Using VMware Chargeback™ for vCloud Director as a Service Provider

Management Packs for vRealize Operations 8.10

vmware®

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

https://docs.vmware.com/

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

Copyright © 2023 VMware, Inc. All rights reserved. Copyright and trademark information.

Contents

Using VMware Chargeback as a Service Provider

The *Using VMware Chargeback as a Service Provider* guide provides information about configuring tenant users for VMware Cloud Director .

Note VMware Chargeback was formerly known as Tenant App.

Intended Audience

The information is written primarily for service providers to create users for an organization in VMware Cloud Director . If you are a tenant, then please refer to the Using VMware Chargeback as a Tenant guide.

Introduction

1

VMware supports its partners to host and sell cloud services built on VMware technology usingVMware Cloud Director (vCD). VMware Cloud Director provides constructs to segment the virtual infrastructure and offers it as a service to tenants of these partners.

There are several variants of infrastructure that are sold by these partners such as, 'Pay as you go', 'Raw capacity' also known as 'Allocation based', 'Raw capacity with minimum guarantee' also known as 'Reservation based'. The combination of these can be offered to same tenants and it becomes challenging to track usage over a period and charge appropriately. It becomes critical for the service providers as the tenants demand for transparency in billing, and it is imperative that service providers offer it.

VMware Chargeback addresses this by accurately metering the infrastructure. It provides options to configure different models for pricing this metered infrastructure. It also provides tenant-specific views that help tenants validate their charges by analyzing their usage.

This documentation provides information about configuring VMware Chargeback for VMware Cloud Director .

Note VMware Chargeback was formerly known as Tenant App.

Join the Customer Experience Improvement Program

2

As part of the enhanced Customer Experience Improvement Program ("CEIP"), VMware Chargeback collects certain technical data about the organization's use of VMware products and services regularly. This data is collected to allow VMware diagnose and improve its products and services, fix product issues, provide technical support, and to advise you on how to deploy and use VMware's products.

Configuring VMware products to participate in the CEIP allows the VMware Chargeback to send product usage data to VMWare as part of the Customer Experience Improvement Program. You can disable your participation in this program at any time.

Prerequisites

Note VMware Chargeback was formerly known as Tenant App.

For additional information regarding the CEIP, refer to the Trust and Assurance Center at Customer Experience Improvement Program.

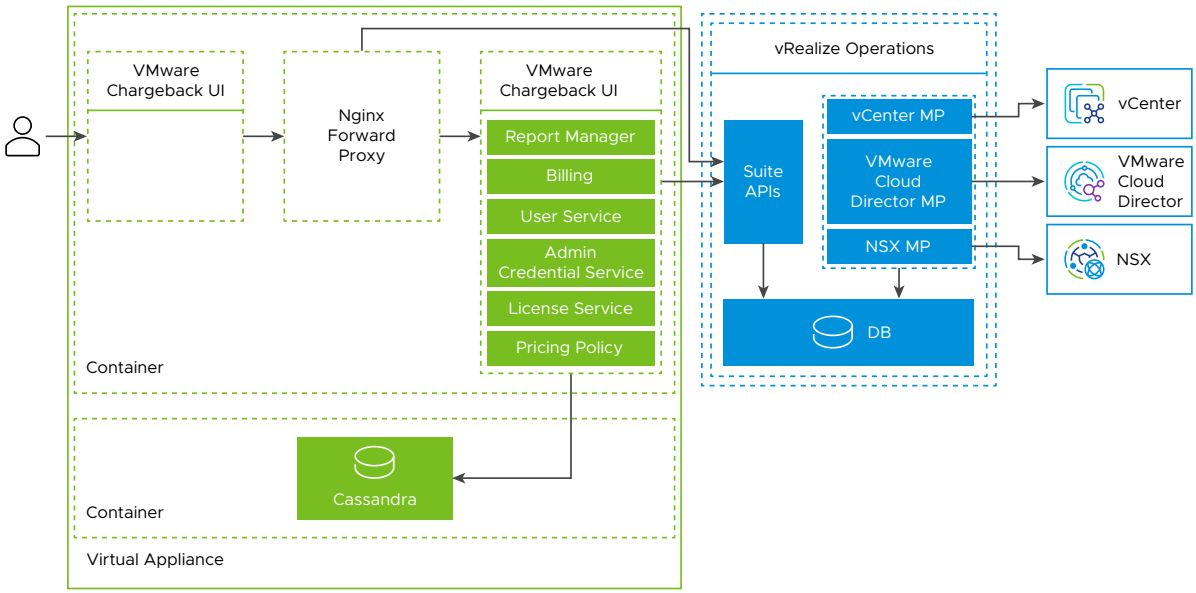
Procedure

1. In the VMware Chargeback UI, click **Admin** and select **CEIP Settings** from the drop-down menu.
2. Select the **Join the VMware Customer Experience Improvement Program** option to enable the program or deselect the option to disable the program.
3. Click **Ok** to save your preference.

Deployment Architecture for VMware Chargeback for VMware Cloud Director

3

The following architecture provides an overview of the deployment process for the vCenter, VMware Cloud Director , and NSX Management Packs. The following architecture provides an overview of integration of VMware Chargeback with vCenter, VMware Cloud Director , and NSX Management Packs.



Note VMware Chargeback was formerly known as Tenant App.

You can receive data from vCenter, VMware Cloud Director , and NSX Management Packs.

- vRealize Operations collects resources from vCenter, VMware Cloud Director , and NSX Management Packs using their respective Management Pack plugins and displays it in the vRealize Operations Database.
- VMware Chargeback for VMware Cloud Director interacts with vRealize Operations using the Suite APIs (internal/external) to collect resources and pricing information.
- A service provider performs configuration actions using the standalone VMware Chargeback UI.
- The tenant can either use VMware Chargeback Plugin UI or the standalone VMware Chargeback UI.

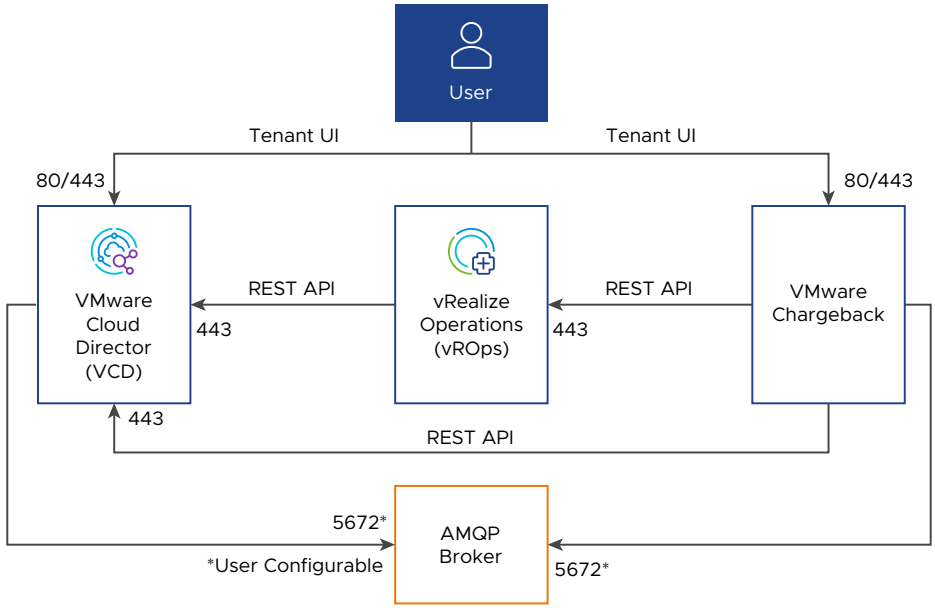
- All requests from VMware Chargeback for VMware Cloud Director are sent through Nginx Forward Proxy and the configuration is as displayed in the Deployment Architecture workflow diagram.

This chapter includes the following topics:

Architecture and Port Requirements

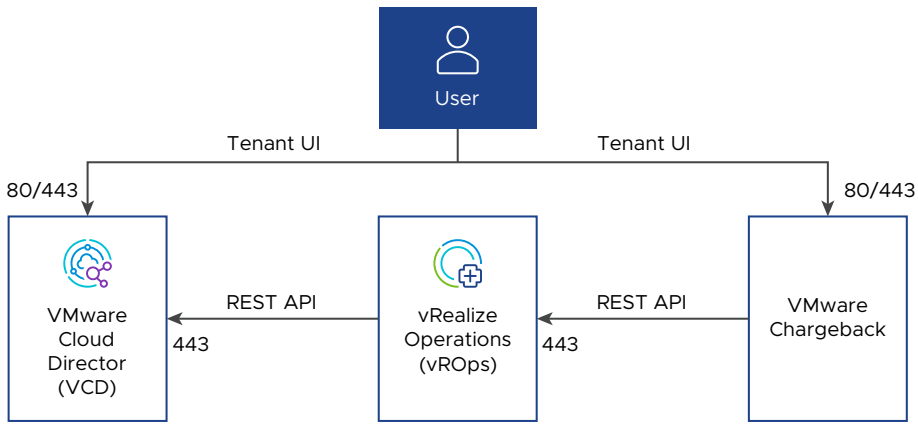
The following architecture provides the port requirement for the integration of VMware Chargeback for VMware Cloud Director .

Figure 3-1. Integration of VMware Chargeback for VMware Cloud Director as a plug-in



The following architecture provides the port requirement of the VMware Chargeback for VMware Cloud Director as a stand-alone app.

Figure 3-2. Integration of VMware Chargeback for VMware Cloud Director as a stand-alone App



Install VMware Chargeback

4

You can integrate VMware Chargeback for VMware Cloud Director with vRealize Operations to deploy the tenant view.

This chapter includes the following topics:

Deploy the OVF File for a VMware Chargeback

To deploy a VMware Chargeback for VMware Cloud Director , you have to download and install the OVF file from the Solution Exchange website. You can install the VMware Chargeback OVF file through vSphere Web Client.

Prerequisites

- Ensure that the vRealize Operations is installed and the VMware Chargeback is installed on the internal network same as vRealize Operations.
- Ensure that the correct license key is entered in the vRealize Operations.
- Verify that you are connected to a vCenter Server system with a vSphere Web Client, and log in to the vSphere Client.
- Verify that you have a data center created and a host system already added to it.

Procedure

1. From the vSphere Web Client navigator, select the host system in the management vCenter where you want to deploy the OVF file.
2. Click the **Actions** drop-down menu and select **Deploy OVF Template**.
3. From the Deploy OVF Template dialog box, select **Local File**.

4 Click **Browse** to locate the OVA file that you downloaded from the Product download page and click **Next**.

5 Rename the OVA file and location at which the OVF is deployed and click **Next**.

6 Verify the resource where you want to run the deployed OVF template and click **Next**.

7 Review the template details and click **Next**.

8 Scroll through the License Agreement and click **Accept > Next**.

9 Select a virtual disk format to store the files for the deployed template and click **Next**.

10 Click **Browse** to select a Destination Network or retain the default destination, and click **Next**.

11 Customize the template by providing the following information.

Option	Description
vRealize Operations Hostname or IP Address	This is a mandatory field. Enter the IP address or the host name of vRealize Operations. **Note** If you have provided the host name, ensure that it is resolvable through DNS.

12 Click **Next**.

13 Review the settings and click **Finish**.

Log in to the VMware Chargeback

To access the tenant view UI, use the IP address of the deployed OVF file.

Prerequisites

Verify that you have deployed the OVF file.

Procedure

1 Open a Web browser and enter the IP address of the deployed OVF file.

2 Select the **vCloud Director** option in the 'Welcome to the VMware Chargeback' page.

3 Enter the vRealize Operations administrator user name and password.

4 Click **Login**.

Note Ensure that you use the vRealize Operations local admin user credentials to log in.

5 From the left menu, click **Administration > Solutions**, and click **vrealize Operations** to save the vRealize Operations administrator credentials.

Note It is necessary to save the administrator credentials in the VMware Chargeback for VMware Cloud Director to access the vRealize Operations Suite APIs and obtain information about organizations and tenants.

Reset Root Password in VMware Chargeback

You can reset the password in VMware Chargeback using root credentials.

Procedure

1 SSH to your VMware Chargeback Virtual Appliance and log in using root credentials.

2 Run the `passwd` command to change the password for root.

3 Enter your new password.

The password is successfully updated.

Note By default, the VMware Chargeback Virtual Appliance is configured with root credentials as 'vmware'.

Managing SSL Certificates

By default, the VMware Chargeback for VMware Cloud Director has a self-signed certificate. You can modify the default certificate, if necessary.

You can resolve a problem by installing a signed certificate using one of the procedures below.

Procedure

1 **Installing a Web Certificate**

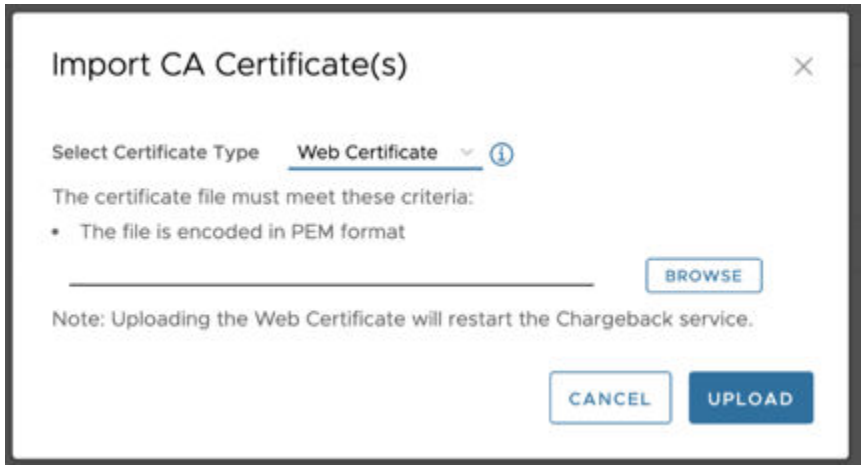
When you attempt to use VMware Chargeback for VMware Cloud Director over a trusted SSL Internet connection, and open the interface in a Web browser; you receive warnings that the connection is untrusted (in Mozilla Firefox) or that problems have been detected with the website's security certificate (in Internet Explorer).

To import certificates of Chargeback that VMware Cloud Director communicates with using the steps mentioned here.

a Go to **Administration > Support**, and click **SSL Certificate**.

b Click **Import.**

c Select Certificate Type: **Web Certificate**.



d Click **Browse** to select a .pem file. The .pem file contains the certificate and private key.

e Click **Upload**.

For information on generating certificates, see KB 71358.

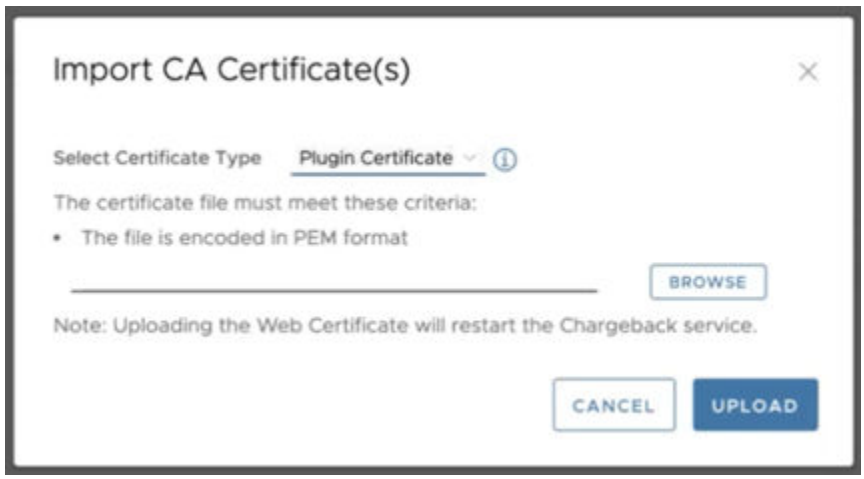
2 **Installing a Plugin Certificate**

In order to successfully integrate with the VCD Tenant UI, the Chargeback application must recognize and trust the associated VCD endpoint. Therefore, it's necessary to upload the VCD certificate to the Chargeback application.

a Go to **Administration > Support**, and click **SSL Certificate**.

b Click **Import.**

c Select Certificate Type: **Plugin Certificate**.



d Click **Browse** to select a .pem file. The .pem file contains the certificate and private key.

e Click **Upload**.

Results

Your uploaded certificate(s) and corresponding details will now appear in the certificate list.

Register a Different vRealize Operations for VMware Chargeback

You can register a different vRealize Operations for VMware Chargeback when the vRealize Operations registered with VMware Chargeback becomes unavailable or when there is a change in the requirement of vRealize Operations for VMware Chargeback.

Procedure

1. Log in to the vCenter environment where VMware Chargeback is deployed.
2. Power off the VMware Chargeback Virtual Machine.
3. Click **Configure > Settings > vApp Options**, and then click **Properties**.
4. Search for vrops_host, and click **SET Value**.
5. Enter the new vRealize Operations IP.
6. Power on the VMware Chargeback.

HA and Backup Configurations for VMware Chargeback

All the data that is processed by VMware Chargeback is stored in vRealize Operations except for the bills generated for the tenant and configuration or the tenant UI access. Therefore, the VMware Chargeback does not have a HA and Backup guide of its own.

Upgrade VMware Chargeback for VMware Cloud Director

5

You can upgrade to the latest version of the VMware Chargeback for VMware Cloud Director .

Procedure

1 Log in to the web console at **`https://<VMware Chargeback for vCD IP address>:5480`** using root credentials.

2 Click the **Update** tab.

3 Click **Check Updates** to view the available updates and to enable the **Install Updates** option.

4 (Optional) Click **Install Updates**.

After successful upgrade, manually reboot the virtual appliance.

5 Click the **System** tab, and verify the updated version number of the appliance.

Note After you upgrade to the latest version of the VMware Chargeback for VMware Cloud Director , for the new Tenant Plugin to take effect, you have to reconfigure the VMware Cloud Director Tenant Plugin from **Administration > Support**. For details, see Configure VMware Cloud Director Tenant UI.

Upgrade VMware Chargeback Using the Downloadable ISO Image

6

You can upgrade VMware Chargeback by using a downloadable ISO image.

.

Procedure

1 Right-click the VMware Chargeback virtual machine and select **Edit Settings**.

2 On the **Virtual Hardware** tab, select **CD/DVD Drive > Datastore ISO File**.

3 Click the ISO image in the datastore.

4 For **File Type**, select **ISO Image**, and then click **OK**.

5 Select the option to connect at power-on and follow the prompts to add the CD/DVD drive to the VMware Chargeback virtual machine.

6 Power on the VMware Chargeback virtual machine.

7 In a Web browser, log in to the virtual appliance management interface (VAMI). The URL for the VAMI is **`https:// vmware chargeback_appliance_address:5480`**

8 Click the **Update** tab.

9 Click **Settings**, and then select **Use CDROM Updates**. Click **Save Settings**.

10 Click **Status**, and then click **Check Updates**. The appliance version appears in the list of available updates.

11 Click **Install Updates**, and then click **OK**.

12 After the updates install, click the **System** tab, and then click **Reboot**

What to do next

Log out of the VMware Chargeback Client, clear the browser cache, and then log in again to see the upgraded appliance.

Install Management Pack for VMware Cloud Director 7

The Management Pack for VMware Cloud Director consists of a PAK file that contains out-of-the-box dashboards for the newer resource objects that are brought in from VMware Cloud Director .

You can install the Management Pack for VMware Cloud Director from the user interface of vRealize Operations Manager or from the command line of vRealize Operations Manager.

This chapter includes the following topics:

Installing from vRealize Operations User Interface

The following procedure is applicable when you have access to the user interface of vRealize Operations. You can install the Management Pack for VMware Cloud Director from the vRealize Operations user interface.

Prerequisites

- Download the PAK file from VMware Marketplace.
- Save the PAK file to a temporary folder on your local system.

Procedure

1. Log in to the vRealize Operations user interface with administrator privileges.
2. From the left menu, click **Data Sources > Integrations**, and then click the **Repository** tab.
3. On the **Repository** tab, click **Add**.
4. Browse to locate the temporary folder and select the PAK file.
5. Click **Upload**. The upload might take several minutes.
6. Read and accept the EULA, and click **Next**.

   Installation details appear in the window during the process.
7. When the installation is complete, click **Finish**.

What to do next

Configure an adapter instance for the management pack.

Installing from Command Line of vRealize Operations

The following procedure is applicable when you have a Chargeback License and do not have access to the user interface of vRealize Operations.

Procedure

1. Download the PAK file for VMware Chargeback on your local machine.
2. Upload the PAK file to your vRealize Operations using any FTP medium.
3. SSH to your vRealize Operations using root credentials (use primary node for Clustered Environment).
4. Upload the PAK file and run the following command from the directory where the PAK File is uploaded.

   ```
   curl -k -X POST -i -u <ADMIN USER NAME>:<ADMIN PASSWORD> -H 'Content-Type:
   multipart/form-data' -H 'Accept: application/json' -F 'pak_handling_advice=CLOBBER'
   -F 'contents=@<PAK FILE NAME>' 'https://<VROPS IP>/casa/upgrade/cluster/pak/
   reserved/operation/upload'
   ```

   Example:

   ```
   curl -k -X POST -i -u admin:Admin@123 -H 'Content-Type: multipart/
   form-data' -H 'Accept: application/json' -F 'pak_handling_advice=CLOBBER'
   -F 'contents=@vmware-vCloud-52014769224.pak' 'https://10.192.64.19/casa/upgrade/
   cluster/pak/reserved/operation/upload'
   ```

5. Copy the PAK_ID from the JSON output.

   For example, the PAK_ID is 'vCloud-52014769224' from the following JSON output.

   ```
   {"filename":"vmware-MPforvCloud-52014769224.pak","links":
   [{"rel":"pak_information","href":"https://10.192.64.19:443/
   casa/upgrade/cluster/pak/vCloud-52014769224/information?
   checkSignature=true"},{"rel":"pak_file_information","href":"https://
   10.192.64.19:443/casa/upgrade/slice/pak/vCloud-52014769224/
   file_information"},{"rel":"pak_cluster_status","href":"https://
   10.192.64.19:443/casa/upgrade/cluster/pak/vCloud-52014769224/
   status"}],"signed":true,"pak_id":"vCloud-52014769224","missing_suite_platforms":
   [],"is_signed":true}
   ```

6 Run the following Install command.

```
curl -k -X POST -i -u <ADMIN USER NAME>:<ADMIN PASSWORD> -H 'Content-Type:
application/json' 'https://<VROPS IP>/casa/upgrade/cluster/pak/<PAK_ID>/operation/
install'
```

Example:

```
curl -k -X POST -i -u admin:Admin@123 -H 'Content-Type: application/json' 'https://
10.192.64.19/casa/upgrade/cluster/pak/vCloud-52014769224/operation/install'
```

7 Check the installation status using the two URLs from the JSON output.

- `https://<VROPS_IP>/casa/upgrade/cluster/pak/<PAK_ID>/status`
- `https://<VROPS_IP>/casa/upgrade/cluster/pak/reserved/current_activity`

Example:

- `https://10.192.64.19/casa/upgrade/cluster/pak/vCloud-52014769224/status`
- `https://10.192.64.19/casa/upgrade/cluster/pak/reserved/current_activity`

Results

Upon successful installation, the 'cluster_pak_install_status' changes from CANDIDATE to COMPLETED.

Install Management Pack for NSX

8

Install the Management Pack for NSX to retrieve the metrics related to metering from VMware Cloud Director . You can install the Management Pack for NSX from the user interface of vRealize Operations or from the command line of vRealize Operations.

The Management Pack for NSX consists of a PAK file.

This chapter includes the following topics:

Installing from vRealize Operations User Interface

The following procedure is applicable when you have access to the user interface of vRealize Operations.

Prerequisites

Download and save the PAK file from Marketplace.

Procedure

1. Log in to vRealize Operations user interface with administrator privileges.
2. From the left menu, click **Data Sources > Integrations**, and then click the **Repository** tab.
3. On the **Repository** tab, click **Add**.
4. Browse to locate and select the PAK file.
5. Click **Upload**. The upload might take several minutes.
6. Read and Accept the EULA and click **Next**.

   Installation details appear in the window during the process.
7. When the installation is finished, click **Finish**.

What to do next

Configure the adapter instance for the management pack.

Installing NSX from Command Line of vRealize Operations

The following procedure is applicable when you have a Chargeback License and do not have access to the user interface of vRealize Operations.

Procedure

1. Download the PAK file for VMware Chargeback on your local machine.
2. Upload the PAK file to your vRealize Operations using any FTP medium.
3. SSH to your vRealize Operations using root credentials (use primary node for Clustered Environment).
4. Upload the PAK file and run the following command from the directory where the PAK File is uploaded.

   ```
   curl -k -X POST -i -u <ADMIN USER NAME>:<ADMIN PASSWORD> -H 'Content-Type:
   multipart/form-data' -H 'Accept: application/json' -F 'pak_handling_advice=CLOBBER'
   -F 'contents=@<PAK FILE NAME>' 'https://<VROPS IP>/casa/upgrade/cluster/pak/
   reserved/operation/upload'
   ```

   Example:

   ```
   curl -k -X POST -i -u admin:Admin@123 -H 'Content-Type: multipart/form-
   data' -H 'Accept: application/json' -F 'pak_handling_advice=CLOBBER' -F
   'contents=@vmware-NSX-vSphere-36014459469.pak' 'https://10.192.64.19/casa/upgrade/
   cluster/pak/reserved/operation/upload'
   ```

5. Copy the PAK_ID from the JSON output.

   For example, the PAK_ID is 'vCloud-52014769224' from the following JSON output.

   ```
   {"filename":"vmware-MPforNSX-vSphere-36014459469.pak","links":
   [{"rel":"pak_information","href":"https://10.192.64.19:443/casa/upgrade/
   cluster/pak/vCloud-52014769224/information?checkSignature=true"},
   {"rel":"pak_file_information","href":"https://10.192.64.19:443/
   casa/upgrade/slice/pak/NSX-vSphere-36014459469/file_information"},
   {"rel":"pak_cluster_status","href":"https://10.192.64.19:443/casa/upgrade/
   cluster/pak/NSX-vSphere-36014459469/status"}],"signed":true,"pak_id":"NSX-
   vSphere-36014459469","missing_suite_platforms":[],"is_signed":true}
   ```

6. Run the following Install command.

   ```
   curl -k -X POST -i -u <ADMIN USER NAME>:<ADMIN PASSWORD> -H 'Content-Type:
   application/json' 'https://<VROPS IP>/casa/upgrade/cluster/pak/<PAK_ID>/operation/
   install'
   ```

   Example:

   ```
   curl -k -X POST -i -u admin:Admin@123 -H 'Content-Type: application/json' 'https://
   10.192.64.19/casa/upgrade/cluster/pak/NSX-vSphere-36014459469/operation/install'
   ```

7 Check the installation status using the two URLs from the JSON output.

- `https://<VROPS_IP>/casa/upgrade/cluster/pak/<PAK_ID>/status`
- `https://<VROPS_IP>/casa/upgrade/cluster/pak/reserved/current_activity`

Example:

- `https://10.192.64.19/casa/upgrade/cluster/pak/NSX-vSphere-36014459469/status`
- `https://10.192.64.19/casa/upgrade/cluster/pak/reserved/current_activity`

Results

Upon successful installation, the 'cluster_pak_install_status' changes from CANDIDATE to COMPLETED.

Install Management Pack for NSX-T

9

Install the Management Pack for NSX-T to retrieve the metrics related to metering from VMware Cloud Director . You can install the Management Pack for NSX-T from the user interface of vRealize Operations or from the command line of vRealize Operations.

The Management Pack for NSX-T consists of a PAK file.

This chapter includes the following topics:

Installing NSX-T from vRealize Operations UI

The following procedure is applicable when you have access to the user interface of vRealize Operations.

Prerequisites

Download and save the PAK file from Marketplace.

Procedure

1. Log in to vRealize Operations user interface with administrator privileges.
2. From the left menu, click **Data Sources > Integrations**, and then click the **Repository** tab.
3. On the **Repository** tab, click **Add**.
4. Browse to locate and select the PAK file.
5. Click **Upload**. The upload might take several minutes.
6. Read and Accept the EULA and click **Next**.

   Installation details appear in the window during the process.
7. When the installation is finished, click **Finish**.

What to do next

Configure the adapter instance for the management pack.

Configuring VMware Chargeback with vCenter, VMware Cloud Director , and NSX Endpoints

10

You can configure the vCenter, VMware Cloud Director , and NSX Endpoints from the VMware Chargeback UI. You can also configure these Endpoints from the vRealize Operations UI.

This procedure is applicable when you configure vCenter, VMware Cloud Director , and NSX Endpoints from the VMware Chargeback UI.

Note Configuring the vCenter, VMware Cloud Director , and NSX Endpoints in the VMware Chargeback creates the respective adapter instances in the vRealize Operations.

Prerequisites

Verify that the Management Packs for VMware Cloud Director and NSX are installed.

Procedure

1. From the left menu, click **Administration > Solutions**.
2. To configure a vCenter adapter instance:
   a. Select the **vCenter Server** tab and click **Add**.
   b. Enter the **Display name** of the vCenter instance and enter a valid **Description**.
   c. Enter the Hostname or FQDN of the **vCenter Server**.
   d. Enter the vCenter Server **Username** and **Password**, and click **Test Connection**. The test connection is successful only when the user name and password are valid.
   e. Click **Save**.
3. To configure a VMware Cloud Director adapter instance:
   a. Select the **vCloud** tab and click **Add**.
   b. Enter the **Display name** of the vCloud instance and enter a valid **Description**.
   c. Enter vCloud Director **Hostname** or **FQDN**.
   d. Enter the **Organization** name.
   e. Enter the **Username** and **Password**.

f (Optional) Enter the **AMQP Password** and then, click **Test Connection**. The test connection is successful only when the user name and password are valid.

g Click **Save**.

Dashboards start displaying data collected from VMware Cloud Director .

4 To configure an NSX adapter instance:

a Select the **NSX** tab and click **Add**.

b Enter the **Display name** of the NSX instance and enter a valid **Description**.

c Enter NSX Manager **Hostname** or **FQDN**.

d Enter the **vCenter Server** Hostname or FQDN.

e Enter the **VC Username** and **Password**.

f Enter the **NSX Username** and **Password**, and then, click **Test Connection**. The test connection is successful only when the user name and password are valid.

g Click **Save**.

Tenant User Interface Management

11

VMware Chargeback for VMware Cloud Director can also be accessed through the VMware Cloud Director as a separate plug-in.

Configure the Tenant User Interface plug-in to allow the organization users of VMware Cloud Director to access their metering information. A tenant can view a separate Welcome page from where the tenant can access the VMware Chargeback features within the VMware Cloud Director user interface. This feature provides easy accessibility without having to access VMware Chargeback in a separate browser. This is an optional feature, however, you can still continue to use VMware Chargeback as a stand-alone UI.

Only the organization users have access to the VMware Chargeback user interface in VMware Cloud Director .

This chapter includes the following topics:

- Configure VMware Cloud Director Tenant UI
- Access Management for Tenants

Configure VMware Cloud Director Tenant UI

Configure the VMware Cloud Director Tenant UI to allow tenants to access their organization-specific information.

Prerequisites

- For the VMware Cloud Director Tenant UI plug-in to work, ensure that the AMQP server is configured on VMware Cloud Director . For details on configuring AMQP Host, see Install and Configure a RabbitMQ AMQP Broker.

  Note This pre-requisite is applicable only for VMware Cloud Director versions below 10.2.

Procedure

1. On the left pane, click **Administration > Support**.
2. Click **Configure with VCD Tenant UI**.

3 Configure the VMware Cloud Director Tenant UI.

Field	Description
Director Host name	Enter the vCloud Director host name.
User Name	Enter the user name for VMware Cloud Director .
Password	Enter the password for VMware Cloud Director .
AMQP Host	Provide the AMQP Host name or IP address information. The host information must be same as the AMQP host that is configured in VMware Cloud Director extensibility settings.
AMQP Password	Provide the AMQP password.
AMQP Port	Default is 5672. Provide the AMQP port number.
AMQP Virtual Host	Provide the virtual host. Retain the AMQP Port / as is. The host information should be similar to the host that is configured in VMware Cloud Director .
AMQP user name and Password	Provide the AMQP user name and password.
AMQP Use SSL	Select this option to make an AMQP connection over SSL.
Tenant App Proxy	The IP address of VMware Chargeback for VMware Cloud Director is allocated automatically. If VMware Chargeback is deployed in a private network, you can configure Load Balancer or a proxy to provide public access to VMware Chargeback. In such cases, public address can be mentioned in this text box.

4 Click **Start**.

The services are listed under the Self Health section. You can click the square icon to start action on the selected service.

5 On the left pane, click **Access Management** and enable the plugin access for your organization users.

Results

View Operations Plugin for your organization at **`https://<vCloud Director IP Address>/tenant/<Organization Name>.`**

Access Management for Tenants

Service providers have access to components like Provider Dashboard, Organization, Resource Pools, and Provider VDCs . They can create users and give them access to an organization. Service providers can also import the user account information that resides on another machine. To do this, the service providers must define the criteria used to import the user accounts from the source machine as an Active Directory user or an OpenLDAP user.

You can provide access to metering and billing information to a Tenant through VMware Cloud Director or by directly logging into VMware Chargeback. To provide access through VMware Cloud Director , see Configure VMware Cloud Director Tenant UI.

Adding Users to an Organization

To provide access to certain resource details, add users to an organization. The users with this access can view the **Organization Overview** for the underlying resources.

Prerequisites

- To integrate with OpenLDAP or Active directory, verify that you have added authentication sources in vRealize Operations and the user names are present in Active Directory or OpenLDAP. For more information on adding authentication sources, see *vRealize Operations Manager* documentation.

Procedure

1. On VMware Chargeback for VMware Cloud Director page, click **Administration > Access Management**.
2. Go to the **Manage Users** tab and click **ADD USER**.
3. Select any Organization and click **Next**.
4. To create a new local user, provide required details and click **Add User**.
5. To import an existing user from Active Directory or Open LDAP, click **Import** and select the import location.
6. Click **Search** and then **Add User**.

Results

You have created a user with permissions to access an organization through VMware Chargeback.

Managing Accessibility of Pages

Service providers can toggle the page access for their tenants.

Procedure

1. On the left pane, click **Admin Setting** and then, click **Access management > Manage Pages**.
2. Use the **Enable Page Access?** option to enable or disable page access for individual pages. You can also enable or disable all page access by clicking the **Enable All** or **Disable All** button on the tool bar.
3. Click **Save** to save the details.

Results

Note Pages that are access disabled are not visible to the tenant.

Managing Accessibility of Metrics

Service providers can toggle the metric access for their tenants.

Procedure

1. On the left pane, click **Admin Setting** and then, click **Access management > Manage Metrics**.
2. Select the **Show price values to tenants** option to display the Total Cost to the tenant.
3. Select the **Resource Type** for which you want to enable or disable the metric access.
4. Select the metric for which you want to enable or disable metric access to the tenant.
5. Click **Save** to save the details.

Results

Note Metrics that are access disabled are not visible to the tenant.

Creating and Assigning Pricing Policies

12

You can calculate the cost for each virtual machine and resources.

You can optionally list the Organizations VDCs for which the adapter instance collects data. For policy allocation models, see *vCloud Director' Administrator's Guide*.

Note The pricing policies apply to VMs at a minimum granularity of five minutes. The VMs that are created and deleted within the short span of five minutes will still be charged.

Prerequisites

- Verify that the Management Packs for vCenter Server, VMware Cloud Director , and NSX is configured. For details, see Chapter 10 Configuring VMware Chargeback with vCenter, VMware Cloud Director , and NSX Endpoints.

Procedure

1. On the left pane, click **Pricing > Configuration**.
2. Select the **Pricing Policies** tab and then, click **Add New Policy**.
3. To create a pricing policy, enter the following details in the **Base Settings** tab.

Option	Description
Policy Name	Enter the policy name that uniquely identifies your policy.
Pricing Policy Type	Select the pricing policy type from the drop-down menu. The pricing policy type determines your billing model based on the Organization VDC type.
Currency	The currency as set in vRealize Operations.
Policy Description	Enter a valid description for the policy.
Price based on sizing policies	Enable this option to charge based on the pricing policy created in VMware Cloud Director instead of charging individually for CPU and Memory.

4 Click **Next** and add more details in the **Pricing** tab.

Option	Description
Sizing Policy	Sizing policies are a way of defining template VM sizes such as Small, Medium, and Large, in terms of vCPU and Memory. This option appears only when you enable the **Price based on sizing policies** option in **Base Settings**. a Select the **Charge Period** which indicates the frequency of charging. b Select the **Sizing Policy Name** from the drop-down menu. c Enter a valid number for **Base Rate**. d Select the **Charge Based on Power State** by selecting the charge from the drop-down menu. This decides whether the charge should be applied based on the power state of the VM. e Click **Add** and then click **Next**.
CPU Rate	You can charge the CPU rate based on GHz or vCPU Count. a For Base Rate, select the **Charge Period** and **Charge Based on** from the drop-down menu. The **Charge Period** indicates the frequency of charging and **Charge Based on** indicates the pricing model based on which the charge is applied. b Enter a valid number for **Default Base Rate** . c Using slabs, you can optionally charge different rates depending on the number of vCPUs used. Enter valid numbers for **Base Rate Slab** and click **Add Slab**. The base rate slab allows you to change the rate of charging based on the resources used. For example, if you enter **5** in **Greater than or equal** and **5** as **Base Rate**, it means if the usage is 5 vCPU and above, then the Base Rate of 5 will be applied for whole usage. d Select the **Charge Based on Power State** by selecting the charge from the drop-down menu. This decides whether the charge should be applied based on the power state of the VM. e For **Fixed Cost**, enter a valid number. Fixed costs do not depend on the units of charging. f Click **Next**.

Option	Description
Memory Rate	a For Base Rate, select the **Charge Period** and **Charge Based** on from the drop-down menu. The **Charge Period** indicates the frequency of charging and **Charge Based on** indicates the pricing model based on which the charge is applied. b Select the **Charge Based on Power State** from the drop-down menu. This decides if the charge should be applied based on the power state of the VM. c Enter a valid number for **Default Base Rate**. d Using slabs, you can optionally charge different rates depending on the memory allocated. Enter valid numbers for **Base Rate Slab** and click **Add Slab**. The base rate slab allows you to change the rate of charging based on the resources used. For example, if you enter **50** in **Greater than or equal** and **10** as **Base Rate**, it means if the usage is 50 GB and above, then the Base Rate of 10 will be applied for whole usage. e For **Fixed Cost**, enter a valid number. Fixed costs do not depend on the units of charging. f Click **Next**.

Option	Description
Storage Rate	You can charge for storage either based on storage policies or independent of it. The **Default Rate** option appears only when you have selected **Aggregate storage charges from Storage profiles for payg Org-VDCs** in the **Pricing Settings** tab. To charge independent of storage policies, select provide the following details: **Note** This way of setting rates will be deprecated in the future release and it is advisable to instead use the **Storage Policy** option. a For Base Rate, select the **Charge Period** and **Charge Based** on from the drop-down menu. The **Charge Period** indicates the frequency of charging and **Charge Based on** indicates the pricing model based on which the charge is applied. b Enter a valid number for **Base Rate**. c Select the **Charge Based on Power State** from the drop-down menu. This decides if the charge should be applied based on the power state of the VM. d For **Fixed Cost**, enter a valid number. Fixed costs do not depend on the units of charging. e Click **Add** and then click **Next**. To charge based on storage policies, select **Storage Policy**, and provide the following details: **Note** Storage prices are calculated based on usage by storage policies that are independent of underlying VMs and templates, or by aggregating the usage from underlying VMs and templates. The difference is that the former considers indirect disks such as log disks and swap disks, whereas the latter considers only the storage used directly by the VMs. You can change this setting under **Configuration > Pricing Settings**. To charge by aggregating the usage from underlying VMs and templates, see Creating and Assigning vCenter Storage Profile Tag in VMware Chargeback. a Select the **Storage Policy Name** from the drop-down menu. **Note** The rate specified using the **Default** option is used for any storage policy for which rate is not explicitly specified. b For Base Rate, select the **Charge Period** and **Charge Based** on from the drop-down menu. The **Charge Period** indicates the frequency of charging and the **Charge Based on** indicates the pricing model based on which the charge is applied. You can charge for used storage or configured storage of the VMs, for example, if a VM has a 20 GB disk and if 12 GB is utilized, setting the **Charge Based on** to **Usage** will charge for 12 GB and setting it to **Limit** will charge for 20 GB. For more details, see c Select the **Charge Based on Power State** from the drop-down menu. This decides if the charge should be applied based on the power state of the VM. d Enter a valid number for **Default Base Rate**. e Using slabs, you can optionally charge different rates depending on the storage allocated. Enter valid numbers for **Base Rate Slab** and click **Add Slab**.

Option	Description
	The base rate slab allows you to change the rate of charging based on the resources used. For example, if you enter **50** in **Greater than or equal** and **10** as **Base Rate**, it means if the usage is 50 GB and above, then the Base Rate of 10 will be applied for whole usage. f Click **Add** and then click **Next**.
Cloudian Storage	A third-party storage service in VMware Cloud Director that allows the Service Providers to provide additional storage to the tenants and charge them for the same. You can charge for the consumption of cloudian storage by creating slabs with different rates for storage values. **Note** The bills for cloudian storage will be generated only at the organization level. a Select the **Charge Period** and **Charge Based** on from the drop-down menu. The **Charge Period** indicates the frequency of charging and **Charge Based on** indicates the pricing model based on which the charge is applied. b Enter a valid number for **Default Base Rate (Per GB)**. c Click **Create Slab** and then click **Next**.
Network Rate	a Enter the **External Network Transmit** and **External Network Receive** rates. **Note** If your network is backed by NSX-T, you will be charged only for the network data transmit and network data receive. b Under Network Transmit Rate, select the **Change Period** from the drop-down menu, and enter the **Default Base Rate** . c Using slabs, you can optionally charge different rates depending on the network data consumed. Enter valid numbers for **Base Rate Slab** and click **Add Slab**. The base rate slab allows you to change the rate of charging based on the resources used. For example, if you enter **50** in **Greater than or equal** and **10** as **Base Rate**, it means if the usage is 50 Mbps and above, then the Base Rate of 10 will be applied for whole usage. d Select the **Usage** based on which you want to charge. e Under Network Receive Rate, select the **Change Period** from the drop-down menu and enter the **Default Base Rate**. f Using slabs, you can optionally charge different rates depending on the network data consumed. Enter valid numbers for **Base Rate Slab** and click **Add Slab**. The base rate slab allows you to change the rate of charging based on the resources used. For example, if you enter **50** in **Greater than or equal** and **10** as **Base Rate**, it means if the usage is 50 Mbps and above, then the Base Rate of 10 will be applied for whole usage. g Select the **Usage** based on which you want to charge. h Click **Next**.

Option	Description
Advanced Network Rate	**Edge Gateway Size**: VMware Chargeback allows you to define the size of the edge gateway (Compact, Large, Extra Large and Quad Large) and assign differential price based on the edge size. **Edge Services**: Apart from the basic data transfer, there are additional value added services offered in VMware Cloud Director in combination with NSX. All the network services associated with specific edge such as HA, DHCP, IPV6, IP Sec, Load Balancer, NAT, SSL VPN, L2 VPN, Firewall, Static Routing, BGP Routing, OSPF Routing are considered for charging based on these services are 'Enabled' or not. If services are enabled for a specific day and base rate is applied for that service, then that particular service gets charged for that specific day. If the service is disabled on any day then base rate will not be applied. **IP Count** is the unique IP counts available on the external network of the Org-VDC. Pricing can be performed based on the count of these IPs. a Under **Edge Gateway Size**, enter the base rates for the corresponding edge gateway sizes. b Enter the **Charge Period** and **Base Rate** in the displayed fields. c Under the **Network Service Pricing (NSXT only)**, **L2VPN charges (per L2VPN count)**, **Load Balancer Charges (per load balancer count)**, enter the **Charge Period** and **Base Rate Slab** in the displayed fields. d Click **Add Slab**. Service Providers can charge for consumption of NSX Advanced Load Balancer based on throughput. You can create slabs with different rates for throughput values. **Note** The unit of charging for 'throughput' is 'mbitsps'. a Under **NSX Advanced Load Balancer (Throughput)**, enter the **Charge Period**, **Usage**, and **Default Base Rate Slab** in the displayed fields b Click **Add Slab** and then, click **Next**.
Guest OS Rate	Use the Guest OS Rate to charge differently for different operating systems . a Enter the **Guest OS Name**. b Select the **Charge Period** and **Charge Based on Power state** from the drop-down menu. c Enter the **Base Rate** and click **Add** and then, click **Next** .

Option	Description
Cloud Director Availability	**Per Replica Charge**: Use this section to set pricing for replications created from Cloud Director Availability. You can charge for each replication object, based on SLA profile they belong to. For charging replications without any SLA Profile assigned, please enter **None** as the SLA Profile name. a Click **Create Per Replication Charge**, and enter **Replication SLA Profile** name, **Charge Period**, and **Base Rate**. b Click **Add**. **Storage Usage Charge**: Use this section to set additional pricing for storage used by Cloud Director Availability replications in Cloud Director. **Note** The storage usage defined in this tab will be added additionally to the Storage Policy Base Rate. a Click **Create Storage Usage Charge**, and enter **Storage Policy Name**, **Charge Period**, and **Default Base Rate**. b Click **Add Slab**, and define **Greater than or equal** and **Base Rate**. c Click **Add** to include the values entered above to the pricing policy.
vCenter Tag Rate	Use the vCenter Tag Rate to charge differently for different tags set on VM . a Enter the **Tag Category** and **Tag Value**. b Select if you want to charge based on **Fixed Rate** or **Alternate Pricing Policy**. c Select the alternate **Pricing Policy** name. This option appears only when you charge based on **Alternate Pricing Policy**. d Select the **Priority** for the alternate pricing policy. This option appears only when you charge based on **Alternate Pricing Policy**. When the metadata or tag-based charges overlap, setting a priority allows you to define which policy should be processed first. e Select the **Charge Period** and **Charge Based on Power state** from the drop-down menu. f Enter the **Base Rate** and click **Add**, and then, click **Next**.
VCD Metadata Rate	Use the VCD Metadata Rate to charge differently for different metadata set on vApps. a Enter the **Tag Key** and **Tag Value**. b Select if you want to charge based on **Fixed Rate** or **Alternate Pricing Policy**. c Select the alternate **Pricing Policy** name. This option appears only when you charge based on **Alternate Pricing Policy**. d Select the **Priority** for the alternate pricing policy. This option appears only when you charge based on **Alternate Pricing Policy**. When the metadata or tag-based charges overlap, setting a priority allows you to define which policy should be processed first. e Select the **Charge Period** and **Charge Based on Power state** from the drop-down menu. f Enter the **Base Rate** and click **Add**, and then, click **Next**.

Option	Description
One Time Fixed Cost	Use the One Time Fixed Cost section to charge for one time incidental charges on Virtual Machines. These costs do not repeat on a recurring basis. a Enter the **One time fixed cost** to charge for the setup fee of the VMs. b Using tags, you can charge for other incidental charges such as 'OS patching charge' based on one time fixed costs. Under VCD Metadata, enter the **Tag Key** and **Tag Value**. c Enter the **One time fixed cost** and click **Add**. d Under vCenter Tag, enter the **Tag Key** and **Tag Value**. e Enter the **One time fixed cost** and click **Add**. f Click **Next**. **Note** User can now even add a negative value for the **One time fixed cost**.
Rate Factors	Use Rate Factors to either increase or discount the prices against individual resources consumed by the Virtual Machines or by whole charges against the Virtual Machine. a For any resource with Metadata, enter the **Tag Key** and **Tag Value** under VCD Metadata. b Select **Change the price of** and increase or decrease the price by entering a valid number in **By applying a factor of**. For example, if you want to increase the price of CPU which has a tag 'Tag1-Value1' by 20% then select `CPU` from the **Change the price of** drop-down menu and enter `1.2` in **By applying a factor of**. c Click **Add**. d For any resource with Tag, enter the **Tag Key** and **Tag Value** under vCenter Tag. e Select **Change the price of** and increase or decrease the price by entering a valid number in **By applying a factor of**. For example, if you want to increase the price of CPU which has a tag 'Tag1-Value1' by 20% then select `CPU` from the **Change the price of** drop-down menu and enter `1.2` in **By applying a factor of**. f Click **Add** and then, click **Next**.
Tanzu Kubernetes Clusters	Use Tanzu Kubernetes Clusters to charge for the clusters and objects, based on attributes like CPU, Storage, Memory etc. a Under the Cluster Fixed Cost, select the **Charge Period** and enter the **Fixed Cost**. b Under the Cluster CPU Rate, select the **Charge Period** and **Charge Based On**. Enter the **Default Base Rate** and **Base Rate Slab**. c Click **Add Slab** and then, click **Next**.

Option	Description
CSE Kubernetes Clusters	Use CSE Kubernetes Clusters to charge for the clusters and objects, based on attributes like CPU, Storage, Memory etc. a Under the Cluster Fixed Cost, select the **Charge Period** and enter the **Fixed Cost**. b Under the Cluster CPU Rate, select the **Charge Period** and **Charge Based On**. Enter the **Default Base Rate** and **Base Rate Slab**. c Click **Add Slab** and then, click **Next**.
Additional Fixed Cost	Use the Additional Fixed Cost section to charge at the Org-VDC level. You can use this for charges such as overall tax, overall discounts, and so on. The charges can be applied to selective Org-VDCs based on Org-VDC metadata. a Under the Fixed Cost, enter the **Charge Period** and **Fixed Cost**. b Under VCD Metadata, enter the **Tag Key** and **Tag Value**. c Enter the **Charge Period** and **Base Rate**, and click **Add**. d Under VCD Metadata One Time, enter the **Tag Key** and **Tag Value**. e Enter the **One time fixed cost** to charge for the Org-VDC, and click **Add**. f Click **Next**.

5 Click **Next** to view the summary in the **Preview** tab, and click **Create**.

6 Go to **Configuration > Resources** tab, select an Organization/Organization VDC, and click **Assign**.

7 Select a policy to assign and click **Assign**.

The policy is assigned to the selected Organization/Organization VDC.

Creating and Assigning vCenter Storage Profile Tag in VMware Chargeback

As a vCenter admin, you must perform the following steps to view the actual usage metric per storage policy.

Procedure

1 Log in to vCenter console.

2 Create a Category called 'storage type'. For details on how to create a new category, refer to *Create a Tag* topic in the *VMware vCenter Server and Host Management* guide.

3 Under the Datastore page, click **Add Tag** and provide the storage policy name and select the category as **Storage Type**. For example, if GOLD is the name of the storage policy and DS1 is the datastore, create GOLD tag and assign it to DS1.

4 Use tag-based storage placements to ensure the created VM disks are associated to the Datastore. For example, GOLD storage policy is existing/created and GOLD tag is added in tag-based placement rule.

5 Repeat step 3 and 4 for existing Datastores.

Note Only one Tag per category 'storage type' must be assigned to Datastore. If there is no specific storage policy assigned, you can assign a Tag called '*', which signifies 'any' storage policy in vCD.

Cloning Policies

You can clone an existing policy with a different name.

Procedure

1 To clone an existing pricing policy, select the pricing policy in the **Pricing Policies** tab, and click **Clone**.

2 Enter a name for the duplicate policy and click **Clone**.

A duplicate of the existing policy is created with a different name.

Managing Email Outbound 13

You can create an email outbound that acts as a gateway to send all emails related to alerts and reports.

This chapter includes the following topics:

- Creating an Email Outbound
- Configuring Emails

Creating an Email Outbound

You can create an email outbound through which the emails have to be sent.

Prerequisites

Ensure that you have an account that you can use as the connection account for the email server. If you choose to require authentication, you must also know the password for this account.

Procedure

1 On the left pane, click **Administration > Configure**.

2 Under **Create Email Outbound**, click **Create** and enter the following details.

Option	Description
Name	Enter a name for the outbound.
Description	Provide a description for the outbound.
Use Secure Connection	Enables secure communication encryption using SSL/TLS. If you select this option, you must select a method in the **Secure Connection Type** drop-down menu. **Note** It is mandatory to enable the **Use Secure Connection** option.
Requires Authentication	Enables authentication on the email user account that you use to configure this SMTP instance. If you select this option, you must provide a password for the user account. **Note** It is mandatory to enable the **Requires Authentication** option.
SMTP Host	Enter a URL or IP address of your email host server.

Option	Description
SMTP Port	Enter the default port SMTP that is used to connect with the server.
Secure Connection Type	Select either SSL/TLS as the communication encryption method used in your environment from the drop-down menu. You must select a connection type if you select Use Secure Connection.
User Name	Email user account that is used to connect to the email server.
Password	Password for the connection user account. A password is required if you select Requires Authentication.
Sender Email Address	Enter the email address of the sender.
Sender Name	Enter a name for the sender email address.

3 Click **Save**.

What to do next

You can configure emails for the outbound that you just created. For details, see Configuring Emails.

Configuring Emails

After creating an email outbound, you can assign email addresses to Org-VDCs. These email addresses receive alerts and reports related to a particular Org-VDC.

Prerequisites

Ensure that you have created an email outbound. For details, see Creating an Email Outbound.

Procedure

1 On the left pane, click **Administration > Configure**.

2 Click **Configure Email** and then, click **Create**.

3 Enter the following details.

Option	Description
Select OVDC	Select an Org-VDC from the drop-down menu.
Email Address	Enter the email address of user to whom the email has to be sent.
Select Email Outbound	Select an email outbound to which you want to send the email.

4 Click **Ok**.

What to do next

You can run or schedule reports for a selected Org-VDC using the Tenant Reports page.

Reports

14

A report is a scheduled snapshot of objects and metrics about them.

This chapter includes the following topics:

Report Templates

On the **Report Templates** tab, you can run reports and schedule report generation.

From the left menu, click **Reports** > **Report Templates** tab.

All templates that are applicable for the selected object are listed on the Report Templates tab. You can order them by report name, subject, date they were modified, last run, or owner.

You can filter the templates list by adding a filter from the right side of the panel.

Table 14-1. Predefined Filter Groups

Filter Group	Description
Name	Filter by the template name. For example, you can list all reports that contain *my template* in their name by typing `my template`.
Subject	Filter by another object. If the report contains more than one view applicable for another type of object, you can filter by those objects.

vSphere users must be logged in until the report generation is complete. If you log out or your session expires, the report generation fails.

Note The maximum number of reports per template is 10. With every new generated report, vRealize Operations deletes the oldest report.

Generated Reports

All reports that are generated for a selected object are listed on the **Generated Reports** tab.

Go to the **Metering** tab and click **Reports > Generated Reports**, to access the Generated Reports tab.

You can order the reports by the date and time that they were created, the report name, the object on which the report is generated, the owner, or the status. If the report is generated through a schedule, the owner is the user who created the schedule.

Note The maximum number of reports per template is 10. With every new generated report, vRealize Operations deletes the oldest report.

You can filter the reports list by adding a filter from the right side of the panel.

Table 14-2. Predefined Filter Groups

Filter Group	Description
Report Name	Filter by the report template name. For example, you can list all reports that contain *my template* in their name by typing **`my template`**.
Template	Filter by the report template. You can select a template from a list of templates applicable for this object.
Subject	Filter by another object. If the report contains more than one view applicable for another type of object, you can filter by those objects.
Status	Filter by the status of the report.
Completion Date/Time	Filter by the date, time, or time range.

You can download a report in a PDF or CSV format.

Tenant Reports

The **Tenant Reports** page allows the service providers to provide tenants, access to the custom reports. Service providers can view all the report templates including the custom templates that are created using the vRealize Operations.

Service providers can generate tenant reports on demand or they can schedule them to be emailed to their tenants. For email configuration, see Configuring Emails.

Generating a Report

You can generate a report for a selected Org-VDC.

Procedure

1 On the left pane, click **Metering > Tenant Reports**.

2 Under the **Report Templates** tab, select a report template, and click **Run**.

The list of Org-VDCs configured are displayed.

3 Select the required Org-VDCs and click **Generate** to generate a report for the selected Org-VDC.

Scheduling a Report

You can schedule a report for the selected Org-VDC.

Procedure

1 On the left pane, click **Metering > Tenant Reports**.

2 Under the **Report Templates** tab, select a report template, and click **Schedule** to schedule a report.

3 Select the Org-VDC for which you want to schedule the report, and click **Next**.

4 Define the schedule by entering the start date, hour, recurrence, and other publishing criteria for the report.

5 Click **Schedule**.

Generated Reports

All reports that are generated for a specific Org-VDC are listed on the **Generated Reports** tab.

From the left menu, click **Metering > Tenant Reports > Generated Reports** to access the generated reports.

You can download a report in a PDF or CSV format.

Note

- Once the service provider shares a report template with the tenant, all the reports that are generated on that template for the tenant's organization are available to the tenant.
- Only local admin users can generate and view the reports. Tenant users can only view the reports.

Prerequisites

Ensure that you have created and configured an email outbound. For details, see Creating an Email Outbound and Configuring Emails.

Billing in VMware Chargeback 15

VMware Chargeback generates monthly bills to provide an account of the overall expenses used for resources in an organization.

Note There is a service in the VMware Chargeback for automatic bill generation. On the first of every month, bills are generated for all the available organization VDCs for the previous month (1st to 30th or 31st). The generated bills are listed under **Bills > My Bills**.

This chapter includes the following topics:

Generate a New Bill

As a Service Provider, you can charge different OVDCs and generate bills at the Organization/ OVDC level. You can provide a bill summary at an organization level by separating the cost incurred by the different OVDCs. You can also charge for resources consumed at an organization level rather than the OVDC level.

Prerequisites

You can generate bills from the VMware Chargeback UI by selecting a resource name from an organization. Verify that pricing policies are created for a selected resource.

Procedure

1. On the left pane, click **Pricing > Bills**.
2. Click **Generate/Schedule New Bill**.
3. Select a resource from the list of resources. You can generate a bill at the organization level or at a specific OVDC level. Select the check box against the Organization name to generate the bill at the organization level or select the check box against any specific OVDC to generate a bill at the OVDC level.

   Note If you select the check box at the Organization level then all the OVDCs under it are selected automatically. Deselecting any of the OVDCs will undo the selection at the Organization level.
4. Click **Next**.

5 Select a policy name and click **Next**. By default, the selected pricing policy will be applied to the VDCs that do not have any other pricing policies assigned previously.

Note When generating a bill, if you have a resource that does not have any pricing policy assigned to it, then the pricing policy of the parent will be used for that bill.

6 Enter a **Title** and specify the period for generating a new bill from the selected resources and policies in the **Start Date** and **End Date** fields.

7 To schedule a bill, enable the **Schedule bill** option and specify the details to generate the bill on the required date. For example, if the **Recurrence** is **`Monthly`**, **From Day** is **`1`**, **To Day** is **`31`**, **Month** is **`Previous`** and **Generate bill on** is **`3`**, then the details are collected for the previous month starting from first of the month to 31st and the bill is generated on the third of every month.

8 Click **Generate**.

What to do next

- You can view the bill that you generated. Go to **My Bills** and select one of the bills from the list and then, click **View** to view the bill.

  For bills generated at the Organization level, you can view the bill summary of the Organization and associated Organization VDCs. The Cloudian Storage section is available only when cloudian storage is configured and applied as part of pricing policy.

- Go to **Bill Schedules** to view the details of the scheduled bills.

Monitoring Infrastructure 16

Service providers can monitor the alerts on their infrastructure using **Monitoring > Alerts** . A service provider can give access to the tenants using **Monitoring > Tenant Alerts** .

This chapter includes the following topics:

- Alerts for Service Providers
- Alerts for Tenants

Alerts for Service Providers

You can view the overall list of alerts that are generated by the resources available in the data center.

VMware Chargeback provides a mechanism to view all the alerts with:

- Criticality of an alert
- Alert Definition
- Object Name
- Object Type

From the home page, navigate to **Monitoring > Alerts** to access alerts.

Alerts for Tenants

Service providers can configure the alert definitions that must be emailed to a tenant using the **Tenant Alerts** page. Notification rules determine the alerts that are sent to the Org-VDC owners.

You can create notification rules for alert definitions that are created using the vRealize Operations. For details on creating alert definitions, see Alert Definitions.

To create notification rules for alert definitions:

Procedure

1 On the left pane, click **Monitoring > Tenant Alerts**.

2 Select the alert definitions for which you want to create a notification rule, and click **Create Notification Rule**.

3 Enter a name for the rule and select the Org-VDC for which you want to create a notification rule.

4 Click **Create** to create the notification rule for the selected Org-VDC.

The owner of the Org-VDC receives an email when the alert is triggered.

What to do next

You can view the notification rules that you created under the **Tenant Alerts > Notification Rules** tab.

Note To delete a notification rule, select the notification rules that you want to delete and click **Delete** in the **Notification Rules** tab.

Dashboards in VMware Chargeback for VMware Cloud Director

17

A service provider can view dashboards of the VMware Chargeback.

Note

- VMware vRealize Operations users with Standard or Chargeback license cannot view the Dashboards and Monitoring tabs. However, the options under the Metering and Administration menu items are available. The same behavior is observed when the license for VMware vRealize Operations expires.
- Dashboards, Monitoring, and Troubleshooting capabilities of vRealize Operations Tenant App are included in the vRealize Operations Advanced and Enterprise editions.

This chapter includes the following topics:

Home

View organization information, alerts, reports, bills, metering configuration, and access management.

You can click each tile to go to the detail page.

- Click **Organizations** to view the organization summary and list of organizations with multiple organization VDCs..
- Click **Access Management** to navigate to the acess management page.
- Click **Alerts** to view the alert summary and the top alerts.
- Click **Reports** to view the predefined templates that you can use for your customers.
- Click **Metering Configuration** to configure pricing policies.
- Click **Bills**

Operations Overview

This dashboard provides an overview of resources for an organization.

Table 17-1. Operational Overview

Widget	Description
Summary	■ Provides the number of organization VDCs, vApps, virtual machines, and number of running virtual machines that are available in an organization. ■ Provides total cost of the entire data center for a given OVDC, and ongoing price in US$.
Capacity Overview	Provides an overview of CPU, memory, and storage use of an organization.
System Status	Provides a system status of the critical, warning, and immdiate alerts generated by the organization.
Organization Details	Provides detailed information about each organization, such as the number of organization VDCs, vApps, VMs, Running VMs, cost in US$ charged to the service provider, and ongoing price in US$ charged to the tenant.

Organizations

The Organizations dashboard contains a list of organizations with multiple organization VDCs.

Table 17-2. Organizations

Widget	Description
Organizations Summary	Provides the number of organizations, organizations VDCs, vApps, and virtual machines that are available in a data center.
List of Organizations	Provides the list of organizations within the provider VDC. Click **Export**, to export the list of provider VDCs in an excel format.

Organization Overview

This dashboard provides an overview of resources for an organization.

Table 17-3. Organization Overview

Widget	Description
Organization Summary	Provides the number of organization VDCs, vApps, and virtual machines that are available in an organization.
Capacity Overview	Provides an overview of CPU, memory, and storage use of an organization.
System Status	Provides a system status of the criticality of alerts generated by the organization.
List of Organization VDCs	Provides list of organization VDCs with vApp and VM information.
vApps Utilization Summary	Provides a summary of vApp utilization of an organization.
VDC Utilization Summary	Provides a summary of VDC utilization of an organization.

Organization VDCs

You can view a list of organizations VDCs associated with your organization.

To view the organization VDC overview, click the VDC Name from the list of organization VDCs.

Table 17-4. Organization VDCs

Widget	Description
Organization VDC Summary	Provides the number of vApps and virtual machines that are available in a data center.
Capacity Overview	Provides information about the CPU, memory, and storage use of an organization VDC.
List of vApps	Provides information of a list of vApps that are used in an organization VDC.
vApp Utilization Summary	Provides a summary of vApp utilization for an organization VDC.

vApps

vApp is a virtual machine that is loaded with an operating system, applications, and data. It is a virtual system that contains one or more individual virtual machines with parameters that define operational details. Cloud resources also provide access to storage and network connectivity.

VMware Chargeback displays a list of vApps that an organization contains.

When you click a vApp name from the list of vApps, you are directed to the page that lists its associated VMs.

Table 17-5. vApps

Widget	Description
vApp Summary	Provides the number of virtual machines, vCPU memory, and storage that is associated to that vApp.
List of Virtual Machines	Provides the list of virtual machines underlying a vApp.

Virtual Machines

You can view a list of VMs that are associated within an organization.

To see a detailed view of your virtual machine, click a virtual machine from the list of VMs.

Widget	Description
VM summary	Provides an overall summary of the Virtual Machine status and its memory allocation.
CPU Information	■ CPU usage (MHz). This field provides an overall CPU usage of the selected VM. ■ CPU Usage (%). This field provides the percentage of CPU usage of a selected VM.
Memory Information	■ Memory usage (MHz). This field provides the overall memory usage of the selected VM. ■ Memory Usage (%). This field provides the percentage of memory usage for a selected VM.
Storage Information	■ Read/Write Throughput (KBPS) ■ Read/Write (IOPS)
Network Information	■ Network Rate (KBPS) ■ Network Packets Dropped (Count)

Metric Selector

The Metric Selector dashboard allows you to view the metrics over a time. You can select a resource type, resource, metric, and time range to view the metric graph. All metrics time stamps are in the UTC time zone in the VMware Chargeback for VMware Cloud Director .

Note Only users with Advanced and Enterprise License can view cost related information in this dashboard.

Use the **Manage Metrics** tab to manage metric access to tenants. For details, see Managing Accessibility of Metrics.

Provider Overview

The dashboard provides an overview of provider virtual data center, which combines the CPU, memory, and storage resources of one or more datastores available for that resource pool.

For more information, see *VMware vCloud Director Documentation center*.

Table 17-6. Provider Overview

Widget	Description
Organizations Summary	Provides the number of organizations, virtual data centers, vApps, and virtual machines that are available in a data center.
Capacity Overview	Provides the capacity of CPU usage, memory, and Storage for each provider.
System Status	Provides a list of all the alerts for objects within a data center.
List of Organizations	Provides the list of organizations within the provider VDC. Click **Export**, to export the list of provider VDCs in an excel format.

Provider VDC

Provider VDC (PVDC) combines the CPU, memory, and storage of one or more datastores available for that resource pool. This page provides a list of all the PVDCs that are available in your data centers.

Table 17-7. Provider VDC

Widget	Description
Provider VDC Summary	Provides the CPU limit, memory limit, number of organization VDCs and resource pools that are available in a data center.
Capacity Overview	Provides an overview of CPU, memory, and storage use for each provider.
List of Organization VDCs	Provides list of organization VDCs with vApp and VM information.
List of Resource Pools	Provides the list of resource pools that are configured for provider VDCs in your data center.

Resource Pools

You can configure resource pools to a provider VDC to allocate resources to provider VDC. This page provides a list of resource pools that are configured for provider VDCs in your data center.

Click **Export**, to export the list of resource pools in an excel format.

Data Retention

18

You can view and manage historical data retention related to system settings. You can tune these settings to manage storage space consumed by VMware Chargeback.

Enter the number of days for which you want to retain the generated bills and click **Save**.

Note You can retain the generated bills to a maximum of 1440 days.

Understanding VMware Chargeback API

19

Service Providers can use the API to build interactive clients of VMware Chargeback. The API follows the REST style and is available to all licensed users.

VMware Chargeback clients communicate with the server over HTTP, exchanging representations of VMware Chargeback objects. These representations take the form of JSON elements. You use HTTP GET requests to retrieve the current representation of an object, HTTP POST, and PUT requests to create or modify an object, and HTTP DELETE requests to delete an object.

This chapter includes the following topics:

How the VMware Chargeback API Works

Use a web browser to communicate with the VMware Chargeback analytics engine, either through the product user interface or through API calls.

The adapter instance collects data from objects in your monitored environment. The VMware Chargeback analytics engine processes the data and displays the complete model in the graphical interface.

Why Use the API

The API is most useful when there is a need to automate a well-defined workflow, such as repeating the same tasks to configure the access control for new VMware Chargeback users. The API is also useful when performing queries on the VMware Chargeback data repository, such as retrieving data for particular assets in your virtual environment. In addition, you can use the API to extract all data from the VMware Chargeback data repository and load it into a separate analytics system.

VMware Chargeback Terminology

The JSON syntax you use to describe the objects for an adapter corresponds to the API code syntax but differs from what you find in the user interface. The following terms appear in the user interface. Included with the description of each term is the corresponding JSON syntax used in an API call.

Adapter types	Defines the adapter used to discover particular object types. For example, the vCenter adapter discovers objects connected to vSphere data centers. The EMC adapter discovers EMC storage system objects. JSON syntax: `adapterkinds`.
Object types	The class of entities that represent objects or information sources. Objects report data to the vRealize Operations analytics engine. Virtual machines, datastores, and host systems are examples of object types defined in a vCenter adapter model. JSON syntax: `resourcekinds`.

Getting Started with the API

API clients and VMware Chargeback servers communicate over HTTPS, exchanging JSON representations of API objects.

Acquire an Authentication Token

VMware Chargeback requires API requests to be authenticated. The first step in this workflow is to obtain an authentication token.

To obtain an authentication token, the login request supplies the user credentials in a form that Basic HTTP authentication requires. In this example, the user is logging in to a VMware Chargeback instance with URL `https://tenantapp.example.com/`.

Prerequisites

- Secure a channel between the web browser and the VMware Chargeback server. Open a browser and enter the URL of the VMware Chargeback instance such as:

  ```
  https://tenantapp.example.com/
  ```

  The system warns that your connection is not private. Click through to confirm the security exception and establish an SSL handshake.
- Verify that you can access the APIs. Enter the URL of your VMware Chargeback instance with `tenant-app-api/swagger-ui.html` added to the end, such as:

  ```
  https://tenantapp.example.com/tenant-app-api/swagger-ui.html
  ```
- Verify that you have the login credentials for a user of your VMware Chargeback instance.

Procedure

1 POST a request to the login URL to acquire a token.

```
POST https://tenantapp.example.com/tenant-app-api/api/suiteapi/internal/auth/token/acquire
```

2 Examine the response.

A successful request returns an ops authorization token, which you must include in subsequent API requests.

Example: Login Request and Response

This example shows a request and response for a user with login user name: **tenantapp-user** and password: **tenantapp-dummy-password**.

Request header:

```
POST https://tenantapp.example.com/suite-api/api/auth/token/acquire
Content-Type: application/json
Accept: application/json
```

Request body in JSON format:

```
{
  "username" : "tenantapp-user",
  "password" : "tenantapp-dummy-password"
}
```

Response in JSON:

```
200 OK
```

```
{
  "token": "8f868cca-27cc-43d6-a838-c5467e73ec45::77cea9b2-1e87-490e-b626-e878beeaa23b",
  "validity": 1470421325035,
  "expiresAt": "Friday, November 5, 2019 6:22:05 PM UTC",
  "roles": []
}
```

Note Add the label 'vRealizeOpsToken' and a space as prefix in the acquired token.

The response code indicates whether the request succeeded, or how it failed.

- If the request is successful, the server returns HTTP response code 200 (OK) and reusable `ops` authorization token that expires after six hours. This token must be included in each subsequent API request.
- If the credentials supplied in the POST body are invalid, the server returns HTTP response code 401.

What to do next

The obtained token must be included in each subsequent API request as the Authorization header.

Include the Authorization header in the format: `vRealizeOpsToken <token value>`.

If the token supplied in the Authorization header is invalid or expired, the server returns HTTP response code 401.

For information on individual APIs, open the VMware Chargeback api documentation url in the format:

```
https://tenantapp.example.com/tenant-app-api/swagger-ui-html
```

Support Bundle for VMware Chargeback for VMware Cloud Director

20

The VMware Chargeback for VMware Cloud Director support bundles contains log and configuration files that help troubleshoot.

To access the Support bundle, navigate to **Administration > Support > Support Bundle**.

To generate a support bundle, click **Generate** . You can also download or delete the support bundle.

Troubleshooting in VMware Chargeback

21

You can troubleshoot general problems that might occur when using the VMware Chargeback.

This chapter includes the following topics:

The Value for Metadata in VMware Chargeback Bills Is Zero

Cause

vRealize Operations does not collect **Metadata** as the **Metadata** is not enabled in the Management Pack for vCloud Director.

Solution

1. In vRealize Operations, from the left menu, click **Administration > Solutions**, and then click **Other Accounts**.
2. Click the specific vCloud Adapter instance and select **Edit** from the list.
3. Under **Advance Settings**, change the **Enable Advanced Metrics** and **Enable Metadata** value to **True**.
4. Click **Save**.

VMware Chargeback Plugin Displays Access Denied Error in the VMware Cloud Director Instance User Interface

Cause

The user has logged in to VMware Cloud Director instance using the system administrator credentials.

Solution

- Use organization-specific user credentials to access the VMware Chargeback Plugin. The VMware Chargeback Plugin is not accessible to system administrators.

Upgrade of VMware Chargeback Fails with Berkely DB Error

Upgrading VMware Chargeback to the latest version fails with a Berkely DB error.

Problem

When you try to upgrade VMware Chargeback to the latest version, the upgrade fails with the error, 'Failed to install updates (Error while running installation tests)'.

You can view `/opt/vmware/var/log/vami/updatecli.log` for the following information:

- Error: rpmdb: BDB0113 Thread/process 2707/139910771108032 failed: BDB1507 Thread died in Berkeley DB library
- Error: db5 error(-30973) from dbenv->failchk: BDB0087 DB_RUNRECOVERY: Fatal error, run database recovery
- Error: cannot open Packages index using db5 - (-30973)
- Error: cannot open Packages database in /var/lib/rpm

Cause

This issue is caused when the rpm process accessing Berkeley DB library is interrupted either during the current run or at some other time.

Solution

1. Move or remove the lock files `mv /var/lib/rpm/__db* /tmp/.`
2. Rebuild the Berkley DB index `rpm --rebuilddb -vv`.
3. Perform a YUM clean all.
4. Update from vami again.

For Unlimited Allocation of Storage, Charging Based on Storage Results in Zero Values

Problem

If the configuration in VMware Cloud Director is to have an unlimited allocation for Storage on a PAYG Org-VDC, then charging based on the storage allocation in VMware Chargeback results in zero values.

Cause

This is because providing unlimited storage and charging for it do not work well.

Solution

Charge based on usage in VMware Chargeback.

Unable to Monitor the Health of VMware Chargeback

Problem

Unable to monitor the health of VMware Chargeback and check if the application is up and running.

Solution

You can use the API from VMware Chargeback to monitor the health of the dockers running in the VMware Chargeback.

- If you do not have a token, then enter the command, `GET : https://<vmware-chargeback-ip>/ui`. A document is displayed as response. If the response code is 200, then we can conclude that the vmware-chargeback-ui container is up and running.
- If you have a token, then enter the command, `POST: https://<vmware-chargeback-ip>/suite-api/api/auth/token/acquire`

  ```
  {

  "username": "<admi-username>",

  "password": "<admin-password>"

  }
  ```

  The following response is displayed:

  ```
  { "token": "string", "validity": 0, "expiresAt": "string", "roles": [ "string" ] }
  ```

- For self-health check of VMware Chargeback, enter the command, `GET : https://<vmware-chargeback-ip>/vmware-chargeback-api/services` and enter the token that you acquired in the header as

  ```
  "Authorization": "vRealizeOpsToken <token>"
  ```

The list of all services in VMware Chargeback along with the status will be displayed.

VMware Chargeback UI Becomes Inaccessible When the Self Signed Certificate Expires

Problem

VMware Chargeback UI becomes inaccessible when the self-signed certificate expires.

Note This issue is relevant only when the UI is accessed over the internet. The UI cannot be accessed by a service provider or tenants if the certificate is not valid.

Solution

You can replace an expired self-signed certificate with a valid certificate for VMware Chargeback.

1. Log in to VMware Chargeback VA as root and navigate to "/etc/ssl" using the command, `# cd /etc/ssl`.
2. Execute the commands in the following sequence.
   - `# openssl genrsa -out app.key 2048`
   - `# openssl rsa -in app.key -out app.key`
3. Replace "/CN=localhost" with customer domain in the command, `# openssl req -sha256 -new -key app.key -out app.csr -subj '/CN=localhost'`.
4. Replace "-day 356" based on your requirement in the command, `# openssl x509 -req -sha256 -days 365 -in app.csr -signkey app.key -out app.crt # cat app.crt app.key > app.pem`.
5. Restart the openssl by using the command, `# systemctl restart sshd`.
6. Reboot VMware Chargeback using the command, `# reboot`.

The Upgrade from VMware Chargeback 2.4.x, 2.5.x, to 2.6.x and Above Versions Cause the Plugin Container to Remain in the 'Restarting' State

Cause

In VMware Chargeback 2.4.x and 2.5.x, the default password of Cassandra was used to communicate with the plugin and the DB container. After the release of 2.6.x, the usage of the default password was removed due to security concerns so when you upgrade from 2.4.x, 2.5.x release to 2.6.x and above release, there is a conflict of old plugin communication with upgraded APP and DB container.

Solution

Unregister the vCloud Director Endpoints and re-register it.

Logging in to VMware Chargeback with Configured Local Users Other than Admin Throws a 403 Error on the Login Page

Cause

The local users other than the admin do not have the REST API permissions.

Solution

Provide "Read Access to APIs" permission while creating the local users.

Known Issues for VMware Chargeback

22

In VMware Chargeback, price-related changes are not displayed in the VMware Cloud Director Tenant UI for the first time

In VCD Tenant UI, the total price in **Overview > All organizations** and other price components are not available for the first time.

Workaround:

1 Log in to VMware Chargeback as a Service Provider.

2 Navigate to **Admin Setting > Access Management**, and click on the **Manage Metrics** tab.

3 Disable and again enable the **Price Settings** checkbox.

4 Click **Save**.

VMware Chargeback Plugin Upload to vCloud Director Instance Fails with Upstream Error in the Network Tab

The VMware Chargeback plugin upload fails if the port 80 is not open on the vCloud Director instance.

Workaround: Open the Port 80 only during plugin registration or upload the plugin through a customized portal from the path '/opt/vmware/plugin/plugin.zip' and restart the plugin.

Unable to Access VMware Chargeback Plugin from vCloud Director and the Network Tab Displays CORS Error

Unable to access VMware Chargeback plugin from vCloud Director operations manager and the Network tab displays Cross-Origin Resource Sharing (CORS) error 'making/api/sources'.

Workaround:

1 SSH to the VMware Chargeback instance.

2 Execute the command `docker exec -it vmware-chargeback-ui bash`.

3 Edit the nginx.conf file: `vi /etc/nginx/nginx.conf`.

4 In the nginx.conf file, search for the section 'location /suite-api/' and append the following attributes with #

- #proxy_hide_header Access-Control-Allow-Origin
- #proxy_hide_header Access-Control-Allow-Credentials

5 Reload the nginx server with the command `/usr/sbin/nginx -s reload`.

Tenant Reports Option Missing on the Manage Pages Tab

After upgrading VMware Chargeback from 2.5 to 8.6, the Tenant Reports option is missing on the Manage Pages tab.

Workaround: Refer to the KB article 88080.

Access Denied for vCloud Director Operations Manager Plugin, as the new permission is not added for the existing plugin user in vRealize Operations Manager

Due to the new permission 'administration.accesscontrol.viewpage' that is added for the vCloud DirectorTenant Admin Role in vRealize Operations Manager, the message 'Access Denied' is displayed in Operations Manager Plugin in vCloud Director.

Workaround:

1 Login to VMware Chargeback as an admin user.

2 Go to Administration -> Access Management -> Access Management.

3 Disable the Organizations for which the Plugin has been enabled, and then Enable again.

Metrics collected for the current date cannot be billed

VMware Chargeback does not bill metrics that are collected on the current date in vRealize Operations. The bills for these metrics are generated after a day.

Workaround: None

Bills cannot be generated for the same day

You cannot generate bills for the same day, for example, you cannot give the date range as '16/10/2019 - 16/10/2019' as the billing is done from 12 AM to 12 AM.

Workaround: To perform billing for one day, the date range should be '15/10/2019/ - 16/10/2019'

Virtual Machine deployed under vSAN Datastore does not display the Datastore Hierarchy in Metric Chart in Dashboards

vSAN Datastore deployed Virtual Machines will have Virtual Disk Metric Hierarchy rather than the Datastore Hierarchy.

Workaround: None

Billing in VMware Chargeback for vCenter does not work if the Virtual Machines are placed under host/cluster

In VMware Chargeback for vCenter, the bill value is zero for Virtual Machines if they are not placed under a resource pool.

Workaround:

1 Add a resource pool under your cluster and move the Virtual Machines under that resource pool.

2 Generate a bill from VMware Chargeback using the resource pool or the cluster.

Upgrade of VMware Chargeback fails in VAMI with an error 'Failed to install updates(Error while running installation tests) on <Day>, <Year> <Month> <Date> <Time>'

When you try to upgrade VMware Chargeback from an older version, it fails with an error 'Failed to install updates (Error while running installation tests)'.You can check if the /opt/vmware/var/log/vami/updatecli.log file contains the error 'Installing package vmware-chargeback-2.0.0-15579401.noarch needs X MB on the / filesystem and X free MB is available in the system'.

Workaround: Run the 'docker image prune -a' to clear the space in VMware Chargeback without affecting the functionality.

Customer security scanning report displays the 'TenantApp exposing Internal IP Address' message

While performing security scanning on VMware Chargeback in the customer environment, the scanning report displays a message that the VMware Chargeback could expose the internal IP address. This is due to the Ngnix configuration.

Workaround:

1 SH into VMware Chargeback using root credentials.

2 Run "docker ps" and note the "CONTAINER ID" of vmware-chargeback-ui docker from the list of dockers that is displayed.

3 Go to vmware-chargeback-ui using "docker exec -it bash" and e dit the nginx.conf file in "/etc/nginx/nginx.conf" location.

4 Search for 'server_name _;' and replace '_' with the vmware-chargeback-ip or vmware-chargeback-hostname.

5 Searh for 'add_header X-Upstream $upstream_addr always;' and include a comment by adding an '#' in front of it, '#add_header X-Upstream $upstream_addr always;'.

6 Save the nginx.conf file.

7 Run the following command to stop the nginx server:

   /usr/sbin/nginx -s stop

8 Run the following command to restart the nginx server:

   /usr/sbin/nginx -s reload

   If the above step results in the error 'nginx: [error] open() "/var/run/nginx.pid" failed (2: No such file or directory)', then execute the following commands:

   - /usr/sbin/nginx -c /etc/nginx/nginx.conf
   - docker restart <containerid>
   - Restart the VMware Chargeback instance.

Operation Manager menu is not available in VMware Cloud Director 10.3 (Tenant Login)

Customers with VMware Chargeback 2.6.1 and vCD 10.3 cannot access the VMware Chargeback UI with the vCD tenant login even when the vCD plugin registration is successful in the VMware Chargeback admin login.

Workaround:

1 SSH to VMware Chargeback VA with root access.

2 Navigate to the location: “/opt/vmware/plugin”.

3 Download the “plugin.zip” to your location machine from the above location.

4 Login to vCD (https://<VCD FQDN>/provider) with root access.

5 Navigate to More -> Customize Portal -> Manage Plugins -> Plugins.

6 Remove existing 'Operations Plugin' (VMware Chargeback for VMware Cloud Director extension), if any.

7 Click Upload, and then click SELECT PLUGIN FILE in the popup wizard.

8 Select the plugin.zip that you downloaded and click NEXT.

9 Select the 'Scope' and 'Publish to' in the Select Scope & Publishing tab.

10 Click NEXT.

11 Review and click FINISH.

12 Logout from vCD (Provider login).

13 Log in to vCD as a tenant.

14 Verify the Operation Manager under the More drop-down menu.

15 Access VMware Chargeback by clicking the “Operation Manager”.

Incorrect information is displayed in the vCenter mode for Metering configuration

When assigning a policy to a resource in the Metering configuration section in the vCenter mode, it displays "OVDC assignment" instead of "VC resource".

Workaround: None

Resolved Issues for VMware Chargeback

23

The following issues have been resolved.

- Storage Rate Discount cannot be applied as there is no option to add a discount in the pricing policy for storage
- The home page of the VMware Chargeback is failing to load
- High CPU usage when querying the bills page in the VMware Chargeback
- High CPU usage when querying the bills page in VMware Chargeback. The memory configuration has been optimized and garbage collection is changed to improve the performance of high load queries.
- Plugin service is in the Restart state instead of Running state and is unable to start the plugin service.
- Creation of native thread failure