EMC® vCloud Director Data Protection Extension

Version 2.0.5

Administration and User Guide

302-001-992

REV 05

EMC²

Published December 2016

EMC Corporation
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.EMC.com

CONTENTS

FIGURES

TABLES

PREFACE

As part of an effort to improve its product lines, EMC periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

If a product does not function correctly or does not function as described in this document contact an EMC technical support professional.

Note

This document was accurate at publication time. Go to EMC Online Support (https://support.EMC.com) to find the latest version of this document.

Purpose

This document describes how to configure and use the vCloud Director Data Protection Extension.

Audience

This document is intended for system administrators who will be configuring and using the vCloud Director Data Protection Extension. The document assumes a high degree of knowledge of how to use and administer vCloud Director.

Revision history

The following table presents the revision history of this document.

Revision	Date	Description
05	December, 2016	GA release of version 2.0.5 of the vCloud Director Data Protection Extension.
04	April, 2016	GA release of version 2.0.4 of the vCloud Director Data Protection Extension.
03	October, 2015	GA release of version 2.0.3 of the Avamar Plug-in for vCloud Director.
02	June, 2015	GA release of version 2.0.2 of the Avamar Plug-in for vCloud Director.
01	September, 2014	Initial GA release of the Avamar Plug-in for vCloud Director.

Related documentation

The following EMC publications provide additional information:

- *EMC vCloud Director Data Protection Extension Release Notes*
- *EMC vCloud Director Data Protection Extension Installation and Upgrade Guide*
- *EMC Avamar Backup Extensions to vCloud Director REST API Reference Guide*
- *EMC vCloud Director Data Protection Extension Message Bus Specification*
- *EMC Avamar for VMware User Guide*

Special notice conventions used in this document

EMC uses the following conventions to alert the reader to particular information.

NOTICE

The Notice convention emphasizes important information about the current topic.

Note

The Note convention addresses specific information that is related to the current topic.

Typographical conventions

In this document, EMC uses the typographical conventions that are shown in the following table.

Table 1 Typographical conventions

Convention	Example	Description
Bold typeface	Click **More Options**.	Use for names of interface elements, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what a user specifically selects or clicks).
Italic typeface	*EMC Avamar Administration Guide*	Use for full titles of publications that are referenced in text.

Monospace font	`Event Type = INFORMATION`
	`Event Severity = OK`
	`Event Summary = New group created`
		Use for:
		• System code
		• System output, such as an error message or script
		• Pathnames, file names, prompts, and syntax
		• Commands and options

Monospace font with italic typeface	Type ***Avamar_server***, where *Avamar_server* is the DNS name or IP address of the Avamar server.	Use for variables.
Monospace font with bold typeface	Type **yes**.	Use for user input.
Square brackets	**[--domain=*String*(/)] --name=*String***	Square brackets enclose optional values.
Vertical bar	**[--domain=*String*(/)] | --name=*String***	Vertical bar indicates alternate selections - the bar means “or”.

Table 1 Typographical conventions (continued)

Convention	Example	Description
Braces	`{[--domain=String(/)] | --name=String}`	Braces enclose content that the user must specify.
Ellipses	`valid hfs ...`	Ellipses indicate nonessential information that is omitted from the example.

Where to get help

The Avamar support page provides access to licensing information, product documentation, advisories, and downloads, as well as how-to and troubleshooting information. This information may enable you to resolve a product issue before you contact EMC Customer Support.

To access the Avamar support page:

1. Go to https://support.EMC.com/products.
2. Type a product name in the **Find a Product** box.
3. Select the product from the list that appears.
4. Click the arrow next to the **Find a Product** box.
5. (Optional) Add the product to the **My Products** list by clicking **Add to my products** in the upper right corner of the **Support by Product** page.

Comments and suggestions

Comments and suggestions help EMC to continue to improve the accuracy, organization, and overall quality of the user publications. Send comments and suggestions about this document to DPAD.Doc.Feedback@emc.com.

Please include the following information:

- Product name and version
- Document name, part number, and revision (for example, 01)
- Page numbers
- Other details to help address documentation issues

CHAPTER 1

Introduction

This chapter includes the following topics:

EMC vCloud Director Data Protection Extension

EMC® vCloud Director Data Protection Extension allows backup administrators to manage backup, restore, and replication operations for the cloud. The backup administrator role is performed by a vCloud Director Administrator who has access rights to the cloud organizations, Org VDCs, and vApps that need to be backed up or restored.

Starting with the 2.0.4 version, a new "Organization Administrator" role has been added. vCloud Director supports the creation of "Organizations" to contain various resources, such as "virtual datacenters" and the resources allocated to them through reservations and other means. Service Providers may use the Organization structure to map to a "tenant" so they can lease cloud resources to them. In that case, the Organization Administrator is essentially the "tenant administrator". This new role will allow vCloud Director Organization Administrators to perform backups and restores at the Organization level. Throughout this document, the Organization Administrator (vCD OA) role will be included in this document to show which transactions the vCD OA can perform.

The vCD Data Protection Extension allows the vCD SA to configure and manage backup appliances through which you map cloud resources to an Avamar backup store (including Avamar with Data Domain). A backup appliance provides a representation layer to the Avamar system, enabling vCloud backup and recovery operations. Backup capacities on the Avamar and connected Data Domain systems are exposed as backup stores.

The vCD SA can then use backup repositories to associate specific vCloud Director Org VDCs to a backup appliance. Backup repositories are logical entities that map a backup store on a backup appliance with an Org VDC. An Org VDC can map to multiple backup repositories; however, only one repository can be made "active" for backups. Non-active repositories are in restore-only mode. This logical construct also enables advanced restore use cases where filters are used to look up backups for protected vApps that are deleted or from another cloud.

After vApp backups have been created and replicated, the backup administrator (vCD SA or vCD OA) can browse and restore the backups of the vApps and of individual VMs to their original locations or to new locations.

Authentication

Authentication is used by a server to determine who is accessing the Application.

The EMC vCloud Director Data Protection Extension UI authentication is integrated with vCloud Director (vCD), where users have to provide their vCD credentials during login to get authenticated.

vCD users can get authenticated by the following methods through the EMC® vCloud Director Data Protection Extension UI:

- System Administrators:
  - vCD Local
  - LDAP
  - vCenter SSO users
- Organization Administrators:

- vCD Local
- LDAP

Note

vCenter SSO users are not supported.

Authorization

Authorization is used to determine which resources are available to specific users.

There are two types of authorization:

- Provided natively by vCloud Director to limit the Organization-specific resources returned and made visible by the UI to the logged in Organization Administrator.
- Provided by the vCD Data Protection Extension to control who has access to the data protection operations (such as policy management and ad hoc backup or restore from the UI).

Note that in the second case above, the UI web app will use and follow the delegated authorization controls as defined by the DPE platform documentation.

Also note that only the vDC SAs and OAs can perform backups and restores, vApp owners will not be able to trigger backups or restores

Org vDC backup operation customization and configuration

Backup policies are assigned and configured by a provider System Administrator. vCD Organization Administrators (vCD OA) are not allowed to modify the backup policies exposed to an Organization vDC, but they can apply poilicies to a vApp or VM.

The purpose of these controls over customization is to support a public provider use case. Aspects of backup policies such as frequency and retention period incur costs to the provider. If the underlying resources associated with backup operations are shared across tenants, enforcement of resource consumption constraints allows predictable service for all tenants. A provider administrator can choose to delegate authority over backup policy at a granular level within each Org vDC.

Element	Default	Description
enableBackupPolicyCustomization	False	Allow Org admins to apply backup policies
enableAdhocBackup	False	Allow Org admins to trigger an adhoc backup request for a vApp

The below table depicts the roles and permissions:

Permissions	vCD System Administrator (vCD SA)	vCD Organization Administrator (vCD OA)
Manage Backup Appliances	Yes	No
Manage Organizations	Yes	No
Manage Repositories	Yes	No
Create Restore-only Repository	Yes	No

Manage Policies	Yes	No
Apply Policies	Yes	Yes, if enableBackupPolicyCustomization is enabled
Manage Replication	Yes	No
Manage Backups	Yes	Yes. Only the backups that are in the OA's organization
Adhoc Backups	Yes	Yes, if enableAdhocBackup is enabled and the vApps/VMs reside in the OA's organization
Restore vApps or VMs (original or new)	Yes	Yes. Only the backups that are in the OA's organization
Restore deleted vApps	Yes	Yes
Restore vApps to a different Org VDC	Yes	Yes, as long as the Org VDC is in the same Organization
Restore vApps using the restore-only repository	Yes	Yes

Note

The vCD OA can manage policies (Create, Read, Update, Delete) through the REST API, but can only apply policies in the UI.

Backup appliances

A backup appliance represents an Avamar backup store. The appliance maps a physical or virtual Avamar store to your cloud resources through a backup gateway server. It also associates one or more vCenter instances from your cloud to Avamar so that you can perform backup, restore, and replication operations. Before you can configure your vCD Data Protection Extension system to perform backups, the vCD SA must add a backup appliance using the vCD Data Protection Extension GUI.

If you need to scale up your cloud backups, you can deploy additional backup storage (for example, add additional Data Domain servers) within your existing backup appliance. You can also configure additional backup appliances to add new backup storage. You can use a backup appliance to provide a coarse level of tenant isolation.

The vCD SA can manage a backup appliance's internal components, such as backup repository, vCD Organization, backup proxies, and vCenter registration.

Organizations and repositories

Once the vCD SA has created a backup appliance, the next step is to register a cloud organization and to map one or more of its virtual datacenters to a backup appliance. The vCD SA can do this by configuring backup repositories, which are required for performing backups and restores.

A backup repository is a configured relationship between a backup appliance and an Org VDC. The vCD SA creates a repository, gives it a name, and selects a backup

store on the backup appliance associated with that Org VDC. The Avamar GSAN and up to 12 Data Domain systems can be attached to the backup appliance.

vApps within virtual datacenters direct their backups through the backup repository to the Avamar backup store. The backup repository also allows for a level of virtual datacenter-based tenant isolation.

Backup policy templates

A backup policy template is a combination of a backup schedule, a retention period, and an option set. Backup policies, which are created using policy templates, control when vApps are backed up, how long to keep the backups, and which, if any, options will be invoked during the backup process.

To create a backup policy template, the vCD SA must first create at least one schedule, one retention period, and one option set. Then the vCD SA creates a catalog to which backup policy templates are added.

Backups

The Backup function provides access to vCloud Director Resources (organizations, Org VDCs, and vApps), allowing the vCD SA to assign policies to a vApp. The vCD SA can browse the cloud resources remotely from the configured vCloud Director. If new resources are added to vCloud Director while browsing, the vCD SA can use the Refresh button to update the Backup view.

The Backup Administrators can also start an ad hoc backup on a vApp by selecting the vApp in the list, and clicking Backup. They can then monitor the backup's progress.

Before vApp backups can occur, the vCD SA must assign policies and repositories to your Org VDCs as described in Creating a backup policy for an Org VDC on page 30.

Restores

Through the vCD Data Protection Extension's restore area, the vCD SA can view organizations and Org VDCs, and browse the backup inventory for the vApps in each VDC (the vCD OA can only see the backup inventory in its own Organization). The vCD SA can also browse the backup inventory through the backup repository that is associated with the Org VDC. Both administrators can then select a backup, and restore it to its original location, or to a new location in the selected Org VDC.

Progress can be monitored while the restore is in progress.

Initial tasks

To get started using the vCD Data Protection Extension, perform the tasks described in the following sections.

Deploy the vCD Data Protection Extension

There are two ways to install and configure the vCD Data Protection Extenstion.

- If you would like to set up a non-production "Proof of Concept" system, follow the instructions in the *EMC vCloud Director Data Protection Extension POC Deployment Guide* for an expedited installation procedure.

For a production system installation, follow the instructions in the *EMC vCloud Director Data Protection Extension Deployment Guide*.

Add one or more backup appliances

Backup appliances allow the vCD SA to associate backup capacity with Org VDCs, and they facilitate the backup and recovery operations on Avamar. The backup gateway component requires credentials to vCloud resource vCenter servers, similar to the way Avamar systems require credentials. These credentials are provided through the backup appliance entity.

The vCD SA can add multiple backup appliances if needed, and use them simultaneously to extend backup capacity based on the size of your cloud. See Adding a backup appliance on page 22 for instructions.

Note

If needed, after creating a backup appliance, you can add additional vCenters managed by your vCloud Director. Also, if your vCenter or appliance credentials change on those remote systems, you can update the backup appliance copy.

Register vCloud Director organizations and add backup repositories

The vCD SA must first register the organizations with the vCD Data Protection Extension. Registering an organization allows the vCD SA to associate any of its VDCs with a backup appliance, and to assign backup and replication policies to it. See Configuring organizations and repositories on page 23 for instructions.

Create backup policies

Backup policies allow you to control backup schedules and retention periods. To create a backup policy, the vCD SA must first create policy templates and organize them into catalogs. The vCD SA can then apply the policy to Org VDCs and to vApps. See Configuring backup policy templates on page 27 and Creating a backup policy for an Org VDC on page 30 for instructions.

CHAPTER 2

Configuration

This chapter includes the following topics:

Adding a backup appliance

To configure the vCD Data Protection Extension to perform backups and restores, you must log in to the plug-in as the vCD SA, and add at least one backup appliance.

To add a new backup appliance, you need the name or address, and the credentials of the backup gateway server associated with your Avamar backup store. Then you can add vCenters that are being managed by vCloud Director to the backup appliance. (These vCenters contain the Org VDCs and the vApps that you want to back up.)

Procedure

1. Log in to the vCD Data Protection Extension:
   a. Open a web browser, and navigate to the following URL:

      `https://UI_server/vcp-ui-server/vcp-ui/`

      where *UI_server* is the IP address or FQDN of the UI server.

   b. Log in using the vCD system administrator credentials (vCD SA) and organization (i.e. "system").

      The vCD OA cannot add backup appliances.
2. Select **Configure** > **Backup Appliances** in the main menu.
3. In the **Backup Appliances** pane, click **Add**.

   The **Add Backup Appliance** dialog box opens.
4. Type a name and a description for the backup appliance.
5. Type the URL of the backup gateway server that is associated with the Avamar backup store.

   An example URL is shown here:
   `https://hostname.vcloud.emc.com:8443`
6. Type the Avamar Management Console administrator's user name and password.
7. Leave the **Enabled** option checked if you want the backup appliance to be available for performing backups and restores.
8. Click **Next**.

   The vCD Data Protection Extension attempts to log in to the backup gateway server to verify the connection. When the verification has completed, the vCenters that are connected to vCloud Director are displayed.
9. Click **Register Now** next to a vCenter to register it.

   The **vCenter Registration** dialog box opens.
10. In the **vCenter Registration** dialog box, type the vCenter's user name and password, and click **Register**.
11. Click **Finish**.

    The vCenter is now displayed in the **vCenters** pane.

Configuring organizations and repositories

To configure a cloud organization, you must first register the organization with the vCD Data Protection Extension. Registering an organization allows you to associate any of its Org VDCs with a backup appliance and to assign backup policies to it.

After you have registered an organization, you can then add a backup repository to it. A repository associates a backup store with the Org VDCs, and is required for performing backups and restores. You can add multiple backup repositories to the Org VDCs; however, only one backup repository per Org VDC can be active for backups at a time.

Procedure

1. Log in to the vCD Data Protection Extension:
   a. Open a web browser, and navigate to the following URL:
      `https://UI_server/vcp-ui-server/vcp-ui/`
      where *UI_server* is the IP address or FQDN of the UI server.
   b. Log in using the vCD SA credentials and organization (i.e. "system").
      The vCD OA cannot configure organizations or repositories.
2. On the vCD Data Protection Extension's main menu, select **Configure** > **Organizations**.
   The organizations that are in vCloud Director are listed in the **Organizations** pane.
3. Select an organization in the **Organizations** list.
   The organization's name, ID, and registration status appear in the right-hand pane. If the organization has not been registered with the vCD Data Protection Extension, the **Register** button is active.
4. Click **Register**.
   When the organization has been registered, a green check mark appears.
5. In the **Organizations** pane, under the organization that you have registered, select the Org VDC to which you want to add a repository.
6. In the right-hand pane, click **Add** in the **Repositories** tab.
   The **Add Repository for *Org _VDC_name* Organization VDC** dialog box opens.
7. Type a name and a description for the repository. You can use any name and description that you want.
8. Leave the **Enabled** option selected if you want this repository to be available for backup and recovery.
9. Adjust the **Total Bytes Allowed** and **Bytes Allowed Per Day** settings if needed.
   These settings are for notification purposes only. If a set limit is reached, a "limit reached" notification is created.
10. Under **Select Backup Store**, select a backup store listed under one of the backup appliances, and click **Add**.

Note

You must select a backup store that is not already being used by another repository on that Org VDC.

CHAPTER 3

Backup

This chapter includes the following topics:

Best practices

The following best practices apply to performing backups using the vCD Data Protection Extension:

- After you have run a successful backup, make sure to create an Avamar checkpoint if you have not done so already. Instructions are provided in Creating an Avamar checkpoint on page 34.
- The vCloud Director Data Protection Extension plug-in does not support the backup or restore of fast-provisioned VMs. Do not back up vApps and VMs that have been fast provisioned. If you do this, any attempted restore will fail.
- Use the vCD Data Protection Extension's GUI or the Backup Extensions to vCloud Director REST API to manage backups, backup policies, and backup retention periods. Using the Avamar Management Console to perform these tasks is not supported.

vApp and VM characteristics captured in a backup

The following table lists the vApp characteristics that are captured in a backup.

Table 2 vApp characteristics captured in a backup

Item	Recorded in backup	Recoverable	Automatically restored	Restorable through UI
Lease settings	Yes	Yes	No[a]	Yes
Startup section	Yes	Yes	No	Yes
Network configuration section	Yes	Yes	No	Yes
Owner	Yes	Yes	No[b]	No
ControlAccess	Yes	Yes	No	No
Metadata	Yes	Yes	Yes/No[c]	No
Snapshot description	Yes	No	No	No
Date created	Yes	No	No	No
vApp name	Yes	Possibly[d]	No[e]	Yes
vApp description	Yes	Yes	No	Yes
ProductSection	Yes[f]	Yes	No	No

a. A LeaseSettingSection is a parameter on a restore to new operation. This can be the original setting or a completely new lease setting.
b. An Owner is a parameter on a restore to new operation. This can be the original owner or a completely new owner.
c. Yes on restore to new; no on restore to original (rollback).
d. In a vApp restore to new, recovering the original vApp name is possible only if the name is no longer in use.
e. A vApp name is a parameter on a restore to new operation. This can be set to the original vApp name, if the name is not in use.
f. ProductSection is not present in all vApps, but will be captured if it is present.

The following table lists the VM characteristics that are captured in a backup.

Table 3 VM characteristics captured in a backup

Item	Recorded in backup	Recoverable	Automatically restored	Restorable through UI
NetworkConnectionSection	Yes	Yes	No	No
GuestCustomization	Yes	Yes	No	No
RuntimeInfoSection	Yes	No	No	No
SnapshotSection	Yes	No	No	No
DateCreated	Yes	No	No	No
StorageProfile	Yes	Yes	No	No
ProductSection	Yes[a]	Yes	No	No
VM name	Yes	Yes	Yes	Yes
VM description and configuration (CPUs and memory)	Yes	Yes	No	Yes
Metadata	Yes	Yes	Yes/No[b]	No

a. ProductSection is not present in all VMs. If it is present it will be captured in the VM backup.
b. Yes on restore to new; no on restore to original (rollback).

Configuring backup policy templates

A backup policy template is a combination of a backup schedule, a retention period, and an option set. Backup policies, which are created using policy templates, control when vApps are backed up, how long to keep the backups, and which, if any, options will be invoked during the backup process.

To create a backup policy template, you must first create at least one schedule, one retention period, and one option set. Then you can create a catalog to which you add backup policy templates.

The following sections provide instructions for performing all of the steps necessary to create backup policy templates and catalogs.

Procedure

1. Open a web browser, and navigate to the following URL:

   `https://`*`UI_server`*`/vcp-ui-server/vcp-ui/`

   where *UI_server* is the IP address or FQDN of the UI server.

2. Log in using vCD SA credentials and organization (i.e. "system").

   The vCD OA cannot configure backup policy templates.

Creating a backup schedule

A backup schedule defines a repeating time period determining when and how often a backup is attempted. Backup schedules are tied to specific time zones. You can create as many backup schedules as you need.

Procedure

1. On the vCD Data Protection Extension's main menu, select **Configure** > **Policy Templates**.
2. In the left pane, click **Schedules** to expand the list of schedules.
3. Click **Add**.

   The **New Schedule** dialog box opens.
4. Type a name and a description for the schedule.
5. Under **Repeat This Schedule**, select **Daily**, **Weekly**, **Monthly**, or **On Demand**, and configure the options accordingly.
6. Select the time zone where the vCD Data Protection Extension is running.
7. Under **Activation Constraints**, select a **Delay Until** date and an **End After** date.
8. Click **Create**.

Creating a backup retention period

A backup retention period determines how long backups will be kept before being deleted. A retention period can be a fixed calendar date or an elapsed time period. You can create as many backup retention periods as you need.

Procedure

1. On the vCD Data Protection Extension's main menu, select **Configure** > **Policy Templates**.
2. In the left pane, click **Retentions** to expand the list of retentions.
3. Click **Add**.

   The **New Retention** dialog box opens.
4. Type a name and a description for the retention.
5. Select an option under **Retention Policy Settings**, or select **Enable Adaptive Retention**:
   - Retention policy settings apply to all of the backups that will use the policy.
   - Adaptive retention settings let you select how long to keep backups based on whether they are daily, weekly, monthly, or yearly backups.
6. Click **Create**.

Creating a backup option set

A backup option set is a collection of Avamar plug-in options that will be invoked during the backup process. You can create as many backup option sets as you need.

By default, you should create an option set named "No Options" that has no flags or values.

Procedure

1. On the vCD Data Protection Extension's main menu, select **Configure** > **Policy Templates**.
2. In the left pane, click **Options** to expand the list of backup options.
3. Click **Add**.

   The **New Options** dialog box opens.
4. Type a name and a description for the option set.

   Note

   Do not specify any flags unless instructed to do so by EMC Support.

   The flags and values that can be specified for either vApp or VM (with Support's help) are listed in the following table.

Flags	Values
`debug`	• true • false
`[avtar]encrypt-strength`	• high • none

5. Click **Create**.

Creating a catalog of backup policy templates

A catalog holds a collection of backup policy templates. A backup policy template is a combination of a backup schedule, a backup retention, and a backup option set. When you create a catalog, you can create and add as many backup policy templates to the catalog as needed. These templates are then used when creating backup policies for Org VDCs.

You can create as many catalogs as needed.

Procedure

1. On the vCD Data Protection Extension's main menu, select **Configure** > **Policy Templates**.
2. In the left pane, click **Catalogs** to expand the list of policy template catalogs.
3. To add a new catalog:
   a. Click **Add**.

      The **New Catalog** dialog box opens.

   b. Type a name and a description for the catalog, and click **Create**.
4. In the **Policy Templates** pane, select the catalog to which you want to add backup policy templates.
5. In the **Catalog Templates** pane, click **Add**.

   The **New Template** dialog box appears.
6. Type a name and a description for the backup policy template.

7. Select a **Schedule**, a **Retention**, and an **Options** template.

   If you want to create a new schedule, retention, or options template, you can click **Create** next to the respective list, and then click **Add** to open the dialog box in which to configure the new template.

8. Click **Create** in the **New Template** dialog box.

Creating a backup policy for an Org VDC

You must create a backup policy, assign it to an Org VDC, and specify it as the default policy to protect all of the vApps that the Org VDC contains.

Before you can create a backup policy for an Org VDC, you must have created at least one backup policy template. Configuring backup policy templates on page 27 provides instructions.

Procedure

1. Log in to the vCD plugin:
   a. Open a web browser, and navigate to the following URL:

      `https://UI_server/vcp-ui-server/vcp-ui/`

      where *UI_server* is the IP address or FQDN of the UI server.

   b. Log in using vCD SA credentials and organization (i.e. "system").

      The vCD OA cannot create backup policies.

2. On the vCD Data Protection Extension's main menu, select **Configure** > **Organizations**.
3. In the **Organizations** pane, click an organization to expand the list of VDCs that it contains.
4. Select the Org VDC to which you want to apply a backup policy.
5. Select the **Policies** tab.

   The **Policies** panel is displayed in the center pane.

6. Click **Add**.
7. In the **Add policy** dialog box, select a policy template from the list.

   The template's details, and name and description are displayed.

8. Modify the policy name and description, and click **Add**.
9. If you want to modify the policy's summary, schedule, retention, or option set:
   a. Select the checkbox next to the policy.

      The **Policy - *policy name*** panel appears.

   b. Select the **Summary**, **Schedule**, **Retention**, and **Option Set** tabs as needed to display the information that you want to modify.

   c. Modify the settings as needed, and click **Update**.

10. Create additional backup policies for the Org VDC as needed.

Managing backup policies

You can manage backup policies by modifying and deleting them, and by setting a default backup policy for an Org VDC.

Before using these instructions, make sure you have performed the previous procedure, Creating a backup policy for an Org VDC on page 30.

Procedure

1. Open a web browser, and navigate to the following URL:

   `https://UI_server/vcp-ui-server/vcp-ui/`

   where *UI_server* is the IP address or FQDN of the UI server.
2. Log in using vCD SA credentials and organization (i.e. "system").

   The vCD OA cannot create backup policies.

Modifying a backup policy

You can modify a backup policy's name, description, schedule, retention, and option set as needed.

Procedure

1. On the vCD Data Protection Extension's main menu, select **Configure** > **Organizations**.
2. In the **Organizations** pane, click an organization to expand the list of VDCs that it contains.
3. Select the Org VDC to which you want to apply a backup policy.
4. Select the **Policies** tab.

   The **Policies** panel is displayed in the center pane.
5. Select the check box next to the policy that you want to modify.

   The **Policy - *policy name*** panel appears on the right-hand side of the screen.
6. Select the **Summary**, **Schedule**, **Retention**, and **Option Set** tabs as needed to display the information that you want to modify.
7. Make your changes as needed, and click **Update**.

Setting a default backup policy

Setting a default backup policy is not required, however it is recommended. A default backup policy will be applied automatically to all of the vApps within the Org VDC. If more than one policy exists for the VDC, you can set any of the policies as the default as needed; however, only one backup policy can be the default policy at a time.

Note

When you configure your backups, you can assign an alternate policy to a vApp, if needed, to override the default policy. For instructions, see Applying a non-default backup policy template to a vApp on page 32.

Procedure

1. On the vCD Data Protection Extension's main menu, select **Configure** > **Organizations**.
2. In the **Organizations** pane, click an organization to expand the list of VDCs that it contains.
3. Select the Org VDC to which you want to set a default policy.
4. Select the **Policies** tab.

   The **Policies** panel is displayed in the center pane.
5. In the **Policy** pane, click the check box next to the policy that you want to use as the Org VDC's default policy.
6. Click **Default**.

Deleting a backup policy

If you have specified a default backup policy, that policy cannot be deleted. When a default policy exists and you delete a non-default backup policy, any vApps that are assigned to the non-default policy will automatically be reassigned to the default policy. However, if a default policy does not exist, you cannot delete a non-default policy that has vApps assigned to it.

Procedure

1. On the vCD Data Protection Extension's main menu, select **Configure** > **Organizations**.
2. In the **Organizations** pane, click an organization to expand the list of VDCs that it contains.
3. Select the Org VDC from which you want to delete a backup policy.
4. Select the **Policies** tab.

   The **Policies** panel is displayed in the center pane.
5. Select the check box next to the policy that you want to delete, and click **Delete**.
6. Click **Yes** to confirm the deletion.

Applying a non-default backup policy template to a vApp

You can override the default backup policy for a particular vApp by applying a different policy to that vApp.

Procedure

1. On the vCD Data Protection Extension's main menu, select **Backup**.
2. Click an organization in the **Organizations** list to expand the list of VDCs that it contains.
3. Select the Org VDC that contains the vApp to which you want to apply the non-default policy.

   Summary and configuration information, and a list of vApps contained in that Org VDC are displayed in the right pane.
4. Select the check box next to the vApp to which you want to apply the policy.
5. Click **Apply Policy**, and select a policy from the list, or select **Create Policy** to create a new one.

You should see a pop-up message saying that the policy was applied to the vApp.

Deleting or editing existing backups

You can delete selected backups, or you can edit their expiration dates.

Procedure

1. Log in to the vCD plugin as follows:
   a. Open a web browser, and navigate to the following URL:
      `https://UI_server/vcp-ui-server/vcp-ui/`
      where *UI_server* is the IP address or FQDN of the UI server.
   b. Enter the vCD SA or vCD OA credentials and organization ("system" for vCD SA).
2. On the vCD Data Protection Extension's main menu, select **Restore**.
3. Click an organization in the **Organizations** list to expand the list of VDCs that it contains.
4. Select the VDC whose backup you want to delete or edit.
5. In the **Repository Summary** pane, select the repository where the backup is located.
6. In the **vApp Inventory** tab, click the name of the vApp.
   The backups that exist for that vApp are displayed in the **Backup Inventory** pane.
7. Click the checkbox next to the backup that you want to delete or edit, and click **Edit Retention**.
8. In the **Edit Retention** dialog box, either select **Delete Now**, or select a new expiration date, and click **Update**.

Performing an ad hoc backup

You can back up one or more vApps at any time by performing an ad hoc backup.

Procedure

1. Log in to the vCD plugin:
   a. Open a web browser, and navigate to the following URL:
      `https://UI_server/vcp-ui-server/vcp-ui/`
      where *UI_server* is the IP address or FQDN of the UI server.
   b. Log in using vCD system administrator credentials.
2. On the vCD Data Protection Extension's main menu, select **Backup**.
3. Click an organization in the **Organizations** list to expand the list of VDCs that it contains.
4. Select the Org VDC for which you want to perform the ad hoc backup.
   Information about the Org VDC appears in the right-hand portion of the window, including the list of vApps that it contains.
   The eligibility of a vApp to be backed up on an ad hoc basis depends on its status, which is displayed in the **Backup Eligibility** and **Status** columns of the

vApps pane. The Backup Eligibility of each vApp is indicated by one of three icons, which represent "eligible for backup," "questionable for backup," and "not eligible for backup." Ad hoc backups can only be performed on backups that are in eligible or questionable status.

Indicator	Eligibility	Statuses
	**Eligible**—The client application requests ad hoc backups for these vApps.	• Suspended • Stopped • Powered on • Powered off • Resolved
	Questionable—The client application requests the ad hoc backup, and relies on the server to report success or failure.	• Waiting for user input • Unknown • Unrecognized • Inconsistent state • Mixed
	**Not Eligible**—The client application blocks you from performing an ad hoc backup for these vApps.	• Failed to create • Unresolved **Note** vApps that do not have VMs are also not eligible for backup.

5. Select the check boxes next to the **Eligible** or **Questionable** vApps that you want to back up.
6. Click **Backup**.
7. Select **Monitor** > **In Progress** on the main menu if you want to view the backup's progress.

Creating an Avamar checkpoint

After you have configured the vCD Data Protection Extension, and run a successful backup, you should create and validate an Avamar checkpoint in case you ever need to roll back the system to a known working state.

Information about checkpoints, including how to create, validate, and roll back to one, is provided in the *EMC Avamar Administration Guide* in the "Advanced Server Administration and Maintenance" chapter.

CHAPTER 4

Restore

This chapter includes the following topics:

Best practices

The following best practices apply to performing backups using the vCD Data Protection Extension:

- Use the vCD Data Protection Extension's GUI or the Backup Extensions to vCloud Director REST API to manage restores. Using the Avamar Management Console to do this is not supported.
- The vCloud Director Data Protection Extension does not support the backup or restore of fast-provisioned VMs:
  - Do not attempt to restore a vApp that was fast provisioned when it was backed up. If you do this, the restore will fail.
  - Do not restore any vApp backup, fast-provisioned or not, to a fast-provisioned vCD.

Restoring a vApp or a VM to the original Org VDC

You can browse a list of vApps that exist in vCloud Director, and select the backup that you want to restore from a backup repository. You can then restore a vApp or a VM to its original location on the Org VDC, or you can restore a vApp to a new location on the VDC.

Note

Fast provisioning is not supported by the vCD Data Protection Extension. It you attempt to restore a vApp that was fast provisioned when it was backed up, the restore will fail.

Before you can restore a backup, the Org VDC must have a backup repository associated with it. Configuring organizations and repositories on page 23 provides instructions.

The following sections provide instructions for performing all of the steps necessary to restore a vApp or a VM to the original Org VDC.

Before using these instructions, log in to the vCD Data Protection Extension.

Procedure

1. Open a web browser, and navigate to the following URL:

   `https://UI_server/vcp-ui-server/vcp-ui/`

   where *UI_server* is the IP address or FQDN of the UI server.
2. Log in using vCD SA or vCD OA credentials and organization ("system" for vCD SA).

Locating a backup to restore

Procedure

1. On the vCD Data Protection Extension's main menu, select **Restore**.
2. Click an organization in the **Organizations** list to expand the list of VDCs that it contains.
3. Select a VDC in the list.

Information about the VDC is displayed.

4. In the **Repository Summary** pane, select the repository where the backup that you want to restore is located.
5. In the **vApp Inventory** tab, click the name of the vApp that you want to restore.

   The backups that exist for that vApp are displayed in the **Backup Inventory** pane.
6. In the **Backup Inventory** pane, click the checkbox next to the backup that you want to restore.

   You can click a backup's date/time identifier to see details about the backup.
7. Click **Restore**, and select one of the options: **Restore New** or **Restore Original**.

   Depending on your selection, follow the instructions in Restoring a vApp to a new location on the Org VDC on page 37 or in Restoring a vApp or a VM to the original location on the Org VDC on page 38.

Restoring a vApp to a new location on the Org VDC

The **Restore New** option will restore a new copy of a vApp on the Org VDC. When you select **Restore New**, the **New vApp Details** dialog box opens.

Note

This procedure works only for vApps, not for individual VMs.

Procedure

1. In the **New vApp Details** dialog box, type a name and a description for the new vApp, and click **Next**.
2. In the **Virtual Machines** pane, review the VMs in the vApp, and click **Next**.

   The VMs in the vApp are listed in the **Virtual Machines in vApp** pane.
3. Click **Next**.

   The **Leases** pane appears.
4. If you want to restore the runtime and storage leases when the vApp is restored, select **Restore leases**.
5. Click **Next**.

   The **Start Order** pane appears. The **Restore start order** option is selected by default.
6. Clear the **Restore start order** checkbox only if you do not want to restore the order in which the VMs were configured to start when the backup occurred.
7. Click **Next**.

   The **Networks** pane appears. Any network configurations that existed when the backup occurred are displayed.
8. If you want to restore the network configurations, select **Restore networks**.
9. Click **Next**.

   The **Network Connections** pane appears.
10. Select **Connected** if you want the network to connect when the vApp is restored.

11. Click **Finish** to initiate the restore.

    You should see a pop-up message stating that the restore is starting.

12. If you want to view the restore's progress, select **Monitor** > **In Progress** on the vCD Data Protection Extension's main menu.

    You can also see the restore's progress in the vCenter by selecting **Inventory** > **VMs and Templates** > **EMCAvamarRestoresInProgress**.

Restoring a vApp or a VM to the original location on the Org VDC

The **Restore Original** option overwrites the original vApp or VM on the Org VDC. When you select **Restore Original**, the **Choose Restore Type** dialog box opens, and you can select **vApp** or **Virtual Machine**.

Depending on your selection, follow the instructions in Restoring a vApp to its original location on page 38 or in Restoring a VM to its original location on page 39.

Restoring a vApp to its original location

When you restore a vApp to its original location, VMs that were deleted from the vApp after the last backup occurred will be restored. You can also select whether to restore VMs that have been added since the last backup.

Note

You must stop a vApp before you restore it.

Procedure

1. In the **Choose Restore Type** dialog box, select **vApp**, and click **Next**.

   The **Restore Original vApp** dialog box opens to the **Virtual Machines** pane. If any disk configurations have changed in the VMs associated with a vApp since the previous backup, you see the warning message:

   ```
   Virtual machine(s) within this vApp will be recreated due
   to disk configuration changes. This will cause a change to
   the virtual machine's id.
   ```

   These VMs will be recreated with a new ID when the vApp is restored.

2. In the **Virtual Machines** pane, select **Delete VMs that were not part of this backup** if you want to restore only those VMs that existed when the backup occurred.
3. Click **Next**.

   The **Start Order** pane appears.

4. Select **Restore start order** if you want to restore the order in which the VMs were configured to start at the time the backup occurred.
5. Click **Next**.

   The **Networks** pane appears. Any network configurations that existed when the backup occurred are displayed.

6. If no networks were found in the backup, click **Finish** to initiate the restore.
7. If networks were found and you want to restore the network configurations:

   a. Select **Restore networks**, and click **Next**.

      The **Network Connections** pane appears.

b. Select **Connected** if you want the network to connect when the vApp is restored.

c. Click **Finish** to initiate the restore.

You should see a pop-up message stating that the restore is starting.

8. If you want to view the restore's progress, select **Monitor** > **In Progress** on the vCD Data Protection Extension's main menu.

   You can also see the restore's progress in the vCenter by selecting **Inventory** > **VMs and Templates** > **EMCAvamarRestoresInProgress**.

Restoring a VM to its original location

When you choose to restore a VM, you can select from a list of VMs contained in the vApp. You can restore only one VM at a time.

Note

You must power down a VM before you restore it.

Procedure

1. In the **Choose Restore Type** dialog box, select **Virtual Machine**, and click **Next**.

   The **Restore Individual VM** dialog box opens and displays a list of the VMs in the backup.

2. Select the VM that you want to restore, and click **Next**.

   The **Review Disks** pane appears, and the VM's hard disks are listed under **Disks in backup**.

   If a configuration change has occurred on one or more of the VM's disks, the changed disks are indicated with a red warning icon and the following message is displayed:

   ```
   Unable to restore this virtual machine. The configuration
   of the disk(s) has changed since the backup.
   ```

   If a disk configuration has changed, you currently have the following choices:

   - Restore the vApp to which this VM belongs. If you do this, all of the VMs in the vApp with changed disk configurations will be recreated, and all other VMs in the vApp will be restored.
   - Cancel the restore.

3. Clear the **Restore virtual machine configuration (CPUs, memory)** option only if you do not want to restore the VM's configuration.
4. Click **Finish** to start the restore.
5. Select **Monitor** > **In Progress** on the vCD Data Protection Extension's main menu to view the restore's progress.

   You can also see the restore's progress in the vCenter by selecting **Inventory** > **VMs and Templates** > **EMCAvamarRestoresInProgress**.

Restoring a deleted vApp

You can restore vApps that have been deleted from vCloud Director since the previous backup. A deleted vApp will be restored to the Org VDC from which it was deleted.

Procedure

1. On the vCD Data Protection Extension's main menu, select **Restore**.
2. Click an organization in the **Organizations** list to expand the list of VDCs that it contains.
3. Select a VDC in the list.
4. In the **Repository Summary** pane, select the repository where the backup that you want to restore is located.
5. Select the **Deleted vApp Inventory** tab.
6. Click the name of the vApp that you want to restore.

   The backups that exist for that vApp are displayed in the **Backup Inventory** pane.
7. In the **Backup Inventory** pane, click the checkbox next to the backup that you want to restore.
8. Click **Restore**.

   The **Restore New vApp** dialog box appears.
9. In the **New vApp Details** pane, type a name and a description for the vApp, and click **Next**.

   The VMs in the vApp are displayed in the **Virtual Machines in vApp** pane.
10. Click **Next**.

    The **Leases** pane appears.
11. If you want to restore the runtime and storage leases when the vApp is restored, select **Restore leases**.
12. Click **Next**.

    The **Start Order** pane appears. The **Restore start order** option is selected by default.
13. Clear the **Restore start order** option only if you do not want to restore the order in which the VMs were configured to start when the backup occurred.
14. Click **Next**.

    The **Networks** pane appears. Any network configurations that existed when the backup occurred are displayed.
15. If no networks were found in the backup, click **Finish** to initiate the restore.
16. If networks were found and you want to restore the network configurations:
    a. Select **Restore networks**, and click **Next**.

       The **Network Connections** pane appears.

    b. Select **Connected** if you want the network to connect when the vApp is restored.

    c. Click **Finish** to initiate the restore.

       You should see a pop-up message stating that the restore is starting.

17. If you want to view the restore's progress, select **Monitor** > **In Progress** on the vCD Data Protection Extension's main menu.

    You can also see the restore's progress in the vCenter by selecting **Inventory** > **VMs and Templates** > **EMCAvamarRestoresInProgress**.

Restoring a vApp to a different Org VDC

You can restore a vApp to an Org VDC that is different from the one on which the vApp was originally installed. To do this, you must use a restore-only repository.

Note

Fast provisioning is not supported by the vCD Data Protection Extension. It you attempt to restore a vApp that was fast provisioned when it was backed up, the restore will fail.

The following sections provide instructions for performing all of the steps necessary to restore a vApp to a different Org VDC. Before using these instructions, log in to the vCD Data Protection Extension.

Procedure

1. Open a web browser, and navigate to the following URL:

   `https://`*`UI_server`*`/vcp-ui-server/vcp-ui/`

   where *UI_server* is the IP address or FQDN of the UI server.

2. Log in using the vCD SA credentials and organization (i.e. "system").

Creating a restore-only repository

To restore a vApp to a different Org VDC, you must first create a restore-only repository. Restore-only repositories are used only for restores, never for backups.

When you create a restore-only repository, you select a source and a destination Org VDC. The source Org VDC is where the vApp that you want to restore is or was originally located; the destination Org VDC is the VDC to which you want to restore the vApp. You must use a restore-only repository when you want to restore:

- A vApp to a different Org VDC
- A vApp that was installed on an Org VDC that has been deleted from vCloud Director
- A vApp backup that was replicated by Avamar

Procedure

1. On the vCD Data Protection Extension's main menu, select **Configure** > **Backup Appliances**.
2. In the **Backup Appliances** pane, select the backup appliance that contains the backup that you want to restore.
3. Select the **Restore Only Repository Sources** tab.

   The clouds on that backup appliance are listed.
4. Click the arrow beside the cloud to expand the list of its organizations.
5. Click the arrow beside an organization to expand the list of its VDCs.

6. Select the Org VDC that contains the vApp that you want to restore, and click **Create Restore Only Repository**.

   The **Create Restore Only Repository** dialog box opens.
7. Type a name and a description for the repository.
8. Leave the **Enabled** option checked if you want the repository to be available for restores.
9. Under **Select Destination Org VDC**, click the arrow beside an organization's name to expand the list of VDCs.
10. Select the Org VDC to which you want to restore the vApp, and click **Create**.

    The restore-only repository is created for this Org VDC.

Restoring the vApp using the restore-only repository

Procedure

1. On the vCD Data Protection Extension's main menu, select **Restore**.
2. Click an organization in the **Organizations** list to expand the list of VDCs that it contains.
3. Select the destination Org VDC (the one to which the vApp will be restored).

   Information about the Org VDC is displayed.
4. In the **Repository Summary** pane, select the restore-only repository in the list of repositories.

   The vApps for the source Org VDC are displayed in the **vApp Inventory** pane.
5. In the **vApp Inventory** tab, click the name of the vApp that you want to restore.
6. In the **Backup Inventory** pane, click the checkbox next to the backup that you want to restore, and click **Restore**.

   The **Restore New vApp** dialog box appears.
7. In the **New vApp Details** pane, type a name and a description for the vApp, and click **Next**.

   The VMs in the vApp are displayed in the **Virtual Machines in vApp** pane.
8. Click **Next**.

   The **Leases** pane appears.
9. If you want to restore the runtime and storage leases when the vApp is restored, select **Restore leases**.
10. Click **Next**.

    The **Start Order** pane appears. The **Restore start order** option is selected by default.
11. Clear the **Restore start order** checkbox only if you do not want to restore the order in which the VMs were configured to start when the backup occurred.
12. Click **Next**.

    The **Networks** pane appears. Any network configurations that existed when the backup occurred are displayed.
13. If no networks were found in the backup, click **Finish** to initiate the restore.
14. If networks were found and you want to restore the network configurations:

a. Select **Restore networks**, and click **Next**.

The **Network Connections** pane appears.

b. Select **Connected** if you want the network to connect when the vApp is restored.

c. Click **Finish** to initiate the restore.

15. If you want to view the restore's progress, select **Monitor** > **In Progress** on the vCD Data Protection Extension's main menu.

You can also see the restore's progress in the vCenter by selecting **Inventory** > **VMs and Templates** > **EMCAvamarRestoresInProgress**.

Performing file-level restores

The FLR (file-level restore) UI server, accessed through a web server, allows you to restore specific files and folders from a source VM that is contained in a vApp backup to a folder in a destination VM contained in a vApp within vCloud Director. You can restore files and folders either to the original machine or to a different machine.

Before you begin

To perform file-level restores:

- You must have vCloud Director credentials to log in to the FLR UI server to browse the source VM for the files or folders you want to restore.
- You must be able to log in to the destination VM to browse to the location where the files or folders will be restored.
- The source VM must exist in vCloud Director.
- The destination VM must be powered on and registered with the vCloud Director Data Protection Extension, and it must have VMware Tools installed.

Note

The file-level restore feature supports restoring files or folders from a Windows backup to a Windows machine and from a Linux backup to a Linux machine.

Procedure

1. In a web browser, navigate to the following URL:

`https://FLR_UI_server:5481/vcp-flr-ui/#/`

The **EMC Cloud Data Protection Restore Client** login dialog box opens.

2. Enter your vCloud Director credentials, and click **Login**.

The **Select the Organization to restore from screen** appears.

3. Double-click the organization from which you want to restore, and click **Next**.

The **Select the Virtual Datacenter to restore from** screen appears.

4. Double-click the data center from which you want to restore, and click **Next**.

The **Select the vApp to restore from screen** appears.

5. Double-click the vApp from which you want to restore, and click **Next**.

The **Select the Backup to restore from screen** appears.

6. Double-click the backup from which you want to restore, and click **Next**.

The **Select the VM to restore from** screen appears.

7. Double-click the VM from which you want to restore, and click **Next**.

   The **Select items to restore screen** appears.

8. Browse to the files or folders that you want to restore, double-click them (or drag them to the **Selected Items** pane), and click **Next**.

   The **Select destination to restore to screen** appears, open on the **Select Organization** tab.

9. Double-click the name of the organization to which you want to restore, and click **Next**.

   The **Select Data Center** tab opens.

10. Double-click the name of the data center to which you want to restore, and click **Next**.

    The **Select vApp** tab opens.

11. Double-click the name of the vApp to which you want to restore, and click **Next**.

    The **Select VM** tab opens.

12. Double-click the name of the VM to which you want to restore, and click **Next**.

    The **Enter credentials of *VM_name*** dialog box opens.

13. Enter the destination VM's credentials, and click **Login**.

    After you have successfully logged in, the **Select Folder** tab opens.

14. Browse to the location to which you want to restore, double-click it, and then click **Finish**.

    The **Restore Confirmation** dialog box opens.

15. Click **Yes** to start the restore.

16. If you want to watch the progress of the restore, click the arrow button located in the lower-right corner of the **EMC Cloud Data Protection Restore Client** window.

    The **Restore Monitor** opens, and you can click the **Refresh** button as the restore progresses to see its progress.

    Note

    You can also watch the progress of the restore in the Avamar Administrator's Activity Monitor if you want.

CHAPTER 5

Replication

This chapter includes the following topics:

Replicating vApp backups

Replication is a feature that enables efficient, encrypted, and asynchronous replication of data stored on an Avamar server to another Avamar server that is deployed in a remote location.

The vCD Data Protection Extension provides the capability to replicate the vApp backups that it has created to a destination Avamar server. To replicate backups, you must create a replication policy and then apply the policy to the vApps whose backups you want to replicate.
The following sections provide instructions for performing all of the steps necessary to replicate vApp backups.

Procedure

1. Open a web browser, and navigate to the following URL:

   `https://`*`UI_server`*`/vcp-ui-server/vcp-ui/`

   where *UI_server* is the IP address or FQDN of the UI server.
2. Log in using vCD SA credentials and organization (i.e. "system").

   The vCD OA cannot replicate vApp backups.

Creating a replication policy

Replication policies define the location to which vApp backups will be replicated, when the backups will be replicated, and how long the replicated backups will be retained.

Procedure

1. On the vCD Data Protection Extension's main menu, select **Configure** > **Organizations**.
2. Click an organization in the **Organizations** list to expand the list of VDCs that it contains.
3. Select the Org VDC for which you want to configure a replication policy.
4. In the **Repositories** tab, select the active repository to display its details.
5. In the **Repository Details** pane, select the **Replication Policies** tab, and click **Add**.

   The **Create Replication Policy** wizard opens.
6. In the **Policy Details** pane:
   a. Type a name and a description for the replication policy.
   b. Select replication filter options:
      - **Encryption Enabled** — By default, encryption is enabled and set to high. Clear the **Encryption Enabled** checkbox only if you want to turn off encryption for this policy.

        Note

        If you set Encryption to **None**, refer to the Avamar documentation on disabling the firewall settings.
      - **Bandwidth limit** — The network bandwidth, up to 2400 Mbps, that will be used for replication.

- **Maximum Backups per Account** — The maximum number of backups for each vApp that will be replicated by this policy. If you do not want to limit the number of backups, select **No limit**.
- **Backup Age Restriction** — The age of the backups that will be replicated by this policy. If you do not want an age restriction, select **None**.

c. Click **Next**.

7. In the **Destination** pane:
   a. For **Destination Address**, specify the IP address or the FQDN of the Avamar server to which you backups to be replicated.
   b. For **User Name**, specify the Avamar replication user account ID (repluser) that is used to log in to the destination Avamar server.
   c. For **Password**, specify the password for the Avamar replication user account ID (repluser).
   d. Click **Next**.
8. In the **Schedule** pane:
   a. Select the options for how often and what time you want the replication policy to run.
   b. Under **Activation Constraints**, select the date range during which you want the policy to ve available for use.
   c. Click **Next**.
9. In the **Retention** pane:
   a. If you want to change the retention period that was originally specified for the backup, select **Override backup expiration**, and select a new expiration time.
   b. Click **Next**.
10. In the **Summary** pane, review the replication policy settings. Use the **Back** button to make changes if necessary.
11. Click **Finish** when you are ready to save the policy.

    The new policy is displayed in the **Replication Policies** list.

Applying a replication policy to one or more vApps

You must apply a replication policy to the vApps whose backups you want to replicate.

Procedure

1. On the vCD plug-in's main menu, select **Restore**.
2. Click an organization in the **Organizations** list to expand the list of VDCs that it contains.
3. Select a VDC in the list.

   The active repository is selected in the list of repositories, and the vApps in the VDC are listed in the **vApp Inventory** tab.

Note

Replication policies are applicable only to the active backup repository. If this repository becomes inactive, the replication policies associated with it will be disabled and all vApps removed from them. If the repository is made active again, the replication policies will not be re-enabled and you will have to recreate them.

The vApps in the VCD are listed in the **vApp Inventory** tab.

4. Click the checkbox beside one or more vApps that you want protected by the replication policy.
5. Click **Apply Replication Policy**, and select a policy in the list.

   If you want to create a new replication policy, select **Create Retention Policy** in the list, and follow the instructions provided in Creating a replication policy on page 46.

Managing replication policies

You can manage replication policies by setting a default replication policy for an Org VDC, and by modifying and deleting the policies.

Before using these instructions, log in to the vCD plug-in.

Procedure

1. Open a web browser, and navigate to the following URL:

   `https://UI_server/vcp-ui-server/vcp-ui/`

   where *UI_server* is the IP address or FQDN of the UI server.
2. Log in using vCD SA credentials and organization (i.e. "system").

   The vCD OA cannot replicate vApp backups.

Setting a default replication policy

Optionally, you can set a replication policy as the default policy. The default policy will replicate the vApp backups in the chosen Org VDC that are available in the backup repository.

Procedure

1. On the vCD Data Protection Extension's main menu, select **Configure** > **Organizations**.
2. Click an organization in the **Organizations** list to expand the list of VDCs that it contains.
3. Select the Org VDC for which you want to set a default replication policy.
4. In the **Repositories** tab, select the active repository to display its details.
5. In the **Repository Details** pane, select the **Replication Policies** tab to display the existing policies.
6. Click the checkbox next the policy that you want to set as default, and click **Default**.

   A green check mark appears next to the policy in the **Default** column.

Modifying a replication policy

You can modify a replication policy's name, description, schedule, and retention as needed.

Procedure

1. On the vCD Data Protection Extension's main menu, select **Configure** > **Organizations**.
2. In the **Organizations** pane, click an organization to expand the list of VDCs that it contains.
3. Select the Org VDC for which you want to modify a replication policy.
4. In the **Repositories** tab, select the active repository to display its details.
5. In the **Repository Details** pane, select the **Replication Policies** tab to display the existing policies.
6. Select the replication policy that you want to modify.

   The policies settings are displayed in the **Replication Policy** pane.
7. In the **Replication Policy** pane, select the tab containing the information that you want to modify.
8. Make the necessary modifications, and click **Update**.

Deleting a replication policy

If you have specified a default replication policy, you can delete that policy. When a default policy exists, you can delete a non-default replication policy, and any vApps that are assigned to that policy will automatically be reassigned to the default policy.

Note

You cannot delete a non-default replication policy with attached vApps if no default policy exists.

Procedure

1. On the vCD Data Protection Extension's main menu, select **Configure** > **Organizations**.
2. In the **Organizations** pane, click an organization to expand the list of VDCs that it contains.
3. Select the Org VDC for which you want to delete a replication policy.
4. In the **Repositories** tab, select the active repository to display its details.
5. In the **Repository Details** pane, select the **Replication Policies** tab to display the existing policies.
6. Click the checkbox next the policy that you want to delete, and click **Delete**.
7. Click **Yes** to confirm the deletion.

Restoring replicated vApp backups

To restore replicated backups, you must configure the Avamar server that is storing the backups as a backup appliance. Then you must create a restore-only repository using the backup appliance as the source and the Org VDC to which you want to

restore as the destination. After the backup appliance and the repository have been created, you can then restore replicated backups.

The following sections provide instructions for performing all of the steps necessary to restore vApp backups that have been replicated.

Before using these instructions, log in to the vCD Data Protection Extension.

Procedure

1. Open a web browser, and navigate to the following URL:

   `https://UI_server/vcp-ui-server/vcp-ui/`

   where *UI_server* is the IP address or FQDN of the UI server.

2. Log in using vCD SA credentials and organization (i.e. "system").

   The vCD OA cannot replicate vApp backups.

Configuring a backup appliance

You must configure a backup appliance using the Avamar server that is storing the replicated backups.

Follow the instructions in Adding a backup appliance on page 22, specifying the URL and the credentials of the backup gateway that is associated with the Avamar server on which the replicated backups are being stored.

Creating a restore-only repository

Restoring a replicated vApp backup requires the use of a restore-only repository.

Follow the instructions in Creating a restore-only repository on page 41.

When you create the repository, select the backup appliance that contains the replicated backup that you want to restore.

For the destination Org VDC, select the VDC to which you want to restore the replicated backup.

Restoring replicated backups

Follow the instructions in Restoring the vApp using the restore-only repository on page 42.

Select the restore-only repository that you created for restoring replicated backups.

Performing an ad hoc replication

To perform an ad hoc replication, you must either have created an enabled replication policy and applied it to the vApps whose backups you want to replicate, or you must have assigned a default replication policy, which will replicate all vApp backups in the chosen Org VDC.

Procedure

1. On the vCD Data Protection Extension's main menu, select **Configure** > **Organizations**.
2. Click an organization in the **Organizations** list to expand the list of VDCs that it contains.
3. Select the Org VDC whose vApp backups you want to replicate.

4. In the **Repositories** tab, select the active repository to display its details.
5. In the **Repository Details** pane, select the **Replication Policies** tab, and click the check box next to the replication policy that you want to execute.
6. Click **Replicate Now**.

CHAPTER 6

Reporting

This chapter includes the following topics:

Introduction

Reporting capability is provided for the vCD Data Protection Extension as an optional reporting server and reporting database, which are deployed as single instances per vCloud. To make use of the reporting feature, you must install the reporting server and then deploy the reporting database. The reporting database enables you to generate reports, based on your specific use cases, using SQL statements. The reports must be displayed using your own reporting tools.

This chapter describes the schemas used by the reporting database, and provides example reports, including the SQL statements that were used to generate them.

The following list provides some considerations that you should keep in mind when deploying the reporting server:

- A stand-alone reporting Postgres database server is recommended. Using the vCP Postgres database server is not supported.
- The database server's event tables only hold a system-enforced maximum of 120 days of event activity. However, the `backup_inventory` table record expiration is governed by the `retention_date`, so backup data in the `backup_inventory` table will exist up to the `retention_date`.

  If you want to maintain a history of all activity, you can supply a database with a separate `sync_job` to gather and accumulate the data from the event tables.
- Once the reporting server has successfully connected to the vCloud Director RabbitMQ, then vCP-related events will be delivered to a queue for the reporting server to consume. If you shut down the reporting server, the queue will fill up as events occur and, with nothing to consume the events from the queue, the available disk space on the RabbitMQ server may fill up.

  If you want to decommission a reporting server permanently, identify the RabbitMQ server that the reporting server is using, and use the RabbitMQ administrative UI to remove the VCPReportingEventQueue.
- When the lockbox is created (for example, when the reporting server is started for the first time), an error message is sent to the log file, indicating that the lockbox file was not found. This is not an error.

Reporting system functional overview

The vCD Data Protection Extension platform publishes notification messages on an AMQP-compliant (typically RabbitMQ) messaging server for important system events. The events that the reporting system observes include:

- vAppBackupEvent
- vAppRestoreEvent
- vappReplicationEvent
- vAppRetentionUpdateEvent
- vAppBackupDeleteEvent

For more information, see the *vCloud Protector Message Bus Event Notifications Specification*.

These notifications form the only source of information for the reporting database. The reporting server subscribes to the notifications and publishes them to your database instance. The reporting server is a tcServer application that runs on a

separate VM and requires access to a Postgres database instance. Once the database is populated by the reporting server, you can author your own reports by interfacing directly with this database instance.

The reporting database consists of the following tables:

- T_VAPP_BACKUP_INVENTORY
- T_VAPP_BACKUP_EVENT
- T_VAPP_RESTORE_EVENT
- T_VAPP_REPLICATION_EVENT
- T_VAPP_RETENTION_UPDATE_EVENT
- T_VAPP_DELETE_BACKUP_EVENT

Based on the subscribed notifications, the reporting server maintains a Backup Inventory table, T_VAPP_BACKUP_INVENTORY, and a list of tables that map to the events. The vApp backup inventory is a list of vApp backups that are known to exist by the reporting server, and are current (not expired).

Reporting system database schemas

The following sections describe the database schemas used by the reporting server. Database table key column names are indicated with an asterisk.

T_VAPP_BACKUP_INVENTORY table

When a vAppBackupEvent occurs, a corresponding vApp backup row is created in the T_VAPP_BACKUP_INVENTORY table. Once a vApp backup inventory row exists, if a vAppRetentionUpdateEvent occurs for that vApp, it will result in an update to the corresponding row in the T_VAPP_BACKUP_INVENTORY table. If a user deletes a vApp backup, or if the vApp backup expires, then the vApp backup is removed from the T_VAPP_BACKUP_INVENTORY table.

Replications are not added as backups in the T_VAPP_BACKUP_INVENTORY table.

Table 4 T_VAPP_BACKUP_INVENTORY table schema

Column name	Column data type/size	Description
* vcloud_id	varchar(50)	The vcd provided cloud guid of the backup. Compound db key.
* vapp_id	varchar(50)	The vcd provided vApp guid of the backup. Compound db key.
* vapp_backup_id	varchar(50)	MC provided backup id (sequence). Compound db key.
backup_type	varchar(20)	Adhoc or scheduled
user_id	varchar(60)	The vcd provided user guid for the user who performed the backup
vapp_name	varchar(128)	The name associated with the vapp_id
org_name	varchar(128)	The name associated with the org_id of the backup
org_id	varchar(50)	The vcd-provided org guid for the org of the backup

Table 4 T_VAPP_BACKUP_INVENTORY table schema (continued)

Column name	Column data type/size	Description
org_vdc_name	varchar(128)	The name associated with the org_vdc_id
org_vdc_id	varchar(50)	The vcd provided orgVdc guid of the orgVdc of the backup
owner_id	varchar(50)	The vcd provided owner guid. The user_id of the owner of the vApp being backed up
owner_name	varchar(128)	The name associated with the owner_id
backup_vm_count	integer	Number of VMs existing in the vApp
vms_selected	integer	Number of VMs selected for this backup (set adhoc or as a result of exclusion criteria)
actual_vms	integer	Number of VMs in this backup
backup_host	varchar(120)	Hostname of the backup system (e.g. AVE hostname)
backup_store_name	varchar(60)	GSAN or DataDomain system name
backup_store_id	varchar(50)	GSAN or DataDomain system id
bytes_modified	bigint	The size of the backup, which should closely track bytes protected
bytes_processed	bigint	Should be equal to the size of the VM
start_time	timestamp	Start time of the vApp backup (from BG)
end_time	timestamp	End time of the vApp backup (from BG)
effective_retention	timestamp	How long to keep the vApp backup (when the vApp backup will expire)

T_VAPP_BACKUP_EVENT table

The following table describes the `T_VAPP_BACKUP_EVENT` table.

Table 5 T_VAPP_BACKUP_EVENT table schema

Column name	Column data type/size	Description
* task_id	varchar(60)	The vcd assigned task guid. Db Key.
vcloud_id	varchar(50)	The vcd provided cloud guid
event_version	varchar(20)	The VCP provided event version id (e.g. 1.0)
user_id	varchar(60)	The vcd provided user guid for the user who performed the backup
event_time	timestamp	The VCP provided timestamp of event emission
backup_type	varchar(20)	Adhoc or scheduled

Table 5 T_VAPP_BACKUP_EVENT table schema (continued)

Column name	Column data type/size	Description
vapp_id	varchar(50)	The vcd provided vApp guid of the vApp being backed up
vapp_name	varchar(128)	The name associated with the vapp_id
org_name	varchar(128)	The name associated with the org_id of the backup
org_id	varchar(50)	The vcd provided org guid for the org of the backup
org_vdc_name	varchar(128)	The name associated with the org_vdc_id
org_vdc_id	varchar(50)	The vcd provided orgVdc guid of the orgVdc of the backup
owner_id	varchar(50)	The vcd provided owner guid. The user_id of the owner of the vApp being backed up
owner_name	varchar(128)	The name associated with the owner_id
vapp_backup_id	varchar(50)	MC provided backup id (sequence)
backup_vm_count	integer	Number of VMs existing in the vApp
vms_selected	integer	Number of VMs selected for this backup (set adhoc or as a result of exclusion criteria)
actual_vms	integer	Number of VMs in this backup
backup_host	varchar(256)	Hostname of backup system (e.g. AVE hostname)
backup_store_name	varchar(256)	GSAN or DataDomain system name
backup_store_id	varchar(50)	GSAN or DataDomain system id
bytes_modified	bigint	Matches the size (in bytes) of the backup, which should closely track bytes protected
bytes_processed	bigint	Should equal the size (in bytes) of the VM
start_time	timestamp	Start time of the vApp backup (from BG)
end_time	timestamp	End time of the vApp backup (from BG)
effective_retention	timestamp	How long to keep the vApp backup (when the vApp backup will expire)

T_VAPP_RESTORE_EVENT table

The following table describes the `T_VAPP_RESTORE_EVENT` table.

Table 6 T_VAPP_RESTORE_EVENT table schema

Column name	Column data type/size	Description
* task_id	varchar(60)	The vcd-assigned task guid. Db Key.
vcloud_id	varchar(50)	The vcd-provided cloud guid of the cloud to which the vApp was restored
vapp_id	varchar(50)	The vcd-provided vApp guid of the new instance of the vApp being restored
event_version	varchar(20)	The VCP-provided event version id (for example, 1.0)
user_id	varchar(60)	The vcd-provided user guid for the user who performed the restore
event_time	timestamp	The VCP-provided timestamp of event emission
restore_type	varchar(20)	Single vm, rollback, new
vapp_name	varchar(128)	The name associated with the vapp_id
org_name	varchar(128)	The name associated with the org_id of the restored vApp
org_id	varchar(50)	The vcd-provided org guid for the org of the restored vApp
org_vdc_name	varchar(128)	The name associated with the org_vdc_id
org_vdc_id	varchar(50)	The vcd-provided orgVdc guid of the orgVdc of the restored vApp
owner_id	varchar(50)	The vcd-provided owner guid. The user_id of the source vApp's owner
owner_name	varchar(128)	The name associated with the owner_id
vapp_backup_id	varchar(50)	The MC provided backup id (sequence) of the vApp being restored
vapp_id_dst	varchar(50)	The vcd-provided restore destination vApp guid
vapp_name_dst	varchar(128)	The restore destination vapp name associated with the vapp_id_dst
vcloud_id_dst	varchar(50)	The vcd-provided restore destination cloud guid
org_name_dst	varchar(128)	The restore destination org name associated with the org_id_dst
org_id_dst	varchar(50)	The vcd-provided restore destination org guid
org_vdc_name_dst	varchar(128)	The restore destination org_vdc name associated with the org_vdc_id_dst
org_vdc_id_dst	varchar(50)	The vcd-provided restore destination orgVdc guid

Table 6 T_VAPP_RESTORE_EVENT table schema (continued)

Column name	Column data type/size	Description
owner_id_dst	varchar(50)	The vcd-provided owner guid. The user_id of the owner of the destination vApp
owner_name_dst	varchar(128)	The restore destination owner name associated with the owner_id_dst
source	varchar(20)	The vapp_id of the vApp (the restore is obtained from this vApp)
backup_vm_count	integer	Number of VMs existing in the vApp
vms_selected	integer	Number of VMs selected for this backup (set adhoc or as a result of exclusion criteria)
backup_host	varchar(256)	Hostname of backup (for example, AVE hostname)
backup_store_name	varchar(256)	GSAN or DataDomain system name
backup_store_id	varchar(50)	GSAN or DataDomain system id
bytes_restored	bigint	Matches the size of the backup, which should closely track bytes protected
bytes_processed	bigint	Should equal to size of the VM
start_time	timestamp	Start time of the vApp backup (from BG)
end_time	timestamp	End time of the vApp backup (from BG)

T_VAPP_REPLICATION_EVENT table

The following table describes the `T_VAPP_REPLICATION_EVENT` table.

Table 7 T_VAPP_REPLICATION_EVENT table schema

Column name	Column data type/ size	Description
* vcloud_id	varchar(50)	The vcd-assigned cloud guid. Compound Db Key.
* task_id	varchar(60)	The vcd-assigned task guid. Compound Db Key.
parent_task_id	varchar(60)	The vcd-provided parent task guid. Task id of the overall replication job
parent_user_id	varchar(60)	The vcd-provided parent user guid. UserId of the user that initiated the adhoc replication
event_version	varchar(20)	The VCP-provided event version id (for example, 1.0)
user_id	varchar(60)	The vcd-provided user guid for the user who performed the replication

Table 7 T_VAPP_REPLICATION_EVENT table schema (continued)

Column name	Column data type/ size	Description
event_time	timestamp	The VCP-provided timestamp of event emission
replication_type	varchar(20)	Adhoc or scheduled
vapp_id	varchar(50)	The vcd-provided vApp guid
vapp_name	varchar(128)	The name associated with the vapp_id
org_name	varchar(128)	The name associated with the org_id of the replication
org_id	varchar(50)	The vcd-provided org guid for the org of the replication
org_vdc_name	varchar(128)	The name associated with the org_vdc_id
org_vdc_id	varchar(50)	The vcd-provided orgVdc guid of the orgVdc of the source of the replicated vApp
owner_id	varchar(50)	The vcd-provided owner guid. The user_id of the owner of the vApp being replicated
owner_name	varchar(128)	The name associated with the owner_id
destination_host	varchar(256)	The name of the host to which the vApp will be replicated.
bytes_processed	bigint	Should equal the size of the VM
bytes_modified	bigint	Matches the size of the backup, which should closely track bytes protected
start_time	timestamp	Start time of the vApp backup (from BG)
end_time	timestamp	End time of the vApp backup (from BG)

T_VAPP_RETENTION_UPDATE_EVENT table

When an update backup retention event occurs, the reporting server writes a row in the T_VAPP_RETENTION_UPDATE_EVENT table and attempts to update the corresponding backup row in the T_VAPP_BACKUP_INVENTORY table. If the reporting server is started after activity has occurred, such as vApp backups, the vapp backup row may not exist in the T_VAPP_BACKUP_INVENTORY table. If this is the case, a warning message is logged; however, this message is no cause for alarm, because it is expected under such conditions.

Table 8 T_VAPP_RETENTION_UPDATE_EVENT table schema

Column name	Column data type/ size	Description
* vcloud_id	varchar(50)	The vcd-provided cloud guid. Compound Db Key.
* vapp_id	varchar(50)	The vcd-provided vApp guid. Compound Db Key.

Table 8 T_VAPP_RETENTION_UPDATE_EVENT table schema (continued)

Column name	Column data type/ size	Description
* vapp_backup_id	varchar(50)	The MC-provided backup id (sequence) of the vApp getting its retention updated. Compound Db Key.
* event_time	timestamp	The VCP-provided timestamp of event emission. Compound Db Key.
event_version	varchar(20)	The VCP-provided event version id (for example, 1.0)
user_id	varchar(60)	The vcd provided user guid for the user who updated the backup retention
vapp_name	varchar(128)	The name associated with the vapp_id
org_name	varchar(128)	The name associated with the org_id
org_id	varchar(50)	The vcd provided org guid
org_vdc_name	varchar(128)	The name associated with the org_vdc_id
org_vdc_id	varchar(50)	The vcd provided orgVdc guid
owner_id	varchar(50)	The vcd provided owner guid. The user_id of the owner of the vApp being updated
owner_name	varchar(128)	The name associated with the owner_id
effective_retention	timestamp	How long to keep the vApp backup (when the vApp backup will expire)

T_VAPP_DELETE_BACKUP_EVENT table

When a delete backup event occurs, the reporting server writes a row in the T_VAPP_DELETE_BACKUP_EVENT table and attempts to remove the backup from the T_VAPP_BACKUP_INVENTORY table. If the reporting server is started after activity has occurred, such as vApp backups, the vApp backup row may not exist in the T_VAPP_BACKUP_INVENTORY table. If this is the case, a warning message is logged; however, this message is no cause for alarm, because it is expected under such conditions.

Table 9 T_VAPP_DELETE_BACKUP_EVENT table schema

Column name	Column data type/size	Description
* vcloud_id	varchar(50)	The vcd-provided cloud guid. Compound Db key.
* vapp_id	varchar(50)	The vcd-provided vApp guid. Compound Db key.
* vapp_backup_id	varchar(50)	The MC-provided backup id (sequence) of the vApp being restored. Compound Db key.
event_version	varchar(20)	The VCP-provided event version id (for example, 1.0)

Table 9 T_VAPP_DELETE_BACKUP_EVENT table schema (continued)

Column name	Column data type/size	Description
user_id	varchar(60)	The vcd-provided user guid. The id of the user performing the vApp backup deletion.
event_time	timestamp	The VCP-provided timestamp of event emission
vapp_name	varchar(128)	The name associated with the vapp_id
org_name	varchar(128)	The name associated with the org_id
org_id	varchar(50)	The vcd-provided org guid. The org_id of the vApp backup being deleted.
org_vdc_name	varchar(128)	The name associated with the org_vdc_id
org_vdc_id	varchar(50)	The vcd-provided orgVdc guid. The org_vdc_id of the vApp backup being deleted.
owner_id	varchar(50)	The vcd-provided owner guid. The user_id of the owner of the vApp being deleted.
owner_name	varchar(128)	The name associated with the owner_id

Reporting capability

You can use the vCD Data Protection Extension's reporting database to create a variety of different reports based on your use cases.

Reports can be based on inventory-derived information and on historical information. Various optional ordering criteria can be added, in any combination, to any of the inventory or historical reports, such as endTime, backupType/replicationType, userId, ownerId, bytesProcessed, or bytesModified. Also, an optional date range filter (to match end times or event times) can be added to some queries.

vApp backup inventory based reports

High-level categories for reports based on backup inventory are described in the following table.

Table 10 vApp backup inventory reports

Report	Description
Backup Inventory	At the Org, OrgVdc and vApp levels, the Backup Inventory report shows the vApp backups in the inventory. This report is useful to see what backups exist, and at what level.
Backup Coverage	At the Org or OrgVdc levels, the Backup Coverage report shows protected vApps for which backups have not occurred since a specified time in the past. This report has the potential to return no records.
Frequent User Backup	At the Org level, the Frequent User Backup report shows a list of users and backup counts in descending order. This report is useful to

Table 10 vApp backup inventory reports (continued)

Report	Description
	determine which users are “heavy users,” or which users may be abusing the system.
Owner Backup Capacity	At the Org level, for the most recent backups only, the Owner Backup Capacity report shows a list of owners and bytesProcessed in descending order.
Protected Bytes	At the Org or OrgVdc levels, for the most recent backups only, the Protected Bytes report shows the sum of bytesProcessed for all vApps in descending order.
Partial Backup	At the Org level, the Partial Backup report shows only the partial backups. Partial backups are defined as backups where the number of selected VMs is not equal to the number of actual VMs.
Backup Duration	At the Org level, the Backup Duration report shows vApp backups whose duration exceeds a given amount of time. This report has the potential to return no records. It also enables you to identify backups that are taking longer than they should, and can help you find performance or configuration problems, or errors.

Historical (event) reports

The historical (or event) reports display information about what happened, by whom, and when. Historical reports can be used to investigate potential errors, or performance and configuration problems that are encountered in an inventory report.

- vApp Backup History – shows vApp backup events per Org, OrgVdc, or vApp.
- vApp Restore History – shows vApp restore events per Org, OrgVdc, or vApp.
- vApp Replication History – shows vApp replication events per Org, OrgVdc, or vApp.
- vApp Backup Delete History – shows vApp backup delete events per Org, OrgVdc, or vApp.
- vApp Retention Update History – shows vApp backup retention update events per Org, OrgVdc, or vApp.

Sample reports

The following sample reports provide the SQL used to generate the reports, followed by actual output from the database. If the report body cannot fit in one table, then multiple tables are used. These examples do not represent all of the reports that can be generated; they are only to be used as a starting point.

Some queries, such as the sample chargeback report query, may have date (or other) input parameters.

Note

Although the reporting server is equipped with the SQL client "psql," connecting to the database and running the sample queries is outside of the scope of this documentation.

Chargeback report

An example query to generate a Chargeback report is provided below:

```
SELECT org_id, org_name, count(*) as total_vapp_backups,
sum(bytes_processed) as total_bytes_processed,
sum(bytes_modified) as total_bytes_modified
FROM "public"."t_vapp_backup_inventory"
where end_time between
to_date('01 Feb 2014 00:00:00', 'DD Mon YYYY HH24:MI:SS') and
to_date('28 Feb 2014 00:00:00', 'DD Mon YYYY HH24:MI:SS')
group by org_id, org_name order by org_name;
```

Example output is shown in the following table.

Table 11 Example Chargeback report output

org_id	org_name	total_ vapps	total_bytes_ processed	total_bytes_ modified
225c1b3d-5ed4-4334-92 72- 9d3d7982e52c	OrgOne	10	172590321543	331156
dfa11cce-3fd4-40f3- a907-4e1e7f2d885f	OrgTwo	294	1292938745117	1284358
5c12f524- a3ba-4069-8e67-0 906e99e39e6	OrgThree	458	515123187028	1089082
f803a5cb-643c-43fc-92e 8-71a328fe11fb	OrgFour	698	1202376589103	1800366

Frequent User Backup report

An example query to generate a Frequent User Backup report is provided below:

```
select
org_id, org_name, user_id, count(*) as total_vapp_backups
from "public"."t_vapp_backup_event"
group by org_id, org_name, user_id
order by count(*) desc;
```

Example output is shown in the following table.

Table 12 Example Frequent User Backup report output

org_id	org_name	user_id	total_vapp_ backups
f803a5cb-643c-43fc-92e8 -71a328fe11fb	OrgFour	urn:vcloud:user:f2ebd2c1- 7406-409f-b55a- cb39248e7cbb	66
5c12f524- a3ba-4069-8e67-0906e99 e39e6	OrgThree	urn:vcloud:user:f2ebd2c1- 7406-409f-b55a- cb39248e7cbb	30

Table 12 Example Frequent User Backup report output (continued)

org_id	org_name	user_id	total_vapp_backups
dfa11cce-3fd4-40f3-a907-4e1e7f2d885f	OrgTwo	urn:vcloud:user:f2ebd2c1-7406-409f-b55a-cb39248e7cbb	16
6ab4f14a-79cb-4219-a5da-c660759cef40	OrgFive	urn:vcloud:user:0b839f8f-6ff2-4890-8d6a-3b61c8bc2656	2

Partial Backup report

An example query to generate a Partial Backup report is provided below:

```
select
org_id, org_name, org_vdc_id, org_vdc_name, vapp_id, vapp_name,
owner_id, owner_name, vapp_backup_id, backup_type, backup_vm_count,
vms_selected, actual_vms, backup_host, bytes_modified,
bytes_processed, start_time, end_time, effective_retention
from "public"."t_vapp_backup_event" where
vms_selected != actual_vms;
```

Example output is shown below using multiple tables in order to show all of the columns.

Table 13 Example Partial Backup report output

org_id	org_name	org_vdc_id	org_vdc_name
5c12f524-a3ba-4069-8e67-0906e99e39e6	OrgThree	35c55d20-5e69-4f34-b1ff-75a33786f79f	OrgVDCThree
f803a5cb-643c-43fc-92e8-71a328fe11fb	OrgFour	56654356-c979-4181-8fb8-a85a7fdbb070	OrgVDCFour
dfa11cce-3fd4-40f3-a907-4e1e7f2d885f	OrgTwo	3ec28a93-becd-4024-a768-6cc858f37d47	OrgVCDTwo
5c12f524-a3ba-4069-8e67-0906e99e39e6	OrgFour	56654356-c979-4181-8fb8-a85a7fdbb070	OrgVDCFour

vapp_id	vapp_name	owner_id	owner_name	vapp_backup_id
bbba8d3f-970c-421e-affa-b3d586bc49b4	vApp_AA	59e0be76-8faf-4d1c-9416-65075f0e4b41	system	309

vapp_id	vapp_name	owner_id	owner_name	vapp_backup_id
7f416ff4-edb7-4bbb-848e-acf0fc62e4bb	vApp13	d4bf78d0-a225-4189-9c43-7a38f6b29a0e	system	296
7e561360-5443-464c-ba0b-46503ad5ebb6	vApp_system_5	e05f6860-62d6-4b5f-8c03-873195aee759	system	323
7f416ff4-edb7-4bbb-848e-acf0fc62e4bb	vApp13	d4bf78d0-a225-4189-9c43-7a38f6b29a0e	system	302

backup_type	backup_vm_count	vms_selected	actual_vms	backup_host
scheduled	2	2	1	host1.example.com
scheduled	2	2	1	host1.example.com
scheduled	2	2	1	host1.example.com
scheduled	2	2	1	host1.example.com

bytes_modified	bytes_processed	start_time	end_time	effective_retention
27120	8592078196	3/4/2014	3/4/2014	5/3/2014
32493	8592078196	3/4/2014	3/4/2014	5/3/2014
33692	8592078196	3/4/2014	3/4/2014	5/4/2014
27101	8592078196	3/4/2014	3/4/2014	5/4/2014

Backup Duration report

An example query to generate a Backup Duration report is provided below:

```
with t_duration as (select ((extract (epoch from end_time)) - (extract
(epoch from start_time))) as duration
from "public"."t_vapp_backup_inventory")
select
t_duration.duration, org_id, org_name, org_vdc_id, org_vdc_name,
vapp_id, vapp_name, owner_id, owner_name, vapp_backup_id, backup_type,
backup_vm_count, vms_selected, actual_vms, backup_host,
bytes_modified,
bytes_processed, start_time, end_time, effective_retention
FROM
"public"."t_vapp_backup_inventory" as vbe, t_duration
where t_duration.duration > 1000
order by duration desc;
```

Example output is shown below using multiple tables in order to show all of the columns.

Table 14 Example Backup Duration report output

duration	ord_id	org_name	org_vcd_id	org_vdc_ name
4413.308	f803a5cb-643c-43fc-92e8-71a328fe11fb	OrgFour	56654356-c979-4181-8fb8-a85a7fdbb070	OrgVDCFour
4413.308	5c12f524-a3ba-4069-8e67-0906e99e39e6	OrgThree	35c55d20-5e69-4f34-b1ff-75a33786f79f	OrgVDCThree
4413.308	225c1b3d-5ed4-4334-9272-9d3d7982e52c	OrgOne	cdf1febb-537e-431d-9ad3-e4755d64bfc9	OrgVDCOne
4413.308	f803a5cb-643c-43fc-92e8-71a328fe11fb	OrgFour	56654356-c979-4181-8fb8-a85a7fdbb070	OrgVDCFour

vapp_id	vapp_ name	owner_id	owner_ name	vapp_ backup_ id
19df594c-2741-4db5-987f-f6980b3a994c	vApp01	d4bf78d0-a225-4189-9c43-7a38f6b29a0e	system	914
6e3459e5-caf2-4444-9b66-9df3d09295ef	vApp_CC	59e0be76-8faf-4d1c-9416-65075f0e4b41	system	963
c4eeda5e-158b-481e-8b88-deceb6a74e1b	vapp1	7f66b954-90b5-45de-8787-9f761498f72d	system	151

vapp_id	vapp_ name	owner_id	owner_ name	vapp_ backup_ id
d1e4139b-dfe6-4341-ad8a-690d33f58698	vApp11	d4bf78d0-a225-4189-9c43-7a38f6b29a0e	system	917

backup_type	backup_ vm_count	vms_ selected	actual_ vms	backup_host
scheduled	1	1	1	host2.example.com
scheduled	1	1	1	host2.example.com
adhoc	2	2	2	host2.example.com
scheduled	1	1	1	host2.example.com

bypes_ modified	bytes_ processed	start_time	end_time	effective_ retention
24792	8592078196	2/20/2014	2/20/2014	4/21/2014
27611	17210764641	2/26/2014	2/26/2014	4/27/2014
33331	17210764641	2/19/2014	2/19/2014	4/20/2014
24832	8592078196	2/20/2014	2/20/2014	4/21/2014

CHAPTER 7

Operations

This chapter includes the following topics:

Shutting down and restarting vCD Data Protection Extension services

Follow these instructions to cleanly shut down and re-start the vCD Data Protection Extension's services in the event of a planned power outage or for maintenance purposes.

Before you begin

Make sure that no backups, restores, or replications are running.

Procedure

1. To shut down the services:
   a. On each backup appliance, set `<IsEnabled>false</IsEnabled>` to disable ad hoc and scheduled backups and restores.
   b. Shut down vCP plug-in components in the following order by shutting down the VMs:
      - VCP UI server
      - vCP server cell
      - Backup gateway VM (to ensure that no pending updates are being passed)
      - Reporting server
   c. Follow the vCD shutdown instructions from VMware to properly shut down the vCD architecture.
   d. Follow the instructions in the *EMC Avamar Administration Guide* to properly shut down the AVE.
2. To restart the services:
   a. Start vCLoud, including all relevant databases.

      Refer to the instructions from VMware for additional details.
   b. Start PostgreSQL.
   c. Start the RabbitMQ VM.
   d. Start Avamar/AVE using the following command:

      ```
      dpnctl start all
      ```
   e. Start the vCD Data Protection Extension components in the following order:
      - Reporting server
      - Backup gateway VM
      - vCP server cell
      - VCP UI server
   f. On each backup appliance, set `<IsEnabled>true</IsEnabled>` to enable ad hoc and scheduled backups and restores.

Changing the lockbox passphrase

This section describes how to change the lockbox passphrase in the `bootstrap.properties` file on the Cell server.

Before you begin

To change the lockbox passphrase, you need the following information:

- The location of the `bootstrap.properties` file. Typically, this file is located in `/etc/vcp`.
- The previous passphrase; for example, the one that was provided during initialization.
- The new passphrase, which must meet the following requirements:
  - Be at least 8 characters long
  - Contain at least one uppercase alphabetic character
  - Contain at least one lowercase alphabetic character
  - Contain at least one numeric character
  - Contain at least one of the following non-alphanumeric characters: !@#%&*_-=+|~

Procedure

1. On the Cell server, open the `/etc/vcp/bootstrap.properties` file in a text editor.
2. Provide the following information in the `bootstrap.properties` file:

```
cst.pw=original_passphrase
cst.changePw=new_passphrase
```

Note

You must provide both the original and new passphrases, or the password will not change.

3. Save and close the file.
4. Restart the Cell server.

Changing IP addresses on vCD Data Protection Extension cells

This procedure describes how to change the IP addresses on the vCD Data Protection Extension cells.

Procedure

1. Power off the VMs.
2. On each VM, edit the settings to change the IP address.
3. Verify that the DNS is updated with the FQDNs to point to the new IP addresses.

4. Power on the VMs.
5. Verify that the VMs can communicate and that their respective services are running.

Deleting backup repositories for deleted Org vDCs

When you delete an Org vDC from vCloud, you should also delete the repositories that were associated with the Org vCD by the vCD Data Protection Extension.

Procedure

1. Delete the vApps from the Org vDC.

   The vCD Data Protection Extension detects the deletion, and automatically removes the vApps from any backup and replication policies.
2. Enter the following command to list the policies associated with the vDC:

   ```
   GET /api/admin/extension/vdc/vdcId/BackupPolicies
   ```
3. Enter the following command for each policy:

   ```
   DELETE /api/admin/extension/vdc/vdcId/BackupPolicy/policyId
   ```

   Once the vApps and policies have been deleted from the repository, you can delete the repository.
4. Enter the following command to list the repositories associated with the vDC:

   ```
   GET /api/admin/extension/vdc/vdcId/BackupRepositories
   ```
5. Enter the following command for reach repository:

   ```
   DELETE /api/admin/extension/vdc/vdcId/BackupRepository/policyId
   ```
6. If the backup appliance has no other repositories or vCenter registrations, delete it as well.

Storage mapping for replicating Data Domain vCD backups

This section describes how to map storage to specific Data Domain systems using Avamar Administrator. Refer to the *EMC Avamar and EMC Data Domain System Integration Guide* for additional information.
In this scenario, backups are being replicating from Source Avamar A to Destination Avamar B. Destination Avamar B has several Data Domains attached to the AVE.

After the first replication, Destination Avamar B will contain the domain structure under the /REPLICATE/Source_Avamar_A tree. Once all of the vApp client accounts are replicated, you can send future backups from particular domains into specific Data Domains on Destination System B.

Procedure

1. Log in to Avamar Administrator, and select the **Replication** tab.
2. In the **Replication** window, select the **Storage Mapping** tab.
3. Right-click anywhere in the tab's white space, and select **New Storage Mapping**.

   The **Select a Domain** dialog box appears.
4. Browse to a domain and select it from the tree.

5. From the **Map to Data Domain System** list, select the Data Domain system to use as the replication target.
6. Click **OK**.

APPENDIX A

Backup and Recovery

This appendix includes the following topics:

Backup steps

This section describes how to back up the components of the vCloud Director Data Protection Extension.

Before you begin

- Set up a dedicated AVE for backing up and restoring the plug-in's virtual machines. This AVE is separate from the AVE being used for VApps and VM backups running on the vCloud.
- Set up an ImageProxy for the AVE on the same host where the plug-in's virtual machines are located, and register it with the dedicated AVE.
- Register the cloud management vCenter (maintaining the ESX Host running the plug-in's components) with the AVE.

Procedure

1. Shut down the plug-in's VMs in the following order:

   Backup Gateway
   vCP server
   Reporting server
   UI server
   Postgres DB
   RabbitMQ

2. In the MC GUI for the dedicated AVE (the first item in "Before you begin"), add the Backup Gateway, vCP server, Reporting server, UI server, Postgres DB, and RabbitMQ VMs as clients under the vCenter by using the following steps:
   a. Navigate to **Administration** > **Account Management**.
   b. Right-click **vCenter**, and select **New Clients** > **VMs & Templates**.
   c. Select the Backup Gateway, vCP server, Reporting server, UI server, Postgres DB, and RabbitMQ VMs.
   d. Click **OK**.
3. Back up the VMs by using the following steps for each VM:
   a. In the MC GUI, select the **Backup & Restore** tab.
   b. In the upper-left pane, select the vCenter IP where you specified the plug-in's VMs as clients.

      The VM clients display in the lower-left pane.
   c. Select a VM in the list, and then select the **Backup** tab.
   d. Back up the VM.
   e. Repeat the previous four steps for each of the plug-in's VMs.

Recovery steps

This section describes how to recover components of the vCloud Director Data Protection Extension that have been backed up.

Procedure

1. Restore the backed up VMs to new VMs (Backup Gateway, vCP server, Reporting ser, UI server, Postgres DB, RabbitMQ) by using the following steps:
   a. In MC GUI, select the **Backup & Restore** tab.
   b. In the upper-left pane, select the vCenter IP where you specified the plug-in's VMs as clients.

      The VM clients display in the lower-left pane.
   c. Select a VM in the list, and then select the **Restore** tab.
   d. Select a backup to restore.
   e. Select the **All virtual disks** checkbox.
   f. Right-click **All virtual disks**, and select **Restore Now**.
   g. In the **Restore Option** dialog box, select **Restore to new virtual machine** > **Configure Destination**.
   h. Select the location where the VM will be restored, specify the name of the VM, and click **OK**.

      The restore process begins.
2. When the restore has completed, power on the VM that has been restored.
3. Verify that the Postgres and Rabbitmq services have started by entering the following commands:

   ```
   service rabbitmq-server status
   pg_ctl status
   ```

4. Perform the following steps on the VCP server, Backup Gateway, and Reporting servers.
   a. Enter the following command to open the bootstrap.properties file on the VM:

      ```
      vim /etc/vcp/bookstrap.properties
      ```

   b. Add the following two key=value pairs and set the cst.overWrite variable to true in the file:

      ```
      cst.pw=<Original_Passphrase>
      cst.resetLb=true
      cst.overWrite==true
      ```

   c. Save and close the file.
   d. Enter the following command to restart the VCP server, Backup Gateway, and Reporting services:

      ```
      service vcpsrv restart
      ```

5. Re-register the vApp Proxy on the Backup Gateway node with the desired AVE.
6. Power on the vCP UI server VM.

APPENDIX B

Troubleshooting

This appendix includes the following topics:

Database Issues

Database issues include problems such as not being able to add or delete backup or replication policies, or seeing incomplete lists of policies or repositories.

You can use a GUI application like pgAdmin to browse the tables in your PostgreSQL database; however, we strongly recommend that you contact EMC Professional Services to troubleshoot database-related issues for you.

Log file locations

Log file locations are listed as follows:

- Cell server logs are located in `/var/log/vcp/vcpserver.log`
- Backup Gateway logs are located in `/var/log/vcp/vcpbg.log`
- UI logs are located in `/var/log/vcp/vcpui.log`

The corresponding tcServer logs for each server are listed as follows:

- For the Cell and UI servers, tcServer logs are located in `/var/opt/emc/vcp/vcpsrv/logs`
- For the Backup Gateway server, tcServer logs are located in `/var/opt/emc/vcp/vcpbg/logs`

Information about tcServer log files is provided in the vFabric documentation, which can be used to diagnose issues where the EMC product web app fails to deploy at the tcServer level (which might result in empty `/var/log/vcp` logs).

The lockbox becomes unreadable on the Cell server and needs to be reset

Before you begin

You must have the original lockbox passphrase to perform this procedure.

The lockbox may become unreadable on the Cell server in the following situations, resulting in a log message that states "unable to obtain credentials:"

- A VM was migrated onto another host that has different characteristics from the original host (for example, CPU type).
- A VM was cloned and its configuration was changed (for example, CPU type or memory allocation).
- One or more operating system values were changed (for example, hostname).

Procedure

1. On the Cell server, open the `/etc/vcp/bootstrap.properties` file in a text editor.
2. Provide the following information in the bootstrap.properties file:

   ```
   cst.pw=<ORIGINAL_PASSPHRASE>
   cst.resetLb=true
   ```

3. Save and close the file.

4. Restart the Cell server.

SSL errors

Missing certificates and hostname mismatches will cause the following errors during backup appliance creation:

`SSL Error: Peer not authenticated` – This error indicates that the certificate is missing.

`SSL Error: mismatch between hostname specified` – This error indicates that the host names provided in the certificate for the client and server do not match.

APPENDIX C

Centralized Logging

This appendix includes the following topics:

Introduction

This chapter describes the procedures for configuring centralized logging on each component of the vCloud Director Data Protection Extension (vCloud Protector, backup gateway and backup gateway plug-in). The rsyslog server must be configured prior to the rsyslog configuration, and the Certificate Authority's (CA) certificate must be provided to all of the rsyslog clients.

The requirements specific to rsyslog configuration are listed as follows:

- The SLES 11 SP3 operating system is being used.
- The person installing the rsyslog components has root privileges.
- The installer must configure their rsyslog server and provide the CA's certificate to all rsyslog clients.
- The installer must configure the port for the centralized logger on the rsyslog server's firewall.

Note

We assume that the customer already has a centralized logging server installed, such as log-insight or equivalent, and that they want to add the vCloud Director Data Protection Extension components to this server. If not, a simple logging server can be created on an existing linux host running rsyslog. In the examples, we use a SLES 11 SP3 VM. You may need to adjust the server-related instructions below as needed for your specific logging server setup.

Unencrypted logging setup

The following sections describe how to set up the server and the client for unencrypted logging.

Setting up the server

Procedure

1. Log in to the central logging server as root, and edit `/etc/rsyslog.d/remote.conf`.
2. Find and uncomment the following lines:

```
$ModLoad imudp.so # provides UDP syslog reception
$UDPServerRun 514 # start a UDP syslog server at standard
port 514
```

3. Save and close the file.
4. Enter the following command to restart the rsyslog service:

   `rcsyslog restart`

5. Configure iptables and firewall for UDP and TCP port 514 (and optionally TCP 10514) as described below.
6. On the server, execute **`tail -f /var/log/messages`** to monitor log messages.

You can verify that the server is receiving messages using the `netcat/nc` utility from the client:

```
netcat –u hostname 514
```

```
Type some text here and it should appear in the /var/log/
messages file on the host
Type Ctrl-C to stop testing.
```

You can optionally enable support for TCP messages instead of UDP. Refer to the rsyslog documentation for this option.

Configuring clients

Procedure

1. Log into the client as root and edit the `/etc/rsyslog.d/remote.conf` file.
2. Locate the following lines:

   ```
   # remote host is: name/ip:port, e.g. 192.168.0.1:514, port
   optional
   #*.* @@remote-host
   ```

3. Add the following line below those in step 2:

   ***.* @*ip_of_server*:514 # forward all local syslog messages to remote host**

   where *ip_of_server* is the IP Address or FQDN of the logging server.

   If you set up the server to listen on TCP (or if you enable SSL as shown in the next section) enter the following line instead:

   ***.* @@ip_of_server:10514 # forward all local syslog messages to remote host**

   The two @@ designates TCP instead of UDP and the port is changed

   This will forward all of the log messages that are handled by the client's rsyslog system to the central logging server.

4. Enter the following command to restart the rsyslog server:

   rcsyslog restart

Results

After you complete these steps, basic setup should be complete. Verify that log entries from the client appear in the logging server's `/var/log/messages` file.

Example rsyslog firewall configuration

The following example illustrates how to modify the SLES 11 SP3 firewall to open ports 514 and 10514 for rsyslog. You must perform this procedure as root, and it only needs to be performed on the logging server. The clients do not need this configuration step.

Procedure

1. Log into the rsyslog server as root and create the following file using a text editor such as vi or Vim:

/etc/sysconfig/SuSEfirewall2.d/services/rsyslog

2. Add the following information to the file:

```
##Name: rsyslog
## Description Open port for rsyslog server running on this
host
UDP="514"
TCP="10514"
```

3. Change the permissions on the rsyslog file to 644 by entering the following command:

   chmod 644 /etc/sysconfig/SuSEfirewall2.d/services/rsyslog

4. Add the new service to the firewall by entering the following command:

   /sbin/yast2 firewall services add service=service:rsyslog zone=EXT

Setting up SSL security

The following sections describe how to set up the server and the client for SSL security.

Server configuration

Procedure

1. Log into the rsyslog server as root and edit the following file:

   /etc/rsyslog.d/remote.conf

2. Find the section titled "Encrypting Syslog Traffic with TLS" and uncomment the lines that start with '#$'.

```
# -- TLS Syslog Server:
## make gtls driver the default
$DefaultNetstreamDriver gtls
#
## certificate files
$DefaultNetstreamDriverCAFile /etc/rsyslog.d/ca.pem
$DefaultNetstreamDriverCertFile /etc/rsyslog.d/server_cert.pem
$DefaultNetstreamDriverKeyFile /etc/rsyslog.d/server_key.pem
#
$ModLoad imtcp # load TCP listener
#
$InputTCPServerStreamDriverMode 1 # run driver in TLS-only
mode
$InputTCPServerStreamDriverAuthMode anon # client is NOT
authenticated
$InputTCPServerRun 10514 # start up listener at port 10514
```

3. Create a set of SSL certificates, and place them in the `/etc/rsyslog.d/ca.pem`, `/etc/rsyslog.d/server_cert.pem` and `/etc/rsyslog.d/server_key.pem`.

   Use openssl or equivalent tools for creating these certificates.

4. Enter the following command to restart the rsyslog server:

```
rcsyslog restart
```

Client Configuration

Procedure

1. Log into the client as root and edit the following file:

   `/etc/rsyslog.d/remote.conf`

2. Find the section titled “TLS Syslog Client” and uncomment the lines that start with ‘#$’.

```
# -- TLS Syslog Client:
## certificate files - just CA for a client
$DefaultNetstreamDriverCAFile /etc/rsyslog.d/ca.pem
#
## set up the action
$DefaultNetstreamDriver gtls # use gtls netstream driver
$ActionSendStreamDriverMode 1 # require TLS for the connection
$ActionSendStreamDriverAuthMode anon # server is NOT
authenticated
*.* @@(o)ip_of_server:10514 # send (all) messages
```

3. Copy the `/etc/rsyslog.d/ca.pem` file from the central logging server to a `/etc/rsyslog.d/ca.pem` file on the client.
4. Enter the following command to restart the rsyslog server:

   ```
   rcsyslog restart
   ```

Example vFabric Postgres server logging configuration

This is an example of how to forward the contents of log files from the filesystem (that do not go through the syslog facility) to the central logging server. This example uses vFabric Postgres, but it can easily be adapted to other applications.

These lines can go be added to `/etc/rsyslog.conf`, or you can add a file in `/etc/rsyslog.d/`*`application`*`.conf`, where *application* can be an reasonable name, as long as it sorts alphabetically before `remote.conf`; otherwise the contents of these files will not be sent to the central logging server.

```
$ModLoad imfile #needs to only be done once, even for multiple files
$InputFileName /var/lib/pgsql/data/pg_log/postgresql-Fri.log
#specifies the path of the file
on the client
$InputFileTag postgres_log #give a tag to the log file being sent
$InputFileStateFile /var/spool/rsyslog/statefile1 #statefile keeps
track of which parts of
monitored file have already been processed. Each individual file
needs a unique statefile(n) file.
$InputRunFileMonitor
```

Repeat the second through the fifth lines for each log file. You can add more files to monitor by using the same process, but you must change the statefile(n) name for each additional file.

APPENDIX D

Password Rotation

This appendix includes the following topics.

Introduction

Many data-center owners and system administrator require the rotation of passwords. This appendix contains a high level overview of the password rotation process. The information is not all-inclusive, but it attempts to describe how to rotate passwords within the vCD Data Protection Extension's service.

The term password is defined in general terms within this appendix to be synonymous with authentication information (user credentials) and not necessarily with authorization information (feature access).

vCD Data Protection Extension service rotatable passwords

The vCD Data Protection Extension service uses three types of passwords: VM, CST, and Connection.

VM passwords

The VM password is provided to gain access to the vCD Data Protection Extension's virtual machines. These VMs contain plug-in components, which include, but are not limited to, VCP cell, Gateway, and Reporting Server. VM passwords are stored in two locations; locally and externally. The next two sections provide information about password storage and usage. The VM password is used to log in to VMs, normally provided by the OS user login, which requires a username and password.

Local

Local passwords are used for local accounts and services. The passwords are stored within and protected by the operating system.

External

External password information is stored within an external server; for example, an LDAP server.

Note

The vCD Data Protection Extension does not support automated OS LDAP client configuration, but the following information is provided for educational purposes.

Within the LDAP server scenario, there are two user authentication possibilities when logging in to the server using a VM password:

- The LDAP server provides a challenge-response value to the LDAP client based on the login information. If both challenge-response values match, the login is successful.
- The LDAP client creates an encrypted connection, such as TLS, to the server where the username and password are provided to the client. The client then compares the provided information with login input. If the information matches, the login is successful.

Connection passwords

Connection passwords are initially stored locally within the CST lockbox. In some cases the credentials are copied and stored securely into a database.

CST password

The CST password is used to access administrative functionality of the CST lockbox. The CST (RSA Common Security Toolkit) lockbox is an RSA product that contains at its foundation an encrypted/protected file that contains key/value pairs. The lockbox within the vCD Data Protection Extension service contains a number of key/value pairs used for vCD Data Protection Extension configuration. However, due to the nature of the CST lockbox, there are scenarios (for example, operating system upgrade where kernel values have changed, or CST upgrades) where the lockbox may no longer be readable, and thus access to CST administrative functionality is required to repair the CST lockbox. Because of this, the CST password must be rotated.

Local

The CST password and all key/value pairs are securely stored internally within the CST lockbox.

External

Within CST, there is a CST Authentication Service that can be configured to use an LDAP authority for authentication.

Note

Currently, the vCD Data Protection Extension does not support the CST LDAP Authentication.

Avamar credentials change

The Avamar Plugin for vCloud Director has two components that communicate with the backend Avamar system. These are both located on the Backup Gateway VM.

In the event that the Avamar username/password is changed, both of these applications need to be updated with the new credentials.

Updating the backup gateway

Procedure

1. Stop the VCP backup gateway.
2. Run the following command on the backup gateway VM:

   ```
   service vcpbg stop
   ```
3. Change the password in Avamar.
4. Log in to the VMA VM and make the appropriate modification in the `<hostname>.properties` file. The modification must reflect the following:
   - The `<hostname>.properties` file must be equivalent to the backup gateway VM that was stopped.
   - Within the `<hostname>.properties` file, the `ave.user` and `ave.pword` keys' values must be changed to match the new Avamar username and password.

5. Run the `deployvm.sh` command with the appropriate values and the `–update` argument on the command line. For example:

   `./deployvm.sh --vm.hostname=<hostname> --vm.type=gateway –update`

   Note that there are two dashes (`--`) preceding the `vm.hostname=hostname=<hostname>` and `vm.type=gateway` options.

Updating the vApp Proxy

Procedure

1. Stop the vApp Proxy.
2. On the backup gateway VM, run the following commands to stop the vApp proxy:

   `cd /usr/local/avamarclient/etc`

   `./initproxyappliance.sh stop`

3. Log in to the Avamar Management Console and select the **Administration** tab.

   The **Administration** screen opens on the **Account Management** tab.

4. Locate the vApp Proxy under clients, and do the following:

   a. In the list of domains in the upper-left pane, select the domain "clients."

      The list of clients registered under this domain are displayed in the lower-left pane.

   b. Locate the client with the name that matches the FQDN of the backup gateway. For example, gateway.example.com. This is the client that represents the registered vApp Proxy.

   c. Right-click the client located in step b, and select **Delete Client**.

   d. Click **Yes** when you are asked to confirm the deletion. You will need to confirm twice to proceed with the delete.

   e. When you see the confirmation that the client was deleted, click **OK**.

5. Log in to the backup gateway VM again, and run the following commands to register the proxy to Avamar using the new password:

   `cd /usr/local/avamarclient/etc`

   `./initproxyappliance.sh start --mcsaddress=<Avamar-FQDN> --avdomain=clients`

   Where *<Avamar-FQDN>* is the FQDN of the Avamar server.

   Note that there are two dashes (`--`) preceding the `--mcsaddress=<Avamar-FQDN>` and `--avdomain=clients` options.

6. Answer the following prompts when they appear:

   `Enter MC Account Name:` Enter the new username of the Avamar account.

   `Enter password for (Your username:` Enter the corresponding password for the Avamar account.

   You will see the message, `Registration Complete`, followed by two other lines. This confirms that the vApp Proxy has been successfully registered with Avamar using the new credentials.

The Avamar Plugin for vCloud Director should now be ready to connect to the Avamar system with the updated credentials.

Rotation scenarios

This section describes the best practices for rotating VM, connection, and CST passwords.

Rotating the VM password

To change the VM password, you can either modify the `<hostname>.properties` file or use the `deployvm.sh` command. (See the last section in this appendix for detailed information about the `deployvm.sh` command.)

Note

The use of the vm.endingPw is only supported on the command line, as described in the following sections.

Changing the VM password during initial VM deployment
Enter the following command on one line:

```
./deployvm.sh --vm.hostname=<hostname> --vm.type=vcpcell
--vm.endingPw=<new_password>
```

Note

The first time you deploy the VM using the `deployvm.sh` command, you can provide the `vm.endingPW`. However, changes that are made after the initial deployment require the `–rotate.components` argument on the command line as shown below.

Changing the VM password after the VM has been deployed
Enter the following command on one line:

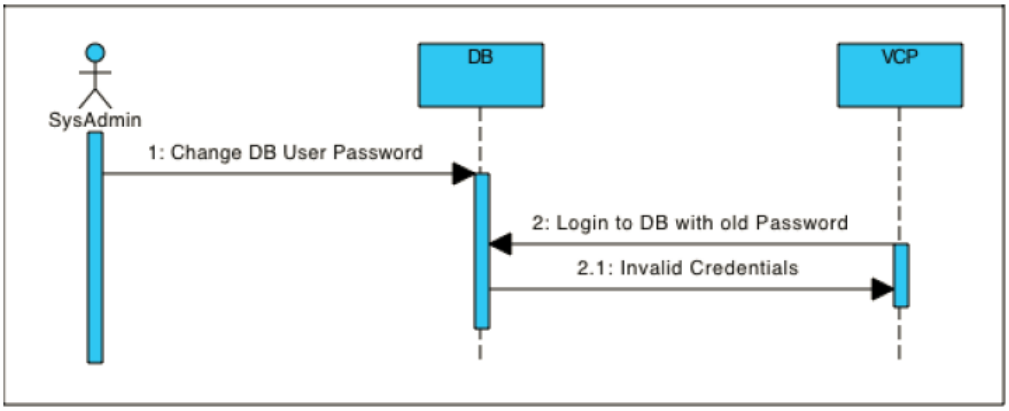
```
./deployvm.sh --vm.hostname=<hostname> --vm.type=vcpcell --
rotate.components --vm.endingPw=<new_password>
```

Rotating a connection password

Connection passwords can be rotated using two different processes. The first process replaces the existing credential password with a new password. For the second process, the system administrator creates an entirely new user credential having the existing user's equivalent authentication and authorization.

In either process, steps must be taken to avert the possibility of making an invalid connection while the passwords are being changed. The following sequence diagram illustrates a scenario where an invalid password connection can occur.

Figure 1 Interruption of service during credential change



In this example, the password issue arises when the database credential changes; however the credentials have not changed within the vCD Data Protection Extension component. When the vCD Data Protection Extension component attempts to log in, it cannot, because the credential information stored on the component is stale.

Process 1: Replacing the existing connection password

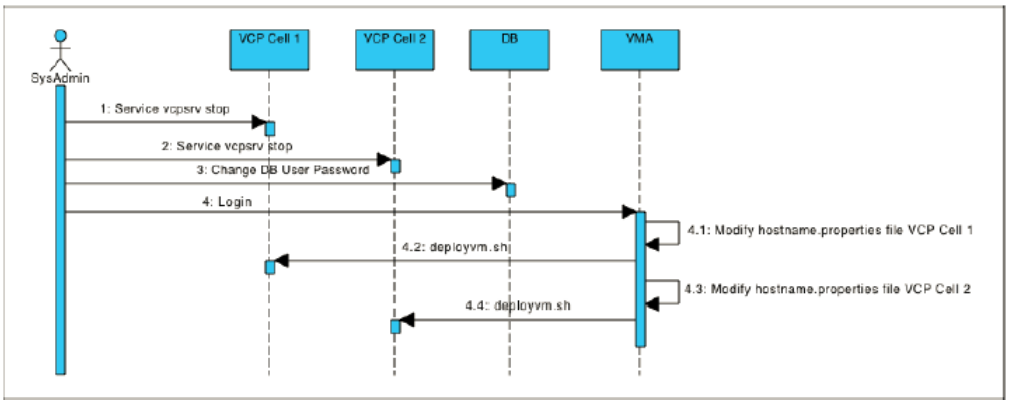
In this example, the database password for the VCP cell is being changed.

Before you begin

Before performing this procedure, review deployvm.sh on page 98 for a detailed description of the `deployvm.sh` command.

The following figure illustrates a successful database password replacement.

Figure 2 Successfully replacing a database password



When you replace the connection password, you must stop all VCP component's services before you make changes to both the database and the associated VCP cells.

Note

Executing the `deployvm.sh` command with the `--rotate.components` argument will, at the end of the script, automatically restart the specific vCD Data Protection Extension service.

Procedure

1. Stop the VCP components that use the connection password.
   On the VCP cell VM, enter the following command:

```
service vcpsrv stop
```

Note

You must stop all VCP cells that are associated with this specific connection password.

2. Make the password change to the database.
3. Log in to the VMA VM and make the appropriate modification in the `<hostname>.properties` file. The modification must reflect the following:
   - The `<hostname>.properties` file must be equivalent to the VCP cell VM that was stopped.
   - Within the `<hostname>.properties` file, the `db.pword` key's value must be changed to be equivalent to the new database password.
4. Execute the `deployvm.sh` command with the appropriate values and the `--rotate.components` argument on the command line. (Enter the command on one line rather than on two as shown in the example).

   For example:
   `./deployvm.sh --vm.hostname=<hostname> --vm.type=vcpcell --rotate.components`

Note

Repeat step 3 and 4 for all components using this specific connection password.

Process 2: Creating a new equivalent credential connection password

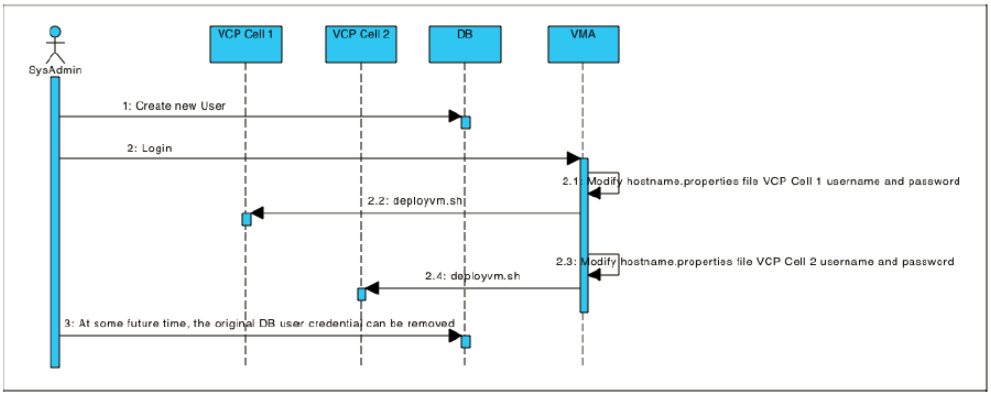
In this example, the database password for the VCP cell is being changed by creating a new connection password with credentials that are equivalent to those of the existing user.

Before you begin

Before performing this procedure, review deployvm.sh on page 98 for a detailed description of the `deployvm.sh` command.

The following figure illustrates this process.

Figure 3 Creating a new equivalent user credential



In this example, a new database user is created with the exact configuration of the existing user first. None of the VCP components need to be stopped, and modification within the VMA is accomplished with minimal downtime of the VCP component. The

additional step of removing the prior database user account is done only after all validation of the new database user within the VCP component has been tested.

Procedure

1. Create a new database user credential with equivalent authentication and authorization of the existing user credential.
2. Login into the VMA VM and make the appropriate modification in the `<hostname>.properties` file.

   The modification must reflect the following:

   - The `<hostname>.properties` file must be equivalent to the VCP cell VM that was stopped.
   - Within the `<hostname>.properties` file, the `db.user` key's value must be changed to be equivalent to the new database user.
   - Within the `<hostname>.properties` file, the `db.pword` key's value must be changed to be equivalent to the new database password.
3. Execute the `deployvm.sh` command with the appropriate values and the `--rotate.components` argument on the command line. (Enter the command on one line rather than on two as shown in the example.)

   For example:
   `./deployvm.sh --vm.hostname=<hostname> --vm.type=vcpcell --rotate.components`

   Note

   Repeat steps 2 and 3 for all components using this same connection password.
4. Validate that the new credentials work properly on all required VCP cells.
5. Remove the old database credentials.

Scheduling password rotation

This topic describes best practices for scheduling the rotation of passwords on the VCP server, and on the Backup Gateway and Reporting servers.

Scheduling password rotation on the VCP server

On the VCP server, you can schedule the rotation of the VM, CST, and Connection passwords.

VM password
The changing of the VM Password can be scheduled at any time, since changing the VM password doesn't require any server/service or VM to be started.

CST password
The changing of the CST password can be scheduled at any time. Since changing the CST password invokes a restart of the service and the configuration of VCP Server Cells requires a minimum of two VCP Server Cells, each VCP Server's CST password can be changed independently.

Note

Do not change all VCP Server Cells' CST passwords simultaneously, because there is a possibility of service delay on pending requests. Make sure that you change the VCP server's CST passwords sequentially.

Connection password

The changing of the Connection password can be scheduled at any time, as long as the following best practices are followed:

- Process 2: Creating a new equivalent credential connection password on page 95 is used when rotating the Connection password for the VCP Server Cell.
- The rotations of the VCP Server Cells connection passwords are performed sequentially and not simultaneously.

Otherwise to ensure the message is not dropped or not processed, the VCP Server Cell's Connection password change must be scheduled during the Avamar maintenance window.

Scheduling password rotation on the Backup Gateway and Reporting servers

On the Backup Gateway and Reporting servers, you can schedule the rotation of the VM, CST, and Connection passwords.

VM password

The changing of the VM Password can be scheduled at any time, since the changing of the VM password doesn't require any server or VM to be started.

CST and Connection passwords

Due to the single-server configuration of the Backup Gateway and Reporting servers, there is a small window of time during which content or messages can be dropped or not processed by either server. This can happen when either of the services need to be restarted when changing the CST or Connection passwords.

Note

To ensure that the message is not dropped or not processed, you must schedule the changing of the CST or Connection password during the Avamar maintenance window.

deployvm.sh

The `deployvm.sh` command deploys and manages the vCloud Protector Component VM.

Description

Note

- CST Administration functionality (change CST password, reset CST lockbox, etc) can be provided via a command line argument using deployvm.sh.
- Command line arguments no longer have the highest precedence. The `<hostname>.properties` file now has the highest precedence.
- VM password changing is preformed on via the deployvm.sh command line. Changing the VM password is no longer supported via the `<hostname>.properties` file.

The `deployvm.sh` command's primary purpose is to deploy a virtual machine within VMware VCenter. The `deployvm.sh` command creates a vCloud Protector component VM.

The command's secondary purpose is to modify values that were used to configure the VM. In the primary purpose scenario, the type of vCloud Protector Component is provided by the `--vm.type` argument. In the secondary purpose scenario, changes and modification require the `--rotate.components` argument.

The command's tertiary purpose is used in either the primary or secondary scenarios. In the tertiary purpose scenario, the password of the VM is being changed; this can occur in either the primary or secondary scenarios.

Syntax

```
./deployvm.sh [Help display] {Primary Required Options} [Secondary
Options] [Tertiary Option]
```

[Help Display]

-h

Displays usage screen; all other arguments should be disregarded.

--help

Long form to display usage screen; all other arguments should be disregarded.

{Primary Required Options}

The primary options, which are required, are needed for all options (primary, secondary and tertiary}. Executing the `deployvm.sh` command using only the primary options creates the VM.

--vm.hostname=<hostname.domain.com>

Specify the hostname of the VM to be deployed (mandatory). Note that `<hostname.domain.com>` should be substituted for the FQDN in your DNS. In addition, an `FQDN.properties` file should be provided within the same directory where the command is executed. Finally, the `FQDN.properties` file provides

specific configuration information used to deploy the <*hostname*.*domain*.com> VM.

--vm.type=<Known vCloud Protector Components>

Specify the type of VM to be deployed (mandatory). Note that gateway|vcpcell|vcprpt|vcpui are currently the known VM types.

[Secondary Options]

The secondary options are needed to modify key/value pairs (for example, component credential, database password, etc). The primary options must both be provided when using the secondary options.

--rotate.components

Specify that within one of the properties files (`default.properties` or <*hostname*>`.properties`, a key/value pair has been modified. Execution of the `deployvm.sh` command with both the primary and secondary options will modify the VM's configuration and restart the service.

--vm.cstChangePw=<NewCSTPassword>

Specify what the VM CST's password should be. The `--rotate.components` argument must also be provided. The <NewCSTPassword> must be substituted for the updated CST password.

Note the following:

- The current `vm.cstpword` key/value pair must be provided in the `hostname.properties` file.
- The <NewCSTPassword> must comply with CST Password requirements. Further, because the CST password can contain special characters (i.e., `!@#%&*_-=+|~`) care *must* be taken; some special characters (for example `|`, `!`, `=` and others) have special uses in the shell script and therefore must be escaped using `\` (for example, `\|` or `\=`).

[Tertiary Option]

The tertiary option is needed to modify key/value pairs (for example, component credential, database password, etc), but it can also be used during the initialization of the VM.

Note

The primary options must both be provided when using the tertiary option.

--vm.endingPw=<TheNewVMPassword>

In the VM creation scenario, this option specifies the ending password of the VM. In the existing VM scenario (`--rotate.components`) this option will change the password of the VM.

If you are instantiating the VM, the `-rotate.components` argument is not required. However, if the VM has already been created, the `-rotate.components` argument is required. The <TheNewVMPassword> must be substituted for the updated VM password.

APPENDIX E

Monitoring vCD Data Protection Extension Components

This appendix includes the following topics:

Introduction

The vCD Data Protection Extension now provides the ability to monitor system health, and to verify system availability and connectivity. The monitoring system provides information on overall system health and connectivity with external components with which Backup Gateway and vCloud Protector cells communicate.

The technology used for building the monitoring system is Java Management Extension (JMX), which allows remote JMX clients to connect to a Java process and to monitor applications running inside the process.

The resources being monitored are exposed as Mbeans with attributes representing the state of the resource.

In this appendix, JConsole is used as the JMX client for monitoring the system. See Other JMX clients on page 108 for a list of other JMX clients that can be used.

Setting up monitoring on the backup gateway

This section describes the necessary configuration for setting up monitoring for the backup gateway. Starting with version 2.0.3, monitoring is enabled by default.

Two java processes run on the backup gateway. Verify that monitoring is enabled for both processes. You can also change the default ports that JMX is configured at for each application.

The following procedure describes how to verify and, optionally, to change the configuration of JMX ports for each application.

Procedure

1. For the BG-ADS application, do the following:

   a. In the VMA used for deploying the backup gateway, open the `gateway.example.com` file that was used to deploy the backup gateway. Look for the `gateway.port.jmx_port_1` setting.

      If the setting is not present, monitoring is enabled for BG-ADS. These are the default port settings:

      - JMX Port : 7010 – The JMX port at which BG-ADS exposes its MBeans.
      - JMX Data Port : 7011 – The JMX Data port that BG-ADS uses internally for JMX data transfer.

   b. To change the default port, specify the following property in the properties file:

      - JMX Port: `gateway.port.jmx_port_1=<desired JMX port>`
      - JMX Data Port: `gateway.port.jmx_rmi_port_1=<another free port>`

2. For the BG-Plugin application, do the following:

   a. In the VMA used for deploying the backup gateway, open the `gateway.example.com` file that was used to deploy the backup gateway. Look for `gateway.port.jmx_port_2` setting.

      If it is not present, monitoring is enabled for BG-Plugin. These are the default port settings:

- JMX Port : 7020 – The JMX port at which BG-Plugin exposes its MBeans.
- JMX Data Port : 7021 – The JMX Data port that BG-Plugin uses internally for JMX data transfer.

b. To change the default port, specify the following property in the properties file:

- JMX Port: `gateway.port.jmx_port_2=<desired JMX port>`
- JMX Data Port: `gateway.port.jmx_rmi_port_2=<another free port>`

3. If you changed the default ports (described in steps 1.b and 2.b) after the install, run the following command on the VMA to update the configuration in the deployed backup gateway:

```
deployvm.sh --vm.hostname=<FQDN> –update
```

Turning off monitoring on the backup gateway

This section describes how to turn off monitoring on the backup gateway.

Procedure

1. For the BG-ADS application, in the VMA used for deploying the backup gateway, add or update the values of the JMX Port and JMX Data Port as follows:
   - JMX Port: `gateway.port.jmx_port_1=-1`
   - JMX Data Port: `gateway.port.jmx_rmi_port_1=-1`
2. For the BG-Plugin application, in the VMA used for deploying the backup gateway, add or update the value of the JMX Port and JMX Data Port as follows:
   - JMX Port: `gateway.port.jmx_port_2=-1`
   - JMX Data Port: `gateway.port.jmx_rmi_port_2=-1`
3. If you perform steps 1 or 2 after an install, run the following command on the VMA to update the configuration in the deployed backup gateway:

```
deployvm.sh --vm.hostname=<BackupGateway-FQDN> –update
```

Setting up monitoring on the vCloud Protector cell

This section describes the necessary configuration for setting up component monitoring for the vCloud Protector cell. Starting with version 2.0.3, monitoring is enabled by default.

Verify that monitoring is enabled for the vCloud Protector cell. You can also change the default ports that JMX is configured at for each application.

The following procedure describes how to verify and, optionally, change the configuration of JMX ports for the vCloud Protector cell.

Procedure

1. In the VMA used for deploying the vCloud Protector cell, open the `vcpcell.example.com` file that was used to deploy the vCloud Protector cell. Look for `vcpcell.port.jmx_port_1` setting.

   If it is not present, monitoring is enabled for the vCloud Protector cell. These are the default port settings:

   - JMX Port: 7010 – The JMX port at which vCloud Protector cell exposes its MBeans.
   - JMX Data Port: 7011 – The JMX Data port that vCloud Protector cell uses internally for JMX data transfer.

2. To change the default port, specify the following property in the properties file:

   - JMX Port: `vcpcell.port.jmx_port_1=<desired JMX port>`
   - JMX Data Port: `vcpcell.port.jmx_rmi_port_1=<another free port>`

3. If any of the ports have been updated as described in step 2 after the install, run the following command on the VMA to update the configuration in the deployed backup gateway:

   `deployvm.sh --vm.hostname=<FQDN> -update`

Turning off monitoring on the vCloud Protector cell

This section describes how to turn off monitoring on the vCloud Protector cell.

Procedure

1. In the VMA used for deploying the vCloud Protector cell, add or update the values of JMX Port and JMX Data Port as follows:

   - JMX Port: `vcpcell.port.jmx_port_1=-1`
   - JMX Data Port: `vcpcell.port.jmx_rmi_port_1=-1`

2. If you perform step 1 after an install, run the following command on the VMA to update the configuration in the deployed vCloud Protector cell:

   `deployvm.sh --vm.hostname=<VCP-FQDN> -update`

Setting up a remote JMX client for monitoring

This section describes how to set up the JMX client VM for remotely monitoring the backup gateway or the vCloud Protector cell.

Procedure

1. Configure a VM to monitor the component, hereafter called “JMX client VM.”
2. Ensure that JMX client VM must have network connectivity to the VM of the component being monitored - backup gateway and/or vCloud Protector cell.
3. Install Java Development Kit (JDK) v7 on the JMX client. JConsole is packaged as part of the JDK.
4. Export the public certificate of the component being monitored (backup gateway or vCloud Protector cell) and copy the certificate to the JMX client VM.

- To export the public certificate of the backup gateway:
  a. On the CPSH VM that was used to deploy the backup gateway, run the following command to export the public certificate of backup gateway:
  keytool -export -alias tomcat -keystore <BackupGatewayFQDN>.truststore -file gateway.example.com.crt
  Alternatively, you can log in to the backup gateway VM, navigate to the folder containing the truststore (`/etc/vcp`) and run the following command to export the public certificate :
  keytool -export -alias tomcat -keystore truststore -file gateway.example.com.crt
  b. Copy the `gateway.example.com.crt` public certificate file to the JMX client VM.
- To export the public certificate of the vCloud Protector cell:
  a. On the CPSH VM that was used to deploy the vCloud Protector cell, run the following command to export the public certificate of vCloud Protector cell:
  keytool -export -alias tomcat -keystore <vcpcell.example.com>.truststore -file vcpcell.example.com.crt
  Alternatively, you can log in to the vCloud Protector VM, navigate to the folder containing the truststore (`/etc/vcp`) and run the following command to export the public certificate:
  keytool -export -alias tomcat -keystore truststore -file vcpcell.example.com.crt
  b. Copy the `vcpcell.example.com.crt` public certificate file to the JMX client VM.

5. On the JMX client VM, enter the following command to create a truststore and to import the public certificate from step 4 into the truststore:
   keytool -import -alias "example-component" -file <example-certificate> -keystore <example-truststore>
6. Enter the following command to launch JConsole, using the truststore built in step 5:
   jconsole -J-Djavax.net.ssl.trustStore=<example-truststore> -J-Djavax.net.ssl.trustStorePassword=<example-truststore-password> <FQDN:Port>
   where:
   - FQDN is the fully qualified domain name of the component being monitored (backup gateway or vCloud Protector cell).
   - Port: JMX Port of the application being monitored – This is the port that was used to deploy the component in the backup gateway or vCloud Protector cell). Depending on the application being monitored, the following ports can be used:
     - Backup gateway – Port for either BG-ADS application or BG-Plugin application. See Setting up monitoring on the backup gateway on page 102.

- vCloud Protector – Port for vCloud Protector. See Setting up monitoring on the vCloud Protector cell on page 103.

Backup gateway health monitoring

The backup gateway has two separate independent Java applications:

- Backup gateway – ADS: Responsible for processing Requests from VCP.
- Backup gateway – Plugin: Responsible for communicating with vApp proxy.

The JMX client can be connected to the backup gateway ADS or plugin applications to monitor the heath of the particular application.

Each application exposes its MBeans for monitoring at separate ports configured during deployment. JMX clients connect to the two ports defined above (ADS-JMX Port or Plugin-JMX Port) to view resource health for that application.

Monitored resources have the following attributes:

- Status: Health Status represented as one of:
  - Uninitialized
  - Running
  - Failed
- Last Poll Time: Represents the last sampling time—the last time the status was updated.

The application resources described in the following sections are currently monitored.

Connectivity to Avamar

The backup gateway communicates with an Avamar system for its operations. The health of Avamar connectivity is shown as one of the following possible states:

- Running: The backup gateway can successfully connect to the Avamar system.
- Failed: The backup gateway cannot connect to the Avamar system.

Connectivity fo the cloud

The backup gateway communicates with one or more vCloud Director servers. The health of cloud connectivity is represented as one of the following states:

- Uninitialized:
  - Expected at server startup.
  - Also indicates a state when the backup gateway has not received any request from VCP, nor processed any scheduled jobs since server startup.
- Running: All cloud sessions that this backup gateway is currently maintaining are in a healthy state.
- Failed: One or more of the cloud sessions are in a Failed state.

Connectivity to the vCenter

The backup gateway communicates with one or more vCenters. The health of vCenter connectivity is represented as one of the following states:

- Uninitialized:
  - Expected at server startup.
  - Also indicates a state when the backup gateway has not processed any requests/jobs that require it to communicate with a vCenter since server startup.
- Running: All vCenter connections that this backup gateway is currently maintaining are in a healthy state.
- Failed: One or more of the vCenter sessions are in a Failed state.

vCloud Protector health monitoring

Unlike the backup gateway, the vCloud Protector is a single Java application.

The vCloud Protector exposes its MBeans for monitoring at a port configured during deployment. JMX clients connect to the two ports defined above (VCP-JMX Port) to view the resource health for that application.

Monitored resources have the following attributes:

- Status: Health status represented as one of:
  - Uninitialized
  - Running
  - Failed
- Last Poll Time: Represents the last sampling time—the last time the status was updated.

The application resources described in the following sections are currently monitored.

Connectivity to the database

vCloud Protector communicates with an internal Postgres database. The health of this database connectivity is shown as one of the following states:

- Uninitialized: The vCloud Protector Cell is probably starting up. Connectivity to the database has not been established.
- Running: The vCloud Protector cell can successfully connect to the database.
- Failed: The vCloud Protector cell cannot connect to the database.

Connectivity to the cloud

vCloud Protector cell receives requests from and communicates with the vCloud director. The health of this cloud connectivity is represented as one of the following states:

- Uninitialized: The vCloud Protector cell is probably starting up. Connectivity to the cloud has not been established.
- Running: The vCloud Protector cell can successfully connect to the cloud.
- Failed: The vCloud Protector cell cannot connect to the cloud.

Connectivity to RabbitMQ

vCloud Protector Cell receives job requests from and communicates with a RabbitMQ server.

The health of the RabbitMQ server connectivity is represented as one of the following states:

- Uninitialized: The vCloud Protector Cell is probably starting up. Connectivity to the RabbitMQ server has not been established.
- Running: The vCloud Protector cell can successfully connect to the RabbitMQ server.
- Failed: The vCloud Protector cell cannot connect to the RabbitMQ server.

Other JMX clients

There are other JMX clients that can be used to monitor the system:

- JMXConsoleTools, VisualVM (Free/OpenSource)
- Hyperic HQ (Community edition, enterprise edition)
- Zenoss (Limited OpenSource edition, commercial edition)

Operations personnel create alerts and notifications in the remote JMX client, based on reading MBean attributes. This is done on a polling basis where the frequency is set by the external monitoring system.

- Example 1, vCloud Protector cell monitoring: once a minute, obtain vCP server's database connection status. If it is down, send an alert.
- Example 2, backup gateway monitoring: once a minute, obtain the ADS application's Avamar connection status. If it is down, send an alert.

Troubleshooting

If JConsole or the JMX client cannot connect to any component, do the following:

- Verify that JMX is turned on for that particular Aries component (for example, vCloud Protector cell or backup gateway). In the VMA used for deploying the component, open the `<example-component>.properties` file and note the value specified for the JMX port specified for that application – component is not -1.
  - For the backup gateway ADS, look for <*gateway.jmx_port_1*>.
  - For the backup gateway plugin, look for <*gateway.jmx_port_2*>. If not specified in the file, the system uses a default value of 7020 (see Setting up monitoring on the backup gateway on page 102).
  - For the vCloud Protector cell, look for <*vcpcell.jmx_port_1*> . If not specified in the file, the system uses a default value of 7010 (see Setting up monitoring on the vCloud Protector cell on page 103).
- Verify that Jconsole is connecting to the right port.
- Verify that the signature on the public certificate in the JMX client truststore matches the one on the private key on the component.

- Verify that the truststore is provided in the path when JConsole is launched.

APPENDIX F

Port Usage

This appendix includes the following topic:

Port usage summary

The following table provides a summary of the ports that are used by the vCD Data Protection Extension.

Table 15 Network connection and port usage summary

Initiator	Target	Protocol	Port	Notes
vCloud Protector cell(s)	vCloud Director	TCP(https)	443	vCloud REST API
vCloud Protector cell(s)	RabbitMQ server	AMQP(TLS)	5671[a]	Message Queue
vCloud Protector cell(s)	vCloud Protector PostgreSQL database server	TCP	5432	SSL encrypted
EMC Backup Gateway	vCenter(s)	TCP (https)	443	vSphere SOAP API
EMC Backup Gateway	vCloud Director	TCP (https)	443	vCloud REST API
EMC Backup Gateway	RabbitMQ server	AMQP(TLS)	5671[b]	Message Queue
EMC Backup Gateway	AVE	TCP(https)	9443	EMC Avamar management WS
VM Image Proxy(s)	vCenter	UDP	902	vSphere SOAP API, VDDK communication
VM Image Proxy(s)	ESXi host(s)	TCP	902	Host access for provisioning
Avamar Backup Appliance	vCenter	TCP (https)	443	Vmfs datastore browse. Upload and download
Avamar Backup Appliance	Data Domain Backup Appliance (optional)	TCP(ssh)	22	
Avamar Backup Appliance	Data Domain Backup Appliance (optional)	TCP(NFS)	2049	nfsd
Avamar Backup Appliance	Data Domain Backup Appliance (optional)	TCP(NFS)	2052	mountd
Avamar Backup Appliance	Data Domain Backup Appliance (optional)	TCP(NFS)	111	portmapper

Table 15 Network connection and port usage summary (continued)

Initiator	Target	Protocol	Port	Notes
Avamar Backup Appliance	Data Domain Backup Appliance (optional)	TCP(NFS)	111	portmapper
Avamar Backup Appliance	Data Domain Backup Appliance (optional)	ICMP(ping)	7	
Avamar Backup Appliance	Data Domain Backup Appliance (optional)	UDP	161	SNMP
VM Image Proxy(s)	vCenter	TCP (https)	443	Vmfs datastore browse. Upload and download
VM Image Proxy(s)	Avamar Virtual Appliance	TCP	28001	EMC Avamar management protocol
EMC Backup Gateway	Avamar Virtual Appliance	TCP	28001	EMC Avamar management protocol
Avamar Backup Appliance	VM Image Proxy(s)	TCP	28002-28033	EMC Avamar management protocol
VM Image Proxy(s)	Avamar Virtual Appliance	TCP	27000, 29000	EMC Avamar storage protocol
Avamar Backup Gateway	Avamar Virtual Appliance	TCP	27000, 29000	EMC Avamar storage protocol
VM Image Proxy(s)	Data Domain Appliance	TCP	111	DDBoost-NFS protocol: RPC portmapper
VM Image Proxy(s)	Data Domain Appliance	TCP	2049	DDBoost, NFS protocol
VM Image Proxy(s)	Data Domain Appliance	TCP	2052[c]	DDBoost, NFS protocol; mountd
Newly deployed EMC Backup Gateway & vCloud Protector cells	EMC VPA	TCP(https)	8140	Puppet API
Newly deployed EMC Backup Gateway & vCloud Protector cells	EMC VPA	TCP(https)	80	Yum repository
vCloud Protector cell(s)	vCloud Director	TCP(https)	443	vCloud REST API
vCloud Protector cell(s)	EMC Gateway	TCP(https)	8443	Control path between cell and gateway

Table 15 Network connection and port usage summary (continued)

Initiator	Target	Protocol	Port	Notes
CPSH	vCenter(s)	TCP(https)	443	vSphere SOAP API
Reporting Server		TCP (http)	9783	Tomcat manager for administration
Reporting Server		TCP (http)	9446	Tomcat manager for administration
Reporting Server	RabbitMQ server	AMQP(TLS)	5672	Message Queue
Reporting Postgres database server	vCloud Protector PostgreSQL database server	TCP	5432	SSL encrypted

a. vSphere SOAP API, VDDK communication
b. vSphere SOAP API, VDDK communication
c. vSphere SOAP API, VDDK communication

GLOSSARY

A

administrator Person who normally installs, configures, and maintains software on network computers, and who adds users and defines user privileges.

Avamar server The server component of the Avamar client/server system. Avamar server is a fault-tolerant, high-availability system that efficiently stores the backups from all protected clients. It also provides essential processes and services required for data restores, client access, and remote system administration. Avamar server runs as a distributed application across multiple networked storage nodes.

B

backup A point-in-time copy of client data that can be restored as individual files, selected data, or as an entire backup.

backup appliance Represents an Avamar backup store, and maps a physical or virtual Avamar store to your cloud resources through a backup gateway server. It also associates one or more vCenter instances from your cloud to Avamar so that you can perform backup, restore, and replication operations.

backup policy template A combination of a backup schedule, a retention period, and an option set. To create a backup policy template, you must first create at least one schedule, one retention period, and one option set.

backup repository Associates a backup store with the Org VDCs in an organization. After you register an organization with the vCD Data Protection Extension, you can add backup repositories to the VDCs within the organization. Backup repositories are required for performing backups and restores.

browse The process of viewing data that is available for backup on a client computer or restore from the Avamar server.

D

DNS Domain Name Server. A dynamic and distributed directory service for assigning domain names to specific IP addresses.

M

MCS Management console server. The server subsystem that provides centralized administration (scheduling, monitoring, and management) for the Avamar server. The MCS also runs the server-side processes used by *Avamar Administrator*.

O

option set A collection of Avamar plug-in options that will be invoked during the backup process. By default, you should create an option set named "No Options" that contains no flags or values. Do not specify any flags unless instructed to do so by EMC Support.

P

plug-in Avamar client software that recognizes a particular kind of data resident on that client.

plug-in options Options that you specify during backup or restore to control backup or restore functionality.

policy A set of rules for client backups that can be named and applied to multiple groups. Groups have dataset, schedule, and retention policies.

R

restore An operation that retrieves one or more file systems, directories, files, or data objects from a backup and writes the data to a designated location.

restore-only repository Used only for restores, never for backups. A restore-only repository is required when you want to restore a vApp to a different Org VDC, a vApp that was installed on an Org VDC that has been deleted from vCloud Director, or a vApp backup that was replicated by Avamar.

retention The time setting to automatically delete backups on an Avamar server. Retention can be set to permanent for backups that should not be deleted from an Avamar server. Retention is a persistent and reusable Avamar policy that can be named and attached to multiple groups.

S

schedule The ability to control the frequency and the start and end time each day for backups of clients in a group. A schedule is a persistent and reusable Avamar policy that can be named and attached to multiple groups.

V

virtual machine (VM) A computer that is a software implementation of a computer. Virtual machines are used to run different operating systems at the same time on one physical computer. Each operating system runs in its own isolated execution environment.