Cisco Catalyst Center 3.1.5 on Azure Deployment Guide

First Published: 2025-10-01

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1

Get Started with Catalyst Center on Azure

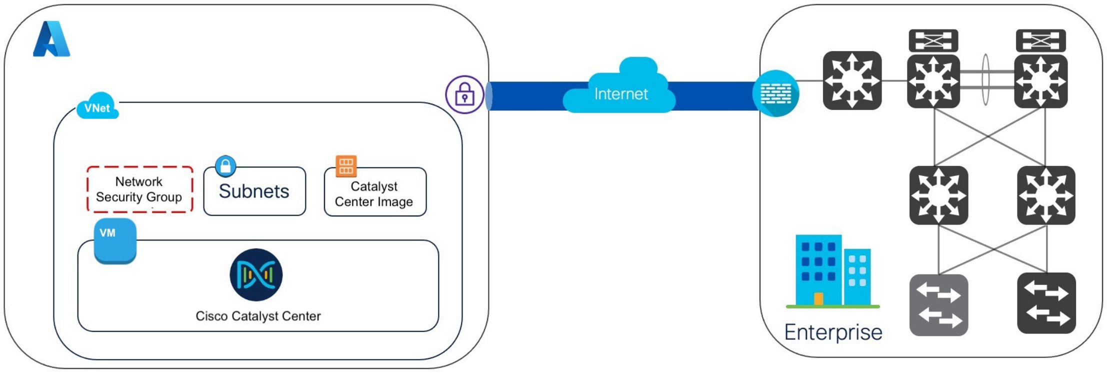
Cisco Catalyst Center on Azure overview

Catalyst Center is a powerful management dashboard and network controller that lets you securely access networks and applications. With Catalyst Center, you can simplify network management, secure interaction between endpoints, optimize network operational costs, deploy services and applications to enhance performance, use AI/ML insights to improve user experience, and use remote access for offsite resources.

Catalyst Center offers centralized, intuitive management that makes it fast and easy to design, provision, and apply policies across your network environment. The Catalyst Center user interface provides end-to-end network visibility and uses network insights to optimize network performance and deliver the best user and application experience.

Catalyst Center on Azure provides the full functionality that a Catalyst Center appliance deployment offers. Catalyst Center on Azure runs in your Azure cloud environment and manages your network from the cloud.

Catalyst Center on Azure can connect to your network using Azure ExpressRoute, Cisco SD-WAN, colocation services, or an IPsec tunnel. See this figure to visually understand how Catalyst Center on Azure can connect to your network.



Deployment overview

You can manually deploy the Catalyst Center image on your Azure infrastructure. To do this, you will manually configure Catalyst Center by creating the Azure infrastructure, establishing a VPN tunnel, and deploying your Catalyst Center.

Key deployment factors

Consider these key deployment factors:

- The Azure ARM file is required to create a Catalyst Center VA on Azure.
- You will create the Azure infrastructure, such as VNets, resource groups, and tunnels, in your Azure account. Then you will establish a VPN tunnel.
- You will deploy Catalyst Center.
- Deployment time is approximately 1 hour.
- You can only configure an on-premises NFS for backups.
- You will manually configure monitoring through the Azure portal.

High availability and Catalyst Center on Azure

Single-node VM HA within an Azure availability zone (AZ) is enabled by leveraging Azure's built-in redundancy features.

If a Catalyst Center VM instance crashes, Azure automatically brings up another instance with the same IP address in the same availability zone. This ensures minimal downtime and uninterrupted connectivity, reducing disruptions during critical network operations.

The experience and recovery time objective (RTO) are similar to the power outage scenario in a traditional bare-metal Catalyst Center appliance. Azure offers Zone Redundant VM (ZRS) and Availability Sets to further enhance resilience for the Catalyst Center deployment.

Guidelines for accessing Catalyst Center on Azure

After you create a virtual instance of Catalyst Center, you can access it through the Catalyst Center GUI and CLI.

Important The Catalyst Center GUI and CLI are accessible only through the enterprise network, not from the public network. You need to ensure that Catalyst Center is not accessible on the public internet for security reasons.

Guidelines for accessing the Catalyst Center GUI

Use these guidelines to access the Catalyst Center GUI:

- Use a compatible browser.

  For a current list of compatible browsers, see the *Cisco Catalyst Center Release Notes*.

- In a browser, enter the IP address of your Catalyst Center instance in this format:

  ```
  https://ip-address
  ```

  For example:

  ```
  https://192.0.2.27
  ```

- Use these credentials for the initial login:
  - Username: **`admin`**
  - Password: **`P@ssword9`**

- Follow the prompts to create a new Catalyst Center account, including configuring credentials.

Note The password must:

- Omit any tab or line breaks.
- Have at least nine characters.
- Include characters from at least three of these categories:
  - Lowercase letters (a to z)
  - Uppercase letters (A to Z)
  - Numbers (0 to 9)
  - Special characters (for example, ! or #)

Guidelines for accessing the Catalyst Center CLI

Use these guidelines to access the Catalyst Center CLI:

- Use the IP address and keys provided by Azure.

Note The key must be a .pem file. If the key file is downloaded as a key.cer file, you must rename the file to key.pem.

- Manually change the access permissions on the key.pem file to 400 by using the Linux `chmod` command.

  For example:

  ```
  chmod 400 key.pem
  ```

- Use this Linux command to access the Catalyst Center CLI:

  ```
  ssh -i key.pem maglev@ip-address -p 2222
  ```

For example:

```
ssh -i key.pem maglev@192.0.2.27 -p 2222
```

CHAPTER 2

Deploy Manually Using an Azure Template

Manual deployment using Azure

This chapter explains how to manually deploy Catalyst Center using Azure. You will manually create the Azure infrastructure, establish a VPN tunnel, and deploy Catalyst Center.

Prerequisites for manual deployment using Azure

Before deploying Catalyst Center on Azure, you must meet these Azure and Catalyst Center requirements.

Azure account requirement

You must download the Azure Resource Manager (ARM) template for Catalyst Center. Contact your Cisco sales representative to request this file.

Azure disk size requirement

Azure supports a maximum disk size of 3 terabytes (TB).

Important In Azure, the default disk size is 1 TB. To increase this disk size to 3 TB, open a case with Azure and request that Azure enables your Azure Entra tenant for increased disk space.

Azure network infrastructure requirements

You must meet these Azure network infrastructure requirements:

- The ARM template deploys only the Catalyst Center VA. Before you begin the Catalyst Center VA deployment, you must manually deploy these required virtual machine resources:

  - Resource group
  - Virtual network name
  - Subnet name
  - Network security groups
  - SSH public key source

- Ensure that you establish a secure tunnel between your Azure resources and enterprise router or firewall for connectivity to the devices in your enterprise network. For example, Catalyst Center on Azure can connect to your network using Azure ExpressRoute, Cisco SD-WAN, colocation services, or an IPsec tunnel.

- For your existing connection from the enterprise router or firewall to Azure, ensure that the correct ports are open for traffic to flow to and from the Catalyst Center VA. You can open them using either the firewall settings or a proxy gateway. For information about the recommended communication ports, see "Required network ports" in the "Plan the Deployment" chapter of the *Cisco Catalyst Center Installation Guide*.

Azure region configuration requirement

Your Azure environment must be configured in one of these regions:

- East Japan
- East US
- East US 2
- North Europe
- South Brazil
- South UK
- Southeast Asia
- West Europe
- West Japan
- West US

Catalyst Center environment requirements

You have this Catalyst Center information and services on hand:

- IP address, netmask, and gateway that are created from the Azure subnet.
- Enterprise DNS server.
- Fully qualified domain name (FQDN) of Catalyst Center, which is for the DNS resolution of Catalyst Center on day one.

Deploy Catalyst Center using an Azure template

Follow this procedure to manually deploy Catalyst Center on Azure using the Azure Resource Manager (ARM) template. The ARM template contains the relevant details for all required parameters.

Procedure

Step 1 Log in to the Azure portal.

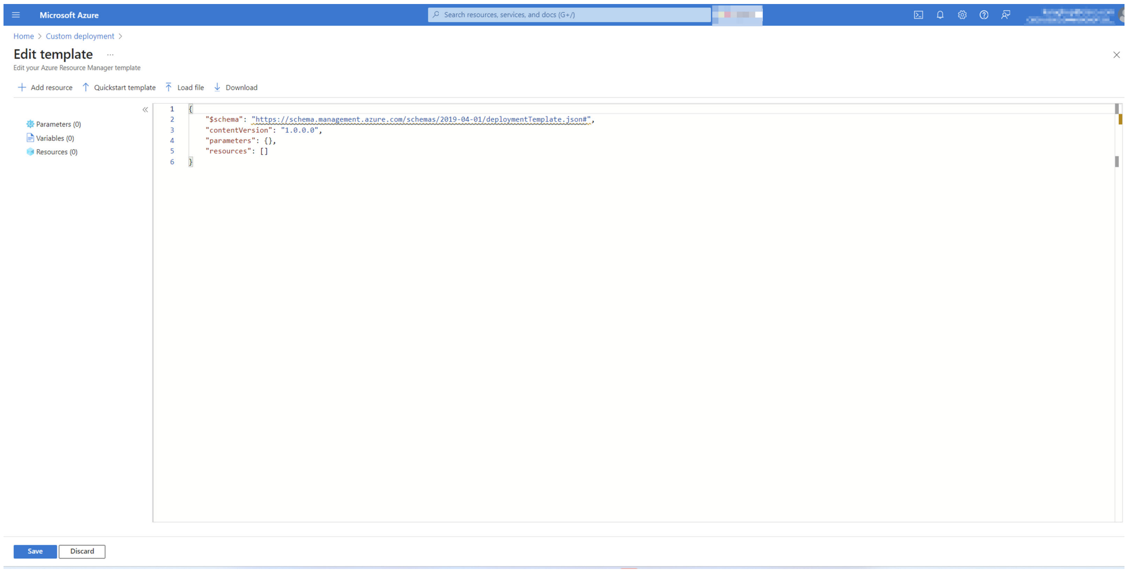
Step 2 In the **Search** field, enter `Deploy a custom template` and press **Enter**.

Step 3 In the **Custom deployment** window, click **Build your own template in the editor**.

Step 4 In the **Edit template** window, create the custom template and then click **Save**.

You can create the custom template by either

- copying and pasting the contents of the template file into the open editor, or
- clicking **Load file** and uploading the file.



```
{
    "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {},
    "resources": []
}
```

Step 5 In the **Custom deployment** window, under **Basics**, configure the template for the Catalyst Center on Azure deployment.

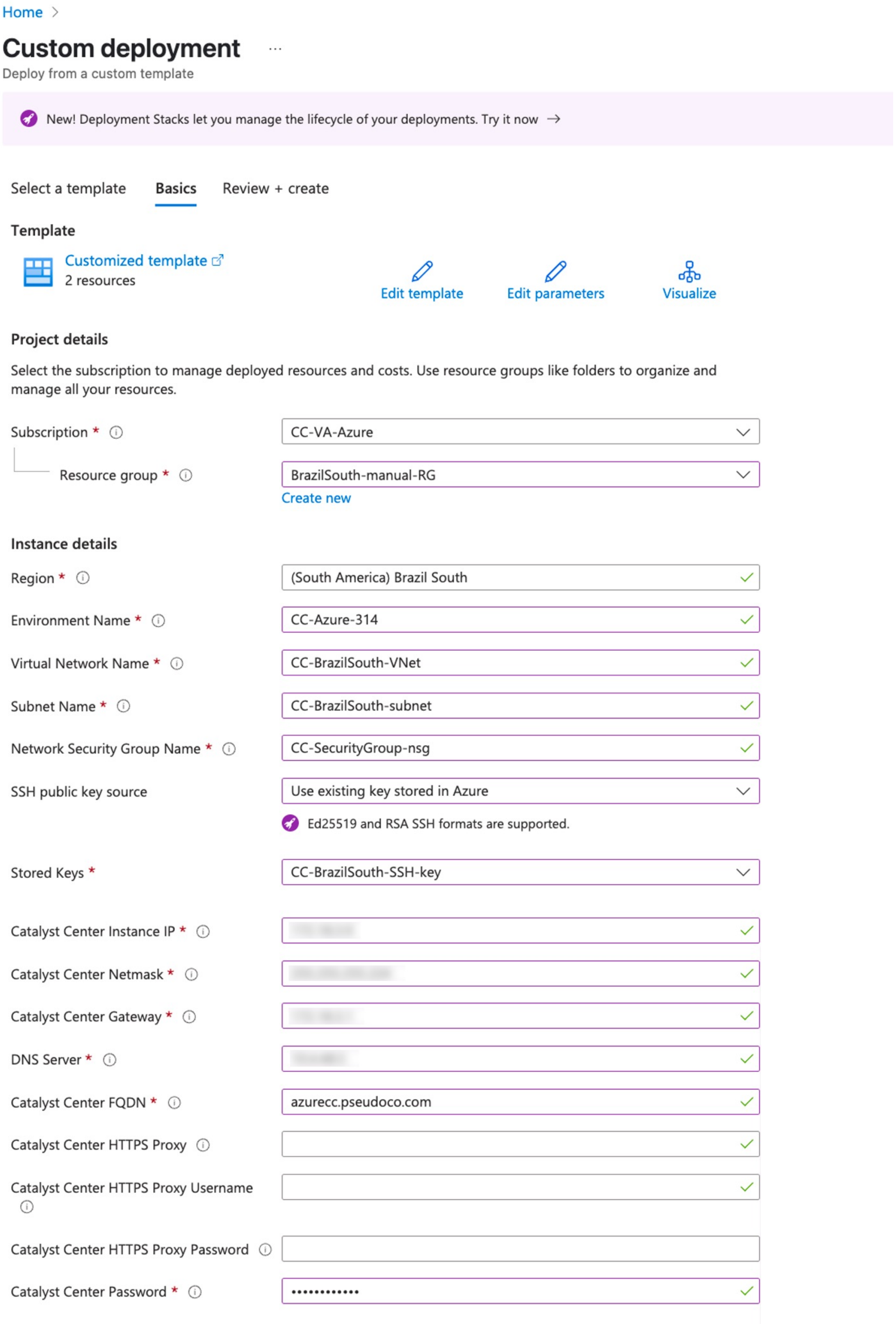
a. Under **Project details**, provide the required details.

- From the **Subscription** drop-down list, choose the subscription.
- From the **Resource group** drop-down list, choose the resource group.

b. Under **Instance details**, provide the required details using this table.

Note
Choose the appropriate network and network security group (NSG) configurations for enabling secure access to your on-premises server. This process includes verifying the subnet routing and implementing the NSG rules to establish connectivity between Azure resources and the on-premises infrastructure.

Parameter	Description
Region	From this drop-down list, choose a region for the deployment.
Environment Name	Enter an environment name for the deployment.
Virtual Network Name	Enter the name of the virtual network where you want to deploy Catalyst Center.
Subnet Name	Enter the subnet name for Catalyst Center.
Network Security Group Name	Enter the name of the network security group for Catalyst Center.
SSH public key source	From this drop-down list, choose the key that the enterprise network uses to establish an SSH connection with Catalyst Center on Azure.
Stored Keys	From this drop-down list, choose the key that the enterprise network uses to establish an SSH connection with Catalyst Center on Azure.
Catalyst Center Instance IP	Enter an unused Catalyst Center instance IP address from the subnet that's being used for Catalyst Center.
Catalyst Center Netmask	Enter the netmask for the subnet that's being used for Catalyst Center.
Catalyst Center Gateway	Enter the gateway IP address for the subnet that's being used for Catalyst Center.
DNS Server	Enter the enterprise DNS server IP address that you want configured on Catalyst Center.
Catalyst Center FQDN	Enter the FQDN that you want configured on Catalyst Center.
(Optional) **Catalyst Center HTTPS Proxy**	Enter the enterprise proxy if needed.
(Optional) **Catalyst Center HTTPS Proxy Username**	Enter the enterprise proxy username if needed.
(Optional) **Catalyst Center HTTPS Proxy Password**	Enter the enterprise proxy password if needed.
Catalyst Center Password	Enter the Catalyst Center password that the Azure console uses to connect to the Catalyst Center CLI.



Home >

Custom deployment ...

Deploy from a custom template

New! Deployment Stacks let you manage the lifecycle of your deployments. Try it now →

Template

Customized template
2 resources

Project details

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

Subscription *	CC-VA-Azure
Resource group *	BrazilSouth-manual-RG Create new

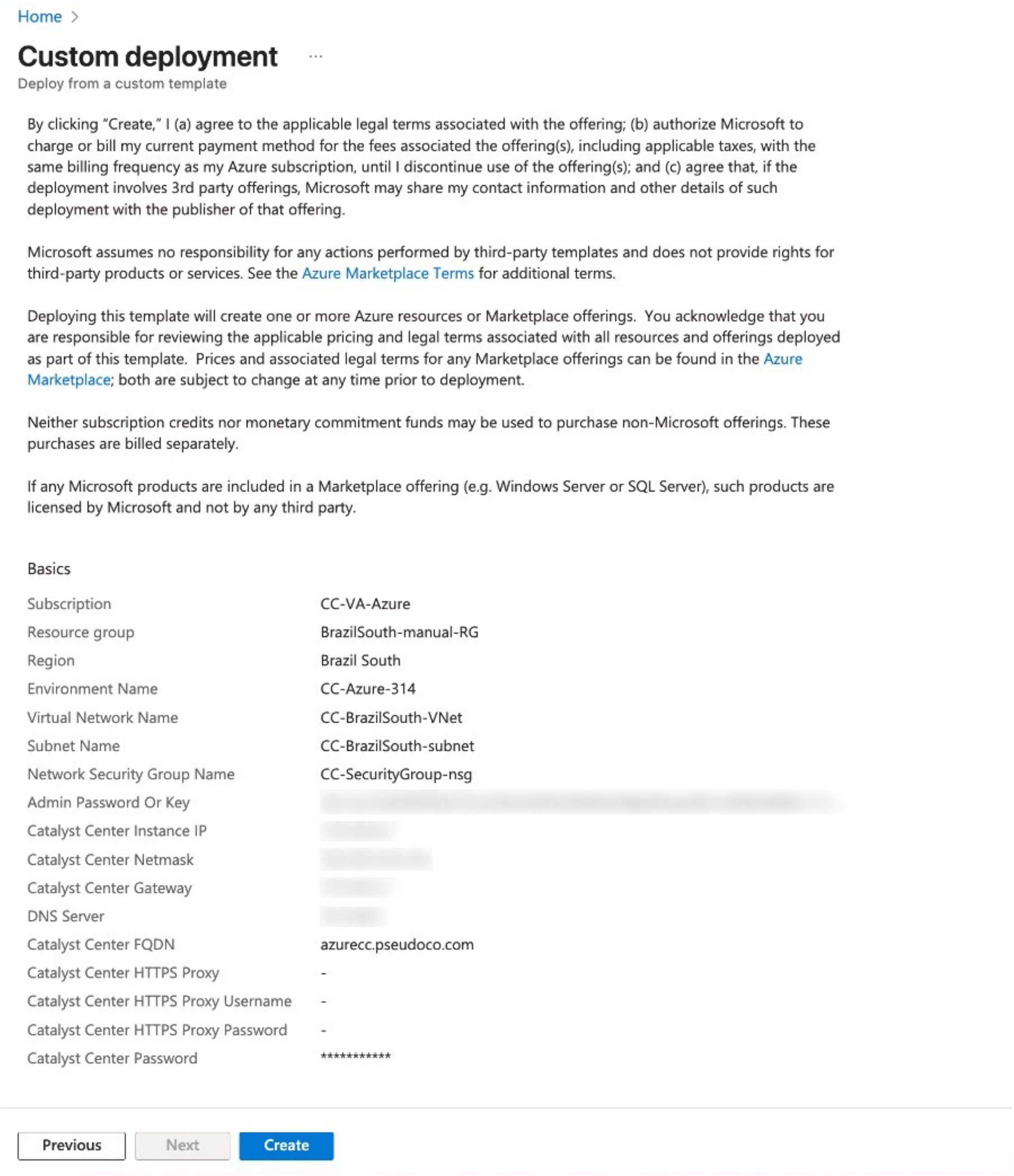
Instance details

Region *	(South America) Brazil South ✓
Environment Name *	CC-Azure-314 ✓
Virtual Network Name *	CC-BrazilSouth-VNet ✓
Subnet Name *	CC-BrazilSouth-subnet ✓
Network Security Group Name *	CC-SecurityGroup-nsg ✓
SSH public key source	Use existing key stored in Azure Ed25519 and RSA SSH formats are supported.
Stored Keys *	CC-BrazilSouth-SSH-key
Catalyst Center Instance IP *	[redacted] ✓
Catalyst Center Netmask *	[redacted] ✓
Catalyst Center Gateway *	[redacted] ✓
DNS Server *	[redacted] ✓
Catalyst Center FQDN *	azurecc.pseudoco.com ✓
Catalyst Center HTTPS Proxy	✓
Catalyst Center HTTPS Proxy Username	✓
Catalyst Center HTTPS Proxy Password	
Catalyst Center Password *	•••••••••••• ✓

c. Click **Next** or **Review + Create**.

Azure performs a basic validation check of the template and displays any warnings or errors.

Step 6 On the **Custom deployment** window, review the configuration and then click **Create** to approve the configuration and start the deployment.



Home >

Custom deployment ...

Deploy from a custom template

By clicking "Create," I (a) agree to the applicable legal terms associated with the offering; (b) authorize Microsoft to charge or bill my current payment method for the fees associated the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s); and (c) agree that, if the deployment involves 3rd party offerings, Microsoft may share my contact information and other details of such deployment with the publisher of that offering.

Microsoft assumes no responsibility for any actions performed by third-party templates and does not provide rights for third-party products or services. See the Azure Marketplace Terms for additional terms.

Deploying this template will create one or more Azure resources or Marketplace offerings. You acknowledge that you are responsible for reviewing the applicable pricing and legal terms associated with all resources and offerings deployed as part of this template. Prices and associated legal terms for any Marketplace offerings can be found in the Azure Marketplace; both are subject to change at any time prior to deployment.

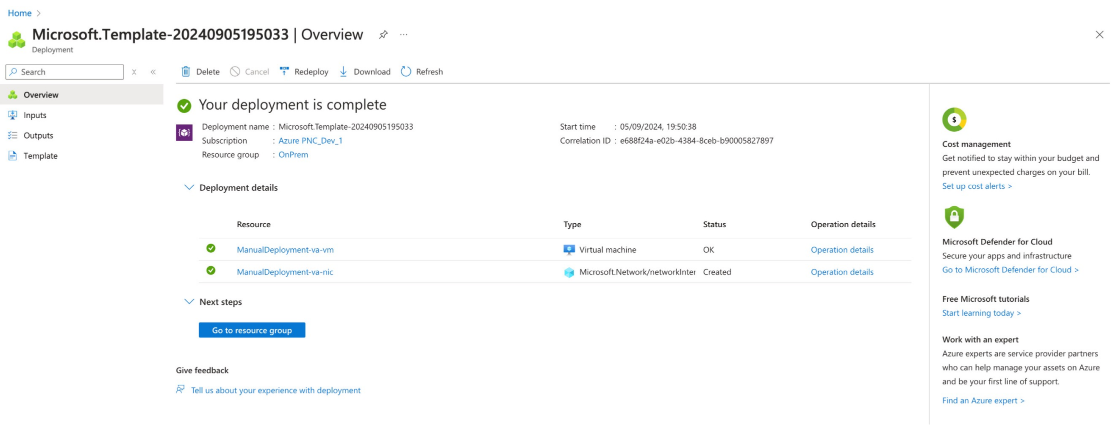
Neither subscription credits nor monetary commitment funds may be used to purchase non-Microsoft offerings. These purchases are billed separately.

If any Microsoft products are included in a Marketplace offering (e.g. Windows Server or SQL Server), such products are licensed by Microsoft and not by any third party.

Basics

Subscription	CC-VA-Azure
Resource group	BrazilSouth-manual-RG
Region	Brazil South
Environment Name	CC-Azure-314
Virtual Network Name	CC-BrazilSouth-VNet
Subnet Name	CC-BrazilSouth-subnet
Network Security Group Name	CC-SecurityGroup-nsg
Admin Password Or Key	[redacted]
Catalyst Center Instance IP	[redacted]
Catalyst Center Netmask	[redacted]
Catalyst Center Gateway	[redacted]
DNS Server	[redacted]
Catalyst Center FQDN	azurecc.pseudoco.com
Catalyst Center HTTPS Proxy	-
Catalyst Center HTTPS Proxy Username	-
Catalyst Center HTTPS Proxy Password	-
Catalyst Center Password	***********

When the deployment successfully completes, the resources display in the corresponding deployed resource group.



Microsoft.Template-20240905195033 | Overview

Deployment

Your deployment is complete

Deployment name : Microsoft.Template-20240905195033

Subscription : Azure PNC_Dev_1

Resource group : OnPrem

Start time : 05/09/2024, 19:50:38

Correlation ID : e688f24a-e02b-4384-8ceb-b90005827897

Deployment details

Resource	Type	Status	Operation details
ManualDeployment-va-vm	Virtual machine	OK	Operation details
ManualDeployment-va-nic	Microsoft.Network/networkInter	Created	Operation details

Next steps

Give feedback

Tell us about your experience with deployment

Cost management

Get notified to stay within your budget and prevent unexpected charges on your bill.

Set up cost alerts >

Microsoft Defender for Cloud

Secure your apps and infrastructure

Go to Microsoft Defender for Cloud >

Free Microsoft tutorials

Start learning today >

Work with an expert

Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support.

Find an Azure expert >

Verify the Catalyst Center deployment

Use this procedure to verify that the Catalyst Center is functioning.

Before you begin

After manually deploying Catalyst Center on Azure, wait 1 hour before logging in to the Catalyst Center UI.

Procedure

Step 1 (Optional) Verify the cloud-init parameters for the Catalyst Center deployment in Azure.

a. Log in to the Azure Portal.

b. Navigate to the **Azure Deployment Environments** service using the search bar.

c. Under **Deployment details**, click the resource with the **Virtual machine** type.

d. Click **Settings** > **Operating System** > **User data**.

e. Verify that the cloud-init parameters are correct.

Step 2 (Optional) Ping the Catalyst Center IP address from an on-premises server.

Step 3 (Optional) Establish an SSH connection with Catalyst Center using port 2222, 15 to 20 minutes after a successful deployment.

Use the SSH public key and stored key that you configured when you manually deployed Catalyst Center.

Step 4 Make sure that the Catalyst Center UI is accessible using the Catalyst Center IP address and port 443.

When you log in for the first time, use the default admin username (**`admin`**) and password (**`P@ssword9`**). After, create a new admin user with a new username and password.

Important

Changing this password is critical to network security, especially when the people who set up a Catalyst Center virtual appliance on Azure are not the same people who will serve as its administrators.

Increase the Catalyst Center instance storage on Azure

After you verify the Catalyst Center on Azure deployment, you must increase the Catalyst Center instance storage on Azure. Increasing the Catalyst Center instance storage size ensures that you have the maximum supported storage on Azure. For disk size information, see Prerequisites for manual deployment using Azure, on page 5.

Follow these steps to increase the Catalyst Center instance storage.

Before you begin

Make sure that you successfully deployed Catalyst Center on Azure.

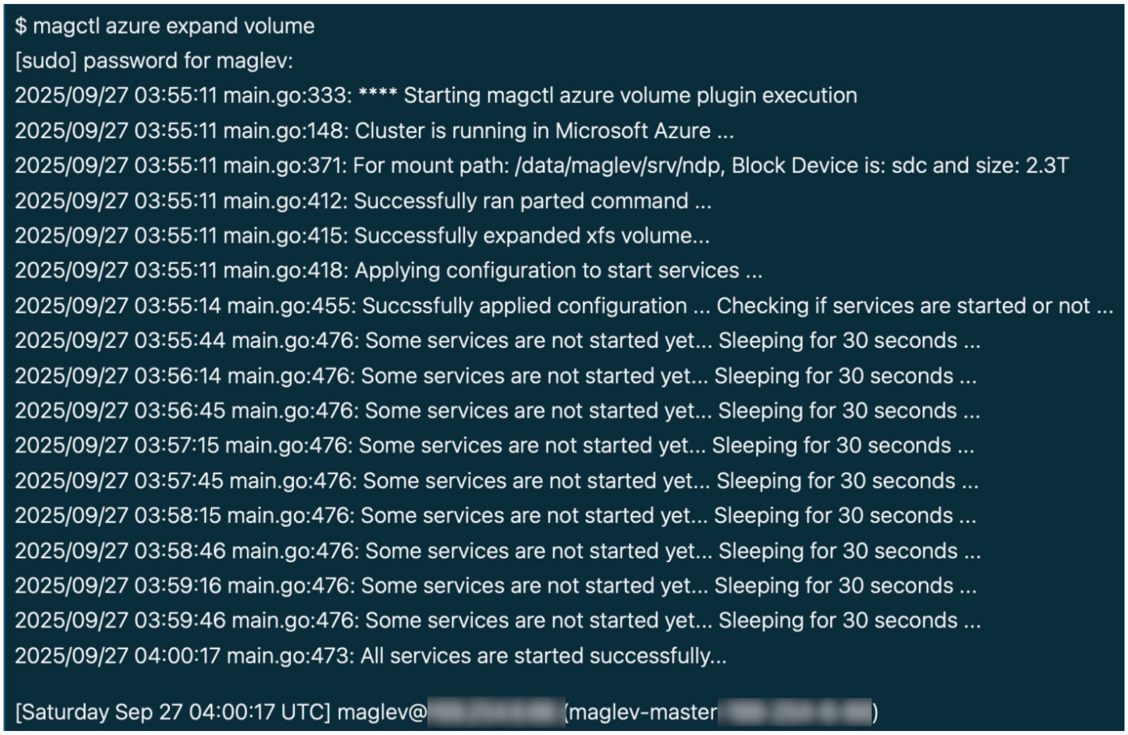
Procedure

Step 1 Use a Secure Shell (SSH) client to log in to the Catalyst Center VA on Azure.

Step 2 In the Catalyst Center VA CLI, enter this command to increase the storage size on Azure.

`magctl azure expand volume`

For example:



```
$ magctl azure expand volume
[sudo] password for maglev:
2025/09/27 03:55:11 main.go:333: **** Starting magctl azure volume plugin execution
2025/09/27 03:55:11 main.go:148: Cluster is running in Microsoft Azure ...
2025/09/27 03:55:11 main.go:371: For mount path: /data/maglev/srv/ndp, Block Device is: sdc and size: 2.3T
2025/09/27 03:55:11 main.go:412: Successfully ran parted command ...
2025/09/27 03:55:11 main.go:415: Successfully expanded xfs volume...
2025/09/27 03:55:11 main.go:418: Applying configuration to start services ...
2025/09/27 03:55:14 main.go:455: Succssfully applied configuration ... Checking if services are started or not ...
2025/09/27 03:55:44 main.go:476: Some services are not started yet... Sleeping for 30 seconds ...
2025/09/27 03:56:14 main.go:476: Some services are not started yet... Sleeping for 30 seconds ...
2025/09/27 03:56:45 main.go:476: Some services are not started yet... Sleeping for 30 seconds ...
2025/09/27 03:57:15 main.go:476: Some services are not started yet... Sleeping for 30 seconds ...
2025/09/27 03:57:45 main.go:476: Some services are not started yet... Sleeping for 30 seconds ...
2025/09/27 03:58:15 main.go:476: Some services are not started yet... Sleeping for 30 seconds ...
2025/09/27 03:58:46 main.go:476: Some services are not started yet... Sleeping for 30 seconds ...
2025/09/27 03:59:16 main.go:476: Some services are not started yet... Sleeping for 30 seconds ...
2025/09/27 03:59:46 main.go:476: Some services are not started yet... Sleeping for 30 seconds ...
2025/09/27 04:00:17 main.go:473: All services are started successfully...

[Saturday Sep 27 04:00:17 UTC] maglev@[redacted](maglev-master[redacted])
```

Note

This command takes about 7 to 8 minutes to complete.

CHAPTER 3

Backup and Restore

About backup and restore

Use the backup and restore functions in your Catalyst Center VA to create backup files. You can restore the backup files to the same appliance (in case your Catalyst Center becomes unusable) or use them to migrate your Catalyst Center to a different appliance.

For example, you can back up data from one Catalyst Center VA on Azure and restore the data to another Catalyst Center VA on Azure.

For more information about backup and restore, see the *Cisco Catalyst Center Administrator Guide*.

Important NetFlow data is not backed up when you back up Catalyst Center automation and Assurance data.

Backup and restore—VA to VA

This procedure provides a high-level overview of how you can back up the data from one (source) Catalyst Center VA on Azure and restore it to another (target) Catalyst Center VA on Azure. For detailed instructions, see the "Backup and Restore" chapter in the *Cisco Catalyst Center Administrator Guide*.

Before you begin

- Make sure that you successfully deployed two Catalyst Center VAs on Azure with Azure Resource Manager (ARM) template.
- Make sure that both Catalyst Center VAs are up and running.
- Make sure that the backup server is connected to the source Catalyst Center VA through a VPN.

- Make sure that the backup server is reachable from the target Catalyst Center VA.
- If you're using a Cloud backup (NFS) server, you'll need to know the backup password to log into the server.

  Your backup server password is dynamically created. The password is composed of the first four characters of the VA pod name and the backup server IP address without the periods. For example, if the VA pod name is DNAC-SJC and the backup server IP address is 10.0.0.1, the backup server password is DNAC10001.

Note

- You can find the VA pod name on the **Dashboard** pane after you choose the region that it's deployed in.
- You can find the backup server IP address in the **View Catalyst Center** pane.

Procedure

Step 1 Back up the data from the source Catalyst Center VA to a backup server.

Step 2 Bring up the target Catalyst Center VA that you want to restore the data to.

Step 3 Connect the target Catalyst Center VA to the backup server. (See Step 1.)

Step 4 Configure the backup server on the target Catalyst Center VA.

Step 5 Restore the data to the target Catalyst Center VA.

Configure backup

To configure backup for Catalyst Center:

Procedure

Step 1 Perform these actions to log in to Catalyst Center:

a) Enter **https://*server-ip*** in your browser, where *server-ip* is the IP address of the server on which Catalyst Center is installed.

b) Enter your Catalyst Center username and password.

Step 2 From the left pane in the **DNA Center** page, choose **System** > **Backup & Restore**.

Step 3 Click **Configure Settings**.

Step 4 If you are adding or updating configuration for an NFS, click **Add NFS**.

Otherwise, skip to Step 8.

Step 5 In the **Add NFS** area:

a) In the **NFS Server** field, enter the IP address of the backup server.
b) In the **Destination Folder** field, enter **/var/nfsShare**.
c) From the **NFS Version** drop-down list, choose **NFS 4**.
d) In the **Port** field, enter **2049**.
e) In the **Port Mapper** field, accept the default value of **111**.
f) Click **Save**.

Step 6 In the Warning dialog box, click **Proceed**.

Step 7 Perform these actions to verify that the information for the NFS that you configured is correct:

a) Click **View NFS List** .
b) Review the information in the **NFS List** .
c) Close the **NFS List** .

Step 8 Perform these actions to mount the NFS path for the NFS that you created:

a) From the **Mount Path** drop-down list, choose the mount path for the NFS that you configured.
b) In the **Encryption Passphrase** and **Confirm Passphrase** fields, enter a passphrase,

   This passphrase is used when you restore a backup.

c) Click **Submit**.

Step 9 Perform these actions to schedule your backups:

a) From the left pane in the **DNA Center** page, choose **Settings** > **Backup & Restore**
b) Click **Scheduled Backup**.
c) In the **Scheduled Backup** pane, configure the options for your backup as desired.
d) Click **Save**.

Restore a backup

To restore backup for Catalyst Center:

Procedure

Step 1 Perform these actions to log in to Catalyst Center:

a) Enter **https://*server-ip*** in your browser, where *server-ip* is the IP address of the server on which Catalyst Center is installed.
b) Enter your Catalyst Center username and password.

Step 2 From the left pane in the **DNA Center** page, choose **System** > **Backup & Restore**.

Step 3 In the **Actions** column that corresponds to the backup that you want to restore, click **…** and choose **Restore**.

Access the Catalyst Center backup VM

Use the following required information to access your backup VM.

- **SSH IP address:** <BACKUP VM IP>
- **SSH port:** 22
- **Server path:** `/var/catalyst-backup/`
- **Username:** `maglev`
- **Password:** Your backup server password is dynamically created. The password is composed of the first four characters of the VA pod name and the backup server's IP address without the periods.

  For example, if the VA pod name is *DNAC-SJC* and the backup server's IP address is *10.0.0.1*, the backup server password is *DNAC10001*.

Note

- You can find the VA pod name on the **Dashboard** pane after you choose the region that it's deployed in.
- You can find the backup server's IP address on the **View Catalyst Center Details** pane. For more information, see View Catalyst Center VA details.

CHAPTER 4

Postdeployment Changes

(Optional) Update the DNS server on your Catalyst Center VA using the Azure portal

Follow these steps to update the DNS server IP address configured on your Catalyst Center VA.

Before you begin

Get a consent token from Cisco TAC for full shell access.

Procedure

Step 1 Log in to the Azure portal.

Step 2 Navigate to the **Resource groups** service using the search bar.

Step 3 Click the virtual machine.

Step 4 Navigate to **Help** > **Serial Console** and click **Connect**.

Step 5 In the Maglev console, update the DNS server IP address to your preferred IP address.

a. At the **Login** prompt, enter **`maglev`** as the username.

b. At the **Password** prompt, enter the password that was configured during the initial deployment, regardless of the deployment method.

c. Gain full shell access by using the consent token that you received from Cisco TAC:

```
$ _shell -v consent-token
```

For example:

```
_shell -v n1+hPAAAAQ000AQAAAABAgAEAAAAAAMBYkk2bmhXcW14OGtqUXoya
09UTXlzM252UnNlUnFwTEFEQVQvejJjQm9kNXloN2thSFk3MzZBek9CMEJRUUZad2QNCkhPNVZMNjhMUXMyb0h
1OXQ2eW1TR01yT1hwZkRPSmNuc1c2QUJ5ZGtVZ0N2OU1mMXZtTC90em1MNldWcVdjY2gNCkh3eEd5MytZWmRVUTN
kek1xOWNiWi9rLzVlTkozQ2RrYy9SMXEya2NOV09uMEdvZE11c1lZN01ENjZvVk5zZlMNCktseHZxTi9tVXF0cW1
vaG9NZFY4SnVOY3NBcXkxQkZOMzZHdS9XQ2N4S2tpdlNUV1VOTVVrRXU1TjVRUDl6d1YNCmYyWW1ZdUFnSGNOcnV
veUhoTzZYYjRIWnJWNDdxSG5qR0REUjV3TE90bnNXalpBL2tsRzNzN0lIa1ZaY0VzMVENCkVoc3FZUGU5Z2ZoTWF
6YXVKRmtxVmc9PQ==
```

d. Set the terminal to display in color:

```
export TERM=xterm
```

e. Run the **sudo maglev-config update** command.

The Configuration wizard presents a shortened series of screens like those described in "Configure a Secondary Node Using the Maglev Wizard" in the *Cisco Catalyst Center Appliance Installation Guide*.

When the DNS server IP address setting is displayed, update it to the preferred IP address. After making changes on each screen, choose **next>>** to continue through the Configuration wizard. At the end of the configuration process, a message states that the Configuration wizard is ready to apply your changes.

f. Review and verify your changes using the available options:

- **proceed>>**: Save and apply the changes.
- <<**back**: Review and verify your changes.
- **<cancel>**: Discard your changes and exit the Configuration wizard.

g. Click **proceed>>** to save and apply the changes.

At the end of the configuration process, a **CONFIGURATION SUCCEEDED!** message is displayed.