Deployment Guide for Cisco CSR 1000v Series on Microsoft Azure

Updated Dec 2nd, 2016

Table of Contents

Overview of Cisco CSR 1000v Deployment on Microsoft Azure

Introduction

The Cisco Cloud Services Router (CSR) 1000v is a full-featured Cisco IOS XE router, enabling IT departments to deploy enterprise-class networking services in the Azure cloud. As a Cisco IOS XE based product, the CSR 1000v includes a wide range of features. Following are some examples of how the CSR is being used to enable enterprise-class hybrid clouds.

- **Extend enterprise VPN architectures into your private cloud:** The CSR 1000v supports IPsec, DMVPN, FlexVPN, Easy VPN, and SSLVPN (, and configuration, monitoring, and troubleshooting are all familiar IOS commands.
- **Interconnect multiple regions and clouds:** Using dynamic routing protocols such as EIGRP, OSPF, and BGP, construct multi-tier architectures within Azure, and interconnect with corporate locations or other clouds. Avoid the limits of native cloud networking tools.
- **Secure, inspect, and audit hybrid cloud network traffic:** Zone Based Firewall on the CSR 1000V provides an application-aware firewall. IP SLA and Application Visibility and Control

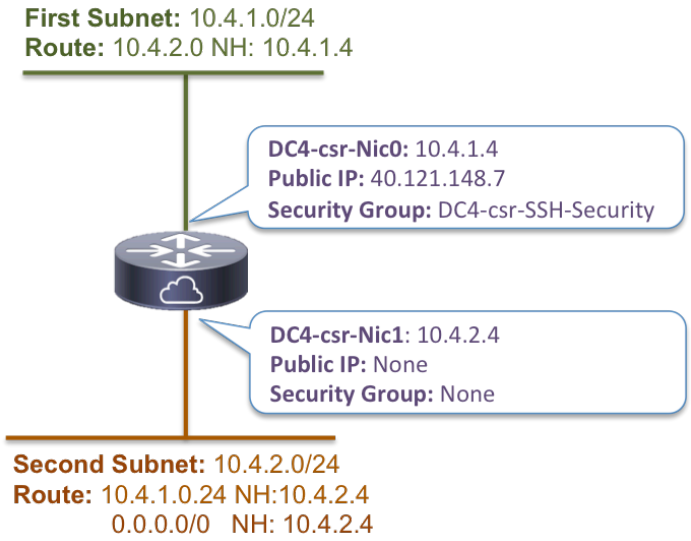
(AVC) on the CSR 1000v can proactively discover performance issues, fingerprint application flows, and export detailed flow data for real-time analysis and network forensics.

What is supported and what is not supported

In this release, to make deployment easier on Azure, the CSR offers a bundle with templates that creates all related resources together in a guided way, which includes the following: CSR + Virtual network + Routing Table + Security Group.

This deployment enables the following:

- Creates CSR virtual machine with 2 vCPU, 7G RAM and max 2 interfaces.
- Create public IP address to the interface on first subnet (NIC0).
- Create security group with inbound rules for the interface on the first subnet (NIC0).
- Create route table on Azure hypervisor router for each CSR subnets and add a default route for second subnet to point to CSR second interface (NIC1) IP address.



The following shows the known limitations for deploying CSR 1000v on Azure:

- Only CSR 1000v with 2 vnic is supported.
- GRE tunnels is not supported, Azure will drop GRE packets sent by CSR.
- Public/private key based ssh feature is not supported.
- Only D2 profile is supported (2 vCPU and 7G RAM).
- High availability through redundant CSR is not supported.

NOTE: This release of CSR 1000v on Azure only supports BYOL (Bring your own license). Users can copy a license to CSR or enable smart licensing.

Deploying Cisco 1000v on Microsoft Azure

Prerequisites

Before deploying CSR, please make sure the following checklist is fulfilled:

- Create an Azure account, for more information, please refer to Microsoft Azure Get Started Guide.
- Request a CSR license to enable throughput above 100K and enable desired technology package. For more information about license, please refer to CSR1000v data sheet.
- Plan out the settings for the CSR as shown in the following table. Note that the items with * are mandatory, and the values in Example column are used throughout the documentation.

Table 1. CSR 1000v Settings on Azure

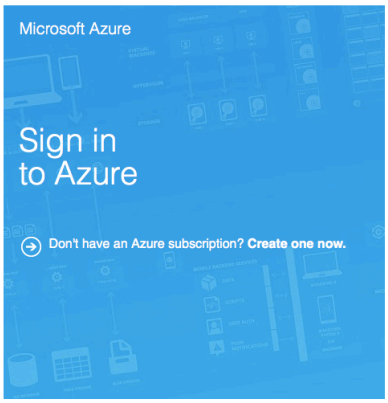
Parameters	Description	Example
***Resource Group name**	Resource Group name	"DC4"
***Subscription**	Azure user account subscription	Free Trial
***Location**	Azure Data center location	East US
***Storage Account name**	Storage account name	"dc4storagegroup"
***Storage Account Type**	Redundancy method provided by Azure	Standard-LRS (Locally Redundant, which is the only supported type in this release)
***Virtual network - name**	Virtual Network name	"vnet01"
***Virtual network - Address space**	CIDR of the virtual network	"10.4.1.0/16"
***Subnets - First subnet name**	Name of the subnet. It will be the subnet for gig1 of CSR	"DC4-pub"
***Subnets - First subnet address prefix**	CIDR for first subnet, which needs to be within Virtual network Address space	"10.4.1.0/24"
***Subnets - Second subnet name**	Name of the subnet. It will be the subnet for gig2 of CSR	"DC4-sub"
***Subnets - Second subnet address prefix**	CIDR for first subnet, which needs to be within Virtual network Address space	"10.4.2.0/24"
***Public IP address name**	Name for public IP address which is the NAT IP for CSR gig0.	"dc4csrpub"
Public IP address DNS name label	DNS name for the public IP address	"dc4csrpub"
***Virtual Machine name**	Name of the Virtual Machine (VM)	"DC4-csr"
Username	Admin Username for the VM	"admindemo"
***Authentication type**	Default is Password, but can highlight SSH public key	Password
***Password**	Password for the VM	"Cisco123"
***Virtual machine size**	The size of VM	1x Standard D2 (this is the default and only option in this release)

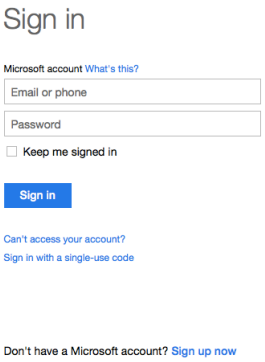
NOTE: The Azure CSR 1000v deployment simplifies the procedure by allowing users to create resources such as Resource Group, Storage Account, Virtual Network and Public IP on the fly during the CSR creation, which are specified in Step 2-5 in this documents. We recommend the first time user to go through the following steps to understand what resources can be created upfront and reused later if need to re-create CSR1000v. But as a quick start, the user can skip Step 2-5 and jump to Step 6 to launch CSR 1000v, and use Step 2-5 as a reference.

Step 1. Sign in and Customize Azure portal GUI

Sign In Azure portal GUI

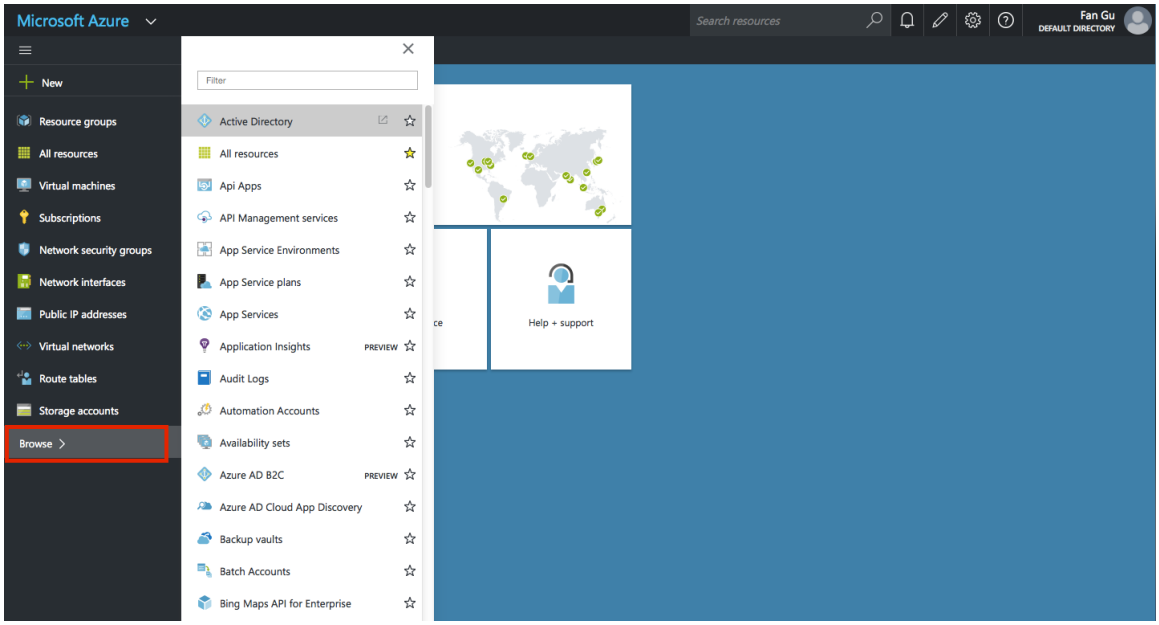
After creating Azure Subscriptions, a user should be able to login to the Azure portal.





Customize Azure portal GUI
In Azure, a user can optionally tag the frequently used objects (e.g. Virtual machines, Virtual network, etc), so they show up in the left hand side panel. This is optional, but we recommend customizing the left hand side panel for easier use.

To customize it, after logging into the Azure portal, click **Browse** and click the "star" and it will show up on the left hand side panel.

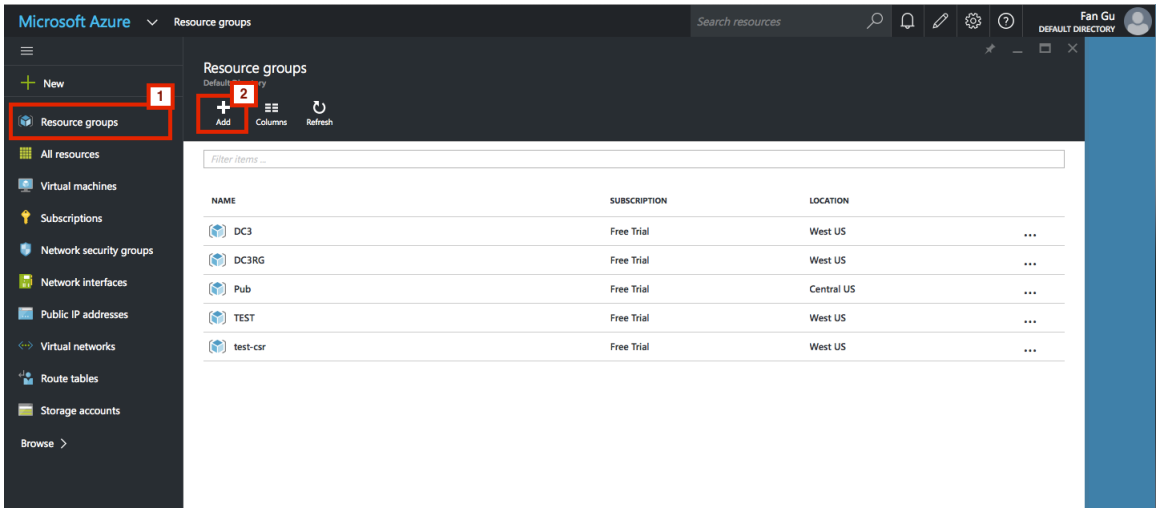


NOTE: In this documentation, it is assumed that the following objects are selected: **Resource group, Virtual machines, Subscriptions, Network security groups, Network interfaces, Public IP addresses, Virtual networks, Route tables, Storage accounts**.

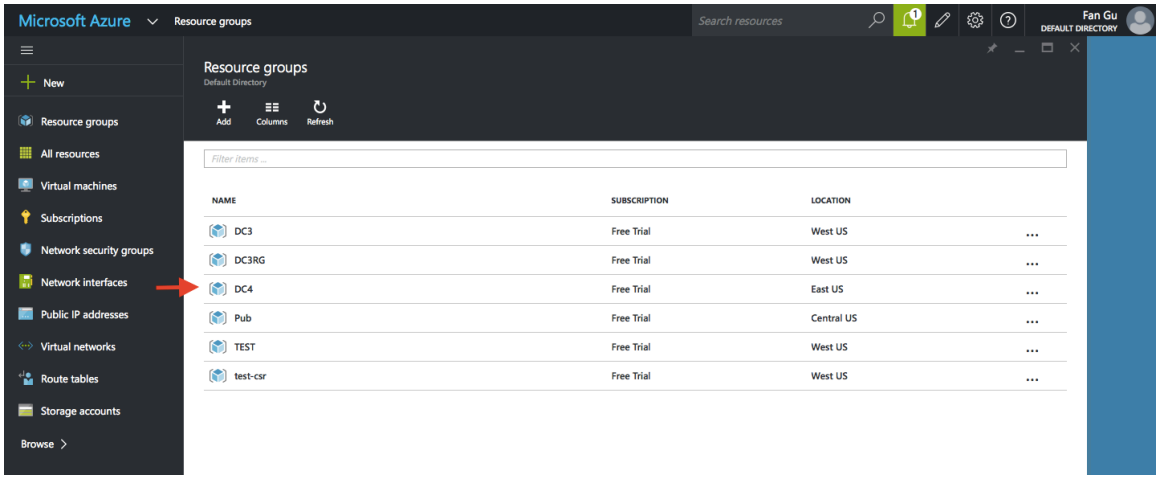
Add an Object
There are different ways to add an object from the GUI, and in this documentation, we do it through the left hand panel.

The following gives an example to create Resource Group, the other objects will be created and verified in the same way, which will not be repeated:

Click **Resource Group** on the left hand side panel, which will expend to *Resource groups* page that lists all the existing Resource groups. Click **Add** to create a new Resource Group as following:



To verify the object is created successfully, click the **Resource group** and it should show up in the Resource Groups listed below:



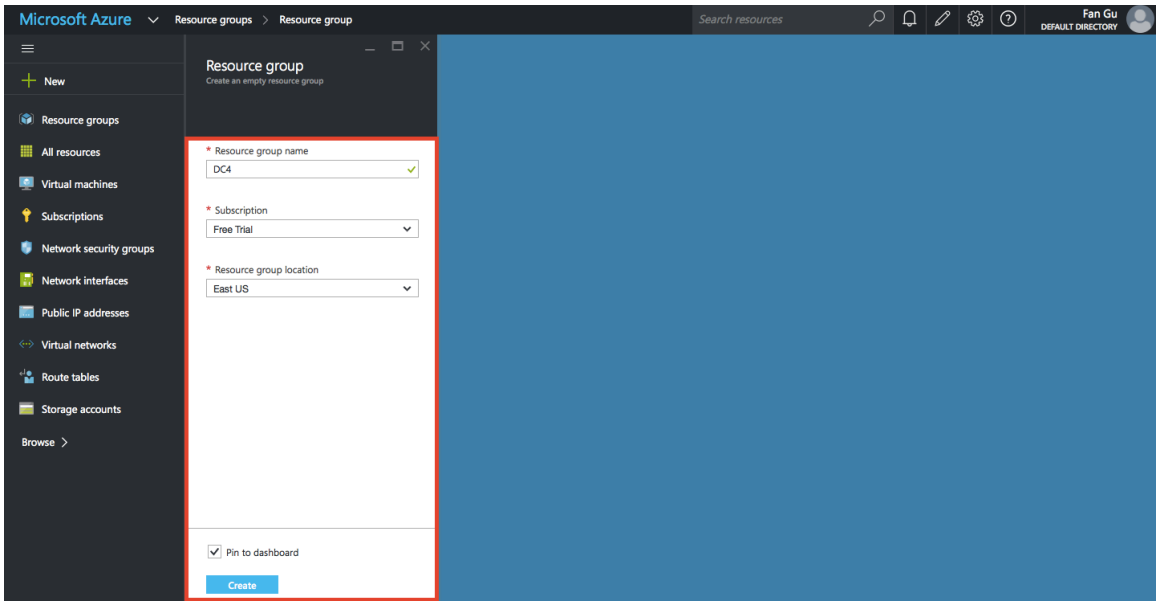
Step 2. Creating a Resource Group

A Resource Group in Azure refers to the set of resources that we can keep and delete all together. The resources include VMs, interfaces, virtual-network, routing-table, public-ip-address, security groups, routing tables, storage accounts. The resources in one resource group need to have a unique name. If you create objects that depend on other objects in different resource groups, the other resource cannot be deleted before you delete your object. Please refer to Resource Group article for more details.

TIP: Resource Group can be created on the fly during CSR deployment as well.

Step 2-1. Click **Resource Group** on the left hand side panel, and it will expand the *Resource Group* page which shows all the existing Resource Groups. Click **Add** on the top and it will expand to *Create Resource group* page**.**

Step 2-2. Type in the **Resource Group name**, select **Subscription** and **Resource group location** from the dropdown list. Click **Create** to create Resource Group "DC4".



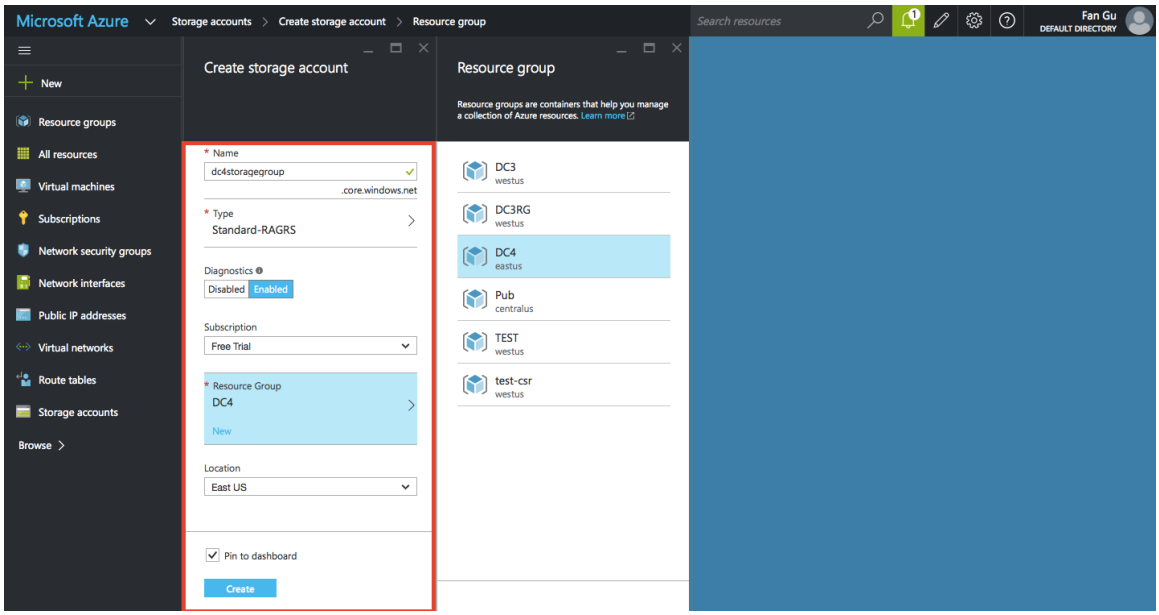
Step 3. Create Storage Account

A Storage Account in Azure is used to keep the VM disk file and boot-log. It belongs to a resource group. Not all resources need to have a storage account. Please refer to Azure Storage article for more details.

TIP: Storage Account can be created on the fly during CSR deployment as well.

Step 3-1. Click **Storage accounts** on the left hand side panel, which will expand the *Storage accounts* GUI. Click **Add** to navigate to the *Create storage account* page.

Step 3-2. Type in the Storage account **name**, select the **Storage account type**, select **Resource Group** "DC4" created in Step 2, make sure the **Location** is correct, in this case "East US". Click **Create** to create Storage account "dc4storageaccount".



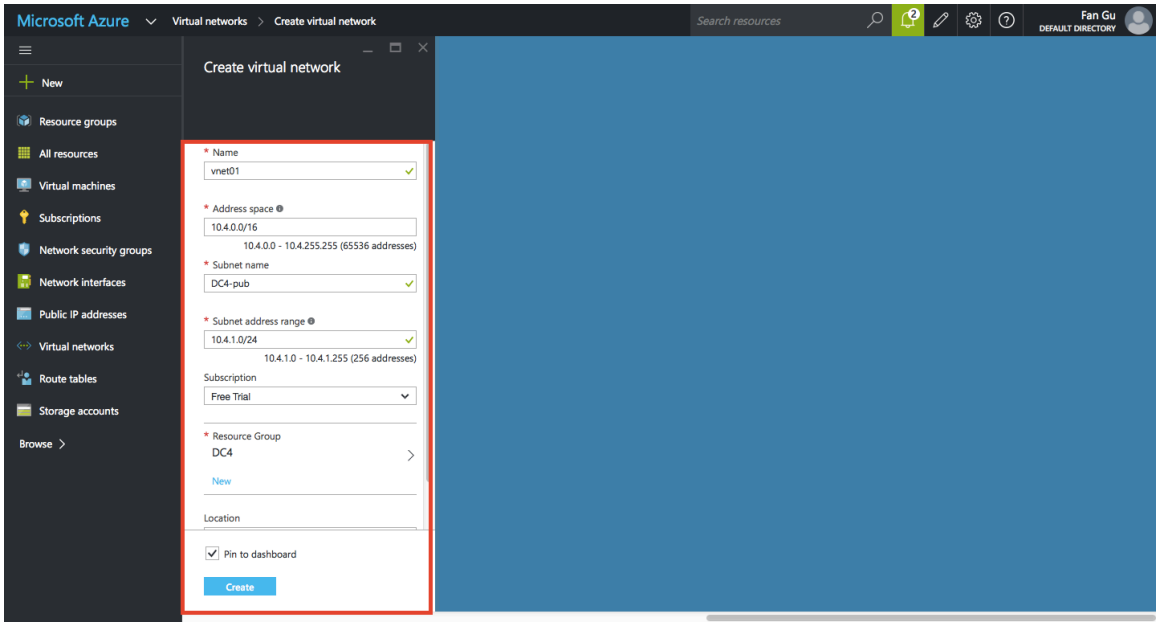
Step 4. Creating Virtual Network

Virtual Network is a representation of the private network, which provides logical isolation of Azure cloud. Please refer to Virtual Network article for more details.

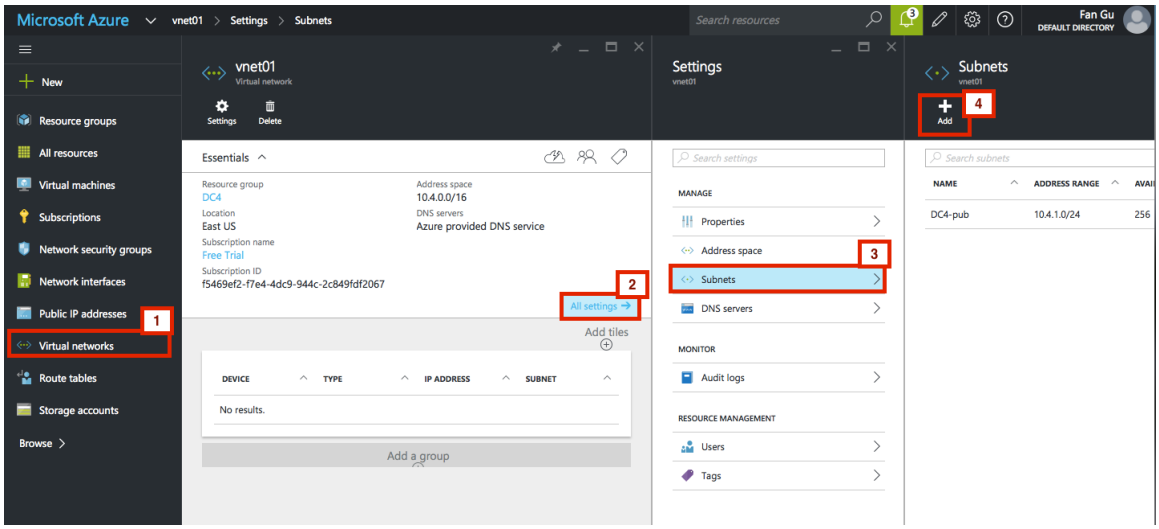
TIP: Virtual Network can be created on the fly during CSR deployment as well.

Step 4-1. Click **Virtual networks** on the left hand side panel, which will expand the **Virtual networks** GUI, then click **Add** to navigate to the *Create virtual network* page.

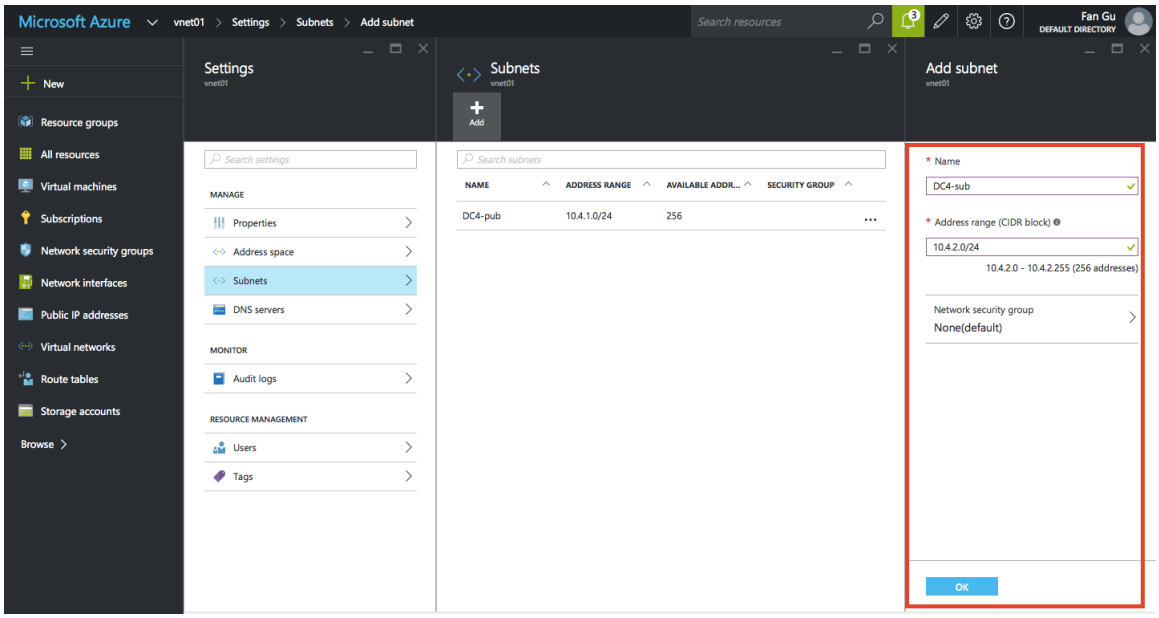
Step 4-2. Fill in the blank with info prepared in Table 1. Make sure that **Location** is correct, which in this case, it is "East US". Note that only one subnet can be created during initial Virtual networks creation.



Step 4-3. Add second subnet to the Virtual network. Click **Virtual networks** on the left hand side panel, and click the virtual network just created, in this case "vnet01", click **All Settings**, which will navigate to *Settings* page. Click **Subnet**, which will navigate to *Subnets* page. Click **Add** to add new Subnet.



Step 4-4. Type in **subnet name** and **CIDR** of the second subnet. Click **OK** to finish.



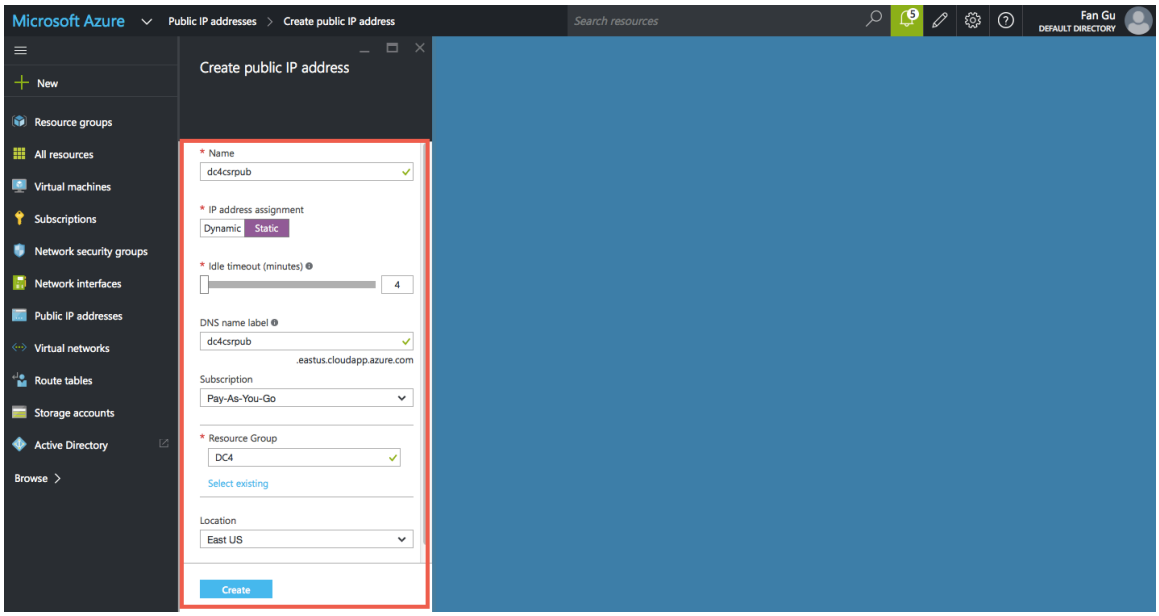
Step 5. Create public IP address

Public IP address is the IP address that users or devices from Internet can reach, and it is associated to a specific IP address. It is an one-to-one NAT performed by Azure hypervisor router. In this case, the CSR 1000v first subnet IP address will be assigned a public IP address. Reserved IP is recommended, since dynamic IP may cause the tunnel malfunction when the VM is shutdown/deallocated and boot up again. Please refer to Public IP article for more details.

TIP: Public IP can be created on the fly during CSR deployment as well.

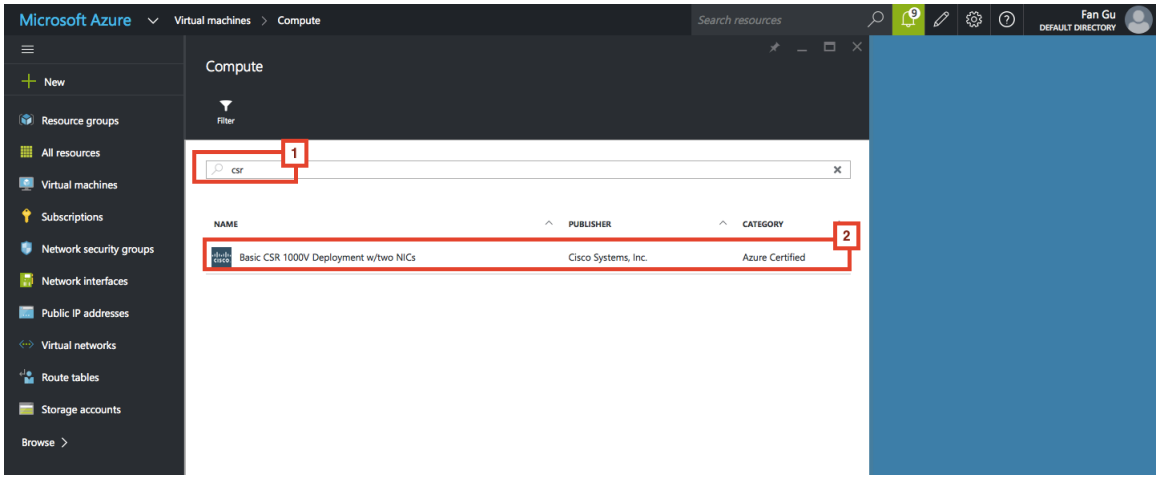
Step 5-1. Click **Public IP address** on the left hand side panel to expand the **Public IP address** page. Click **Add**, which will expand the *Create public IP address* page.

Step 5-2. Fill in the info from Table 1. Change the IP address assignment from **Dynamic** to **Static**. Click **Create** to finish.

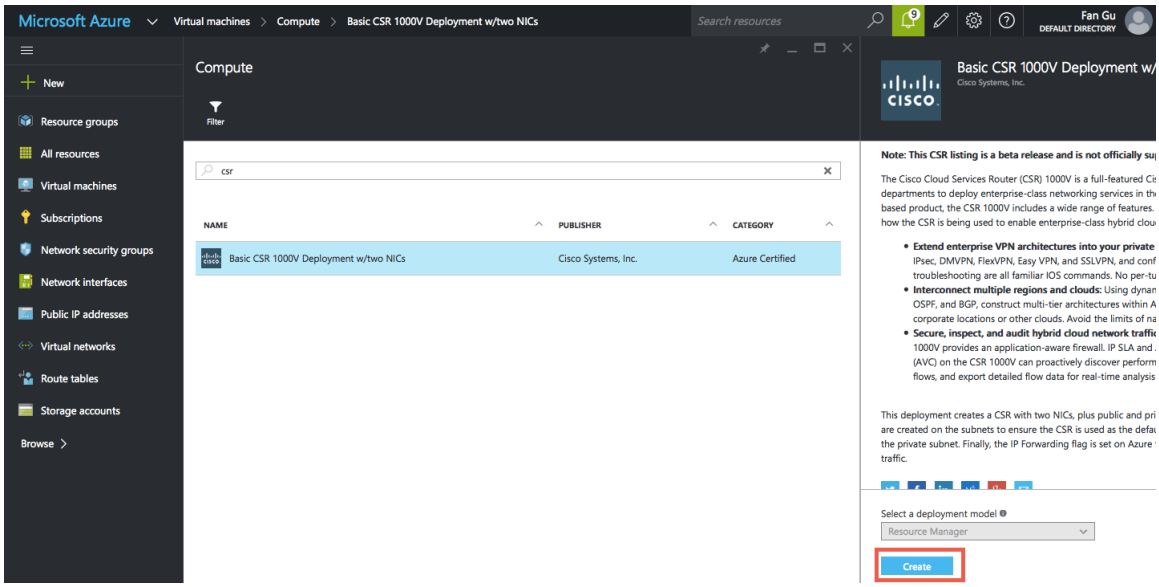


Step 6. Launching Cisco CSR 1000v virtual machine

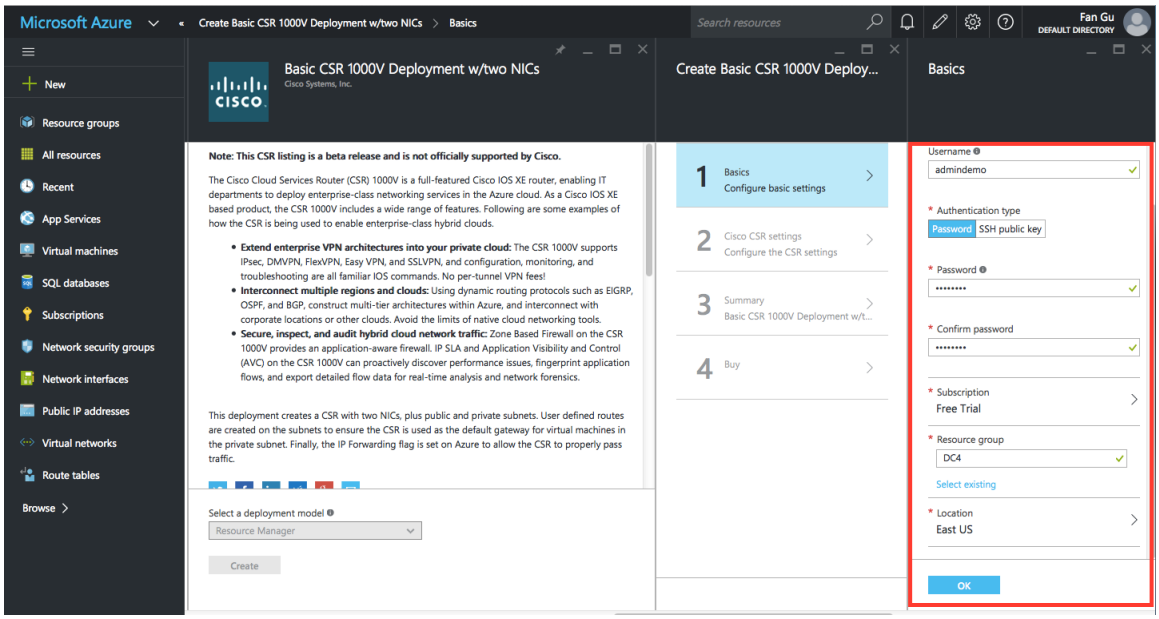
Step 6-1. Click **Virtual machines** from the left hand side panel, and it will expand the *Virtual machines* page. Click **Add** which will expand the *Compute* page. Type in "csr" and hit Enter on the keyboard, and it will find all the CSR available in Marketplace. Click **Basic CSR 1000v Deployment w/two NICs**.



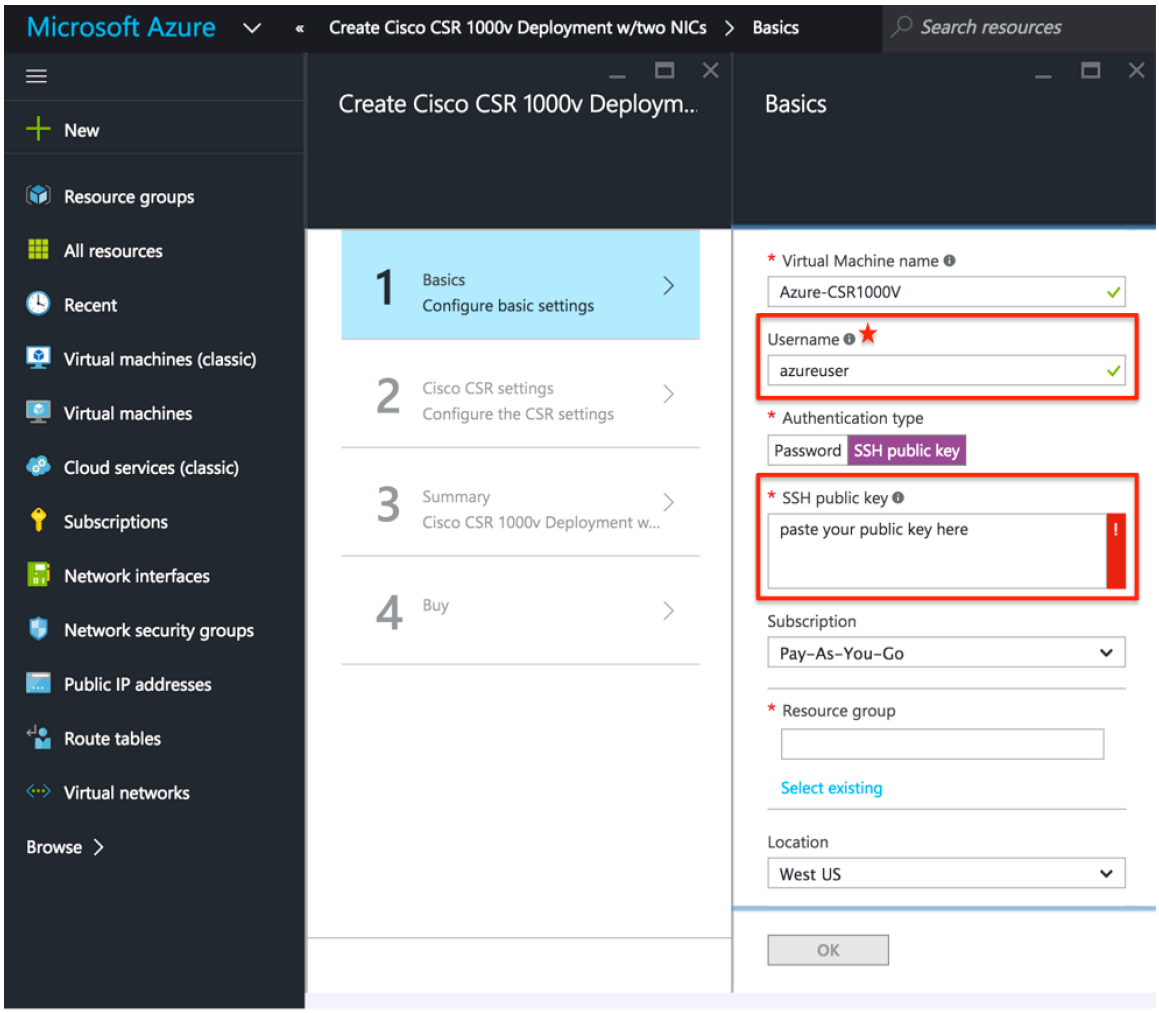
Step 6-2. At the end of introduction page, click **Create**.



Step 6-3. Click **1 Basics.** Fill in the blank with the info you prepared in Table 1., and click **OK**.

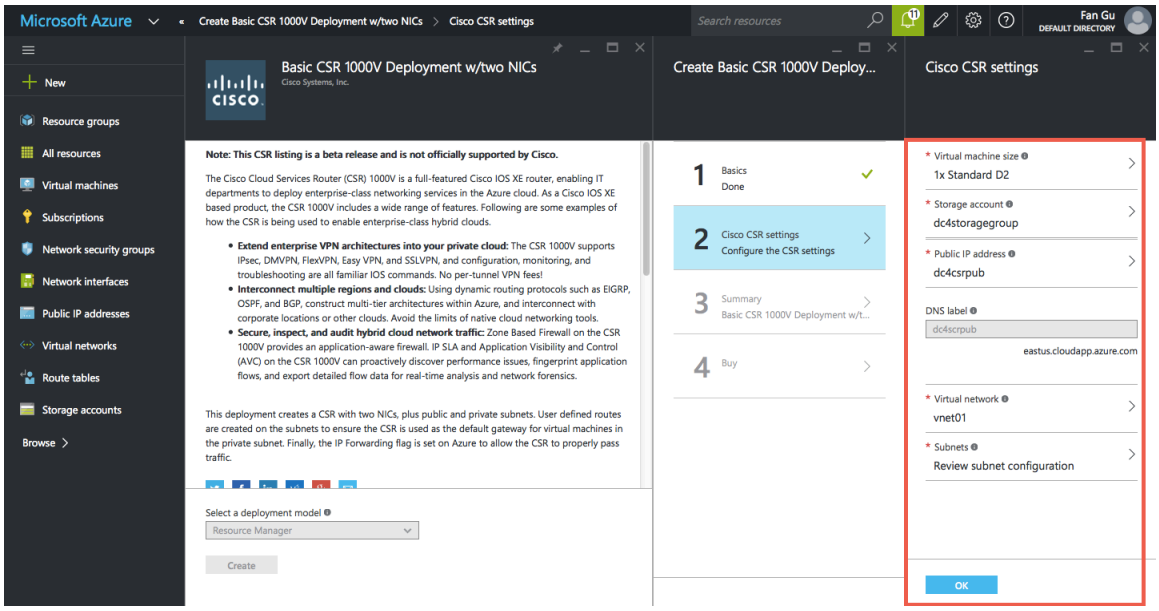


Starting from IOS-XE 3.16.02, you can use SSH public key to access the CSR. To use SSH public key, the "Username" field need to be "**azureuser**" due to current limitation. In the launching page, you can click the right small icon "i" (information) for help next to "Username" input field. You will find notice information of username restriction there.

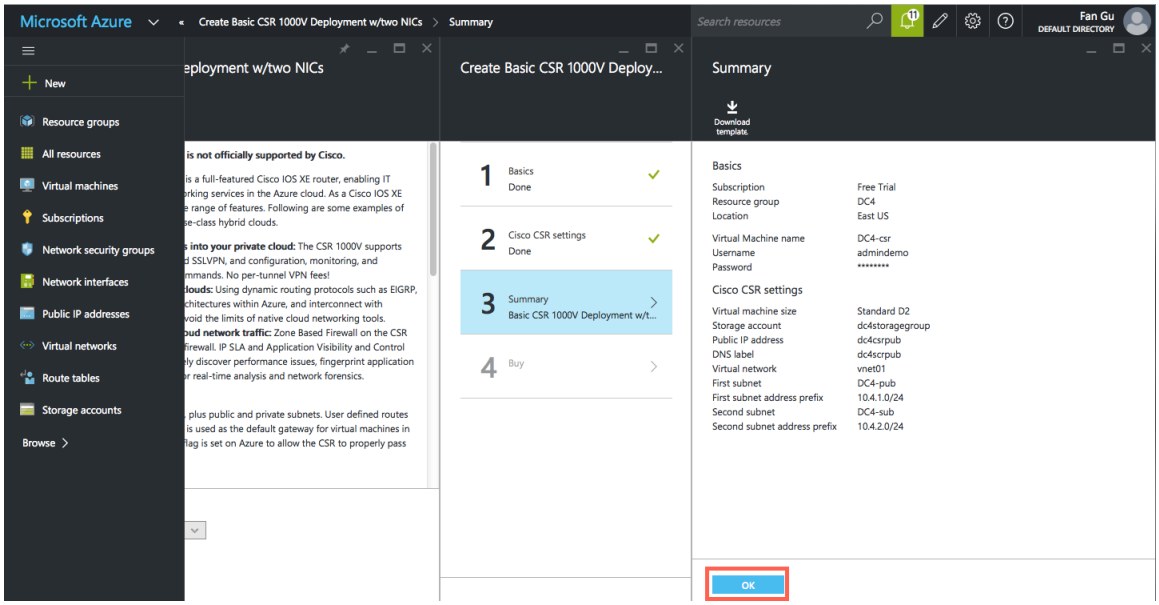


Step 6-4. The GUI will navigate to **2 Cisco CSR settings**. Click **Virtual machine size** to select the desired value (which in this release is Standard D2 only). Click **Storage group, Public IP address, Virtual network, and Subnets** to select the items created in previous steps if they are created previously. If they don't exit, you may create them on the fly, please refer to the previous steps for details. Then click **OK** to finish.

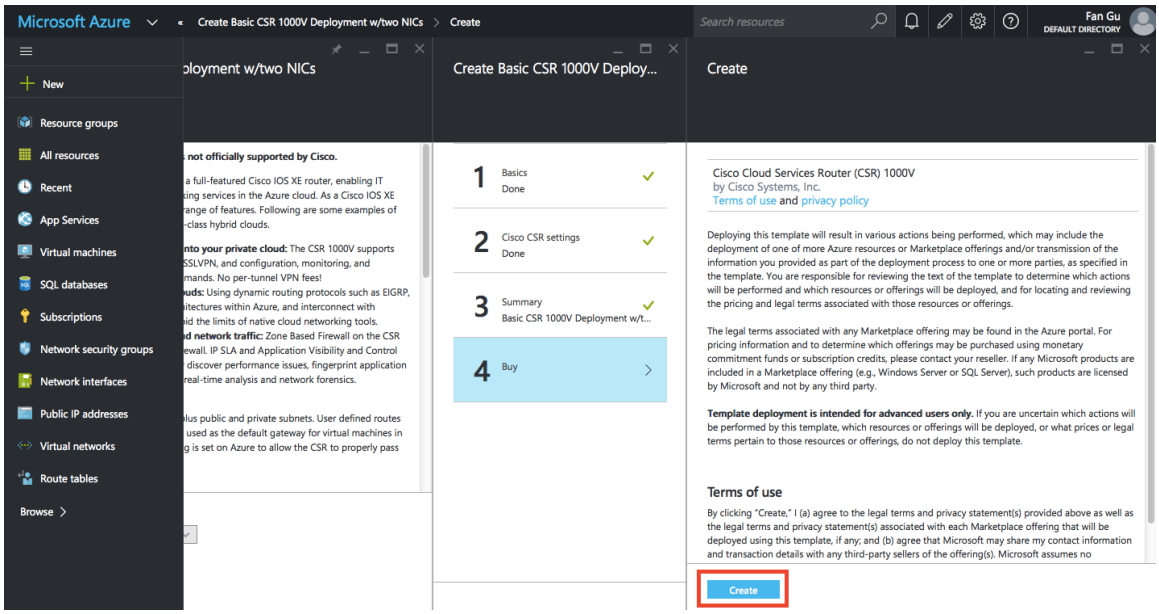
If your CSR has multiple NICs (we support 2 NICs or 4 NICs on Azure currently), first NIC will be used in public subnet. The other NICs will be used in the private subnets. The ip address of other NIC can be assigned by DHCP with "ip dhcp address" under interface configuration. It can also be set up statically, however make sure it's same with the ip address assigned by Azure.



Step 6-5. The GUI will navigate to **3 Summary**. Review and Click **OK** to confirm settings.

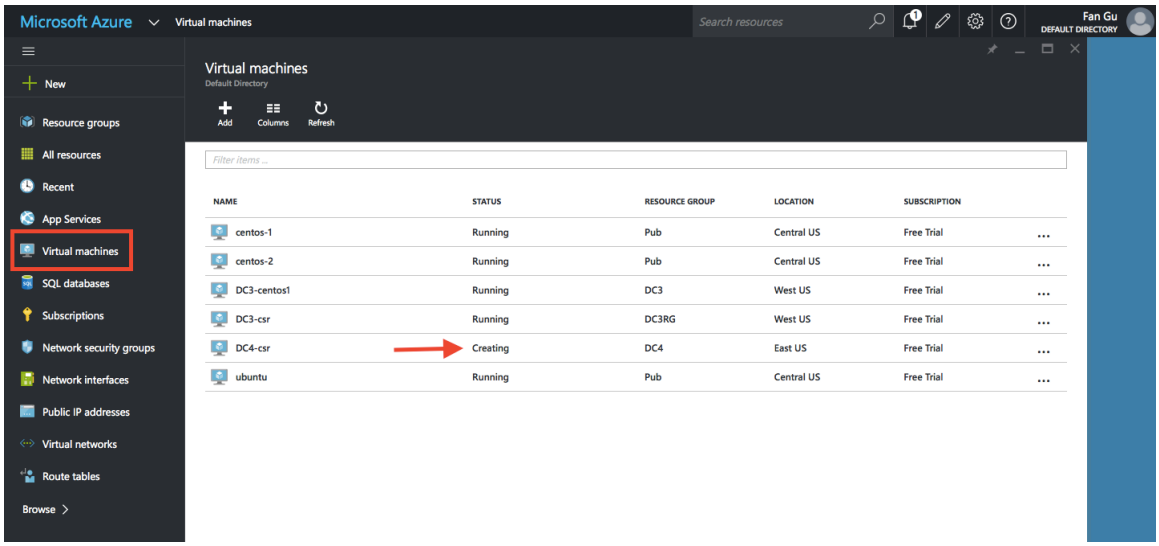


Step 6-6. The GUI will navigate to **4 Buy**, and click **Create** to confirm the purchase. It will take a couple of minutes for the VM to come up.

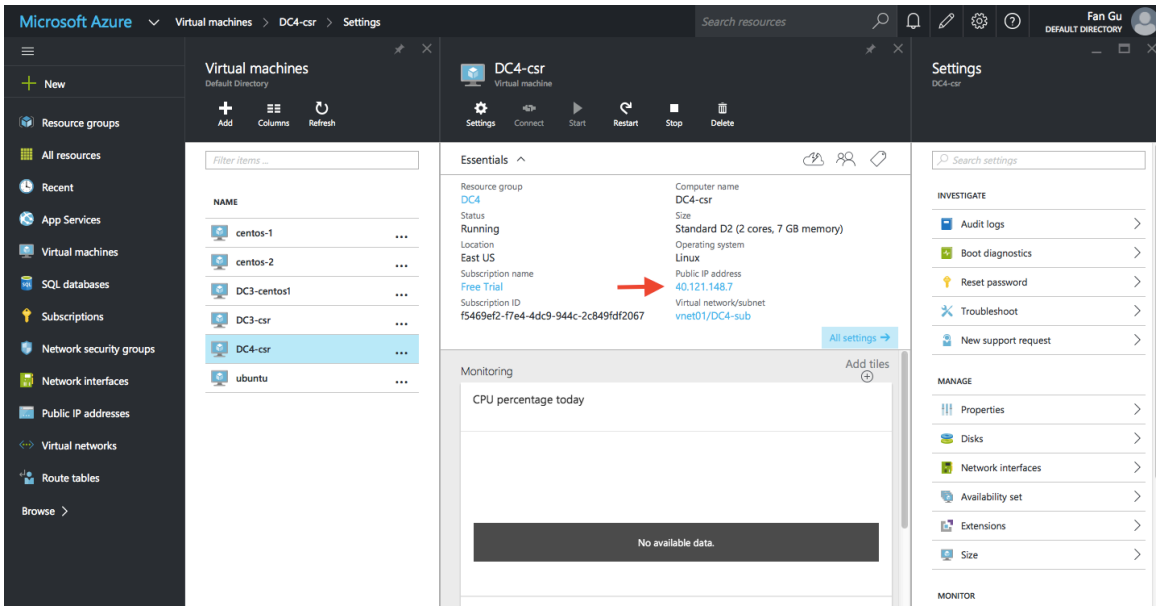


Step 7. Accessing the Cisco CSR 1000v virtual machine

To verify the VM creation status, on the left hand side panel, click **Virtual machines:**



When the status changed to **Running**, click the VM to see details. Take notes of the Public IP address.



In a terminal server of your choice, ssh to the server and use the username and password configured when creating the VM:

NOTE: Due to the mismatch of terminal timeout timing between Azure (4mins) and CSR (infinite), the user can be locked out of SSH after 4 mins idle status, without the line being cleared. Please refer to "Best Practice and Caveats" Section in this paper for details.

```
FANGU-M-40A8:~ fangu$ ssh -o ServerAliveInterval=60 admindemo@40.121.148.7
The authenticity of host '40.121.148.7 (40.121.148.7)' can't be established.
RSA key fingerprint is 94:79:e9:d2:2e:85:93:d6:52:41:cc:a3:d9:14:7f:5f.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '40.121.148.7' (RSA) to the list of known hosts.
Password: Cisco123

DC4-csr#

DC4-csr#show ip int br
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       10.4.1.4        YES DHCP   up                    up
GigabitEthernet2       10.4.2.4        YES DHCP   up                    up
DC4-csr#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 10.4.1.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 10.4.1.1
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C        10.4.1.0/24 is directly connected, GigabitEthernet1
L        10.4.1.4/32 is directly connected, GigabitEthernet1
C        10.4.2.0/24 is directly connected, GigabitEthernet2
L        10.4.2.4/32 is directly connected, GigabitEthernet2
      168.63.0.0/32 is subnetted, 1 subnets
S        168.63.129.16 [254/0] via 10.4.1.1
```

If you have set SSH public key at Step 6. You can access your CSR by

ssh –i <key> –o ServerAliveInterval=60 azureuser@<csr_address>

Step 8. Apply License to the CSR 1000v virtual machine

Cisco CSR1000v offers a variety of throughput and technology package licenses to meet each customer's requirements. Cisco CSR1000v also offers two licensing models: Cisco Software License (CSL) which is our traditional PAK based licensing model and Cisco Smart Licensing which allows customers to assign license to Cisco CSR1000v instances dynamically. Please see the CSR1000v datasheet and the CSR1000v managing licenses documents for more information.

A default CSR 1000v deployed has throughput of 100K with technology package AX, in order to increase the throughput to the desired level and enable the desired technology package a customer needs to install a CSR license as follows:

The following is an example of traditional manual licensing:

Copy the license file to CSR 1000v bootflash from local computer:

```
scp <license file>   <username>@<CSRAddress>:<license file name>
```

Login to CSR 1000v and install license:

```
license install bootflash:<license file>
```

After the license is applied, user can change the throughput as following:

```
DC4-csr(config)#platform hardware throughput level MB 250
```

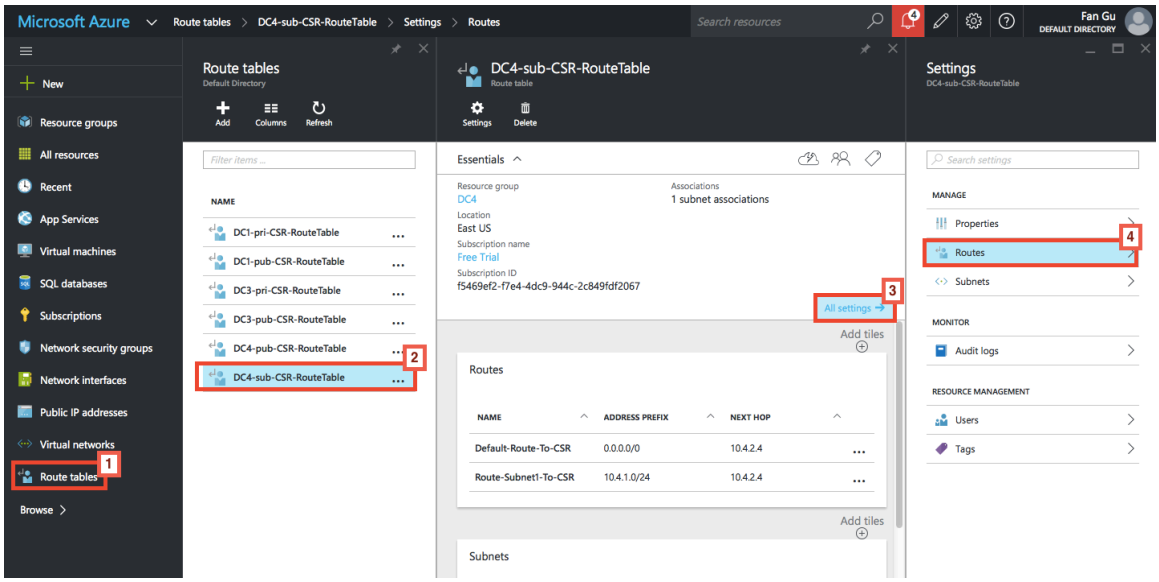
Modifying settings for CSR 1000v on Azure

Update Route Tables

In Azure, all VMs send packets to a hypervisor router, and the hypervisor forwards the packets based on the routing table associated with that subnet.

When creating CSR 1000v, two route tables are created and they are associated to each subnet respectively. A default route is created for the second subnet to point to the CSR, so all the VMs created on this subnet will use CSR as the default route. Please refer to Figure 1.

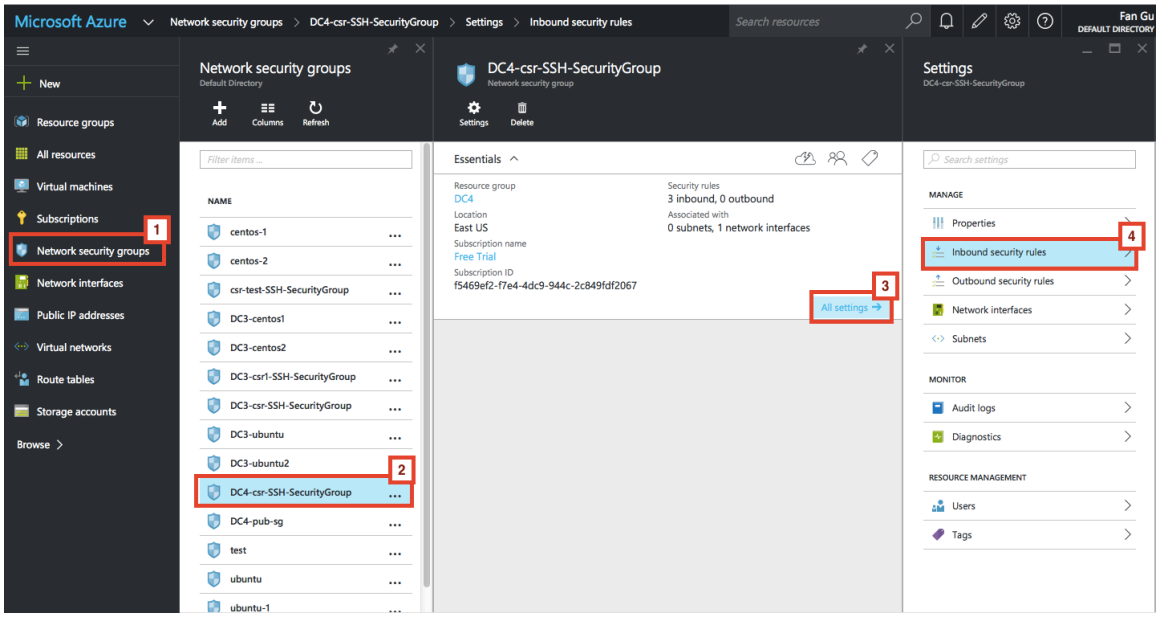
But if this behavior needs to change, a user can change it from the Azure portal GUI. Click **Route Table** on the left hand side panel, which will navigate to *Route tables* page, find the target route table, and click **All Settings**, which will expend the *Settings* page, click **Routes** to add/modify routes.



Update Security Group

A Security Group controls what ports/destinations the hypervisor allows/denies for certain interfaces. When creating CSR, a new Security Group is created for First subnet inbound interface by default. For CSR1000v virtual machines, if deployed through this deployment, the following ports are added for inbound Internet traffic: tcp 22, UDP 500 and UDP 4500, the rest are denied.

To modify Security group, click **Network security group** on left hand side panel, which will navigate to *Network security group* page. Click the target network security group, which will expand the details page. Click **All Settings**, which will expand the *Settings* page. Click **inbound security rules** from *Settings* GUI page, and click **Add** to add additional rules.



Configuration Example

Enable IPsec VPN between CSR 1000v on Azure and AWS clouds

IPSec VPN can be setup between CSRs in Azure and AWS cloud, below is an example:

Azure CSR Configuration	AWS CSR Configuration
crypto isakmp policy 1 encr aes hash sha256 authentication pre-share group 14 crypto isakmp key cisco123 address 0.0.0.0 crypto ipsec transform-set T1 esp-3des esp-md5-hmac mode transport crypto ipsec profile P1 set transform-set T1 interface Tunnel0 ip address 3.3.3.1 255.255.255.0 tunnel source GigabitEthernet1 tunnel mode ipsec ipv4 tunnel destination 104.45.154.184 tunnel protection ipsec profile P1 end !!!! To test, create loop back interface and static route!!!!! interface Loopback1 ip address 5.5.5.5 255.255.255.255 end ip route 6.6.6.6 255.255.255.255 Tunnel0	crypto isakmp policy 1 encr aes hash sha256 authentication pre-share group 14 crypto isakmp key cisco123 address 0.0.0.0 crypto ipsec transform-set T1 esp-3des esp-md5-hmac mode transport crypto ipsec profile P1 set transform-set T1 interface Tunnel0 ip address 3.3.3.2 255.255.255.0 tunnel source GigabitEthernet1 tunnel mode ipsec ipv4 tunnel destination 52.8.244.19 tunnel protection ipsec profile P1 end !!!! To test, create loop back interface and static route!!!!! interface Loopback1 ip address 6.6.6.6 255.255.255.255 end ip route 5.5.5.5 255.255.255.255 Tunnel0

Differences between CSR 1000v on Azure and AWS

There are some differences when deploying CSR 1000v on Azure and AWS. The following table highlights some of the differences:

Table 2. Comparing CSR 1000v on Azure and AWS

Function	CSR1000v on Azure	CSR1000v on AWS
Number of vNICs	2/4/8 interfaces	Multiple interfaces (>2)
Multiple IP address	Multiple IP per vNIC	Multiple IP per vNIC
GRE tunnel	Doesn't support GRE tunnel	Support GRE tunnel
Redundancy	Doesn't support Redundancy. It's coming in 2017.	Support Routing Redundancy through 2 CSR instances
Attach/Detach interface on the running CSR	Not supported	Supported
Overlapping IP subnet	Doesn't support overlapping IP subnet in different virtual network	Support overlapping IP subnet in different VPC

Best Practices and Caveats

1. It is recommended to keep all resources in the same Resource Group, so when need to clean up the whole setup, just need to remove the Resource Group.

2. When the CSR virtual machine is deleted, not all the resources are deleted (route table, security group, public IP, network interfaces), so when creating a new CSR with the same name, the resources maybe re-used, if it is not desired, please either manually remove these resources , remove the Route Group that contains these resources, or create a new CSR with a different name.

3. This applies to the current 3.16.0 image. By default, CSR configuration configured terminal VTY time out as infinite (exec-timeout 0 0), but Azure has a default timeout for the terminal server every 4 minutes. This causes the user to be locked out of the terminal session without clearing the line. To work around it, there are two methods: 1. Set ServerAliveInterval=60 during ssh session (as shown below). 2. Change the exec-timeout to non-zero values (e.g. exec-timeout 4 0).

4. Currently, the only supported login is through username/password that user created during the CSR 1000v launching.

Other Related Resources

DMVPN is supported on Azure as well, and the configuration is similar to AWS, please refer to Extending Your IT Infrastructure Into Amazon Web Services Using Cisco DMVPN and the Cisco Cloud Services Router 1000v Series white paper.