Cisco Telemetry Broker

User Guide 1.0.0

TOC

Introduction

This guide provides a reference for the Cisco Telemetry Broker manager web interface.

Cisco Telemetry Broker allows you to ingest network telemetry from many sources, transform the data format, and forward that telemetry to one or multiple destinations.

Audience

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

Common Abbreviations

The following abbreviations appear in this guide:

Abbreviation	Description
DMZ	Demilitarized Zone (a perimeter network)
DNS	Domain Name Server
FC	Flow Collector
FS	Flow Sensor
FTP	File Transfer Protocol
Gbps	Gigabits per second
HTTPS	Hypertext Transfer Protocol (Secure)
ISE	Identity Services Engine
Mbps	Megabits per second
NAT	Network Address Translation
NIC	Network Interface Card
NTP	Network Time Protocol

Abbreviation	Description
PCIe	Peripheral Component Interconnect Express
SMC	Stealthwatch Management Console
SNMP	Simple Network Management Protocol
SPAN	Switch Port Analyzer
SSH	Secure Shell
TAP	Test Access Port
UDPD	UDP Director
UPS	Uninterruptible Power Supply
URL	Universal Resource Locator
USB	Universal Serial Bus
VLAN	Virtual Local Area Network

Destinations

Cisco Telemetry Broker sends telemetry to destinations. A destination is identified on the network by its IP address and the UDP port that it is listening on.

A rule describes the telemetry that a destination would like to receive from a particular telemetry stream. A destination may have multiple rules.

The Cisco Telemetry Broker Destinations page shows graphs of all your destinations. For each destination, you can see the following:

- Destination name
- IP address and port
- Telemetry received over the past day
- If the destination is actively receiving telemetry and reachable by the manager
- Data sources sending telemetry to the destination

From this page, you can add additional destinations as well as modify and update them. For each destination, you can add additional rules and receive telemetry from different data sources. You can configure multiple rules (1 data source per rule) per destination.

If you choose a destination, you can view more detailed information, including the following:

- Destination's display name, hostname, and IP address and port over which it receives Cisco Telemetry Broker
- Current destination status
- Number of rules to data sources
- Number of data sources from which this destination is receiving Cisco Telemetry Broker
- The current daily total of amount of data received

You can also view the following metrics related to this destination:

- The rules configured for this destination

You can view these metrics over several time frames:

- Last hour
- Last 4 hours
- Last day

- Last week
- Last month

View Destinations

Log in to Cisco Telemetry Broker. The Destination tab displays by default or choose **Destinations**.

Add a Destination

1. In the upper right corner of the page, click **+ Add Destination**.
2. Enter a destination **Name**.
3. Enter a **Destination IP Address** and **Destination UDP Port** for this destination.
4. Enable **Check Destination Availability** if you want to establish an inactivity interval between the manager node and the destination. This allows you to identify when a destination is nonresponsive or not receiving telemetry. See **General Settings** for more information.
5. Click **Save**.

Edit a Destination

1. On the Destinations tab, click the  (**Edit**) icon for a destination to edit its settings.
2. Update the **Name**, **IP Address**, **Port**, and **Check Destination Availability**.
3. Click **Save**.

Add a Rule for a Destination

1. On the Destinations tab, in the lower left corner of the applicable destination summary, click **+ Add Rule**.
2. Enter a **Receiving UDP Port**.
3. If you want to specify subnets over which this destination will receive certain traffic, add one or more **Subnets**.
4. Click **Save**.

Edit a Rule

1. On the Destinations tab, click a destination to view its detail.
2. Click the **Edit** icon.
3. Modify the **Receiving UDP Port** and **Subnets**.
4. Click **Save**.

Remove a Rule

1. On the Destinations tab, click a destination to view its detail.
2. To remove the rule, click the  (**Delete**) icon.

Importing and Exporting UDP Director Configuration

From either the UDP Director, or the Stealthwatch Management Console that manages the UDP Director, you can export your current UDP Director destination and rule configuration as an XML file and import it into Cisco Telemetry Broker.

> ⚠ Importing a UDP Director configuration overwrites your current Cisco Telemetry Broker configuration, including all currently configured destinations and rules.

Import Your UDP Director Configuration

To import your saved UDP Director configuration into Cisco Telemetry Broker, complete the following steps.

1. Log in to the Cisco Telemetry Broker manager node.
2. Click the ⚙ **(Settings) icon**.
3. Click the **Configuration** tab.
4. Click **Import Configuration**.
5. Click **Upload** to upload your saved XML configuration. Review the preview to ensure that this file contains your expected configuration.
6. Check the check box to confirm that you want to continue.
7. Click **Import**.

Export Your UDP Director Configuration From a UDP Director

To export a UDP Director configuration from a UDP Director, complete the following steps.

1. Log in to the UDP Director console as an **admin**.
2. Click the **Configuration** tab.
3. Click **Forwarding Rules**.
4. Choose **Export (Export the configuration file to local system)**.
5. Save the file to your workstation.

Export Your UDP Director Configuration From an SMC

To export your UDP Director configuration from a Stealthwatch Management Console (SMC), complete the following steps.

1. Log in to the SMC Web App as **sysadmin**.
2. Click the ⚙ **(Global Settings) icon**.
3. From the drop-down menu, choose **UDP Director Configuration**.
4. Click the **Actions** menu.
5. Choose **Export Forwarding Rules**.
6. Click **Save**.

View Destination Information and Metrics

1. Log in to the Cisco Telemetry Broker manager node.
2. Click the **Destination** tab.
3. Click a destination to view its detail.
4. Choose one of the following values to view metrics within that timeframe:
    - **Last Hour**
    - **Last 4 Hours**
    - **Last 24 Hours**
    - **Last 7 Days**
    - **Last 30 Days**

Dead Destination Detection

Dead Destination Detection is a feature of Cisco Telemetry Broker that alerts the operator to the unreachability of a destination so that they can mitigate any network damage caused by the forwarding of telemetry to a non-existent destination.

The feature crafts zero-length UDP packets and sends them to the configured UDP port of the destination. The broker nodes then listens for ICMP Host Unreachable or Port

Unreachable responses to determine if the destination is unreachable. The absence of any response indicates that the destination is most likely receiving telemetry.

You can disable this feature on a per destination basis.

Sources

On this tab you can view the number of rules configured for each source. It shows information about your telemetry UDP sources and AWS VPC Flow log sources, including the following:

- IP address and port used to send telemetry to Cisco Telemetry Broker
- Status, and last time it sent telemetry if it has not sent telemetry for a period
- Number of rules to destinations
- Bytes sent to Cisco Telemetry Broker and the rate (in bytes per second)

You do not need to explicitly configure the broker nodes to listen on particular UDP ports for telemetry. Cisco Telemetry Broker listens on every port and reports on everything that travels through the box over UDP. Therefore, you can simply configure sources to send their UDP telemetry to the address of the telemetry network interface on any of the broker nodes. On the Sources tab you can then see a list of those sources and the telemetry they are sending. If a source fails to send telemetry to Cisco Telemetry Broker for more than 15 minutes, you will receive a "No Data" warning.

You can configure the rules on this screen after you configure destinations. You must have at least one destination to configure a rule.

For information about the following, see AWS Configuration:

- Configure your AWS deployment to send Virtual Private Cloud (VPC) Flow Logs to Cisco Telemetry Broker.
- Configure Cisco Telemetry Broker to transform the VPC Flow Logs to IPFIX for ingestion by destinations.

View Data Sources

1. From the Cisco Telemetry Broker main menu, choose **Sources**.
2. Click the applicable tab to view a list of either the UDP sources or the VPC Flow log sources.

Broker Nodes

The Cisco Telemetry Broker Nodes Overview shows details about all of your broker nodes, including the following:

- Broker node name and IP address
- Telemetry interface IP address, speed, and traffic received and sent
- Broker node's status, and the last time the manager communicated with it
- Which high availability cluster it belongs to, if any

From here, you can add a broker node, remove a broker node, configure clusters, and configure a broker node's telemetry interface.

You can also choose a broker node to view detailed information about it, including the following:

- Traffic this broker node receives over time, per data source or total
- Traffic sent over time from this broker node to destinations
- CPU usage over time
- Memory consumption and total available memory
- Disk storage used and total available storage

You can view these metrics over several time frames by clicking the desired time frame in the upper right corner of the page:

- Last hour
- Last 4 hours
- Last day
- Last week
- Last month

View a Broker Node's Metrics

1. Choose **Broker Nodes**.
2. Click the broker node whose metrics you want to view.
3. Choose one of the following values to view metrics within that time frame:
    - **Last Hour**
    - **Last 4 Hours**

- **Last 24 Hours**
- **Last 7 Days**
- **Last 30 Days**

High Availability Clusters

Cisco Telemetry Broker high availability provides highly available IPv4 and IPv6 virtual IP addresses to be targets for your sources, ensuring reliable delivery of telemetry from sources 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 Cisco 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. (To view these commands, see the "Move a VIP to a Specific Node" section in the Cisco Telemetry Broker Virtual Appliance Deployment and Configuration Guide.)
- 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, then add broker nodes later.
- You can assign either a virtual IPv4 or virtual IPv6 address, or both, to a cluster. Cisco 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 Cisco Telemetry Broker.

Add a Cluster

1. From the Cisco Telemetry Broker main menu, choose **Broker Nodes**.
2. Click **Add Cluster**.
3. Enter a descriptive cluster name.

4. Choose one or more broker nodes to include in the cluster.
5. Enter a cluster virtual IPv4 Address, IPv6 Address, or both.
6. Click **Add Cluster**.

> It can take up to 3 minutes for the configuration to propagate and for the VIP addresses to become available on your network.

Modify a Cluster's Configuration

1. From the Cisco Telemetry Broker main menu, choose **Broker Nodes**.
2. In the Broker Node Name column, click the applicable broker node.
3. Click the **(Edit)** icon for a cluster.

Remove a Cluster

1. From the Cisco Telemetry Broker main menu, choose **Broker Nodes**.
2. In the Broker Node Name column, click the applicable broker node.
3. Click the **(Delete)** icon for a cluster and confirm your selection.

> For information about managing clusters, refer to the "Manage High Availability Clusters" section in the Cisco Telemetry Broker Virtual Deployment Guide.

Manager Node

The Cisco Telemetry Broker Manager view shows metrics for your Cisco Telemetry Broker manager. You can view the following information:

- the manager name, hostname, and IP address
- current manager status
- current memory use and total memory available
- current disk storage use and total disk storage space available

You can also view metrics related to your manager:

- Traffic this broker node receives over time, per data source or total
- Traffic sent over time from this broker node to destinations
- CPU usage over time
- Memory consumption and total available memory
- Disk storage used and total available storage

You can view these metrics over several time frames by clicking the desired time frame in the upper right corner of the Metrics section:

- Last hour
- Last 4 hours
- Last day
- Last week
- Last month

View Manager Information and Metrics

1. From the Cisco Telemetry Broker main menu, click **Manager Node**.
2. Choose one of the following values to view metrics within that time frame:
    - **Last Hour**
    - **Last 4 Hours**
    - **Last 24 Hours**
    - **Last 7 Days**
    - **Last 30 Days**

Integrations

The Cisco Telemetry Broker Integrations shows information about your VPC Flow Logs. You can configure your AWS deployment to export Virtual Private Cloud (VPC) Flow Logs to Cisco Telemetry Broker, then configure Cisco Telemetry Broker to transform the VPC Flow Logs to IPFIX for ingestion by destinations.

Below is a high-level overview of the integration process. You must complete the steps in the order shown below. The detailed steps for these sections are documented in the remaining pages of this section.

AWS Configuration - Part 1

1. Enable flow logging for one or more VPCs, then export the VPC Flow Logs to an S3 bucket.
2. Create an IAM user that has access to the S3 bucket, and record the access key ID and Secret access key.

Cisco Telemetry Broker Configuration - Part 1

1. Upload your AWS access and secret access keys to Cisco Telemetry Broker.
2. Configure the VPC Flow Log source, and upload the bucket policy to AWS.

AWS Configuration - Part 2

1. Create the S3 bucket policy.
2. Create a user group, assign the policy to an IAM group, then add your IAM user to the IAM group.

Cisco Telemetry Broker Configuration - Part 2

1. Complete your Data Source configuration, defining a broker node to process the VPC Flow Logs, and destinations to ingest the flow log information.

AWS Configuration - Part 1

Enable Flow Logging

To enable flow logging for one or more VPCs, then send the flow logs to an S3 bucket, complete the following steps.

1. From the AWS VPC main menu, choose **Your VPCs**.
2. Right-click a VPC, then choose **Create Flow Log**.

3. From the Filter drop-down,choose **All** to log accepted and rejected traffic, or **Accept** to log only accepted traffic.
4. Choose **Send to an S3 bucket destination**.
5. Enter an **S3 bucket ARN** in which you want to store flow log data.
6. Click **Create**.

Create an IAM User

To create an IAM user that has access to the S3 bucket and record the access key ID and Secret access key, complete the following steps.

1. From the AWS IAM main menu, choose **Users > Add user**.
2. Enter a **User Name**.
3. Choose **Programmatic access**.
4. Click **Next: Permissions**.
5. Click **Next: Tags**.
6. Click **Next: Review**.
7. Click **Create User**.
8. For both the access key ID and the secret access key, click **Show**.
9. Record your Access key ID and Secret access key or click **Download** and save the keys in a secure location.

Cisco Telemetry Broker Configuration – Part 1

Upload Your AWS Access

To upload your AWS access and secret access keys to Cisco Telemetry Broker, complete the following steps.

1. From the Cisco Telemetry Broker main menu, choose **Integrations > VPC Flow Logs**.
2. Click **Add AWS Credentials**.
3. Enter a descriptive **Credentials Name**.
4. Enter the **AWS Access Key ID** and **AWS Secret Access Key**.
5. Click **Save**.
6. If you have additional S3 credentials, repeat Step 1 through Step 5.

Configure the VPC Flow Log Source

To configure the VPC Flow Log source and upload the bucket policy to AWS, complete the following steps.

1. From the Cisco Telemetry Broker main menu, choose **Integrations > VPC Flow Logs**.
2. In the Credentials line item you just added, click **Add** in the **VPC Flow Logs** column.

   *The **Add VPC Flow Log** dialog opens.*
3. In the **S3 Bucket Path** field, enter this command:

   ```
   [bucket-name]/[path]
   ```
4. In the **Region Code** field, enter the AWS region where you created the S3 bucket.
5. Choose your **Credentials** based on the access key and secret access key that you uploaded.
6. Click **Policy to use** to expand the pane. Copy the S3 bucket policy and use if for S3 Bucket configuration in AWS.

AWS Configuration – Part 2

Create the S3 Bucket Policy

1. From the AWS IAM main menu, choose **Policies**.
2. Click **Create policy**.
3. Select the JSON tab.
4. Paste the policy you copied from Cisco Telemetry Broker into the JSON editor.
5. Click **Review policy**.
6. In the **Name** field, enter a unique name to identify the policy (for example, **ctb_policy**).
7. Enter a description, such as **Policy to allow Cisco Telemetry Broker access to VPC Flow Logs**.
8. Click **Create Policy**.

Create a User Group

To create a user group, assign the policy to an IAM group, and add your IAM user to the IAM group, complete the following steps.

1. From the AWS IAM main menu, choose **Groups > Create New Group**.
2. Enter the **group name**.
3. Click **Next Step**.
4. Select the Cisco Telemetry Broker policy that you created.
5. Click **Next Step**.
6. Click **Create Group**.
7. From the IAM console, choose **Groups > [Group Name]**.
8. Click the **Users** tab.
9. Click **Add Users to Group** and choose your **Cisco Telemetry Broker user**.
10. Click **Add Users**.

Cisco Telemetry Broker Configuration – Part 2

Define a Broker Node

To define a broker node to process the VPC Flow Logs and destinations to ingest the flow log information, complete the following steps.

1. In Cisco Telemetry Broker, in the **Add VPC Flow Log** dialog (refer to Step 2 in Configure the VPC Flow Log Source), enter a **Source Name**.
2. Enter a **Source IP Address**. This will be added as the source IP address for each VPC flow log sent to the destination.

   Cisco Telemetry Broker places the following restrictions on the Source IP value to ensure proper brokering of packets. If any of the following conditions are not met, Cisco Telemetry Broker displays an error message:

   - Source IP must **not** overlap with the subnet of the Assigned Node's telemetry interface.
   - Source IP must **not** conflict with any existing source IPs in the system.
   - Source IP must **not** conflict with any destination IPs in the system.

1. From the drop-down menu, choose an **Assigned Node**. This broker node will process all flow log data from the S3 bucket.
2. Choose one or more destinations to ingest the flow log data. Note that Cisco Telemetry Broker transforms VPC Flow Logs to IPFIX.
3. Click **Add VPC Flow Log**.

4. If you have multiple VPC Flow Logs to configure, complete the following steps, in order, for each VPC Flow Log you configure:
    a. Repeat every step in **Configure the VPC Flow Log Source** .
    b. Repeat every step in **Create the S3 Bucket Policy**.
    c. Repeat every step in **Create a User Group**.
    d. Repeat Step 1 through Step 5 in this section.

Application Settings

The Application Settings control your Cisco Telemetry Broker deployment. The following settings are available:

General Settings

Software Update

Smart Licensing

TLS Certificate

User Management

General Settings

Configure Inactivity Interval

The data sources configuration allows you to configure the amount of time before Cisco Telemetry Broker marks an data source as inactive.

Configure source inactivity interval

1. Click the ⚙ **(Settings)** icon.

   The Application Settings page opens.

2. Click the **General** tab.
3. Choose an **Inactivity Interval** in minutes from the drop-down list.
4. Click **Save**.

Configure HTTPS Proxy

The HTTPS Proxy configuration allows you to configure HTTPS proxy server settings if Cisco Telemetry Broker connects to the internet using an HTTPS proxy.

> ℹ Cisco Telemetry Broker does not support using HTTP proxy servers.

Configure HTTPS proxy settings

1. Click the **Settings** icon.

   The Application Settings page opens.

2. Click the **General** tab.
3. Enable **Use HTTPS proxy**.

4. Enter an **IP Address** and **Port**.
5. Click **Save**.

Software Update

The Software Update page shows the current Cisco Telemetry Broker version of your manager node and broker nodes, and allows you to upgrade to the current released version.

The update upgrades your manager and all of your managed broker nodes to the newest version. Before the update starts, the system creates a backup of your data. If an error occurs, the system restores the previous Cisco Telemetry Broker state. In this case, retry the update.

The system is unresponsive during update, and updates your manager first, then the broker nodes. While your manager updates, you may not see the proper state of your Cisco Telemetry Broker deployment. While your broker nodes update, they may not properly pass sent traffic to destinations.

Upgrade Your Cisco Telemetry Broker Deployment

1. Download the Update file from software.cisco.com.
2. In Cisco Telemetry Broker, click the ⚙ **(Settings)** icon.

   The Application Settings page opens.
3. Click the **Software Update** tab.
4. In the upper right corner of the page, click **Upload an Update File**.
5. Choose the file you downloaded in Step 1.

   You may need to wait several minutes for the upload to finish, based on the time estimates displayed. After the file is uploaded, you will receive a message informing you that a software update is now available.
6. Click **Update Cisco Telemetry Broker**.

   You will not be able to navigate within Cisco Telemetry Broker while the Manager node is updated to the latest version. The update process takes about 10 minutes.
7. When the update has completed, you will be prompted to log back in to Cisco Telemetry Broker.

   A loading indicator will appear next to each broker node that is being updated.

Smart Licensing

The Smart Software Licensing page shows the state of your Cisco Telemetry Broker Smart Licensing.

Cisco Telemetry Broker licensing is based on GB ingested by your broker nodes per day.

1. Click the ⚙**(Settings)** icon.

   The Application Settings page opens.

2. Click the **Smart Licensing** tab.

TLS Certificate

Upload TLS Certificate

1. Click the ⚙ **(Settings)** icon.

   The Application Settings page opens.

2. Click the **TLS Certificate** tab.
3. In the upper right corner of the page, click **Upload TLS Certificate**.
4. In the Upload TLS certificate dialog that opens, click **Choose File** for each certificate and each private key you want to upload.

   Certificate details are displayed beneath the associated files so you can verify that all related information is correct.

5. Click **Upload**.

Re-register Broker Nodes

After you upload the appropriate TLS certificates, you need to enable the connection between the Manager node and the broker nodes by re-registering each broker node.

1. Use SSH or the VM server console to log in to the appliance as **admin**.
2. Enter this command:

   ```
   sudo ctb-manage
   ```

   You are informed that a manager configuration already exists.

3. Choose **Option C "Re-fetch the manager's certificate but keep everything else"**.

User Management

Add a User

1. Click the ⚙**(Settings)** icon.

   The Application Settings page opens.

2. Click the **User Management** tab.
3. Click **Add User**.
4. Enter the user's **First Name** and **Last Name**.
5. Enter the **Username**. Neither you or the user can change this username once it is created.
6. Enter a password in the **New Password** field and enter it again in the **Confirm Password** field. Make sure to adhere to the password guidelines.
7. Click **Add User**.

Edit a User

1. Click the **Settings** icon.

   The Application Settings page opens.

2. Click the **User Management** tab.
3. In the row that contains the user you want to edit, click the ••• (**Actions**) icon > **Edit Profile**.
4. Complete your edits.
5. Click **Save**.

Remove a User

1. Click the **Settings** icon.

   The Application Settings page opens.

2. Click the **User Management** tab.
3. In the row that contains the user you want to remove, click the **Actions** icon > **Remove User**.
4. Click **Remove**.

Change a User's Password

1. Click the **Settings** icon.

   The Application Settings page opens.

2. Click the **User Management** tab.
3. In the row that contains the user whose password you want to change, click the **Actions** icon > **Change Password**.
4. Enter a new password in the **Password** field, and enter it again in the **Confirm Password** field.
5. Click **Change Password**.

Profile Settings

Edit Your Personal Information

1. Click the **(User)** icon.

   The Profile Settings page opens.

2. In the Personal Information section, click the (**Edit**) icon.
3. Complete your edits.
4. Click **Save**.

Change Your Password

1. Click the **User** icon.

   The Profile Settings page opens.

2. In the Password section, click **Change Password**.
3. Enter a new password in the **Password** field, and enter it again in the **Confirm Password** field.
4. Click **Change Password**.

Expand Cisco Telemetry Broker Manager Disk Size

1. Back Up the Partition Table Information

1. Log in to the appliance and run the following command.

   ```
   admin@ctb-nfik72TO:~$ sudo sgdisk -p /dev/sda
   ```

2. Copy the file in case you need it in the future. The contents of the file should look similar to the following:

```
Disk /dev/sda: 81920000 sectors, 39.1 GiB
Model: Virtual disk
Sector size (logical/physical): 512/512 bytes
Disk identifier (GUID): B078BED8-2BD0-4EEA-9149-BA93FC8A299D
Partition table holds up to 128 entries
Main partition table begins at sector 2 and ends at sector 33
First usable sector is 34, last usable sector is 81919966
Partitions will be aligned on 2048-sector boundaries
Total free space is 4029 sectors (2.0 MiB)

Number  Start (sector)    End (sector)  Size       Code  Name
   1            2048            4095   1024.0 KiB  EF02
   2            4096          491519   238.0 MiB   8300
   3          491520         3844095   1.6 GiB     8200
   4         3844096        33767423   14.3 GiB    8300
   5        33767424        63690751   14.3 GiB    8300
   6        63690752        81917951   8.7 GiB     8300
```

   The total size of the disk (/dev/ada) is 39.1 GB and the size of the Cisco Telemetry Broker application partition (/dev/sda6) is 8.7 GB.

2. Delete All Existing VM Snapshots for the Appliance

You cannot resize the ESXi VM disk when snapshots exist. In order to increase the disk size we need to delete all existing snapshots.

1. Log in to the ESXi console (vSphere or Web Client).
2. Right-click the VM and choose **Snapshots > Manage Snapshots > Delete All**.

3. Increase the Disk Size of the Appliance

1. Log in to the ESXi console (vSphere or Web Client).
2. From the list of VMs in the left panel, select the appliance.
3. From the toolbar at the top of the page, click the **Edit** icon.

4. In the Hard Disk 1 row, increase to the desired size.
5. Reboot the VM.
6. Log in and verity that the new size has been applied by running this command:

```
$ sudo sgdisk -p /dev/sda
Disk /dev/sda: 125829120 sectors, 60.0 GiB
Model: Virtual disk
Sector size (logical/physical): 512/512 bytes
Disk identifier (GUID): B078BED8-2BD0-4EEA-9149-BA93FC8A299D
Partition table holds up to 128 entries
Main partition table begins at sector 2 and ends at sector 33
First usable sector is 34, last usable sector is 81919966
Partitions will be aligned on 2048-sector boundaries
Total free space is 4029 sectors (2.0 MiB)

Number  Start (sector)    End (sector)  Size       Code  Name
   1            2048            4095   1024.0 KiB  EF02
   2            4096          491519   238.0 MiB   8300
   3          491520         3844095   1.6 GiB     8200
   4         3844096        33767423   14.3 GiB    8300
   5        33767424        63690751   14.3 GiB    8300
   6        63690752        81917951   8.7 GiB     8300
```

4. Run ctb-part-resize.sh Script

1. Take a snapshot of the VM.
2. Run the following command:

```
$ sudo /opt/titan/bin/ctb-part-resize.sh

WARNING

This program will update /dev/sda6 to use the full remaining free space
available on /dev/sda.

It is HIGHLY RECOMMENDED that you take a backup of any important data/configuration
before proceeding.

Do you wish to proceed?y
<134>Mar  8 15:35:30 ctb-disk-resize: Moving the partition table header to the end of the disk(/
Warning: The kernel is still using the old partition table.
The new table will be used at the next reboot or after you
run partprobe(8) or kpartx(8)
The operation has completed successfully.
<134>Mar  8 15:35:31 ctb-disk-resize: Deleting CTB application partition (/dev/sda6)
Warning: The kernel is still using the old partition table.
The new table will be used at the next reboot or after you
run partprobe(8) or kpartx(8)
The operation has completed successfully.
<134>Mar  8 15:35:32 ctb-disk-resize: Creating the CTB application partition (/dev/sda6)
Warning: The kernel is still using the old partition table.
The new table will be used at the next reboot or after you
run partprobe(8) or kpartx(8)
The operation has completed successfully.
<134>Mar  8 15:35:33 ctb-disk-resize: Updating kernel partition tables
<134>Mar  8 15:35:34 ctb-disk-resize: Resizing /dev/sda6
resize2fs 1.44.5 (15-Dec-2018)
Filesystem at /dev/sda6 is mounted on /var/lib/titan; on-line resizing required
old_desc_blocks = 2, new_desc_blocks = 2
The filesystem on /dev/sda6 is now 2412283 (4k) blocks long.
```

5. Verify that Space has been Allocated

Run the following command:

```
$ df -h /dev/sda
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda4        14G  5.6G  7.7G  42% /
/dev/sda2       227M   80M  132M  38% /boot
/dev/sda5        14G   41M   14G   1% /mnt/alt_root
/dev/sda6       8.5G  172M  7.9G   3% /var/lib/titan
```

Contact Support

For assistance with or questions about Cisco Telemetry Broker, contact support@cisco.com.

Copyright Information