Connecting Cisco Data Center and a Public Cloud

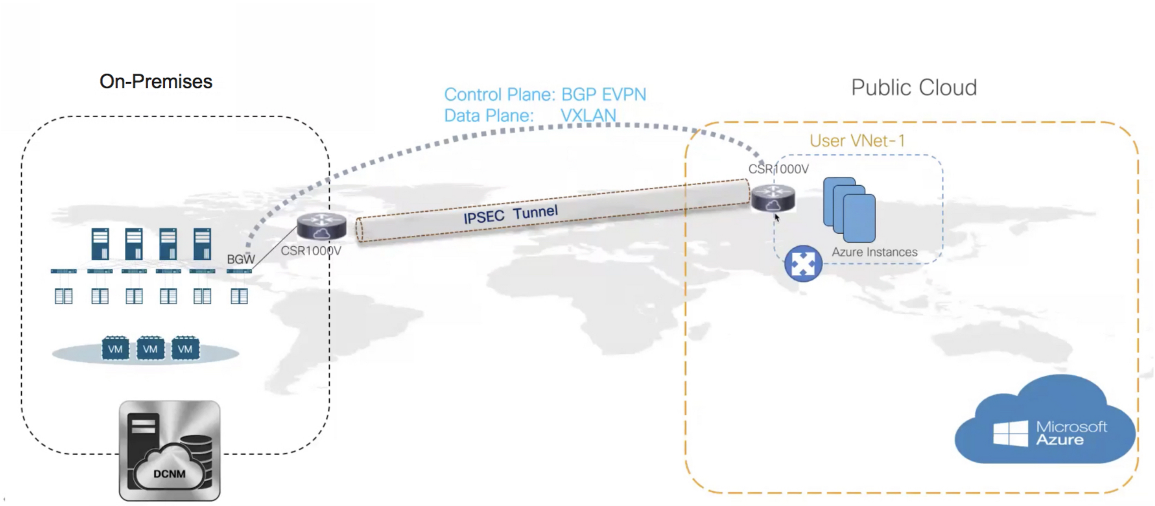
Connecting Cisco Data Center and a Public Cloud

This section explains the functionality that allows public cloud connectivity from a Cisco DCNM provisioned VXLAN EVPN fabric to the Microsoft Azure public cloud. The layer-3 connectivity ensures a seamless and secure communication between the workloads on premise and the Microsoft Azure cloud. The connectivity is provisioned through the Cisco Cloud Services Router 1000v (Cisco CSR 1000v) that is managed by Cisco DCNM. BGP EVPN is employed for the control plane and VXLAN is employed for the data plane. A secure IPsec tunnel is established between the Cisco CSR 1000v in the premise and the Cisco CSR 1000v in the public cloud.

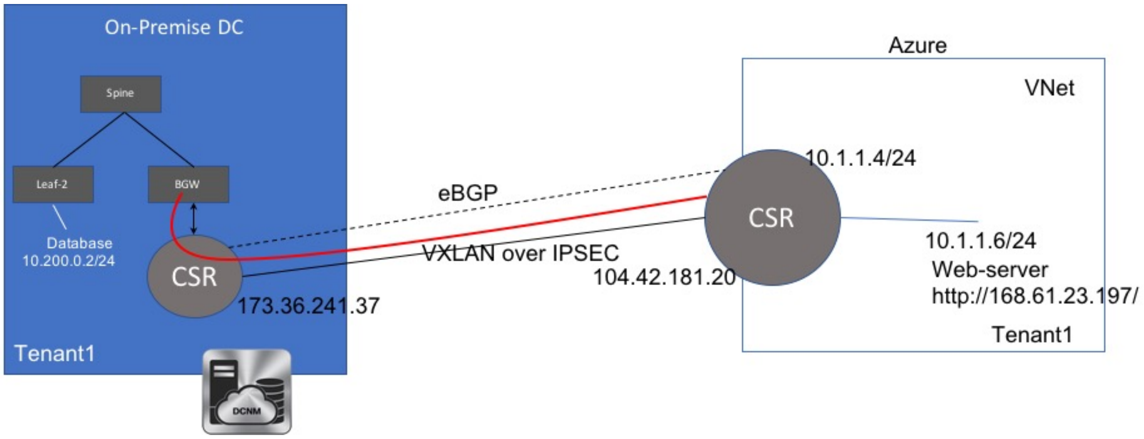
Note Cisco DCNM supports discovery and management Cisco CSR 1000v. This functionality is a preview feature in Cisco DCNM Release 11.2(1). After an inline upgrade to Cisco DCNM Release 11.3(1), this feature is enabled by default.

Topology Overview

Figure 1: Topology Overview



The on-premise data center has the required switches. One of these switches is a border gateway (BGW) that interfaces with an core router for WAN connectivity to the public cloud. The Cisco CSR 1000v is the core router in this use case. You can import this core router into an external fabric in Cisco DCNM. The following figure depicts the sample topology that is employed.



In this example, we list the tasks that are required to provide a layer-3 connectivity between a VM behind standalone leaf and a VM in the Microsoft Azure cloud in a specific user VNET.

The public cloud has a Cisco CSR 1000v, Microsoft Azure instances, Azure Virtual Networks (Azure VNets), and a VM. The Cisco CSR 1000v in the cloud has an interface with the VM.

We are using eBGP between the two core routers for exchanging underlay routing and reachability. The VXLAN connects the on-premises BGW and the core router on Microsoft Azure, over the IPsec tunnel.

In this use-case, we are going to configure the setup as follows:

Guidelines and Limitations

The following are the guidelines and limitations for connecting an on-premises data center and a public cloud:

- Cisco CSR 1000v Series Routers support route-based IP Security (IPsec) tunnel interface.
- Use Cisco Nexus 9000 Series Switches or Cisco Nexus 3000 Series Switches in the VXLAN EVPN Easy fabric in Cisco DCNM.
- The IP addresses specified in this document are sample addresses. Ensure that your setup reflects the IP addresses used in the production network.

Prerequisites

- Create an account with Microsoft Azure.
- Create VNets for the public-cloud core router in Microsoft Azure.
- Deploy a Cisco CSR 1000v in Microsoft Azure. This Cisco CSR 1000v is the public-cloud core router. See the Deploying Cisco CSR 1000v on Microsoft Azure, on page 21 section for more information.
- Use switches that support Cisco NX-OS Release 7.0(3)I7(x) or higher versions as border gateways are required.
- Set up the Cisco DCNM, switches, Cisco CSR 1000v, and other devices in a DMZ or equivalent zone to have access to the public internet.
- Familiarity with VXLAN BGP EVPN data center fabric architecture and configuration through DCNM.
- Familiarity with MSD fabrics.

Note Refer to the *Control* chapter in the *Cisco DCNM LAN Fabric Configuration Guide*, for information on various tasks that are required in setting up.

Task Summary

The following sections list the task summary to establish a connection between the on-premises data center and the public cloud.

On-premises Data Center

1. Set the polling time.
2. Create a fabric with switches for the on-premises data center, and configure one of the switches with BGW role.
3. Create an external fabric for the on-premises core router. Discover a Cisco CSR 1000v as the core router.
4. Simulate an IP address as on-premises host on the BGW.

Public Cloud

1. Create an external fabric for the public cloud core router.
2. Discover a Cisco CSR 1000v for the public cloud, which is the core router.

Connectivity

1. Create an MSD fabric and import the fabrics that were created previously.
2. Connect the BGW and the on-premises core router.
3. Create an IPsec tunnel between the on-premises core router and the public-cloud core router.
4. Create an eBGP underlay connection between the core routers that runs over the IPsec Tunnel.
5. Connect the BGW and the public cloud core router using VXLAN EVPN.
6. Extend the VRFs in fabrics.

The procedure that is involved in each task in this section is explained in the following sections.

Setting the Polling Time

Cisco DCNM queries the on-premises core router and updates the state of the routing table depending on the polling time you set. To set the polling time from the Cisco DCNM Web UI, perform the following steps:

Procedure

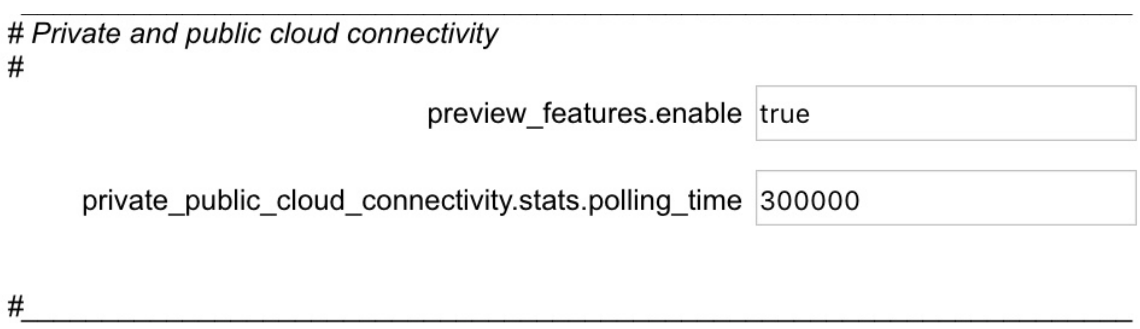
Step 1 Choose **Administration > DCNM Server > Server Properties**.

The **Server Properties** window appears.

Step 2 Locate the **Private and public cloud connectivity** properties.

Step 3 Set the polling time in the **private_public_cloud_connectivity.stats.polling_time** field.

The value is in milliseconds.



```
# Private and public cloud connectivity
#
                                      preview_features.enable  true

        private_public_cloud_connectivity.stats.polling_time  300000

#______________________________________________________________________
```

Step 4 Click **Apply Changes**.

Step 5 Restart Cisco DCNM using the **appmgr restart dcnm** command.

A warning about the preview features enabled appears after you log in to the Cisco DCNM Web UI.

Note This is a preview only feature. We recommend that you use this feature only in lab setups, and not in production environments.

Setting Up the On-premise External Fabric with CSR 1000v

Create an external fabric for the on-premises edge router.

Creating an External Fabric

To create an external fabric from Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Control** > **Fabrics** > **Fabric Builder**.

The **Fabric Builder** window appears.

Step 2 Click **Create Fabric**.

The **Add Fabric** dialog box appears.

Step 3 Enter the fabric name as **CSR-OnPrem** in the **Fabric Name** field.

Step 4 Choose **External_Fabric_11_1** from the Fabric Template drop-down list.

Step 5 Enter the BGP AS number in the **BGP AS #** field.

Step 6 Uncheck the **Fabric Monitor Mode** check box.

Step 7 Click **Save**.

A fabric is created and the fabric topology window appears.

What to do next

Discover the on-premises core router.

Discovering the On-Premises Core Router

Cisco CSR 1000v is used for on-premises core routing. To discover the core router in the fabric topology window, perform the following steps:

Before you begin

Ensure that you know the credentials of the core router.

Procedure

Step 1 Click **Add switches** in the Actions pane.

The **Inventory Management** dialog box appears.

Step 2 Enter values for the following fields under the **Discover Existing Switches** tab:

Field	Description
Seed IP	Enter the IP address of the core router.
Device Type	Choose **IOS XE** from the drop-down list, and click the **CSR** radio button.
Username	Enter the username of the core router for SSH access.
Password	Enter the password of the core router for SSH access.

Note An error appears if you try to discover a switch that is already discovered.

Step 3 Click **Start Discovery**.

The fabric topology window appears, and a pop-up message appears at the bottom-right about the discovery.

For example: <*ip-address*> added for discovery.

Note Discovering switches might take some time.

Step 4 Click **Tabular view** in the Actions pane.

The switches and links window appears, where you can view the scan details. The discovery status is discovering in red with a warning icon next to it if the discovery is in progress.

Step 5 View the details of the core router.

After the router is discovered:

- The discovery status changes to **ok** in green with a check box checked next to it.
- The value of the router under the **Fabric Status** column will be **In-Sync**.

Step 6 Go back to the fabric topology window and refresh the topology.

What to do next

Set the role of the router to **Core Router**. Right-click the router, choose **Set role > Core Router**.

Set up a VXLAN EVPN fabric for the on-premises data center, which has a BGW.

Setting Up the VXLAN EVPN Fabric

Create a fabric for the BGW.

Creating a VXLAN EVPN Fabric

To create a VXLAN EVPN fabric from Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Control** > **Fabrics** > **Fabric Builder**.

The **Fabric Builder** window appears.

Step 2 Click **Create Fabric**.

The **Add Fabric** dialog box appears.

Step 3 Enter the fabric name as **site2** in the **Fabric Name** field.

Step 4 Choose **Easy_Fabric_11_1** from the **Fabric Template** drop-down list.

Step 5 Enter values in all the mandatory fields.

Step 6 Click **Save**.

A fabric is created and the fabric topology window appears.

What to do next

Add switches in this fabric and assign the BGW role for one of the switches.

Assigning the BGW Role

To assign a switch with the BGW role, perform the following steps:

Before you begin

Add switches to the **site2** fabric.

Procedure

Step 1 Right-click the switch for which you need to set the BGW role.

A list of actions that you can perform on the switch appears.

Step 2 Choose **Set role** > **Border Gateway**.

What to do next

Set up a fabric for the public cloud.

Setting Up the External Fabric with CSR in Azure

Create an external fabric for the public cloud core router.

Creating an External Fabric

To create an external fabric from Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Control** > **Fabrics** > **Fabric Builder**.

The **Fabric Builder** window appears.

Step 2 Click **Create Fabric**.

The **Add Fabric** dialog box appears.

Step 3 Enter the fabric name as **CSR-Azure** in the **Fabric Name** field.

Step 4 Choose **External_Fabric_11_1** from the **Fabric Template** drop-down list.

Step 5 Enter the BGP AS number in the **BGP AS # field**.

Step 6 Uncheck the **Fabric Monitor Mode** check box.

Step 7 Click **Save**.

A fabric is created and the fabric topology window appears.

What to do next

Discover the public-cloud core router in this fabric.

Discovering the Core Router

Cisco CSR 1000v Series router is used for the public-cloud core routing as well. To discover the core router in the fabric topology window, perform the following steps:

Before you begin

Ensure that you know the credentials of the core router.

Procedure

Step 1 Click **Add switches** in the **Actions** pane.

The **Inventory Management** dialog box appears.

Step 2 Enter values for the following fields under the **Discover Existing Switches** tab:

Field	Description
Seed IP	Enter the IP address of the core router.
Device Type	Choose **IOS XE** from the drop-down list, and click the **CSR** radio button.
Username	Enter the username of the core router for SSH access.
Password	Enter the password of the core router for SSH access.

Note An error message appears if you try to discover a switch that is already discovered.

Step 3 Click **Start Discovery**.

The fabric topology window appears, and a pop-up message appears at the bottom-right about the switch discovery. For example: **<ip-address> added for discovery**

Note Discovering switches takes some time.

Step 4 Click **Tabular view** in the **Actions** pane.

The switches and links window appears, where you can view the scan details. The discovery status is **discovering** in red with a warning icon next to it if the discovery is in progress.

Step 5 View the details of the core router.

After the discovery of the router:

- The discovery status changes to **ok** in green with a check box checked next to it.
- The value of the router under the **Fabric Status** column changes to **In-Sync**.

Step 6 Go back to the fabric topology window and refresh the topology.

What to do next

Set the role of the router to **Core Router**. Right-click the router, choose **Set role > Core Router**.

Create an MSD fabric and import other fabrics, created previously, into it.

Setting Up the MSD Fabric for Connectivity

Create an MSD fabric to bring all the standalone fabrics together for connectivity.

Creating an MSD Fabric

To create an MSD fabric from Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Control** > **Fabrics** > **Fabric Builder**.

The **Fabric Builder** window appears.

Step 2 Click **Create Fabric**.

The **Add Fabric** dialog box appears.

Step 3 Enter the fabric name as **Cloud-Connect** in the **Fabric Name** field.

Step 4 Choose **MSD_Fabric_11_1** from the **Fabric Template** drop-down list.

Step 5 Enter values in all the mandatory fields.

Step 6 Click **Save**.

A fabric is created and the fabric topology window appears.

What to do next

Move other fabrics into this MSD fabric.

Moving Other Fabrics into the MSD Fabric

To move other fabrics into the **Cloud-Connect** fabric from the fabric topology window, perform the following steps:

Procedure

Step 1 Click **Move Fabric** in the **Actions** pane.

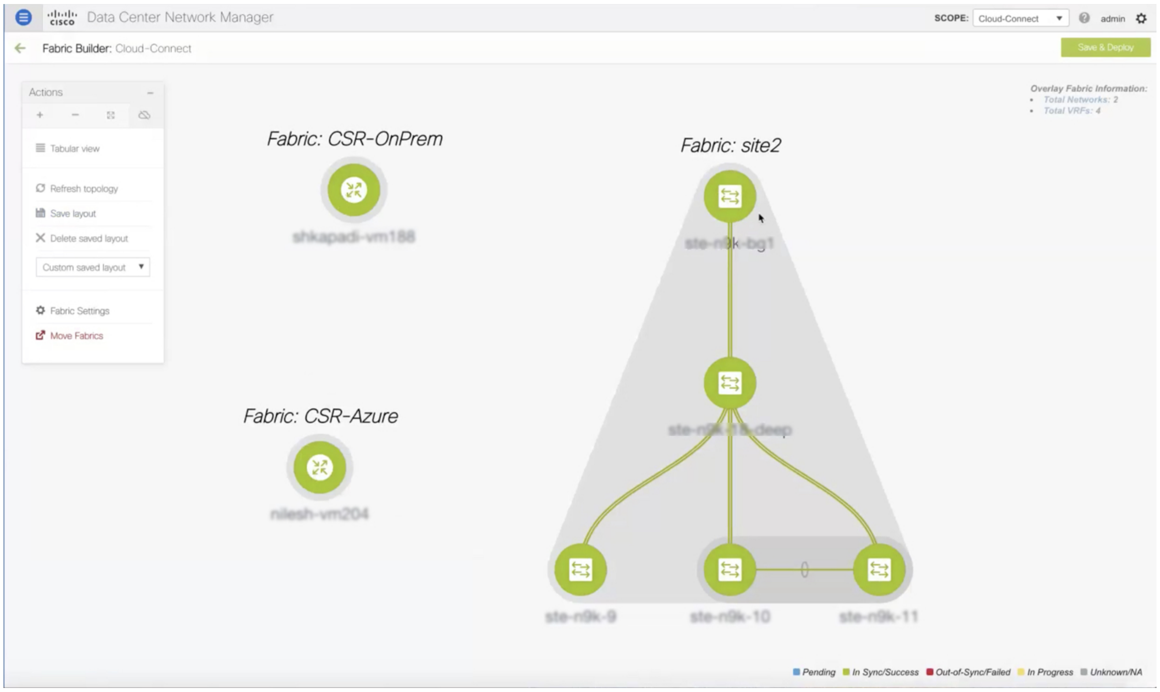
The **Move Fabric** dialog box appears. It contains a list of fabrics.

Step 2 Choose **CSR-OnPRem**, **site2**, and **CSR-Azure** fabrics.

Step 3 Click **Add**.

Step 4 Close the dialog box and refresh the fabric topology.

All the member fabrics appear in the **Cloud-Connect** fabric.



What to do next

Set up the connections between fabrics.

Setting Up Connections

Connect the fabrics that you created previously using different links.

Connecting the On-Premises BGW and the On-Premises Core Router

To add a link between the on-premises BGW and the on-premises core router, perform the following steps:

Procedure

Step 1 Right-click anywhere in the **Cloud-Connect** topology window.

The actions that you can perform in the fabric appears in a list. Alternatively, from the fabric topology window, choose **Tabular view** in the **Actions** pane, and click the **Links** tab.

Step 2 Choose **Add Link**.

The **Link Management - Add Link** dialog box appears.

Step 3 Enter values for the following fields:

Field	Description
Link Type	Choose the **Inter-Fabric** link type from the drop-down list.
Link Sub-Type	Choose the **MULTISITE_UNDERLAY** link sub-type from the drop-down list.
Link Template	Choose the **csr_ext_multisite_underlay_setup** link template from the drop-down list. **Note** This template is available only after you enable the preview functionality and restart the DCNM.
Source Fabric	Choose **site2** as the source fabric from the drop-down list.
Destination Fabric	Choose **CSR-OnPrem** as the destination fabric from the drop-down list.
Source Device	Choose the BGW from the drop-down list.
Source Interface	Choose the BGW’s interface.
Destination Device	Choose the on-premises core router from the drop-down list.
Destination Interface	Choose the on-premises core router’s interface from the drop-down list.

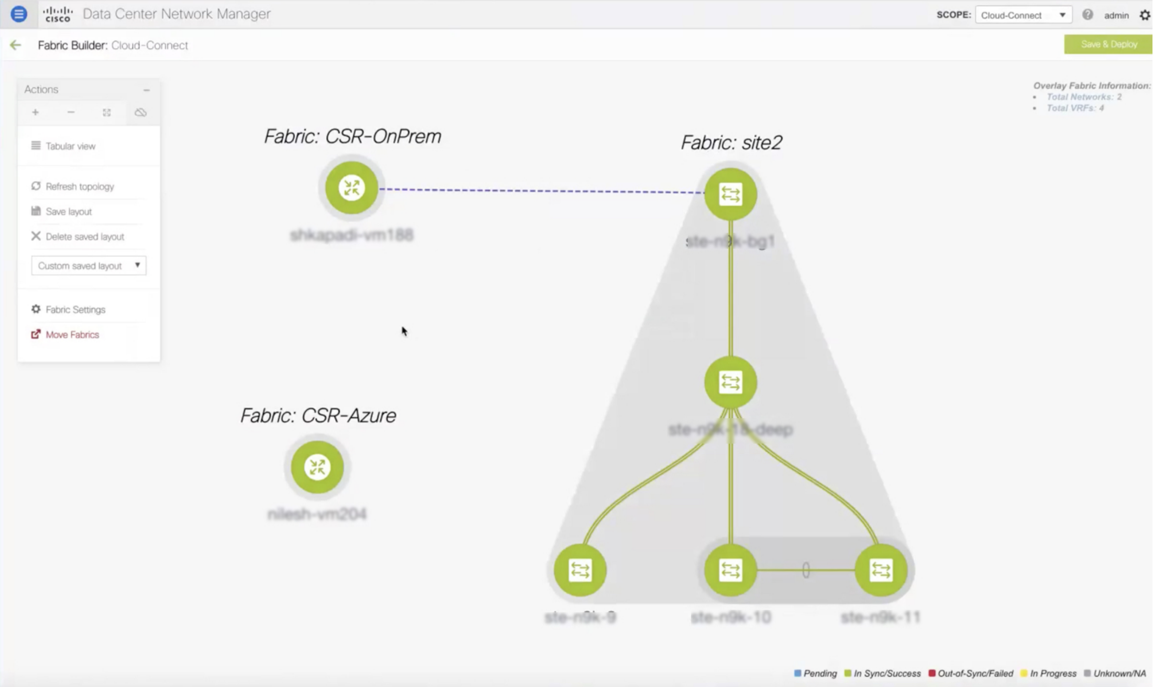
Step 4 Enter values for the following fields under the **Link Profile** area in the **General** tab:

Field	Description
IP_MASK	Enter the IPv4 address of the source interface with a subnet.
NEIGHBOR_IP	Enter the IPv4 address of the destination interface.

To verify the IP address from the Cisco DCNM Web UI, choose **Control** > **Fabrics** > **Interfaces**. Choose the fabric from the **Scope** drop-down list, and search the device. The IP address of the device will be listed in the **IP/Prefix** column.

Step 5 Click **Save**.

The fabric topology window refreshes. A link is added between the on-premises BGW in the **site2** fabric and the on-premises core router in the **CSR-OnPrem** fabric.



SCOPE: Cloud-Connect

What to do next

Connect the on-premises core router and the public-cloud core router.

Connecting the On-prem Core Router and the Public-cloud Core Router with IPsec Tunnel

To add a link between the on-prem core router and the public-cloud core router, perform the following steps:

Procedure

Step 1 Right-click anywhere in the **Cloud-Connect** topology window.

The actions that you can perform in the fabric appears in a list. Alternatively, from the fabric topology window, choose **Tabular view** in the **Actions** pane, and click the **Links** tab.

Step 2 Choose **Add Link**.

The **Link Management - Add Link** dialog box appears.

Step 3 Enter values for the following fields:

Field	Description
Link Type	Choose the **Inter-Fabric** link type from the drop-down list.
Link Sub-Type	Choose the **BGP_OVER_IPSEC** link sub-type from the drop-down list.
Link Template	Choose the **csr_link_template** link template from the drop-down list.
Source Fabric	Choose **CSR-OnPrem** as the source fabric from the drop-down list.
Destination Fabric	Choose **CSR-Azure** as the destination fabric from the drop-down list.
Source Device	Choose the on-prem core router from the drop-down list.
Source Interface	Choose the on-prem core router's interface.
Destination Device	Choose the public-cloud core router from the drop-down list.
Destination Interface	Choose the public-cloud core router's interface from the drop-down list.

Step 4 In the **Link Profile** area under the **General** tab, enter the the pass key used for IPSec tunnel in the **SHARED_KEY** field.

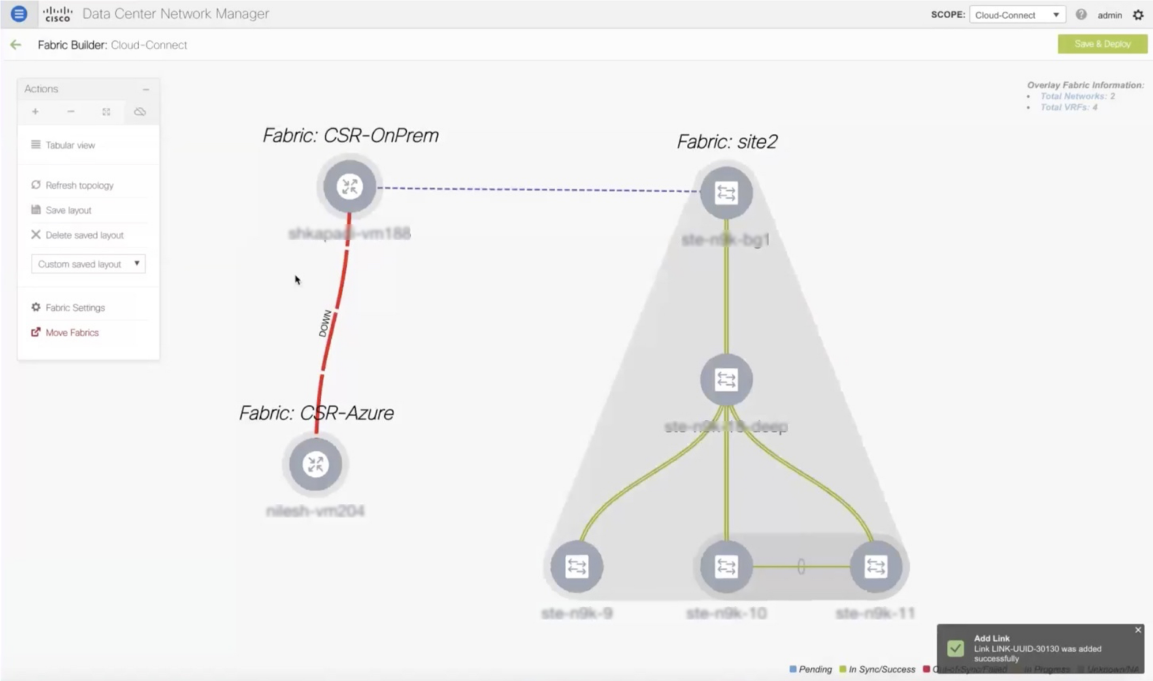
Step 5 (Optional) In the Link Profile area, choose the **Advanced** tab.

The fields under this tab have default values populated. Change the values if needed. This will create a loopback for which the eBGP peering is configured between the two core routers.

Step 6 Click **Save**.

The fabric topology window refreshes, and a link is added between the core routers in the **CSR-OnPrem** fabric and the **CSR-Azure** fabric.

Note The link will be down till you push it into the configuration.



Overlay Fabric Information:

- Total Networks: 2
- Total VRFs: 4

Add Link
Link LINK-UUID-30130 was added successfully

What to do next

Connect the on-prem BGW and the public-cloud core router.

Connecting the On-prem BGW and the Public-cloud Core Router using EVPN Peering

To add a link between the on-prem core router and the public-cloud core router, perform the following steps:

Procedure

Step 1 Right-click anywhere in the **Cloud-Connect** topology window.

The actions that you can perform in the fabric appears in a list. Alternatively, from the fabric topology window, choose **Tabular view** in the **Actions** pane, and click the **Links** tab.

Step 2 Choose **Add Link**.

The **Link Management - Add Link** dialog box appears.

Step 3 Enter values for the following fields:

Field	Description
Link Type	Choose the **Inter-Fabric** link type from the drop-down list.
Link Sub-Type	Choose the **MULTISITE_OVERLAY** link sub-type from the drop-down list.
Link Template	Choose the **csr_ext_evpn_multisite_overlay_setup** link template from the drop-down list.

Field	Description
Source Fabric	Choose **site2** as the source fabric from the drop-down list.
Destination Fabric	Choose **CSR-Azure** as the destination fabric from the drop-down list.
Source Device	Choose the on-prem BGW from the drop-down list.
Source Interface	Choose the on-prem BGW's loopback interface.
Destination Device	Choose the public-cloud core router from the drop-down list.
Destination Interface	Choose the public-cloud core router's interface from the drop-down list. **Note** If you did not create an interface, the destination interface will not appear in the drop-down list and you have to enter the destination interface.

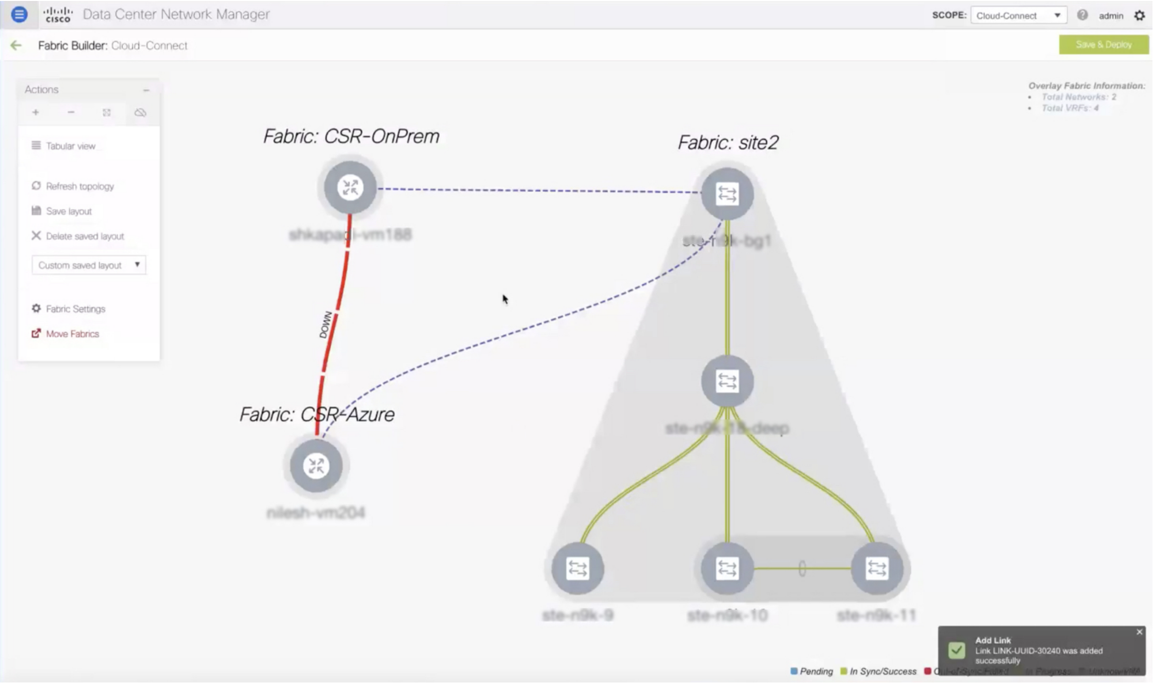
Step 4 Enter values for the following fields under the **Link Profile** area in the **General** tab:

Field	Description
IP_MASK	Enter the IPv4 address of the source interface with subnet.
NEIGHBOR_IP	Enter the IPV4 address of the destination interface.

Step 5 Click **Save**.

The fabric topology window refreshes, and a link is added between the BGW in the **site2** fabric and the core router in the **CSR-Azure** fabric.

Note The link will be down till you push it into the configuration.



Add Link
Link LINK-UUID-30240 was added successfully

What to do next

Save and deploy the configurations.

Saving and Deploying Configurations

To save and deploy the configurations in the fabric topology window, perform the following steps:

Procedure

Step 1 Click **Save & Deploy**.

The **Config Deployment** dialog box appears, and you will see the **Configuration Preview** step. The intents for the links created among the BGW, on-prem data center, and the public cloud are generated.

Step 2 (Optional) Click the field against the BGW in the **Preview Config** column.

The **Config Preview** dialog box appears for the BGW.

Step 3 (Optional) View the configuration details in the **Pending Config** column.

It includes details about the underlay peering and overlay peering.

Step 4 (Optional) Click the field against the on-prem core router in the **Preview Config** column.

The **Config Preview** dialog box appears for the on-prem core router.

Step 5 (Optional) View the configuration details in the **Pending Config** column.

It includes details about the interfaces, the IPsec tunnel, shared key, BGP peering between the core routers, and EVPN peering. Route maps are added indicating that all the BGP traffic and the data traffic should go through the tunnel.

Step 6 (Optional) Click the field against the public cloud core router in the **Preview Config** column.

The **Config Preview** dialog box appears for the on-prem core router.

Step 7 (Optional) View the configuration details in the **Pending Config** column.

It includes the details about VTEPs in addition to the details mentioned for the on-prem core router.

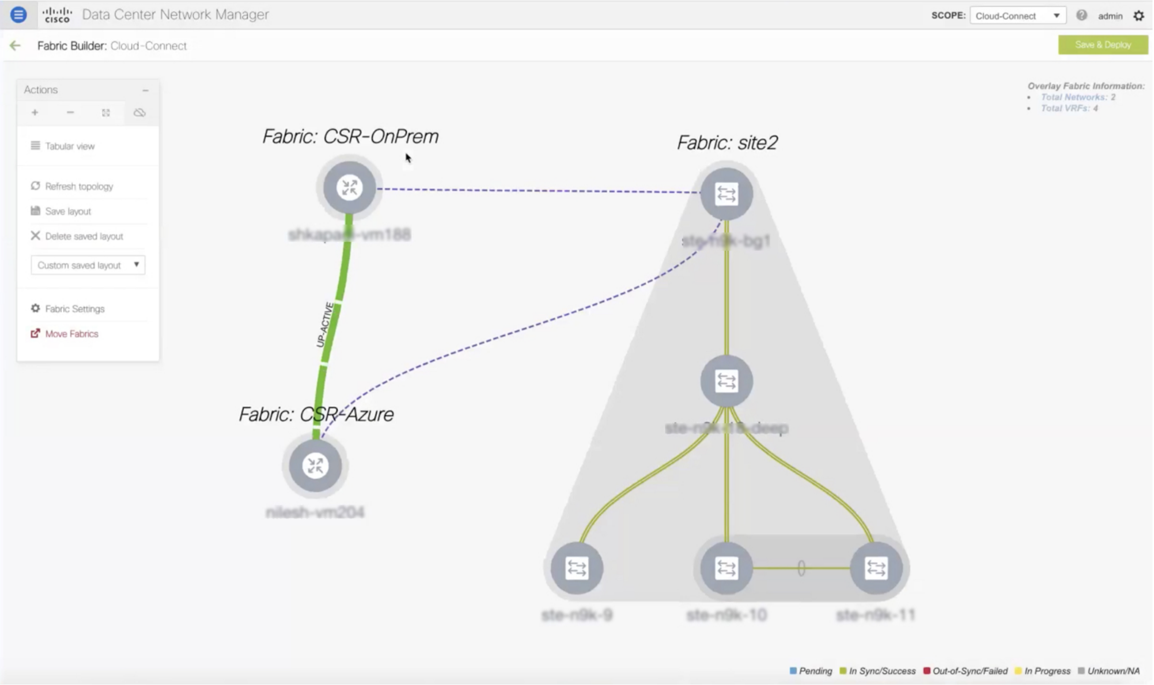
Step 8 Click **Deploy Config**.

The **Configuration Deployment Status** step appears, where you can see the deployment status of the configurations.

Step 9 Click **Close** after the successful deployment.

The fabric topology window appears. The IPsec tunnel will be up and active.

Note The deployment might take some time.



What to do next

Extend VRFs and deploy them.

Extending VRFs

VRFs are extended so that the workloads can be shared between the data center and the public cloud.

Deploying and Extending the VRF On-prem Core Router

To extend a VRF and deploy it on the on-prem core router from the fabric topology window of the MSD fabric, perform the following steps:

Procedure

Step 1 Click the **Total VRF** link in the **Overlay Fabric Information** area, which is below the **Save & Deploy** icon.

The **Network / VRF Selection** area of the VRFs window appears for the fabric.

Step 2 Choose the VRF for the on-prem core router and click **Continue**.

The **Network / VRF Deployment** area of the VRFs window appears. The network topology of the fabric appears. You can hide the undiscovered cloud.

Step 3 Double-click the BGW.

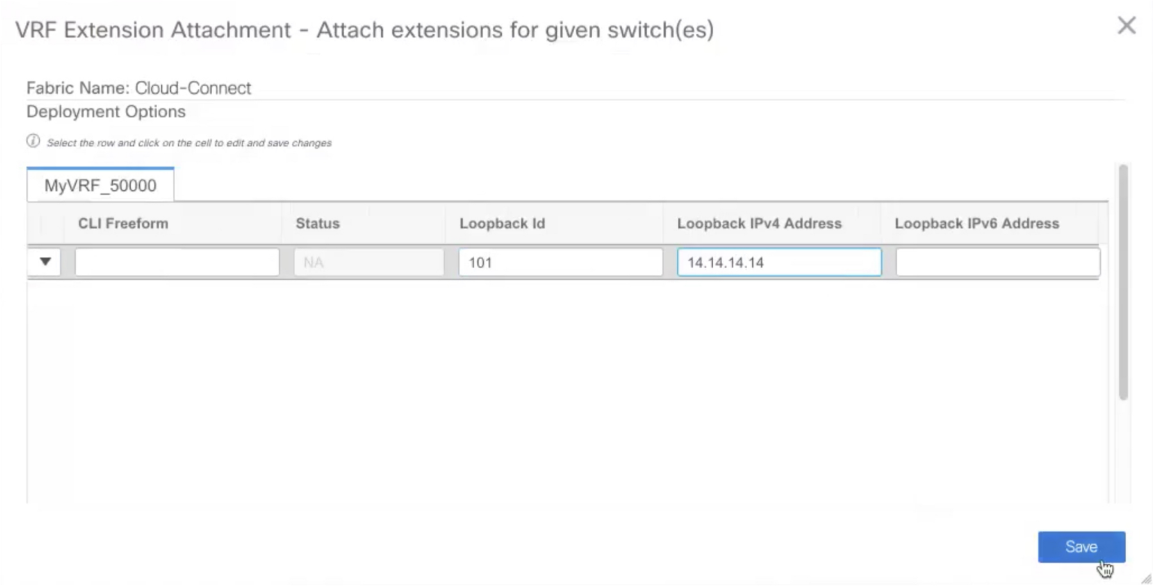
The **VRF Extension Attachment** dialog box appears.

Step 4 Choose the BGW and click the edit icon under the **Extend** column, to enable multi-site on it.

A drop-down list appears under the **Extend** column.

Step 5 Choose **MULTISITE** from the drop-down list.

Step 6 Enter the loopback ID and the loopback IPv4 address under the respective columns to simulate the host on BGW.



VRF Extension Attachment - Attach extensions for given switch(es)

Fabric Name: Cloud-Connect

Deployment Options

Select the row and click on the cell to edit and save changes

MyVRF_50000

	CLI Freeform	Status	Loopback Id	Loopback IPv4 Address	Loopback IPv6 Address
▼		NA	101	14.14.14.14	

Step 7 Click **Save**.

The network topology of the fabric appears and the BGW will turn blue indicating that the deployment is pending.

Step 8 Click the preview option.

The **Preview Configuration** dialog box appears. The EVPN configurations are pushed and the loopback interface is created.

Step 9 Click **Deploy**.

What to do next

Create a VRF and deploy it on the public cloud.

Creating and Deploying VRF on Public Cloud

To extend a VRF and deploy it on the public cloud core router from the fabric topology window, perform the following steps:

Before you begin

Ensure the VM is up and running. The VM should be attached to the public-cloud core router.

Procedure

Step 1 Choose the **CSR-Azure** fabric from the **Fabric Builder** window.

The fabric topology window appears.

Step 2 Right-click the public cloud core router.

A list of actions that you can perform on the router appears.

Step 3 Choose **View/edit policies** from the list.

The **View/Edit Policies** dialog box appears.

Step 4 Click the **Add Policy** icon.

The **Add Policy** dialog box appears.

Step 5 Choose the **csr_vrf_evpn** policy from the **Policy** drop-down list.

Step 6 Enter values in mandatory fields in the **General** tab.

Step 7 Click **Save**.

The **View/Edit Policies** dialog box appears.

Step 8 Click **View All** to view the networks and interfaces created.

The **Generated Config** dialog box appears. Details about the VRF, bridge domain, and the mapped VNI can also be viewed in this dialog box.

What to do next

Configure a default gateway on the public-cloud core router for the VM in the public cloud.

Configuring Default Gateway for the VM

To configure a default gateway on the public-cloud core router from the fabric topology window, perform the following steps:

Procedure

Step 1 Choose the **CSR-Azure** fabric from the Fabric Builder window.

The fabric topology window appears.

Step 2 Right-click the public-cloud core router.

A list of actions that you can perform on the router appears.

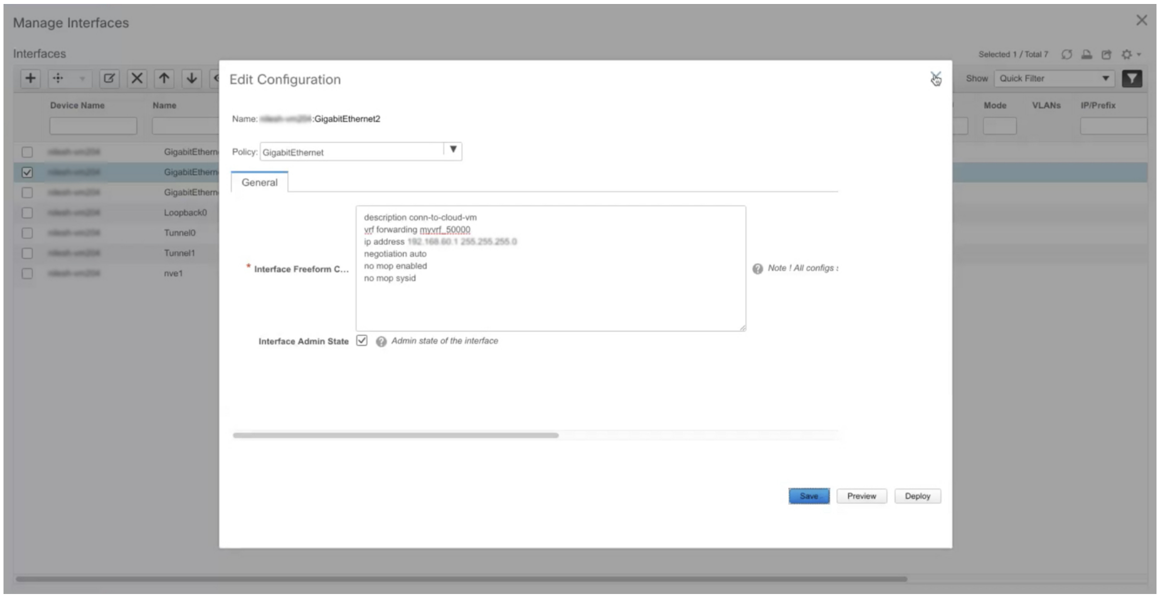
Step 3 Choose **Manage Interfaces** from the list.

The **Manage Interfaces** dialog box appears.

Step 4 Click **Edit Configuration** to edit the interface for which the policy is created.

The **Edit Configuration** dialog box appears.

Step 5 Edit the freeform config, click **Save**, and close the **Manage Interfaces** dialog box.



Name: [redacted]:GigabitEthernet2

Policy: GigabitEthernet

* Interface Freeform C...

```
description conn-to-cloud-vm
vrf forwarding myvrf_50000
ip address [redacted]
negotiation auto
no mop enabled
no mop sysid
```

Interface Admin State ☑ Admin state of the interface

The fabric topology window appears.

Step 6 Right-click the public-cloud core router and choose **Deploy Config** from the list.

The **Config Deployment** dialog box appears.

Step 7 Click the value under the **Preview Config** column to check the preview configuration.

Step 8 Click **Deploy Config** to deploy the configuration.

The configuration will be pushed and deployed.

Step 9 Click **Close**.

Step 10 Log on to the CLI to view the traffic flow.

The traffic flows between the core routers and through the VRF.

Verifying the Connectivity

To verify the connectivity between the on-prem data center and the public cloud from Cisco DCNM Web UI, perform the following steps:

Procedure

Step 1 Choose **Control** > **Fabrics** > **VRFs**.

The **VRFs** window appears.

Step 2 Choose the **Cloud-Connect** fabric.

VRFs in this fabric are listed.

Step 3 Choose the VRF and click **Continue**.

Step 4 Right-click the BGW.

The **VRF Extension Attachment** dialog box appears.

Step 5 Uncheck the check box and click **Save**.

The network topology window appears.

Step 6 Click **Deploy** to push the configurations.

The VRF is disabled on the BGW.

Step 7 Check the CLI.

The traffic will stop.

Step 8 Enable the VRF again on BGW.

Step 9 Check the CLI.

The traffic will flow. Alternatively, access the HTTP address of the web server in the public cloud. You will get a **Database Reachable** message.

Deploying Cisco CSR 1000v on Microsoft Azure

To deploy a Cisco CSR 1000v in Microsoft Azure, perform the following steps:

Procedure

Step 1 From the **Microsoft Azure** UI, choose **Virtual Machines**.

The **Virtual Machines** window appears.

Step 2 Click **Add**.

The **Create a virtual machine** window appears.

Step 3 Click the **Create VM from Azure Marketplace** hyperlink.

The **Marketplace** window appears, where you can search for the standard classic VMs.

Step 4 Search for the CSR deployments in the marketplace.

Step 5 Choose **Cisco Cloud Services Router (CSR) 1000V** from the search results.

Step 6 Choose **Cisco CSR 1000V Bring Your Own License – XE 16.9** or higher versions from the **Select a software plan** drop-down list.

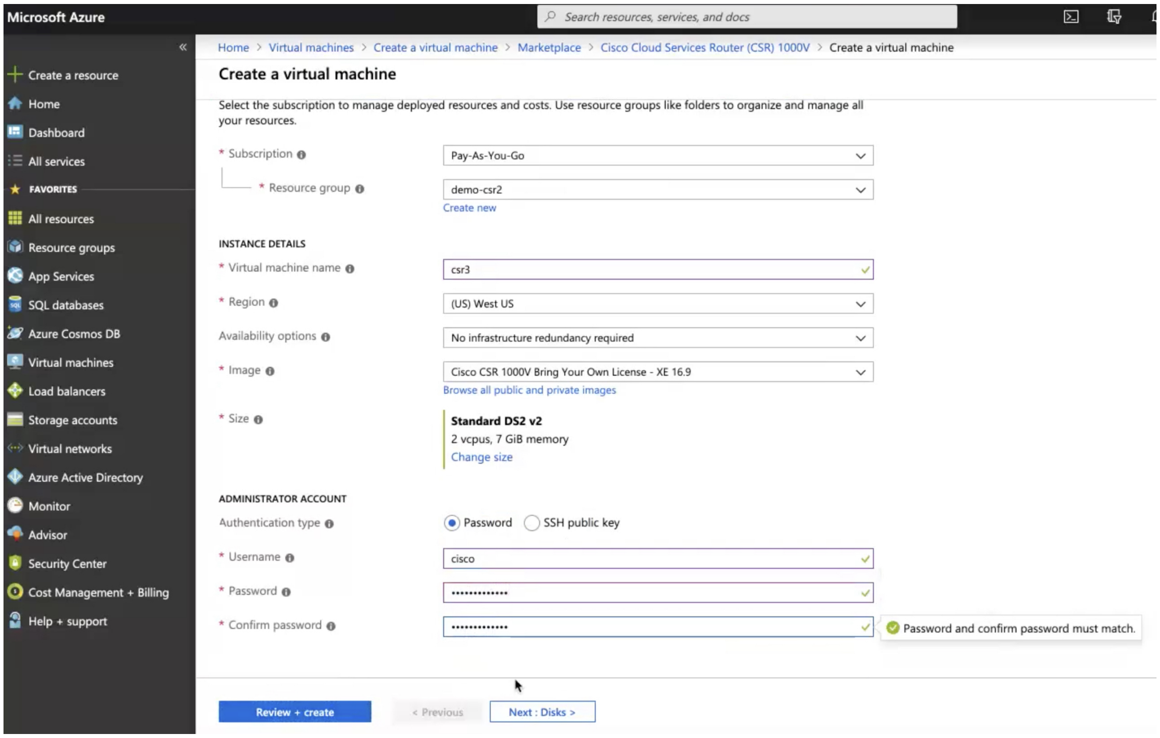
Step 7 Click **Create**.

Step 8 Enter the project details and instance details in the **Create a virtual machine** window.

Step 9 Choose the **Password** authentication type in the administrator account section.

Cisco DCNM does not support the SSH public key.

Step 10 Create a username and password.



Create a virtual machine

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

* Subscription: Pay-As-You-Go

* Resource group: demo-csr2

Create new

INSTANCE DETAILS

* Virtual machine name: csr3

* Region: (US) West US

Availability options: No infrastructure redundancy required

* Image: Cisco CSR 1000V Bring Your Own License - XE 16.9

Browse all public and private images

* Size: Standard DS2 v2
2 vcpus, 7 GiB memory
Change size

ADMINISTRATOR ACCOUNT

Authentication type: ● Password ○ SSH public key

* Username: cisco

* Password: ••••••••••••

* Confirm password: •••••••••••• ✓ Password and confirm password must match.

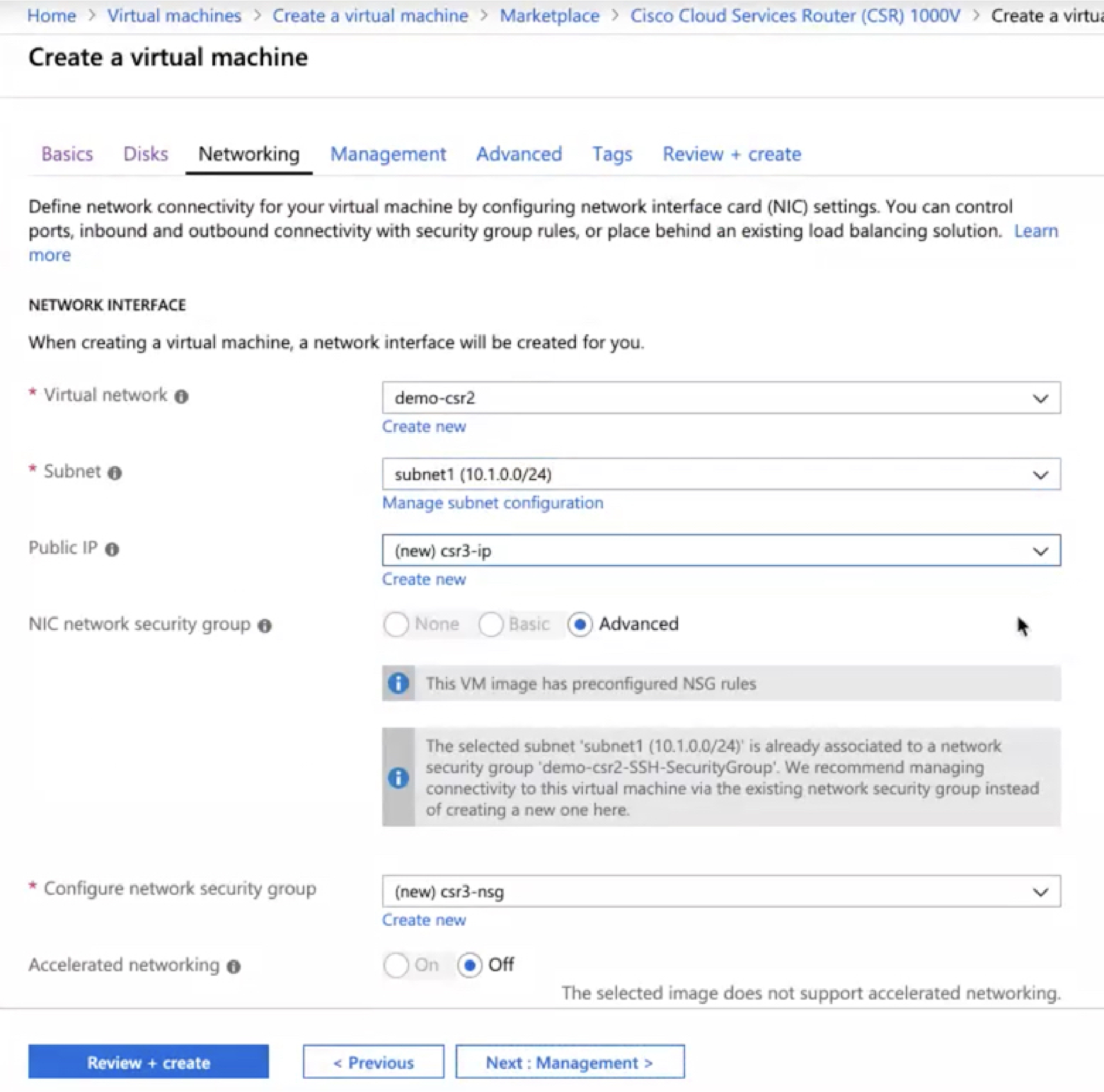
Step 11 Click **Next : Disks** >.

Step 12 Choose the **Standard HDD** option from the OS disk type drop-down list.

Step 13 Click **Next : Networking** >.

Step 14 Enter values in the required fields.

Step 15 Choose a public IP for the network.



Home > Virtual machines > Create a virtual machine > Marketplace > Cisco Cloud Services Router (CSR) 1000V > Create a virtua
Basics
Disks
Networking
Management
Advanced
Tags
Review + create
Review + create
< Previous
Next : Management >

Create a virtual machine

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: demo-csr2 (Create new)

* Subnet: subnet1 (10.1.0.0/24) (Manage subnet configuration)

Public IP: (new) csr3-ip (Create new)

NIC network security group: ○ None ○ Basic ● Advanced

This VM image has preconfigured NSG rules

The selected subnet 'subnet1 (10.1.0.0/24)' is already associated to a network security group 'demo-csr2-SSH-SecurityGroup'. We recommend managing connectivity to this virtual machine via the existing network security group instead of creating a new one here.

* Configure network security group: (new) csr3-nsg (Create new)

Accelerated networking: ○ On ● Off

The selected image does not support accelerated networking.

Step 16 Use the default values in other fields.

Step 17 Click **Review + create**.

A VM will be created for Cisco CSR 1000v in Microsoft Azure with a public IP address.

What to do next

- Attach network interfaces:

1. Choose the **Networking** setting of the VM.

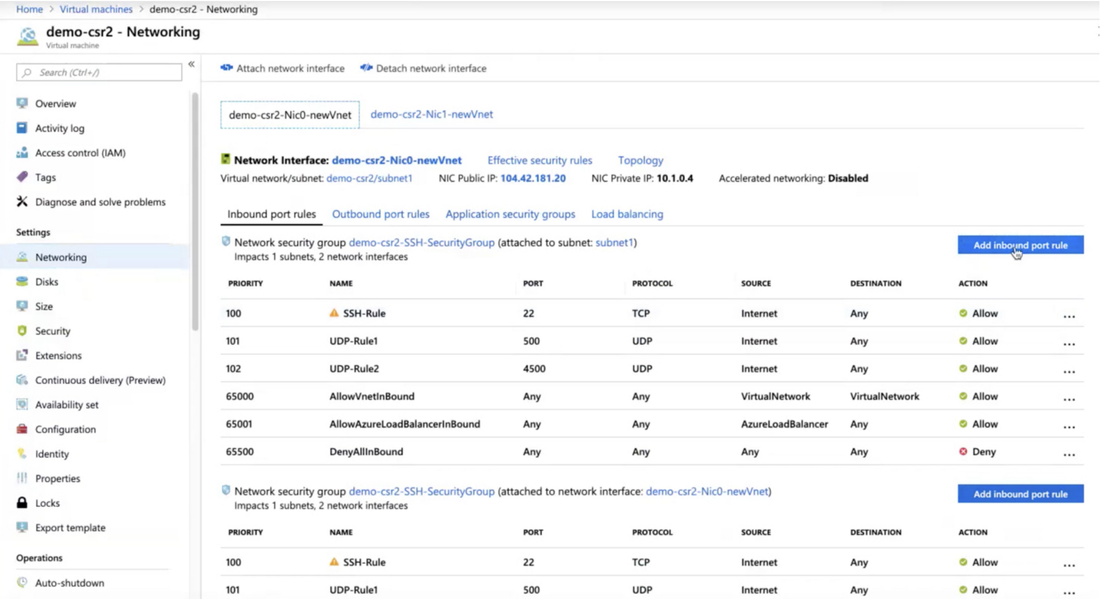
2. Choose **Attach network interface** to add a Nic.

   Attach one Nic each for both the subnets. IP addresses are automatically assigned.

3. Add an SSH rule using the port 22 to enable the SSH access of the core router.

   Cisco DCNM discovers the core router using this SSH access.

   Note Two UDP rules using the ports 500 and 4500 to enable the IPsec tunnel are added automatically.



Network Interface: demo-csr2-Nic0-newVnet

Virtual network/subnet: demo-csr2/subnet1 NIC Public IP: 104.42.181.20 NIC Private IP: 10.1.0.4 Accelerated networking: Disabled

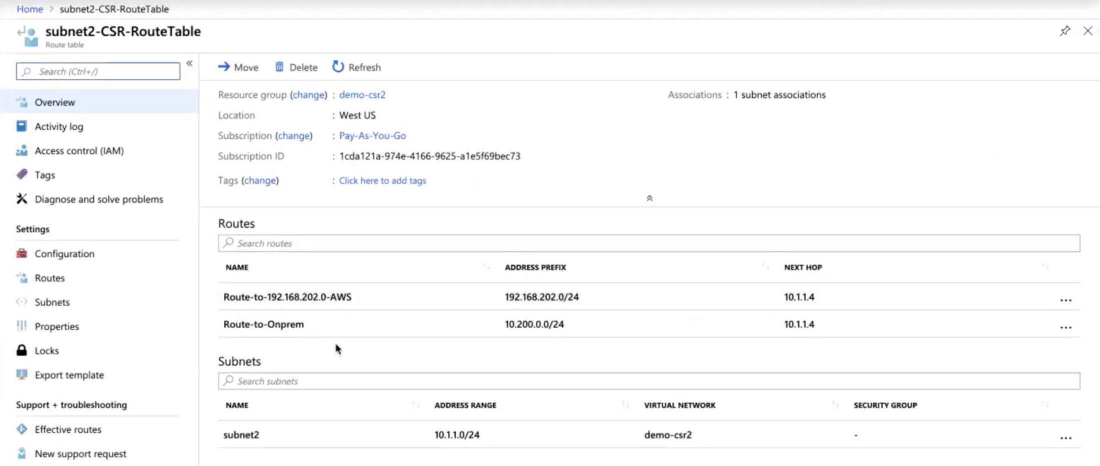
Network security group demo-csr2-SSH-SecurityGroup (attached to subnet: subnet1)
Impacts 1 subnets, 2 network interfaces

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
100	SSH-Rule	22	TCP	Internet	Any	Allow
101	UDP-Rule1	500	UDP	Internet	Any	Allow
102	UDP-Rule2	4500	UDP	Internet	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Network security group demo-csr2-SSH-SecurityGroup (attached to network interface: demo-csr2-Nic0-newVnet)
Impacts 1 subnets, 2 network interfaces

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
100	SSH-Rule	22	TCP	Internet	Any	Allow
101	UDP-Rule1	500	UDP	Internet	Any	Allow

- Create routes in the **Routes** setting of the VM to create traffic routes between the on-prem data center and Microsoft Azure. You can use the default route to redirect traffic from the VNet to Cisco CSR 1000v.



Resource group (change) : demo-csr2
Location : West US
Subscription (change) : Pay-As-You-Go
Subscription ID : 1cda121a-974e-4166-9625-a1e5f69bec73
Tags (change) : Click here to add tags
Associations : 1 subnet associations

Routes

NAME	ADDRESS PREFIX	NEXT HOP
Route-to-192.168.202.0-AWS	192.168.202.0/24	10.1.1.4
Route-to-Onprem	10.200.0.0/24	10.1.1.4

Subnets

NAME	ADDRESS RANGE	VIRTUAL NETWORK	SECURITY GROUP
subnet2	10.1.1.0/24	demo-csr2	-

See *Cisco CSR 1000v Deployment Guide for Microsoft Azure* for more information.

Viewing Links and Core Routers Details

To view the details of links and core routers from the fabric topology window, perform the following steps:

Procedure

Step 1 From the **Actions** pane, choose **Tabular view** > **Links**.

The **Links** window appears.

Step 2 Refresh the window.

The three links that you created will appear in the list.

Step 3 (Optional) Double-click the on-prem core router to view the IP route information.

The **IP Route Information** dialog box appears.

Step 4 (Optional) Click the **Crypto Session** tab to view the details about the IPsec tunnel.

Step 5 (Optional) Click the **BGP Session** tab to view the details about the BGP session.

Step 6 (Optional) Click the **Packet Counter** tab to view the packet counter details.

You can reset the counter value you see in the **Packet Counter** tab. See the Resetting Packet Counter Using API, on page 25 section more information.

Resetting Packet Counter Using API

To reset the packet counter, perform the following steps:

Procedure

Step 1 Log into Cisco DCNM.

Step 2 Navigate to the https://*DCNM-IP*/api-docs URL.

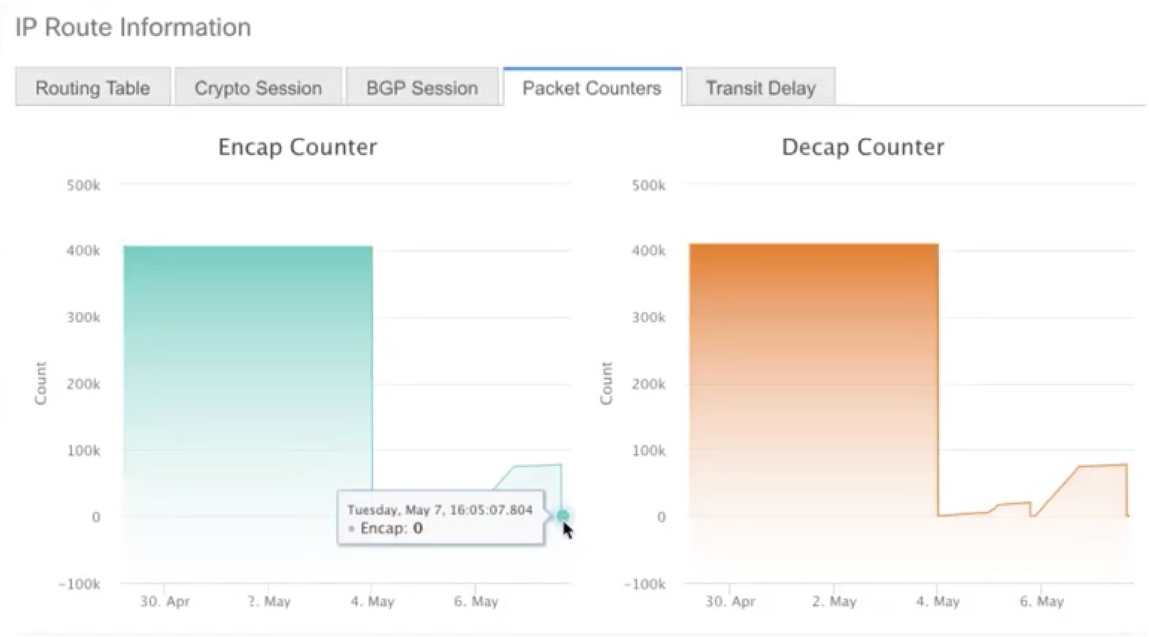
Step 3 Expand the GET **/cloud-extension/status/{ipAddress}** API under cloud extension.

Step 4 Enter the IP address of the on-prem core router.

Step 5 Set the **fetchLatestFromSwitch** value to **true**.

Step 6 Click **Try it out**.

The packet counter is cleared and the count drops to zero.


IP Route Information
Routing Table
Crypto Session
BGP Session
Packet Counters
Transit Delay
Encap Counter
500k
400k
300k
200k
100k
0
-100k
Count
30. Apr
2. May
4. May
6. May
Tuesday, May 7, 16:05:07.804
• Encap: 0
Decap Counter
500k
400k
300k
200k
100k
0
-100k
Count
30. Apr
2. May
4. May
6. May