



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.

Microsoft Azure Search resources, services, and docs (G+/-)

Home > Resource groups

Resource groups

Default Directory

[+ Add](#) [Manage view](#) [Refresh](#) [Export to CSV](#) [Assign tags](#) [Feedback](#)

Filter by name... Subscription == all Location == all [Add filter](#)

Showing 1 to 80 of 80 records.

Name ↑↓	Subscription ↑↓	Location ↑↓
[Abhishubham-US]	Pay-As-You-Go	West US
[Azure-Device-Bug-42186-Test-Tunnel]	Pay-As-You-Go	Central India
[Azure-Perf-Branch1]	Pay-As-You-Go	West US
[Azure-vWANTest]	Pay-As-You-Go	West US
[Branch-20-3-Azure-vWAN-Azure-S2S]	Pay-As-You-Go	Central India
[Branch-Azure-PubIP-VRRP-Fix-1]	Pay-As-You-Go	West US
[Branch-Azure-PubIP-VRRP-Fix-2]	Pay-As-You-Go	West US
[Branch-Azure-VRRP-Primary]	Pay-As-You-Go	West US
[Branch-Azure-VRRP-Secondary]	Pay-As-You-Go	West US
[Branch-Azure-vWAN-Test-AzureT1]	Pay-As-You-Go	Central India
[Branch-ROCC-Azure]	Pay-As-You-Go	West US
[Branch-UDR-Test-1]	Pay-As-You-Go	West US

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

Microsoft Azure Search resources, services, and docs (G+/-)

Home > Resource groups > Create a resource group

Create a resource group

[Basics](#) Tags Review + create

Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more](#)

Project details

Subscription * ⓘ

Resource group * ⓘ

Resource details

Region * ⓘ

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

The screenshot shows the Microsoft Azure portal interface for managing Virtual Networks. At the top, there's a search bar and a navigation bar with icons for Home, Virtual networks, and other services. Below the navigation is a toolbar with buttons for Add, Manage view, Refresh, Export to CSV, Assign tags, and Feedback. A filter bar allows filtering by Name, Subscription, Resource group, Location, and adding a custom filter. The main area displays a table of 40 records, each row representing a virtual network with columns for Name, Resource group, Location, Subscription, and three-dot ellipsis for more options.

<input type="checkbox"/> Name ↑	Resource group ↑↓	Location ↑↓	Subscription ↑↓	
<input type="checkbox"/> Abhishubham-US-vnet	Abhishubham-US	West US	Pay-As-You-Go	...
<input type="checkbox"/> BP-VNet-CentralUS	VersaCentralUS	Central US	Pay-As-You-Go	...
<input type="checkbox"/> BP-VNet-WestUS	versa	West US	Pay-As-You-Go	...
<input type="checkbox"/> CTL-LAB-DEMO-VNET	CTL-LAB-DEMO	East US	Pay-As-You-Go	...
<input type="checkbox"/> ctlabwest	CTL-LAB-WEST	West US	Pay-As-You-Go	...
<input type="checkbox"/> HK-Net	HK-Test	East Asia	Pay-As-You-Go	...
<input type="checkbox"/> Hub-VNET	versa	West US	Pay-As-You-Go	...
<input type="checkbox"/> John-Demo-Net	John-Resource-group	West US	Pay-As-You-Go	...
<input type="checkbox"/> MEC-VNET-A	MEC-SDWAN	West US	Pay-As-You-Go	...
<input type="checkbox"/> NSS-Public	NSS-SDWAN	West US	Pay-As-You-Go	...
<input type="checkbox"/> PKAPOOR-VNET	PKAPOOR-VERSA-HE	West US	Pay-As-You-Go	...
<input type="checkbox"/> Prakash-Cloud-Connect-Test	Prakash-Cloud-Connect-Demo	West US	Pay-As-You-Go	...

- 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.

The screenshot shows the 'Create virtual network' wizard on the 'IP Addresses' tab. It displays the IPv4 address space configuration. Under 'IPv4 address space', the range '10.16.0.0/16' is listed with a note that it covers '10.16.0.0 - 10.16.255.255 (65536 addresses)'. A specific subnet '10.231.0.0/16' is highlighted with a red box. Below this, there's a checkbox for 'Add IPv6 address space'. The 'Subnet address range' section shows a single entry for 'default' with the range '10.16.0.0/24'. At the bottom, there are navigation buttons for 'Review + create', 'Previous', 'Next : Security >', 'Download a template for this configuration', and 'Screenshot'.

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

https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Initial_Configuration/...

Updated: Wed, 23 Oct 2024 07:22:49 GMT

Copyright © 2024, Versa Networks, Inc.

Network security groups			
Default Directory			
Filter by name...	All resource groups	All locations	All tags
107 items			No grouping
<input type="checkbox"/> Name ↑	Resource group ↑	Location ↑↓	Subscription ↑↓
<input type="checkbox"/> 16-IR2-S6-Director-Lab-nsg	Versa-Lab	West US	Pay-As-You-Go
<input type="checkbox"/> ABHI-VM-nsg	Abhishubham-US	West US	Pay-As-You-Go
<input type="checkbox"/> Abhishek-Ubu-14-Client-2-n... versa		West US	Pay-As-You-Go
<input type="checkbox"/> AnalyticsTest-nsg	versa	West US	Pay-As-You-Go
<input type="checkbox"/> Branch-Abhishek-MLXTest-n... versa		West US	Pay-As-You-Go
<input type="checkbox"/> Client-3-nsg	Azure-vWANTest	West US	Pay-As-You-Go
<input type="checkbox"/> Client-New-nsg	versa	West US	Pay-As-You-Go
<input type="checkbox"/> Client-vWAN-India-nsg	versa-india	Central India	Pay-As-You-Go
<input type="checkbox"/> ControllerTest-nsg	versa	West US	Pay-As-You-Go
<input type="checkbox"/> Director-1-nsg	Test-WAN	West US	Pay-As-You-Go
<input type="checkbox"/> Director-16-1-R2-56-nsg	Versa-Lab	West US	Pay-As-You-Go
<input type="checkbox"/> Director-16IR2S6-preetam-... Versa-Lab		West US	Pay-As-You-Go
<input type="checkbox"/> Director-Dec-12-nsg	versa	West US	Pay-As-You-Go
<input type="checkbox"/> Director-Lab-Task-nsg	versa	West US	Pay-As-You-Go

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.

PrakashCloudSecurityGroup

Priority	Name	Port	Protocol	Source	Destination	Action
100	Allow-All	Any	Any	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

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.

https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Initial_Configuration/

Updated: Wed, 23 Oct 2024 07:22:49 GMT

Copyright © 2024, Versa Networks, Inc.

Microsoft Azure

Search resources, services, and docs (G+ /)

Home > Prakash-Cloud-Connect-Test | Subnets

Prakash-Cloud-Connect-Test | Subnets

Virtual network

Search (Cmd+ /) Subnet Gateway subnet Refresh

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Settings Address space Connected devices Subnets DDoS protection

Name	Address range	IPv4 available addresses	Delegated to	Security group
LAN1-Subnet-CloudConnect	10.224.21.0/24	250	-	-
MGMT-Subnet-CloudConnect	10.224.22.0/24	250	-	PrakashCloudSecurityGroup
WAN1-INET-CloudConnect	10.224.20.0/24	250	-	PrakashCloudSecurityGroup

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.

Add subnet >

Prakash-Cloud-Connect-Test

Name *

Address range (CIDR block) * ⓘ

 ✓
10.224.0.0 - 10.224.0.255 (251 + 5 Azure reserved addresses)

NAT gateway ⓘ

 ▾
 Add IPv6 address space

Network security group

 ▾

Route table

 ▾

Service endpoints

Services ⓘ

 ▾

Subnet delegation

Delegate subnet to a service ⓘ

 ▾

OK

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

The screenshot shows the Microsoft Azure portal interface. On the left, there is a sidebar with various service icons and links. The 'Azure Active Directory' icon is highlighted with a red box. The main content area displays a grid of service icons: Azure Active Directory, Storage accounts, Resource groups, Subscriptions, Virtual machines, App Services, SQL databases, and Azure Database for PostgreSQL. Below this is a section titled 'resources' with a table showing items like Resource group, Image, Storage account, etc., with their last viewed times. A detailed view of 'Azure Active Directory' is shown on the right, including sections for 'Free training from Microsoft', 'Useful links', and 'Overview', 'Get Started', and 'Pricing' buttons.

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

The screenshot shows the 'Default Directory | User settings' page in the Microsoft Azure portal. The left sidebar has a 'User settings' tab selected, which is highlighted with a red box. The main content area includes sections for 'Enterprise applications', 'App registrations' (with a 'Users can register applications' toggle set to 'Yes', also highlighted with a red box), 'Administration portal' (with a 'Restrict access to Azure AD administration portal' toggle set to 'No'), 'LinkedIn account connections' (with a 'Allow users to connect their work or school account with LinkedIn' toggle set to 'No'), 'External users' (with a 'Manage external collaboration settings' link), and 'Properties', 'Security', and 'Monitoring' sections.

- 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.

https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Initial_Configuration

Updated: Wed, 23 Oct 2024 07:22:49 GMT

Copyright © 2024, Versa Networks, Inc.

The screenshot shows the Azure portal interface under the 'User' section. On the left, there's a sidebar with various management options like 'Diagnose and solve problems', 'Manage', 'Profile', 'Assigned roles', etc. The 'Azure role assignments' option is selected and highlighted with a grey background. The main content area is titled 'Azure role assignments' and shows a table of role assignments. A note at the top says, 'If this identity has role assignments that you don't have permission to read, they won't be shown in the list.' Below this, a dropdown menu shows 'Subscription *' set to 'Pay-As-You-Go'. The table has columns for 'Role', 'Resource Name', 'Resource Type', and 'Assigned To'. It lists one 'Owner' role assigned to 'versa' (Resource Name) under 'Resource Group' 'devtest'. Below it, a 'Contributor' role is assigned to 'Pay-As-You-Go' under 'Subscription'. This last row is highlighted with a red border.

- 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.

The screenshot shows the Azure portal interface under the 'Default Directory' section. The 'App registrations' option is selected and highlighted with a grey background. The main content area is titled 'Default Directory | App registrations'. At the top, there's a search bar and a 'New registration' button, which is highlighted with a red box. Below this, there are tabs for 'All applications' (which is selected) and 'Owned applications'. A search bar allows filtering by application name. The main table lists various registered applications, each with a color-coded icon (e.g., Terraform, az, AB, AZ, CT, AZ, PI, AZ, AZ, AZ, AD) and a unique ID. Columns include 'Display name', 'Application (client) ID', 'Created on', and 'Certificates & secrets'. Most entries show 'Expired' or 'Current' status for certificates.

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

Register an application

* Name

The user-facing display name for this application (this can be changed later).

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (Default Directory only - Single tenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

[By proceeding, you agree to the Microsoft Platform Policies](#)

[Register](#)

[Screenshot](#)

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.

Azure services

- Create a resource
- Subscriptions
- Azure Active Directory
- Storage accounts
- Resource groups
- Virtual machines
- App Services
- SQL databases
- Azure Database for PostgreSQL...
- More services

Recent resources

Name	Type	Last Viewed
versa	Resource group	15 hours ago
20.2.1-GA-FlexVNF	Image	15 hours ago
versavhd	Storage account	15 hours ago
versaofficialvhdimages	Storage account	23 hours ago
20.2.1-GA-Director-Final-21-Feb	Image	23 hours ago
16.1R2-S10-GA-Analytics	Image	23 hours ago
20.2.1-GA-FlexVNF-1	Image	2 days ago
16.1R2-S5-GA-Director	Image	a year ago
16.1R2-S1-GA-Analytics	Image	a year ago
161R2-S1-GA-FlexVNF	Image	2 years ago
161R2-S1-GA-Analytics	Image	2 years ago

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

Subscriptions

Default Directory

+ Add

Show subscriptions in Default Directory. Don't see a subscription? [Switch directories](#)

My role: 8 selected

Status: 3 selected

Apply

Showing 1 of 1 subscriptions Show only subscriptions selected in the [global subscriptions filter](#)

Search to filter items...

Subscription name	Subscription ID	My role	Current cost	Status	...
Pay-As-You-Go	[Redacted]	Resource access	Unauthorized	Active	...

- 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.

The screenshot shows the Microsoft Azure Subscriptions page. On the left, there's a sidebar with filters for 'My role' (8 selected), 'Status' (3 selected), and a search bar. The main area is titled 'Pay-As-You-Go' and shows a single subscription named 'Pay-As-You-Go'. A prominent yellow warning banner at the top right states 'UNAUTHORIZED. Insufficient privilege to see the billing data.' Below the banner, detailed information about the subscription is listed:

Subscription ID	Subscription name
[Redacted]	Pay-As-You-Go
Default Directory	Subscription name : Pay-As-You-Go
Resource access	Current billing period : Unauthorized
Pay-As-You-Go	Currency : Unauthorized
Unauthorized	Status : Active

On the far right, there are buttons for 'Manage', 'Cancel subscription', 'Rename', and 'Change directory'.

- 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.

The screenshot shows the 'Default Directory | Overview' page in Azure Active Directory. The left sidebar has sections for 'Overview', 'Getting started', 'Diagnose and solve problems', 'Manage' (with options like Users, Groups, etc.), and 'Azure AD Connect' (status: Not enabled). The main area displays the 'Default Directory' overview, including the 'Tenant ID' (e479f988-55a8-4145-9259-2bc0b8502cff) which is highlighted with a red box. To the right, there's a 'Find' section for users and a search bar.

- 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:

- Select the registered application, and then click Certificates and Secrets.

- Click the new key to copy it, and then save it in Notepad or elsewhere.
- 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.

https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Initial_Configuration

Updated: Wed, 23 Oct 2024 07:22:49 GMT

Copyright © 2024, Versa Networks, Inc.

Add role assignment

>

Role ⓘ

Contributor ⓘ

Assign access to ⓘ

Azure AD user, group, or service principal



Select ⓘ

Prakash-cloud

No users, groups, or service principals found.

Selected members:



Prakash-Cloud-Connector

Remove

Save

Discard

- 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.

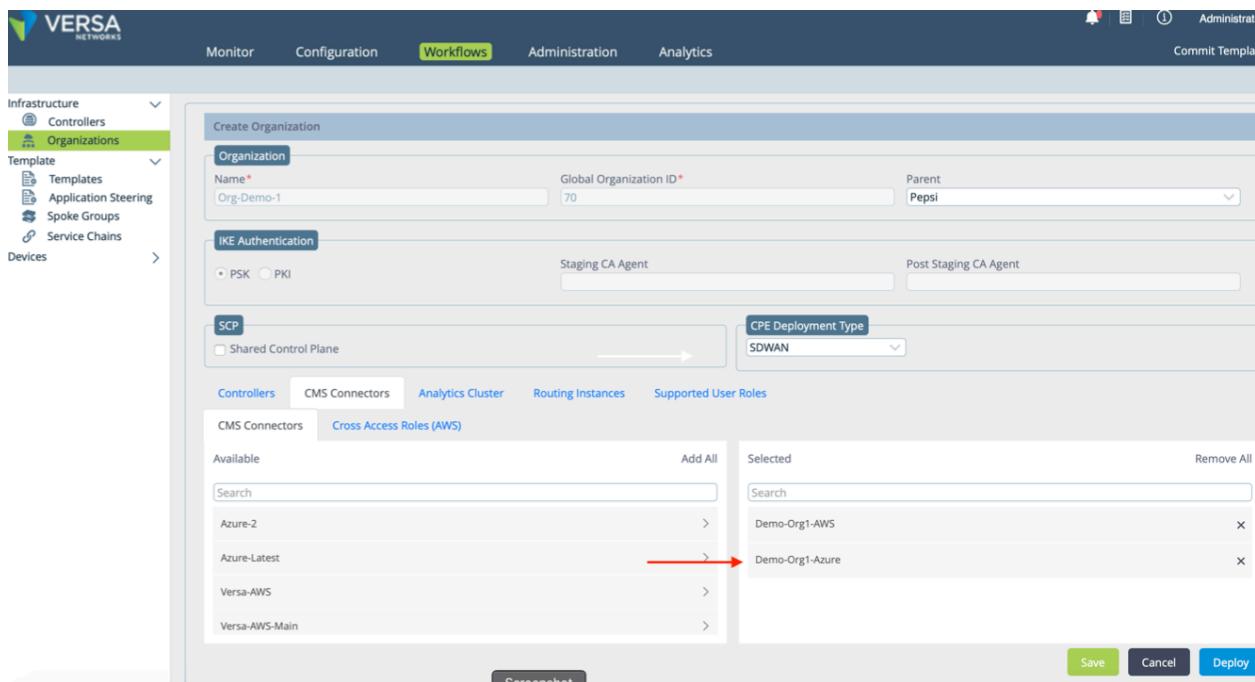
5. Click OK.
6. Select Workflows in the top menu bar.
7. Select Infrastructure > Organizations in the left menu bar.

[https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Initial_Configuration/...](https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Initial_Configuration/)

Updated: Wed, 23 Oct 2024 07:22:49 GMT

Copyright © 2024, Versa Networks, Inc.

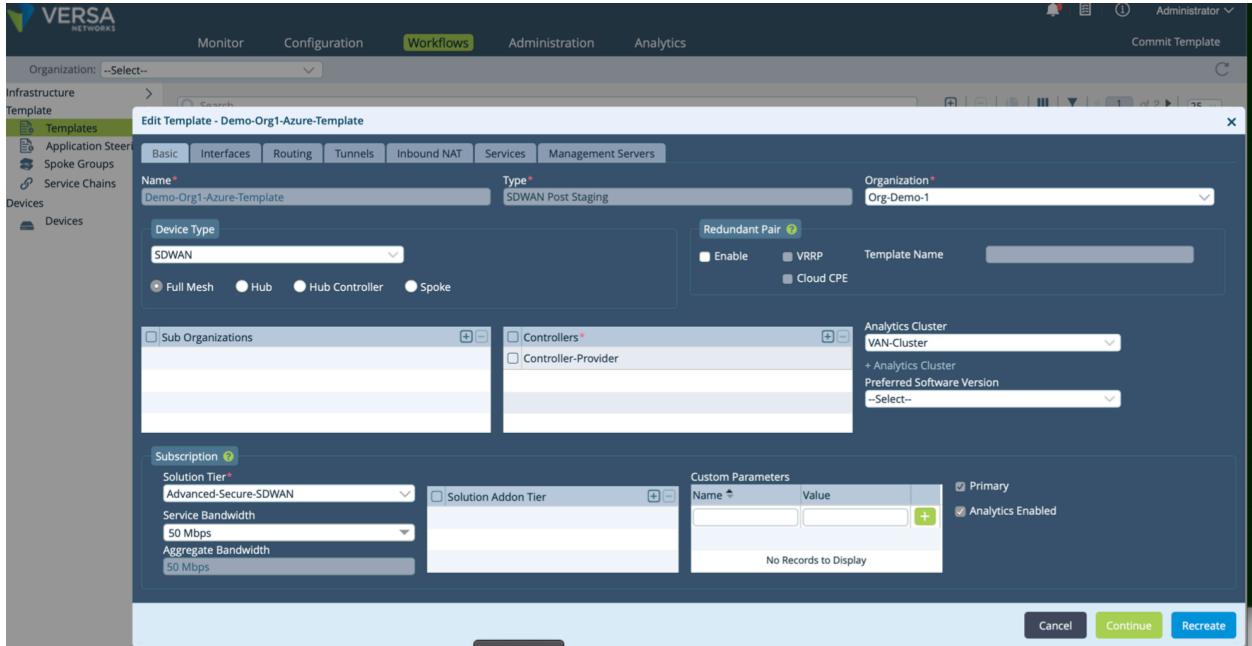
- Select the CMS Connectors tab in the horizontal menu bar, and then click the CMS connector in the Available table to move it to the Selected table. Moving the CMS connector attaches it to the organization.



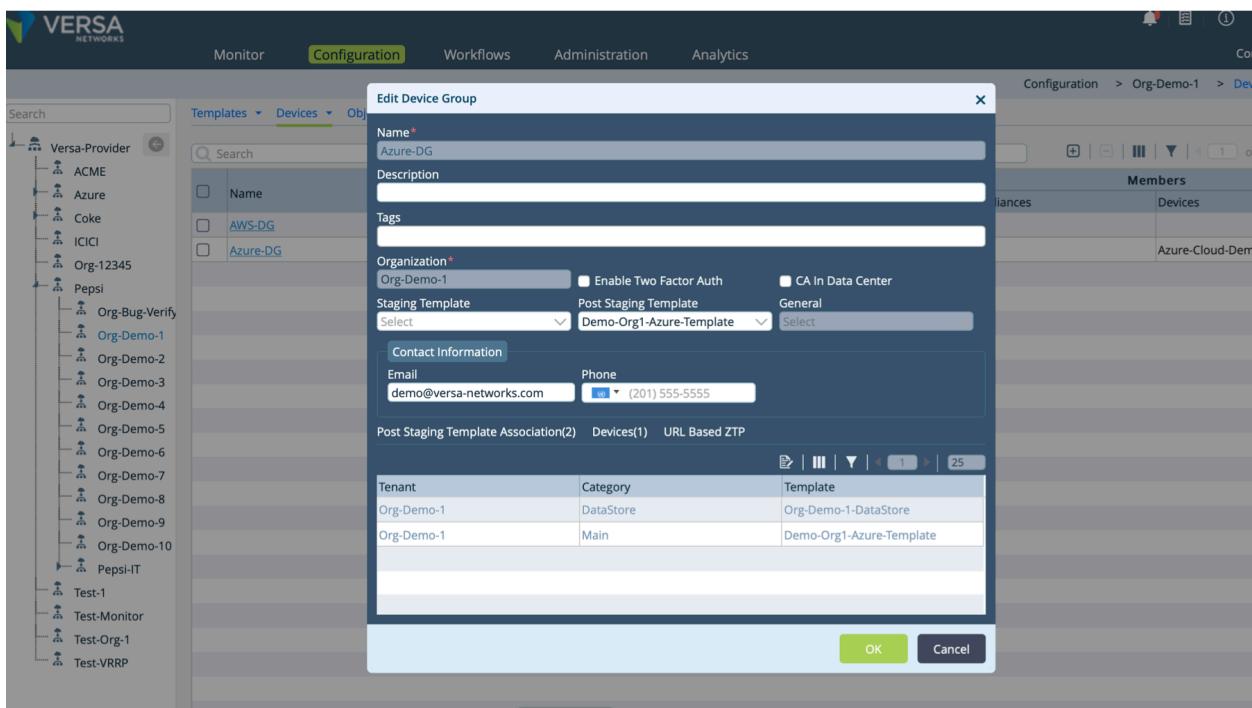
- Click Deploy to create the CMS cloud connector.

Deploy a VOS Branch Using a CMS Connector

- Log in to the Director node.
- Select the Workflows tab in the top menu bar.
- Select Template > Templates in the left menu bar.
- 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.

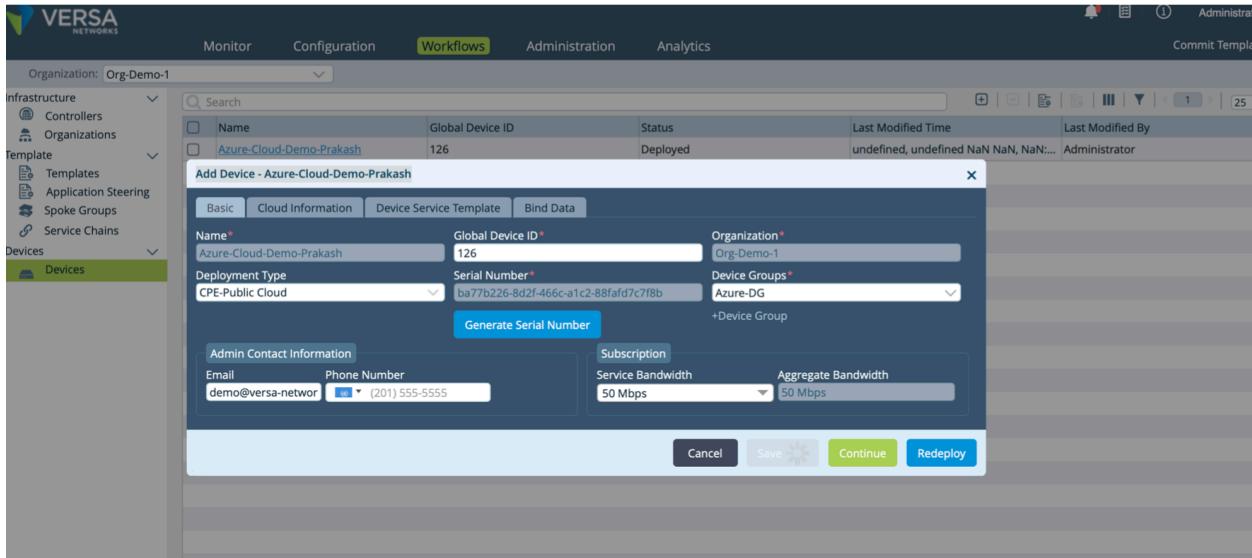


6. Select the Workflows tab in the top menu bar.
7. Select Devices > Devices in the left menu bar.
8. Create a new device. In the Deployment Type field, select the public cloud option, click Generate Serial Number to create a random serial number, and in the Device Groups field, select the newly created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

[https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Initial_Configuration/...](https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Initial_Configuration/)

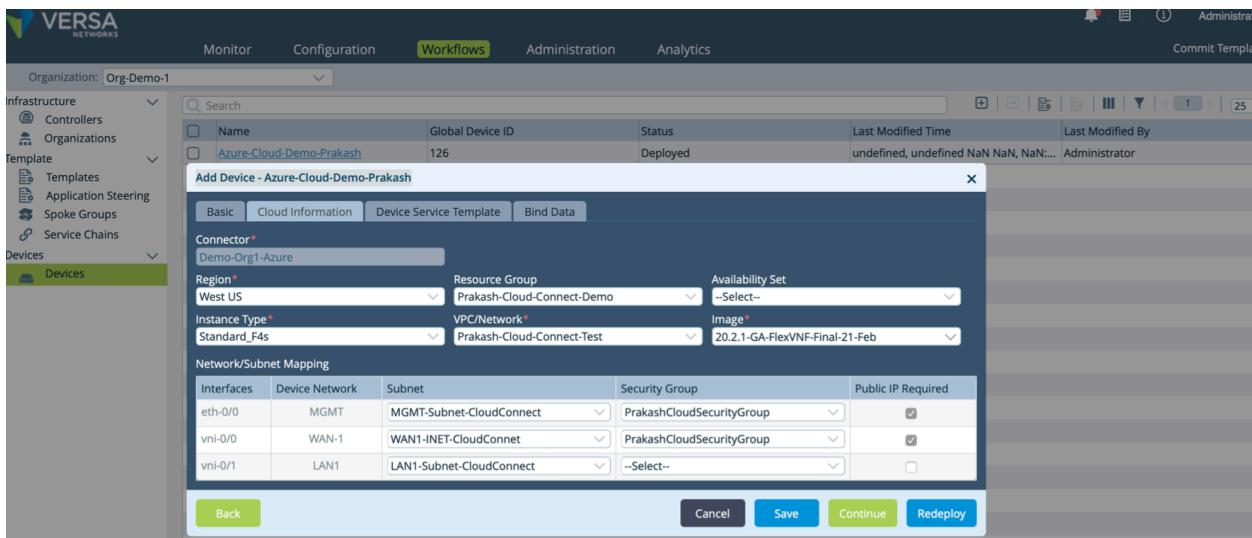
Updated: Wed, 23 Oct 2024 07:22:49 GMT

Copyright © 2024, Versa Networks, Inc.



- 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.



- Select the resource group, instance type, VPC network, and the image that is available for your subscription to use for the deployment.
- 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

[https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Initial_Configuration/...](https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Initial_Configuration/)

Updated: Wed, 23 Oct 2024 07:22:49 GMT

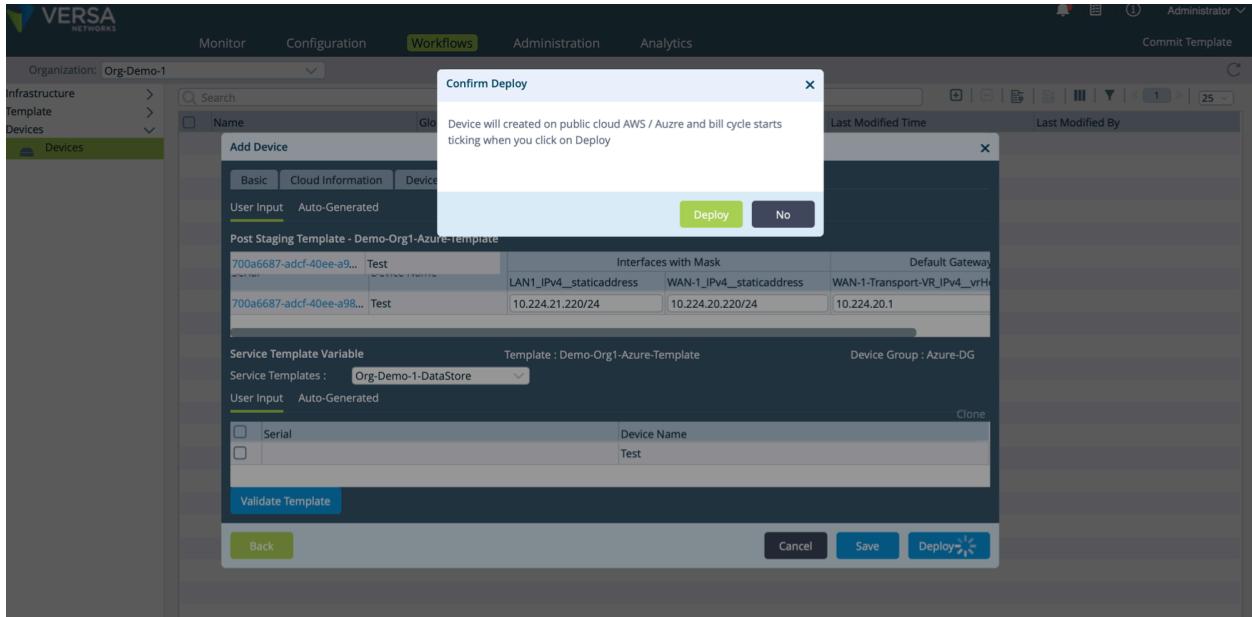
Copyright © 2024, Versa Networks, Inc.

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

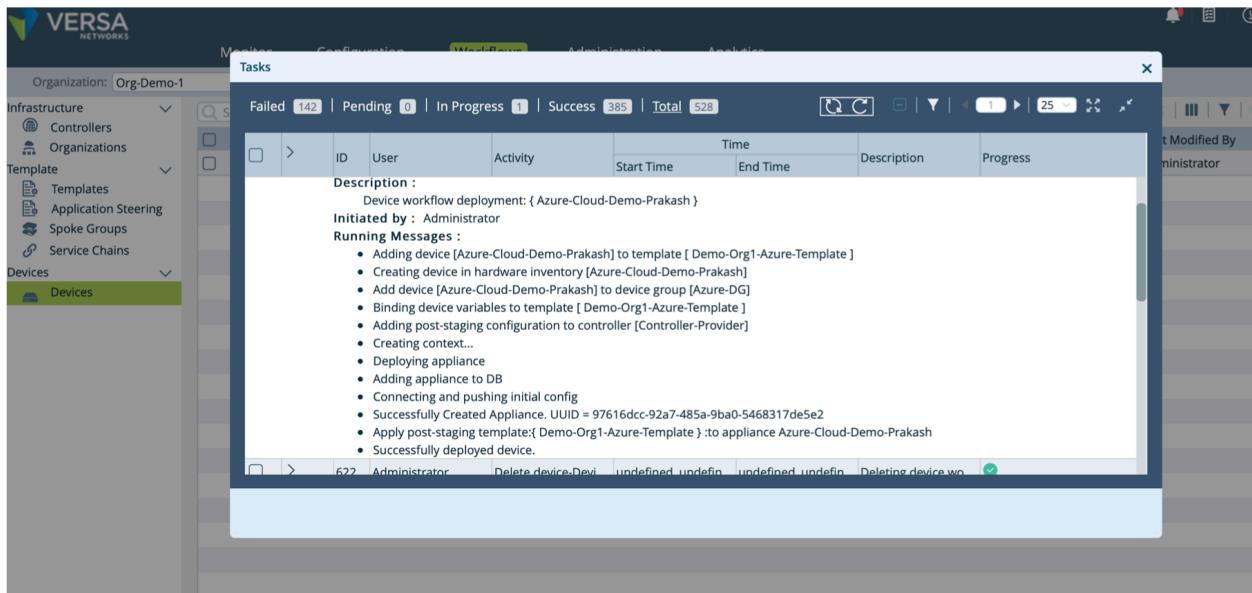
12. Select the Bind Data tab. Because we use static IP addressing in the template, select one unused IP address from each CIDR that you allocated in Azure for each of these subnets and enter it here. For our example, we select 10.224.20.221/24 for the WAN subnet, with the gateway as 10.224.20.1, and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

The screenshot shows the Versa Networks interface with the 'Devices' tab selected. A modal window titled 'Add Device - Azure-Cloud-Demo-Prakash' is open, specifically on the 'Bind Data' tab. The 'User Input' section is set to 'Auto-Generated'. The 'Post Staging Template - Demo-Org1-Azure-Template' section shows a table with two rows. The first row has columns: Serial (ba77b226-8d2f-466c-a1c2-88fafd7cf8b), Device Name (Azure-Cloud-Demo-Prakash), Interfaces with Mask (LAN1_IPv4_staticaddress), and Default Gateway (WAN-1-Transport-VR_IPv4_vrf). The second row has the same structure. Below this, the 'Service Template Variable' section shows 'Template : Demo-Org1-Azure-Template' and 'Device Group : Azure-DG'. The 'Service Templates' dropdown is set to 'Org-Demo-1-DataStore'. The 'User Input' section is again set to 'Auto-Generated'. At the bottom of the modal are buttons for 'Validate Template', 'Back', 'Cancel', 'Save', and 'Redeploy'.

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.

The screenshot shows the Versa Networks Administration interface. The left sidebar has a tree view with 'Organizations', 'Appliances' (selected), 'Notification Config...', 'Director User Mana...', and 'Inventory'. The main area title is 'Total Appliances : 1'. A search bar is at the top. Below is a table with columns: Name, Mgmt. Address, Type, Time Created, Service Start T..., Software Version, Site ID, Organizations, Snap..., Status, Config Syncr..., Reachability, Service, and Locked. One row is selected, showing 'Azure-Cloud-Demo...' with status 'Up'.

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.

This screenshot shows the Microsoft Azure portal's Virtual Machines list. The URL is 'https://portal.azure.com/#blade/HubsBlade'. The page header includes 'Microsoft Azure' and a search bar. The main content area shows a table of virtual machines. One row is selected, showing 'Azure-Cloud-Demo-Prakash' as a 'Virtual machine' in the 'Deleting' state. Other columns include 'Name', 'Status', 'Resource group', 'Location', 'Source', 'Maintenance status', and 'Subscription'.

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.

```
Prakashs-MacBook-Pro:Downloads prakash$ puttygen -t rsa -b 2048 -C -o Azure-prakash-keyfile.ppk
puttygen: cannot both load and generate a key
Prakashs-MacBook-Pro:Downloads prakash$ puttygen -t rsa -b 2048 -o Azure-prakash-keyfile.ppk
+++++
+++++
Enter passphrase to save key:
Re-enter passphrase to verify:
```

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

https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Initial_Configuration

Updated: Wed, 23 Oct 2024 07:22:49 GMT

Copyright © 2024, Versa Networks, Inc.

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

- 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 AAAAB3NzaC1yc2EAAAQEAhemgqF8hK+jsWFrdqnuRu9lhARIDPChPFT7zYbbZNiIU1xg+xb8iXRYG0jqmMlzf0+a0VcozGGrVJQXj2PzBM7MDCP8EPFo5/SDXG1ru+x
QIBbwZbsTbMvP/StSjbgpPqNhftBa64XzcQmfjRU3w== imported-openssh-key
```

- Log in to the Director node.
- Select the deployed instance, and go to Appliance mode.
- Select the Configuration tab in the top menu bar.
- Select Others > System > Appliance User Management > System Users in the left menu bar.
- 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.

Name	Contents*
Azure-Key1	ssh-rsa AAAAB3NzaC1yc2EAAAQEAhemgqF8hK+jsWFrdqnuRu9lhARIDPChPFT7zYbbZNiIU1xg+xb8iXRYG0jqmMlzf0+a0VcozGGrVJQXj2PzBM7MDCP8EPFo5/SDXG1ru+xQIBbwZbsTbMvP/StSjbgpPqNhftBa64XzcQmfjRU3w== imported-openssh-key

- Enter the public key that you extracted earlier, and then click OK.
- 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:

```
admin connected from 122.172.183.253 using ssh on Azure-Cloud-Demo-Prakash
admin@Azure-Cloud-Demo-Prakash-cli> show interfaces brief | tab
NAME          MAC          OPER  ADMIN   TENANT    VRF          IP
-----+-----+-----+-----+-----+-----+
eth-0/0      00:0d:3a:37:de:b9  up    up     0    global      10.224.22.4/24
ptvi70      n/a          up    up     1    Org-Demo-1-Control-VR 10.0.0.3/32
tvi-0/140    n/a          up    up     -    -
tvi-0/140.0   n/a          up    up     1    Org-Demo-1-Control-VR 10.0.0.68/32
tvi-0/141    n/a          up    up     -    -
tvi-0/141.0   n/a          up    up     1    Org-Demo-1-Control-VR 10.0.0.69/32
tvi-0/602    n/a          up    up     -    -
tvi-0/602.0   n/a          up    up     1    WAN-1-Transport-VR 169.254.0.2/31
tvi-0/603    n/a          up    up     -    -
tvi-0/603.0   n/a          up    up     1    Org-Demo-1           169.254.0.3/31
vni-0/0      00:0d:3a:37:d2:50  up    up     -    -
vni-0/0.0    00:0d:3a:37:d2:50  up    up     1    WAN-1-Transport-VR 10.224.20.221/24
vni-0/1      00:0d:3a:37:da:97  up    up     -    -
vni-0/1.0    00:0d:3a:37:da:97 up    up     1    Org-Demo-1           10.224.21.221/24

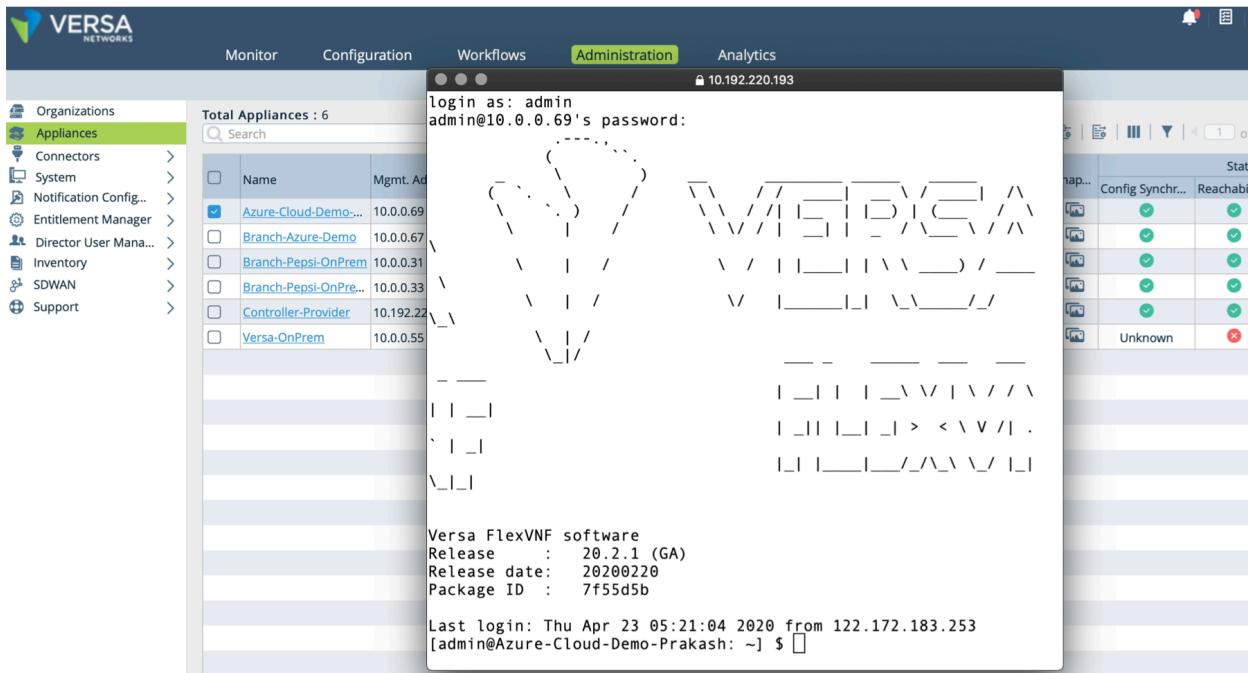
[ok][2020-04-23 05:21:50]
admin@Azure-Cloud-Demo-Prakash-cli>
```

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

https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Initial_Configuration

Updated: Wed, 23 Oct 2024 07:22:49 GMT

Copyright © 2024 Versa Networks, Inc.



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](#)