

v1.0

31-August-2022

USER MANUAL

AZURE ARM TEMPLATE 3NIC-2VM-HA

# PATENT PROTECTION

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

# TRADEMARKS

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

# CONFIDENTIALITY

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

# DISCLAIMER

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

# ENVIRONMENTAL CONSIDERATIONS

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

# FURTHER INFORMATION

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

Contents

[PATENT PROTECTION 1](#_Toc122533658)

[TRADEMARKS 1](#_Toc122533659)

[CONFIDENTIALITY 1](#_Toc122533660)

[DISCLAIMER 1](#_Toc122533661)

[ENVIRONMENTAL CONSIDERATIONS 2](#_Toc122533662)

[FURTHER INFORMATION 2](#_Toc122533663)

[Introduction to Installing vThunder on Microsoft Azure 4](#_Toc122533664)

[Overview of Microsoft Azure 5](#_Toc122533665)

[Azure Terminology 7](#_Toc122533666)

[System Requirements 8](#_Toc122533667)

[Pre-requisites 11](#_Toc122533668)

[Installation vThunder on Microsoft Azure 12](#_Toc122533669)

[Chapter 1 - Core vThunder Installation & Basic Setup. 12](#_Toc122533670)

[Configure 12](#_Toc122533671)

[Install 16](#_Toc122533672)

[Verify 17](#_Toc122533673)

[Configure – Client Servers Setup 18](#_Toc122533674)

[Chapter 2 - vThunder Change Password. 29](#_Toc122533675)

[Configure 29](#_Toc122533676)

[Install 29](#_Toc122533677)

[Chapter 3 - Configuring Server Load Balancer (SLB) and SSL Certificate. 30](#_Toc122533678)

[Configure 30](#_Toc122533679)

[Install 34](#_Toc122533680)

[Chapter 4 - Configuring High Availability (HA) 34](#_Toc122533681)

[Configure Azure Access Key 34](#_Toc122533682)

[Configure 51](#_Toc122533683)

[Install 52](#_Toc122533684)

[Chapter 4 - Let us Verify. 53](#_Toc122533685)

[Login to vThunder 53](#_Toc122533686)

[vThunder GUI Verification 53](#_Toc122533687)

[SLB Verification 55](#_Toc122533688)

[SSL Certificate Verification 55](#_Toc122533689)

[HA Verification 56](#_Toc122533690)

# Introduction to Installing vThunder on Microsoft Azure

vThunder for Microsoft Azure is a fully operational, software-only version of the ACOS Application Delivery Controller (ADC) device. It is configurable by ACOS CLI, GUI, AXAPI, and Harmony Controller. For more information see Virtual Instances in Harmony Controller.

vThunder is a virtual appliance, yet it retains most of the functionality available on the hard- ware based ACOS appliances. Managing vThunder is the same as managing hardware based ACOS device, and vThunder has the same CLI configurations and GUI presentation.

The networking configuration for vThunder is also like hardware based ACOS devices. The maximum throughput of vThunder for Azure is variable and depends on vThunder software license purchase and type instance used to deploy vThunder.

*A10 Networks brings Out-Of-Box template to deploy vThunder along with multiple features and functionality with pre-defined format into azure cloud.*

Please refer below section for more details.

* Three Network Card Interface (3NIC).
* 2 numbers of Virtual Machines (2VM).
* Server Load Balancer (SLB)
* TLS/SSL Certification (SSL).
* vThunder in High Availability (HA)

# Overview of Microsoft Azure

With the move to the cloud, many teams have adopted agile development methods. These teams iterate quickly. They need to repeatedly deploy their solutions to the cloud, and know their infrastructure is in a reliable state. As infrastructure has become part of the iterative process, the division between operations and development has disappeared. Teams need to manage infrastructure and application code through a unified process.

To meet these challenges, you can automate deployments and use the practice of infrastructure as code. In code, you define the infrastructure that needs to be deployed. The infrastructure code becomes part of your project. Just like application code, you store the infrastructure code in a source repository and version it. Any one on your team can run the code and deploy similar environments.

To implement infrastructure as code for your Azure solutions, use azure resource manager templates. The template is a json native file that defines the infrastructure and configuration for your project. The template uses declarative syntax, which lets you state what you intend to deploy without having to write the sequence of programming commands to create it. In the template, you specify the resources to deploy and the properties for those resources.

**Microsoft Azure** (formerly known as Windows Azure) is Microsoft’s cloud computing platform. Azure is an industry leader for both infrastructure-as-a-service (IaaS) and platform-as-a-ser- vice (PaaS). Azure offers a combination of managed and unmanaged services that lets customers deploy and manage their applications as they see fit.

The Azure cloud computing platform runs on Microsoft data center and is globally dis- tributed across more than a dozen countries. Such global distribution helps ensure customers receive high performance, regardless of where they are located.

Azure is flexible and can support virtually any operating system, from Windows to Linux, any programming language, from Java to C++, and any database, from SQL to Oracle. Azure also offers 99.95% uptime and is the platform that Microsoft uses to run many of its popular ser- vices, such as Bing, Skype, Xbox, and Office 365.

A10 Networks vThunder virtual device can be set up as an instance in Azure’s cloud and can be used to provide a robust server load balancing (SLB) service.

Microsoft Azure uses the following tools to create and manage resources:

**Azure Portal** - A web console to create and monitor Azure resources. For more information, refer to <https://azure.microsoft.com/en-in/features/azure-portal/>

**Azure PowerShell** - A set of cmdlets used for managing Azure resources from the command line. Launch Azure PowerShell from a browser within the Azure Cloud Shell or install the software on the system to start a local PowerShell session.

For more information, refer to <https://docs.microsoft.com/en-us/powershell/>

**Azure CLI—** Can also be launched from a browser within the Azure Cloud Shell or install the software on the system to start a local CLI session. For more information, refer to <https://docs.microsoft.com/en-us/cli/azure/overview?view=azure-cli-latest>

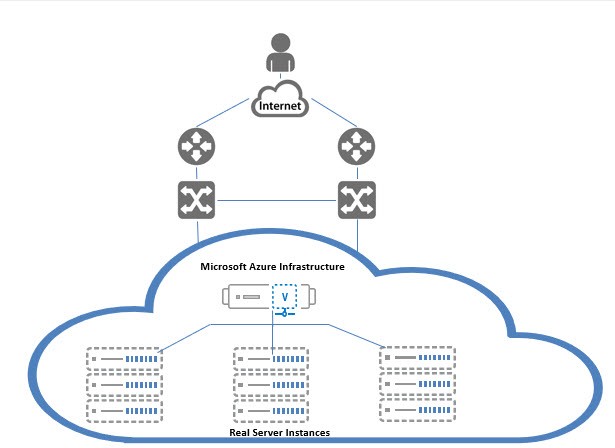
You **can** launch Cloud Shell from the top navigation bar of the Azure portal.

FIGURE 1-1: Launching Cloud Shell



The following figure shows how vThunder fits into the Microsoft Azure infrastructure.

FIGURE 1-2: vThunder for Microsoft Azure



# Azure Terminology

**Azure account** — The Azure account created has different support plans for different regions. For more information on different Azure regions and availability of types of virtual machines in these regions, refer to

<https://docs.microsoft.com/en-us/azure/virtual-machines/linux/overview>

**Resource group** — A resource group is a logical group of all the resources related to an Azure solution. Azure offers flexibility in the allocation of resources to resource groups.

For more information, refer to

[https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group- overview](https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-%20overview/)

**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, refer to

[https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group- overview](https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-%20overview/)

**Virtual network** — The Microsoft Azure Virtual Network service enables resources to securely communicate with other resources in an Azure network in the cloud. A virtual network is hence logical isolation of the Azure cloud for an Azure account. You can connect different virtual networks and to on-premises networks. For more information, refer to

[https://docs.microsoft.com/en-us/azure/virtual-machines/windows/tutorial-avail- ability-sets](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/tutorial-avail-%20ability-sets/)

**Network security group (NSG)** — A network security group (NSG) contains a list of security rules that allow or deny network traffic to resources connected to Azure virtual networks (VNet). The NSGs can be associated with subnets or individual NICs attached to the VMs. When an NSG is associated with a subnet, the rules apply to all the resources connected to the subnet.

# System Requirements

Below all azure cloud resources will be created.

All templates come with default value it can be change while execution.

1. Azure Resource Group.

New resource group will be created with the specified name and location, in case does not exist.

Default name: *vth-rg1*

1. Azure Storage Account.

New storage account will be created inside resource group.

In case storage account already exists, it will prompt error “The storage account named is already taken”.

**Details:**

**Storage Account Name:** *vthunderstorage*

**Performance**: Standard

**Replication**: Read-access geo-redundant storage (RA-GRS)

**Account kind**: StorageV2 (general purpose v2)

1. Virtual Machine Instance.

**Basic Details:**

**Product: A10 vThunder**

**Instance Name:** *vth-inst1*

**Operating system**: Linux

**Default Size**: Standard\_B4ms (4 vCPUs, 16 GiB Memory)

**Basic Details:**

**Product: A10 vThunder**

**Instance Name:** *vth-inst2*

**Operating system**: Linux

**Default Size**: Standard\_B4ms (4 vCPUs, 16 GiB Memory)

Note:

\*\*Highly recommended to do assessment of your projected traffic before selecting any size.

\*\* Instances name and size can be customized in parameter file.

**Supported VM Sizes**

|  |  |  |
| --- | --- | --- |
| ***Series*** | ***Size*** | ***Qualified Name*** |
| A series | Standard A4\_v2  Standard A4m\_v2  Standard/Basic A4  Standard A8\_v2 | Standard\_A4\_v2  Standard\_A4m\_v2  Standard\_A4  Standard\_A8\_v2 |
| B series | Standard B2\_s  Standard B2ms  Standard B4ms | Standard\_B2\_s  Standard\_B2ms  Standard\_B4ms |
| D series | Standard D3\_v2  Standard DS3\_v2  Standard D5\_v2 | Standard\_D3\_v2  Standard\_DS3\_v2  Standard\_D5\_v2 |
| F series | Standard F4s  Standard F8  Standard F16s | Standard\_F4s  Standard\_F8  Standard\_F16s |

Few of sizes are getting retried soon from azure, please refer [Virtual Machine series | Microsoft Azure](https://azure.microsoft.com/en-in/pricing/details/virtual-machines/series/).

For more information, please refer as below.

<https://docs.microsoft.com/en-us/azure/virtual-machines/sizes-> [general](http://sales@a10networks.com/)

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

1. Virtual Cloud Network. [VCN]

Default address prefix for virtual network is 10.0.0.0/16.

Default name: *vth-vnet*

1. Public IP address.

Default public IP name:

*vth-inst1-mgmt-nic1-ip*

*vth-inst2-mgmt-nic1-ip*

1. Network Security Group. [NSG]

Default all interfaces are associated with security group.

Default name: *vth-inst1-nsg, vth-inst2-nsg*

Default Security Rules:

Table

Description automatically generated

1. Network Interface Card. [NIC]

Default name:

*vth-inst1-mgmt-nic1*

*vth-inst1-data-nic2*

*vth-inst1-data-nic3*

*vth-inst2-mgmt-nic1*

*vth-inst2-data-nic2*

*vth-inst2-data-nic3*

Each vThunder consist of two types of NIC.

* Management Interface with public IP
* Data Interfaces with private IP. [Ethernet 1, Ethernet 2]

Note: Interfaces holds IP from DHCP.

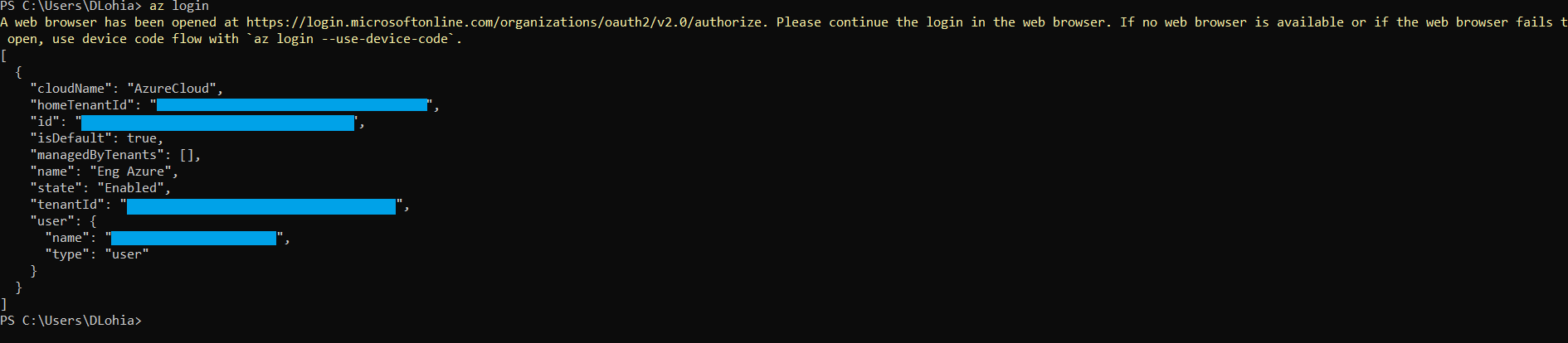
# Pre-requisites

Please find below detailed pre-requisites to install template using ARM.

1. Azure account and valid subscription.

Azure Portal—A web console to create and monitor Azure resources. For more information, refer to <https://azure.microsoft.com/en-in/features/azure-portal/>

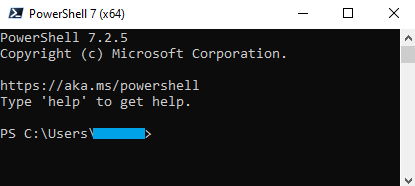
1. Azure CLI— Can also be launched from a browser within the Azure Cloud Shell or install the software on the system to start a local CLI session. For more information, refer to <https://docs.microsoft.com/en-us/cli/azure/overview?view=azure-cli-latest>



1. Windows PowerShell 7.0.6 LTS or 7.1.3, 7.2.2 or any higher. Recommended 7.2.2.

[Installing PowerShell on Windows - PowerShell | Microsoft Docs](https://docs.microsoft.com/en-us/powershell/scripting/install/installing-powershell-on-windows?view=powershell-7.2)

Azure PowerShell—A set of cmdlets used for managing Azure resources from the command line. Launch Azure PowerShell from a browser within the Azure Cloud Shell or install the software on the system to start a local PowerShell session. For more information, refer to <https://docs.microsoft.com/en-us/powershell/>

  
Install Az Modules: Install-Module Az



1. Policy Setting in PowerShell.

Set execution policy to Unrestricted:

Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass



1. Generate SSL certificate to apply on vThunder (Optional).
2. Document editor Notepad++ or Notepad or Any.

[Downloads | Notepad++ (notepad-plus-plus.org)](https://notepad-plus-plus.org/downloads/)

1. Artifacts:
2. [https://gitlab.a10networks.com/ax/a10-azure-arm-templates-internal/-/tree/develop/ARM-TEMPLATES/ARM-3NIC-2VM-HA](https://gitlab.a10networks.com/ax/a10-azure-arm-templates-internal/-/tree/feature/CLOUD-355/POWERSHELL-TEMPLATES/POWERSHELL-3NIC-VMSS )

# Installation vThunder on Microsoft Azure

## Chapter 1 - Core vThunder Installation & Basic Setup.

### Configure

Refer ARM\_TMPL\_3NIC\_2VM\_HA\_PARAM.json file to customize default values. Please find below in details.

**Setting vThunder Default Credentials**

Default credential is mentioned in below image, this is only required during VM creation.

Username: *vth-user*

Password: *vth-Password*

Text

Description automatically generated

Note: vThunder will get provision using above credential but those are temporary. As soon as it gets provision, vThunder will auto delete all users other than default user.

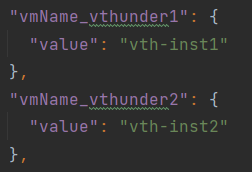
So, use below credentials for login.

Username: admin

Password: a10

**VM Name**

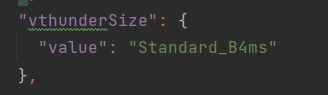
Default vthunder VM name.



**VM Size [VThunder]**

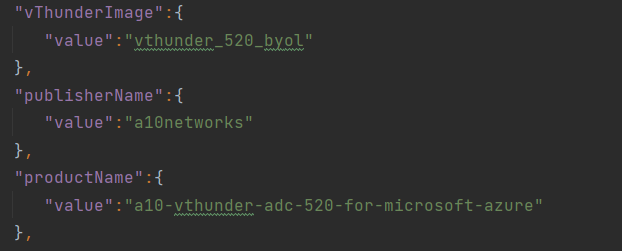
Any size which supports at least 3 NIC.

Please refer ‘Qualified Name’ column under [supported vm sizes](#_System_Requirements) section to select any other size.

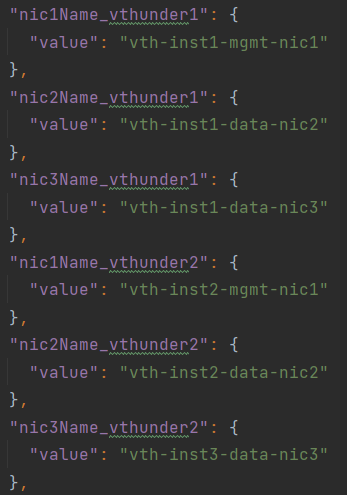


**vThunder Image**

User can pick available image from Azure marketplace.



**Network Interfaces Card**

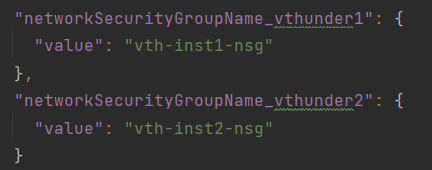


**Subnets**

Default subnets value

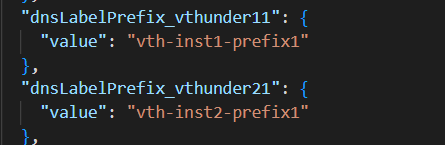


**Network Security Group**



**DNS Label Prefix**

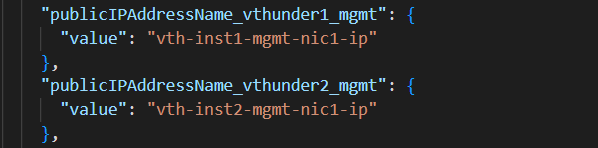
Default DNS Label Prefix value for vThunder1, vThunder2



**Public IP Name**

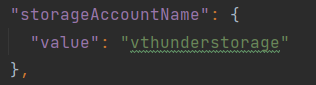
Default Public IP name for management, eth1 and eth2 of

vThunder1 and vThunder2.



**Storage Account Name**

If storage account is already existed, script will give the error “The storage account named is already taken.”



### Install

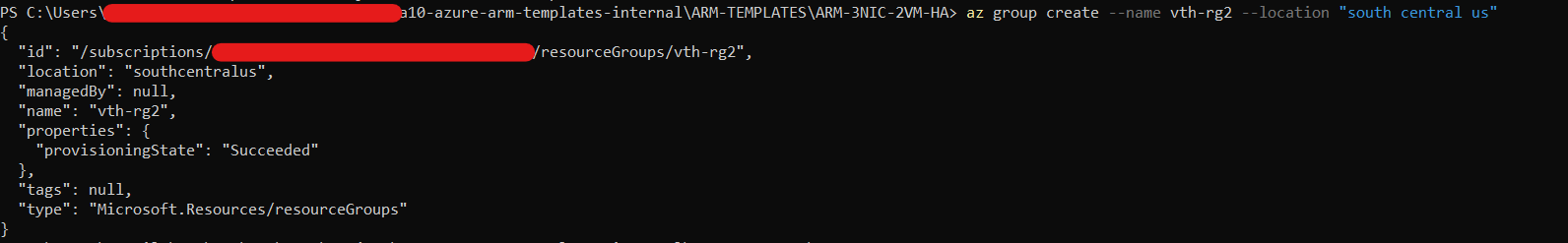
1. Open powershell 7 from start menu.

Graphical user interface, text, application

Description automatically generated

2. Create azure resource group.

Default name: *vth-rg1*



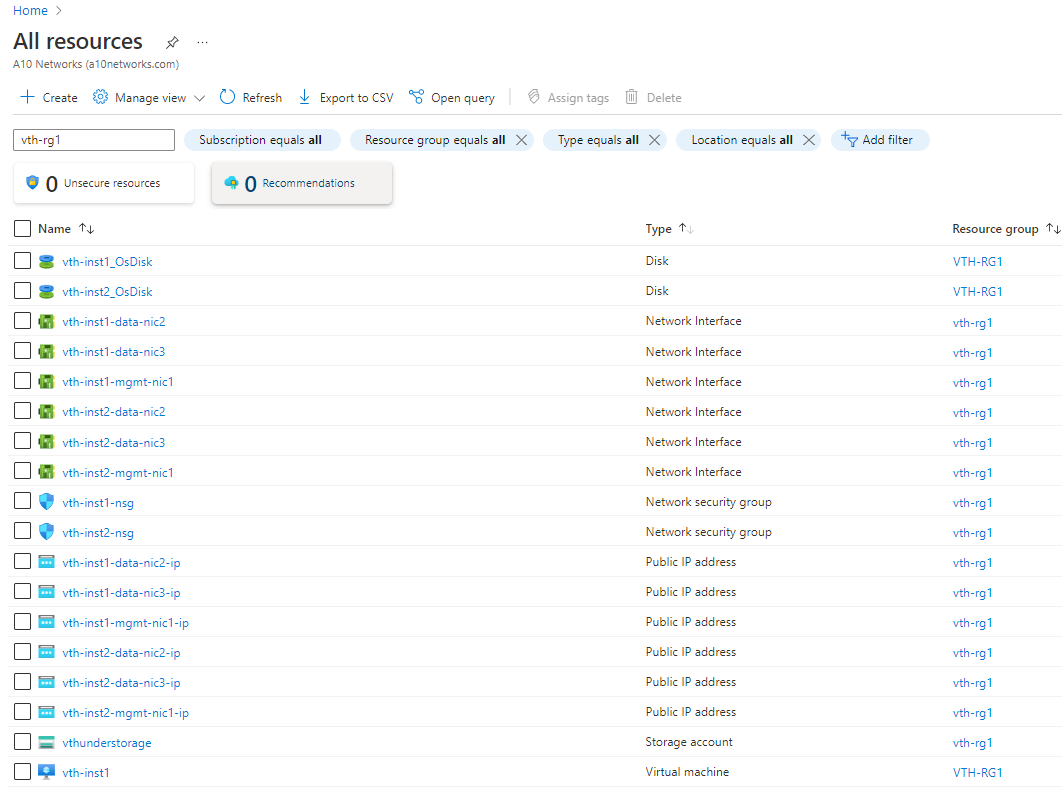
az group create --name vth-rg1 --location "south central us"

3. Run below command. 

az deployment group create -g *vth-rg1* --template-file ARM\_TMPL\_3NIC\_2VM\_HA\_1.json --parameters ARM\_TMPL\_3NIC\_2VM\_HA\_PARAM.json

### Verify

1. Resources list.

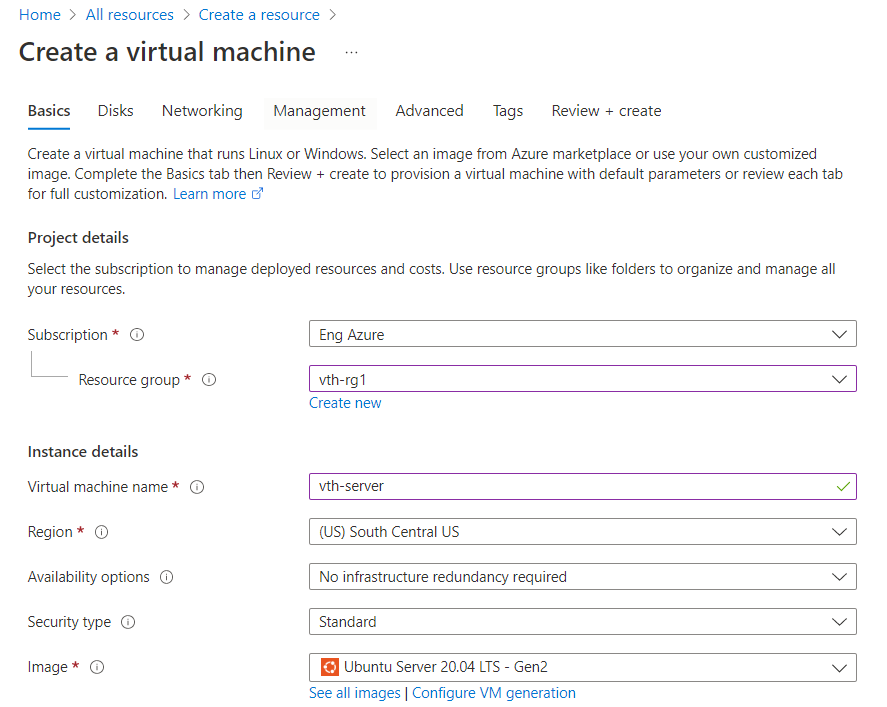


### Configure – Client Servers Setup

Go to Azure Portal-> Virtual machine -> Create

Add basic information.

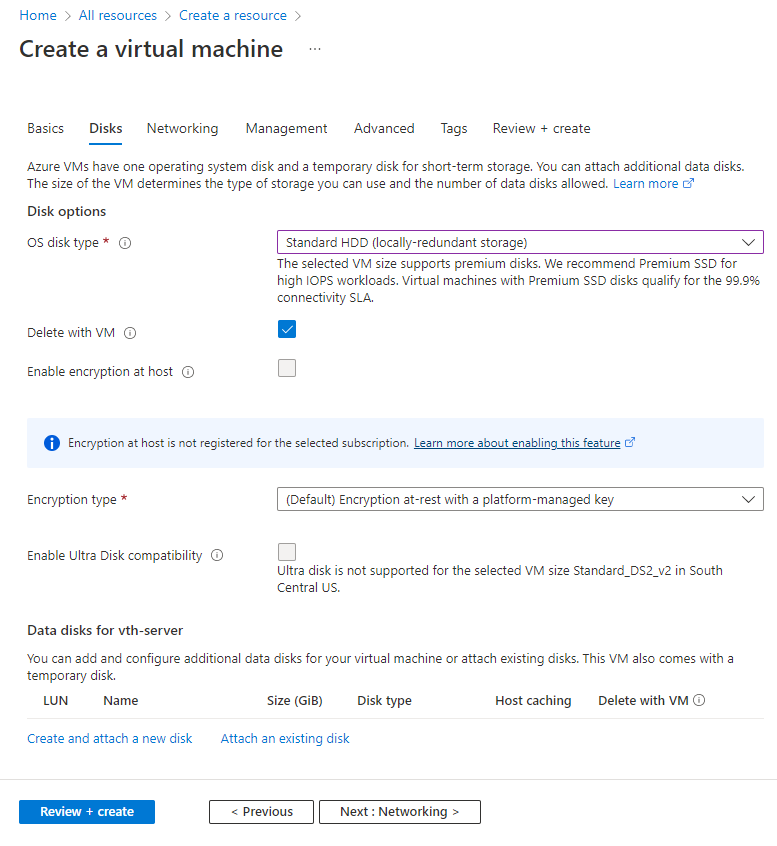
#### Create server machine.



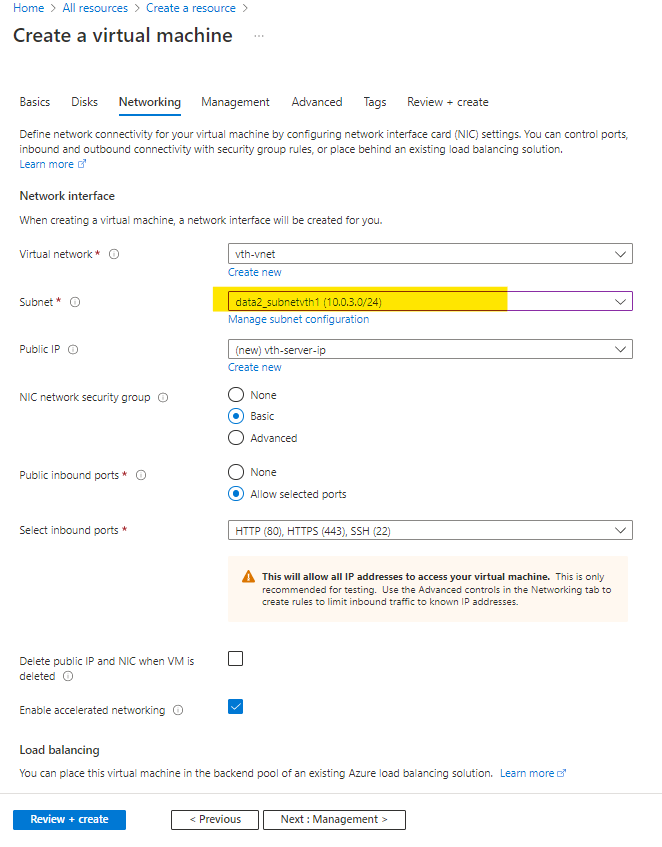
Graphical user interface, text, application, email

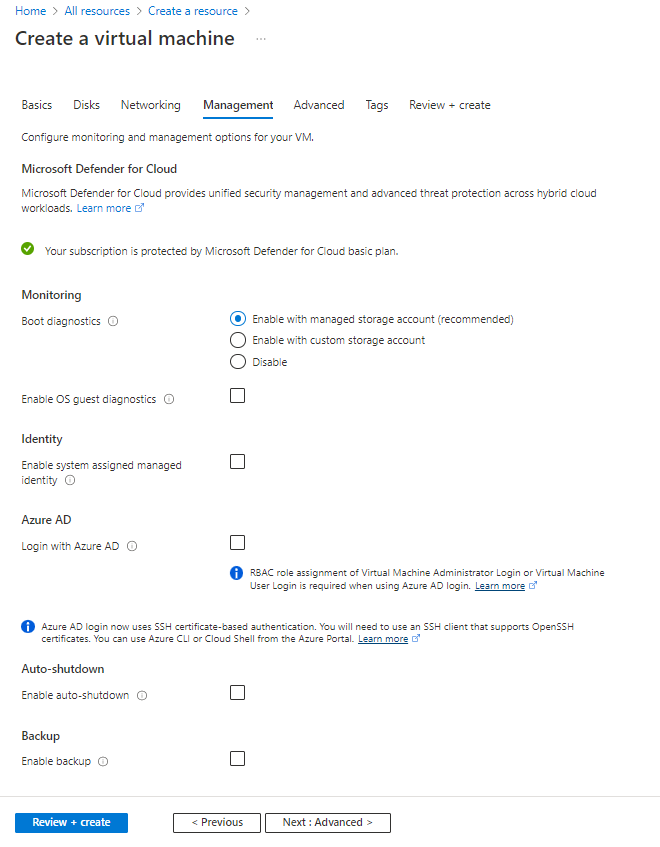
Description automatically generated

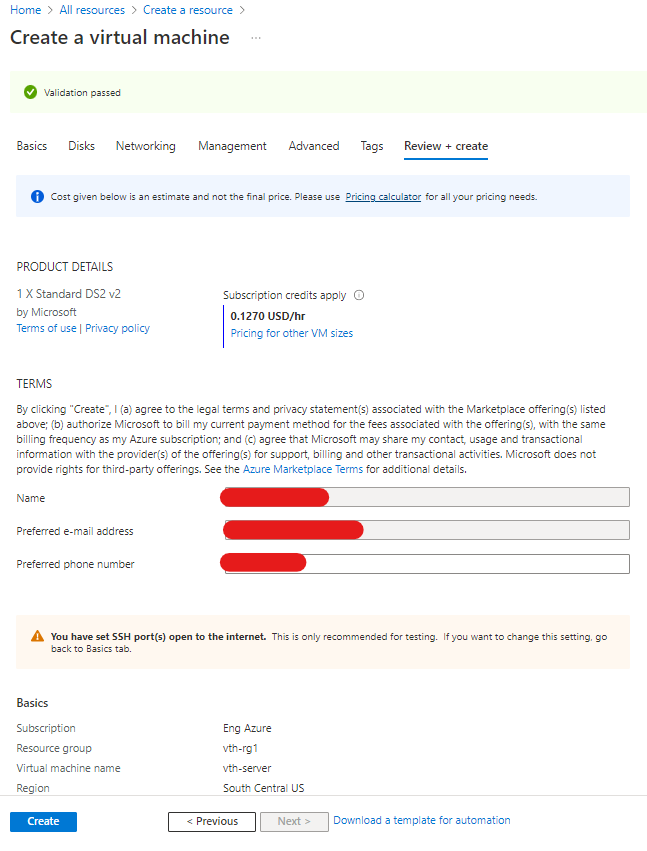
Select Next.



Select data subnet2



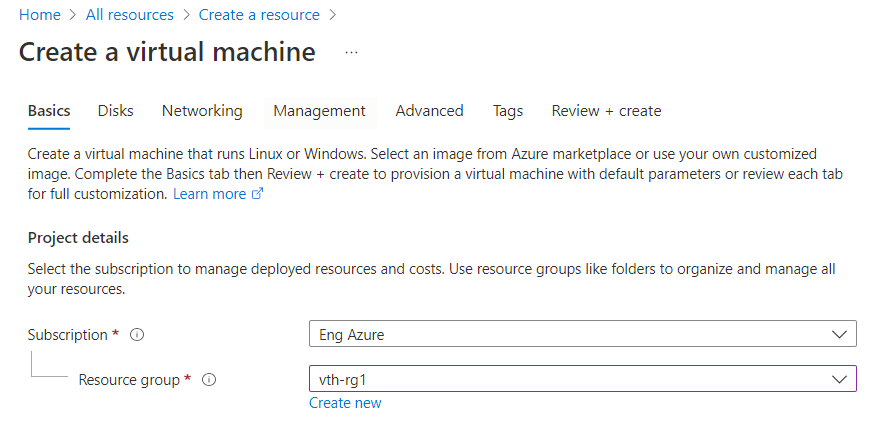


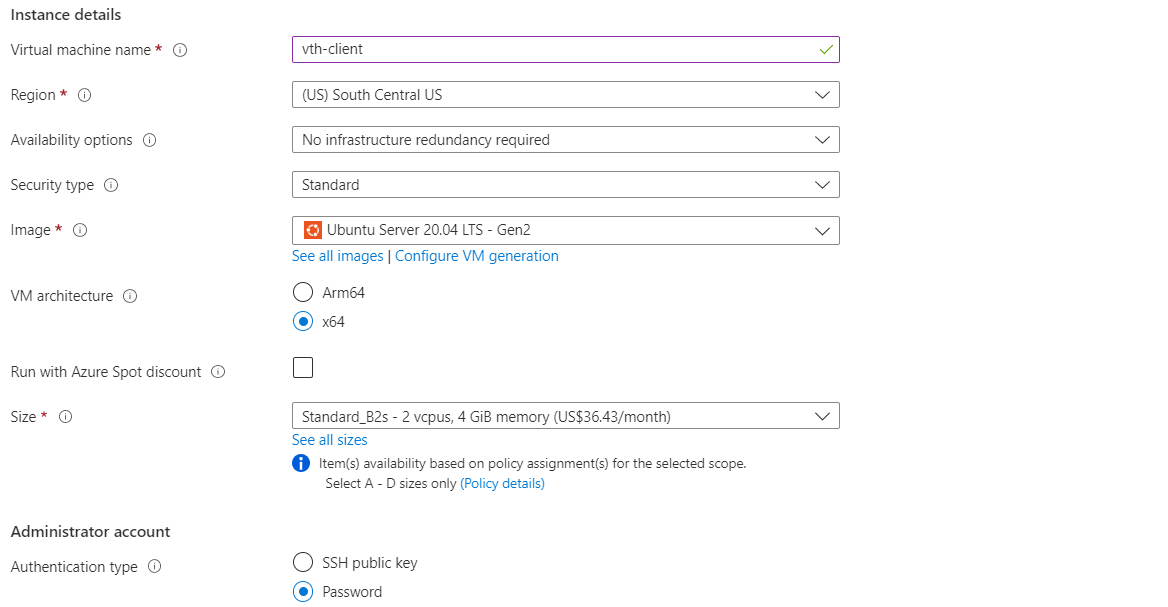


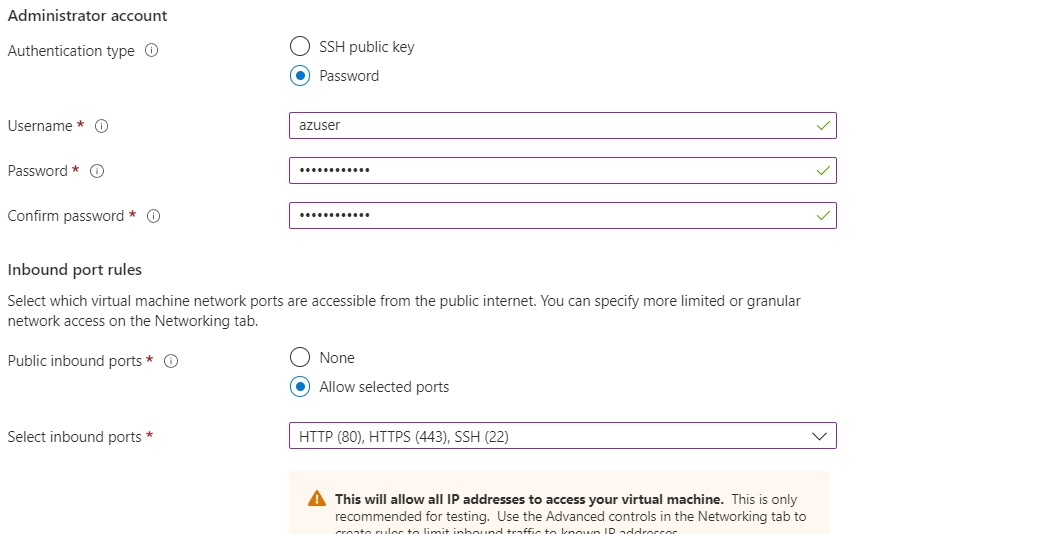
Go to Azure Portal-> Virtual machine -> Create

Add basic information.

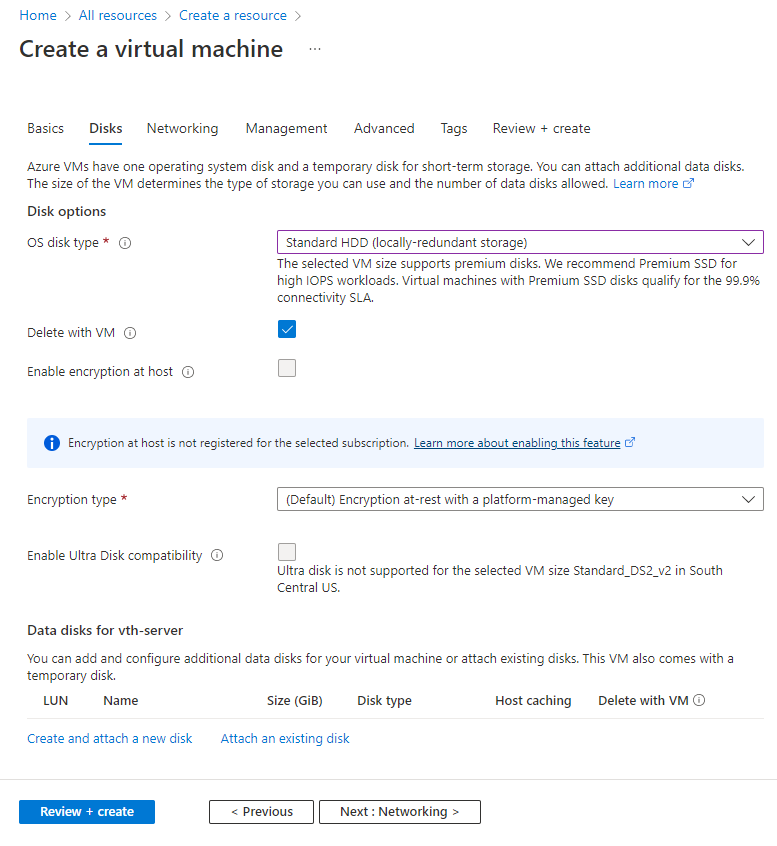
#### Create client machine



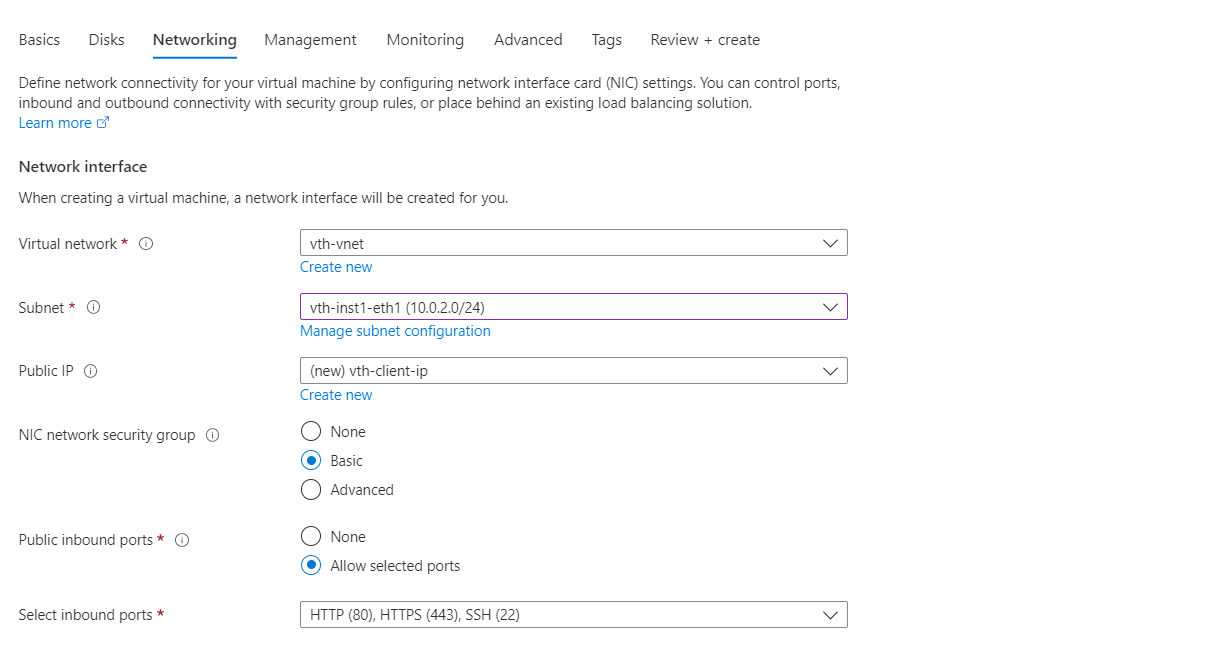


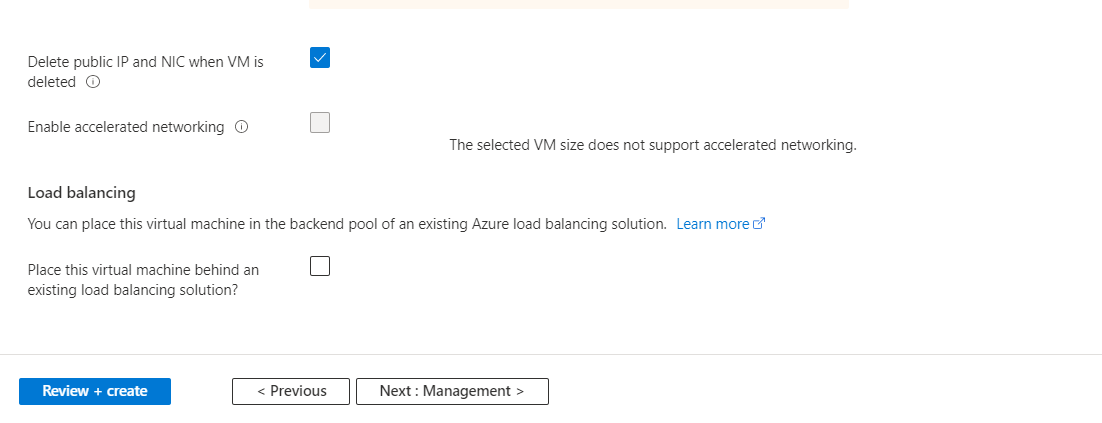


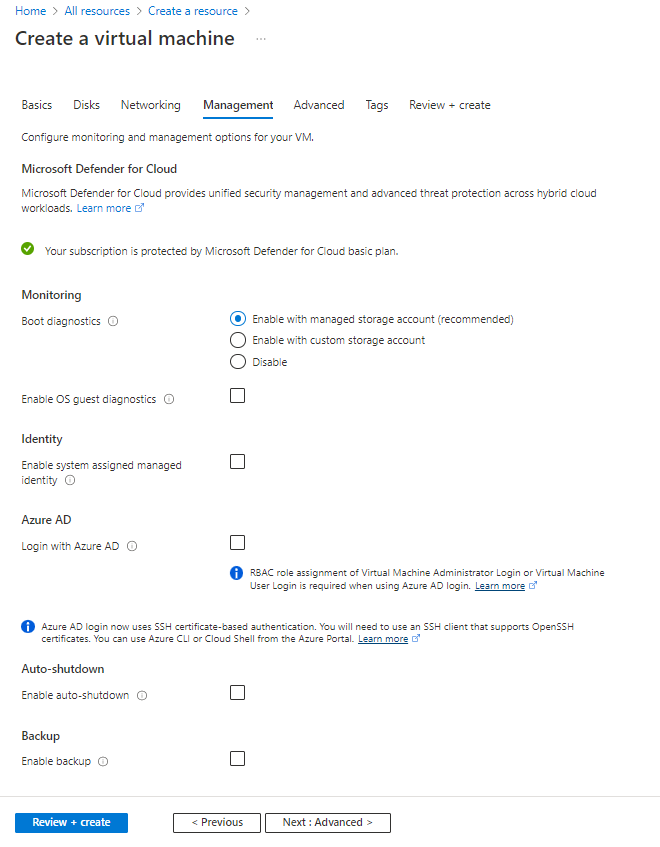
Select Next.

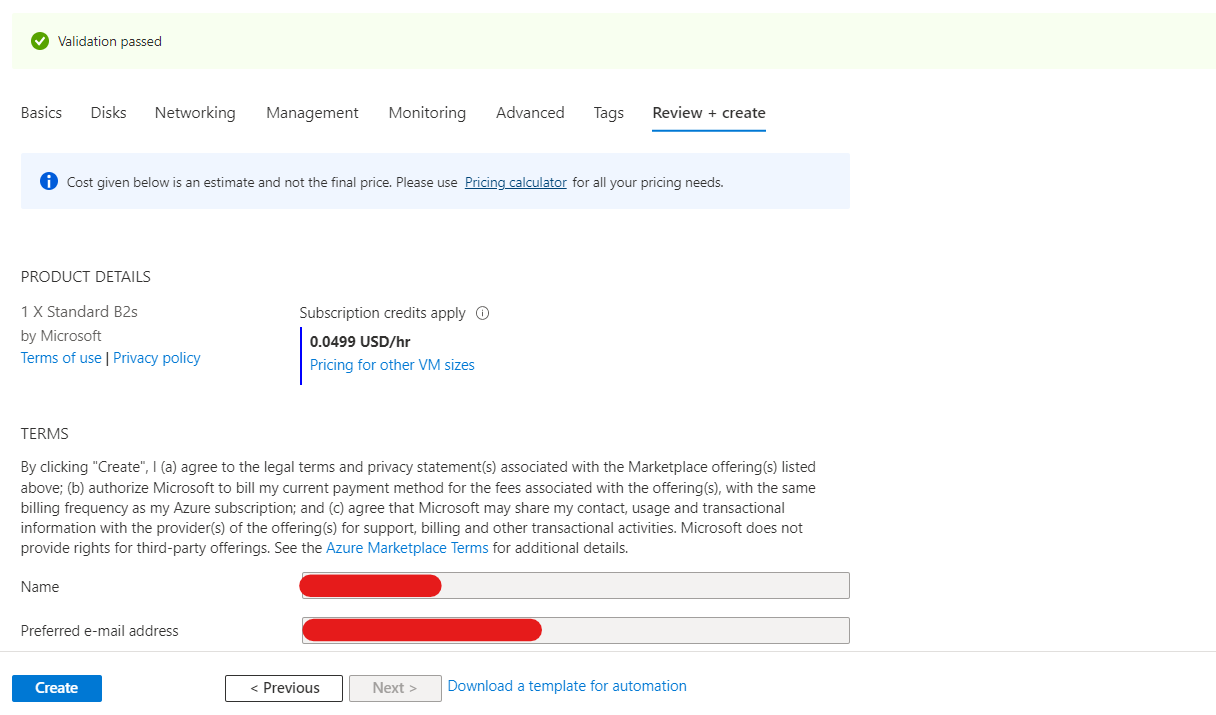


Select data subnet1









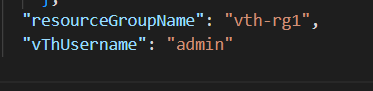
## Chapter 2 - vThunder Change Password.

### Configure

Please configure below parameters in ARM\_TMPL\_3NIC\_2VM\_HA\_SLB\_CONFIG\_PARAM.json

Resource group name: vth-rg1

vThUsername: admin.

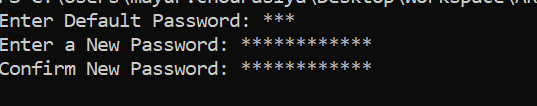


### Install

Users need to run the following script for change vThunder password.

.\ARM\_TMPL\_3NIC\_2VM\_HA\_CHANGE\_PASSWORD\_2.ps1

While running the change password script, user need to provide default and new password in the command prompt.



Description: - Default password value will be a10.

## Chapter 3 - Configuring Server Load Balancer (SLB) and SSL Certificate.

Note: In case you want to apply SSL certification then you need to create an SSL certificate and mention location of SSL certificate on ARM\_TMPL\_3NIC\_2VM\_HA\_SLB\_CONFIG\_PARAM.json file else you can skip SSL certificate on cli.

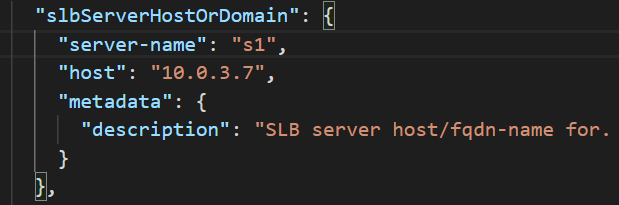
### Configure

Refer ARM\_TMPL\_3NIC\_2VM\_HA\_SLB\_CONFIG\_PARAM.json file to customize default values.

Please find below in details.

##### SLB Server Host/Domain

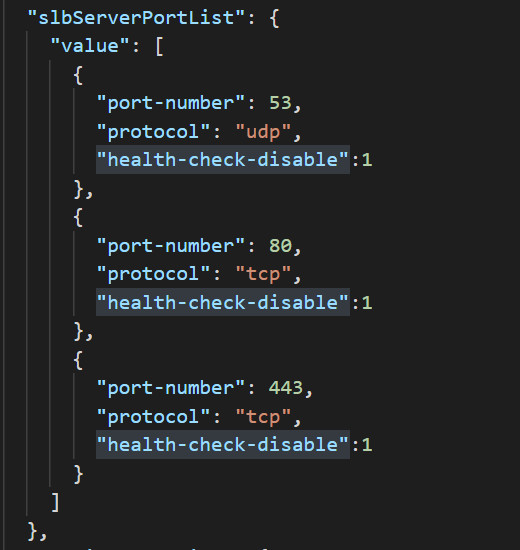
SLB server host value is management NIC private IP address of instance acting as vth-server. Instead of host domain name also can be used by replacing key host with fqdn-name.



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

Default ports are



##### Service Group List

Default service group list



Text

Description automatically generated

##### Virtual Server

1. Default of virtual server name is “vip”.
2. Vip address is generated dynamically.
3. After deploying arm template, in networking section You will get vip address, you will have to put that same vip address in this slb parameter file.
4. “ha-conn-mirror” does not work on port 80 and 443.

Steps to find VIP:

1. Login into azure
2. Go to the resource group which you have created
3. You will get all the resources, go to the first vthunder (virtual machine), for example suppose you have given name (in parameter file) of vthunder’s as vth-inst1, vth-inst2. So, you will get vip on vth-inst1.
4. Then go to the networking section -> 2nd interface -> IP configuration (drop-down menu) -> vip. Copy this vip and paste it on virtual server list ip-address (slb parameter file).

A screenshot of a computer

Description automatically generated with medium confidence Text

Description automatically generated

##### Note

1. Check ARM\_TMPL\_3NIC\_2VM\_HA\_SLB\_CONFIG\_PARAM.json file, vip is assigned dynamically so update in slb parameter file according to assigned value.
2. SLB script check management interface name presents in ARM PARAM file and using this name gets public IP of vthunder instance.

##### SSL Configuration

1. Default SSL configuration is disable.
2. You will get option to enable.
3. Default value of SSL certificate.

Text

Description automatically generated

For example:

*“sslConfig”: {*

*“requestTimeOut”: 40,*

*“Path”: “C:\Users\........\........\......\certs\sslcertificate.pem”,*

*“File”: “sslcertificate”,*

*“CertificationType”: “pem”*

*}*

1. Supported certification type .pem.

### Install

.\ARM\_TMPL\_3NIC\_2VM\_HA\_SLB\_CONFIG\_3.ps1

While running the SLB script user need to provide the correct password in the command prompt



## Chapter 4 - Configuring High Availability (HA)

### Configure Azure Access Key

Azure access key is required to access resources. To create the Azure access key, perform the following steps:

1. [Create a Role](#_Create_a_Role)
2. [Register a Service Application](#_Register_a_Service)
3. [Associate Service Application with a Role](#_Associate_Service_Application)
4. [Create Certificate and Secrets](#_Create_Certificate_and)
5. [Collect Azure Access Key](#_Collect_Azure_Access)
6. [Importing Azure Access Key](#_Importing_Azure_Access)

#### 1. Create a Role

To create a custom role, perform the following steps:

1. Navigate to the Home > Subscriptions > Registered Subscription Name > Access control (IAM) from left panel.

FIGURE 3-1: Subscriptions - Access control (IAM) window



1. On the Select Access control (IAM) page, select the Roles tab. The Role window is dis- played.

FIGURE 3-2: Access Control - Role Window



1. Click on the +Add tab and select Add custom role option. The Create a custom role window is displayed.

FIGURE 3-3: Add custom role window



1. Enter Customer role name and Description (optional).

FIGURE 3-4: Create a custom role window



1. Click on the **Next** button. The Permission window is displayed.

*FIGURE 3-5: Permission window*



1. Click on the **+Add Permissions** button to create a custom role.
2. Search for the permission to add the custom role.

For example, select **Microsoft Compute** from Add Permissions page.

*FIGURE 3-6: Add permission window*



The Microsoft Compute permission window is displayed.

*FIGURE 3-7: Microsoft Compute permissions window*



1. Select the **Permission** check box(es) and click **Add** button.
2. To add **Microsoft Network** from Add Permissions page, click on the **+Add Permissions**

on Create a custom role page.

*FIGURE 3-8: Create a custom role - Add permissions*



1. Search and select **Microsoft Network** from Add Permissions page.

*FIGURE 3-9: Add permissions - Microsoft Network page*



1. Select the **Permission** check box and click **Add** and **Review + create**.

*FIGURE 3-10: Microsoft Network permissions window*



The **Create a custom role** confirmation window is displayed.



1. Click OK to successfully create the custom role with permissions.

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

#### 2. Register a Service Application

To register a service application, perform the following steps:

1. Navigate to the Home > Services > Azure Active Directory option.

*FIGURE 3-11: Azure Active Directory page*



1. On the Azure Active Directory page, click on the App registrations menu option from the left panel. The App registration window to register an application is displayed.

*FIGURE 3-12: App registrations window*



1. Click on the **+New Registration** tab. The Register an application window is displayed.

*FIGURE 3-13: Register an application window*



1. Enter the **Name** of the application. For example, acos-sapp.
2. Click on the **Register** button to register the application. The application gets displayed in the list of Azure Active Directory - Apps registrations window.

#### 3. Associate Service Application with a Role

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

1. Navigate to the **Home** > **Subscriptions** > **Registered Subscription Name** > **Access control (IAM)**.

The Subscription > Access control (IAM) window is displayed.

*FIGURE 3-14: Subscription - Access control (IAM) window*



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

*FIGURE 3-15: Add a role assignment -1*



1. Select a **Role** from the drop-down list. For example, acos-role.
2. Select the **Assign Access to** option from the drop-down list.
3. Enter a string to search and select for a name or email address. For example, acos.
4. Click the **Save** button to save the configuration.

#### 4. Create Certificate and Secrets

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

1. Navigate to the **Home** > **Services** > **Azure Active Directory** option.

*FIGURE 3-16: Azure Active Directory - Overview page*



1. On the Azure Active Directory - Overview page, click on the App registrations menu option from the left panel. The App registration window with a registered application(s) is displayed.

*FIGURE 3-17: App registrations - Overall applications window*



1. Select a service application from list of applications. The selected service application window is displayed.
2. Select the **Certificates & secrets** option from the left Manage navigation pane. The acos sapp - Certificates & secrets window is displayed.
3. 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 3-18: Add a client secret window*



1. Enter the New client secret **Description**, **Expires** value. The entered value is displayed on the acos-Certificates & secrets window.

*FIGURE 3-19: acos-sapp Certificates & secrets window*



NOTE:

Copy the new client secret value, as it is not visible once the page is refreshed.

#### 5. Collect Azure Access Key

To collect Azure access keys, perform the following steps:

1. Navigate to the **Home** > **Azure Active Directory** - **App registrations**.

*FIGURE 3-20: App registrations - Azure Active Directory window*



1. Select service application from the list of applications. The selected service application page is displayed.

*FIGURE 3-21: Selected Service application window*



1. Copy the Client ID, Tenant ID from the service application page. client\_id= 'cc4c86xx-65b3-48xx-a3xx-610cxxxxxxxx’ tenant\_id= '91d27axx-8cxx-41xx-82xx-3d1bxxxxxxxx'
2. Navigate to the **Home** > **Subscriptions** > **Registered Subscription Name**, and copy subscription ID value.

*FIGURE 3-22: Subscriptions window*



1. Create a text file with as subscription, client\_id, client\_secret and tenant\_id 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’

#### 6. Import Azure Access Key

Each vThunder instance requires a copy of the Azure Access key. The recommended method of importing the Azure Access key by using any of the file transfer methods.

Perform the following steps.

1. Log into the vThunder instance.
2. Go to the config mode.

**vThunder>**enable

Password:

**vThunder#**config

1. Go to the admin mode.

**vThunder(config)#**admin ?

admin

NAME<length:1-31> System admin user name

**vThunder(config)#**admin admin

1. Import the Azure Access key by using any of the file transfer methods recommended.

**vThunder(config-admin:admin)#azure-cred import ?**

use-mgmt-port Use management port as source port

tftp: Remote file path of tftp: file system(Format: tftp://host/file) ftp: Remote file path of ftp: file system(Format: ftp://[user@]host[:port]/file)

scp: Remote file path of scp: file system(Format: scp://[user@]host/file)

sftp: Remote file path of sftp: file system(Format:

sftp://[user@]host/file)

To delete the key, use the command **Azure-cred delete**.

1. Verify the imported Azure Access keys by below mentioned commands:

vThunder-Active(config)(NOLICENSE)#admin ad vThunder-Active(config)(NOLICENSE)#admin admin

vThunder-Active(config-admin:admin)(NOLICENSE)#azure-cred import scp://user- name@<ip-addr>:/<file-path>/cred.txt

vThunder-Active(config-admin:admin)(NOLICENSE)#azure-cred sh vThunder-Active(config-admin:admin)(NOLICENSE)#azure-cred show SUB\_ID = '07d34bxx-61xx-47xx-abxx-006bxxxxxxxx'

client\_id = 'cc4c86xx-65xx-48xx-a3xx-610cxxxxxxxx’

secret = 'G0x\_hVDzZxxxx-o1Vsw.xxxx.Zxxxx-xx'

tenant = '91d2xxxx-8xxe-41xx-82xx-3d1bxxxxxxxx’

vThunder-Active(config-admin:admin)(NOLICENSE)#

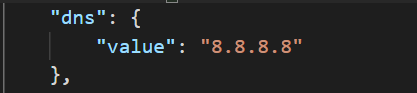
### Configure

Refer ARM\_TMPL\_3NIC\_2VM\_HA\_CONFIG\_PARAM.json file to customize default values.

Please find below in details.

##### DNS

Default value is google dns address.



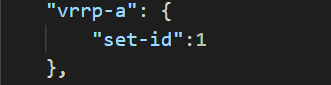
##### Network Gateway IP

Default value of network gateway IP address is 10.0.1.1 since this is first IP address of default management subnet configuration.



##### Vrrp

Default value of set id is 1



##### Terminal Idle Timeout

Default value for idle timeout is 0

Text

Description automatically generated

##### Vrid

1. Default value of vrid is 0
2. Default priority for vThunder-1 is is 100, and vThunder-2 will have 99 (100-1) priority.
3. FIP value generated dynamically in ARM template, so after creating ARM 3nic template You should have to enter same FIP in HA parameter file.

Steps to find fIP:

1. *Login into azure*
2. *Go to the resource group which you have created*
3. *You will get all the resources, go to the first vthunder (virtual machine), for example suppose you have given name (in parameter file) of vthunders as vth-inst1, vth-inst2. So, you will get fip on vthunder1.*
4. *Then go to the networking section -> 3rd interface -> IP configuration (drop-down menu) -> fip. Copy this fip and paste it on HA param file under the floating-ip as you can see in below image.*



### Install

1. [Import Azure Access Key.](#_Configure_Azure_Access)

Import Azure access key on both the vthunder

1. Run command to configure both VM in HA mode

.\ARM\_TMPL\_3NIC\_2VM\_HA\_CONFIG\_4.ps1

While running the HA script user need to provide the correct password in the command prompt



## Chapter 4 - Let us Verify.

### Login to vThunder

vThunder can be access by ssh to instance or GUI.

SSH to vThunder Instance:

Open putty and connect.

IP: Get from Azure Console -> Virtual Machine scale sets -> vth-vmss -> Select Instance -> public IP.

User Id [Default]: admin

Password [Default]: a10

After login.

Execute Command -> enable

Password -> <just press enter>

Text

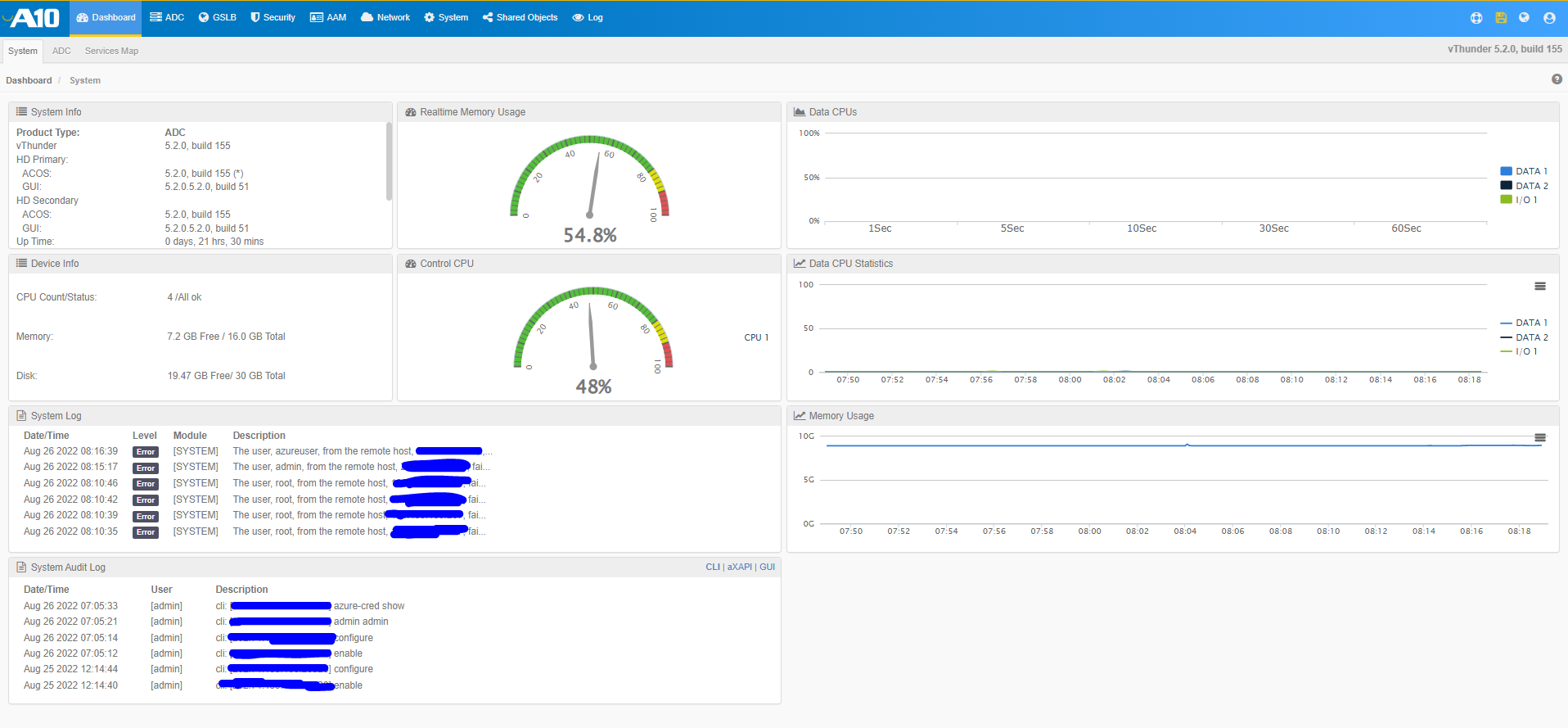
Description automatically generated

### vThunder GUI Verification

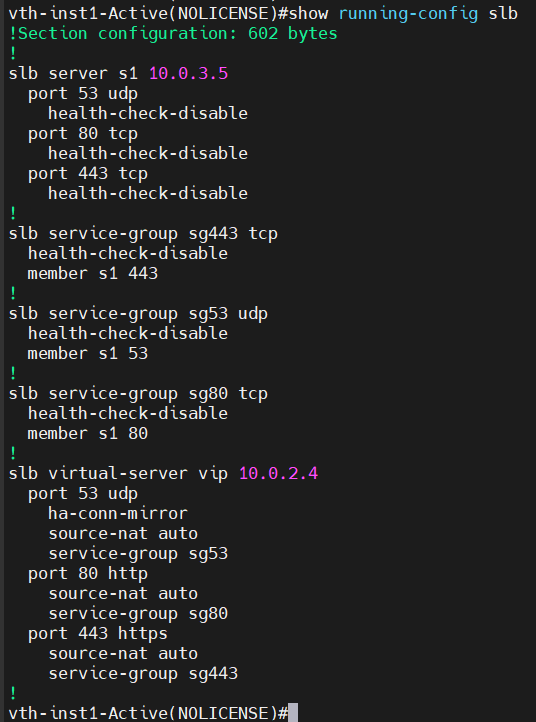
GUI: Check below vThunder GUI

Web URL: http://IP

<https://ip/gui/auth/login/>



### SLB Verification



### SSL Certificate Verification

****

### HA Verification

