Cisco Catalyst Center 3.1.x on Azure Deployment Guide

Cisco Catalyst Center
Updated July 30, 2026

Topics included

1 Get Started with Catalyst Center on Azure....4
Cisco Catalyst Center on Azure overview....5
Deployment overview....5
High availability and Catalyst Center on Azure....6
Guidelines for accessing Catalyst Center on Azure....6

2 Deploy Manually Using an ARM Template....8
Manual deployment using an ARM template....9
Prerequisites for manual deployment using an ARM template....9
Configure a custom NTP server....10
Deploy your Catalyst Center VA using an ARM template....11
Verify the Catalyst Center deployment....17

3 Deploy Manually Using Azure Marketplace....20
Manual deployment using Azure Marketplace....21
Prerequisites for manual deployment using Azure Marketplace....21
Deploy your Catalyst Center VA using Azure Marketplace....22
Verify the Catalyst Center deployment....30

4 Backup and Restore....32
About backup and restore....33
Backup and restore–hardware appliance to VA....33
Backup and restore–VA to VA....34
Configure a backup....35
Restore a backup....36

5 Postdeployment Changes....38
(Optional) Update the DNS server on your Catalyst Center VA using the Azure portal....39

1 Get Started with Catalyst Center on Azure

Topics:

- Cisco Catalyst Center on Azure overview
- Deployment overview
- High availability and Catalyst Center on Azure
- Guidelines for accessing Catalyst Center on Azure

Cisco Catalyst Center on Azure overview

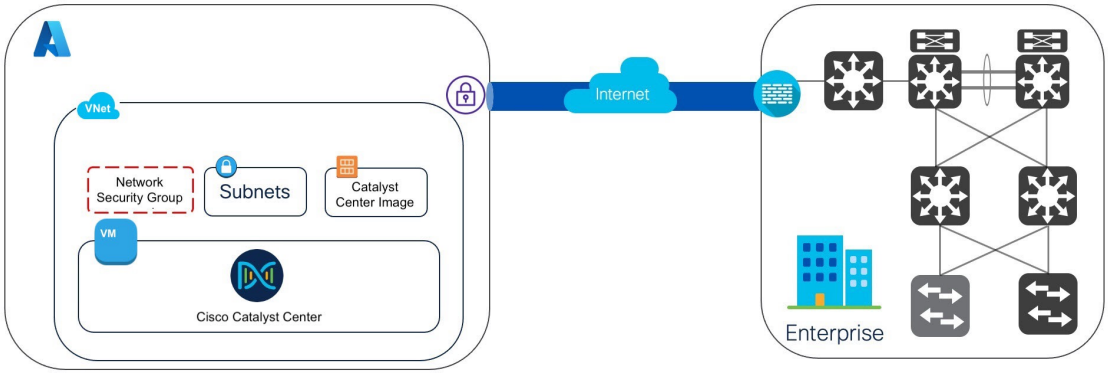
Defines Catalyst Center on Azure as a virtual appliance (VA) that runs in your Azure cloud environment, providing the full functionality of a hardware appliance while managing your network remotely from the cloud.

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 Microsoft 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

Outlines the supported deployment methods for Catalyst Center on Azure and summarizes the benefits and drawbacks of each method.

There are two ways to deploy Catalyst Center on Microsoft Azure:

- Manual deployment using an Azure Resource Manager (ARM) template
- Manual deployment using Azure Marketplace

Manual deployment using an ARM template

You manually deploy the Catalyst Center image on Azure using a custom ARM template. Then you manually configure Catalyst Center by creating the Azure infrastructure, establishing a VPN tunnel, and deploying your Catalyst Center VA.

Manual deployment using Azure Marketplace

You manually deploy the Catalyst Center image on Azure using Azure Marketplace, an online software store. Then you manually configure Catalyst Center by creating the Azure infrastructure, establishing a VPN tunnel, and deploying your Catalyst Center VA.

Choosing a deployment method

Consider the benefits and drawbacks of each method using this table.

Manual deployment using an ARM template	Manual deployment using Azure Marketplace
The custom ARM file is required to create a Catalyst Center VA on Azure.	The custom ARM file is *not* 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 configure either ▪ **an on-premises NFS for backups or** ▪ **a cloud backup server if you create and manage it.**	
You will manually configure monitoring through the Azure portal.	

High availability and Catalyst Center on Azure

Explains how single-node VM HA uses the built-in redundancy features in Azure to automatically recover instances and ensure minimal downtime during critical operations.

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

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

Provides guidelines for accessing the Catalyst Center GUI and CLI, including security and connection requirements for both interfaces.

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

  This password must meet the Catalyst Center password requirements. If it does not meet these requirements, the deployment will fail with a password constraint error. For more information, see "Password requirements" in the "Plan the Deployment" chapter of the *Cisco Catalyst Center Installation Guide*.

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
  ```

2 Deploy Manually Using an ARM Template

Topics:

- Manual deployment using an ARM template
- Prerequisites for manual deployment using an ARM template
- Configure a custom NTP server
- Deploy your Catalyst Center VA using an ARM template
- Verify the Catalyst Center deployment

Manual deployment using an ARM template

Describes how to manually deploy Catalyst Center on Azure using an ARM template.

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

Prerequisites for manual deployment using an ARM template

Lists the requirements for your Azure account, disk size, network infrastructure, and region configuration, as well as the Catalyst Center environment, before starting the deployment.

Before you deploy Catalyst Center on Azure using an ARM template, you must meet these Azure and Catalyst Center requirements.

Azure account requirement

You must download this ARM template for Catalyst Center from the Cisco Software Download site:

CatC-3.1.6-75524.200-VA-ARM-template.tar.gz

Azure disk size requirement

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

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. Make sure that the network security groups are configured to match the list of required ports. For information about the recommended communication ports, see "Communication ports" in the "Plan the Deployment" chapter of the *Cisco Catalyst Center Installation Guide*.
- The ARM template provided by your Cisco sales representative will configure the Azure cloud Network Time Protocol (NTP) server as 168.61.215.74 for time synchronization with the Catalyst Center VA. NTP connectivity is required for a successful configuration of the Catalyst Center VA. Ensure that the NTP connection is allowed in the network security group and any perimeter firewall.

Azure region configuration requirement

You must deploy Catalyst Center in an Azure region that supports the E32s_v4 VM size.

Azure subscription requirement

You must use a supported Azure subscription type. Catalyst Center on Azure is not supported on Cloud Solution Provider (CSP) plans. You must use a non-CSP plan, such as Pay-As-You-Go, Microsoft Customer Agreement (MCA), and Enterprise Agreement (EA).

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.

Configure a custom NTP server

Shows how to configure a custom NTP server in the Catalyst Center ARM template using a text editor.

Use this procedure to configure a custom Network Time Protocol (NTP) server for your Catalyst Center on Azure deployment.

When Catalyst Center on Azure is deployed using the ARM template, the default NTP server for time synchronization is the Azure cloud NTP server at IP address 168.61.215.74.

Before you begin

The NTP server configuration plays a critical role during the initial configuration and ongoing functionality of the system. So, the custom NTP server must be reachable and meet these requirements:

- The NTP server must be low stratum, no more than four.
- Jitter and offset must not exceed these maximum values:
  - Maximum offset: 500 ms
  - Maximum jitter: 299 ms

You also must contact your Cisco sales representative to request the required files for this release.

Procedure

1. Open the downloaded file for the Catalyst Center ARM template in a text editor.
2. Search for lines 123 and 124.

   Note

   Do not modify lines 123 and 124. Each line is long.

3. Search for the NTP server property in each line. Enter the custom IP address instead of the default IP address 168.61.215.74.

You must keep the existing format, including the double quotes.

For example, in this figure, you would need to replace the existing NTP IP address with the required value. Do not make any other modifications.



4. Save the updated file locally.

The Catalyst Center ARM template is updated with the custom NTP server configuration.

What to do next

Deploy Catalyst Center on Azure using the ARM template. For instructions, see Deploy your Catalyst Center VA using an ARM template on page 11.

Deploy your Catalyst Center VA using an ARM template

Provides step-by-step instructions for deploying a Catalyst Center VA on Azure using a custom ARM template and the Azure portal.

Use this procedure to manually deploy Catalyst Center on Azure using a custom ARM template. The ARM template contains the relevant details for all required parameters.

Before you begin

If you want to use a custom NTP server instead of the default Azure cloud NTP server, configure a custom NTP server in the ARM template before following this procedure. For instructions, see Configure a custom NTP server on page 10.

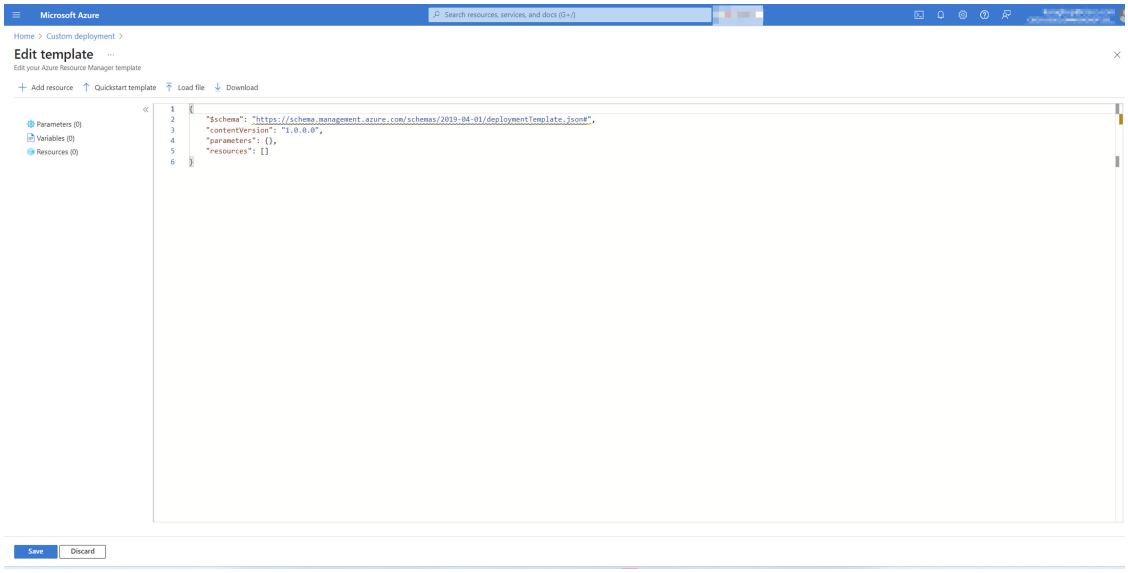
Procedure

1. Log in to the Azure portal.
2. In the **Search** field, enter `Deploy a custom template` and press **Enter**.
3. In the **Custom deployment** window, click **Build your own template in the editor**.
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.

> **Note**
>
> If you configured a custom NTP server in the custom ARM template, make sure that you provide this updated version of the template.



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.

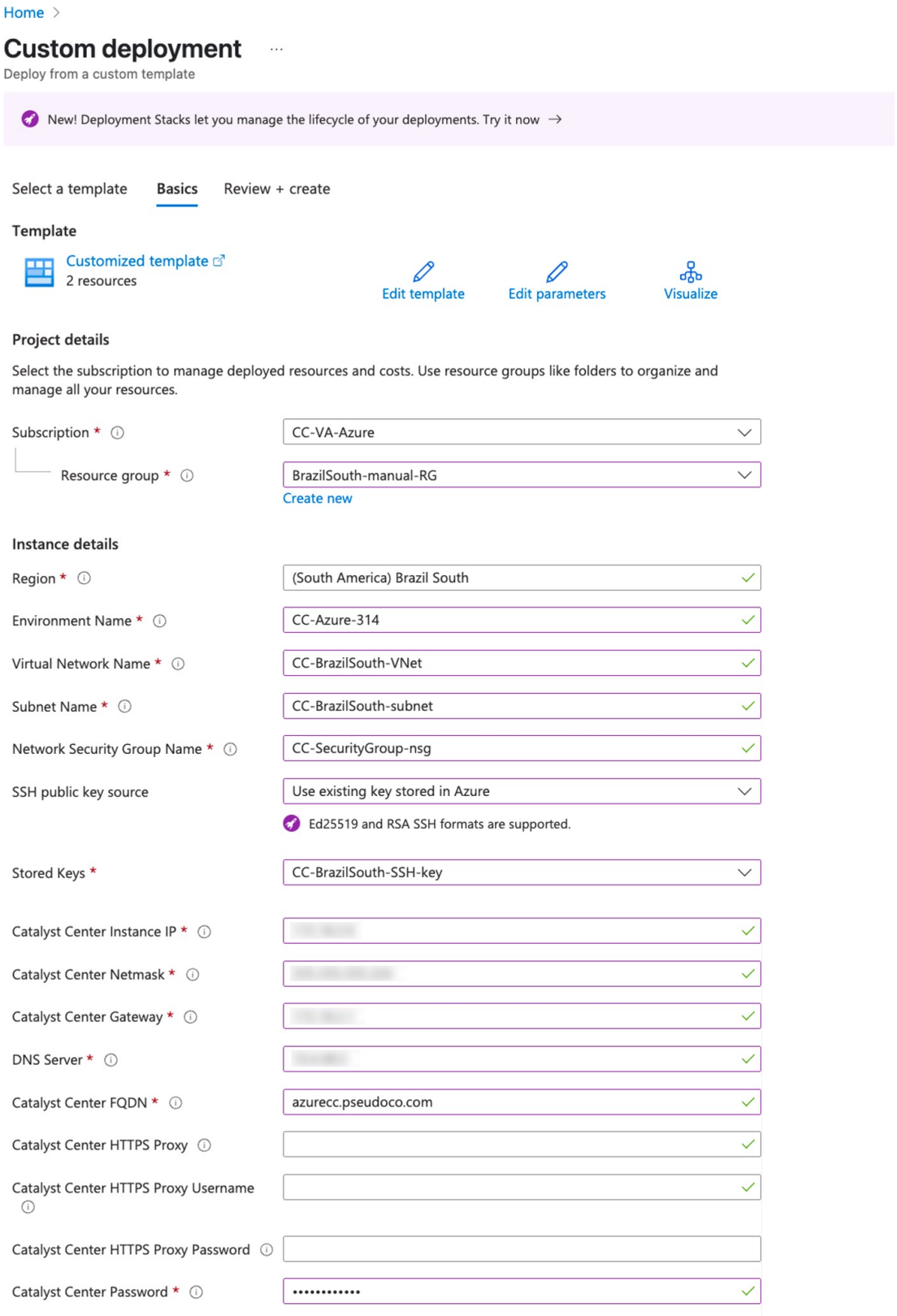
> **Note**
>
> Choose the appropriate network and network security group (NSG) configurations for enabling secure access to your on-premises server. This process includes verifying the subnet routing and implementing the NSG rules to establish connectivity between Azure resources and the on-premises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

Parameter	Description
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.

Parameter	Description

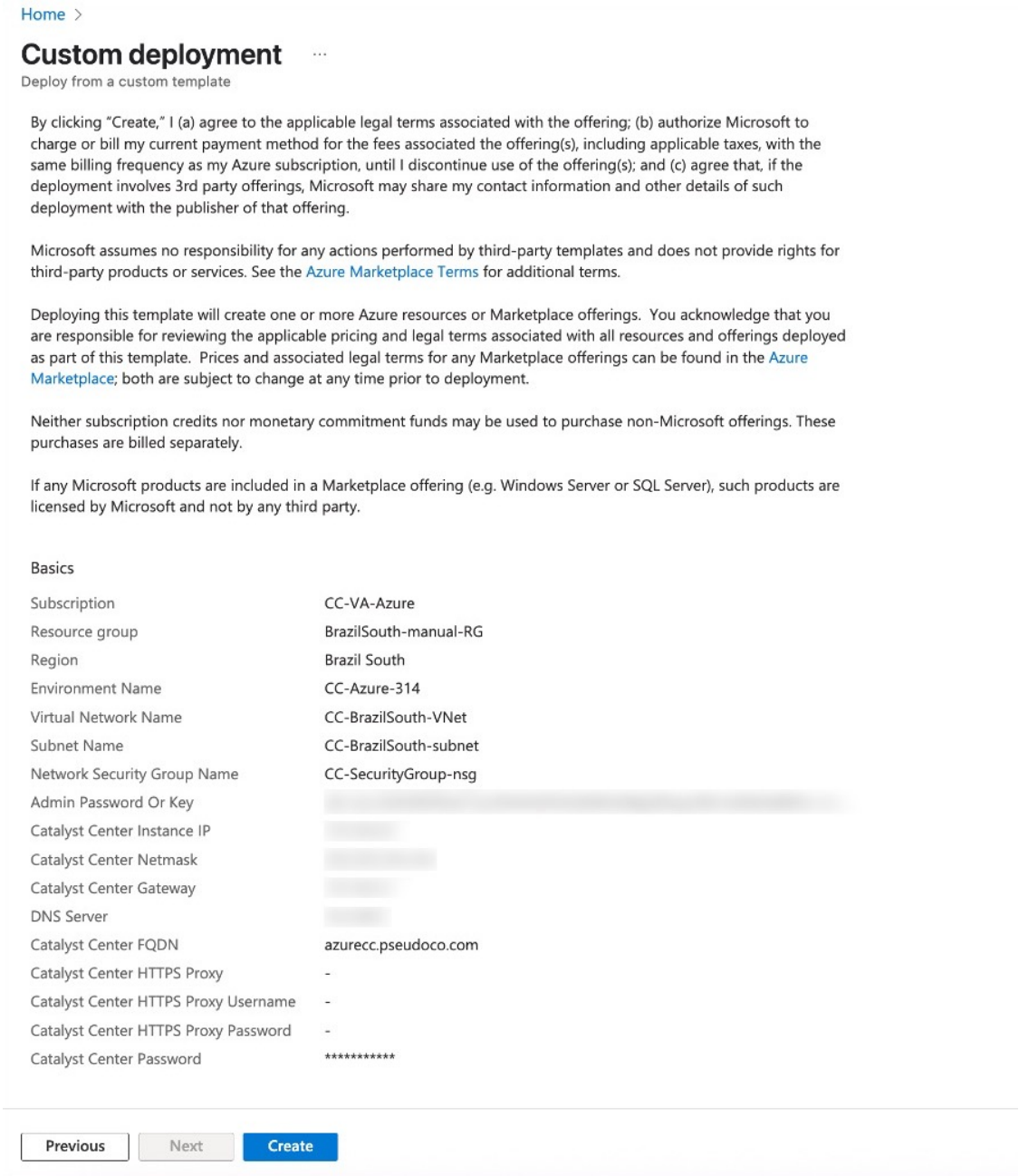
Catalyst Center Password	Enter the Catalyst Center password that the Azure console uses to connect to the Catalyst Center CLI.
	
	Note
	
	The password must
	• be 9 to 64 characters long, and
	• contain at least three of these categories:
	  • Uppercase letters (A through Z)
	  • Lowercase letters (a through z)
	  • Numbers (0 to 9)
	  • Special characters (for example, !, $, and #)
	
	The password must not include
	• the username or any two consecutive characters of the username
	• context-specific words, such as the service name, username, derivatives, Cisco, and maglev
	• four consecutive characters, except for special characters, and
	• any tabs or line breaks.



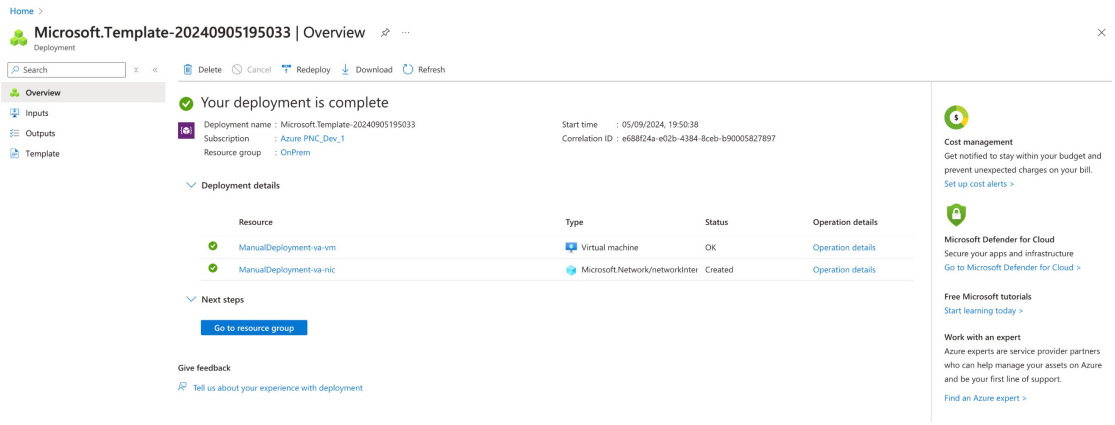
c. Click **Next** or **Review + Create**.

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

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



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



Verify the Catalyst Center deployment

Outlines the steps to verify that the Catalyst Center VA is functioning correctly by checking the IP address configurations and testing access to the management interfaces.

Use this procedure to verify that Catalyst Center is functioning.

Before you begin

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

Procedure

1. Verify that the IP address for the Catalyst Center VA matches the corresponding configuration on the Azure network interface.
   a. Log in to the Azure portal.
   b. Navigate to the virtual machine page using the search bar.
   c. Select your virtual machine.
   d. Under **Network**, click **Network Settings**.
   e. Go to the network interface.
   f. Verify that the IP address for the Catalyst Center VA matches the corresponding configuration on the Azure network interface.
2. Optional: Ping the Catalyst Center IP address from an on-premises server.
3. Optional: After a successful deployment, wait 45 to 50 minutes and then establish an SSH connection with Catalyst Center using port 2222.

   Use the SSH public key and stored key that you configured when you manually deployed Catalyst Center.
4. Verify 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 if the people who set up the Catalyst Center VA on Azure are different from those who will serve as its administrators.

3 Deploy Manually Using Azure Marketplace

Topics:

- Manual deployment using Azure Marketplace
- Prerequisites for manual deployment using Azure Marketplace
- Deploy your Catalyst Center VA using Azure Marketplace
- Verify the Catalyst Center deployment

Manual deployment using Azure Marketplace

Describes how to manually deploy Catalyst Center on Azure using Azure Marketplace.

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

Prerequisites for manual deployment using Azure Marketplace

Lists the requirements for your Azure disk size, network infrastructure, and region configuration, as well as the Catalyst Center environment, before starting the deployment.

Before you deploy Catalyst Center on Azure using Azure Marketplace, you must meet these Azure and Catalyst Center requirements.

Azure disk size requirement

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

Azure network infrastructure requirements

You must meet these Azure network infrastructure requirements:

- 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. Make sure that the network security groups are configured to match the list of required ports. For information about the recommended communication ports, see "Communication ports" in the "Plan the Deployment" chapter of the *Cisco Catalyst Center Installation Guide*.

Azure region configuration requirement

You must deploy Catalyst Center in an Azure region that supports the E32s_v4 VM size.

Azure subscription requirement

You must use a supported Azure subscription type. Catalyst Center on Azure is not supported on Cloud Solution Provider (CSP) plans. You must use a non-CSP plan, such as Pay-As-You-Go, Microsoft Customer Agreement (MCA), and Enterprise Agreement (EA).

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 your Catalyst Center VA using Azure Marketplace

Provides step-by-step instructions for deploying a Catalyst Center VA on Azure using the Azure portal, Azure Marketplace, and a cloud-init script file.

Use this procedure to manually deploy Catalyst Center on Azure using Azure Marketplace.

Before you begin

Ensure that you meet the prerequisites for this deployment method. For more information, see Prerequisites for manual deployment using Azure Marketplace on page 21.

Procedure

1. Log in to the Azure portal.
2. Create a new resource.
   a. In the left navigation pane, click **Create a resource**.
   b. In the **Search the Marketplace** field, type `Cisco Catalyst Center` and press `Enter`.
   c. From the search results, click **Cisco Catalyst Center**.
   d. Click **Create** to start the deployment wizard.
3. In the Azure deployment wizard, under **Basics**, configure your Catalyst Center VA for deployment.
   a. Under **Project details**, provide the required details:
      - From the **Subscription** drop-down list, choose a subscription.
      - From the **Resource group** drop-down list, choose an existing resource group or create a new one.
   b. Under **Instance details**, provide the required details.

      This table lists the required fields, their descriptions, and input examples.

Field	Description	Example
Virtual machine name	Enter a unique name for the Catalyst Center VA.	catalyst-center-va-eastus
Region	From this drop-down list, choose a region for the deployment.	(US) East US

Field	Description	Example
Deploy to an Azure Extended Zone	Make sure that this check box is unchecked. Check this check box only if you need to deploy Catalyst Center to an Azure extended zone.	–
Availability options	Choose a VM availability option.	Availability zone
Zone options	Indicate how you want the zone to be assigned.	Self-selected zone
Availability zone	Choose one availability zone or multiple availability zones. **Note** One availability zone supports one VM. If you choose multiple availability zones, choose a VM for each zone.	Zone 1
Security type	Choose a VM security type.	Standard
Image	Choose the Catalyst Center image in Azure Marketplace.	Cisco Catalyst Center Virtual Appliance - x64 Gen1
VM architecture	Indicate the VM architecture. It must match the image architecture.	x64
Run with Azure Spot discount	Make sure that this check box is unchecked.	–
Size	Choose the VM size.	Standard_E32s_v4 - 32 vCPUs, 256 GiB ($1,132.96/mo)
Enable Hibernation	Make sure that this check box is unchecked. **Note** This option is not supported for the selected image and size.	–

c. Under **Administer account**, provide the required details.

This table lists the required fields, their descriptions, and input examples.

Field	Description	Example
Authentication type	Choose the SSH public key login method.	SSH public key
Username	Enter the default admin username (maglev) for Catalyst Center.	maglev
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.	Generate new key pair
SSH Key Type	From this drop-down list, choose the key type that the enterprise network uses to establish an SSH connection with Catalyst Center on Azure. **Note** The RSA SSH format is the recommended key type.	RSA SSH Format
Key pair name	Enter a name for the SSH key pair. **Note** Azure automatically generates and stores the SSH key pair for secure access. You can also pass the existing key name.	catalyst-center-ssh-key

d. Under **Disks**, verify that the disk configuration is configured by default.

The Catalyst Center image in Azure Marketplace predetermines the disk configuration.

Note

Do not manually modify the existing disks or add new disks.

e. Under **Networking**, provide the required details:

- **Virtual Network (VNet)**: Choose an existing virtual network or create a new one.
- **Subnet**: Select a subnet within the virtual network.
- **Public IP**: Select **None**.

> **Caution**
>
> Ensure that the Catalyst Center VA is not accessible on the public internet for security reasons.

- **NIC Network Security Group (NSG)**: Choose **Advanced**. Then select an existing security group or create one. Make sure that the security group contains the required inbound and outbound rules.

f. Under **Monitoring & Management**, enable boot diagnostics and other options if required.

g. Under **Advanced tab – Custom Data (cloud-init)**, pass a cloud-init script file into the VM user data during provisioning.

> **Caution**
>
> Azure does not allow the selection of private IP addresses during an Azure Marketplace deployment. You must use the next available IP address in the virtual network. Make sure to use this IP address in the cloud-init script.

If you are using a proxy, include the proxy details in the cloud-init script. For example:

```
#cloud-config
write_files:
  - path: /etc/cloud.json
    content: |
      {
        "mks_cloudinit_version": 1,
        "addressing_mode": "ipv4",
        "network": [
          {
            "address": "10.10.0.10",
            "netmask": "255.255.255.0",
            "gateway": "10.10.0.1",
            "routes": [],
            "name": "enterprise"
          }
        ],
        "upstream_dns_servers": ["10.0.0.2"],
        "proxy": {
          "server": "http://10.30.0.42:3128",
          "username": "proxyadmin",
          "password": "Proxypass"
        },
        "ntp": {
          "servers": ["168.61.215.74"]
        },
        "fqdn": "catalyst.center.example.com",
        "cli_password": "Public1@3"
      }

  - path: /usr/local/bin/wait_for_ndp_and_expand.sh
    permissions: '0755'
    content: |-
      #!/bin/sh
```

```
      LOG_FILE="/var/log/magctl-expand.log"
      echo "$(date) : Waiting 35 minutes before expanding volume" >>
"$LOG_FILE"
      sleep 2100  # 35 minutes

      echo "$(date) : Executing magctl azure expand volume" >> "$LOG_FILE"

      echo "Public1@3" | sudo -S magctl azure expand volume >> "$LOG_FILE"
 2>&1

      if [ $? -eq 0 ]; then
       echo "$(date) : magctl expand completed successfully" >> "$LOG_FILE"

      else
        echo "$(date) : ERROR - magctl expand failed" >> "$LOG_FILE"
      fi

cloud_final_modules:
  - ssh-authkey-fingerprints
  - keys-to-console
  - phone-home
  - scripts-user

runcmd:
  - [ "sh", "-c", "/usr/local/bin/wait_for_ndp_and_expand.sh" ]
```

If you are not using a proxy, remove the proxy details from the cloud-init script. For example:

```
#cloud-config
write_files:
  - path: /etc/cloud.json
    permissions: '0644'
    content: |-
      {
        "mks_cloudinit_version": 1,
        "addressing_mode": "ipv4",
        "network": [
          {
            "name": "enterprise",
            "gateway": "10.30.0.1",
            "address": "10.30.0.6",
            "netmask": "255.255.255.0",
            "routes": []
          }
        ],
        "upstream_dns_servers": [
          "172.20.0.5"
        ],
        "ntp": {
          "servers": [
            "168.61.215.74"
          ]
        },
        "fqdn": "catalyst.center.example.com",
        "cli_password": "P@ssword10"
      }

  - path: /usr/local/bin/wait_for_ndp_and_expand.sh
    permissions: '0755'
    content: |-
      #!/bin/sh
```

```
      LOG_FILE="/var/log/magctl-expand.log"
      echo "$(date) : Waiting 35 minutes before expanding volume" >>
"$LOG_FILE"
      sleep 2100  # 35 minutes

      echo "$(date) : Executing magctl azure expand volume" >> "$LOG_FILE"

     echo "P@ssword10" | sudo -S magctl azure expand volume >> "$LOG_FILE"
 2>&1

      if [ $? -eq 0 ]; then
       echo "$(date) : magctl expand completed successfully" >> "$LOG_FILE"

      else
        echo "$(date) : ERROR - magctl expand failed" >> "$LOG_FILE"
      fi

cloud_final_modules:
  - ssh-authkey-fingerprints
  - keys-to-console
  - phone-home
  - scripts-user

runcmd:
  - [ "sh", "-c", "/usr/local/bin/wait_for_ndp_and_expand.sh" ]
```

Azure provisions the VM and automatically applies the configuration during the first boot.

This table lists the required cloud-init script keys and their descriptions.

Key	Description
`mks_cloudinit_version`	Ensure the cloud-init version is `1`.
`addressing_mode`	Ensure the addressing mode is `ipv4`.
Network configuration	
`address`	Enter the static IP address for Catalyst Center.
`netmask`	Enter the netmask for Catalyst Center.
`gateway`	Enter the gateway address for Catalyst Center.
`routes`	Do not enter a route in this field.
`name`	Ensure the name is `enterprise`.
`upstream_dns_servers`	Enter the enterprise Domain Name System (DNS) server address.
Proxy configuration	
`server`	(Optional) Enter the enterprise HTTPS proxy server address.
`username`	(Optional) Enter the HTTPS proxy username.
`password`	(Optional) Enter the HTTPS proxy password.
Network Time Protocol (NTP) configuration	

Key	Description
`servers`	Enter a custom NTP server address that is reachable from the Catalyst Center subnet. You can use the default NTP server address: 168.61.215.74.
Catalyst Center configuration	
`fqdn`	Enter the fully-qualified domain name (FQDN) for Catalyst Center.

Key	Description

`cli_password`	Enter the CLI password for Catalyst Center.
	
	Note
	
	The password must
	• be 9 to 64 characters long, and
	• contain at least three of these categories:
	  • Uppercase letters (A through Z)
	  • Lowercase letters (a through z)
	  • Numbers (0 to 9)
	  • Special characters (for example, !, $, and #)
	
	The password must not include
	• the username or any two consecutive characters of the username
	• context-specific words, such as the service name, username, derivatives, Cisco, and maglev
	• four consecutive characters, except for special characters, and
	• any tabs or line breaks.

Note

- The Catalyst Center image in Azure Marketplace uses cloud-init to process custom data.
- Each key in the user data script specifies a mandatory value that Catalyst Center uses.
- Use the correct syntax for each key that you configure. Azure does not validate the syntax of the input. If the syntax or values are invalid, the Catalyst Center VA may not boot.
- Use the same CLI password for `cli_password` and `echo "password"` in the script. The CLI password must be passed within the script.
- The volume expansion logs are available at: `/var/log/magctl-expand.log`
- To verify the successful expansion of the Catalyst Center instance storage on Azure, run:

```
xfs_quota -xc 'report -h -p /data/maglev/srv/ndp'
```

4. Under **Review + Create**, review and deploy the configuration.
   a. Review the configuration.

      Azure validates the settings.

   b. Click **Create** to deploy the Catalyst Center VA.

      You can monitor the deployment progress under notifications by clicking the bell icon.

5. After successfully deploying Catalyst Center on Azure, go to **Home** > **Virtual Machines** and verify the IP address, disk settings, and network settings.

   Remember

   Verify that the private IP address matches the IP address specified in the cloud-init script. If the IP addresses don't match, assign the private IP address as a static private IP address in the VM networking settings.

Verify the Catalyst Center deployment

Outlines the steps to verify that the Catalyst Center VA is functioning correctly by checking the IP address configurations and testing access to the management interfaces.

Use this procedure to verify that Catalyst Center is functioning.

Before you begin

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

Procedure

1. Verify that the IP address and cloud-init parameters for the Catalyst Center VA match the corresponding configuration on the Azure network interface.
   a. Log in to the Azure portal.
   b. Navigate to the virtual machine page using the search bar.
   c. Select your virtual machine.
   d. Under **Network**, click **Network Settings**.
   e. Go to the network interface.
   f. Verify that the IP address and cloud-init parameters for the Catalyst Center VA match the corresponding configuration on the Azure network interface.
2. Optional: Ping the Catalyst Center IP address from an on-premises server.
3. Optional: After a successful deployment, wait 45 to 50 minutes and then establish an SSH connection with Catalyst Center using port 2222.

   Use the SSH public key and stored key that you configured when you manually deployed Catalyst Center.
4. Verify 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 if the people who set up the Catalyst Center VA on Azure are different from those who will serve as its administrators.

4 Backup and Restore

Topics:

- About backup and restore
- Backup and restore—hardware appliance to VA
- Backup and restore—VA to VA
- Configure a backup
- Restore a backup

About backup and restore

Describes how to use the backup and restore functions to create backup files for system recovery or migration.

This section provides information on how to 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 if your Catalyst Center becomes unusable or use those files to migrate your Catalyst Center to a different appliance.

For example, you can:

- Back up data from a Catalyst Center hardware appliance and restore the data to a Catalyst Center VA.
- Back up data from one Catalyst Center VA on Azure or ESXi and restore the data to another Catalyst Center VA on Azure.

> ⚠ **Caution**
>
> NetFlow data is not backed up when you back up Catalyst Center automation and Assurance data.

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

Backup and restore—hardware appliance to VA

Outlines high-level steps for backing up data from a Catalyst Center hardware appliance and restoring the data to a Catalyst Center VA.

If the backup is completed on Catalyst Center 3.x, you can directly restore your backup files to your Catalyst Center deployment using this procedure.

> ⚠ **Caution**
>
> If the backup was completed on Catalyst Center 2.3.x, you must upgrade the Catalyst Center architecture first so that you can restore your backup files successfully. Complete "Scenario 9: Upgrade Catalyst Center on Azure" in the *Cisco Catalyst Center 3.x Upgrade* article instead of this procedure.

This procedure provides a high-level overview for backing up the data from a Catalyst Center hardware appliance and restoring it to a Catalyst Center VA. For detailed instructions, refer to the "Backup and Restore" chapter in the *Cisco Catalyst Center Administrator Guide*.

Before you begin

Ensure that the hardware appliance used for the backup is a 44-core Catalyst Center appliance.

Procedure

1. Back up the data from the Catalyst Center hardware appliance.

Ensure that the backup server is reachable from Catalyst Center.

> **Caution**
>
> If you are backing up data from Catalyst Center 2.3.x, you must upgrade the Catalyst Center architecture first. Complete "Scenario 9: Upgrade Catalyst Center on Azure" in the *Cisco Catalyst Center 3.x Upgrade* article instead of this procedure.

2. Create a Catalyst Center VA.

   Ensure that the Catalyst Center VA is up and running.

3. Connect the Catalyst Center VA to the backup server described in Step 1.

   Ensure that the backup server is reachable from the Catalyst Center VA.

4. Configure the backup server on the Catalyst Center VA.
5. Restore the data to the Catalyst Center VA.

Backup and restore—VA to VA

Lists the prerequisites and high-level steps to back up data from a source Catalyst Center VA and restore it to a target Catalyst Center VA, including network reachability and cloud backup server access requirements.

Use this procedure to back up the data from one Catalyst Center VA on Azure or ESXi and restore the data onto another Catalyst Center VA on Azure.

This procedure provides a high-level overview of how you can back up the data from one (source) Catalyst Center VA on Azure or ESXi 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 meet these prerequisites:

- You have successfully deployed two Catalyst Center VAs on Azure, or one Catalyst Center VA on ESXi and one Catalyst Center VA on Azure.
- Both Catalyst Center VAs are up and running.
- The backup server is reachable from the source Catalyst Center VA and target Catalyst Center VA.

Procedure

1. Back up the data from the source Catalyst Center VA to a backup server.
2. Bring up the target Catalyst Center VA that you want to restore the data to.
3. Connect the target Catalyst Center VA to the backup server.
4. Configure the backup server on the target Catalyst Center VA.
5. Restore the data to the target Catalyst Center VA.

The data from the source Catalyst Center VA on Azure or ESXi is successfully restored onto the target Catalyst Center VA on Azure.

Configure a backup

Provides step-by-step instructions to configure an NFS backup server, establish a mount path with an encryption passphrase, and schedule automated backups through the Catalyst Center GUI.

Use this procedure to configure a backup for Catalyst Center.

Procedure

1. Log in to Catalyst Center:
   a) Enter `https://server-ip` in your browser.

      server-ip is the IP address of the server on which Catalyst Center is installed.

   b) Enter your Catalyst Center username and password.
2. From the main menu, choose **System** > **Backup & Restore**.
3. Click **Configure Settings**.
4. If you are adding or updating the configuration for an NFS, click **Add NFS**.

   Otherwise, skip to Step 8.
5. In the **Add NFS** area, do these steps:
   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 **111**.
   f) Click **Save**.
6. In the **Warning** dialog box, click **Proceed**.
7. Verify that the NFS configuration is correct:
   a) Click **View NFS List**.
   b) Review the information in the **NFS List**.
   c) Close the **NFS List**.
8. 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**.
9. Schedule your backup:
   a) From the main menu, choose **Settings** > **Backup & Restore**.
   b) Click **Scheduled Backup**.
   c) In the **Scheduled Backup** pane, configure the options for your backup as needed.
   d) Click **Save**.

Restore a backup

Provides step-by-step instructions to restore a backup to a Catalyst Center VA using the Catalyst Center GUI.

Use this procedure to restore a backup for Catalyst Center.

Procedure

1. Log in to Catalyst Center:
   a) Enter `https://server-ip` in your browser.

      server-ip is the IP address of the server on which Catalyst Center is installed.

   b) Enter your Catalyst Center username and password.
2. From the main menu, choose **System** > **Backup & Restore**.
3. In the **Actions** column for your backup, click **...** and choose **Restore**.

5 Postdeployment Changes

Topics:

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

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

Provides the prerequisite and step-by-step instructions to update the DNS server IP address that is configured on your Catalyst Center VA using the Azure portal.

Use this procedure to update the DNS server IP address that is configured on your Catalyst Center VA.

Before you begin

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

Procedure

1. Log in to the Azure portal.
2. Navigate to the **Resource groups** service using the search bar.
3. Click the virtual machine.
4. Navigate to **Help** > **Serial Console** and click **Connect**.
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
      veUhoTzZYYjRIWnJWNDdxSG5qR0REUjV3TE90bnNXalpBL2tsRzNzN01Ia1ZaY0VzMVENCkVoc3FZUGU5Z2ZoTWF
      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.