Cisco Telemetry Broker

Virtual Appliance Deployment and Configuration Guide 1.3.x

TOC

Introduction

This guide explains how to install Cisco Telemetry Broker. It describes the Cisco Telemetry Broker components and how they are placed within your network.

Cisco Telemetry Broker enables you to do the following:

- Install Cisco Telemetry Broker
- Update Cisco Telemetry Broker
- Configure destinations and rules
- Migrate from Secure Network Analytics UDP Director
- Check the unreachability of a destination
- Use IPv6 Destinations
- Pass through NIC for 10G throughput
- Use high availability

Audience

This guide is designed for the person responsible for maintaining network telemetry flow and monitoring network telemetry.

Common Abbreviations

The following abbreviations appear in this guide:

Abbreviation	Description
DNS	Domain Name Server/Service
FTP	File Transfer Protocol
Gbps	Gigabits per second
HTTPS	Hypertext Transfer Protocol (Secure)
Mbps	Megabits per second
NAT	Network Address Translation
NTP	Network Time Protocol

Abbreviation	Description
SSH	Secure Shell
UDPD	UDP Director
URL	Universal Resource Locator
VLAN	Virtual Local Area Network

Concepts and Architecture

Cisco Telemetry Broker allows you to ingest network telemetry from many inputs, transform the telemetry format, and forward that telemetry to one or multiple destinations. Refer to the following table for examples.

You can ingest any of the following telemetry:	And forward that telemetry to any or all of the following destinations:
• On-premises network telemetry, including NetFlow, syslog, and IPFIX • Cloud-based telemetry inputs, such as Amazon Web Services (AWS) Virtual Private Cloud (VPC) Flow Logs	• Analytics platforms, such as Secure Network Analytics or Secure Cloud Analytics • Network management and automation platforms, such as Cisco DNA Center • Security Information and Event Management (SIEM) platforms

To accomplish this, you deploy one or more Cisco Telemetry Broker nodes, which ingest telemetry over UDP and forward it to the configured destinations.

Out of the box, Cisco Telemetry Broker supports the following transformations:

Ingested Data Format	Forwarded Data Format
VPC Flow Logs	IPFIX
Microsoft Network Security Group (NSG) Flow Logs	IPFIX
IPFIX	Json (only to SCA destinations)

Your broker nodes are all managed by one Cisco Telemetry Broker manager. You can log in to this manager's web interface and perform various configuration tasks, including managing the broker nodes, setting up the forwarding rules, creating users, and reviewing the dashboard for usage.

You deploy these broker nodes and manager as virtual appliances to a hypervisor.

Deployment Requirements

The following lists the prerequisites and recommendations for deploying Cisco Telemetry Broker to your network to forward telemetry from a given input to a destination.

Browser Requirements

Cisco Telemetry Broker supports the following browsers (as tested with the latest rapid release and with resolution at 1024 x 768 px):

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

Network Requirements

You must do the following before deployment:

- Download two OVA files and create a minimum of two virtual machines.
- Reserve one IP address for the manager node and two IP addresses for each broker node you deploy.

Networks

Management Network: Every node (manager or broker) in your deployment must have one IPv4 network interface connected to the Management Network to provide for administration over SSH and HTTPS (if the node is running the management functions).

Telemetry Network: The broker node must have a second interface (IPv4 or IPv6) that must be connected to the Telemetry Network. On this network the node will receive telemetry from inputs and forward it to destinations.

The Management Network and the Telemetry Network can be the same network.

Management Network Connection Configuration

Before installing Cisco Telemetry Broker, determine the following settings for the Management Network:

- IPv4 address
- IPv4 subnet mask
- IPv4 default gateway address
- IPv4 DNS nameserver

Telemetry Network Connection Configuration

Before installing Cisco Telemetry Broker, determine the following settings for the Telemetry Network:

- IPv4 IP address
- IPv4 subnet
- IPv4 default gateway address
- IPv6 IP address
- IPv6 subnet
- IPv6 default gateway address

You can configure the interface to be active on both an IPv4 and IPv6 address simultaneously.

Virtual Machine Requirements

For KVM deployments, telemetry brokering uses only 2 CPUs on the broker node. Assigning additional CPUs improves the performance only if the broker node is performing telemetry transformation.

Hardware Configuration

You can deploy a broker node using any one of the following three different performance profiles, depending on the performance type you want to achieve:

- **1 Gbit/s** Use this profile to achieve line-rate packet brokering for a 1 Gbit/s NIC.
- **10 Gbit/s** Use this profile to achieve line-rate packet brokering for a 10 Gbit/s NIC.
- **Transformation Capable** Use this profile to achieve telemetry transformation (for example, sending IPFIX to Secure Cloud Analytics).

Configuration	Manager	Broker
CPU	4	1 Gbit/s: 2 10 Gbit/s: 5 Transformation Capable: 8
Memory	8GB	1 GBit/s: 12 GB 10 GBit/s: 12 GB

		Transformation Capable: 12 GB
Storage	80GB	70 GB

The broker uses CPUs according to the information described in the following table. Use this table as a reference to understand how different CPU allocations help to achieve the desired performance type.

CPUs	1 Gbit/s	10 Gbit/s	Transformation Capable
1	Degraded	Degraded	Degraded
2	Supported	Degraded	Degraded
3	Supported	Degraded	Degraded
4	Supported	Degraded	Degraded
5	Supported	Supported	Degraded
6	Supported	Supported	Degraded
7	Supported	Supported	Degraded
8	Supported	Supported	Supported

VMWare ESXi

Resource	Manager	Broker
Network Interface #1 Connection to Management Network	e1000e	e1000e
Network Interface #2 Connection to Telemetry Network	Not installed	vmxnext

We recommend that you use the OVA defaults for all other values.

KVM QEMU

Resource	Manager	Broker
Disk	virtio-scsi	virtio-scsi
Network Interface #1 Connection to Management Network	virtio	virtio
Network Interface #2 Connection to Telemetry Network	Not installed	vmxnext

Time Synchronization

The Cisco Telemetry Broker VM synchronizes its system time with the hypervisor. To ensure that features like TLS work correctly, hypervisor time needs to be accurate.

VMWare ESXi

To learn how to run NTP on the ESXi hypervisor, refer to this VMWare knowledge base article.

KVM QEMU

To ensure that the hypervisor and the guest are synced, confirm that you have defined the *track='guest'* attribute for the guest machine 's XML configuration as shown in the following image. For more information, refer to `libvirt` documentation.

```
<clock offset='utc'>
    <timer name='rtc' tickpolicy='catchup' track='guest'/>
    <timer name='pit' tickpolicy='delay'/>
    <timer name='hpet' present='no'/>
</clock>
```

This will synchronize the guest clock to the host clock value. However, you need to accurately maintain the hypervisor host clock. To accomplish this, you can use an NTP daemon.

Open Communication Ports

The following table provides details for all the network connections made to and from your Cisco Telemetry Broker appliances. To ensure that your network permits these connections, you need to modify the applicable access controls you currently have in place (for example, your firewall).

Client	Server	Port	Description
users	broker nodes and manager node	22/TCP	SSH access to the console
manager	external internet	443/TCP	HTTPS for secure external communications, such as Smart Licensing and Software Update
manager	customer syslog server	customer-defined port	Syslog telemetry for Cisco Telemetry Broker notifications
manager	customer SMTP server	customer-defined port	SMTP telemetry for Cisco Telemetry Broker notifications
each broker node	manager	443/TCP	HTTPS for secure management connections
each broker node	external internet	443/TCP	HTTPS for retrieving VPC/NSG Flow Logs from AWS S3/Azure SAS storage buckets, respectively
users	manager	443/TCP	HTTPS for secure web interface access
broker nodes and manager node	customer DNS servers	53/UDP	DNS telemetry
each broker node	external internet	443/TCP	HTTPS for broker node to secure access SCA server and upload files to SCA S3 bucket.

In addition, you must open ports based on both the telemetry type that is sent to a broker node and the telemetry type that a broker node sends to a destination. The following table provides details about common ports for various telemetry types:

Port	Description
514/UDP	syslog
2055/UDP	NetFlow v5, NetFlow v9
4739/UDP	IPFIX
6343/UDP	sFlow

Migrate Configuration to a New System

Complete the following processes to back up and restore the CTB configuration rules that you set up in the Cisco Telemetry Broker manager.

- It is possible for UDPD customers to migrate their existing UDPD configuration to Cisco Telemetry Broker. For more details, see the "Importing and Exporting UDP Director Configuration" section in the Cisco Telemetry Broker User Guide.

Back Up CTB Configuration Rules

Run the following command on the CTB Manager Node:

```
$ sudo ctb-backup-config -v -f ctb_config.json
```

When this process has finished, the configuration rules will be backed up to the file at ~/.ctb_config.json, after which you can copy the configuration rules to another location.

- VPC/NSG flow log rules are not backed up, so you need to re-create your VPC/NSG flow log rules upon migrating to a new system.
- You can back up and restore your CTB configuration rules only within the same version. If you try to do so across versions, the process may fail.

Restore the CTB Configuration Rules

You must run `ctb-restore-config` immediately after you run `ctb-install` on the manager node.

Run the following command on the CTB Manager Node:

```
$ sudo ctb-restore-config -v -f ctb_config.json
```

- Any inputs that you add to Cisco Telemetry Broker due to the restore are not assigned to any nodes or clusters. You will need to assign them as required.

Determine Network Configuration

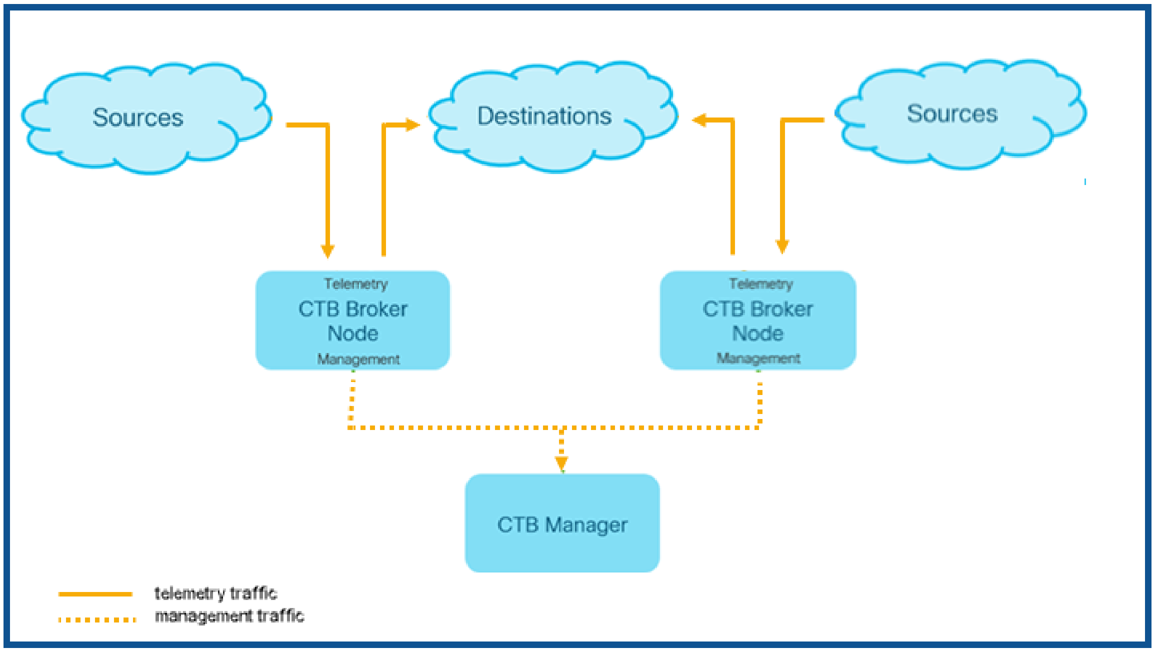
Cisco Telemetry Broker supports multi-node setups, where a single Cisco Telemetry Broker manager can manage multiple broker nodes. Since Cisco Telemetry Broker updates every broker node with all destinations and rules, you must carefully plan your configuration to avoid a few common issues, which are listed below.

- You can deploy broker nodes in different telemetry segments, where the telemetry interfaces of each broker node may not be accessible across the network. You need to carefully construct rules so that packets from an exporter that reach a specific node are not forwarded to destinations that are not accessible from that node. To achieve this, you need to construct rules that exclude exporters that might cause this routing issue. One example would be to not use any default rules, since these would match all inputs.
- Not all destinations may be relevant to each broker node. However, with the Check Destination Reachability feature, since each broker node attempts to ascertain accessibility for each destination, the broker nodes could report conflicting information back to the manager. If the possibility exists that some broker nodes will not be able to connect with some destinations, turn off Check Destination Reachability for those destinations.

If you are migrating to Cisco Telemetry Broker from the UDP Director, then before you deploy the manager node and the broker node OVA files, you need to plan how you will connect the two VMs to the network, as differences exist between how you configure both Cisco Telemetry Broker and the UDP Director.

Cisco Telemetry Broker differentiates telemetry traffic from management traffic. The broker node has two interfaces: The Telemetry Network Interface and the Management Network Interface. The manager node has only the Management Network Interface. The following diagram shows how to logically deploy the manager node and the broker nodes.

> Note that the examples in this topic represent typical deployment scenarios. To learn how to set up a more advanced deployment (for example, one that uses VLANs), contact a network administrator.



Cisco Telemetry Broker receives management traffic *only* on the Management Network Interface; it uses this interface for all communications between the broker node and the manager node. Telemetry traffic is brokered primarily on the Telemetry Network Interface of the broker node. The only exception to this is when Cisco Telemetry Broker retrieves AWS VPC flow log, which occurs over the broker node's Management Network Interface.

You can place the manager node anywhere in the network on any subnet, but you must have TCP connectivity over port 443 with the broker nodes.

You can use one of the following deployment modes with the broker node:

1. The telemetry subnets and management subnets are the same. In this mode, the Telemetry Network Interface and the Management Network Interface on the broker node belong to the same subnet. See Interfaces Belong to the Same Subnet.

2. The telemetry subnets and management subnets are different, so the broker node retains its Telemetry Network Interface and Management Network Interface on two separate subnets. See Interfaces Belong to Different Subnets.

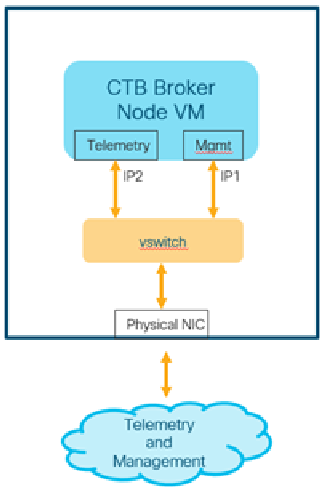
Providing separate paths for both telemetry traffic and management traffic offers the following advantages:

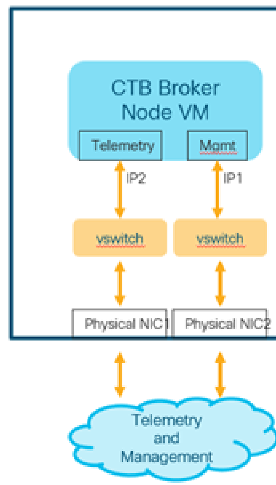
- Separate paths increases performance, especially when it approaches interface line rate performance, since traffic doesn't need to share resources (such as virtual switches and physical NICs).
- Separating management traffic from telemetry traffic simply makes good sense for a network configuration.

Interfaces Belong to the Same Subnet

This deployment mode is very similar to that of the UDP Director, where the management interface and the Telemetry interface are the same. The only difference in this first deployment mode is that you need separate IP addresses for the broker node interfaces.

Refer to the following images to see how to configure this type of deployment.





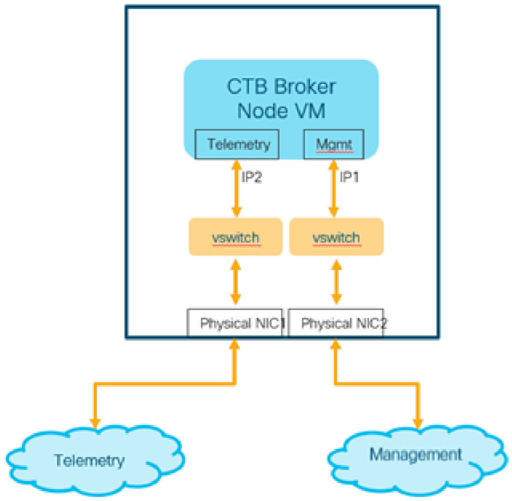
In a virtual environment, you can accomplish this in one of the following two ways:

1. You connect the broker node's Telemetry Network Interface and Management Network Interface to the same virtual switch in the hypervisor.
2. You connect the broker node's Telemetry Network Interface and Management Network Interface to different virtual switches, but you connect the underlying NICs to the same physical switch and thus the same subnet.

Interfaces Belong to Different Subnets

In this deployment mode, the Telemetry Network Interface and the Management Network interface are on different subnets. In this case you typically need separate virtual switches for the two interfaces.

Refer to the following image to see how to configure this type of deployment.


CTB Broker
Node VM
Telemetry
Mgmt
IP2
IP1
vswitch
vswitch
Physical NIC1
Physical NIC2
Telemetry
Management

Deploy Cisco Telemetry Broker

The following describes the high-level steps for deploying broker nodes to your network and configuring them to ingest telemetry from inputs and export telemetry to destinations:

- Deploy a manager node and one or more broker nodes to your hypervisor
- Configure Cisco Telemetry Broker Smart Licensing
- Configure the manager node to manage your broker nodes
- Configure one or more rules to control how broker nodes ingest and export telemetry
- Review the state of your deployment performance from the dashboard

Note that the broker node continuously polls the telemetry interface NIC for incoming telemetry, resulting in high CPU utilization. It is normal to see high CPU utilization of the Broker Node.

Technical Limitations

- A single Cisco Telemetry Broker deployment supports a maximum of 10 destinations per input and 10 broker nodes per Manager node.
- If you disable exporters tracking, each broker node supports a maximum of 100k exporters. If you enable exporters tracking for one or more inputs, we recommend that you do not track more than 1000 exporters (totaled across all inputs), as this may result in degraded performance.

  (For information about disabling and enabling exporters tracking, see the "UDP Inputs" topic in the Cisco Telemetry Broker User Guide.)
- A destination supports a maximum of 1000 subnets (totaled across all rules for that destination). Adding more than 1000 subnets may result in data loss.

VMWare Setup

We have tested the following instructions on VMWare ESXi 6.7.

> You need to install and configure the Manager Node before you install the Broker Node(s).

VMWare: Install the Manager Node

Complete the following steps in order:

1. Download the Manager Node OVA file.
2. Deploy the Manager Node.
3. Verify VM Time Settings.
4. Log in as the install user.
5. Run the sudo ctb-install command.
6. Configure the first super user account.
7. Log out.

> You need to install and configure the Manager Node before you install the Broker Node(s).

1. Download the Manager Node OVA File

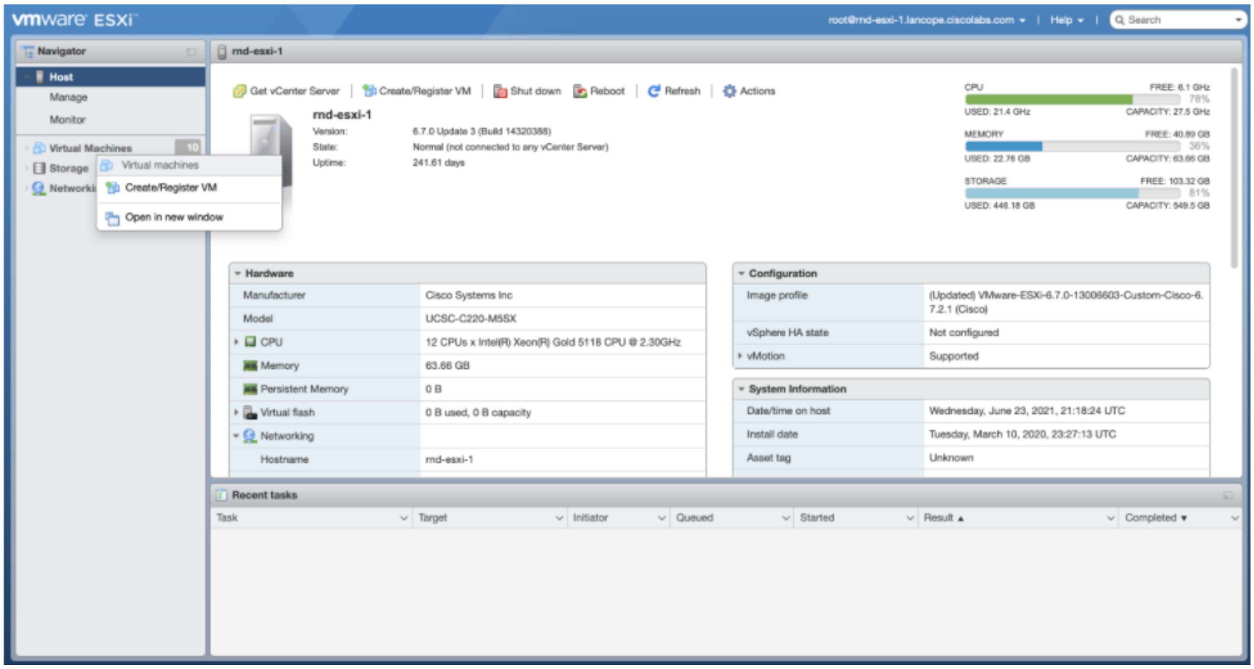
1. Download the Manager Node OVA file.
2. On software.cisco.com, check the SHA512sum value of the OVA file.
3. After the OVA file is downloaded, verify that the SHA512sum value of the OVA file matches the SHA512 Checksum value on software.cisco.com. To do this, run the following command:

   ```
   sha512sum <path/to/file>
   ```

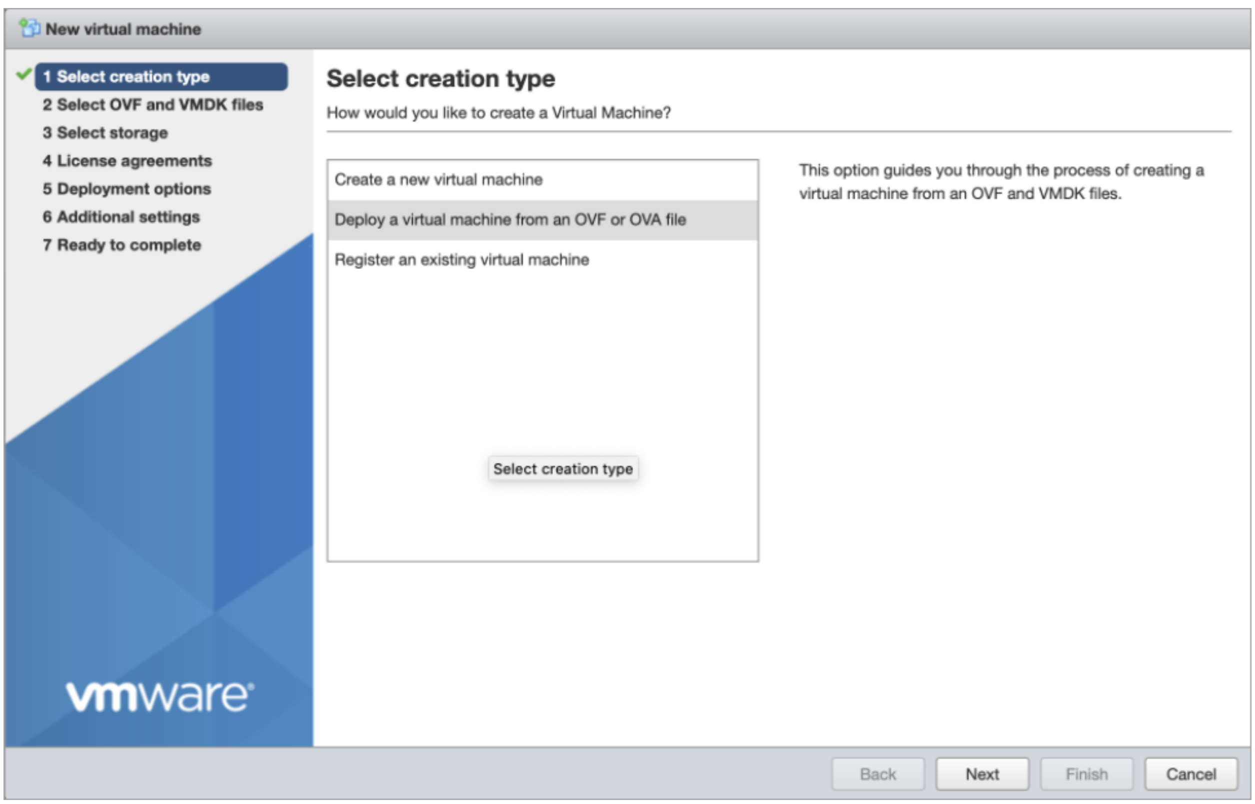
   On software.cisco.com, you can view the SHA512sum value by hovering your cursor over the tooltip for the link.

2. Deploy the Manager Node

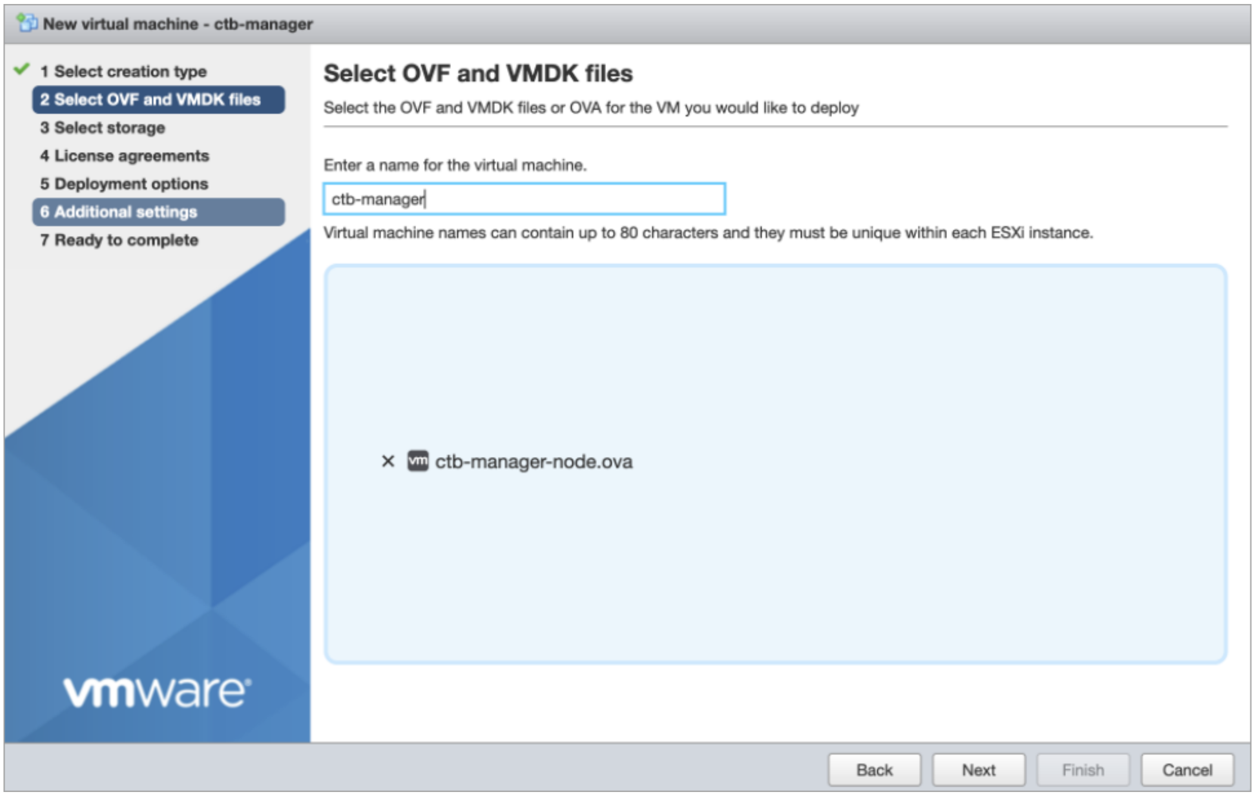
1. Log in to the VMWare vSphere web user interface console.
2. From the side menu, right-click **Virtual Machine** and then choose **Create/Register VM.**



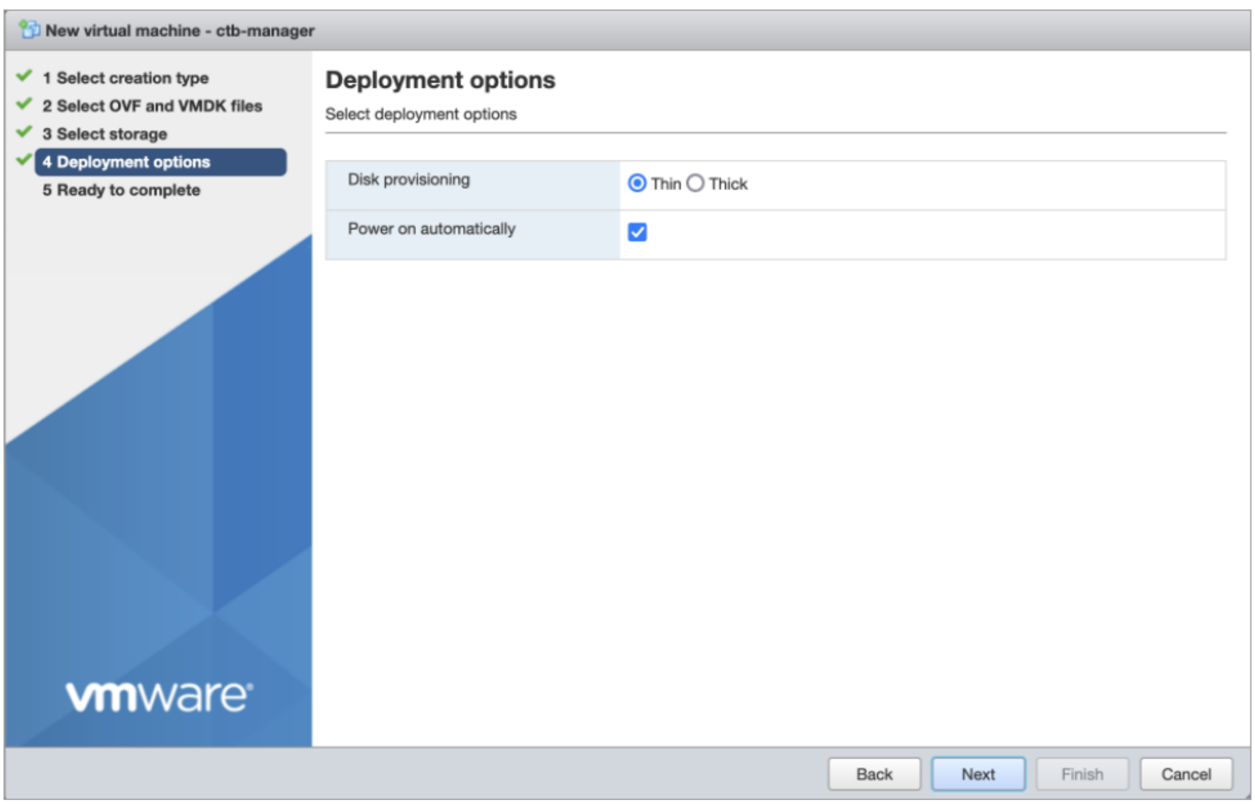
3. Choose **Deploy a virtual machine from an OVF or OVA file**.



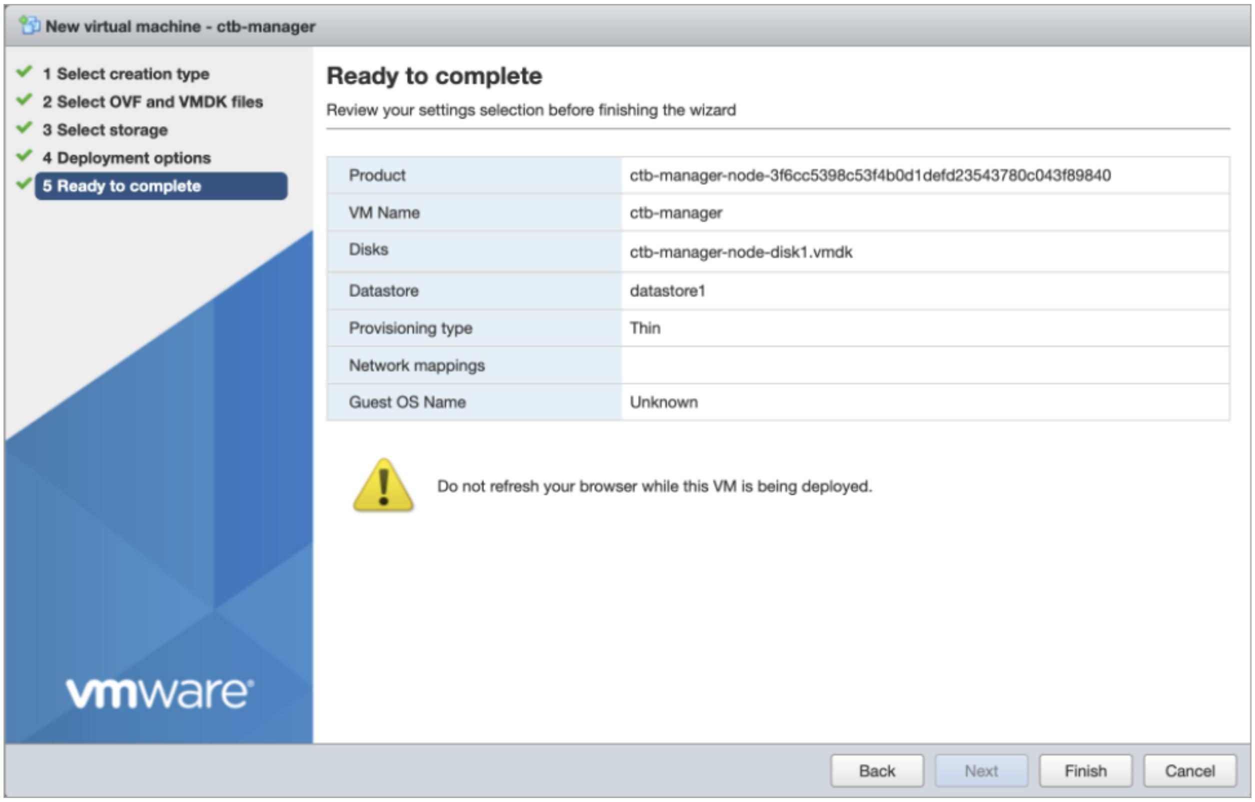
4. Enter the **name of the OVA file**.



5. Configure the settings as shown in the following image.



6. Click **Finish**. The system will start and prompt you to log in.



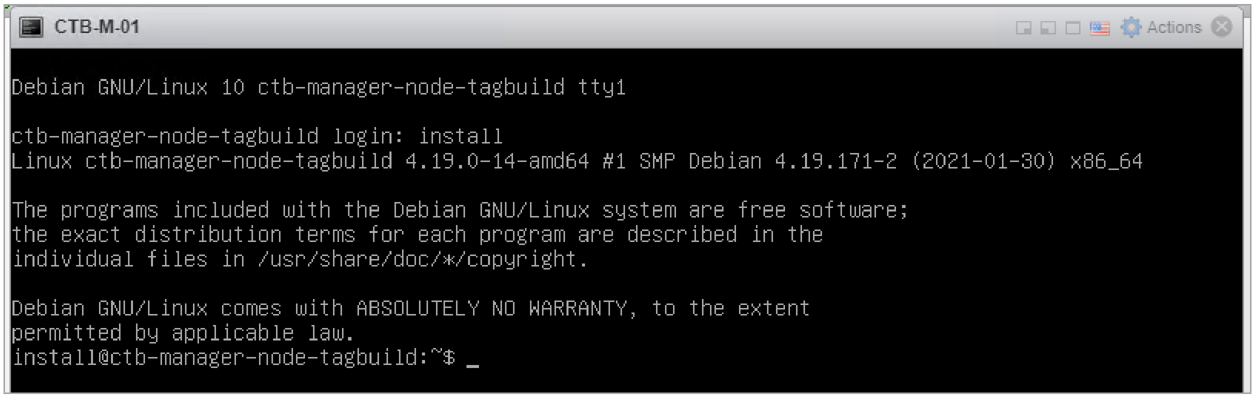
3. Verify VM Time Settings

The VM relies on the hypervisor to provide accurate time, and the default settings should ensure this is occurring. However, we recommend that you verify this by completing the following steps:

1. In the VMware interface, click the manager node VM that you deployed in the previous section, Deploy the Manager Node.
2. Click **Edit** to open the window in which you will edit the VM's settings.
3. Choose **VM Options > VMware Tools > Time**.
4. Ensure the **Synchronize guest time with host** check box is checked.
5. Click **Save** to save these settings.

4. Log In as the Install User

From the manager node virtual machine within the vmware user interface, open a web console and log in to the virtual machine (the username is **install**; there is no password).



5. Run the sudo ctb-install Command

> ⚠ If you plan on restoring config from a different CTB deployment, then you must run `ctb-restore-config` immediately after you run `ctb-install` on the manager node. See **Migrate Configuration to a New System**.

1. Run the `sudo ctb-install` command.
2. Enter the following information:
   - Password for the **admin** user

     The password must meet the following requirements:
     - Contain at least 8 characters
     - Contain at least 1 lowercase letter
     - Contain at least 1 uppercase letter
     - Contain at least 1 digit
     - Contains at least 1 of these special characters: @ # $ % ^ & * ! + ?
     - Cannot be a commonly-used phrase or sequence
     - Cannot be similar to any identifying attributes of the user (such as the username)
   - IPv4 address, subnet mask, and default gateway address for the Management Network interface
   - Valid DNS nameserver IP address that is reachable from the virtual machine

6. Configure the First Super User Account

If this is the first time you are logging in to the manager web interface, you must first create the first Super user account before you install any broker nodes. We suggest assigning the user name of **webadmin** so as not to confuse it with the **admin** user.

- In a web browser, navigate to the following site to create it: https://<manager_ip_address>.

7. Logout

To log out, type `exit`.

VMWare: Install the Broker Node

Complete the following steps in order:

1. Download the Broker Node OVA file.
2. Deploy the Broker Node.
3. Configure Resource Reservations.
4. Verify VM Time Settings.
5. Log in as the install user.
6. Run the sudo ctb-install command.
7. Run the sudo ctb-manage command.
8. Log out.
9. Configure the Telemetry Interface.

> You need to install and configure the Manager Node before you install the Broker Node(s).

1. Download the Broker Node OVA File

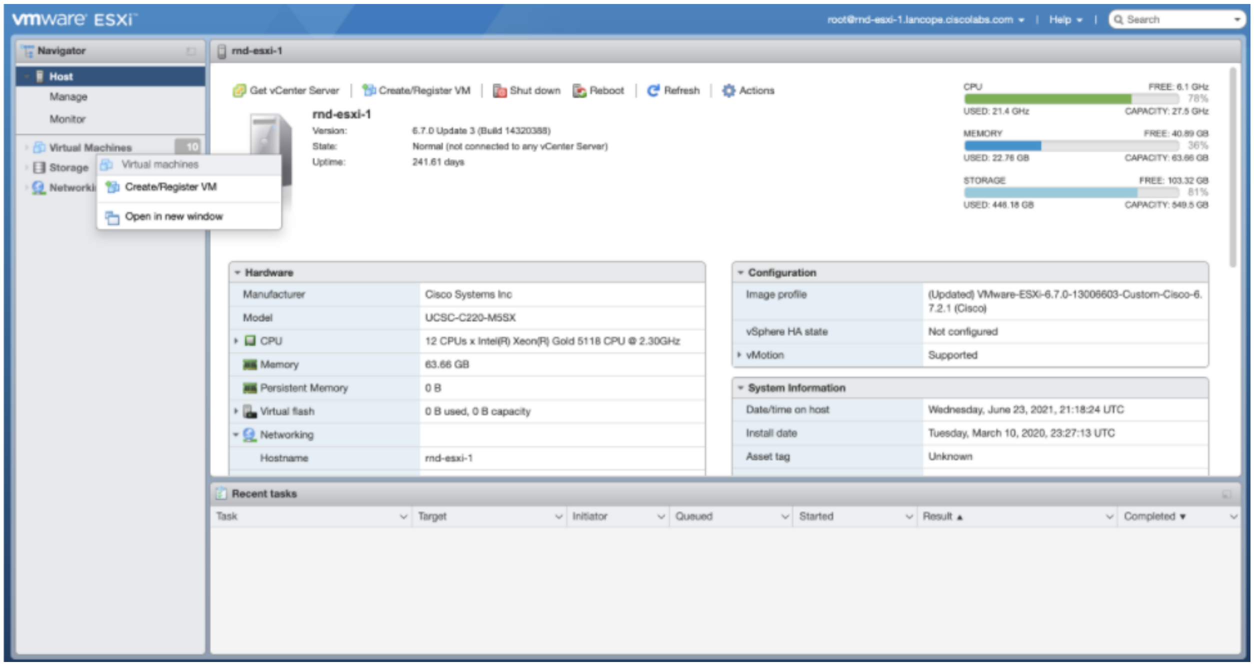
1. Download the Broker Node OVA file.
2. On software.cisco.com, check the SHA512sum value of the OVA file.
3. After the OVA file is downloaded, verify that the SHA512sum value of the OVA file matches the SHA512 Checksum value on software.cisco.com. To do this, run the following command:

   ```
   sha512sum <path/to/file>
   ```

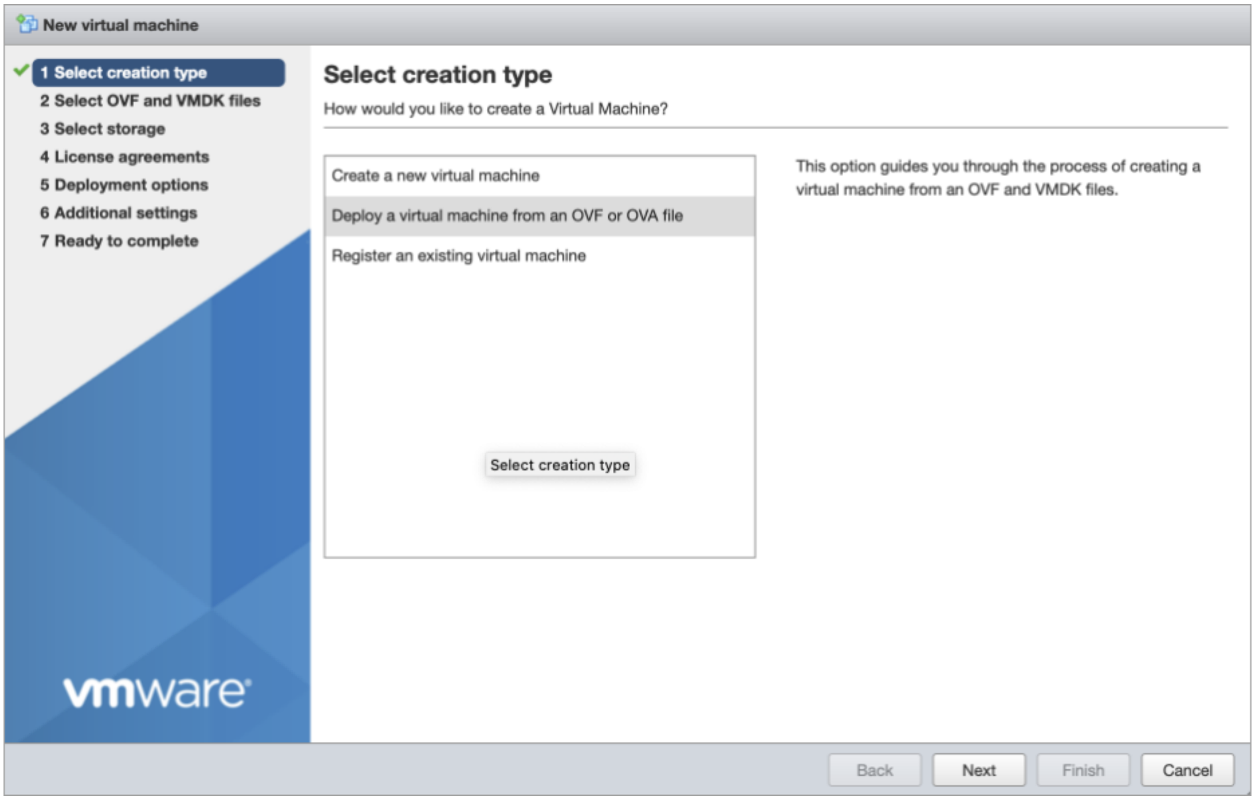
   On software.cisco.com, you can view the SHA512sum value by hovering your cursor over the tooltip for the link.

2. Deploy the Broker Node

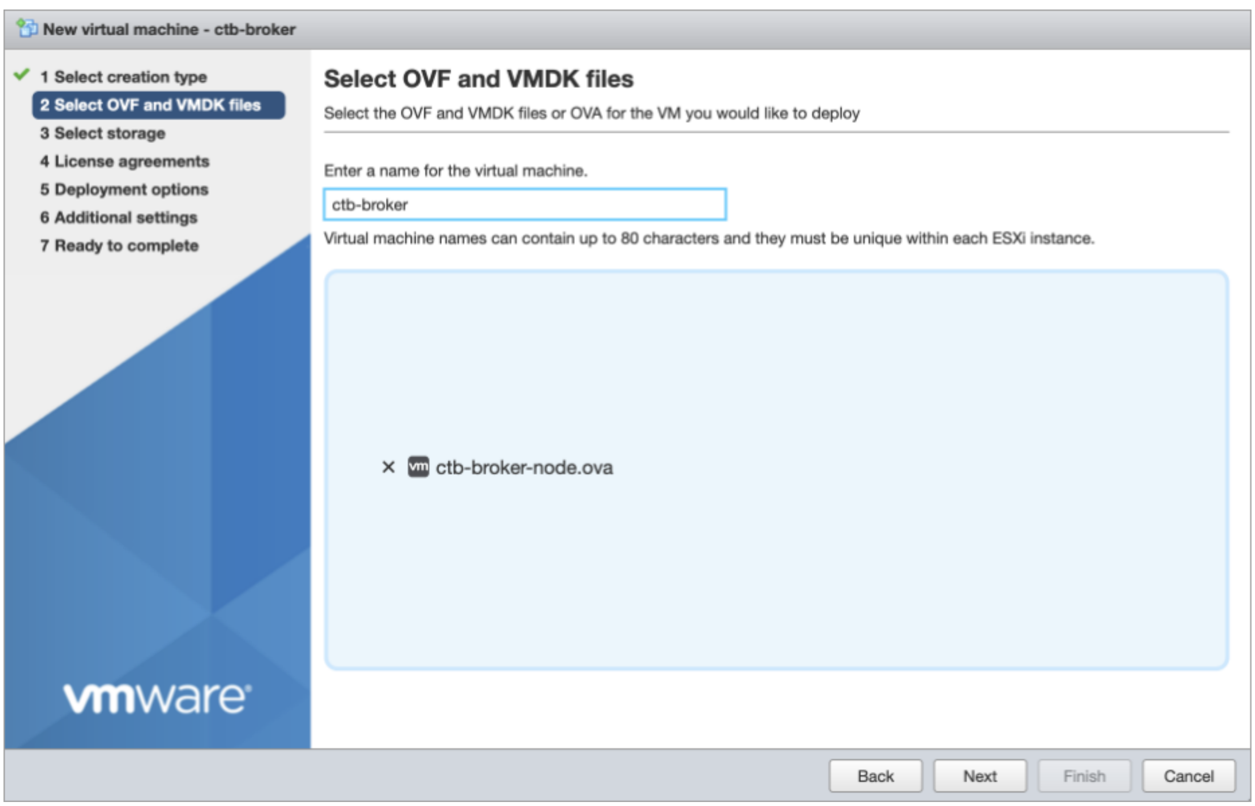
1. Log in to the VMWare vSphere web user interface console.
2. From the side menu, right-click **Virtual Machine** and then choose **Create/Register VM.**



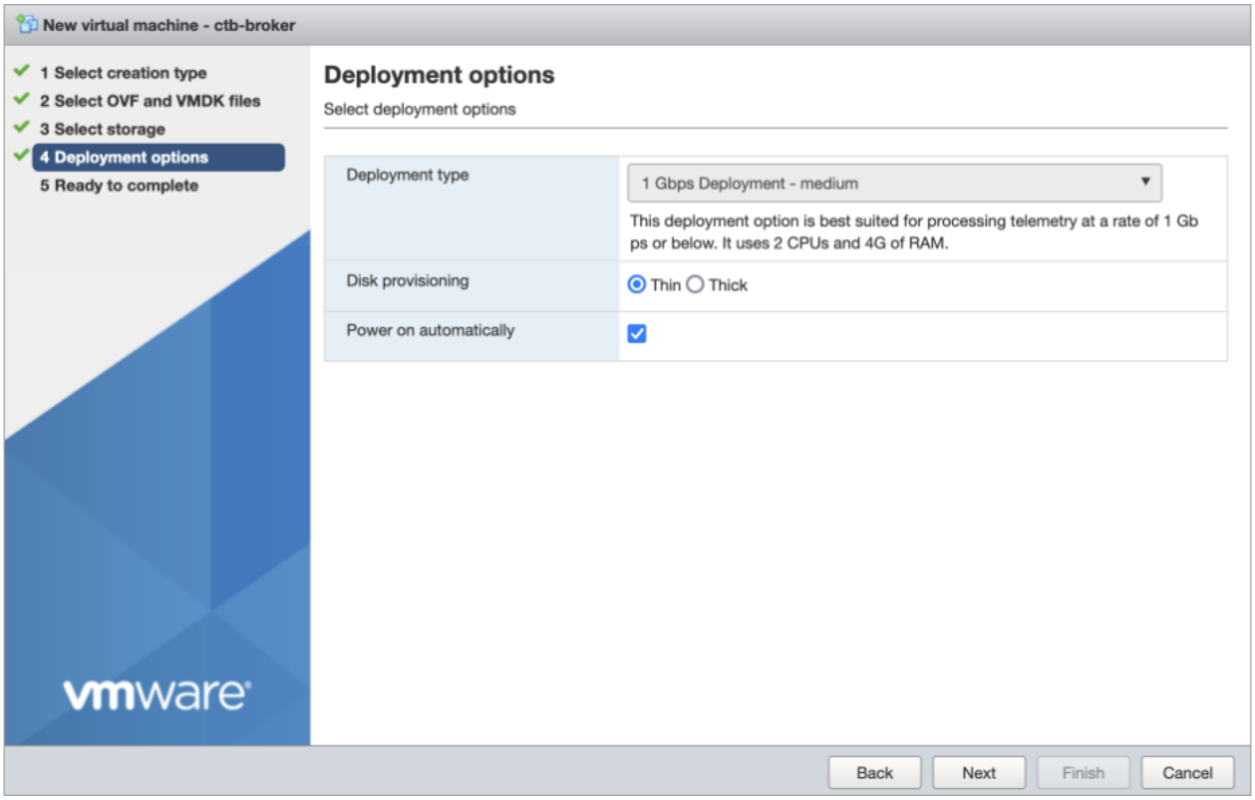
3. Choose **Deploy a virtual machine from an OVF or OVA file.**



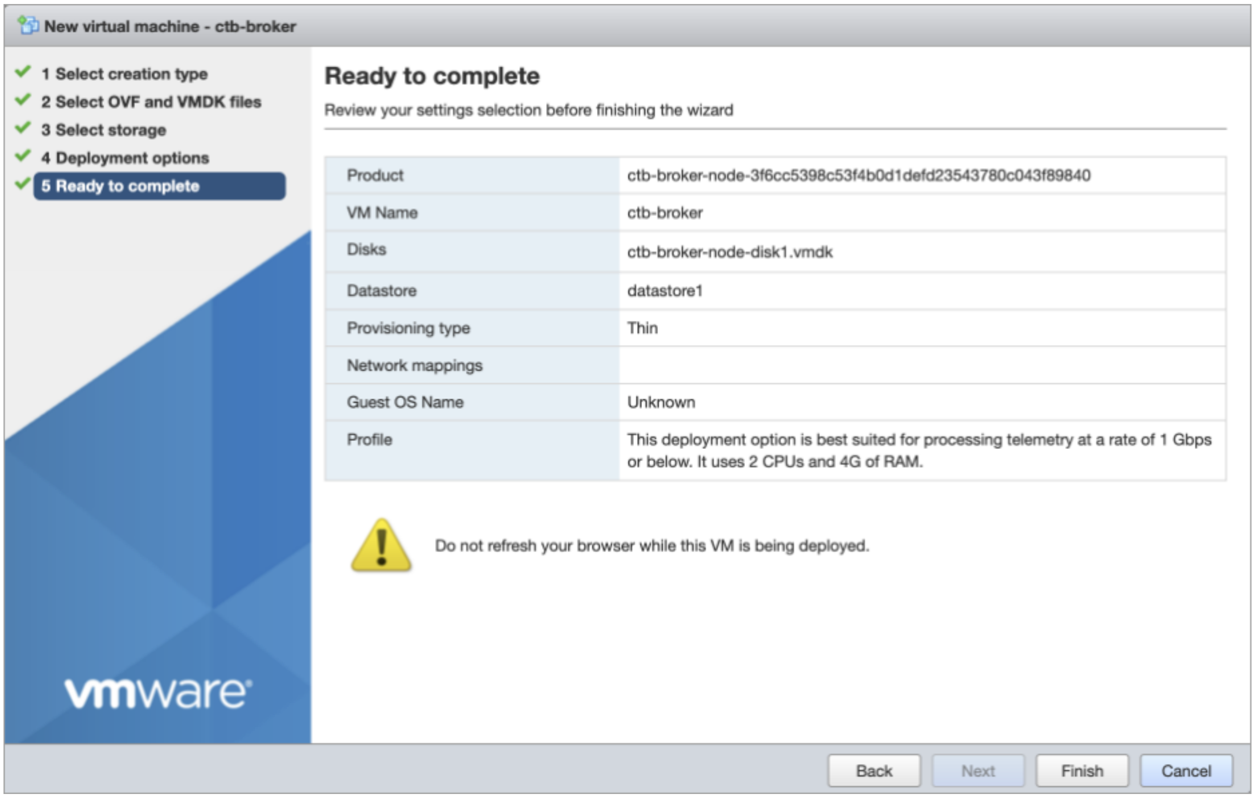
4. Enter the **name of the OVA file** you downloaded in Step 3.



5. Set the Default type to 1 Gbps, 10 Gbps, or Transformation Capable as appropriate for your installation. Configure the remaining settings as shown in the following image.



6. Click **Finish**.



3. Configure Resource Reservations

The broker node requires that all computer resources are dedicated to the VM. To ensure this occurs, complete the following steps:

1. In the VMware interface, click the broker node VM that you deployed in the previous section, Deploy the Broker Node.
2. Click **Edit** to open the window in which you will edit the VM's settings.
3. Choose **Virtual Hardware > CPU > Reservations.**
4. To determine the Reservations value, multiply the number of CPUs on the VM by the GHz value of your hypervisor's processor type (which you can find on the Hypervisors **Summary > CPU > Processor Type** screen).
    - For example, if your hypervisor lists the processor type as *@2.40 GHz*, and your VM is allocated 8 CPUs, then you would use this formula: 8 x 2.40 GHz = 19200 MHz. In this case, you should specify **19200 MHz** as the Reservation value.
    - Some VMware products (for example, VCenter) provide a drop-down list that includes a value labeled as **Maximum** that reflects the pre-calculated value for you.

5. Choose **Virtual Hardware > Memory > Reservations**.
6. Check the **Reserve all guest memory (all locked)** check box.
7. Click **Save** to save these settings.

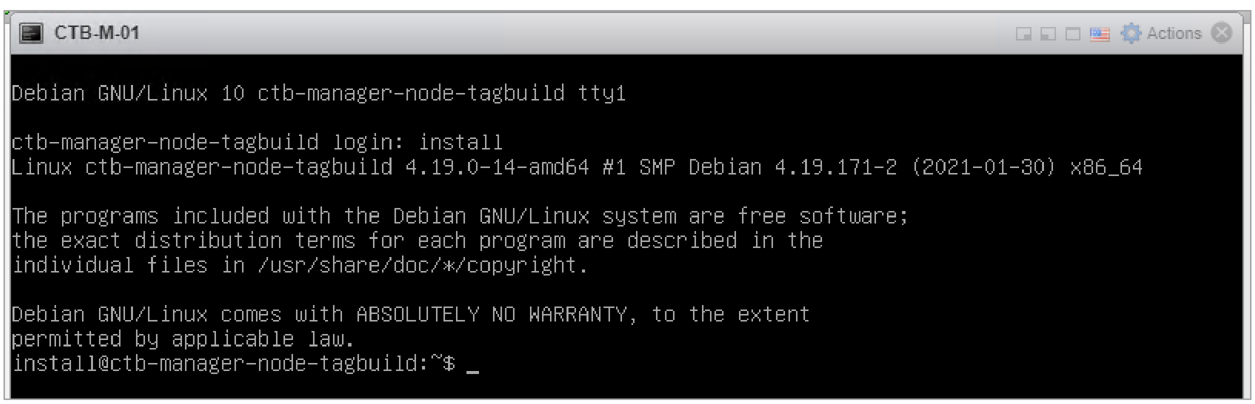
4. Verify VM Time Settings

The VM relies on the hypervisor to provide accurate time, and the default settings should ensure this is occurring. However, we recommend that you verify this by completing the following steps:

1. In the VMware interface, click the broker node VM that you deployed in Section 2, Deploy the Broker Node.
2. Click **Edit** to open the window in which you will edit the VM's settings.
3. Choose **VM Options > VMware Tools > Time**.
4. Ensure the **Synchronize guest time with host** check box is checked.
5. Click **Save** to save these settings.

5. Log In as the Install User

From the broker node virtual machine within the vmware user interface, open a web console and log in to the virtual machine (the username is **install**; there is no password).



6. Run the sudo ctb-install Command

1. Run the `sudo ctb-install` command.
2. Enter the following information:
   - Password for the **admin** user

     The password must meet the following requirements:

    - Contain at least 8 characters
    - Contain at least 1 lowercase letter
    - Contain at least 1 uppercase letter
    - Contain at least 1 digit
    - Contains at least 1 of these special characters: @ # $ % ^ & * ! + ?
    - Cannot be a commonly-used phrase or sequence
    - Cannot be similar to any identifying attributes of the user (such as the username)
- IPv4 address, subnet mask, and default gateway address for the Management Network interface
- Valid DNS nameserver IP address that are reachable from the virtual machine

7. Run the sudo ctb-manage Command

1. Run the `sudo ctb-manage` command.
2. Enter the following information:
    - IP address of the manager node
    - Username of the super user account you create in the manager node
    - Password of the super user account you create in the manager node

8. Logout

To log out, type `exit`.

9. Configure the Telemetry Interface

Go to **Configure the Telemetry Interface**.

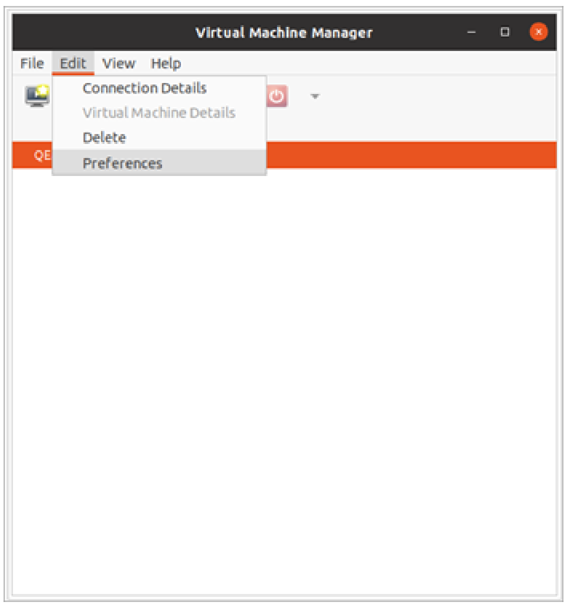
KVM Setup

The following instructions for setting up your KVM (Kernel[based] Virtual Machine) are based on the following:

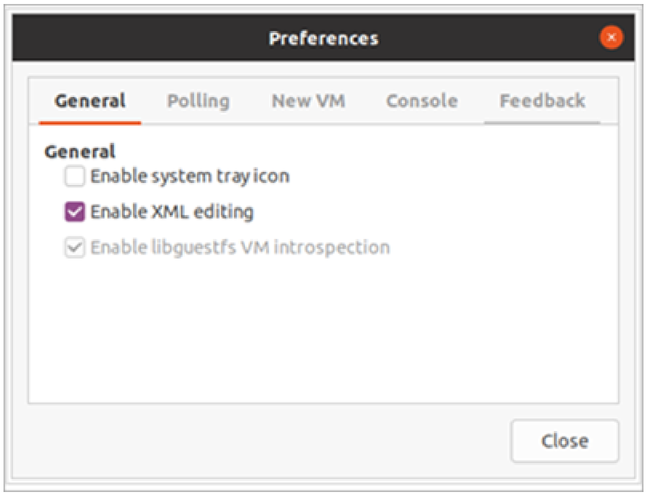
- libvirt 7.1.0
- qemu-kvm 5.2.0
- Linux Kernel 5.10.26
- Virtual Machine Manager (virt-manager) Ubuntu 2.2.1

Before you proceed, confirm in your Virtual Machine Manager that you have chosen the **Enable XML Editing** option. If your version of Virtual Machine Manager does not support XML editing, you can perform the same step using the *virsh edit* command on your KVM host.

1. Open the VM Manager and choose **Edit > Preferences**.



2. Check the **Enable XML Editing** check box and click **Close.**



KVM: Install the Manager Node

Complete the following steps in order:

1. Download the Manager Node QCOW2 file.
2. Launch the virtual machine.
3. Log in as the install user.
4. Run the sudo ctb-install command.
5. Configure the first super user account.
6. Log out.

> You need to install and configure the Manager Node before you install the Broker Node(s).

1. Download the Manager Node QCOW2 File

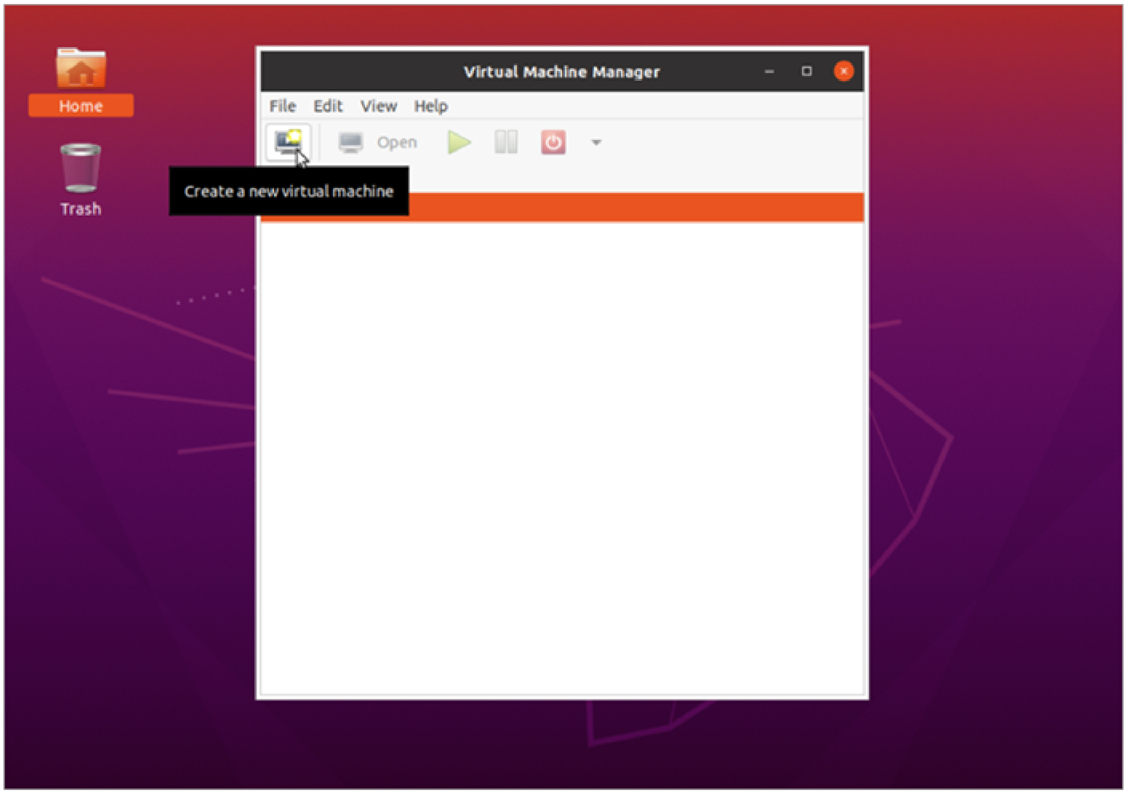
1. Download the Manager Node QCOW2 file.
2. On software.cisco.com, check the SHA512sum value of the QCOW2 file.
3. After the QCOW2 file is downloaded, verify that the SHA512sum value of the QCOW2 file matches the SHA512 Checksum value on software.cisco.com. To do this, run the following command:

   ```
   sha512sum <path/to/file>
   ```

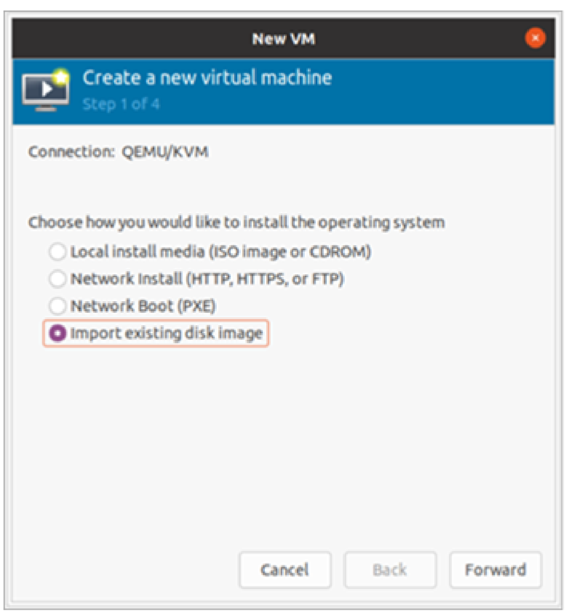
   On software.cisco.com, you can view the SHA512sum value by hovering your cursor over the tooltip for the link.

2. Launch the Virtual Machine

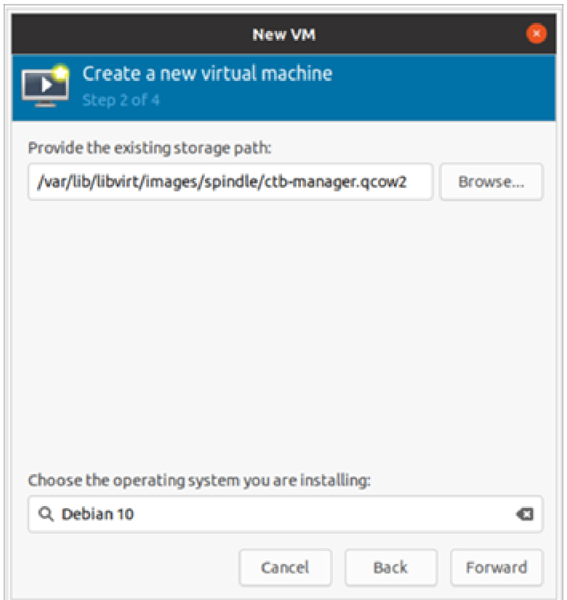
1. Open the Virtual Machine Manager on your Linux system running KVM and click **Create a new virtual machine.**



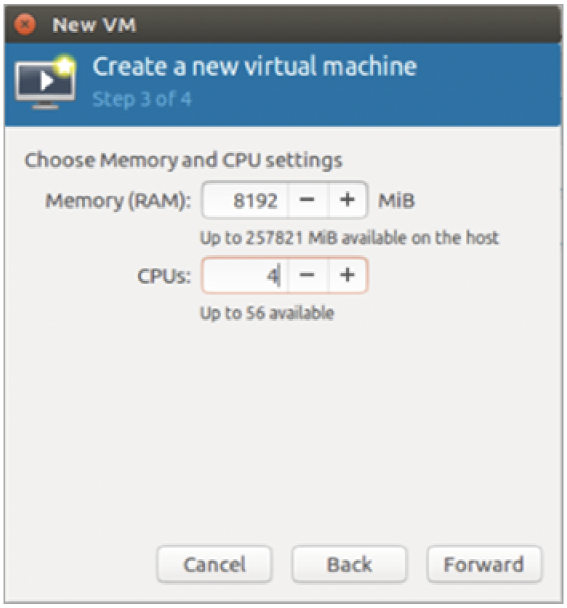
2. In Step 1 of the **Create a new virtual machine** dialog, check the **Import existing disk image** option. Click **Forward.**



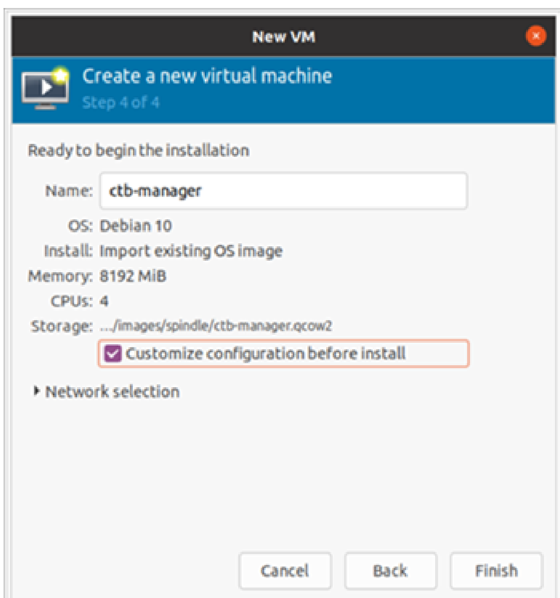
3. In Step 2 of the **Create a new virtual machine** dialog, do the following:
    a. Enter the existing storage path to your QCOW2 file that you downloaded in Step 1.
    b. For the operating system, choose **Debian Buster**.
    c. Click **Forward**.



4. In Step 3 of the **Create a new virtual machine** dialog, do the following:
    a. In the Memory (RAM) field, set the entry to at least **8 GB.**
    b. In the CPUs field, set the entry to at least **4.**
    c. Click **Forward.**



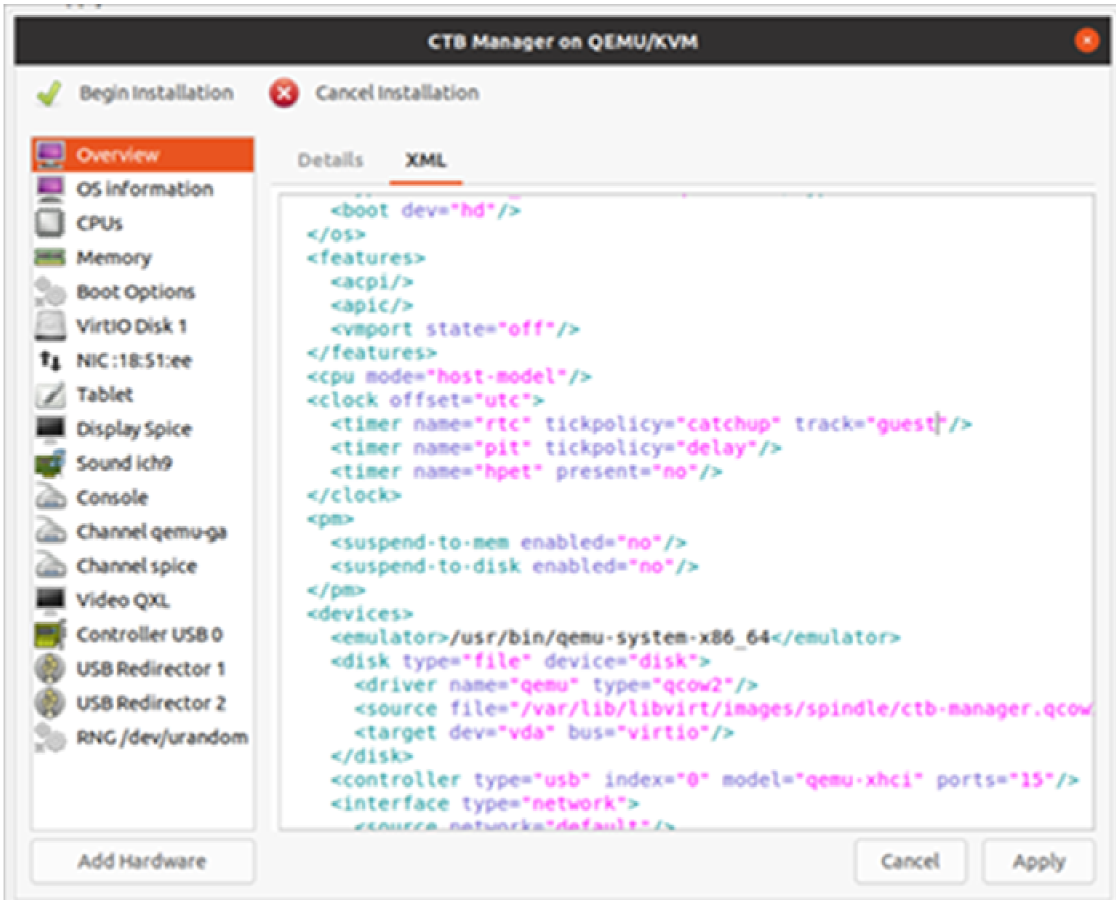
5. In Step 4 of the **Create a new virtual machine** dialog, do the following:
    a. In the Name field, enter **ctb-manager.**
    b. Check the **Customize configuration before install** check box.
    c. Click **Finish.**



6. Do the following:
    a. From the side menu, choose **Overview**.
    b. Click the **XML** tab.

c. Change the line <timer name="rtc" tickpolicy="catchup"/> to <timer name="rtc" tickpolicy="catchup" track="guest"/>

d. Click **Apply**.

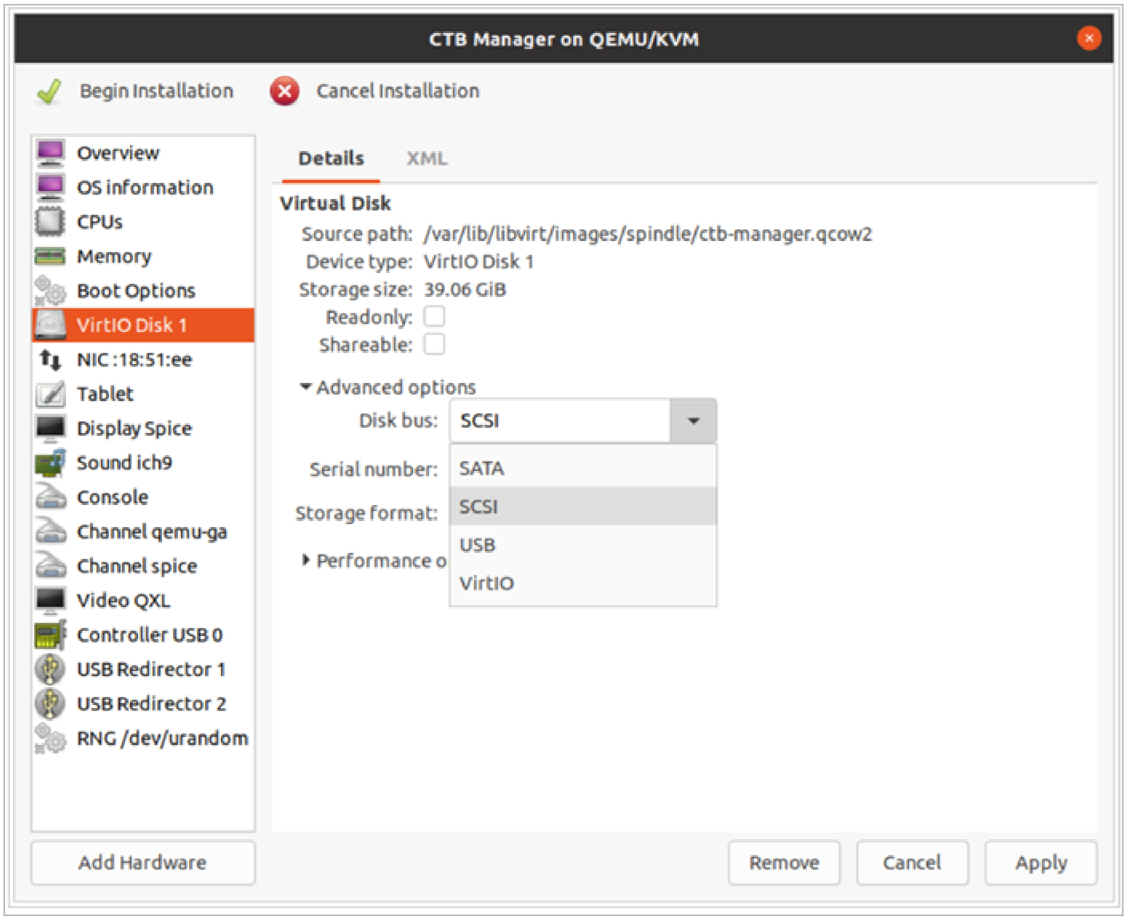


7. Do the following:

   a. From the side menu, choose **Virtiov Disk 1**.

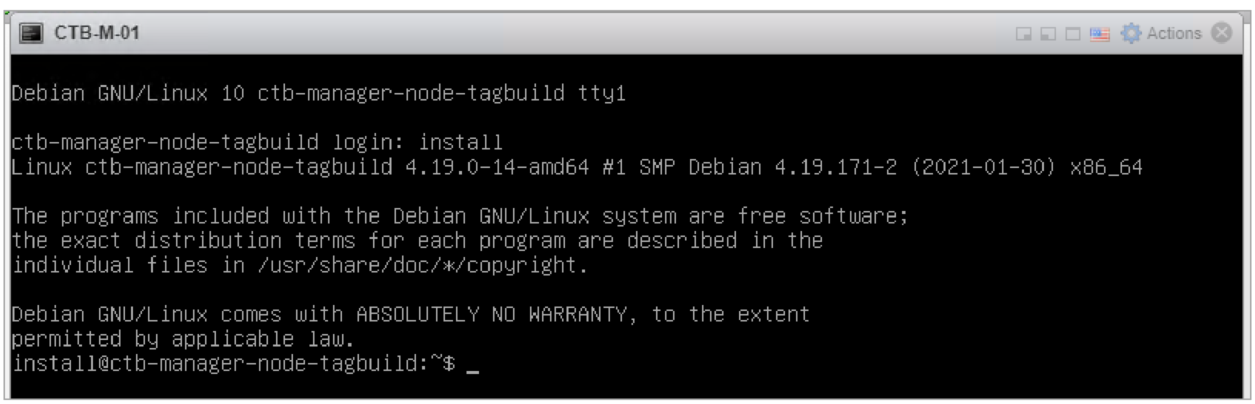
   b. On the Details tab, in the Disk bus drop-down list, choose **SCSI**.

   c. Click **Apply**.



3. Log In as the Install User

From the manager node virtual machine within the vmware user interface, open a web console and log in to the virtual machine (the username is **install**; there is no password).



4. Run the sudo ctb-install Command

> ⚠ If you plan on restoring config from a different CTB deployment, then you must run `ctb-restore-config` immediately after you run `ctb-install` on the manager node. See **Migrate Configuration to a New System**.

1. Run the `sudo ctb-install` command.
2. Enter the following information:
   - Password for the **admin** user

     The password must meet the following requirements:
     - Contain at least 8 characters
     - Contain at least 1 lowercase letter
     - Contain at least 1 uppercase letter
     - Contain at least 1 digit
     - Contains at least 1 of these special characters: @ # $ % ^ & * ! + ?
     - Cannot be a commonly-used phrase or sequence
     - Cannot be similar to any identifying attributes of the user (such as the username)
   - IPv4 address, subnet mask, and default gateway address for the Management Network interface
   - Valid DNS nameserver IP address that is reachable from the virtual machine

5. Configure the First Super User Account

If this is the first time you are logging in to the manager web interface, you must first create the first Super user account before you install any broker nodes. We suggest assigning the user name of **webadmin** so as not to confuse it with the **admin** user.

- In a web browser, navigate to the following site to create it: https://<manager_ip_address>.

6. Logout

To log out, type `exit`.

KVM: Install the Broker Node

Complete the following steps in order:

1. Download the Broker Node QCOW2 file.
2. Launch the virtual machine.
3. Log in as the install user.
4. Run the sudo ctb-install command.
5. Run the sudo ctb-manage command.
6. Log out.
7. Configure the Telemetry Interface.

> You need to install and configure the Manager Node before you install the Broker Node(s).

1. Download the Broker Node QCOW2 File

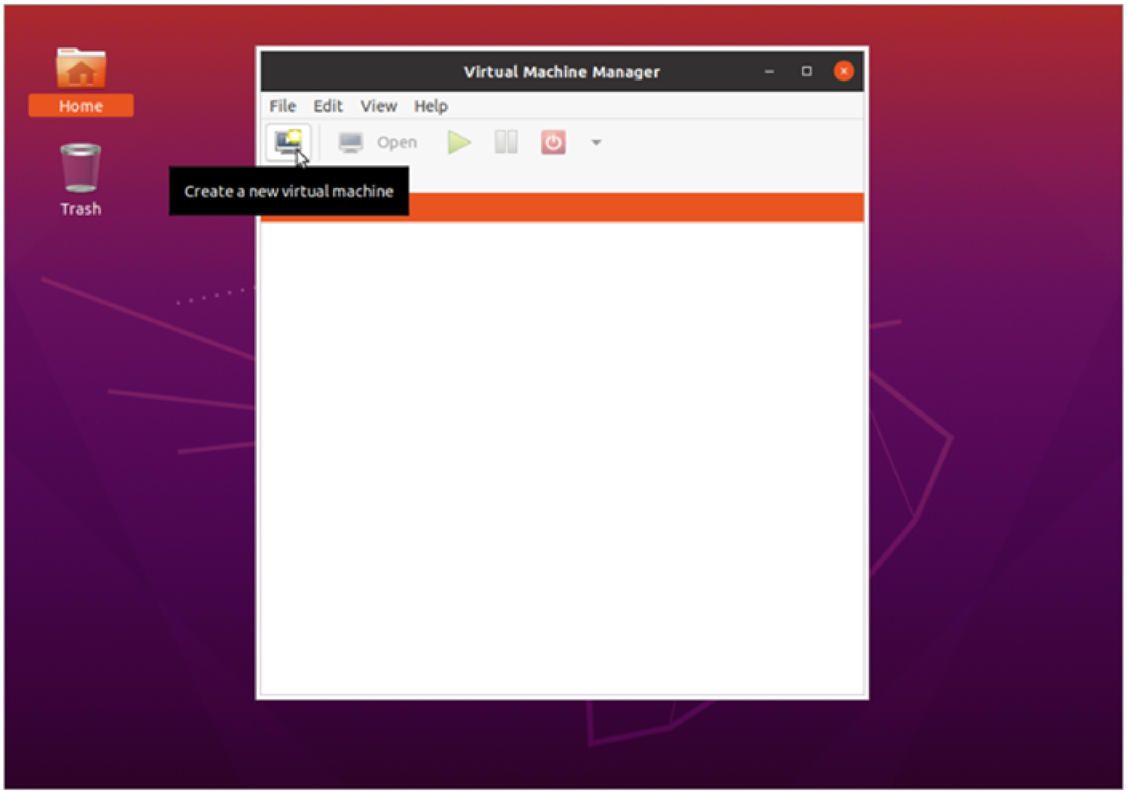
1. Download the Broker Node QCOW2 file.
2. On software.cisco.com, check the SHA512sum value of the QCOW2 file.
3. After the OVA file is downloaded, verify that the SHA512sum value of the OVA file matches the SHA512 Checksum value on software.cisco.com. To do this, run the following command:

   ```
   sha512sum <path/to/file>
   ```

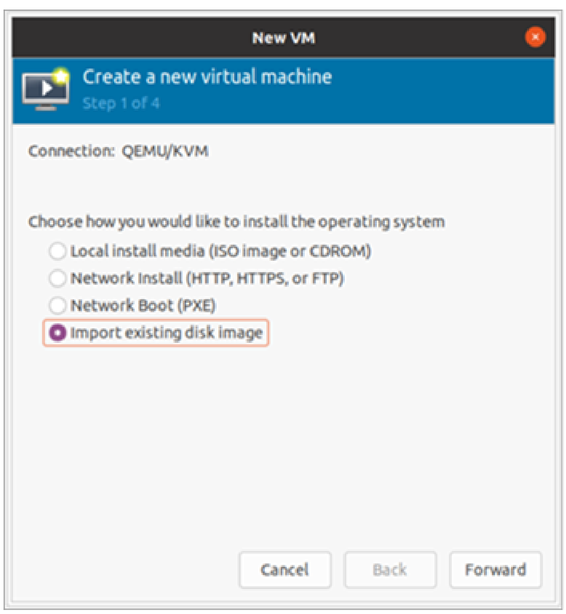
   On software.cisco.com, you can view the SHA512sum value by hovering your cursor over the tooltip for the link.

2. Launch the Virtual Machine

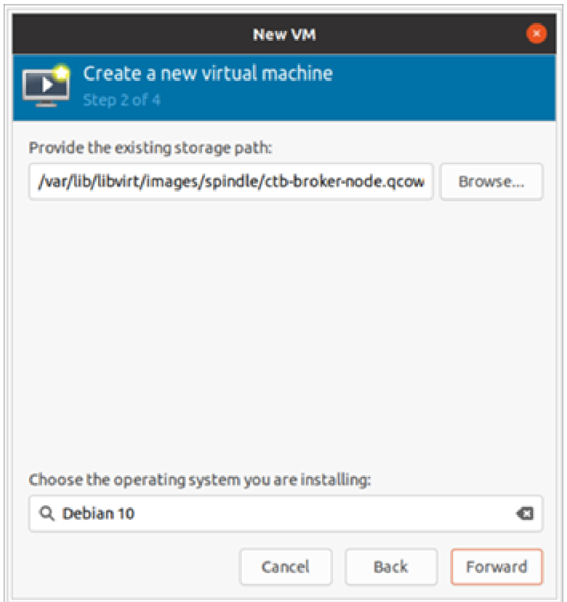
1. Open the Virtual Machine Manager on your Linux system running KVM and click **Create a new virtual machine.**



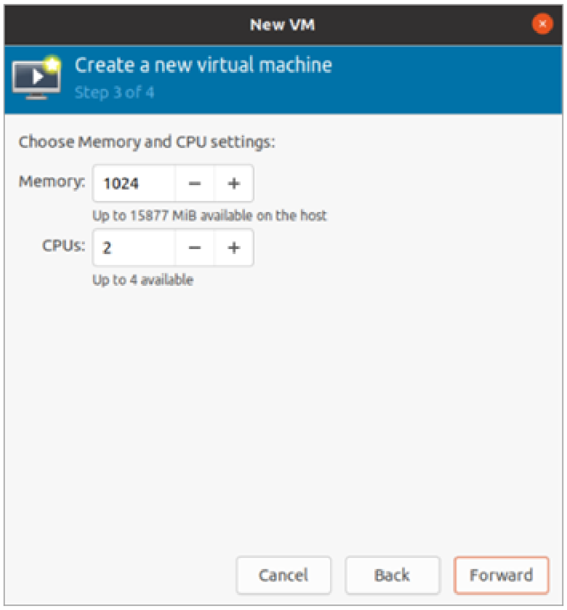
2. In Step 1 of the **Create a new virtual machine** dialog, check the **Import existing disk image** option. **Click Forward**.



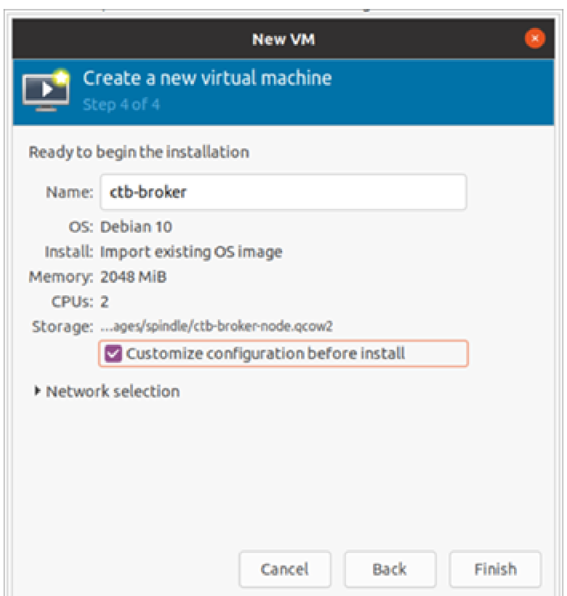
3. In Step 2 of the **Create a new virtual machine** dialog, do the following:
    a. Enter the existing storage path to your QCOW2 file that you downloaded in Step 1.
    b. For the operating system, choose **Debian Buster**.
    c. **Click Forward**.



4. In Step 3 of the **Create a new virtual machine** dialog, do the following:
    a. In the Memory (RAM) field, set the entry to at least **2 GB.**
    b. In the CPUs field, set the entry to **2** (assigning additional CPU to the broker does not necessarily improve performance on KVM).
    c. Click **Forward.**



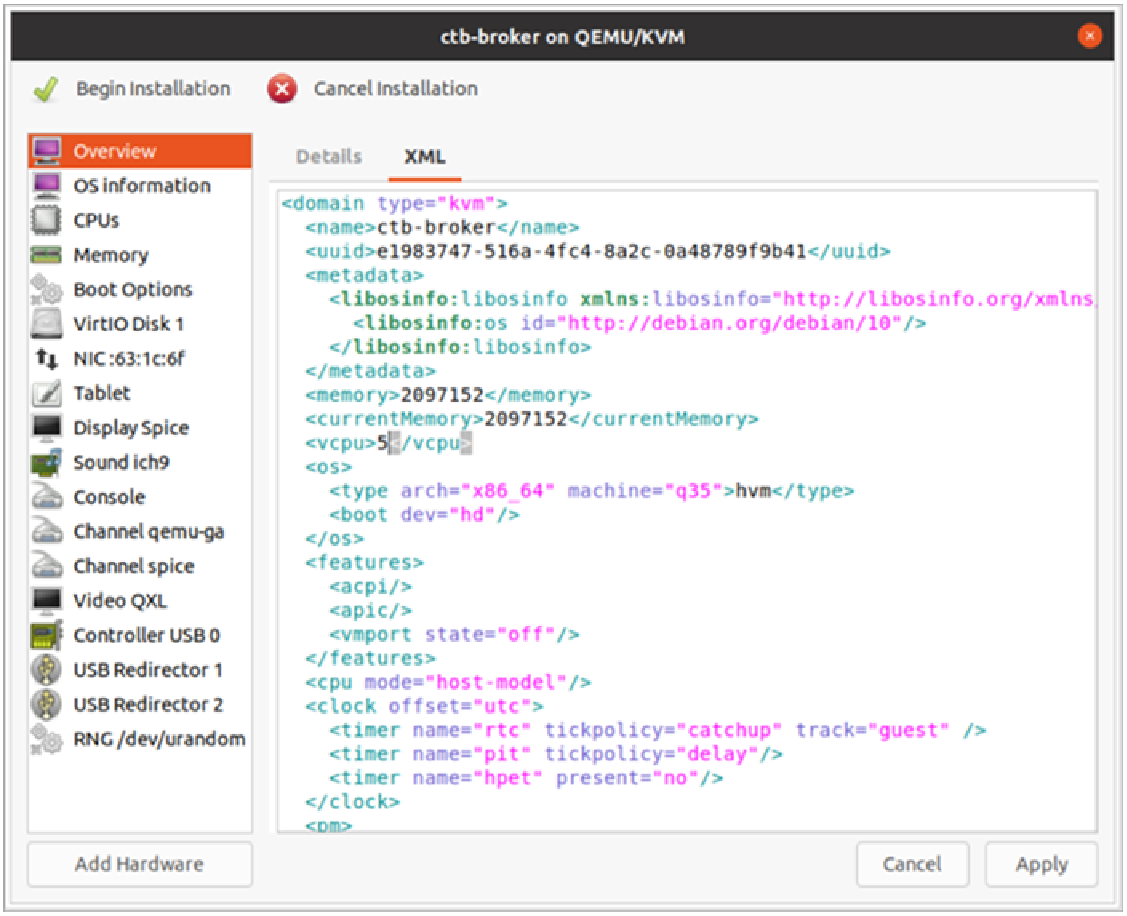
5. In Step 4 of the **Create a new virtual machine** dialog, do the following:
    a. In the Name field, enter **ctb-broker**.
    b. Check the **Customize configuration before install** check box.
    c. Click **Finish**.



6. Do the following:
    a. From the side menu, choose **Overview**.
    b. Click the **XML** tab.

c. Change the line `<timer name="rtc" tickpolicy="catchup"/>` to `<timer name="rtc" tickpolicy="catchup" track="guest"/>`

d. Click **Apply**.

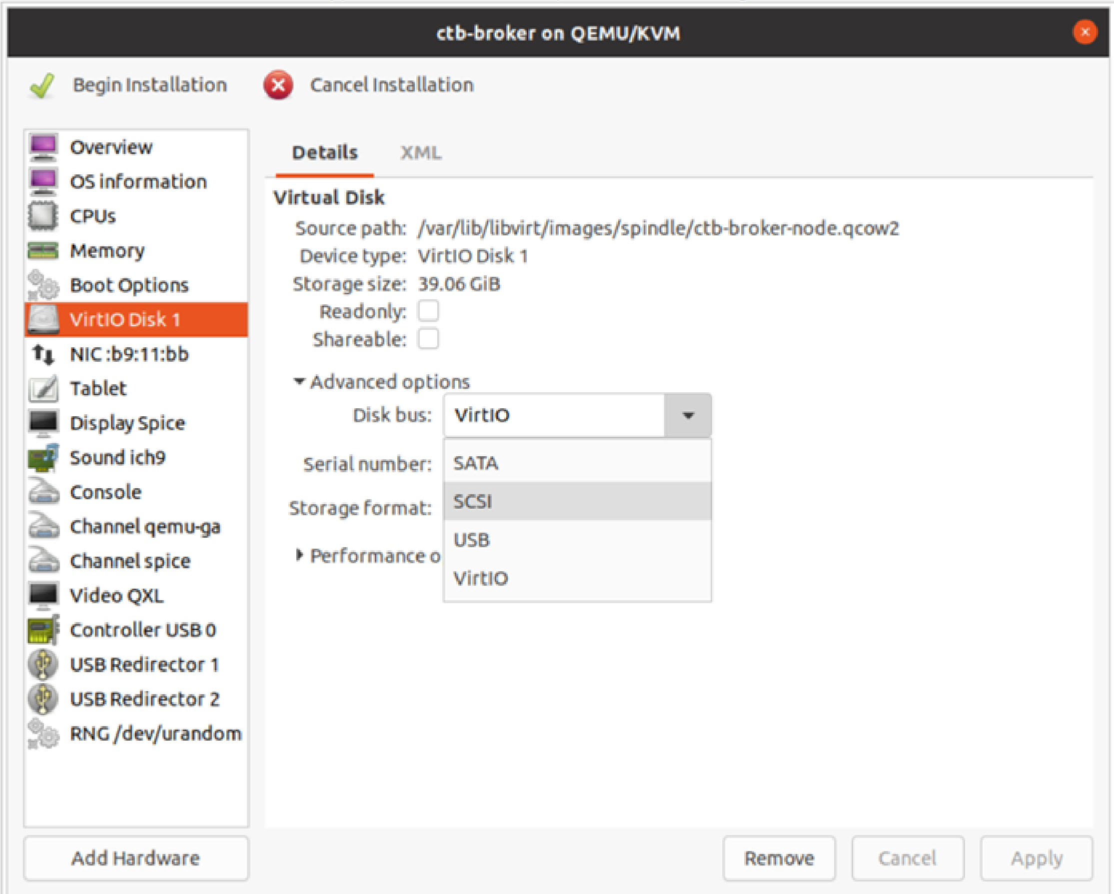


7. Do the following:

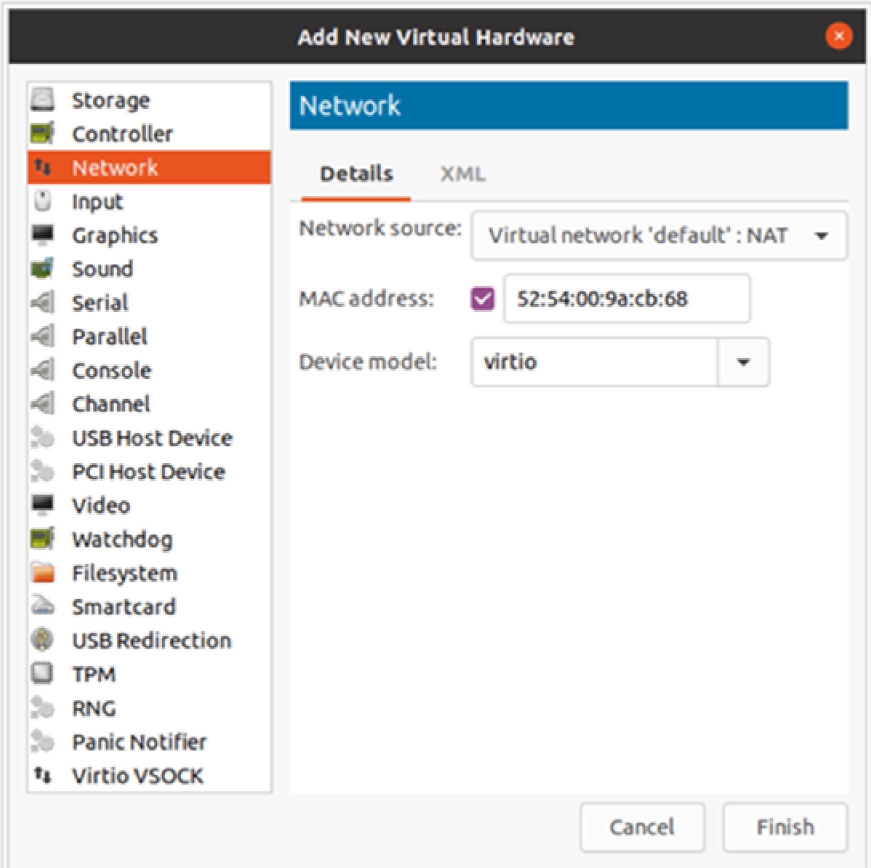
   a. From the side menu, choose **Virtiov Disk 1**.

   b. On the Details tab, in the Disk bus drop-down list, choose **VirtiO.**

   c. Click **Apply**.



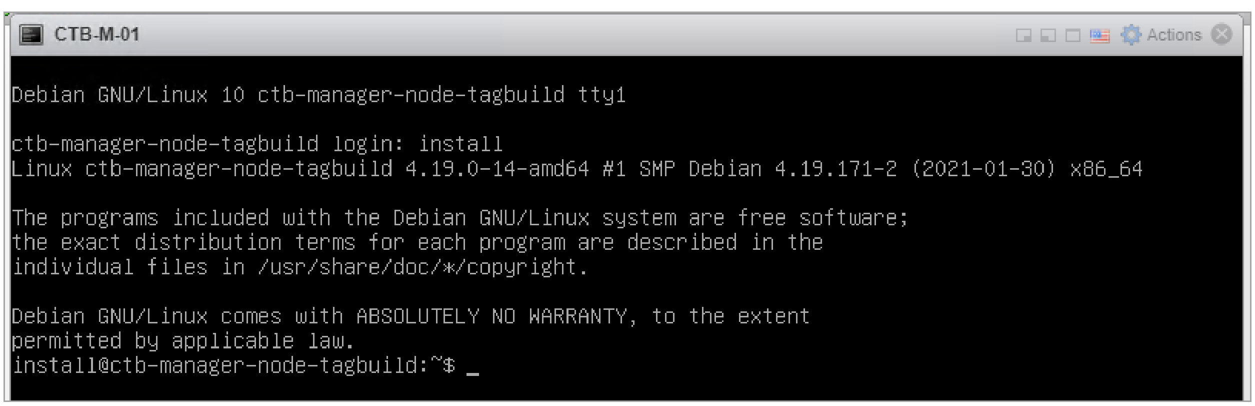
6. From the side menu, choose **Add Hardware > Network**. Click **Finish.**



7. Click **Begin Installation**.

3. Log In as the Install User

From the broker node virtual machine within the vmware user interface, open a web console and log in to the virtual machine (the username is **install**; there is no password).



4. Run the sudo ctb-install Command

1. Run the `sudo ctb-install` command.

2. Enter the following information:
    - Password for the **admin** user

      The password must meet the following requirements:
        - Contain at least 8 characters
        - Contain at least 1 lowercase letter
        - Contain at least 1 uppercase letter
        - Contain at least 1 digit
        - Contains at least 1 of these special characters: @ # $ % ^ & * ! + ?
        - Cannot be a commonly-used phrase or sequence
        - Cannot be similar to any identifying attributes of the user (such as the username)
    - IPv4 address, subnet mask, and default gateway address for the Management Network interface
    - Valid DNS nameserver IP address that are reachable from the virtual machine

5. Run the sudo ctb-manage Command

1. Run the `sudo ctb-manage` command.
2. Enter the following information:
    - IP address of the manager node
    - Username of the super user account you create in the manager node
    - Password of the super user account you create in the manager node

6. Logout

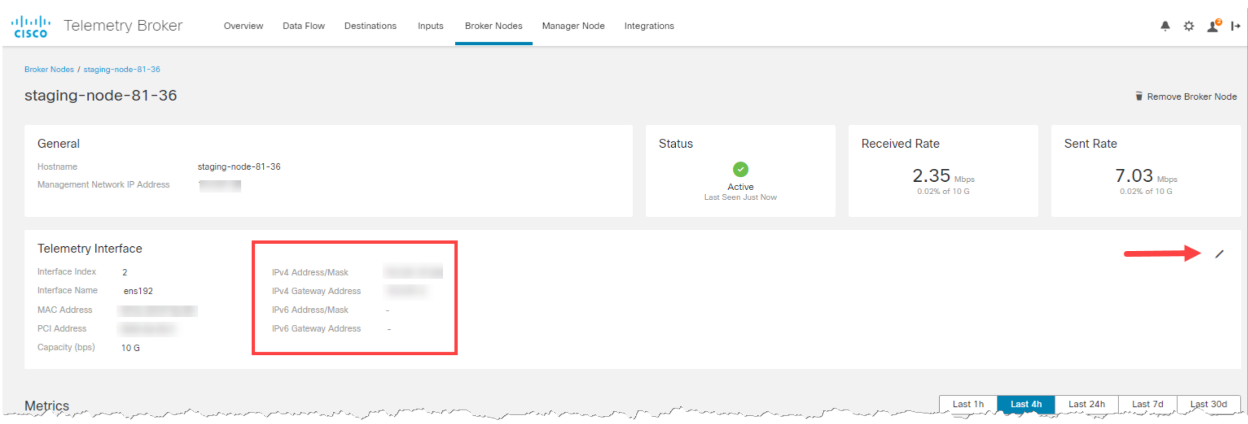
To log out, type `exit`.

7. Configure the Telemetry Interface

Go to **Configure the Telemetry Interface**.

Configure the Telemetry Interface

1. Log in to Cisco Telemetry Broker. In a web browser, enter the manager's management interface IP address and press **Enter** to navigate to the manager's web interface login.
2. From the main menu, choose **Broker Nodes**.
3. In the Broker Nodes table, click the applicable broker node.
4. In the Telemetry Interface section, click the **(Edit)** icon (indicated by the arrow in the following image).



5. Configure the IP and Gateway addresses (enclosed in red border).

Manage High Availability Clusters

Cisco Telemetry Broker high availability provides highly available IPv4 and IPv6 virtual IP addresses to be targets for your inputs, ensuring reliable delivery of telemetry from inputs to destinations.

To establish Broker Node high availability, you can create high availability clusters and assign multiple broker nodes to each. In each cluster, one broker node is designated *Active*, meaning it passes telemetry and serves metrics to Cisco Telemetry Broker, and the rest are designated *Passive*, meaning they are not passing telemetry or serving metrics currently. If an Active broker node stops passing telemetry or otherwise loses connectivity with Telemetry Broker, one of the Passive broker nodes is promoted to Active broker node and starts passing telemetry.

Note the following about clusters:

- Each broker node can only belong to one cluster at a time.
- You cannot choose which broker node is active in a given cluster.
- If an Active broker node for a Virtual IP address fails, one of the Passive broker nodes in the same cluster becomes the Active broker node for the Virtual IP address. When the failed broker node comes back up again, it remains a Passive broker node. If you want to make that node active again, you will need to do so manually using the provided commands.
- You can create a cluster with only one broker node, but if this broker node fails, no clusters within the broker node can be promoted to Active broker node. Similarly, if all broker nodes within a cluster fail, no broker node can be promoted to Active broker node. If a broker node fails, bring it back online as soon as possible.
- You can create a cluster with no broker nodes and add broker nodes later.
- You can assign either a virtual IPv4 or virtual IPv6 address, or both, to a cluster. Telemetry Broker uses this virtual IP address to communicate with the cluster and promote Passive broker nodes to Active broker nodes when an Active broker node loses connectivity with Telemetry Broker.

VIPs and Routing

High availability configures the VIP address broker node's Telemetry Network interface. Note that the Telemetry Network interface on each broker node in the cluster *must already be configured* with a primary IPv4 or IPv6 IP address, as well as with a subnet mask and a gateway. You can configure these in the Telemetry Network interface.

You must configure the IPv4 or IPv6 VIP IP addresses to be in the same subnet as the primary IP addresses in the cluster, since the VIP must be in the same subnet as well. This ensures proper routing via the preconfigured Gateway and fast failover.

If the VIP addresses are not in the same subnet as the primary IP addresses of the Telemetry Network interfaces, or if the Telemetry Network interfaces within a Cluster are configured with different subnets, then it is very likely that high availability will not work.

Manage Clusters

The Cisco Telemetry Broker implementation relies on two commonly used Linux packages to provide the underlying high availability infrastructure:

Corosync: This is the low-level cluster engine that provides the underlying communication between cluster nodes. It also provides the quorum capability to make the decision on the role of each node (Active or Standby).

Pacemaker: This is Cluster Resource Manager which manages all the relationships between the machines and the applications. It uses Corosync to communicate.

View Current Cluster Status

To view the current status of the cluster, including the status (Offline or Online) of each node and the location of the IPv4 VIP (vip4) and the IPv6 VIP (vip6) IP address, complete the following steps:

1. Log in as the **admin** to any of the broker nodes in the cluster from the console into the virtual machine provided by VMWare vCenter, or via SSH. Use the password that was supplied during node installation.
2. Run the `sudo crm_mon` command. This presents a view of the currently configured attributes on the cluster. You can see more details about this command here.
3. Exit the tool by pressing **Ctrl+C**.

```
Stack: corosync
Current DC: 10.0.81.31 (version 2.0.1-9e909a5bdd) - partition with quorum
Last updated: Tue Jan 26 16:16:24 2021
Last change: Tue Jan 26 15:45:04 2021 by root via cibadmin on 10.0.81.31

2 nodes configured
1 resource configured

Online: [ 10.0.81.31 10.0.81.32 ]

Active resources:

vip4    (ocf::titan:telemetry-vip):     Started 10.0.81.31
```

The previous image describes a cluster of two nodes, 10.0.81.31 and 10.0.81.32, which both have the status of *Online*. The IPv4 VIP (vip4) is currently running on 10.0.81.31. The IPv6 VIP (vip6) is not visible because it has not been configured.

If 10.0.81.31 failed, its status would look like this:

```
Stack: corosync
Current DC: 10.0.81.32 (version 2.0.1-9e909a5bdd) - partition with quorum
Last updated: Tue Jan 26 16:17:22 2021
Last change: Tue Jan 26 15:45:04 2021 by root via cibadmin on 10.0.81.31

2 nodes configured
1 resource configured

Online: [ 10.0.81.32 ]
OFFLINE: [ 10.0.81.31 ]

Active resources:

vip4    (ocf::titan:telemetry-vip):     Started 10.0.81.32
```

Notice how 10.0.81.31 is now shown as *OFFLINE* and the vip4 has moved to 10.0.81.32.

View Current Cluster Configuration

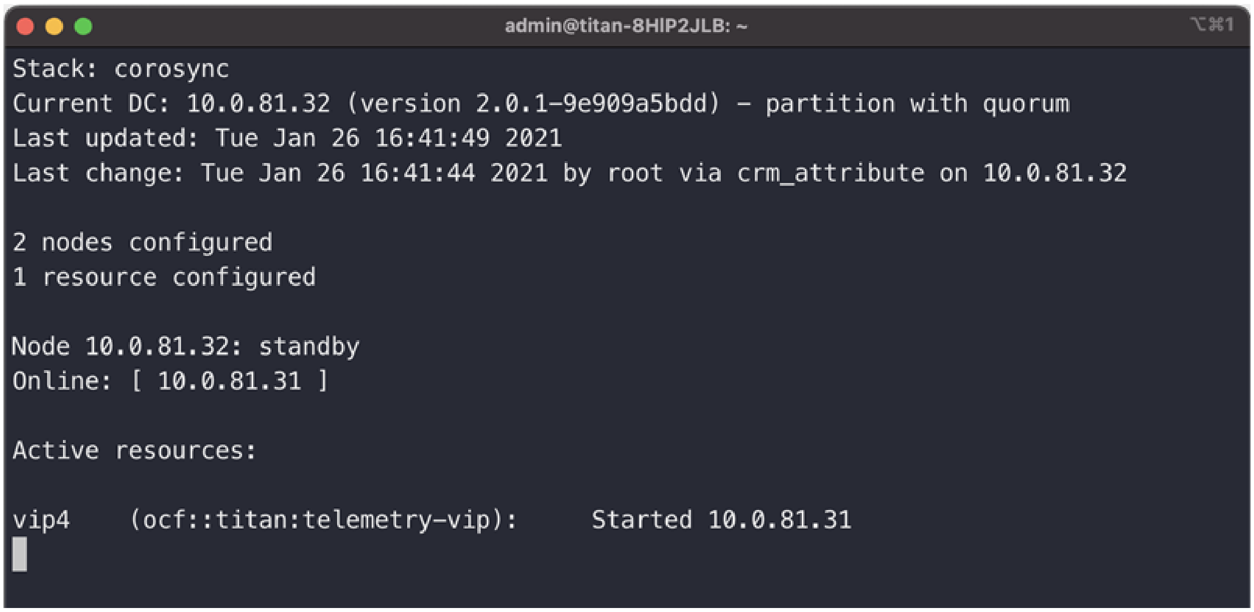
To view the current configuration of the cluster to verify that the Corosync and Pacemaker configuration is correct, complete the following steps:

1. Log in as the **admin** to any of the broker nodes in the cluster from the console into the virtual machine provided by VMWare vCenter, or via SSH. Use the password that was supplied during node installation.
2. Run the `sudo crm configure show` command. This presents a view of the currently configured attribute on the cluster. You can see more details about this command here.

Enable and Disable Node Standby Mode

In standby mode, the node cannot host the IPv4 or IPv6 virtual IP addresses.

1. Log in as the **admin** to any of the broker nodes in the cluster from the console into the virtual machine provided by VMWare vCenter, or via SSH. Use the password that was supplied during node installation.
2. Run the `sudo crm node standby 10.0.81.32` command. You can omit the node name if you are running this command on that node. You can see more details about this command here.
3. Run the `sudo crm node online 10.0.81.32` command to move the node out of *Standby* status. You can see more details about the command here.



As you can see, *crm_mon* displays the standby status of the 10.0.81.32 node.

Move a VIP to a Specific Node

You may encounter circumstances in which you want to specify which node is running the IPv4 or IPv6 virtual IP address. If so, complete the following steps:

1. Log in as the **admin** to any of the broker nodes in the cluster from the console into the virtual machine provided by VMWare vCenter, or via SSH. Use the password that was supplied during node installation.
2. Run the `sudo crm resource move vip4 10.0.81.32` command. You can see more details about this command here.
3. Run the `sudo crm resource unmove vip4` command to make sure the VIP stays on the targeted node, otherwise the VIP will move back to the node it was previously on (before the move) at the next opportunity.

Configure Your Virtual Machine to use a Physical NIC

We have pre-configured the ctb-node OVA file with a Telemetry Network interface using the vmxnet3 virtual driver. The vmxnet3 driver should work fine for workloads up to approximately 1Gbps, but it will begin to lag for workloads that exceed approximately 1 Gbps.

To support full 10Gbps telemetry, you need to configure your VM to use a physical NIC, which in VMWare is called VMDirectPath I/O passthrough. The Configuring VMDirect I/O pass-through knowledgebase article explains how to configure a physical NIC as a pass-through device.

After you set up the ESXi server with a passthrough device, complete the following to add it to the ctb-node VM:

1. After you import the OVA file, shut down the VM.
2. In the vSphere Client, right-click the **virtual machine** and click **Edit Settings**.
    a. Click **Add New Device**.
    b. Choose **PCI Device**.
    c. Choose the pci pass-through device you configured.
    d. To update the VM memory settings, check the **Reserve all guest memory (All locked)** check box.
    e. Click **OK**.
3. Start the VM and run through the install process as described above. After you enter your password you will be prompted to choose the **Management Network interface** and **Telemetry Network interface** from a list of three different NICs.
    a. Use the **82574L Gigabit Network Connection** NIC as the Management Network interface.
    b. Use the **pass-through NIC** as the Telemetry Network interface (the description will most likely say (*10Gbps*).

Your virtual machine is now running with a pass-through interface.

Enable Your Telemetry Broker License

Cisco Smart Licensing is a flexible licensing model that provides you with an easier, faster, and more consistent way to purchase and manage software across the Cisco portfolio and across your organization. And it's secure – you control what users can access. With Smart Licensing you get:

- **Easy Activation:** Smart Licensing establishes a pool of software licenses that can be used across the entire organization—no more PAKS (Product Activation Keys).
- **Unified Management:** My Cisco Entitlements (MCE) provides a complete view into all of your Cisco products and services in an easy-to-use portal, so you always know what you have and what you are using.
- **License Flexibility:** Your software is not node-locked to your hardware, so you can easily use and transfer licenses as needed.

To use Smart Licensing, you must first set up a Smart Account on Cisco Software Central (software.cisco.com).

For a more detailed overview on Cisco Licensing, got to cisco.com/go/licensingguide.

Assistance

For assistance with your Cisco Smart Account and Smart Licensing, please contact us through either of the following resources:

- Go to Support Case Manager at https://mycase.cloudapps.cisco.com/case and choose **Software Licensing** > **Security Related Licensing** as a case type.
- Call your TAC world-wide support number at https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html and open a licensing request.

Licensing Overview

After you deploy the manager, perform the following actions:

1. Create the initial super user account.
2. Create a Cisco Smart Account.
3. Open Smart Licensing in Telemetry Broker.
4. Review Evaluation Mode Status.
5. Register Your Product Instance.

If your Cisco Telemetry Broker does not have direct access to your Cisco Smart Account and will communicate through a Smart Software Manager On-Prem (also known as Transport Gateway), select **Transport Gateway** for your Transport Settings.

> Cisco Telemetry Broker requires Smart Software Manager On-Prem v8-202010 or higher.

Review the following On-Prem guide to complete the installation and configuration.

- **Smart Software On-Prem:**

  https://www.cisco.com/c/en/us/support/cloud-systems-management/smart-software-manager-satellite/tsd-products-support-series-home.html

1. Create the Initial Super User Account

When you use Cisco Telemetry Broker in Evaluation mode, you can use it for 90 days. Evaluation Mode is based on active usage of Cisco Telemetry Broker. For example, if you shut down Cisco Telemetry Broker, the countdown resumes when it is turned on again.

To use Cisco Telemetry Broker with maximum default functionality, and to add licenses and features to your account, register your product instance with your Smart Software Manager in Smart Licensing.

> Make sure you register your product instance before the 90-day evaluation period expires. When the evaluation period expires, Cisco Telemetry Broker stops receiving telemetry from inputs and sending telemetry to destinations. To resume functionality, register your product instance.

1. In a web browser, enter the manager's management interface IP address and press **Enter** to navigate to the manager's web interface login.
2. Enter your first and last names, email address, user name (we suggest assigning the user name of **webadmin** so as not to confuse it with the **admin** user), and password, and click **Create** to create the initial super user account.

2. Create a Cisco Smart Account

With a Cisco Smart Account, you can view your software, services, and devices in one portal (also known as Cisco Smart Software Manager).

To use Smart Licensing with Cisco Telemetry Broker, you must have a Cisco Smart Account. With a Cisco Smart Account, you can view your software, services, and devices in one portal (also known as Cisco Smart Software Manager).

For licensing Cisco Telemetry Broker, you will use your Smart Account to register your product instance, manage licenses, run reports, and configure notifications. For more information, refer to Smart Licensing on cisco.com.

- **Tutorials:** For video tutorials, refer to Smart Licensing Resources.
- **Instructions:** For detailed instructions about using your Cisco Smart Account, log in to your Cisco Smart Account. Click Help or use the online assistant.

3. Open Smart Software Licensing in Telemetry Broker

1. Log in to Cisco Telemetry Broker.
2. Click the ⚙ (**Global Settings**) icon in the toolbar in the upper right corner of any page and choose **Settings**.
3. Click the **Smart Licensing** tab.

4. Review Evaluation Mode Status

1. Open Smart Licensing in Cisco Telemetry Broker.
2. Click the **Global Settings** icon in the toolbar in the upper right corner of any page and choose **Settings**.
3. Click the **Smart Licensing** tab.
4. In the Smart Software Licensing Status section, review **Registration Status** and **License Authorization Status**.

	Status	Details
Registration Status	Unregistered	Your product instance is not registered to a Cisco Smart Account. Register your product instance before the evaluation period expires. When the evaluation period expires, Cisco Telemetry Broker stops receiving telemetry from inputs and sending telemetry to destinations. To resume functionality, register your product instance.

License Authorization Status	No Licenses in Use	After you have launched a Cisco Telemetry Broker deployment and it has started processing telemetry, it takes 24 hours for Cisco Telemetry Broker to calculate and report entitlement usage.
	Evaluation Mode	Your product instance is using Evaluation Mode and the number of days remaining is shown. To see more detailed information, hover your pointer over the status.

5. Register Your Product Instance

To use Smart Licensing with Cisco Telemetry Broker, you must have a Cisco Smart Account. With a Cisco Smart Account, you can view your software, services, and devices in one portal (also known as Cisco Smart Software Manager).

For licensing Cisco Telemetry Broker, you will use your Smart Account to register your product instance, manage licenses, run reports, and configure notifications. For more information, refer to Smart Licensing on cisco.com.

- **Tutorials:** For video tutorials, refer to Smart Licensing Resources.
- **Instructions:** For detailed instructions about using your Cisco Smart Account, log in to your Cisco Smart Account. Click Help or use the online assistant.

Use the following instructions in the order of the following steps to register your product instance before the evaluation period expires.

a. Log in to your Cisco Smart Software Manager.
b. Configure transport settings.
c. Create the registration token.
d. Register in Telemetry Broker.
e. (As Needed) Change product instance registration.

> ⚠ Make sure you register your product instance before the 90-day evaluation period expires. When the evaluation period expires, Cisco Telemetry Broker stops receiving telemetry from inputs and sending telemetry to destinations. To resume functionality, register your product instance.

a. Log in to Your Cisco Smart Software Manager

To use Cisco Telemetry Broker with maximum default functionality, and to access purchased licenses and features on your account, log in to your Cisco Smart Account and register your product instance with your Smart Software Manager in Smart Licensing.

1. Go to Cisco Software Central at https://software.cisco.com.
2. Click the (**User**) icon.
3. Log in with your CCOID credentials.
    - **Log In:** If you have an account, click **Log In**.
    - **Create an Account:** If you do not have an account, click **Create an Account**. Follow the on-screen prompts to set up your account.
4. In the License section, choose **Smart Software Licensing**.

b. Configure Transport Settings

Configure how Cisco Telemetry Broker communicates with your Cisco Smart Account (Cisco Smart Software Manager). If you change the configuration here, those changes will apply to Smart Call Home and other features using this service.

1. Log in to Cisco Telemetry Broker.
2. Click the **Smart Licensing** tab.
3. In the Smart Software Licensing Status section, locate **Transport Settings**.
4. Click **View/Edit**.

> If the product instance is already registered, deregister it before you change the transport settings. Refer to **Deregister** for details.

5. Select a transport setting.

Transport Settings	Description
Direct	Use this option if your Cisco Telemetry Broker has direct access to your Cisco Smart Account and it is not blocked by a firewall. Cisco Telemetry Broker lists the URL that Cisco Telemetry Broker will attempt to directly access.

Transport Gateway	If Cisco Telemetry Broker does not have direct access to your Cisco Smart Account and will communicate through Transport Gateway or Smart Software Manager On-Prem, choose **Transport Gateway**. In the URL field, enter the location of the Smart Software Manager On-Prem that contains the licenses for your product instance. **For Example:** https://<SSM-ON-PREM-URL>SmartTransport
HTTPS Proxy	This option is available only if you've configured Cisco Telemetry Broker to use a proxy. If so, you can choose the **HTTPS Proxy** option to tell Cisco Telemetry Broker to use the proxy for communicating with the Cisco Smart Licensing server. To configure the proxy, refer to the next section, **c. Configure the Internet Proxy**, for instructions.

6. Select **Save**.

c. Configure the Internet Proxy

To enable the HTTPS Proxy option for your Cisco Telemetry Broker Transport Settings, make sure your Internet Proxy is configured.

1. Log in to Cisco Telemetry Broker.
2. Click the **Global Settings** icon in the toolbar in the upper right corner of any page.
3. Click the **Use HTTPS proxy** Toggle icon to enable HTTPS proxy functionality (the icon bar will turn blue).
4. In the **IP Address** field, enter the proxy server IP address.
5. In the **Port** field, enter the port number Cisco Telemetry Broker uses to communicate with the proxy server.
6. Click **Save**.

d. Create the Registration Token

1. Log in to your Cisco Smart Account at https://software.cisco.com.
2. In the License section, choose **Smart Software Licensing**.

3. Select **Inventory**.
4. In the Product Instance Registration Tokens section, click **New Token**.
5. Complete the fields in the Create Registration Token dialog box to identify the token on your account and specify how it can be used.
6. Click **Create Token**.
7. Locate your token in the Product Instance Registration Tokens list.
8. **Copy the Token:** Click the token name and copy it, or choose one of the following:

    - **Copy:** To copy the token, click **Actions** > **Copy**
    - **Download:** To download the token as a text file, click **Actions** > **Download**.

e. Register in Cisco Telemetry Broker

1. Open Smart Licensing in Cisco Telemetry Broker.
2. Click **Register**.
3. Paste the token as plain text or type it into the Product Instance Registration Token window.
4. Click **Register**.

> If the communication times out during registration, review your transport settings.

5. Review the Smart Software Licensing Status section and confirm:

    - **Registration Status:** Registered
    - **License Authorization Status:** Authorized
    - **Out of Compliance:** If the status is shown as *Out of Compliance*, you may need to add licenses to your account. Refer to **Troubleshoot Licensing** for more information.

6. Review the Smart License Usage section. Confirm all licenses are shown as Authorized.
    - **Status Details:** Open Smart Licensing in Cisco Telemetry Broker and review Smart License usage to determine which licenses are out of compliance.
    - **Out of Compliance:** If any licenses are shown as *Out of Compliance*, you may need to add licenses to your account. Refer to **Troubleshoot Licensing** for more information.

f. (As Needed) Change Product Instance Registration

Use the following instructions to change or update your product instance registration with your Smart Software Manager in Smart Licensing.

Deregister

Use the following instructions to remove your product instance from your Cisco Smart Account. If you deregister your product instance, note the following:

- **Virtual Account Inventory:** The licenses it was using are returned to the virtual account, and other product instances in your account can use those licenses.
- **Evaluation Mode:** Your product instance will return to Evaluation Mode if there are days remaining in your evaluation period.

Use deregister before you change your transport settings or for troubleshooting.

1. Open Smart Licensing in Cisco Telemetry Broker.
2. Click **Actions**.
3. Select **Deregister**.

Reregister

If your product instance was disconnected or Cisco Telemetry Broker could not connect with the Cisco Smart Account after repeated attempts, the License Authorization Status shows *Registration Expired*. Use the following instructions to resolve any communication issues and reregister the product instance.

1. Open Smart Licensing in Cisco Telemetry Broker.
2. Check your Transport Settings and review your Cisco Smart Account to confirm communications.

> ⚠ If you need to change your transport settings, deregister your product instance first.

3. Click **Actions** > **Reregister**.
4. Log in to your Cisco Smart Account at https://software.cisco.com.
5. In the License section, choose **Smart Software Licensing**.
6. Select **Inventory**.
7. In the Product Instance Registration Tokens section, click **New Token**, or locate your token in the Product Instance Registration Tokens list.

8. Copy the token and paste it into the Product Instance Registration Token window in Cisco Telemetry Broker.
9. Click **Reregister**.
10. Review your Smart Software Licensing Status to confirm:
    - **Registration Status:** Registered
    - **License Authorization Status:** Authorized

Review Status and Usage

When you register your product instance with your Smart Software Manager in Smart Licensing, the Cisco Telemetry Broker Smart Licensing page shows your Cisco Smart Account and product instance details, including the following:

Product Instance Details

Information	Details
Registration Status	Refer to **Registration Status** for details.
License Authorization Status	Refer to **License Authorization Status** for details.
Export Control Functionality	Refer to the online help in your Cisco Smart Account.
Smart Account	Refer to the online help in your Cisco Smart Account.
Virtual Account	Refer to the online help in your Cisco Smart Account.
Product Instance Name	The Product Instance Name is the identifier we use for your Cisco Telemetry Broker product instance, which includes your Cisco Telemetry Broker Manager Node and broker nodes. Use your product instance name to identify your product instance in your Cisco Smart Account.
Transport Settings	Refer to Step 2 in the "Register Your Product Instance'" section in **Enable Your Telemetry Broker License** for details.

Registration Status

Cisco Telemetry Broker connects to your Cisco Smart Account and reports the licensing status and usage.

1. Open Smart Licensing in Telemetry Broker.
2. Review the Smart Software Licensing Status section.

Status	Details
Registered	Your product instance is registered and reporting license usage to your Cisco Smart Account. To see renewal and expiration details, hover your pointer over the status.
Unregistered	Your product instance is not registered to a Cisco Smart Account. Register your product instance before the evaluation period expires. Refer to "Evaluation Mode (90 Days)" and "Register your Product Instance" in **Enable Your Telemetry Broker License** for details.

License Authorization Status

Status	Details
Authorization Expired	If Cisco Telemetry Broker loses communication with your Cisco Smart Account, your authorization may expire. Authorization Expired indicates the communication status. It is does not indicate license status. To review license status (purchased, expired, and usage), review your Cisco Smart Account.
Authorized	Your product instance is registered and your licenses are authorized. To see authorization attempts and details, hover your pointer over the status.
Evaluation Period Expired	Your evaluation period has expired and telemetry processing has stopped. To see more detailed information, hover your pointer over the status. Refer to "Evaluation Mode (90 Days)" and "Register your Product Instance" in **Enable Your Telemetry Broker License** for details.
Evaluation Mode	Your product instance is using Evaluation Mode and the number of days remaining is shown. To see more detailed information, hover your pointer over the status. Refer to "Evaluation Mode (90 Days)" and "Register your Product Instance" in **Enable Your Telemetry Broker License**for details.
Out of Compliance	If there is a license shortage for Cisco Telemetry Broker, it is out of compliance. Refer to "Resolve Out of Compliance" in **Troubleshoot Licensing** for details.

Review Smart License Usage

Cisco Telemetry Broker reports license usage to your Cisco Smart Account.

If your Smart License status shows *Out of Compliance*, this indicates that Cisco Telemetry Broker has a license shortage and is using more licenses than are allocated in your Cisco Smart Account. Refer to the "Resolve out of Compliance" section in **Troubleshoot Licensing.**

Troubleshoot Licensing

Use the following instructions to resolve any license-related errors shown in Smart Licensing.

Resolve Out of Compliance

If the License Authorization Status or Smart License Usage shows *Out of Compliance*, an appliance or feature has a license shortage and is using more licenses than are allocated in your Cisco Smart Account.

Review your Licenses

Review the following:

- Open Smart Licensing in Cisco Telemetry Broker and review Smart License usage to determine which licenses are out of compliance.
- Confirm you have sufficient licenses assigned to your virtual account. Refer to your Cisco Smart Account for details.
- If you need to purchase additional licenses, please contact your account manager or the Cisco Telemetry Broker Sales team at stealthwatch-sales@cisco.com.

Update Cisco Telemetry Broker

After you add or move licenses to your virtual account, use the following instructions to update the status in Telemetry Broker.

Renew Authorization Now

Cisco Telemetry Broker reports license usage to your Cisco Smart Account. Use **Renew Authorization Now** to connect to your account and update your license usage telemetry immediately. Use these instructions if you've changed the licenses on your Cisco Smart Account, but they are not shown on your Smart Licensing page.

1. Open Smart Licensing in Cisco Telemetry Broker.
2. Click **Actions** > **Renew Authorization Now**.

Renew Registration Now

If your product instance was disconnected or Cisco Telemetry Broker could not connect with the Cisco Smart Account after repeated attempts, the License Authorization Status shows **Registration Expired**. Use **Renew Registration Now** to connect to your account and update your registration status.

1. Select the **Actions** menu.
2. Select **Renew Registration Now**.

   Registration Expired: If the License Authorization Status continues to show Registration Expired, you may need to reregister the product instance. Refer to "Reregister" in **Enable Your Telemetry Broker License** for details.

Review License Expiration Status

Your purchased licenses, allocations, expiration status, and usage are shown in your Cisco Smart Account. For more information, refer to "Cisco Smart Account" in **Enable Your Telemetry Broker License**.

Troubleshoot Cisco Telemetry Broker

General: Since the appliance is running a stock Debian 10 operating system, you can apply most general Linux system administration practices to troubleshooting.

Management Networking: The Management Network interface on the appliance is managed through the systemd-networkd service rather than the ifup, ifdown or ifconfig tools that you may be familiar with. After you have completed the installation of Cisco Telemetry Broker, you can find configuration information in this file:

/etc/systemd/network/management.network

Telemetry Networking: The Manager Node manages the Telemetry Network interface on the appliance. After installation, the Telemetry Network interface is mostly invisible to the operating system. Therefore, you must make configurations using the Cisco Telemetry Broker management layer.

Telemetry Packet Capture: Just as with configuration, you use a custom Cisco Telemetry Broker tool to capture packets on the Telemetry Network interface instead of operation system utilities. To do this, you must SSH to the appliance and run the following command:

```
$ sudo ctb-pcap -V -n 1000 -t 15 -s 10.203.3.3 -o test_tx_src.pcap
rx
```

This command writes the captured output to /var/lib/titan/pcap/test_tx_src.pcap. You can use the **–help** option to view all the available options.

Diagnostics: The appliance contains a diagnostic tool named *Mayday* that can capture debug information for the Cisco Telemetry Broker engineering team. You should include this helpful information to bug reports.

To create a diagnostic pack with *Mayday*, simply SSH to the appliance and run the following command:

```
sudo mayday
```

This will compile the relevant system information into a tar ball that can be copied off the node to another location using the SCP tool. The location of the resulting tar ball will be included in the Mayday logs.

Example:

```
$ ssh admin@<ctb-node-ip>

ctb-node> sudo mayday

<output-redacted>

2020/08/05 19:04:45 Output saved in /tmp/mayday-ctb-5SWVTpSx-
202008051904.677025165.tar.gz

2020/08/05 19:04:45 All done!
```

Finish Configuring Your System

To finish configuring your system, refer to the following sections in the Cisco Telemetry Broker User Guide:

- Destinations
- Inputs
- Broker Nodes

Contact Support

If you need technical support, please do one of the following:

- Contact your local Cisco Telemetry Broker Partner
- Contact Cisco Telemetry Broker Support
- To open a case by web: http://www.cisco.com/c/en/us/support/index.html
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers:
  https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Copyright Information

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)