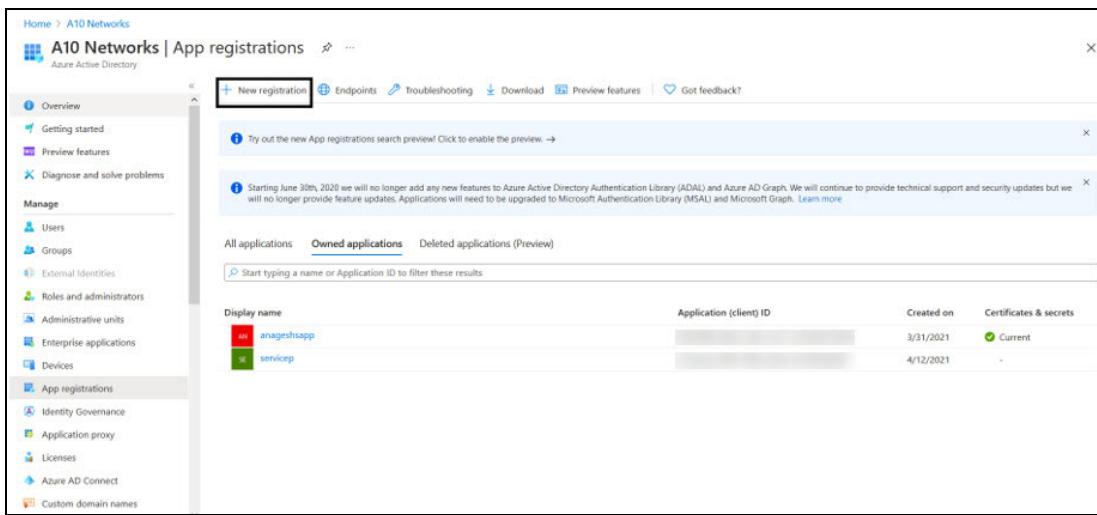
Figure 201 : Azure Active Directory window



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.

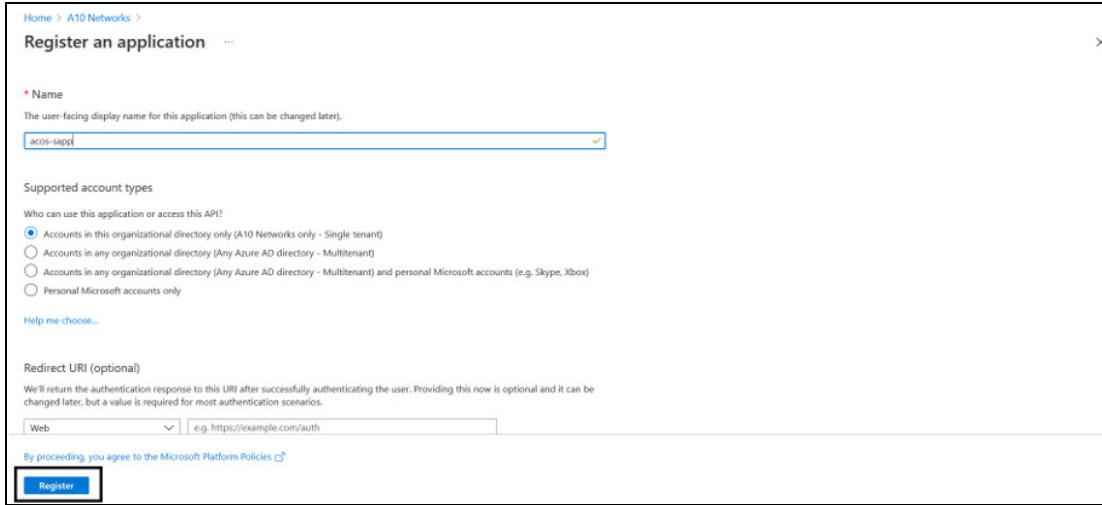
Figure 202 : App registrations window



3. Click **New Registration**.

The Register an application window is displayed.

Figure 203 : Register an application window



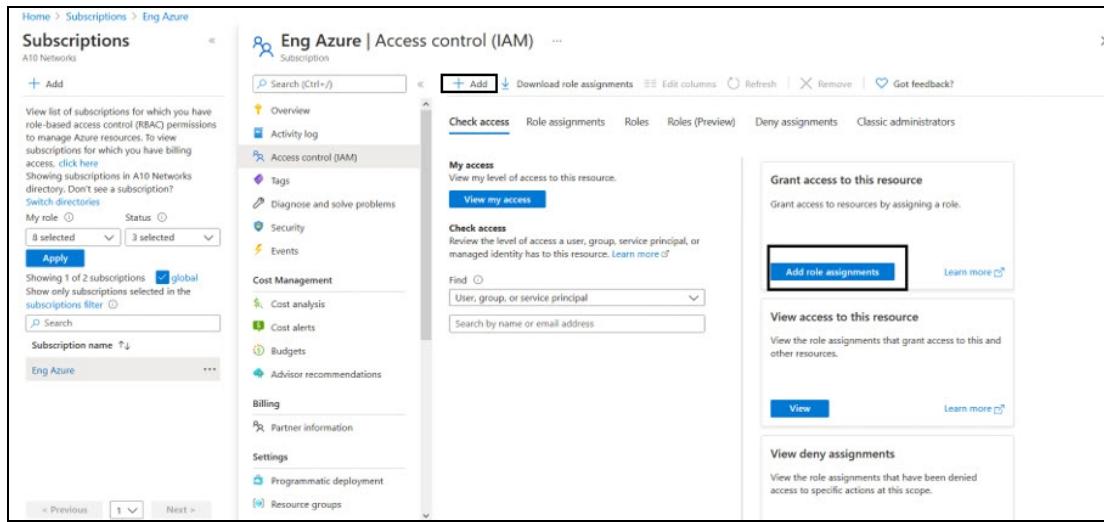
4. Enter the **Name** of the application. For example, acos-sapp.
5. Click **Register** to register the application. The application gets listed under Azure Active Directory - Apps registrations window.

Associate Service Application with a Role

To associate service application with a role, perform the following steps:

1. From **Home**, navigate thru **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.

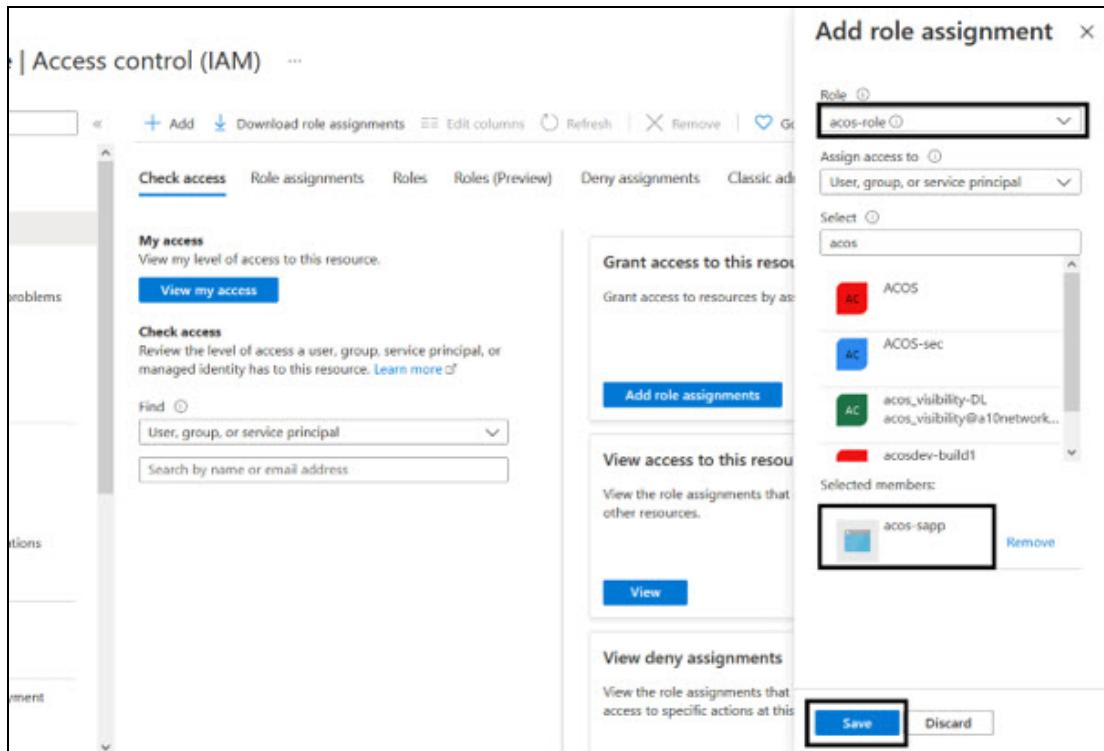
Figure 204 : Subscription - Access control (IAM) window



The screenshot shows the Azure portal's 'Access control (IAM)' interface for a specific subscription named 'Eng Azure'. The left sidebar lists various management categories like Subscriptions, Activity log, and Cost Management. The main content area has tabs for 'Check access', 'Role assignments', 'Roles', 'Roles (Preview)', 'Deny assignments', and 'Classic administrators'. Under 'Check access', there are sections for 'My access' (with a 'View my access' button), 'Check access' (with a 'Find' dropdown set to 'User, group, or service principal'), and 'Find by name or email address'. To the right, three boxes provide options for managing access: 'Grant access to this resource' (containing a 'Add role assignments' button), 'View access to this resource' (with a 'View' button), and 'View deny assignments' (with a 'View' button). The 'Add role assignments' button is highlighted with a red box.

- To assign a role to the above scope, click **Add** from the main menu options. The Add role assignment window is displayed.

Figure 205 : Add a role assignment -1



This screenshot shows the 'Add role assignment' dialog box. On the left, a list of roles is shown with 'acos-role' selected. On the right, a list of users or groups is shown with 'acos-sapp' selected and highlighted with a red box. At the bottom, there are 'Save' and 'Discard' buttons, with 'Save' also highlighted with a red box.

- Select a **Role** from the drop-down list. For example, acos-role.

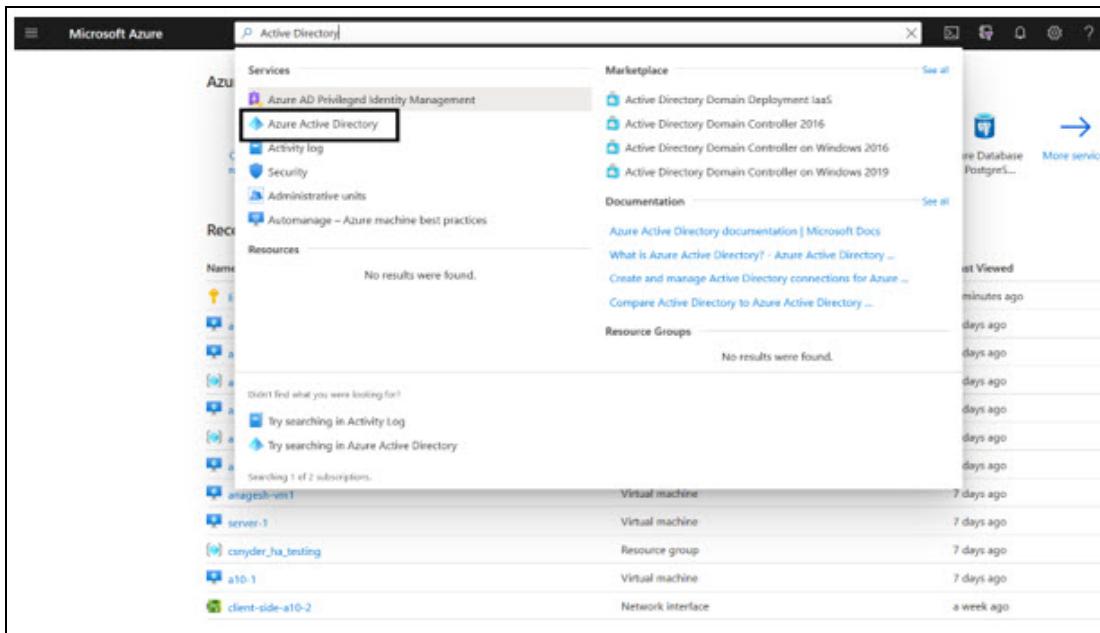
5. Select the required **Assign Access to** option from the drop-down list.
6. Enter a string to search and select for a name or email address. For example, acos.
7. Click the **Save** button to save the configuration.

Create Certificate and Secrets

To create certificate and secrets for the assigned role, perform the following steps:

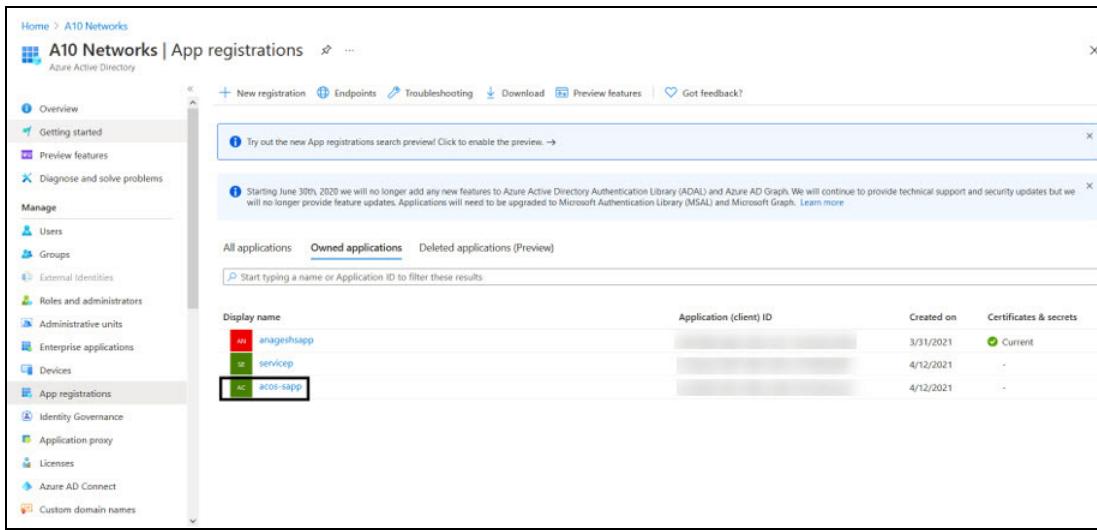
1. From **Home**, navigate thru **Azure Services > Azure Active Directory** option.

Figure 206 : 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 207 : App registrations - Overall applications window



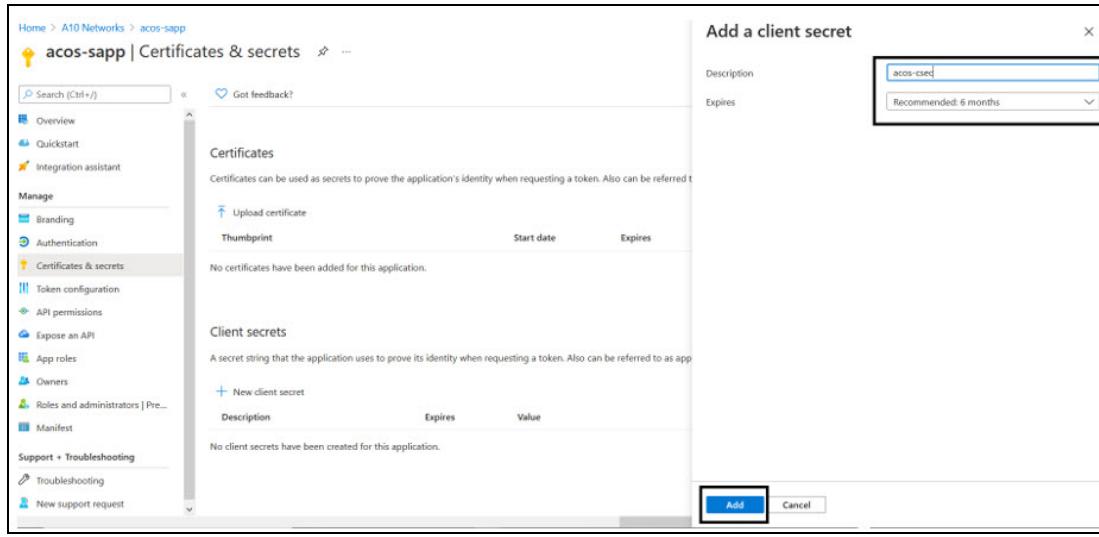
The screenshot shows the 'App registrations' section of the Azure Active Directory portal. The left sidebar includes options like Overview, Getting started, Preview features, Diagnose and solve problems, Manage (with sub-options like Users, Groups, External identities, Roles and administrators, etc.), and App registrations (which is selected). The main area displays a table of registered applications:

Display name	Application (client) ID	Created on	Certificates & secrets
anagnishapp	[Redacted]	3/31/2021	Current
serviceip	[Redacted]	4/12/2021	-
acos-sapp	[Redacted]	4/12/2021	-

A message at the top indicates that starting June 30th, 2020, no new features will be added to ADAL and Azure AD Graph.

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.

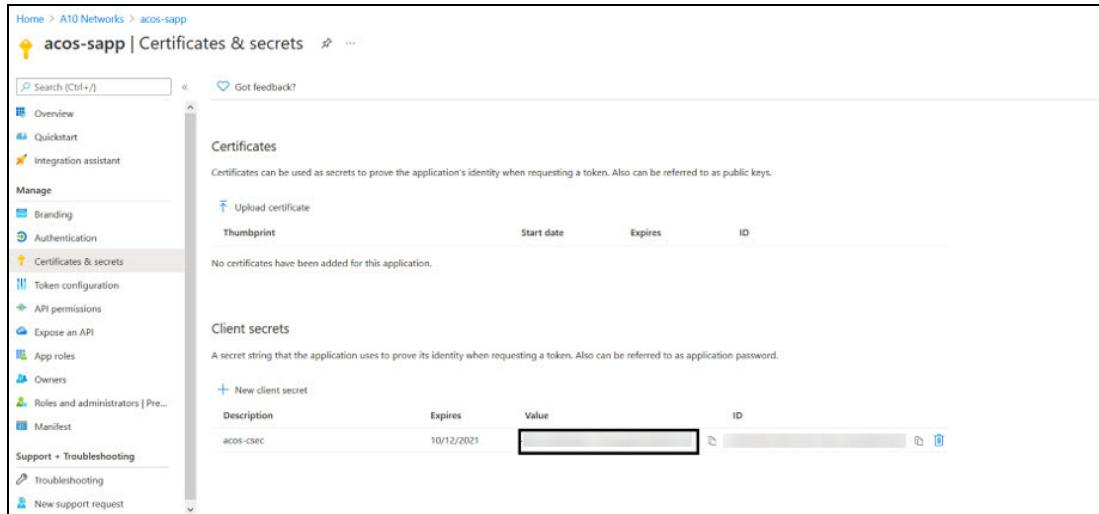
Figure 208 : Add a client secret window



7. Enter the New client secret **Description**, **Expires** value.

The entered value is displayed on theacos-Certificates & secrets window.

Figure 209 :acos-sapp Certificates & secrets window



NOTE:

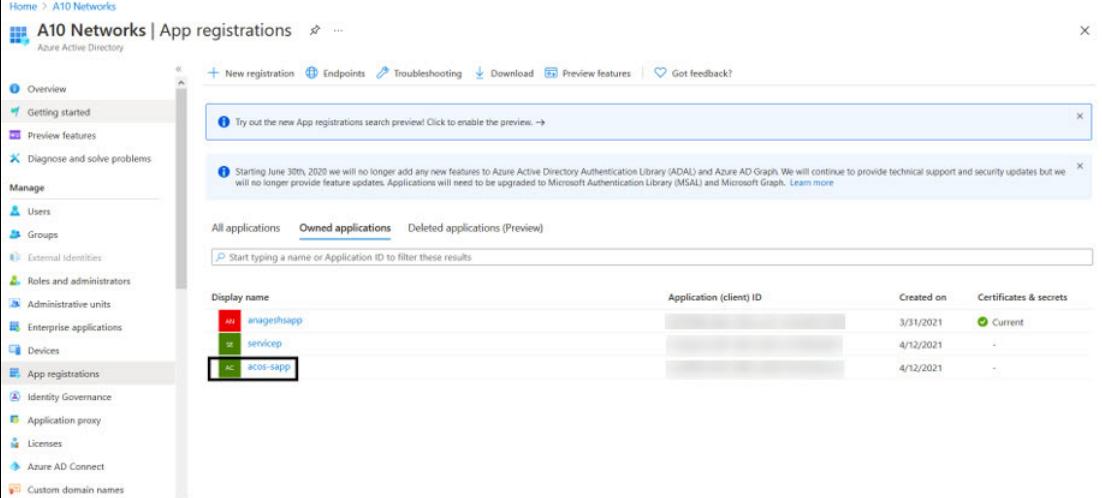
Save the new client secret value in a text file, as it is not visible once the window is refreshed.

Collect Azure Access Key

To collect Azure access keys, perform the following steps:

- From **Home**, navigate thru **Azure Services > Azure Active Directory > App registrations**.

Figure 210 : Azure Active Directory - App registrations window

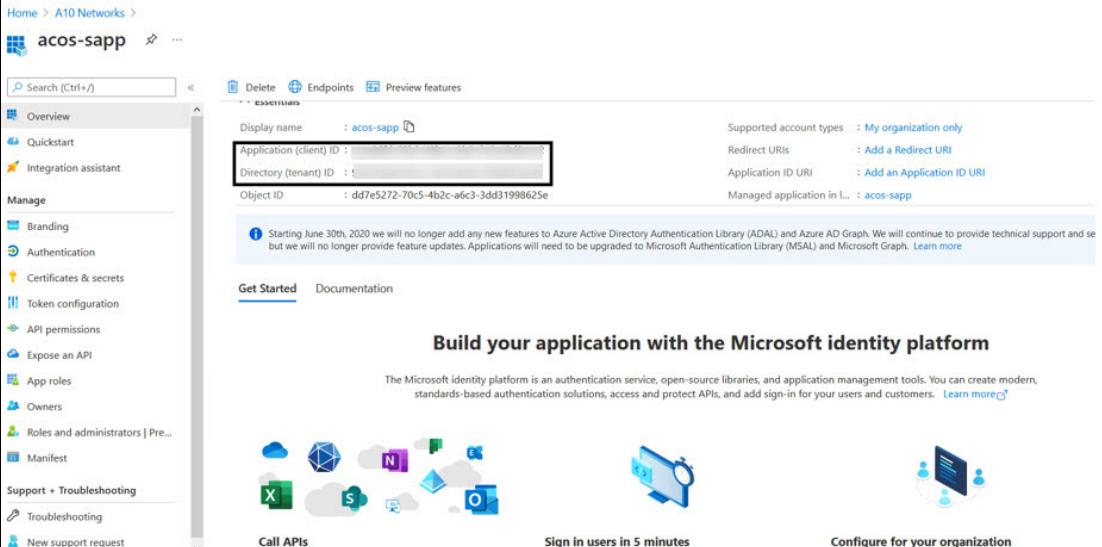


The screenshot shows the 'App registrations' page under 'Azure Active Directory'. The left sidebar includes 'Overview', 'Getting started', 'Preview features', 'Diagnose and solve problems', 'Manage' (with options like 'Users', 'Groups', 'External identities', 'Administrative units', 'Enterprise applications', 'Devices', 'App registrations', 'Identity Governance', 'Application proxy', 'Licenses', 'Azure AD Connect', and 'Custom domain names'), and a 'New registration' button. The main area has tabs for 'All applications', 'Owned applications' (which is selected), and 'Deleted applications (Preview)'. A search bar allows filtering by application name or ID. Below the search bar is a table with columns: 'Display name', 'Application (client) ID', 'Created on', and 'Certificates & secrets'. Three entries are listed: 'managersapp' (client ID 70c5-4b2c-a6c3-3dd31998625e, created 3/31/2021), 'servicecp' (client ID 412/2021), and 'acos-sapp' (client ID dd7e5272-70c5-4b2c-a6c3-3dd31998625e, created 4/12/2021). A message at the top indicates that starting June 30th, 2020, new features will no longer be added to ADAL and Azure AD Graph.

- From the **Owned applications** tab, select service application from the list of applications.

The selected service application window is displayed.

Figure 211 : Selected Service application window



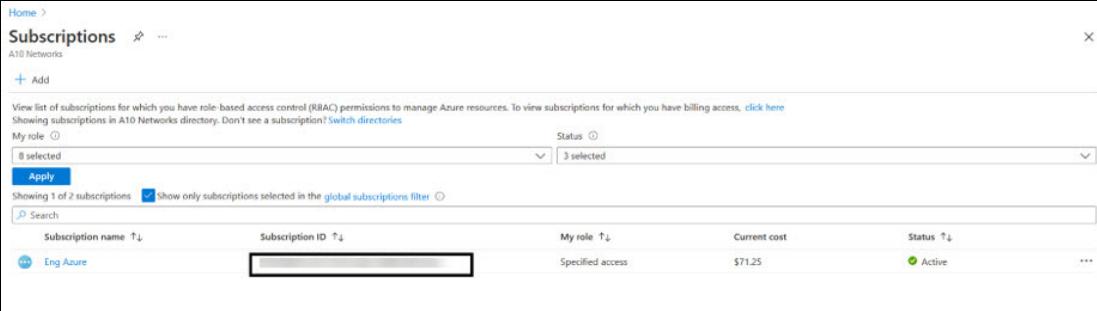
The screenshot shows the 'acos-sapp' service application details page. The left sidebar includes 'Overview', 'Quickstart', 'Integration assistant', 'Manage' (with options like 'Branding', 'Authentication', 'Certificates & secrets', 'Token configuration', 'API permissions', 'Expose an API', 'App roles', 'Owners', 'Roles and administrators | Pre...', 'Manifest', 'Support + Troubleshooting', 'Troubleshooting', and 'New support request'), and a 'Get Started' button. The main area displays application details: 'Display name' (acos-sapp), 'Application (client) ID' (redacted), 'Directory (tenant) ID' (redacted), and 'Object ID' (dd7e5272-70c5-4b2c-a6c3-3dd31998625e). It also shows supported account types ('My organization only'), redirect URIs ('Add a Redirect URI'), application ID URI ('Add an Application ID URI'), and managed applications ('acos-sapp'). A message at the bottom indicates that starting June 30th, 2020, new features will no longer be added to ADAL and Azure AD Graph. Below the application details is a section titled 'Build your application with the Microsoft identity platform' which links to the Microsoft identity platform documentation. At the bottom are three call-to-action buttons: 'Call APIs' (with icons for Excel, Power BI, SharePoint, OneDrive, etc.), 'Sign in users in 5 minutes' (with a user sign-in icon), and 'Configure for your organization' (with a server icon).

- Copy the Client ID, Tenant ID from the service application window.

```
client_id= 'cc4c86xx-65b3-48xx-a3xx-610xxxxxxxx'
tenant_id= '91d27axx-8cxx-41xx-82xx-3d1xxxxxxxx'
```

4. Navigate to the **Home > Subscriptions > Registered Subscription Name**, and copy subscription ID value.

Figure 212 : Subscriptions window



The screenshot shows the 'Subscriptions' page in the Azure portal. It displays a single subscription named 'Eng Azure'. The table includes columns for Subscription name, Subscription ID, My role, Current cost, and Status. The status is shown as 'Active'.

Subscription name	Subscription ID	My role	Current cost	Status
Eng Azure		Specified access	\$71.25	Active

5. Create a text file having subscription, client_id, client_secret, and tenant_id information as shown below:

```
subscription='07d34bxx-61xx-47xx-abxx-006xxxxxxxx'
client_id='cc4c86xx-65xx-48xx-a3xx-610xxxxxxxx'
client_secret='G0x_hVDzZxxxx-o1Vsw.xxxx.Zxxxx-xx'
tenant_id='91d2xxxx-8xxe-41xx-82xx-3d1xxxxxxxx'
```

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-baf8-e03cc942aa66'
secret = '*****_XGEdu0Or+M2Css=*****-0b'
tenant = '1e94d773-****-****-b25d-3b3e1b64948d'
vThunder-Active(config-admin:admin) (NOLICENSE) #
```

