Installing vThunder ADC using ARM Templates

Version 1.2.0

February, 2024

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

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

The A10 Thunder® Application Delivery Controller (ADC) is a high-performance solution designed to accelerate and optimize critical applications, ensuring their reliable and efficient delivery.

This documentation assists you in deploying Thunder® ADC instances on the Azure Cloud using ARM templates.

The following steps provide a high-level overview of the deployment process:

1. Provision the Azure Cloud network infrastructure.

   There are custom templates available for new creating network security groups (NSGs), subnets, virtual network (VNet), and public IP to provision the new infrastructure. The creation of NSG, subnets, and VNet are optional; if it already exists, it can be reused.

   For more information, see Create VNet, Subnet, and NSG and Create Public IP address.

   For more information on other prerequisites, see Prerequisites.

2. Create Thunder virtual machine/s on the Azure Cloud.

   There are custom templates available for creating new network interface cards (NICs) and Thunder virtual machines (VMs) on Azure Cloud with built-in Thunder and for applying network settings. Various templates are available for different deployment requirements.

   For more information on the specific use-cases, see Deployment Templates.

   You can deploy Thunder on the Azure Cloud using either of the following recommended ways:

   - Using Azure Resource Manager (ARM) templates

     These templates can be deployed using the Azure Portal Console or Azure CLI.

- Using Powershell templates

  These templates can be deployed using the Powershell command prompt.

3. Configure Thunder.

   There are custom Powershell scripts available to apply the new Thunder configurations. Different scripts are available for various configuration needs.

   For more information, see ADC Configuration Templates.

Terminology

- **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 here.
- **Availability Zone** — A distinct data center within an Azure region. It is designed to be an isolated location to ensure resilience and high availability. For more information, see here.
- **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 here.
- **Azure Application Insights** — The application insights are custom metrics used to analyze CPU utilization and configure alerts.
- **Azure Automation** — Azure automation is a cloud-based solution to automate recurring and manual tasks. For more information, see here.
- **Azure Automation Account** — An automation account is a logical group of all the resources related to Azure automation within a resource group.
- **Azure Automation Webhook** — A webhook is a custom URL that is sent to Azure automation with a runbook-specific data payload.
- **Azure CLI** — A set of command-line tools provided by Microsoft Azure to interact with the Azure platform using commands and manage Azure services and resources.

- **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.
- **Azure Log Analytics Workspace** — A log analytics workspace is a custom workspace to collect system logs from virtual machine instances.
- **Azure Resource Manager (ARM) Template** — A JavaScript Object Notation (JSON) file used to specify the resources and its properties which are deployed on the Azure cloud.
- **Azure Runbook** — A runbook is a PowerShell script used to start the automation jobs in Azure.
- **Azure Service Application Access Key** — An access key is used to automate scale set creation and configuration.
- **Backend Pool** — A backend pool is used to define the group of resources that serves traffic for a given load-balancing rule.
- **Global Server Load Balancing (GSLB)** — A process to distribute incoming network traffic across multiple servers or data centers located in different geographical locations.
- **Health Probe** — A health probe is used to determine the health status of the virtual machine instances in the backend pool.
- **High Availability (HA)** — A capability to remain operational and accessible for a significantly high percentage of the time.
- **Hybrid Cloud** — A cloud computing model that combines private cloud and public cloud services within the same seamless infrastructure.
- **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.
- **PowerShell** — A task automation and configuration management framework used for scripting.
- **Python3** — The latest major version of the Python programming language.

- **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 here.
- **Virtual Machine Scale Set (VMSS)** — A virtual machine scale set is used to manage and deploy multiple identical virtual machine instances.
- **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 a logical isolation of the Azure cloud for an Azure account. You can connect different virtual networks to on-premises networks. For more information, see here.
- **vThunder** — An A10 Thunder instance for virtual machine.

Prerequisites

To create and configure Thunder virtual machine on the Azure cloud using ARM template, you must ensure that the following prerequisites are met:

1. Download A10 custom ARM templates from GitHub.
2. Azure account with sufficient permissible role. For more information, see List of Custom Role Permissions.
3. Access Azure Portal to create Thunder virtual machine using ARM templates from the Azure Portal console.
4. Download and install Azure CLI to create Thunder virtual machine using ARM templates from the Azure CLI command prompt.
   For more information, see Install Azure CLI on PowerShell.
5. Download and install PowerShell to configure Thunder from powershell command prompt.
   For more information, see Install PowerShell.
6. Sign up here to get Thunder Trial license.

For any queries, reach out to A10 Networks Support.

Image Repository

Table 1 provides the list of ACOS versions and modules that support the CFT templates:

Table 1 : Supported ACOS versions

ACOS Version	ADC	CGN	SSLi	TPS
64-bit Advanced Core OS (ACOS) version 6.0.2	√	X	X	X
64-bit Advanced Core OS (ACOS) version 6.0.1	√	X	X	X
64-bit Advanced Core OS (ACOS) version 6.0.0-P2-SP1	√	X	X	X
64-bit Advanced Core OS (ACOS) version 6.0.0-P1	√	X	X	X
64-bit Advanced Core OS (ACOS) version 5.2.1-P8	√	X	X	X
64-bit Advanced Core OS (ACOS) version 5.2.1-P7	√	X	X	X
64-bit Advanced Core OS (ACOS) version 5.2.1-P6	√	X	X	X

Deployment Templates

This section helps you in provisioning a new Thunder virtual machine on the Azure cloud.

Before proceeding, it is recommended to review the Prerequisites.

To provision a new virtual Thunder ADC instance on an Azure cloud, perform the following steps:

1. Create VNet, Subnet, and NSG.
   It is not mandatory to create new resources, the existing resources can be used in deployment and configuration.
2. Create Public IP address.
   It is not mandatory to create new resource, the existing resource can be used in deployment and configuration.
3. Select an appropriate template for deploying vThunder ADC on Azure cloud according to your use case.

   Table 2 provides a list of various use cases along with their respective supported ARM templates.

Table 2 : Supported ARM Templates

Use Case	Template Name	Number of Thunder/s	Number of NICs	Data-in NIC VIP	Description
Standalone Thunder ADC	Thunder-2NIC-1VM	1	2	Private	• Creates one vThunder instance with one management and one data NIC (data-in), see Figure 1. • Applies additional

Table 2 : Supported ARM Templates

Use Case	Template Name	Number of Thunder/s	Number of NICs	Data-in NIC VIP	Description
					configuration on vThunder as required: ◦ Change Password ◦ Basic Server Load Balancer ◦ A10 License ◦ SSL Certificate
Thunder ADC in High Availability mode with Private VIP.	Thunder-3NIC-2VM-PVTVIP	2	3	Private	• Creates two vThunder instances with HA setup and each vThunder has one management and two data NICs (data-in and data-out), see Figure 27. • Configures data-in network interface card (NIC) with Private IP on VIP. • Applies additional configuration on vThunder as required: ◦ Change Password

Table 2 : Supported ARM Templates

Use Case	Template Name	Number of Thunder/s	Number of NICs	Data-in NIC VIP	Description
					◦ Basic Server Load Balancer ◦ A10 License ◦ SSL Certificate ◦ High Availability • When one instance becomes unavailable, another instance seamlessly handles the request without requiring manual intervention. • High availability can be configured within the same or different availability zone within a same region.
Thunder ADC in High Availability mode with Public VIP.	Thunder-3NIC-2VM-PUBVIP	2	3	Public	• Creates two vThunder instances with HA setup and each vThunder has one management and two data NICs

Table 2 : Supported ARM Templates

Use Case	Template Name	Number of Thunder/s	Number of NICs	Data-in NIC VIP	Description
					(data-in and data-out), see Figure 54. • Configures data-in network interface card (NIC) with Public IP on VIP. • Applies additional configuration on vThunder as required: ◦ Change Password ◦ Basic Server Load Balancer ◦ A10 License ◦ SSL Certificate ◦ High Availability • When one instance becomes unavailable, another instance seamlessly handles the request without requiring manual intervention.

Table 2 : Supported ARM Templates

Use Case	Template Name	Number of Thunder/s	Number of NICs	Data-in NIC VIP	Description
					• High availability can be configured within the same or different availability zone within a same region.
Thunder ADC in High Availability mode with Private VIP and Backend Server Autoscale.	Thunder-3NIC-2VM-PVTVIP	2	3	Private	• Creates two vThunder instances with HA setup and each vThunder has one management and two data NICs (data-in and data-out), see Figure 28. • Configures data-in network interface card (NIC) with Private IP on VIP. • Applies additional configuration on vThunder as required: ◦ Change Password ◦ Server Load Balancer on Backend

Table 2 : Supported ARM Templates

Use Case	Template Name	Number of Thunder/s	Number of NICs	Data-in NIC VIP	Description
					Autoscale ◦ A10 License ◦ SSL Certificate ◦ High Availability • Applies SLB configuration using a webhook URL on vThunder for newly added or deleted web/app servers through backend server VMSS autoscaling. • When one instance becomes unavailable, another instance seamlessly handles the request without requiring manual intervention. • High availability can be configured within the same or different availability zone

Table 2 : Supported ARM Templates

Use Case	Template Name	Number of Thunder/s	Number of NICs	Data-in NIC VIP	Description
					within a same region.
Thunder ADC in High Availability mode with Public VIP and Backend Server Autoscale.	Thunder-3NIC-2VM-PUBVIP	2	3	Public	• Creates two vThunder instances with HA setup and each vThunder has one management and two data NICs (data-in and data-out), see Figure 55. • Configures data-in network interface card (NIC) with Public IP and Private IP on VIP. • Applies additional configuration on vThunder as required: ◦ Change Password ◦ Server Load Balancer on Backend Autoscale ◦ A10 License ◦ SSL Certificate

Table 2 : Supported ARM Templates

Use Case	Template Name	Number of Thunder/s	Number of NICs	Data-in NIC VIP	Description
					○ High Availability • Applies SLB configuration using a webhook URL on vThunder for newly added or deleted web/app servers through backend server VMSS autoscaling. • When one instance becomes unavailable, another instance seamlessly handles the request without requiring manual intervention. • High availability can be configured within the same or different availability zone within a same region.
Thunder ADC with	Thunder-3NIC-	3	3	Public	• Creates three vThunder

Table 2 : Supported ARM Templates

Use Case	Template Name	Number of Thunder/s	Number of NICs	Data-in NIC VIP	Description
GSLB (Disaster Recovery Site in a cross-region or hybrid cloud environment)	3VM				instances each vThunder has one management and two data NICs (data-in and data-out) in the same region1 and zone1, see Figure 84. These three vThunder instances are referred as Master Controller (Active), Site1 and Site2. • Applies additional configuration on vThunder as required: ◦ Change Password ◦ Basic Server Load Balancer ◦ A10 License ◦ SSL Certificate ◦ Hybrid Cloud GSLB • The identical set

Table 2 : Supported ARM Templates

Use Case	Template Name	Number of Thunder/s	Number of NICs	Data-in NIC VIP	Description
					of vThunder resources should be deployed in region2 zone1 using the same template. The three vThunder instances in region2 zone1 are referred as the Member Controller (Standby), Site1, and Site2. • When region1 experiences an outage, region2 seamlessly handles all requests through DNS switch over.
Thunder ADC in AutoScale Mode.	Thunder-3NIC-VMSS	'N' number of vThunder instances	3	Private	• Creates the vThunder instances in a self-autoscaling mode, allowing for automatic scaling based on traffic volume, see Figure 110. The maximum number

Table 2 : Supported ARM Templates

Use Case	Template Name	Number of Thunder/s	Number of NICs	Data-in NIC VIP	Description
					of Thunder replicas allowed can be defined. Each vThunder instance contains three NICs. • Creates Virtual Machine Scale Set (VMSS) and auto scale-in or scale-out based on the performance metric threshold rule. • Auto-applies additional configuration on vThunder upon the creation of a webhook URL: ◦ SSL Certificate ◦ Server Load Balancer ◦ A10 License • Applies SLB configuration using a webhook URL on vThunder for newly added

Table 2 : Supported ARM Templates

Use Case	Template Name	Number of Thunder/s	Number of NICs	Data-in NIC VIP	Description
					or deleted web/app servers through backend server VMSS autoscaling. • Auto-deploys a Certificate Authority SSL Certificate in Storage account and Server Load Balancer and license in Automation Account Variable. • Configures log analysis capabilities using Azure Log Analytics workspace integration. • Configures metrics monitoring using Azure Application Insights integration. • When one instance becomes

Table 2 : Supported ARM Templates

Use Case	Template Name	Number of Thunder/s	Number of NICs	Data-in NIC VIP	Description
					unavailable, another instance seamlessly handles the request without requiring manual intervention. • Auto configures all vThunder configurations that are pre-defined in the template. **NOTE:** All the configured vThunder instances do not synchronize their SLB configurations.

After completing the deployment process, proceed to configure your setup. For more information, see ADC Configuration Templates.

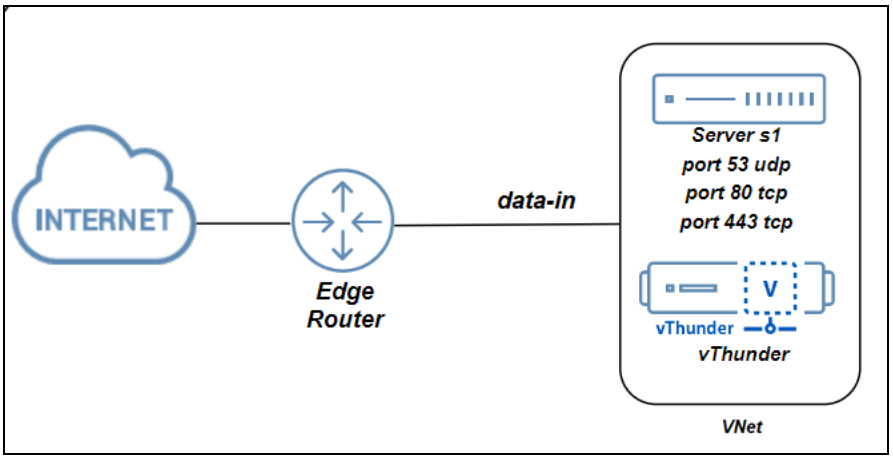
Thunder-2NIC-1VM

This template creates a new virtual machine with pre-loaded Thunder instance and attaches two new network interface cards (NICs).

For more information, see Create Thunder Virtual Machine.

NOTE: Use a suitable VM size that supports at least two NICs. For VM sizes, see Supported VM Sizes.

Figure 1 : Standalone Thunder ADC



Additional Thunder configurations are available that can be applied as needed:

- Change Password
- Basic Server Load Balancer
- A10 License
- SSL Certificate

Various templates are available for different deployment needs.

For more information, see Deployment Templates.

The following topics are covered:

Create Thunder Virtual Machine

The A10-vThunder-2NIC-1VM template is used to create a Thunder virtual machine with two network interface cards.

Before deploying this template, it is recommended to review the Prerequisites.

There are two ways to deploy this template:

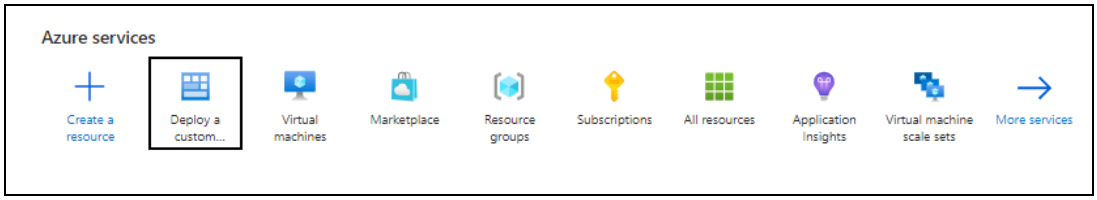
- Upload using Azure Portal Console
- Execute using Azure CLI

Upload using Azure Portal Console

To deploy the A10-vThunder-2NIC-1VM template using Azure Portal Console, perform the following steps:

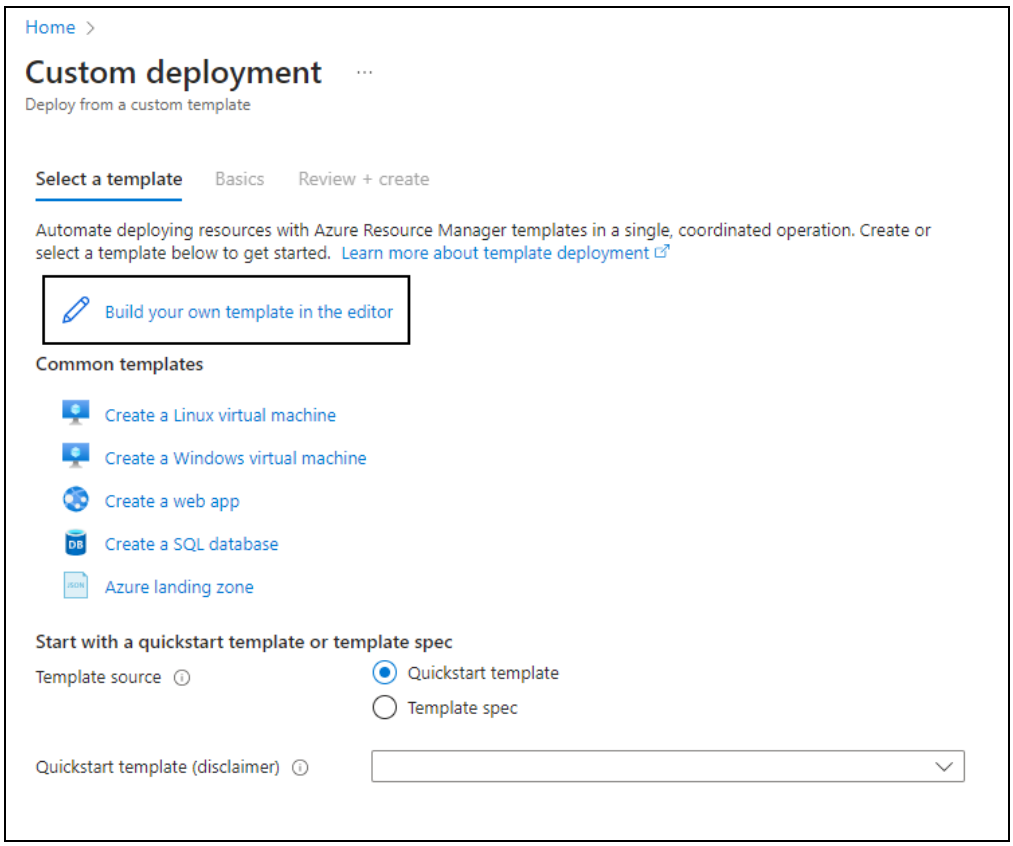
1. Download A10-vThunder-2NIC-1VM template.
2. From the **Azure Portal** > **Azure services**, click **Deploy a custom template**.

Figure 2 : Azure services



3. Under the **Custom deployment** window > **Select a template** tab, click **Build your own template in the editor**.

Figure 3 : Custom deployment window

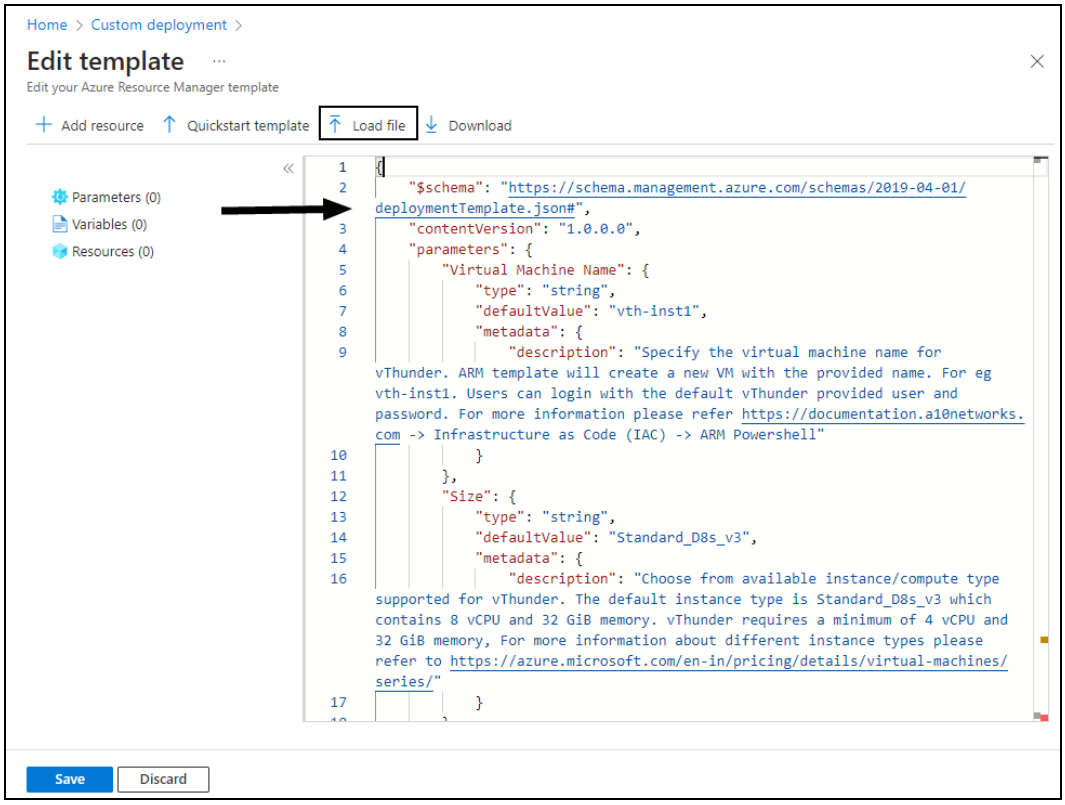


4. From the **Edit template** window, perform either of the following step:

   - Click **Load file** and browse to the folder where you have downloaded the ARM template. Select **ARM_TMPL_2NIC_1VM.json** to upload.

- From Windows Explorer, navigate to the folder where you have downloaded the ARM template. Copy **ARM_TMPL_2NIC_1VM.json** content and paste it in the editor.

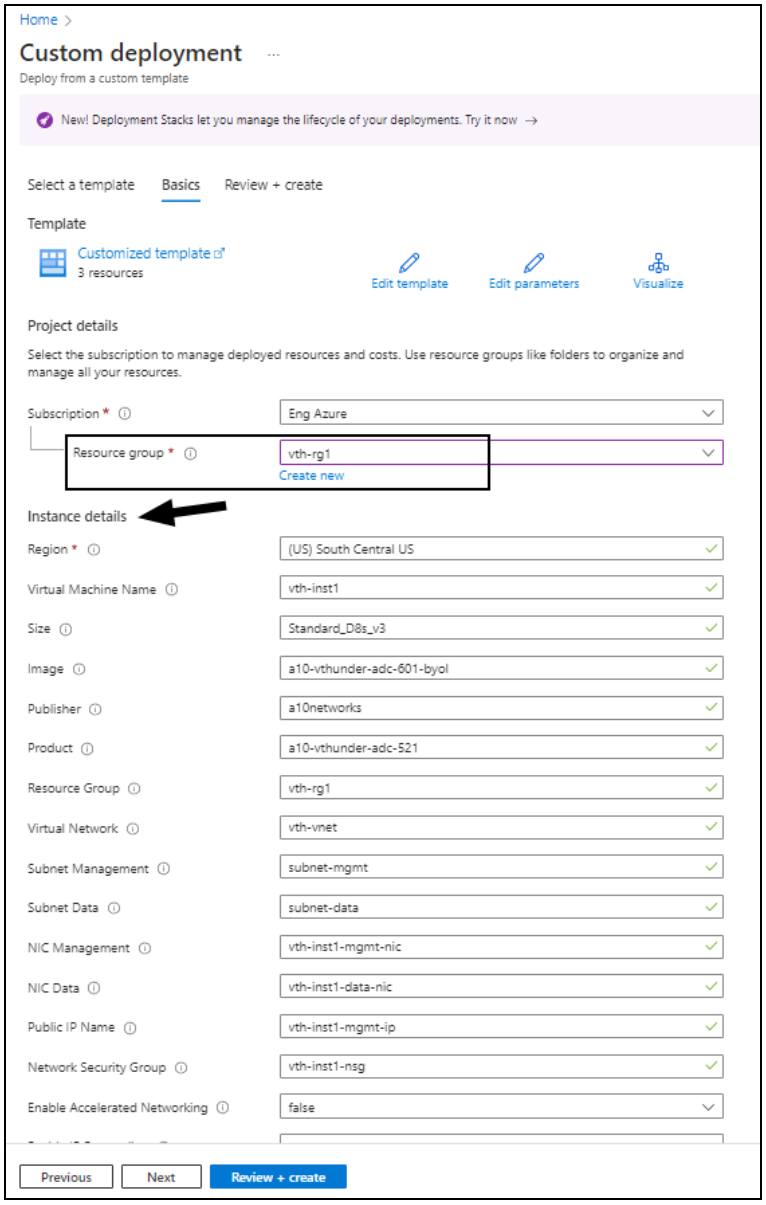
  Figure 4 : Edit template window



5. Click **Save**.

   The **Custom deployment** window is displayed with the template parameters and default values.

Figure 5 : Custom deployment template



6. Select an existing or create a new **Resource group** under which you want to deploy the custom template resources.

NOTE: Hover ⓘ for description of each corresponding parameter.

7. Update the default values and also provide the values in the empty fields as

appropriate in the **Instance details** section shown in Figure 5.

NOTE: Use a suitable VM size that supports at least two NICs. For VM sizes, Supported VM Sizes.

8. Click **Review+create**.

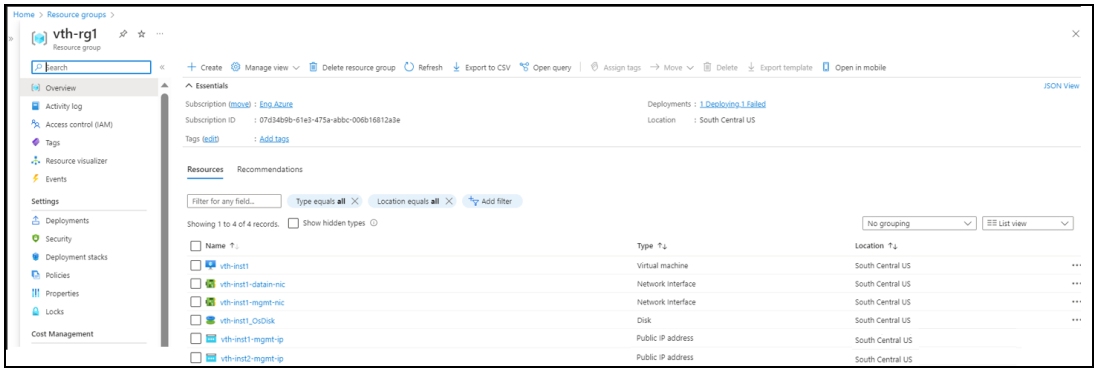
   The validation appears.

9. Click **Create**.

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

10. Verify if all the above listed resources are created under **Home** > **Azure services** > **Resource Groups** > <*resource_group_name*>.

Figure 6 : Resource listing under resource group



Execute using Azure CLI

To deploy the A10-vThunder-2NIC-1VM template using Azure CLI commands, perform the following steps:

1. Download A10-vThunder-2NIC-1VM template.

NOTE: This template contains pre-populated default values that can be modified as required and it does not create new virtual network, network security group, subnets, and Public IP.

2. From Windows Explorer, navigate to the folder where you have downloaded the ARM template.

3. Open the ARM_TMPL_2NIC_1VM_PARAM.json with a text editor.
4. Configure the following parameters as appropriate:

Table 3 : JSON Parameters

Resource Name	Description
Virtual Machine	Specify a virtual machine name for vThunder. `"Virtual Machine Name": { "value": "vth-inst1" },`
Size	Specify a suitable size for the vThunder instance that supports at least 2 NICs. For VM sizes, see Supported VM Sizes. `"Size": { "value": "Standard_D8s_v3" },`
Image	Specify the desired vThunder Image name and Product name from the Azure Marketplace. `"Image": { "value":"a10-vthunder-adc-601-byol" }, "Publisher": { "value": "a10networks" }, "Product": { "value": "a10-vthunder-adc-521" },` **NOTE:** Do NOT change the publisher name.
Resource Group	Specify the name of an existing resource group under which the virtual network, network security group, and subnets are already created.

Table 3 : JSON Parameters

Resource Name	Description

	<pre>"ResourceGroup": {
	  "value": "<existing VN NSG ResourceGroupName>"
	},</pre>

Virtual Network	Specify an existing virtual network name for vThunder.
	<pre>"Virtual Network": {
	  "value": "<existing virtual network name>"
	},</pre>

Management Subnet	Specify an existing subnet name that is available within the selected virtual network for inbound management traffic.
	<pre>"SubnetManagement": {
	  "value": "<existing subnet-mgmt name>"
	},</pre>

Data Subnet	Specify an existing subnet name that is available within a selected virtual network for inbound and outbound data traffic.
	<pre>"SubnetData": {
	  "value": "<existing subnet-data name>"
	},</pre>

Network Interface Cards	Specify a unique network interface card for management and data traffic.
	<pre>"NIC Management": {
	  "value": "vth-inst1-mgmt-nic"
	},
	"NIC Data": {
	  "value": "vth-inst1-data-nic"
	},</pre>

Public IP address	Specify an existing Public IP address for management traffic.

Table 3 : JSON Parameters

Resource Name	Description

	<pre>"Public IP Name": {
	  "value": "<existing Public IP Name>"
	},</pre>

Network Security Group	Specify an existing network security group name for all the NICs.
	<pre>"Network Security Group": {
	  "value": "<existing Network Security Group>"
	},</pre>

Enable Accelerated Networking	Specify 'true' to enable low latency and high throughput on the NICs. For more information, see Accelerated Networking.
	<pre>"Enable Accelerated Networking": {
	  "value": false
	},</pre>
	NOTE: By default, accelerated networking is disabled for all type of compute instances and it can be enabled only for certain compute instances. For the compatible compute instances, see Supported VM Sizes.

Enable IP Forwarding	Specify 'true' to allow the virtual machine to forward the network traffic between networks to improve the network performance. This high-performance forwarded path bypasses the host from the usual data path, thus, reducing latency, jitter, and CPU utilization when using the most demanding network workloads on the supported VM types. For more information, see IP Forwarding.
	<pre>"Enable IP Forwarding": {
	  "value": false
	}</pre>

Table 3 : JSON Parameters

Resource Name	Description
	NOTE: By default, IP forwarding is disabled.

5. Verify if all the configurations in the ARM_TMPL_2NIC_1VM_PARAM.json file are correct and then save the changes.
6. From Start menu, open PowerShell and navigate to the folder where you have downloaded the ARM template.
7. Run the following command to create an Azure resource group:

```
PS C:\Users\TestUser\Templates> az group create --name <resource_
group_name> --location "<location_name>"
```

Example:

```
PS C:\Users\TestUser\Templates> az group create --name vth-rg1 --
location "south central us"
 {
    "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/resourceGroups/vth-rg1",
    "location": "southcentralus",
    "managedBy": null,
    "name": "vth-rg1",
    "properties": {
      "provisioningState": "Succeeded"
    },
    "tags": null,
    "type": "Microsoft.Resources/resourceGroups"
  }
```

8. Run the following command to create an Azure deployment group.

```
PS C:\Users\TestUser\Templates> az deployment group create -g
<resource_group_name> --template-file <template_name> --parameters
<param_template_name>
```

Example:

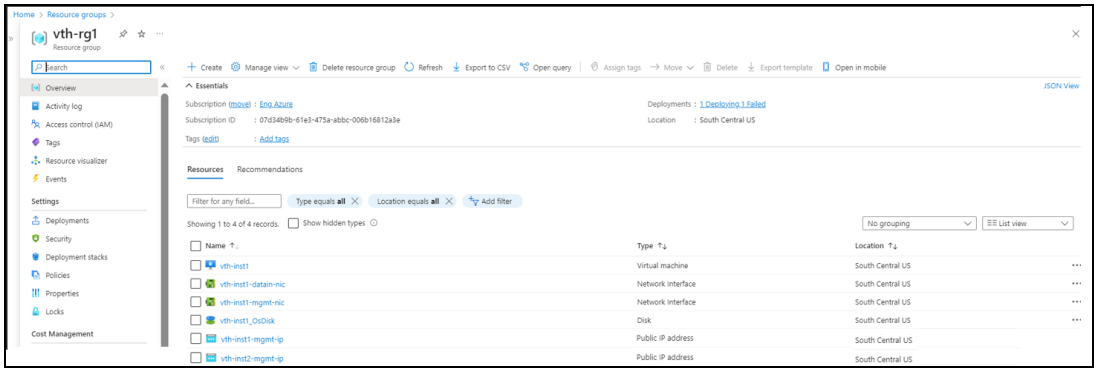
```
PS C:\Users\TestUser\Templates> az deployment group create -g vth-rg1
--template-file ARM_TMPL_2NIC_1VM.json --parameters ARM_TMPL_2NIC_
1VM_PARAM.json
```

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

NOTE: The resource group of the deployed vThunder instance and it's resources can be same or different from the resource group of virtual network, NSG, and Public IP.

9. Verify if all the above listed resources are created under **Home** > **Azure services** > **Resource Groups** > <*resource_group_name*>.

Figure 7 : Resource listing under resource group



Access Thunder Virtual Machine

The Thunder virtual machine can be accessed using any of the following ways:

- Access vThunder using CLI
- Access vThunder using GUI

Access vThunder using CLI

To access vThunder using CLI, perform the following steps:

1. Open any SSH client.
2. Enter or select the following basic information in the configuration window:
   - Hostname: Public IPv4 address
     Here, Public IP of **`vth-inst1`**.

- Username: Enter username provided by A10 Networks Support
- Password: Enter password provided by A10 Networks Support

3. Connect to the session.

   If the session connection is successful, the following response is displayed:

```
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--->
```

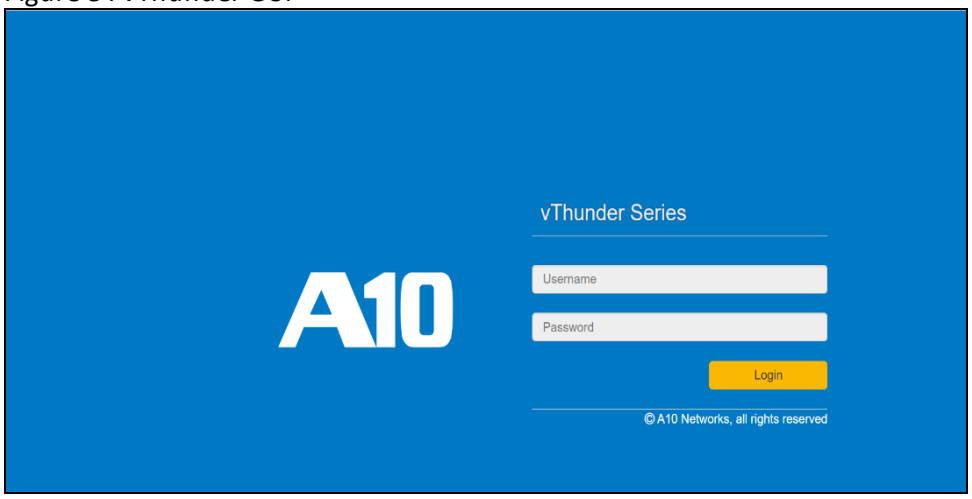
   The vThunder instance is ready to use.

Access vThunder using GUI

To access vThunder using GUI, perform the following steps:

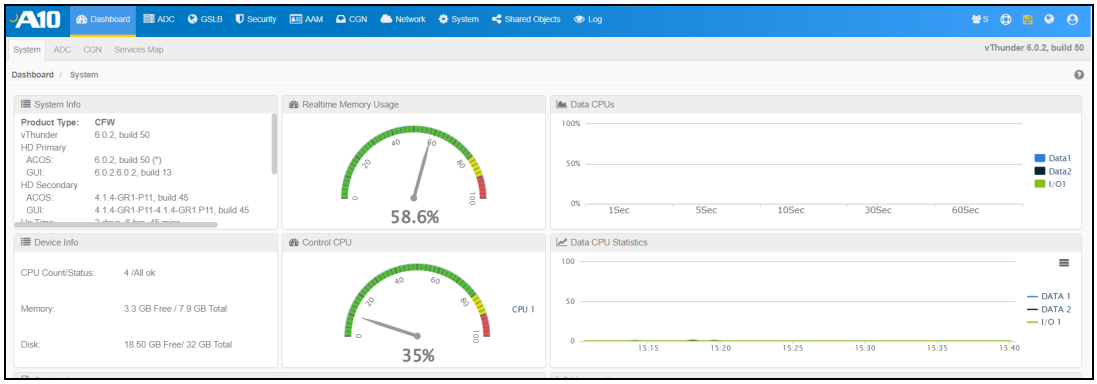
1. Open any browser.
2. Enter *https://<vthunder_public_IP>/gui/auth/login/* in the address bar.

   Figure 8 : vThunder GUI



3. Enter the username and password provided by A10 Networks Support. The home page gets displayed.

Figure 9 : Home page



Configure Server and Client Machine

The following topics are covered:

- Create and Configure a Server Machine
- Create and Configure a Client Machine

Create and Configure a Server Machine

To create a Server machine, perform the following steps:

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

   Project details

   - Subscription
   - Resource group

   Instance details

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

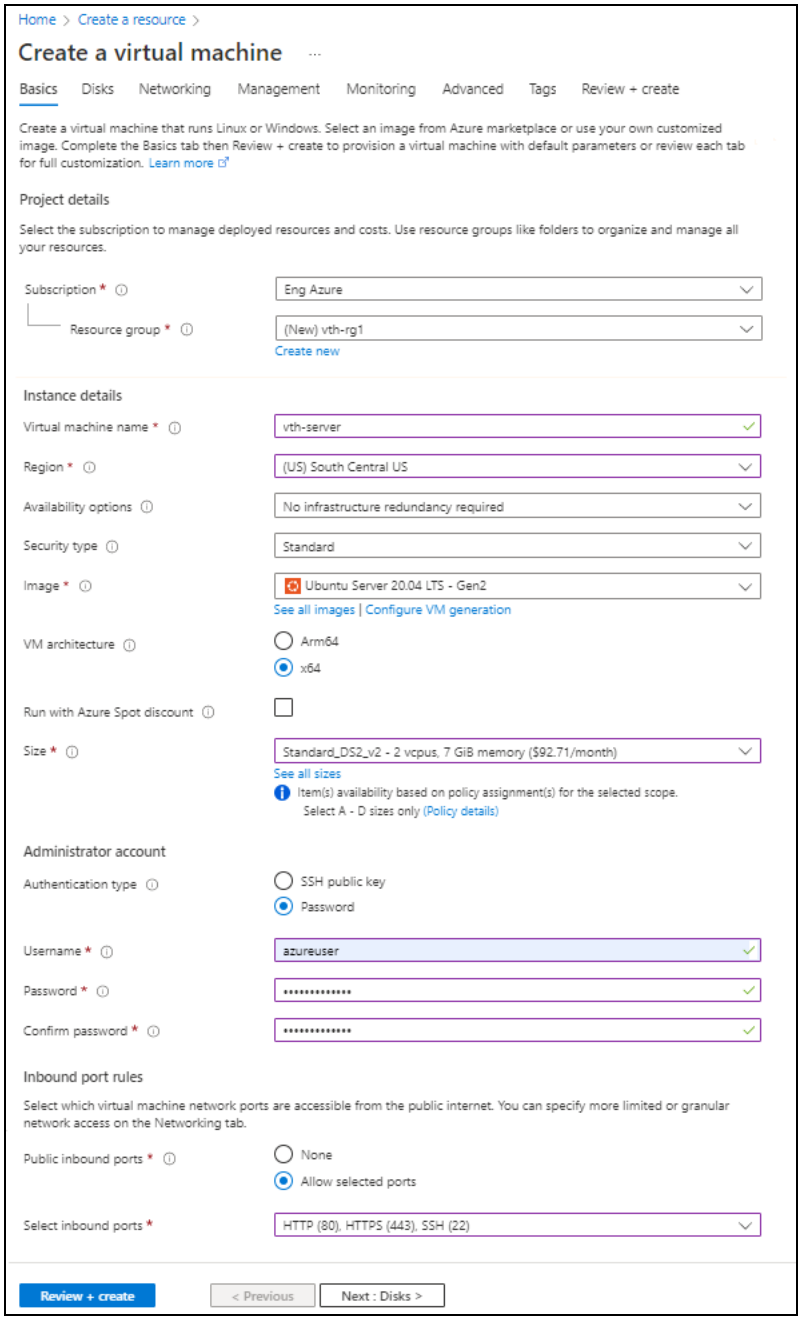
Administrator account

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

Inbound port rules

- Public inbound ports
- Select inbound ports

Figure 10 : Create a virtual machine window - Basics tab



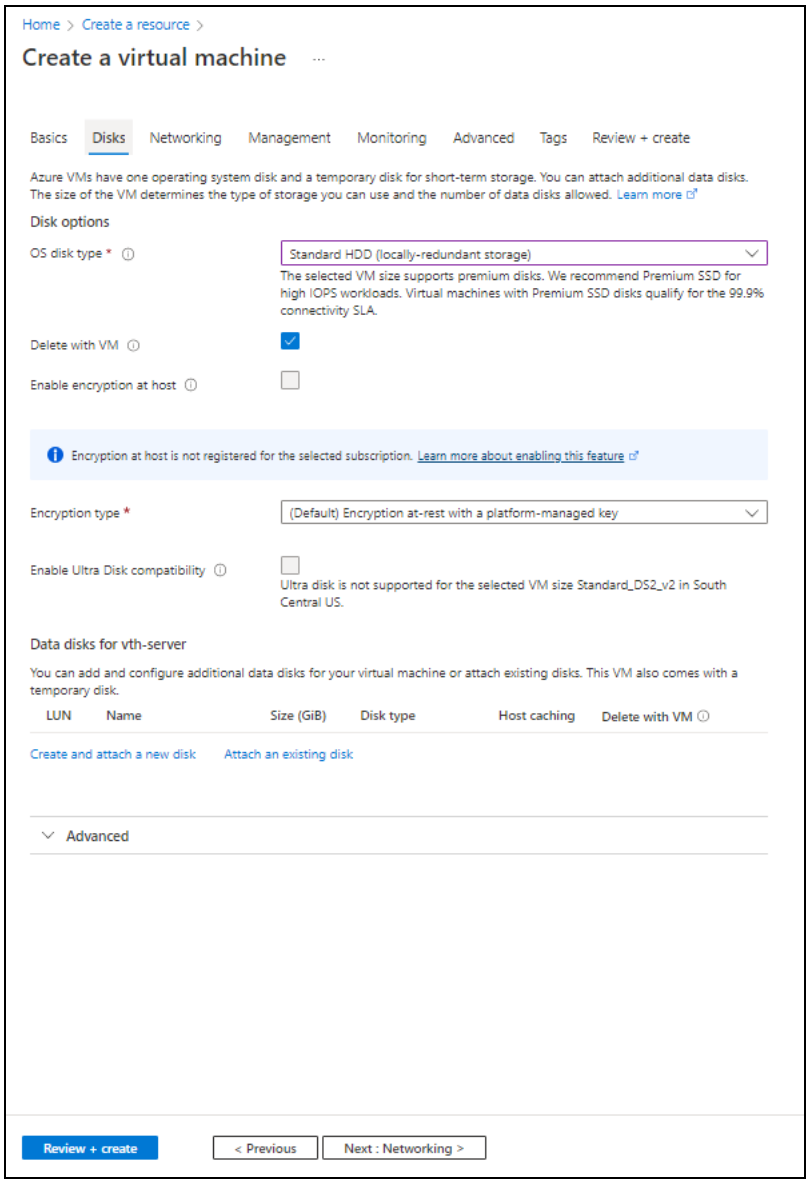
3. Leave the values in other fields unchanged and click **Next : Disks** at the bottom of the window.

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

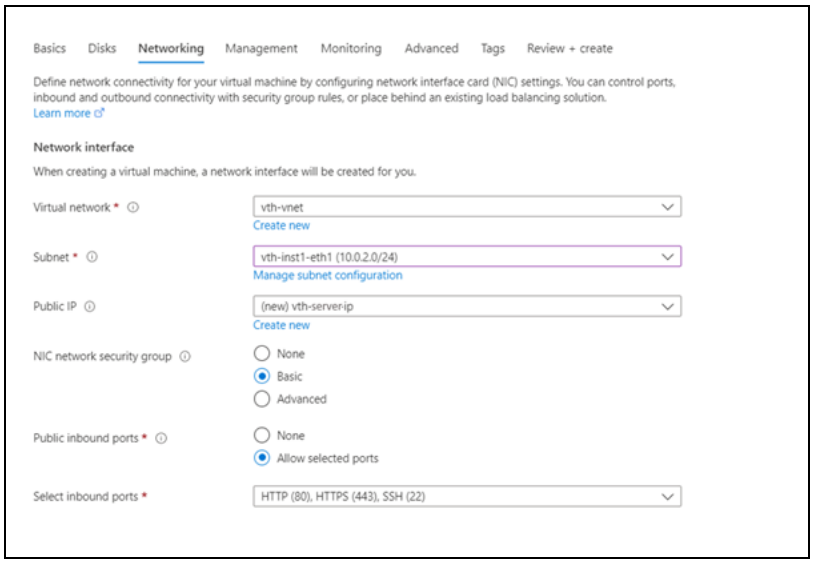


5. Leave the values in other fields unchanged and click **Next : Networking** at the bottom of the window.
6. Select or enter the following mandatory information in the **Networking** tab:

   Network interface

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

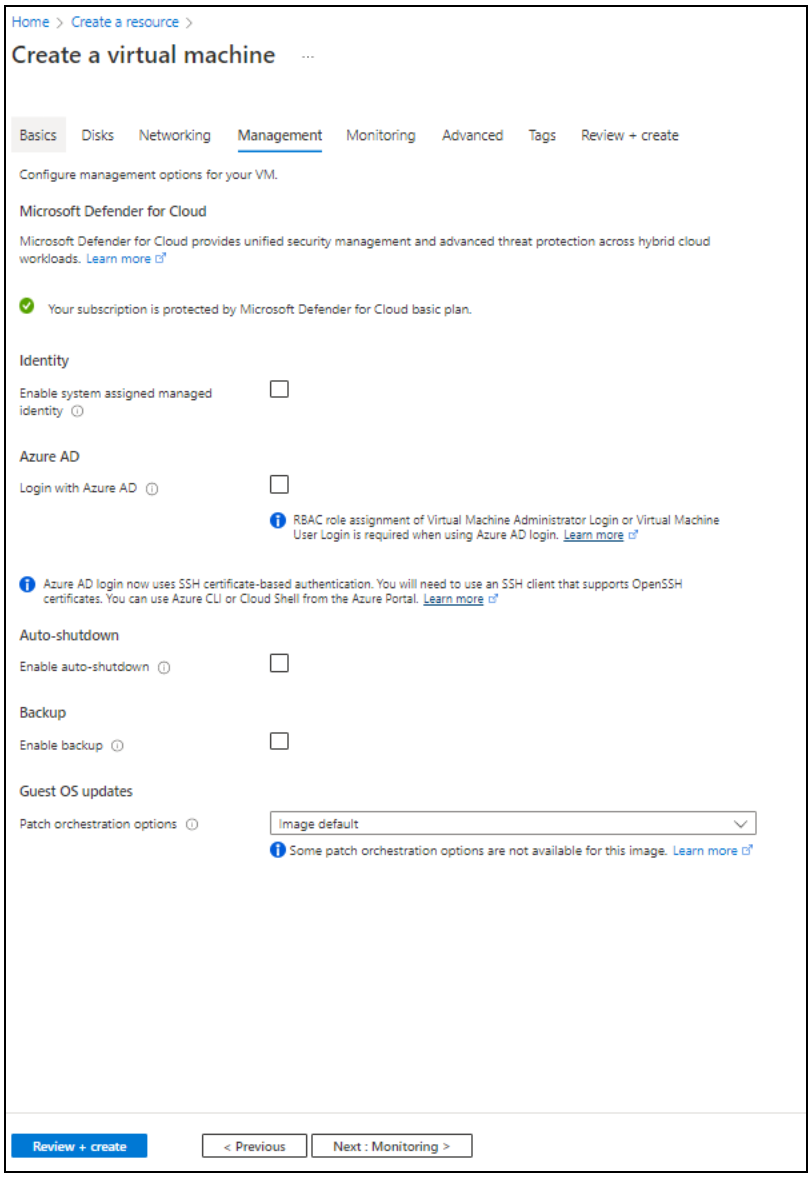
   Figure 12 : Create a virtual machine window - Networking tab



7. Leave the values in other fields unchanged and click **Next : Management** at the bottom of the window.

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

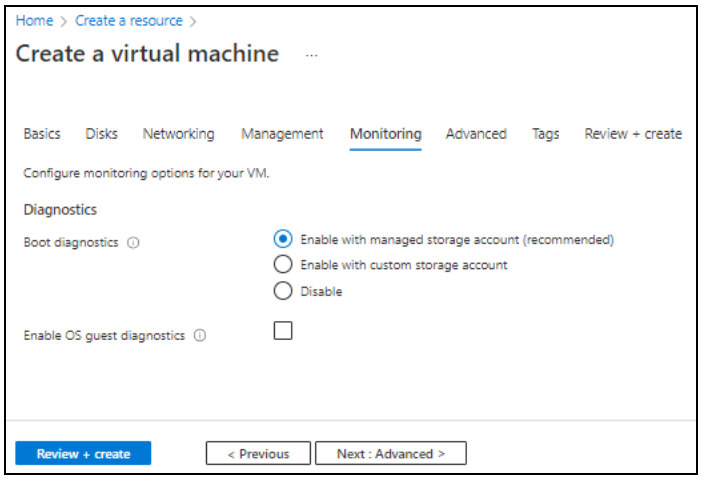
Figure 13 : Create a virtual machine window - Management tab



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

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

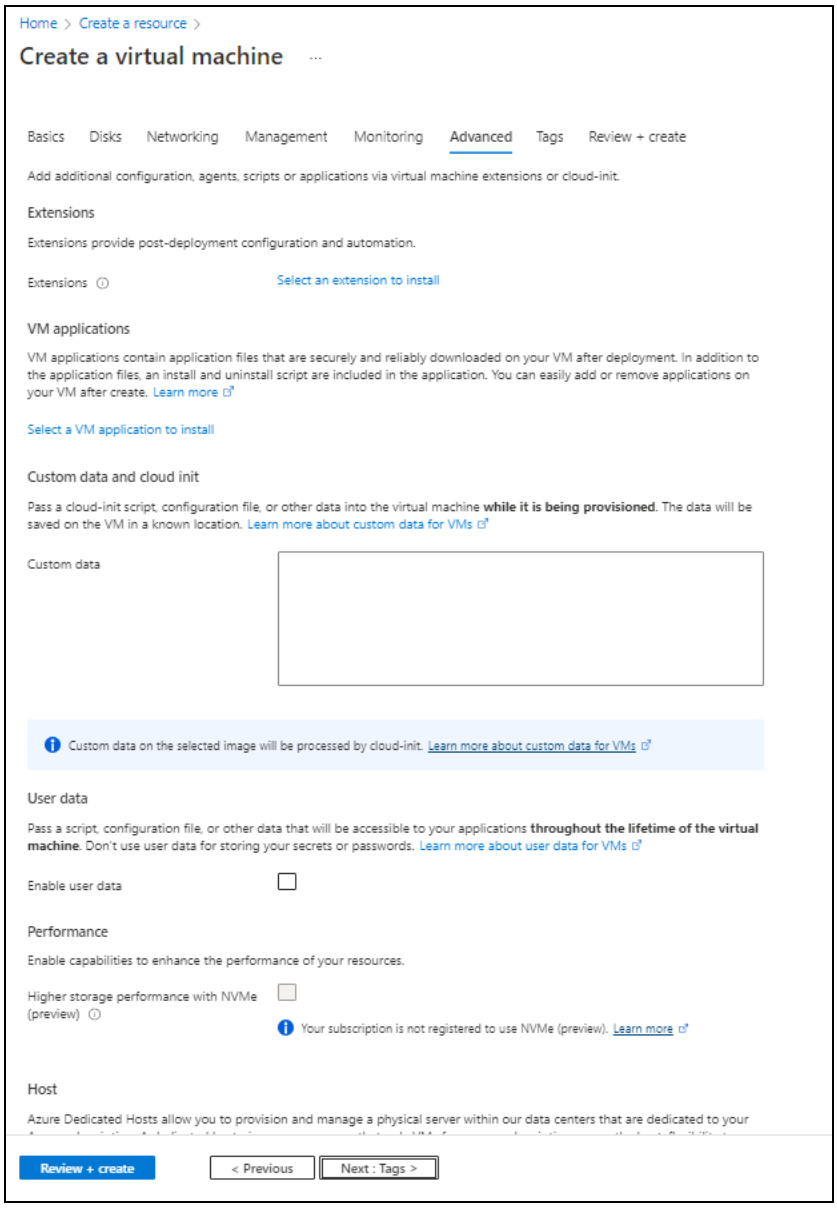
Figure 14 : Create a virtual machine window - Monitoring tab



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

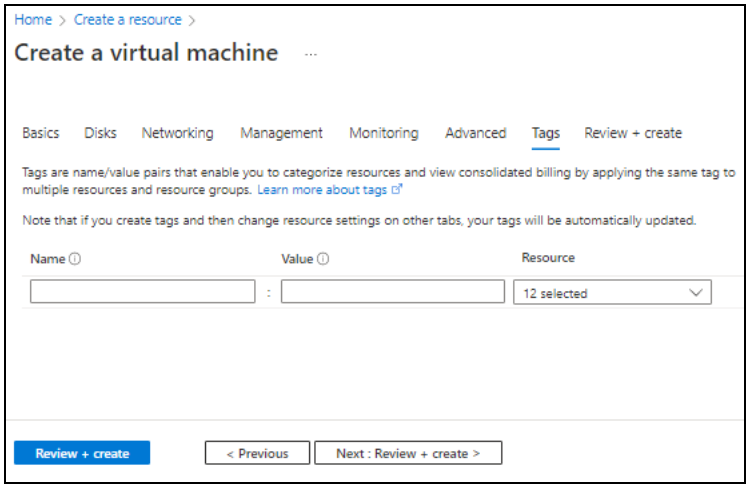
12. Select or enter the additional configuration in the **Advanced** tab as needed.

Figure 15 : Create a virtual machine window - Advanced tab



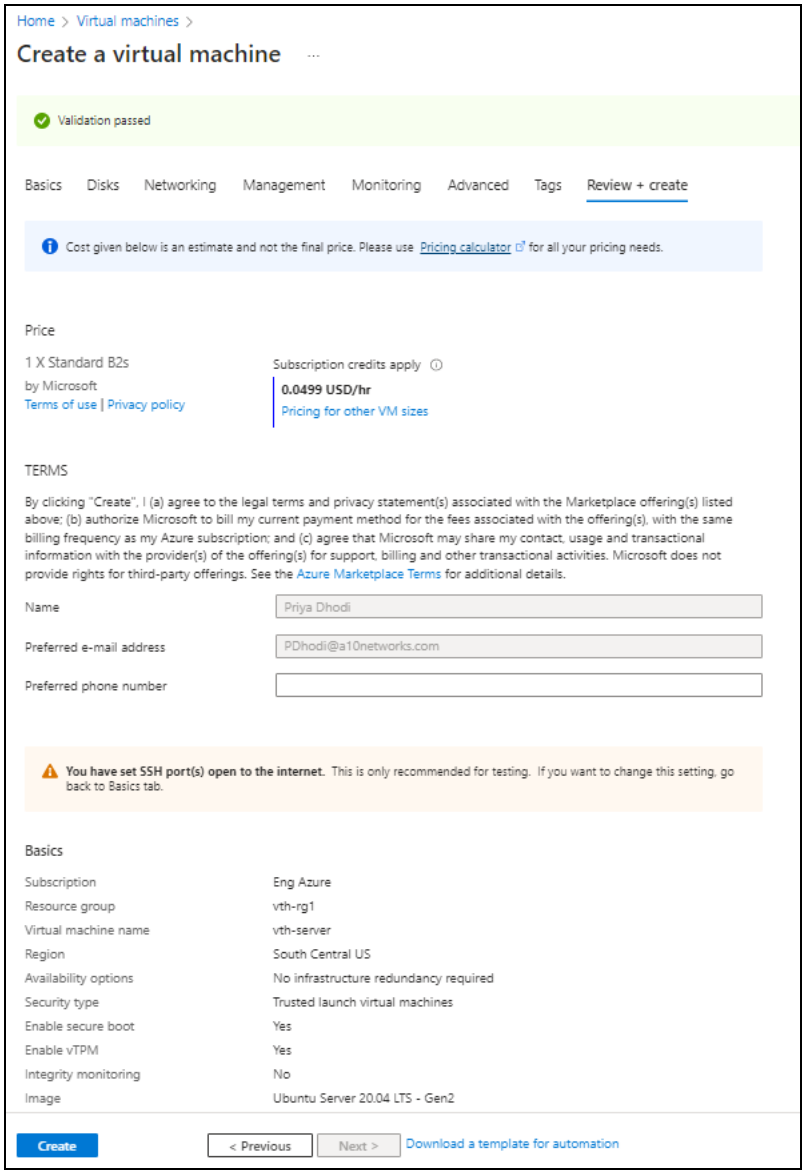
13. Click **Next : Tags** at the bottom of the window.
14. Select or enter the information to categorized resources in the **Tags** tab as needed.

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

```
sudo apt install apache2
```

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

18. If you want to configure HTTP template, perform the following steps:

    a. SSH the Apache Server and run the following command:

    ```
    sudo vim /etc/apache2/apache2.conf
    ```

    The Apache2 configuration file is displayed.

    b. Add the following configuration and save the file:

    ```
    Alias /<url-match-string> /var/www/html
    ```

    c. Restart the Apache server to enable the HTTP service.

    ```
    sudo systemctl restart apache2
    ```

    The server may take a few minutes to restart.

Create and Configure a Client Machine

To create a Client machine, perform the following steps:

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

   Project details

   - Subscription
   - Resource group

   Instance details

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

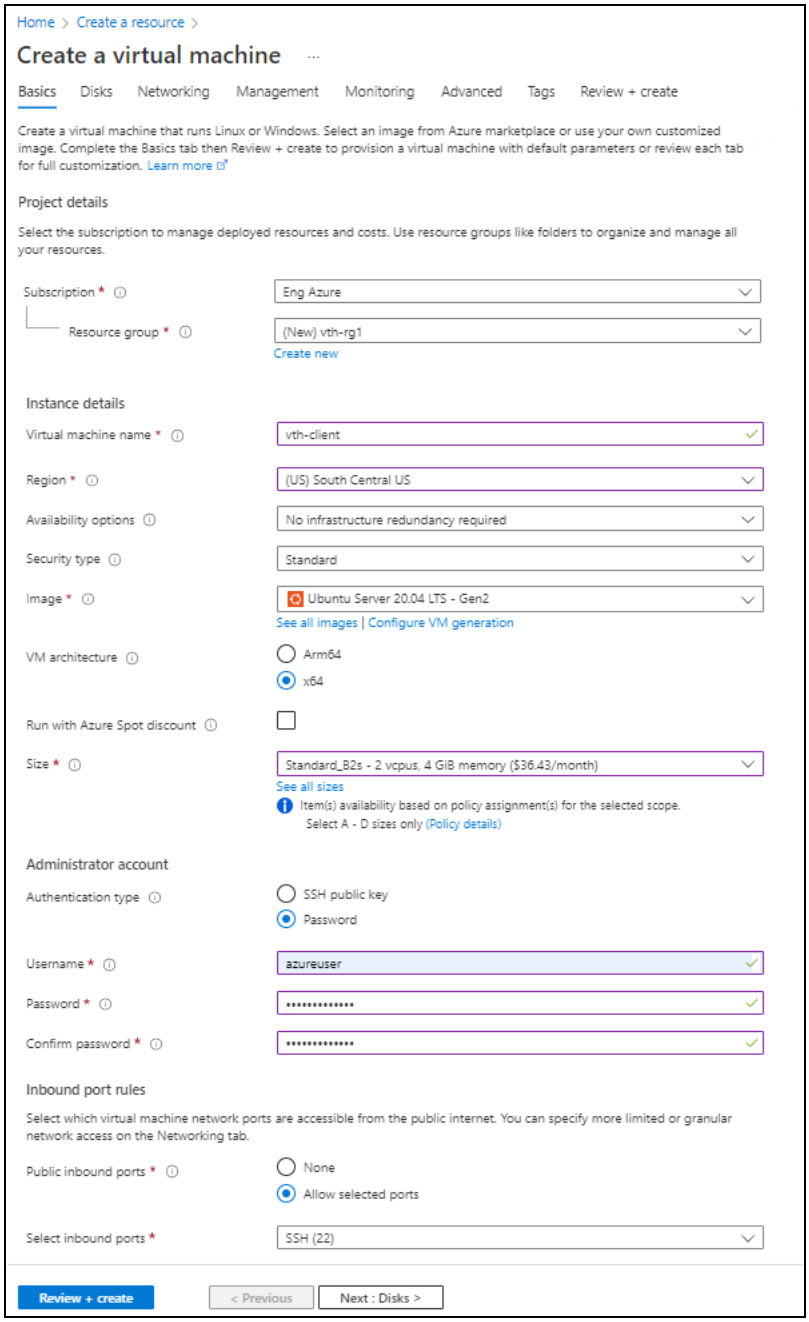
   Administrator account

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

Inbound port rules

- Public inbound ports
- Select inbound ports

Figure 18 : Create a virtual machine window - Basics tab



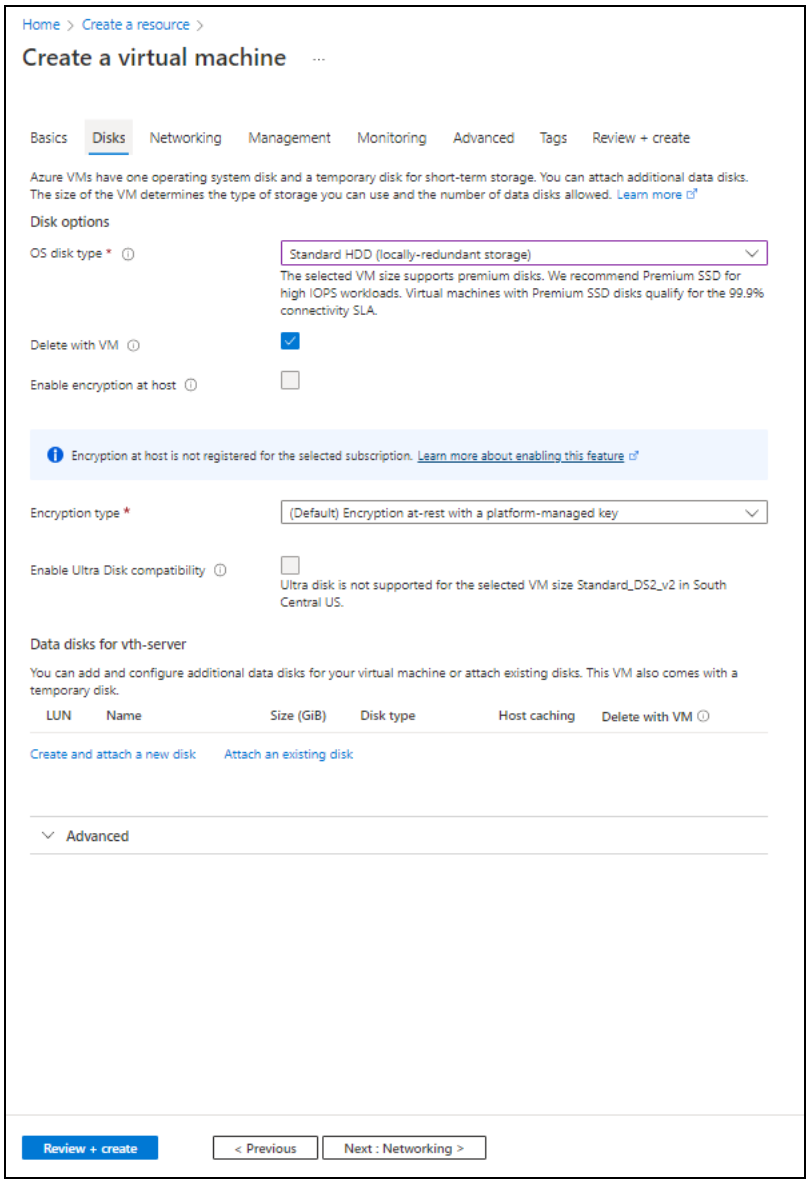
3. Leave the values in other fields unchanged and click **Next : Disks** at the bottom of the window.

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

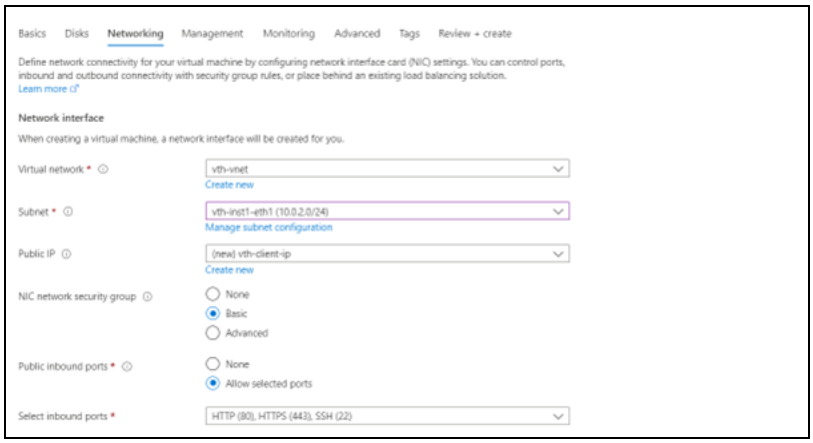


5. Leave the values in other fields unchanged and click **Next : Networking** at the bottom of the window.
6. Select or enter the following mandatory information in the **Networking** tab:

   Network interface

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

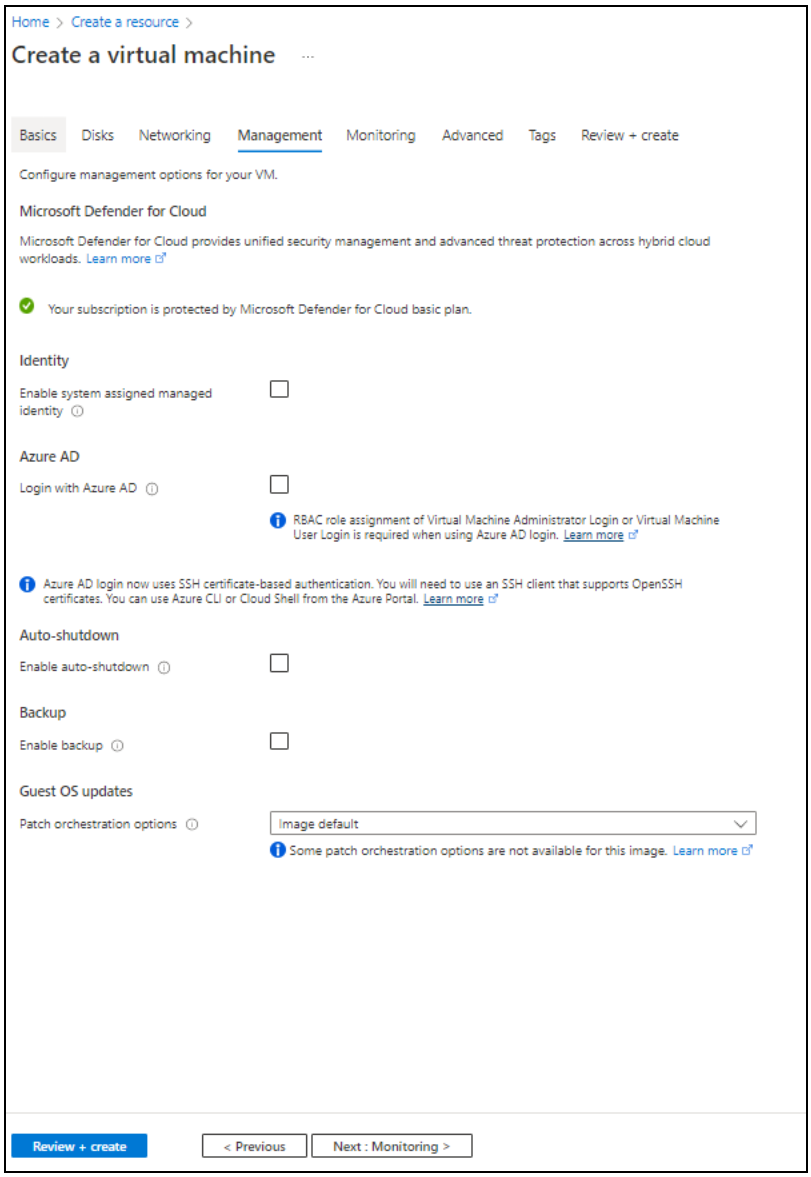
   Figure 20 : Create a virtual machine window - Networking tab



7. Leave the values in other fields unchanged and click **Next : Management** at the bottom of the window.

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

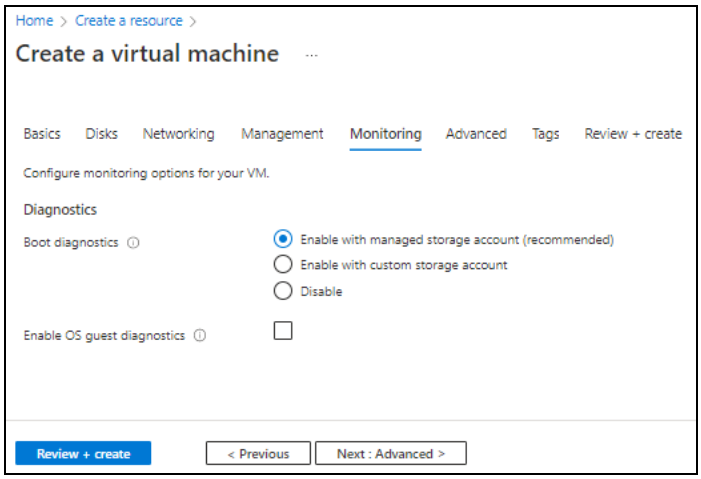
Figure 21 : Create a virtual machine window - Management tab



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

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

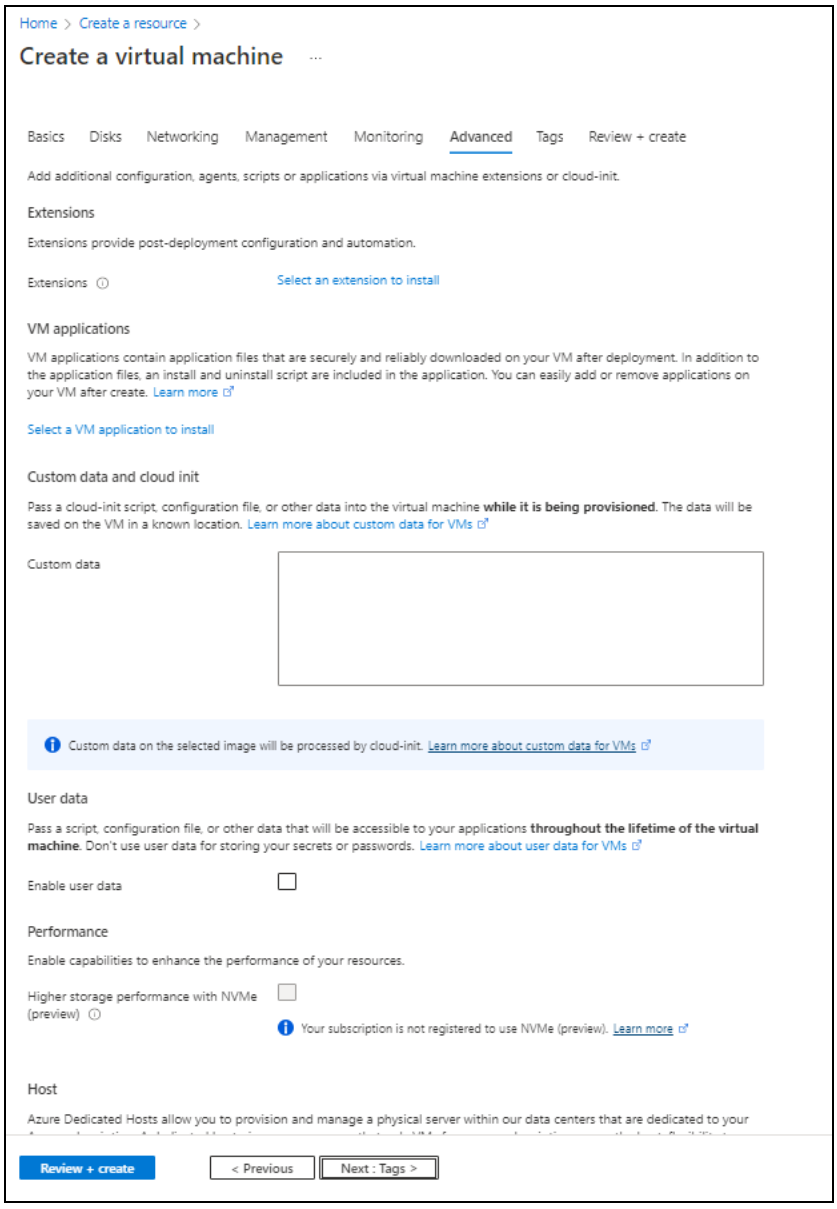
Figure 22 : Create a virtual machine window - Monitoring tab



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

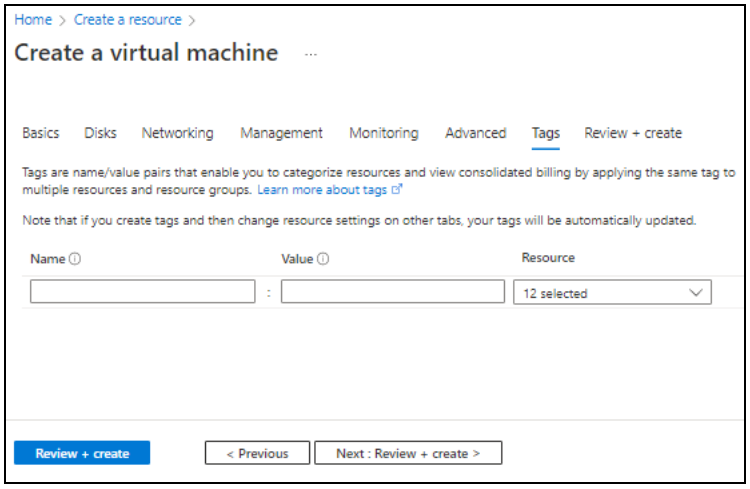
12. Select or enter the additional configuration in the **Advanced** tab as needed.

Figure 23 : Create a virtual machine window - Advanced tab



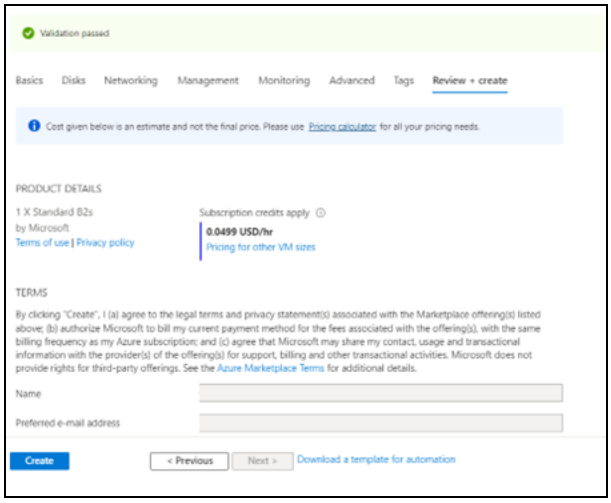
13. Click **Next : Tags** at the bottom of the window.
14. Select or enter the information to categorized resources in the **Tags** tab as needed.

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 Thunder

The following configurations can be applied to the deployed vThunder instance:

- Change Password
- A10 License
- SSL Certificate
- Basic Server Load Balancer

Verify Deployment

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

1. Run the following command on the vThunder instance to verify SLB configuration:

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

If the deployment is successful with basic SLB, HTTP template, and Persist-cookie template configuration, the following output is displayed:

```
!
interface ethernet 1
  enable
  ip address dhcp
!
!
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 template persist cookie persist-cookie
```

```
  expire 60
  encrypt-level 0
  name a10-cookies
  match-type service-group
!
slb template http hostname-test
  host-switching contains s1 service-group sg80
!
slb template http url-test
  url-switching regex-match s1 service-group sg80
!
slb virtual-server vip 10.0.2.9
  port 53 udp
    source-nat auto
    service-group sg53
  port 80 http
    source-nat auto
    service-group sg80
    template persist cookie persist-cookie
    template http url-test
  port 443 https
    source-nat auto
    service-group sg443
!
!
end
```

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

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

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

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

3. Run the following command on the vThunder instance to verify GLM configuration:

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

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

```
Host ID         : 5DCB01EC264BECCCFECB3C2ED42E02384EE8C527
USB ID          : Not Available
Billing Serials: A10f771cecbe0000
Token           : A10f771cecbe
Product         : ADC
Platform        : vThunder
Burst           : Disabled
GLM Ping Interval In Hours : 24
-----------------------------------------------------------------
Enabled Licenses Expiry Date             Notes
-----------------------------------------------------------------
SLB              None
CGN              None
GSLB             None
RC               None
DAF              None
WAF              None
AAM              None
FP               None
WEBROOT          N/A         Requires an additional Webroot license.
THREATSTOP       N/A         Requires an additional ThreatSTOP license.
QOSMOS           N/A         Requires an additional QOSMOS license.
WEBROOT_TI       N/A         Requires an additional Webroot Threat Intel
license.
CYLANCE          N/A         Requires an additional Cylance license.
IPSEC_VPN        N/A         Requires an additional IPsec VPN license.
25 Mbps Bandwidth 21-December-2022
```

Verify Traffic Flow

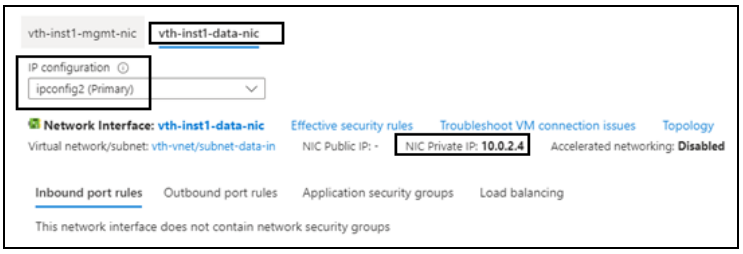
To verify the traffic flow from client machine to server machine through vThunder instance, perform the following:

1. From **Azure Portal** > **Azure services** > **Resource Group** > <*resource_group_name*> > <*virtual_machine_instance*> > **Settings** > **Networking**.

   Here, **`vth-inst1`** is the vThunder instance name.

2. Select the Data NIC tab > **IP configuration** > **`ipconfig2 (primary)`**. Here, Data NIC is **`vth-inst1-data-nic`**.

   Figure 26 : vThunder instance Data Subnet Private IP



3. Select your client instance from the **Virtual machine** list.

   Here, **`vth-client`** is the client instance name.

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

   ```
   curl <vThunder_instance_data-nic_private_ip>
   ```

   Example

   ```
   curl 10.0.2.4
   ```

   Verify if a response is received from client server (For example: Apache Index page).

5. SSH your client machine and run the following command to verify the HTTP template traffic flow:

   ```
   curl <vThunder_instance_data-nic_private_ip>:<port_number>/<host-match-string or url-match-string>/
   ```

   Example

   ```
   curl 10.0.2.4:80/s1/
   ```

   Verify if a response is received from client server (For example: Apache Index page).

6. SSH your client machine and run the following commands to verify the Persist

cookie template traffic flow:

a. Verify the current cookie configuration:

```
curl --head <vThunder_instance_data-nic_private_ip>
```

b. Run the following commands to save the cookies in the **cookie.txt** file:

```
curl -b cookie.txt -c cookie.txt <vThunder_instance_data-nic_
private_ip>
cat cookie.txt
```

Example

```
curl --head 10.0.2.4
curl -b cookie.txt -c cookie.txt 10.0.2.4
cat cookie.txt
```

7. Run the following command on the vThunder instance to view the persistence load-balancing statistics:

```
vThunder(config)#show slb persist
```

If the deployment is successful, the following summary persistence statistics is displayed:

```
                                        Total
-----------------------------------------------
URL hash persist (pri)                   0
URL hash persist (sec)                   0
URL hash persist fail                    0
SRC IP persist ok                        0
SRC IP persist fail                      0
SRC IP hash persist(pri)                 0
SRC IP hash persist(sec)                 0
SRC IP hash persist fail                 0
DST IP persist ok                        0
DST IP persist fail                      0
DST IP hash persist(pri)                 0
DST IP hash persist(sec)                 0
DST IP hash persist fail                 0
SSL SID persist ok                       0
SSL SID persist fail                     0
Cookie persist ok                        1
Cookie persist fail                      0
Persist cookie not found                 2
Persist cookie Pass-thru                 0
Enforce higher priority                  0
```

If the Persist-cookie configuration is successful, a value is displayed for the **`Cookie persist ok`** parameter else the value is 0.

Thunder-3NIC-2VM-PVTVIP

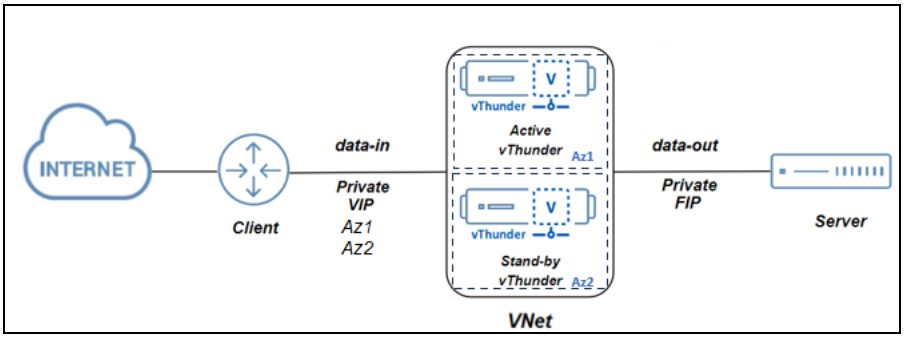
This template creates two vThunder instances with HA setup and each vThunder has one management and two data NICs (data-in and data-out). It configures data-in network interface card (NIC) with Private IP on VIP.

High availability can be configured within the same or different availability zone within a same region. If one instance goes down, other instance takes the request without any manual intervention.

For more information, see Create Thunder Virtual Machines.

NOTE: Use a suitable VM size that supports at least three NICs. For VM sizes, see Supported VM Sizes.

Figure 27 : SLB Thunder ADC in High Availability mode with Private VIP

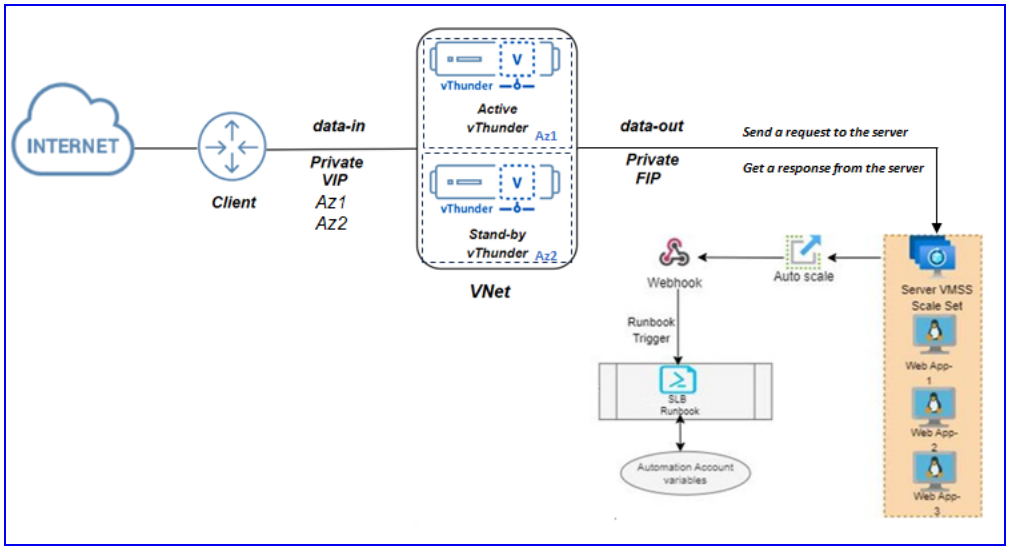


Additional Thunder configurations are available that can be applied as needed:

- Change Password
- A10 License
- SSL Certificate

- Basic Server Load Balancer
- High Availability

Figure 28 : SLB Thunder ADC in High Availability mode with Private VIP and Backend Server Autoscale



Following are the Thunder configurations can be applied:

- Change Password
- A10 License
- SSL Certificate
- Server Load Balancer on Backend Autoscale
- High Availability

Various templates are available for different deployment needs.

For more information, see Deployment Templates.

The following topics are covered:

Create Thunder Virtual Machines

The A10-vThunder-3NIC-2VM-PVTVIP template is used to create two Thunder virtual machines with three network interface cards each and configure the data-in network interface card with Private IP on VIP.

Before deploying this template, it is recommended to review the Prerequisites.

vThunder instances should have the same versions; otherwise, traffic flow will be disrupted.

There are two ways to deploy this template:

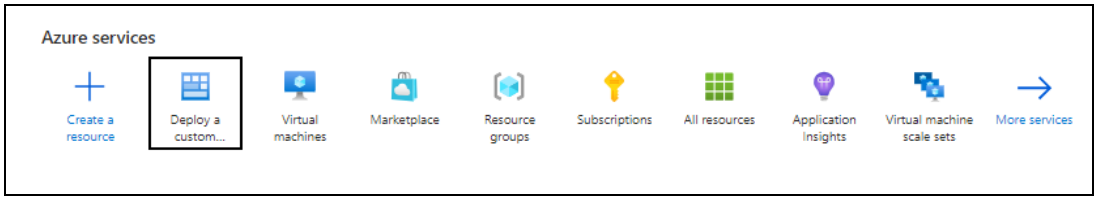
- Upload using Azure Portal Console
- Execute using Azure CLI

Upload using Azure Portal Console

To deploy the A10-vThunder-3NIC-2VM-PVTVIP template using Azure Portal Console, perform the following steps:

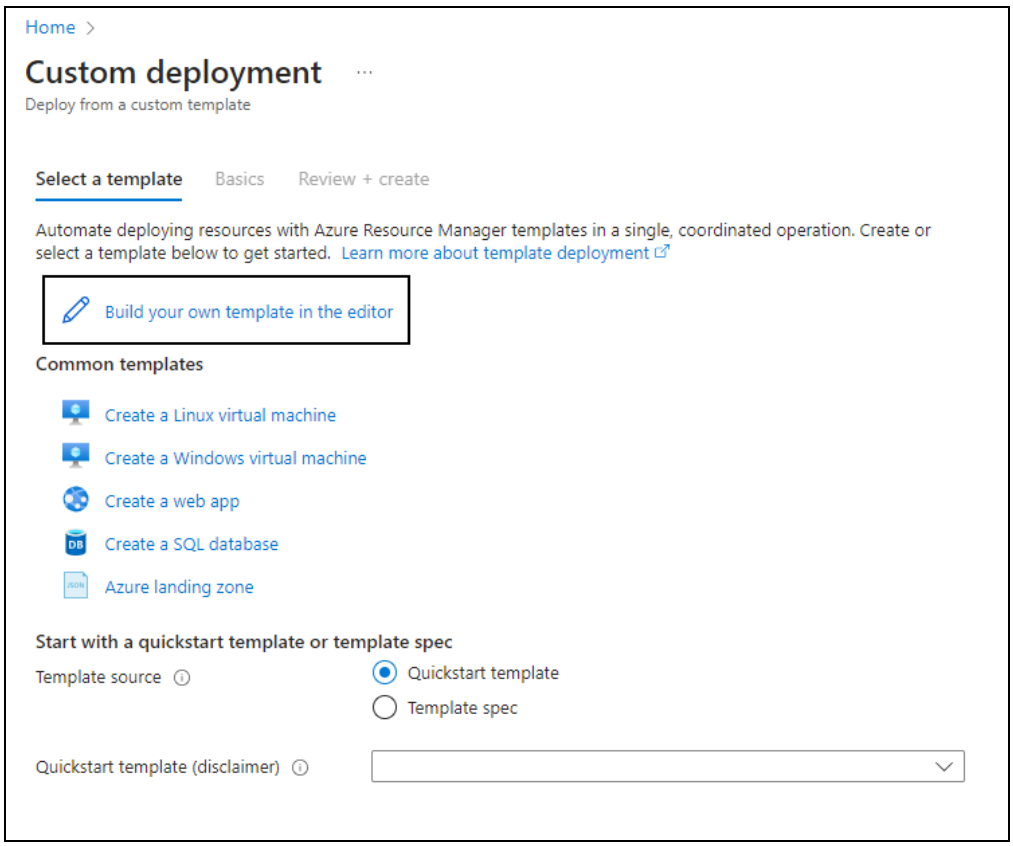
1. Download A10-vThunder-3NIC-2VM-PVTVIP template.
2. From the **Azure Portal** > **Azure services**, click **Deploy a custom template**.

Figure 29 : Azure services



3. Under the **Custom deployment** window > **Select a template** tab, click **Build your own template in the editor**.

Figure 30 : Custom deployment window

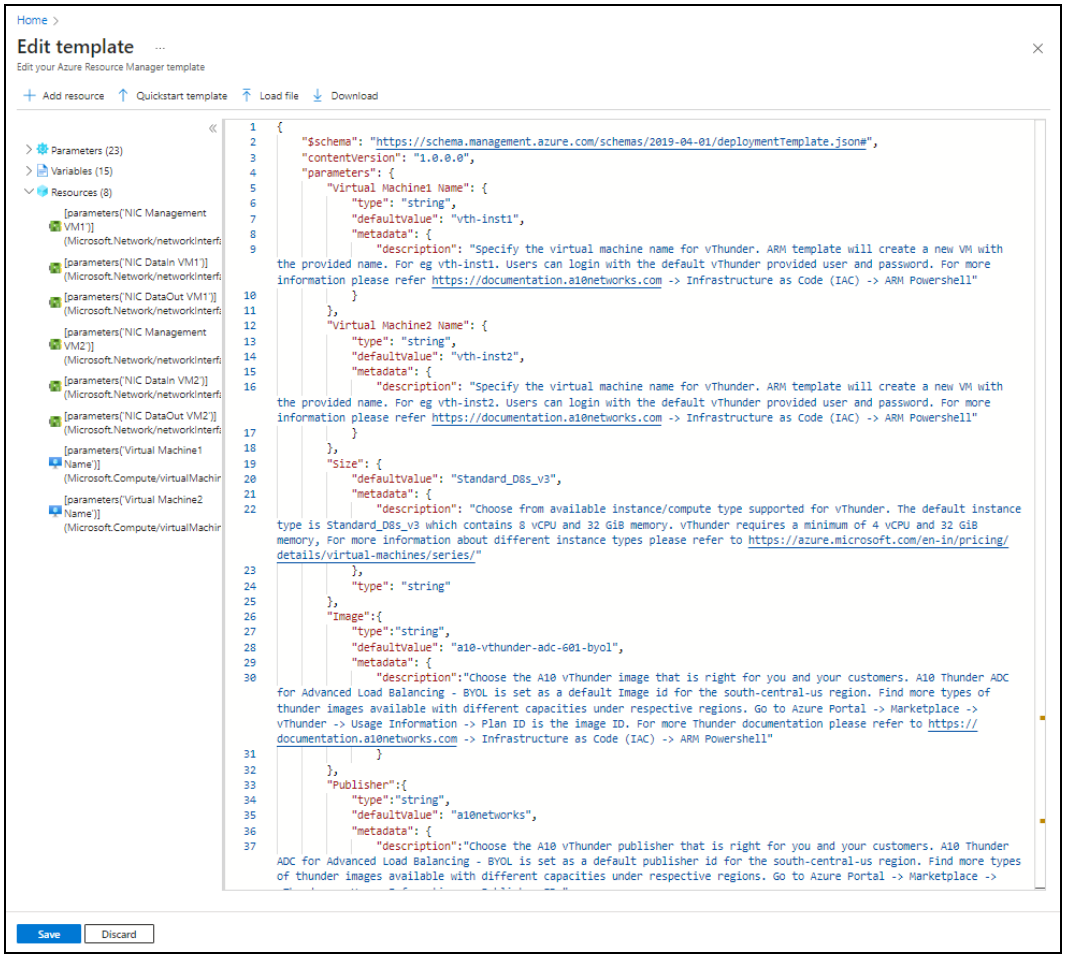


4. From the **Edit template** window, perform either of the following step:

   - Click **Load file** and browse to the folder where you have downloaded the ARM template. Select **ARM_TMPL_3NIC_2VM_PVTVIP.json** to upload.

- From Windows Explorer, navigate to the folder where you have downloaded the ARM template. Copy **ARM_TMPL_3NIC_2VM_PVTVIP.json** content and paste it in the editor.

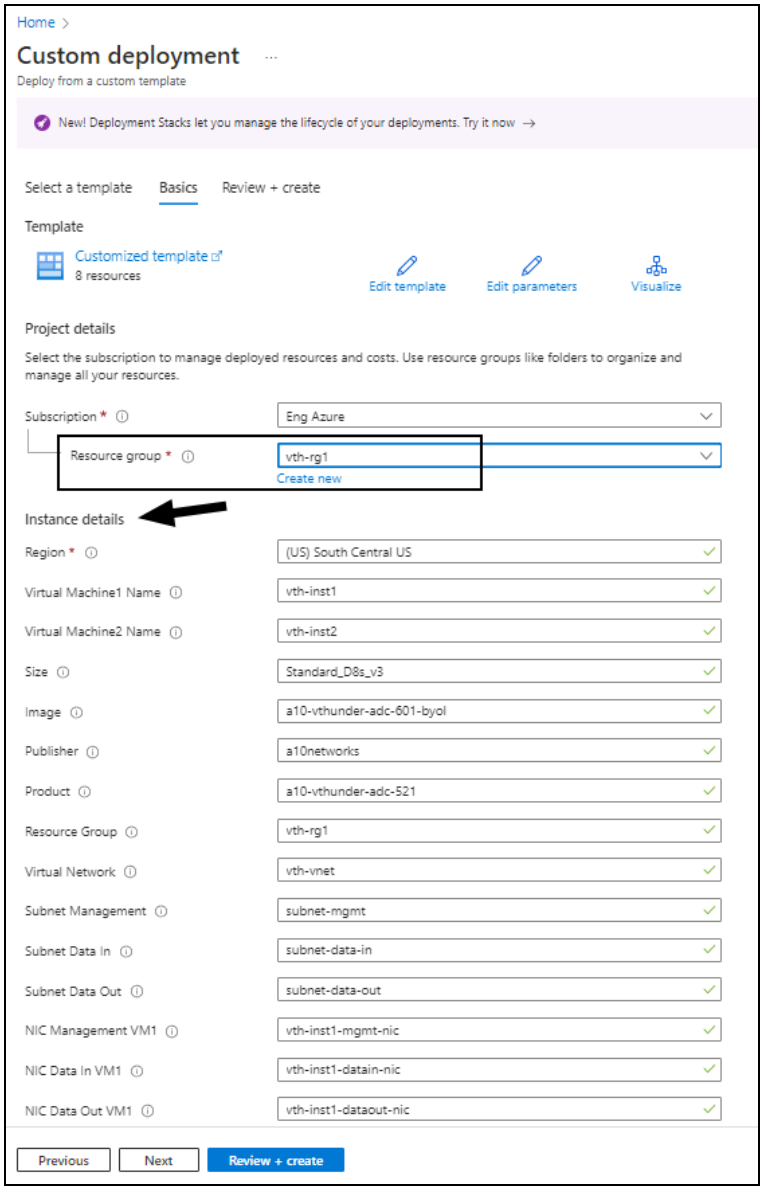
  Figure 31 : Edit template window



5. Click **Save**.

   The **Custom deployment** window is displayed with the template parameters and default values.

Figure 32 : Custom deployment template



6. Select an existing or create a new **Resource group** under which you want to deploy the custom template resources.

NOTE: Hover ⓘ for description of each corresponding parameter.

7. Update the default values and also provide the values in the empty fields as

appropriate in the **Instance details** section shown in Figure 32.

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

8. Click **Review+create**.

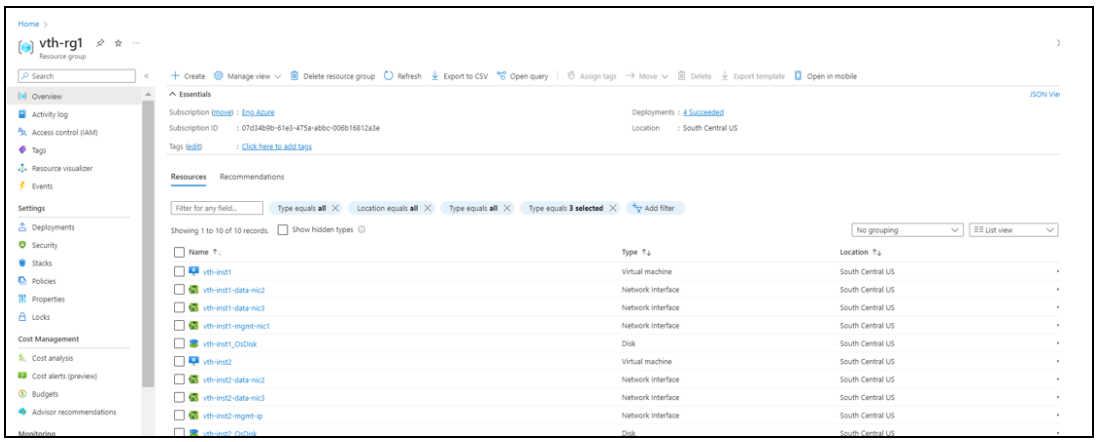
   The validation appears.

9. Click **Create**.

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

10. Verify if all the above listed resources are created under **Home** > **Azure services** > **Resource Groups** > <*resource_group_name*>.

Figure 33 : Resource listing under resource group



Execute using Azure CLI

To deploy the A10-vThunder-3NIC-2VM-PVTVIP template using Azure CLI commands, perform the following steps:

1. Download A10-vThunder-3NIC-2VM-PVTVIP template.

NOTE: This template contains pre-populated default values that can be modified as required and it does not create new virtual network, network security group, subnets, and Public IP.

2. From Windows Explorer, navigate to the folder where you have downloaded the ARM template.
3. Open the ARM_TMPL_3NIC_2VM_PVTVIP_PARAM.json with a text editor.
4. Configure the following parameters as appropriate:

Table 4 : JSON Parameters

Resource Name	Description

Virtual Machines	Specify a virtual machine name for each of the two vThunder instances.
	`"Virtual Machine1 Name": {`
	`"value": "vth-inst1"`
	`},`
	`"Virtual Machine2 Name": {`
	`"value": "vth-inst2"`
	`}`

Virtual Machine Zones	Specify an availability zone in which to deploy your virtual machine. If you have an existing Public IP, then it should be available in the same availability zone as the virtual machine.
	`"Virtual Machine1 Zone": {`
	`"value": "1"`
	`},`
	`"Virtual Machine2 Zone": {`
	`"value": "1"`
	`},`

Size	Specify a suitable size for the vThunder instance that supports at least 3 NICs. For VM sizes, see Supported VM Sizes.
	`"Size": {`
	`"value": "Standard_D8s_v3"`
	`},`

Image	Specify the desired vThunder Image name and Product name from the Azure Marketplace.

Table 4 : JSON Parameters

Resource Name	Description

	<pre>"Image": {
	"value":"a10-vthunder-adc-601-byol"
	},
	"Publisher": {
	"value": "a10networks"
	},
	"Product": {
	"value": "a10-vthunder-adc-521"
	},</pre>
	NOTE: Do not change the publisher name.

Resource Group	Specify the name of an existing resource group under which the virtual network, network security group, and subnets are already created.
	<pre>"ResourceGroup": {
	"value": "<existing VN NSG ResourceGroupName>"
	},</pre>

Virtual Network	Specify an existing virtual network name for vThunder.
	<pre>"Virtual Network": {
	"value": "<existing virtual network name>"
	},</pre>

Management Subnet	Specify an existing subnet name that is available within the selected virtual network for inbound management traffic.
	<pre>"SubnetManagement": {
	"value": "<existing subnet-mgmt name>"
	},</pre>

Data Subnet	Specify an existing subnet name that is available within a selected virtual network for inbound and outbound data traffic.

Table 4 : JSON Parameters

Resource Name	Description

	"SubnetDataIn": {
	"value": "<existing subnet-data-in name>"
	},
	"SubnetDataOut": {
	"value": "<existing subnet-data-out name>"
	},

Network Interface Cards	Specify a unique network interface card for management, datain, and dataout traffic.
	"NIC Management VM1": {
	"value": "vth-inst1-mgmt-nic"
	},
	"NIC Management VM2": {
	"value": "vth-inst2-mgmt-nic"
	},
	"NIC DataIn VM1": {
	"value": "vth-inst1-datain-nic"
	},
	"NIC DataOut VM1": {
	"value": "vth-inst1-dataout-nic"
	},
	"NIC DataIn VM2": {
	"value": "vth-inst2-datain-nic"
	},
	"NIC DataOut VM2": {
	"value": "vth-inst2-dataout-nic"
	},

Public IP address	Specify the existing Public IP addresses for management traffic.

Table 4 : JSON Parameters

Resource Name	Description

	<pre>"Public IP Name VM1": {
	"value": "<existing Public IP Name VM1>"
	},
	"Public IP Name VM2": {
	"value": "<existing Public IP Name VM2>"
	},</pre>
	NOTE: For cross-zone high availability, ensure the Zone-redundant policy is implied to the Management IP.

Network Security Groups	Specify an existing network security group name for all the NICs.
	<pre>"Network Security Group VM1": {
	"value": "<existing Network Security Group VM1 Name>"
	},
	"Network Security Group VM2": {
	"value": "<existing Network Security Group VM2 Name>"
	},</pre>

Enable Accelerated Networking	Specify 'true' to enable low latency and high throughput on the NICs. For more information, see Accelerated Networking.
	<pre>"Enable Accelerated Networking": {
	"value": false
	},</pre>
	NOTE: By default, accelerated networking is disabled for all type of compute instances and it can be enabled for the selected compute instances. For the supported compute instances, see Supported VM Sizes.

Table 4 : JSON Parameters

Resource Name	Description
Enable IP Forwarding	Specify 'true' to allow the virtual machine to forward the network traffic between networks to improve the network performance. This high-performance forwarded path bypasses the host from the usual data path, thus, reducing latency, jitter, and CPU utilization when using the most demanding network workloads on the supported VM types. For more information, see IP Forwarding. `"Enable IP Forwarding": { "value": false }` **NOTE:** By default, IP forwarding is disabled.

5. Verify if all the configurations in the ARM_TMPL_3NIC_2VM_PVTVIP_PARAM.json file are correct and then save the changes.
6. From Start menu, open PowerShell and navigate to the folder where you have downloaded the ARM template.
7. Run the following command to create an Azure resource group:

```
PS C:\Users\TestUser\Templates> az group create --name <resource_group_name> --location "<location_name>"
```

Example:

```
PS C:\Users\TestUser\Templates> az group create --name vth-rg1 --location "south central us"
```

```
{
    "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/resourceGroups/vth-rg1",
    "location": "southcentralus",
    "managedBy": null,
    "name": "vth-rg1",
    "properties": {
      "provisioningState": "Succeeded"
    },
    "tags": null,
    "type": "Microsoft.Resources/resourceGroups"
  }
```

8. Run the following command to create an Azure deployment group.

```
PS C:\Users\TestUser\Templates> az deployment group create -g
<resource_group_name> --template-file <template_name> --parameters
<param_template_name>
```

Example:

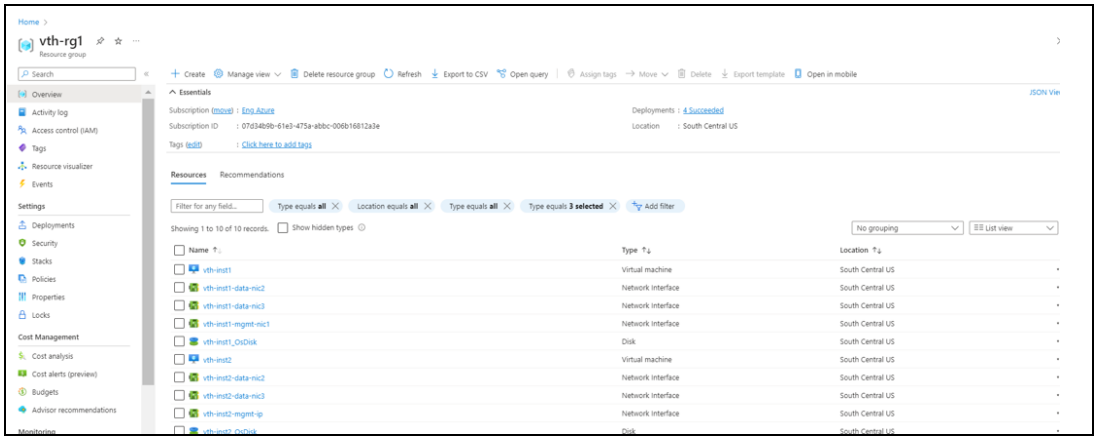
```
PS C:\Users\TestUser\Templates> az deployment group create -g vth-rg1
--template-file ARM_TMPL_3NIC_2VM_PVTVIP.json --parameters ARM_TMPL_
3NIC_2VM_PVTVIP_PARAM.json
```

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

NOTE: The resource group of the deployed vThunder instance and it's resources can be same or different from the resource group of virtual network, NSG, and public IP.

9. Verify if all the above listed resources are created under **Home** > **Azure services** > **Resource Groups** > <*resource_group_name*>.

Figure 34 : Resource listing under resource group



Access Thunder Virtual Machine

The Thunder virtual machine can be accessed using any of the following ways:

- Access vThunder using CLI
- Access vThunder using GUI

Access vThunder using CLI

To access vThunder using CLI, perform the following steps:

1. Open any SSH client.
2. Enter or select the following basic information in the configuration window:
   - Hostname: Public IPv4 address
     Here, Public IP of **`vth-inst1`**, **`vth-inst2`**.
   - Username: Enter username provided by A10 Networks Support
   - Password: Enter password provided by A10 Networks Support
3. Connect to the session.

   If the session connection is successful, the following response is displayed:

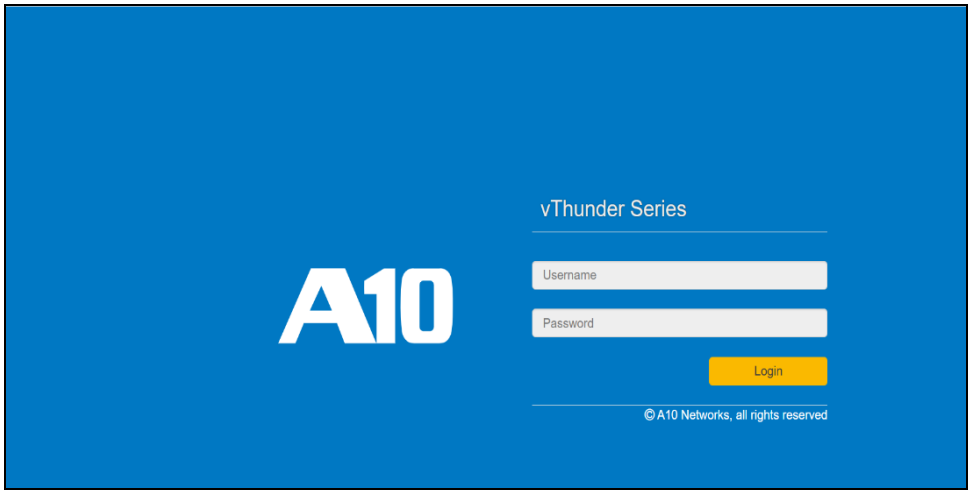
```
Last login: Day MM DD HH:MM:SS from a.b.c.d

System is ready now.

[type ? for help]

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

The vThunder instance is ready to use.

Access vThunder using GUI

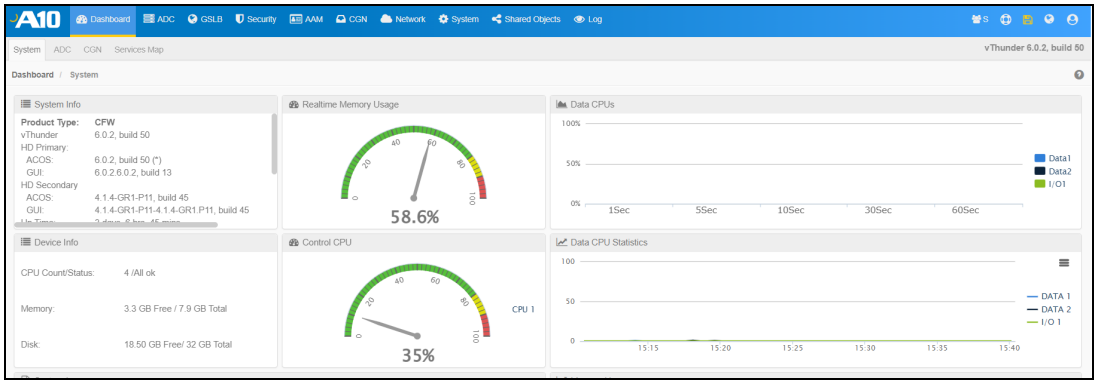
To access vThunder using GUI, perform the following steps:

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



3. Enter the username and password provided by A10 Networks Support. The home page gets displayed.

Figure 35 : Home page



Configure Server and Client Machine

The following topics are covered:

- Create and Configure Server Machine
- Create and Configure a Client Machine

Create and Configure Server Machine

To create a Server machine, perform the following steps:

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

   Project details

   - Subscription
   - Resource group

   Instance details

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

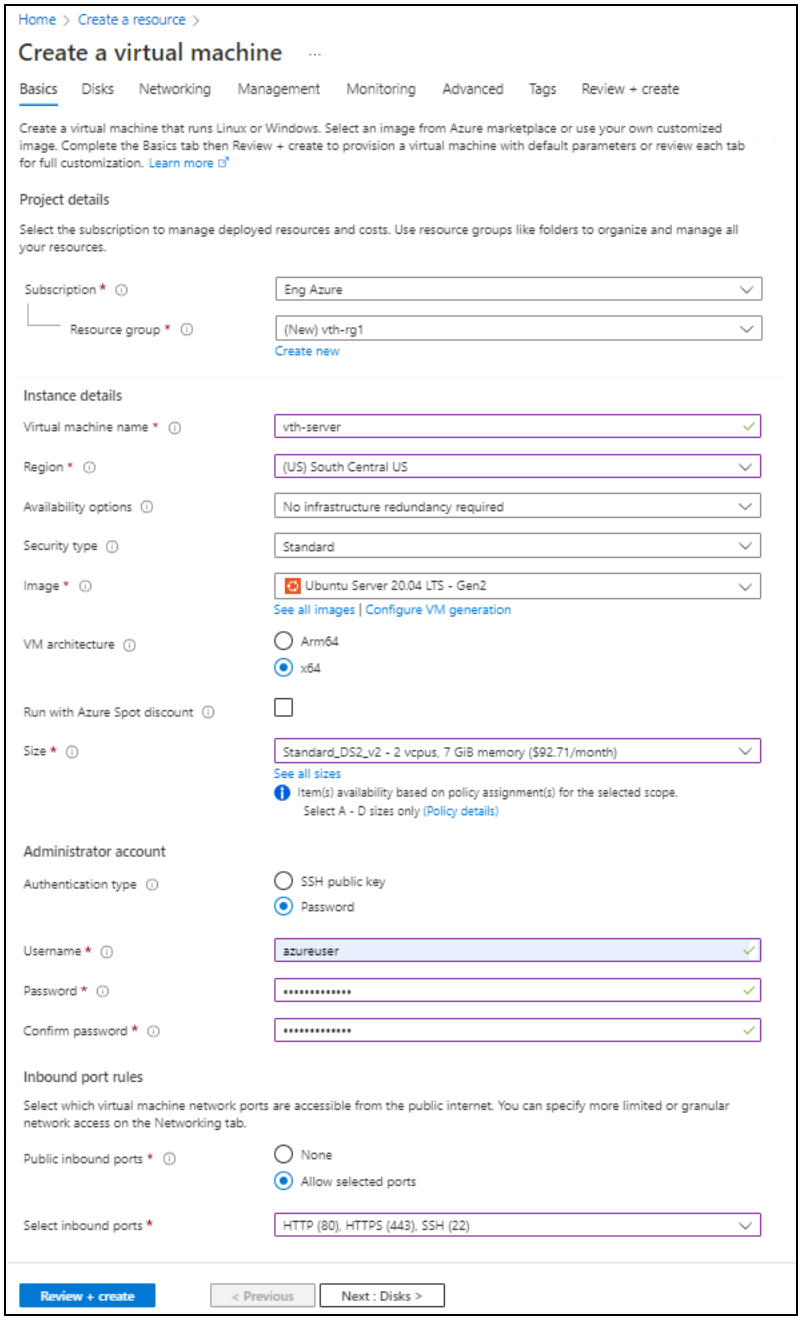
Administrator account

- Depending upon the Authentication type, provide the information.

Inbound port rules

- Public inbound ports
- Select inbound ports

Figure 36 : Create a virtual machine window - Basics tab



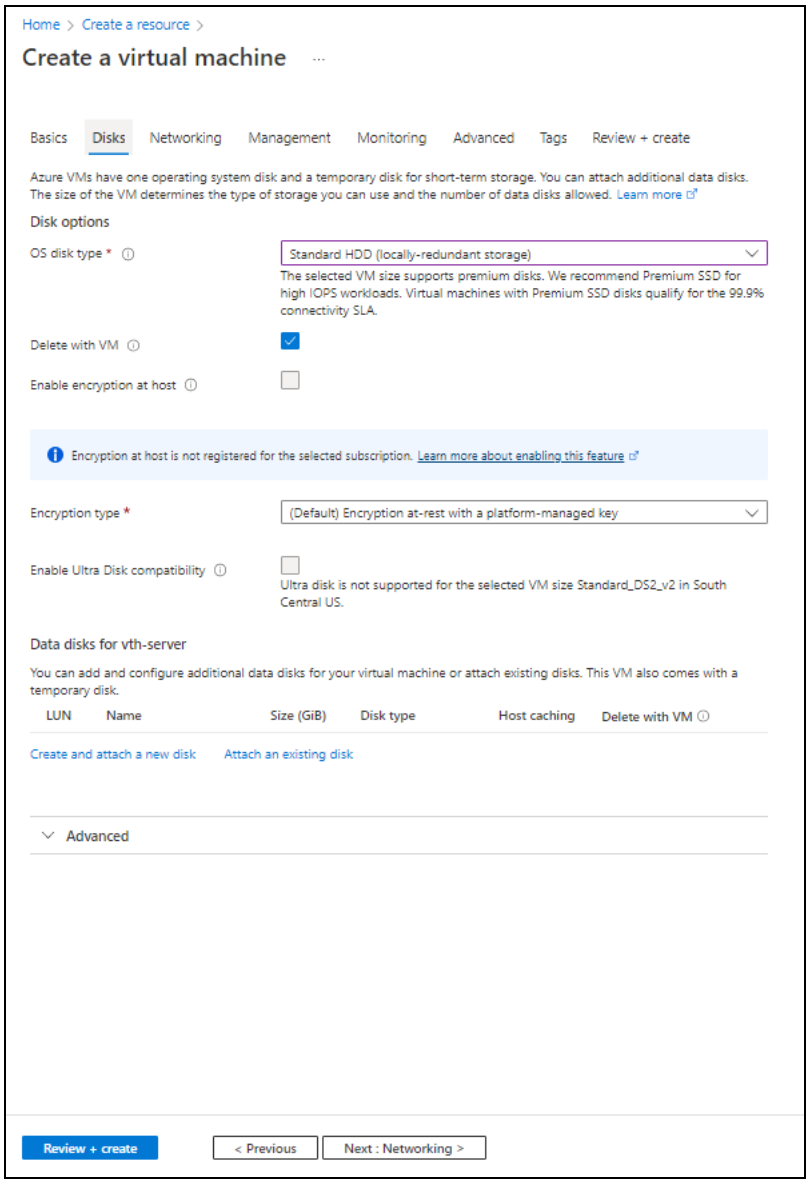
3. Leave the values in other fields unchanged and click **Next : Disks** at the bottom of the window.

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

   Disk options

   - OS disk type
   - Encryption type

Figure 37 : Create a virtual machine window - Disks tab

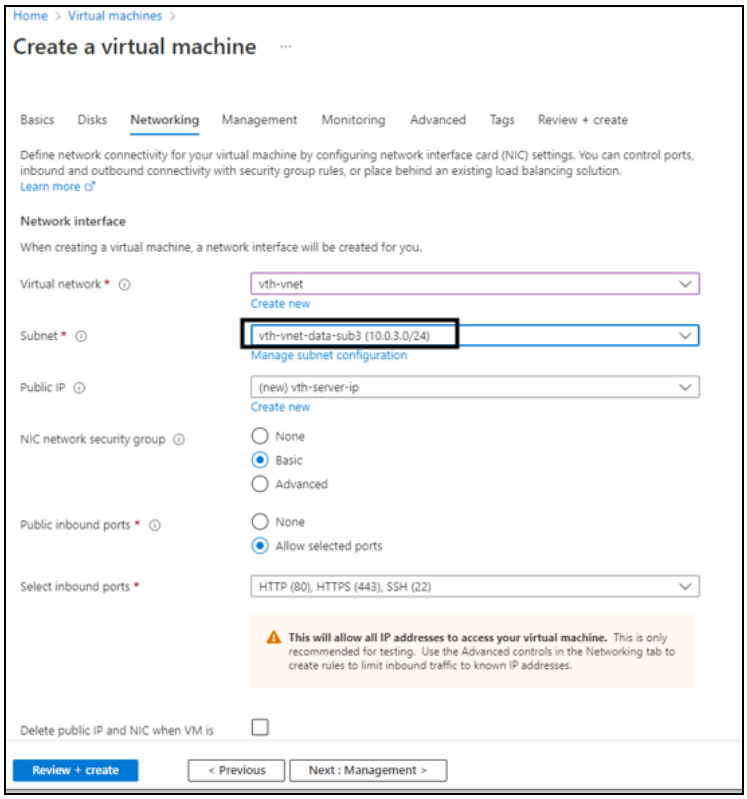


5. Leave the values in other fields unchanged and click **Next : Networking** at the bottom of the window.
6. Select or enter the following mandatory information in the **Networking** tab:

   Network interface

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

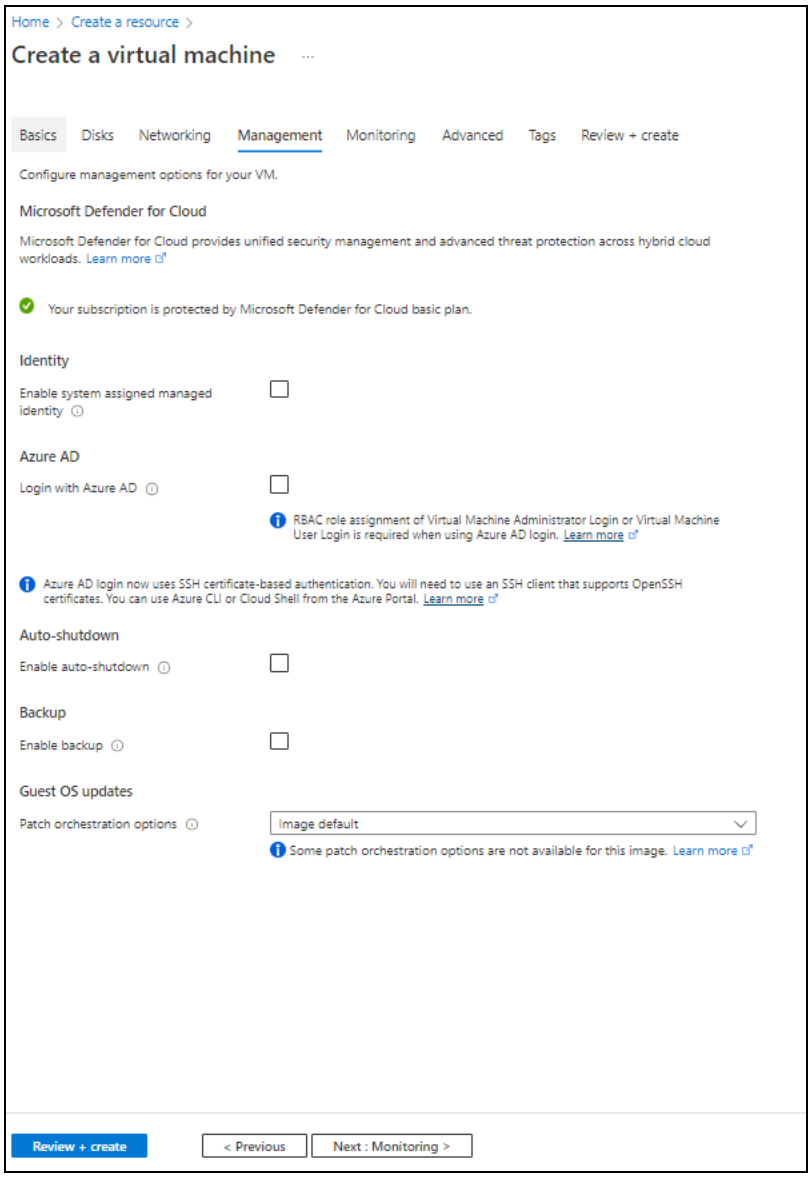
   Figure 38 : Create a virtual machine window - Networking tab



7. Leave the values in other fields unchanged and click **Next : Management** at the bottom of the window.

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

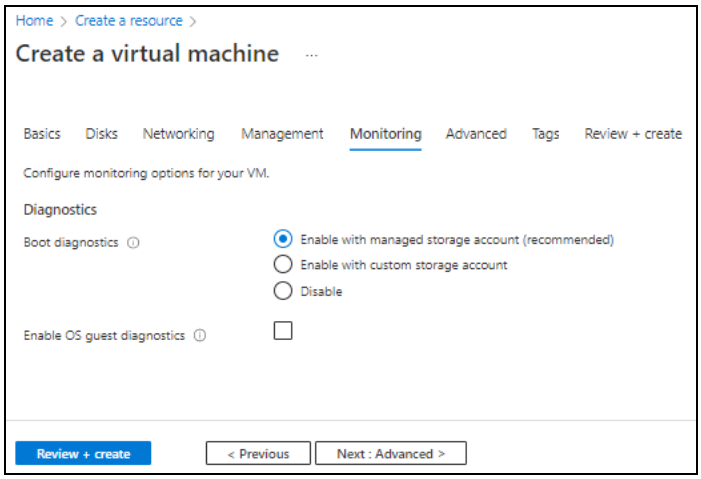
Figure 39 : Create a virtual machine window - Management tab



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

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

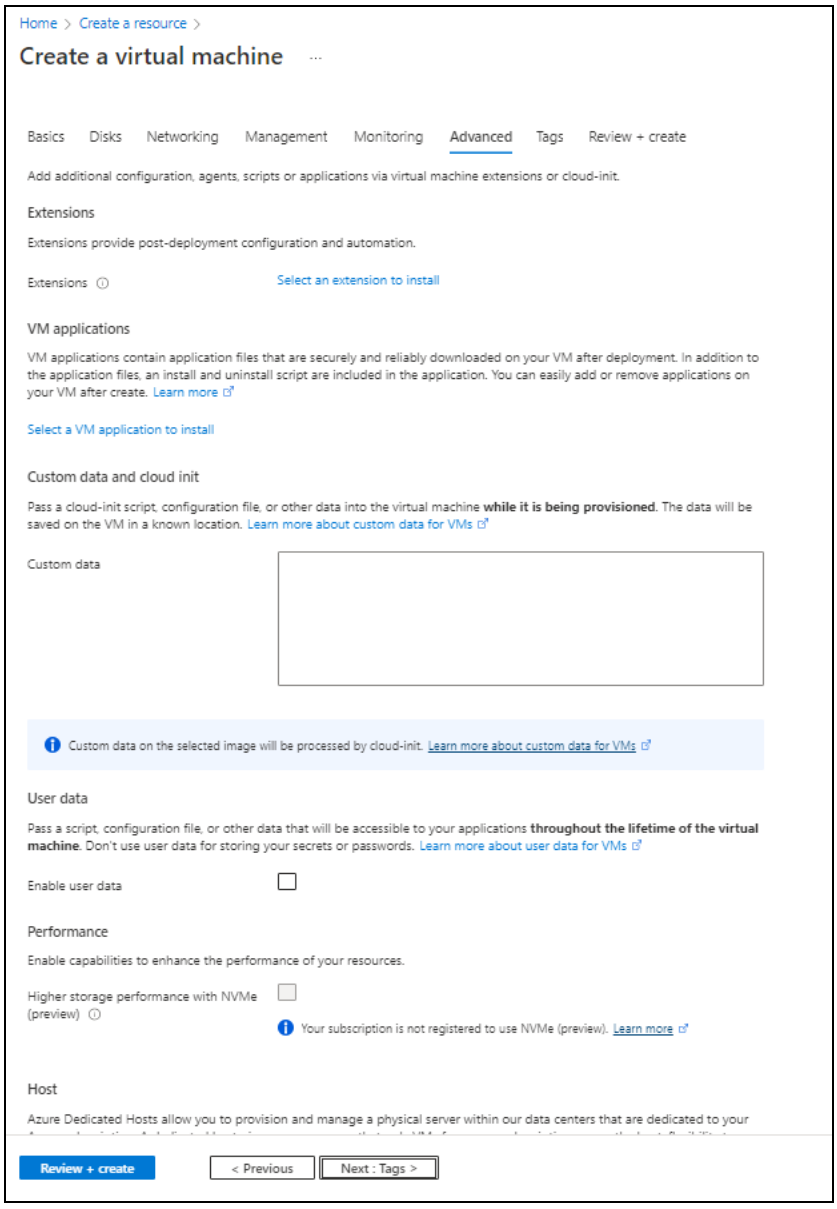
Figure 40 : Create a virtual machine window - Monitoring tab



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

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

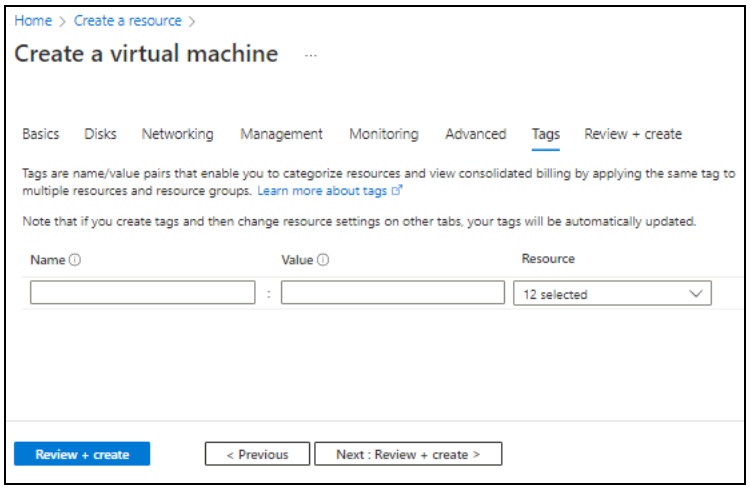
Figure 41 : Create a virtual machine window - Advanced tab



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

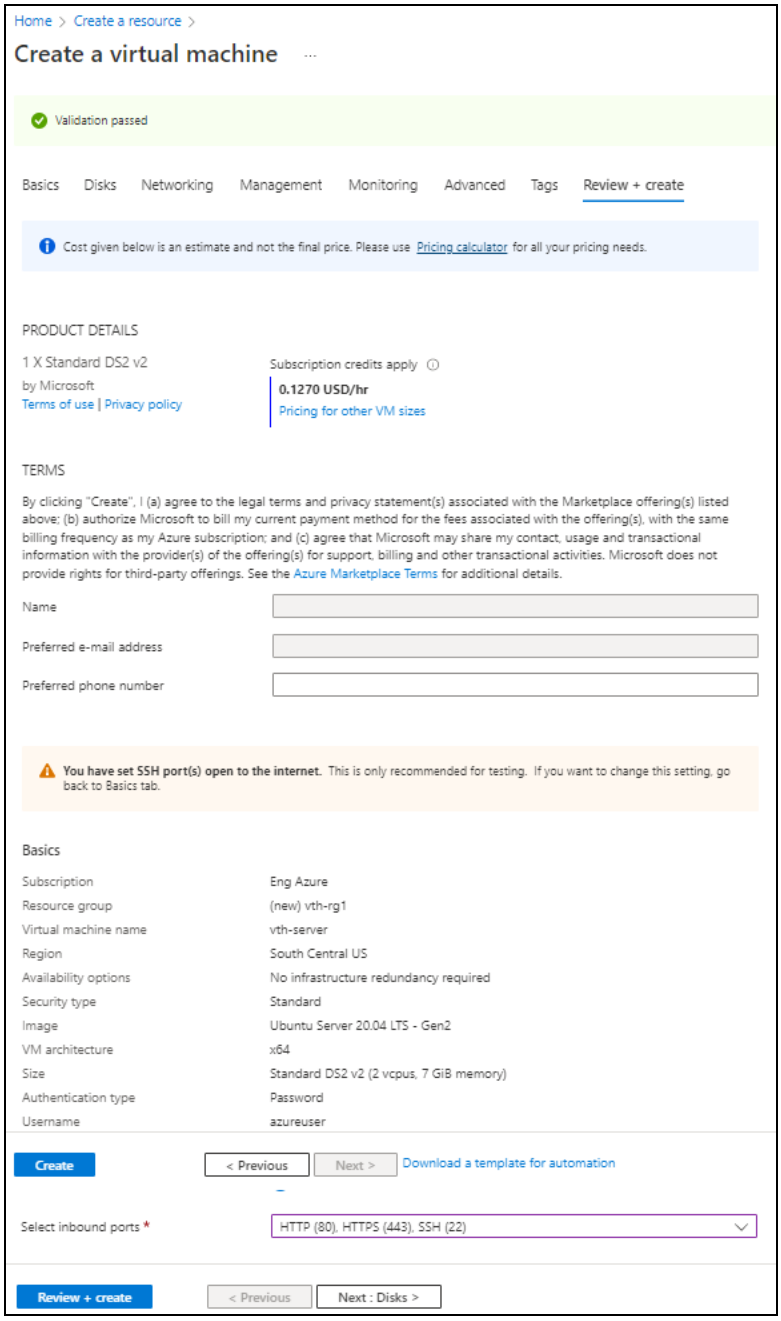
14. Select or enter the information in the **Tags** tab as needed.

Figure 42 : 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 43 : Create a virtual machine window - Review + create tab



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

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

```
sudo apt install apache2
```

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

18. If you want to configure HTTP template, perform the following steps:

    a. SSH the Apache Server and run the following command:

    ```
    sudo vim /etc/apache2/apache2.conf
    ```

    The Apache2 configuration file is displayed.

    b. Add the following configuration and save the file:

    ```
    Alias /<url-match-string> /var/www/html
    ```

    c. Restart the Apache server to enable the HTTP service.

    ```
    sudo systemctl restart apache2
    ```

    The server may take a few minutes to restart.

Create and Configure a Client Machine

To create a Client machine, perform the following steps:

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

   Project details

   - Subscription
   - Resource group

   Instance details

   - Virtual machine name - Client machine
   - Region

- Image
- Size

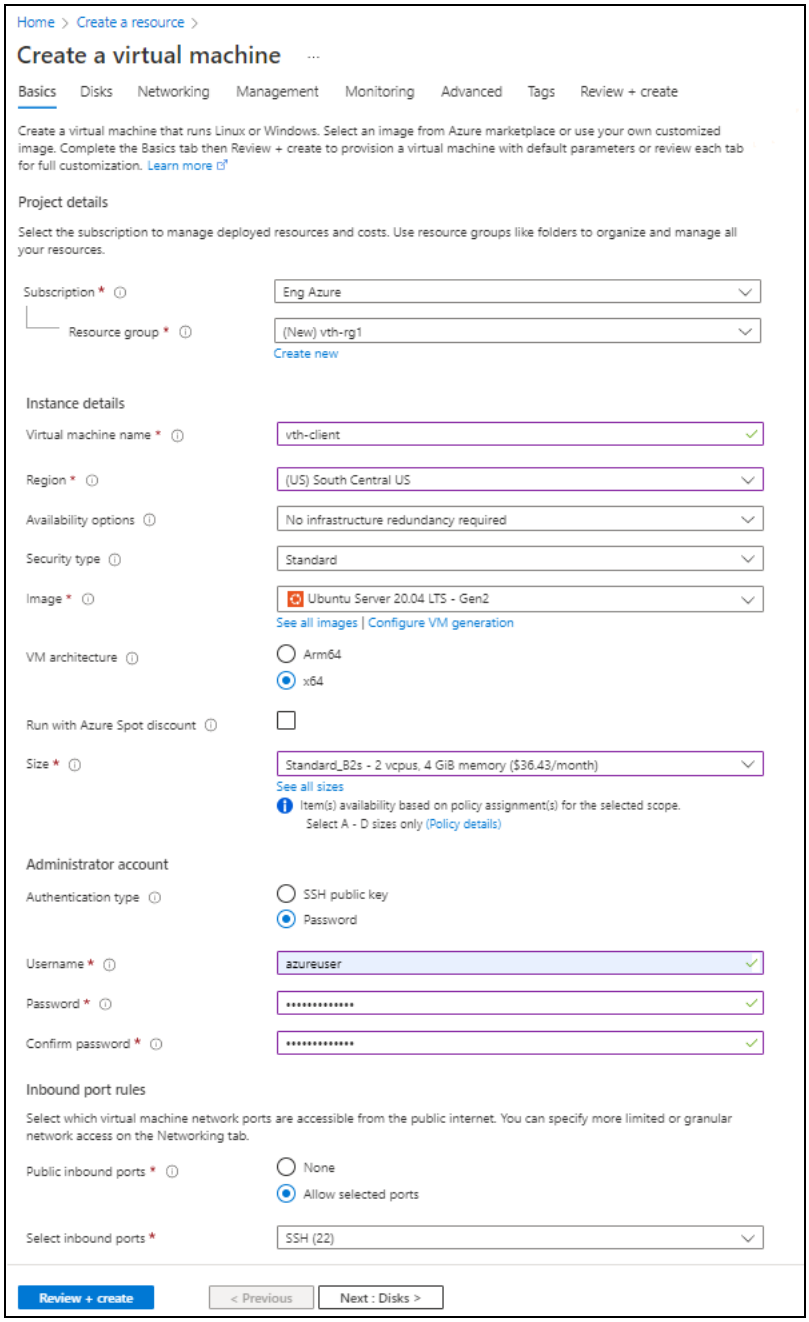
Administrator account

- Depending upon the Authentication type, provide the information.

Inbound port rules

- Public inbound ports
- Select inbound ports

Figure 44 : Create a virtual machine window - Basics tab



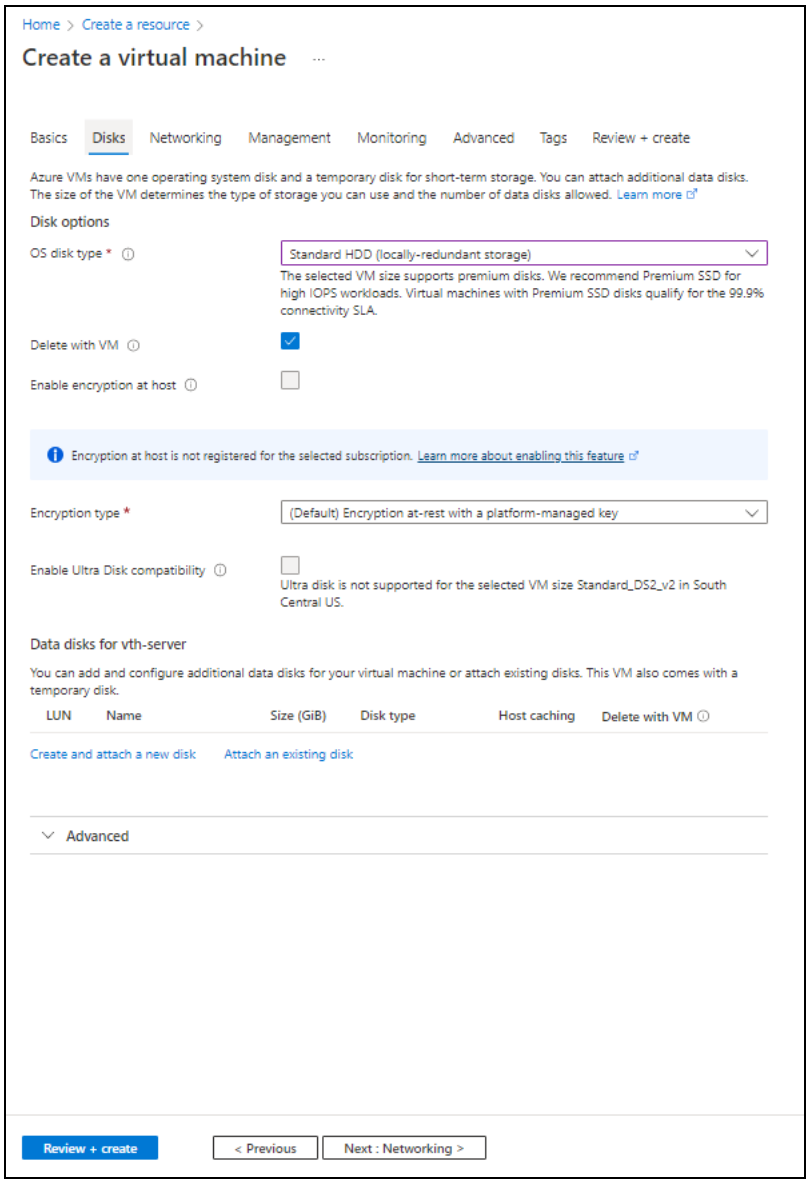
3. Leave the values in other fields unchanged and click **Next : Disks** at the bottom of the window.

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

   Disk options

   - OS disk type
   - Encryption type

Figure 45 : Create a virtual machine window - Disks tab

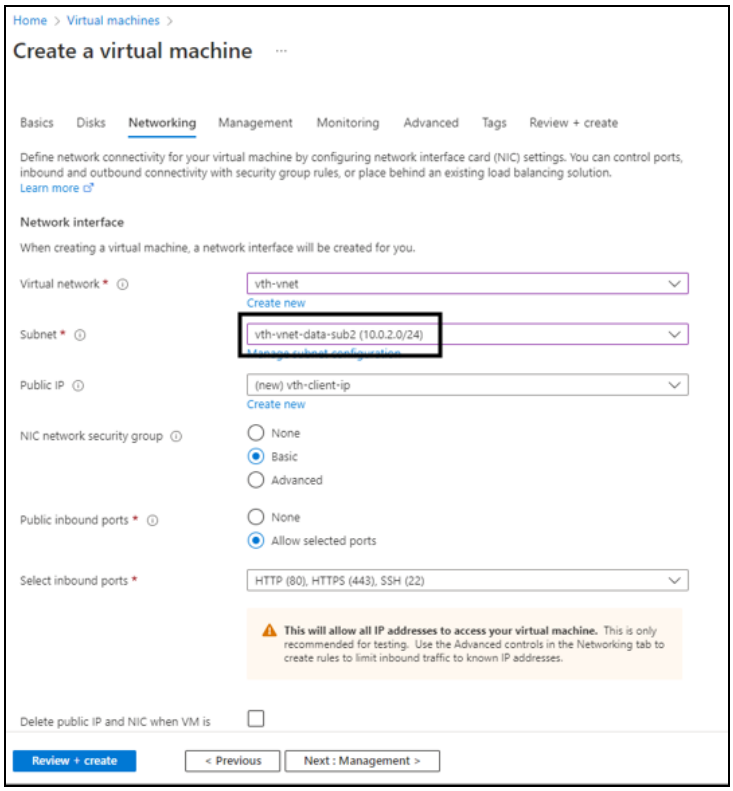


5. Leave the values in other fields unchanged and click **Next : Networking** at the bottom of the window.
6. Select or enter the following mandatory information in the **Networking** tab:

   Network interface

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

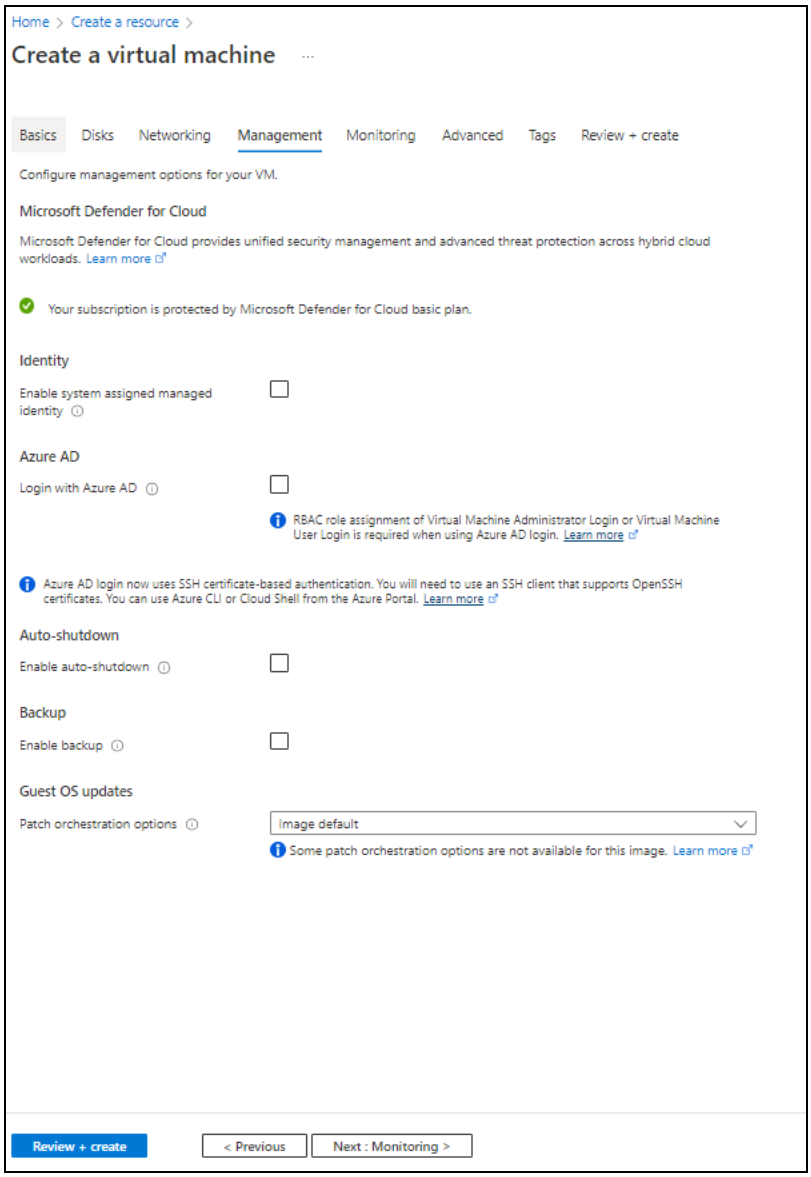
   Figure 46 : Create a virtual machine window - Networking tab



7. Leave the values in other fields unchanged and click **Next : Management** at the bottom of the window.

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

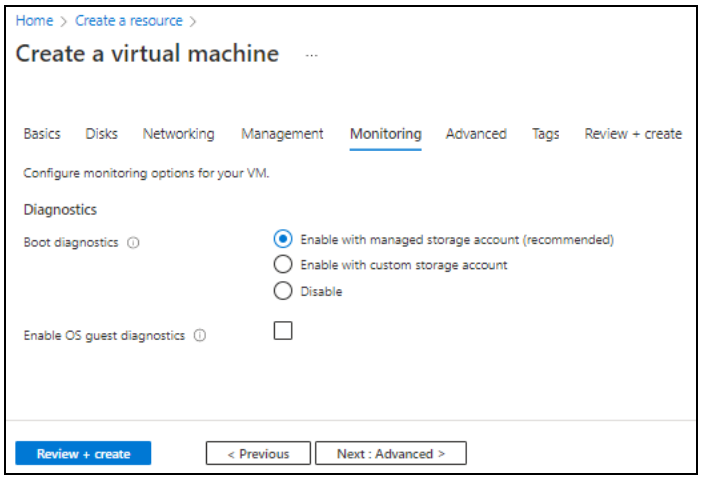
Figure 47 : Create a virtual machine window - Management tab



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

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

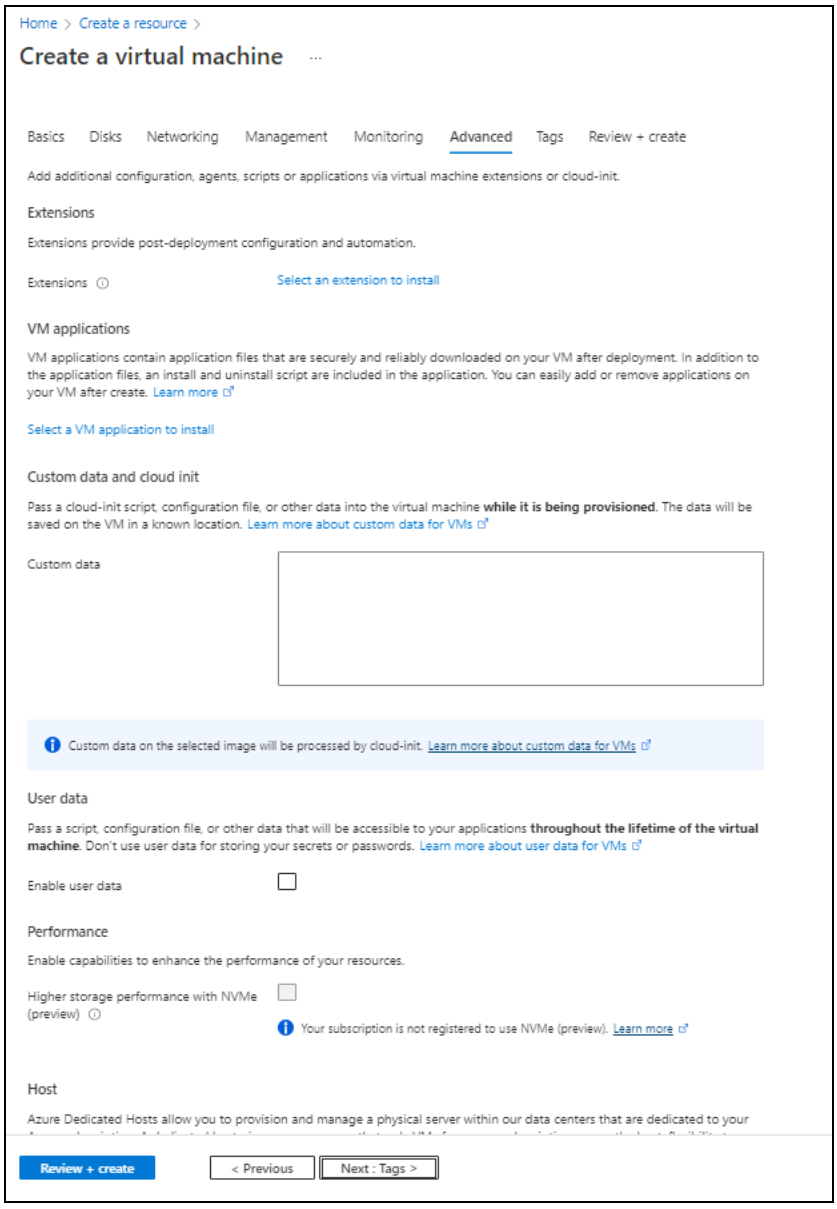
Figure 48 : Create a virtual machine window - Monitoring tab



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

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

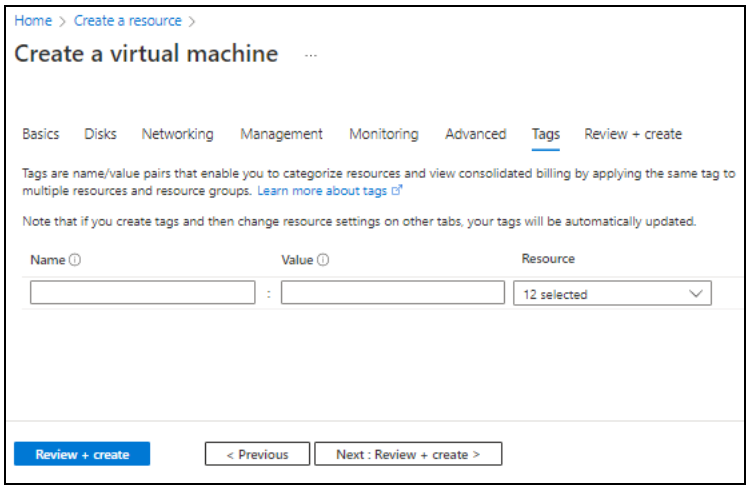
Figure 49 : Create a virtual machine window - Advanced tab



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

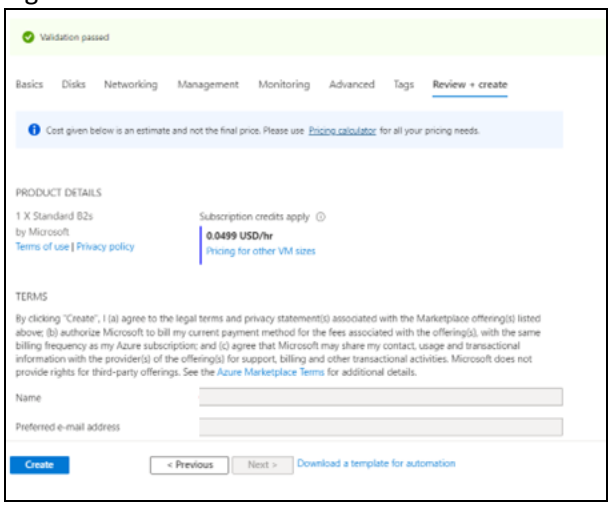
14. Select or enter the information in the **Tags** tab as needed.

Figure 50 : Create a virtual machine window - Tags tab



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

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



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

Configure Thunder

The following configurations can be applied to the deployed vThunder instance:

- Change Password
- A10 License
- SSL Certificate
- Basic Server Load Balancer or Server Load Balancer on Backend Autoscale (depending on your use case, see Deployment Templates)
- High Availability

Verify Deployment

To verify deployment using the ARM template, perform the following steps:

1. Run the following command on the active vThunder instance:

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

   If the deployment is successful with basic SLB, HA, HTTP template, and Persist-cookie template configuration, the following output is displayed:

```
!
vrrp-a common
  device-id 1
  set-id 1
  enable
!
terminal idle-timeout 0
!
ip dns primary 8.8.8.8
!
!
interface ethernet 1
  enable
  ip address dhcp
!
interface ethernet 2
  enable
  ip address dhcp
!
vrrp-a vrid 0
  floating-ip 10.0.3.8
  floating-ip 10.0.2.9
  blade-parameters
    priority 100
!
vrrp-a peer-group
  peer 10.0.2.7
  peer 10.0.2.6
!
ip route 0.0.0.0 /0 10.0.2.1
!
slb server s1 10.0.3.4
  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 template persist cookie persist-cookie
  expire 60
  encrypt-level 0
  name a10-cookies
  match-type service-group
!
slb template http hostname-test
  host-switching contains s1 service-group sg80
!
slb template http url-test
  url-switching regex-match s1 service-group sg80
!
slb virtual-server vip 10.0.2.9
  port 53 udp
    source-nat auto
    service-group sg53
  port 80 http
    source-nat auto
    service-group sg80
    template persist cookie persist-cookie
    template http url-test
  port 443 https
    source-nat auto
    service-group sg443
!
!
end
```

2. Run the following command on active vThunder instance to verify the SSL

Certificate configuration:

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

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

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

3. Run the following command on active vThunder instance to verify the GLM License Provision configuration:

```
vThunder-Active(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
```

4. Run the following command on the standby vThunder instance:

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

If the deployment is successful with basic SLB, HA, HTTP template, and Persist-cookie template configuration, the following output is displayed:

```
!
vrrp-a common
  device-id 2
  set-id 1
  enable
!
!
system password-policy complexity Default username-check enable
system password-policy complexity Default repeat-character-check enable
system password-policy complexity Default forbid-consecutive-character
4
!
terminal idle-timeout 0
!
ip dns primary 8.8.8.8
!
!
interface ethernet 1
  enable
  ip address dhcp
!
interface ethernet 2
  enable
  ip address dhcp
!
vrrp-a vrid 0
  floating-ip 10.0.3.8
  floating-ip 10.0.2.9
  blade-parameters
    priority 99
!
vrrp-a peer-group
  peer 10.0.2.7
  peer 10.0.2.6
!
ip route 0.0.0.0 /0 10.0.2.1
!
```

```
slb server s1 10.0.3.4
  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 template persist cookie persist-cookie
  expire 60
  encrypt-level 0
  match-type service-group
!
slb template http hostname-test
  host-switching contains s1 service-group sg80
!
slb template http url-test
  url-switching regex-match s1 service-group sg80
!
slb virtual-server vip 10.0.2.9
  port 53 udp
    source-nat auto
    service-group sg53
  port 80 http
    source-nat auto
    service-group sg80
    template persist cookie persist-cookie
    template http url-test
  port 443 https
    source-nat auto
    service-group sg443
```

```
!
!
end
```

5. Run the following command to force stop the active vThunder instance and make the standby vThunder instance as active device:

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

6. Run the following command to disable the active standby vThunder instance:

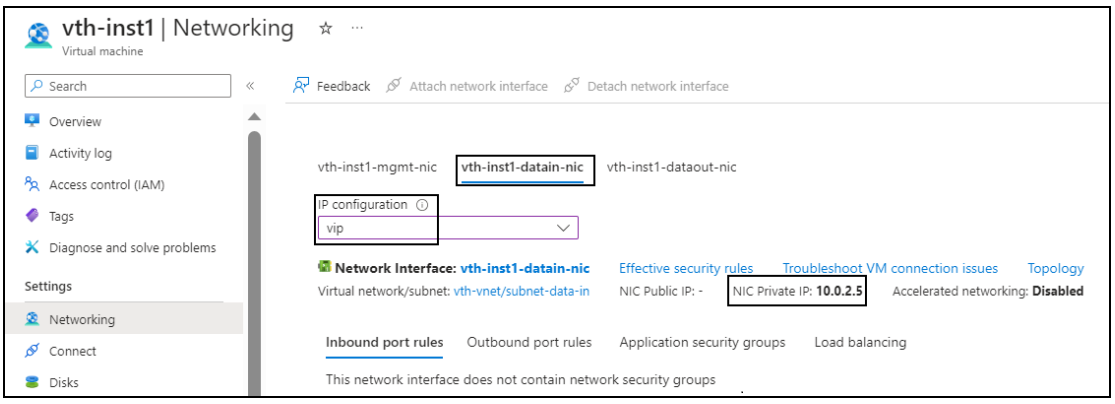
```
vThunder-ForcedStandby(config)#vrrp-a force-self-standby disable
vThunder-Active(config)#
```

Verify Traffic Flow

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

1. From **Azure Portal** > **Azure services** > **Resource Group** > <*resource_group_name*> > <*active_virtual_machine_instance*> > **Settings** > **Networking**.
   Here, **`vth-inst1`** is the active vThunder instance name.
2. Select the Datain NIC tab > **IP configuration** > **`vip`**. Here, Datain NIC is **`vth-inst1-datain-nic`**.
3. Copy the VIP address of the active vThunder instance.

   Figure 52 : Active vThunder instance 1 VIP



4. Select your client instance from the **Virtual machine** list.
   Here, **`vth-client`** is the client instance name.

5. SSH your client machine and run the following command using the copied VIP address to verify the traffic flow:

```
curl <vThunder_instance_datain-nic_vip>
```

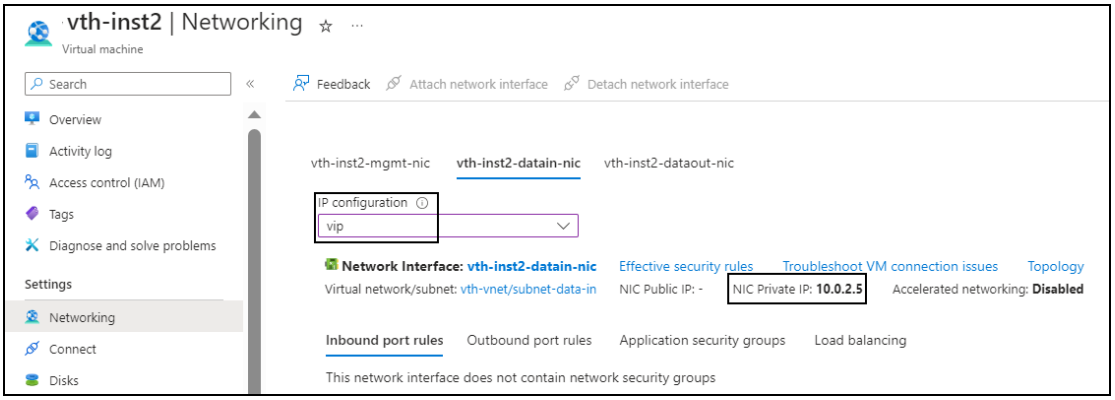
Example

```
curl 10.0.2.5
```

Verify if a response is received.

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

Figure 53 : Active vThunder instance 2 VIP



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

```
curl <vThunder_instance_datain-nic_vip>
```

Example

```
curl 10.0.2.5
```

Verify if a response is received.

8. SSH your client machine and run the following command to verify the HTTP template traffic flow:

```
curl <vThunder_instance_datain-nic_vip>:<port_number>/<host-match-string or url-match-string>/
```

Example

```
curl 10.0.2.5:80/s1/
```

Verify if a response is received from client server (For example: Apache Index page).

9. SSH your client machine and run the following commands to verify the Persist cookie template traffic flow:

   a. Verify the current cookie configuration:

   ```
   curl --head <vThunder_instance_datain-nic_private_ip>
   ```

   b. Run the following commands to save the cookies in the **cookie.txt** file:

   ```
   curl -b cookie.txt -c cookie.txt <vThunder_instance_datain-nic_
   private_ip>
   cat cookie.txt
   ```

   Example

   ```
   curl --head 10.0.2.4
   curl -b cookie.txt -c cookie.txt 10.0.2.4
   cat cookie.txt
   ```

10. Run the following command on the active vThunder instance to view the persistence load-balancing statistics:

    ```
    vThunder(config)#show slb persist
    ```

    If the deployment is successful, the following summary persistence statistics is displayed:

```
                                        Total
-----------------------------------------------
URL hash persist (pri)                    0
URL hash persist (sec)                    0
URL hash persist fail                     0
SRC IP persist ok                         0
SRC IP persist fail                       0
SRC IP hash persist(pri)                  0
SRC IP hash persist(sec)                  0
SRC IP hash persist fail                  0
DST IP persist ok                         0
DST IP persist fail                       0
DST IP hash persist(pri)                  0
DST IP hash persist(sec)                  0
DST IP hash persist fail                  0
SSL SID persist ok                        0
SSL SID persist fail                      0
Cookie persist ok                         1
Cookie persist fail                       0
Persist cookie not found                  2
Persist cookie Pass-thru                  0
Enforce higher priority                   0
```

If the Persist-cookie configuration is successful, a value is displayed for the **`Cookie persist ok`** else the value is 0.

Thunder-3NIC-2VM-PUBVIP

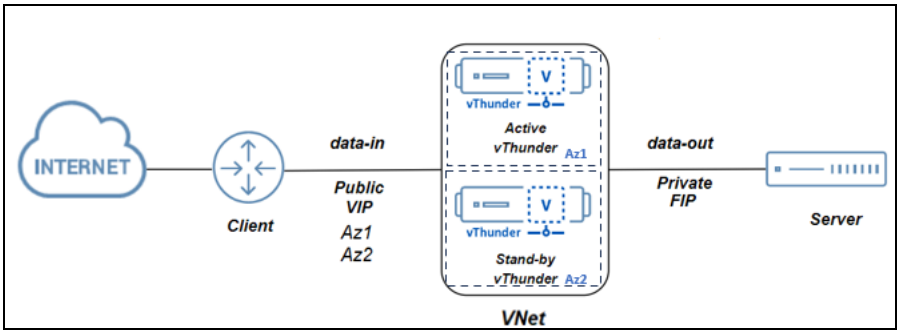
This template creates two vThunder instances with HA setup and each vThunder has one management and two data NICs (data-in and data-out). It configures data-in network interface card (NIC) with Public IP on VIP.

High availability can be configured within the same or different availability zone within a same region. If one instance goes down, other instance takes the request without any manual intervention.

For more information, see Create Thunder Virtual Machines.

NOTE: Use a suitable VM size that supports at least three NICs. For VM sizes, see Supported VM Sizes.

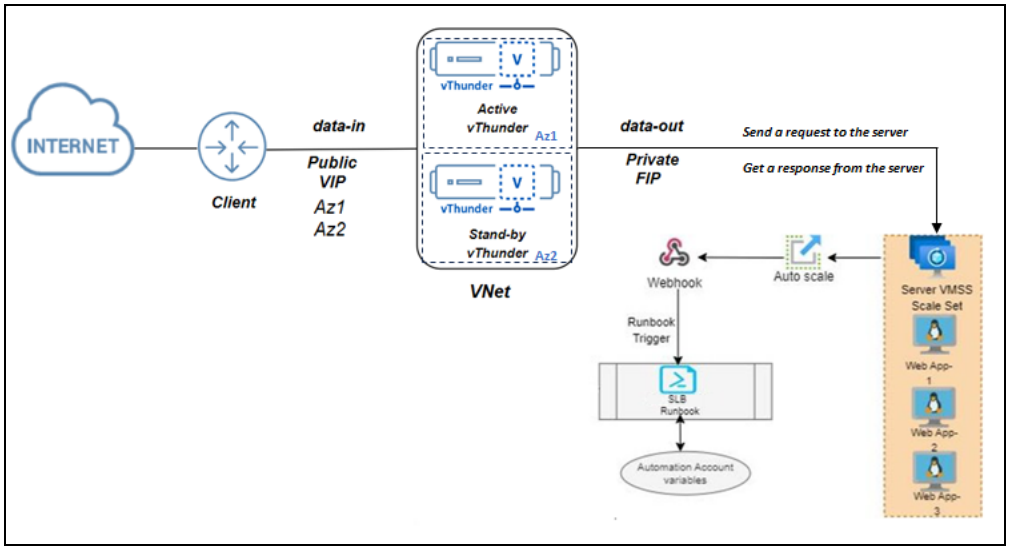
Figure 54 : SLB Thunder ADC in High Availability mode with Public VIP



Following are the Thunder configurations that can be applied as needed:

- Change Password
- A10 License
- SSL Certificate
- Basic Server Load Balancer
- High Availability

Figure 55 : SLB Thunder ADC in High Availability mode with Public VIP and Backend Server Autoscale



Following are the Thunder configurations that can be applied as needed:

- Change Password
- A10 License
- SSL Certificate
- Server Load Balancer on Backend Autoscale
- High Availability

Various templates are available for different deployment needs.

For more information, see Deployment Templates.

The following topics are covered:

Create Thunder Virtual Machines

The A10-vThunder-3NIC-2VM-PUBVIP template is used to create two Thunder virtual machines with three network interface cards each and configure the data-in network interface card with Public IP on VIP.

Before deploying this template, it is recommended to review the Prerequisites.

vThunder instances should have the same versions; otherwise, traffic flow will be disrupted.

There are two ways to deploy this template:

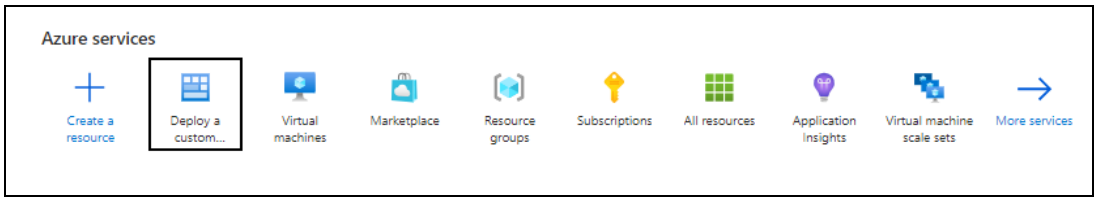
- Upload using Azure Portal Console
- Execute using Azure CLI

Upload using Azure Portal Console

To deploy the A10-vThunder-3NIC-2VM-PUBVIP template using Azure Portal Console, perform the following steps:

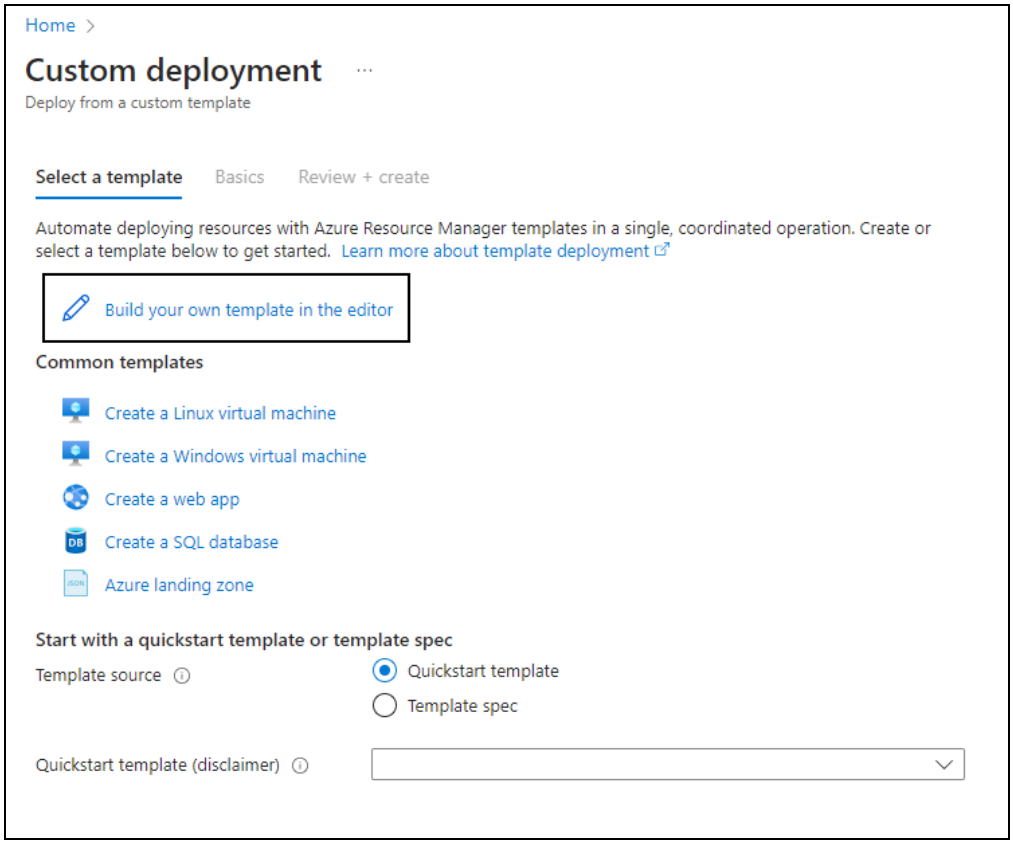
1. Download A10-vThunder-3NIC-2VM-PUBVIP template.
2. From the **Azure Portal** > **Azure services**, click **Deploy a custom template**.

Figure 56 : Azure services



3. Under the **Custom deployment** window > **Select a template** tab, click **Build your own template in the editor**.

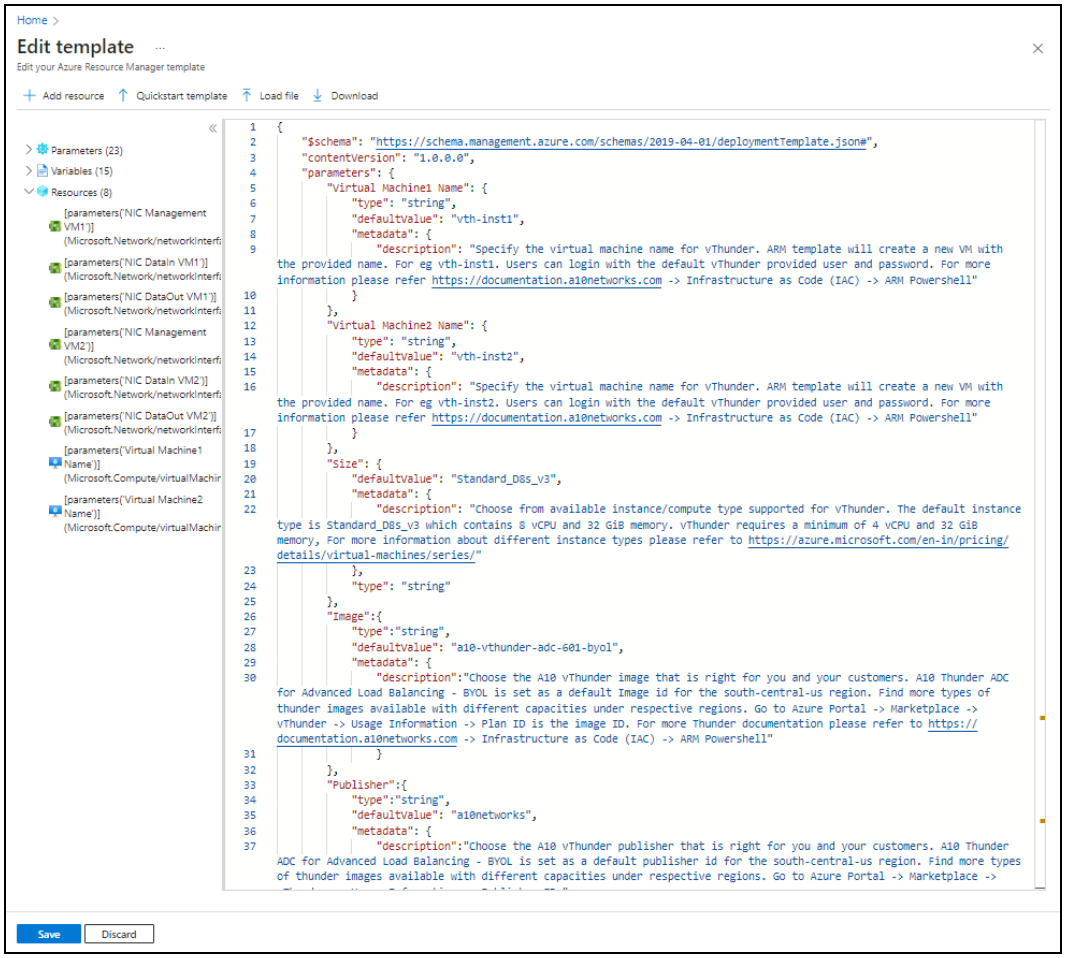
Figure 57 : Custom deployment window



4. From the **Edit template** window, perform either of the following step:

   - Click **Load file** and browse to the folder where you have downloaded the ARM template. Select **ARM_TMPL_3NIC_2VM_PUBVIP.json** to upload.
   - From Windows Explorer, navigate to the folder where you have downloaded the ARM template. Copy **ARM_TMPL_3NIC_2VM_PUBVIP.json** content and paste it in the editor.

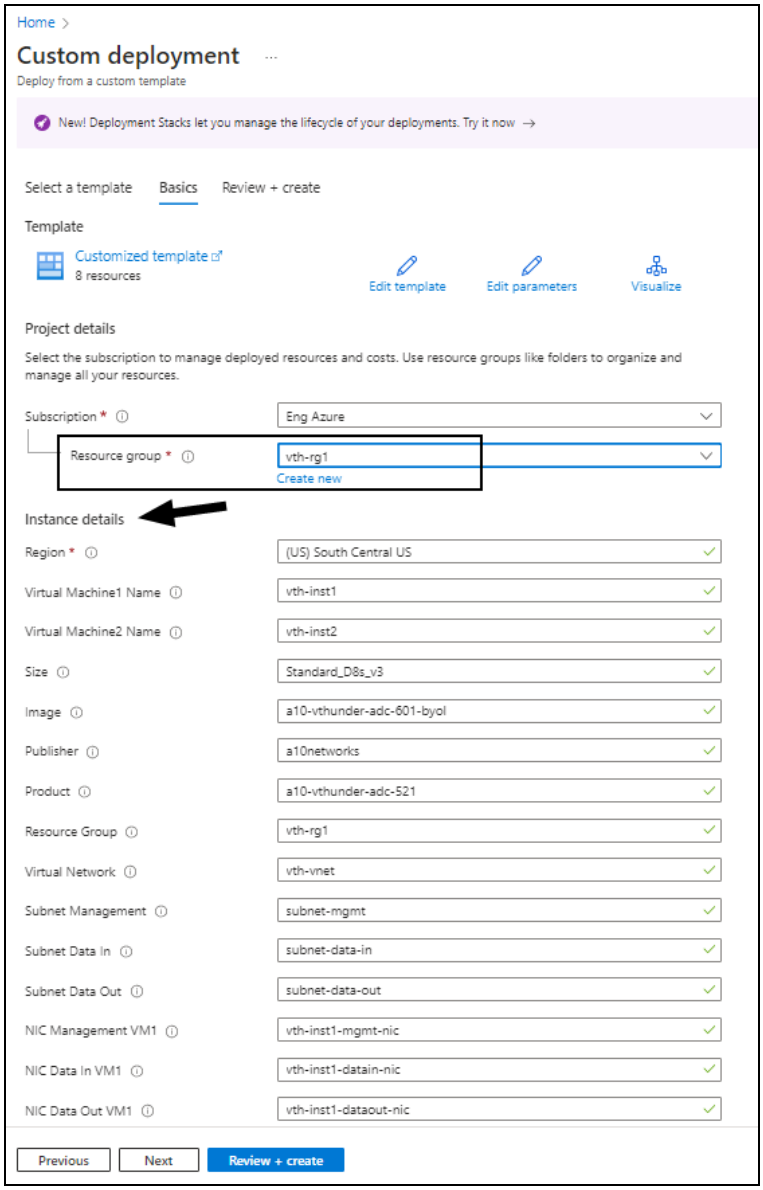
Figure 58 : Edit template window



5. Click **Save**.

   The **Custom deployment** window is displayed with the template parameters and default values.

Figure 59 : Custom deployment template



6. Select an existing or create a new **Resource group** under which you want to deploy the custom template resources.

NOTE: Hover ⓘ for description of each corresponding parameter.

7. Update the default values and also provide the values in the empty fields as

appropriate in the **Instance details** section shown in Figure 59.

NOTE: Use a suitable VM size that supports at least three NICs. For VM sizes, see Supported VM Sizes.
For cross-zone high availability, ensure the Zone-redundant policy is implied to the Management IP and Public IP VIP.

8. Click **Review+create**.

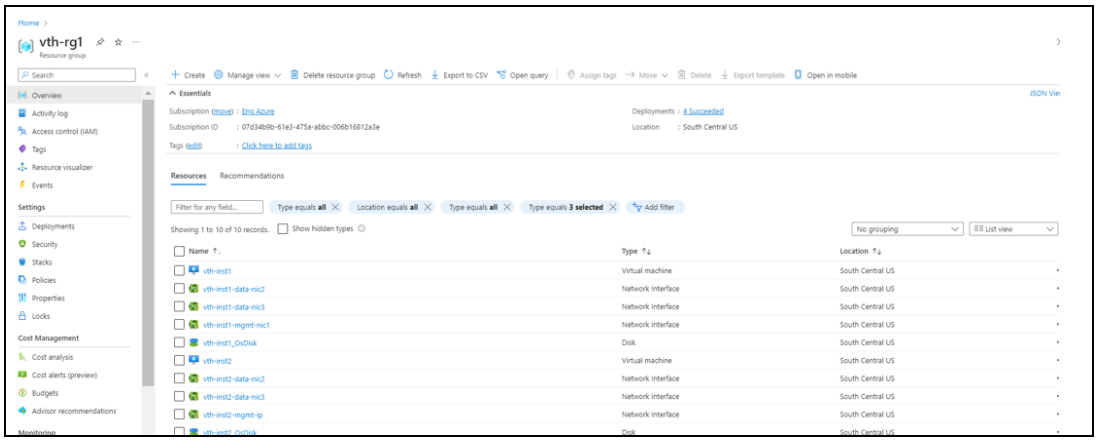
   The validation appears.

9. Click **Create**.

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

10. Verify if all the above listed resources are created under **Home** > **Azure services** > **Resource Groups** > <*resource_group_name*>.

Figure 60 : Resource listing under resource group



Execute using Azure CLI

To deploy the A10-vThunder-3NIC-2VM-PUBVIP template using Azure CLI commands, perform the following steps:

1. Download A10-vThunder-3NIC-2VM-PUBVIP template.

NOTE: This template contains pre-populated default values that can be modified as appropriate and it does not create new virtual network, network security group, subnets, and Public IP.

2. From Windows Explorer, navigate to the folder where you have downloaded the ARM template.
3. Open the ARM_TMPL_3NIC_2VM_PUBVIP_PARAM.json with a text editor.
4. Configure the following parameters as appropriate:

Table 5 : JSON Parameters

Resource Name	Description

Virtual Machines	Specify a virtual machine name for each of the two vThunder instances.
	`"Virtual Machine1 Name": {`
	`"value": "vth-inst1"`
	`},`
	`"Virtual Machine2 Name": {`
	`"value": "vth-inst2"`
	`}`

Virtual Machine Zones	Specify an availability zone in which to deploy your virtual machine. If you have an existing Public IP, then it should be available in the same availability zone as the virtual machine.
	`"Virtual Machine1 Zone": {`
	`"value": "1"`
	`},`
	`"Virtual Machine2 Zone": {`
	`"value": "1"`
	`},`

Size	Specify a suitable size for the vThunder instance.

Table 5 : JSON Parameters

Resource Name	Description

	<pre>"Size": {
	  "value": "Standard_D8s_v3"
	},</pre>
	NOTE: Use a suitable VM size that supports at least 3 NICs. For VM sizes, see Supported VM Sizes.

Image	Specify the desired vThunder Image name and Product name from the Azure Marketplace.
	<pre>"Image": {
	  "value":"a10-vthunder-adc-601-byol"
	},
	"Publisher": {
	  "value": "a10networks"
	},
	"Product": {
	  "value": "a10-vthunder-adc-521"
	},</pre>
	NOTE: Do not change the publisher name.

Resource Group	Specify the name of an existing resource group under which the virtual network, network security group, and subnets are already created.
	<pre>"ResourceGroup": {
	  "value": "<existing VN NSG ResourceGroupName>"
	},</pre>

Virtual Network	Specify an existing virtual network name for vThunder.
	<pre>"Virtual Network": {
	  "value": "<existing virtual network name>"
	},</pre>

Management	Specify an existing subnet name that is available within the

Table 5 : JSON Parameters

Resource Name	Description
Subnet	selected virtual network for inbound management traffic. `"SubnetManagement": { "value": "<existing subnet-mgmt name>" },`
Data Subnet	Specify an existing subnet name that is available within a selected virtual network for inbound and outbound data traffic. `"SubnetDataIn": { "value": "<existing subnet-data-in name>" }, "SubnetDataOut": { "value": "<existing subnet-data-out name>" },`
Network Interface Cards	Specify a unique network interface card for management, datain, and dataout traffic. `"NIC Management VM1": { "value": "vth-inst1-mgmt-nic" }, "NIC Management VM2": { "value": "vth-inst2-mgmt-nic" },`

Table 5 : JSON Parameters

Resource Name	Description

	<pre>"NIC DataIn VM1": {
	"value": "vth-inst1-datain-nic"
	},
	"NIC DataOut VM1": {
	"value": "vth-inst1-dataout-nic"
	},
	"NIC DataIn VM2": {
	"value": "vth-inst2-datain-nic"
	},
	"NIC DataOut VM2": {
	"value": "vth-inst2-dataout-nic"
	},</pre>

Public IP address	Specify the existing Public IP addresses for management traffic.
	<pre>"Public IP Name VM1": {
	"value": "<existing Public IP Name VM1>"
	},
	"Public IP Name VM2": {
	"value": "<existing Public IP Name VM2>"
	},
	"Public IP Name VIP": {
	"value": "<existing Public VIP Name>"
	},</pre>
	NOTE: For cross-zone high availability, ensure the Zone-redundant policy is implied to the Management IP and Public IP VIP.

Network Security Groups	Specify an existing network security group name for all the NICs.

Table 5 : JSON Parameters

Resource Name	Description

	<pre>"Network Security Group VM1": {
	"value": "<existing Network Security Group VM1 Name>"
	},
	"Network Security Group VM2": {
	"value": "<existing Network Security Group VM2 Name>"
	},</pre>

Enable Accelerated Networking	Specify 'true' to enable low latency and high throughput on the NICs. For more information, see Accelerated Networking.
	<pre>"Enable Accelerated Networking": {
	"value": false
	},</pre>
	NOTE: By default, accelerated networking is disabled for all type of compute instances and it can be enabled for the selected compute instances. For the supported compute instances, see Supported VM Sizes.

Table 5 : JSON Parameters

Resource Name	Description
Enable IP Forwarding	Specify 'true' to allow the virtual machine to forward the network traffic between networks to improve the network performance. This high-performance forwarded path bypasses the host from the usual data path, thus, reducing latency, jitter, and CPU utilization when using the most demanding network workloads on the supported VM types. For more information, see IP Forwarding. `"Enable IP Forwarding": { "value": false }` **NOTE:** By default, IP forwarding is disabled.

5. Verify if all the configurations in the ARM_TMPL_3NIC_2VM_PUBVIP_PARAM.json file are correct and then save the changes.
6. From Start menu, open PowerShell and navigate to the folder where you have downloaded the ARM template.
7. Run the following command to create an Azure resource group:

```
PS C:\Users\TestUser\Templates> az group create --name <resource_group_name> --location "<location_name>"
```

Example:

```
PS C:\Users\TestUser\Templates> az group create --name vth-rg1 --location "south central us"
```

```
{
    "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/resourceGroups/vth-rg1",
    "location": "southcentralus",
    "managedBy": null,
    "name": "vth-rg1",
    "properties": {
      "provisioningState": "Succeeded"
    },
    "tags": null,
    "type": "Microsoft.Resources/resourceGroups"
  }
```

8. Run the following command to create an Azure deployment group.

```
PS C:\Users\TestUser\Templates> az deployment group create -g
<resource_group_name> --template-file <template_name> --parameters
<param_template_name>
```

Example:

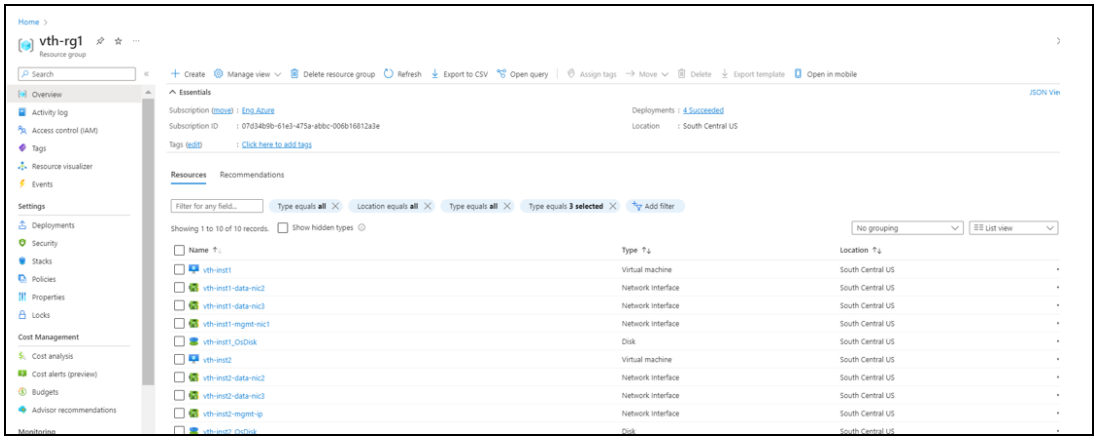
```
PS C:\Users\TestUser\Templates> az deployment group create -g vth-rg1
--template-file ARM_TMPL_3NIC_2VM_PUBVIP.json --parameters ARM_TMPL_
3NIC_2VM_PUBVIP_PARAM.json
```

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

NOTE: The resource group of the deployed vThunder instance and it's resources can be same or different from the resource group of virtual network, NSG, and public IP.

9. Verify if all the above listed resources are created under **Home** > **Azure services** > **Resource Groups** > *<resource_group_name>*.

Figure 61 : Resource listing under resource group



Access Thunder Virtual Machine

The Thunder virtual machine can be accessed using any of the following ways:

- Access vThunder using CLI
- Access vThunder using GUI

Access vThunder using CLI

To access the two vThunder instances using CLI, perform the following steps:

1. Open any SSH client.
2. Enter or select the following basic information in the configuration window:
   - Hostname: Public IPv4 address
     Here, Public IP of **`vth-inst1`**, **`vth-inst2`**.
   - Username: Enter username provided by A10 Networks Support
   - Password: Enter password provided by A10 Networks Support
3. Connect to the session.

   If the session connection is successful, the following response is displayed:

```
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--->
```

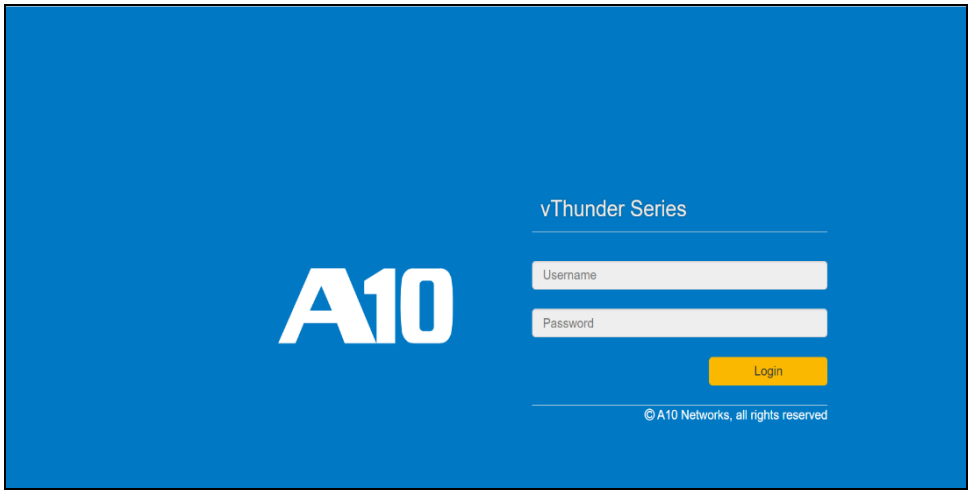
The vThunder instance is ready to use.

Access vThunder using GUI

To access the two vThunder instances using GUI, perform the following steps:

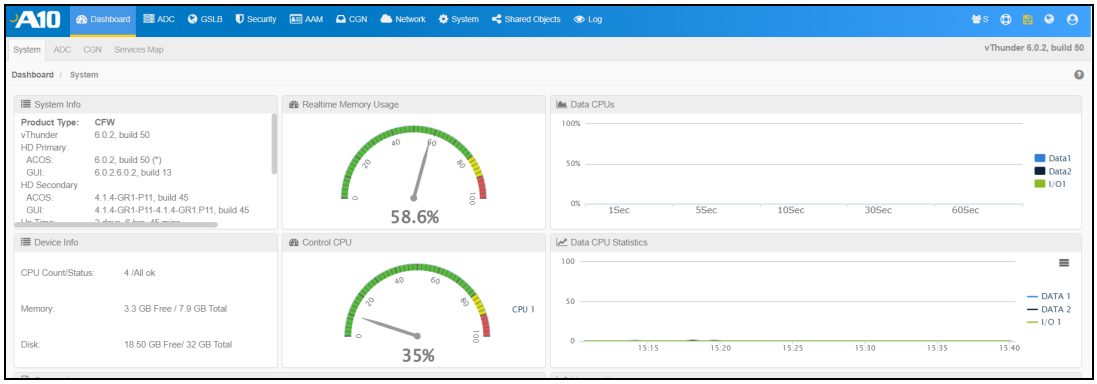
1. Open any browser.
2. Enter *https://<vthunder_public_IP>/gui/auth/login/* in the address bar.

Figure 62 : vThunder GUI



3. Enter the username and password provided by A10 Networks Support. The home page gets displayed.

Figure 63 : Home page



Configure Server VMSS

The following topics are covered:

- Create and Configure a VMSS Server Machine
- Verify the Server VMSS Creation

Create and Configure a VMSS Server Machine

To create a Server machine, perform the following steps:

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

   Project details

   - Subscription
   - Resource group

   Scale set details

   - Virtual machine scale set name - Server machine
   - Region

   Orchestration

   - Orchestration mode

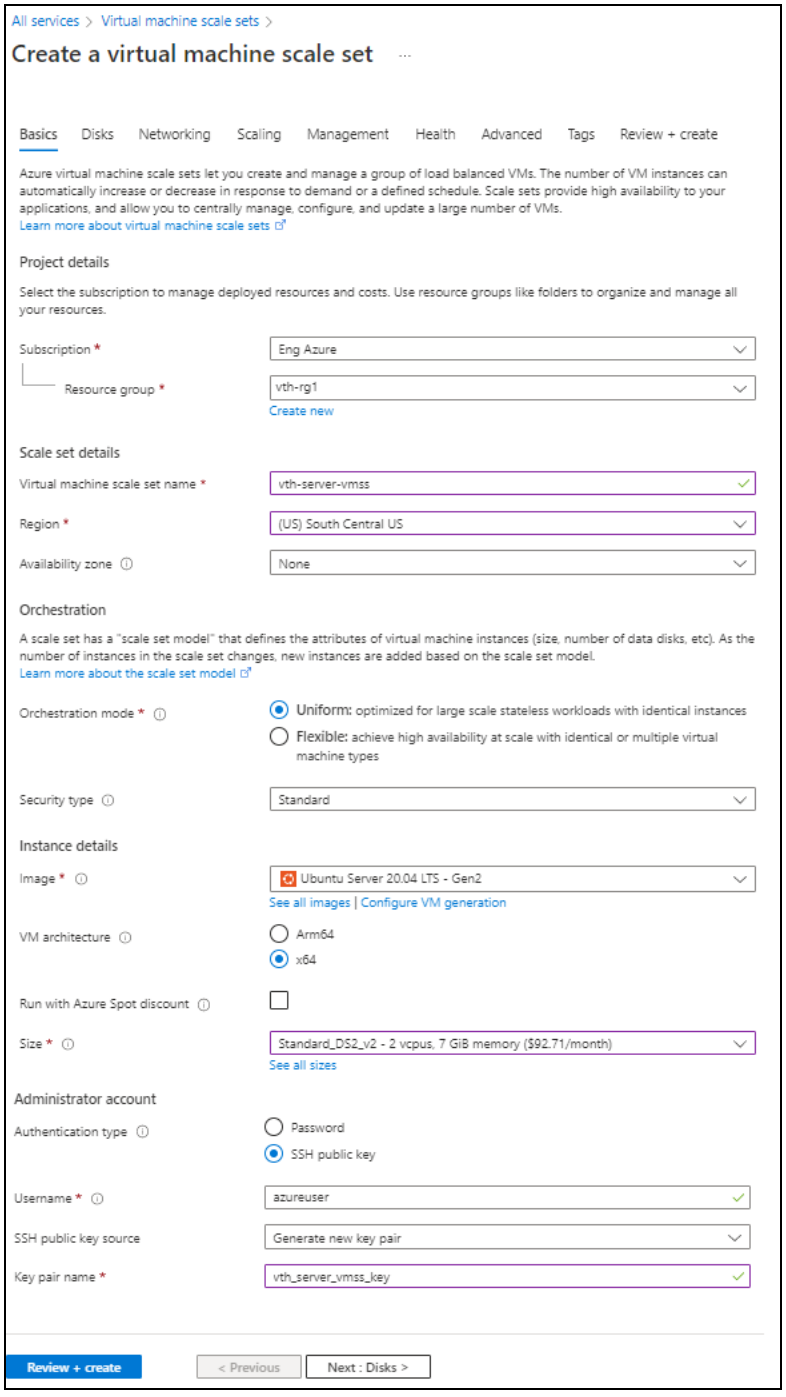
Instance details

- Image
- Size

Administrator account

- Authentication type - Provide the information accordingly.

Figure 64 : Create a virtual machine scale set window - Basics tab



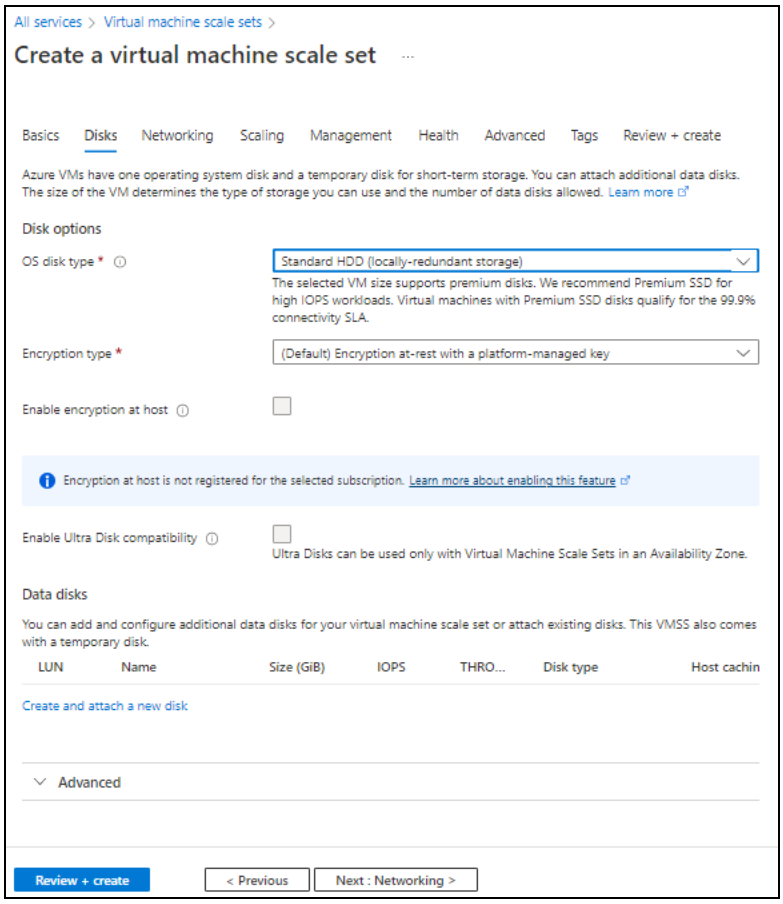
3. Leave the values in other fields unchanged and click **Next : Disks** at the bottom of the window.

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

   Disk options

   - OS disk type
   - Encryption type

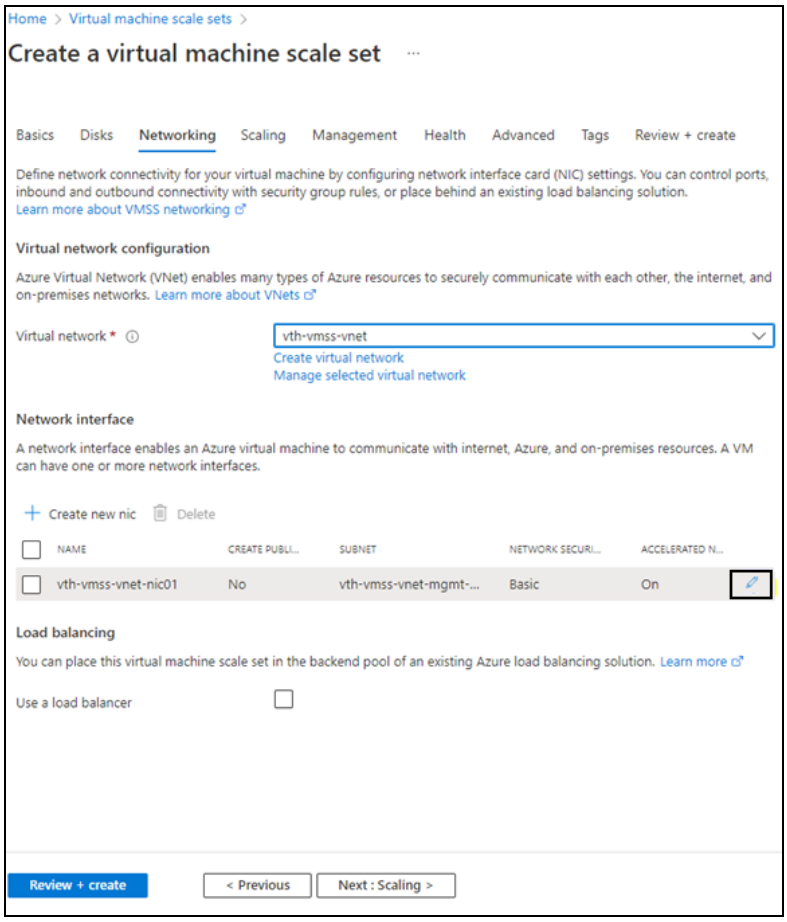
   Figure 65 : Create a virtual machine scale set window - Disks tab



5. Leave the values in other fields unchanged and click **Next : Networking** at the bottom of the window.

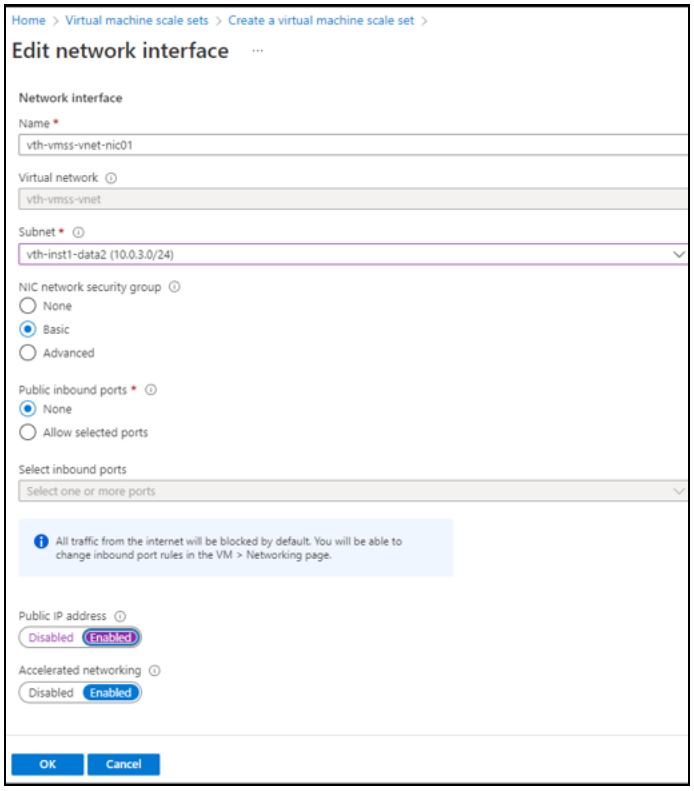
6. Select the Virtual network in the **Networking** tab.

Figure 66 : Create a virtual machine scale set window - Networking tab



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

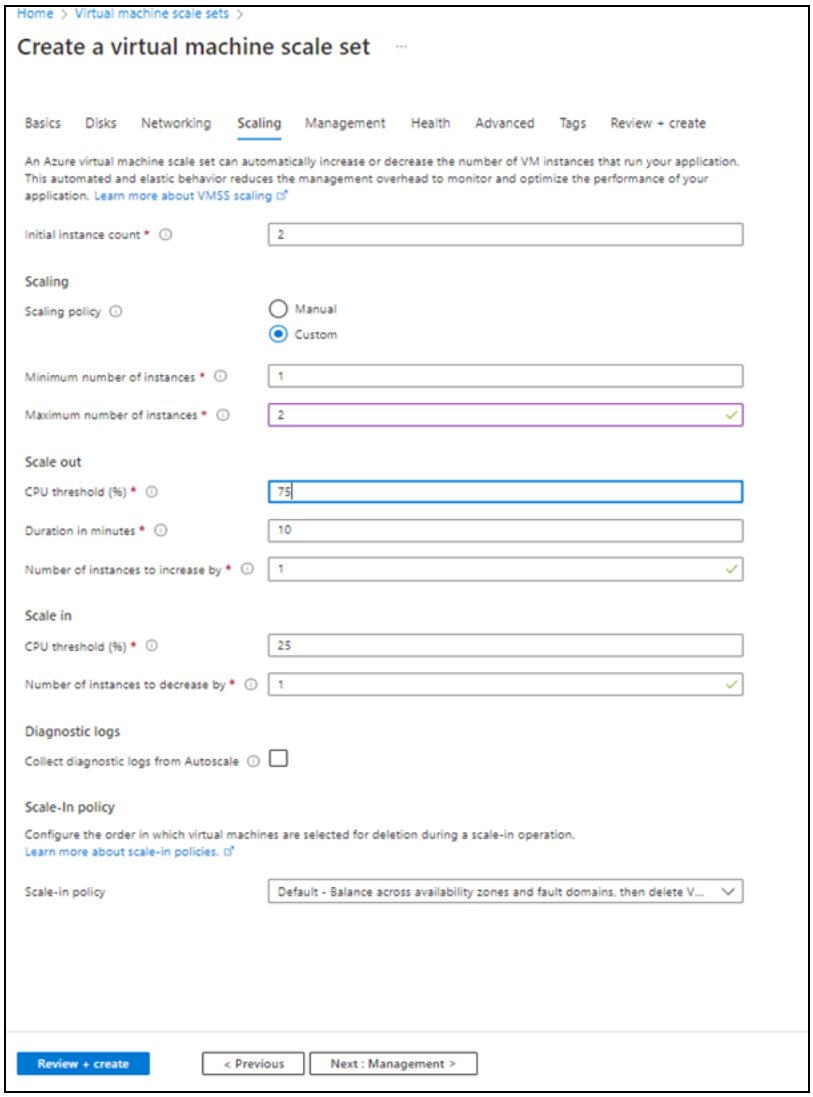
Figure 67 : Edit network interface window



9. Leave the values in other fields unchanged in the **Networking** tab and click **Next : Scaling** at the bottom of the window.

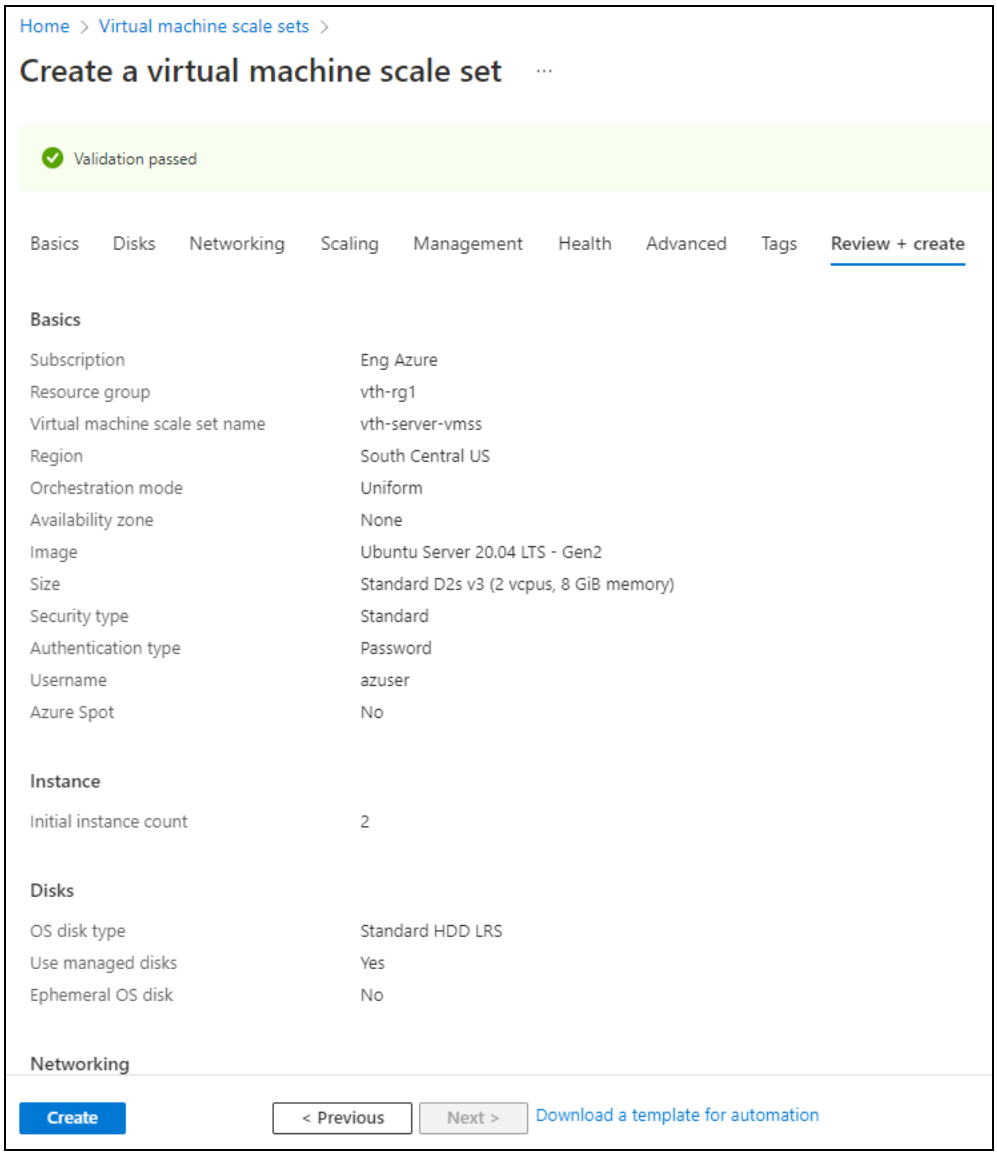
10. Select or enter the information in the **Scaling** tab as shown below.

Figure 68 : Create a virtual machine scale set window - Scaling tab



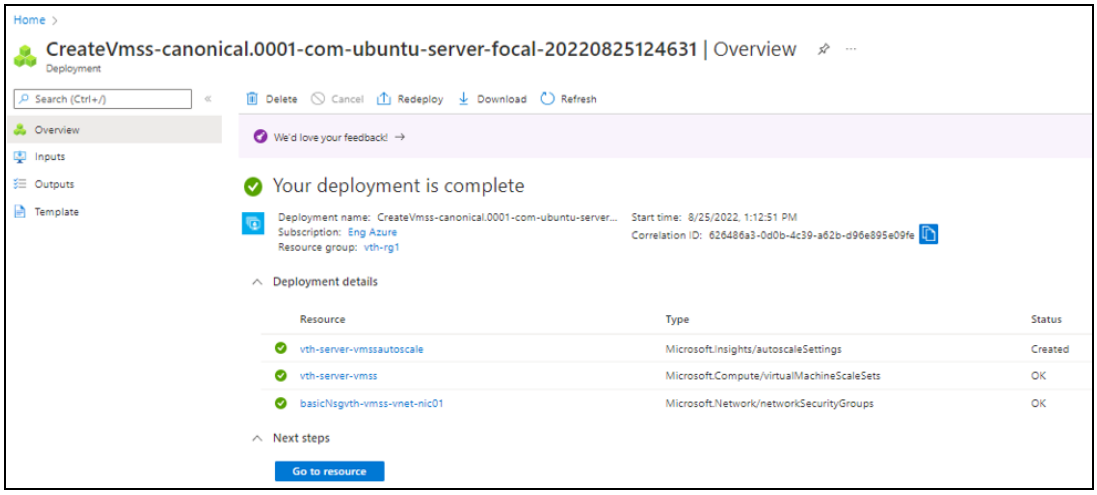
11. Click **Review + create** at the bottom of the window to skip the other tabs.

Figure 69 : 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 70 : Create VMSS window



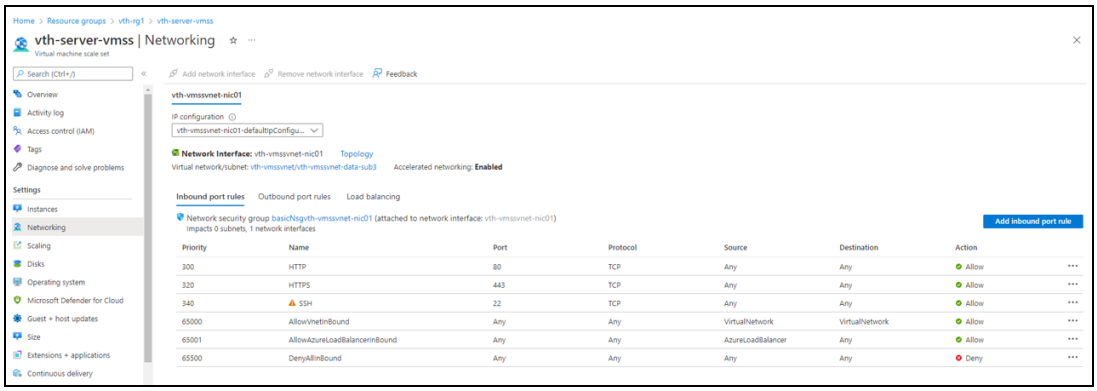
NOTE: It may take the system several minutes to display your resources.

Verify the Server VMSS Creation

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

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

   Figure 71 : VMSS > Inbound port rules



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

Apache:

```
sudo apt-get install apache2
```

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

Configure Client Machine

The following topic is covered:

- Create and Configure a Client Machine

Create and Configure a Client Machine

To create a Client machine, perform the following steps:

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

   Project details

   - Subscription
   - Resource group

   Instance details

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

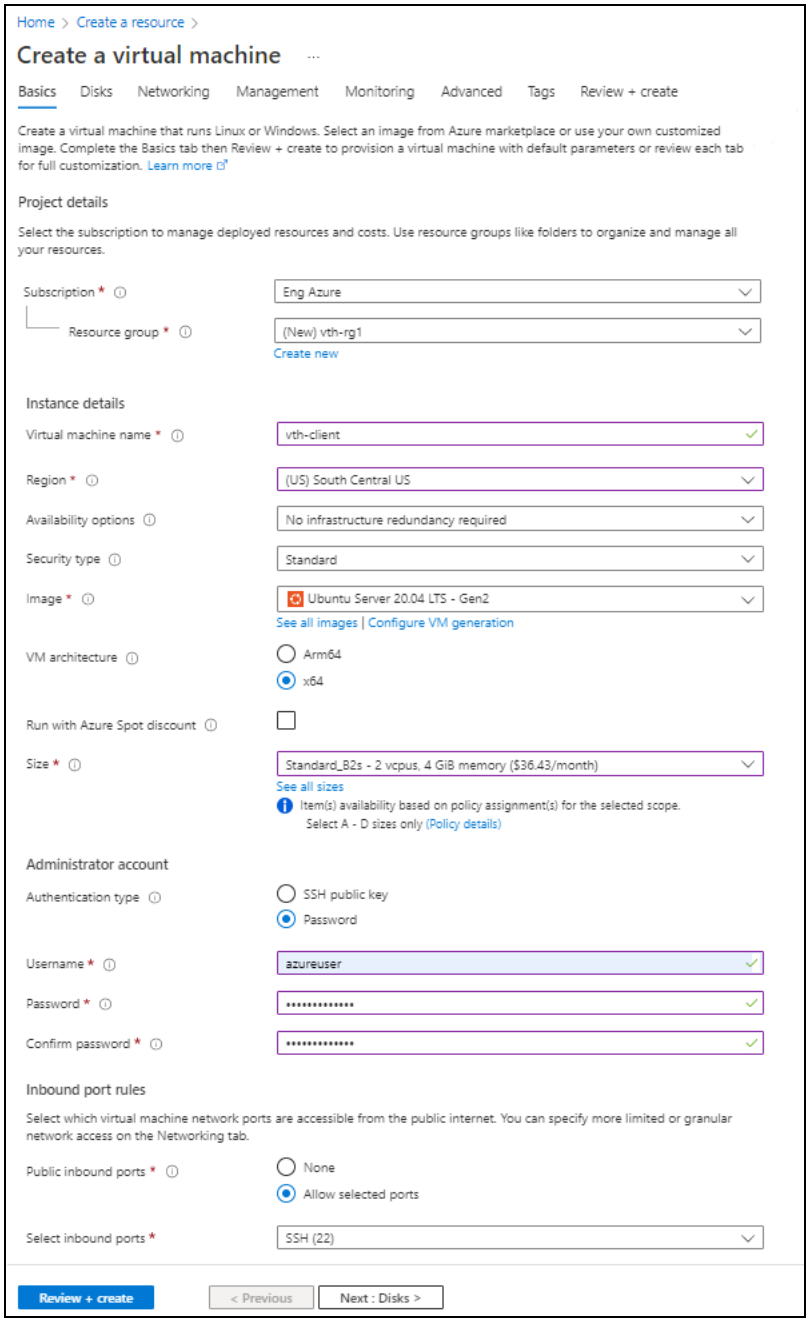
   Administrator account

   - Depending upon the Authentication type, provide the information.

   Inbound port rules

- Public inbound ports
- Select inbound ports

Figure 72 : Create a virtual machine window - Basics tab

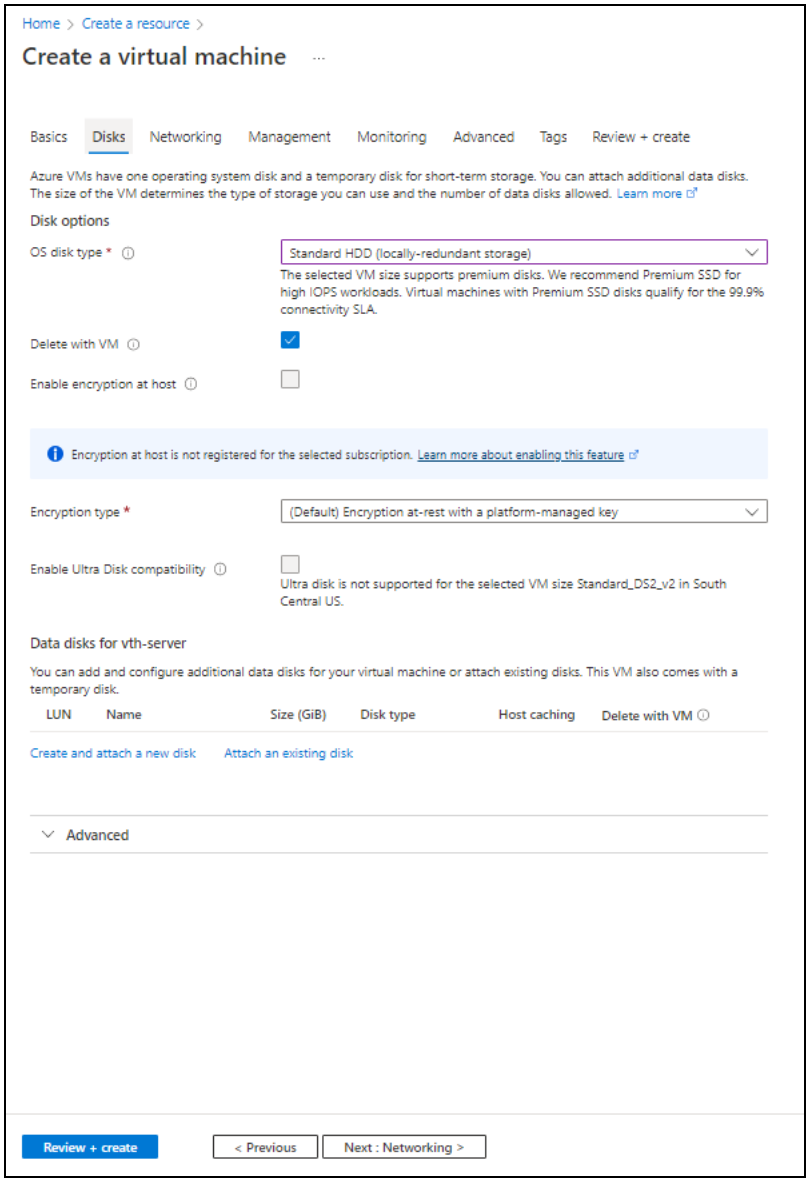


3. Leave the values in other fields unchanged and click **Next : Disks** at the bottom of the window.
4. Select or enter the following mandatory information in the **Disks** tab:

   Disk options

   - OS disk type
   - Encryption type

Figure 73 : Create a virtual machine window - Disks tab

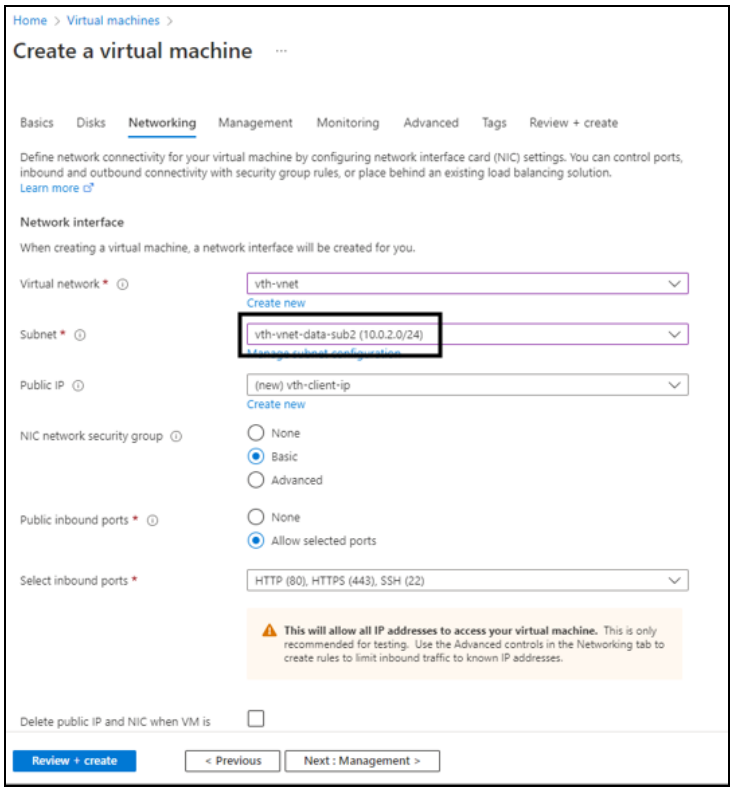


5. Leave the values in other fields unchanged and click **Next : Networking** at the bottom of the window.
6. Select or enter the following mandatory information in the **Networking** tab:

   Network interface

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

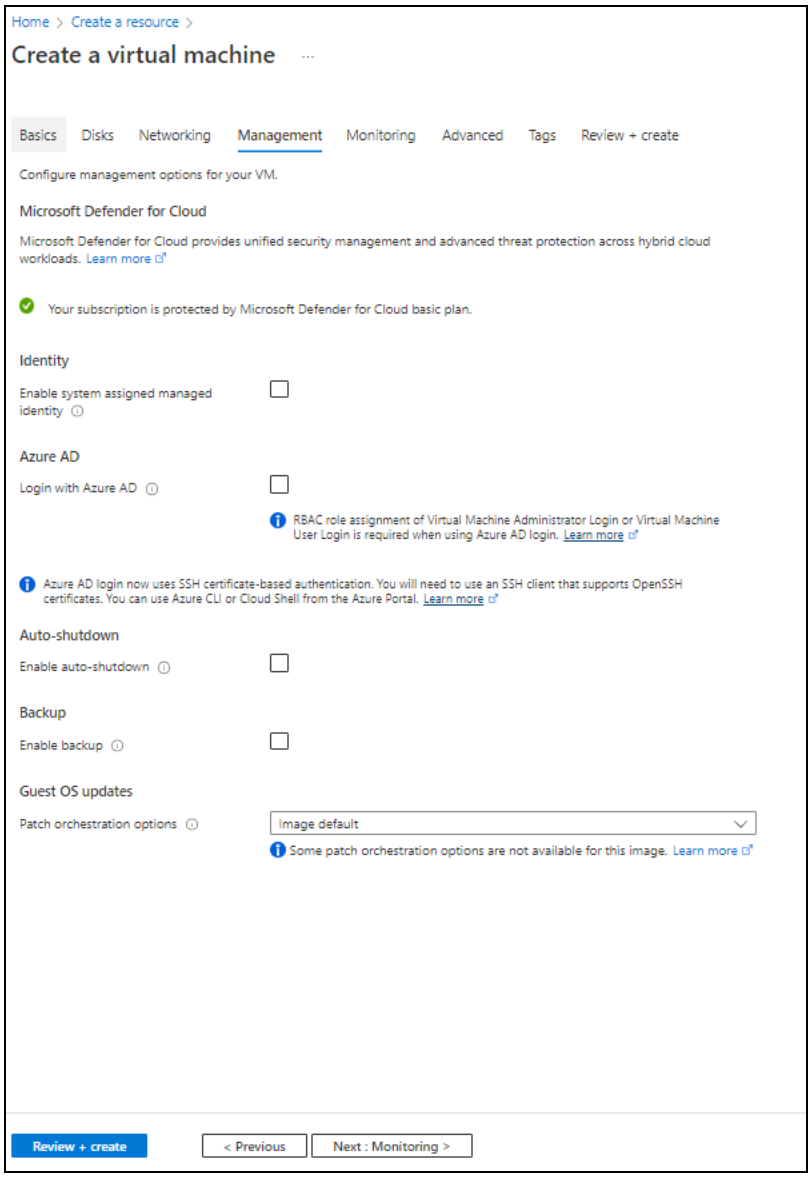
Figure 74 : Create a virtual machine window - Networking tab



7. Leave the values in other fields unchanged and click **Next : Management** at the bottom of the window.

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

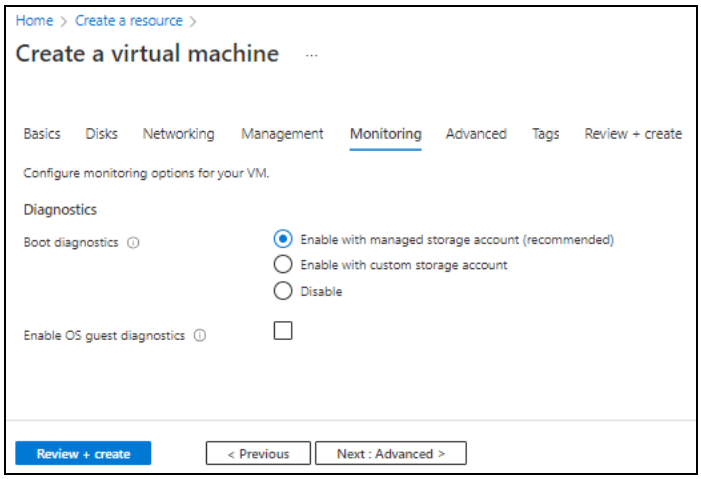
Figure 75 : Create a virtual machine window - Management tab



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

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

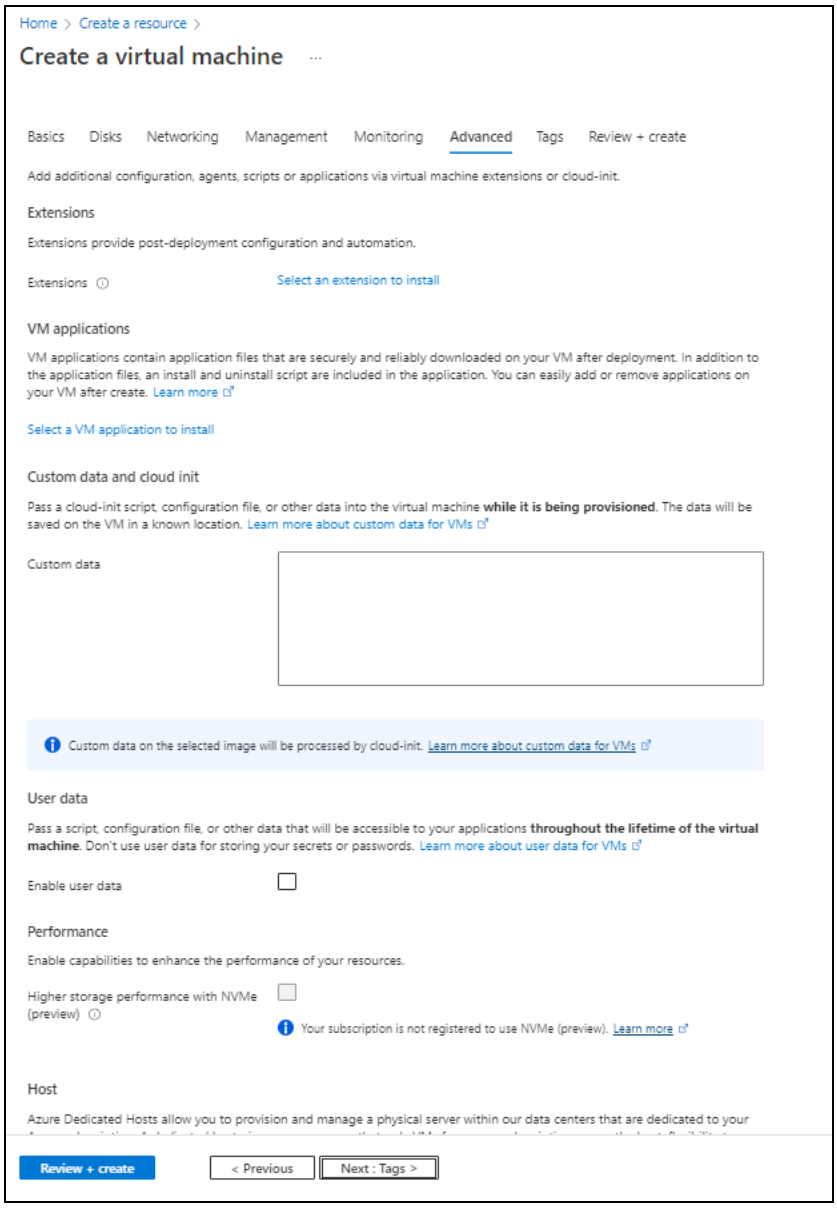
Figure 76 : Create a virtual machine window - Monitoring tab



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

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

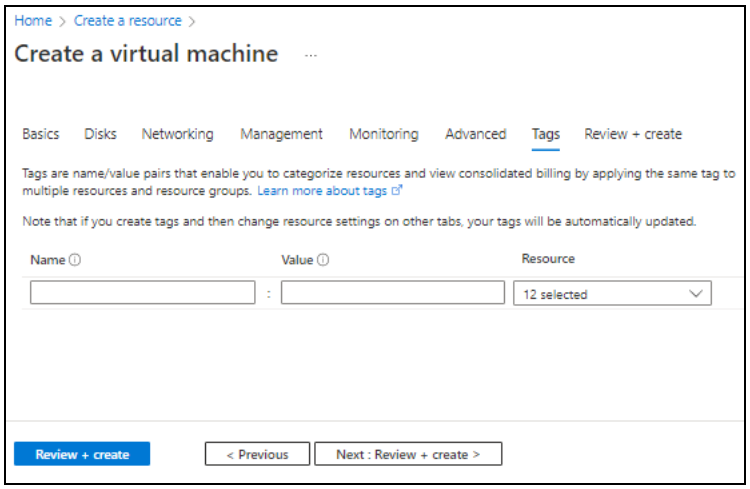
Figure 77 : Create a virtual machine window - Advanced tab



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

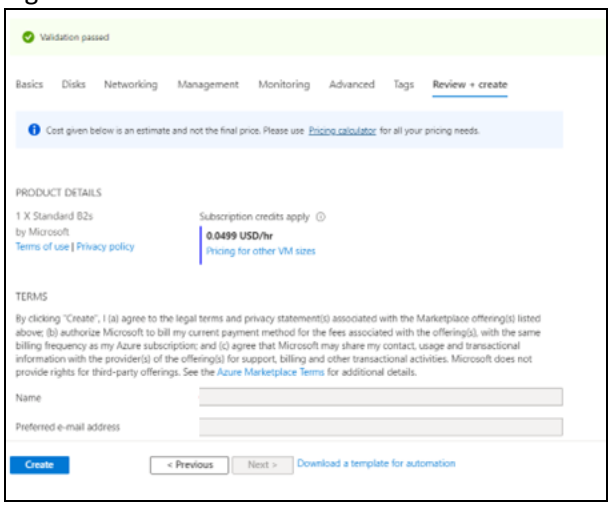
14. Select or enter the information in the **Tags** tab as needed.

Figure 78 : 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 79 : Create a virtual machine window - Review + create tab



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

Configure Thunder

The following configurations can be applied to the deployed vThunder instance:

- A10 License
- SSL Certificate
- Basic Server Load Balancer or Server Load Balancer on Backend Autoscale (depending on your use case, see Deployment Templates)
- Configure High Availability

Verify Deployment

To verify deployment using the ARM template, perform the following steps:

1. Run the following command on the active vThunder instance:

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

   If the deployment is successful with basic SLB, HA, HTTP template, and Persist-cookie template configuration, the following output is displayed:

```
!
vrrp-a common
  device-id 1
  set-id 1
  enable
!
terminal idle-timeout 0
!
ip dns primary 8.8.8.8
!
!
interface ethernet 1
  enable
  ip address dhcp
!
interface ethernet 2
  enable
  ip address dhcp
!
vrrp-a vrid 0
  floating-ip 10.0.3.8
  floating-ip 10.0.2.9
  blade-parameters
    priority 100
!
vrrp-a peer-group
  peer 10.0.2.7
  peer 10.0.2.6
!
ip route 0.0.0.0 /0 10.0.2.1
!
slb server s1 10.0.3.4
  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 template persist cookie persist-cookie
  expire 60
  encrypt-level 0
  name a10-cookies
  match-type service-group
!
slb template http hostname-test
  host-switching contains s1 service-group sg80
!
slb template http url-test
  url-switching regex-match s1 service-group sg80
!
slb virtual-server vip 10.0.2.9
  port 53 udp
    source-nat auto
    service-group sg53
  port 80 http
    source-nat auto
    service-group sg80
    template persist cookie persist-cookie
    template http url-test
  port 443 https
    source-nat auto
    service-group sg443
!
!
end
```

2. Run the following command on active vThunder instance to verify the SSL

Certificate configuration:

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

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

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

3. Run the following command on active vThunder instance to verify the GLM License Provision configuration:

```
vThunder-Active(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
```

4. Run the following command on the standby vThunder instance:

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

If the deployment is successful with basic SLB, HA, HTTP template, and Persist-cookie template configuration, the following output is displayed:

```
!
vrrp-a common
  device-id 2
  set-id 1
  enable
!
!
system password-policy complexity Default username-check enable
system password-policy complexity Default repeat-character-check enable
system password-policy complexity Default forbid-consecutive-character
4
!
terminal idle-timeout 0
!
ip dns primary 8.8.8.8
!
!
interface ethernet 1
  enable
  ip address dhcp
!
interface ethernet 2
  enable
  ip address dhcp
!
vrrp-a vrid 0
  floating-ip 10.0.3.8
  floating-ip 10.0.2.9
  blade-parameters
    priority 99
!
vrrp-a peer-group
  peer 10.0.2.7
  peer 10.0.2.6
!
ip route 0.0.0.0 /0 10.0.2.1
!
```

```
slb server s1 10.0.3.4
  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 template persist cookie persist-cookie
  expire 60
  encrypt-level 0
  match-type service-group
!
slb template http hostname-test
  host-switching contains s1 service-group sg80
!
slb template http url-test
  url-switching regex-match s1 service-group sg80
!
slb virtual-server vip 10.0.2.9
  port 53 udp
    source-nat auto
    service-group sg53
  port 80 http
    source-nat auto
    service-group sg80
    template persist cookie persist-cookie
    template http url-test
  port 443 https
    source-nat auto
    service-group sg443
```

```
!
!
end
```

5. Run the following command to force stop the active vThunder instance and make the standby vThunder instance as active device:

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

6. Run the following command to disable the active standby vThunder instance:

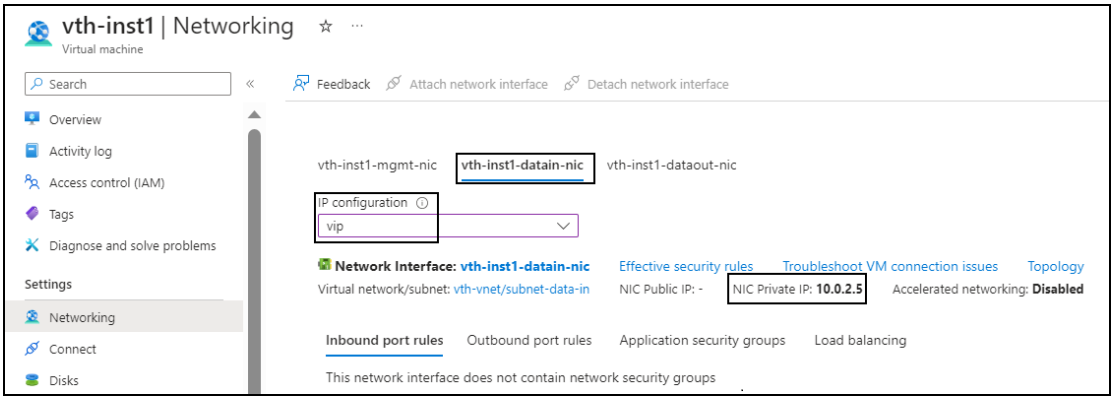
```
vThunder-ForcedStandby(config)#vrrp-a force-self-standby disable
vThunder-Active(config)#
```

Verify Traffic Flow

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

1. From **Azure Portal** > **Azure services** > **Resource Group** > <*resource_group_name*> > <*active_virtual_machine_instance*> > **Settings** > **Networking**.
   Here, **`vth-inst1`** is the active vThunder instance name.
2. Select the Datain NIC tab > **IP configuration** > **`vip`**. Here, Datain NIC is **`vth-inst1-datain-nic`**.
3. Copy the VIP address of the active vThunder instance.

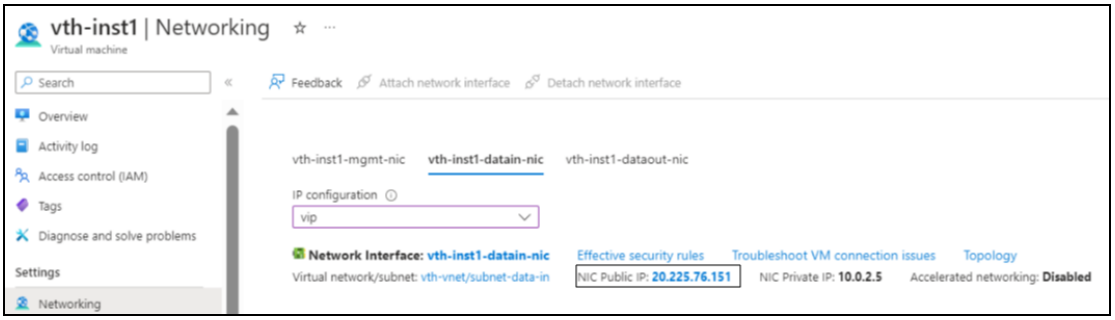
   Figure 80 : Active vThunder instance 1 VIP



4. Select your client instance from the **Virtual machine** list.
   Here, **`vth-client`** is the client instance name.

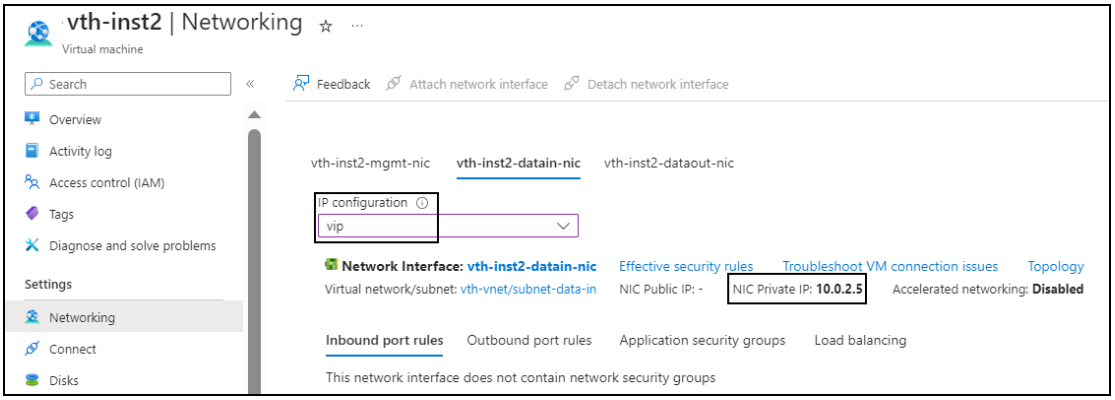
5. SSH your client machine and run the following command to verify the traffic flow:
   ```
   curl <vThunder_instance1_datain-nic_vip_private_ip>
   ```
   Example
   ```
   curl 10.0.2.5
   ```
   Verify if a response is received.
   curl *<vThunder_instance1_datain-nic_vip_private_ip>*
6. Copy the Public IP address of the active vThunder instance 1 data subnet 1.

   Figure 81 : Active vThunder instance 1 Public IP address



7. Run the following command from the client machine to verify the traffic flow:
   ```
   curl <vThunder_instance1_datain-nic_vip_public_ip>
   ```
   Example
   ```
   curl 20.225.76.151
   ```
   Verify if a response is received.
8. After the switchover, vThunder instance 2 is active, so copy the VIP address of the vThunder instance 2.

Figure 82 : Active vThunder instance 2 VIP



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

```
curl <vThunder_instance2_datain-nic_vip_private_ip>
```

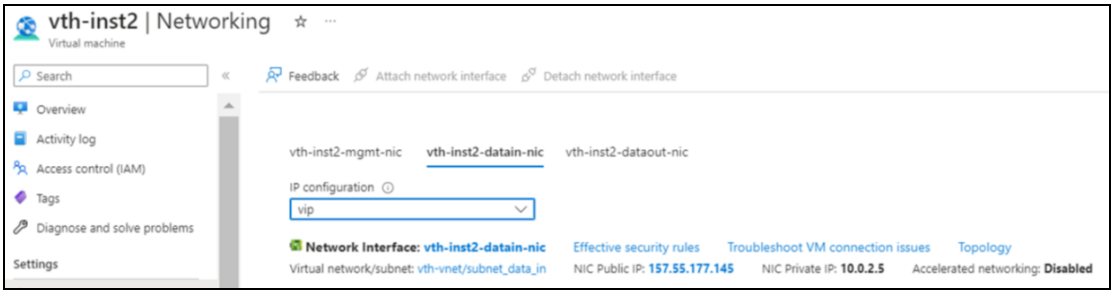
Example

```
curl 10.0.2.5
```

Verify if a response is received.

10. Copy the Public IP address of the active vThunder instance 2 data subnet 1.

Figure 83 : Active vThunder instance 2 Public IP address



11.

12. Run the following command from the client machine to verify the traffic flow:

```
curl <vThunder_instance2_datain-nic_vip_public_ip>
```

Example

```
curl 157.55.177.145
```

Verify if a response is received.

13. SSH your client machine and run the following command to verify the HTTP template traffic flow:

```
curl <vThunder_instance_datain-nic_vip_private_ip>:<port_number>/<host-match-string or url-match-string>/
```

Example

```
curl 10.0.2.5:80/s1/
```

Verify if a response is received from client server (For example: Apache Index page).

14. SSH your client machine and run the following commands to verify the Persist cookie template traffic flow:

    a. Verify the current cookie configuration:

    ```
    curl --head <vThunder_instance_datain-nic_vip_private_ip>
    ```

    b. Run the following commands to save the cookies in the **cookie.txt** file:

    ```
    curl -b cookie.txt -c cookie.txt <vThunder_instance_datain-nic_vip_private_ip>
    cat cookie.txt
    ```

    Example

    ```
    curl --head 10.0.2.5
    curl -b cookie.txt -c cookie.txt 10.0.2.5
    cat cookie.txt
    ```

15. Run the following command on the active vThunder instance to view the persistence load-balancing statistics:

```
vThunder(config)#show slb persist
```

If the deployment is successful, the following summary persistence statistics is displayed:

```
                                        Total
-----------------------------------------------
URL hash persist (pri)                   0
URL hash persist (sec)                   0
URL hash persist fail                    0
SRC IP persist ok                        0
SRC IP persist fail                      0
SRC IP hash persist(pri)                 0
SRC IP hash persist(sec)                 0
SRC IP hash persist fail                 0
DST IP persist ok                        0
DST IP persist fail                      0
DST IP hash persist(pri)                 0
DST IP hash persist(sec)                 0
DST IP hash persist fail                 0
SSL SID persist ok                       0
SSL SID persist fail                     0
Cookie persist ok                        1
Cookie persist fail                      0
Persist cookie not found                 2
Persist cookie Pass-thru                 0
Enforce higher priority                  0
```

If the Persist-cookie configuration is successful, a value is displayed for the **`Cookie persist ok`** else the value is 0.

Thunder-3NIC-3VM

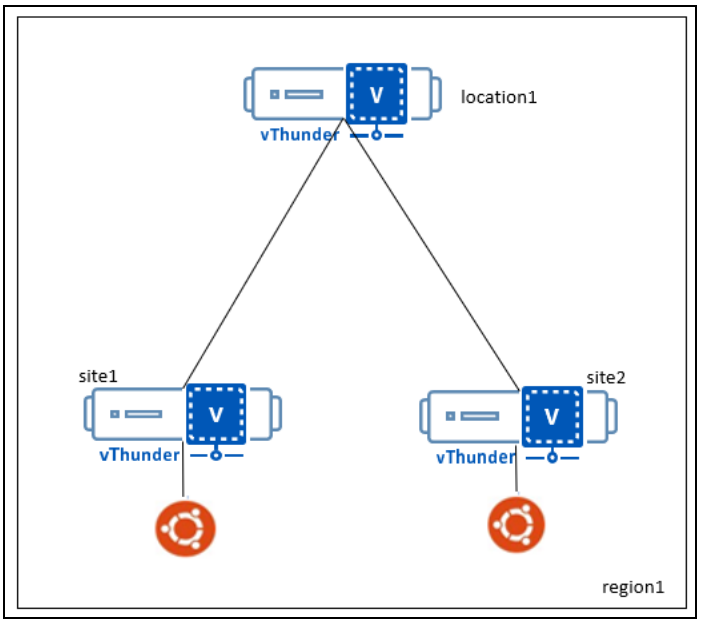
This template creates three new virtual machine with pre-loaded Thunder instance in the same region and zone and attaches three new network interface cards (NICs). These three vThunder instances are referred as Master Controller (Active), Site1 and Site2. Same template can be used to install identical number of resources in another region. The three vThunder instances in another region are referred as Member Controller, Site1 and Site2.

This template is used to setup disaster recovery site in a cross-region or hybrid cloud environment.

For more information, see Create Thunder Virtual Machines.

NOTE: Use a suitable VM size that supports at least three NICs. For VM sizes, see Supported VM Sizes.

Figure 84 : Thunder ADC with GSLB



Additional Thunder configurations are available that can be applied as needed:

- Change Password
- A10 License
- SSL Certificate
- Hybrid Cloud GSLB

Various templates are available for different deployment needs.

For more information, see Deployment Templates.

The following topics are covered:

Create Thunder Virtual Machines

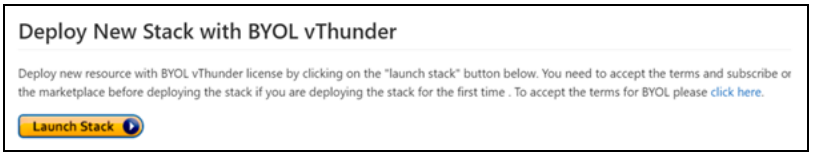
The A10-vThunder-3NIC-3VM template is used to create three Thunder virtual machines with three network interface cards each. This template is deployed using Azure Portal Console.

Before deploying this template, it is recommended to review the Prerequisites.

To deploy the A10-vThunder-3NIC-3VM template using Azure Portal Console, perform the following steps:

1. Download A10-vThunder-3NIC-3VM template.
2. From GitHub, click **Launch Stack**.

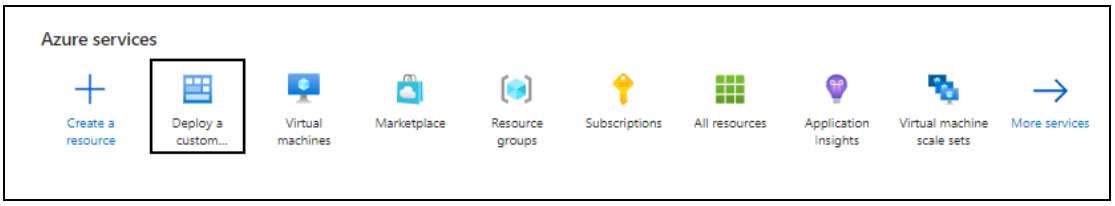
Figure 85 : GitHub



Or

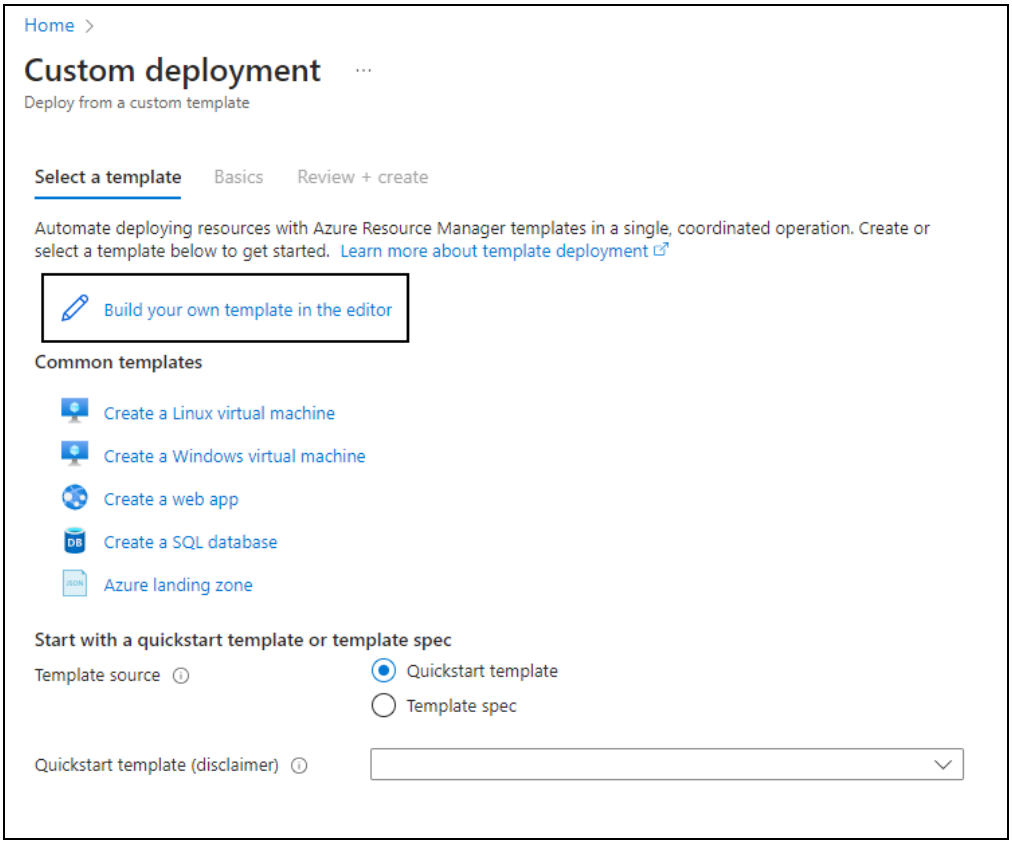
From the **Azure Portal** > **Azure services**, click **Deploy a custom template**.

Figure 86 : Azure services



3. Under the **Custom deployment** window > **Select a template** tab, click **Build your own template in the editor**.

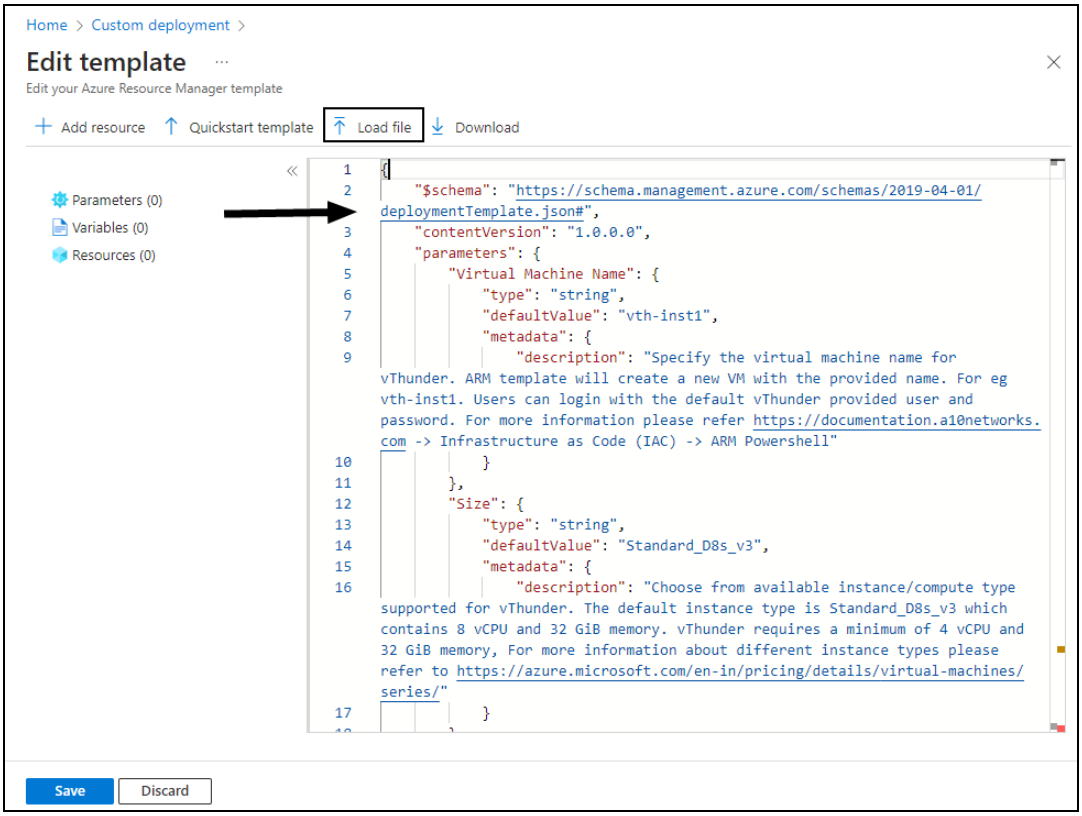
Figure 87 : Custom deployment window



4. From the **Edit template** window, perform either of the following step:

   - Click **Load file** and browse to the folder where you have downloaded the ARM template. Select **ARM_TMPL_3NIC_3VM.json** to upload.
   - From Windows Explorer, navigate to the folder where you have downloaded the ARM template. Copy **ARM_TMPL_3NIC_3VM.json** content and paste it in the editor.

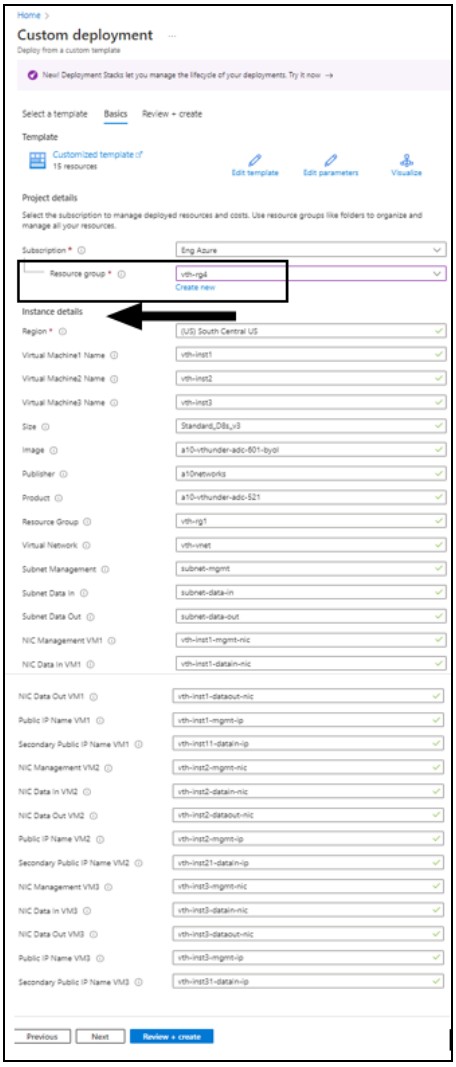
Figure 88 : Edit template window



5. Click **Save**.

   The **Custom deployment** window is displayed with the template parameters and default values.

Figure 89 : Custom deployment template



6. Select an existing or create a new **Resource group** under which you want to deploy the custom template resources.

NOTE: Hover ⓘ for description of each corresponding parameter.

7. Update the default values and also provide the values in the empty fields as appropriate in the **Instance details** section shown in Figure 89.

NOTE: Use a suitable VM size that supports at least three NICs. For VM sizes, see Supported VM Sizes.

8. Click **Review+create**.

   The validation appears.

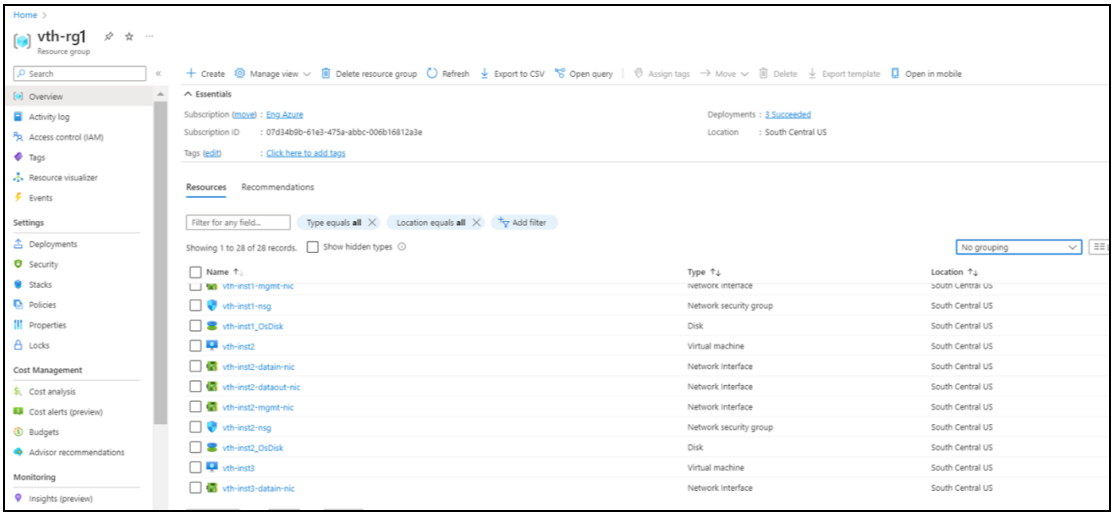
9. Click **Create**.

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

10. Verify if all the above listed resources are created under **Home** > **Azure services** > **Resource Groups** > <*resource_group_name*>:

    - Three vThunder instances
    - Three network security groups
    - One management and two data interface for each vThunder instance
    - Public IPs for each vThunder instance
    - Virtual private network

Figure 90 : Resource listing under resource group



11. Verify if all the vThunder instances that are created are up and running.

Access Thunder Virtual Machine

The Thunder virtual machine can be accessed using any of the following ways:

- Access vThunder using CLI
- Access vThunder using GUI

Access vThunder using CLI

To access vThunder using CLI, perform the following steps:

1. Open any SSH client.
2. Enter or select the following basic information in the configuration window:
   - Hostname: Public IP of virtual machine instance
     Here, Public IP of **`vth-inst1, vth-inst2, vth-inst3`**

     To get the Public IP address of the vThunder instances, see Get IP Address.
   - Username: Enter username provided by A10 Networks Support
   - Password: Enter password provided by A10 Networks Support
3. Connect to the session.

   If the session connection is successful, the following response is displayed:

```
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--->
```

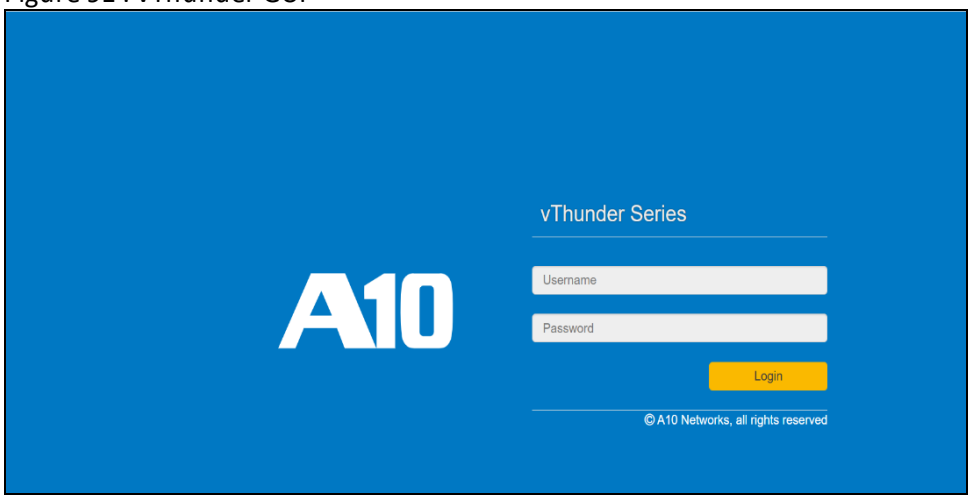
   The vThunder instance is ready to use.

Access vThunder using GUI

To access vThunder using GUI, perform the following steps:

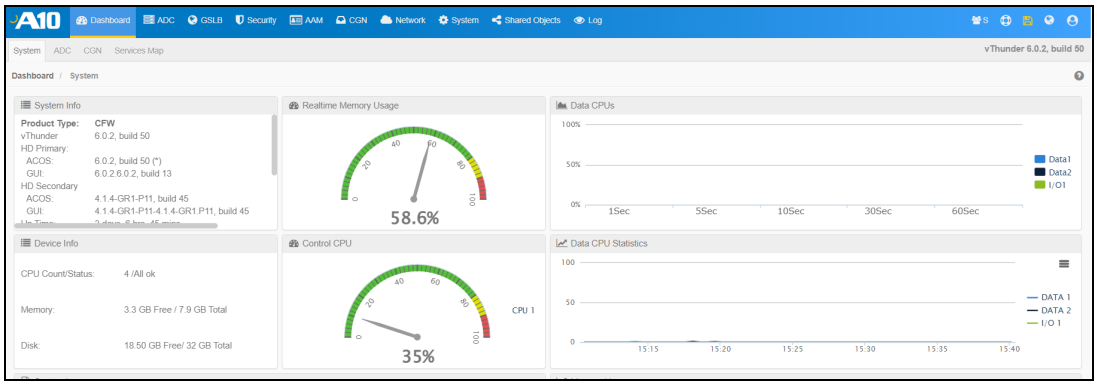
1. Open any browser.
2. Enter *https://<vthunder_public_IP>* in the address bar.

Figure 91 : vThunder GUI



3. Enter the username and password provided by A10 Networks Support. The home page gets displayed.

Figure 92 : Home page



Configure Server and Client Machine

The following topics are covered:

- Create and Configure a Server Machine
- Create and Configure a Client Machine

Create and Configure a Server Machine

To create a Server machine, perform the following steps:

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

   Project details

   - Subscription
   - Resource group

   Instance details

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

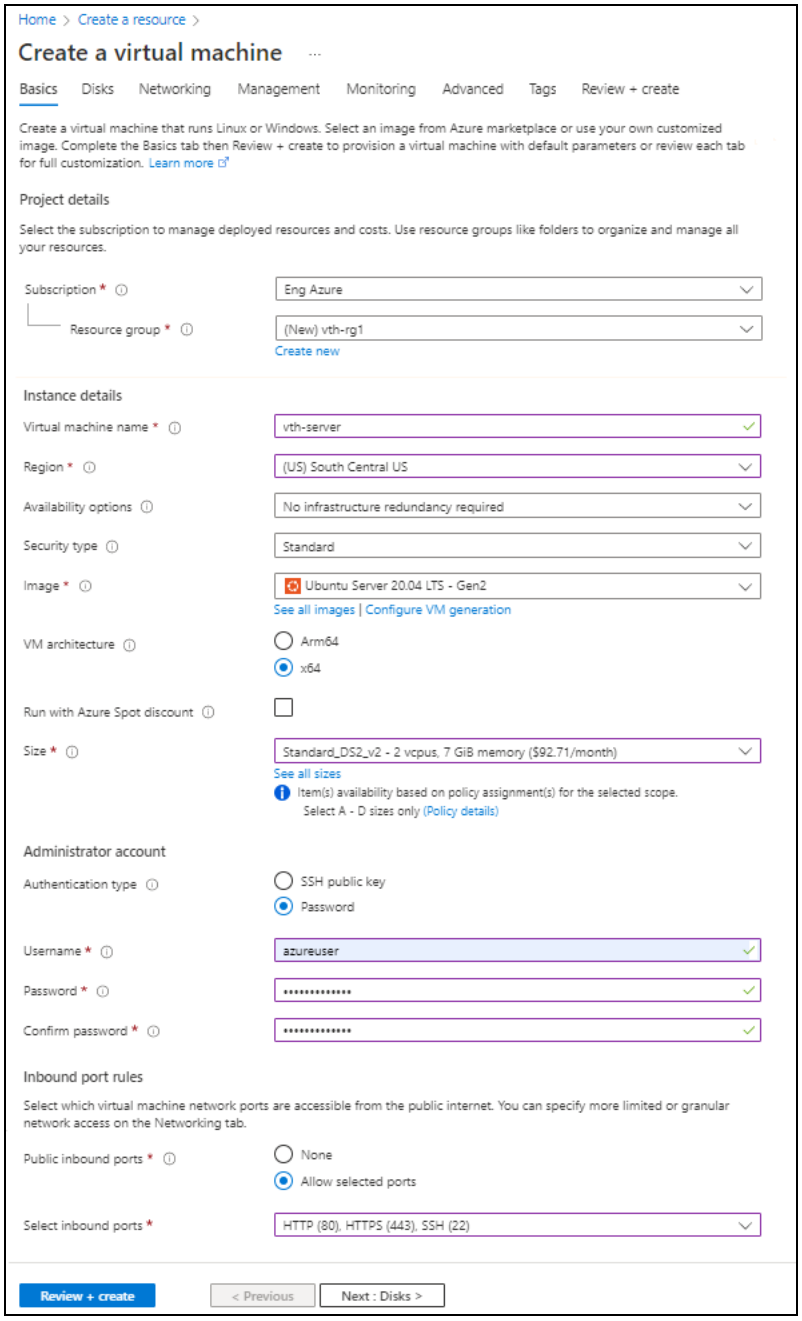
   Administrator account

   - Depending upon the Authentication type, provide the information.

   Inbound port rules

   - Public inbound ports
   - Select inbound ports

Figure 93 : Create a virtual machine window - Basics tab



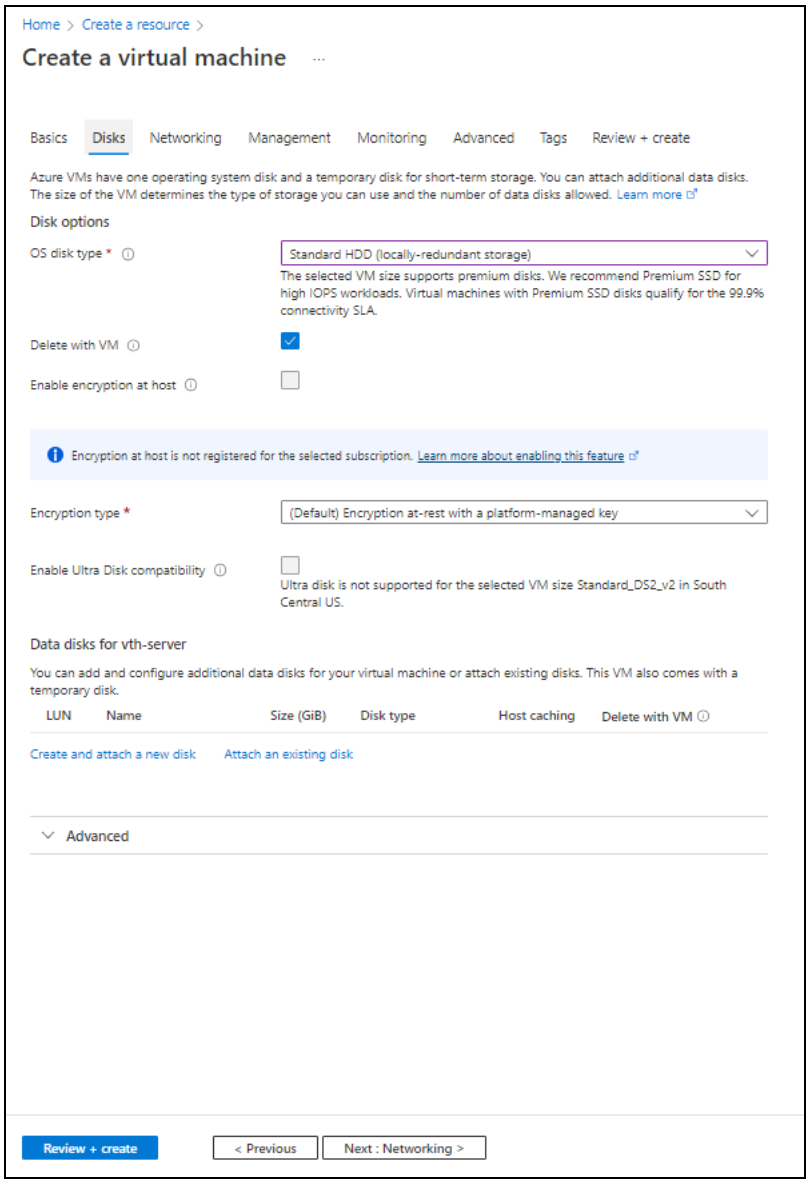
3. Leave the values in other fields unchanged and click **Next : Disks** at the bottom of the window.

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

   Disk options

   - OS disk type
   - Encryption type

Figure 94 : Create a virtual machine window - Disks tab

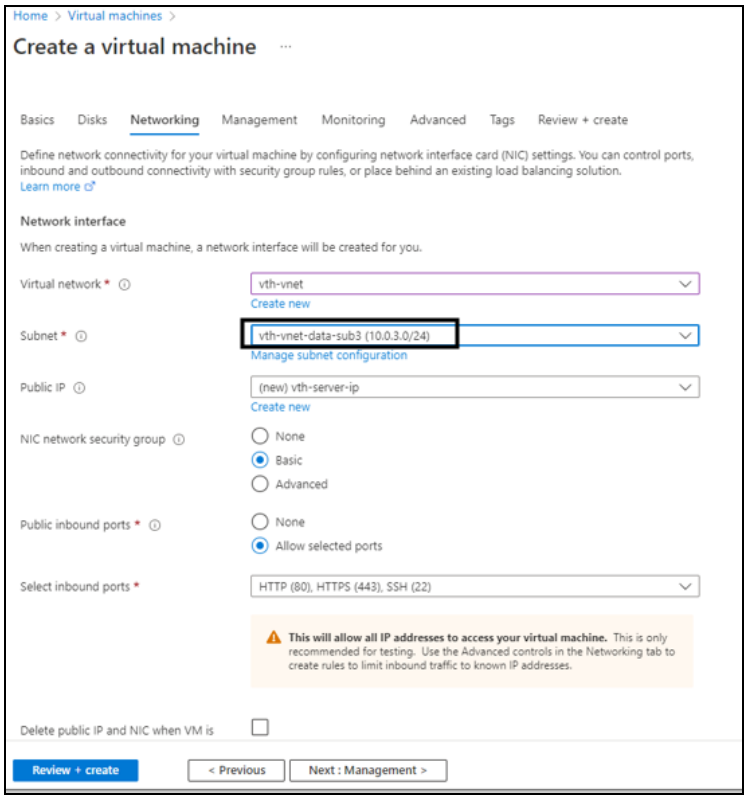


5. Leave the values in other fields unchanged and click **Next : Networking** at the bottom of the window.
6. Select or enter the following mandatory information in the **Networking** tab:

   Network interface

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

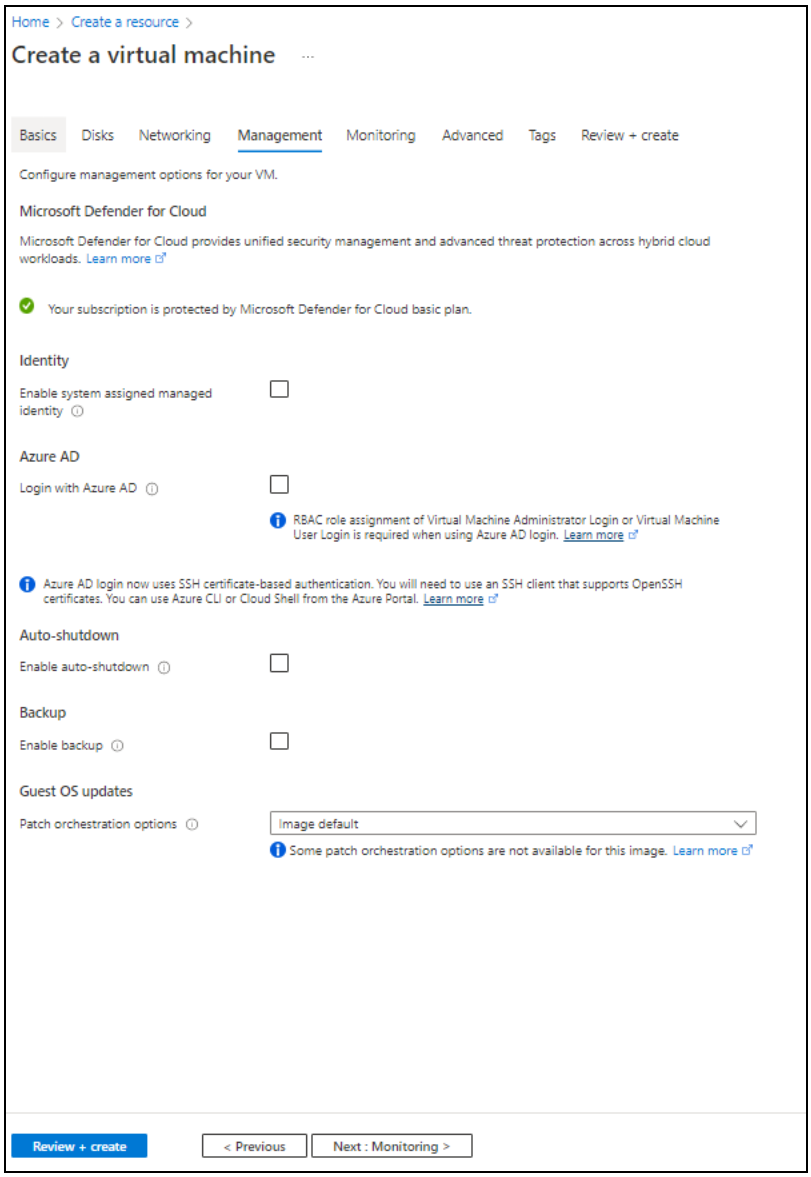
   Figure 95 : Create a virtual machine window - Networking tab



7. Leave the values in other fields unchanged and click **Next : Management** at the bottom of the window.

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

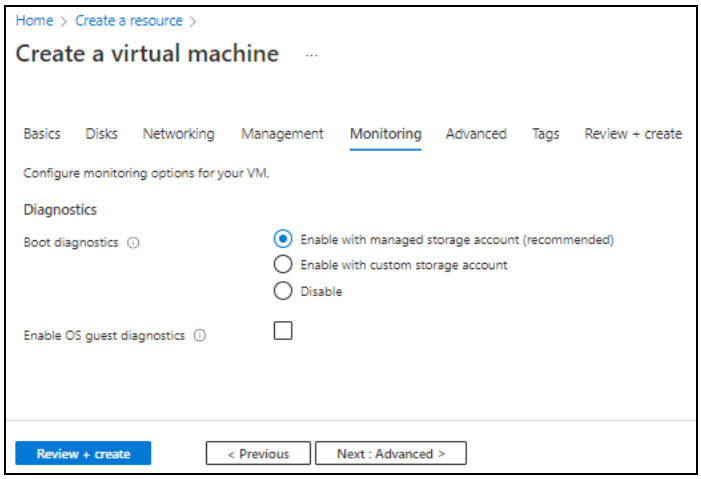
Figure 96 : Create a virtual machine window - Management tab



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

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

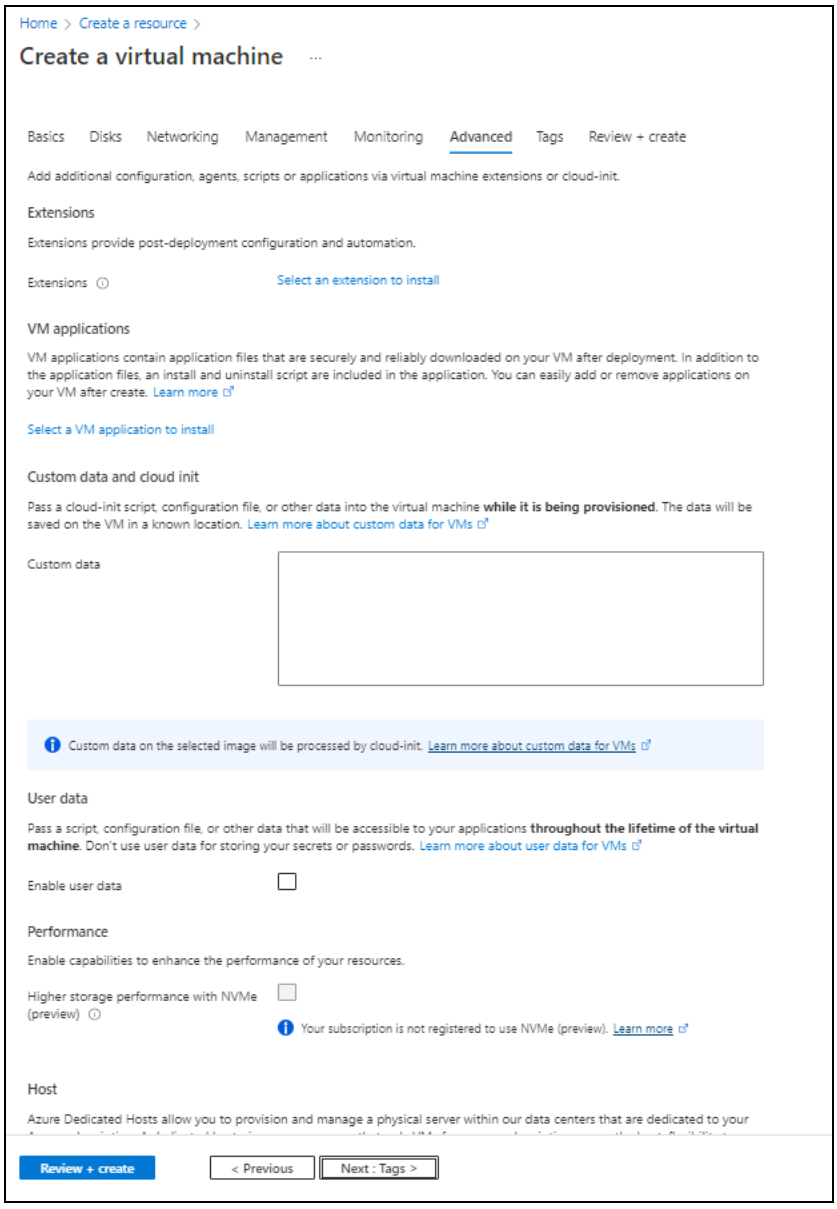
Figure 97 : Create a virtual machine window - Monitoring tab



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

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

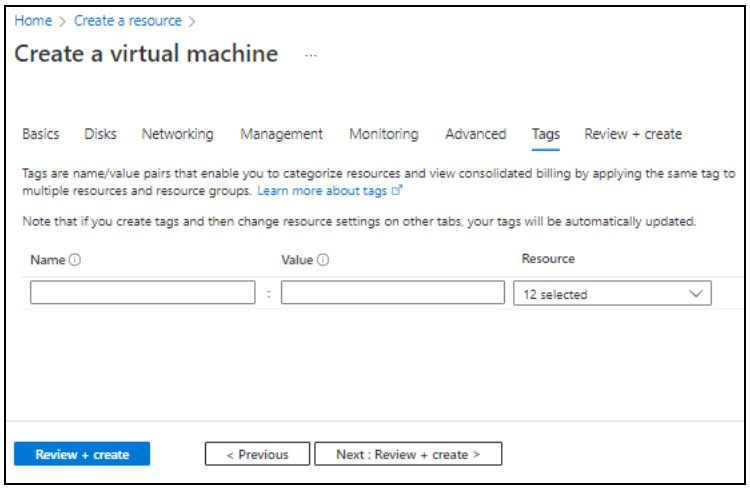
Figure 98 : Create a virtual machine window - Advanced tab



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

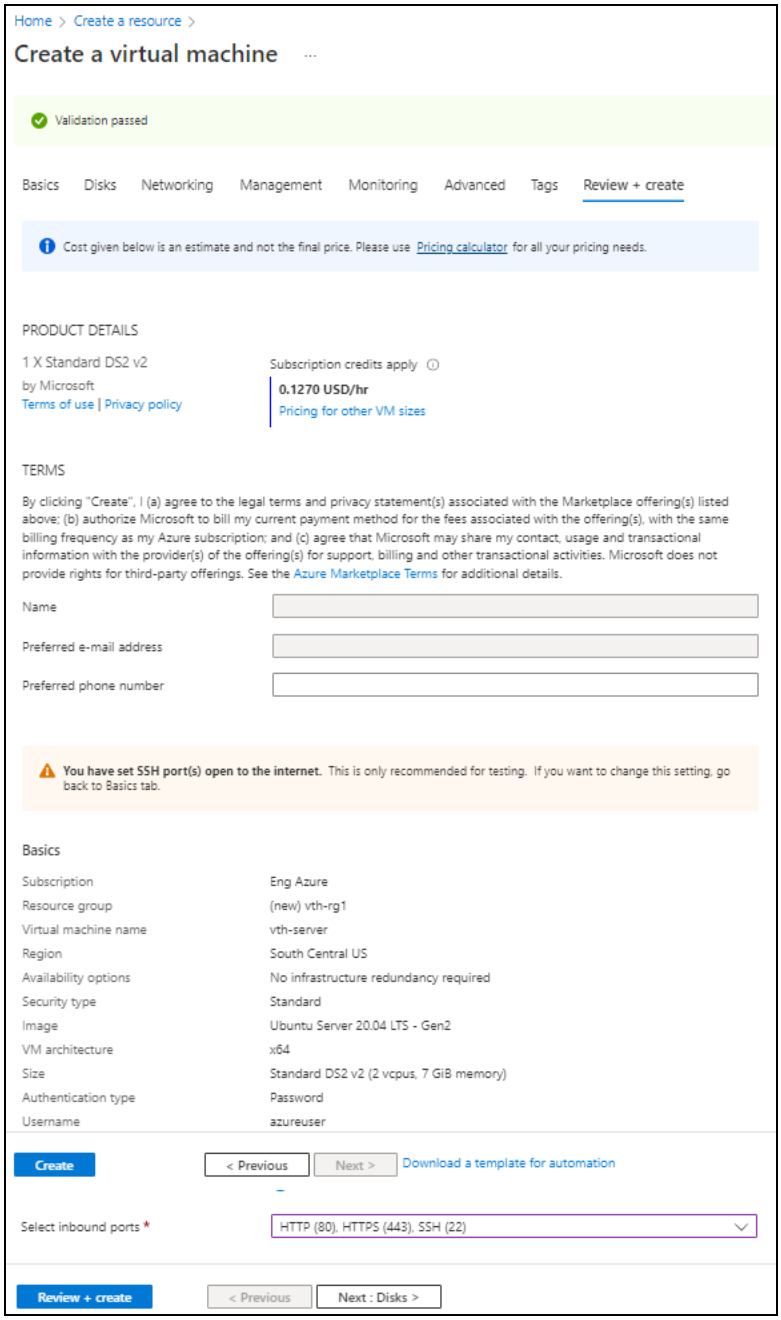
14. Select or enter the information in the **Tags** tab as needed.

Figure 99 : 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 100 : Create a virtual machine window - Review + create tab



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

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

```
sudo apt install apache2
```

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

18. If you want to configure HTTP template, perform the following steps:

    a. SSH the Apache Server and run the following command:

    ```
    sudo vim /etc/apache2/apache2.conf
    ```

    The Apache2 configuration file is displayed.

    b. Add the following configuration and save the file:

    ```
    Alias /<url-match-string> /var/www/html
    ```

    c. Restart the Apache server to enable the HTTP service.

    ```
    sudo systemctl restart apache2
    ```

    The server may take a few minutes to restart.

Create and Configure a Client Machine

To create a Client machine, perform the following steps:

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

   Project details

   - Subscription
   - Resource group

   Instance details

   - Virtual machine name - Client machine
   - Region

- Image
- Size

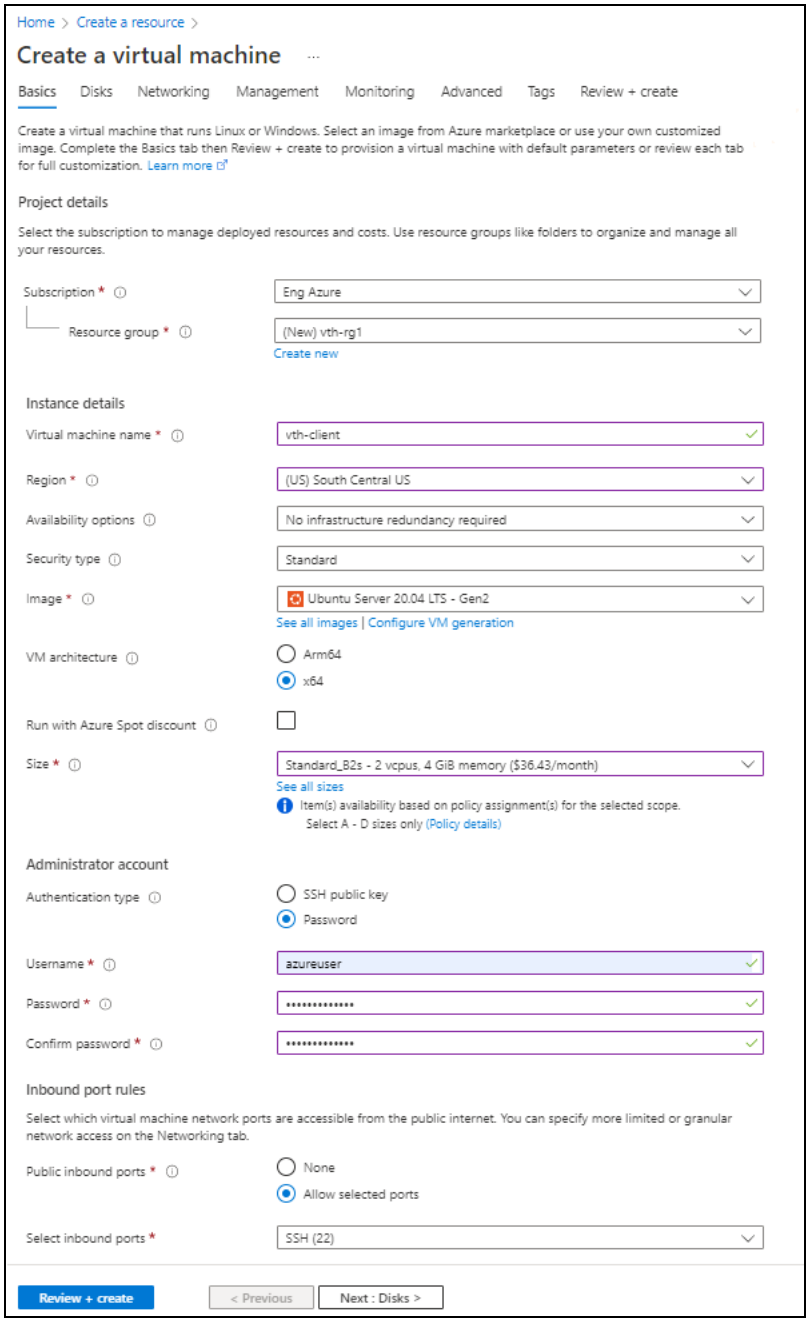
Administrator account

- Depending upon the Authentication type, provide the information.

Inbound port rules

- Public inbound ports
- Select inbound ports

Figure 101 : Create a virtual machine window - Basics tab



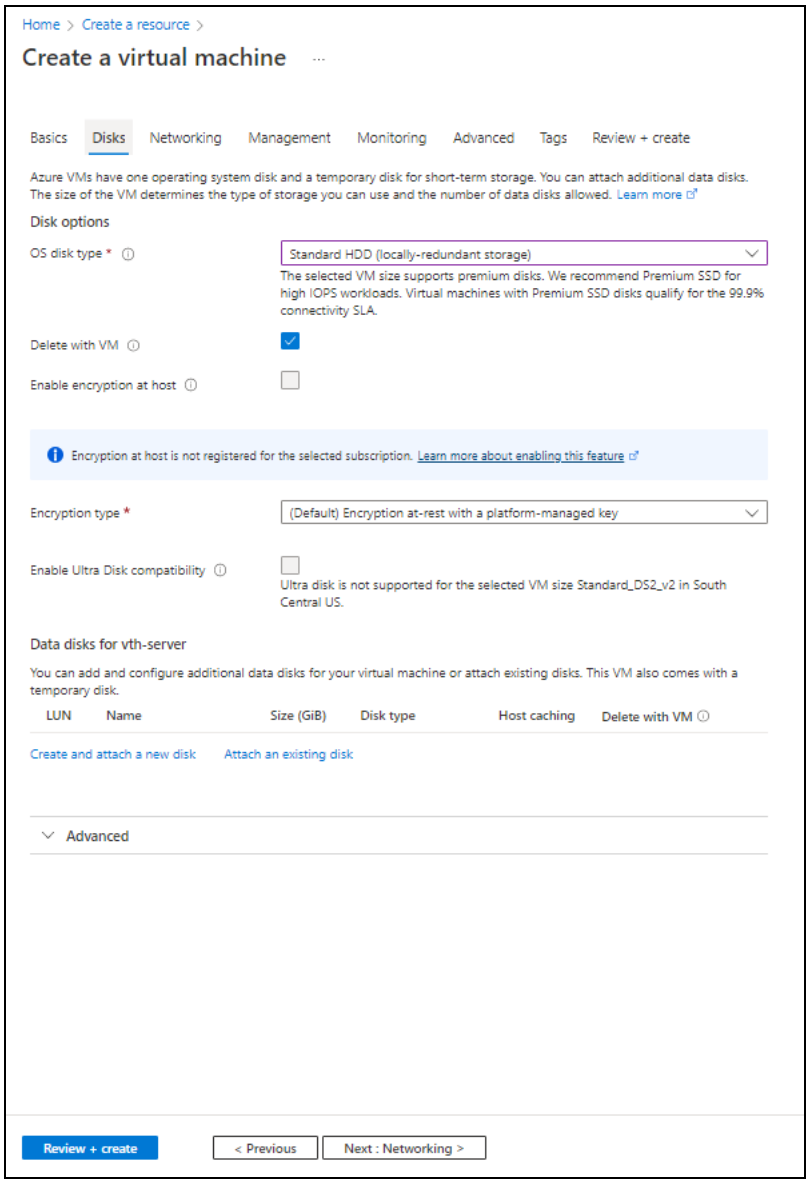
3. Leave the values in other fields unchanged and click **Next : Disks** at the bottom of the window.

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

   Disk options

   - OS disk type
   - Encryption type

Figure 102 : Create a virtual machine window - Disks tab

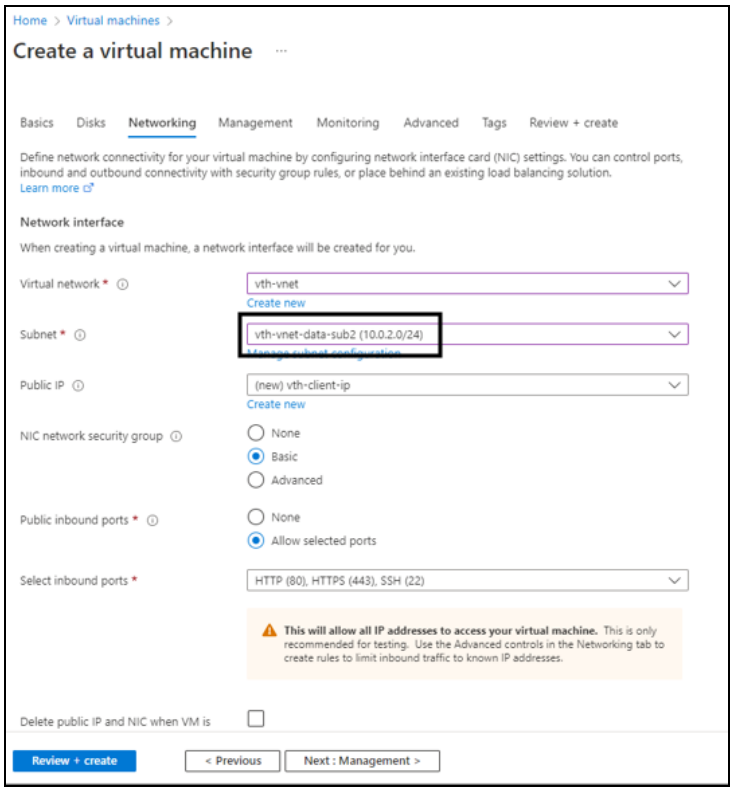


5. Leave the values in other fields unchanged and click **Next : Networking** at the bottom of the window.
6. Select or enter the following mandatory information in the **Networking** tab:

   Network interface

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

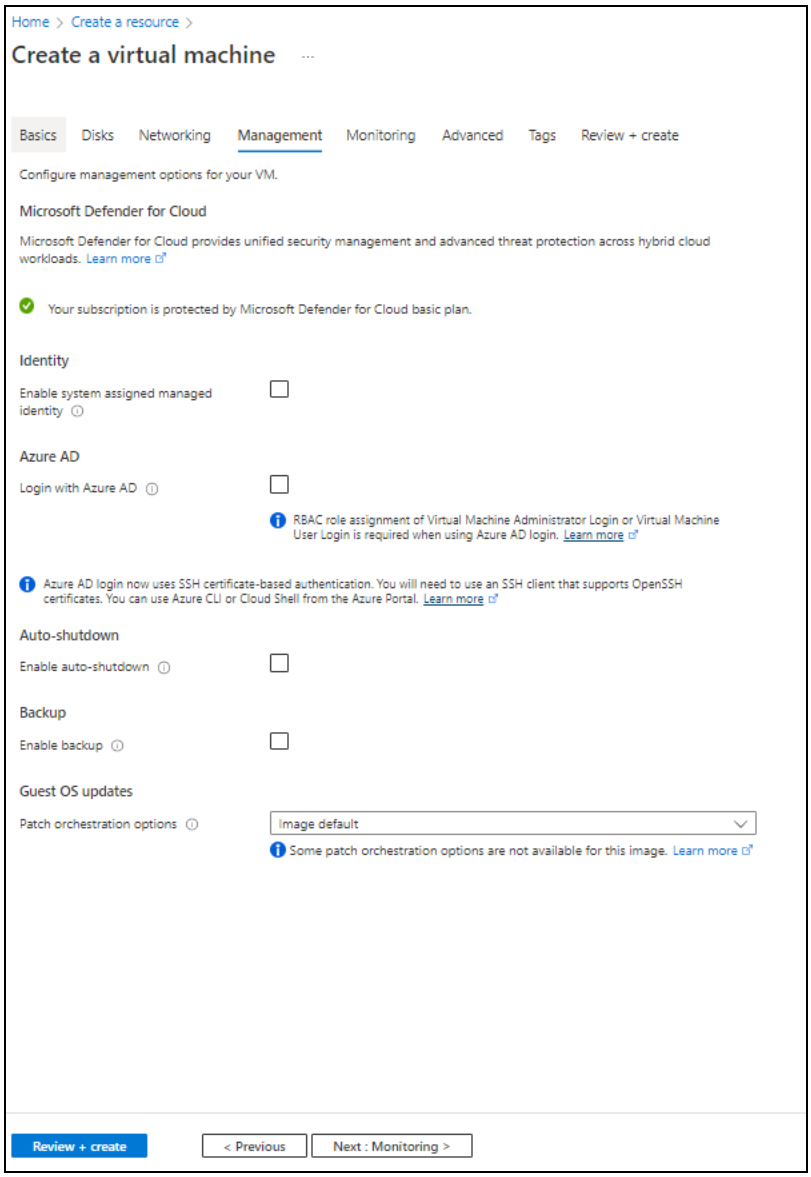
   Figure 103 : Create a virtual machine window - Networking tab



7. Leave the values in other fields unchanged and click **Next : Management** at the bottom of the window.

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

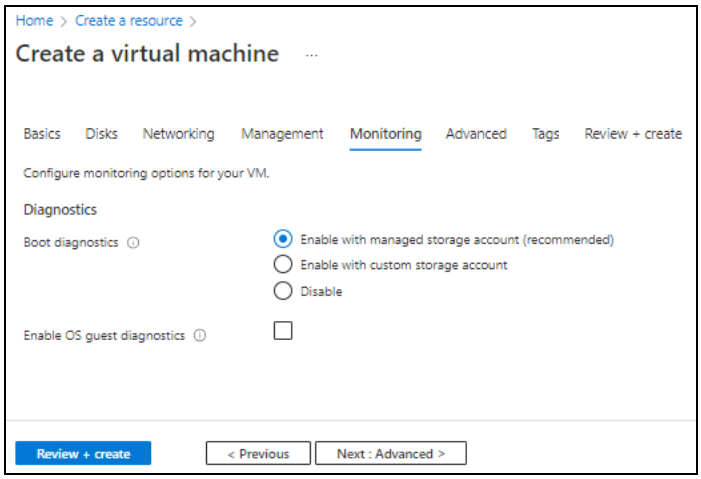
Figure 104 : Create a virtual machine window - Management tab



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

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

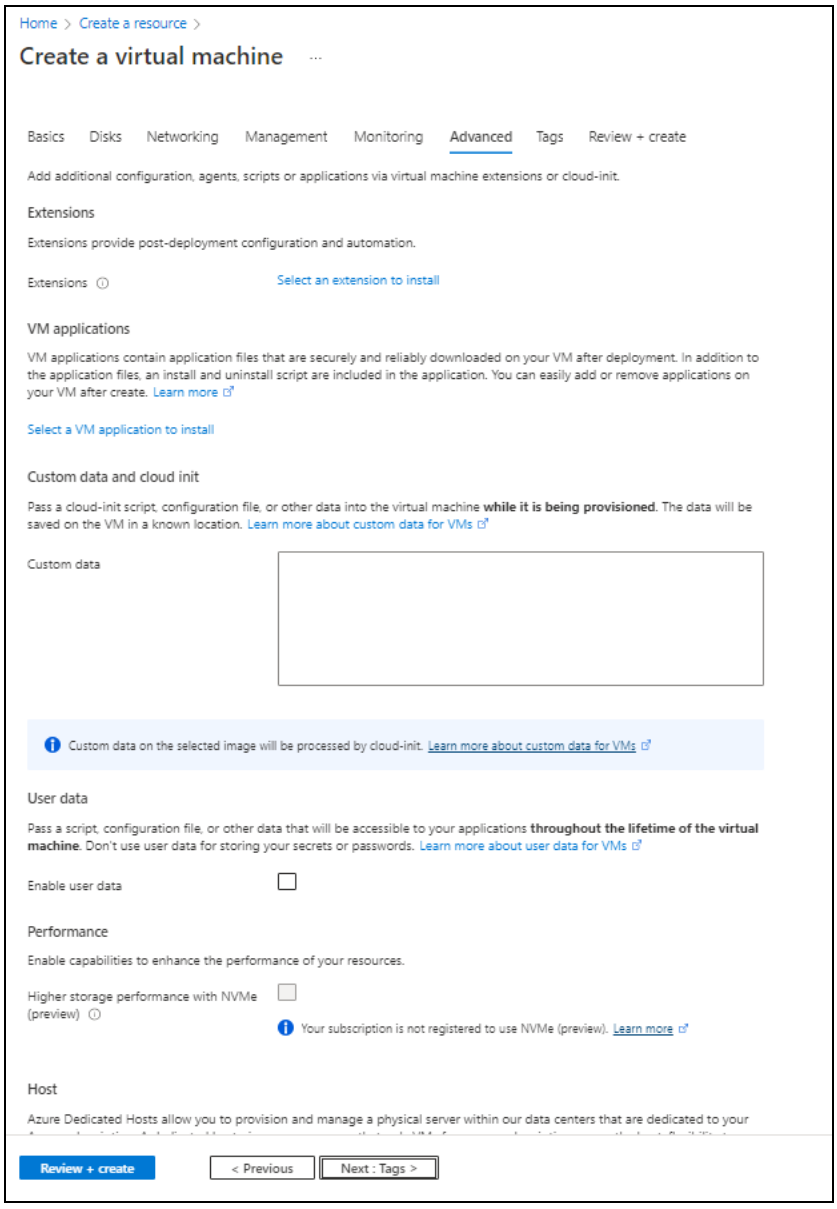
Figure 105 : Create a virtual machine window - Monitoring tab



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

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

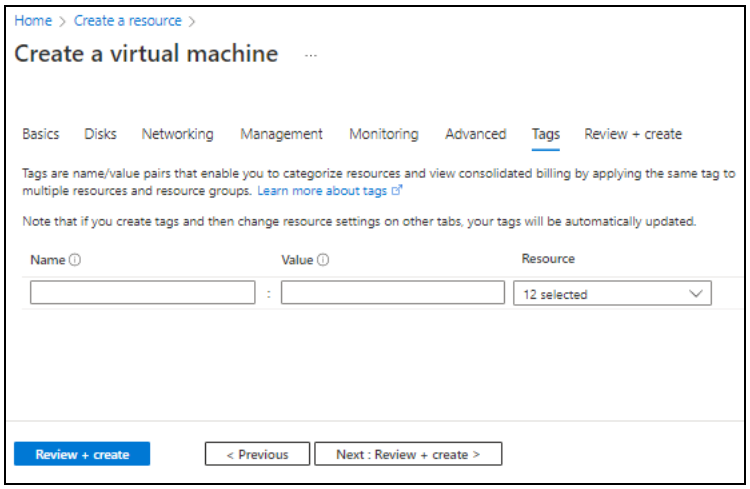
Figure 106 : Create a virtual machine window - Advanced tab



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

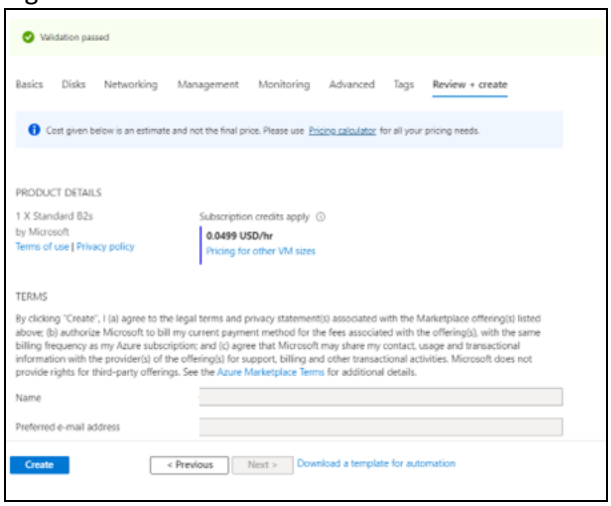
14. Select or enter the information in the **Tags** tab as needed.

Figure 107 : 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 108 : Create a virtual machine window - Review + create tab



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

Configure Thunder

The following configurations can be applied to the deployed vThunder instance:

- Change Password
- A10 License
- SSL Certificate
- Hybrid Cloud GSLB

Verify Deployment

To verify ARM template deployment using CLI, perform the following steps:

1. Verify SLB configuration on the following vThunder instances:

   CONTROLLER 1 - Master configuration

   Run the following command:

   ```
   vThunder-gslb:Master(config)(NOLICENSE)#show running-config
   ```

   If the deployment is successful, the following controller and site configuration is displayed on vThunder master controller:

```
no system geo-location load iana
system geo-location load GeoLite2-City
!
!
interface management
  ip address dhcp
!
interface ethernet 1
  enable
  ip address dhcp
!
interface ethernet 2
  enable
  ip address dhcp
!
!
ip route 0.0.0.0 /0 10.1.20.1
!
!
slb virtual-server gslb-server 10.1.20.8
  port 53 udp
    gslb-enable
!
gslb service-ip vs1 10.1.20.9
  external-ip 137.117.81.170
  port 80 tcp
!
gslb service-ip vs2 10.1.20.10
  external-ip 137.117.81.196
  port 80 tcp
!
gslb service-ip vs3 10.2.20.9
  external-ip 20.246.2.117
  port 80 tcp
!
gslb service-ip vs4 10.2.20.10
```

```
  external-ip 20.230.84.149
  port 80 tcp
!
gslb group default
  enable
  priority 255
!
gslb site eastus_1
  geo-location "North America,United States"
  slb-dev slb1 104.211.58.124
    vip-server vs1
!
gslb site eastus_2
  geo-location "North America,United States"
  slb-dev slb2 104.211.58.122
    vip-server vs2
!
gslb site eastus2_1
  geo-location "North America.United States.California.San Jose"
  slb-dev slb3 20.230.76.141
    vip-server vs3
!
gslb site eastus2_2
  geo-location "North America.United States.California.San Jose"
  slb-dev slb4 20.230.78.91
    vip-server vs4
!
gslb policy a10
  metric-order health-check geographic
  dns server authoritative
!
gslb zone gslb.a10.com
  policy a10
  service 80 www
    dns-a-record vs1 static
    dns-a-record vs2 static
```

```
    dns-a-record vs3 static
    dns-a-record vs4 static
!
gslb protocol status-interval 1
!
gslb protocol enable controller
!
!
```

CONTROLLER 2 - Member configuration

Run the following command:

```
vThunder-gslb:Member(config)(NOLICENSE)#show running-config
```

If the deployment is successful, the following controller and site configuration is displayed on vThunder member controller:

```
interface management
  ip address dhcp
!
interface ethernet 1
  enable
  ip address dhcp
!
interface ethernet 2
  enable
  ip address dhcp
!
!
ip route 0.0.0.0 /0 10.2.20.1
!
slb virtual-server gslb-server 10.2.20.8
  port 53 udp
    gslb-enable
!
gslb service-ip vs1 10.1.20.9
  external-ip 137.117.81.170
  port 80 tcp
!
gslb service-ip vs2 10.1.20.10
  external-ip 137.117.81.196
  port 80 tcp
!
gslb service-ip vs3 10.2.20.9
  external-ip 20.246.2.117
  port 80 tcp
!
gslb service-ip vs4 10.2.20.10
  external-ip 20.230.84.149
  port 80 tcp
!
gslb group default
  enable
```

```
  primary 20.232.185.150
!
gslb site eastus_1
  geo-location "North America,United States"
  slb-dev slb1 104.211.58.124
    vip-server vs1
!
gslb site eastus_2
  geo-location "North America,United States"
  slb-dev slb2 104.211.58.122
    vip-server vs2
!
gslb site eastus2_1
  geo-location "North America.United States.California.San Jose"
  slb-dev slb3 20.230.76.141
    vip-server vs3
!
gslb site eastus2_2
  geo-location "North America.United States.California.San Jose"
  slb-dev slb4 20.230.78.91
    vip-server vs4
!
gslb policy a10
  metric-order health-check geographic
  dns server authoritative
!
gslb zone gslb.a10.com
  policy a10
  service 80 www
    dns-a-record vs1 static
    dns-a-record vs2 static
    dns-a-record vs3 static
    dns-a-record vs4 static
!
gslb protocol status-interval 1
!
```

```
gslb protocol enable controller
!
!
```

SITE1 REGION1 configuration

Run the following command:

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

If the deployment is successful, the following controller and site configuration is displayed on vThunder site1 region1:

```
interface management
  ip address dhcp
!
interface ethernet 1
  enable
  ip address dhcp
!
interface ethernet 2
  enable
  ip address dhcp
!
!
ip route 0.0.0.0 /0 10.1.20.1
!
slb server vth-server1 10.1.30.8
  health-check disable
  port 80 tcp
       health-check disable
!
slb service-group sg tcp
  member vth-server1 80
!
slb virtual-server vs1 10.1.20.9
  port 80 tcp
    source-nat auto
    service-group sg
!
!
gslb protocol enable device
!
!
```

SITE2 REGION1 configuration

Run the following command:

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

If the deployment is successful, the following controller and site configuration is displayed on vThunder site1 region2:

```
interface management
  ip address dhcp
!
interface ethernet 1
  enable
  ip address dhcp
!
interface ethernet 2
  enable
  ip address dhcp
!
!
ip route 0.0.0.0 /0 10.1.20.1
!
slb server vth-server2 10.1.30.9
  health-check disable
  port 80 tcp
    health-check disable
!
slb service-group sg tcp
  member vth-server2 80
!
slb virtual-server vs1 10.1.20.10
  port 80 tcp
    source-nat auto
    service-group sg
!
!
gslb protocol enable device
!
!
```

SITE1 REGION2 configuration

Run the following command:

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

If the deployment is successful, the following controller and site configuration is displayed on vThunder site1 region2:

```
interface management
  ip address dhcp
!
interface ethernet 1
  enable
  ip address dhcp
!
interface ethernet 2
  enable
  ip address dhcp
!
!
ip route 0.0.0.0 /0 10.2.20.1
!
slb server vth-server3 10.2.30.8
  health-check disable
  port 80 tcp
       health-check disable
!
slb service-group sg tcp
  member vth-server3 80
!
slb virtual-server vs1 10.2.20.9
  port 80 tcp
    source-nat auto
    service-group sg
!
!
gslb protocol enable device

!
!
```

SITE2 REGION2 configuration

Run the following command:

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

If the deployment is successful, the following controller and site configuration is displayed on vThunder site2 region2:

```
interface management
  ip address dhcp
!
interface ethernet 1
  enable
  ip address dhcp
!
interface ethernet 2
  enable
  ip address dhcp
!
!
ip route 0.0.0.0 /0 10.2.20.1
!
slb server vth-server4 10.2.30.9
  health-check disable
  port 80 tcp
       health-check disable
!
slb service-group sg tcp
  member vth-server4 80
!
slb virtual-server vs1 10.2.20.10
  port 80 tcp
    source-nat auto
    service-group sg
!
!
gslb protocol enable device
```

2. Verify the GSLB group information on the following vThunder instances:

CONTROLLER - Master configuration

Run the following command:

```
vThunder-gslb:Master(config)(NOLICENSE)#show gslb group
```

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

```
                    Pri = Priority, Attrs = Attributes
                    S-Cfg = Secure Config
                    S-State = Secure Status
                        D = Disabled, L = Learn
                        P = Passive, * = Master
                        E = Enabled, EF = Enable-Fallback
                        Unsec = Unsecure, Unkwn = Unknown
                        Estng = Establishing, Estd = Established
Group: default, Master: local
Member                          Sys-ID    Pri Attrs  Status      S-Cfg
S-State Address
-------------------------------------------------------------------------
-----------
local                           e592163a 255 L*     OK
vThunder                        58547cbd 100 L      Synced      D
Unsec   20.109.98.187
```

CONTROLLER - Member configuration

Run the following command:

```
vThunder-gslb:Member(config)(NOLICENSE)#show gslb group
```

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

```
                    Pri = Priority, Attrs = Attributes
                    S-Cfg = Secure Config
                    S-State = Secure Status
                        D = Disabled, L = Learn
                        P = Passive, * = Master
                        E = Enabled, EF = Enable-Fallback
                        Unsec = Unsecure, Unkwn = Unknown
                        Estng = Establishing, Estd = Established
Group: default, Master: vThunder
Member                          Sys-ID    Pri Attrs  Status      S-Cfg
S-State Address
-------------------------------------------------------------------------
-----------
local                           58547cbd 100 L      OK
vThunder                        e592163a 255 PL*    Synced      D
Unsec   20.232.185.150
```

3. Verify the GSLB protocol information on the following vThunder instances:

CONTROLLER - Master configuration

Run the following command:

```
vThunder-gslb:Master(config)(NOLICENSE)#show gslb protocol
```

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

```
GSLB site: eastus_1
  SLB device: slb1 (10.1.20.5:4108) Established
 Session ID:    2869
 Secure Config:                      Disable |Current SSL State:
               Unsecure
 Connection succeeded:                     1 |Connection failed:
                      1
 Open packet sent:                         1 |Open packet received:
                      1
 Open session succeeded:                   1 |Open session failed:
                      0
 Sessions Dropped:                         0 |Update packet received:
                   7346
 Keepalive packet sent:                  123 |Keepalive packet
received:                    122
 Notify packet sent:                       0 |Notify packet received:
                      0
 Message Header Error:                     0 |Protocol RDT(ms):
                     40
 GSLB Protocol Version:                    2 |Peer ACOS Version:
     5.2.0 Build 155
 Secure negotiation Success:               0 |Secure negotiation
Failures:                    0
 SSL handshake Success:                    0 |SSL handshake Failures:
                      0

GSLB site: eastus_2
  SLB device: slb2 (10.1.20.5:2260) Established
 Session ID:    7186
 Secure Config:                      Disable |Current SSL State:
               Unsecure
 Connection succeeded:                     1 |Connection failed:
                      1
 Open packet sent:                         1 |Open packet received:
                      1
 Open session succeeded:                   1 |Open session failed:
```

```
                      0
 Sessions Dropped:                          0 |Update packet received:
                   7344
 Keepalive packet sent:                   123 |Keepalive packet
received:                    122
 Notify packet sent:                        0 |Notify packet received:
                      0
 Message Header Error:                      0 |Protocol RDT(ms):
                     32
 GSLB Protocol Version:                     2 |Peer ACOS Version:
     5.2.0 Build 155
 Secure negotiation Success:                0 |Secure negotiation
Failures:                    0
 SSL handshake Success:                     0 |SSL handshake Failures:
                      0

GSLB site: eastus2_1
  SLB device: slb3 (10.1.20.5:6668) Established
 Session ID:    1353
 Secure Config:                       Disable |Current SSL State:
               Unsecure
 Connection succeeded:                      1 |Connection failed:
                      0
 Open packet sent:                          1 |Open packet received:
                      1
 Open session succeeded:                    1 |Open session failed:
                      0
 Sessions Dropped:                          0 |Update packet received:
                   7346
 Keepalive packet sent:                   123 |Keepalive packet
received:                    122
 Notify packet sent:                        0 |Notify packet received:
                      0
 Message Header Error:                      0 |Protocol RDT(ms):
                     20
 GSLB Protocol Version:                     2 |Peer ACOS Version:
```

```
     5.2.0 Build 155
 Secure negotiation Success:               0 |Secure negotiation
Failures:                    0
 SSL handshake Success:                    0 |SSL handshake Failures:
                         0

GSLB site: eastus2_2
  SLB device: slb4 (10.1.20.5:12936) Established
 Session ID:    46932
 Secure Config:                       Disable |Current SSL State:
               Unsecure
 Connection succeeded:                     1 |Connection failed:
                         0
 Open packet sent:                         1 |Open packet received:
                         1
 Open session succeeded:                   1 |Open session failed:
                         0
 Sessions Dropped:                         0 |Update packet received:
                    7348
 Keepalive packet sent:                  124 |Keepalive packet
received:                    123
 Notify packet sent:                       0 |Notify packet received:
                         0
 Message Header Error:                     0 |Protocol RDT(ms):
                        20
 GSLB Protocol Version:                    2 |Peer ACOS Version:
     5.2.0 Build 155
 Secure negotiation Success:               0 |Secure negotiation
Failures:                    0
 SSL handshake Success:                    0 |SSL handshake Failures:
                         0

GSLB protocol is disabled for site devices.
```

CONTROLLER - Member configuration

Run the following command on vThunder to verify the GSLB protocol information:

```
vThunder-gslb:Member(config)(NOLICENSE)#show gslb protocol
```

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

```
 GSLB site: eastus_1
  SLB device: slb1 (10.2.20.5:4626) GroupControl
 Session ID:    Not Available
 Secure Config:                          None |Current SSL State:
                    None
 Connection succeeded:                      1 |Connection failed:
                       1
 Open packet sent:                          1 |Open packet received:
                       1
 Open session succeeded:                    1 |Open session failed:
                       0
 Sessions Dropped:                          1 |Update packet received:
                      12
 Keepalive packet sent:                     2 |Keepalive packet
received:                     1
 Notify packet sent:                        0 |Notify packet received:
                       0
 Message Header Error:                      0 |Protocol RDT(ms):
                       0
 GSLB Protocol Version:                     2
 Secure negotiation Success:                0 |Secure negotiation
Failures:                    0
 SSL handshake Success:                     0 |SSL handshake Failures:
                       0

GSLB site: eastus_2
  SLB device: slb2 (10.2.20.5:18556) GroupControl
 Session ID:    Not Available
 Secure Config:                          None |Current SSL State:
                    None
 Connection succeeded:                      1 |Connection failed:
                       1
 Open packet sent:                          1 |Open packet received:
                       1
 Open session succeeded:                    1 |Open session failed:
                       0
```

```
 Sessions Dropped:                          1 |Update packet received:
                     14
 Keepalive packet sent:                     2 |Keepalive packet
received:                     1
 Notify packet sent:                        0 |Notify packet received:
                      0
 Message Header Error:                      0 |Protocol RDT(ms):
                      0
 GSLB Protocol Version:                     2
 Secure negotiation Success:                0 |Secure negotiation
Failures:                     0
 SSL handshake Success:                     0 |SSL handshake Failures:
                      0

GSLB site: eastus2_1
  SLB device: slb3 (10.2.20.5:13002) GroupControl
 Session ID:    Not Available
 Secure Config:                          None |Current SSL State:
                   None
 Connection succeeded:                      1 |Connection failed:
                      1
 Open packet sent:                          1 |Open packet received:
                      1
 Open session succeeded:                    1 |Open session failed:
                      0
 Sessions Dropped:                          1 |Update packet received:
                     10
 Keepalive packet sent:                     2 |Keepalive packet
received:                     1
 Notify packet sent:                        0 |Notify packet received:
                      0
 Message Header Error:                      0 |Protocol RDT(ms):
                      0
 GSLB Protocol Version:                     2
 Secure negotiation Success:                0 |Secure negotiation
Failures:                     0
```

```
 SSL handshake Success:                    0 |SSL handshake Failures:
                       0

GSLB site: eastus2_2
  SLB device: slb4 (10.2.20.5:1200) GroupControl
 Session ID:    Not Available
 Secure Config:                          None |Current SSL State:
                   None
 Connection succeeded:                     1 |Connection failed:
                       0
 Open packet sent:                         1 |Open packet received:
                       1
 Open session succeeded:                   1 |Open session failed:
                       0
 Sessions Dropped:                         1 |Update packet received:
                      18
 Keepalive packet sent:                    2 |Keepalive packet
received:                     1
 Notify packet sent:                       0 |Notify packet received:
                       0
 Message Header Error:                     0 |Protocol RDT(ms):
                       0
 GSLB Protocol Version:                    2
 Secure negotiation Success:               0 |Secure negotiation
Failures:                     0
 SSL handshake Success:                    0 |SSL handshake Failures:
                       0

GSLB protocol is disabled for site devices.
```

Verify Traffic Flow

The traffic flow can be tested using the following:

- DNS Lookup
- WGET

DNS Lookup

To verify the traffic flow from via vThunder, perform the following:

1. Perform a DNS lookup on client machine using the master controller's client-side data interface public IP in the following command:

```
$ dig @master_controller_data_public_IP  www.gslb.a10.com
```

The master controller's client-side data interface public IP is used as DNS server IP. You can get the public IP from **Azure Portal** > **Azure services** > **Resource Group** > <*resource_group_name*> > <*master_controller_region1*> > **Settings** > **Networking**.

Figure 109 : Master Controller Data Interface Public IP

The following response is received:

```
$ dig @20.232.184.46  www.gslb.a10.com

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.8 <<>> @20.232.184.46
www.gslb.a10.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11393
;; flags: qr rd; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1400
;; QUESTION SECTION:
;www.gslb.a10.com.              IN      A

;; ANSWER SECTION:
www.gslb.a10.com.       10      IN      A       20.1.129.29
www.gslb.a10.com.       10      IN      A       20.97.231.193
www.gslb.a10.com.       10      IN      A       20.232.22.199
www.gslb.a10.com.       10      IN      A       20.232.18.146

;; Query time: 82 msec
;; SERVER: 20.232.184.46#53(20.232.184.46)
;; WHEN: Wed Aug 31 00:11:40 PDT 2022
;; MSG SIZE  rcvd: 125
```

2. Stop the site1 of region1 and then perform the DNS lookup again.

```
$ dig @20.232.184.46  www.gslb.a10.com

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.8 <<>> @20.232.184.46
www.gslb.a10.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57272
;; flags: qr rd; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1400
;; QUESTION SECTION:
;www.gslb.a10.com.              IN      A

;; ANSWER SECTION:
www.gslb.a10.com.       10      IN      A       20.97.231.193
www.gslb.a10.com.       10      IN      A       20.1.129.29
www.gslb.a10.com.       10      IN      A       20.232.22.199
www.gslb.a10.com.       10      IN      A       20.232.18.146

;; Query time: 85 msec
;; SERVER: 20.232.184.46#53(20.232.184.46)
;; WHEN: Wed Aug 31 00:11:46 PDT 2022
;; MSG SIZE  rcvd: 125
```

The response is received with shuffled server IP addresses.

WGET

To verify the traffic flow on the load balancer, perform the following:

1. Run the following command in the Terminal window of the server1 of region1 instance to create an Apache Server virtual machine:

```
$ sudo apt install apache2
```

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

2. From **Azure Portal** > **Azure services** > **Resource Group** > *<resource_group_name>* > *<site_device_region1>* > **Settings** > **Networking**, select the secondary data interface public IP.
3. Run the following command on the client machine:

```
$ wget site_device_secondary_data_public_ip
```

The following response is received:

```
$ wget 20.232.22.199
--2023-01-09 17:49:47--  http://20.232.22.199/
Connecting to 20.232.22.199:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11321 (11K) [text/html]
Saving to: 'index.html.4'

index.html.4                                  100%
[=============================================================================
==========]  10.42K  --.-KB/s    in 0s

                      2023-01-09 17:49:47 (63.8 MB/s) - 'index.html.4'
saved [10671/10671]
```

Thunder-3NIC-VMSS

This template creates a new Virtual Machine Scale Set (VMSS) with pre-loaded Thunder instance. . The auto scale-in or scale-out occurs based on the performance metric threshold rule. The maximum number of Thunder replicas allowed can be defined. Each vThunder instance attach three new network interface cards (NICs).

When one instance becomes unavailable, another instance spins without any manual intervention.

For more information, see Create Thunder Virtual Machines.

NOTE: Use a suitable VM size that supports at least three NICs. For VM sizes, see Supported VM Sizes.

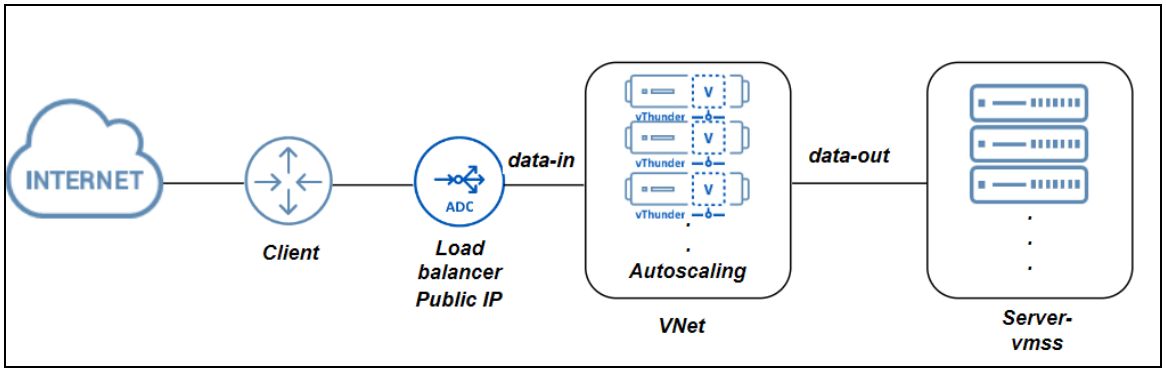
This template auto-applies the following vThunder configuration after the webhook URL is created:

- Server Load Balancer using a webhook URL on vThunder for newly added or deleted web/app servers through backend server VMSS autoscaling.
- SSL Certificate in Storage account and Server Load Balancer.
- A10 License in Automation Account Variable.

It configures log analysis capabilities using Azure Log Analytics workspace integration and metrics monitoring using Azure Application Insights integration.

NOTE: All the configured vThunder instances do not synchronize their SLB configurations.

Figure 110 : Thunder ADC in AutoScale Mode.



Various templates are available for different deployment needs.

For more information, see Deployment Templates.

The following topics are covered:

Create Thunder Virtual Machines

The A10-vThunder-3NIC-VMSS template is used to create multiple Thunder virtual machines with three network interface cards.

Before deploying this template, it is recommended to review the Prerequisites.

There are two ways to deploy this template:

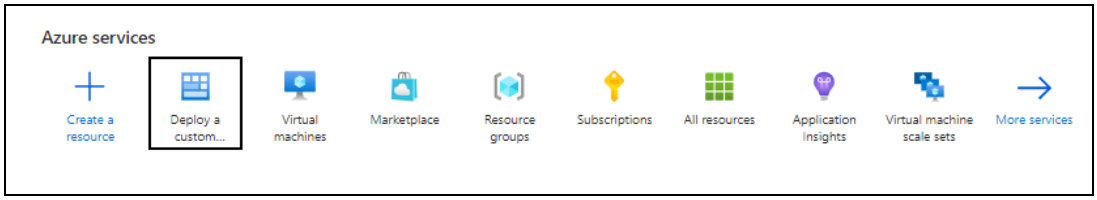
- Upload using Azure Portal Console
- Execute using Azure CLI

Upload using Azure Portal Console

To deploy the A10-vThunder-3NIC-VMSS template using Azure Portal Console, perform the following steps:

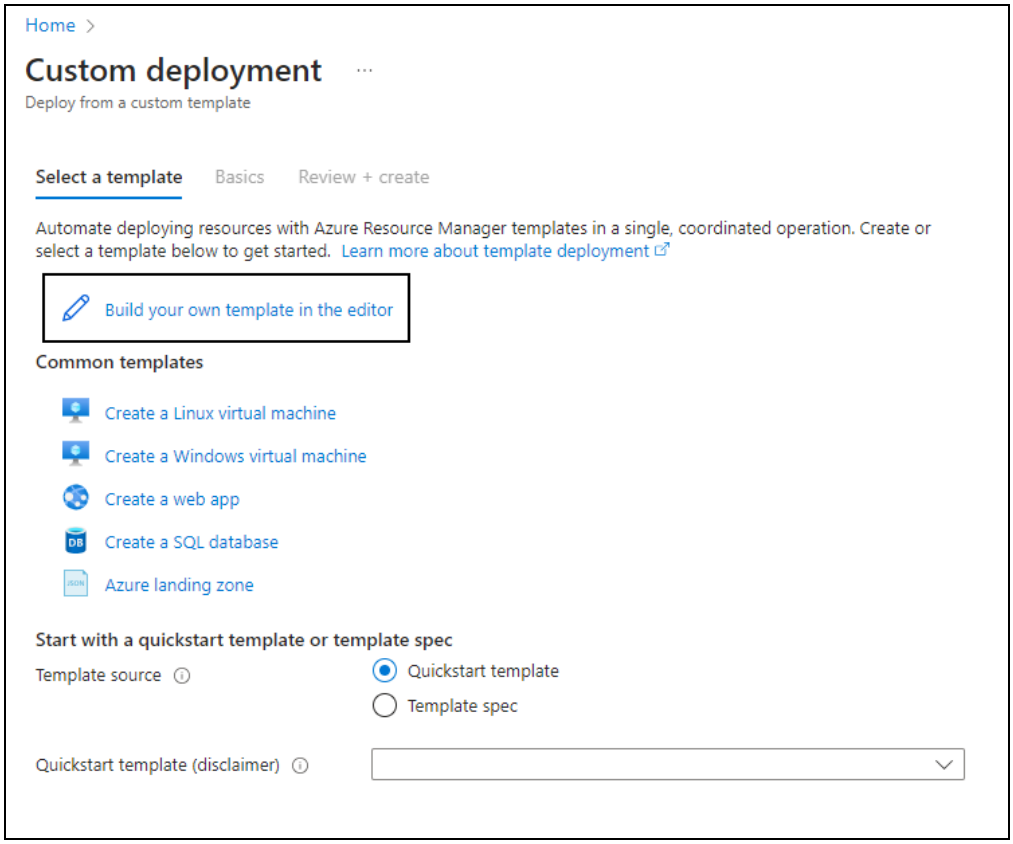
1. Download A10-vThunder-3NIC-VMSS template.
2. From the **Azure Portal** > **Azure services**, click **Deploy a custom template**.

   Figure 111 : Azure services



3. Under the **Custom deployment** window > **Select a template** tab, click **Build your own template in the editor**.

Figure 112 : Custom deployment window



4. From the **Edit template** window, perform either of the following step:

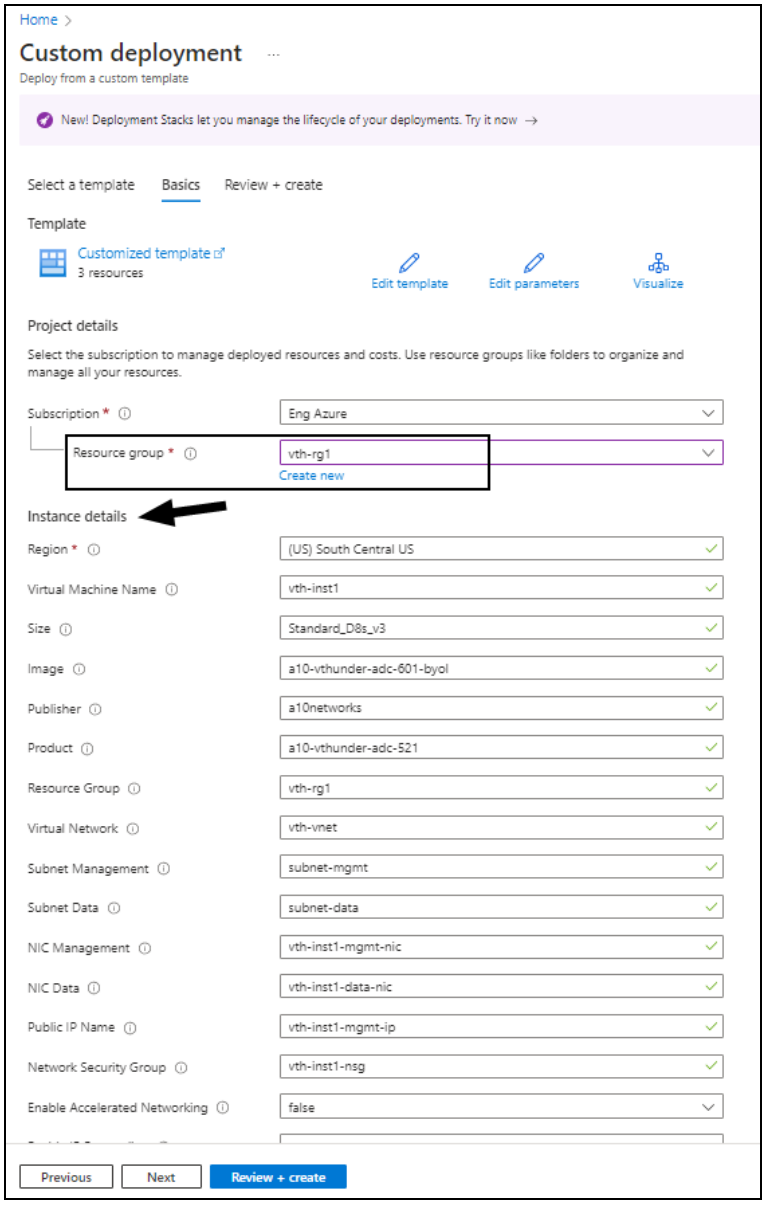
   - Click **Load file** and browse to the folder where you have downloaded the ARM template. Select **ARM_TMPL_3NIC_NVM_VMSS_1** to upload.
   - From Windows Explorer, navigate to the folder where you have downloaded the ARM template. Copy **ARM_TMPL_3NIC_NVM_VMSS_1** content and paste it in the editor.

Figure 113 : Edit template window

5. Click **Save**.

   The **Custom deployment** window is displayed with the template parameters and default values.

Figure 114 : Custom deployment template



6. Select an existing or create a new **Resource group** under which you want to deploy the custom template resources.

NOTE: Hover ⓘ for description of each corresponding parameter.

7. Update the default values and also provide the values in the empty fields as

appropriate in the **Instance details** section shown in Figure 114.

NOTE: Use a suitable VM size that supports at least three NICs. For VM sizes, see Supported VM Sizes.

8. Click **Review+create**.

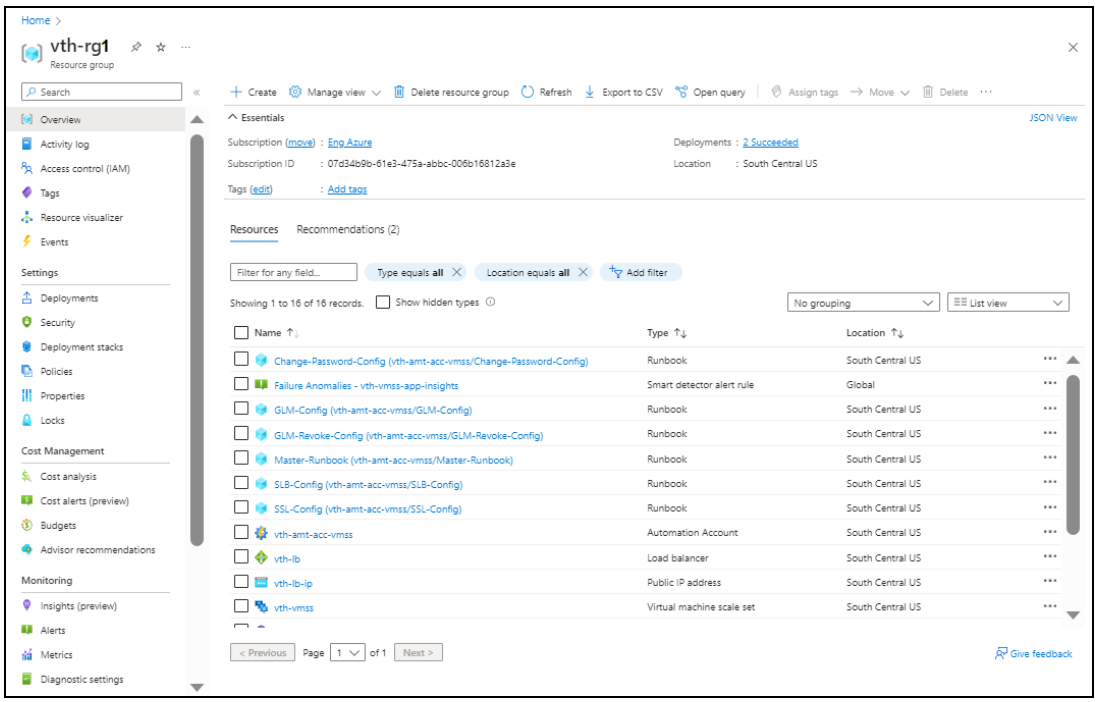
   The validation appears.

9. Click **Create**.

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

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

Figure 115 : Resource listing under resource group



Execute using Azure CLI

To deploy the A10-vThunder-3NIC-VMSS template using Azure CLI commands, perform the following steps:

1. Download A10-vThunder-3NIC-VMSS template.

NOTE: This template contains pre-populated default values that can be modified as required and it does not create new virtual network, network security group, subnets, and Public IP.

2. From Windows Explorer, navigate to the folder where you have downloaded the ARM template.
3. Open the ARM_TMPL_3NIC_NVM_VMSS_PARAM.json with a text editor.
4. Configure the following parameters as appropriate:

Table 6 : JSON Parameters

Resource Name	Description

Virtual Machine Scale Set Name	Specify a name for the Virtual Machine Scale Set (VMSS). The VMSS automatically scale-out or scale-in based on the specified capacity rules. It manages a group of identical virtual machines efficiently. For more information, see Virtual Machine Scale Set.
	`"VMSS Name":{`
	`"value":"vth-vmss"`
	`},`

Virtual Machine Scale Set Size	Specify a suitable VM size that supports at least 3 NICs for the vThunder instance. For VM sizes, see Supported VM Sizes.
	`"VMSS Size":{`
	`"value":"Standard_D8s_v3"`
	`},`

Instance count	Specify the number of virtual machines to be created with identical configuration inside VMSS. It allows to adjust the number of instances based on changing workload demands. For more information, see Virtual Machine Scale Set.
	`"Instance Count":{`
	`"value":1`

Table 6 : JSON Parameters

Resource Name	Description
	NOTE: The instance count cannot be less than 1.
vThunder Image	Specify the desired vThunder Image name and Product name from the Azure Marketplace. `"Image": { "value":"a10-vthunder-adc-601-byol" }, "Publisher": { "value": "a10networks" }, "Product": { "value": "a10-vthunder-adc-521" },` **NOTE:** Do not change the publisher name.
Network Interface Cards	Specify a unique network interface card for management, data-in, and data-out traffic. `"NIC Management":{ "value":"vth-inst-mgmt-nic" }, "NIC DataIn":{ "value":"vth-inst-datain-nic" }, "NIC DataOut":{ "value":"vth-inst-dataout-nic" },`
Management Public IP	Specify an existing Public IP address for management traffic. `"Management Public IP Name":{ "value":"vth-inst-mgmt-ip" },`
Subnet CIDR	Specify the CIDR range for management, datain, and datout

Table 6 : JSON Parameters

Resource Name	Description

	subnets.
	`"Subnet Mgmt CIDR":{`
	`"value":"10.0.1.0/24"`
	`},`
	`"Subnet DataIn CIDR":{`
	`"value":"10.0.2.0/24"`
	`},`
	`"Subnet DataOut CIDR":{`
	`"value":"10.0.3.0/24"`
	`},`

Network Security Group	Specify the network security group name for all the NICs.
	`"Network Security Group":{`
	`"value": "vth-vmss-nsg"`
	`},`

Storage Account	Specify a unique name for the Azure storage account. The name must be in lowercase, 3 - 24 characters long, and can contain numbers and lowercase letters only. It is used as a part of the URL for accessing the data stored within the account. If a name is not provided, the default value is used, but it is recommended to change it to a unique and meaningful name. For more information on naming rules and considerations, see Resource name rules.
	`"Storage Account Name": {`
	`"value": "vthunderstorage"`
	`},`

Load Balancer	Specify a unique name for the Azure load balancer. The name must be globally unique within the Azure subscription and 1 - 80 characters long. It can include numbers, lowercase letters, and hyphens, but cannot start or end with a hyphen. The Load Balancer name is used to identify and access the load

Table 6 : JSON Parameters

Resource Name	Description
	balancer and its associated resources. If a name is not provided, the default value is used. For more information on naming rules and considerations, see Resource name rules. `"LB Name": { "value": "vth-lb" }, "LB Public IP Name": { "value": "vth-lb-ip" },`
Automation Account	Specify a unique name for the Azure automation account. The name must 2 - 50 characters long and can contain numbers, lowercase letters, and hyphens, but cannot start or end with a hyphen. If a name is not provided, the default value is used. An Azure automation account is a central hub for automating and orchestrating tasks and processes within the Azure environment and beyond. It provides a platform to create, monitor, and manage automation runbooks, which are scripts that can perform various tasks on Azure resources and external systems. Automation runbooks can be scheduled to run at specific intervals or triggered by specific events, enabling proactive maintenance and resource management. `"Automation Account Name": { "value": "vth-amt-acc" },`
Log Analytics Workspace	Specify a unique name for the Azure log analytics workspace. The name must be 2 - 64 characters long, can contain numbers, lowercase letters, and hyphens, but cannot start or end with a hyphen. If a name is not provided, the default value is used. An Azure log analytics workspace is a central repository for collecting, analyzing, and visualizing data from various sources. It allows you to ingest and store logs and

Table 6 : JSON Parameters

Resource Name	Description
	monitoring data from Azure resources, on-premises servers, applications, and other cloud environments. Once data is collected in the workspace, you can perform queries, create custom dashboards, and set up alerts to gain valuable insights into the performance, health, and security of your infrastructure and applications. `"Log Analytics Workspace Name": { "value": "vth-vmss-log-workspace" },`
Application Insights	Specify a unique name for the Azure application insights resource. The name must be 2 - 256 characters long, can contain numbers, lowercase letters, and hyphens, but cannot start or end with a hyphen. If a name is not provided, the default value is used. Azure application insights is a comprehensive application performance monitoring service that helps you gain insights into the availability, performance, and usage of your applications. It allows you to track and analyze telemetry data from vThunder. With application insights, you can detect and diagnose performance issues, identify trends, and optimize application performance to deliver better user experiences. `"Application Insights Name": { "value": "vth-vmss-app-insights" },`
Enable Accelerated Networking	Specify 'true' to enable low latency and high throughput on the NICs. For more information, see Accelerated Networking. `"Enable Accelerated Networking": { "value": false },`

Table 6 : JSON Parameters

Resource Name	Description
	NOTE: By default, accelerated networking is disabled for all type of compute instances and it can be enabled for the selected compute instances. For the supported compute instances, see Supported VM Sizes.
Enable IP Forwarding	Specify 'true' to allow the virtual machine to forward the network traffic between networks to improve the network performance. This high-performance forwarded path bypasses the host from the usual data path, thus, reducing latency, jitter, and CPU utilization when using the most demanding network workloads on the supported VM types. For more information, see IP Forwarding. `"Enable IP Forwarding": { "value": false }` **NOTE:** By default, IP forwarding is disabled.

5. Verify if all the configurations in the ARM_TMPL_3NIC_NVM_VMSS_PARAM.json file are correct and then save the changes.
6. From the Start menu, open PowerShell and navigate to the folder where you have downloaded the ARM template.
7. Run the following command to create a resource group in Azure:

```
PS C:\Users\TestUser\Templates> az group create --name <resource_group_name> --location "<location_name>"
```

Example:

```
PS C:\Users\TestUser\Templates> az group create --name vth-rg1 --location "south central us"
```

```
 {
    "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/resourceGroups/vth-rg1",
    "location": "southcentralus",
    "managedBy": null,
    "name": "vth-rg1",
    "properties": {
      "provisioningState": "Succeeded"
    },
    "tags": null,
    "type": "Microsoft.Resources/resourceGroups"
  }
```

8. Run the following command to create a deployment group in Azure.

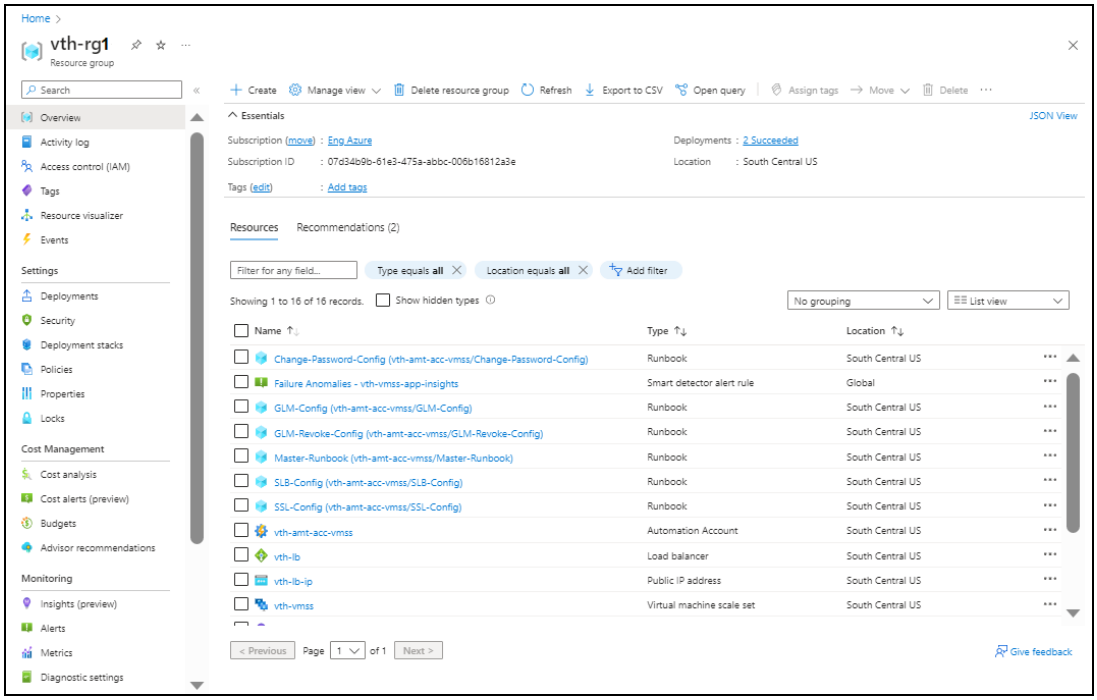
```
PS C:\Users\TestUser\Templates> az deployment group create -g
<resource_group_name> --template-file <template_name> --parameters
<param_template_name>
```

Example:

```
PS C:\Users\TestUser\Templates> az deployment group create -g vth-rg1
--template-file ARM_TMPL_3NIC_NVM_VMSS_1.json --parameters ARM_TMPL_
3NIC_NVM_VMSS_PARAM.json
```

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

Figure 116 : Resource listing under resource group



After deploying the vThunder instances, verify the resources created:

Verify Resources Creation

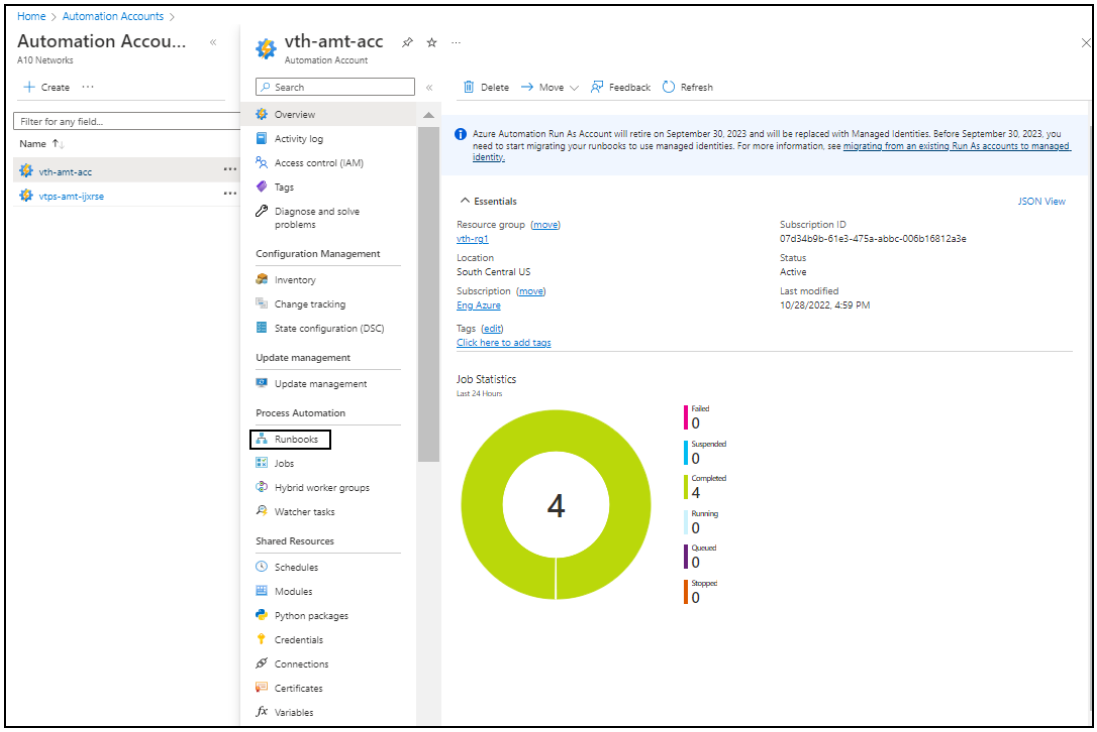
Runbook

To verify the creation of runbooks, perform the following steps:

1. From **Home**, navigate to **Azure services** > **Automation Accounts** > <*automation_account_name*>.

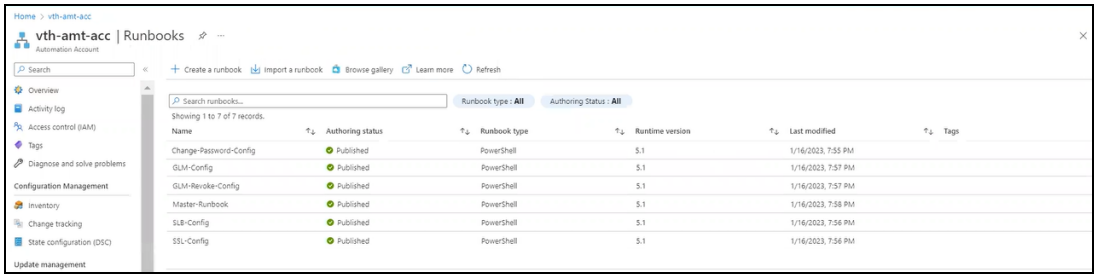
   The selected automation account - Overview window is displayed.

Figure 117 : Selected automation account - Overview window



2. Click **Runbooks** from the left **Process Automation** panel.
   The selected automation account - Jobs window is displayed.

Figure 118 : Selected automation account - Runbooks window



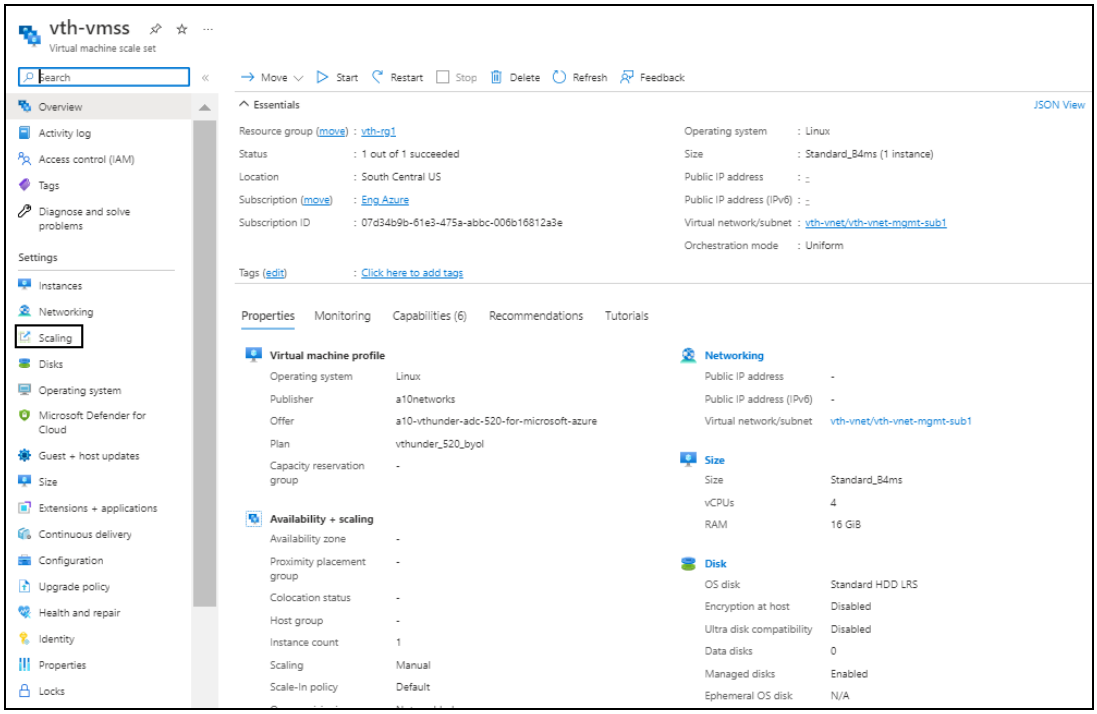
Instance Count

To verify the instance count, perform the following steps:

1. From **Home**, navigate to **Azure services** > **Virtual machine scale set** > <*vmss_name*>.

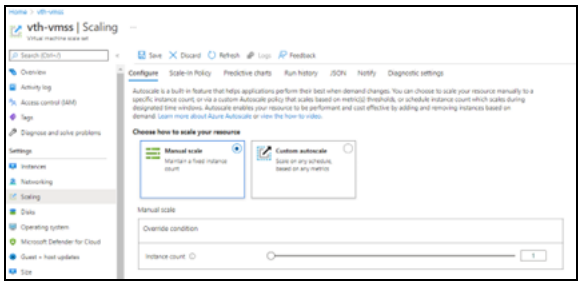
The selected VMSS - Overview window is displayed. Here, the VMSS name is **`vth-vmss`**.

Figure 119 : Virtual machine scale set - Overview window



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

   Figure 120 : Virtual machine scale set - Scaling window - Configure tab



3. Verify the configured instance count.
   If the instance gets deleted either manually or automatically, VMSS creates a new instance.

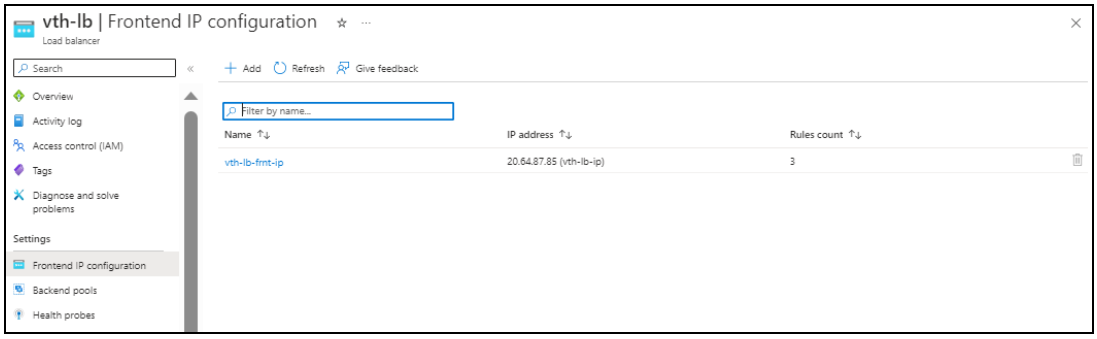
LB creation

To verify LB resource creation, perform the following steps:

a. From **Home**, navigate to **Azure services** > **Load balancer** > <*lb_name*>.
The selected LB - Overview window is displayed. Here, the LB name is **`vth-lb`**.

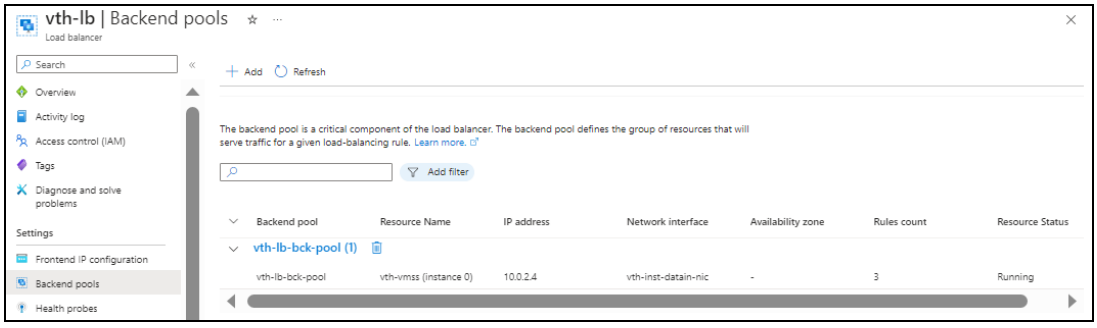
b. Click **Frontend IP configuration** from the left **Settings** panel to verify if the LB frontend IP is created.

Figure 121 : Selected Frontend IP configuration window



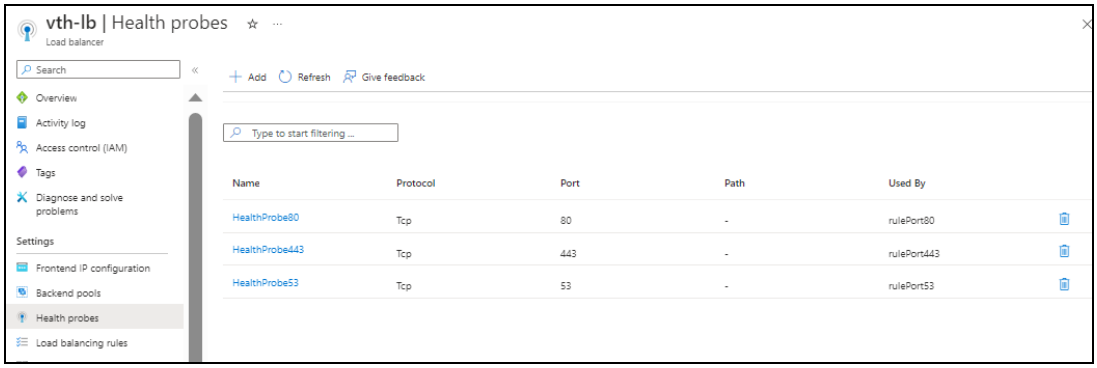
c. Click **Backend pools** from the left **Settings** panel to verify if the backend pools are created.

Figure 122 : Selected Backend pools window



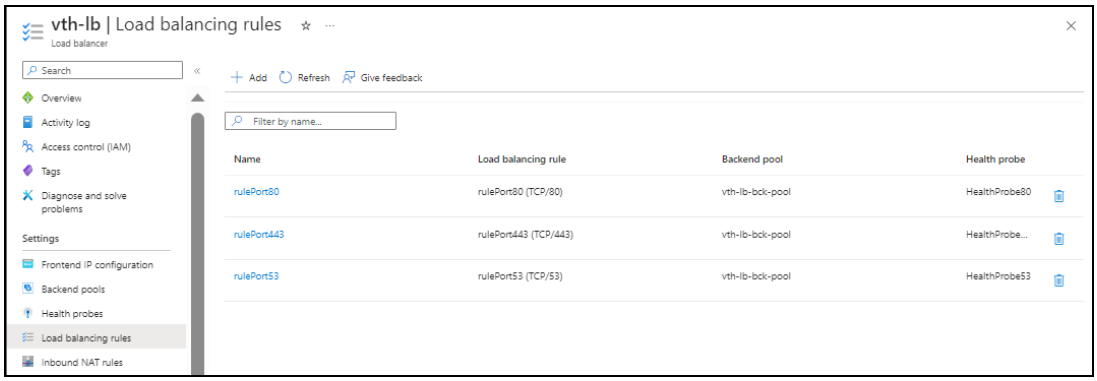
d. Click **Health probes** from the left **Settings** panel to verify if the health probes are created.

Figure 123 : Selected Health Probes window



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

Figure 124 : Selected load balancing rules window



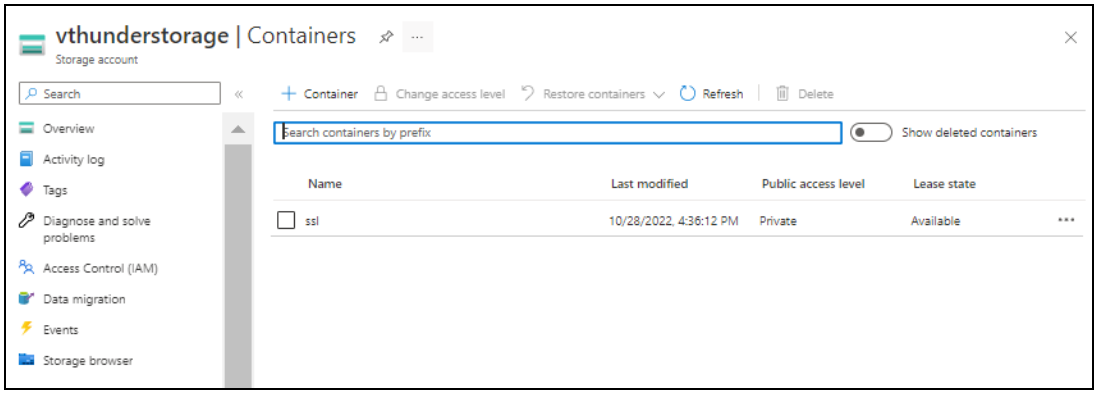
Storage Account Container

To verify storage account container, perform the following steps:

a. From **Home**, navigate to **Azure services** > **Storage account** > <*storage_account_name*>.
The selected storage account - Overview window is displayed. Here, the storage account name is **`vthunderstorage`**.

b. Click **Containers** from the left **Data storage** panel.
The selected storage account - Containers window is displayed.

Figure 125 : Selected storage account - Containers window



Access Thunder Virtual Machine

The Thunder Virtual Machine can be accessed using any of the following ways:

- Access vThunder using CLI
- Access vThunder using GUI

Access vThunder using CLI

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

1. Open any SSH client.
2. Enter or select the following basic information in the configuration window:
   - Hostname: Public IP of Virtual Machine Instance under the VMSS
     Here, Public IP of **`vth-vmss`**
   - Username: Enter username provided by A10 Networks Support
   - Password: Enter password provided by A10 Networks Support
3. Connect to the session.

   If the session connection is successful, the following response is displayed:

```
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--->
```

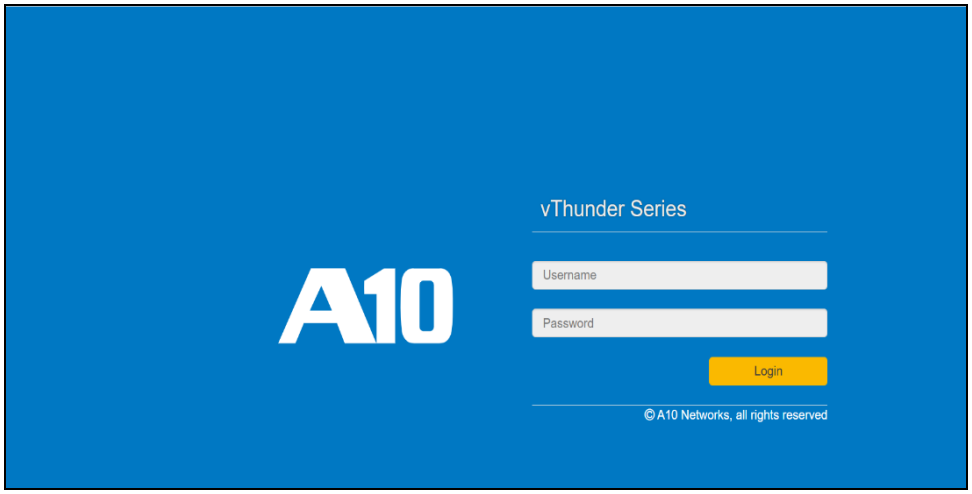
The vThunder instance is ready to use.

Access vThunder using GUI

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

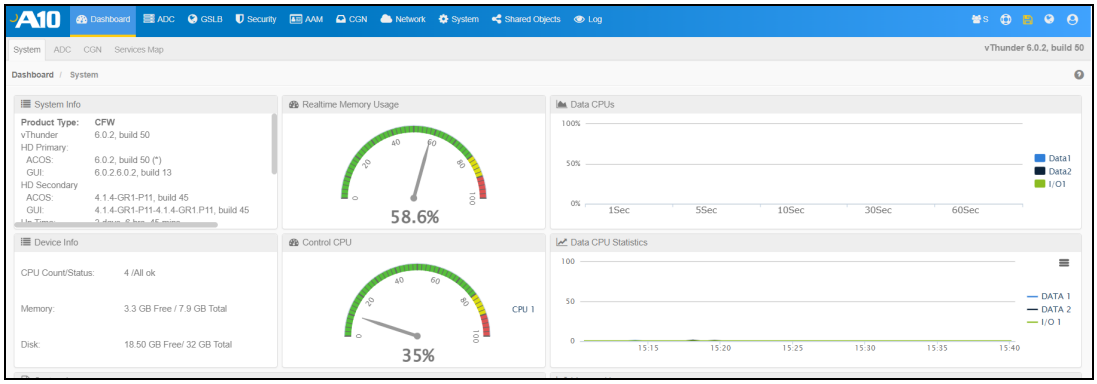
1. Open any browser.
2. Enter *https://<vthunder_public_IP>/gui/auth/login/* in the address bar.

Figure 126 : vThunder GUI



3. Enter the username and password provided by A10 Networks Support. The home page gets displayed.

Figure 127 : Home page



Configure Server VMSS

The following topics are covered:

- Create and Configure Server VMSS
- Verify the Server VMSS Creation

Create and Configure Server VMSS

To create a Server VMSS, perform the following steps:

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

   Project details

   - Subscription
   - Resource group

   Scale set details

   - Virtual machine scale set name - Server machine
   - Region

   Orchestration

   - Orchestration mode - **Uniform**

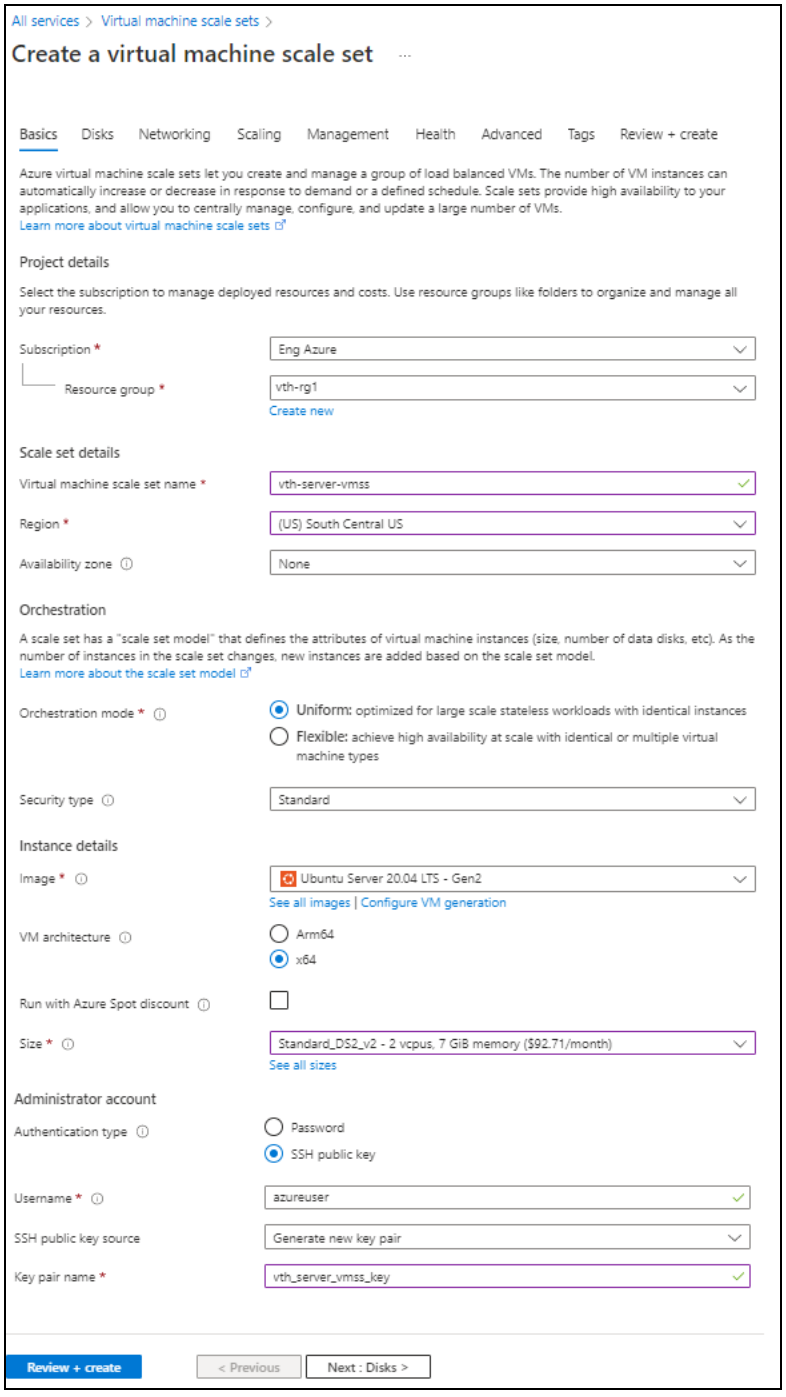
Instance details

- Image
- Size

Administrator account

- Depending upon the Authentication type, provide the information.

Figure 128 : Create a virtual machine scale set window - Basics tab



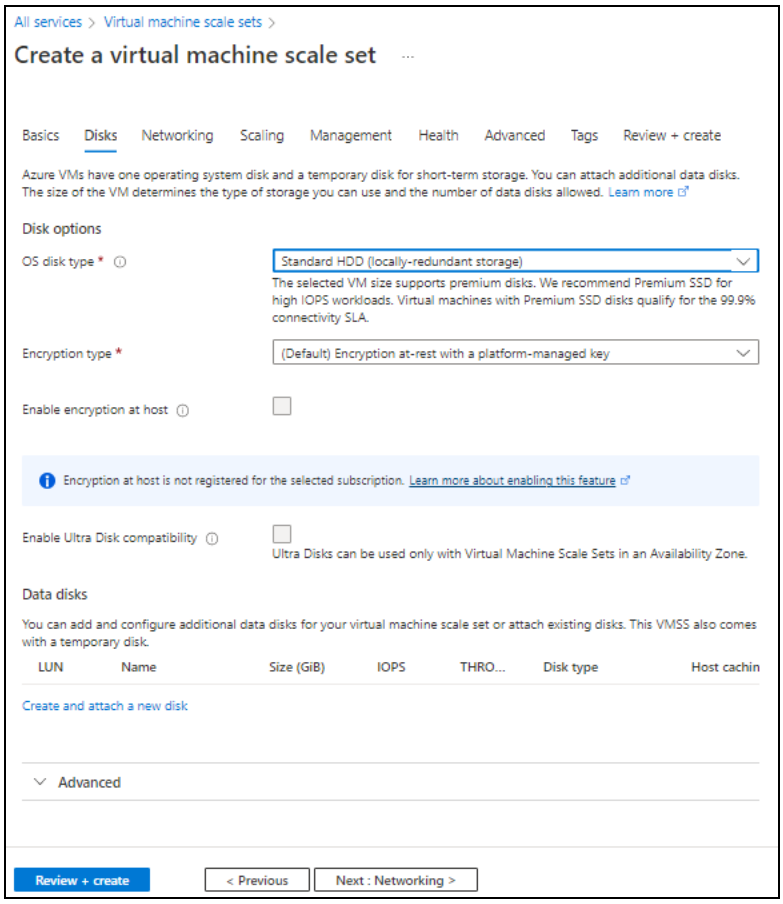
3. Leave the values in other fields unchanged and click **Next : Disks** at the bottom of the window.

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

   Disk options

   - OS disk type
   - Encryption type

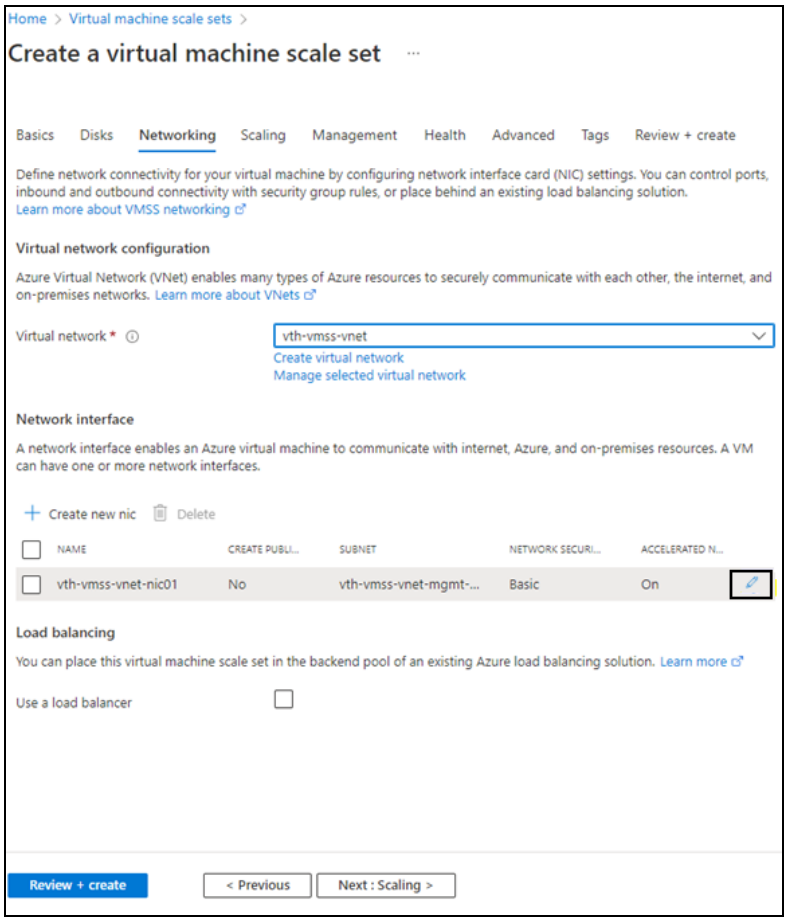
   Figure 129 : Create a virtual machine scale set window - Disks tab



5. Leave the values in other fields unchanged and click **Next : Networking** at the bottom of the window.

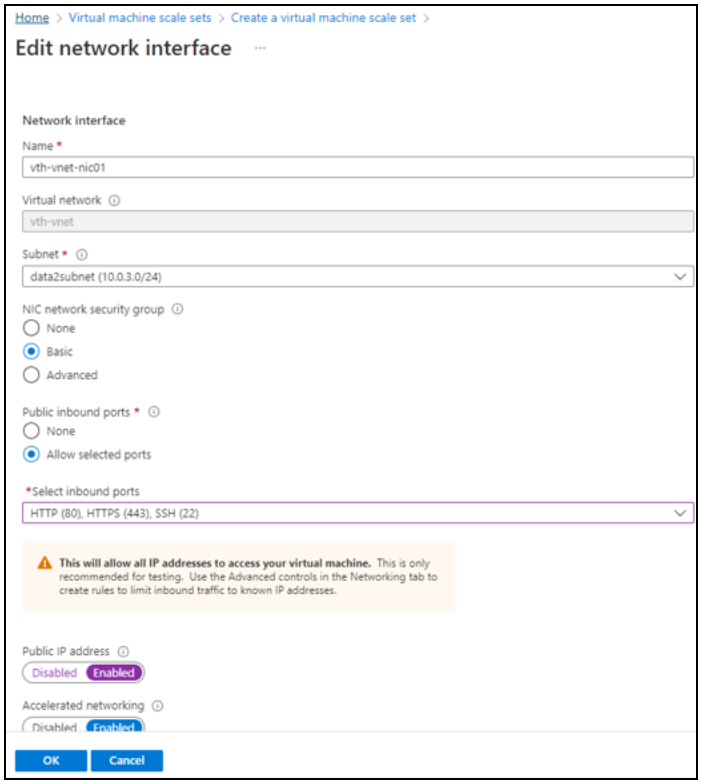
6. Select the Virtual network in the **Networking** tab.

Figure 130 : 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`.

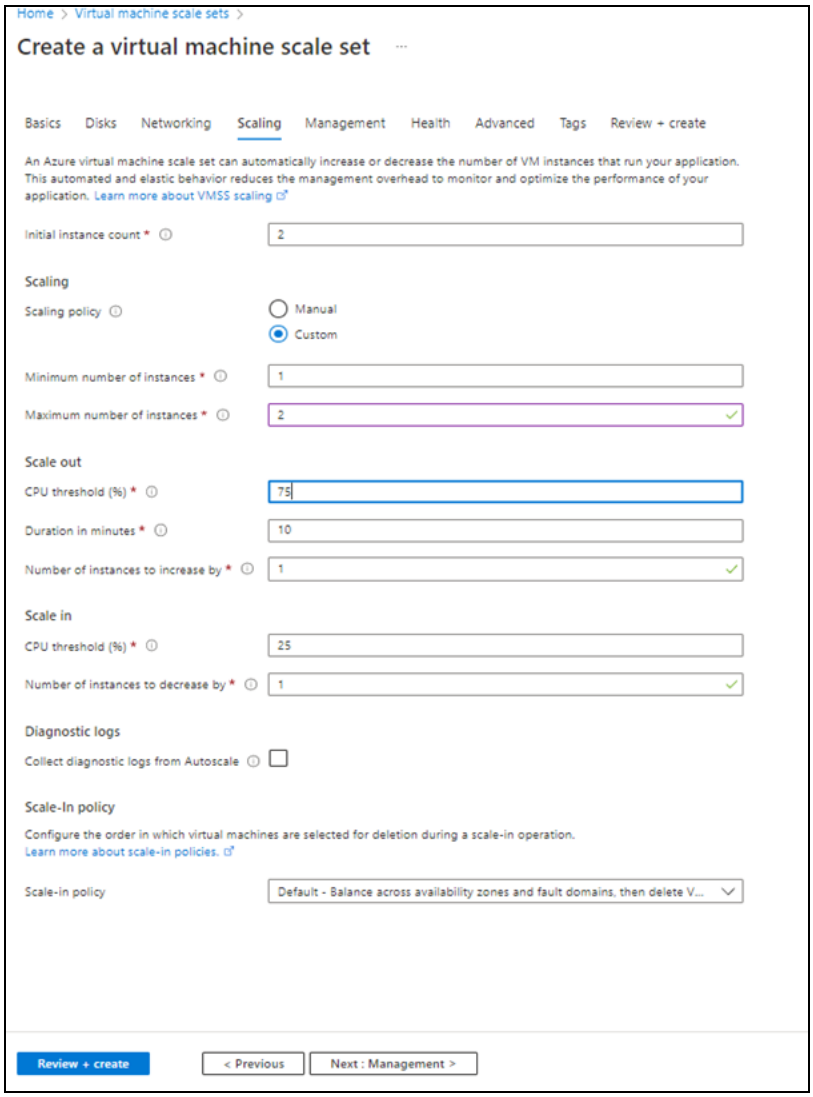
Figure 131 : Edit network interface window



9. Leave the values in other fields unchanged in the **Networking** tab and click **Next : Scaling** at the bottom of the window

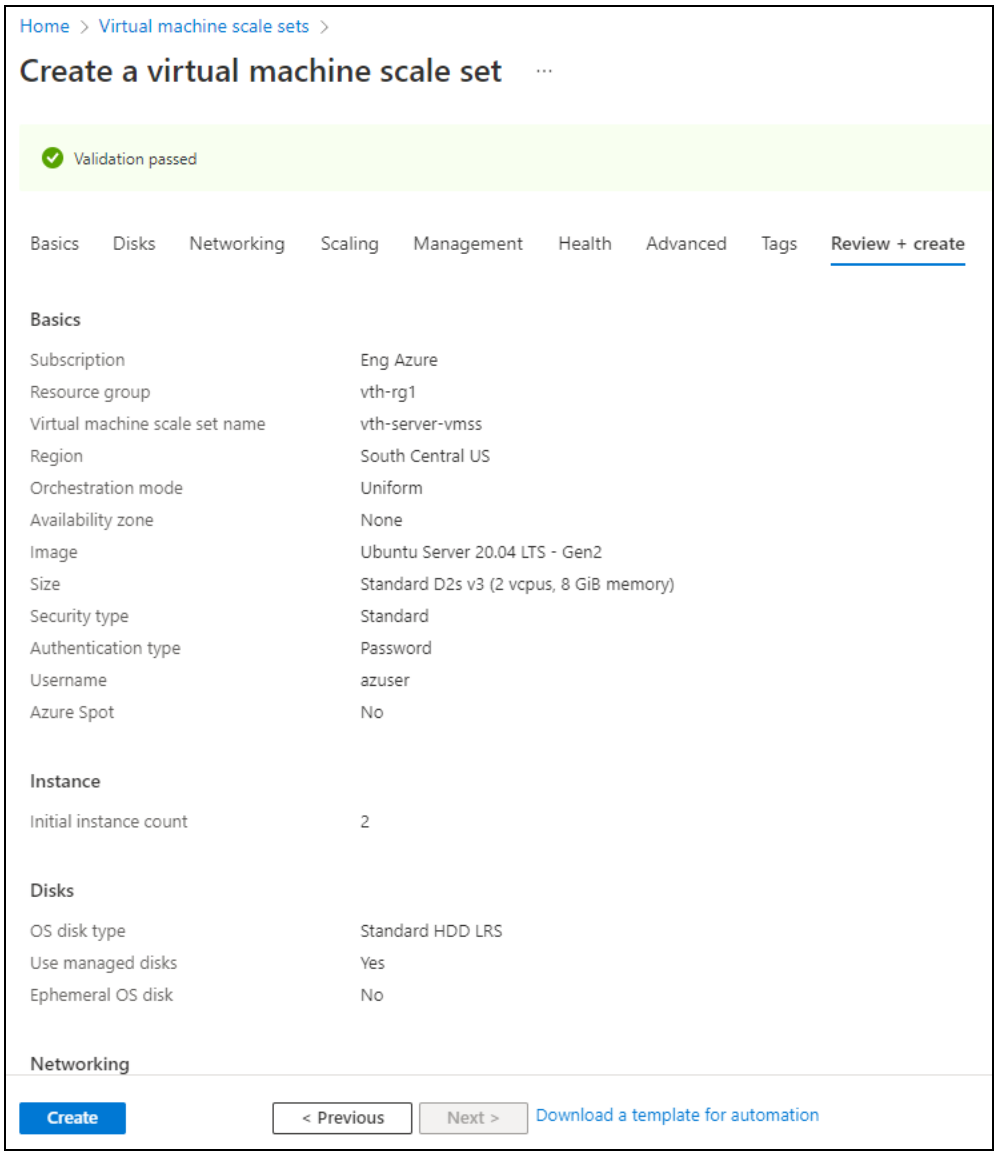
10. Select or enter the information in the **Scaling** tab as shown below.

Figure 132 : Create a virtual machine scale set window - Scaling tab



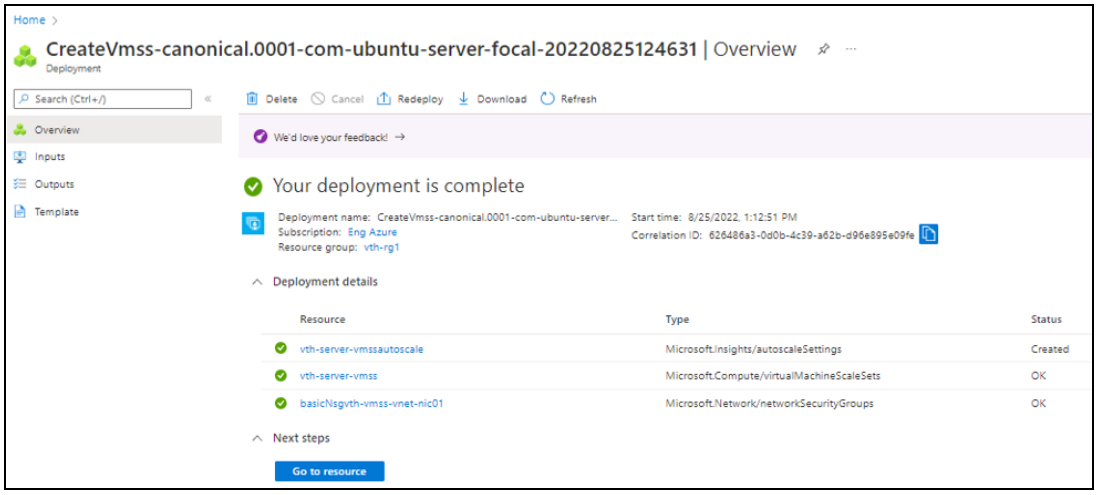
11. Click **Review + create** at the bottom of the window to skip the other tabs.

Figure 133 : 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 134 : Create VMSS window



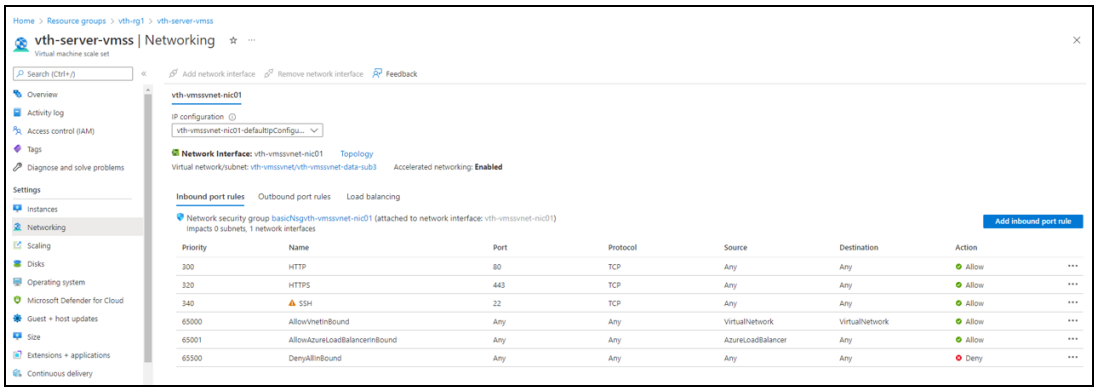
NOTE: It may take the system several minutes to display your resources.

Verify the Server VMSS Creation

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

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

   Figure 135 : VMSS > Inbound port rules



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

Apache:

```
sudo apt install apache2
```

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

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 ARM template.

To configure the parameters, perform the following steps:

1. From Windows Explorer, navigate to the folder where you have downloaded the ARM template.
2. Open the ARM_TMPL_3NIC_NVM_VMSS_RUNBOOK_VARIABLES.json with a text editor.

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

3. Configure the following parameters as appropriate:

Table 7 : JSON Parameters

Resource Name	Description
Azure autos	Specify the autoscale resource details. If the automation account does not exist, then a new automation

Table 7 : JSON Parameters

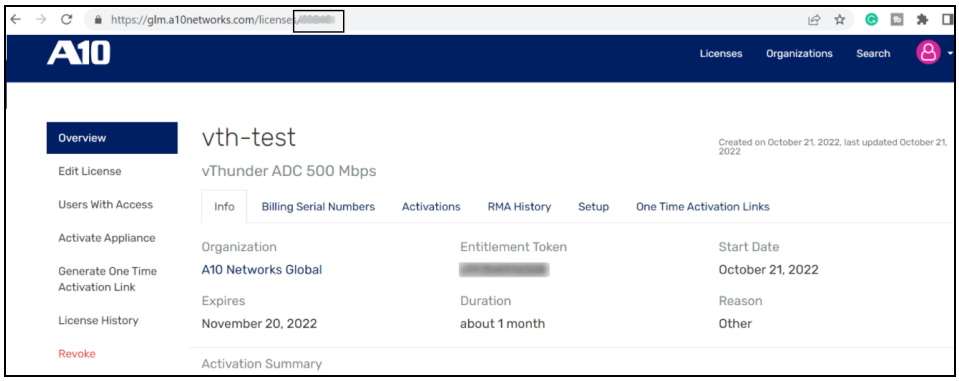
Resource Name	Description

cale resources	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": "10724xxx-xxx-xxxx-xxxx-xxxx2c14726d",`
	`"tenantId": "91d27xxx-xxxx-xxxx-xxxx-xxxxf81fcb2f",`
	`"masterWebhookUrl": "<master-runbook-webhook-url>",`
	`"location": "southcentralus",`
	`"logAnalyticsWorkspaceName": "vth-vmss-log-workspace",`
	`"appInsightsName": "vth-vmss-app-insights"`
	`},`
	
	NOTE: Do not change the **Master Webhook url**. It gets updated automatically.

GLM	Specify the GLM details.

Table 7 : JSON Parameters

Resource Name	Description

	<pre>"glmParam": {
	"userName": "youremail@a10networks.com",
	"userPassword": "your_password",
	"entitlementToken": "A10xxa2fxxxx",
	"licenseId": "59xxx"
	},</pre>
	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
	 

SSL	Specify the SSL details.
	<pre>"sslParam": {
	"requestTimeout": 40,
	"path": "SERVER.pem",
	"file": "SERVER",
	"certificationType": "pem",
	"containerName": "ssl",
	
	"storageAccountKey":"LX6z8xxxxxxehXx0xxxv7xxxx/xxxOfzxxxxxRO
	xxx5gXzxxxxfhxcx0gxxxxx9rxxASxxxsx=="
	},</pre>

Table 7 : JSON Parameters

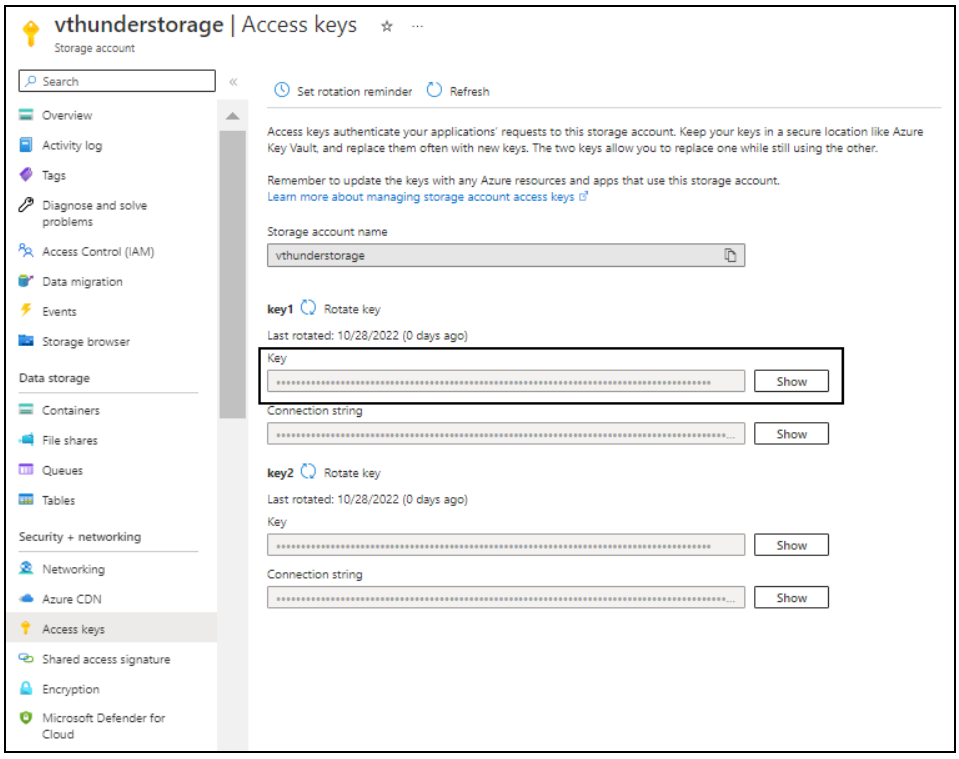
Resource Name	Description
	NOTE: The **`server.pem`** file should be placed in the same downloaded folder from which your are executing the scripts. For example, the server.pem should be placed in 'C:\Users\TestUser\Templates\' folder. You can get the storage account key from **Azure Portal** > **Azure services** > **Storage accounts** > <*storage_account_name*> > **Access Keys** > **Key1** > **Key**. Figure 136 : Selected storage account - Access keys window 
SLB	Specify SLB details.

Table 7 : JSON Parameters

Resource Name	Description

	<pre>"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
	}
	]
	},</pre>

VIP Port	Specify the VIP port details.

Table 7 : JSON Parameters

Resource Name	Description

	<pre>"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"
	}
	]
	},,</pre>

RIB List	Specify the RIB details.

Table 7 : JSON Parameters

Resource Name	Description

	<pre>"rib_list": [
	{
	"ip-dest-addr":"0.0.0.0",
	"ip-mask":"/0",
	"ip-nexthop-ipv4": [
	{
	"ip-next-hop":"10.0.2.1"
	},
	{
	"ip-next-hop":"10.0.1.1"
	}
	]
	},
	{
	"ip-dest-addr":"8.8.8.8",
	"ip-mask":"/32",
	"ip-nexthop-ipv4": [
	{
	"ip-next-hop":"10.0.1.1"
	}
	]
	}
	]
	},</pre>

vThunder IP	<pre>"vThunderIP": "",</pre> **NOTE:** Do NOT provide any IP address. Master runbook updates the vThunder IP automatically.
Client Secret	Specify the client secret. To get this value, go to **Azure Portal** > **Azure services** > **Azure Active Directory** > **App Registration** > **Owned applications** > <*application_name*> > **Certificates & secrets**.

Table 7 : JSON Parameters

Resource Name	Description
	`"clientSecret": "9-xxx~jIxxxEVyxxxxHNxxxOwv_xxxxZLxxxTM",`
vThunder instance username	Specify a 'Read/Write/HM' privilege username. `"vThUsername": "admin"`
vThunder new password application flag	Keep this flag as 'False' initially. `"vThNewPassApplyFlag": "False"`

4. Verify if all the configurations in the ARM_TMPL_3NIC_NVM_VMSS_RUNBOOK_VARIABLES.json file are correct and then save the changes.

Create an Automation Account

To create an automation account, perform the following steps:

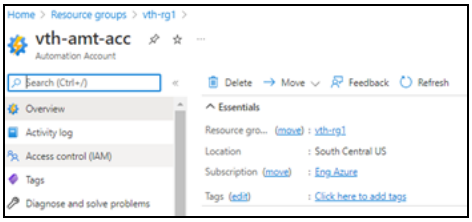
1. Run the following command:
```
PS C:\Users\TestUser\Templates> .\ARM_TMPL_3NIC_NVM_VMSS_AUTOMATION_ACCOUNT_2.ps1
```
2. Provide the default and new password when prompted:
```
Enter Default Password:***
Enter New Password:*********
Confirm New Password:*********
```
The default password is provided by the A10 Networks Support. The new password should follow the Default password policy. For more information, see Default Password Policy.

Verify the Automation Account Creation

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

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

   Figure 137 : Selected automation account - Overview window



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

   Figure 138 : Selected automation account - Variables window

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

Create Automation Account Webhook

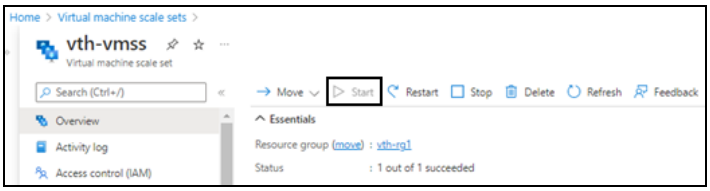
The following topics are covered:

Initial Setup

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

1. From **Home**, navigate to **Azure services** > **Resource Group** > *<resource_group_name>*.
   The selected resource group - Overview window is displayed.

   Figure 139 : VMSS window

2. Under **Resources** tab, group the resources based on the resource type.
3. Select the virtual machine scale set instance under **Virtual machine scale set** type and verify that the instance is in **Start** mode.

Create a Webhook

To create a webhook, perform the following steps:

1. From Start menu, open PowerShell and navigate to the folder where you have downloaded the ARM template.
2. Run the following command to create the webhook:

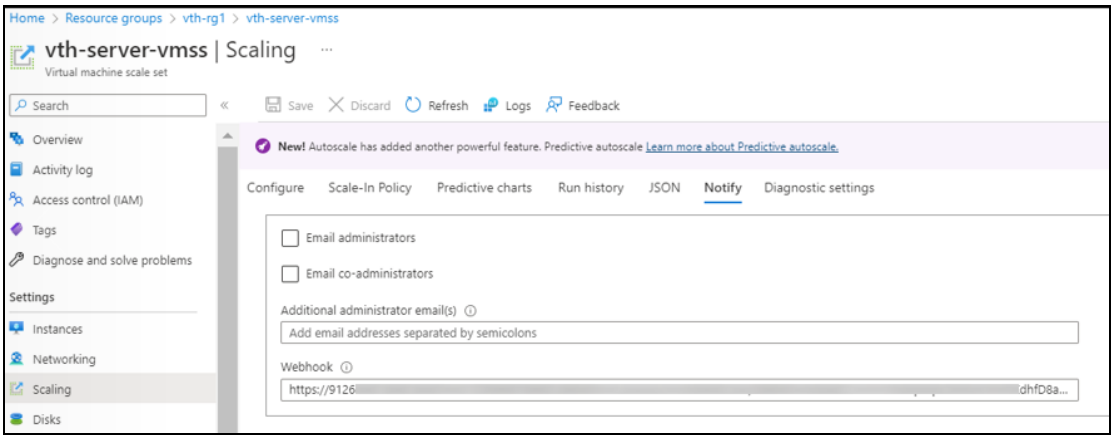
```
PS C:\Users\TestUser\Templates> .\ARM_TMPL_3NIC_NVM_VMSS_WEBHOOK_3.ps1
```

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

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

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

   Figure 140 : VMSS-Scaling - Notify tab



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

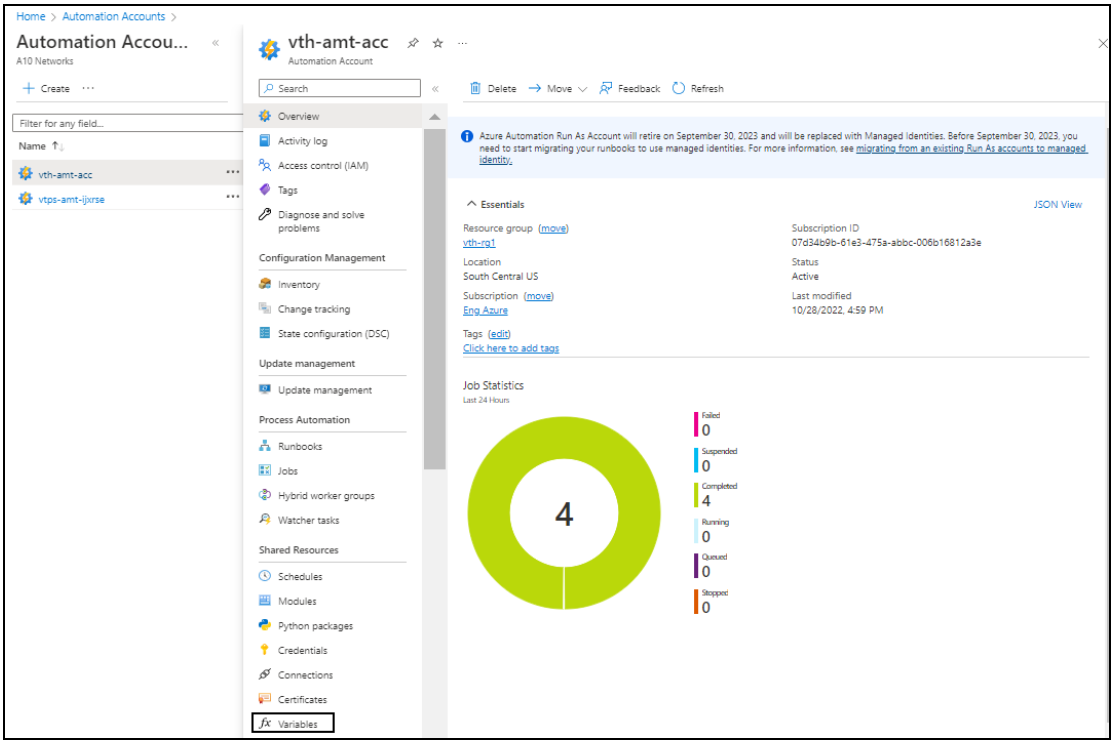
Verify the AutoScale Resource Variable creation

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

1. From **Home**, navigate to **Azure services** > **Automation Accounts** > <*automation_ account_name*>.

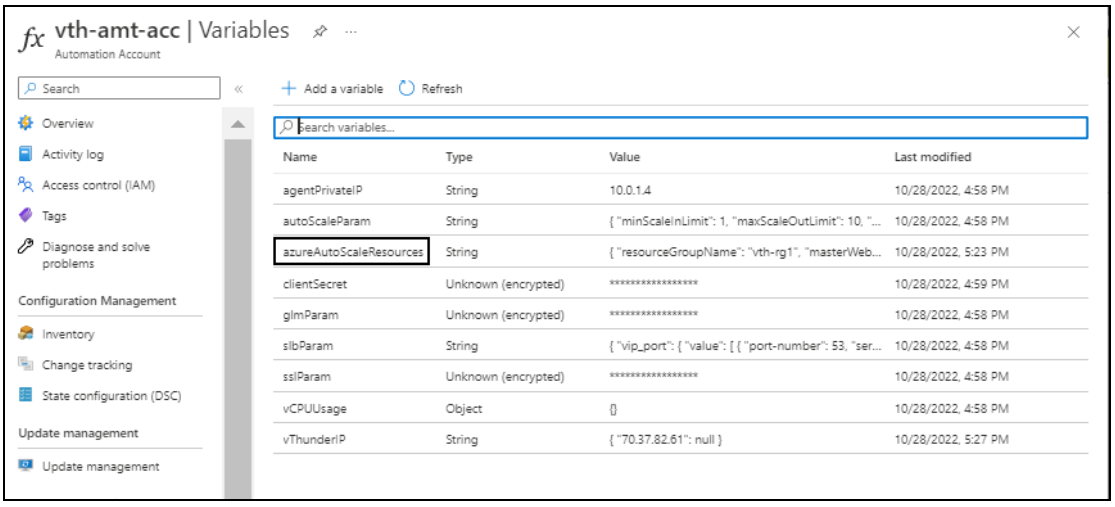
   The selected automation account - Overview window is displayed.

Figure 141 : Selected automation account - Overview window



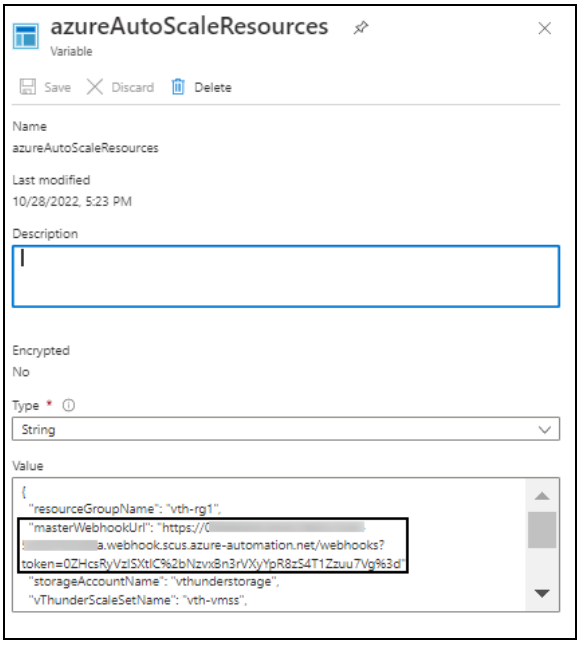
2. Click **Variables** from the left **Shared Resources** panel.
The selected automation account - Variables window is displayed.

Figure 142 : Selected automation account - Variables window



3. Select the **azureAutoScaleResources** variable.
The azureAutoScaleResources variable window is displayed.

Figure 143 : AzureAutoScaleResources variable window



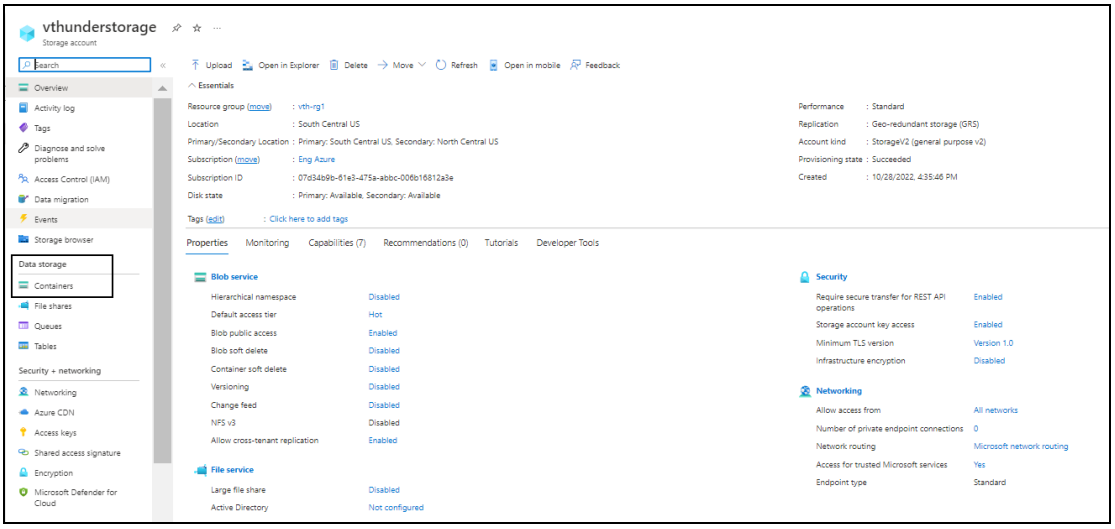
4. Verify the master webhook URL in the **Value** field.

Verify the SSL File availability

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

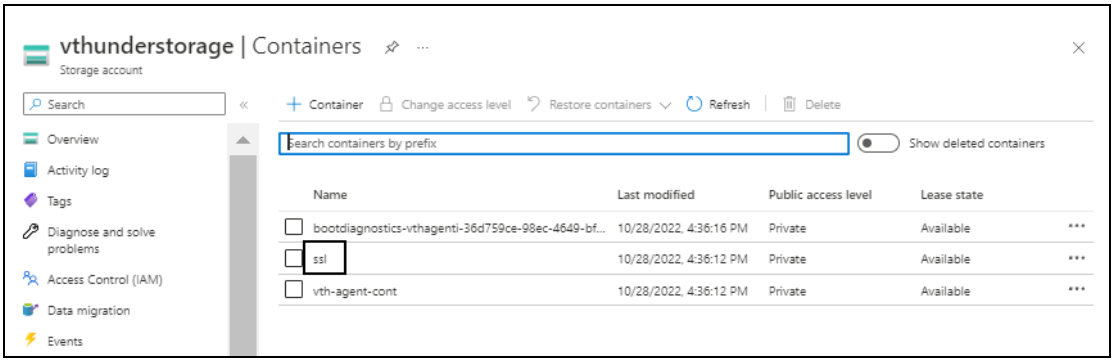
1. From **Home**, navigate to **Azure services** > **Storage Accounts** > <*storage_account_name*>.
   The selected storage account - Overview window is displayed.

Figure 144 : Selected storage account - Overview window



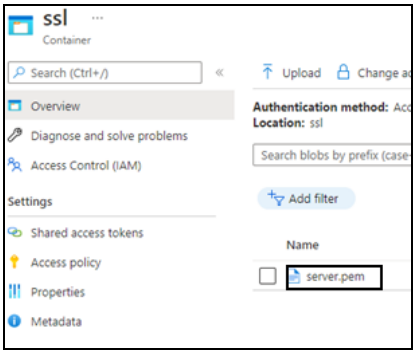
2. Click **Containers** from the left **Data Storage** panel.
   The selected storage account - Containers window is displayed.

Figure 145 : Selected storage account - Containers window



3. Select the SSL container.
   The SSL container window is displayed.

Figure 146 : SSL Container window



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

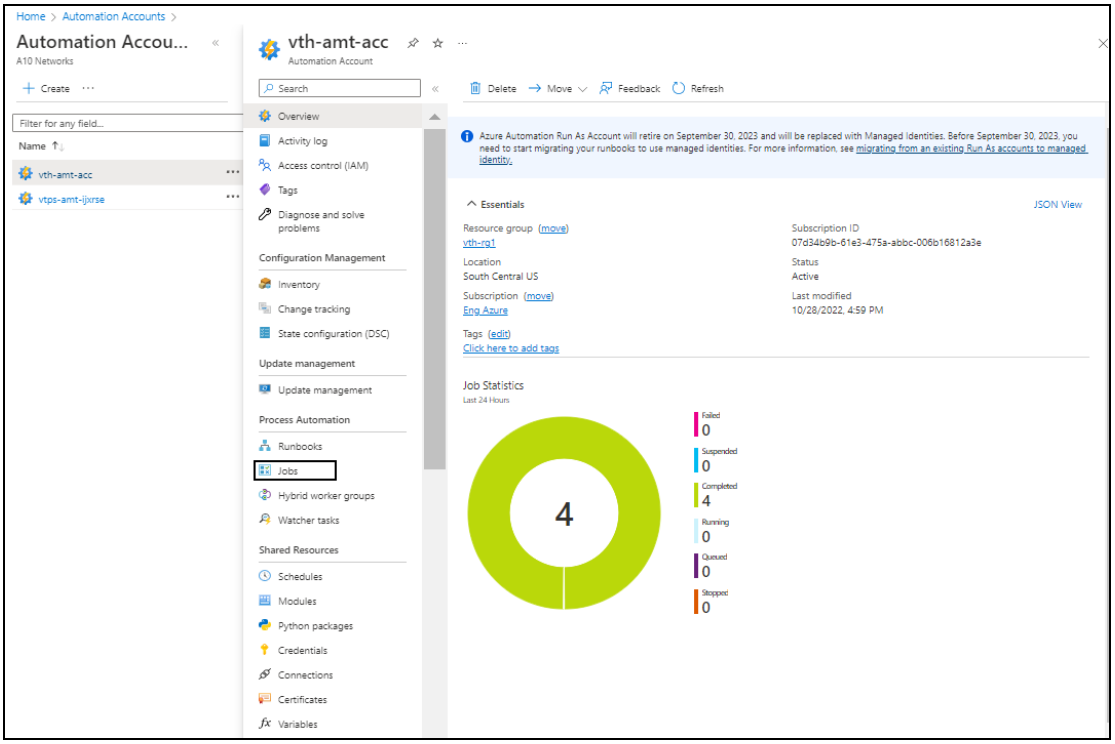
Verify the Runbook Jobs creation

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

1. From **Home**, navigate to **Azure services** > **Automation Accounts** > <*automation_account_name*>.

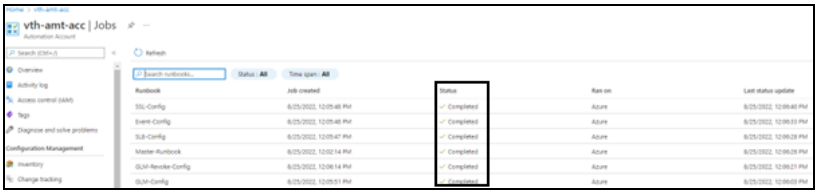
   The selected automation account - Overview window is displayed.

Figure 147 : Selected automation account - Overview window



2. Click **Jobs** from the left **Process Automation** panel.
   The selected automation account - Jobs window is displayed.

   Figure 148 : Selected automation account - Jobs window



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

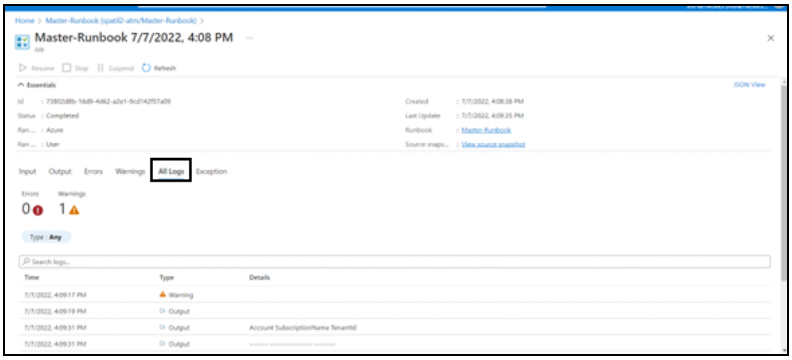
   The master runbook automatically triggers all the jobs one-by-one.

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

   If any job has failed or if it is not working, refer Common Errors.

4. Select each runbook job > **All Logs** tab to verify the logs.
   The selected automation account - selected job - Jobs window is displayed.

Figure 149 : Selected runbook job window



Install Thunder Observability Agent

The A10 Thunder Observability Agent is introduced to monitor A10 Thunder® Application Delivery Agent (ADC) performance metrics and syslogs.

There are two types of A10 Thunder Observability Agent available:

Internal Thunder Observability Agent (iTOA)

This is an in-built Python plugin within ACOS which is configured using ACOS Command Line Interface (CLI) or aXAPI.

You can use iTOA:

- For ACOS v6.0.1 or later.
- For configuring vThunder using aXAPI or CLI to publish the 14 performance metrics directly on the same AWS, Azure, or VMware platform where the vThunder instance is deployed with outbound internet connectivity.
- For configuring vThunder using aXAPI or CLI to publish the syslogs on:
  - AWS CloudWatch directly from vThunder with outbound internet connectivity.
  - Azure Log Analytics Workspace directly from vThunder with outbound internet connectivity to access '**.microsoftonline.com*' and '**.azure.com*'.
  - VMware vRealize Log Insight (vRLI) which is accessible from vThunder.
- For managing the data collection, processing, aggregation, and publishing internally for configured L3V partitions.

- For supporting maximum 20 partitions per vThunder instance.
- For publishing metrics or logs every one minute.

To configure the Internal Thunder Observability Agent, see Internal Thunder Observability Agent.

External Thunder Observability Agent (TOA)

This external plugin can be installed on Linux, CentOS, and Ubuntu platforms as a Python Plugin installation package and Docker containerization.

You can use TOA:

- For any ACOS deployment platform.
- For any ACOS software version.
- For a Thunder with outbound internet connectivity restrictions.

  In this case, TOA can have outbound internet connectivity. It can collect data from Thunder and then publish the metrics and syslogs on the cloud monitoring tool through internet.

To install the external Thunder Observability Agent, see External Thunder Observability Agent.

NOTE: It is recommended to configure any one TOA at a time.

Configure Autoscaling

An Azure virtual machine scale set can automatically increase or decrease the number of vThunder VM instances to meet the changing demand. The Azure metrics and logs can be monitored using an internal Thunder Observability Agent (iTOA) or external Thunder Observability Agent (TOA).

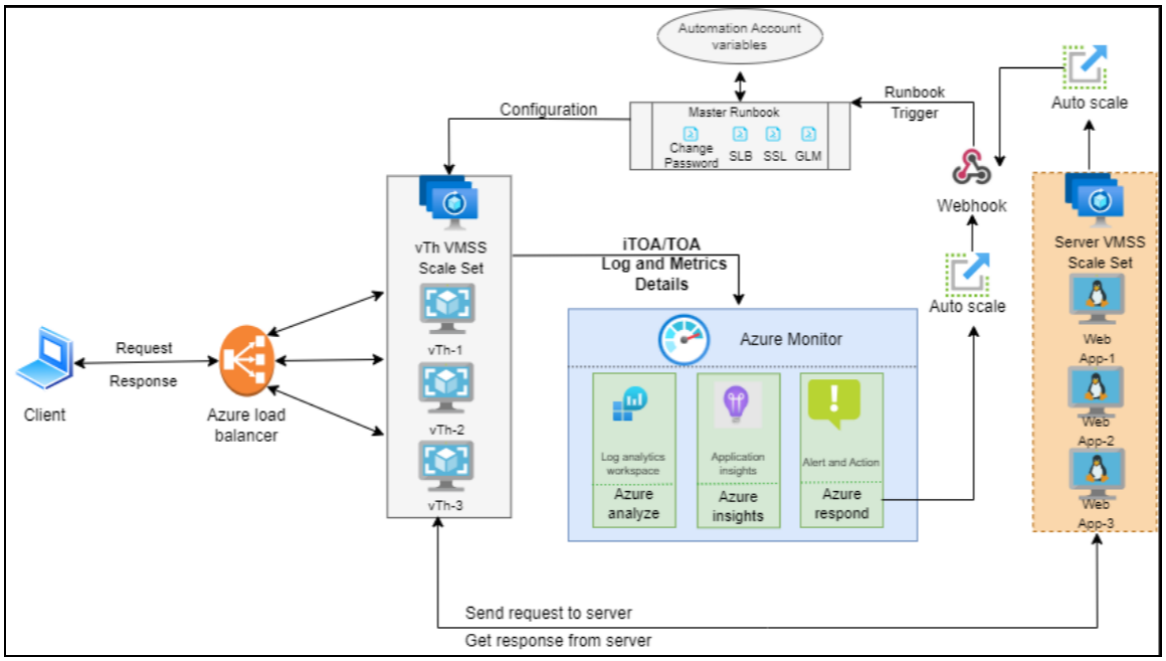
Using iTOA or TOA:

- Custom metrics of vThunder can be collected and published into Azure Application Insights service and same metrics can be used along with VMSS rule for autoscaling. See Create Autoscale Rule.
- Alerts can be scheduled using VMSS alert rule. See Create Autoscale Alert.

- vThunder metrics can be viewed in the Azure Application Insights console.
- vThunder logs can be viewed in the Azure Log Analytics Workspace.

Figure 150 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 iTOA or TOA.

Figure 150 : Process Flow



The following topics are covered:

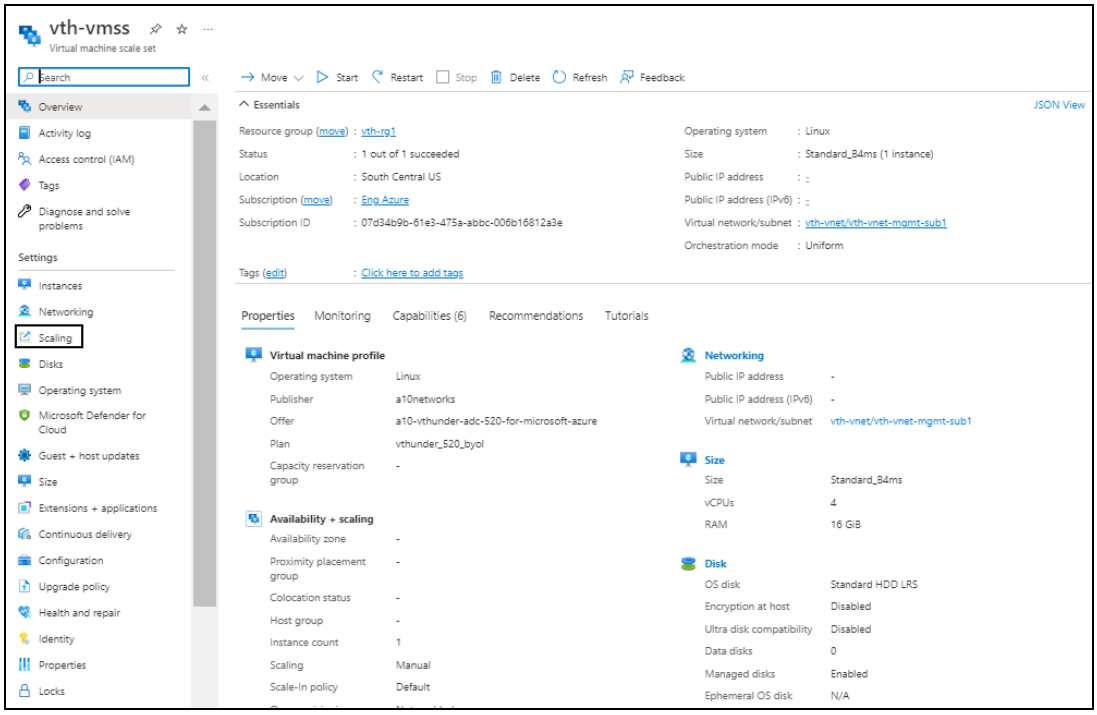
1. Create Autoscale Rule
2. Create Autoscale Alert

Create Autoscale Rule

To create autoscale rule, perform the following steps:

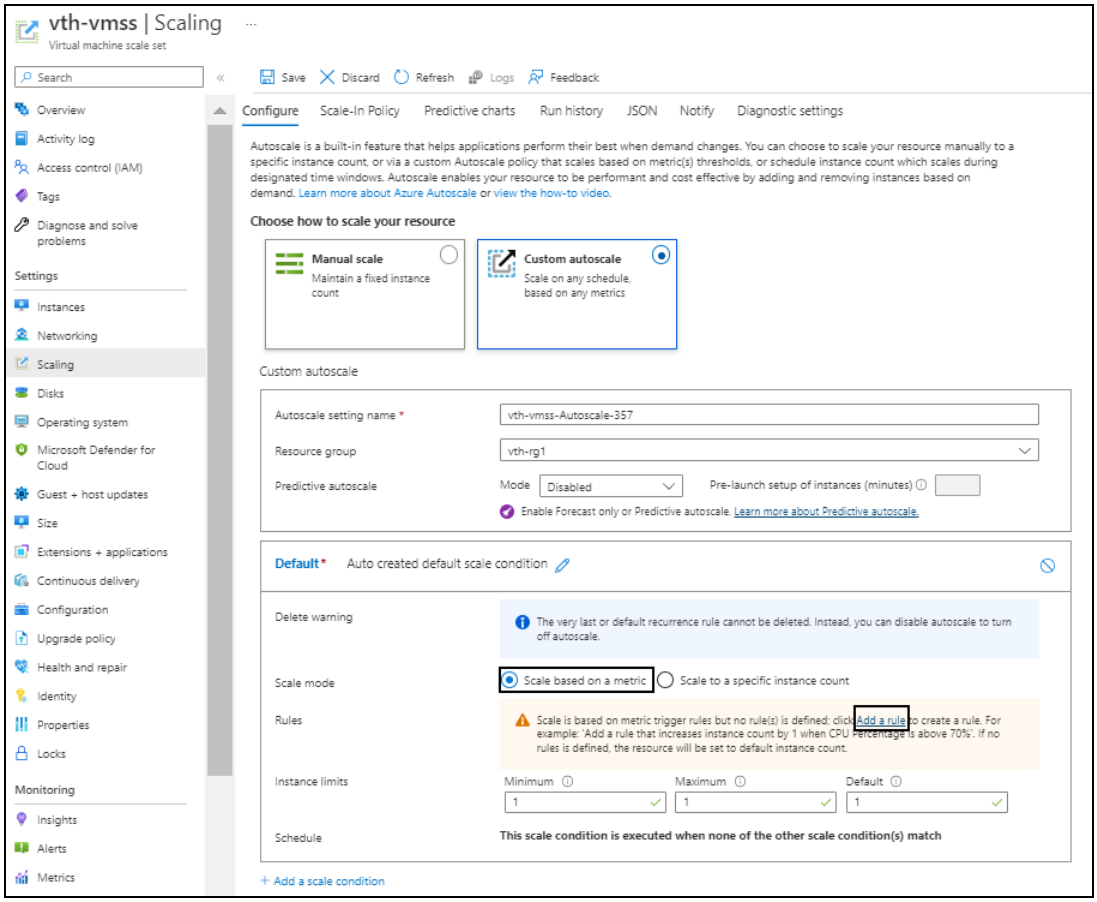
1. From **Home**, navigate to **Azure services** > **Virtual machine scale set** > <*vmss_name*>.
   The selected vmss - Overview window is displayed.

Figure 151 : Selected VMSS - Overview window



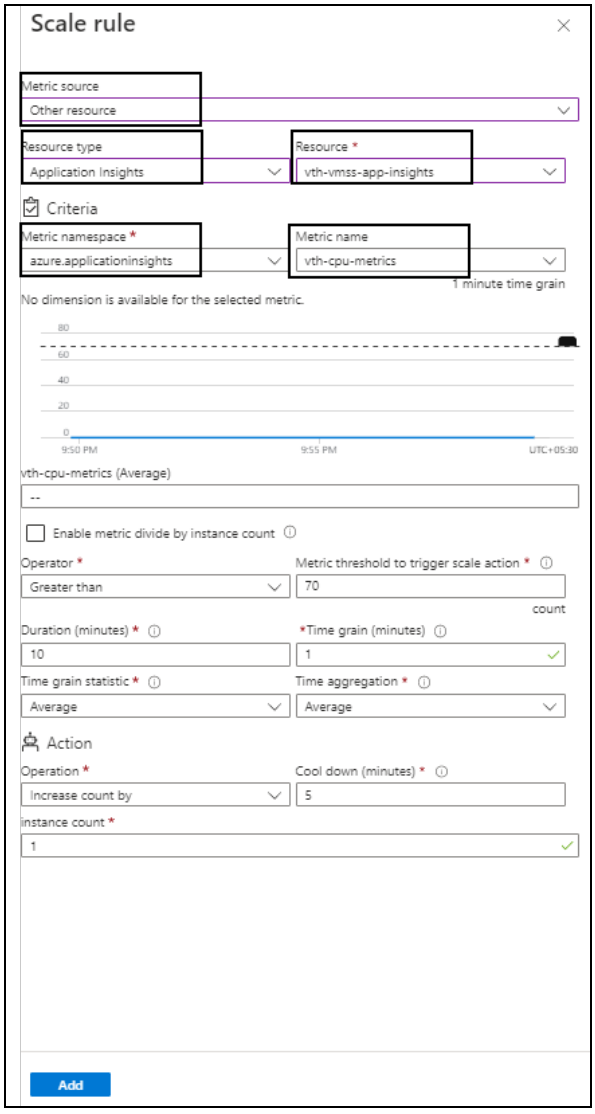
2. Click **Scaling** from the left **Settings** panel.
   The selected vmss - Scaling window is displayed.

Figure 152 : 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 153 : Scale rule window

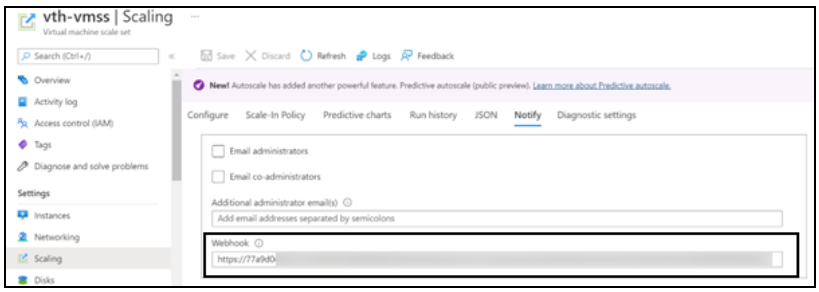


6. Select or enter the information in the following fields:
   - Metric source: Other resource
   - Resource type: Application Insights
   - Resource
   - Time aggregation

- Metric namespace
- Metric name: <*custom_metrics_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**.

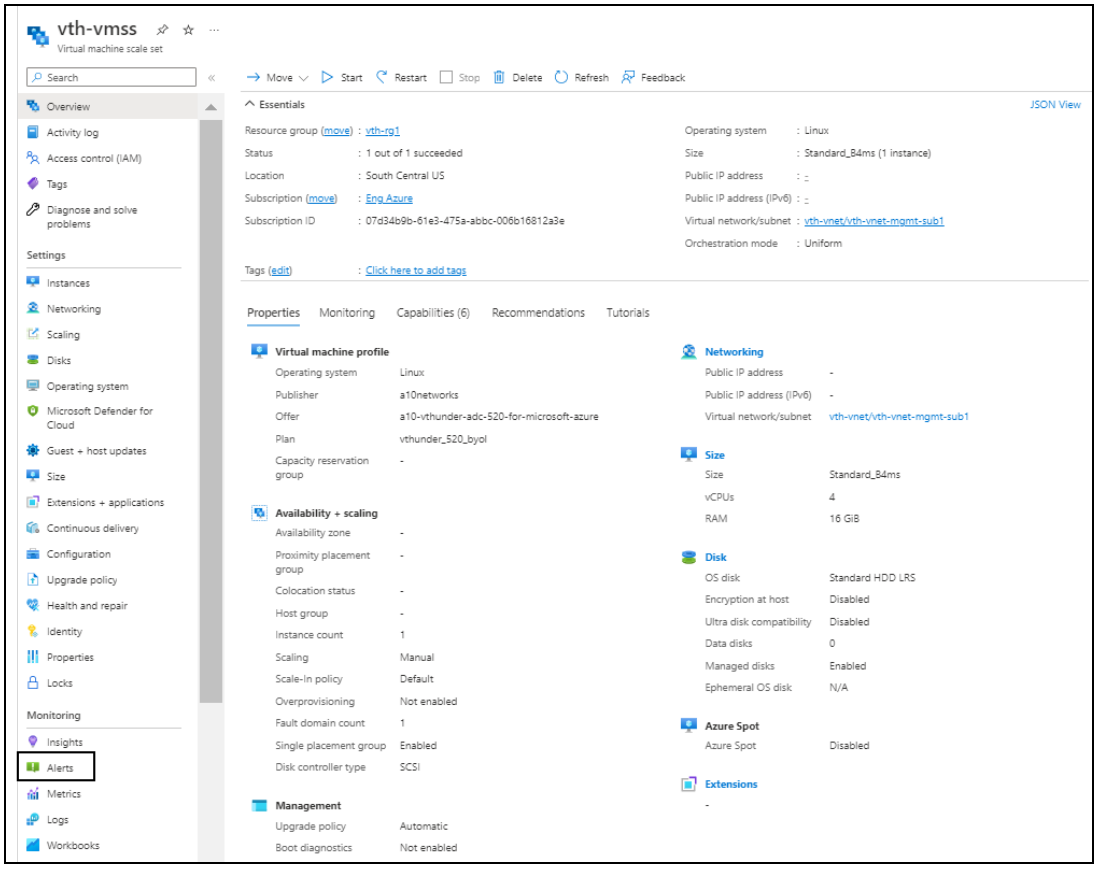
   Figure 154 : Selected VMSS - Scaling window - Notify tab



Create Autoscale Alert

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

Figure 155 : Selected VMSS - Overview window

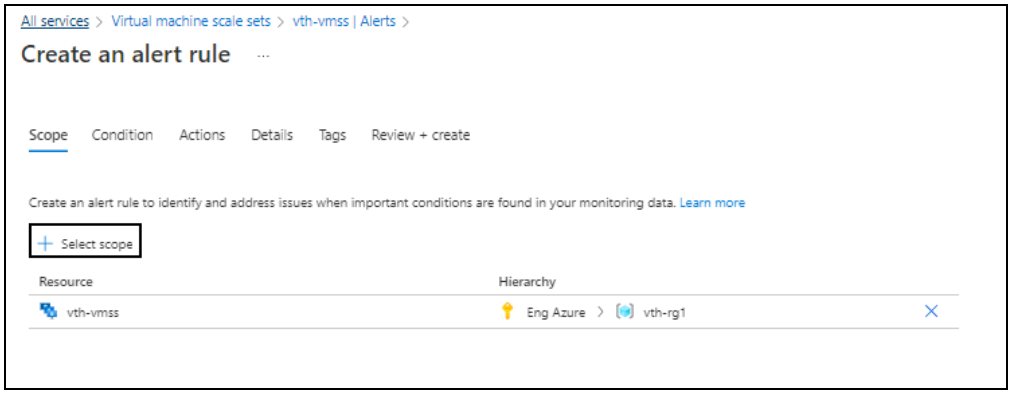


2. Click **Alerts** from the left **Monitoring** panel.
   The selected vmss - Alerts window is displayed.

Figure 156 : Selected VMSS - Alerts window

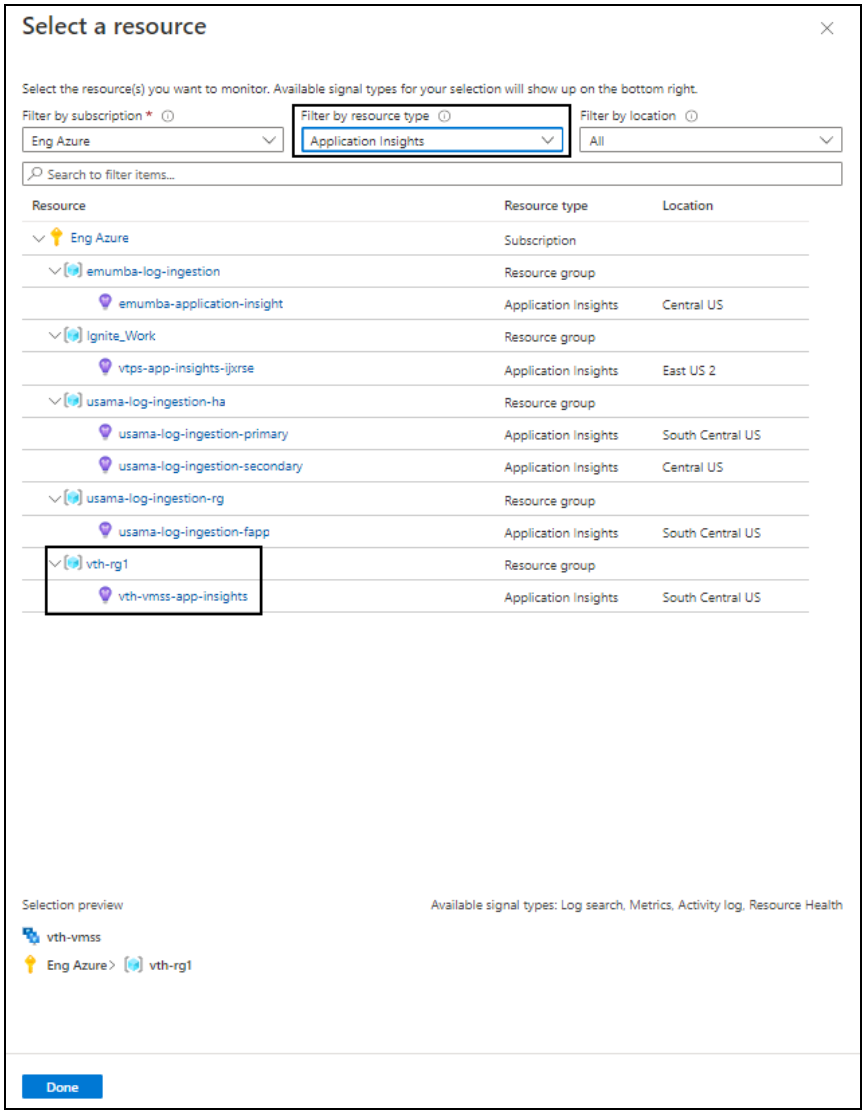
3. Click **Create** > **Alert rule**.
   The Create an alert rule - Scope window is displayed.

Figure 157 : Create an alert rule window - Scope tab



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

Figure 158 : Select a resource window

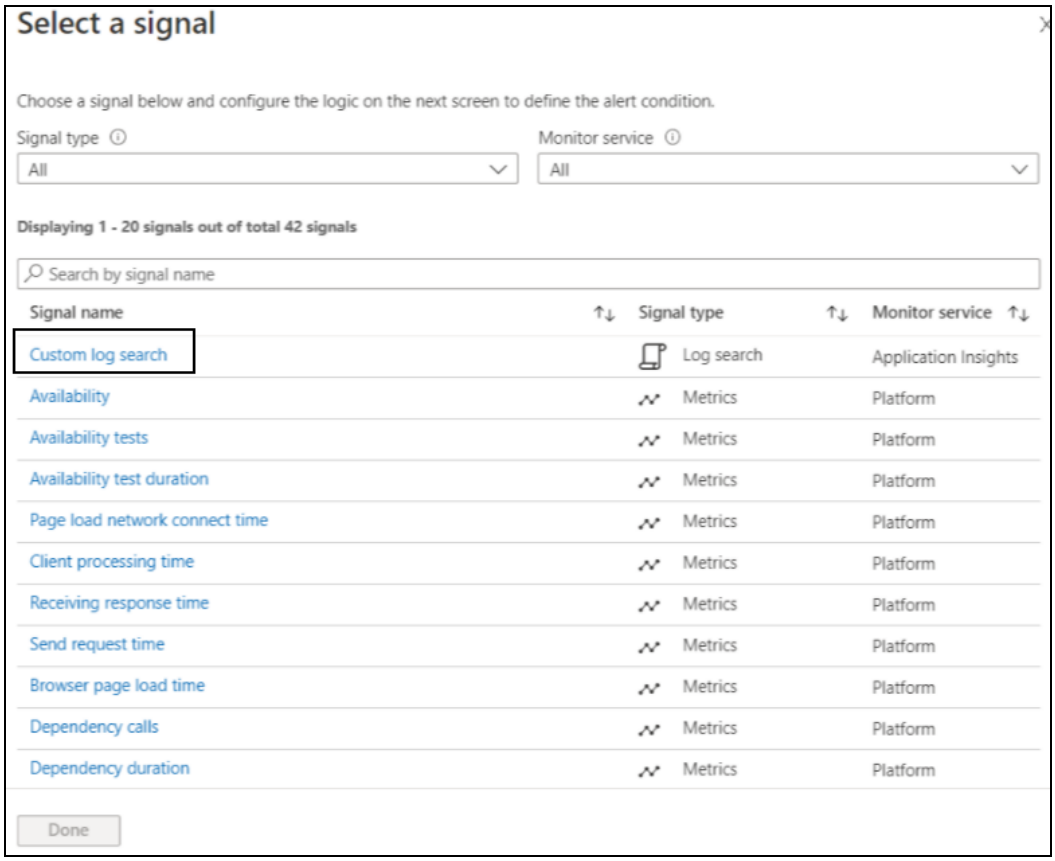


5. From **Filter by resource type**, select **Application Insights**.
   The resource group having application insight resources are displayed.
6. Select the required application insight resource and click **Done**.
   The selected application insight resource is listed under the alert rule scope.
7. Click **Next : Condition** at the bottom of the window.
   The **Create an alert rule** - **Condition** tab window is displayed.

Figure 159 : Create an alert rule window - Condition tab

8. Click **Add condition** in the **Condition** tab.
   The **Select a signal** window is displayed.

Figure 160 : Select a signal window

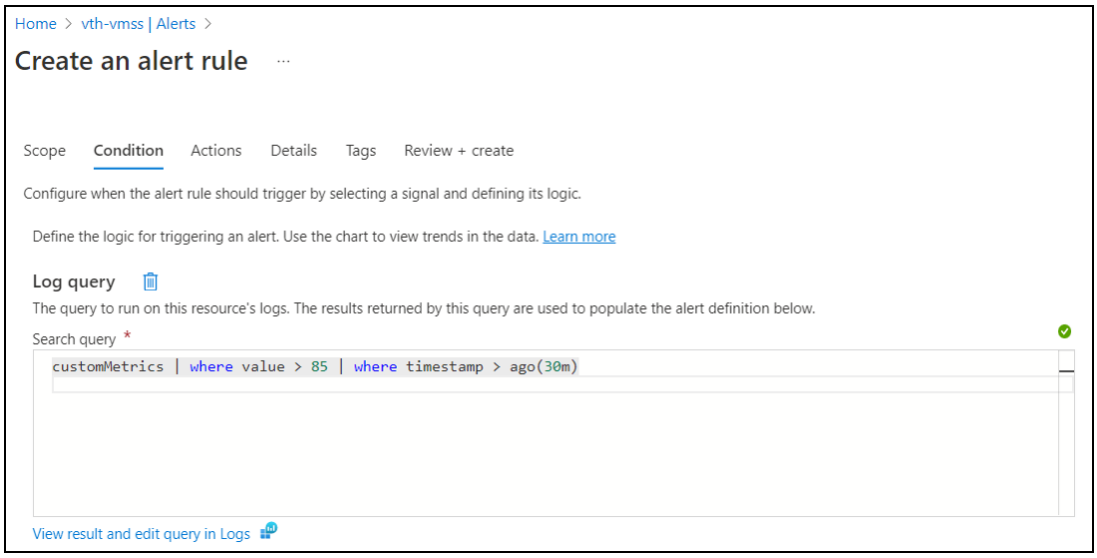


9. Select **Custom log search** as the signal.
   The window to define the signal's logic is displayed in the alert rule condition.
10. Enter any of the following query to fetch the data in the **Search query** field:

```
THUNDER_SYSLOGS_CL | where value > 85 | where timestamp > ago(30m)
THUNDER_SYSLOGS_CL | where value > 85 | where timestamp > ago(24h)
THUNDER_SYSLOGS_CL | where value > 85 | where timestamp > ago(7d)
```

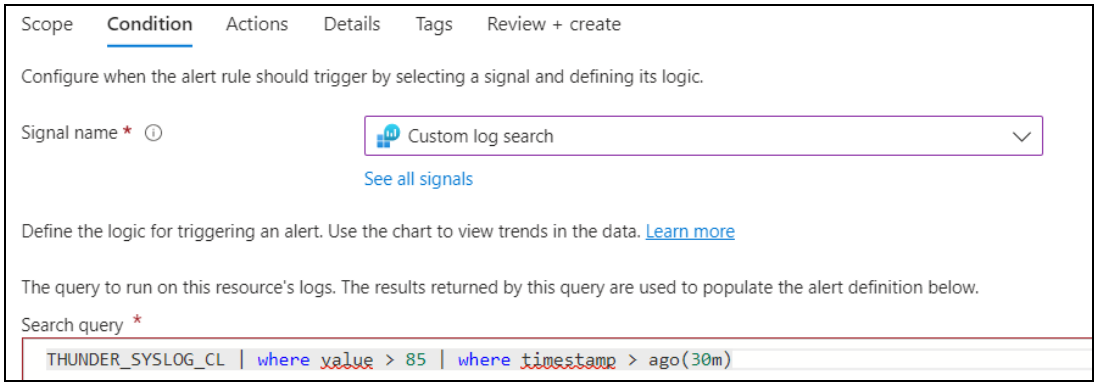
The above query specifies the frequency for alert data.

Figure 161 : Create an alert rule window - Condition tab



11. Configure alert logic in the **Alert logic** section.

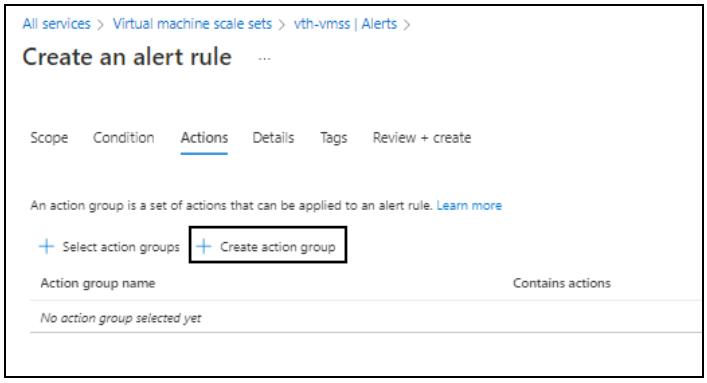
Figure 162 : Alert logic section



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

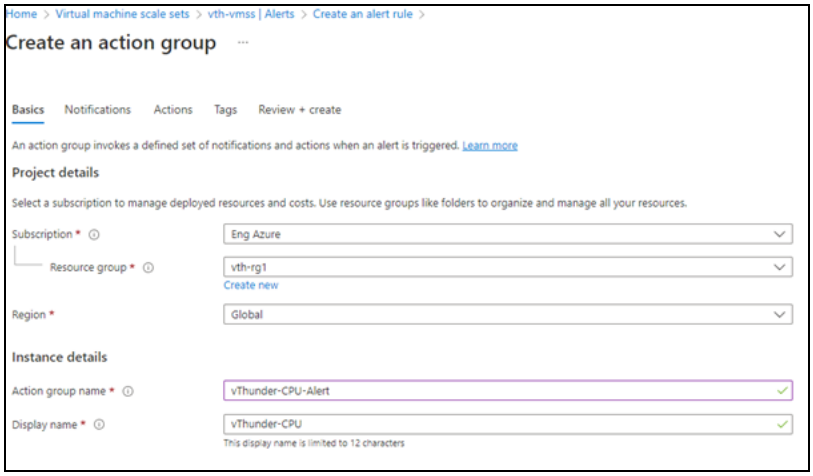
12. Click **Next : Actions** at the bottom of the window.
The **Create an alert rule** - **Actions** window is displayed.

Figure 163 : Create an alert rule window - Actions tab



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

Figure 164 : 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

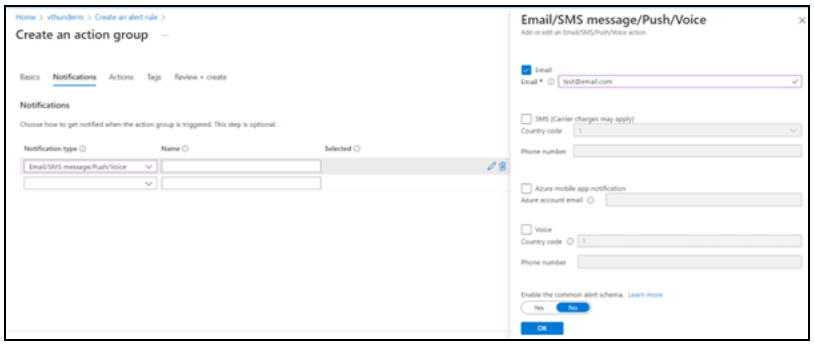
Instance details

- 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.

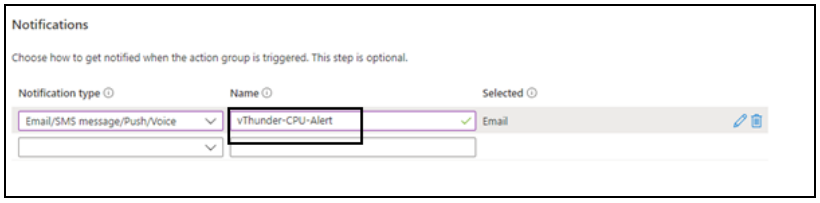
Figure 165 : Create an action group window - Notifications tab - Type



d. Select the **Email** option and provide the correct email ID in the **Email** field and then click **OK**.

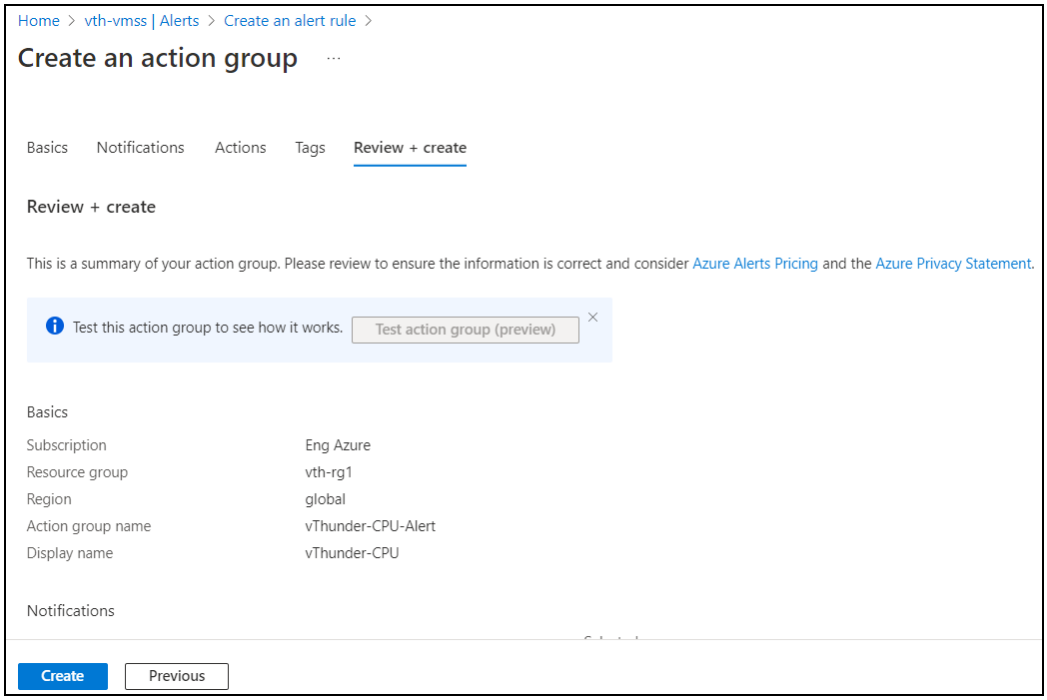
e. Enter a unique name for the notification in the **Name** field.

Figure 166 : Create an action group window - Notifications tab



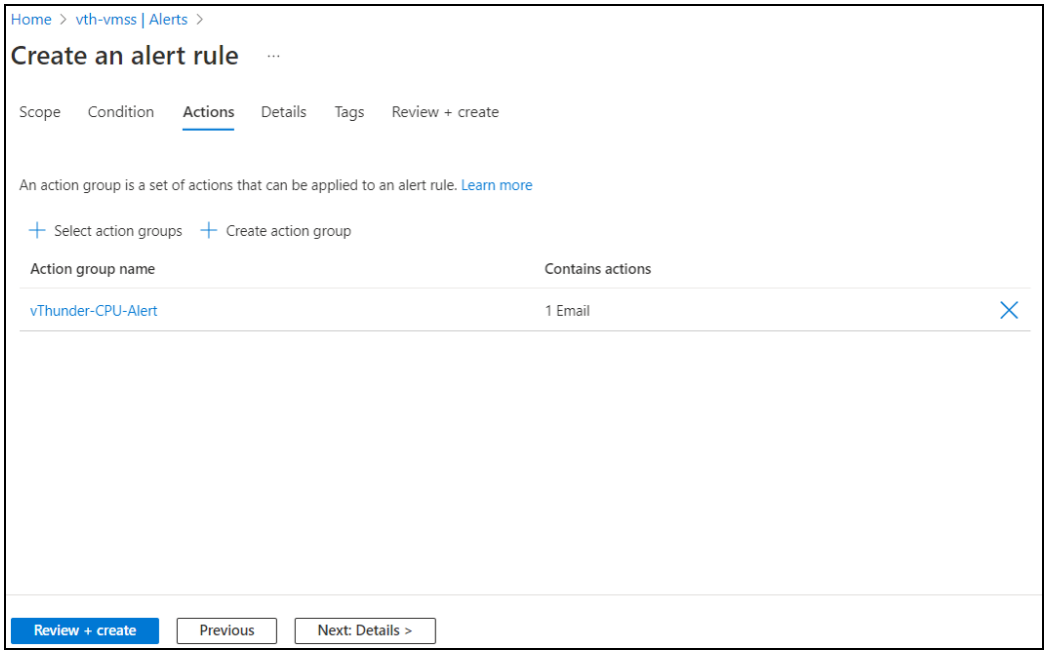
f. Skip the other tabs and click **Review + create** at the bottom of the window.
The **Create an action group** - **Review + create** window is displayed.

Figure 167 : Create an action group window - Review + create tab



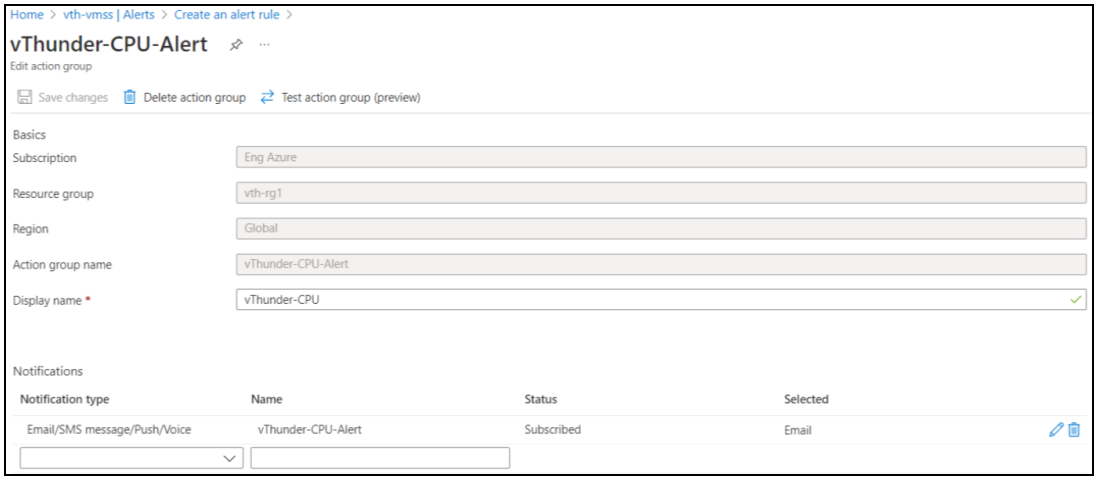
g. Click **Create**.
The action group is listed under **Actions** tab.

Figure 168 : Create an alert rule window - Actions tab



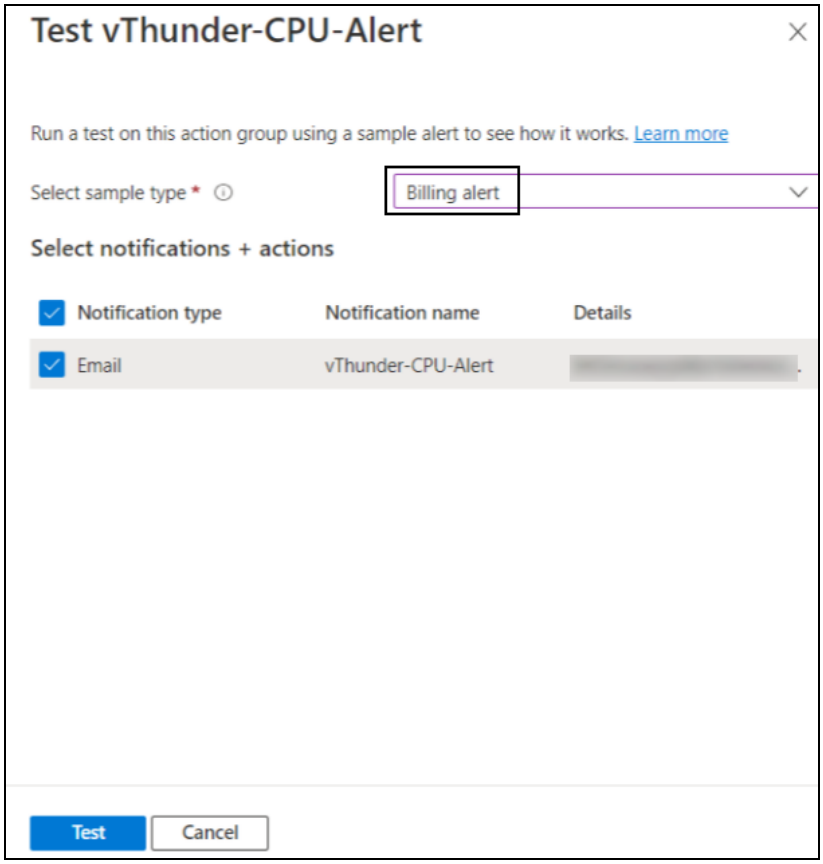
14. Select the recently created action group.
The selected action group is displayed.

Figure 169 : Selected action group



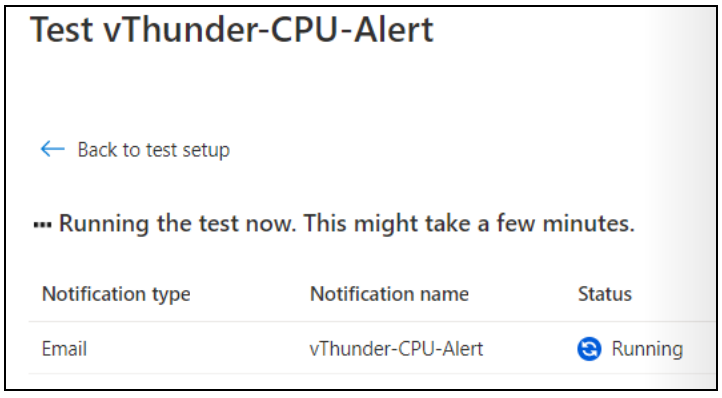
15. Click **Test action group (preview)**.
The Test <*action_group_name*>-alert window is displayed.

Figure 170 : Test <action_group_name>-alert window



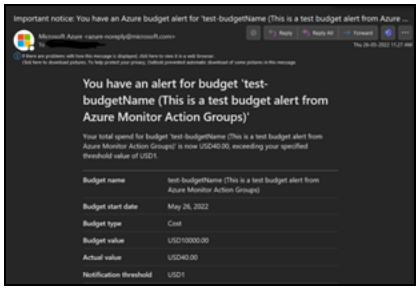
16. Select **Billing alert** as the Sample type and click **Test**.
The running status for the test rule is displayed.

Figure 171 : Test <action_group_name>-alert window - Running status



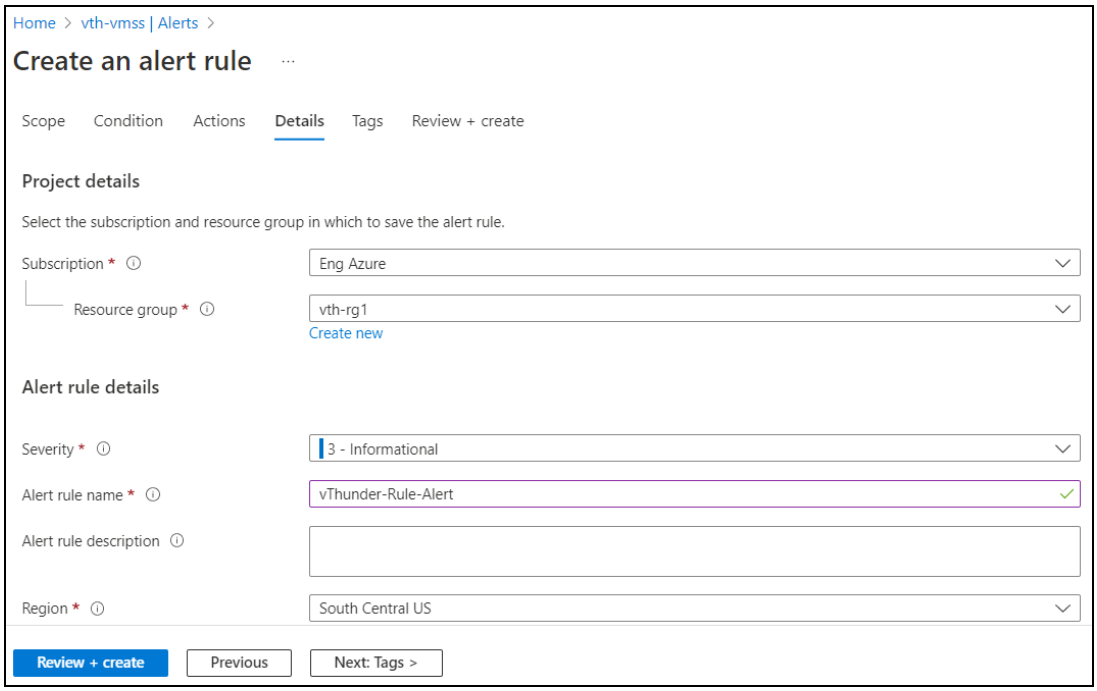
When the success status is displayed, an email notification is triggered to the email ID provided in the Email Notification step.

Figure 172 : Email Notification



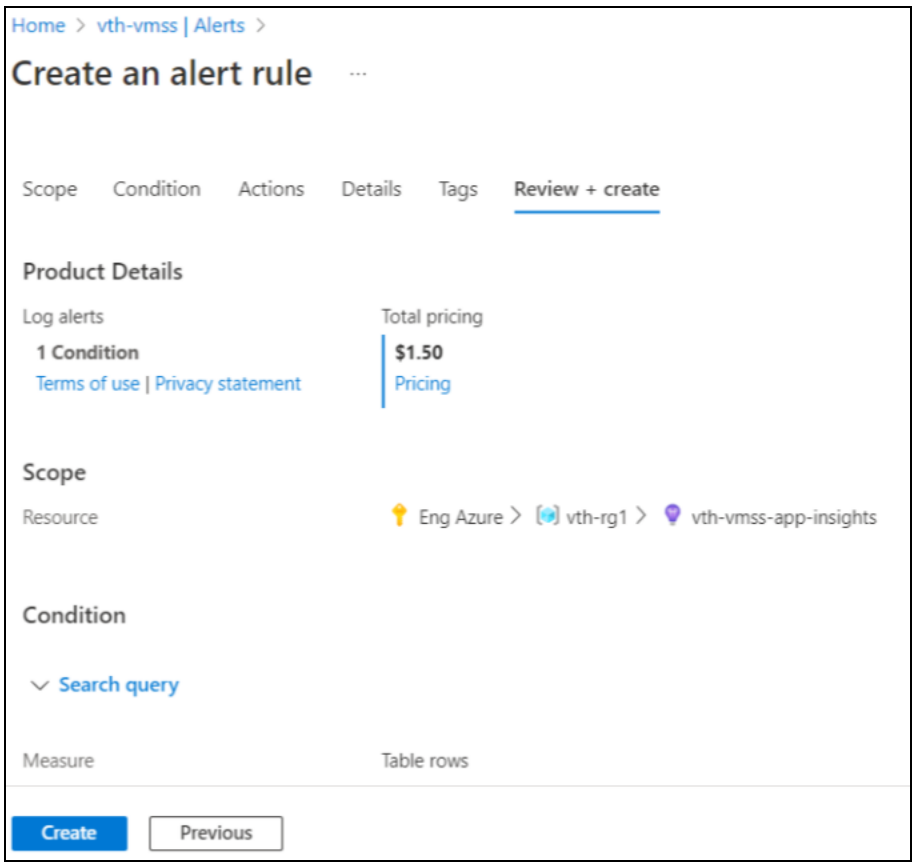
17. Click **Done** on Test <*action_group_name*>-alert window.
The selected action group is displayed.
18. Close the selected action group window.
The Create an alert rule - Actions window is displayed.
19. Click **Next : Details** at the bottom of the window.
The **Create an alert rule** - **Details** window is displayed.

Figure 173 : Create an alert rule window - Details tab



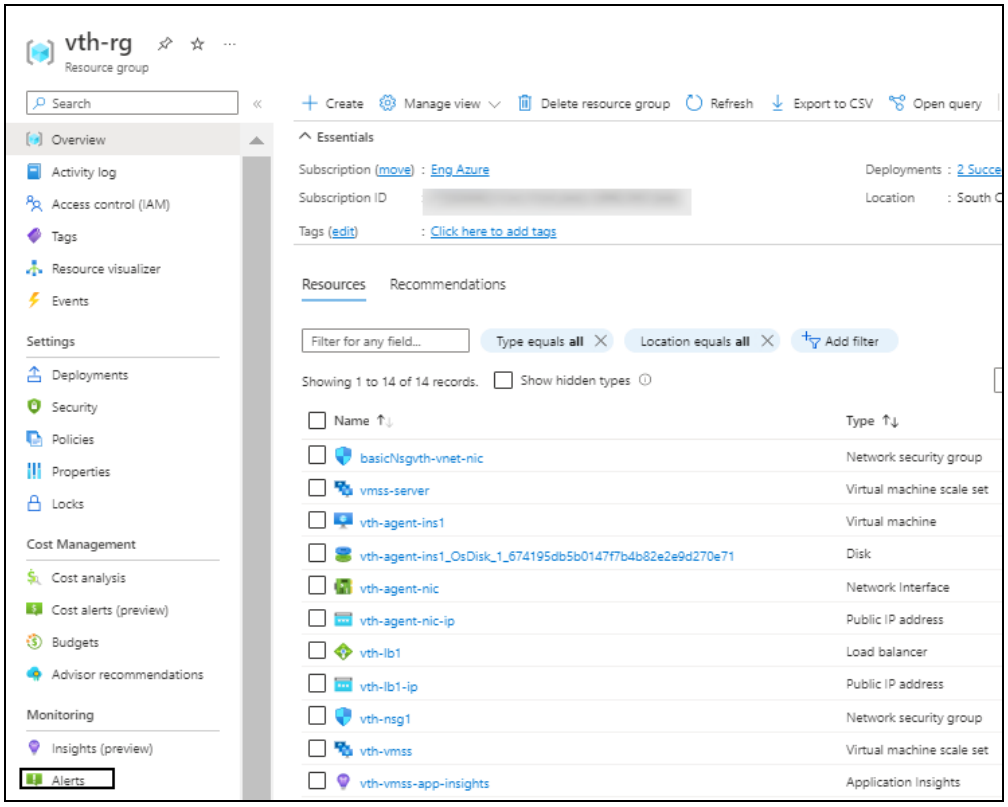
20. Enter the Alert rule name and provide the other mandatory details.
21. Skip the other tabs and click **Review + create** at the bottom of the window.
    The **Create an alert rule** - **Review + create** window is displayed.

    Figure 174 : Create an alert rule window - Review + create tab



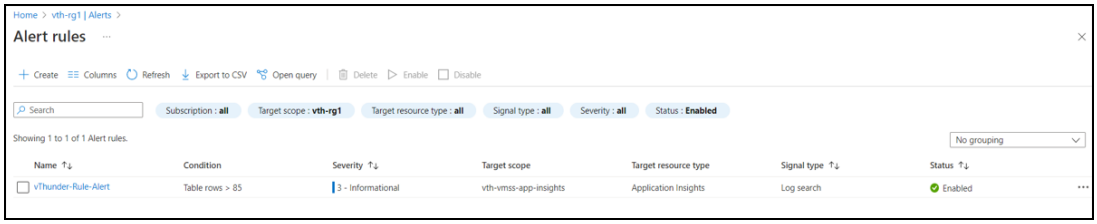
22. Click **Create**.
    The alert rule is created.
23. From **Home**, navigate to **Azure services** > **Resource groups** > *<resource_group_name>*.
    The selected resource group - Overview window is displayed.

Figure 175 : 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 176 : Selected resource group - Alert rules window



Verify Deployment

To verify deployment using the ARM template, perform the following steps:

1. Run the following command on vThunder:

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

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

```
!Section configuration: 711 bytes
!
slb server vth-server-vmss_0 10.0.3.5
  port 53 udp
       health-check-disable
  port 80 tcp
       health-check-disable
  port 443 tcp
       health-check-disable
!
```

```
slb service-group sg443 tcp
  health-check-disable
  member vth-server-vmss_0 443
!
slb service-group sg53 udp
  health-check-disable
  member vth-server-vmss_0 53
!
slb service-group sg80 tcp
  health-check-disable
  member vth-server-vmss_0 80
!
slb virtual-server vip use-if-ip ethernet 1
  port 53 udp
    ha-conn-mirror
    source-nat auto
    service-group sg53
  port 80 http
    source-nat auto
    service-group sg80
  port 443 https
    source-nat auto
    service-group sg443
!
slb virtual-server vip2 10.0.2.10
!
```

2. Run the following command on vThunder to verify the GLM License Provision configuration:

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

If the master webhook is executed successfully, the following GLM configuration is displayed:

```
Host ID         : 5DCB01EC264BECCCFECB3C2ED42E02384EE8C527
USB ID          : Not Available
Billing Serials: A10f771cecbe0000
Token           : A10f771cecbe
Product         : ADC
Platform        : vThunder
Burst           : Disabled
GLM Ping Interval In Hours : 24
-----------------------------------------------------------------
Enabled Licenses Expiry Date (UTC)            Notes
-----------------------------------------------------------------
SLB              None
CGN              None
GSLB             None
RC               None
DAF              None
WAF              None
AAM              None
FP               None
WEBROOT          N/A         Requires an additional Webroot license.
THREATSTOP       N/A         Requires an additional ThreatSTOP license.
QOSMOS           N/A         Requires an additional QOSMOS license.
WEBROOT_TI       N/A         Requires an additional Webroot Threat Intel
license.
CYLANCE          N/A         Requires an additional Cylance license.
IPSEC_VPN        N/A         Requires an additional IPsec VPN license.
500 Mbps Bandwidth 14-November-2022
```

3. From vThunder Console, navigate to **Home** > **License History** to verify your license:

Figure 177 : License History

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

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

If the SSL Certificate configuration is correct and applied successfully, the following SSL configuration is displayed:

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

Verify Traffic Flow

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

1. From **Azure Portal** > **Azure services** > **Resource Group** > <*resource_group_name*> > <*load_balancer*> > **Settings** > **Frontend IP configuration**.
   Here, **`vth-lb`** is the load balancer.
2. Copy the Load balancer frontend IP address.

   Figure 178 : Load balancer frontend IP address

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

```
curl <vth-lb-frontend-ip>
```

Example

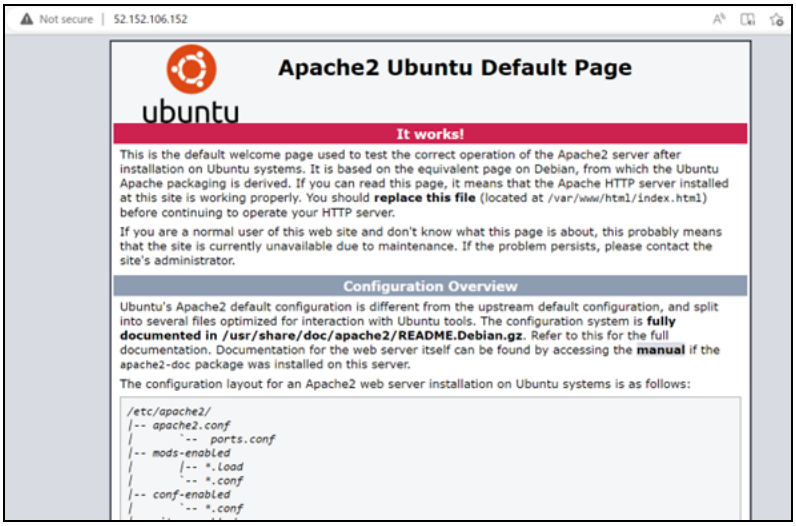
```
curl 20.64.87.85
```

Verify if a response is received.

or

Copy the load balancer frontend IP address in the browser.

Figure 179 : API response



Verify if the API response is received.

ADC Configuration Templates

This section guides you in applying new Application Delivery Controller (ADC) configurations on Thunder using PowerShell scripts. These PowerShell scripts make Thunder aXAPI calls over the HTTPS protocol.

PowerShell is required to execute the PowerShell script. For more information, see Prerequisites.

Table 8 provides an overview of the different supported Thunder configurations. These configurations are optional. You can choose to apply them based on your specific use cases. For more information, see Deployment Templates.

Table 8 : Supported Thunder configurations

Configuration	Description
Change Password	Applies a new vThunder instance password. **NOTE:** After the deployment of vThunder instance, it is highly recommended to change the default password for `admin` user.
Basic Server Load Balancer	Applies an SLB configuration for inbound traffic, outbound traffic, policies, server grouping, and routing to destination virtual servers.
Server Load Balancer on Backend Autoscale	Applies an SLB configuration automatically whenever backend app/web servers

Table 8 : Supported Thunder configurations

Configuration	Description
	are autoscaled. When the backend web/app servers are in a Virtual Machine Scale Set (VMSS) group within the Azure cloud, autoscale-in or autoscale-out of server triggers a defined webhook for SLB configuration, applying or removing virtual server configuration in Thunder.
A10 License	Applies an A10 license to the vThunder instance. **NOTE:** A10 Thunder is proprietary software that requires either a trial or BYOL (Bring Your Own License) subscription. However, pre-licensed subscription-based images from the Azure Marketplace do not require this configuration.
SSL Certificate	Applies a server connection certificate configuration. An SSL certificate is a digital certificate that authenticates a website's

Table 8 : Supported Thunder configurations

Configuration	Description
	identity and enables an encrypted connection. SSL stands for Secure Sockets Layer, a security protocol that creates an encrypted link between a web server and a web browser. Applies server connection certificate configurations. A Secure Sockets Layer (SSL) certificate is a digital certificate that verifies a website's identity and facilitates an encrypted connection. SSL is a security protocol that establishes an encrypted link between a web server and a web browser.
High Availability	Applies a high availability configuration. These configurations automatically synchronize Thunder configurations between the active and standby Thunder instances. In the event of a failover, it designates the other Thunder instance as active to ensure uninterrupted traffic routing. For this functionality, it is essential for both Thunder instances

Table 8 : Supported Thunder configurations

Configuration	Description
	to have identical resources and configurations.
Hybrid Cloud GSLB	Applies a disaster recovery configuration using a global server load balancer across any two regions or locations, whether same cloud, hybrid-cloud or on-premise. It requires a minimum of two Thunder instances in each region or location —one acting as the master controller and the other as a site device. Multiple site devices can be configured but it is recommended to have minimum of three site devices for seamless failover and effective disaster recovery. For a configuration with three Thunders instances, the recommended setup includes one as the master controller and the other two as a site device. Ensure that both regions have identical set of resources. To create and install three thunder instances in one

Table 8 : Supported Thunder configurations

Configuration	Description
	region use Thunder-3NIC-3VM template. Same template can be used to install in another region.

Change Password

After provisioning the vThunder instance, you can change the vThunder instance password at any given time.

NOTE: It is highly recommended to change the default password. For default password, see Support Information.

To change the password of the deployed vThunder instance, perform the following steps:

1. Download **A10-vThunder_ADC-CONFIGURATION** > **CHANGE-PASSWORD** template from GitHub.
2. From Start menu, open PowerShell and navigate to this downloaded folder to run the following command:

   ```
   PS C:\Users\TestUser\A10-vThunder_ADC-CONFIGURATION\CHANGE-PASSWORD>
   .\CHANGE_PASSWORD_SETUP.ps1
   ```

   A message is prompted displaying the primary conditions for password validation:

   ```
   Primary conditions for password validation, user should provide the
   new password according to the given combination:

   Minimum length of 9 characters
   Minimum lowercase character should be 1
   Minimum uppercase character should be 1
   Minimum number should be 1
   Minimum special character should be 1
   Should not include repeated characters
   Should not include more than 3 keyboard consecutive characters.
   ```

3. Provide the vThunder instance's Host/IP, username, current and new password when prompted:

```
Enter thunder host/ip: x.x.x.x
Enter thunder username: admin
Enter thunder current password x.x.x.x: ***
Enter thunder new password: *********
Confirm new password: *********
```

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

4. If the password is changed successfully, the following message is displayed:

```
Password successfully changed for x.x.x.x
Password change configurations saved on partition: shared
```

5. Enter 'N' to exit the change password process.

```
Do you want to continue?,(Y/N):N
```

Basic Server Load Balancer

This template configures vThunder instance as a Server Load Balancer (SLB) to evenly distribute the traffic across the a set of predefined servers and requires manual scaling.

To configure vThunder as an SLB, perform the following steps:

1. Download **A10-vThunder_ADC-CONFIGURATION** > **BASIC-SLB** template from GitHub.
2. From Start menu, open PowerShell and navigate to this downloaded folder and open the SLB_CONFIG_PARAM.json with a text editor.

NOTE: Each parameter has a default value mentioned in the parameter file which can be modified as required.

3. Configure the following parameters:

Table 9 : JSON Parameters

Resource Name	Description
vThunder instance username	Specify a 'Read/Write/HM' privilege username. `"vThUsername": "admin",` **NOTE:** The vThunder instance user should have 'Read/Write/HM' privilege to configure vThunder as an SLB.
Data Interface Count	Specify the number of data NICs. The value should be 1 for 2 NICs and 2 for 3 NICs. `"dataInterfaceCount": 2,`
Host IP addresses	Specify the Public IP address of one or more vThunder instance/s depending on the deployed template.

Table 9 : JSON Parameters

Resource Name	Description

	<pre>"hostIPAddress": {
	"vThunderIP": [
	"<vThunder1_Public_IP>",
	"<vThunder2_Public_IP>"
	]
	},</pre>

Template HTTP	Specify the value as 1 if you want to configure the HTTP template. For more information on SLB HTTP template, see *Command Line Interface Reference*. <pre>"templateHTTP": 0,</pre>**NOTE:** By default, the template HTTP value is 0.
Template Persist Cookie	Specify the value as 1 if you want to configure the Persist-Cookie template. For more information on SLB persist cookie template, see *Command Line Interface Reference*. <pre>"templatePersistCookie": 0,</pre>**NOTE:** By default, the template Persist-Cookie value is 0.
SLB server host or domain	Specify name and host IP address or domain name of one or more SLB servers. The SLB server host value is the datain 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.

Table 9 : JSON Parameters

Resource Name	Description
	"slbServerHostOrDomain": { "value": [{ "server-name": "s1", "host": "10.0.3.5", "metadata": { "description": "SLB server host/fqdn-name for. To use domain name replace host with fqdn-name and ip address with domain name" } }, { "server-name": "s2", "host": "10.0.3.7", "metadata": { "description": "SLB server host/fqdn-name for. To use domain name replace host with fqdn-name and ip address with domain name" } }] },
SLB server ports	Specify the SLB Server ports details.

Table 9 : JSON Parameters

Resource Name	Description

	<pre>"slbServerPortList": {
	  "value": [
	  {
	  "port-number": 53,
	  "protocol": "udp",
	  "health-check-disable":0
	  },
	  {
	  "port-number": 80,
	  "protocol": "tcp",
	  "health-check-disable":0
	  },
	  {
	  "port-number": 443,
	  "protocol": "tcp",
	  "health-check-disable":0
	  }
	  ]
	},</pre>
	NOTE: For 3NICs, the **`health-check-disable`** value is recommended to be 1.

Service Group List	Specify the SLB Service group.

Table 9 : JSON Parameters

Resource Name	Description

Table 9 : JSON Parameters

Resource Name	Description

HTTP Template	Specify the HTTP template details if **templateHTTP = 1**.
	`"httpList": {`
	`"value": [`
	`{`
	`"name":"<host-switching-template-name>",`
	`"host-switching": [`
	`{`
	`"host-switching-type":"contains",`
	`"host-match-string":"s1",`
	`"host-service-group":"sg80"`
	`}`
	`]`
	`},`
	`{`
	`"name":"<url-switching-template-name>",`
	`"url-switching": [`
	`{`
	`"url-switching-type":"regex-match",`
	`"url-match-string":"s1",`
	`"url-service-group":"sg80"`
	`}`
	`]`
	`}`
	`]`
	`},`

Persist Cookie Template	Specify the Persist Cookies template details if **templatePersistCookie = 1**.

Table 9 : JSON Parameters

Resource Name	Description

	<pre>"cookieList": {
	  "value": [
	  {
	  "encrypt-level": 0,
	  "expire": 60,
	  "match-type": 1,
	  "name": "persist-cookie-template-name",
	  "cookie-name": "cookie-template-name",
	  "service-group": 1
	  }
	  ]
	},</pre>

Virtual Server	Specify virtual server details. The virtual server default name is “vip”. **NOTE:** The vip address is generated dynamically after deploying the ARM template. Therefore, its default value under virtualServerList should be replaced, see Get VIP address If you want to configure an HTTP template (**templateHTTP = 1**), provide the HTTP template name in the **template-http** parameter. If you want to configure a Persist-Cookie template (**templatePersistCookie = 1**), provide the Persist-Cookie template name in the **template-persist-cookie** parameter.

Table 9 : JSON Parameters

Resource Name	Description

	"virtualServerList": {
	"virtual-server-name": "vip",
	"ip-address": "10.0.2.5",
	"metadata": {
	"description": "specify ethernet 1 primary private ip address in case of 2nic's or ethernet1 secondary private ip address in case of 3nic's"
	},
	"value": [
	{
	"port-number":53,
	"protocol":"udp",
	"ha-conn-mirror":0,
	"auto":1,
	"service-group":"sg53"
	},
	{
	"port-number":80,
	"protocol":"http",
	"auto":1,
	"service-group":"sg80",
	"template-http":"<host-switching-template-name or url-switching-template-name>",
	"template-persist-cookie":"<persist-cookie-template-name>"
	},
	{
	"port-number":443,
	"protocol":"https",
	"auto":1,
	"service-group":"sg443"
	}
	]

Table 9 : JSON Parameters

Resource Name	Description
	NOTE: Either `host-switching-template-name` or `url-switching-template-name` can be used in the `template-http`. For 3NICs, the `ha-conn-mirror` value is recommended to be 1. The `ha-conn-mirror` does not work on ports 80 and 443.

Get VIP address

To get the vip address after deploying the vThunder instances, perform the following steps:

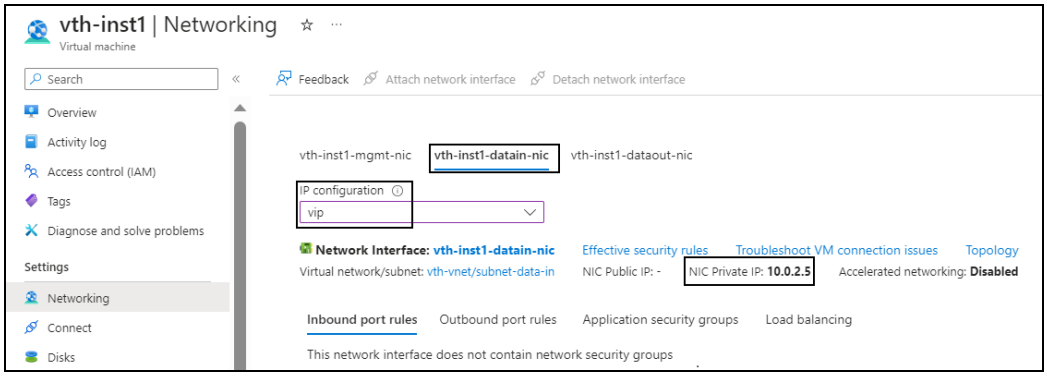
a. From **Home**, navigate to **Azure services** > **Resource Group** > <*resource_group_name*>.

b. Go to the first vThunder instance. Here, the first vThunder instance is `vth-inst1`.

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

d. Select the Datain NIC tab > **IP configuration** > `vip`. Here, Datain NIC is `vth-inst1-datain-nic`.

Figure 180 : Virtual machine - Networking window - Datain NIC 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"
          },
```

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

4. Verify if all the configurations in the SLB_CONFIG_PARAM.json file are correct and save the changes.
5. Run the following command to configure the vThunder instance/s as an SLB:

```
PS C:\Users\TestUser\A10-vThunder_ADC-CONFIGURATION\BASIC-SLB> .\SLB_
CONFIG.ps1
```

6. Provide password for the vThunder instances/s whose IP address is mentioned in the SLB_CONFIG_PARAM.json file.
   If SLB is configured successfully for 2NIC-1VM, the following message is displayed:

```
Enter Password for x.x.x.x : *********
Configuring vthunder
configured ethernet- 1 ip
Configured server s1
Configured service group
Slb Http Template Created.
Slb Persist Cookie Template Created.
0
Configured virtual server
Configurations are saved on partition:  shared
Configured vThunder Instance  1
Session ID closed for x.x.x.x.
----------------------------------------------------------------------
```

The above configuration has one server, an HTTP template, and a Persist-Cookie template configured for 2NIC-1VM.

If SLB is configured successfully for 3NIC-2VM, the following message is displayed:

```
Enter Password for x.x.x.x : *********
Configuring vthunder
configured ethernet- 1 ip
configured ethernet- 2 ip
Configured server s1
Configured server s2
Configured service group
Slb Http Template Created.
Slb Persist Cookie Template Created.
0
Configured virtual server
Configurations are saved on partition:  shared
Configured vThunder Instance  1
Session ID closed for x.x.x.x.
-----------------------------------------------------------------
Enter Password for x.x.x.x : *********
Configuring vthunder
configured ethernet- 1 ip
configured ethernet- 2 ip
Configured server s1
Configured server s2
Configured service group
Slb Http Template Created.
Slb Persist Cookie Template Created.
0
Configured virtual server
Configurations are saved on partition:  shared
Configured vThunder Instance  2
Session ID closed for x.x.x.x.
-----------------------------------------------------------------
```

The above configuration has two servers, an HTTP template, and a Persist-Cookie template configured for 3NIC-2VM.

7. In case of only basic SLB configuration without High availability, run the following commands on both the Thunder instances:

```
vth-inst1#config
vth-inst1(config)# ip route 0.0.0.0 /0 10.0.2.1
vth-inst1(config)# write memory
Building configuration...
Write configuration to default primary startup-config
[OK]
vth-inst1(config)#
```

Server Load Balancer on Backend Autoscale

This template configures vThunder instance as a Server Load Balancer (SLB) to automate the scaling process allowing dynamic adjustment of servers based on the workload.

To configure vThunder as an SLB on Backend Autoscale, perform the following steps:

1. Create Automation Account

To create the automation account, perform the following steps:

a. Create an Automation Account

b. Verify the Automation Account creation

a. Create an Automation Account

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

To configure the parameters, perform the following steps:

1. Download **A10-vThunder_ADC-CONFIGURATION** > **CONFIG-SLB_ON_BACKEND-AUTOSCALE** template from GitHub.
2. From Start menu, open PowerShell and navigate to this downloaded folder and open the CREATE_AUTOMATION_ACCOUNT_PARAM.json with a text editor.

NOTE:	Each parameter has a default value mentioned in the parameter file which can be modified as required.

3. Configure the following parameters:

Table 10 : JSON Parameters

Resource Name	Description
Automation Account	Specify the automation

Table 10 : JSON Parameters

Resource Name	Description
	account name. 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",`
Location	Specify the location. `"location": "South Central US",`

Table 10 : JSON Parameters

Resource Name	Description

Client Secret	Specify the client secret, application ID, and tenant ID.
	
	To get these values, go to **Home** > **Azure services** > **Azure Active Directory** > **App Registration** > **Owned applications** > <*application_name*>.
	
	`"clientSecret": "9-xxx~jIxxxEVyxxxxHNxxxOwv_xxxxZLxxxTM",`
	`"appId": "10724xxx-xxx-xxxx-xxxx-xxxx2c14726d",`
	`"tenantId": "91d27xxx-xxxx-xxxx-xxxx-xxxxf81fcb2f",`

Application ID	
Tenant ID	
VMSS	Specify the server VMSS name. `"vmssName": "vth-server-vmss",`

Management Interfaces	Specify a unique network interface card for management traffic.
	
	`"mgmtInterface1": "vth-inst1-mgmt-nic",`
	`"mgmtInterface2": "vth-inst2-mgmt-nic",`

vThunder instances	Specify the virtual machine names.

Table 10 : JSON Parameters

Resource Name	Description
	`"vThunderName1": "vth-inst1",` `"vThunderName2": "vth-inst2",`
Resource Group	Specify the resource group where virtual machine scale set having vThunder servers and resources created by the ARM template are available. `"resourceGroupName": "vth-rg1",`
Virtual Resource Group	Specify the name of an existing resource group under which the virtual network is already created. `"vnetresourceGroupName" : "<existing virtual network resource group name>",`
vThunder Username	Specify a 'Read/Write/HM' privilege username. `"vThUsername": "admin",`
Port List	Specify port details.

Table 10 : JSON Parameters

Resource Name	Description

	<pre>"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
	}
	]
	}</pre>

4. Verify if all the configurations in the CREATE_AUTOMATION_ACCOUNT_PARAM.json file are correct and then save the changes.
5. Run the following command to create an automation account:

```
PS C:\Users\TestUser\Templates> .\CREATE_AUTOMATION_ACCOUNT_1.ps1
```

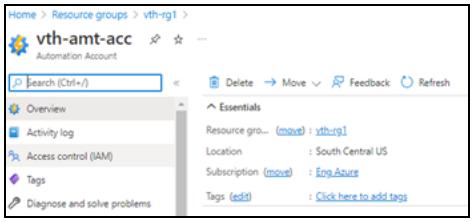
b. Verify the Automation Account creation

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

1. From **Home**, navigate to **Azure services** > **Resource Group** > *<resource_group_name>*.
   The selected resource group - Overview window is displayed.

2. Under **Resources** tab, group the resources based on the resource type.
3. Verify if the recently created automation account is listed under **Automation Accounts** type.
4. Select the recently created automation account.
   The selected automation account - Overview window is displayed.

   Figure 181 : Selected automation account - Overview window



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

   Figure 182 : Selected automation account - Variables window

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

2. Change Password

First-time Password Change

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

1. From Start menu, open PowerShell and navigate to **A10-vThunder_ADC-CONFIGURATION** > **CONFIG-SLB_ON_BACKEND-AUTOSCALE** template.
2. Run the following command to change the password:

```
PS C:\Users\TestUser\Templates> .\CHANGE_PASSWORD_2.ps1
```

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

3. Provide the default and new password when prompted:

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

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

4. Go to **Azure services** > **Resource Group** > *<vmss_resource_group_name>* > *<automation_account>* > **Variables**.
5. Verify if the timestamp in the **Last modified** column of the **vThPassword** variable is updated.

Figure 183 : Updated Variables window

Subsequent Password Change

To change the Backend Autoscale vThunder password subsequently, perform the following steps:

1. Go to **Azure services** > **Resource Group** > *<vmss_resource_group_name>* > *<automation_account>* > **Variables**.
2. Update the password in the **vThPassword** variable manually and save the changes.
   The password gets encrypted.

3. Configure SLB

To configure vThunder as an SLB on-demand, perform the following steps:

1. From Start menu, open PowerShell and navigate to **A10-vThunder_ADC-CONFIGURATION** > **CONFIG-SLB_ON_BACKEND-AUTOSCALE** template.
2. Open the SLB_CONFIG_ONDEMAND_PARAM.json with a text editor.

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

3. Configure the following parameters:

Table 11 : JSON Parameters

Resource Name	Description
Service Group List	Specify the service group details. `"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 } ] },`

Table 11 : JSON Parameters

Resource Name	Description
Virtual Server	Specify the virtual server details. The virtual server default name is “vip”. The vip address is generated dynamically after deploying the vThunder instances. Thereafter, its default value under **`virtualServerList`** should be replaced, see Get VIP address .

Table 11 : JSON Parameters

Resource Name	Description

	"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"
	}
	]
	}

Get VIP address

To get the vip address after deploying the vThunder instances, perform the

following steps:

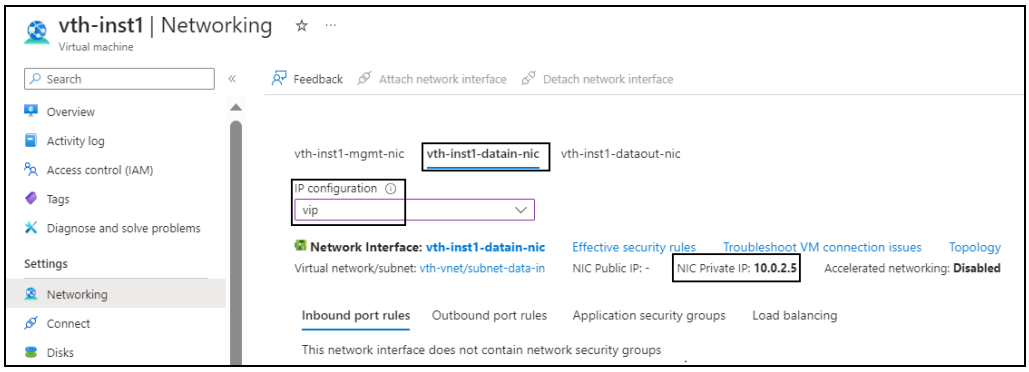
a. From **Home**, navigate to **Azure services** > **Resource Group** > *<resource_group_name>*.

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

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

d. Select the Datain NIC tab > **IP configuration** > **`vip`**.
Here, Datain NIC is **`vth-inst1-datain-nic`**.

Figure 184 : Virtual machine - Networking window - Datain NIC 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"
          },
```

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

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

5. Run the following command to configure vThunder instance as an SLB:

```
PS C:\Users\TestUser\A10-vThunder_ADC-CONFIGURATION\BASIC-SLB> .\SLB_
CONFIG_ONDEMAND_3.ps1
```

6. Provide the correct vThunder instance password when prompted:

```
Enter New Password:*********
```

7. If the SLB is configured successfully, the following message is displayed:

```
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
```

8. In case of only basic SLB configuration without High availability, run the following commands on both the Thunder instances:

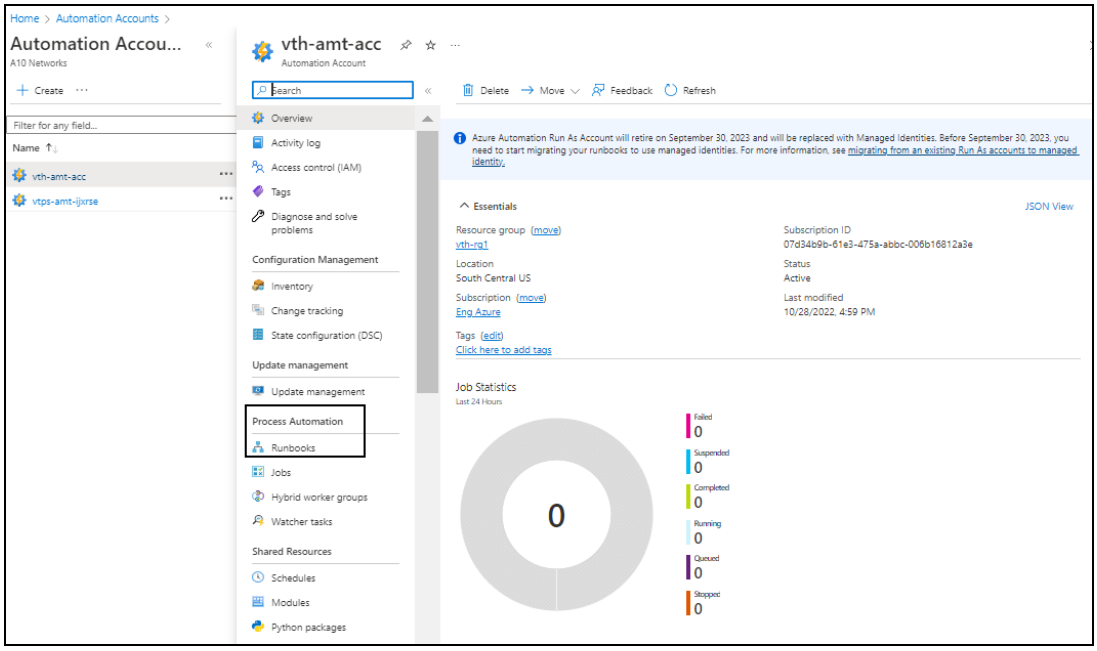
```
vth-inst1#config
vth-inst1(config)# ip route 0.0.0.0 /0 10.0.2.1
vth-inst1(config)# write memory
Building configuration...
Write configuration to default primary startup-config
[OK]
vth-inst1(config)#
```

4. Create Runbook

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

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

   Figure 185 : Selected automation account window

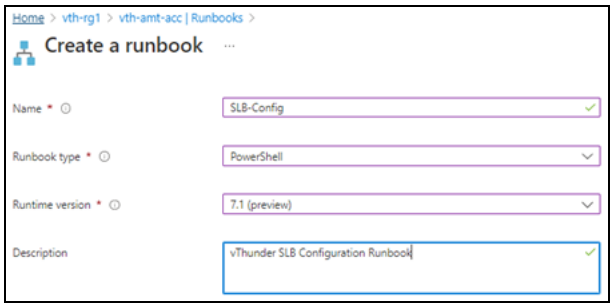


2. Select **Runbooks** from left **Process Automation** panel.
   The <*automation_account_name*> - Runbooks window is displayed.

Figure 186 : Selected automation account - Runbooks window

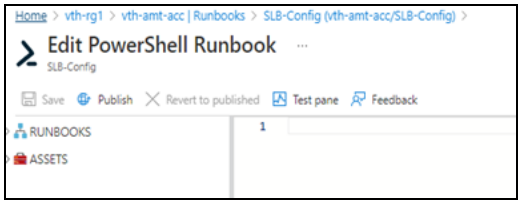
3. Click **Create a runbook**.
   The **Create a runbook** window is displayed.

   Figure 187 : 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 188 : Edit PowerShell Runbook window



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

6. From Start menu, open PowerShell and navigate to **A10-vThunder_ADC-CONFIGURATION** > **CONFIG-SLB_ON_BACKEND-AUTOSCALE** template.

7. Open **SLB_SERVER_RUNBOOK.ps1** with a text editor and copy the entire content of the runbook.
8. Paste this content in the right panel of the **Edit PowerShell Runbook** window.
9. Click **Save** and then click **Publish**.
   The runbook gets created for the selected automation account.

5. Create Automation Account Webhook

The following topics are covered:

a. Initial Setup

b. Create a Webhook

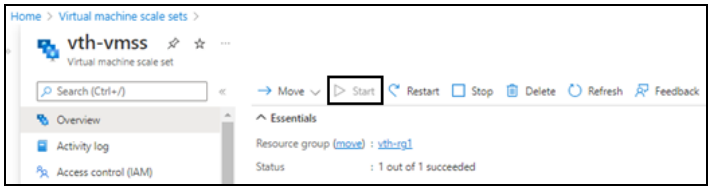
c. Verify the Runbook Job creation

a. Initial Setup

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

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

Figure 189 : VMSS window



b. 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 ARM template.

2. Run the following command to create the webhook:

```
PS C:\Users\TestUser\Templates> .\CREATE_WEBHOOK_4.ps1 -runBookName
"<runbook_name>"
```

Example:

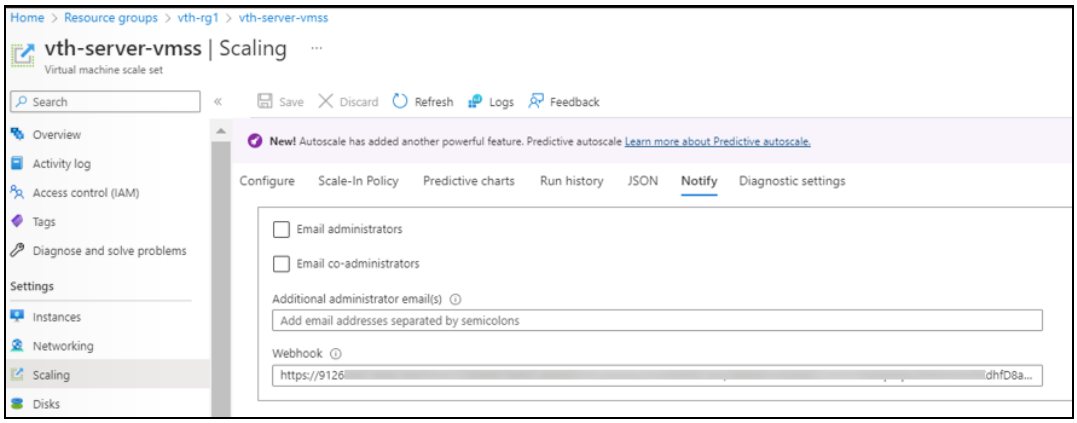
```
PS C:\Users\TestUser\Templates> .\CREATE_WEBHOOK_4.ps1 -runBookName
"SLB-Config"
```

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

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

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

   Figure 190 : VMSS-Scaling - Notify tab



6. Select **Notify** tab.
7. Copy the saved webhook url and paste it in the **Webhook** field.

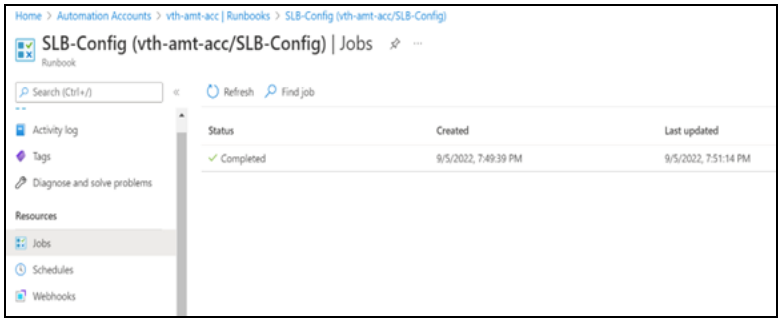
8. Click **Save** to save the changes.

c. Verify the Runbook Job creation

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

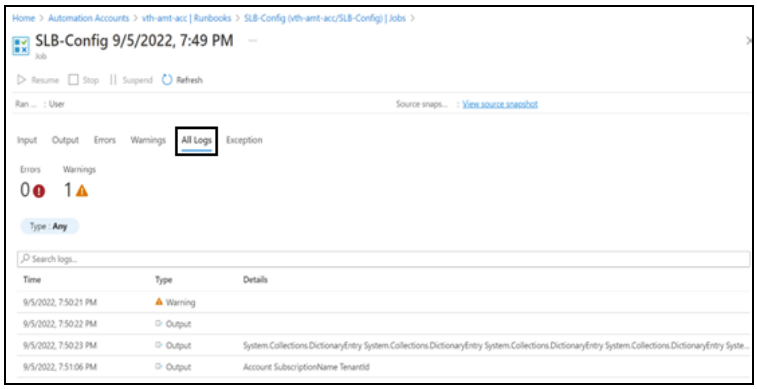
1. From **Home**, navigate to **Azure services** > **Automation Accounts** > <automation_account_name>.
   The selected automation account - Overview window is displayed.
2. Click **Jobs** from the left **Process Automation** panel.
   The selected automation account - Jobs window is displayed. Here,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

   Figure 191 : 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 192 : Selected runbook job window



SSL Certificate

This template applies Certificate Authority SSL Certificate to the vThunder instance. This certificate establishes an encrypted link between a server and your browser, ensuring that all data transferred between them remains private and secure.

To configure SSL certificate for a vThunder instance, perform the following steps:

1. Download **A10-vThunder_ADC-CONFIGURATION** > **SSL-CERTIFICATE** from GitHub.
2. From Start menu, open PowerShell and navigate to this downloaded folder and open the SSL_CONFIG_PARAM.json with a text editor.

NOTE: Each parameter has a default value mentioned in the parameter file which can be modified as required.

3. Configure the following parameters:

Table 12 : JSON Parameters

Resource Name	Description
SSL Configuration	Specify SSL details. `"sslConfig": { "requestTimeOut": 40, "path": "<absolute file path of certificate file>", "file": "<certificate file name>", "certificationType": "<certificate file type>" },` **NOTE:** By default, SSL configuration is disabled i.e. no SSL configuration is applied. **Example**

Table 12 : JSON Parameters

Resource Name	Description
	The sample values for the SSL certificate are as shown below: `"sslConfig": { "requestTimeOut": 40, "Path": "C:\\.............. \\server.pem", "File": "server", "CertificationType": "pem" }`
vThunder instance/s details	Specify a 'Read/Write/HM' privilege username and the Public IP address of one or more vThunder instance/s depending on the deployed template. `"vThUsername": "admin", "hostIPAddress": { "vThunderIP": [ "<vThunder1 public IP>", "<vThunder2 public IP>" ] }`

4. Verify if the configurations in the SSL_CONFIG_PARAM.json file are correct and then save the changes.
5. Run the following command to apply SSL configuration on the vThunder instance/s:

```
PS C:\Users\TestUser\A10-vThunder_ADC-CONFIGURATION\SSL-CERTIFICATE>
.\SSL_CONFIG.ps1
```

6. Enter 'Y' to upload the SSL certificate when prompted:

```
Executing SSL-Configuration


SSL Certificate
Do you want to upload ssl certificate ?
[Y] Yes  [No] No [?] Help (default is "N"): Y
```

The certificate available at the 'sslConfig path' is uploaded.

7. Provide password for the vThunder instances/s whose IP address is mentioned in the SSL_CONFIG_PARAM.json file:

```
Enter Password for x.x.x.x : *********
```

8. If the SSL certificate is uploaded successfully, the following message is displayed:

```
SSL Configured.
Configurations are saved on partition:  shared
Session ID closed for x.x.x.x.
```

A10 License

This template applies GLM license to the vThunder instance for legal compliance, security, all feature access, and support.

To configure GLM license for vThunder instance, perform the following steps:

1. Download **A10-vThunder_ADC-CONFIGURATION** > **GLM-LICENSE** from GitHub.
2. From Start menu, open PowerShell and navigate to this downloaded folder and open the GLM_CONFIG_PARAM.json with a text editor.

NOTE: Each parameter has a default value mentioned in the parameter file which can be modified as required.

3. Configure the following parameters:

Table 13 : JSON Parameters

Resource Name	Description

Entitlement Token	Specify the entitlement token.
	`"entitlementToken": {`
	`"value": "<license entitlementToken>"`
	`},`

vThunder details	Specify a 'Read/Write/HM' privilege username and the Public IP address of one or more vThunder instance/s depending on the deployed template.

Table 13 : JSON Parameters

Resource Name	Description

	<pre>"vThUsername": {
	"value": "admin"
	},
	"dnsPrimary": {
	"value": "<dns primary address>"
	},
	"hostIPAddress": {
	"vThunderIP": [
	"<vThunder1-PublicIP>",
	"<vThunder2-PublicIP>"]
	}
	}</pre>

4. Verify if the configurations in the GLM_CONFIG_PARAM.json file are correct and then save the changes.
5. Run the following command to apply GLM license on the vThunder instance/s:

```
PS C:\Users\TestUser\A10-vThunder_ADC-CONFIGURATION\GLM-LICENSE> .\GLM_
CONFIG.ps1
```

6. Provide password for the vThunder instances/s whose IP address is mentioned in the GLM_CONFIG_PARAM.json file.

```
applying GLM license on :  x.x.x.x
Enter Password for x.x.x.x : *********
```

If the GLM license is applied successfully, a message 'BASE License successfully updated' is displayed.

High Availability

This template applies high availability configuration to the Thunder instances. It automatically synchronizes Thunder configurations between the active and standby Thunder instances. In the event of a failover, it designates the other Thunder instance as active to ensure uninterrupted traffic routing. For this functionality, it is essential for both Thunder instances to have identical resources and configurations.

High availability can be configured within same or different availability zone (cross-zone) within a same region. The cross-zone functionality is supported with ACOS 6.x.x.

Thunder instances should have the same versions; otherwise, traffic flow will be disrupted.

To configure HA for Thunder instances, perform the following steps:

1. Download **A10-vThunder_ADC-CONFIGURATION** > **HIGH-AVAILABILITY** template from GitHub.
2. From Start menu, open PowerShell and navigate to this downloaded folder and open the HA_CONFIG_PARAM.json with a text editor.

NOTE: Each parameter has a default value mentioned in the parameter file which can be modified as required.

3. Configure the following parameters:

Table 14 : JSON Parameters

Resource Name	Description
DNS	Specify a domain namespace.

Table 14 : JSON Parameters

Resource Name	Description

	<pre>"dns": {
	"value": "8.8.8.8"
	},</pre>

Network Gateway IP	Specify a Network Gateway IP.
	The default value of network gateway IP address is 10.0.2.1 as this is the first IP address of the data subnet 1 configuration.
	<pre>"rib-list": [
	{
	"ip-dest-addr":"0.0.0.0",
	"ip-mask":"/0",
	"ip-nexthop-ipv4": [
	{
	"ip-next-hop":"10.0.2.1"
	}
	]
	}
	],</pre>

VRRP-A	Specify the value as 1 to enable VRRP-A.
	<pre>"vrrp-a": {
	"set-id":1
	},</pre>

Terminal Idle Timeout	Specify the interval in minutes for closing connection when there is no input detected. The value '0' means never timeout.
	<pre>"terminal": {
	"idle-timeout":0
	},</pre>

VRID details	Specify 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

Table 14 : JSON Parameters

Resource Name	Description
	value is generated dynamically after deploying the template. Therefore, its default value under **`vrid-list`** should be replaced, see Get FIP address . `"vrid-list": [ { "vrid-val":0, "blade-parameters": { "priority": 100 }, "floating-ip": { "ip-address-cfg": [ { "ip-address":"10.0.3.6" } ] } } ],`
vThunder Host IP	Specify the Public IP address of one or more vThunder instance/s depending on the deployed template. `"hostIPAddress": { "vThunderIP": [ "<vThunder1_IP>", "<vThunder2_IP>"] },`
vThunder details	Specify a 'Read/Write/HM' privilege username, virtual IP address of vThunder instance, and primary private IP address of datain NIC of both vThunder instances.

Table 14 : JSON Parameters

Resource Name	Description
	"vThUsername": "admin", "vip": "<Datain NIC vip private address of active vThunder>", "eth1PrivateIpAddressVm1": "<Datain NIC Primary Private address of vThunder1>", "eth1PrivateIpAddressVm2": "<Datain NIC Primary Private address of vThunder2>"

Get FIP address

To get the FIP address deploying the vThunder instances, perform the following steps:

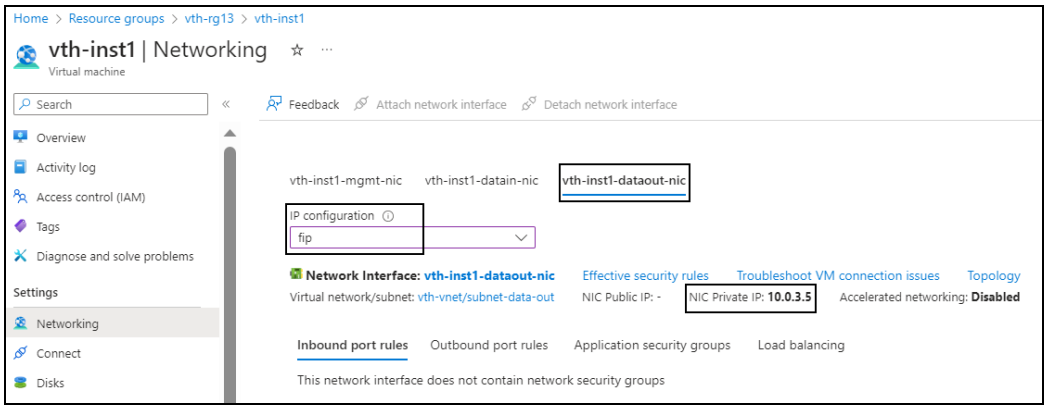
a. From the **Home**, navigate to **Azure services** > **Resource Group** > *<resource_group_name>*.

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

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

d. Select the Dataout NIC tab > **IP configuration**. Here, **`vth-inst1-dataout-nic`**.

Figure 193 : Virtual machine - Networking window - Dataout NIC 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"
                    }
                  ]
                }
            }
        ]
```

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

4. Verify if all the configurations in the HA_CONFIG_PARAM.json file are correct and save the changes.
5. Import Azure access key on both the vThunder instances. For more information, refer Import Azure Access Key File.
6. Run the following command to configure HA:

```
PS C:\Users\TestUser\A10-vThunder_ADC-CONFIGURATION\HIGH-AVAILABILITY>
.\HA_CONFIG.ps1
```

7. Provide password for the vThunder instances/s whose IP address is mentioned in the HA_CONFIG_PARAM.json file.
   If HA is configured successfully, the following message is displayed:

```
Enter Password for x.x.x.x : *********
Configured primary dns
Configured ip route
configured vrrp-a common
configured terminal timeout
1
Configured vrid
0
1
Configured peer-group
Configurations are saved on partition: shared
Configured HA on vThunder Instance 1
Session ID closed for x.x.x.x.
-----------------------------------------------------
Enter Password for x.x.x.x : ************
Configured primary dns
Configured ip route
Configured vrrp-a common
Configured terminal timeout
2
Configured vrid
0
1
Configured peer-group
Configurations are saved on partition: shared
Configured HA on vThunder Instance 2
Session ID closed for x.x.x.x.
-----------------------------------------------------
```

Hybrid Cloud GSLB

A hybrid cloud configuration as a Global Server Load balancer (GSLB) between two regions residing in same or different cloud or on-premise environments. It provides flexibility to implement disaster recovery site.

It requires atleast two Thunder instances in each region or location. One instance serves as the master controller, while the other functions as the site device. It is possible to configure multiple site devices, but it is recommended to have a minimum of three site devices to ensure seamless failover and effective disaster recovery.

Both regions should maintain an equivalent number of resources, whether hosted in the cloud or on-premise.

To create and install three thunder instances in any one region use Thunder-3NIC-3VM template. Same template can be used to install in another region.

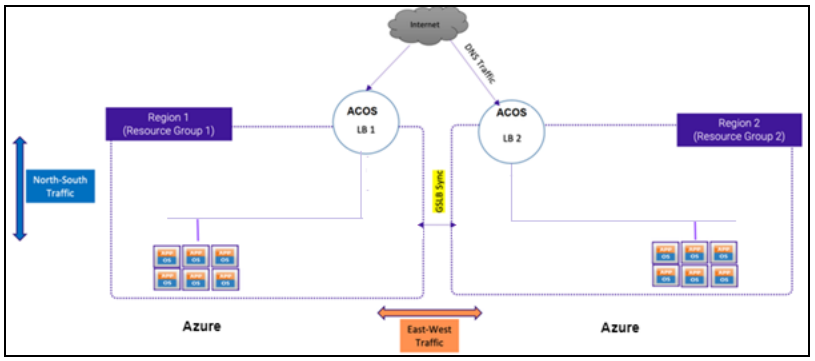
Architectural References

Refer to the following for architectural references:

- Azure-to-Azure

  Region1 and Region2 both are in Azure cloud.

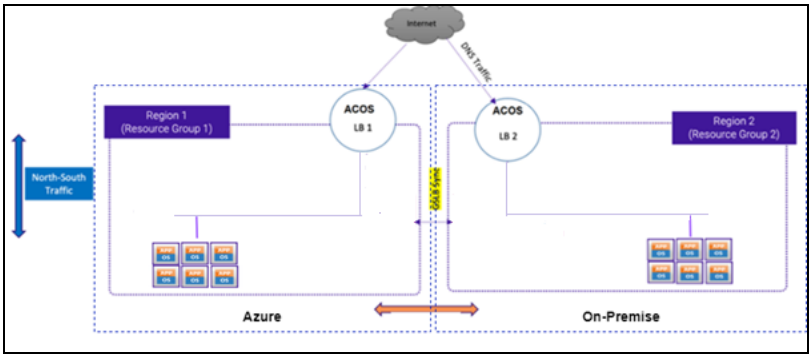
  Figure 194 : Azure-to-Azure Cloud



- Azure-to-On-Premises (any)

Region1 is in Azure cloud and Region2 is on-premise or vice versa.

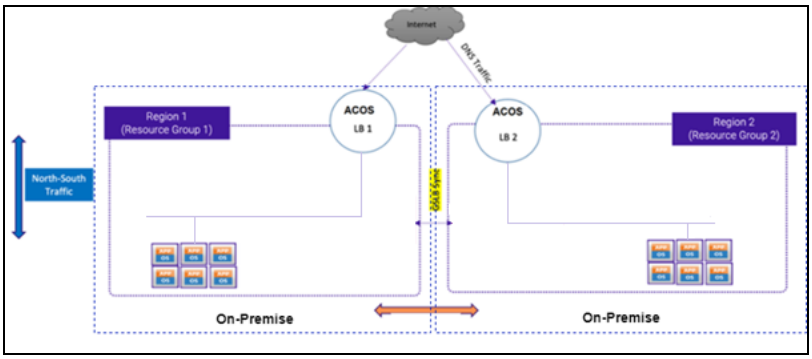
Figure 195 : Azure-to-On-Premise



- On-Premise-to-On-Premise (any)

  Region1 and Region2 are on-premises.

  Figure 196 : On-Premise-to-On-Premise



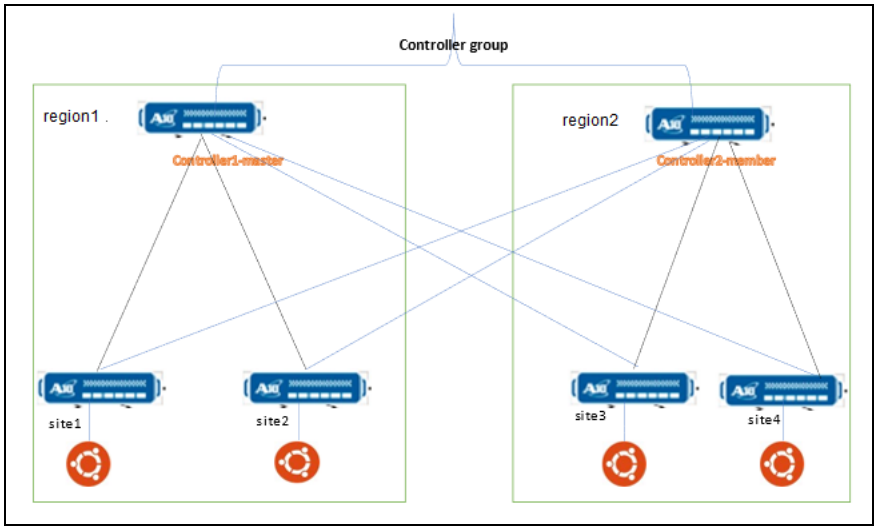
GSLB Deployment Topology

Figure 197 shows the GSLB deployment topology having two regions, Region1 and Region2. Both the regions must have identical number of resources:

- One GSLB controller
  This Thunder instance act as a DNS server that directs client to reach the active load balancer.
  GLSB controller of Region1 is considered as 'Master' and Region2 is considered as 'Member'.
- Two site devices
  These Thunder instances act as a load balancer and sends traffic to the server.

Each site device may have multiple app or web servers configured and route the traffic accordingly.

Figure 197 : Hybrid Cloud GSLB Deployment Topology



Configure Hybrid Cloud GSLB

Hybrid Cloud GSLB configuration requires two regions and each region should host three Thunder instances.

Python3 should be installed on your machine from where the scripts are executed to run the Hybrid Cloud GSLB configuration. For more information, see Install Python3.

To configure hybrid cloud GSLB, perform the following:

1. Run the following command to verify if all the PIP dependencies are installed:

```
pip3 install -r REQUIREMENTS.txt
```

2. Create three vThunder instances if not already created. For more information, see Thunder-3NIC-3VM.
3. Download **A10-vThunder_ADC-CONFIGURATION** > **HYBRID-CLOUD-GSLB** folder from GitHub.
4. From Start menu, open PowerShell and navigate to this downloaded folder and

open the HYBRID_CLOUD_CONFIG_GSLB_PARAM.json with a text editor.

NOTE: Each parameter has a default value mentioned in the parameter file which can be modified as required.

5. Configure Master Controller for Region1.

   Master Controller is the first vThunder instance in Region1 and it could be any vThunder instance.

   a. Collect Master Controller Parameter Details information.

   b. Update this information under `masterConfigDetails` section of the **//A10-vThunder_ADC-CONFIGURATION/HYBRID-CLOUD-GSLB/HYBRID_CLOUD_CONFIG_GSLB_PARAM.json** file.

6. Configure Site1 for Region1.

   Site1 is the second vThunder instance in Region1 and it could be any vThunder instance.

   a. Collect Site Details information.

   b. Update this information under `siteList1` section of the **//A10-vThunder_ADC-CONFIGURATION/HYBRID-CLOUD-GSLB/HYBRID_CLOUD_CONFIG_GSLB_PARAM.json** file.

7. Configure Site2 for Region1.

   Site2 is the third vThunder instance in Region1 and it could be any vThunder instance.

   a. Collect Site Details information.

   b. Update this information under `siteList2` section of the **//A10-vThunder_ADC-CONFIGURATION/HYBRID-CLOUD-GSLB/HYBRID_CLOUD_CONFIG_GSLB_PARAM.json** file.

8. Configure Member Controller for Region2.

   Member Controller is the first vThunder instance in Region2 and it could be any vThunder instance.

a. Collect Member Controller Parameter Details information.

b. Update this information under **`memberConfigDetails`** section of the //**A10-vThunder_ADC-CONFIGURATION/HYBRID-CLOUD-GSLB/HYBRID_CLOUD_CONFIG_GSLB_PARAM.json** file.

9. Configure Site1 for Region2.

   Site1 is the second vThunder instance in Region2 and it could be any vThunder instance.

   a. Collect Site Details information.

   b. Update this information under **`siteList3`** section of the //**A10-vThunder_ADC-CONFIGURATION/HYBRID-CLOUD-GSLB/HYBRID_CLOUD_CONFIG_GSLB_PARAM.json** file.

10. Configure Site2 for Region2.

    Site2 is the third vThunder instance in Region2 and it could be any vThunder instance.

    a. Collect Site Details information.

    b. Update this information under **`siteList4`** section of the //**A10-vThunder_ADC-CONFIGURATION/HYBRID-CLOUD-GSLB/HYBRID_CLOUD_CONFIG_GSLB_PARAM.json** file.

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

12. Run the following command to configure GSLB:

```
PS C:\Users\TestUser\A10-vThunder_ADC-CONFIGURATION\HYBRID-CLOUD-GSLB>
python HYBRID_CLOUD_CONFIG_GSLB.py
```

13. If the Hybrid cloud is configured successfully, the following message is displayed:

```
Gathering public and private ip address for site devices.
-----------------------------------------------------------
configured ethernet- 1 ip
configured ethernet- 2 ip
Configuring slb server for site: site1
Successfully Configured slb server for site: site1
Configuring service group for site: site1
Successfully Configured service group for site:site1
Successfully Configured virtual server for site: site1
Successfully Configured gslb site: site1
Successfully Configured default route:site1
Configurations are saved on partition: shared
-----------------------------------------------------------
configured ethernet- 1 ip
configured ethernet- 2 ip
Configuring slb server for site: site2
Successfully Configured slb server for site: site2
Configuring service group for site: site2
Successfully Configured service group for site:site2
Successfully Configured virtual server for site: site2
Successfully Configured gslb site: site2
Successfully Configured default route:site2
Configurations are saved on partition: shared
-----------------------------------------------------------
configured ethernet- 1 ip
configured ethernet- 2 ip
Configuring slb server for site: site3
Successfully Configured slb server for site: site3
Configuring service group for site: site3
Successfully Configured service group for site:site3
Successfully Configured virtual server for site: site3
Successfully Configured gslb site: site3
Successfully Configured default route:site3
Configurations are saved on partition: shared
-----------------------------------------------------------
configured ethernet- 1 ip
configured ethernet- 2 ip
Configuring slb server for site: site4
```

```
Successfully Configured slb server for site: site4
Configuring service group for site: site4
Successfully Configured service group for site:site4
Successfully Configured virtual server for site: site4
Successfully Configured gslb site: site4
Successfully Configured default route:site4
Configurations are saved on partition: shared
-----------------------------------------------------------
Configuring controller devices
configured ethernet- 1 ip
configured ethernet- 2 ip
Successfully Configuring gslb server for controller: masterController
Successfully Configured ServiceIp for site: masterController
Successfully Configured ServiceIp for site: masterController
Successfully Configured ServiceIp for site: masterController
Successfully Configured ServiceIp for site: masterController
Successfully Configured site information for: masterController
Successfully Configured site information for: masterController
Successfully Configured site information for: masterController
Successfully Configured site information for: masterController
Successfully Configured gslb policy for: masterController
Successfully Configured gslb zone for: masterController
Successfully Configured gslb controller and status interval:
masterController
Successfully Configured gslb controller group: masterController
Successfully Configured geo location: masterController
Successfully Configured default route:masterController
Configurations are saved on partition: shared
configured ethernet- 1 ip
configured ethernet- 2 ip
Successfully Configured gslb server for controller: memberController
Successfully Configured gslb controller group: memberController
Successfully Configured default route:memberController
Configurations are saved on partition: shared
```

Master Controller Parameter Details

Table 15 : Master Controller Parameter details

Parameter	Description	Sample value
controllerMngmtPublicIp	Public IP of Management Interface of Region1 Controller.	104.45.152.126
controllerPassword	vThunder instance Login password of Region1 Controller.	***
controllerSecPrivateIpData1	Secondary Private IP of Data Interface Subnet1 of Region1 Controller.	10.1.20.8
site1MngmtPublicIp	Public IP of Management Interface of Region1 Site1.	20.163.190.244
site1Password	vThunder instance Login password of Region1 Site1 .	***
site2MngmtPublicIp	Public IP of Management Interface of Region1 Site2.	20.85.217.94
site2Password	vThunder instance Login password of Region1 Site2 .	***
site1SecPrivateIpData1	Secondary Private IP of DataSubnet1 of Region1 Site1 vThunder.	10.1.20.9
site1SecPublicIpData1	Secondary Public IP of DataSubnet1 of Region1 Site1 vThunder.	20.163.190.244
site2SecPrivateIpData1	Secondary Private IP of DataSubnet1 of Region1 Site2 vThunder.	10.1.20.10
site2SecPublicIpData1	Secondary Public IP of DataSubnet1 of Region1 Site2 vThunder.	20.85.217.94
server1PrivateIp	Private IPv4 address of Server1 of Region1.	10.2.20.9
server2PrivateIp	Private IPv4 address of Server1	10.2.20.10

Table 15 : Master Controller Parameter details

Parameter	Description	Sample value
	of Region1.	

Member Controller Parameter Details

Table 16 : Member Controller Parameter details

Parameter	Description	Sample value
controllerMngmtPublicIp	Public IP of Management Interface of Region2 Controller.	20.124.0.232
controllerPassword	vThunder instance Login password of Region2 Controller.	***
controllerSecPrivateIpData1	Secondary Private IP of Data Interface Subnet1 of Region2 Controller.	10.1.20.14
site1MngmtPublicIp	Public IP of Management Interface of Region2 Site1.	20.163.190.244
site1Password	vThunder instance Login password of Region2 Site1 .	***
site2MngmtPublicIp	Public IP of Management Interface of Region2 Site2.	20.85.217.94
site2Password	vThunder instance Login password of Region2 Site2 .	***
site1SecPrivateIpData1	Secondary Private IP of DataSubnet1 of Region2 Site1 vThunder.	10.1.20.15
site1SecPublicIpData1	Secondary Public IP of DataSubnet1 of Region2 Site1 vThunder.	20.65.88.231
site2SecPrivateIpData1	Secondary Private IP of DataSubnet1 of Region2 Site2 vThunder.	10.1.20.16
site2SecPublicIpData1	Secondary Public IP of	20.65.95.155

Table 16 : Member Controller Parameter details

Parameter	Description	Sample value
	DataSubnet1 of Region2 Site2 vThunder.	
server1PrivateIp	Private IPv4 address of Server1 of Region2.	`10.2.20.9`
server2PrivateIp	Private IPv4 address of Server1 of Region2.	`10.2.20.10`

Site Details

Table 17 : Site details

Site Name	VIP Name	Device Name	GEO Location
eastus_1	vs1	slb1	North America, United States
eastus_2	vs2	slb2	North America, United States
eastus2_1	vs3	slb3	North America.United States.California.San Jose
eastus2_2	vs4	slb4	North America.United States.California.San Jose

IP Routes

Table 18 : IP routes

RIB List Of Region	Destination IP Address	Subnet Mask	Next Hop
Region1	0.0.0.0	/0	10.1.20.1
Region2	0.0.0.0	/0	10.1.20.1

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.

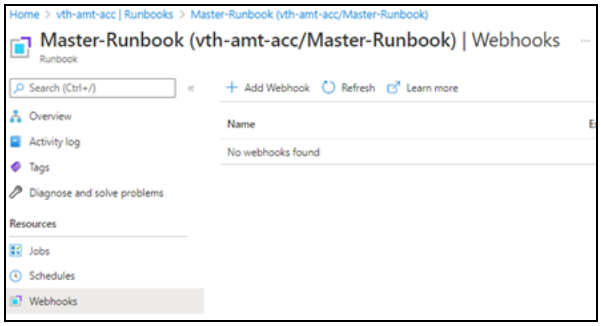
Given below is an example of the error:

```
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 198 : Master Runbook



Given below is an example of the error:

```
... -Invoke-WebRequest -Method POst -Uri $webHookURL.WebhookURI -UseBas
...
Cannot validate argument on parameter 'Uri'. The argument is null or
empty. Provide an argument that is not null or empty, and then try the
command again.
```

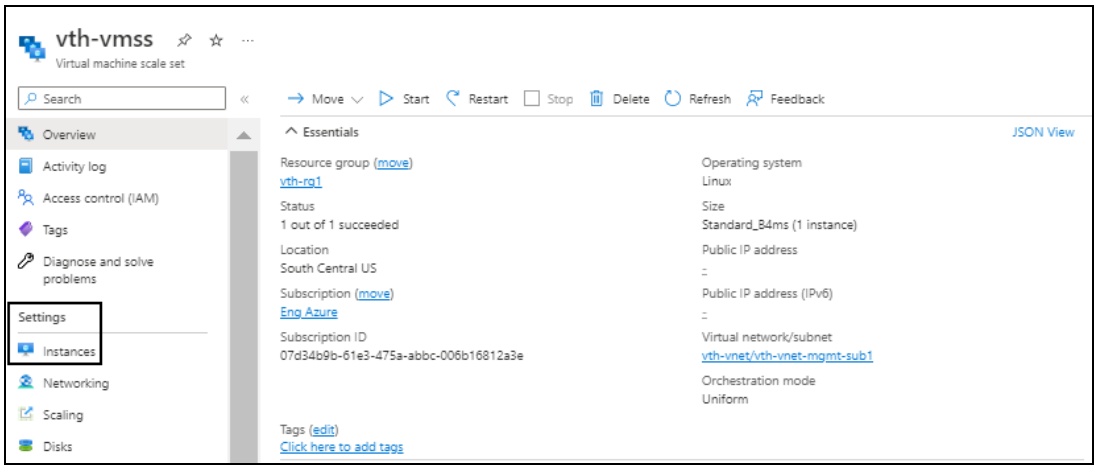
Runbook Job failed or not working

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

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

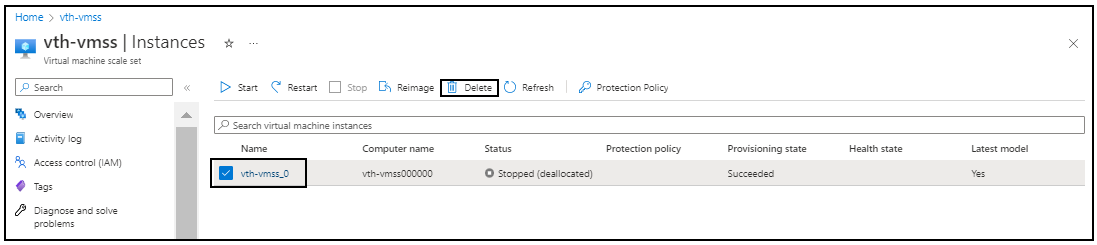
1. From **Azure Portal**, navigate to **Azure services** > **Virtual machine scale sets** > <vmss_name>.
   The selected vmss - Overview window is displayed.

   Figure 199 : Selected vmss - Overview window



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

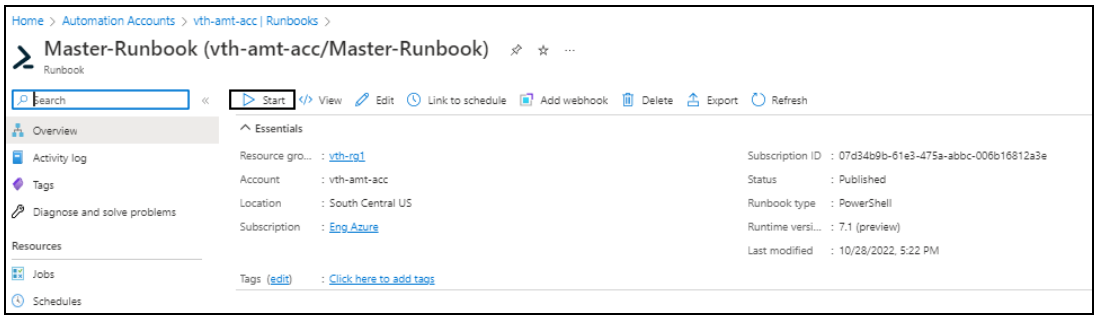
   Figure 200 : Selected vmss - Instances window



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

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

Figure 201 : 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

Azure Service Application Access Key

The Azure service application access key is required to access the Azure resources. You can either use an existing Azure service application access key or create a new key. For more information, see Create a new Azure Access Key.

To upload the Azure service application access key, perform the following:

1. Collect Azure Access Key
2. Upload the Azure Access Key
3. Import Azure Access Key File

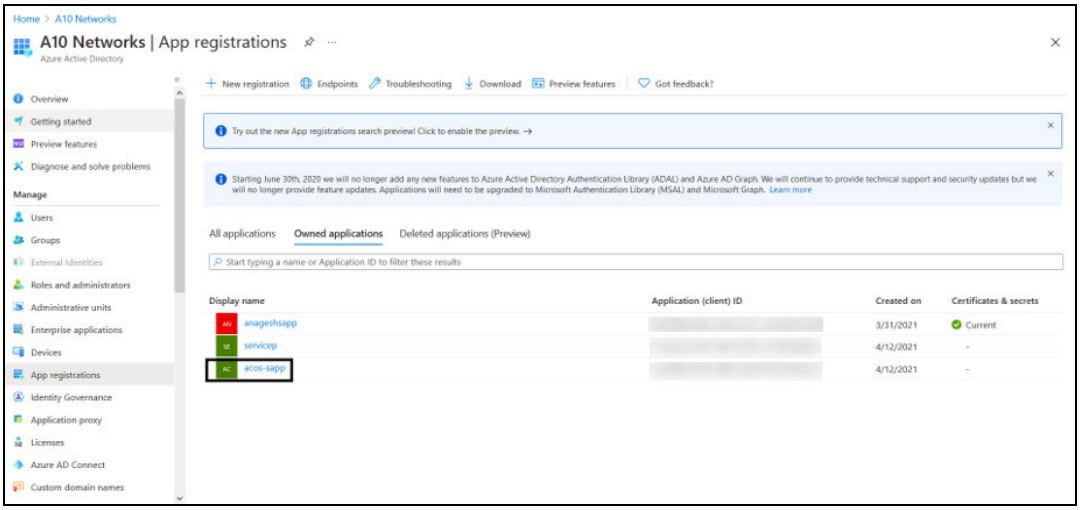
If you want to delete any existing Azure Access Key, see Delete an Azure Access Key.

Collect Azure Access Key

To collect the Azure access keys from Azure Portal, perform the following steps:

1. From **Azure Portal**, navigate to **Azure services** > **Azure Active Directory** > **App registrations**.

Figure 202 : Azure Active Directory - App registrations window



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.

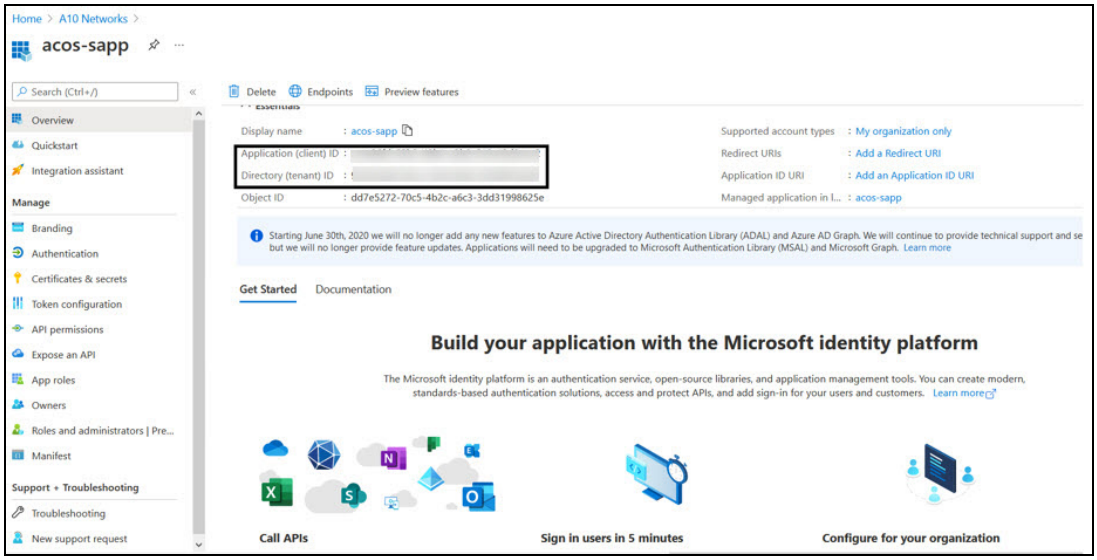
   b. Select **Add** to get a list of user accounts.

   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 203 : Selected Service application window

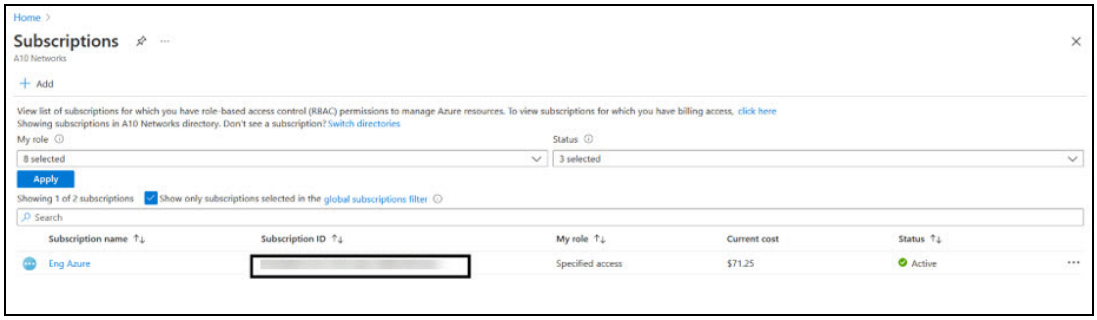


4. Copy the Client ID, Tenant ID from the service application window.

```
client_id= 'cc4c86xx-65b3-48xx-a3xx-610cxxxxxxxx'
tenant_id= '91d27axx-8cxx-41xx-82xx-3d1bxxxxxxxx'
```

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

Figure 204 : Subscriptions window



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

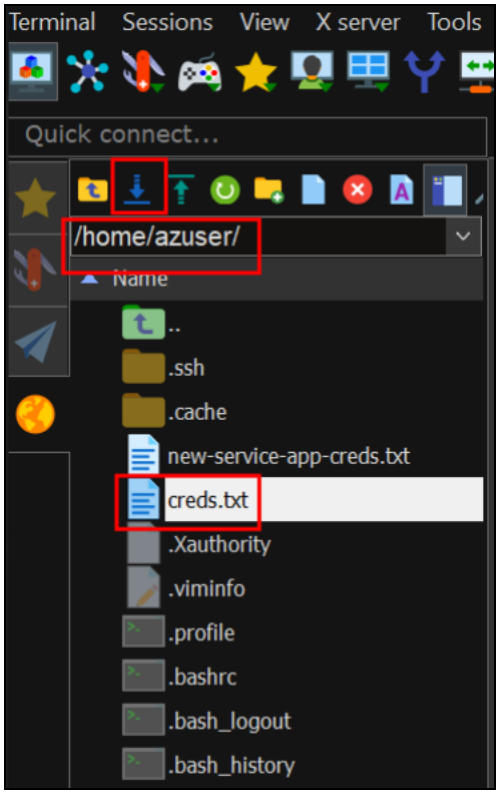
```
subscription='07d34bxx-61xx-47xx-abxx-006bxxxxxxxx'
client_id='cc4c86xx-65xx-48xx-a3xx-610cxxxxxxxx'
client_secret='G0x_hVDzZxxxx-o1Vsw.xxxx.Zxxxx-xx'
tenant_id='91d2xxxx-8xxe-41xx-82xx-3d1bxxxxxxxx'
```

7. Save this text file.

Upload the Azure Access Key

To upload the Azure access key text file to the appropriate server machine, login to the server using any FTP tool and upload them.

Figure 205 : Upload Azure access key file



Import Azure Access Key File

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 ?
  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)
```

   For example

```
vThunder-Active(config)(NOLICENSE)#admin admin
vThunder-Active(config-admin:admin)(NOLICENSE)#azure-cred import use-
mgmt-port scp://username@<ip-addr>:/<file-path>/cred.txt
```

   Here, the **username** is the server username, **ip-addr** is the Public Management IP address of the server, and **file-path** is the path where the Azure access key file is uploaded on the server.

5. Verify the imported Azure Access key file content using the following command:

```
vThunder-Active(config-admin:admin)(NOLICENSE)#azure-cred show
subscription='07d34bxx-61xx-47xx-abxx-006bxxxxxxxx'
client_id='cc4c86xx-65xx-48xx-a3xx-610cxxxxxxxx'
client_secret='G0x_hVDzZxxxx-o1Vsw.xxxx.Zxxxx-xx'
tenant_id='91d2xxxx-8xxe-41xx-82xx-3d1bxxxxxxxx'
```

Create a new Azure Access Key

To create a new Azure service application access key, perform the following steps with Administrator privileges:

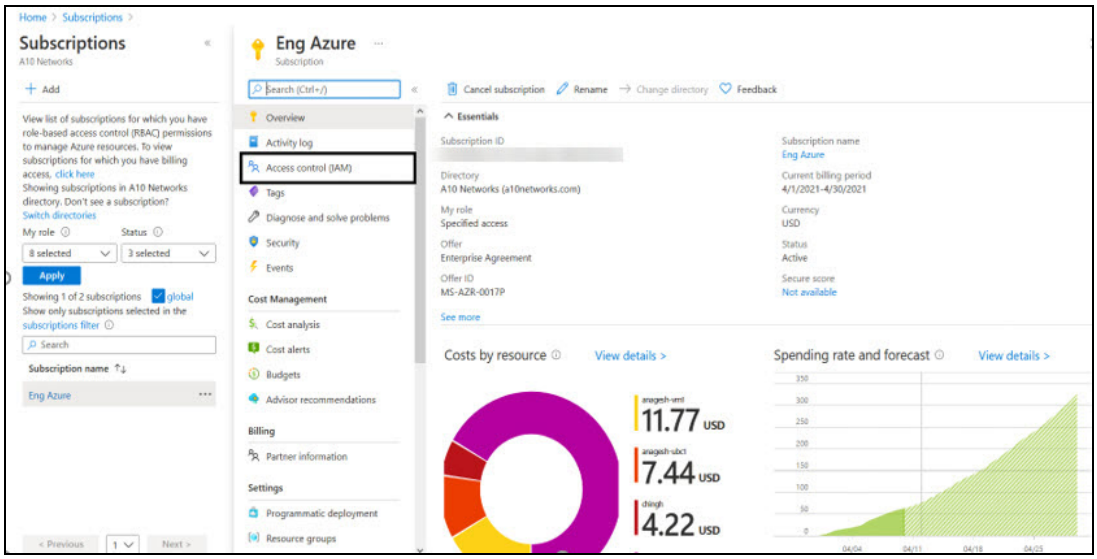
1. Create a Role
2. Register a Service Application
3. Associate Service Application with a Role
4. Create Certificate and Secrets

Create a Role

To create a custom role, perform the following steps:

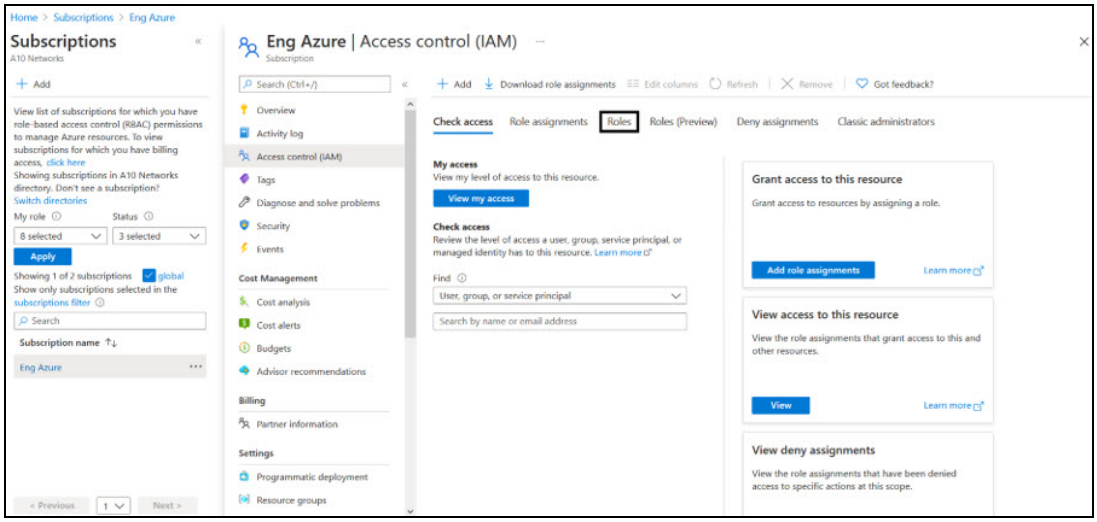
1. From **Home**, navigate to **Azure services** > **Subscriptions** > <*subscription_name*>.
   The selected Subscription - Overview window is displayed. Here, the subscription is *Eng Azure*.

   Figure 206 : Subscriptions - Overview window



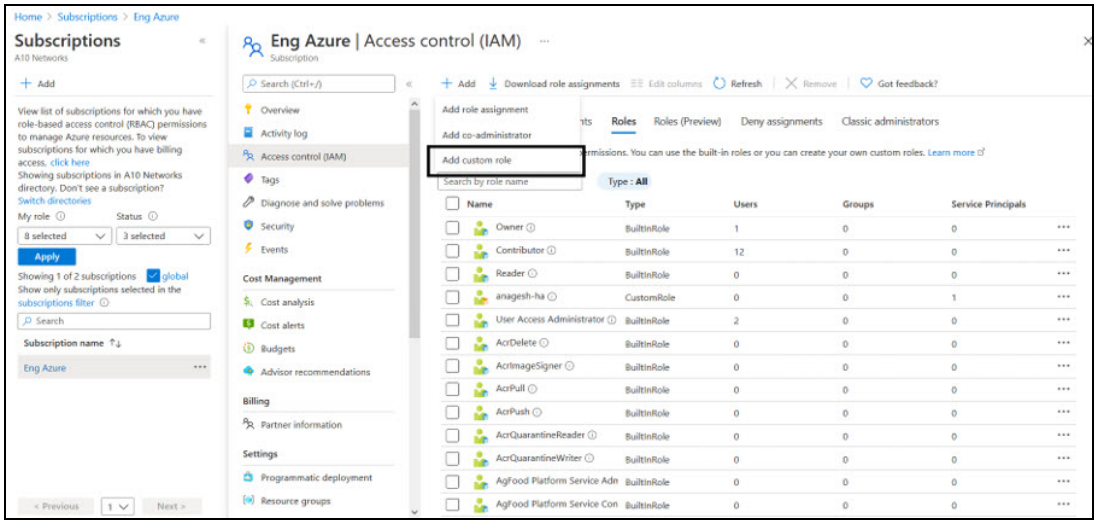
2. Click **Access control (IAM)** from left panel.
   The selected Subscription - Access control (IAM) window is displayed.
3. Select the **Roles** tab.
   The Roles window is displayed.

Figure 207 : Access Control - Role Window



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

Figure 208 : Add custom role window

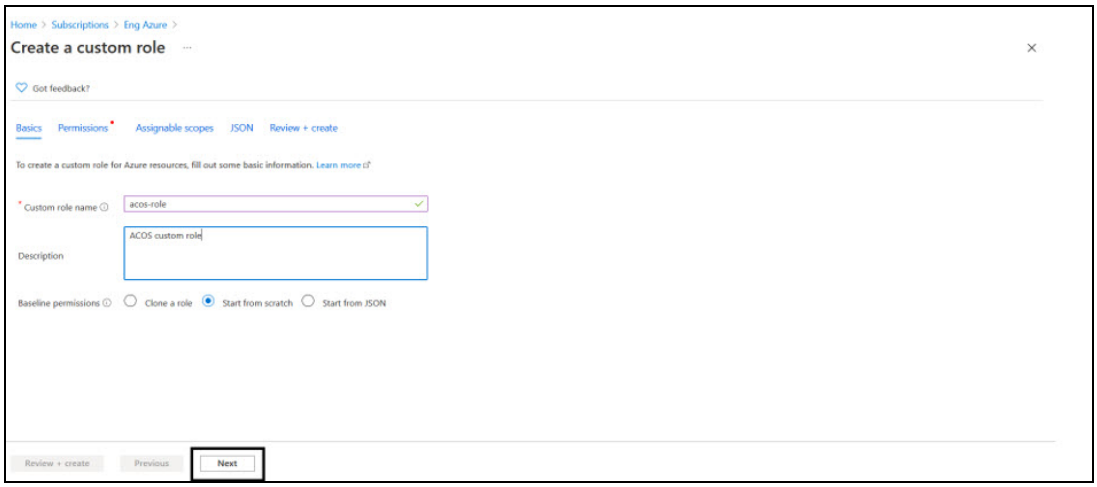


5. In the **Basics** tab, enter or select the following:

   - Customer role name
   - Description (optional)

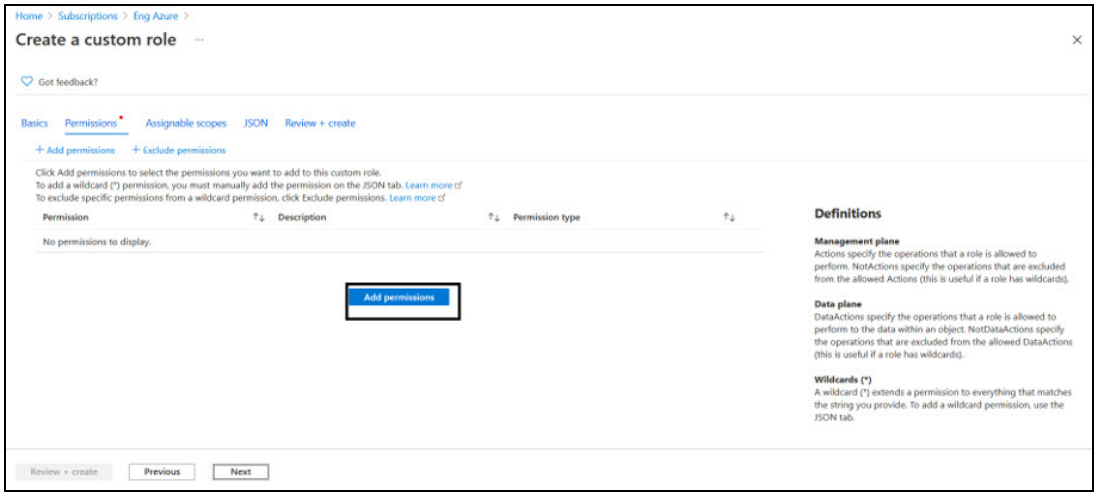
- Baseline permission

Figure 209 : Create a custom role window



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

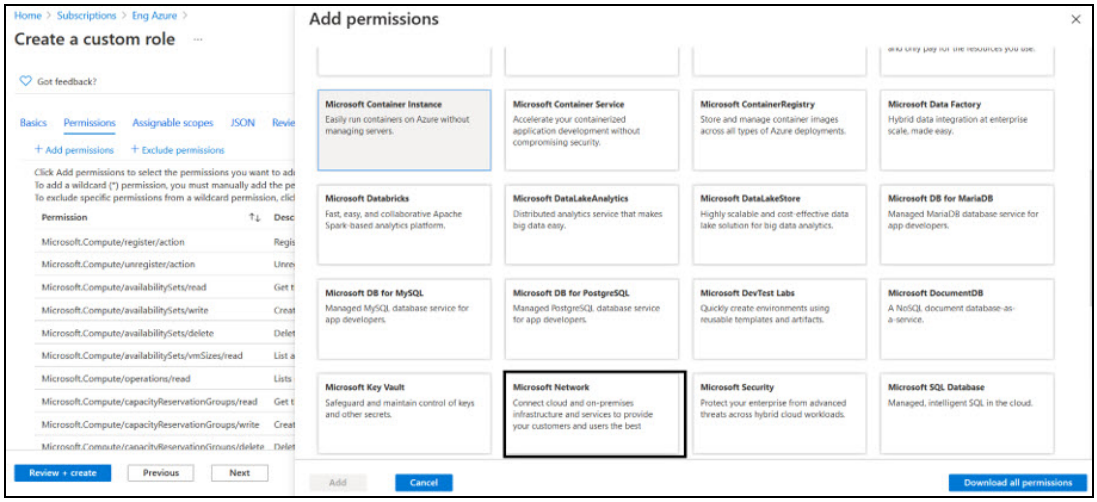
Figure 210 : Permission window



7. Click **Add Permissions** to add permissions to the custom role.

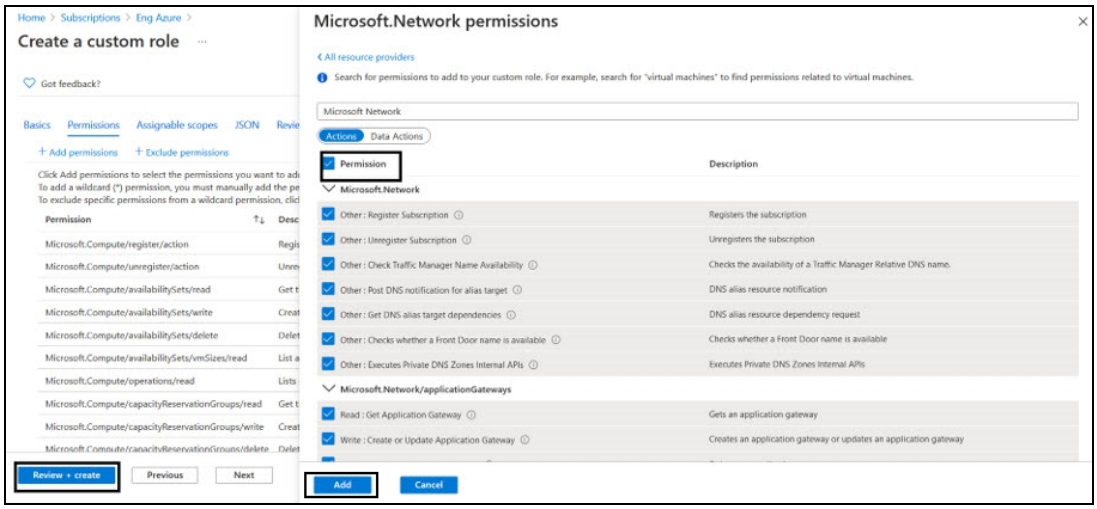
   The Add Permissions window is displayed.

Figure 211 : Add permissions window



6. Search the following permission groups in the **Add Permissions** window, select the corresponding permissions listed in the List of Custom Role Permissions, and then click **Add**:
   - Microsoft Automation
   - Microsoft Operational Insights
   - Microsoft Compute
   - Microsoft Network

Figure 212 : Microsoft Network permissions window



The selected permissions are listed under **Create a custom role** > **Permissions** tab.

8. Click **Review + create** at the bottom of the window to skip the other tabs. The **Create a custom role** confirmation window is displayed.

9. Click **OK** to successfully create the custom role with permissions.

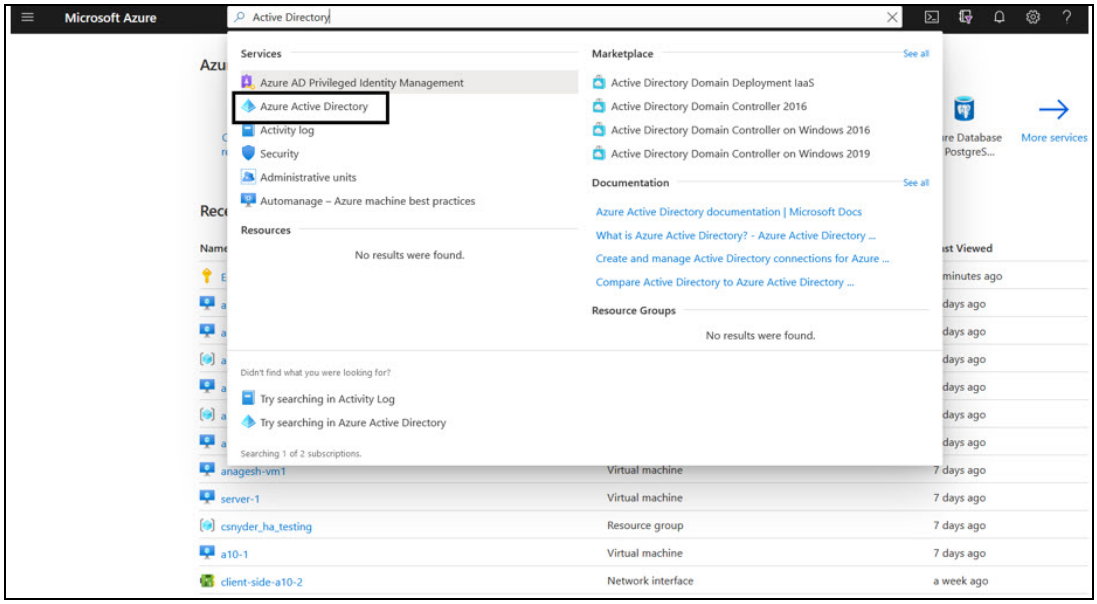
NOTE: It may take the system a few minutes to display your role everywhere.

Register a Service Application

To register a service application, perform the following steps:

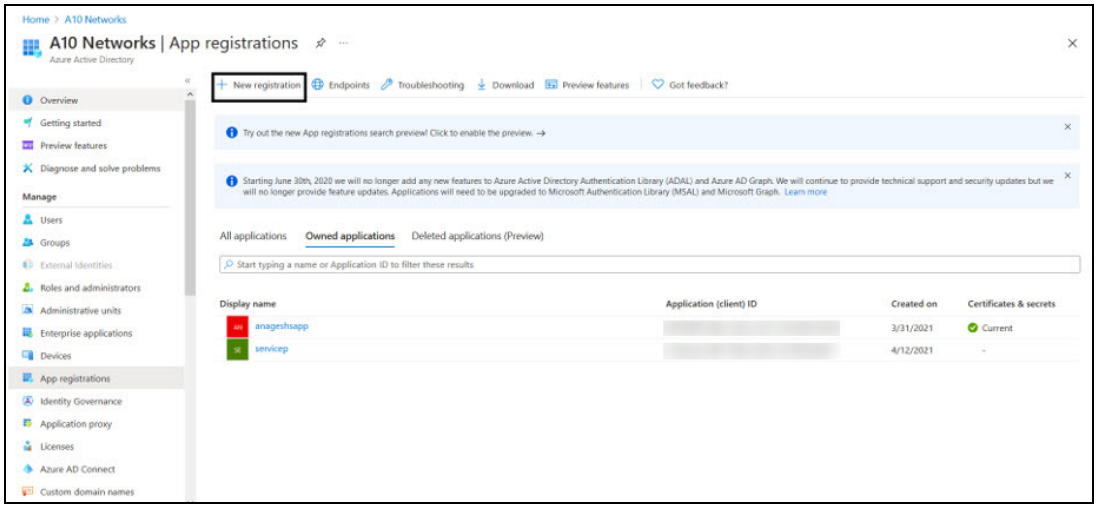
1. From **Home**, navigate to **Azure services** > **Azure Active Directory** option.

Figure 213 : Azure Active Directory window



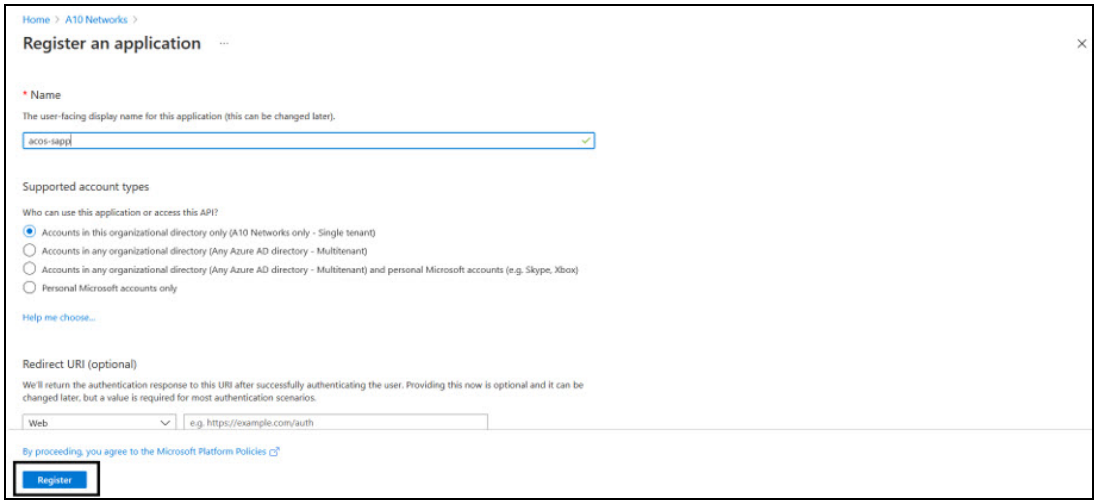
2. On the Azure Active Directory window, click **App registrations** menu option from the left **Manage** panel.
The App registration window to register an application is displayed.

Figure 214 : App registrations window



3. Click **New registration**.
The Register an application window is displayed.

Figure 215 : Register an application window



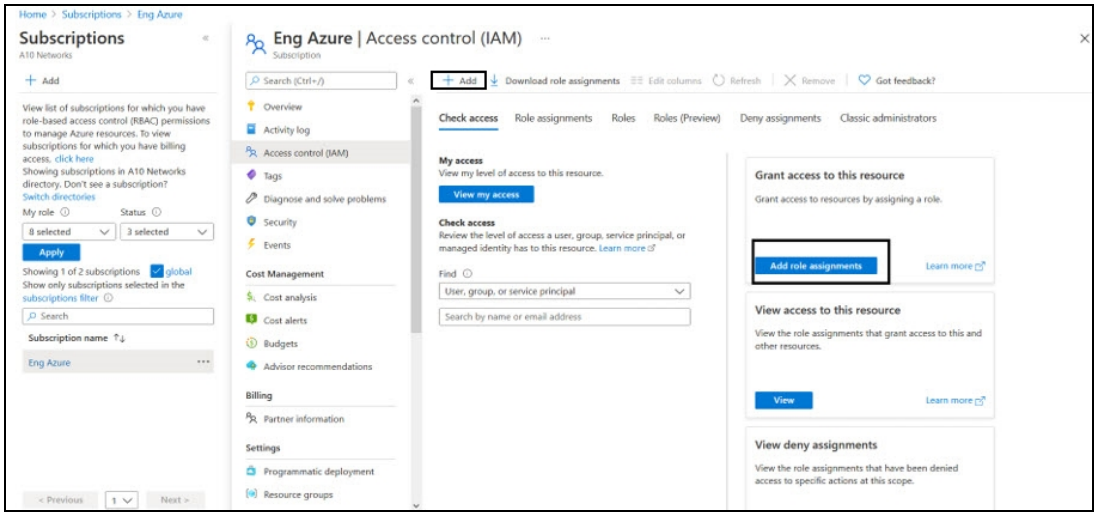
4. Enter the **Name** of the application. For example, *acos-sapp*.
5. Click **Register** to register the application. The application gets listed under Azure Active Directory - Apps registrations window.

Associate Service Application with a Role

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

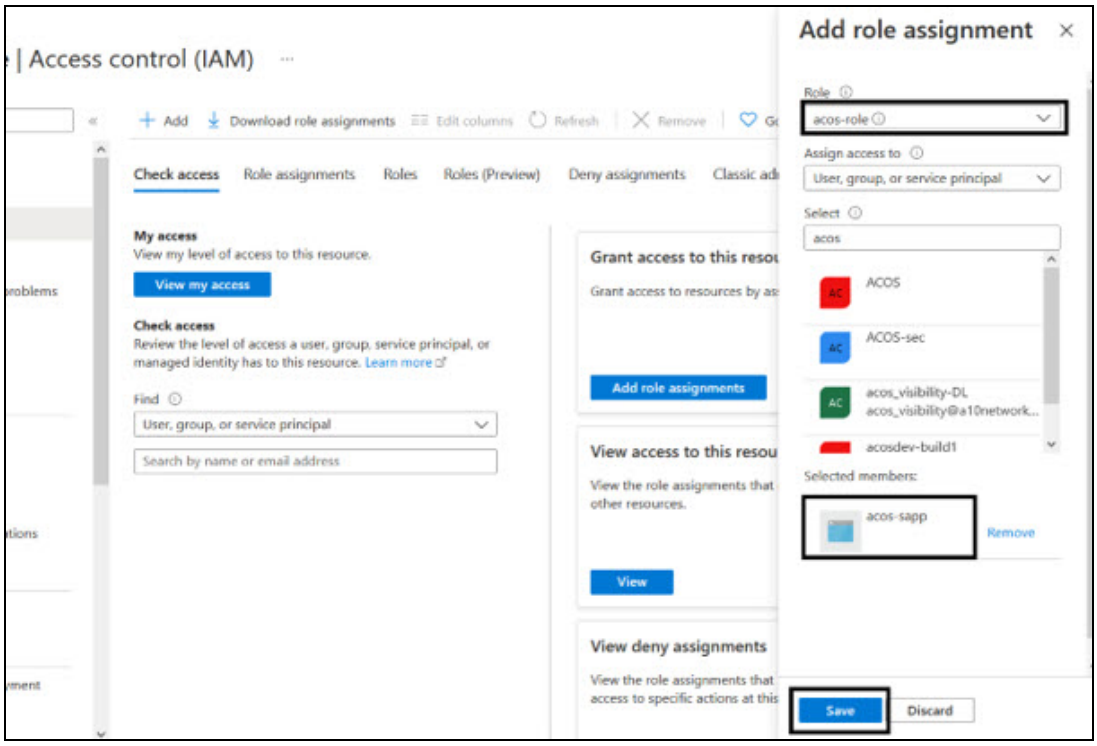
1. From **Home**, navigate to **Azure services** > **Subscriptions** > <*subscription_name*>. The selected Subscription - Overview window is displayed. Here, the subscription is Eng Azure.
2. Click **Access control (IAM)** from left panel.
   The selected Subscription - Access control (IAM) window is displayed.

Figure 216 : Subscription - Access control (IAM) window



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

Figure 217 : Add a role assignment -1



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

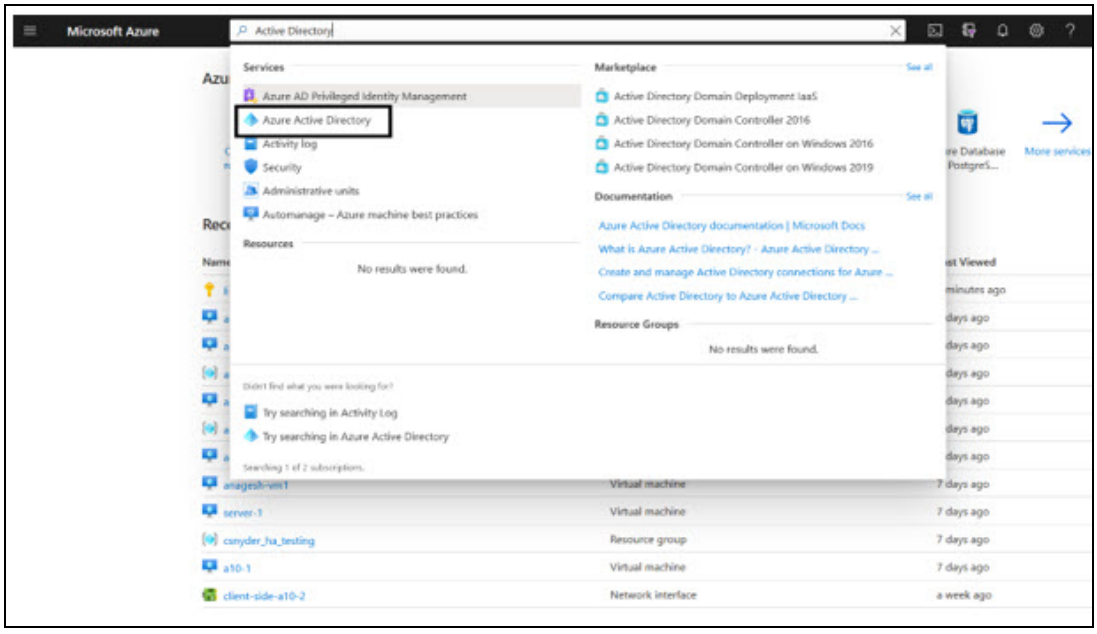
5. Select the required **Assign access to** option from the drop-down list.
6. Search and select your service application. For example, acos-sapp.
7. Click the **Save** button to save the configuration.

Create Certificate and Secrets

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

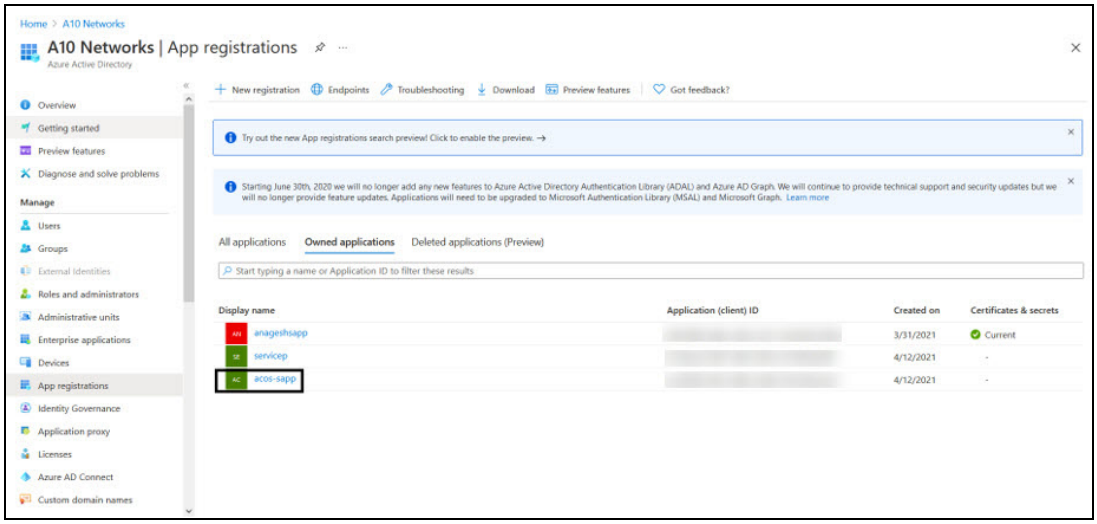
1. From **Home**, navigate to **Azure services** > **Azure Active Directory** option.

   Figure 218 : Azure Active Directory - Overview window



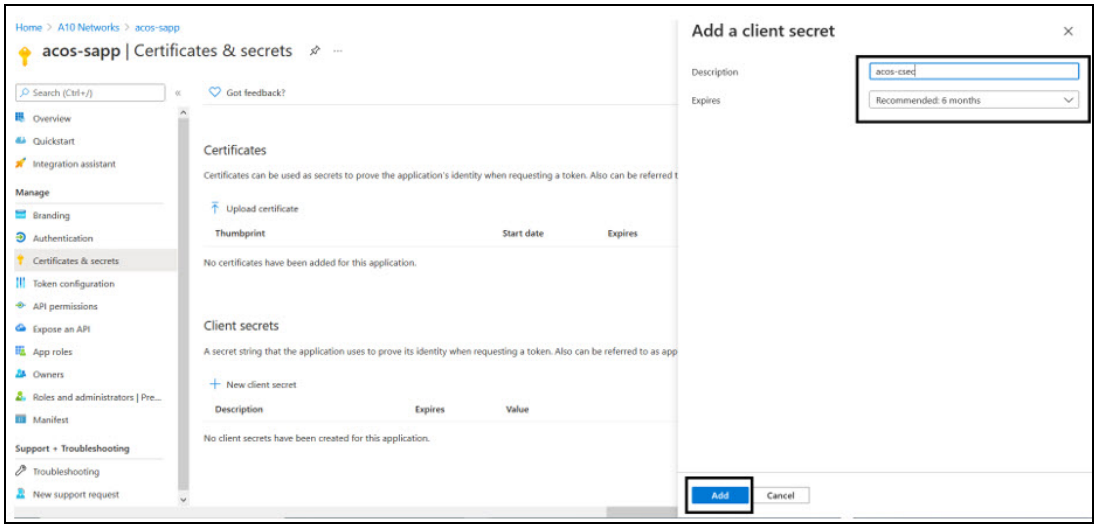
2. On the Azure Active Directory - Overview window, click **App registrations** menu option from the left panel.
   The App registration window with a registered application(s) is displayed.

Figure 219 : App registrations - Overall applications window



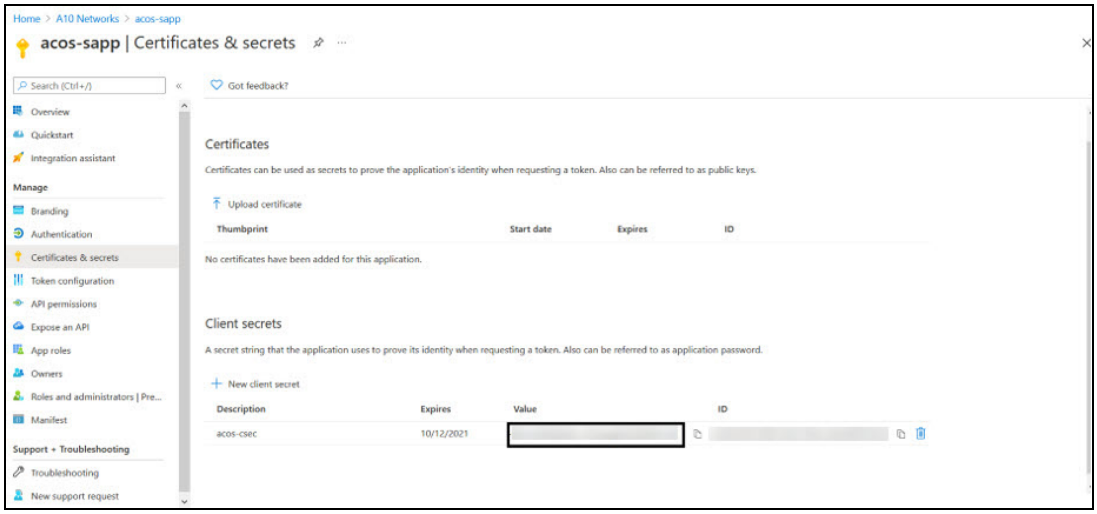
3. Select the service application from the list of applications.
   The selected service application window is displayed.
4. Select the **Certificates & secrets** option from the left Manage navigation pane.
   The <*service_application*> - Certificates & secrets window is displayed.
5. Browse and upload 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 220 : Add a client secret window



7. Enter the New client secret **Description** and **Expires** value.
   The entered value is displayed on the <*service_application*> Certificates & secrets window.

Figure 221 : 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.

Delete an Azure Access Key

To delete the Azure access key, use the following command:

```
vThunder-Active(config-admin:admin)(NOLICENSE)#azure-cred delete
```

Create VNet, Subnet, and NSG

The VNET-SUBNET-NSG template is used to create a new virtual network (VNET), three new subnets, and two new network security group (NSGs) in the specified resource group.

It is not mandatory to create new resources, the existing resources can be used in deployment and configuration.

Before deploying this template, it is recommended to review the Prerequisites.

There are two ways to deploy this template:

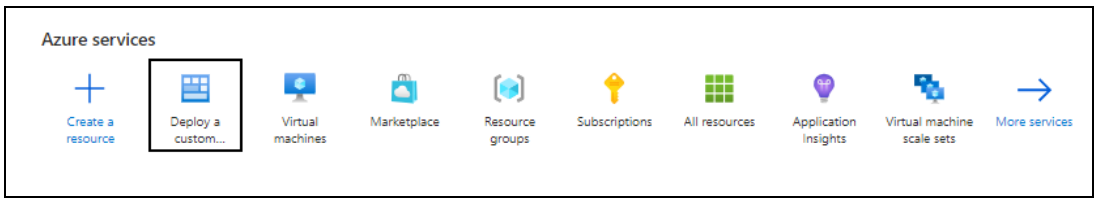
- Upload using Azure Portal Console
- Execute using Azure CLI

Upload using Azure Portal Console

To deploy the VNET-SUBNET-NSG template using Azure Portal Console, perform the following steps:

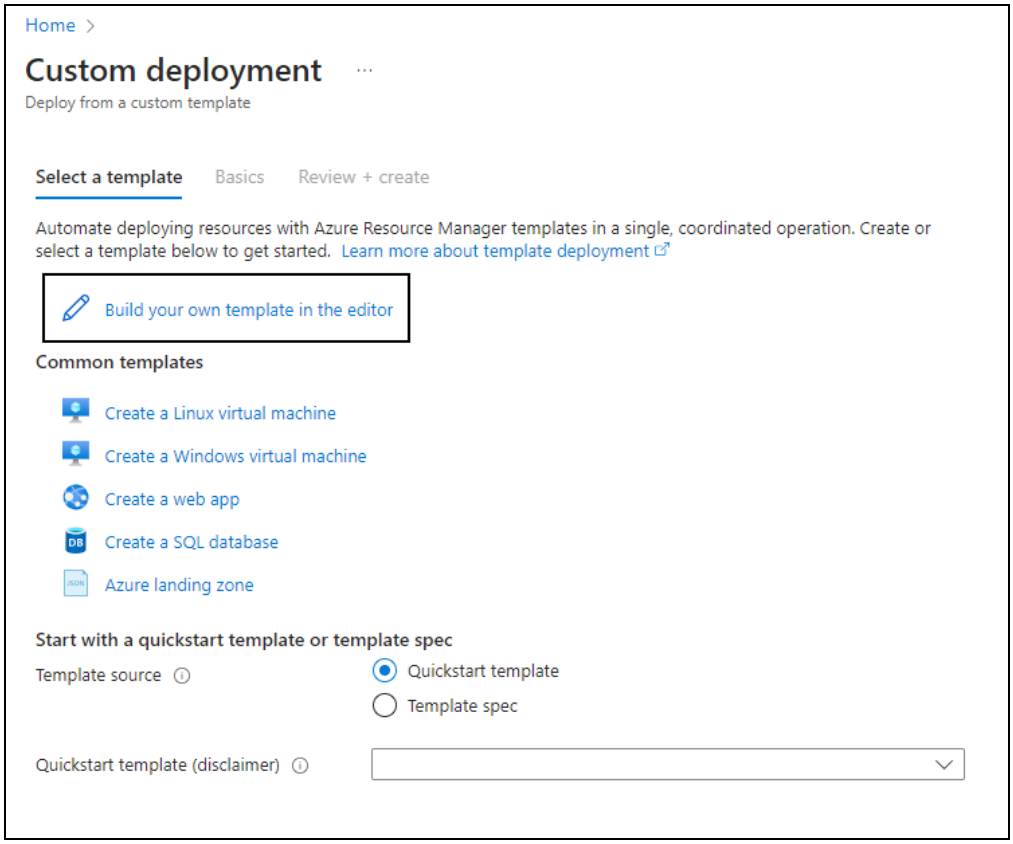
1. Download VNET-SUBNET-NSG template.
2. From the **Azure Portal** > **Azure services**, click **Deploy a custom template**.

   Figure 222 : Azure services



3. Under the **Custom deployment** window > **Select a template** tab, click **Build your own template in the editor**.

Figure 223 : Custom deployment window



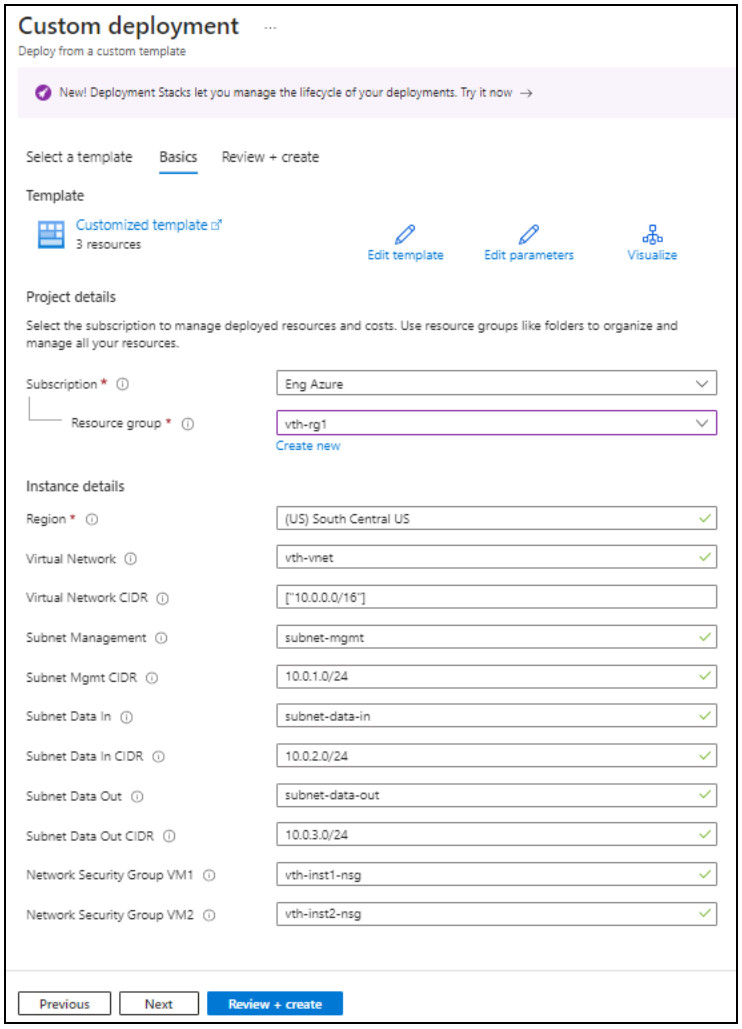
4. From the **Edit template** window, perform either of the following step:
   - Click **Load file** and browse to the folder where you have downloaded the ARM template. Select **ARM_TMPL_VNET_SUBNET_NSG.json** to upload.
   - From Windows Explorer, navigate to the folder where you have downloaded the ARM template. Copy **ARM_TMPL_VNET_SUBNET_NSG.json** content and paste it in the editor.

Figure 224 : Edit template window

5. Click **Save**.

   The **Custom deployment** window is displayed with the template parameters and default values.

Figure 225 : Custom deployment template



6. Select an existing or create a new **Resource group** under which you want to deploy the custom template resources.

NOTE: Hover ⓘ for description of each corresponding parameter.

7. Update the default values and provide the values in the empty fields as appropriate in the **Instance details** section shown in Figure 225.

8. Click **Review+create**.

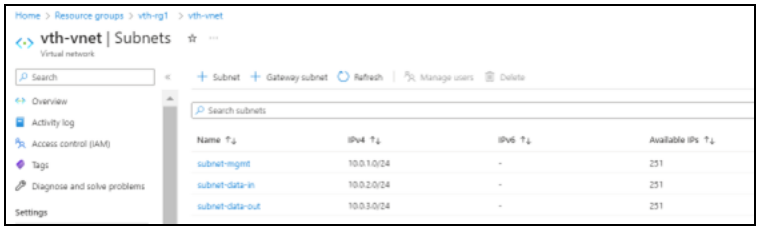
   The validation appears.

9. Click **Create**.

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

10. Verify if the Subnet resources are created under **Home** > **Azure services** > **Resource Groups** > <*resource_group_name*> > <*virtual_network_name*>.

Figure 226 : Resource listing under Virtual Network



Execute using Azure CLI

To deploy the VNET-SUBNET-NSG template using Azure CLI commands, perform the following steps:

1. Download VNET-SUBNET-NSG template.

NOTE: This template contains pre-populated default values that can be modified as required and it does not create new virtual network, network security group, subnets, and Public IP.

2. From Windows Explorer, navigate to the folder where you have downloaded the ARM template.
3. Open the ARM_TMPL_VNET_SUBNET_NSG_PARAM.json with a text editor.
4. Configure the following parameters depending upon your requirements:

Table 19 : JSON Parameters

Resource Name	Description

Virtual Network	Specify the virtual network name for virtual machines.
	`"Virtual Network": {`
	`"value": "vth-vnet"`
	`},`

Table 19 : JSON Parameters

Resource Name	Description
Virtual Network CIDR	Specify the CIDR range for the virtual network. `"Virtual Network CIDR": { "value": [ "10.0.0.0/16" ] },`
Subnets	Specify the subnet name for inbound management traffic, inbound data traffic, and outbound data traffic. `"SubnetManagement": { "value": "subnet-mgmt" }, "SubnetDataIn": { "value": "subnet-data-in" }, "SubnetDataOut": { "value": "subnet-data-out"`
Subnets CIDR	Specify the CIDR range for management, datain, and datout subnets. `"Subnet Mgmt CIDR": { "value": "10.0.1.0/24" }, "Subnet DataIn CIDR": { "value": "10.0.2.0/24" }, "Subnet DataOut CIDR": { "value": "10.0.3.0/24" },`
Network	Specify the network security group name for all the NICs.

Table 19 : JSON Parameters

Resource Name	Description

Security Groups	"Network Security Group VM1": {
	"value": "vth-inst1-nsg"
	},
	"Network Security Group VM2": {
	"value": "vth-inst2-nsg"
	}

NOTE: The Virtual Network (VNet), Subnets, Network Security Group (NSG), and Public IP Address should be deployed in the same resource group.

5. Verify if all the configurations in the ARM_TMPL_VNET_SUBNET_NSG_ PARAM.json file are correct and then save the changes.
6. From the Start menu, open PowerShell and navigate to the folder where you have downloaded the ARM template.
7. Run the following command to create an Azure resource group:

```
PS C:\Users\TestUser\Templates> az group create --name <resource_
group_name> --location "<location_name>"
```

Example:

```
PS C:\Users\TestUser\Templates> az group create --name vth-rg1 --
location "south central us"
```

```
 {
    "id": "/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/resourceGroups/vth-rg1",
    "location": "southcentralus",
    "managedBy": null,
    "name": "vth-rg1",
    "properties": {
      "provisioningState": "Succeeded"
    },
    "tags": null,
    "type": "Microsoft.Resources/resourceGroups"
  }
```

8. Run the following command to create an Azure deployment group.

```
PS C:\Users\TestUser\Templates> az deployment group create -g
<resource_group_name> --template-file <template_name> --parameters
<param_template_name>
```

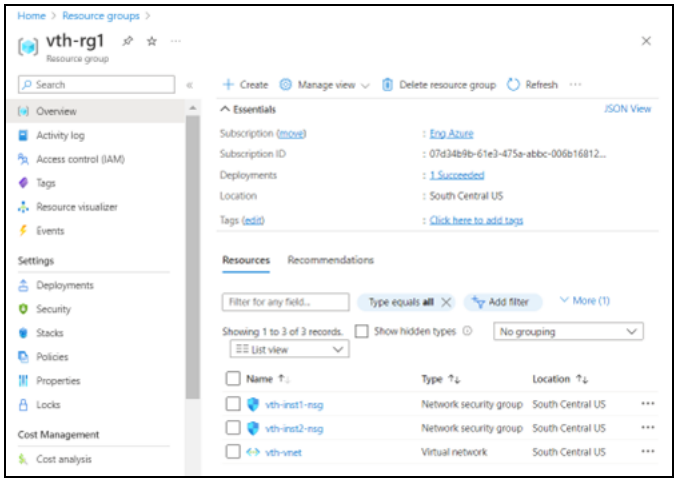
Example:

```
PS C:\Users\TestUser\Templates> az deployment group create -g vth-rg1
--template-file ARM_TMPL_VNET_SUBNET_NSG.json--parameters ARM_TMPL_
VNET_SUBNET_NSG_PARAM.json
```

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

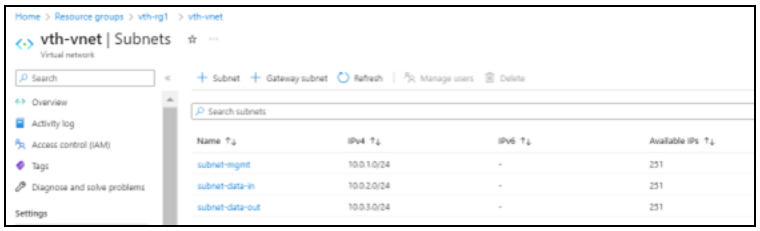
9. Verify if the VNET and NSG resources are created deploy **Home** > **Azure services** > **Resource Groups** > *<resource_group_name>*.

Figure 227 : Resource listing under Resource Group



10. Verify if the Subnet resources are created under **Home** > **Azure services** > **Resource Groups** > <*resource_group_name*> > <*virtual_network_name*>.

Figure 228 : Resource listing under Virtual Network



Create Public IP address

The PUBLIC-IP template is used to create three new Public IP addresses in the specified resource group.

It is not mandatory to create new resources, the existing resources can be used in deployment and configuration.

Before deploying this template, it is recommended to review the Prerequisites.

There are two ways to deploy this template:

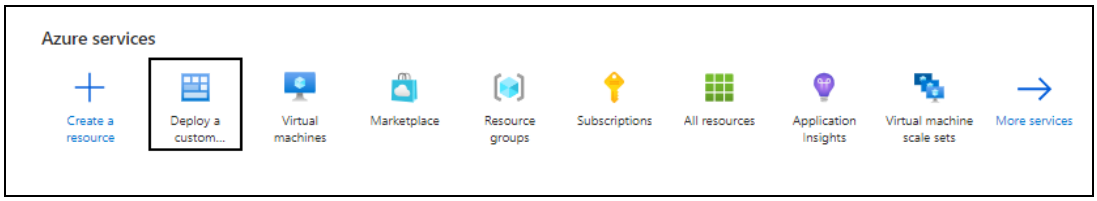
- Upload using Azure Portal Console
- Execute using Azure CLI

Upload using Azure Portal Console

To deploy the PUBLIC-IP template using Azure Portal Console, perform the following steps:

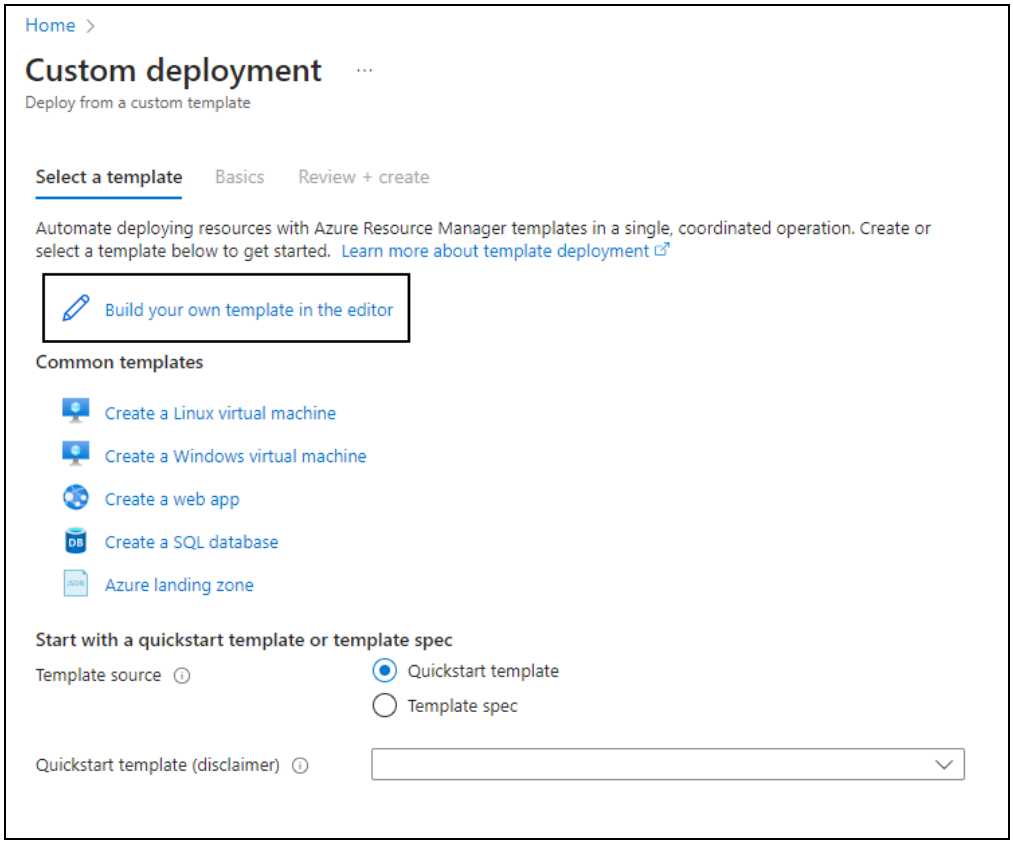
1. Download PUBLIC-IP template.
2. From the **Azure Portal** > **Azure services**, click **Deploy a custom template**.

   Figure 229 : Azure services



3. Under the **Custom deployment** window > **Select a template** tab, click **Build your own template in the editor**.

Figure 230 : Custom deployment window



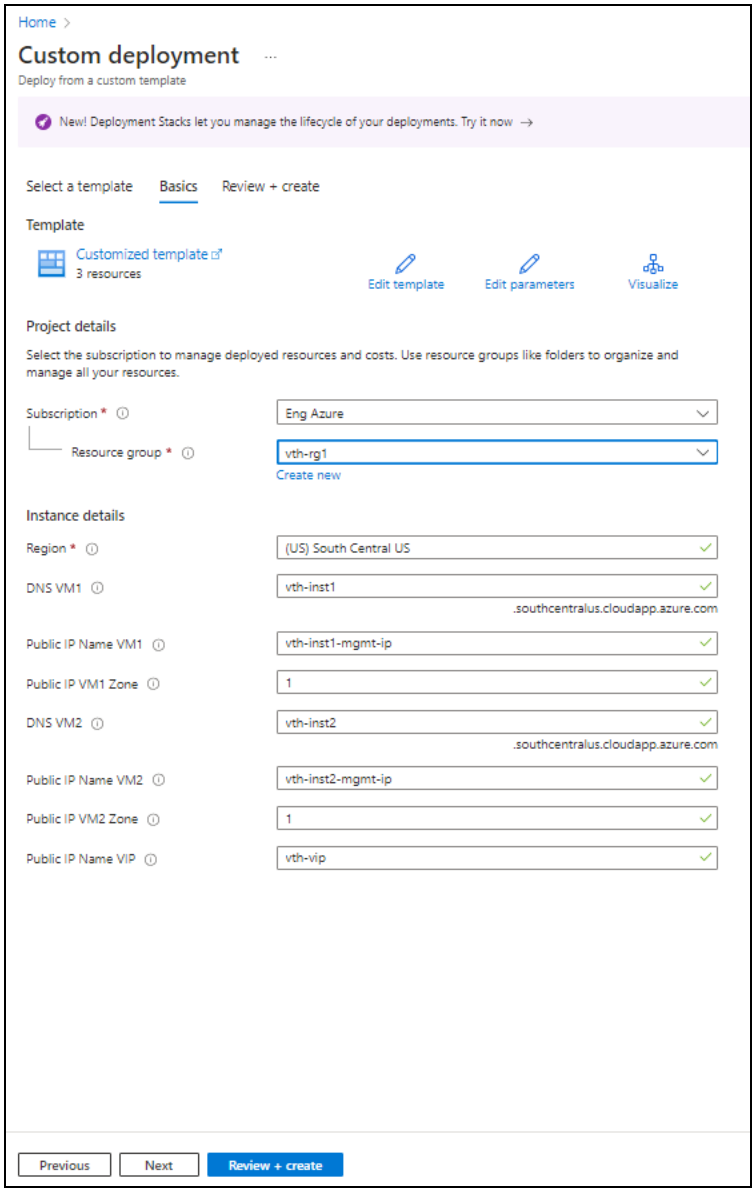
4. From the **Edit template** window, perform either of the following step:
   - Click **Load file** and browse to the folder where you have downloaded the ARM template. Select **ARM_TMPL_PUBLIC_IP.json** to upload.
   - From Windows Explorer, navigate to the folder where you have downloaded the ARM template. Copy **ARM_TMPL_PUBLIC_IP.json** content and paste it in the editor.

Figure 231 : Edit template window

5. Click **Save**.

   The **Custom deployment** window is displayed with the template parameters and default values.

Figure 232 : Custom deployment template



6. Select an existing or create a new **Resource group** under which you want to deploy the custom template resources.

NOTE: Hover ⓘ for description of each corresponding parameter.

7. Update the default values and provide the values in the empty fields as

appropriate in the **Instance details** section shown in Figure 232.

NOTE: Use a suitable VM size that supports at least three NICs. For VM sizes, see Supported VM Sizes.

For cross-zone high availability, the Zone-redundant policy is implied to the Management IP and Public IP VIP.

8. Click **Review+create**.

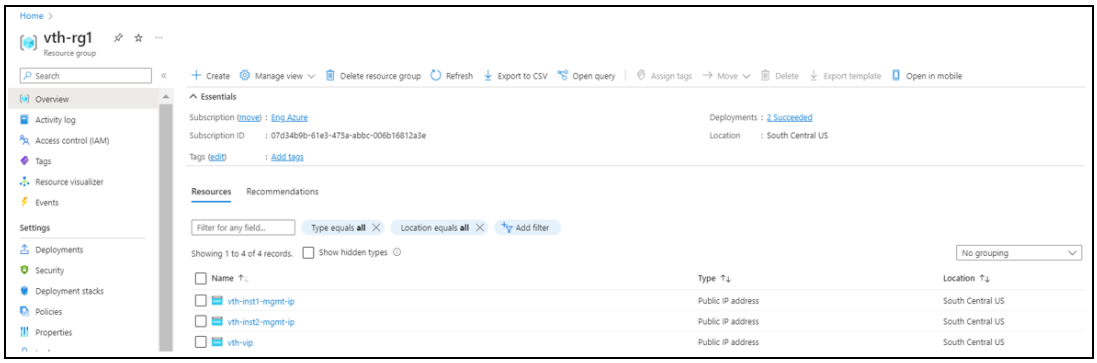
   The validation appears.

9. Click **Create**.

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

10. Verify if the above listed resources are created under **Home** > **Azure services** > **Resource Groups** > <*resource_group_name*>.

Figure 233 : Resource listing under resource group



Execute using Azure CLI

To deploy the PUBLIC-IP template using Azure CLI commands, perform the following steps:

1. Download PUBLIC-IP template.

NOTE: This template contains pre-populated default values that can be modified as required and it does not create new virtual network, network security group, subnets, and Public IP.

2. Navigate to the folder where you have downloaded the ARM template, and open the ARM_TMPL_PUBLIC_IP_PARAM.json with a text editor.

NOTE: Each parameter has a default value mentioned in the parameter file that can be modified as appropriate.

3. Configure the following parameters depending upon your requirements:

Table 20 : JSON Parameters

Resource Name	Description

DNS Label Prefix for Virtual Machine 1	Specify a unique DNS Name prefix for Thunder virtual machine 1.
	`"DNS VM1": {`
	`"value": "vth-inst1"`
	`},`

Public IP address name for Virtual Machine 1	Specify a unique public IP name for management traffic for Thunder virtual machine 1.
	`"Public IP Name VM1": {`
	`"value": "vth-inst1-mgmt-ip"`
	`},`
	NOTE: For cross-zone high availability, the Zone-redundant policy is implied to the Management IP.

DNS Label Prefix for Virtual Machine 2	Specify a unique DNS Name prefix for Thunder virtual machine 2.
	`"DNS VM2": {`
	`"value": "vth-inst2"`
	`},`

Public IP address name for Virtual Machine 2	Specify a unique public IP name for management traffic for Thunder virtual machine 1.

Table 20 : JSON Parameters

Resource Name	Description

	<pre>"Public IP Name VM2": {
	"value": "vth-inst2-mgmt-ip"
	},</pre>
	NOTE: For cross-zone high availability, the Zone-redundant policy is implied to the Management IP.

Virtual IP address (VIP) Public IP	Specify a unique public IP name for VIP.
	<pre>"Public IP Name VIP": {
	"value": "vth-vip"
	}</pre>
	NOTE: For cross-zone high availability, the Zone-redundant policy is implied to the Public IP VIP.

NOTE: The Virtual Network (VN), Subnets, Network Security Group (NSG), and Public IP Address should be deployed in the same resource group.

4. Verify if all the configurations in the ARM_TMPL_PUBLIC_IP_PARAM.json file are correct and then save the changes.
5. From Start menu, open PowerShell and navigate to the folder where you have downloaded the ARM template.
6. Run the following command to create an Azure deployment group.

```
PS C:\Users\TestUser\Templates> az deployment group create -g
<resource_group_name> --template-file <template_name> --parameters
<param_template_name>
```

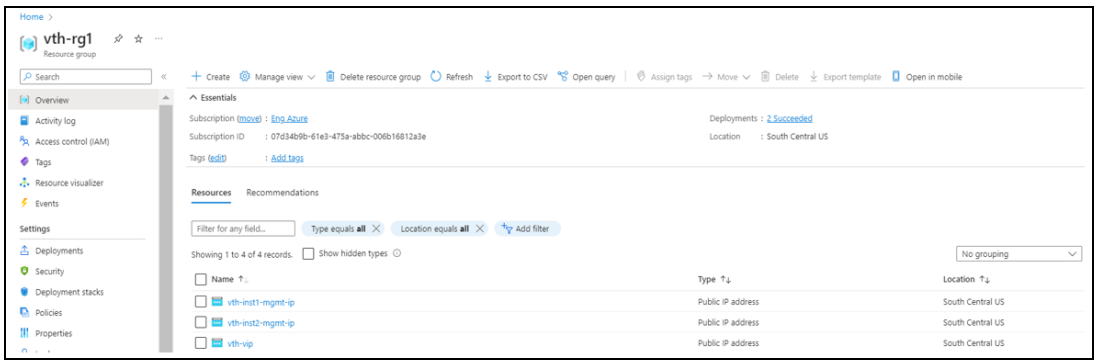
Example:

```
PS C:\Users\TestUser\Templates> az deployment group create -g vth-rg1
--template-file ARM_TMPL_PUBLIC_IP.json --parameters ARM_TMPL_PUBLIC_
IP_PARAM.json
```

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

7. Verify if the above listed resources are created under **Home** > **Azure services** > **Resource Groups** > <*resource_group_name*>.

Figure 234 : Resource listing under Resource Group



Default Password Policy

The default password policy has the following criteria:

- The password should be at least nine characters in length.
- The password should contain at least one number, an uppercase letter (English), a lowercase letter (English), and a special character.
- The password should have at least one letter or number different from the previous password.
- The password should not contain its corresponding username with the same capitalization of letters.
- The password should not contain repeated characters of the same letter or number with the same capitalization of letters.
- The password should not contain the sequential row keyboard input of four letters or numbers with the same capitalization of letters.

Delete the resources

To delete the resources, perform the following steps:

1. From **Azure Portal** > **Azure services** > **Resource Groups** > <*resource_group_name*>, select the resource to be deleted.

   The <selected_resource_name> - Overview tab is displayed.

2. Click **Stop** or **Delete**.

   The resource is stopped or deleted.

Get IP Address

The following topics are covered:

- vThunder Management Interface Public IP address
- vThunder Data Interface Primary Private IP address
- vThunder Data Interface Secondary Private IP address
- Server Private IP address

vThunder Management Interface Public IP address

To get the Public IP address of vThunder instance's management interface, perform the following steps:

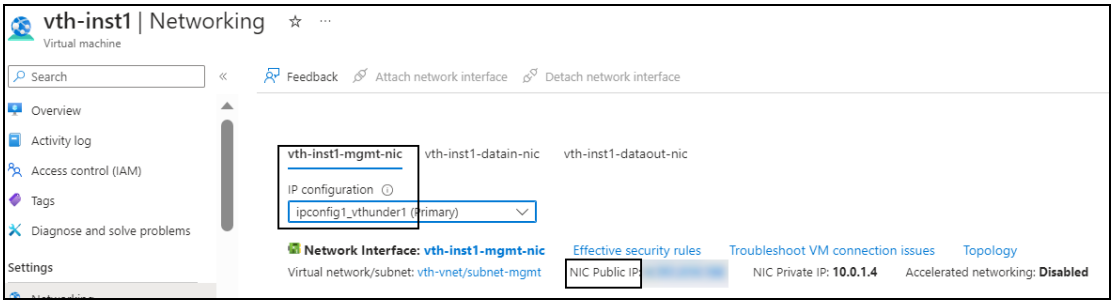
1. From **Home**, navigate to **Azure services** > **Resource Group** > <*resource_group_name*>.
2. Go to the required vThunder instance.

   For example, **`vth-inst1`**

3. Select **Networking** from the left **Settings** panel.
4. Select the Management tab > **IP configuration** > *ipconfig*.

   For example, under **`vth-inst-mgmt-vm1`** select **`ipconfig1`** as the IP configuration.

Figure 235 : vThunder Instance - Public IP of Management Interface



5. Select the **NIC Public IP**.

vThunder Data Interface Primary Private IP address

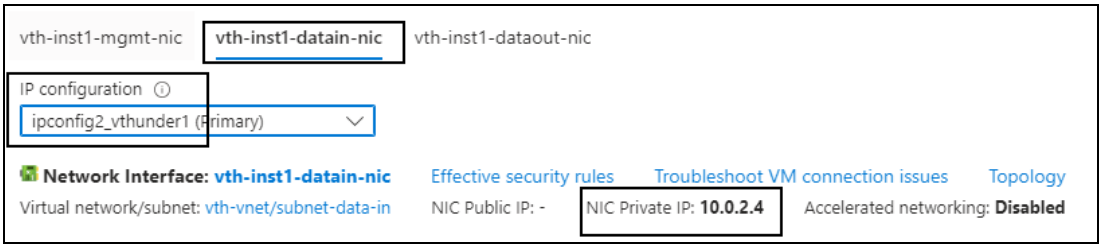
To get the Primary Private IP address of vThunder instance's Data1 or Data2 interface, perform the following steps:

1. From **Home**, navigate to **Azure services** > **Resource Group** > *<resource_group_name>*.
2. Go to the required vThunder instance.

   For example, **`vth-inst1`**
3. Select **Networking** from the left **Settings** panel.
4. Select the Data interface tab > **IP configuration** > *primary ipconfig*.

   For example, under **`vth-inst-datain-nic`** select **`primary_ipconfig2`** as the IP configuration.

   Figure 236 : vThunder Instance - Primary Private IP of Data1 Interface



5. Select the **NIC Private IP**.

vThunder Data Interface Secondary Private IP address

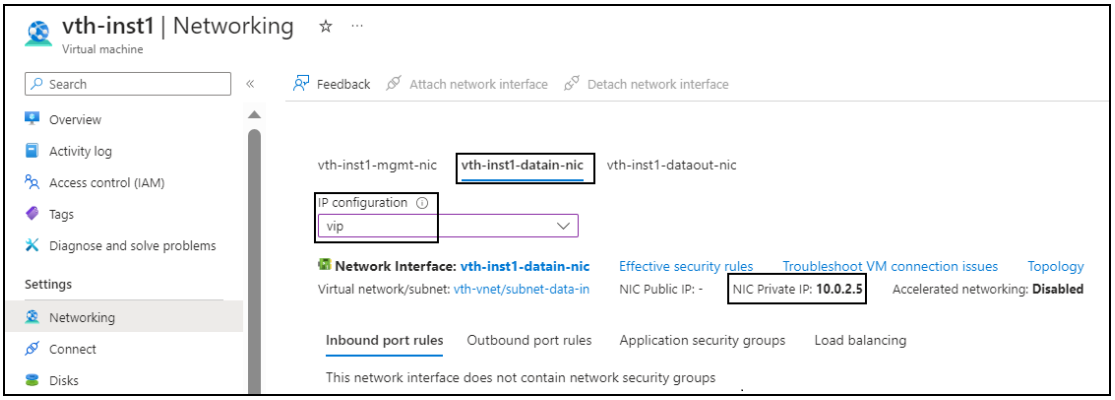
To get the Secondary Private IP address of vThunder instance's Data1 or Data2 interface, perform the following steps:

1. From **Home**, navigate to **Azure services** > **Resource Group** > *<resource_group_name>*.
2. Go to the required vThunder instance.

   For example, **`vth-inst1`**
3. Select **Networking** from the left **Settings** panel.
4. Select the Data interface tab > **IP configuration** > *secondary ipconfig*.

   For example, under **`vth-inst-datain-nic`** select **`vip`** as the IP configuration.

   Figure 237 : vThunder Instance - Secondary Private IP of Datain Interface



5. Select the **NIC Private IP**.

Server Private IP address

To get the Server Private IP address, perform the following steps:

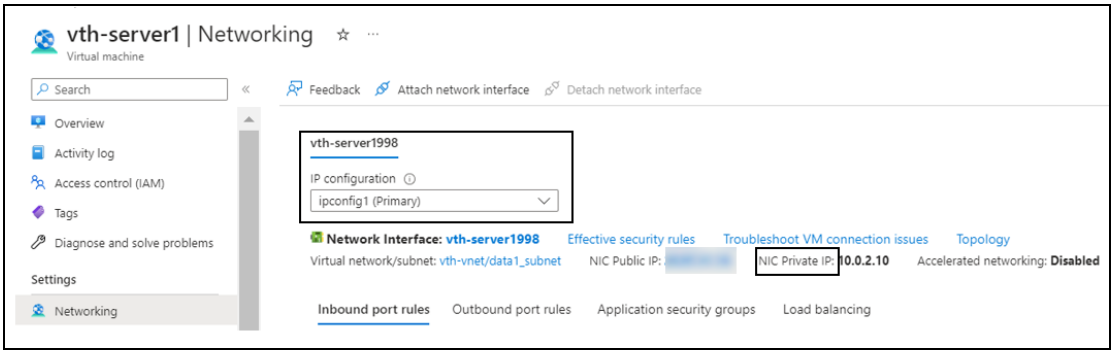
1. From **Home**, navigate to **Azure services** > **Resource Group** > *<resource_group_name>*.
2. Go to the required server instance.

   For example, **`vth-server1`**

3. Select **Networking** from the left **Settings** panel.
4. Select *ipconfig (Primary)* under **IP configuration**.

   For example, under **`vth-server1998`** select **`ipconfig1 (Primary)`** as the IP configuration.

   Figure 238 : Server Private IP address



5. Select the **NIC Private IP**.

Install Azure CLI on PowerShell

To install Azure CLI on PowerShell, perform the following steps:

1. In your PowerShell command prompt, execute the following command to download Azure CLI executable file:

```
PS C:\Users\TestUser> $ProgressPreference = 'SilentlyContinue'; Invoke-WebRequest -Uri https://azcliprod.blob.core.windows.net/msi/azure-cli-2.51.0.msi -OutFile .\AzureCLI.msi; Start-Process msiexec.exe -Wait -ArgumentList '/I AzureCLI.msi /quiet'; Remove-Item .\AzureCLI.msi
```

2. Install Az PowerShell module.

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

   The latest version of the Az PowerShell module from the PowerShell repository is downloaded and installed.

3. Log in using your Azure account to start a CLI session.

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

4. Authorize your session.

   Once the authorization is complete, 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>
```

5. Navigate to the downloaded ARM template folder and set the execution policy for this folder.

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

For more information, see here.

Install PowerShell

To install PowerShell, perform the following steps:

On MacOS

To install PowerShell on MacOS, perform the following steps:

1. Download the executable file:
   - MacOS x64
   - MacOS ARM64
2. Run the executable file.

   ```
   sudo installer -pkg powershell-7.3.6-osx-x64.pkg -target /
   ```

   For more information, see here.

On Ubuntu

To install PowerShell on Ubuntu, perform the following steps:

1. Download the Ubuntu executable package from here.
2. Run the following command to install the downloaded package.

   ```
   sudo dpkg -i powershell-lts_7.2.13-1.deb_amd64.deb
   ```

3. Run the following command to resolve the missing dependencies if needed.

   ```
   sudo apt-get install -f
   ```

4. Run the following command to verify the installation:

   terraform -version

   For more information, see here.

On Windows

To install PowerShell on Windows, perform the following steps:

1. Download the PowerShell Windows executable file:
   - Windows x64
   - Windows x86
2. Run the PowerShell Windows executable file.

   For more information, see here.

Install Python3

Depending on your operation system, install Python (3.8.5 or higher):

CentOS

To install latest Python3 from OS repository, perform the following steps:

```
yum install -y python3
```

Linux/Ubuntu

To install Python3, perform the following steps:

```
apt update
apt-get install python3.10
apt install python3-pip
```

List of Custom Role Permissions

The following is the list of custom role permissions:

```
"Microsoft.Automation/automationAccounts/variables/read",
"Microsoft.Automation/automationAccounts/variables/write",
"Microsoft.Automation/automationAccounts/variables/delete",
"Microsoft.Automation/automationAccounts/runbooks/read",
"Microsoft.Automation/automationAccounts/runbooks/content/read",
"Microsoft.Automation/automationAccounts/jobs/write",
"Microsoft.Automation/automationAccounts/jobSchedules/write",
"Microsoft.Automation/automationAccounts/jobs/read",
"Microsoft.Automation/automationAccounts/jobs/output/read",
"Microsoft.Automation/automationAccounts/runbooks/operationResults/read",
"Microsoft.Automation/automationAccounts/jobs/streams/read",
"Microsoft.Automation/automationAccounts/jobSchedules/read",
"Microsoft.OperationalInsights/workspaces/sharedKeys/action",
"Microsoft.OperationalInsights/workspaces/read"

"Microsoft.Compute/virtualMachineScaleSets/read",
"Microsoft.Compute/virtualMachineScaleSets/write",
"Microsoft.Compute/virtualMachineScaleSets/delete",
```

```
"Microsoft.Compute/virtualMachineScaleSets/delete/action",
"Microsoft.Compute/virtualMachineScaleSets/start/action",
"Microsoft.Compute/virtualMachineScaleSets/powerOff/action",
"Microsoft.Compute/virtualMachineScaleSets/restart/action",
"Microsoft.Compute/virtualMachineScaleSets/deallocate/action",
"Microsoft.Compute/virtualMachineScaleSets/scale/action",
"Microsoft.Compute/virtualMachineScaleSets/networkInterfaces/read",
"Microsoft.Compute/virtualMachineScaleSets/publicIPAddresses/read",

"Microsoft.Compute/virtualMachineScaleSets/providers/Microsoft.Insights/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/diagnosticSe
ttings/read",

"Microsoft.Network/loadBalancers/providers/Microsoft.Insights/diagnosticSe
ttings/write",
"Microsoft.Network/loadBalancers/frontendIPConfigurations/read",
"Microsoft.Network/loadBalancers/frontendIPConfigurations/join/action",

"Microsoft.Network/loadBalancers/frontendIPConfigurations/loadBalancerPool
s/read",

"Microsoft.Network/loadBalancers/frontendIPConfigurations/loadBalancerPool
s/write",

"Microsoft.Network/loadBalancers/frontendIPConfigurations/loadBalancerPool
s/delete",

"Microsoft.Network/loadBalancers/frontendIPConfigurations/loadBalancerPool
s/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/logDefinitio
ns/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/metricDefini
tions/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",
```

Supported VM Sizes

The following table lists the VM sizes compatible with the ARM template.

Table 21 : Supported VM sizes

Series	Size	Qualified Name	Accelerated Network
A series	Standard A2 Standard A2v2 Standard A2mv2 Standard A4v2 Standard A4mv2	Standard_A2 Standard_A2_v2 Standard_A2m_ v2 Standard_A4_v2 Standard_A4m_v2	Not Supported Not Supported Not Supported

Table 21 : Supported VM sizes

Series	Size	Qualified Name	Accelerated Network
	Standard A3 Standard A4 Standard A8v2	Standard_A3 Standard_A4 Standard_A8_v2	Not Supported Not Supported Not Supported Not Supported Not Supported
B series	Standard B2s Standard B2ms Standard B4ms	Standard_B2_s Standard_B2ms Standard_B4ms	Not Supported Not Supported Not Supported
D series	Standard D2v2 Standard D4v3 Standard D4sv3 Standard D3v2 Standard Ds3v2 Standard D5v2	Standard_D2_v2 Standard_D4_v3 Standard_D4s_v3 Standard_D3_v2 Standard_Ds3_v2 Standard_D5_v2	Supported Supported Supported Supported Supported Supported
F series	Standard F4s Standard F8 Standard F16s	Standard_F4s Standard_F8 Standard_F16s	Not Supported Not Supported Not Supported

Table 21 : Supported VM sizes

Series	Size	Qualified Name	Accelerated Network
			Not Supported

ACOS 6.0.0 and later versions support accelerated networking.

NOTE: Azure plans 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 available sizes in Azure, see Sizes for Cloud Services and Sizes for virtual machines.

License Information

This product includes software covered by the MIT License.

For more information, see MIT License.

Support Information

For any issues or queries related to ARM templates, open a case at A10 Networks Support or reach out to support@a10networks.com and mention "A10-azure-arm-templates" in the subject line.

What's New

1.2.0

This release has the following enhancements for Thunder® Application Delivery Controller (ADC):

- Added support for ACOS 6.0.2, ACOS 6.0.1, and ACOS 5.2.1-P8.
- Added a template for creating a new virtual network (VNET), subnets, and network security group (NSGs) in the specified resource group.
- Added a template for creating new Public IP address in the specified resource group.
- Separated the deployment and configuration parameters to ensure a clear distinction between the resources needed for initial deployment and those required for subsequent configuration and customization.
- Introduced two new SLB templates, SLB HTTP and Persist Cookie to enhance the functionality and performance of the Server Load Balancer (SLB) by optimizing HTTP traffic distribution and implementing efficient cookie persistence.
- Added support for Accelerated Networking and IP Forwarding to provide enhanced networking capabilities and improved performance.
- Added support for Thunder Observability Agent (TOA) to collect, process and publish Thunder metrics and syslogs.
- Added new hybrid cloud GSLB configuration to optimize performance, reliability, and ease of use in hybrid cloud environments.

1.1.0

This release has the following enhancement for Thunder® Application Delivery Controller (ADC):

- Added support for ACOS 5.2.1-P7, ACOS 6.0.0-P1 and ACOS 6.0.0-P2.
- Added Thunder password change capability.

1.0.0

This release has the following enhancements for Thunder® Application Delivery Controller (ADC):

- Added support for ACOS 5.2.1-P6.
- Added GLM, HA, SLB, and SSL vThunder configuration.
- Added the following deployment templates:
  - A10-vThunder_ADC-2NIC-1VM-GLM
  - A10-vThunder_ADC-2NIC-1VM
  - A10-vThunder_ADC-3NIC-2VM-HA-GLM-PUBVIP-BACKAUTO
  - A10-vThunder_ADC-3NIC-2VM-HA-GLM-PVTVIP
  - A10-vThunder_ADC-3NIC-2VM-HA
  - A10-vThunder_ADC-3NIC-6VM-2RG-GSLB
  - A10-vThunder_ADC-3NIC-VMSS

Contact Us