

Best Practices and Troubleshooting Guide

vCenter Chargeback Manager 2.7.0

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see <http://www.vmware.com/support/pubs>.

EN-001576-00

vmware[®]

You can find the most up-to-date technical documentation on the VMware Web site at:

<http://www.vmware.com/support/>

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

Copyright © 2014 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About the Guide	5
1 Best Practices for Installing and Configuring vCenter Chargeback Manager	7
Best Practices for Installing vCenter Chargeback Manager	7
Best Practices for Adding vCenter Server in vCenter Chargeback Manager	9
Best Practices for Creating Database Users that vCenter Chargeback Manager Uses	9
Best Practices for Upgrading vCenter Servers Added to vCenter Chargeback Manager	10
Best Practice to Set External Network Received and Transmitted Values and Rates	10
2 Best Practices for Integrating vCloud Director with vCenter Chargeback Manager	13
Best Practices for Installing and Running Cloud Data Collectors	13
Best Practices for Configuring Cloud Data Collectors	14
Stats Migration Tool	15
3 Troubleshooting vCenter Chargeback Manager	17
vCenter Chargeback Manager Log Files	17
Troubleshooting Utility	19
Troubleshooting Issues in vCenter Chargeback Manager	19
Index	41

About the Guide

The *vCenter Chargeback Manager Best Practices and Troubleshooting Guide* provides information about various best practices for installing, configuring, and using VMware® vCenter Chargeback Manager. It also provides troubleshooting information for issues commonly encountered by users when installing, configuring, and using vCenter Chargeback Manager.

Intended Audience

This information is intended for anyone who wants to install, configure, and use vCenter Chargeback Manager. The information in this book is written for experienced system administrators who are familiar with Windows, VMware vSphere®, and basic database administration. vCenter Chargeback Manager 2.6 is the last enterprise version of the release. Chargeback Manager 2.7 is intended for use only by service providers under the terms and conditions of VMware Service Provider Partner (VSPP) Program. If you are a member of VSPP Program, locate your license key before proceeding.

Best Practices for Installing and Configuring vCenter Chargeback Manager

1

Following the best practices listed here helps ensure that you set up and use your vCenter Chargeback Manager environment in an efficient and secure manner.

This chapter includes the following topics:

- [“Best Practices for Installing vCenter Chargeback Manager,”](#) on page 7
- [“Best Practices for Adding vCenter Server in vCenter Chargeback Manager,”](#) on page 9
- [“Best Practices for Creating Database Users that vCenter Chargeback Manager Uses,”](#) on page 9
- [“Best Practices for Upgrading vCenter Servers Added to vCenter Chargeback Manager,”](#) on page 10
- [“Best Practice to Set External Network Received and Transmitted Values and Rates,”](#) on page 10

Best Practices for Installing vCenter Chargeback Manager

vCenter Chargeback Manager communicates with various servers and databases. It must be installed in an efficient manner to ensure that the resources are used correctly and the entire set up is secure.

Perform the following tasks before installing vCenter Chargeback Manager:

- Create a database for vCenter Chargeback Manager. Ensure that you provide sufficient database size or configure the database such that additional space can be provisioned as and when required.
- Ensure that the vCenter Server database and the vCenter Chargeback Manager database are not on the same database server.
- Ensure that the Chargeback Manager server and the database server locale are same. If you plan to install a separate data collector on a different machine, then the locale of the machine must be same with that of the Chargeback Manager server and the database server.
- Create a database user that vCenter Chargeback Manager and the data collector can use to connect to the database.

In Oracle Database, assign the following system roles and privilege to the user:

- CONNECT
- RESOURCE
- CREATE TRIGGER
- CREATE TABLE
- CREATE VIEW
- CREATE PROCEDURE
- CREATE SEQUENCE

In SQL Server, assign the privileges to the database user by running the following command:

```
CREATE ROLE CB_ADMIN_ROLE;
GRANT ALTER ON SCHEMA :: DBO TO CB_ADMIN_ROLE;
GRANT REFERENCES ON SCHEMA :: DBO TO CB_ADMIN_ROLE;
GRANT INSERT ON SCHEMA :: DBO TO CB_ADMIN_ROLE;
GRANT SELECT ON SCHEMA :: DBO TO CB_ADMIN_ROLE;
GRANT DELETE ON SCHEMA :: DBO TO CB_ADMIN_ROLE;
GRANT UPDATE ON SCHEMA :: DBO TO CB_ADMIN_ROLE;
GRANT EXECUTE ON SCHEMA :: DBO TO CB_ADMIN_ROLE;
GRANT CREATE TABLE to CB_ADMIN_ROLE;
GRANT CREATE VIEW to CB_ADMIN_ROLE;
GRANT CREATE PROCEDURE to CB_ADMIN_ROLE;
GRANT CREATE FUNCTION TO CB_ADMIN_ROLE;
GO
sp_addrolemember CB_ADMIN_ROLE, <db_username>
```

- Configure the machines on which you install the vCenter Chargeback Manager, vCenter Server, the corresponding databases, and the data collectors with the same time zone. Also, the date and time on all the machines must be synchronized. If the system time of the machines are not synchronized, then the data collectors might fail to process the chargeback-related events.

Synchronizing Time at Virtual Machine level for Windows machine

- 1 On a Windows virtual machine right click on the taskbar Date and Time option and select Adjust Date/Time from the pop-up menu.
- 2 Date and Time Properties screen is displayed. From the Internet Time tab select Automatically synchronize with an Internet server
- 3 Specify a local NTP server or an Internet NTP server and click **Apply**

Synchronizing Time at Virtual Machine level for Linux machine

- 1 Install NTP using the default package manager for that distribution
- 2 Ensure that you configure NTP to start on boot.
- 3 Edit `/etc/ntp.conf` to configure a preferred server for time syncing
- 4 Run `service ntpd start`

NOTE Please avoid the time sync option that is available as part of the VMware Tools. Ensure that all the setups that Chargeback integrates with (VCD, VC, vCOPS) and the respective backend Databases are time synced and are in the same time zone. Repeat the above steps for all the setups that interact with Chargeback.

Perform the following tasks when installing vCenter Chargeback Manager to create a secure setup:

- Install the load balancer in the DMZ perimeter of your network.
- Generate an SSL certificate.
- Install vCenter Chargeback Manager server, vCenter Chargeback Manager database, and data collectors in an internal secured network.
- Create an IPSec VPN tunnel between the DMZ and internal network. Define rules such that the load balancer can communicate with the vCenter Chargeback Manager server over the VPN tunnel. This will ensure that the communication between the load balancer and the vCenter Chargeback Manager server is secured.

Best Practices for Adding vCenter Server in vCenter Chargeback Manager

To obtain the resource utilization data for the virtual machines in a vCenter Server hierarchy, you must add the vCenter Server to vCenter Chargeback Manager.

Perform the following tasks to ensure that adding a vCenter Server to vCenter Chargeback Manager does not impact the functioning of the vCenter Server:

- Create a user in vCenter Server that vCenter Chargeback Manager can use to communicate with the vCenter Server.
- Create a clone of the Read only role in vCenter Server and add the following privileges to this role:
 - **Storage views.View**
 - **Global.Licenses**
 - **Extension.Register extension**
 - **Extension.Unregister extension**
 - **Extension.Update extension**
 - **Profile-driven storage.Profile-driven storage view**; if you are using vCenter Server 5.0
 - **Global.vCenter Operations User**; if you have integrated the vCenter Server with VMware vCenter Operations.
- Assign the cloned role with the additional privileges to the vCenter Server user on the root folder of the vCenter Server.
- Create a user in the vCenter Server database that data collectors can use to authenticate in to the database and fetch the relevant data. Ensure that this user has only read privilege in the database.
- When adding a vCenter Server to vCenter Chargeback Manager, do not use the Administrator vCenter Server user and the database user that vCenter Server uses to communicate with the vCenter Server database.
- Ensure that you register only one vCenter Chargeback Manager instance as a vSphere plug-in with a vCenter Server.
- After you add a vCenter Server to vCenter Chargeback Manager, the data collector synchronizes the data from the vCenter Server database in to the vCenter Chargeback Manager database if you have selected the **Enable Stats Replication** option. By default, the stats collection level is set to 1 in vCenter Server. With this level setting, the split utilization data for disk read and disk write, and network transmitted and network received cannot be fetched. To obtain this split utilization data, you must run a tool that modifies the stats collection level for these specific counters. See [KB 2010099](#) for further details.

Best Practices for Creating Database Users that vCenter Chargeback Manager Uses

vCenter Chargeback Manager provides data collectors that communicate with the vCenter Server database and vCloud Director database.

The vCenter Chargeback Manager data collector communicates with the vCenter Server database and replicates the necessary information in the vCenter Chargeback Manager database. The vCloud Director Data Collector communicates with the vCloud Director database and fetches the relevant information to integrate a vCloud Director instance with a vCenter Chargeback Manager instance.

These data collectors use a database user to authenticate in to the corresponding database and fetch the required information. These data collectors only read data from the corresponding databases and do not write any data in to them. Therefore, create separate users in these databases with only read privileges that the data collectors can use.

Best Practices for Upgrading vCenter Servers Added to vCenter Chargeback Manager

You can add one or more vCenter Servers, which are of the same version or different versions, to vCenter Chargeback Manager.

vCenter Servers added to vCenter Chargeback Manager can be upgraded to a higher version. However, you must perform the following tasks to ensure that the vCenter Chargeback Manager and the data collectors do not fail during the vCenter Server upgrade.

NOTE If you have registered vCenter Chargeback Manager as a vSphere plug-in for a vCenter Server, then after upgrading the vCenter Server the plug-in might not show the vendor name. This does not impact the functioning of the plug-in.

Procedure

- 1 If you have added only one vCenter Server to vCenter Chargeback Manager, then stop the data collector services.

If you have more than one vCenter Server added to vCenter Chargeback Manager, then stopping the data collector services is not recommended. In this case, the data collector fails to connect to the vCenter Server database during the upgrade and the corresponding jobs fail. However, after the vCenter Server is started post-upgrade, the data collector jobs are restarted automatically.

- 2 Upgrade the vCenter Server.
- 3 Check whether the vCenter Server service is running correctly post-upgrade.
- 4 Check whether the vCenter Server user used to add the vCenter Server to vCenter Chargeback Manager has the appropriate privileges.

You can obtain information about the required privileges from the *Add vCenter Server Information* section of the *vCenter Chargeback Manager User's Guide*.

- 5 Start the data collector services.
- 6 Check the **Data Collectors** page of the **Settings** tab in vCenter Chargeback Manager to see whether the data collector jobs are running successfully.

Best Practice to Set External Network Received and Transmitted Values and Rates

In Chargeback Manager, if you are generating a report on the vCenter Server hierarchy other than vCloud Director hierarchy, then the values and rates for External Network appear as 0 because Network Received and Transmitted information is derived from vCenter Server and External Network Transmit, Receive information is derived from vCloud VSM.

Procedure

- 1 Verify that you have selected the correct pricing model, the default Chargeback Manager pricing model does not work for vCloud Director report generation.
- 2 Verify the type of the Network Edge created in vCloud Director. Chargeback Manager can charge for virtual machines that are connected only to routed network or a vApp network.

- 3 Create routed Org vDC Networks.
 - a Navigate to **Home > Manage organization VDCs**.
 - b Double-click any Org VDC.
 - c On the **Org VDC Networks** tab, create a new Organization VDC Network by selecting **Create a routed network by connecting to an existing gateway**. Only when you select this option, the virtual machines are charged in Chargeback Manager.
- 4 Create a custom billing policy and a pricing model.
 - a Create a custom billing policy with the following rules.


```
external network transmit = usage;

external network receive = usage;
(optional) external network transmit rate = burstableutilization; (set this parameter if
you want the external network received and transmitted rates in the report)

(optional) external network receive rate = burstableutilization; (set this parameter if
you want the external network received and transmitted rates in the report)
other resources = usage or allocation (depending on the requirement);
```
 - b Create a custom pricing model with the billing policy that you have created. Set the required base rates for the required parameters on the **Base Rates** tab of pricing model.
 - c Generate the report on the vCloud Director hierarchy with the pricing model that you have created.

Both external network received and transmitted rates use burstableutilization for calculation purpose. Burstableutilization calculation works with 95 percentile method. By this method, chances to get the value as 0 is more if there is less network traffic for a virtual machine. A virtual machine should have more network activity (at least 12 hours) to reach to 95 percentile. For example, copying 1GB of data, repeating the same process for 15 times, and then generating one day report gives you some values for the external rates.

Best Practices for Integrating vCloud Director with vCenter Chargeback Manager

2

The best practices listed here help you integrate your vCloud Director setup with your vCenter Chargeback Manager instance in an efficient and secure manner.

This chapter includes the following topics:

- [“Best Practices for Installing and Running Cloud Data Collectors,”](#) on page 13
- [“Best Practices for Configuring Cloud Data Collectors,”](#) on page 14
- [“Stats Migration Tool,”](#) on page 15

Best Practices for Installing and Running Cloud Data Collectors

You must install and run the VMware vCloud Director Data Collector and the vShield Manager Data Collector to integrate your vCloud Director setup with your vCenter Chargeback Manager instance.

Perform the following tasks for successful installation and running of the cloud data collectors:

- Check whether vCenter Chargeback Manager has a valid license. If the license is empty or invalid, the data collectors cannot perform the jobs and keep failing till a valid license is added to vCenter Chargeback Manager.
- Ensure that the data collectors are reachable over the network. Preferably, install vCenter Chargeback Manager, vCenter Chargeback Manager database, vCloud Director, vCloud Director database, and all the data collectors on machines that are on the same network.
- Configure the machines on which you install the vCenter Chargeback Manager, vCenter Chargeback Manager database, vCloud Director, vCloud Director database, and all the data collectors with the same time zone. Also, the date and time on all the machines must be synchronized. If the system time of the machines are not synchronized, then the data collectors might fail to process the chargeback-related events.
- Install the vCloud Director Data Collector before you install the vShield Manager Data Collector.
- Provide the correct details for the vCloud Director database. Ensure the database user account provided has read privileges to fetch the necessary data from the vCloud Director database. After installation, you can verify the vCloud Director database information in vCenter Chargeback Manager from **Settings > Data Collectors > VMware Cloud Director**. The database details are required only if you integrate with vCloud Director 1.5 and vCloud Director 1.51
- Ensure that you provide the account information of a vCenter Chargeback Manager user with the Super User role when installing the vCloud Director Data Collector and vShield Manager Data Collector.

- After you install the vShield Manager Data Collector, you can see the vShield Manager instances in the vCenter Chargeback Manager in **Settings > Data Collectors > vShield Manager**. Ensure that the correct user name and password is provided for each vShield Manager instance by selecting the instance and clicking **Edit**. Else the data collector will not be able to collect the network statistics.
- You can install multiple instances of the vCloud Director Data Collector and vShield Manager Data Collector. However, only one instance of the cloud data collectors is used at any given time. The other installed cloud data collector instances are available and will be used only if the currently used data collector instance fails or is unreachable.
- If you have a vCloud Director installation which is more than a year old and you want it to be integrated with vCenter Chargeback, then you need to follow the process mentioned in the KB article <http://kb.vmware.com/kb/2007533>

Best Practices for Configuring Cloud Data Collectors

You must configure the VMware vCloud Director data collector and the vShield Manager data collector properly to ensure that the org vDCs are reflected in vCenter Chargeback Manager and their corresponding resource usage data can be obtained.

Perform the following tasks when configuring the cloud data collectors:

- Add all the vCenter Servers in your vCloud Director setup to vCenter Chargeback Manager. When adding a vCenter Server to vCenter Chargeback Manager, ensure that you provide the same vCenter Server URL that you used when configuring the vCenter Server in vCloud Director.

If the vCenter Servers are not added, vCenter Chargeback Manager cannot obtain the vCenter Server inventory information and the resource utilization data for the virtual machines in the vCenter Server inventory. Also, the virtual machines belonging to the org vDCs in your vCloud Director setup cannot be seen in the corresponding hierarchies in vCenter Chargeback Manager.

- Add vCenter Servers to vCenter Chargeback Manager before you add virtual machines to the org vDCs.

The virtual machines are reflected in the hierarchies in vCenter Chargeback Manager only after the first run of the data collector synchronization jobs are completed. As a result, only the resource utilization by the virtual machines after they are reflected in the vCenter Chargeback Manager hierarchies is accounted for during cost calculation.

- Ensure that at least one instance of the all the data collectors are running. The health of the data collectors can be monitored from the System Health tab of the vCenter Chargeback Manager. You can configure the Alert Settings to ensure that you are notified as soon as a vCenter Chargeback Manager component, including the data collectors, goes down.

The cloud data collectors process chargeback-related events and various different information from the vCloud Director setup and vShield Manager instances to the vCenter Chargeback Manager. If these data collectors are down, then some of the events that occurred during the data collector down-time might not be processed. Therefore, avoid changes to the inventory during the data collector down-time.

If the vCenter Chargeback Manager data collector fails and no other vCenter Chargeback Manager data collector instance is running, then the following issues might occur:

- During the data collector down-time, virtual machines that are created and deleted, that is, short-lived virtual machines, are not added to the vCenter Chargeback Manager hierarchy and, therefore, are not accounted for during cost calculation.

- Virtual machines that are created but not deleted during the data collector down-time are added to the hierarchy when the data collector is restored. However, the virtual machine resources are accounted for as follows:
 - For the vCloud Director configurations, vCPU count (allocation), memory (allocation), storage (allocation), network count (allocation) and DHCP/Firewall/NAT network services (allocation), virtual machines are charged properly from the time the virtual machines were created.
 - For the vSphere stats values, CPU (usage), memory (usage), disk I/O (usage), and network I/O (usage), virtual machines are charged properly from the time the virtual machines were created.
 - For the vSphere property values, vCPU count (usage), storage (usage), memory (size, reservation), CPU (reservation), and for pricing models with billing policy that accounts for the virtual machine power state, virtual machines are charged properly only from the time the data collectors restored.
- Virtual machines that are deleted during the data collector down-time, vCenter Chargeback Manager accounts for the virtual machines till the data collector is restored and not till the actual time of deletion.
- If the vCloud Director database is created in an Oracle RAC environment or if you want to use Windows Authentication for a vCloud Director database that is created on Microsoft SQL Server, you must use a well formed JDBC URL. However, if you provide a JDBC URL, the values for the VMware vCloud Director Database Host and VMware vCloud Director Database Name properties are ignored. You do not need to specify the vCloud Director database details if you integrate with a vCloud Director 5.1 setup.
- By default, the logging level for the cloud data collectors is set to the **warn** level. You cannot modify the data collector logging level from the vCenter Chargeback Manager. If you want more information in the logs, then you must set the logging level to **info**. The log levels must be changed in the `log4j.properties` file in the `Installation_Directory\classes` folder. You do not need to restart the data collector service after changing the logging level. The updated logging level is automatically reflected within 2 minutes of the change.
- If the password for the user account provided during the cloud data collector installation is changed, then you must notify this change to the cloud data collectors. You can update the password used by the cloud data collectors for this user by clicking the **Change password for '\$user' for cloud data collectors** link in **Settings > Data Collectors > VMware Cloud Director**.
- For VCD 5.1 and above, the chargeback events are not separately maintained by VCD, but they are the same as VCD audit events. You can configure the VCD Audit Events via Activity Log History from the VCD user interface. By default, VCD retains the audit events for 90 days.

Stats Migration Tool

Stats Migration Tool enables you to partition the unpartitioned Chargeback database performance stats table to a partitioned one without requiring you to do an application upgrade.

Stats Migration Tool allows you to partition the unpartitioned Chargeback database performance stats table to a partitioned one without requiring you to do an application upgrade. In the earlier version of Chargeback, this option was available only as a part of the Chargeback installer.

If you had to upgrade Chargeback from an earlier version to version 2.5 without opting for partition, then you did not have the option to enable the partition at a later stage, then you could partition the Chargeback database only if you opted for an upgrade of Chargeback from the exiting version to the 2.5 version. This tool is useful when you upgrade Chargeback Manager from 2.0 or 2.1 version to Chargeback Manager version 2.5, provided the Chargeback Manager database is not yet partitioned.

Prerequisites

Before starting the migration process, the Stats Migration tool performs the following pre-run checks.

- Check whether Chargeback Manager version is greater than or equal to 2.5, exit otherwise.
- Check whether the Chargeback vCenter Performance stat table is already partitioned.
- Run clean up script before starting a fresh migration process.

If the Chargeback Manager database is Oracle, you have to perform the following steps .

- Ensure that the Chargeback user has execute privilege on dbms_lock.
- Run the following command using sysdbaaccount to grant the DBMS_LOCK privilege

```
grant execute on DBMS_LOCK to %CBM_DB_USER%
where
```

%CBM_DB_USER% should be replaced by the name of CBM database user

NOTE This privilege is required temporarily to run the Stats Migration tool. After successful run of the tool, the privilege can be revoked.

Procedure to run the Stats Migration Tool

- 1 Go to the Chargeback Manager Installation directory and create a Stats Migration Tool folder within the vCenter Chargeback Manager Tools folder.

- 2 Copy the Stats Migration.zip files in the Stats Migration Tool folder.

Chargeback Installation Directory\vCenter-CB-Tools\Stats-Migration

where

Chargeback Installation Directory = Program Files\VMware\VMware vCenter Chargeback

- 3 Extract the Stats Migration.zip files inside the same folder
- 4 Navigate to the bin folder and run migrate-stats.bat
- 5 In the command prompt enter Y/y to start the Stats Migration process

On successful migration of the Chargeback vCenter Performance stat table, the following information is displayed on the user's console.

- Total time elapsed in xx hours: yy minutes :zz seconds format
- The message Migration is Successful

NOTE If the migration process fails, the original Chargeback vCenter Performance stat table will remain in a safe state. The log files of the Stats Migration process will be available at stats-migration\bin\statsmigration.log. You can download the Stats MigrationTool zip file from the Knowledge Base article [2053665](#).

Troubleshooting vCenter Chargeback Manager

3

VMware provides a troubleshooting utility and few troubleshooting tips for some of the common issues that you might face when installing and using vCenter Chargeback Manager.

This chapter includes the following topics:

- [“vCenter Chargeback Manager Log Files,”](#) on page 17
- [“Troubleshooting Utility,”](#) on page 19
- [“Troubleshooting Issues in vCenter Chargeback Manager,”](#) on page 19

vCenter Chargeback Manager Log Files

The components of vCenter Chargeback Manager have corresponding log files that include information about the various events that have occurred.

The [Table 3-1](#) table provides information about the log files and their locations for each vCenter Chargeback Manager component.

Table 3-1. vCenter Chargeback Manager Logs

Component	Log File Location	Log Files and Description
Installer	<i>Installation_Directory</i>	The VMware_vCenter_Chargeback_Install Log.log file provides information about the tasks performed and their corresponding status during the install process.
Load Balancer	<i>Installation_Directory\Apache2.2\logs</i>	Standard Apache log files.
vCenter Chargeback Manager server	<i>Installation_Directory\apache-tomcat\logs</i>	<ul style="list-style-type: none">■ Standard Apache Tomcat logs■ vCenterCB.log: Includes log information based on the log level set in the vCenter Chargeback Manager.■ vCenterCB_Errors.log: Includes log about errors occurred in the application, except authentication failures■ vCenterCB_Authentication_Errors.log: Includes log about authentication failures to the application

Table 3-1. vCenter Chargeback Manager Logs (Continued)

Component	Log File Location	Log Files and Description
vCenter Chargeback Manager Data Collector	<i>Installation_Directory</i> \DataCollector-Embedded\logs For stand-alone or individually installed data collectors, the log file location is as follows: <i>Installation_Directory</i> \DataCollector_ <i>Name</i> \logs	<ul style="list-style-type: none"> ■ vCenterDC.log: Includes log information based on the data collector log level. The default log level is INFO. ■ vCenterDC_Errors.log: Includes log about errors occurred in the data collector, based on the logging level set, including authentication failures.
VMware vCloud Director Data Collector	<i>Installation_Directory</i> \CloudDirector_ <i>DataCollector_Name</i> \logs	<ul style="list-style-type: none"> ■ vCloud-DC.log: Includes log information based on the data collector log level. The default log level is INFO. ■ vCloud-DC_Errors.log: Includes log about errors occurred in the data collector, based on the logging level set, including authentication failures.
vShield Manager Data Collector	<i>Installation_Directory</i> \vShieldManager_ <i>DataCollector_Name</i> \logs	<ul style="list-style-type: none"> ■ VSM-DC.log: Includes log information based on the data collector log level. The default log level is INFO. ■ VSM-DC_Errors.log: Includes log about errors occurred in the data collector, based on the logging level set, including authentication failures.

The maximum size of the vCenter Chargeback Manager log file, vCenterCB.log, is 50MB. After the log file reaches the 50MB size limit, the log file is rolled up. The maximum roll-up limit is of 10 log files. The rolled-up log files are compressed (ZIP) to save disk space.

The log level for the data collectors, include vCloud Director and vShield Manager data collectors, cannot be configured from vCenter Chargeback Manager. To modify the data collector logging level, you must configure the log4j.logger property in

Installation_Directory\DataCollector_*Name*\classes\log4j.properties file. The applicable values for this property are as follows:

- **ALL**: This level is intended to turn on all logging.
- **DEBUG**: This level designates fine-grained informational events that are most useful to debug an application.
- **ERROR**: This level designates error events that might still allow the application to continue running.
- **FATAL**: This level designates very severe error events that will presumably lead the application to abort.
- **INFO**: This level designates informational messages that highlight the progress of the application at coarse-grained level.
- **OFF**: This level is intended to turn off logging.
- **WARN**: This level designates potentially harmful situations.

You can additionally modify the following entries in the log4j.properties file to configure the number and size of the log files:

- **MaxFileSize**: Defines the maximum size of each log file. The default value is 50MB.
- **MaxBackupIndex**: Defines the maximum number of log files. The default value is 10.

You need not restart the data collector services after modifying any of the property values in the log4j.properties file. The changes are automatically picked up by the data collectors.

Troubleshooting Utility

vCenter Chargeback Manager provides a troubleshooting utility that is bundled with the application and can be used to collect event and system logs.

You must belong to the Administrators group to run the troubleshooting utility. The utility when run generates a ZIP file with the name `vCenter-CB-TroubleshootInfo-date.zip`. The size of the ZIP file can exceed up to 300MB. The ZIP file contains the following files:

- A `.csv` file for each table in the vCenter Chargeback Manager database schema that stores event-related information.
- The system logs, `Application.log` and `System.log`.
- Configuration files for the installer, vCenter Chargeback Manager (including the Apache Tomcat Server), data collectors, and the load balancer running of the machine on which you run the utility.
- Log files for the installer, vCenter Chargeback Manager (including the Apache Tomcat Server), data collectors, and the load balancer running of the machine on which you run the utility.

NOTE The troubleshooting utility does not collect files from remote machines. Also, the `.csv` file with the event-related information from the database is collected only if you run the utility on the machine on which the vCenter Chargeback Manager is installed.

You can run the troubleshooting utility by running the following command from the command prompt:

```
cd Installation_Directory\vCenter-CB-Tools\troubleshooting\bin
vCenterCB-support.bat
```

You can also run this utility by selecting **Collect vCenter Chargeback Manager Logs** from the **Start > Programs > VMware > VMware vCenter Chargeback > vCenter Chargeback Manager Tools** menu.

The logs are collected and archived, and the corresponding ZIP file is stored in `Installation_Directory\vCenter-CB-Tools\troubleshooting\collected_logs`.

Troubleshooting Issues in vCenter Chargeback Manager

VMware provides troubleshooting tips that enable you to fix or workaround some of the issues that might occur when installing and using vCenter Chargeback Manager.

Changed Timezone Setting Is Not Reflected

vCenter Chargeback Manager uses the timezone set on the machine. In the case of a cluster installation, the timezone set on the machine on which the load balancer service is running is used.

Problem

After the timezone is changed on the machine, the corresponding change is not reflected in vCenter Chargeback Manager.

Solution

- ◆ Restart the vCenter Chargeback Manager service for this change to be reflected.

Changes to Chargeback Hierarchy Are Not Reflected in the Concurrent User-Sessions

Multiple users can access a vCenter Chargeback Manager instance simultaneously. Changes made by a user are visible in concurrent user-sessions.

Problem

Creation, deletion, and renaming of a chargeback hierarchy by a user are not automatically reflected in the concurrent user-sessions. Any other change to the chargeback hierarchy, such as adding or deleting an entity, might not reflect immediately in the concurrent user-sessions.

Solution

- 1 Log out from vCenter Chargeback Manager.
- 2 Log in again to vCenter Chargeback Manager.

The changes made in the concurrent user sessions are reflected in vCenter Chargeback Manager.

- 3 Refresh the hierarchy to view the changes made to the hierarchy in the concurrent user sessions.

You can refresh a chargeback hierarchy by clicking the refresh button next to the chargeback hierarchy or by loading another chargeback hierarchy and then reloading the required chargeback hierarchy.

Changes to the vCenter Server Hierarchy Are Not Reflected in vCenter Chargeback Manager

Changes made to the vCenter Server hierarchy are not reflected in vCenter Chargeback Manager immediately.

Problem

Any change made to the vCenter Server hierarchy is not reflected in vCenter Chargeback Manager immediately.

Solution

- ◆ Click the refresh button next to the vCenter Server hierarchy in vCenter Chargeback Manager.

The refresh button is displayed only if there is a change in the vCenter Server hierarchy that is not reflected in the chargeback hierarchy.

The tab can be refreshed by user actions, such as clicking another tab of the application and then clicking the **Manage Hierarchy** tab.

NOTE In the case of a vCloud Director Org, the hierarchy changes are reflected every 10 minutes because the corresponding events are processed by the vCloud Director Data Collector every 10 minutes.

Data Collector Service Fails and Stops Automatically

Data collector service fail and stop and do not start automatically.

Problem

Data collector service fails and stops automatically. Also, the data collector does not start automatically.

Cause

The data collector is unable to connect to the database.

Solution

- 1 Check whether the database service is started and running.
- 2 Check whether the database is reachable over the network.
- 3 Check whether the database details are configured correctly on the data collector.

Check whether the database details, such as the database URL and database user name and password, are entered correctly for each data collector installed. These details can be configured from the **Data Collectors** page of the **Settings** tab.

- 4 If you have installed the data collector on a virtual machine, check whether VMware Tools is installed on the virtual machine.

The data collector service fails to start on a virtual machine if VMware Tools is not installed on the virtual machine.

- 5 Restart the data collector service.

You can also configure the **Alert Settings** in the **System Health** tab to ensure that you are notified through email as soon as a vCenter Chargeback Manager component fails and goes down.

Installer Throws the SQL Driver Not Found Error

When installing or upgrading vCenter Chargeback Manager, the installer throws an SQL driver-related error.

Problem

The vCenter Chargeback Manager installer fails and displays a Connection Failed error with the following message:

```
Reason for failure:SQL JDBC Driver not found.
```

Cause

You might be running the installer from a shared location on the network.

Solution

- 1 Copy the installer files on to the local machine.
- 2 Run the installer from the local machine.

The installer fails if run from a remote location. An alternative is to map the shared location of the installer to a network drive and then run the installer.

Network Statistics are not Included in the Reports

The network statistics for the entities in the vCloud Director hierarchy are not included in the reports generated in vCenter Chargeback Manager.

Problem

You have integrated your vCloud Director setup with vCenter Chargeback Manager by installing and configuring the vCloud Director Data Collector and the vShield Manager Data Collector. However, the reports generated on the vCloud Director hierarchy or any of its entities does not include the network statistics and corresponding cost.

Cause

This issue might occur due to multiple reasons.

- The date and time on the machines on which vCloud Director, vCenter Chargeback Manager, vCenter Server, the corresponding databases, and all the data collectors are installed are not synchronized.
- The vCloud Director database user account provided during vCloud Director Data Collector configuration does not have sufficient privileges to fetch the relevant data from the database.
- The user account details for the vShield Manager instances in vCenter Chargeback Manager are incorrect.

Solution

- 1 Synchronize the date and time on the machines on which you install vCenter Server, vCenter Chargeback Manager, vCloud Director, the corresponding databases, and all the data collectors.

All the machines must be configured with the same time zone. If the machines are not time synchronized, then some of the events might not be processed by the data collectors.

- 2 Ensure that the vCloud Director database user account provided when installing the vCloud Director Data Collector has sufficient privileges to read the chargeback-related events data from the vCloud Director Database.

If the events are not read and processed, the corresponding information is not available in the vCenter Chargeback Manager database.

- 3 After you install the vShield Manager Data Collector, ensure that all the vShield Manager instances are displayed in vCenter Chargeback Manager and the corresponding user account details are correct.
 - a In the **Settings** tab of the vCenter Chargeback Manager, click **Data Collectors**.
 - b Select the **vShield Manager** tab.
 - c Check whether all the vShield Manager instances are displayed on the page.
 - d Select a vShield Manager instance and click **Edit**.
 - e Verify whether the correct user name and password is provided.
 - f Repeat Step d and Step e for each vShield Manager instance displayed on the page.

Non-English Characters Are Not Correctly Stored in the vCenter Chargeback Manager Database

You can store data with non-English characters in the vCenter Chargeback Manager database.

Problem

The vCenter Chargeback Manager database might be deployed in a non-English locale or synchronized with a vCenter Server database that contains non-English data. However, the vCenter Chargeback Manager database does not store the non-English characters correctly. Therefore, this information is not displayed correctly in the application.

Cause

If you are using Oracle Database for the vCenter Chargeback Manager database, the character set configured on the database might not be supporting non-English data.

Solution

Configure the Oracle Database to use the Unicode (AL32UTF8) character set.

Report Does Not Display the Disk Read and Disk Write Information

A vCenter Chargeback Manager report displays the disk read and write information and the corresponding cost if the disk read and disk write computing resources are selected when the report is generated.

Problem

Although the disk read and disk write computing resources are selected when generating a report, the disk read and disk write information and the corresponding costs are not displayed in the report.

Cause

A probable reason might be that the statistics collection level is not properly set on the vCenter Server.

Solution

- ◆ To obtain this split utilization data for disk read and disk write, you must run a tool that modifies the stats collection level for these specific counters. See [KB 2010099](#) for further details.

By default, the stats collection level is set to 1 in vCenter Server. With this level setting, the split utilization data for disk read and disk write cannot be fetched.

Report Does Not Display the Network Transmitted and Network Received Information

A vCenter Chargeback Manager report displays the network bandwidth usage and cost information if the network transmitted and network received computing resources are selected when the report is generated.

Problem

Although the network transmitted and network received computing resources are selected when generating a report, the network bandwidth usage and cost information is not displayed in the report.

Cause

A probable reason might be that the statistics collection level is not properly set on the vCenter Server.

Solution

- ◆ To obtain this split utilization data for network transmitted and network received, you must run a tool that modifies the stats collection level for these specific counters. See [KB 2010099](#) for further details.

By default, the stats collection level is set to 1 in vCenter Server. With this level setting, the split utilization data for network transmitted and network received cannot be fetched.

Service Temporarily Unavailable Error

To access and use the vCenter Chargeback Manager, all the related services must be running.

Problem

When accessing vCenter Chargeback Manager, the Service Temporarily Unavailable error is thrown.

Cause

A probable reason might be that the relevant services are not running.

Solution

Check whether all the services related to the vCenter Chargeback Manager are running. Ensure that at least the load balancer and vCenter Chargeback Manager services are running. If you have just started the system or virtual machine on which vCenter Chargeback Manager is installed, you might have to wait for few minutes for the relevant services to start before accessing the application.

Status of Failed Data Collector Is Not Reflected Immediately on the System Health Tab

The System Health tab of the vCenter Chargeback Manager lets you monitor the overall system health. The tab shows the status of the various servers, databases, and data collectors.

Problem

If a data collector fails, the **System Health** tab of the vCenter Chargeback Manager does not show the status of the data collector as failed immediately.

Cause

The data collector heart beat is set to 30 seconds. If the data collector fails, vCenter Chargeback Manager waits for at least 90 seconds before updating the status of the data collector in the application. Therefore, the **System Health** tab does not reflect the failed status of the data collector immediately.

Solution

You can also configure the **Alert Settings** in the **System Health** tab to ensure that you are notified through email when a vCenter Chargeback Manager component fails and goes down.

Storage Synchronization Job Fails

The storage synchronization job run by the data collector fails.

Problem

The storage synchronization job of the data collector fails and the vCenter Server storage information is not synchronized in the vCenter Chargeback Manager database. The job state is reported as failed. This might result in the storage usage and corresponding cost reported as zero.

Cause

A probable reason might be that the VirtualCenter Management Webservices service is stopped. If you are using vCenter Server 5.0 Update 1b or later, then probably the VMware vSphere Profile-Driven Storage service is not running.

Solution

- 1 On the machine on which vCenter Server is installed, check whether the VirtualCenter Management Webservices service is started and running.

If you are using vCenter Server 5.0 Update 1b or later, then check whether the VMware vSphere Profile-Driven Storage service is started and running.

Ensure that the services are running for all the vCenter Server instances that are added to the vCenter Chargeback Manager. The service might fail to run due to port conflict with another service. The service uses port 8080 for HTTP communication and port 8443 for HTTPS communication by default. The default port for VMware vSphere Profile-Driven Storage service is 31000.

- 2 In vSphere Client, check whether the storage details are listed for the vCenter Server on the **Storage Views** tab.
- 3 Ensure that the **Storage views.View** permission is assigned on the root folder of the vCenter Server to the vCenter Server user, whose details are provided when adding the vCenter Server to vCenter Chargeback Manager.

If you are using vCenter Server 5.0 or later, then ensure that the **Profile-driven storage.Profile-driven storage view** permission is also assigned on the root folder of the vCenter Server to the vCenter Server user.

We recommend that you do not add a vCenter Server 5.0 or vCenter Server 5.0 Update 1 server to vCenter Chargeback Manager because of a known memory leak issue. Also, do not add a vCenter Server 5.0 Update 1a server because of a known upgrade issue in vCenter Server. If you have a vCenter Server 5.0, vCenter Server 5.0 Update 1, or vCenter Server 5.0 Update 1a server, then first upgrade this to vCenter Server 5.0 Update 1b and then configure it in vCenter Chargeback Manager.

Text and Messages on the vCenter Chargeback Manager User Interface Are Not Correctly Displayed

When accessing a vCenter Chargeback Manager instance that is installed on a non-English locale, the Web browser encoding must be set correctly.

Problem

vCenter Chargeback Manager is installed on a non-English locale and accessed by using a Web browser from an English locale. However, the texts on the application user interface and the messages displayed by the application do not appear correctly.

Cause

The Web browser encoding is not set correctly on the client machine.

Solution

Set the Web browser encoding to Unicode (UTF-8) on the client machine for the texts and messages to appear correctly in the user interface.

Unable to Access the vCenter Chargeback Manager

The vCenter Chargeback Manager services must be running for you to access the application.

Problem

Although you have provided the correct URL, you are unable to access the application.

Cause

The issue might occur due to multiple reasons.

- The application-related services are not started or not running.
- Windows Firewall is enabled on the machine on which vCenter Chargeback Manager and the load balancer is installed and running.

Solution

- 1 Check whether all the relevant services are running.

The following services must be started and running:

- VMware vCenter Chargeback Manager Service
- VMware vCenter Chargeback Manager Load Balancer Service
- VMware vCenter Chargeback Manager DataCollector

- 2 If Windows Firewall is enabled, ensure that port exceptions are added for the HTTP, load balancer, and HTTPS ports that are configured for vCenter Chargeback Manager during the installation.

Ensure that you set an inbound rule for these port. That is, allow access to the machine through these ports.

Unable to Add an LDAP Server

vCenter Chargeback Manager lets you configure one or more LDAP servers in the application.

Problem

When configuring the LDAP server in vCenter Chargeback Manager, an error is thrown and the operation fails. The error is similar to the following message:

An error occurred. Entity not found in LDAP server.

Cause

A probable cause is that you are adding a sever that is a child domain of a primary LDAP server and not provided the base DN.

Solution

If you are adding an LDAP server that is a child domain of a primary LDAP server, then you must specify the base DN. vCenter Chargeback Manager cannot automatically fetch the correct base DN in this case.

Unable to Add vCenter Server in vCenter Chargeback Manager

You must add a vCenter Server in vCenter Chargeback Manager before you can add entities from the vCenter Server to a hierarchy in vCenter Chargeback Manager.

Problem

When adding a vCenter Server to vCenter Chargeback Manager, the add operation fails.

Cause

The issue might occur due to multiple reasons.

- The vCenter Server is not running.
- The vCenter Server is not reachable on the network.
- The proxy settings on the Web browser are inappropriate.

Solution

- 1 Check whether the vCenter Server is started and running.
- 2 Check whether the vCenter Server is reachable over the network.
- 3 Check whether the proxy settings on the Web browser are correct.

If you have configured the proxy server settings on the Web browser and included the IP address of the vCenter Chargeback Manager machine in the bypass proxy list (No Proxy for or Exceptions), ensure that the complete IP address or the FQDN of the vCenter Chargeback Manager machine is entered in the list and not a partial address. For example, if the IP address of the machine is 90.0.1.1 and the host name is chargeserver, you must provide the full IP address and not 90.0.*.*, or the FQDN chargeserver.example.com.

Unable to Configure Alert Settings

In vCenter Chargeback Manager you can configure the alert settings to get email notifications as and when a component in your vCenter Chargeback Manager setup fails and goes down.

Problem

Although you have configured the SMTP server setting in vCenter Chargeback Manager, you get an error stating that SMTP server must be configured before you configure the alert settings on the **System Health** tab.

Solution

Refresh the System Health page by clicking the refresh icon on the page in vCenter Chargeback Manager.

Unable to Configure Another VMware vCloud Director Setup with vCenter Chargeback Manager

A vCenter Chargeback Manager instance can communicate with a VMware vCloud Director setup through the VMware vCloud Director Data Collector.

Problem

A VMware vCloud Director Data Collector is registered with vCenter Chargeback Manager for a VMware vCloud Director setup. However, you are unable to configure another VMware vCloud Director Data Collector with the same vCenter Chargeback Manager instance but different VMware vCloud Director setup.

Cause

A vCenter Chargeback Manager instance can communicate with only a single VMware vCloud Director setup. You can have multiple VMware vCloud Director Data Collector instances registered with this vCenter Chargeback Manager instance. However, each data collector instance must communicate with the same VMware vCloud Director setup. You can modify the VMware vCloud Director setup details in vCenter Chargeback Manager and the corresponding VMware vCloud Director Data Collector.

Solution

- 1 Stop all the VMware vCloud Director Data Collector instances.
- 2 Modify the host and database information for the VMware vCloud Director setup in the **VMware Cloud Director** tab on the Data Collectors page in vCenter Chargeback Manager.

You must modify the following properties:

- VMware vCloud Director database host
 - VMware vCloud Director database name
 - VMware vCloud Director database username
 - VMware vCloud Director database port
 - VMware vCloud Director database password
- 3 Delete all the hierarchies imported in to vCenter Chargeback Manager from the original VMware vCloud Director setup.

- 4 Run the following database commands.

```
delete from cb_vcloud_unprocessed_event
delete from cb_vsm_server
delete from cb_vsm_network
delete from cb_vsm_ip
delete from cb_server_property where
server_property_name='cbEventListRawView.lastProcessTime'
delete from cb_server_property where server_property_name like '%vclLastProcessTime-%'
```

- 5 Restart the VMware vCloud Director Data Collector instances.

This issue does not occur with vCloud Director 5.1.

Unable to Connect to the vCenter Chargeback Manager Database

vCenter Chargeback Manager can function only if it can connect to the vCenter Chargeback Manager database.

Problem

vCenter Chargeback Manager is unable to connect to the corresponding vCenter Chargeback Manager database. A database connection failed error is displayed.

Cause

This issue can occur due to multiple reasons.

- The database service is not started and running.
- The database is not reachable over the network.
- The port number for the SQL Server named database instance has changed.
- The number of server processes for the Oracle Database has exceeded the set maximum limit.

Solution

- 1 Check whether the database service is started and running.
- 2 Check whether the database machine is reachable over the network.
- 3 If you are using SQL Server for the vCenter Chargeback Manager database and using the port number of the named database instance to connect to it, ensure that the port is a dedicated or static port for the database instance.
 - a Modify the database configuration to use dedicated ports for the named database instances.
In SQL Server, the default configuration is to use dynamic ports for named database instances.
 - b Configure the database named instance with the formerly configured port number.
 - c Restart the database service and the vCenter Chargeback Manager services, including the data collector services.

- 4 If you are using Oracle Database for vCenter Chargeback Manager database, then you must set the maximum limit of server appropriately.

vCenter Chargeback Manager and each data collector registered with it connect to the vCenter Chargeback Manager database. In the case of a cluster installation the number of connections to the database is higher. To ensure the smooth functioning of vCenter Chargeback Manager, the Oracle Database must be configured to allow a larger number of server process to run.

- a In the Oracle Database, run the following command from the SQL prompt.

```
ALTER SYSTEM SET PROCESSES=NNN SCOPE=SPFILE;
```

Here, *NNN* is the maximum limit for server processes. The default value is 150.

- b Restart the Oracle Database service and the corresponding Oracle TNS Listener service.
- c Restart the vCenter Chargeback Manager and data collector services.

Unable to Connect to the vCenter Server Database

vCenter Chargeback Manager data collector must connect to the vCenter Server database to synchronize the vCenter Chargeback Manager database.

Problem

- The vCenter Chargeback Manager data collector is unable to connect to the vCenter Server database.
- vCenter Chargeback Manager is unable to connect to the vCenter Server database when adding the vCenter Server.

Cause

This issue can occur due to multiple reasons.

- The database service is not started and running.
- The database is not reachable over the network.
- The port number for the SQL Server named database instance has changed.
- TCP/IP protocol is not enabled for the vCenter Server database.
- The password for the database user is incorrect.

Solution

- 1 Check whether the database service is started and running.
- 2 Check whether the database machine is reachable over the network.
- 3 If you are using SQL Server for the vCenter Server database and using the port number of the named database instance to connect to it, ensure that the port is a dedicated or static port for the database instance.

In SQL Server, the default configuration is to use dynamic ports for named database instances. You must modify it to use dedicated ports. You must also configure the database named instance with the formerly configured port number. If you configure the database named instance with a different static port, ensure that you make the necessary changes in vCenter Chargeback Manager so that the connection to the vCenter Server database is restored.

- 4 If you are using SQL Server or SQL Express for the vCenter Server database, ensure that the TCP/IP protocol is enabled for the vCenter Server database.

The TCP/IP protocol is enabled by default. You can use the SQL Server Configuration Manager to check whether the TCP/IP protocol is enabled for the database.

Use the SQL Server Surface Area Configuration tool to ensure that the SQL Server Browser Service and Database Engine Service & Remote Connections services are running.

- 5 If the password for the vCenter Server database user is changed, the same must be updated in vCenter Chargeback Manager.

You can change the database user and password details from the **vCenter Servers** page of the **Settings** tab.

Do not use the vCenter Server database user account that vCenter Server uses to connect to the database.

Unable to Email Report

Although the report is generated and can be successfully archived or exported, the email report operation fails.

Problem

vCenter Chargeback Manager fails to send the report through email. The following error might be displayed:

Check if the email settings are properly configured. If not, configure them before sending an email.

Cause

Probable causes for the failure of the email report operation are:

- The SMTP server is not configured.
- The SMTP server is not reachable.
- A third-party application is blocking vCenter Chargeback Manager from sending email.

Solution

- 1 Check whether the SMTP server is configured in the application.

If the SMTP server is configured, then an email address is displayed in the **Email Setting** section of the General page of the **Settings** tab.

- 2 Check whether the SMTP server is reachable over the network.
- 3 Check whether any third-party application, such as an anti-virus application, is blocking vCenter Chargeback Manager from sending emails.

If there is such an application running and has the option of excluding some applications from being blocked, include the application `tomcat6.exe` in the excludes list.

Unable to Fetch the Primary Group of a LDAP User

Only the groups and users defined under the specified DN in the Active Directory hierarchy can be viewed from and added to vCenter Chargeback Manager.

Problem

Although you can view an LDAP user added to vCenter Chargeback Manager, you are unable to add the primary group of the LDAP user to the application.

Cause

A probable reason might be that the primary group does not come under the provided base DN.

Solution

Modify the base DN of the LDAP server added to the application such that the primary group is defined under it in the Active Directory hierarchy.

Unable to Log In to vCenter Chargeback Manager as an LDAP User

Logging in to vCenter Chargeback Manager by using an LDAP user account fails.

Problem

Although the LDAP Server is configured in vCenter Chargeback Manager, an LDAP user is unable to log in to vCenter Chargeback Manager.

Cause

The issue might occur due to multiple reasons.

- The LDAP user or group is not added to vCenter Chargeback Manager.
- vCenter Chargeback Manager is unable to communicate with the LDAP Server.
- The base DN of LDAP Server is changed in vCenter Chargeback Manager.
- The SSL Certificate for the LDAP Server has changed.
- The LDAP user name contains special characters.

Solution

- 1 Check whether the LDAP user or the LDAP group to which the user belongs is added to vCenter Chargeback Manager.

You can add and manage user from the **Users** page of the **Users & Roles** tab.

- 2 Ensure that the vCenter Chargeback Manager is able to communicate with the LDAP Server over the network.

Also check whether the LDAP Server is started and running correctly.

- 3 If the base DN for the LDAP Server is changed, then the LDAP users and group that are added to vCenter Chargeback Manager but do not exist in the LDAP hierarchy under the current base DN cannot log in to vCenter Chargeback Manager.

To enable log in for such users, you must modify the base DN for the LDAP server configuration in vCenter Chargeback Manager and might have to re-add these users and groups.

- 4 If you have enabled LDAPS (that is LDAP over SSL), you must have a valid SSL certificate for the LDAP Server on the vCenter Chargeback Manager machine.

If the SSL certificate for the LDAP Server is changed, then you must import the new SSL certificate on to the vCenter Chargeback Manager machine. To import the new SSL certificate, perform the following tasks:

- a Log in to vCenter Chargeback Manager as a super user.
- b Click **Settings**.
- c Click **LDAP Servers**.

A table listing the LDAP Servers configured in vCenter Chargeback Manager is displayed.

- d Select the LDAP Server for which you want to import the new SSL certificate and click **Edit**.

- e Enter the user name and password, and click **Save**.
Ensure that **Enable LDAPS** is selected.
A dialog requesting you to view and instal the new SSL certificate is displayed.
 - f Install the new SSL certificate.
- 5 If the LDAP user contains special characters in the user name, then to log in to vCenter Chargeback Manager as such a user, replace each special character with an underscore (_) in the user name.

Unable to Perform any Operation in vCenter Chargeback Manager

Any operation performed in vCenter Chargeback Manager fails with an error.

Problem

In an active user session, when any operation is performed in vCenter Chargeback Manager, the UI throws an error similar to the following:

An error has occurred. Please contact the administrator or try later.

Unable to log in to vCenter Chargeback Manager.

Cause

A probable cause could be that the database server on which the vCenter Chargeback Manager database is created has ran out of disk space.

Solution

Inform your system administrator or database administrator about the disk space issue.

Unable to Use Custom SSL Certificates

vCenter Chargeback Manager can be accessed through a Web browser using HTTPS protocol.

Problem

Prior to vCenter Chargeback 1.5, the application was shipped with a default SSL certificate that was generated using OpenSSL. However, to use a custom self-signed or CA signed SSL certificate or a wild card certificate for secure communication, you must replace the certificate related files in your installation directory.

Solution

- 1 Replace the security-related files, `default.cert` and `default.key`, with the custom SSL files.
The `default.cert` and `default.key` files are stored in the following directory:
Installation_Directory/Apache2.2/conf/ssl
You can use a custom CA signed SSL certificate or a wild-card certificate.
- 2 In the *Installation_Directory*/Apache2.2/conf/httpd.conf file, modify the SSL certificate file-related entries.

```
SSLCertificateFile conf/ssl/default.cert  
SSLCertificateKeyFile conf/ssl/default.key
```

In the above entries, replace the default security-related file names with the custom SSL file names.
- 3 Restart the vCenter Chargeback Manager service.

Starting with vCenter Chargeback 1.5, you can generate your own SSL certificate after installing the application. vCenter Chargeback uses this SSL certificate. You need not copy any files, if you generate an SSL certificate using the utility provided with the application. You can generate your own SSL certificates by using the **Generate SSL Certificate** option from the **Start > Programs > VMware > vCenter Chargeback Manager > vCenter Chargeback Manager Tools** menu.

Unable to Install Custom SSL Certificate With Certificate Chain

vCenter Chargeback Manager can be configured to use custom SSL certificates.

Problem

You have added a custom certificate to vCenter Chargeback Manager, but the application throws an error stating the certificate cannot be verified up to a trusted certification authority.

Cause

If you have a signed SSL certificate that requires the root certificate and intermediate certificates to be imported to verify the SSL certificate, then the entire certificate chain must be configured in the load balancer.

Solution

- 1 Replace the security-related files, `default.cert` and `default.key`, with the custom signed SSL certificate files.

The `default.cert` and `default.key` files are stored in the following directory:

Installation_Directory/Apache2.2/conf/ssl

- 2 Edit the `defaultchain.cert` file in the *Installation_Directory*/Apache2.2/conf/ssl folder by using a text editor.
- 3 Include the certificate content of the root certificate and the intermediate certificates in the correct order of the trust chain in the `defaultchain.cert` file.

Every certificate content is of the following form:

```
-----BEGIN CERTIFICATE-----
MIICpDCCAg2gAwIBAgIJAIq6Kgg0yj9MA0GCSqGSIb3DQEBBQUAMGsxCzAJBgNV
.....
yKARQOW12cu79r0RbwzT8bYQHx1pd/Dj7vZH0JPuKOS686v4AzzZE0VDkQGSnRWR
-----END CERTIFICATE-----
```

After you include the certificate content of the root and intermediate certificates in the `defaultchain.cert` file, the file contents should be similar to the following content:

```
-----BEGIN CERTIFICATE-----
Root certificate (Signed by third-party CA)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Intermediate Cert1
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Intermediate Cert2
```

```
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Intermediate Cert3
-----END CERTIFICATE-----
```

Ensure that the `defaultchain.cert` file does not include the certificate contents of the final signed SSL certificate of the certificate chain, that is, the contents of the `default.cert` file.

- 4 In the `Installation_Directory/Apache2.2/conf/httpd.conf` file, modify the SSL certificate file-related entries in the Virtual Host section.

```
SSLCertificateFile conf/ssl/default.cert
SSLCertificateKeyFile conf/ssl/default.key
SSLCertificateChainFile conf/ssl/defaultchain.cert
```

In the above entries, replace the default security-related file names with the custom SSL file names.

- 5 Restart the Apache load balancer, that is, the VMware vCenter Chargeback Load Balancer Service.

Unable to View the vCenter Chargeback Manager Plug-In in the vSphere Client

vCenter Chargeback Manager can be registered as a plug-in with a vCenter Server when you add the vCenter Server to the application. You can then access vCenter Chargeback Manager from the vSphere Client when you log in to the vCenter Server.

Problem

Although vCenter Chargeback Manager is registered as a plug-in when adding the vCenter Server to vCenter Chargeback Manager, the plug-in does not appear in the vSphere Client when accessing the vCenter Server.

Cause

This issue might occur due to multiple reasons.

- vCenter Chargeback Manager is not registered as a plug-in with the vCenter Server.
- The vSphere Client is unable to communicate with vCenter Chargeback Manager.
- The SSL certificate for the vCenter Chargeback Manager was not accepted on the vSphere Client.
- The vSphere Client was open and connected to the vCenter Server when the application was registered with the vCenter Server instance.
- You logged in to the vCenter Server by specifying `localhost` as the IP address of the vCenter Server.

Solution

- 1 Check whether the application has been registered as a plug-in with the vCenter Server.

This information can be obtained from the vCenter Servers page of the **Settings** tab of the application. The **Plugin Registered** column in the table on this page should have the value `true` for this vCenter Server. If the value is `false`, edit this vCenter Server entry and select the **Register As vSphere Client Plugin** option.

- 2 Check whether the vCenter Chargeback Manager service is running. Try accessing the vCenter Chargeback Manager through a Web browser from the machine on which the vSphere Client is installed.
- 3 Check whether the vSphere Client machine and the vCenter Chargeback Manager machine are on the same network domain.

- 4 Check whether the SSL certificate for the vCenter Chargeback Manager is installed on the vSphere Client machine.

After you register vCenter Chargeback Manager as a plug-in with a vCenter Server, when you log in to the vCenter Server by using vSphere Client, a Security Warning message is displayed for the SSL certificate. You must either install the certificate or click **Ignore** on the message window. If you click **Cancel**, you must restart the vSphere Client and accept the certificate.

- 5 Specify the IP address or DNS name of the vCenter Server machine when logging in using vSphere Client.

If the vCenter Server and the vSphere Client are on the same machine, then when you log in to the vCenter Server through the vSphere Client, you must specify the actual IP address or DNS name of the machine and not use localhost.

Upgrade Succeeded but Database Partitioning Failed

Upgrade to vCenter Chargeback Manager 2.5 succeeded. However, the installer log file shows that the database partitioning failed.

Problem

When you upgrade an existing vCenter Chargeback manager 2.0 or 2.0.1 setup, the installer checks whether the existing database supports database partitioning. If the database supports partitioning, the installer provides you with an option to partition the vCenter Chargeback Manager database. If you select the **Use database partitions** option, the installer runs scripts in the database to partition the database, create partition tables, and migrate the data.

You upgrade your existing setup to vCenter Chargeback Manager 2.5. The upgrade has succeeded. However, the install log shows error similar to the following:

```
Status: FATAL ERROR
Additional Notes: FATAL ERROR - Tue Sep 11 10:53:42 GMT 2012
FATAL ERROR - Db operation failed partitioning database
FATAL ERROR - com.microsoft.sqlserver.jdbc.SQLServerException: Duplicate range boundary values
are not allowed in partition function boundary values list. The boundary value being added is
already present at ordinal 6 of the boundary value list.
at com.microsoft.sqlserver.jdbc.SQLServerException.makeFromDatabaseError(SQLServerException.java:
196)
at com.microsoft.sqlserver.jdbc.SQLServerStatement.getNextResult(SQLServerStatement.java:1454)
at com.microsoft.sqlserver.jdbc.SQLServerStatement.processResults(SQLServerStatement.java:1083)
at
com.microsoft.sqlserver.jdbc.SQLServerCallableStatement.getOutParameter(SQLServerCallableStatemen
t.java:112)
at
com.microsoft.sqlserver.jdbc.SQLServerCallableStatement.getterGetParam(SQLServerCallableStatement
.java:387)
at
com.microsoft.sqlserver.jdbc.SQLServerCallableStatement.getValue(SQLServerCallableStatement.java:
393)
at
com.microsoft.sqlserver.jdbc.SQLServerCallableStatement.getInt(SQLServerCallableStatement.java:
437)
at
com.vmware.vim.vcenter.chargeback.installer.cbm.action.operation.module.installer.db.PartitionDat
abase.install(PartitionDatabase.java:78)
at com.zerog.ia.installer.actions.CustomAction.installSelf(DashoA10*..)
at com.zerog.ia.installer.InstallablePiece.install(DashoA10*..)
```

```

at com.zerog.ia.installer.InstallablePiece.install(DashoA10*..)
at com.zerog.ia.installer.GhostDirectory.install(DashoA10*..)
at com.zerog.ia.installer.InstallablePiece.install(DashoA10*..)
at com.zerog.ia.installer.Installer.install(DashoA10*..)
at com.zerog.ia.installer.actions.InstallProgressAction.n(DashoA10*..)
at com.zerog.ia.installer.actions.ProgressPanelAction$1.run(DashoA10*..)

```

This indicates that the database partitioning has failed.

Although the database partitioning has failed, vCenter Chargeback Manager and all the components, such as the load balancer and data collectors, run successfully. The database partitioning failure does not impact the functioning of vCenter Chargeback Manager and its components. The data collectors run successfully and synchronize the vCenter Chargeback Manager database with the vCenter Server databases.

Cause

This issue occurs if the data collectors have not synchronized the vCenter Chargeback Manager database with the vCenter Server database before the upgrade. That is the last successful run of the synchronization jobs was not in the recent past before the upgrade.

Solution

- 1 Stop the vCenter Chargeback Manager service.
- 2 Stop all the data collector services.
- 3 Take a backup of the vCenter Chargeback Manager database.
- 4 Ensure that enough free space is available for data migration and for the log files.

You can use the following guidelines for the data and log space:

- Free space of at least 1.25 times the current data size is available in the database.
- The logs are configured with unrestricted growth mode. Else ensure that you have provided sufficient space for the logs to grow.

We have observed the logs to grow by 20GB when migrating the vCenter Chargeback Manager database with 100 million rows in our test environment.

- 5 Log in to the vCenter Chargeback Manager database.

Log in as a database administrator or as a user with at least the required privileges. The privileges required by the database user are listed in the *Database Management Prerequisites* section of the *vCenter Chargeback Manager Install and Upgrade Guide*.
- 6 Run the CB_MIGRATE_DATA procedure.

The procedure creates partition tables and migrate the data to the new tables. The time taken for the procedure to partition the database and migrate the data depends on the data size and the memory allocated to the database management system. Preferably, ensure that the changes in the vCenter Server inventory is minimal during the time when the procedure is run in the vCenter Chargeback Manager database.
- 7 If the procedure is successfully completed, start the vCenter Chargeback Manager service and the corresponding load balancer and data collector services.
- 8 Check whether the data collector jobs are running and at least one run of all the data collector jobs is successfully completed.

If you do not want to partition the database and use it as is after the upgrade, then ensure that you remove the `data_migration_in_progress` property from the `CB_SERVER_PROPERTY` table in the vCenter Chargeback Manager database. Else, you cannot generate reports (both scheduled and on-demand) in vCenter Chargeback Manager for 3 days from the time the upgrade was started.

vCenter Chargeback Manager Sends Packets to Unknown Network

vCenter Chargeback Manager sends packets with an unknown destination IP.

Problem

Packets with unknown destination IP are detected in the network. These packets might be originating from vCenter Chargeback Manager.

Solution

Check whether the IP address is same as the multicast address configured in the Apache Tomcat server (the vCenter Chargeback Manager load balancer). This address is configured in the `server.xml` file in `<Installation_Directory>\apache-tomcat\conf\`

If the address is same as the mutlicast address, you can configure the mutlicast address as per your network requirements. You must restart the load balancer after changing the multicast address. The multicast service must run for the load balancer to function correctly.

Virtual Machines are not Displayed in the Imported vCloud Director Hierarchies

Some or all of the virtual machines in the vCloud Director hierarchy are not displayed in vCenter Chargeback Manager.

Problem

You have integrated your vCloud Director setup with vCenter Chargeback Manager by installing and configuring the vCloud Director Data Collector and the vShield Manager Data Collector. However, the virtual machines in the vCloud Director hierarchy are not displayed in the corresponding hierarchy imported in to vCenter Chargeback Manager.

Cause

This issue might occur due to multiple reasons.

- vCenter Servers configured in vCloud Director are not added to vCenter Chargeback Manager.
- The URL used to add vCenter Server to vCenter Chargeback Manager is different from the one that was used to configure the vCenter Server in vCloud Director.
- The vCloud Director database user account provided during vCloud Director Data Collector configuration does not have sufficient privileges to fetch the relevant data from the database.
- The date and time on the machines on which vCloud Director, vCenter Chargeback Manager, vCenter Server, the corresponding databases, and all the data collectors are installed are not synchronized.

Solution

- 1 Add all the vCenter Servers configured in vCloud Director to vCenter Chargeback Manager.

If the vCenter Servers are not added, the data collectors cannot fetch the inventory information from the vCenter Server databases.

- 2 Ensure that you use the same vCenter Server URL in vCloud Director and vCenter Chargeback Manager.

When adding the vCenter Servers to vCenter Chargeback Manager, you must use the same URL that you provided when configuring the vCenter Servers in vCloud Director.

- 3 Ensure that the vCloud Director database user account provided when installing the vCloud Director Data Collector has sufficient privileges to read the chargeback-related events data from the vCloud Director Database.

- 4 Synchronize the date and time on the machines on which you install vCenter Server, vCenter Chargeback Manager, vCloud Director, the corresponding databases, and all the data collectors.

All the machines must be configured with the same time zone. If the machines are not time synchronized, then some of the events might not be processed by the data collectors.

Error Because of Cancellation of Dashboard Report

New dashboard reports are not generated in the next cycle if you cancel a dashboard report that is currently running.

Problem

If you cancel a Dashboard report which is currently running, the new dashboard reports are not generated in the subsequent Dashboard schedule cycles. The backend logs reports the error message, Requested report information cannot be found!.

Solution

It is recommended that you do not cancel a running Dashboard report. If it is necessary to cancel a Dashboard report and if the problem occurs, un-configure the dashboard report for the hierarchy and re-configure it again.

Reports run on different dates produce different values for the same date range

Reports run on different dates for the same date range produce different values

Problem

Report values are different depending on when the report is run, even if the report covers the same report period.

Solution

- 1 Add additional servers to the NTP configuration file on Windows and Linux systems.
- 2 Location of the file on Windows - `c:\Tools\NTP\etc\ntp.conf`
Restart the NTP service.
- 3 Location of the configuration file on vCD/ vSM - `/etc/ntp.conf`
Restart the NTP service.

Add the additional NTP servers and restart the NTP service

Newly Added Hierarchical Entities are not Displayed After Upgrading to VMware vCenter Chargeback Manager

After upgrading to vCloud Director 5.5 from vCloud Director 1.5.2 against vCenter Chargeback Manager 2.5 or higher, newly created Hierarchical Entities are not visible in Chargeback Manager.

Problem

VMware Cloud Director Data Collector in Chargeback Manager tries to upgrade vCloud Director from 1.5.2 to 5.5 version and fails.

Cause

Direct upgrade path from vCloud Director 1.5.2 to vCloud Director 5.5 is not supported.

Solution

- 1 If you have Chargeback Manager 2.5 or lower version for vCloud Director 1.5.2 in your environment, upgrade Chargeback Manager to 2.5.1 or above version.
- 2 Upgrade vCloud Director to 5.1 version, and restart all Chargeback Manager services. Allow the data collector to run for 6 to 8 hours.
- 3 Upgrade vCloud Director to 5.5 version and restart the Chargeback Manager services again.

Index

B

- best practices
 - adding vCenter Server **9**
 - configuring VMware vCloud Director data collector **14**
 - configuring vShield Manager data collector **14**
 - creating database users for data collectors **9**
 - installing vCenter Chargeback Manager **7**
 - installing VMware vCloud Director data collector **13**
 - installing vShield Manager data collector **13**
 - integrating vCloud Director **13**
 - upgrading vCenter Server **10**

E

- external network received value **10**
- external network transmitted value **10**

L

- log files **17**

S

- Stats Migration, Stats Migration Tool **15**

T

- troubleshooting
 - about **17**
 - common issues **19**
 - utility **19**
- troubleshooting issue, modify VMware vCloud Director setup information **27**
- troubleshooting issues
 - add LDAP server **26**
 - add vCenter Server **26**
 - alert setting configuration **27**
 - custom SSL certificate **32**
 - custom SSL certificate chain **33**
 - Dashboard reports cancelled **38**
 - data collector failure **20**
 - data collector status **24**
 - database connection failure **28, 29**
 - deleting vCenter Server **32**
 - email report failure **30**
 - fetch primary LDAP group **30**
 - GUI display issue **25**
 - hierarchy changes **20**

- install failure **21**
- LDAP user login **31**
- network statistics missing **21**
- packets sent to unknown network **37**
- report data display issue **23**
- Reports run on different dates **38**
- service unavailable **23**
- storage information missing **24**
- storage synchronization job failure **24**
- storing localized data in database **22**
- timezone setting change **19**
- unable to access application **25**
- vCenter Chargeback Manager plug-in **34**
- vCenter Server hierarchy changes **20**
- virtual machines missing **37**

U

- utilities, troubleshooting **19**

V

- vCenter Chargeback Manager, best practices **7**

