

A10

Installing vThunder on Microsoft Azure

September, 2023

© 2023 A10 Networks, Inc. All rights reserved.

Information in this document is subject to change without notice.

PATENT PROTECTION

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

[a10-virtual-patent-marking](#).

TRADEMARKS

A10 Networks, Inc. trademarks are listed at: [a10-trademarks](#)

CONFIDENTIALITY

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

DISCLAIMER

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

ENVIRONMENTAL CONSIDERATIONS

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

FURTHER INFORMATION

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

Table of Contents

Introduction to Installing vThunder on Microsoft Azure	1
Overview of Microsoft Azure	2
Azure Terminology	3
System Requirements	4
Global License Manager and Types of vThunder Licenses	5
Interfaces	7
Feature Support	8
Limitations	9
Installing vThunder on Microsoft Azure	11
Prerequisites for Installing vThunder	12
List of Available Azure Images for vThunder	12
Create a Single-Interface vThunder Instance	13
Create a Multiple-Interface vThunder Instance	25
Creating Multiple-Interface vThunder Instance Using Azure Portal	25
Creating Multiple-Interface vThunder Instance Using Azure PowerShell	28
About Multiple IP Addresses for a Network Interface	34
Associating Public IP and Secondary IP address by Using Azure Portal	34
Adding a Public IP Address to a NIC Using Azure CLI	37
Adding a Secondary IP Address to a NIC by Using Azure CLI	37
Access vThunder by Using ACOS CLI	38
Configure Endpoint Mapping	39
Access vThunder by Using ACOS GUI	40
Microsoft Azure High Availability	42
Creating Azure Access Key	42
Create a Role	42
Register a Service Application	48
Associate Service Application with a Role	50
Create Certificate and Secrets	52

Collect Azure Access Key	54
Importing Azure Access Key	56
Azure HA Architecture	57
Configuring HA	59
Initial vThunder Configuration	67
Configuring DHCP and the VIP in vThunder	68
Changing the VM Size	68
Changing the Disk Size	68
Adding More NICs by Using the Azure CLI	69
Deleting NICs by Using the Azure CLI	69
Initial vThunder Configuration	70
Login via ACOS CLI	70
Changing the Admin Password	71
Saving the Configuration Changes – write memory	71
Additional Resources – Where to go from here?	71
Configuring One Arm Mode SLB vThunder on Azure	72
ACOS Code for Single-Interface SLB	72
Configuring a Multiple-Interface vThunder on Azure as an SLB	73
ACOS Code for Multiple-Interface SLB	74
Advanced vThunder Configuration on Microsoft Azure	76
About Shared Polling Mode	77
Enabling Shared Polling Mode	78
Disabling Shared Polling Mode	79
About Jumbo Frames	80
Enabling Jumbo Frames for vThunder	80
Memory Support	81
vThunder Configuration on SLB or CGN	81
Configure Thunder Observability Agent	85
Internal Thunder Observability Agent (iTOA)	85
External Thunder Observability Agent (TOA)	86

Introduction to Installing vThunder on Microsoft Azure

vThunder for Microsoft Azure is a fully operational, software-only version of the ACOS Series Server Load Balancer (SLB), or 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 hardware 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.

The following topics are covered:

Overview of Microsoft Azure	2
Azure Terminology	3
System Requirements	4
Global License Manager and Types of vThunder Licenses	5
Interfaces	7
Feature Support	8
Limitations	9

Overview of Microsoft Azure

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-service (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 centers and is globally distributed 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 services, such as Bing, Skype, Xbox, and Office 365.

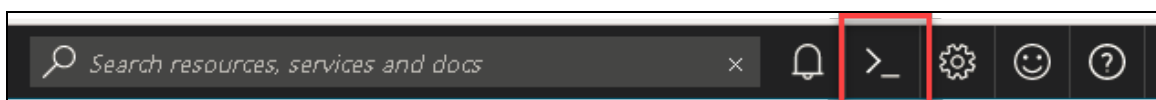
A10 Networks vThunder virtual device can be set up as an instance in Azure's cloud and can be used to provide a robust server load balancing (SLB) service.

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>.

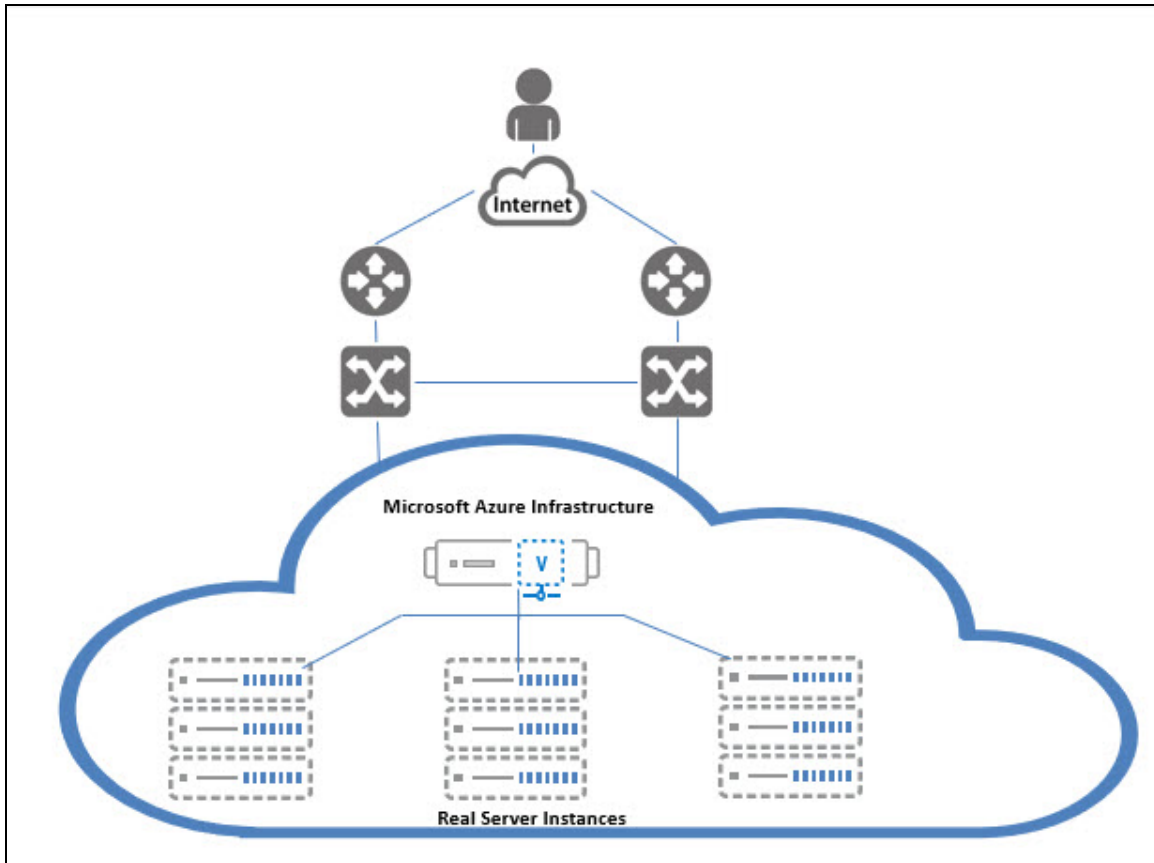
You can launch Cloud Shell from the top navigation bar of the Azure portal.

Figure 1 : Launching Cloud Shell



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

Figure 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>.

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

System Requirements

The following VM sizes are supported:

Table 1 : Verified VM sizes

Series	Size
A series	Standard/Basic A2
	Standard A2_v2
	Standard A2m_v2
	Standard A4_v2
	Standard A4m_v2
	Standard/Basic A3

Table 1 : Verified VM sizes

Series	Size
	Standard/Basic A4 Standard A8_v2
B series	Standard B2_s Standard B2ms Standard B4ms
D series	Standard D2_v2 Standard D2s_v3 Standard D4_v3 Standard D4s_v3 Standard D3_v2 Standard Ds3_v2 Standard D5_v2
F series	Standard F4s Standard F8 Standard F16s

For more information, see <https://docs.microsoft.com/en-us/azure/virtual-machines/sizes-general>.

Global License Manager and Types of vThunder Licenses

The GLM is the master licensing system for A10 Networks. The GLM is managed by A10 Networks and is the primary portal for license management for A10 products. The GLM provides a GUI where you can view and manage advanced licensing functions. Creating a GLM account is optional. You can use the ACOS CLI or GUI to license the ACOS devices. A GLM account enables you to perform advanced licensing functions and, where applicable, view, and monitor device usage. The GLM portal is

available at <https://glm.a10networks.com>. If you do not yet have a GLM account, contact sales@a10networks.com.

vThunder requires a license. Without a license, the product cannot run production traffic, and the amount of bandwidth is only sufficient for testing network connectivity. After downloading and installing the vThunder software on Microsoft Azure Cloud, a vThunder license is needed to pass live traffic.

A10 Networks offers different types of licenses for the vThunder instance. vThunder supports the following licensing models:

- **Trial license**—Create a trial license in the ACOS GUI.
For more information, refer to the [Global License Manager User Guide](#).
- **Perpetual license**—This licensing model is based on bandwidth. It is obtained by activation key license for your A10 virtual appliance, URL Classification License installation, and GLM account management. All licenses are generated and installed manually. For more information, refer to the [Global License Manager User Guide; chapter Obtaining your Activation Key License](#).
- **Pay As You Go (PAYG) license**—This licensing model is subscription-based. There are two types of licensing models under PAYG licenses. Both these licensing models require that the vThunder instance has internet access to request the licenses from an A10 license server. The license models are as follows:
 - The **Rental Billing Model (RBM)** is designed for cloud service providers (CSPs) who offer Advanced Delivery Controller (ADC) services. This model enables such providers to bill their customers for a fixed amount of bandwidth, as well as adding surcharges for extra bandwidth consumed.
 - The **Utility Billing Model (UBM)** is based on actual data usage, in bytes, in which unlimited vThunder instances can be deployed and in which no bandwidth settings are required. For more information, refer to the [vThunder Pay-as-you-Go License](#).
- **Capacity Pool (FlexPool) license**—This licensing model enables you to subscribe to a specific bandwidth pool in the Global License Manager (GLM) for a specific time period, with an additional option of automatically renewing your license before the license expiry date. Unlike previous license models supported by A10 Networks, capacity pool (FlexPool) license is not node-locked. You can configure multiple ACOS devices to share bandwidth from the common license pool. For more information, refer to the [Capacity Pool License User Guide](#).

NOTE: When a vThunder license has expired, vThunder functionality continues with reduced bandwidth.

To view any of the above license types, its features, and how to activate follow the following steps:

1. Sign In to *Global License Manager* through <https://documentation.a10networks.com/signin.html> page.
2. Enter your valid A10 **Email, Password**, and then click **Sign In** tab. The A10 product documentation page is displayed.
3. On the *A10 Products* page, go to **Installation Guides for Form Factors** section. Choose the product.
4. Click the **View** tab. The Software Installation Guides page is displayed. (i.e. https://documentation.a10networks.com/Install/Software/A10_ACOS/Install/index.html).
5. Click the **View Licensing Guides** option. The portal displays the *Licensing User Guide* section.
6. Click **Download PDF** tab to open the appropriate Global License Manager guide.

Interfaces

Starting from ACOS 4.1.4 GR1 multi NIC vThunder deployment on Azure Cloud is supported. The number of interfaces that can be created is dependent on the VM size provided by Azure. For more information on different VM sizes and the number of NICs supported for each VM size, see <https://docs.microsoft.com/en-us/azure/virtual-machines/linux/sizes>.

NOTE: From 4.1.4-P3 version onwards, single NIC deployments for the vThunder on Azure Cloud are not supported.

[Create a Single-Interface vThunder Instance](#) in the Azure portal. After an instance or VM is created, use the Azure portal to add more interfaces to the VM. Additionally, use the Azure Power Shell or the Azure CLI to create a multiple-interface VM.

The following operations are supported for multiple NICs:

- The Azure portal can be used to instantiate a vThunder instance, which supports four NICs, but if there is only two NICs are created, then you can add two more NICs before shutting down the instance and use the Power Shell or Azure CLI to add the remaining NICs. For more information, refer to [Adding More NICs by Using the Azure CLI](#).
- The Azure portal can be used to instantiate an instance, which supports only two NICs, and you want to add more NICs, then users first shut-down the instance and change the VM size from within the Azure Portal, as described in [Changing the VM Size](#). After that, repeat the steps in [Adding More NICs by Using the Azure CLI](#).
- The Azure portal can be used to instantiate an instance with multiple NICs, then shut down the VM and delete NICs as described in [Deleting NICs by Using the Azure CLI](#).

NOTE: Users cannot delete all the NICs from a VM.

In the example in [Create a Multiple-Interface vThunder Instance](#), a vThunder instance is created with the following interfaces, each interface is associated with a different subnet:

- Management – Dedicated management interface
- Ethernet 1 – Data interface
- Ethernet 2 – Data interface

In a typical deployment, one of the data interfaces is connected to the server farm, and the other data interface is connected to the clients. However, one-arm deployment is also supported which requires one data port and one management port. You also can add additional data interfaces as needed.

Feature Support

vThunder for Azure supports many of the same features as the Thunder Series hardware-based models, but the exact set of supported features varies based on whether vThunder is running as an ADC, CFW, or as an SSLi solution.

Refer to the [vThunder Software for Virtual and Cloud Infrastructure Data Sheet](#) for a complete summary of supported features.

Limitations

The following limitations that user can encounter, while using vThunder for Azure:

- It is recommended to configure “ip address DHCP” before performing other configurations because there is no predefined DHCP in the start-up config file.

See [Configuring DHCP and the VIP in vThunder](#) for details.

- LACP and Static trunk groups are not supported on Azure Cloud.
- Port Mirror is not supported.
- vThunder for Azure does not support L3V partition and service partition.
- RIP (v1 and v2), OSPF, and ISIS routing protocols are not supported.
- VLAN, Tagged VLAN, and Virtual Ethernet (VE) interfaces are not supported.
- Layer 2 Switching (VLAN) is not supported.
- Layer 2 deployment is not supported.
- The Azure extensions are not supported.
- Bridge Protocol Data Unit (BPDU) Forward Group is not supported.
- When using vThunder for Azure and SLB, a VPN tunnel (IPsec) cannot be brought up if an SLB virtual server is also enabled. This limitation is because vThunder for Azure only has one data interface for ACOS releases before 4.1.4 version.

As a workaround, create loopback interfaces and use the interfaces as VPN gateway IP addresses. Then SLB and IPsec can be up at the same time. Add Azure Route Tables or User Defined Routing (UDR) on the Azure portal for the loop-back interface IP addresses to be accessible for each other.

- If the endpoint port number in the Azure portal is changed, then make sure to clear the Internet browser's cache before attempting to navigate to the vThunder GUI. If not cleared, the browser uses the previously saved public port and fails to access the vThunder GUI.
- System promiscuous mode is not supported by Microsoft Azure.

- At the interface Ethernet config level, the following commands are disabled:
 - `mtu`
 - `trunk-group` (command exists, but the function is disabled)
 - `device-context`
 - `duplexity`
 - `flow-control`
 - `monitor`
 - `speed`
 - `use-if-ip`
- The reload command causes kernel panic on Azure due to the limitation imposed by DPDK Netvsc PMD. Use the reboot command whenever reload is required. For information about the limitation, see https://doc.dpdk.org/guides/rel_notes/known_issues.html#netvsc-driver-and-application-restart.
- The maximum binding limitations are as follows:
 - For vTPS 3.2.x and 5.0.x, maximum vCPU is 48.
 - For ACOS 5.2.1-Px, maximum vCPU is 96.
- When using the serial console on the Azure portal, it is recommended to use a non-zero value for the terminal length. Printing a large amount of output on the serial console at once can result in a high CPU load and cause the system unstable. Especially, if you want to execute the `show tech` command on the serial console, use the `show tech page` command with terminal length non-zero value on the serial console.

Installing vThunder on Microsoft Azure

This chapter describes how to install vThunder on Microsoft Azure.

The following topics are covered:

Prerequisites for Installing vThunder	12
Create a Single-Interface vThunder Instance	13
Create a Multiple-Interface vThunder Instance	25
About Multiple IP Addresses for a Network Interface	34
Access vThunder by Using ACOS CLI	38
Configure Endpoint Mapping	39
Access vThunder by Using ACOS GUI	40

Prerequisites for Installing vThunder

Before installing vThunder, set up an account with Microsoft Azure or use your MSDN credentials, or use a free trial account from the following location:

<http://azure.microsoft.com/en-us/pricing/free-trial/>

List of Available Azure Images for vThunder

The following is the list of images available for vThunder:

Table 2 : Some vThunder SKUs

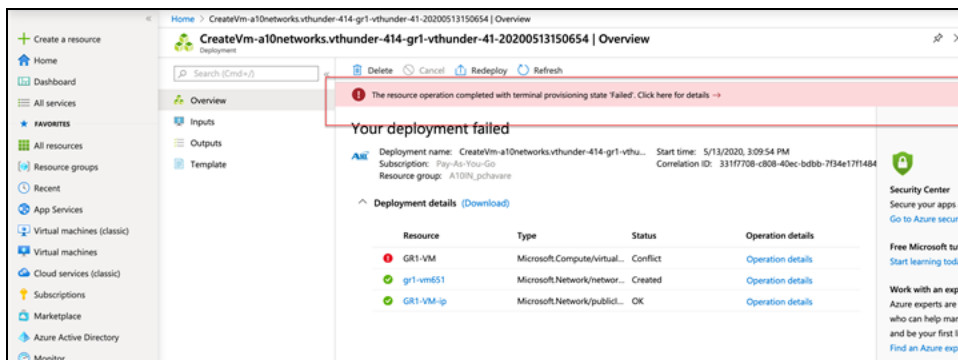
SKUs	Offer	Publisher Name	Location
vthunder_100mbps	a10-vthunder- adc	a10networks	eastus
vthunder_10mbps	a10-vthunder- adc	a10networks	eastus
vthunder_200mbps	a10-vthunder- adc	a10networks	eastus
vthunder_410_100mbps	a10-vthunder- adc	a10networks	eastus
vthunder_410_500mbps	a10-vthunder- adc	a10networks	eastus
vthunder_410_byol	a10-vthunder- adc	a10networks	eastus
vthunder_500mbps	a10-vthunder- adc	a10networks	eastus
vthunder_50mbps	a10-vthunder- adc	a10networks	eastus
vthunder_byol	a10-vthunder- adc	a10networks	eastus

For more information, contact sales@a10networks.com.

Create a Single-Interface vThunder Instance

From ACOS 4.1.4-P3 version onwards, single NIC deployments for the vThunder on Azure Cloud are not supported. If the user deploys ACOS 4.1.4-P3 or higher ACOS version for single NIC deployment for vThunder, then an error “Your deployment failed” message is displayed.

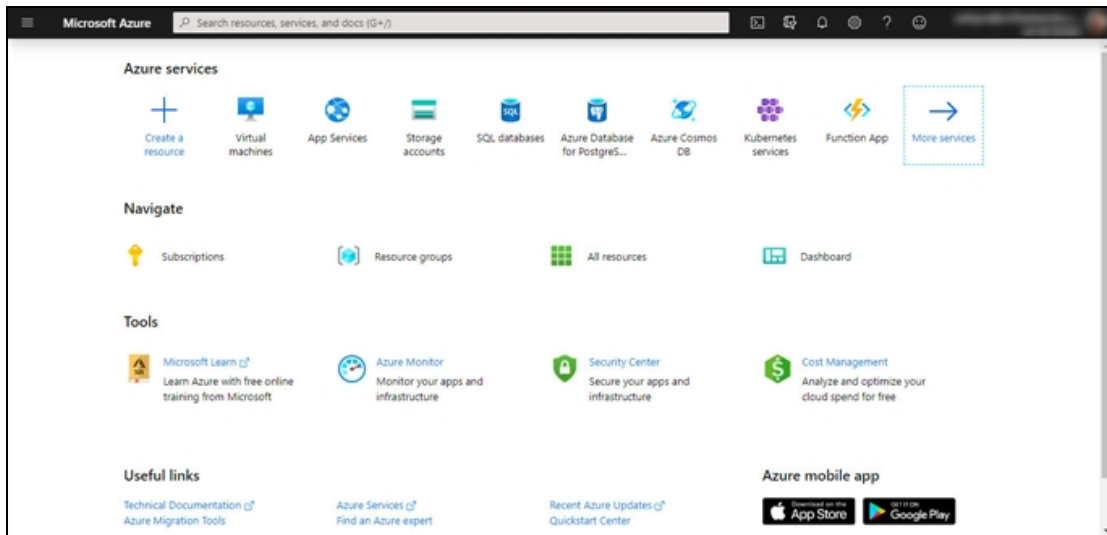
Figure 3 : Error Message



To create a single interface vThunder instance with the ACOS version that is below to ACOS 4.1.4-P3 version, perform the following steps:

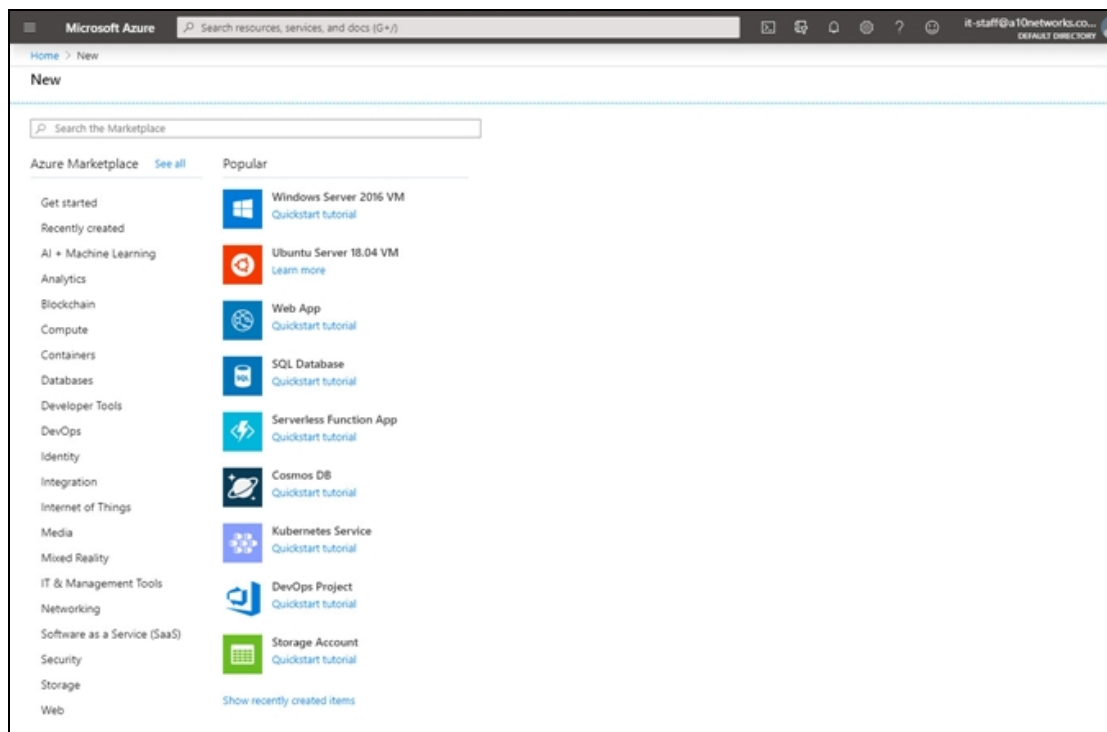
1. Navigate to <https://portal.azure.com>.
The **Microsoft Azure - Services** window is displayed.

Figure 4 : Microsoft Azure - Services window



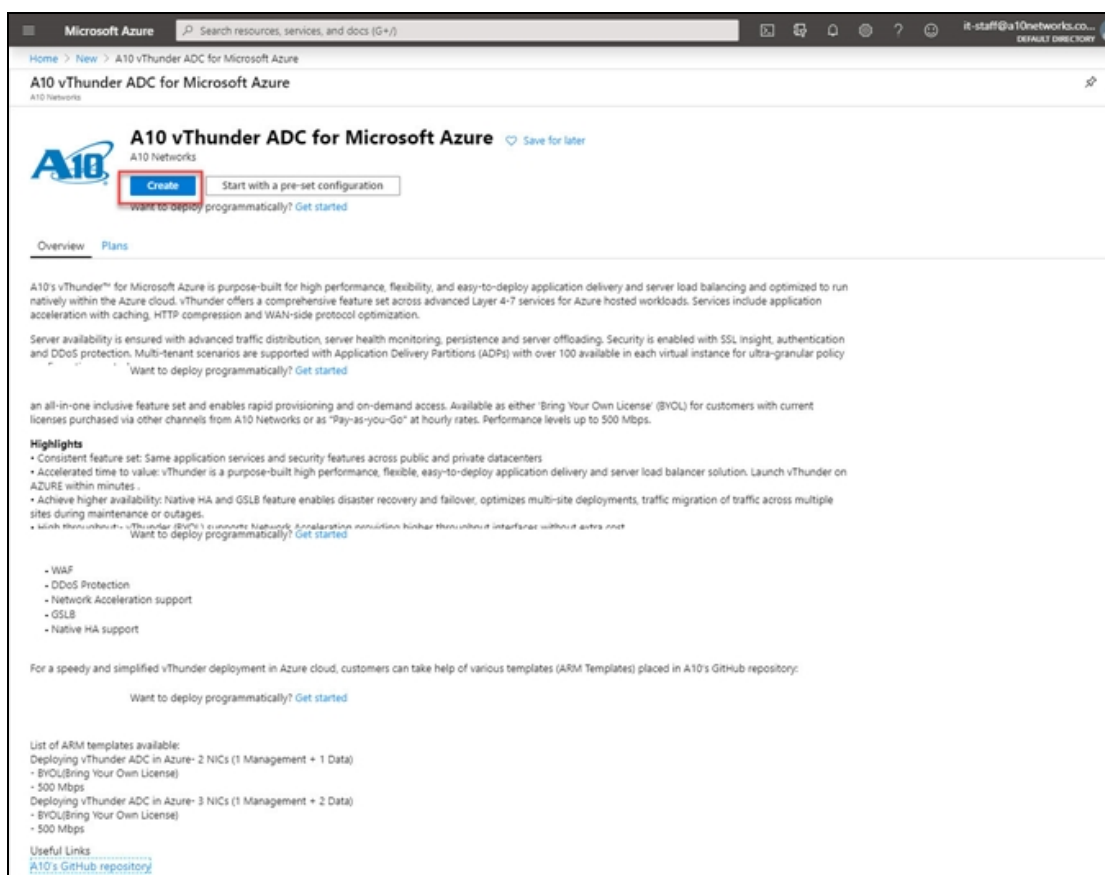
2. Click **Create a resource** from the Microsoft Azure Services menu options. The **New** window with **Search the Marketplace** text box is displayed.

Figure 5 : New window



3. Enter the search string **A10 Networks** and press **Enter**.
The search displays several types of images that can be grouped into two types: BYOL and fixed throughput images. As the name suggests, for BYOL images, you must contact A10 Networks Sales for the license you require. For fixed throughput images, the license is preinstalled.
4. Select the A10 Networks image that you require. For example, A10 vThunder ADC for Microsoft Azure.
The selected image window is displayed.

Figure 6 : A10 vThunder ADC for Microsoft Azure window

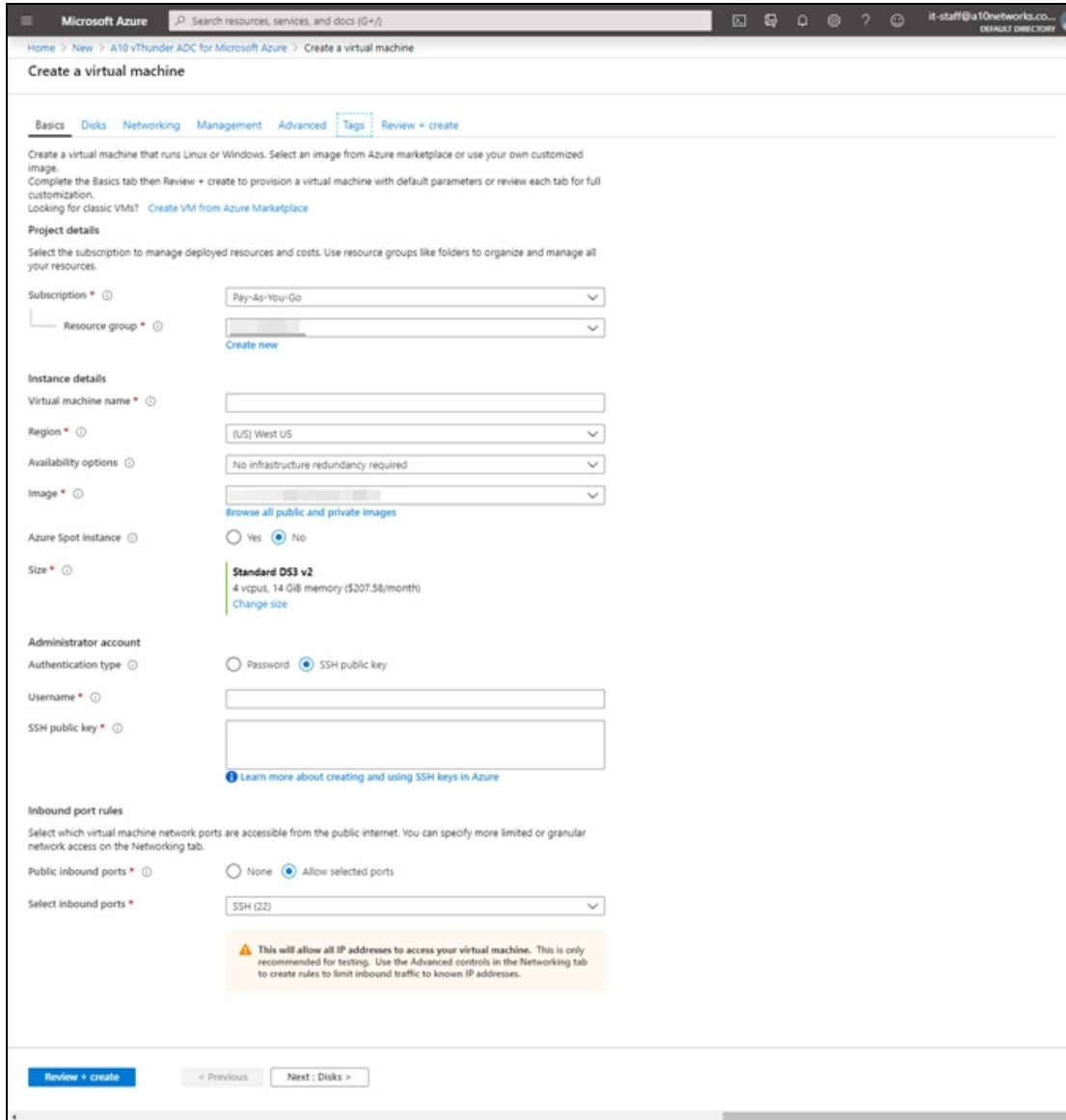


NOTE: Azure supports two types of deployment: Classic and Resource Manager. Classic is a legacy deployment model and is not currently support.

5. Click **Create**.

The **Create virtual machine** work-flow tabs are displayed.

Figure 7 : Create a virtual machine window



The screenshot shows the 'Create a virtual machine' page in the Microsoft Azure portal. The 'Basics' tab is active, and the 'Review + create' button is highlighted. The form includes the following sections:

- Project details:** Subscription (Pay-As-You-Go), Resource group (Create new).
- Instance details:** Virtual machine name, Region (US West US), Availability options (No infrastructure redundancy required), Image (Browse all public and private images), Azure Spot instance (No), Size (Standard D53 v2, 4 vcpus, 14 GiB memory).
- Administrator account:** Authentication type (SSH public key), Username, SSH public key.
- Inbound port rules:** Public inbound ports (Allow selected ports), Select inbound ports (SSH (22)).

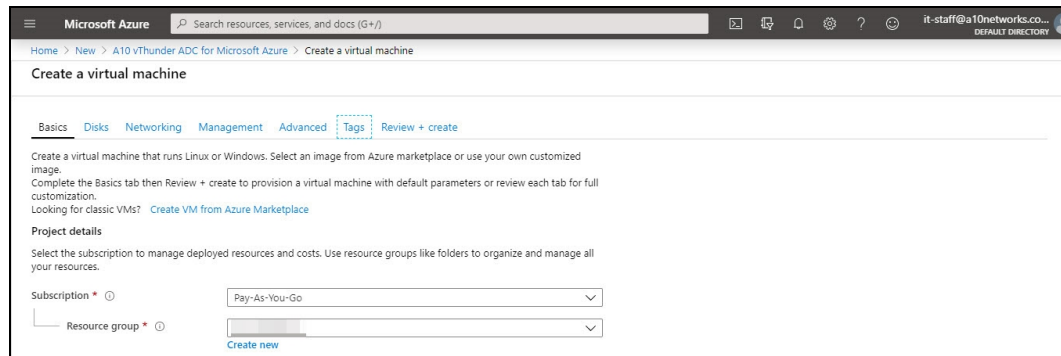
A warning message at the bottom states: "This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses."

6. Click the **Basics** tab. The Basic window is displayed.

In the **Basic** window, enter the following:

- a. Under the Project details section, select the correct **Subscription** and **Resource group**, or choose to **Create new** resource group.

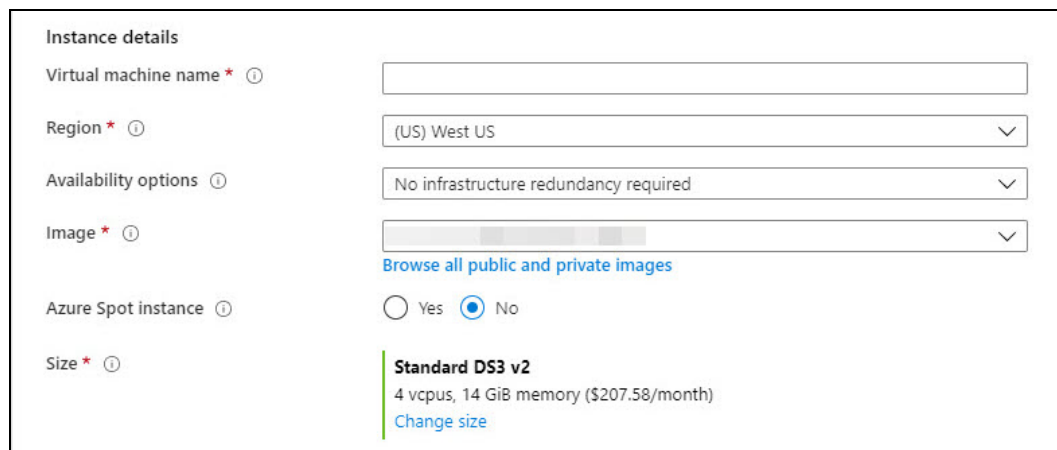
Figure 8 : Basics window- Project details



NOTE: A resource group is a container that holds related resources for an Azure solution.

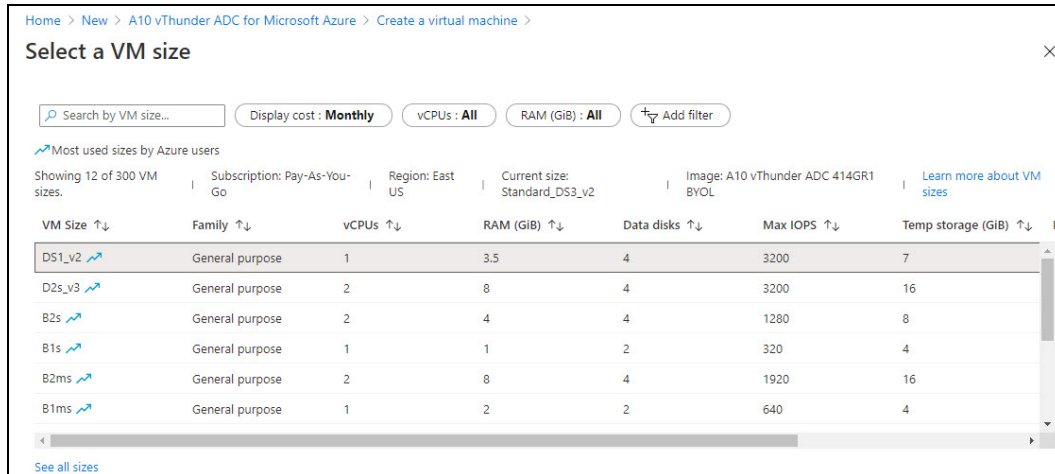
- b. In the Instance details section, enter the **Virtual machine name**, select the **Region**, and choose the A10 vThunder **Image** from drop-down list.

Figure 9 : Basic window- Instance details



- c. Click **Change Size** to select Size of virtual Machine and their features as below:

Figure 10 : Selecting a VM Size



Home > New > A10 vThunder ADC for Microsoft Azure > Create a virtual machine >

Select a VM size

Search by VM size... | Display cost: **Monthly** | vCPUs: **All** | RAM (GiB): **All** | Add filter

Most used sizes by Azure users

Showing 12 of 300 VM sizes. | Subscription: Pay-As-You-Go | Region: East US | Current size: Standard_DS3_v2 | Image: A10 vThunder ADC 414GR1 BYOL | [Learn more about VM sizes](#)

VM Size ↑↓	Family ↑↓	vCPUs ↑↓	RAM (GiB) ↑↓	Data disks ↑↓	Max IOPS ↑↓	Temp storage (GiB) ↑↓
DS1_v2 ↗	General purpose	1	3.5	4	3200	7
D2s_v3 ↗	General purpose	2	8	4	3200	16
B2s ↗	General purpose	2	4	4	1280	8
B1s ↗	General purpose	1	1	2	320	4
B2ms ↗	General purpose	2	8	4	1920	16
B1ms ↗	General purpose	1	2	2	640	4

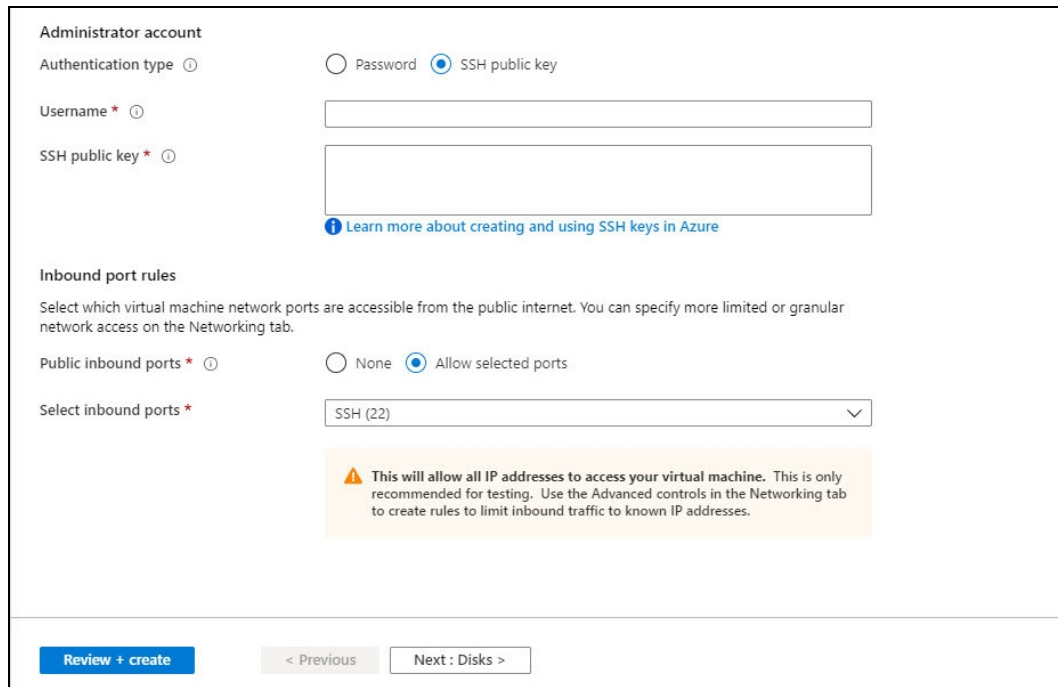
[See all sizes](#)

- In the **Select a VM size** window, select any one of the recommended options, and click **Select** button.

NOTE: Each pane displays a combination of Family, vCPUs, RAM size, data disks, IOPS value, and so on. By default, the size is set to **Standard DS1 v2**.

- d. In the Administrator Account details section, the Authentication type is Password or SSH public key.

Figure 11 : Basic details - Administrator account and Inbound port rules



- e. Select the **SSH Public Key** radio button to enter and Username and the SSH public key.
or
Select the **Password** radio button to enter Username and Password. The entered password must have 12 characters, one lower case, one upper case, a digit, and one special character.

NOTE: Re-entered password must match to the entered Password.

- f. In the **Inbound port rules > Public inbound ports**, choose **Allow selected ports** radio button and then select SSH (22) and HTTP (80) from the drop-down list.

You can leave the remaining as defaults and select the **Review + create** button at the bottom of the page or, perform the following:

7. Click the **Disks** tab. The Disk option window is displayed.



Figure 12 : Disk window

Create a virtual machine


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

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

Disk options

OS disk type *  Standard HDD 

The selected VM size supports premium disks. We recommend Premium SSD for high IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.


Enable Ultra Disk compatibility  Yes No

Ultra Disk compatibility is not available for this VM size and location.

Data disks

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching
Create and attach a new disk Attach an existing disk				


 **Advanced**

- In Disk option, select OS disk type from the available list of options. Leave the remaining as defaults.
- Click the **Tag** tab. The Tag window is displayed.




Figure 13 : Tag window

Create a virtual machine

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

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn more about tags](#) 

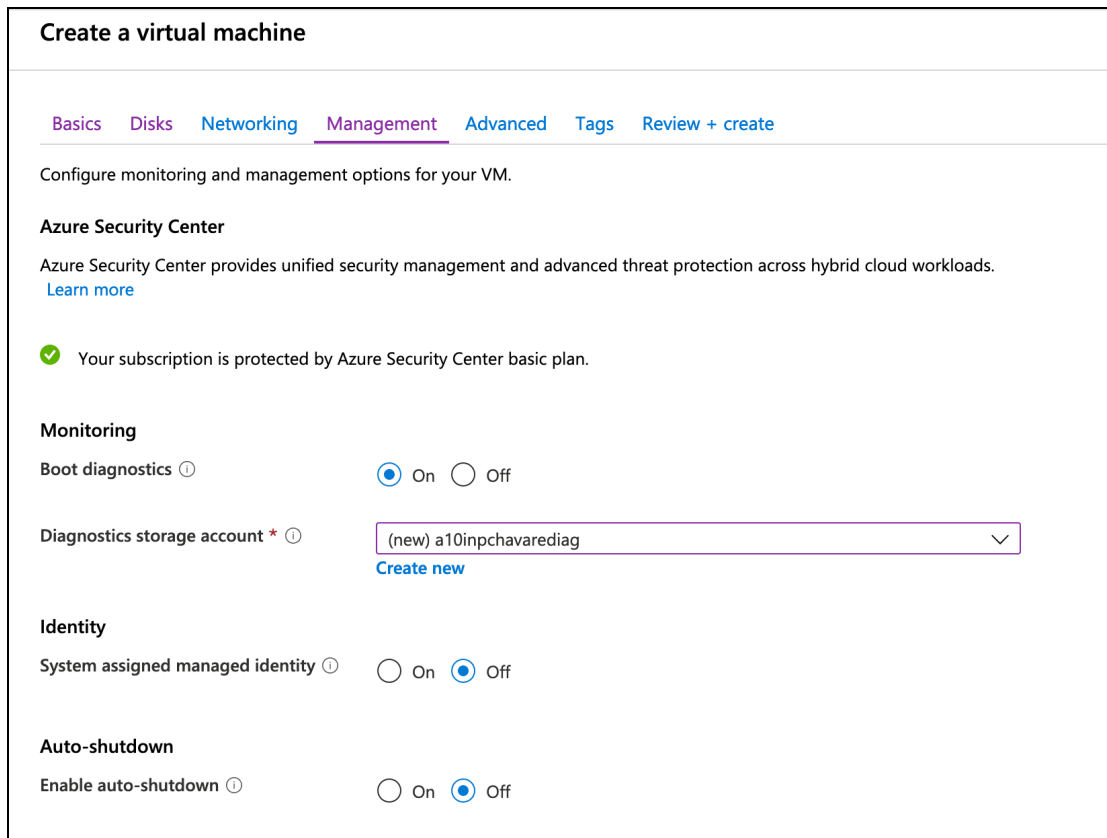
Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name 	Value 	Resource
<input type="text"/>	: <input type="text"/>	11 selected 

Tags enable you to categorize resources and view consolidated billing for paired with name or values.

10. Click the **Management** tab to configure monitoring and management options for your VM.

Figure 14 : Management window



Create a virtual machine

Basics Disks Networking **Management** Advanced Tags Review + create

Configure monitoring and management options for your VM.

Azure Security Center
Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads.
[Learn more](#)

✔ Your subscription is protected by Azure Security Center basic plan.

Monitoring

Boot diagnostics ⓘ On Off

Diagnostics storage account * ⓘ [Create new](#)

Identity

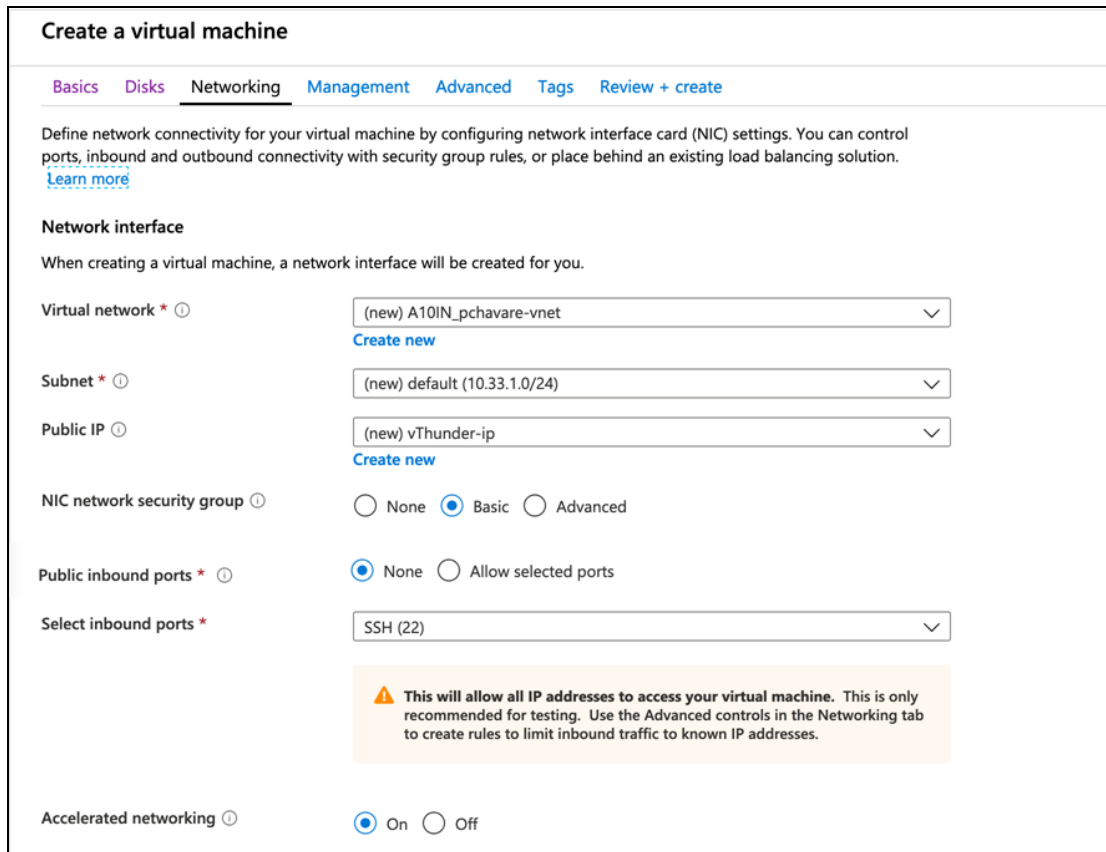
System assigned managed identity ⓘ On Off

Auto-shutdown

Enable auto-shutdown ⓘ On Off

11. Click the **Network** tab. The Network window is displayed.

Figure 15 : Network window



Create a virtual machine

Basics Disks **Networking** Management Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more](#)

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * [Create new](#)

Subnet * [Create new](#)

Public IP [Create new](#)

NIC network security group None Basic Advanced

Public inbound ports * None Allow selected ports

Select inbound ports *

⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Accelerated networking On Off

12. Select **Virtual Network**, **Subnet**, NIC network security group.

NOTE: To create a new virtual network, Subscription, resource group, name, and location must be selected to select a virtual network.

13. Select the Public inbound ports as **None**.
14. **Select inbound ports** from a list of options.
15. Click the **Advance** tab to add additional details about **Cloud-init** or **Host**.

For provisioning the vThunder instance, edit the following cloud-init configuration as appropriate, copy the configuration, and paste it in the blank field:

```
a10_blob: |
  !TEST
```

```
ip dns pri 8.8.8.8
glm use-mgmt-port
glm token vThxxxxxxxxxx
glm enable-requests
glm send license-request
wr mem
```

Figure 16 : Advance window

Create a virtual machine

Basics Disks Networking Management Monitoring **Advanced** Tags Review + create

Add additional configuration, agents, scripts or applications via virtual machine extensions or cloud-init.

Extensions

Extensions provide post-deployment configuration and automation.

Extensions [Select an extension to install](#)

VM applications

VM applications contain application files that are securely and reliably downloaded on your VM after deployment. In addition to the application files, an install and uninstall script are included in the application. You can easily add or remove applications on your VM after create. [Learn more](#)

[Select a VM application to install](#)

Custom data and cloud init

Pass a cloud-init script, configuration file, or other data into the virtual machine **while it is being provisioned**. The data will be saved on the VM in a known location. [Learn more about custom data for VMs](#)

Custom data

```
a10_blob: |
ITEST
ip dns pri 8.8.8.8
glm use-mgmt-port
glm token vTh
glm enable-requests
glm send license-request
```

i Custom data on the selected image will be processed by cloud-init. [Learn more about custom data for VMs](#)

User data

Pass a script, configuration file, or other data that will be accessible to your applications **throughout the lifetime of the virtual machine**. Don't use user data for storing your secrets or passwords. [Learn more about user data for VMs](#)

Enable user data

Performance (NVMe)

Enable capabilities to enhance the performance of your resources.

Higher remote disk storage performance with NVMe

i The selected size is not supported for NVMe. [See supported size families](#)

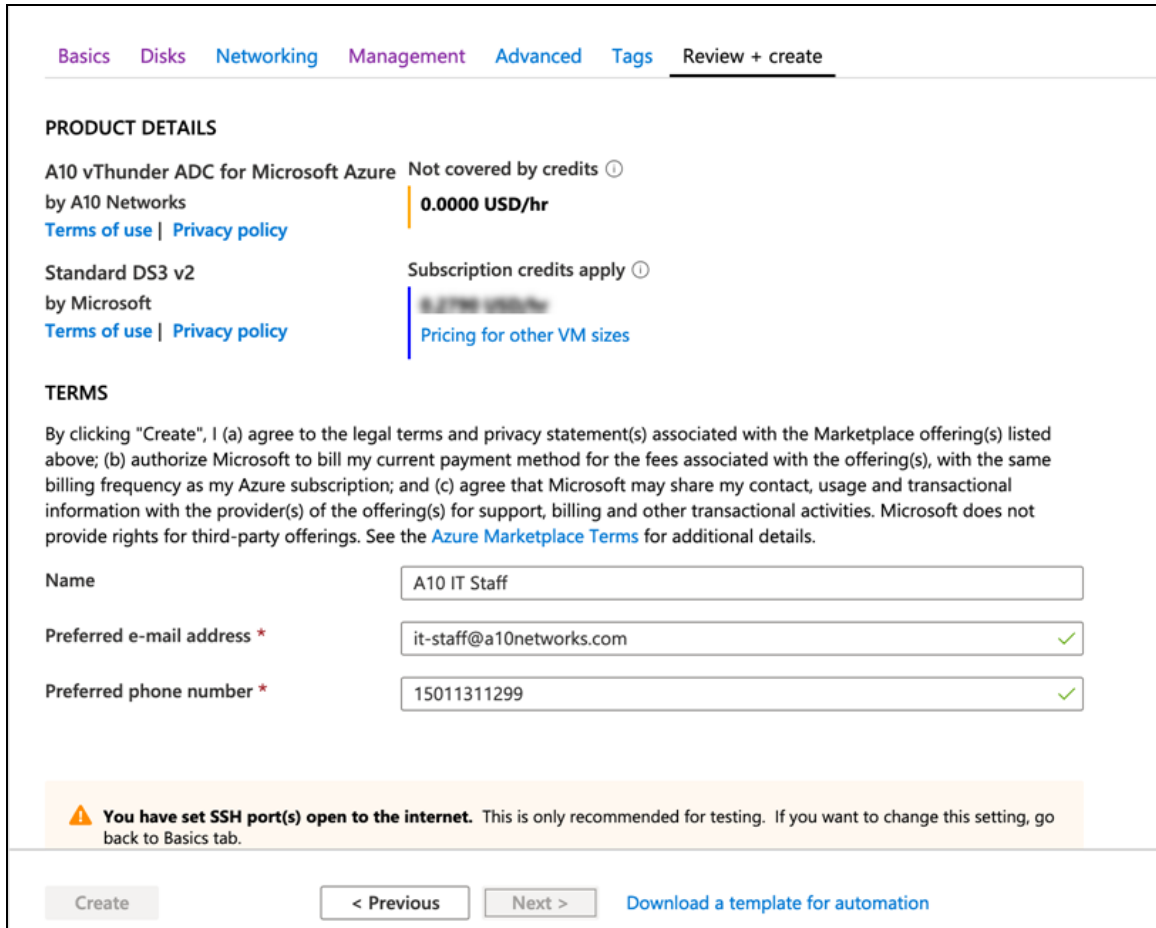
Host

Azure Dedicated Hosts allow you to provision and manage a physical server within our data centers that are dedicated to your Azure subscription. A dedicated host gives you assurance that only VMs from your subscription are on the host, flexibility to choose VMs from your subscription that will be provisioned on the host, and the control of platform maintenance at the level of the host. [Learn more](#)

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

- Click the **Review + Create** tab to view the **Product details, Terms** of use with user details.

Figure 17 : Review + create window



Basics Disks Networking Management Advanced Tags **Review + create**

PRODUCT DETAILS

A10 vThunder ADC for Microsoft Azure Not covered by credits ⓘ
 by A10 Networks **0.0000 USD/hr**
[Terms of use](#) | [Privacy policy](#)

Standard DS3 v2 Subscription credits apply ⓘ
 by Microsoft **0.0000 USD/hr**
[Terms of use](#) | [Privacy policy](#) [Pricing for other VM sizes](#)

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

Name

Preferred e-mail address * ✓

Preferred phone number * ✓

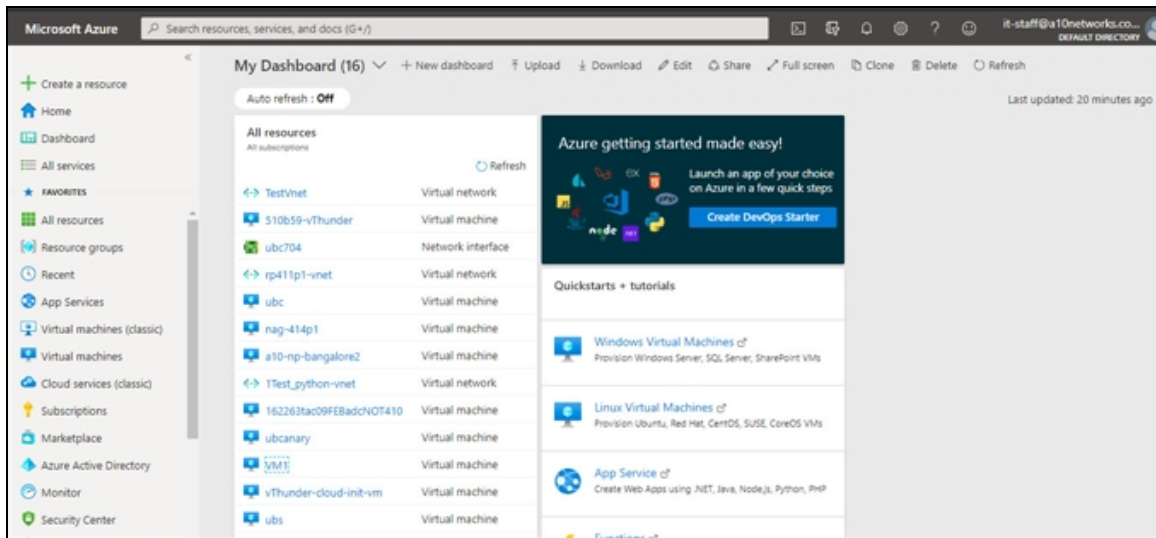
⚠ You have set SSH port(s) open to the internet. This is only recommended for testing. If you want to change this setting, go back to Basics tab.

[Download a template for automation](#)

The preferred e-mail address and phone number display a green check. Click **Create** button to create a virtual machine. In the Azure My Dashboard window, a pane displays the VM just created.

NOTE: Creating the VM may take several minutes depending on several factors.

Figure 18 : My Dashboard - All resources window



Create a Multiple-Interface vThunder Instance

To create a multiple-interface vThunder instance, use any one of the following methods:

- [Creating Multiple-Interface vThunder Instance Using Azure Portal](#)
- [Creating Multiple-Interface vThunder Instance Using Azure PowerShell](#)

After a VM is created with multiple NICs, you can use the Azure portal to configure the VM.

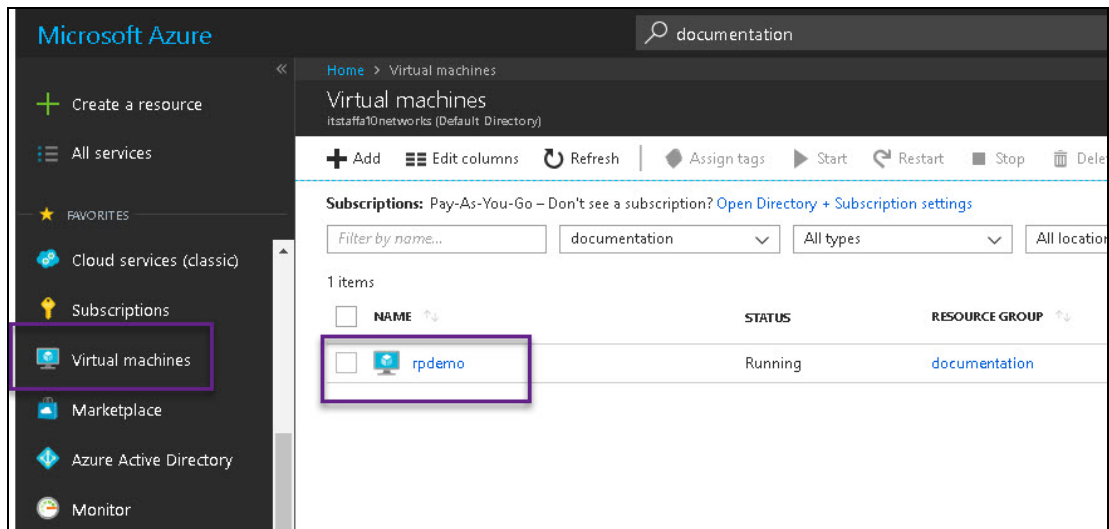
Creating Multiple-Interface vThunder Instance Using Azure Portal

To create a multiple-interface vThunder instance by using the Azure portal, perform the steps from [Create a Single-Interface vThunder Instance](#). The VM is created with one interface.

Perform the following steps:

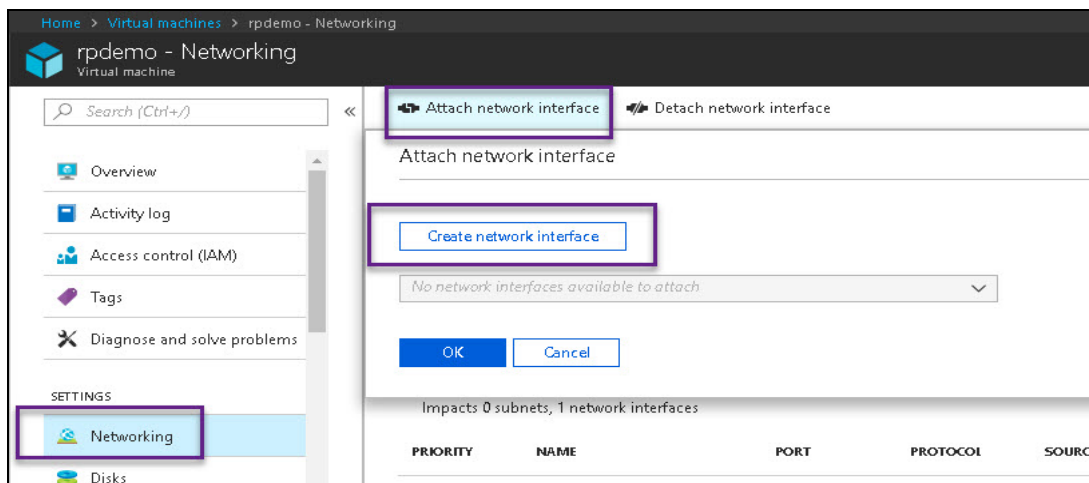
1. Click **Virtual Machines** and select the VM from the right-pane.

Figure 19 : Virtual machines window



2. In the VM window, click **Stop** to stop the VM.
3. From the right pane, select **Networking > Attach network interface > Create network interface**.

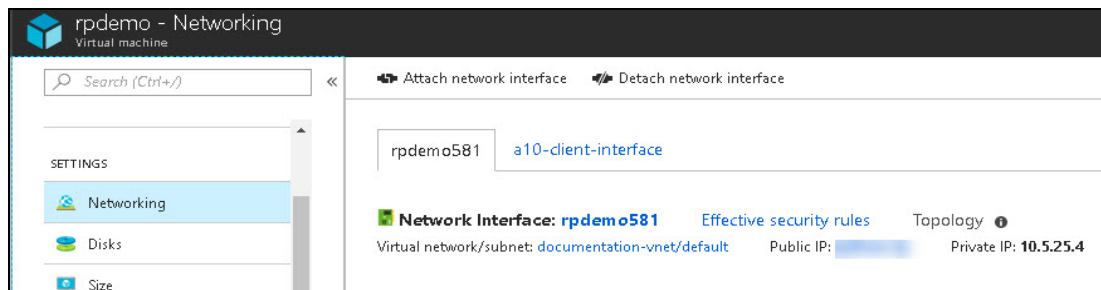
Figure 20 : Attach network interface



4. In the **Create network interface** page, enter the following information:

- **Name:** a10-client-interface
 - **Virtual Network:** Already filled in.
 - **Subnet:** Select one of the existing subnets as appropriate. Each interface must belong to a different subnet.
 - **Private IP address assignment:** Dynamic
 - **Network security group:** Select one of the existing groups or create a new one.
 - **Private IP address (IPv6):** Not required
 - **Subscription:** Already filled in.
 - **Resource group:** Select one of the existing ones or create a new one.
 - **Location:** Already filled in.
5. After the network interface is created, select it from the drop-down of the right-pane, and select **OK**.

Figure 21 : VM with Two Network Interfaces



6. Similarly, create and attach another network interface card for the server-side connection.

NOTE: Applicable for ACOS 5.0.2, the Thunder TPS supports Azure Accelerated Networking which improves network performance by using a high-performance path and reducing latency. It is also supported on the data interfaces and not supported on the management interface. See below for details for enabling Accelerated Networking.

7. After the interfaces are created and attached, start the VM.

Creating Multiple-Interface vThunder Instance Using Azure PowerShell

In this example, a vThunder VM with three NICs is created by using the Azure PowerShell. One NIC is used for the management interface while the other two NICs are used for data interfaces.

NOTE: Provide the inputs to the script which azure cloud portal accepts otherwise deployment fails.

To deploy Azure VM from the market place, perform the following:

1. Deploy the Azure VM from the market place:

```
#Deploying azure VM from marketplace
```

```
Login-AzureRmAccount

$location = Read-Host 'Enter the location'
$resourceGroup = Read-Host 'Enter resource group name'
$storageaccount = Read-Host 'Enter storage account name'
$vmName = Read-Host 'VM Name'
$vmSize = Read-Host 'Enter VM size'
```

2. Create a new resource for the deployment:

```
#Create new resource group for deployment
```

```
New-AzureRmResourceGroup -Name
  $resourceGroup -Location
  $location
```

3. Create a storage account for the new resource:

```
#Create storage account
```

```
New-AzureRmStorageAccount
  -ResourceGroupName $resourceGroup
  -AccountName $storageaccount
  -Location $location
  -SkuName Standard_RAGRS
```



```
-Kind StorageV2  
-AssignIdentity
```

4. Create a virtual network, subnet, and a public IP address. These resources are used to provide network connectivity to the VM and connect it to the internet:

```
# Create a subnet configuration
```

```
$mgmtsubnet = New-AzureRmVirtualNetworkSubnetConfig  
-Name "subnet1"  
-AddressPrefix "192.168.1.0/24"  
$data1subnet = New-AzureRmVirtualNetworkSubnetConfig  
-Name "subnet2" -AddressPrefix "192.168.2.0/24"  
$data2subnet = New-AzureRmVirtualNetworkSubnetConfig  
-Name "subnet3" -AddressPrefix "192.168.3.0/24"
```

```
# Create a virtual network
```

```
$vnet = New-AzureRmVirtualNetwork  
-ResourceGroupName $resourceGroup  
-Location $location  
-Name "Vnet"  
-AddressPrefix 192.168.0.0/16  
-Subnet $mgmtsubnet,$data1subnet,$data2subnet
```

```
# Create a public IP address and specify a DNS name
```

```
$mgmtpip = New-AzureRmPublicIpAddress  
-ResourceGroupName  
$resourceGroup  
-Location $location  
-AllocationMethod Dynamic  
-IdleTimeoutInMinutes 4  
-Name "myip$(Get-Random)"  
$data1pip = New-AzureRmPublicIpAddress  
-ResourceGroupName $resourceGroup  
-Location $location  
-AllocationMethod Dynamic  
-IdleTimeoutInMinutes 4  
-Name "myip$(Get-Random)"  
$data2pip = New-AzureRmPublicIpAddress  
-ResourceGroupName $resourceGroup
```

```
-Location $location
-AllocationMethod Dynamic
-IdleTimeoutInMinutes 4
-Name "myip$(Get-Random) "
```

5. Create an Azure Network Security Group and traffic rule. The Network Security Group secures the VM with inbound and outbound rules. In the following example, an inbound rule is created for TCP port 22 that allows SSH connections. To allow incoming web traffic, an inbound rule for TCP port 80 is also created:

```
# Create an inbound network security group rule for port 22
```

```
$nsgRuleSSH = New-AzureRmNetworkSecurityRuleConfig
-Name "myNetworkSecurityGroupRuleSSH"
-Protocol "Tcp"
-Direction "Inbound"
-Priority 1000 -SourceAddressPrefix *
-SourcePortRange *
-DestinationAddressPrefix *
-DestinationPortRange 22
-Access "Allow"
```

```
# Create an inbound network security group rule for port 80
```

```
$nsgRuleWeb = New-AzureRmNetworkSecurityRuleConfig
-Name "myNetworkSecurityGroupRuleHTTP"
-Protocol "Tcp"
-Direction "Inbound"
-Priority 1001
-SourceAddressPrefix *
-SourcePortRange *
-DestinationAddressPrefix *
-DestinationPortRange 80
-Access "Allow"
```

```
# Create a network security group
```

```
$nsg = New-AzureRmNetworkSecurityGroup
-ResourceGroupName $resourceGroup
-Location $location
-Name "myNetworkSecurityGroup"
-SecurityRules $nsgRuleSSH,
```

```
$nsgRuleWeb
```

- a. Create a virtual network interface card (NIC) with **New-AzNetworkInterface**. The virtual NIC connects the VM to a subnet, Network Security Group, and public IP address.

```
# Create a virtual network card and associate with public IP
address and NSG
```

```
$mgmtsubnet = $vnet.Subnets | ?{ $_.Name -eq 'subnet1' }
$mgmtnic = New-AzureRmNetworkInterface
  -ResourceGroupName $resourceGroup
  -Name "nic1"
  -Location $location
  -SubnetId $mgmtsubnet.Id
  -PublicIpAddressId $mgmtpip.Id
  -NetworkSecurityGroupId
  $nsg.Id
```

NOTE: Applicable for ACOS 5.0.2. Accelerated Networking is only supported on the data interfaces and not supported on the management interface.

```
$datalsubnet = $vnet.Subnets | ?{ $_.Name -eq 'subnet2' }
$datalnic = New-AzureRmNetworkInterface
  -ResourceGroupName $resourceGroup
  -Name "nic2"
  -Location $location
  -SubnetId $datalsubnet.Id
  -PublicIpAddressId $datalpip.Id
  -NetworkSecurityGroupId $nsg.Id
```

To create data interface 1 and enable Accelerated Networking on data interface 1 (nic2), use the following commands:

```
$datalnic = New-AzureRmNetworkInterface
  -ResourceGroupName $resourceGroup
  -Name "nic2"
  -Location $location
  -SubnetId $datalsubnet.Id
```

```
-PublicIpAddressId $data1pip.Id
-NetworkSecurityGroupId $nsg.Id
-EnableAcceleratedNetworking

$data2subnet = $vnet.Subnets | ?{ $_.Name -eq 'subnet3' }
$data2nic = New-AzureRmNetworkInterface
  -ResourceGroupName $resourceGroup
  -Name "nic3"
  -Location $location
  -SubnetId $data2subnet.Id
  -PublicIpAddressId $data2pip.Id
  -NetworkSecurityGroupId $nsg.Id
```

Similarly, use the following commands to create data interface 2 (nic3) with Accelerated Networking enabled:

```
$data2nic = New-AzureRmNetworkInterface
```

```
-ResourceGroupName $resourceGroup
-Name "nic3"
-Location $location
-SubnetId $data2subnet.Id
-PublicIpAddressId $data2pip.Id
-NetworkSecurityGroupId $nsg.Id
-EnableAcceleratedNetworking
```

NOTE: For Accelerated Networking support with multiple NICs, Accelerated Networking must be enabled on both data interfaces.

6. To create a VM in PowerShell, firstly create a configuration that has settings like the image to use, size, and authentication options. Then the configuration is used to build the VM.

```
# Define a credential object
```

```
$name= Read-Host 'Enter Username'
$securePassword = Read-Host 'Enter the password' -AsSecureString
$cred = New-Object System.Management.Automation.PSCredential ($name,
$securePassword)
```

```
# Start building the VM configuration
$vmConfig = New-AzureRmVMConfig -VMName
$vmName -VMSize
$vmSize

#Create the rest of configuration
$vmConfig = Set-AzureRmVMOperatingSystem -VM
$vmConfig
  -Linux
  -ComputerName
$vmName -Credential
$cred
$vmConfig = Set-AzureRmVMSourceImage -VM
$vmConfig
  -PublisherName "a10networks"
  -Offer "vthunder-414-gr1"
  -skus "vthunder-414gr1-byol"
  -Version "latest"
$vmConfig = Set-AzureRmVMPlan
  -Name "vthunder-414gr1-byol"
  -Product "vthunder-414-gr1"
  -Publisher "a10networks"
  -VM
$vmconfig

# for bootdiag
$vmConfig = Set-AzureRmVMBootDiagnostics -VM
$vmconfig -Enable
  -ResourceGroupName $resourceGroup
  -StorageAccountName $storageaccount

#Attach the NIC that are created
$vmConfig = Add-AzureRmVMNetworkInterface -VM
$vmConfig -Id
$mgmtnic.Id -Primary
$vmConfig = Add-AzureRmVMNetworkInterface -VM
$vmConfig -Id
$datalnic.Id
$vmConfig = Add-AzureRmVMNetworkInterface -VM
```

```
$vmConfig -Id  
$data2nic.Id  
  
#Creating VM with all configuration  
New-AzureRmVM -ResourceGroupName  
$resourceGroup -Location  
$location -VM  
$vmConfig
```

NOTE: Starting from ACOS 4.1.4-P3, single NIC deployments for the vThunder on Azure Cloud are not supported.

About Multiple IP Addresses for a Network Interface

An Azure VM can have multiple private and public IP addresses. Guidelines for the IP addresses are:

- A network interface can have one or more static or dynamic public and private IP addresses assigned to it.
- There is a limit to how many private and public IP addresses can be assigned to a network interface. This limitation is dependent on the type of Azure subscription that you have.
- When there are multiple IP addresses assigned to a network interface, only one IP address can be a primary IP address. The other IP addresses are all secondary IP addresses.
- The secondary IP addresses can be configured as VIP. In this document, the secondary IP address is configured as the VIP.

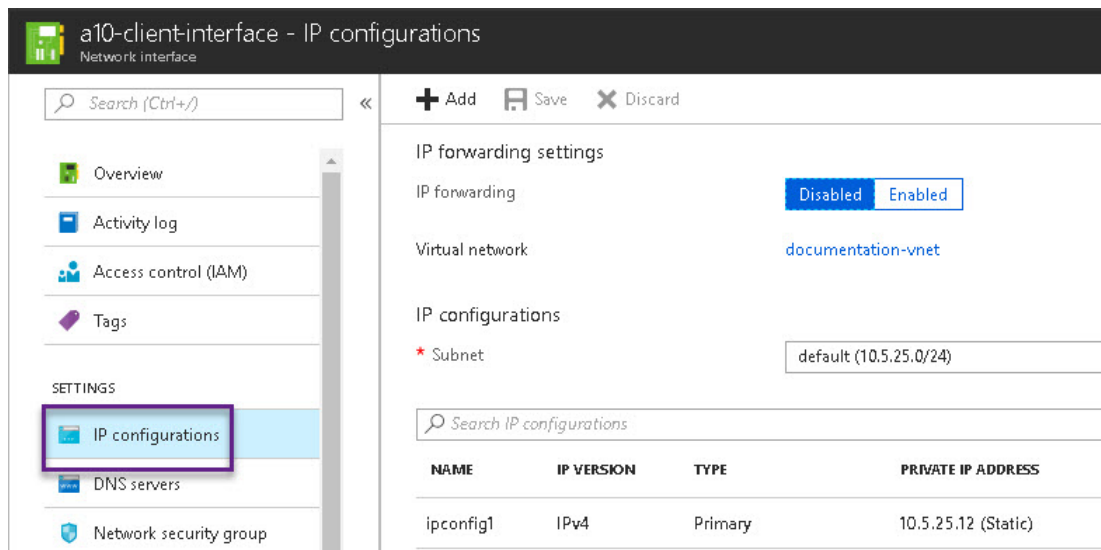
Associating Public IP and Secondary IP address by Using Azure Portal

In this example, the primary IP address is associated with a public IP address, and the secondary IP address is associated with its public IP address. The secondary IP address is configured as a VIP for the ACOS configurations.

Perform the following steps to add a public IP address to a network interface:

1. From the Microsoft Azure left-most pane, select **Virtual networks**, and then from the list of virtual networks, select the virtual network to which the network interface belongs.
2. Under the virtual network, select the network interface card for which you want to add a public IP address.
3. Under **Settings**, select **IP configurations**.

Figure 22 : Select IP configurations



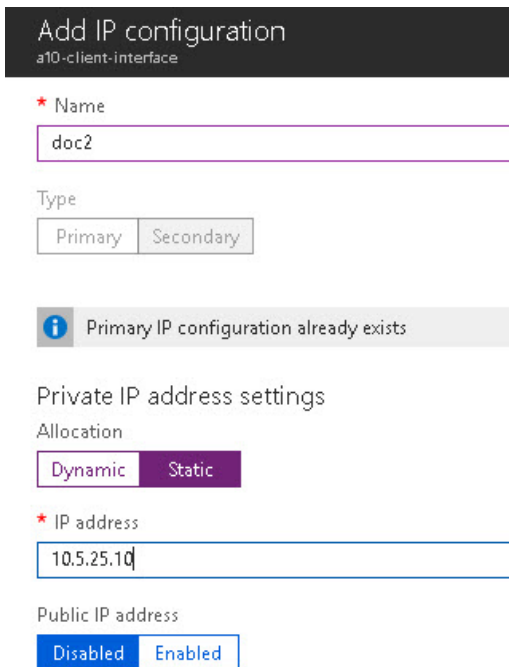
4. Click the **Public IP address** in the main window.
5. Fill in the following details, and then click **Save**:
 - **Public ip address**: Enabled
 - **IP address**: Select from existing or create new.
 - Private IP address settings: Keep default for the subnet.
 - IP address

Perform the following steps to add a secondary IP address to a network interface:

1. From the Microsoft Azure left-most pane, select **Virtual networks**, and then from the list of virtual networks, select the virtual network to which the network interface belongs.

2. Under the virtual network, select the network interface for which you want to add a secondary IP address.
 3. Under **Settings**, select **IP configurations** and then **Add** in the main window.
 4. In the Add IP configuration window, fill in the following details and click **OK**.
- **Name:** Doc1
 - **Type:** Secondary (by default)
 - **Private IP address settings:** Static. Fill in an IP address.
 - **Public IP address:** Disabled

Figure 23 : Add Secondary IP address



Add IP configuration
a10-client-interface

* Name

Type
 Primary Secondary

i Primary IP configuration already exists

Private IP address settings
Allocation
 Dynamic Static

* IP address

Public IP address
 Disabled Enabled

The secondary IP address is created.

Adding a Public IP Address to a NIC Using Azure CLI

Azure resources cannot receive and send Internet communication without an assigned public IP address. Public IP addresses have a nominal charge. For more information, refer to <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-public-ip-address>.

To add a public IP address to a NIC, perform the following steps:

1. Create the public IP address:

```
az network public-ip create -g
testResourceGroup -n testip --dns-name MyLabel --allocation-method
dynamic
```

2. Create an IP configuration on the NIC:

```
az network nic ip-config create --name ipconfig2
--nic-name data1nic
--resource-group testResourceGroup
[--application-security-groups]
[--lb-address-pools]
[--lb-inbound-nat-rules]
[--lb-name]
[--make-primary]
[--private-ip-address]
[--private-ip-address-version {IPv4,
IPv6}]
[--public-ip-address]
[--subnet]
[--vnet-name]
```

Adding a Secondary IP Address to a NIC by Using Azure CLI

The private IP address that is used as a VIP must be attached to the data interface in Azure Portal as a secondary (private) IP to the interface.

To create a secondary IP address, perform the following steps:

```
az network nic ip-config create --name ipconfigtest
```

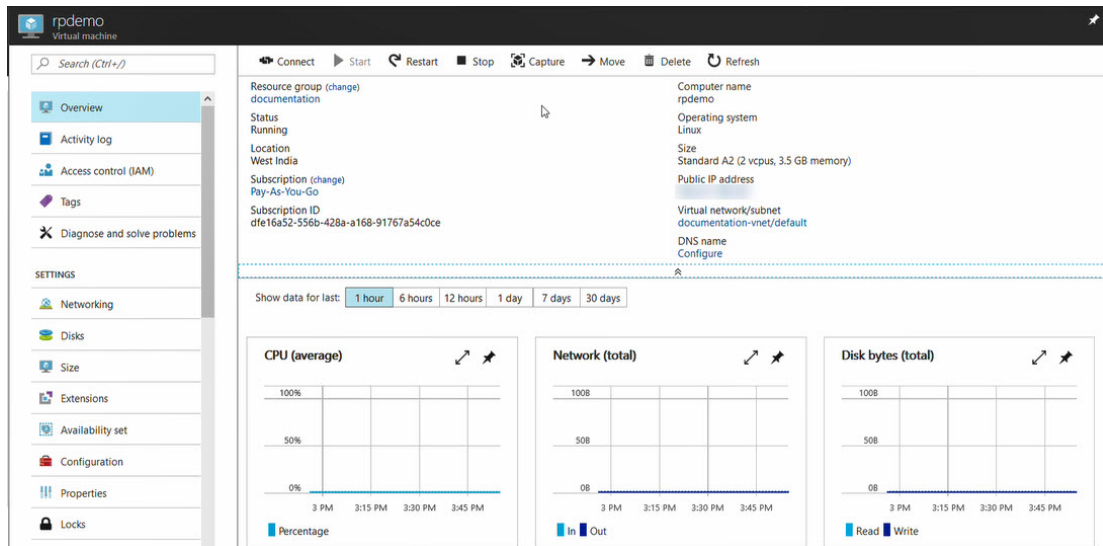
```
--nic-name data1nic
--resource-group testResourceGroup
[--application-security-groups]
[--lb-address-pools]
[--lb-inbound-nat-rules]
[--lb-name]
[--make-primary]
[--private-ip-address]
[--private-ip-address-version {IPv4,
IPv6}]
[--subnet]
[--vnet-name]
```

Access vThunder by Using ACOS CLI

To connect to the VM, perform the steps:

1. After the VM is created, type the VM name in the Azure search box and click Enter.
The search results display the VM.
2. Click on the link to launch the VM details page.
3. Wait until the Status column for the VM has changed to **Running**.
When the status has changed to **Running**, you can establish a PuTTY session with the virtual machine.
4. Select the public IP address from the VM Overview page.

Figure 24 : VM Overview Page



5. Open an SSH client and access the IP address on the client.
6. Enter the following credentials to access the VM:
 User name: `admin`
 Password: `a10`
 The vThunder prompt is displayed.

Configure Endpoint Mapping

To access the web GUI for configured VM images, configure endpoint mapping in the Azure management portal. The public IP address for the web GUI will NOT work unless this is set up per the procedure below.

To configure endpoint mapping:

1. Navigate to **Virtual Machines**.
2. Click on the configured VM and select **Networking**.
3. Select the management interface and add an inbound HTTPS rule as follows:
 - a. A high priority.
 - b. Name as HTTPS.

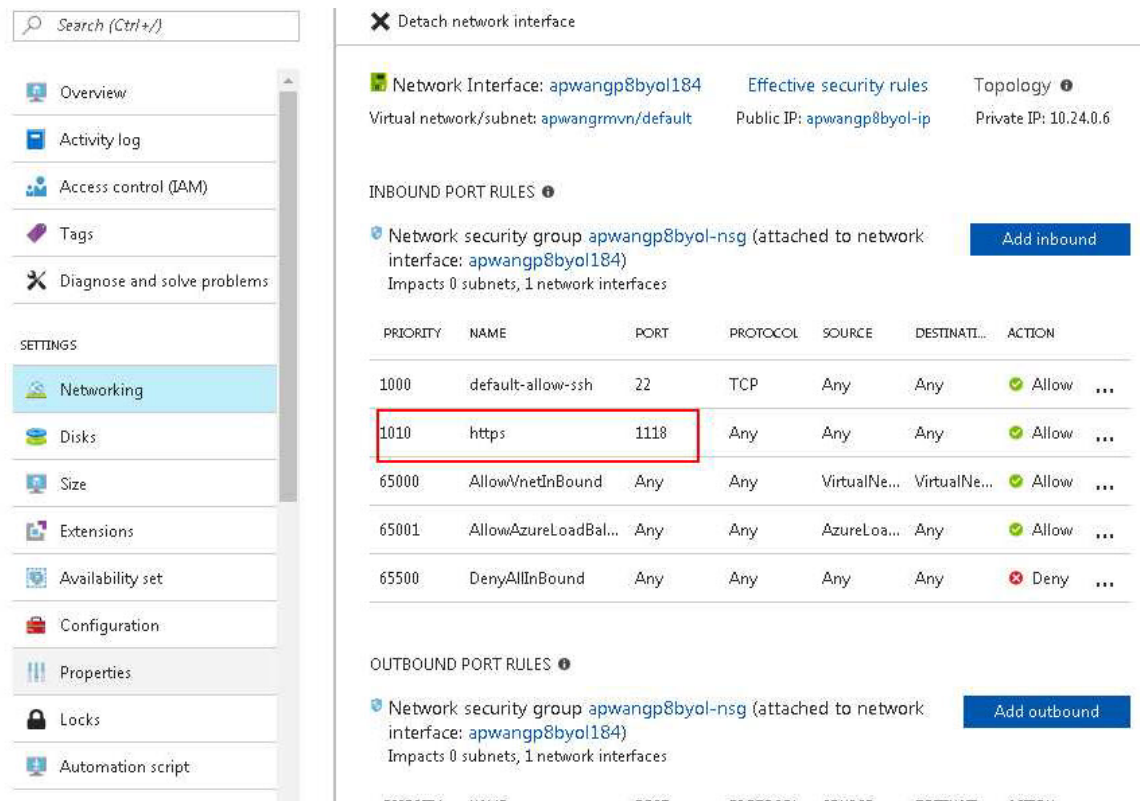
- c. A designated port such as 1113.

You can now access the ACOS GUI at `https://<azure_public_ip>:1113`.

4. Select the management interface and add an inbound HTTP rule as follows:
 - a. A high priority.
 - b. Name as HTTP.
 - c. A designated port such as 1115.

Now user can access the ACOS GUI at `http://<azure_public_ip>:1115`.

Figure 25 : Editing Endpoint Mapping within the Azure Management Portal



The screenshot shows the Azure Management Portal interface for editing a Network Security Group (NSG) rule. The left sidebar contains navigation options like Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. The main content area displays the configuration for a Network Interface (apwangp8byol184) and its associated Network Security Group (apwangp8byol-nsg). The INBOUND PORT RULES section shows a table of rules, with the 'https' rule (Priority 1010, Port 1118) highlighted by a red box. The rule is configured to allow traffic on port 1118. The OUTBOUND PORT RULES section is also visible below.

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATI...	ACTION
1000	default-allow-ssh	22	TCP	Any	Any	Allow
1010	https	1118	Any	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNe...	VirtualNe...	Allow
65001	AllowAzureLoadBal...	Any	Any	AzureLoa...	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Access vThunder by Using ACOS GUI

If the vThunder VM uses Network Security Group, then configure endpoint mapping to access the VM by using the ACOS GUI.

For single interface VMs, launch a web browser and enter the following URL `https://public IP: 8443`. The public IP portion of this URL can be obtained by looking up the public IP address, as in [VM Overview Page](#).

For multiple-interface VMs, enter the URL `https://public IP`. When accessing the web GUI, the default value is port 80.

Microsoft Azure High Availability

Starting from ACOS 5.0, configuring vThunder in High Availability (HA) mode is supported for Microsoft Azure. HA is supported within the availability zone. You cannot configure HA of vThunder instances across different availability zones. vThunder already supports unicast-based VRRP to make it highly available when an active vThunder instance fails. However, in the Azure cloud, the floating IP address (FIP) is mapped to the secondary IP address (VIP) of the data interface. During fail-over, the floating IP (FIP) and the VIP moves from the active vThunder instance to the standby vThunder instance, making it the new active instance.

The following topics are covered:

Creating Azure Access Key	42
Importing Azure Access Key	56
Azure HA Architecture	57
Configuring HA	59

Creating Azure Access Key

Configuring vThunder for HA in an Azure environment requires access to the Azure Access key. To create the Azure access key, perform the following steps:

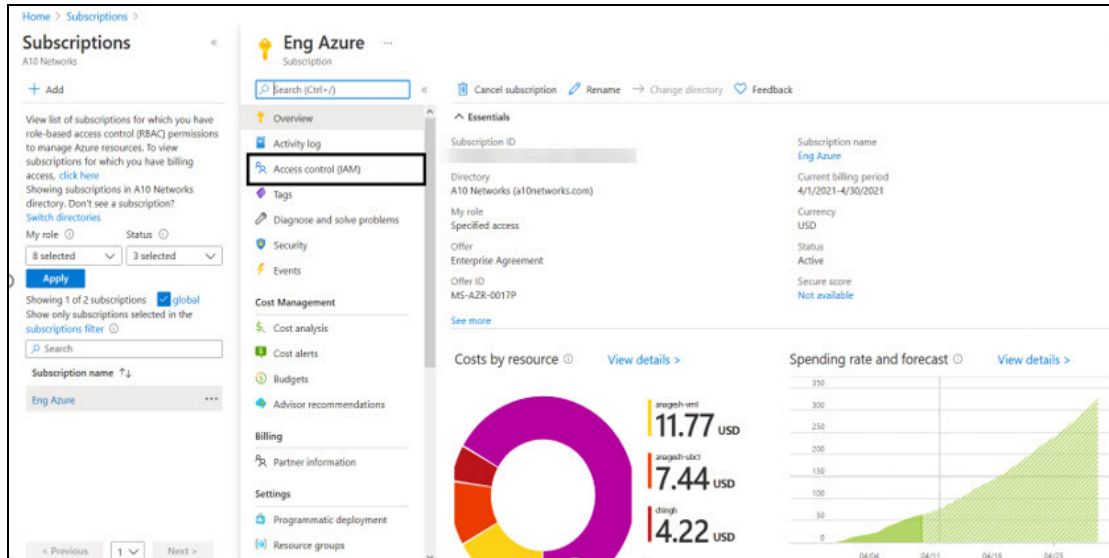
1. [Create a Role](#)
2. [Register a Service Application](#)
3. [Associate Service Application with a Role](#)
4. [Create Certificate and Secrets](#)
5. [Collect Azure Access Key](#)

Create a Role

To create a custom role, perform the following steps:

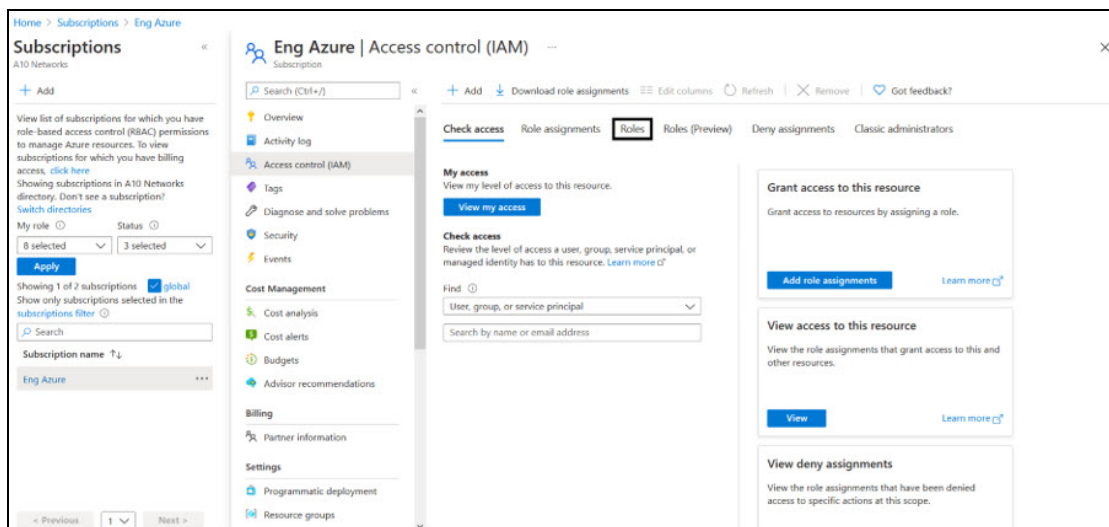
1. Navigate to the **Home > Subscriptions > Registered Subscription Name > Access control (IAM)** from left panel.

Figure 26 : Subscriptions - Access control (IAM) window



2. On the Select Access control (IAM) page, select the **Roles** tab. The Role window is displayed.

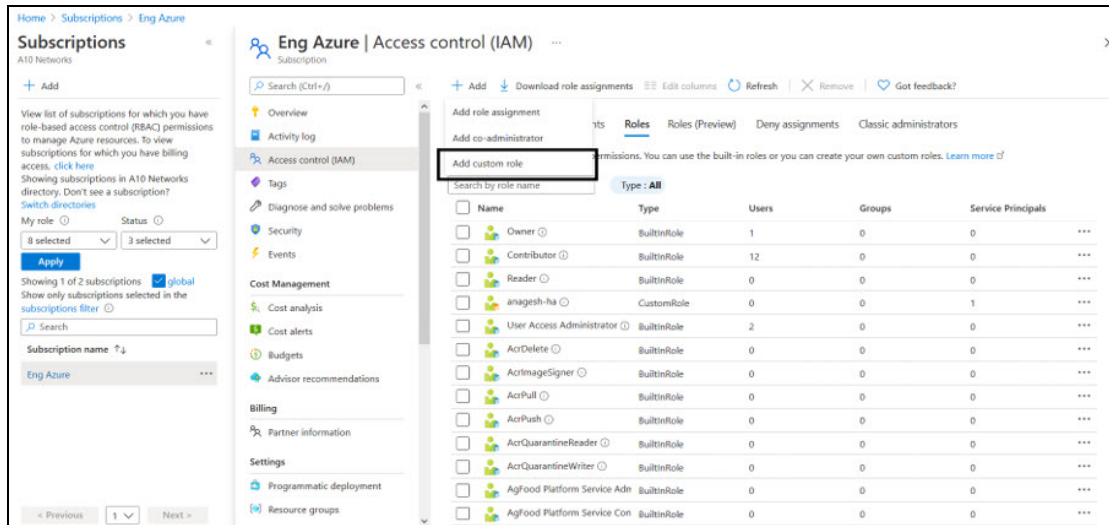
Figure 27 : Access Control - Role Window



3. Click on the **+Add** tab and select **Add custom role** option. The Create a custom

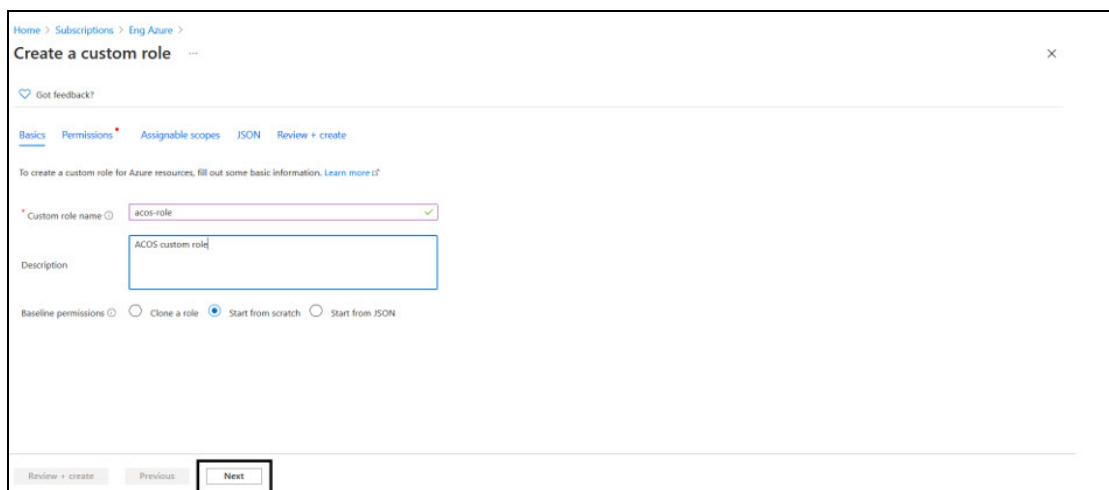
role window is displayed.

Figure 28 : Add custom role window



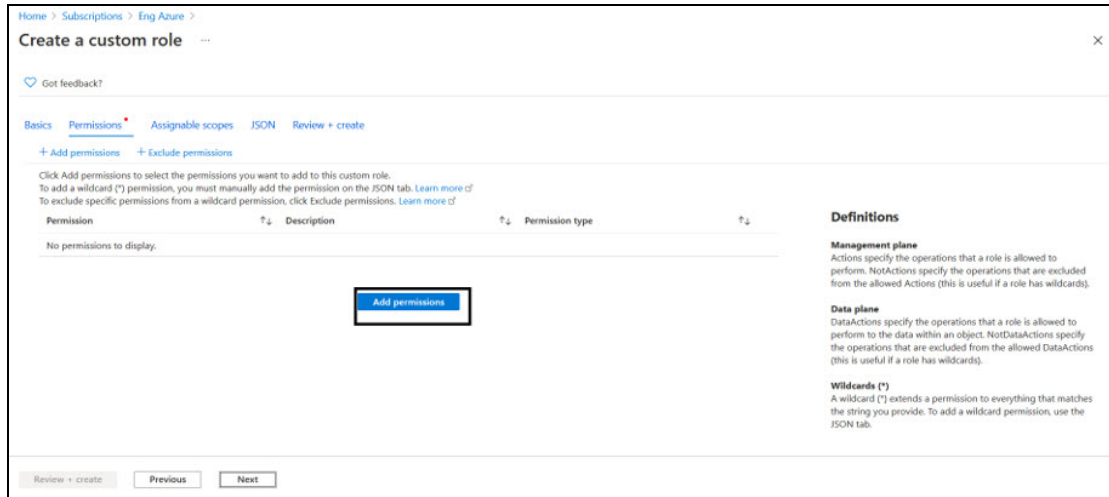
4. Enter **Customer** role name and **Description** (optional).

Figure 29 : Create a custom role window



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

Figure 30 : Permission window

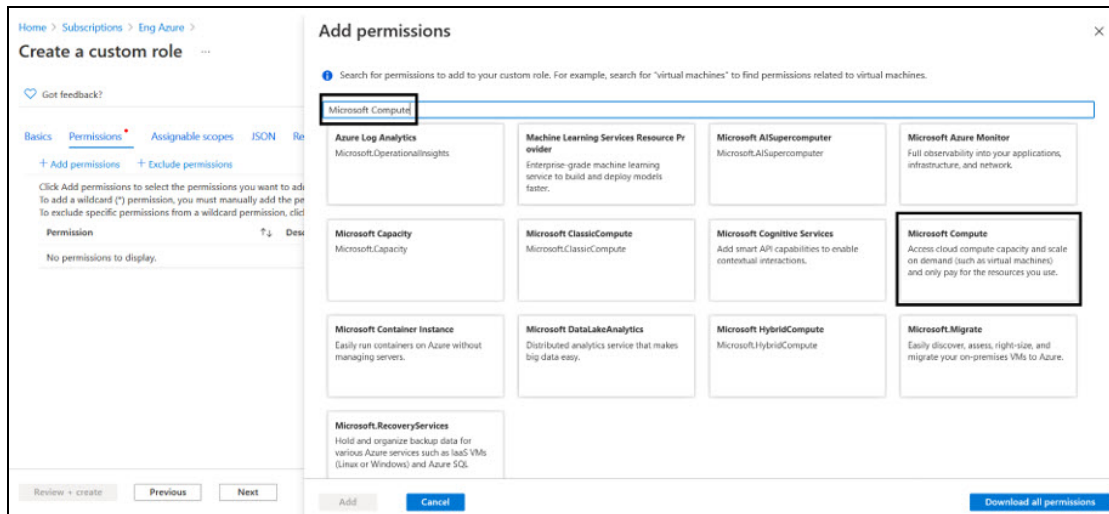


6. Click on the **+Add Permissions** button to create a custom role.

7. Search for the permission to add the custom role.

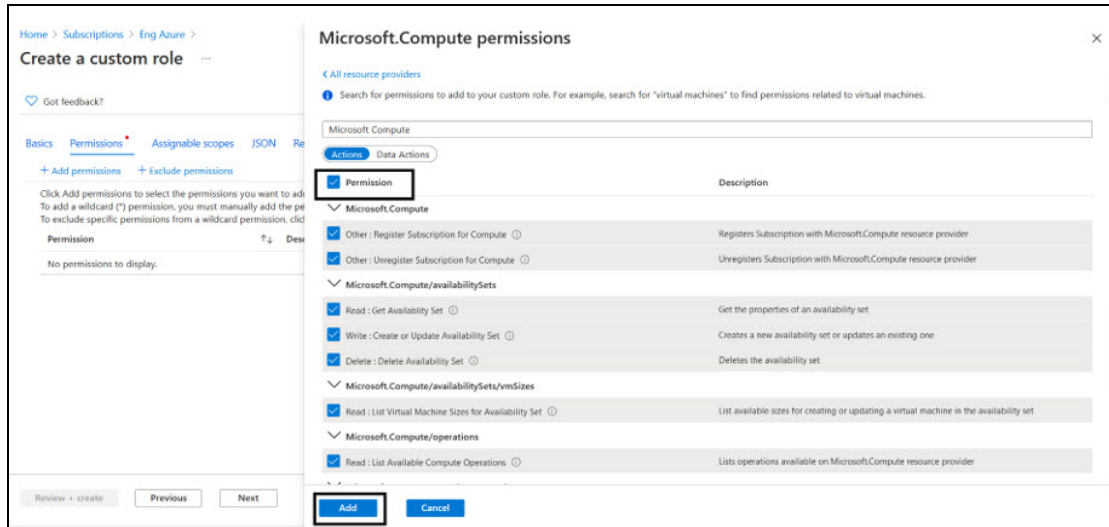
For example, select **Microsoft Compute** from Add Permissions page.

Figure 31 : Add permission window



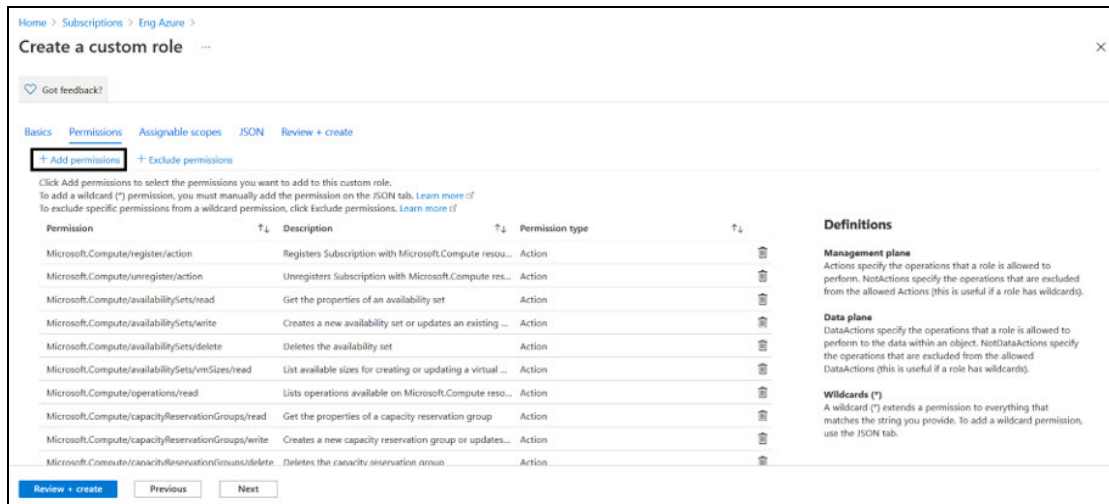
The Microsoft Compute permission window is displayed.

Figure 32 : Microsoft Compute permissions window



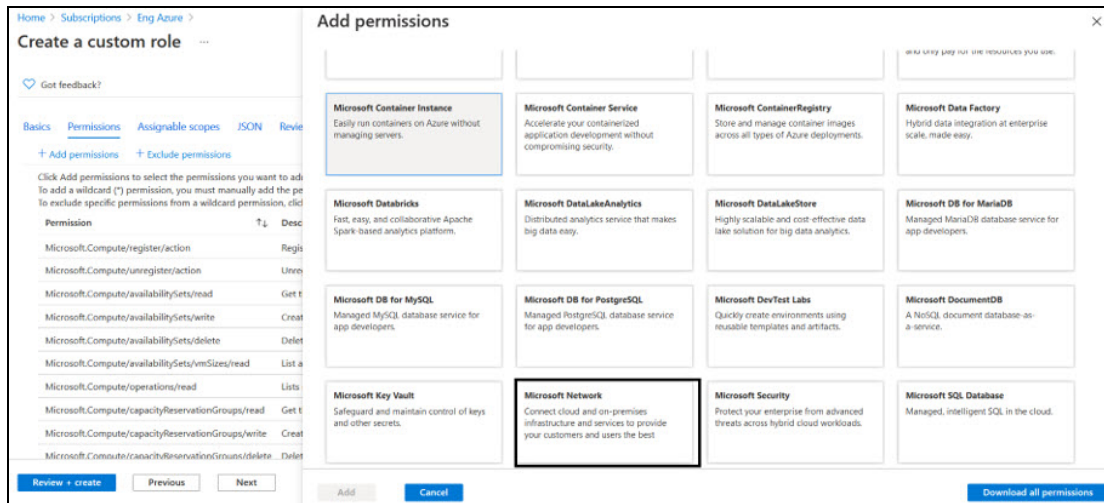
8. Select the **Permission** check box(es) and click **Add** button.
9. To add **Microsoft Network** from Add Permissions page, click on the **+Add Permissions** on Create a custom role page.

Figure 33 : Create a custom role - Add permissions



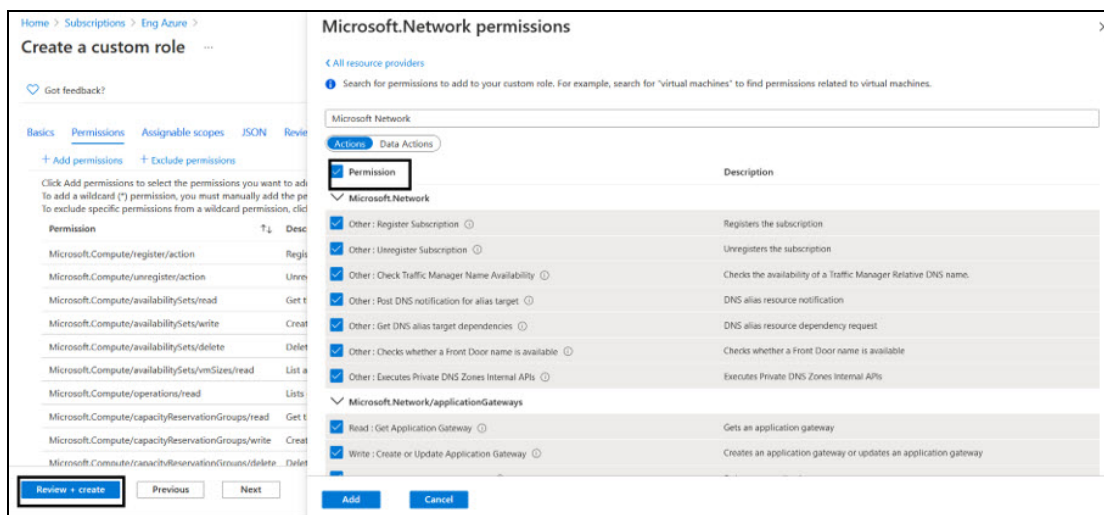
10. Search and select **Microsoft Network** from Add Permissions page.

Figure 34 : Add permissions - Microsoft Network page



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

Figure 35 : Microsoft Network permissions window



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



12. Click **OK** to successfully create the custom role with permissions.

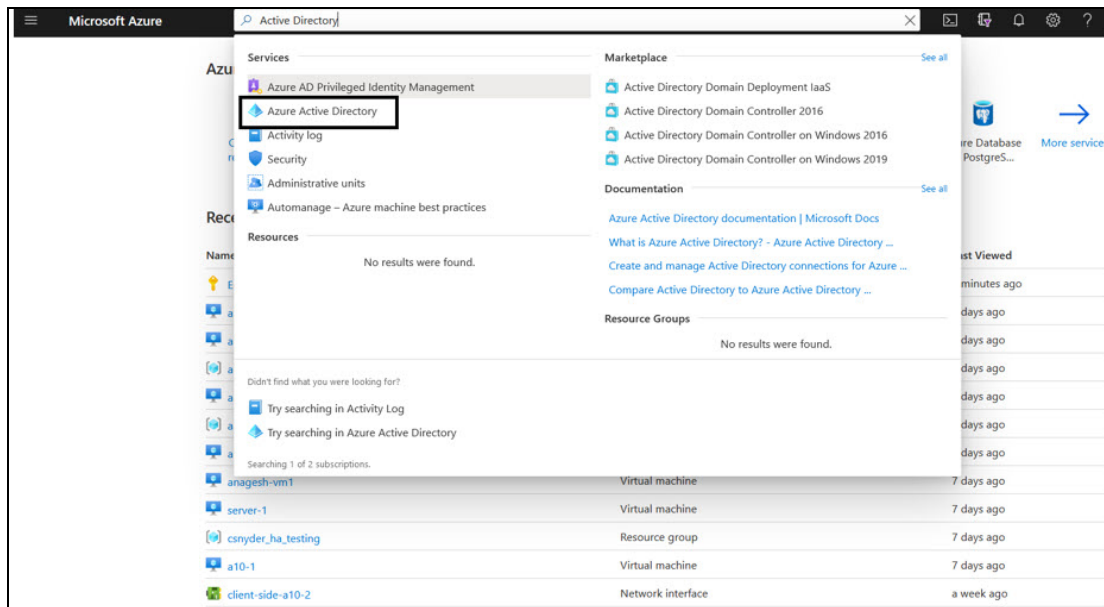
NOTE: It may take the system a few minutes to display your role everywhere.

Register a Service Application

To register a service application, perform the following steps:

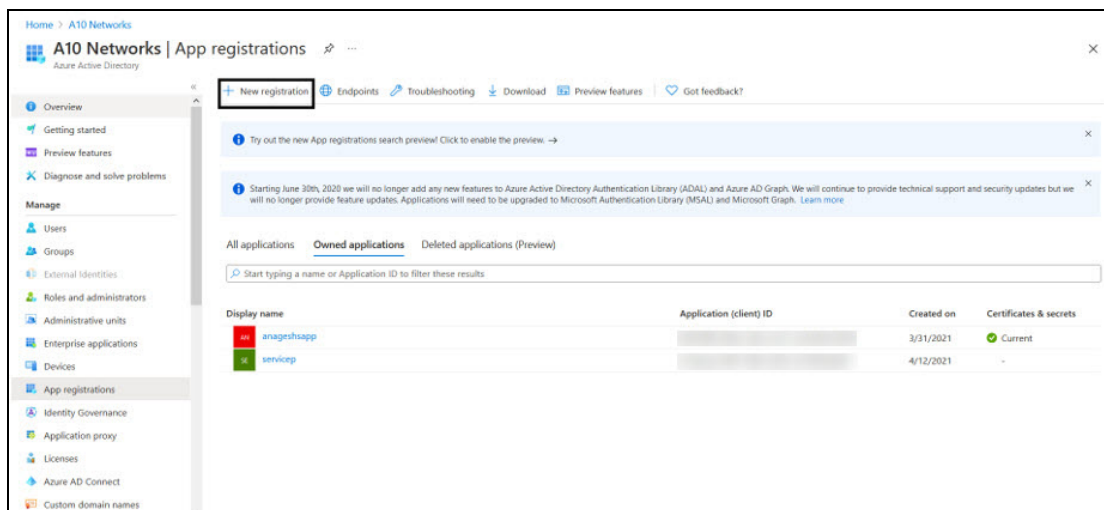
1. Navigate to the **Home > Services > Azure Active Directory** option.

Figure 36 : Azure Active Directory page



2. 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.

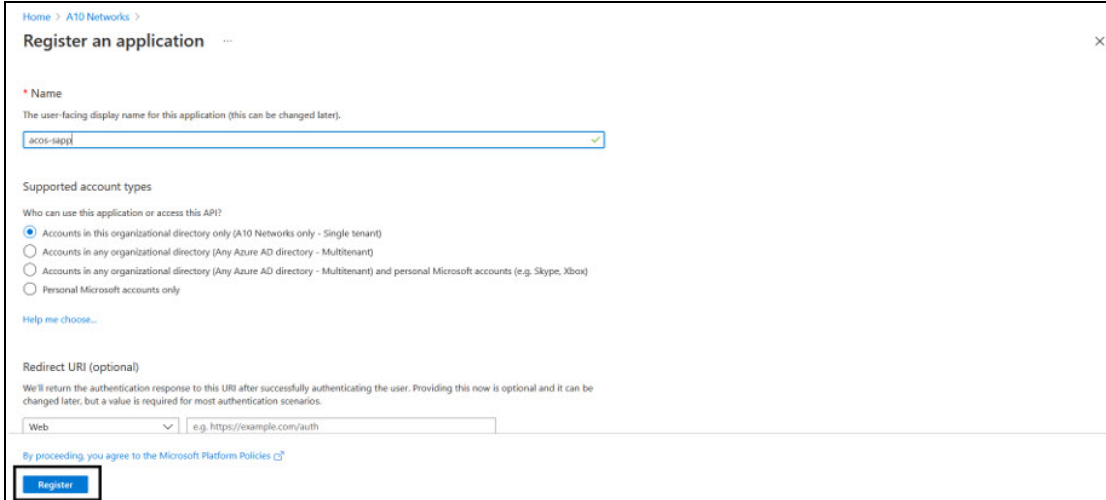
Figure 37 : App registrations window



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

displayed.

Figure 38 : Register an application window



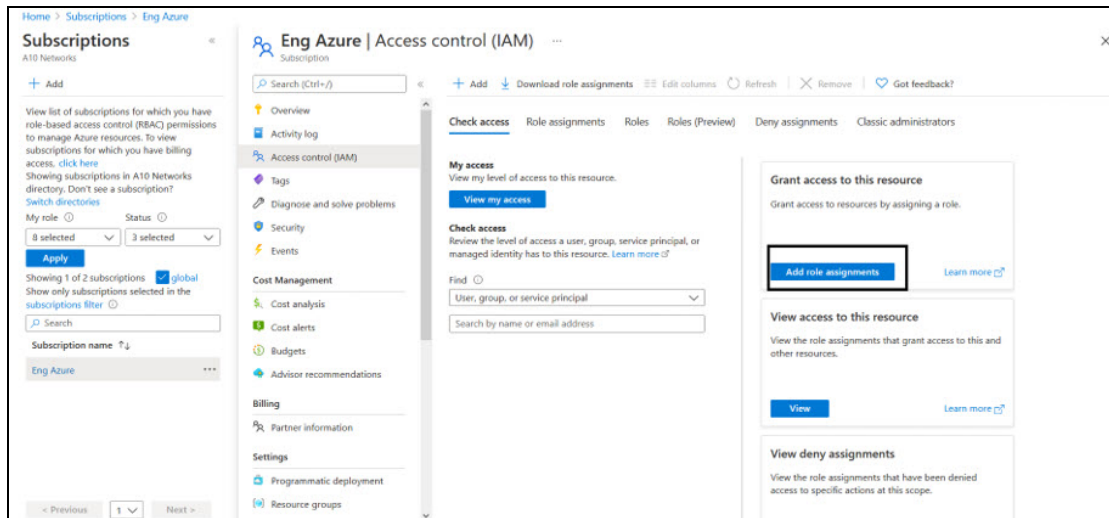
4. Enter the **Name** of the application. For example, acos-sapp.
5. Click on the **Register** button to register the application. The application gets displayed in the list of Azure Active Directory - Apps registrations window.

Associate Service Application with a Role

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

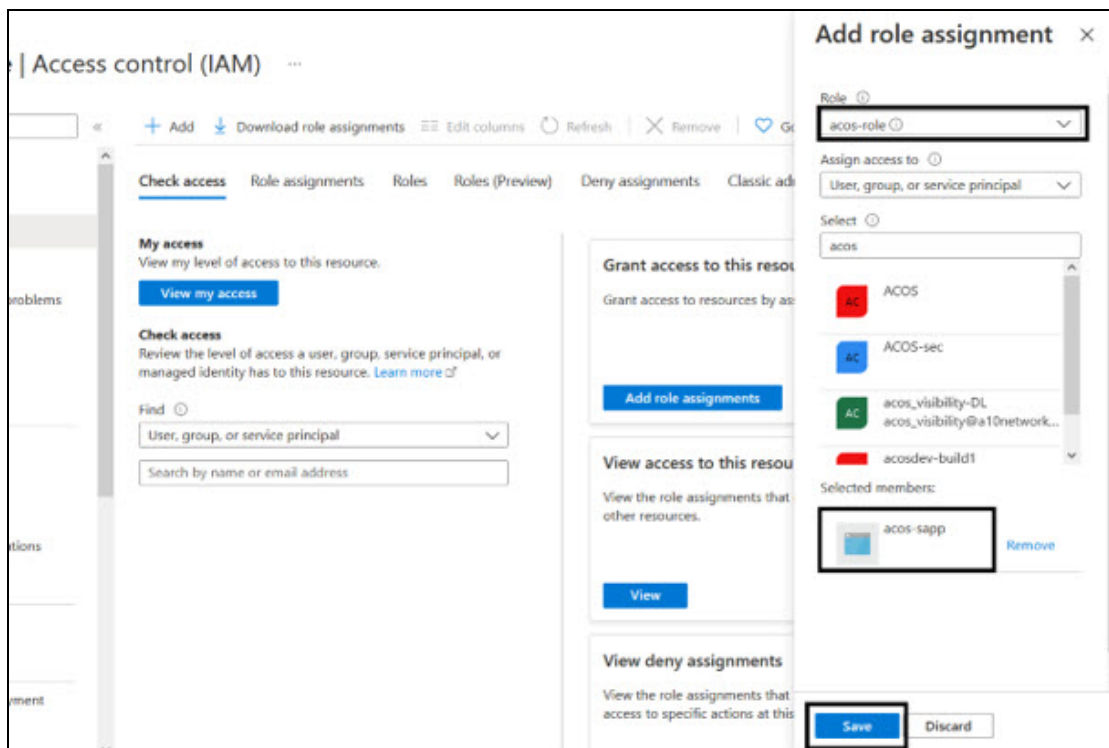
1. Navigate to the **Home > Subscriptions > Registered Subscription Name > Access control (IAM)**.
The Subscription > Access control (IAM) window is displayed.

Figure 39 : Subscription - Access control (IAM) window



- 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 40 : Add a role assignment -1



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

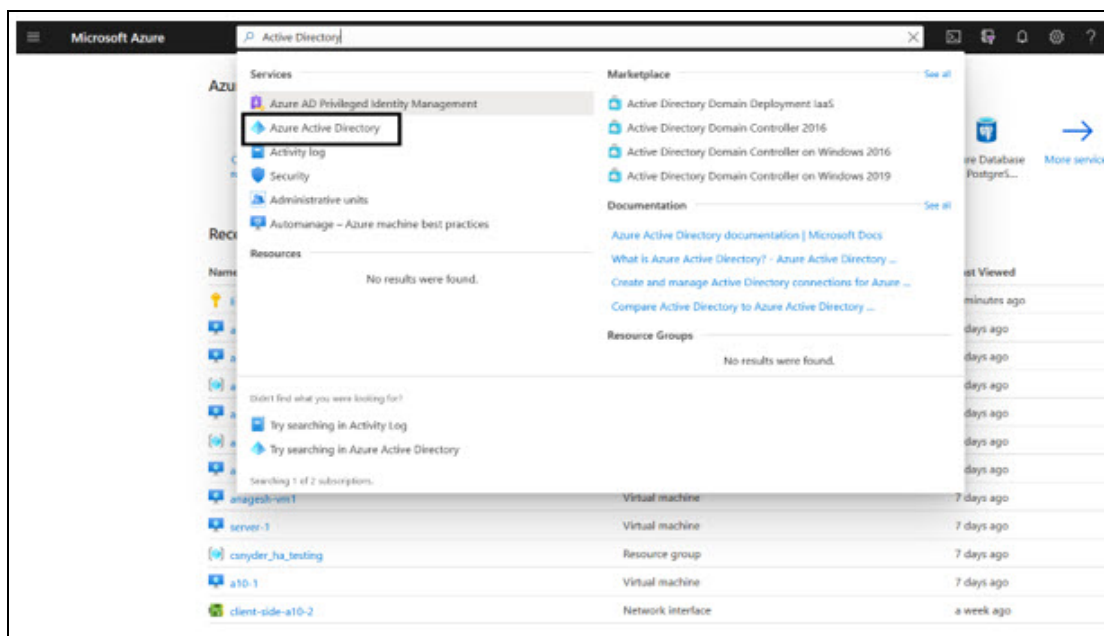
4. Select the **Assign Access to** option from the drop-down list.
5. Enter a string to search and select for a name or email address. For example, `acos`.
6. Click the **Save** button to save the configuration.

Create Certificate and Secrets

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

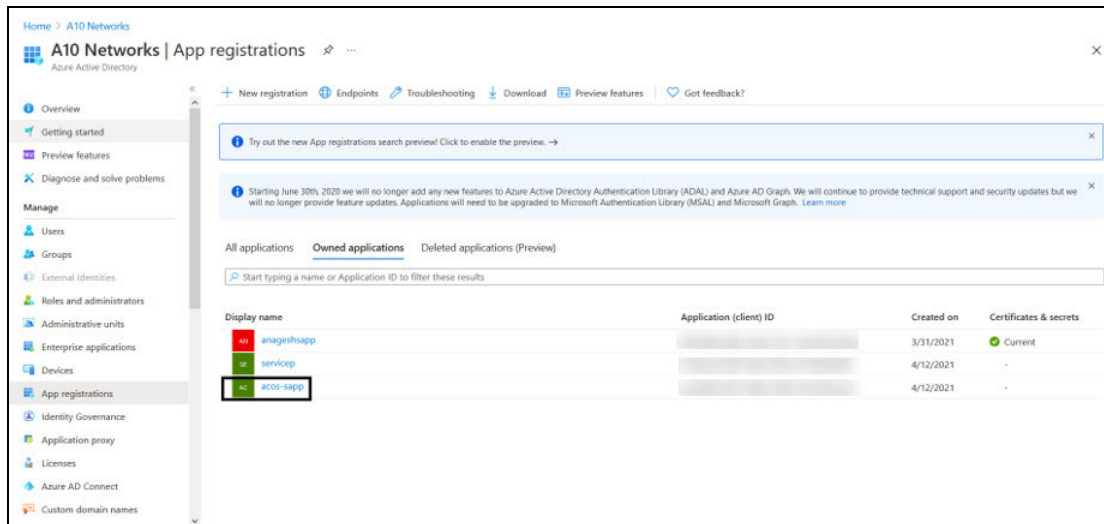
1. Navigate to the **Home > Services > Azure Active Directory** option.

Figure 41 : Azure Active Directory - Overview page



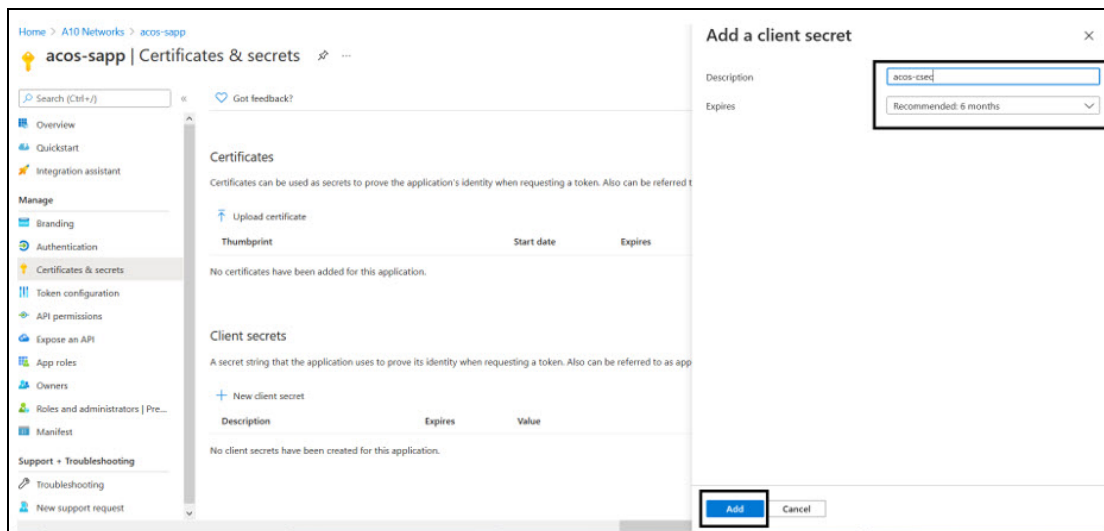
2. On the Azure Active Directory - Overview page, click on the **App registrations** menu option from the left panel. The App registration window with a registered application(s) is displayed.

Figure 42 : App registrations - Overall applications window



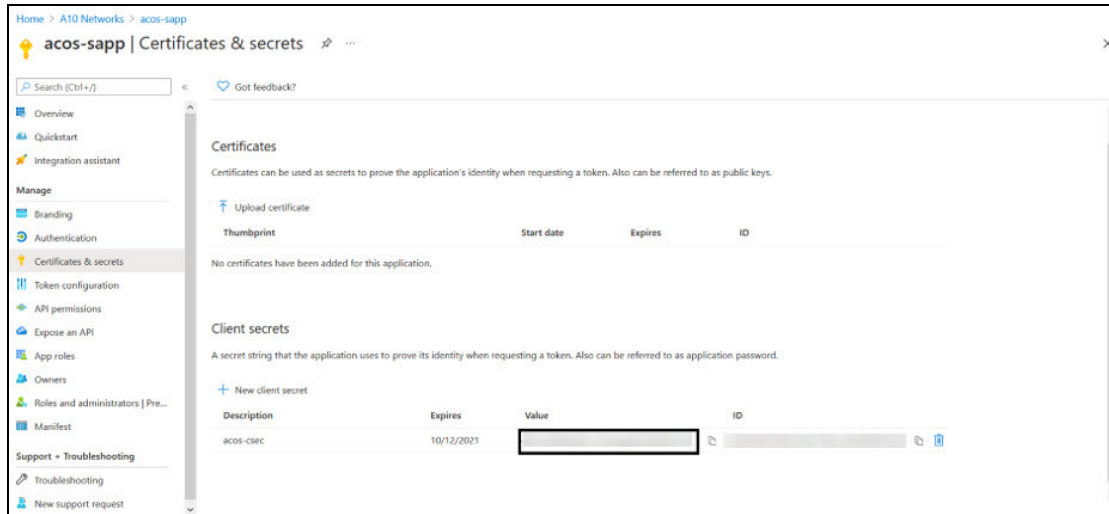
3. Select a service application from list of applications. The selected service application window is displayed.
4. Select the **Certificates & secrets** option from the left Manage navigation pane. The acos sapp - Certificates & secrets window is displayed.
5. Select the **Start date** and **Expires** date from the date picker. Or Click the **New client secret** button. The Add a client secret window is displayed.

Figure 43 : Add a client secret window



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

Figure 44 : acos-sapp Certificates & secrets window



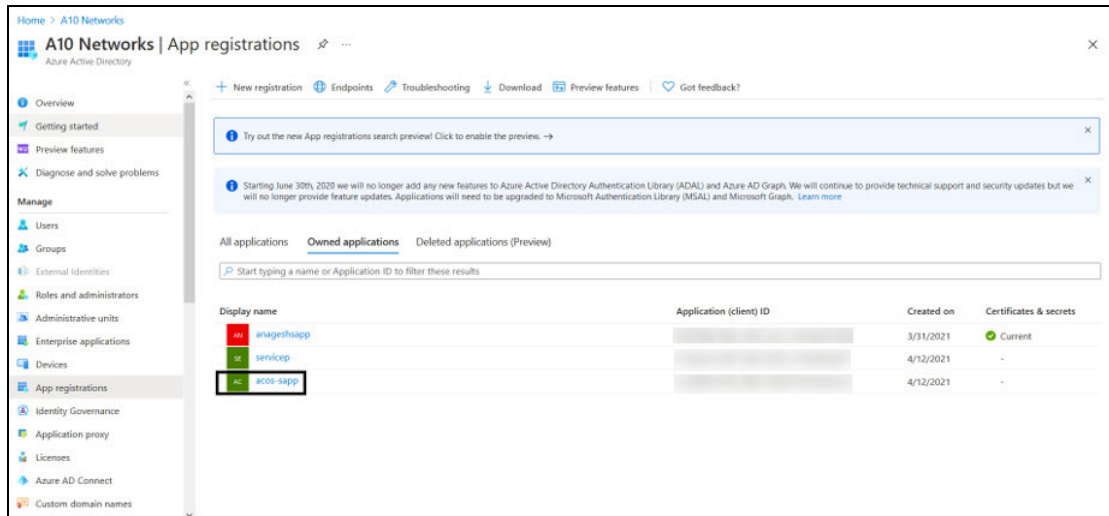
NOTE: Copy the new client secret value, as it is not visible once the page is refreshed.

Collect Azure Access Key

To collect Azure access keys, perform the following steps:

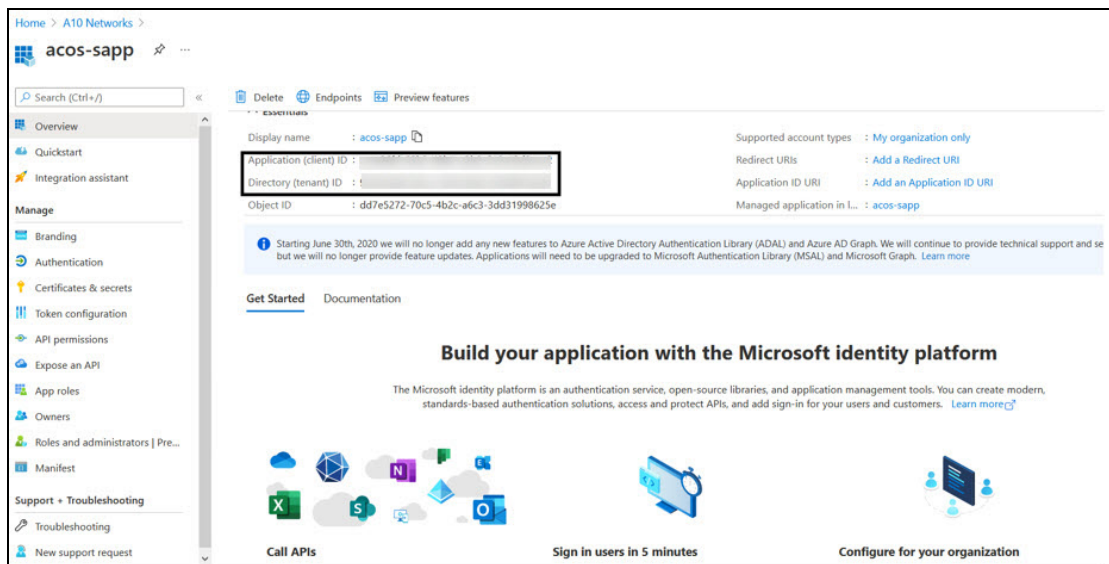
1. Navigate to the **Home > Azure Active Directory - App registrations**.

Figure 45 : App registrations - Azure Active Directory window



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

Figure 46 : Selected Service application window



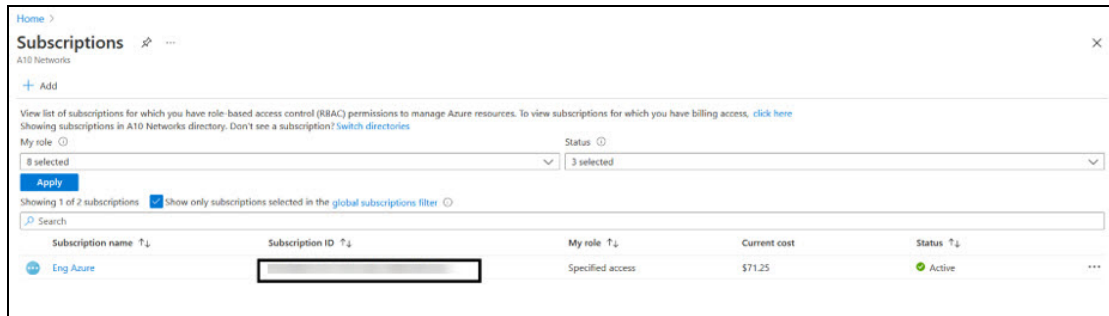
3. Copy the Client ID, Tenant ID from the service application page.

```
client_id= 'cc4c86xx-65b3-48xx-a3xx-610cxxxxxxxxxx'
```

```
tenant_id= '91d27axx-8cxx-41xx-82xx-3d1bxxxxxxxxx'
```

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

Figure 47 : Subscriptions window



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

```
subscription='07d34bxx-61xx-47xx-abxx-006bxxxxxxxxx'
```

```
client_id='cc4c86xx-65xx-48xx-a3xx-610cxxxxxxxxx'
```

```
client_secret='G0x_hVDzZxxxx-o1Vsw.xxxx.Zxxxx-xx'
```

```
tenant_id='91d2xxxx-8xxe-41xx-82xx-3d1bxxxxxxxxx'
```

Importing 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
```

3. Go to the admin mode.

```
vThunder (config) #admin ?
NAME<length:1-31> System admin user name
vThunder (config) #admin admin
```

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

```
vThunder (config-admin:admin) #azure-cred import ?
use-mgmt-port Use management port as source port
tftp: Remote file path of tftp: file system(Format:
tftp://host/file)
ftp: Remote file path of ftp: file system(Format:
ftp://[user@]host[:port]/file)
scp: Remote file path of scp: file system(Format:
scp://[user@]host/file)
sftp: Remote file path of sftp: file system(Format:
sftp://[user@]host/file)
```

To delete the key, use the following command:

```
azure-cred delete
```

5. 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://username@<ip-addr>:/<file-path>/cred.txt
vThunder-Active (config-admin:admin) (NOLICENSE) #azure-cred sh
vThunder-Active (config-admin:admin) (NOLICENSE) #azure-cred show
SUB_ID = 'dfe16a52-556b-428a-a168-91767a54c0Ce'
client_id = 'b8d52c6f-0c65-460d-bafd-e03cc942aa66'
secret = 'bVcK_XGE9u0Or+M2Css=fmCL?8bf-0b'
tenant = '1e94d773-1e01-442d-b25d-3b3e1b64948d'
vThunder-Active (config-admin:admin) (NOLICENSE) #
```

Azure HA Architecture

Configuring of HA for vThunder instances in Microsoft Azure is supported only for the same availability zone. In a sample HA architecture, create two vThunder

instances. Both the vThunder instances require at least one management interface and one data interface. To achieve HA the following configurations are required:

- For the active vThunder only, a secondary IP address for the client-facing data interface is reassigned. Select the reassignment option to create the secondary IP address. This secondary IP address is then assigned to a standby VM during fail-over without un-assigning it from the active vThunder.
- Assign the public IP address to the management interface and to the secondary IP address assigned to the data interface (VIP). Also, assign the public IP address to the management IP address of the standby vThunder.
- Additionally, each vThunder instance requires a copy of the Azure Access key. For more information, see "[Importing Azure Access Key](#)."

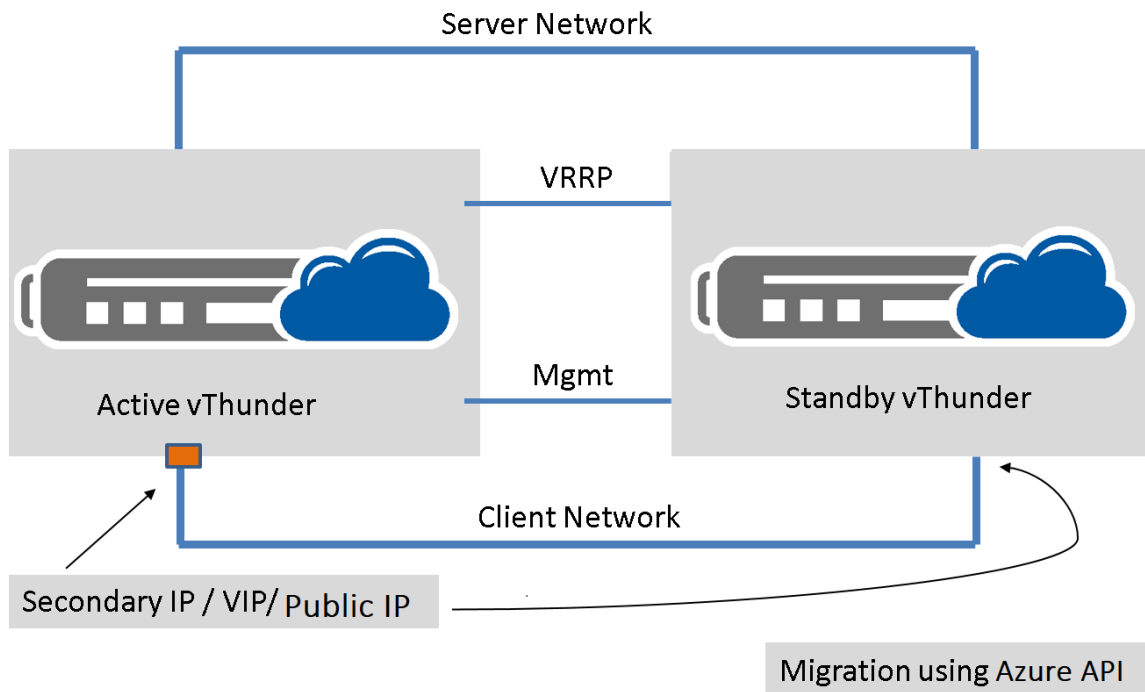
NOTE:

In ACOS 5.2.1-P7 and later releases, the `ip control-apps-use-mgmt-port` command controls the outgoing interface for vThunder device API calls. If this command is enabled, API uses the management interface. Otherwise, it uses the data interface. In the previous releases, the outgoing interface used the route settings for API calls.

The following is an architectural representation of the HA architecture and how the migration happens from an active HA instance to a standby HA instance.

In the figure, for the red box, which is the data port of the active vThunder, there is also a secondary IP address assigned, and the FIP is mapped to the secondary IP address. The VIP is a logical name for these IP addresses

Figure 48 : Azure HA Architecture



Configuring HA

The example discussed in this section uses two vThunder for HA. Each vThunder instance is configured to run a simple SLB configuration. Make appropriate changes in the steps if the vThunder is running a different configuration.

Perform the following steps:

1. Create two vThunder in a VNET.
Each vThunder must have one management interface and one or more data interfaces.
2. Launch two vThunder on Azure cloud. Each of this vThunder should have one management interface, one VRRP interface, and one or more data interfaces.
3. Complete the SLB configuration on both the vThunder instances.
4. Configure both vThunder to have unicast VRRP. One vThunder will be inactive state and other in a standby state after VRRP configuration as:

For example,

```
Running config on vThunder-1:
!
vrrp-a common
  device-id 1
  set-id 1
  enable
!
terminal idle-timeout 0
!
interface management
  ip address dhcp
!
interface ethernet 1
  enable
  ip address dhcp
!
interface ethernet 2
  enable
  ip address dhcp
!
vrrp-a vrid 0
  floating-ip 10.22.3.99
!
vrrp-a peer-group
  peer 10.22.2.7
  peer 10.22.2.8
!
slb server s1 10.22.3.6
  port 80 tcp
  health-check-disable
!
slb service-group sg1 tcp
  health-check-disable
  member s1 80
!
slb virtual-server vip 10.22.2.99
  port 80 http
```



```
    source-nat auto
    service-group sg1
!
!
end
```

Running config on vThunder 2:

```
!
vrrp-a common
  device-id 2
  set-id 1
  enable
!
terminal idle-timeout 0
!
interface management
  ip address dhcp
!
interface ethernet 1
  enable
  ip address dhcp
!
interface ethernet 2
  enable
  ip address dhcp
!
vrrp-a vrid 0
  floating-ip 10.22.3.99
!
vrrp-a peer-group
  peer 10.22.2.7
  peer 10.22.2.8
!
ip route 169.254.169.254 /32 10.22.1.0
!
slb server s1 10.22.3.6
  port 80 tcp
```

```

    health-check-disable
!
slb service-group sg1 tcp
    health-check-disable
    member s1 80
!
slb virtual-server vip 10.22.2.99
    port 80 http
    source-nat auto
    service-group sg1
!
!
end

```

5. Configure virtual IP address (VIP) on client-facing interface of active vThunder. Configure floating IP address (FIP) on server facing interface of active vThunder. Both IP addresses are private. To configure IP, apply the following steps:
 - a. Navigate to Azure portal. Select **network interface** which is client-facing.
 - b. Select the **Ip configurations** option from sidebar menu options.
 - c. Click **+Add** to add the VIP configuration which is mentioned in vThunder configuration. For outside traffic, attach public IP address. It will show the option to “enable” public IP address while creating a VIP configuration.
 - d. For floating IP, select **network interface** which is server facing and follow the same procedure mentioned in step b and c.
6. Configure public IP address to the client-facing VIP interface.

NOTE: While creating the VIP configuration from portal, you can enable public IP address for VIP configuration and attach Public IP address (if you have already created) if not then created new one and attach

7. Pass Data traffic through the active vThunder at this stage. Also, all the HTTP sessions needs to be synced on standby vThunder.
8. Run **vrrp-a config sync** command to sync the configuration between both vrrp-a neighbors as:

```
vThunder-Active(config) (NOLICENSE)#configure sync all <mgmt-ip-address>
```

```

User name []?admin
Password []?
vThunder-Active(config) (NOLICENSE)#sh log
Log Buffer: 30000
Jun 13 2019 08:27:58 Notice      [CLI]:Configuration sync to 10.22.1.8
succeeded
Jun 13 2019 08:27:56 Notice      [CLI]:HA SYNC : prepare to send
Jun 13 2019 08:27:56 Notice      [CLI]:HA SYNC : prepare completely
Jun 13 2019 08:27:56 Info        [CLI]:CONFIG SYNC: prepare to send
sync package
Jun 13 2019 08:27:56 Info        [CLI]:CONFIG SYNC : uuid file for
startup config [/a10data/etc/.startup-config.pri.uuid]
Jun 13 2019 08:27:56 Info        [CLI]:copy startup configuration for
HA sync
Jun 13 2019 08:27:56 Info        [CLI]:copy running configuration for
HA sync
Jun 13 2019 08:27:56 Info        [CLI]:CONFIG SYNC : partition (shared)
Jun 13 2019 08:27:56 Info        [CLI]:CONFIG SYNC : Start to prepare
Jun 13 2019 08:27:56 Info        [CLI]:CONFIG SYNC: whole sync
Jun 13 2019 08:27:56 Info        [SYSTEM]:config sync for partition
(shared)

```

9. Initiate “failover.” After fail-over, the new **Active** vThunder process the VIP, FIP and public IP addresses, by following step:
 - a. Perform “vrrp-a force-self-standby enable” on active vThunder.
 - b. Verify active becomes a new standby and old standby becomes new active.
 - c. Verify migration is under process by checking the ip configuration of interfaces from Azure portal.
10. To verify the configuration use `show run` command to shows configuration on active and standby vThunder as:

Basic Configuration For Azure HA: Running config on vThunder1:

```

!
vrrp-a common
 device-id 1
 set-id 1
 enable

```

```
!  
terminal idle-timeout 0  
!  
interface management  
  ip address dhcp  
!  
interface ethernet 1  
  enable  
  ip address dhcp  
!  
interface ethernet 2  
  enable  
  ip address dhcp  
!  
vrrp-a vrid 0  
  floating-ip 10.22.3.99  
!  
vrrp-a peer-group  
  peer 10.22.2.7  
  peer 10.22.2.8  
!  
slb server s1 10.22.3.6  
  port 80 tcp  
  health-check-disable  
!  
slb service-group sg1 tcp  
  health-check-disable  
  member s1 80  
!  
slb virtual-server vip 10.22.2.99  
  port 80 http  
  source-nat auto  
  service-group sg1  
!  
!  
end
```

Running config on vThunder 2:

```
!
```

```
vrrp-a common
  device-id 2
  set-id 1
  enable
!
terminal idle-timeout 0
!
interface management
  ip address dhcp
!
interface ethernet 1
  enable
  ip address dhcp
!
interface ethernet 2
  enable
  ip address dhcp
!
vrrp-a vrid 0
  floating-ip 10.22.3.99
!
vrrp-a peer-group
  peer 10.22.2.7
  peer 10.22.2.8
!
ip route 169.254.169.254 /32 10.22.1.0
!
slb server s1 10.22.3.6
  port 80 tcp
  health-check-disable
!
slb service-group sg1 tcp
  health-check-disable
  member s1 80
!
slb virtual-server vip 10.22.2.99
  port 80 http
  source-nat auto
  service-group sg1
```

```
!  
!  
end
```

If VM is deployed on Azure before 01/08/2019, then the following configuration for vThunder is mandatory to work with a service principal.

For example, Static Route:

```
ip route 168.63.129.16 /32 <mgmt g/w>
```

Initial vThunder Configuration

This chapter describes how to configure vThunder for Microsoft Azure.

The following topics are covered:

Configuring DHCP and the VIP in vThunder	68
Changing the VM Size	68
Changing the Disk Size	68
Adding More NICs by Using the Azure CLI	69
Deleting NICs by Using the Azure CLI	69
Initial vThunder Configuration	70
Configuring One Arm Mode SLB vThunder on Azure	72
Configuring a Multiple-Interface vThunder on Azure as an SLB	73

Configuring DHCP and the VIP in vThunder

1. SSH to the IP address of the vThunder instance.
2. Use the following CLI commands to force the interface to use the IP assigned by DHCP.

The following commands are required, and if not entered properly, other SLB-related commands may fail.

```
interface ethernet 1
    ip address dhcp
```

NOTE: Do not use the “no ip address dhcp” command or you will lose your SSH connection to vThunder. The workaround for a lost connection is to restart the vThunder instance.

Changing the VM Size

You can change the size of a vThunder VM by using either the Windows Azure Management Portal or Power Shell commands. The size of a virtual machine determines the vCPUs, RAM size, data disks, IOPS value, and so on for the VM.

For information on changing VM sizes, refer to [Resize a Linux virtual machine using CLI 2.0](https://docs.microsoft.com/en-us/azure/virtual-machines/linux/change-vm-size) at <https://docs.microsoft.com/en-us/azure/virtual-machines/linux/change-vm-size>.

Changing the Disk Size

You can expand the existing data storage of a vThunder VM. The default virtual hard disk size is 30 GB. It can be expanded upto 2048 GB.

NOTE: Once the disk is expanded, it cannot shrink.

For information on changing disk size, refer to <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/expand-os-disk>

Adding More NICs by Using the Azure CLI

You can add more NICs to a vThunder VM, if the VM size supports the NICs. If your vThunder VM does not support more NICs, you can change the VM size as described in [Changing the VM Size](#) and then add more NICs. For more information, refer to <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface-vm>.

1. To add a NIC to an existing vThunder instance, first deallocate and shutdown the VM:

```
az vm deallocate --resource-group testResourceGroup --name vThunderVM
az vm stop --resource-group testResourceGroup --name vThunderVM
```

2. Add the NIC with the **az vm nic add** command.

```
az vm nic add \
  --resource-group testResourceGroup \
  --vm-name vThunderVM\
  --nics myNic3
```

3. Start the VM with the following command:

```
az vm start --resource-group testResourceGroup --name vThunderVM
```

Deleting NICs by Using the Azure CLI

Before you delete a NIC from a vThunder instance, ensure that the VM is stopped and that there are at least two network interfaces attached to the VM. If you remove a primary network interface, Azure assigns the primary attribute to the network interface connected the longest to the VM. For more information, refer to <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface-vm>.

1. To remove a NIC from an vThunder VM, first deallocate and stop the VM as follows:

```
az vm deallocate --resource-group testResourceGroup --name vThunderVM
az vm stop --resource-group testResourceGroup --name vThunderVM
```

2. Remove the NIC with the `az vm nic remove` command.

```
az vm nic remove \  
  --resource-group testResourceGroup \  
  --vm-name vThunderVM \  
  --nics myNic3
```

3. Start the VM with the following command:

```
az vm start --resource-group testResourceGroup --name vThunderVM
```

Initial vThunder Configuration

This section describes how to configure IP connectivity on the vThunder management and data interfaces.

NOTE: To display a list of commands for a level of the CLI, enter a question mark as (?), and press **Enter**. It displays the list separately for each level. For syntax help, enter a command or keyword followed by a "space", then enter (?), then press **Enter**.

Login via ACOS CLI

1. Log into vThunder with the default **Username** and **Password** or the **ssh key-pair associated** with this instance.
2. Enable the Privileged EXEC level by typing `enable` and pressing the Enter key. There is no default password for Privileged EXEC mode; just press Enter.

```
vThunder>enable
```

```
Password:(just press Enter on a new system)  
vThunder#
```

3. Enable the configuration mode by typing `config` and pressing Enter.

```
vThunder#config
```

```
vThunder(config)#
```

It is strongly suggested that a Privileged EXEC enable password be set up as follows:

```
vThunder(config)#enable-password newpassword
```

Changing the Admin Password

A10 Networks recommends that you change the admin password immediately for security.

```
vThunder(config)#admin admin password newpassword  
vThunder(config-admin:admin)#
```

The vThunder is now network accessible for configuration under the new IP address and admin password.

Saving the Configuration Changes – write memory

Configuration changes must be saved to system memory to take effect the next time the vThunder is powered on. Otherwise, the changes are lost if the vThunder virtual machine or its host machine are powered down.

To write the current configuration to system memory:

```
vThunder(config)# write memory  
Building configuration...  
[OK]
```

Additional Resources – Where to go from here?

After you have logged into the vThunder GUI or CLI, you may be in need of some assistance to configure the device. More information can be found in the latest ACOS Release Notes. This document has a list of new features, known issues, and other information to help get you started.

It is recommended to use the basic deployment instructions that appear in the System Configuration and Administration Guide that is available on the [A10 Networks support](#) site.

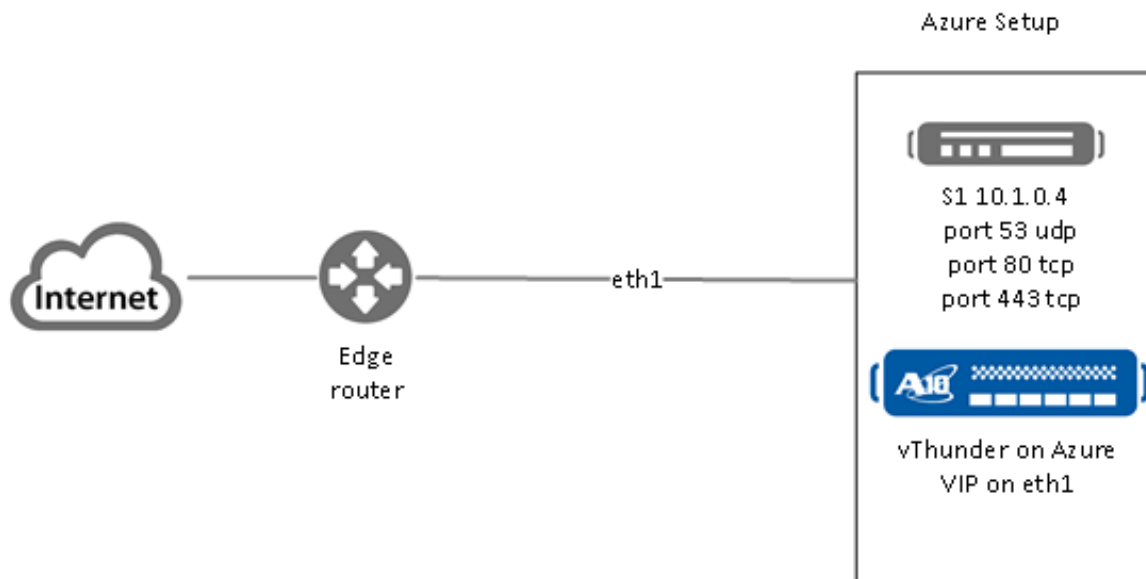
Configuring One Arm Mode SLB vThunder on Azure

The following image is a simple topological example of configuring vThunder on Azure as an SLB. In this example, the vThunder device has only one interface, ethernet1. The vThunder is connected to the gateway router and the real server s1 on ethernet1. Requests from clients for the virtual server are routed by the Layer 3 router to the vThunder device, which then forwards the request on the appropriate port on the real server. The server reply passes back through the vThunder device to the client.

To configure the vThunder instance on Azure as an SLB, perform the following:

1. Instantiate a 2-NIC vthunder in Azure.
For more information, see [Create a Single-Interface vThunder Instance](#).

Figure 49 : Single-Interface vThunder on Azure as an SLB



ACOS Code for Single-Interface SLB

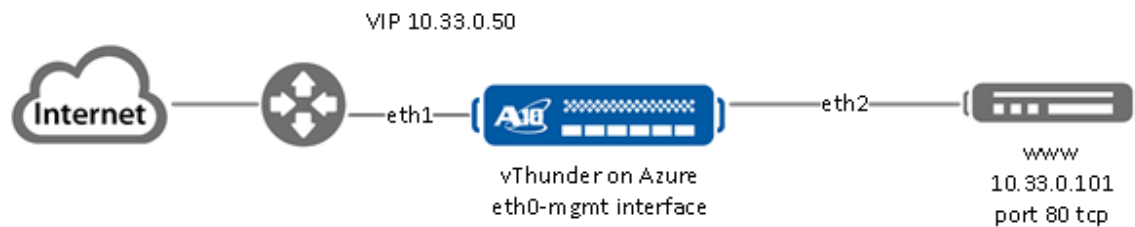
```
!Configure ethernet 1 interface.
interface ethernet 1
  enable
  ip address 10.1.0.1 255.255.255.224
```

```
! Configure the real server s1 by running the following commands.
ip nat pool p1 use-if-ip ethernet 1
slb server s1 10.1.0.4
    port 53 udp
    port 80 tcp
    port 443 tcp
!
!Configure the service groups and associate S1 to each service group.
slb service-group sg53 udp
    member s1 53
!
slb service-group sg80 tcp
    member s1 80
!
slb service-group sg443 tcp
    member s1 443
!
!Configure the virtual server vs1 and configure the ports.
slb virtual-server vs1 use-if-ip ethernet 1
    port 53 udp
        source-nat pool p1
        service-group sg53
    port 80 http
        source-nat pool p1
        service-group sg80
    port 443 https
        source-nat pool p1
service-group sg443
```

Configuring a Multiple-Interface vThunder on Azure as an SLB

The following image is a simple topological example of configuring vThunder on Azure as an SLB. In this example, the vThunder device is inserted directly between the gateway router and the real server. Requests from clients are routed by the Layer 3 router to the vThunder device, which then selects the real server and sends the request. The server reply passes back through the vThunder device to the client.

Figure 50 : Configuring vThunder on Azure as an SLB



Follow the procedure in [Create a Multiple-Interface vThunder Instance](#) to create the vThunder instance. While creating the instance, create the two interfaces, eth1 and eth2. Make sure all the interfaces are in different subnets. Associate a secondary IP address to any one of the data interfaces so that you can create a VIP for the interface. For more information, see [Adding a Secondary IP Address to a NIC by Using Azure CLI](#). Configure the vThunder as an SLB, for more information see [ACOS Code for Multiple-Interface SLB](#).

For example, the VIP for this example is 10.33.0.50.

ACOS Code for Multiple-Interface SLB

```
!Enable the interfaces for vThunder by performing the following commands.

interface ethernet 1
  enable
  ip address 10.33.0.36 255.255.255.224
!
interface ethernet 2
  enable
  ip address 10.33.0.100 255.255.255.224

!
!Configure the real server www and port by performing the following
commands.
slb server www 10.33.0.101
  port 80 tcp
!
```

```
!Configure the service group and associate the real server to the service
group.
slb service-group www tcp
  member www 80

!
!Configure the SLB server.
slb virtual-server www 10.33.0.50
  port 53 dns-udp
  gslb-enable
  port 80 http
  source-nat pool P2
  service-group www
!
!
end
```

Advanced vThunder Configuration on Microsoft Azure

This chapter describes advanced vThunder configurations for Microsoft Azure.

- [About Shared Polling Mode](#)
 - [Enabling Shared Polling Mode](#)
 - [Disabling Shared Polling Mode](#)
- [About Jumbo Frames](#)
 - [Enabling Jumbo Frames for vThunder](#)
- [Memory Support](#)
 - [vThunder Configuration on SLB or CGN](#)

About Shared Polling Mode

ACOS release 4.1.4-GR1-P1 and later only supports shared polling mode¹ for deployments having a total number of CPUs less than four. From ACOS release 5.2.0 onwards, this support is also provided for deployments having a total number of CPUs greater than four.

When shared polling mode is enabled, both I/O and data processing both are performed by all the vCPUs except the control CPU. If there is no I/O and data processing task in the queue, then the system automatically switches the CPU to idle mode to conserve CPU cycles.

NOTE: This mode is only preferred when performance or latency is not the key criterion for the success and the user wants to maximize host CPU utilization due to multiple VMs running on it.

Table 3 : ACOS Modes and Selection Criteria

Mode	Behavior	Criteria	Additional Requirements	Performance
Polling Mode	<p>In polling mode, both I/O and Data threads continuously poll for the packet and process it.</p> <p>This mode always consumes 100% of the allotted CPU cycles.</p> <p>Note: System poll mode is default for more than 4 vCPUs.</p>	High performance + low latency required, combined with SR-IOV.	Configure CPU pinning with NUMA.	High Performance

¹This support is available on BareMetal and vThunder on KVM, ESXi, Hyper V, AWS, Azure, and OpenStack.

Mode	Behavior	Criteria	Additional Requirements	Performance
Shared Polling Mode	When the shared poll mode is enabled, I/O and data processing are both performed on all cores except the control CPU.	Maximum utilization of CPU resources with some compromise on latency and performance.	The host needs to share physical CPUs with multiple VMs.	Lower CPU cycles consumed by the host.

NOTE: The shared polling mode feature is supported for ACOS 5.2.0 and later versions.

Enabling Shared Polling Mode

By default, shared polling mode is disabled. The following procedure has to be followed to enable Shared Polling mode:

1. Use the following CLI command from global config mode:

```
vThunder(config)#system shared-poll-mode enable
```

2. Exit global config mode and reload the vThunder instance using the following command:

```
vThunder(config)#exit
vThunder#reload
```

After vThunder finishes reloading, Shared Polling Mode will be enabled.

3. To verify Shared Polling Mode is enabled on the vThunder instance, check the output from the "show system shared-poll-mode" command.

```
vThunder(config)# show system shared-poll-mode
```

For example,

```
A2# show system shared-poll-mode
Shared poll mode is enabled
A2#
```

4. CPU distribution can be viewed, with the "show cpu" command as shown below. From

the output, it can be observed that no CPU does IO processing exclusively.

For example,

```
vThunder#show cpu
Time: Mar-2-2019, 01:39
          1Sec          5Sec          10Sec          30Sec
60Sec
-----
----
Controll  15%          15%          14%          18%
18%
Data1     0%           0%           0%           0%
0%
Data2     0%           0%           0%           0%
0%
Data3     0%           0%           0%           0%
0%
```

Disabling Shared Polling Mode

The following procedure is followed to disable Shared Polling mode:

1. Use the following command from global config mode to **disable** shared polling mode:

For example:

```
vThunder(config)#system shared-poll-mode disable
```

2. Exit global config mode and reload the vThunder instance using the following command:

```
vThunder(config)#exit
vThunder#reload
```

After vThunder finishes reloading, Shared Polling Mode will be disabled.

3. CPU distribution can be viewed, when shared poll mode is disabled with the "show cpu" command as shown below. From the output, it can be observed that some CPUs are designated for IO processing.

For example:

```
vThunder(config)#show cpu
Time: Mar-2-2019, 01:37
          1Sec          5Sec          10Sec          30Sec
60Sec
```

Control1	20%	21%	21%	21%
21%				
Data1	0%	0%	0%	0%
0%				
Data2	0%	0%	0%	0%
0%				
I/O1	0%	0%	0%	0%

NOTE: For one vCPU, the control and data usage are shown separately, but both share the same vCPU. The actual usage of the CPU is cumulative of control and data usage.

About Jumbo Frames

A jumbo frame is an Ethernet frame with a payload greater than the standard maximum transmission unit (MTU) of 1,500 bytes. This modification improves vThunder throughput and performance. Additional advantages of enabling jumbo frames include reduced interrupts and lower RAM utilization. For vThunder, jumbo frames are supported on ACOS 2.7.x, 2.8.x, 4.x, 5.x versions, and non-FTA platforms.

The following is a list of limitations and requirements for running jumbo frames for the vThunder-Intel and ENA devices:

- The vThunder instance must be running on top of an Intel 10Gb Ethernet Controller.
- Jumbo frames are not supported on 1Gb NICs.
- Supported jumbo frame packet types include: ICMP, UDP, and TCP
- vThunder can support jumbo frame packets up to a maximum size of 9216 bytes.

Enabling Jumbo Frames for vThunder

By default, jumbo frame support is disabled. Use the following appropriate CLI command to enable jumbo frame support on a vThunder data interface:

- For ACOS version 2.7.x: `enable-jumbo`
- For ACOS version 4.1.x: `system-jumbo-global enable-jumbo`

Set the MTU size on the vThunder data interface to a value ranging from 1500 to 9216 bytes. The configured value must be larger than any jumbo packet expected to arrive on

that data interface. To disable Jumbo Frames, run the command `no system-jumbo-global enable-jumbo`.

Memory Support

vThunder devices support 128 GB memory and provision the resources to satisfy the high number of users and their throughput in a virtualized environment.

Both NUMAs inside the compute host are used for provisioning the resources. Memory allocation is 64 GB from NUMA0 and 64 GB from NUMA1. This feature supports all platforms with 2 NUMA, 128 GB memory, and 35 virtual CPUs.

NOTE: The memory allocation limits change according to available memory.

vThunder Configuration on SLB or CGN

To configure vThunder and validate 128 GB memory support, perform the following:

1. Configure the vThunder on SLB or CGN.

For example

Configure vThunder with SLB as:

```
slb server s1 <Server-IP>
  port 80 tcp

slb server s2 <Server-IP>
  port 80 tcp

slb service-group sg1 tcp
  member s1 80
  member s2 80

slb virtual-server Platform-vip <VIP>
  port 80 tcp
  source-nat auto
  service-group sg1
```

Configure vThunder with CGN as:

```
interface ethernet {cli}
  enable
```

```

ip address <Data1-IP> <net mask>
ip nat inside

interface ethernet {srv}
enable
ip address <Data2-IP> 2xx.xxx.xxx.0
ip nat outside

class-list cgn_test
<cli_subnet> lsn-lid 1

cgnv6 lsn inside source class-list cgn_test

cgnv6 nat pool lsn-pool {pool} netmask /<net-mask>

cgnv6 lsn-lid 1
source-nat-pool lsn-pool

```

2. Verify 128 GB memory support for each vThunder instance in terms of vCPUs and increased application resources such as fixed-NAT public IP addresses, private users count, etc, perform the following:

- a. Launch the vThunder system with 128GB memory and 35 vCPUs ACOS image.
- b. Verify the limits using `show system resource-usage` and `show cgnv6 resource-usage` command.

```

vThunder(NOLICENSE)#sh system resource-usage
Resource
Maximum
-----
-----
14-session-count
201326592
nat-pool-addr-count
15000
class-list-ipv6-addr-count
1048576
class-list-ac-entry-count
9216000
auth-portal-html-file-size
auth-portal-image-file-size
max-aflex-file-size

```

Resource	Current	Default	Minimum	
14-session-count	12582912	12582912	3145728	
nat-pool-addr-count	10	10	10	
class-list-ipv6-addr-count	524288	524288	524288	
class-list-ac-entry-count	65536	65536	65536	
auth-portal-html-file-size	20	20	4	120
auth-portal-image-file-size	6	6	1	80
max-aflex-file-size	32	32	16	256

```

aflex-table-entry-count      102400      102400      102400
15728640
max-aflex-authz-collection-number  512         512         256
4096
radius-table-size           12000000    12000000    2000000
12000000
monitored-entity-count      32960       32960       32816
800288
authz-policy-number         128         128         32
2000
ram-cache-memory-limit      27648       27648       6912
27648
ipsec-sa-number             30000       30000       120
30000

```

cg n resource-usage

```

vThunder#show cg n resource-usage
Resource                               Current      Default      Minimum
Maximum
-----
--
lsn-nat-addr-count                   2048        2048         2048        20000
fixed-nat-ip-addr-count              20480       20480        20480       512000
fixed-nat-inside-user-count          256000     256000       256000
8000000
radius-table-size                    8000000     8000000      2000000
8000000
vThunder#

```

- c. Configure the maximum fixed-NAT IPs and inside users per the default limits and verify that they can be achieved. The default value is 30720k.
- d. Change the system resource for L4 sessions and reach the count.

NOTE: The accumulative L4 session count should be lesser than the current value. Every value don't exceed the current configured value.

- e. Verify that the configured limits take effect only after reboot.

NOTE: For some of the parameter update, reboot is not required. For example

- auth-portal-html-file-size
- auth-portal-image-file-size
- max-aflex-file-size

- f. On reboot configure the Minimum - maximum number of fixed-NAT IPs and inside "User/RADIUS/IP-List" value between pre-defined range (Min-Max).
- g. Reboot or reload the system to view the updated value.

Configure 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 \(iTOA\)](#)
- [External Thunder Observability Agent \(TOA\)](#)

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

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 the following:

- For ACOS v6.0.1 or later.
- For configuring vThunder using aXAPI or CLI to publish the 14 performance metrics on on Azure Application Insights directly from vThunder with outbound internet connectivity to access '*.microsoftonline.com' and '*.azure.com'.
- 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 1 minute.

To configure the Internal Thunder Observability Agent for a vThunder deployed on Azure, 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 on Azure, [External Thunder Observability Agent](#).



©2023 A10 Networks, Inc. All rights reserved. A10 Networks, the A10 Networks logo, ACOS, A10 Thunder, Thunder TPS, A10 Harmony, SSLi and SSL Insight are trademarks or registered trademarks of A10 Networks, Inc. in the United States and other countries. All other trademarks are property of their respective owners. A10 Networks assumes no responsibility for any inaccuracies in this document. A10 Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. For the full list of trademarks, visit: www.a10networks.com/company/legal/trademarks/.