Deploy a VOS Branch in Azure Using a CMS Connector in Versa Director

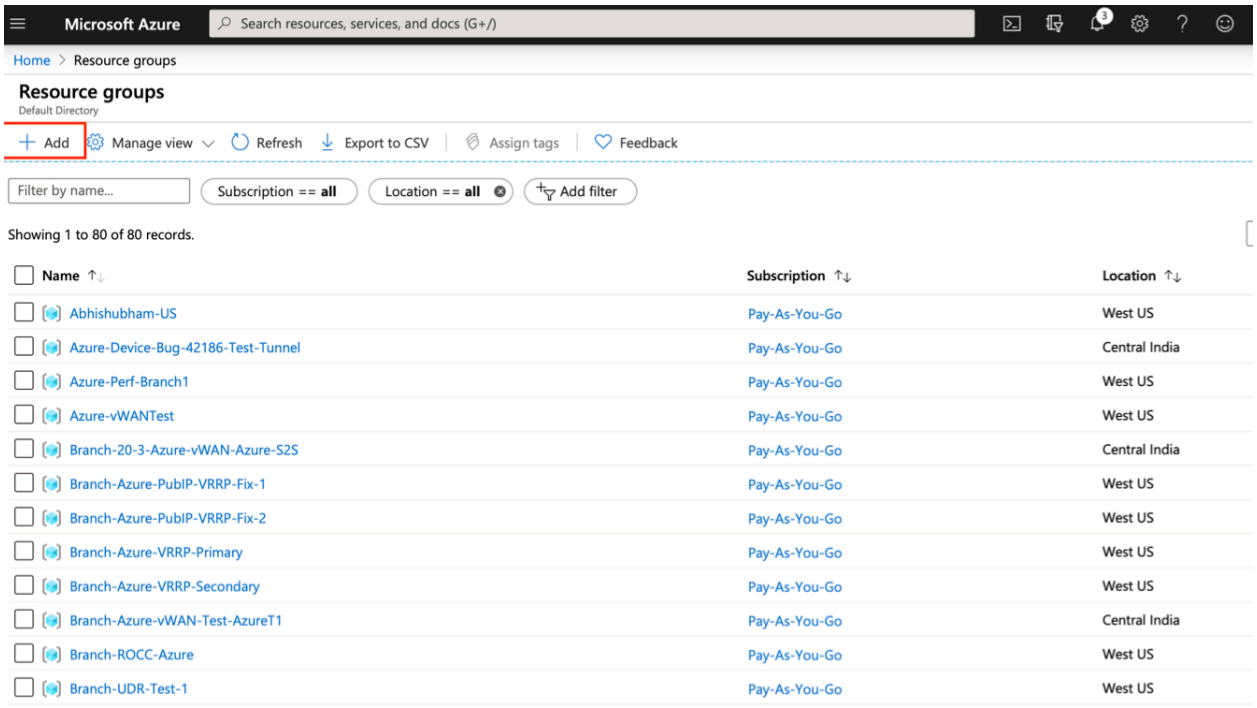
For supported software information, click here.

This article describes how to create a CMS connector on a Director node to automate the bringup of a Versa Operating System™ (VOS™) branch in Azure. To create the CMS connector, you do the following:

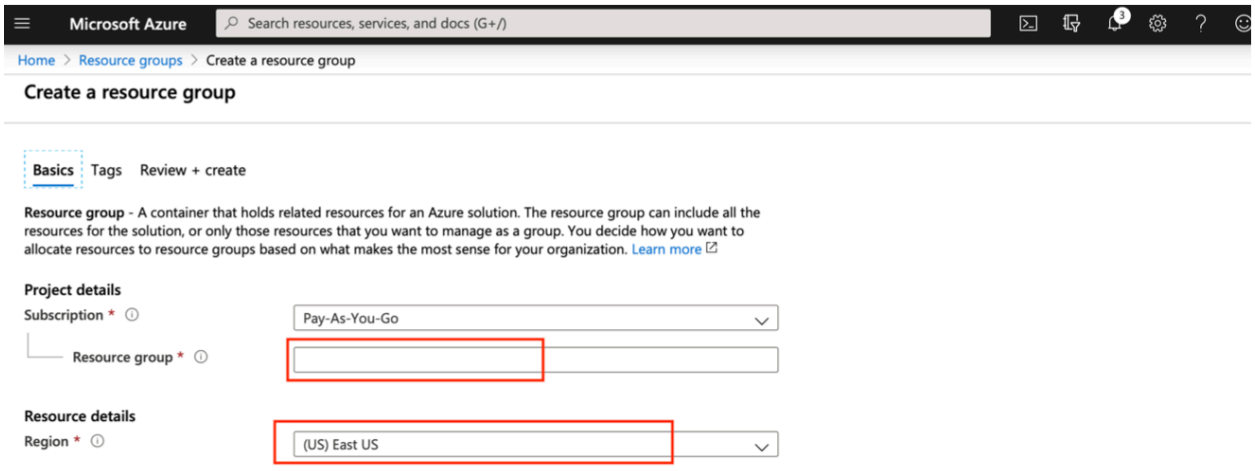
1. Create resources in Azure.
2. Gather information from Azure.
3. Create a CMS cloud connector on the Director node.
4. Deploy the VOS branch using the CMS connector.
5. Connect to the VM instance and verify it.

Create Resources in Azure

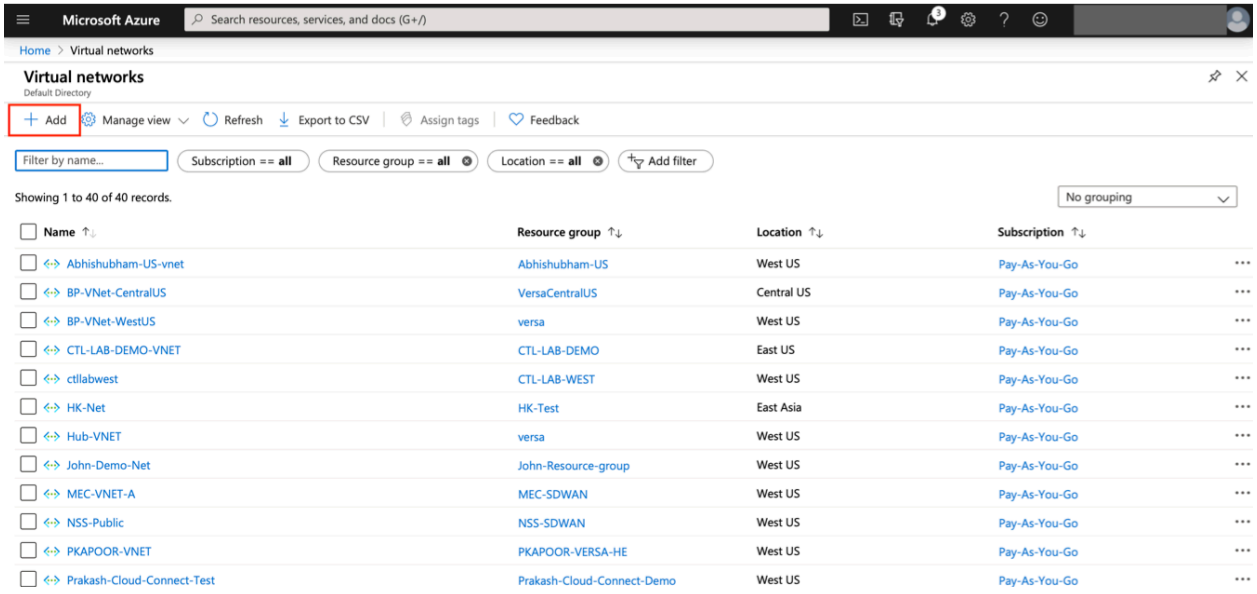
1. Log in to the Azure portal with the user's credentials.
2. Modify one of the user's existing resource groups, or create a new one. To create a new resource group, in the Resource Groups section, click Add.



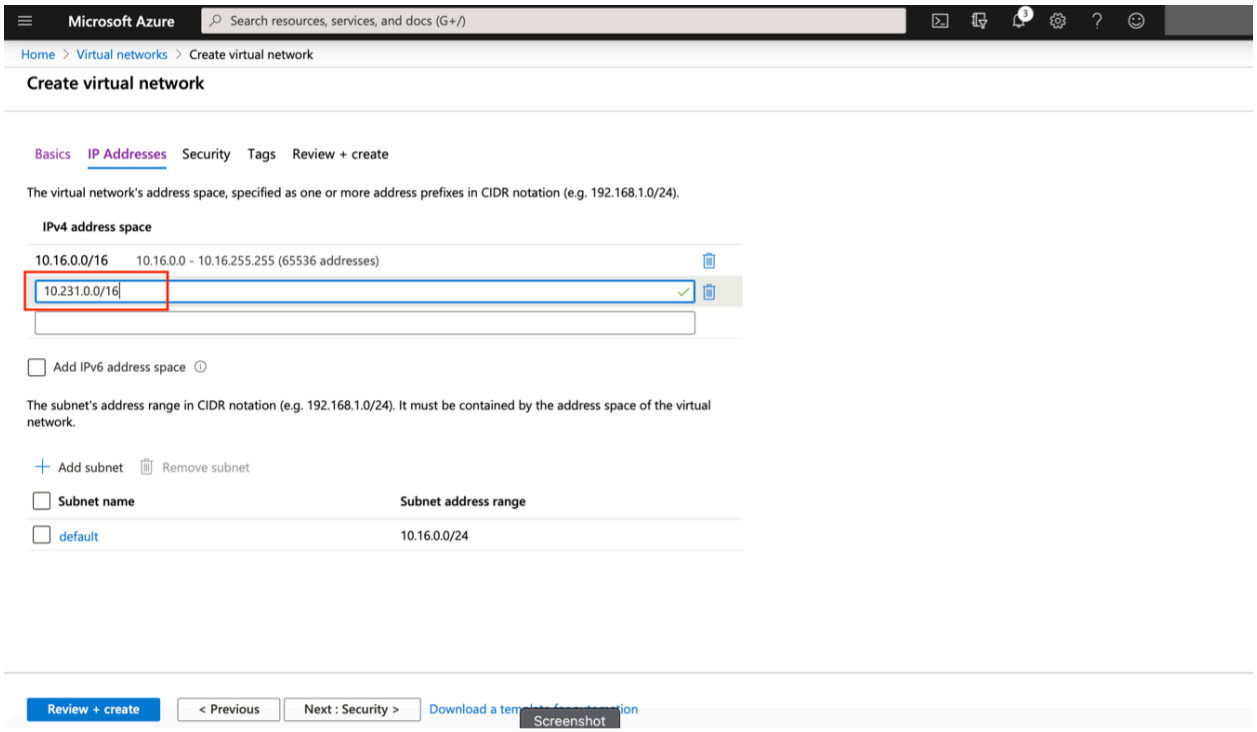
3. Enter a name for the resource group, and select the region in which to create it.



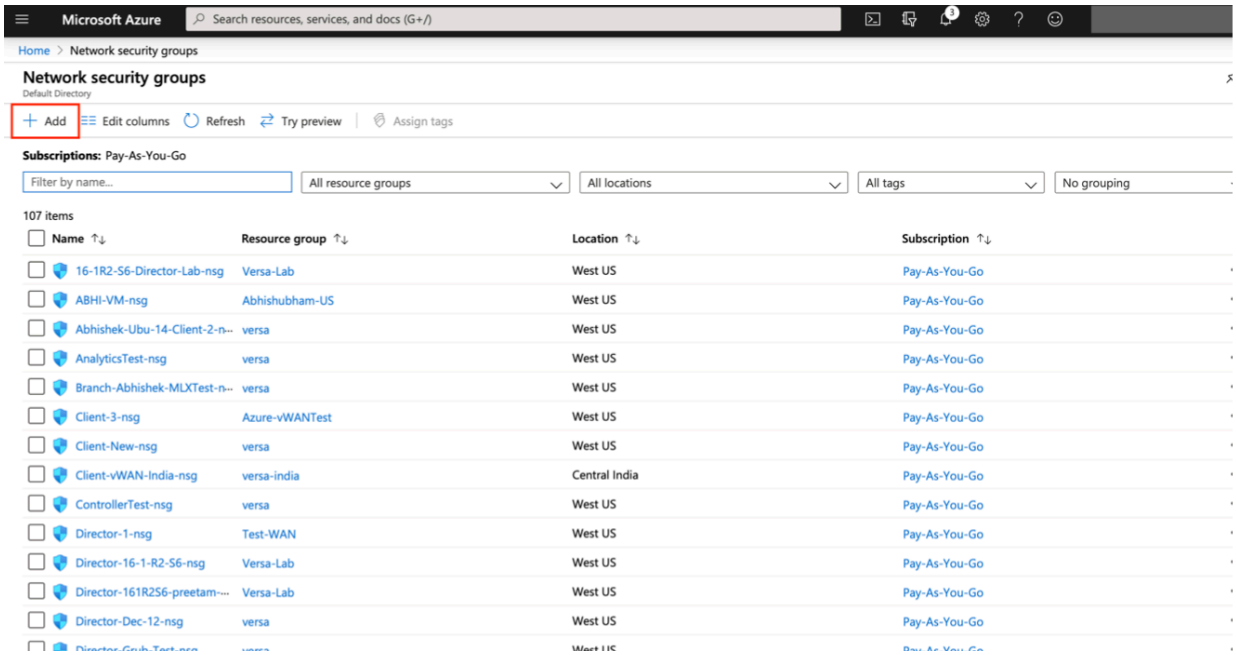
4. To create a new virtual network, click + Add under Virtual Networks.



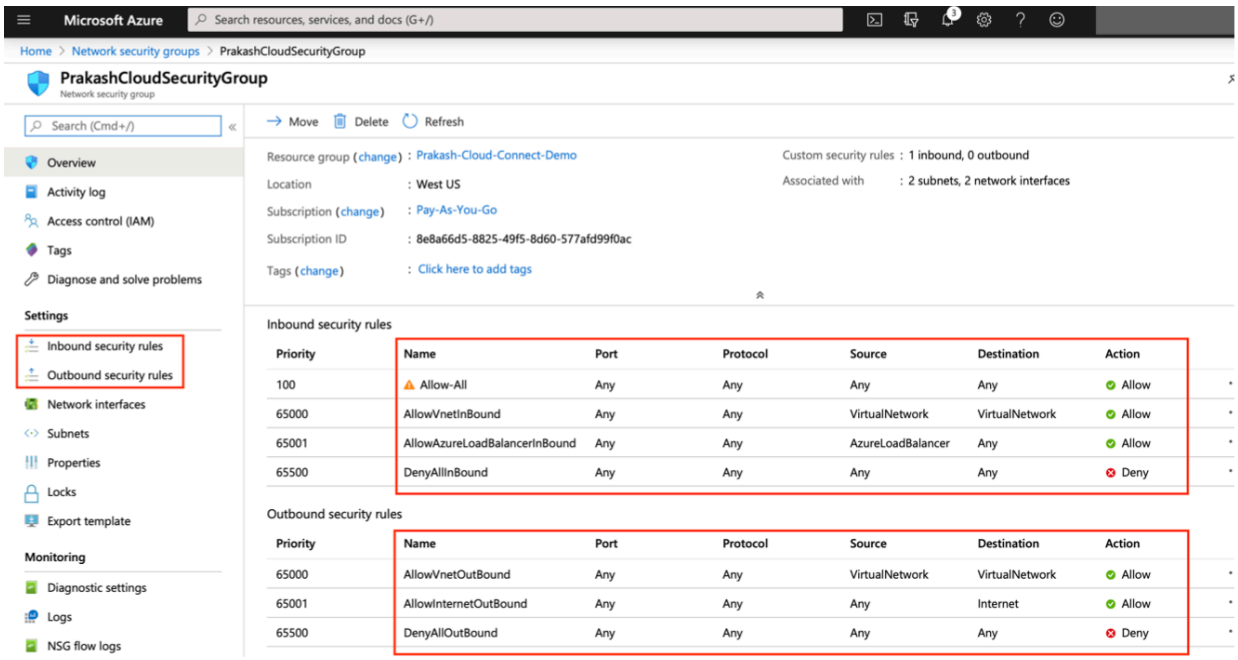
5. Enter the virtual network (VNET) CIDR address range to use for the virtual network. The screenshot below shows the address range 10.231.0.0/16.



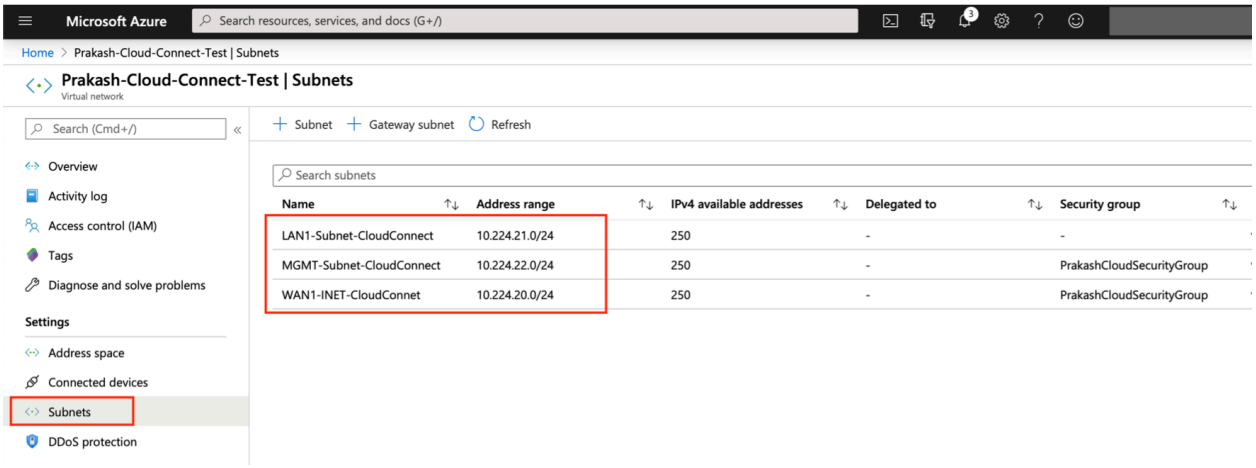
6. Optionally, configure other parameters, such as those under the Security tab.
7. Select the Review + Create tab.
8. Click Review + Create.
9. Create new security group to protect the virtual network subnets, especially the WAN and management subnets, that face public networks.



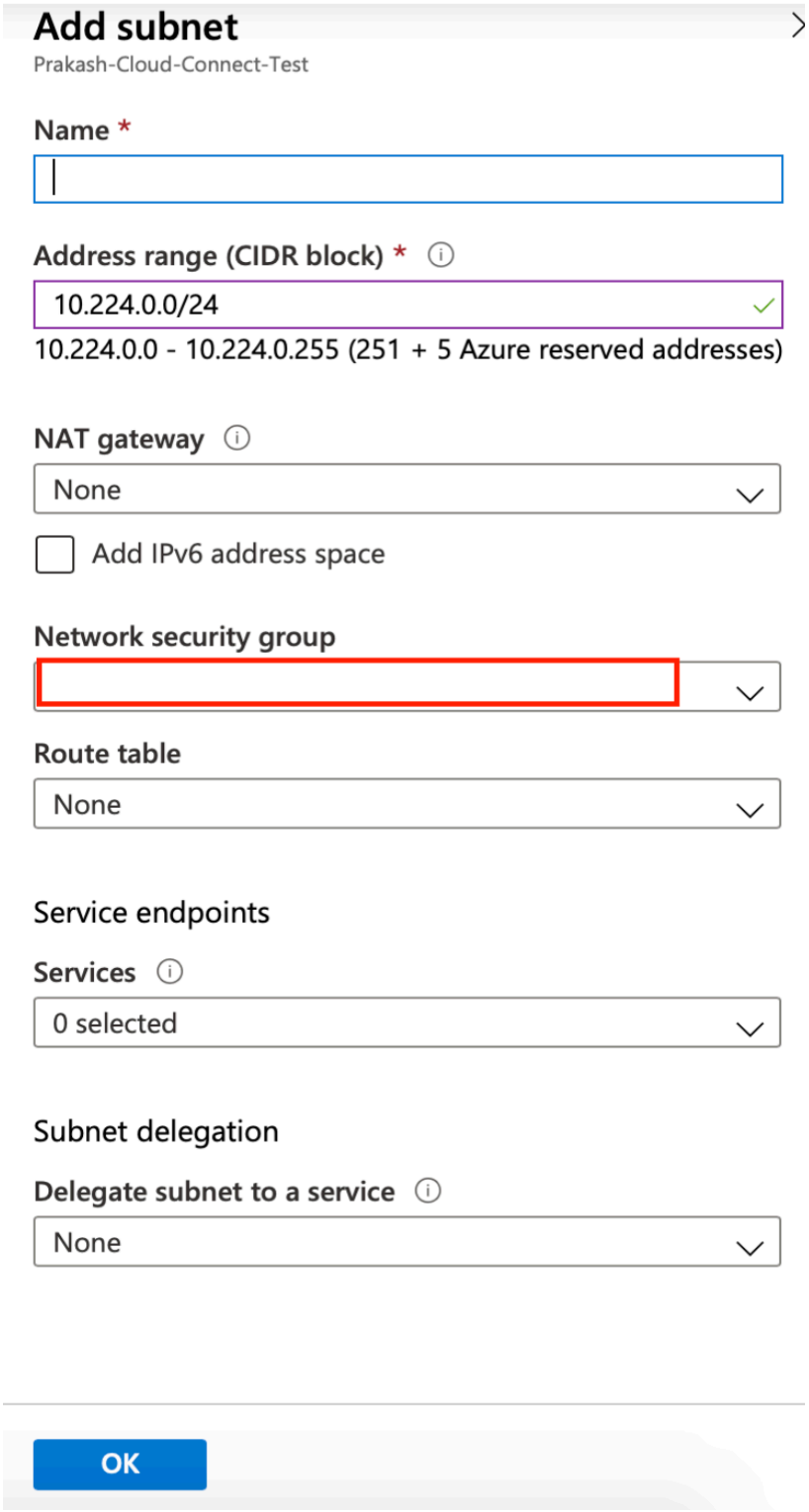
10. If you are deploying a VOS branch in a production environment, open the necessary inbound and outbound ports. For more information, see Firewall Requirements.
11. Verify traffic flow by creating an Allow All rule to accept (whitelist) all inbound and outbound traffic from all sources.



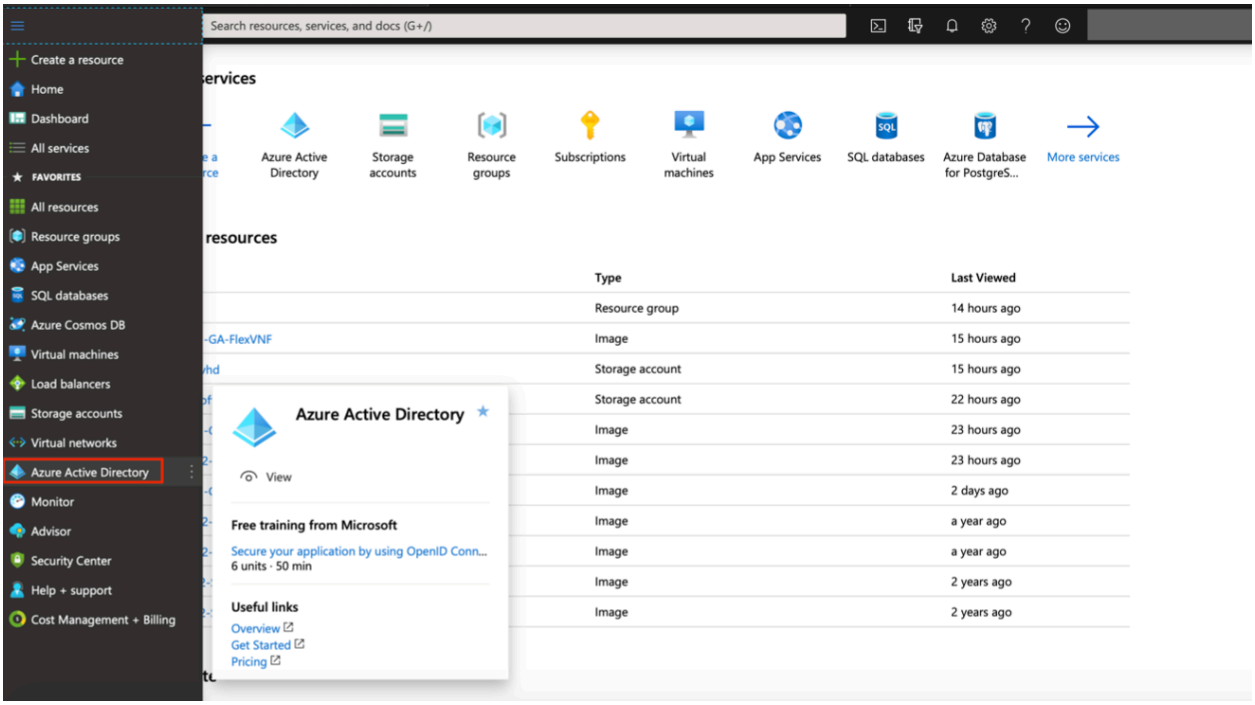
12. Open the virtual network that you just deployed and create new subnets. Create a minimum of three subnets—one management, one WAN, and one LAN—that you can use later in Versa Director while deploying. The total number of subnets you create depends on the deployment use case.



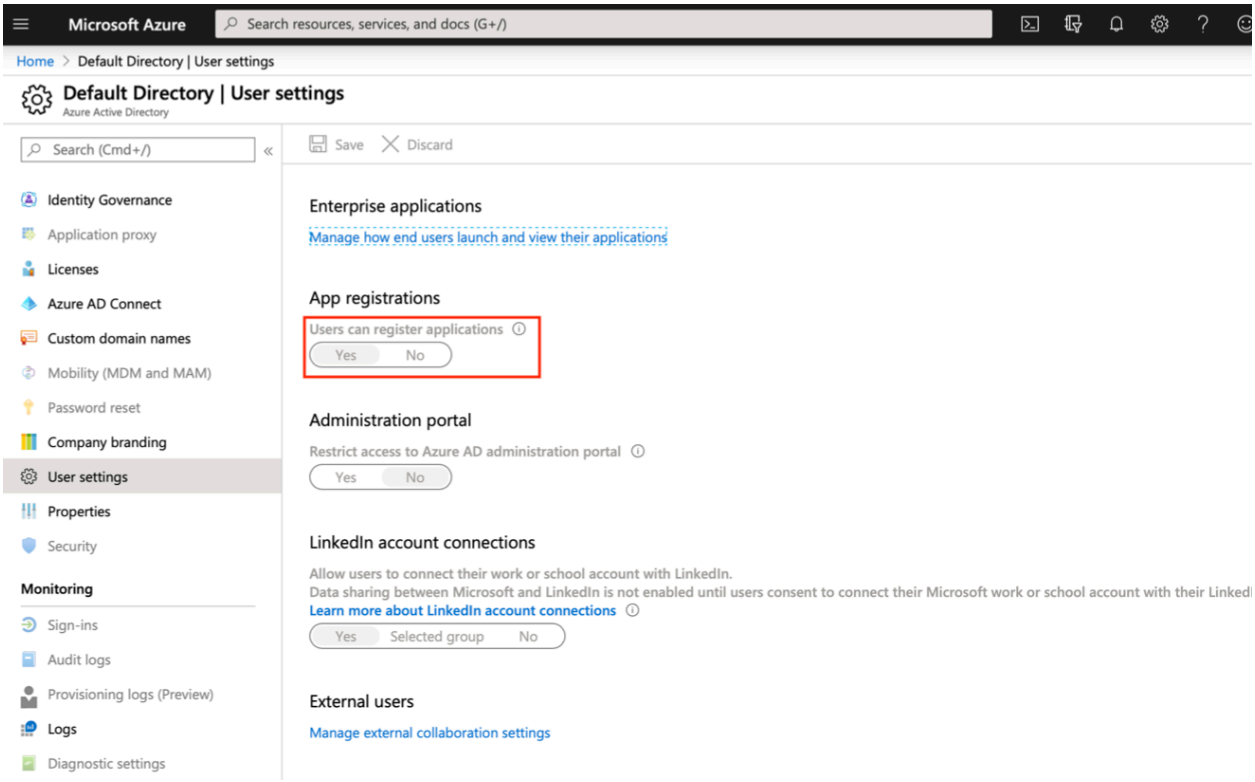
13. When creating each subnet, attach it to the security group that you created earlier, preferably to the security group for the WAN and management networks.



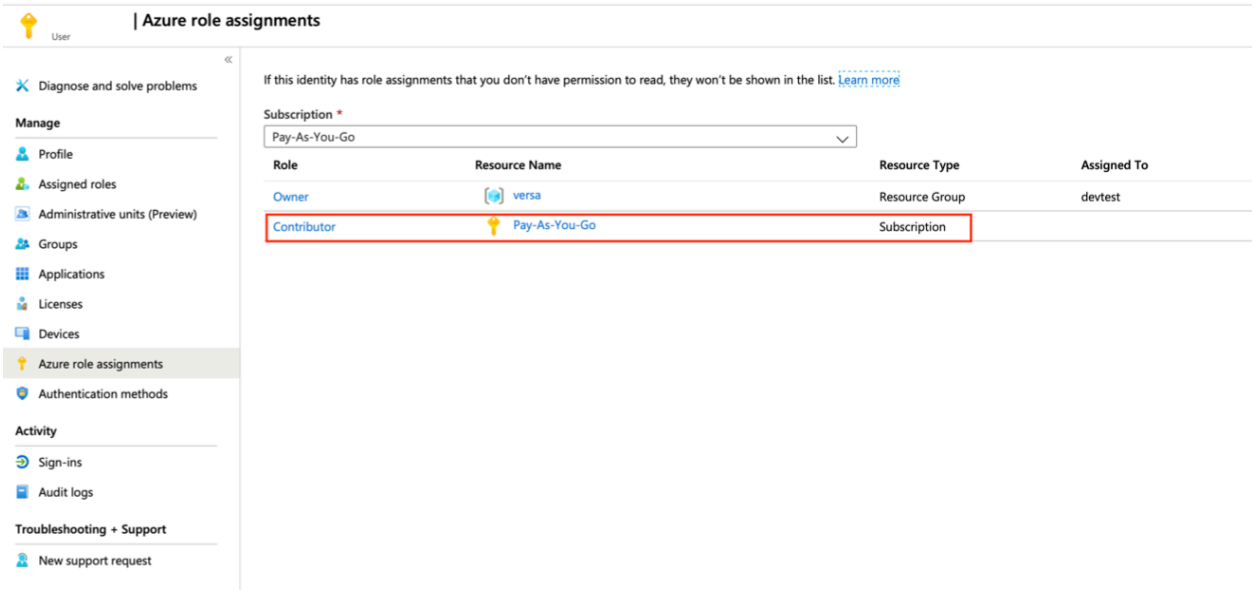
14. Check under Azure Active Directory that the user has permission to register a new application.



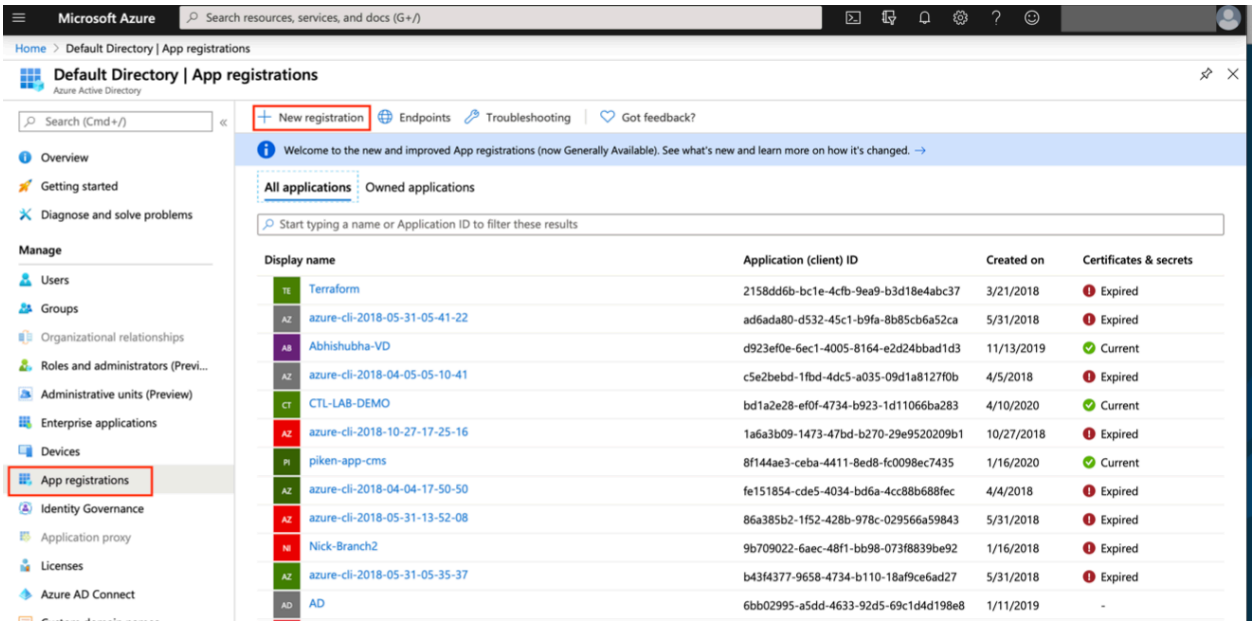
15. Check that the permission is set to Yes. If it is not, ask the account administrator to enable it.



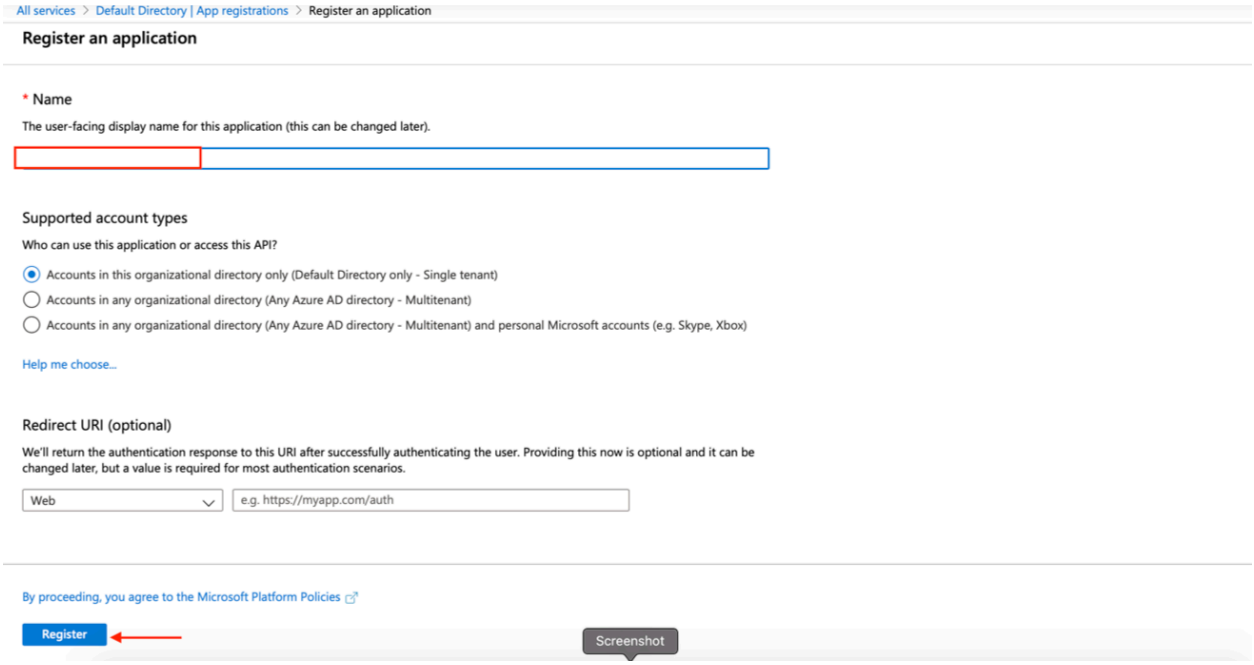
16. Ensure that the user account you use to deploy the new instance has at least limited administrator or contributor privilege for the subscription resource type so that they can create the necessary resources.



17. To create a new application to register Versa Director that you use to deploy new VOS branch instances, click the App Registrations section in Azure Active Directory.



18. Enter a name for your application (Versa Director Registration), and then click Register to register it.



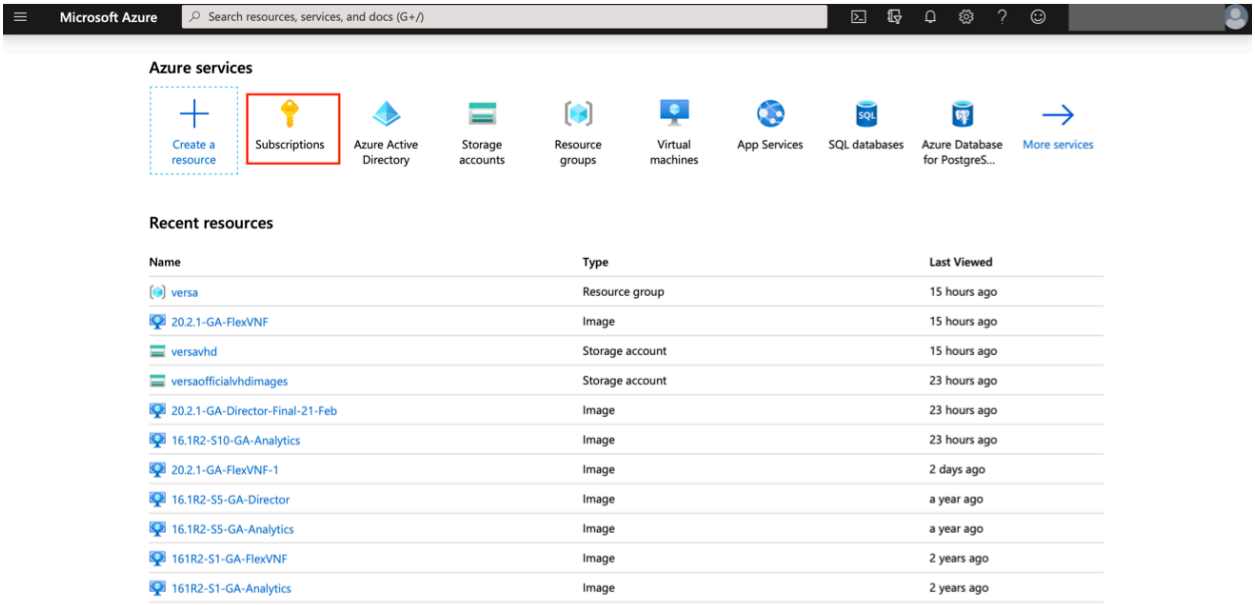
For the user, you have now created a resource group, a virtual network, subnets, and security groups, and you have created a new application for Versa Director on which the required privileges are enabled.

Gather Information from Azure

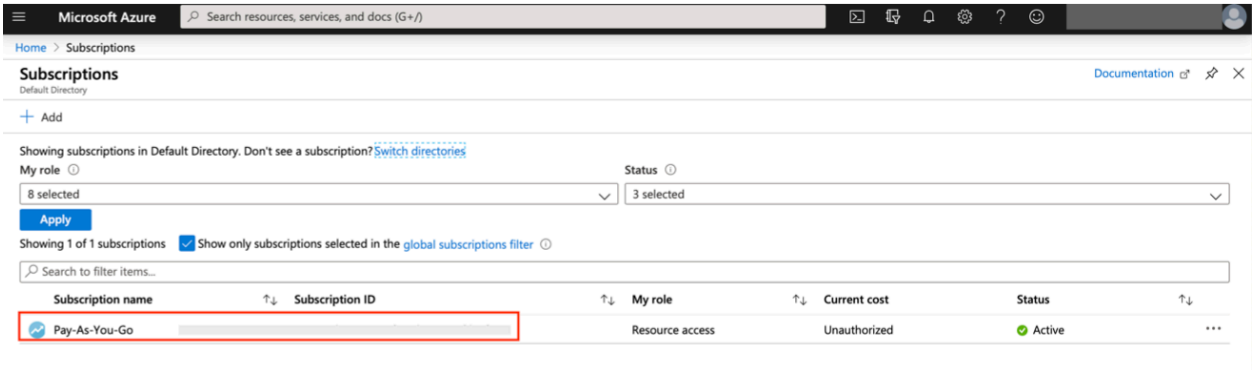
When you can create the CMS cloud connector in Versa Director, you must have the subscription ID, the tenant ID, the application/client ID, and the secret key for the user. You can find all this information in Azure.

To gather the information from Azure:

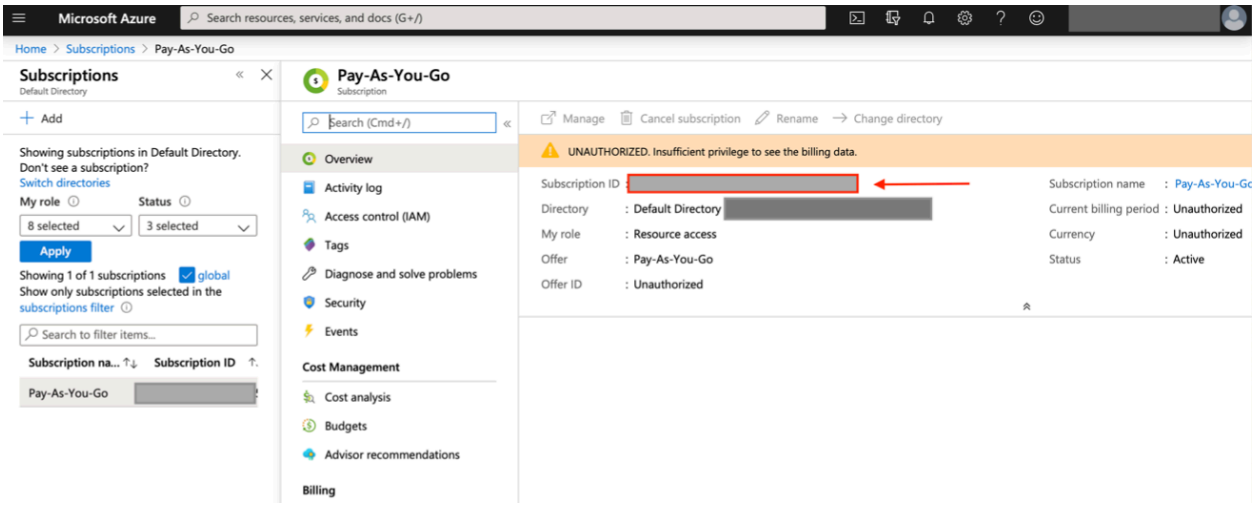
1. To obtain the subscription ID from the Azure account that you plan to use to deploy the new instance:
    a. Select the Subscriptions tab to open the user subscription.



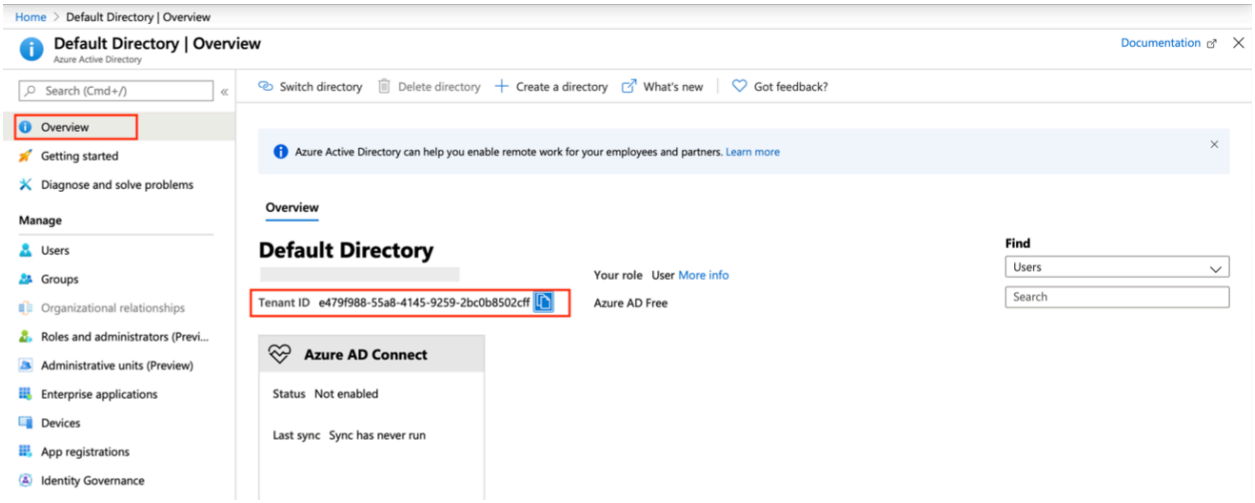
b. Select the available subscription that the user account is using.



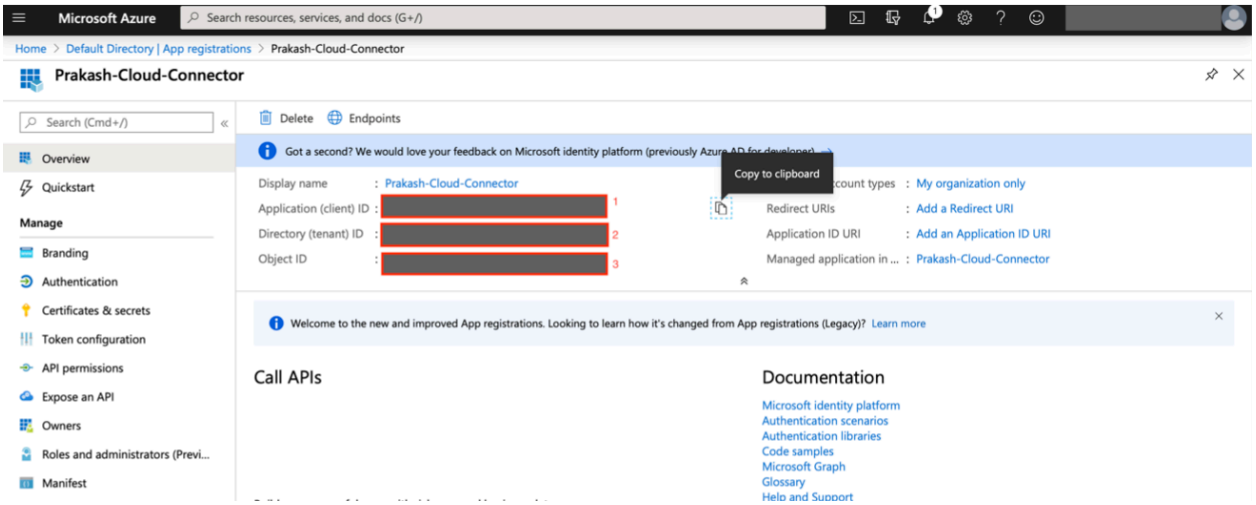
c. Make a note of the subscription ID that is listed under the selected subscription, as shown in the following screenshot. Click to copy it, and then save it in Notepad or elsewhere.



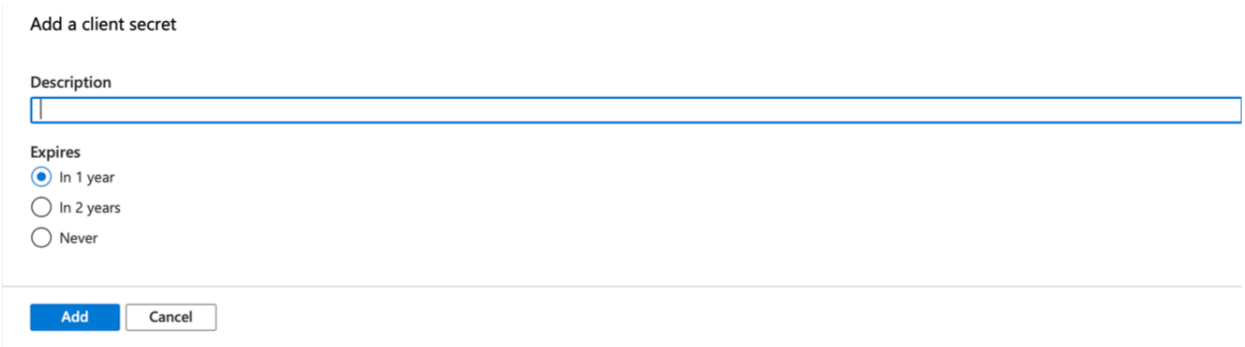
2. To obtain the tenant ID, go to Active Directory Overview. Then, click the tenant ID to copy it, and save it in Notepad or elsewhere.



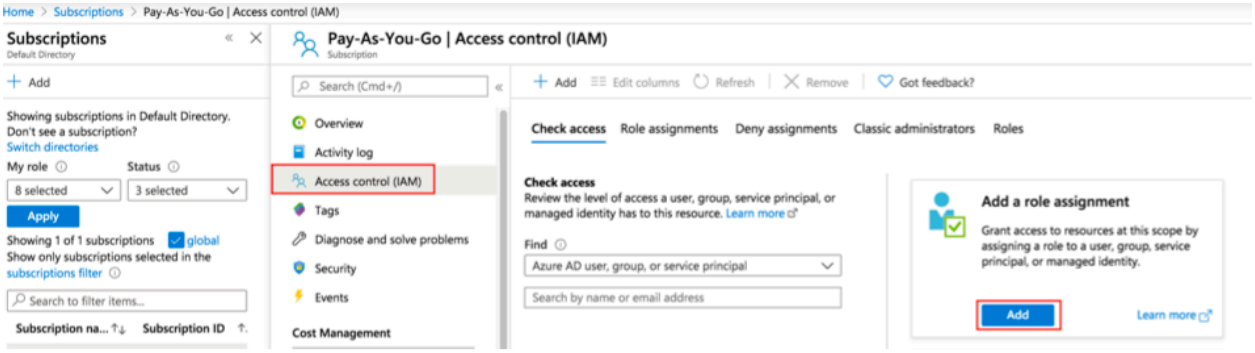
3. To obtain the client/application ID, click the application that you registered in the previous section, and make a note of the client/application ID. Click to copy it, and then save it in Notepad or elsewhere.

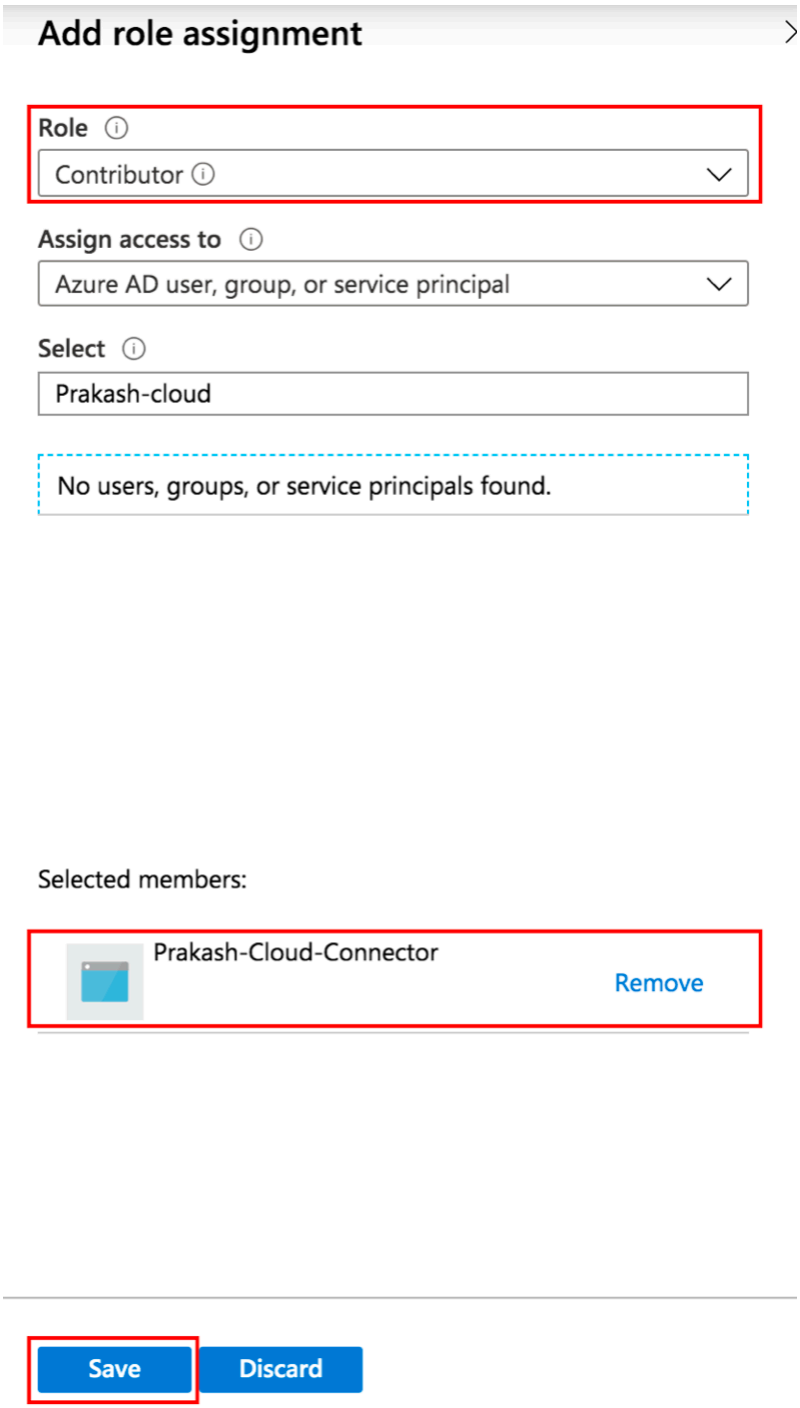


4. To create a new client secret to use for the registered application:
   a. Select the registered application, and then click Certificates and Secrets.

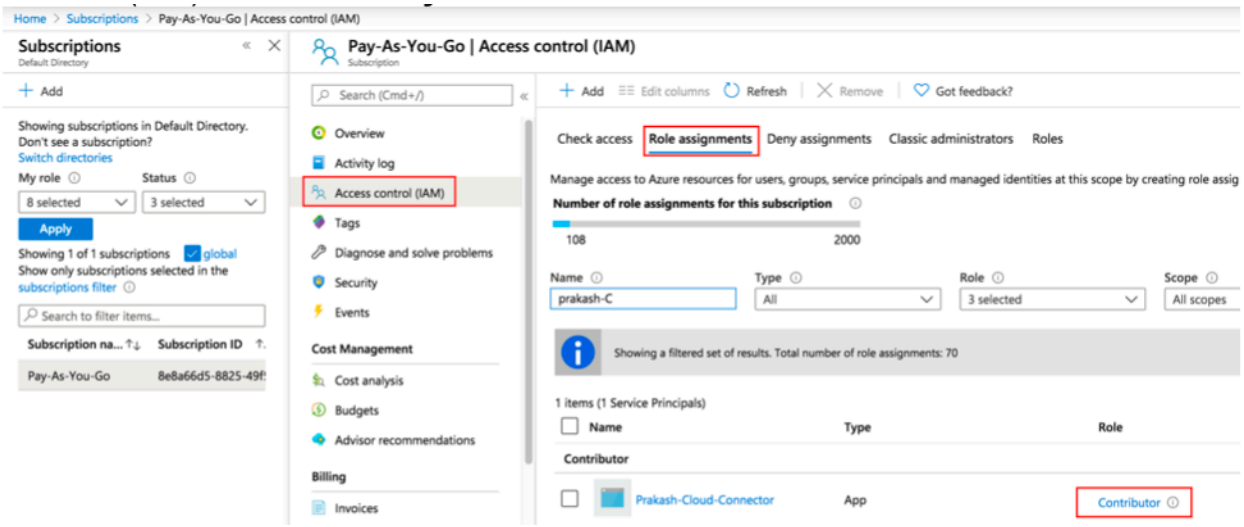


   b. Click the new key to copy it, and then save it in Notepad or elsewhere.
   c. To elevate the privileges of the newly created application to Contributor, navigate to Subscription > Access control (IAM) > Add Role Assignments. To assign Contributor level access to any Azure object, the user must have the Owner role for that subscription.





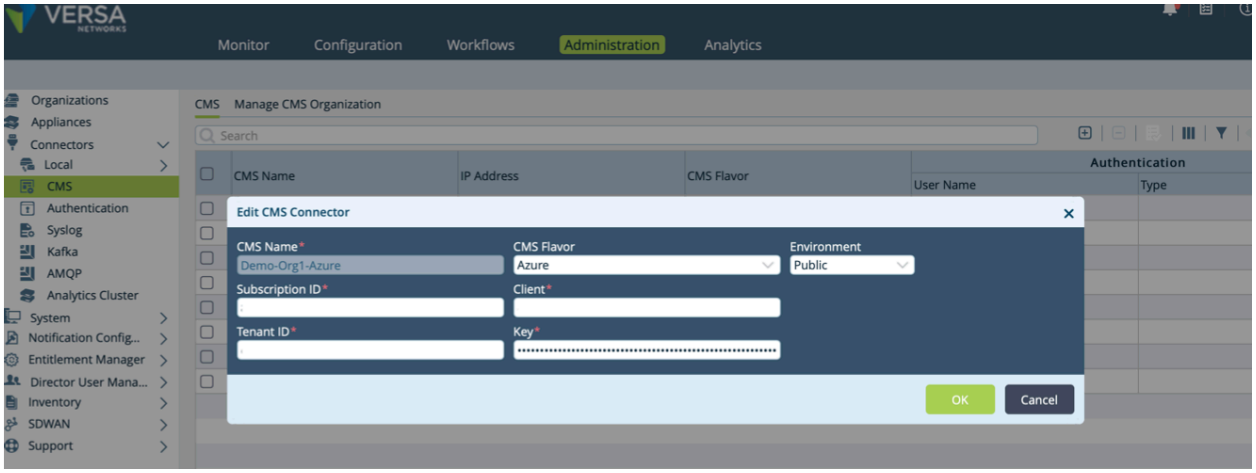
d. To view and validate the access level assigned to the Azure application, navigate to Subscription > Access control (IAM) > Role Assignments.



The user now has a subscription ID, a tenant ID, an application/client ID and secret key noted down and ready to use for deployment.

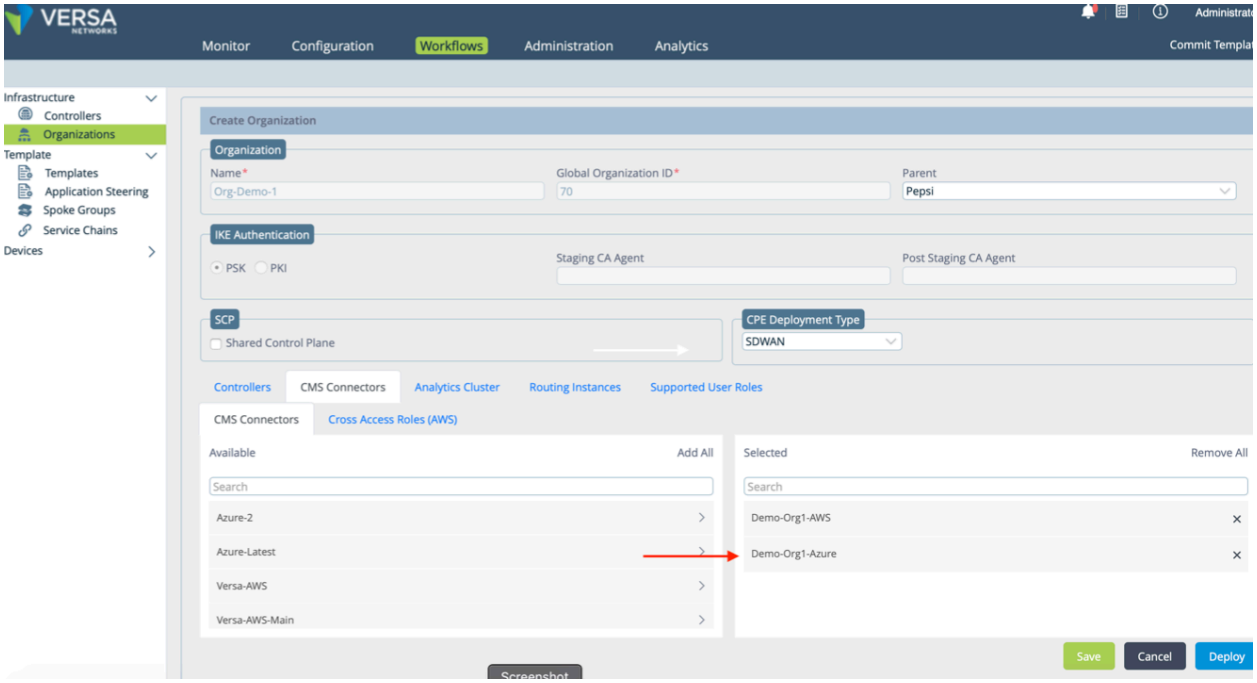
Create a CMS Cloud Connector in Versa Director

1. Log in to Versa Director.
2. Select the Administration tab in the top menu bar.
3. Select Connectors > CMS in the left menu bar.
4. Click the Add icon to add a new CMS connector. In the Add CMS Connector popup window, enter the subscription ID, tenant ID, application/client ID, and secret key that you obtained in the Gather Information from Azure, above.



5. Click OK.
6. Select Workflows in the top menu bar.
7. Select Infrastructure > Organizations in the left menu bar.

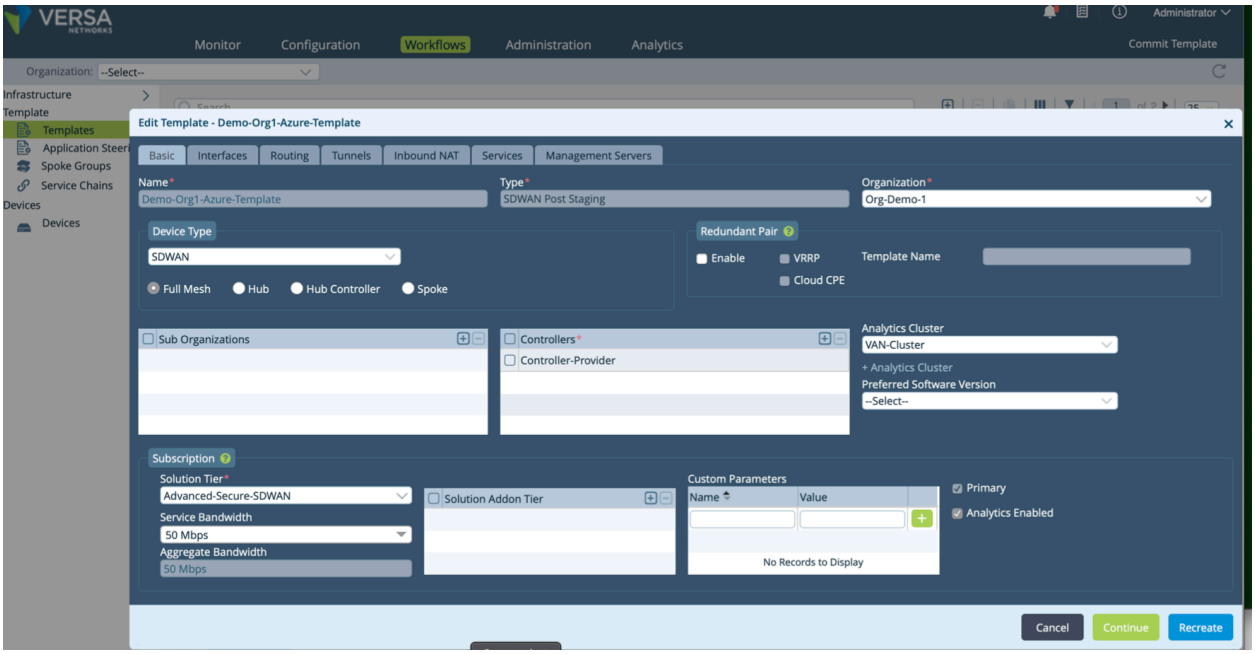
8. Select the CMS Connectors tab in the horizontal menu bar, and then click the CMS connector in the Available table to move it to the Selected table. Moving the CMS connector attaches it to the organization.



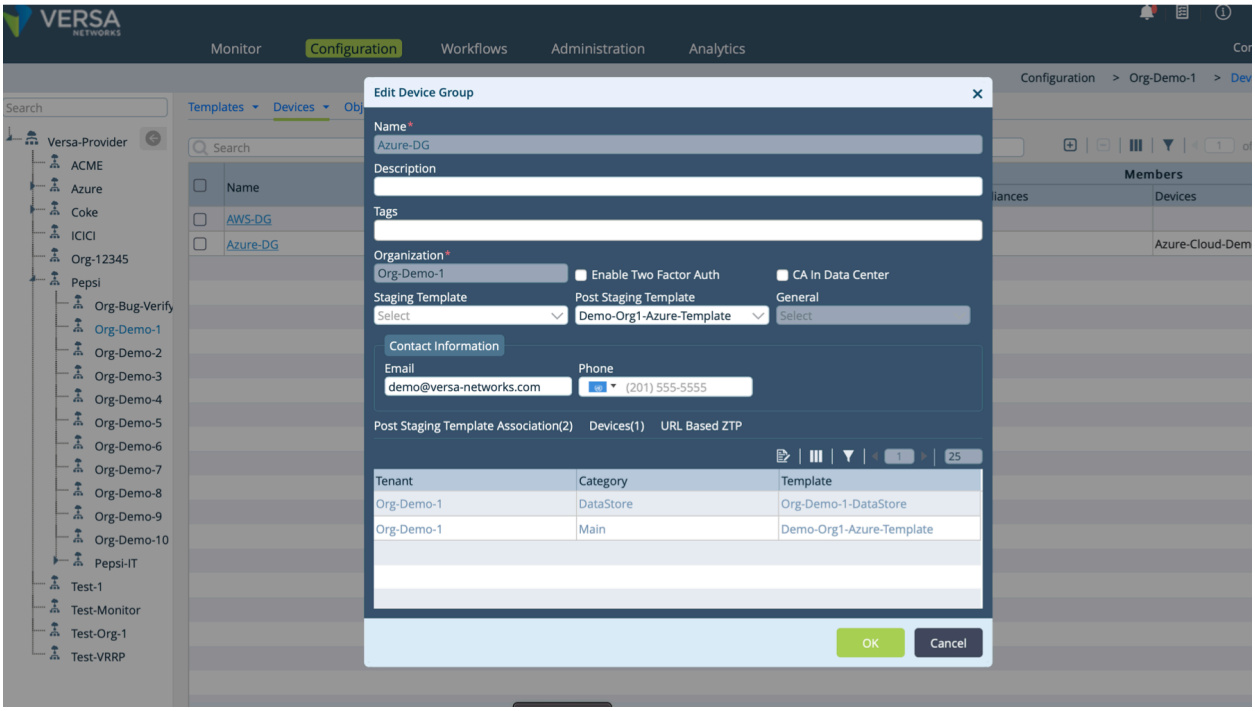
9. Click Deploy to create the CMS cloud connector.

Deploy a VOS Branch Using a CMS Connector

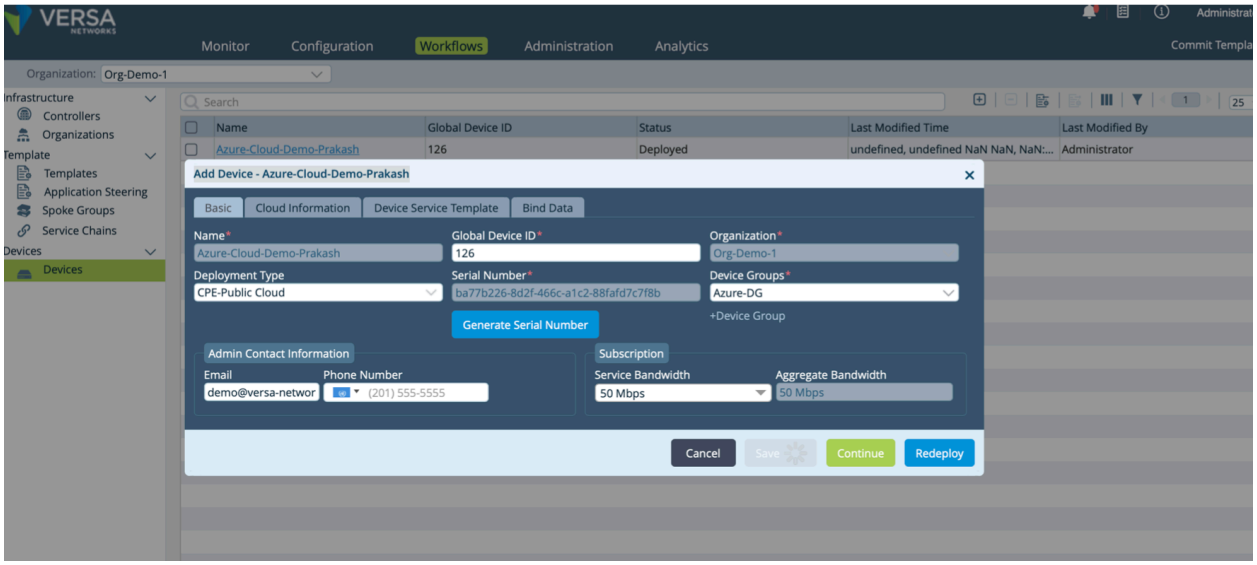
1. Log in to the Director node.
2. Select the Workflows tab in the top menu bar.
3. Select Template > Templates in the left menu bar.
4. Click the Add icon to create a new template to use for deploying a VOS branch device, and then configure all required information, including the number of WAN/LAN interfaces and other service information.



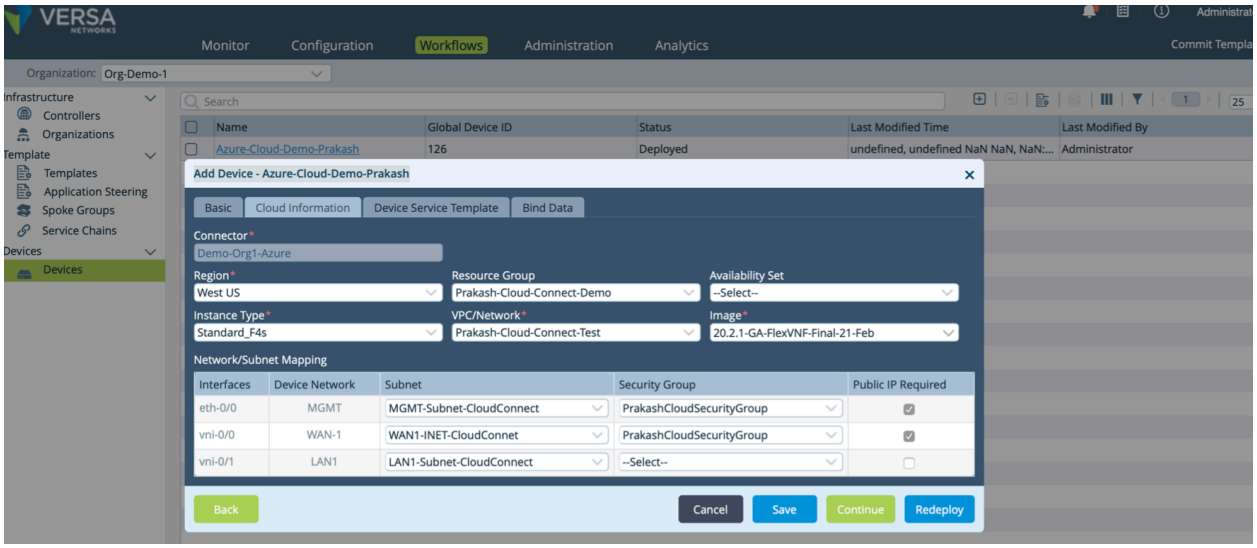
5. Create a device group and attach it to the new template.



6. Select the Workflows tab in the top menu bar.
7. Select Devices > Devices in the left menu bar.
8. Create a new device. In the Deployment Type field, select the public cloud option, click Generate Serial Number to create a random serial number, and in the Device Groups field, select the newly created device group.



9. Select the Cloud Information tab, and then select the connector that you created earlier. In the example here, the connector is Demo-Org1-Azure. After you select the connector, the VOS device pulls information from the Azure account and refreshes, which may take some time. After the refresh completes, select the desired region to display the Azure account information.
   Note that after deploying the cloud VOS branch/hub-controller with the CMS connector, you must remove the public IP address of eth0 from the Azure portal. The Director node will manage the VOS branch/hub-controller using the SD-WAN overlay IP address, and will not use the eth0 public IP address. Additionally, you must change the default passwords for all cloud-hosted VOS nodes, for admin and versa accounts.

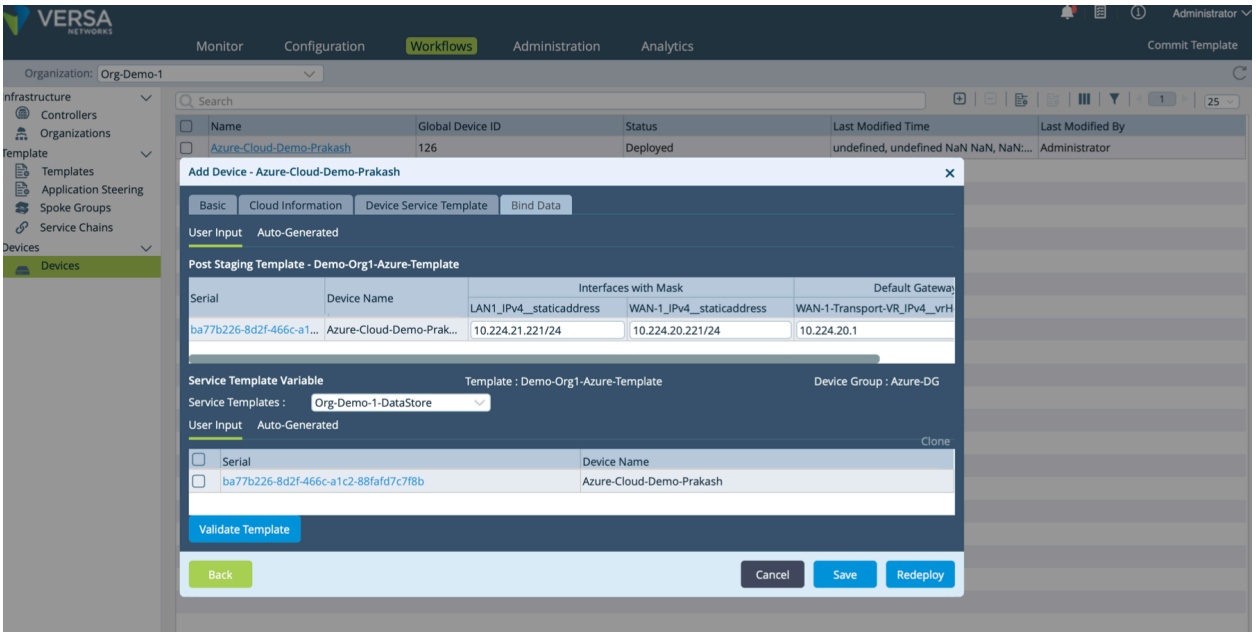


10. Select the resource group, instance type, VPC network, and the image that is available for your subscription to use for the deployment.
11. In the Network/Subnet Mapping table, select the subnets for the management, WAN, and LAN networks, and attach the security group to the WAN and management subnets. These subnets are the resources that you created in Create Resources in Azure, above.

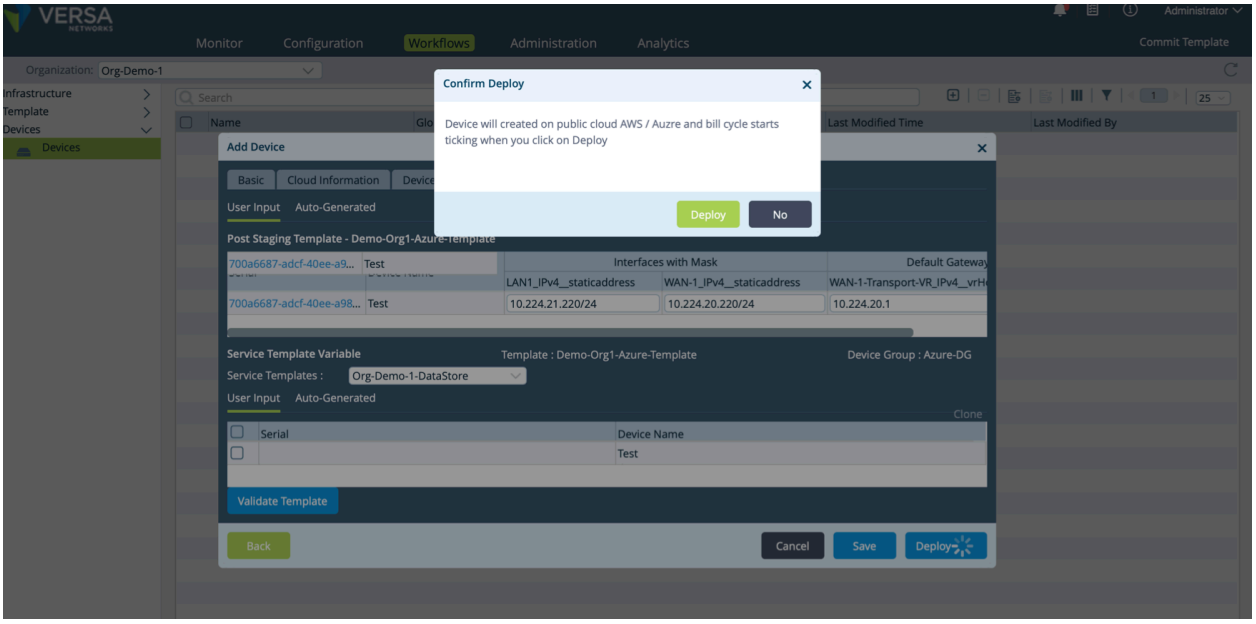
    Caution: You must add a separate security group for the management port (eth-0/0) and, once the site is

onboarded, remove access to ports 2022/ICMP and 22/SSH from eth-0/0. Ensure the node is accessible only by using a key.

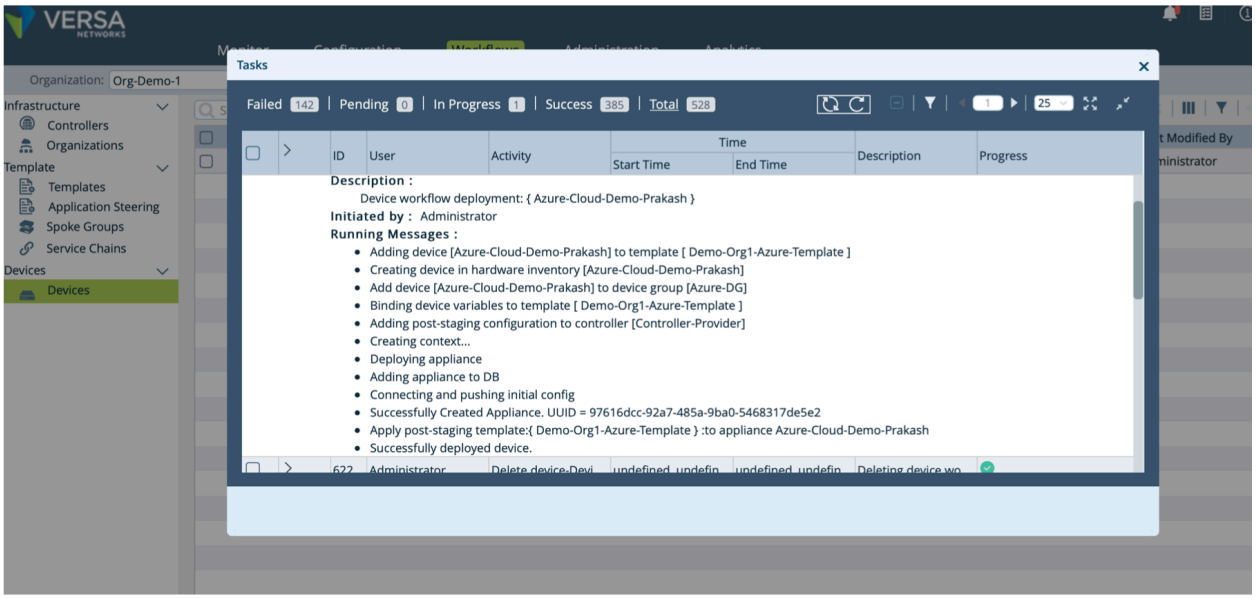
12. Select the Bind Data tab. Because we use static IP addressing in the template, select one unused IP address from each CIDR that you allocated in Azure for each of these subnets and enter it here. For our example, we select 10.224.20.221/24 for the WAN subnet, with the gateway as 10.224.20.1, and we select 10.224.21.221/24 for the LAN subnet.



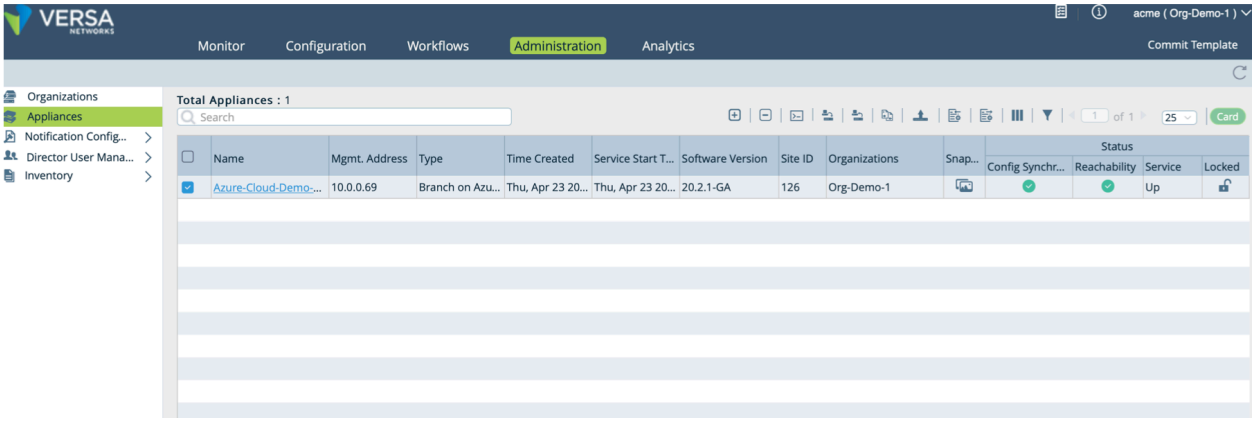
13. Click Redeploy to deploy the Azure VM instance using the Workflow template. The deploy operation creates a new VM instance in Azure. Note that the billing cycle for your VM starts as soon as the new VM resources are created in Azure.



14. The device deployment takes some time. When it completes successfully, the Tasks popup window displays.

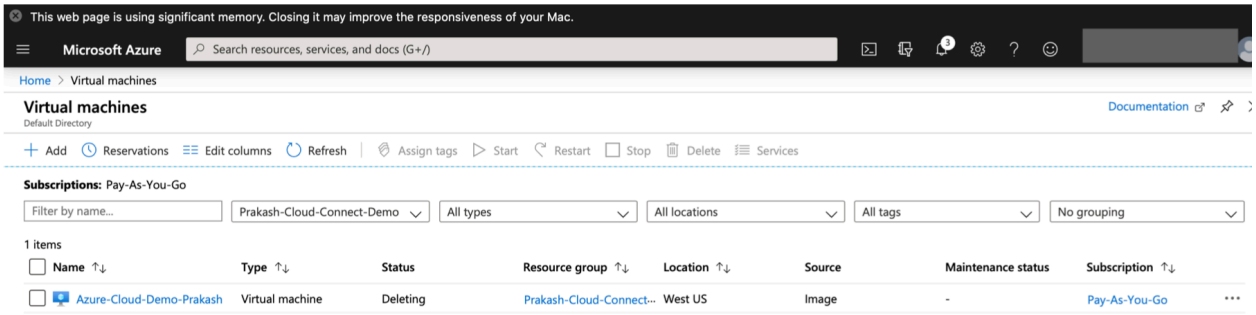


15. To display the VOS branch deployed through the Workflow template, select Administration > Appliances. You can now configure more properties as desired.

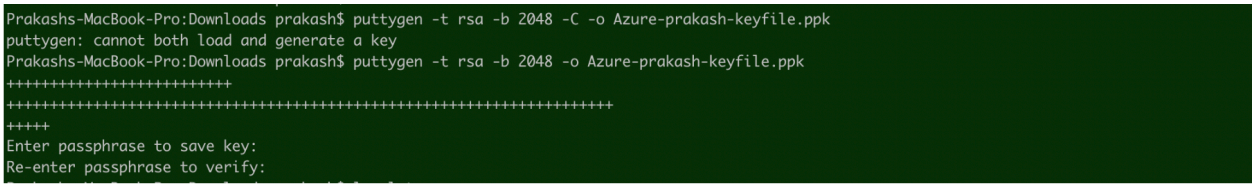


Connect To and Verify the Deployed VM Instance

1. Log in to the Azure portal with the user's credentials.
2. To verify that the newly deployed Virtual machine exists in Azure and is in the Running state, click Virtual Machines.



3. To access the VM using management IP, locate the public IP address used for management interface under the details of the virtual machine.
4. Create new public/private key using key-generation software, such as PuTTYgen.



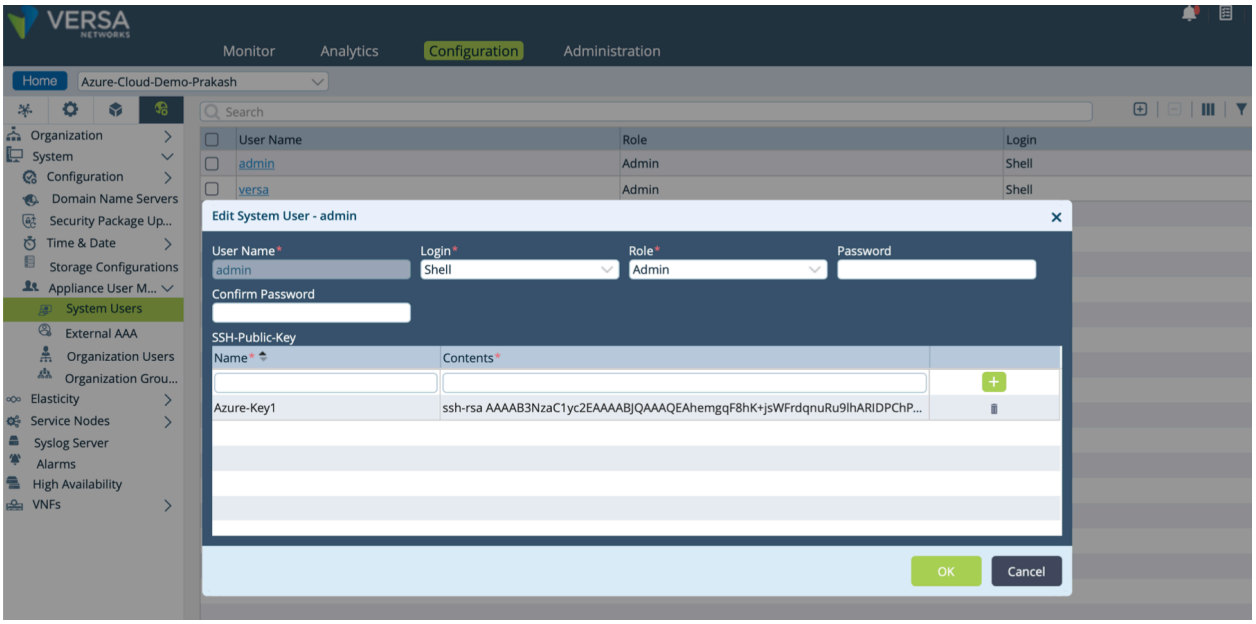
5. Convert the PuTTYgen output file, which is in .ppk format, to .pem format so that you can use it in OpenSSH.

```
Prakashs-MacBook-Pro:Downloads prakash$ puttygen Azure-prakash-keyfile.ppk -O private-openssh -o Azure-prakash-keyfile.pem
Enter passphrase to load key:
```

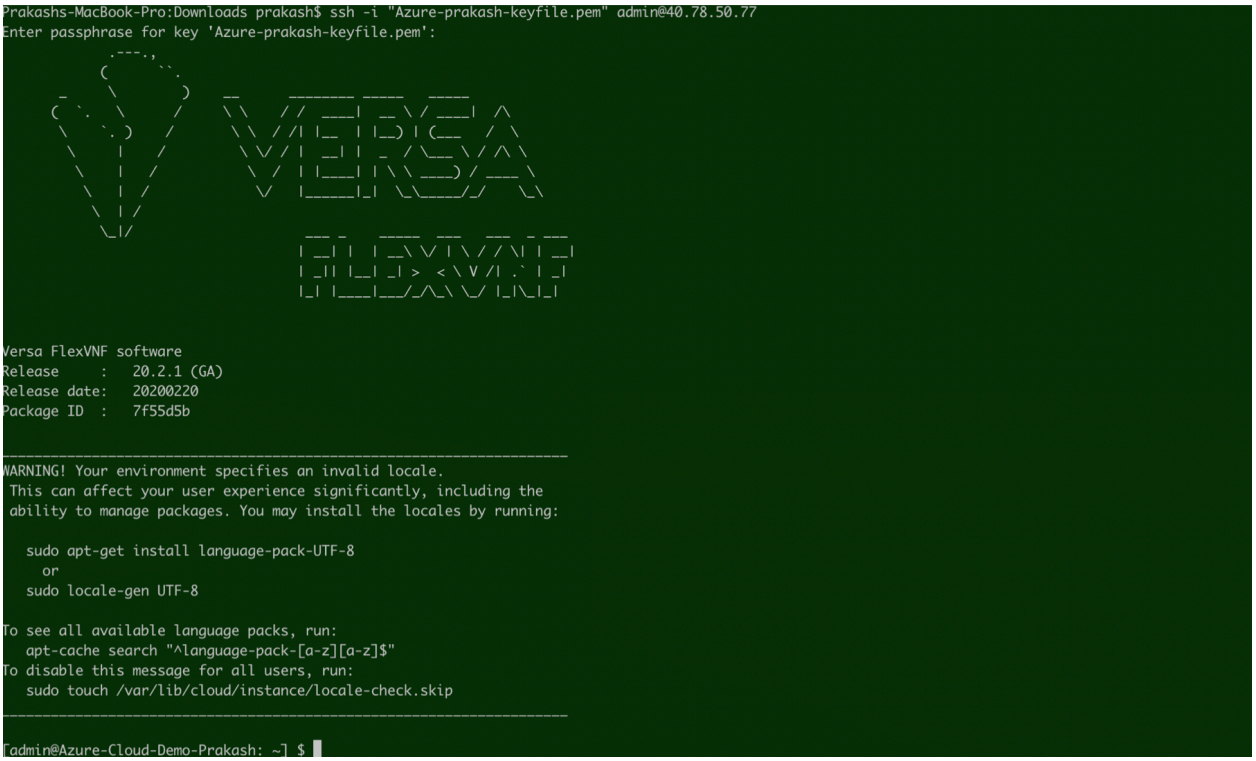
6. Extract the public key from the .pem file.

```
Prakashs-MacBook-Pro:Downloads prakash$ puttygen -L Azure-prakash-keyfile.pem
Enter passphrase to load key:
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAhemgqF8hK+jsWFrdqnuRu9lhARIDPChPFT7zYbbZNiIU1xg+xb8iXRYGOjqmMlzrfo+aOVcozGGrVJQXj2PzBM7MDCP8EPFo5/SDXG1ru+x
QIBbwZbsTDmMvP/StSjbgpPqNhftBa64XzcQmfjRU3w== imported-openssh-key
```

7. Log in to the Director node.
8. Select the deployed instance, and go to Appliance mode.
9. Select the Configuration tab in the top menu bar.
10. Select Others > System > Appliance User Management > System Users in the left menu bar.
11. In the main pane, select the username used for accessing the VM. The Edit System User popup window displays. The Role field shows the Admin user, because the VOS device is primarily accessed by an admin user.

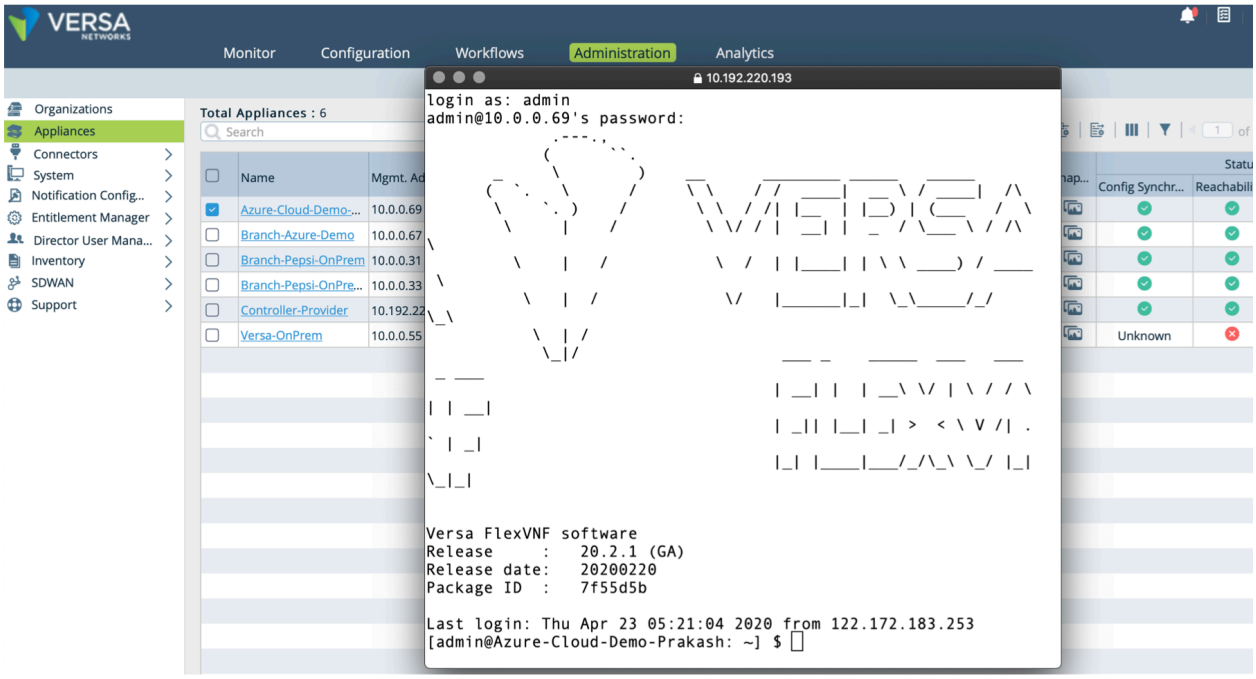


12. Enter the public key that you extracted earlier, and then click OK.
13. Access the VM using the management IP address (public IP address) that you obtained from Azure VM details and the private key .pem file.



14. From in the shell, enter the **cli** command to start the CLI, and then perform further health checks on the VOS device. For example:

15. From the Director node, access the CLI access, and then use the Shell In a Box utility to access to the Azure VM.



Supported Software Information

Releases 20.2 and later support all content described in this article.

Additional Information

[Configure Basic Features]
[Firewall Requirements]
[Install on Azure]