Dell EMC vCloud Director Data Protection Extension

Version 19.2

Installation and Upgrade Guide

302-005-848
Rev 01
November 2019

DELL EMC

Copyright © 2001-2019 Dell Inc. or its subsidiaries. All rights reserved.

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS-IS." DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. USE, COPYING, AND DISTRIBUTION OF ANY DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA.

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

CONTENTS

PREFACE 7

Chapter 1 Installation Prerequisites 9
Installation overview 10
Naming conventions 10
Checklist for installation prerequisites 10
Checklist for general prerequisites 11
Installation assumptions 11
vCloud Director prerequisites 11
Networking prerequisites 12
Avamar prerequisites 12
Security prerequisites 13
Monitoring prerequisites 13

Chapter 2 vCD DPE Architecture 15
Architecture 16
List of components 16
Component deployment summary 17
Hardware and software requirements 17
Resource requirements 18
vSphere configuration requirements 18
Licensing requirements 19
Supported node operating systems 19
Supported databases 19
Supported Java versions 19
Supported TLS and SSL protocol versions and cipher suites 19
DNS and time sync requirements 19
Network security recommendations 19
Network connection and port usage summary 20
Cell network usage overview 22
Backup gateway network usage overview 23
Deployment example with network segregation 23

Chapter 3 Prepare the vPA 25
Deploy the vPA on the management vCenter 26
Install VMware components 26
About the deployment plan 27
Deployment plan parameters 27
Prepare the deployment plan 30
Encrypt and decrypt the deployment plan 31

Chapter 4 Deployment 33
About deployment 34
Perform an all-in-one deployment 34
Deploy a single node 35
Install the UI plug-in on vCloud Director 36
Deployment scenarios 36

Deploy nodes with an existing RabbitMQ (AMQP) configuration 36
Scale out the cell or backup gateway..... 37
Deploy the UI server and FLR UI server with a user-provided certificate 39

Chapter 5 Upgrade 43
Introduction..... 44
Upgrade prerequisites..... 44
Prepare for upgrade.....44
Upgrade the vPA.....44
Perform an all-in-one upgrade..... 45
Upgrade using the existing PostgreSQL database and RabbitMQ server..... 46
Migrate the existing PostgreSQL databases to the utility node.....47
Dump the existing PostgreSQL databases..... 48
Prepare the utility node.....48
Import the existing PostgreSQL databases..... 50
Perform an upgrade on a single node.....51
Verify completion of the upgrade..... 51
Verify the backup gateway upgrade.....51
Verify the cell upgrade..... 52
Verify the reporting server upgrade..... 52
Verify the UI server upgrade..... 53
Verify the FLR UI server upgrade..... 53
Log in to the vCD DPE..... 54

Chapter 6 Troubleshooting 55
Logfile locations.....56
Partial updates to the deployment plan.....56
Master password encryption and decryption errors.....56
Deployment plan validation errors.....56
Shared secret errors..... 57
Property file errors.....57
Unable to obtain vCenter information from the vPA..... 57
Verify that all services are running..... 58
Verify the UI server.....58
Verify the FLR UI server.....58
Verify the cells..... 58
Verify the backup gateway.....60
Verify the reporting server..... 61
SSL certificate errors..... 61
Partial updates to the bootstrap.properties file.....62
Composing a partial bootstrap.properties file.....62
Credentials.....63
Independent keys.....63
Reset the lockbox..... 63
Cannot add a private key for a node.....64
Nodes do not successfully upgrade.....64
Cannot log in using plaintext authentication.....64
The vPA OVA template certificate has expired..... 65

Appendix RabbitMQ Server 67
Generate public/private key pairs for SSL servers.....68
Installing and configuring a RabbitMQ server.....71
Deploying RabbitMQ.....71

Monitor RabbitMQ..... 72
Install an SSL certificate on a RabbitMQ server..... 73
Publish an SSL certificate on a RabbitMQ server..... 73

PREFACE

As part of an effort to improve its product lines, Dell 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.

Contact the technical support professional when a product does not function correctly or does not function as described in this document.

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

Purpose

This guide describes how to install, configure, and upgrade the Dell EMC vCloud Director Data Protection Extension (vCD DPE).

Revision history

The following table presents the revision history of this document.

Table 1 Revision History

Revision	Date	Description
01	November 15, 2019	First release of vCloud Director Data Protection Extension 19.2

Related documentation

The following publications provide additional information:

- *vCloud Director Data Protection Extension Release Notes*
- *vCloud Director Data Protection Extension Administration and User Guide*
- *vCloud Director Data Protection Extension REST API Reference Guide*
- *vCloud Director Data Protection Extension Message Bus Specification Reference Guide*
- *Avamar for VMware User Guide*

Typographical conventions

These type style conventions are used in this document.

Table 2 Typographical conventions

Bold	Used for names of interface elements, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what the user specifically selects or clicks)
Italic	Used for full titles of publications that are referenced in text
`Monospace`	Used for: • System code • System output, such as an error message or script

Table 2 Typographical conventions (continued)

	• Pathnames, filenames, prompts, and syntax • Commands and options
Monospace italic	Used for variables
`Monospace bold`	Used for user input
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections - the bar means "or"
{ }	Braces enclose content that the user must specify, such as x or y or z
...	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 resolve a product issue before contacting Customer Support.

To access the Avamar support page:

1. Go to https://www.dell.com/support/home/us/en/19.
2. Type a product name in the **Enter a Service Tag, Serial Number, Service Request, Model, or Keyword** search box.
3. Select the product from the list that appears. When you select a product, the **Product Support** page loads automatically.
4. (Optional) Add the product to the **My Products** list by clicking **Add to My Saved Products** in the upper right corner of the **Product Support** page.

Comments and suggestions

Comments and suggestions help 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

Installation Prerequisites

This chapter includes the following topics:

- Installation overview 10
- Naming conventions 10
- Checklist for installation prerequisites 10
- Checklist for general prerequisites 11
- Installation assumptions 11
- vCloud Director prerequisites 11
- Networking prerequisites 12
- Avamar prerequisites 12
- Security prerequisites 13
- Monitoring prerequisites 13

Installation overview

The vCloud Director Data Protection Extension (vCD DPE) requires deployment of multiple VMs in the cloud infrastructure where a VM or a group of VMs are configured with a specific application payload (cell, backup gateway, utility node (RabbitMQ and PostgreSQL), UI server, reporting server, and FLR UI server). The number of Avamar servers under management by the vCD DPE determines the scale of the number of VMs to deploy, based on the customer environment.

Since the vCD DPE is targeted for the service provider market, the installation process supports a wide-scale scripted and automated deployment and configuration of the vCD DPE VMs. To fulfill this requirement, the vCD DPE installation process uses Puppet, which is an open source configuration management tool along with other utilities and libraries (`ovftool`, VIX API).

Virtual Provisioning Appliance (vPA)

Instead of delivering specific OVAs for each application, the vCD DPE comes as a single OVA (the vPA) which acts as a Puppet Master. This VM hosts a baseline SLES 12 SP4 OVA template, as well as a `yum` repository which carries the application payload.

About installation

Before beginning the installation process, validate that all of the prerequisites have been met. The install process begins with the deployment of the vPA. After you deploy the vPA, the management tool deploys, upgrades, migrates, and configures the VMs from the vPA. The management tool reads a deployment plan with the name `deploy_plan.conf`. The deployment plan contains the information that is required to deploy the VMs.

Naming conventions

Consider the following naming conventions:

The fully qualified domain name (FQDN) must be lowercase.

Checklist for installation prerequisites

The following installation information is required:

Table 3 Checklist for installation prerequisites

☐	vCD address
☐	vCD admin account username
☐	vCD admin account password
☐	RabbitMQ server address[a]
☐	RabbitMQ server management account username[a]
☐	RabbitMQ server management password[a]

a. Only required if you have configured your own RabbitMQ server.

Checklist for general prerequisites

Record the following information about the vCloud Director backup environment:

Table 4 vCloud Director checklist

☐	Number of Avamar Data Stores	(Physical Avamar servers)
☐	Number of AVE servers	
☐	Total number of Avamar servers	(Add previous values)
☐	Number of backup gateways	(The ratio of backup gateways to Avamar servers is 1:1)
☐	Number of cells	
☐	Number of management vCenters	
☐	Number of resource vCenters	

Using the information in the previous table, calculate the number and type of nodes to install:

Table 5 Node quantity checklist

☐	Number of backup gateway VMs	(The same as the number of backup gateways)
☐	Number of cell VMs	(The same as the number of cells)
☐	Optional components	
☐	UI server	1 per vCD DPE instance
☐	Reporting server	1 per vCD DPE instance
☐	FLR UI server	1 per vCD DPE instance

Installation assumptions

The following assumptions about the installation apply:

- All inter-component connections use SSL.
- The default installation is not configured for centralized logging. This topic is covered in the *vCloud Director Data Protection Extension Administration and User Guide* as a separate post-installation procedure.

vCloud Director prerequisites

Complete the following prerequisites before you install the software:

- Configure public IP addresses.

- Configure the public REST API base URL:
  1. Select **vCloud Director UI** > **Administration** > **Public Addresses**.
  2. Enable "Customer Public Endpoints," and configure the "HTTPS REST API base URL" as "https://*<FQDN>*."
  3. Enable "Tenant Portal: "Copy API URL Settings." Then you can log in to the vCloud Director Tenant Portal with the base URL.
- Collect the cloud deployment details, including the management vCenters and resource vCenters.
- Verify that the vCenters are registered in vCloud Director by their fully qualified domain names and not by IP addresses.
- Provision a vCloud Director service account with provider-level access for use by the vCD DPE.

Networking prerequisites

Complete the following networking prerequisites before you install the software:

- Collect network deployment details, such as VLANs, network segments, and firewall rules.
- Open the required firewall ports.
- Provision DNS records and IP addresses for the nodes, based on the calculated configuration. Configure DNS to resolve all IP addresses and corresponding fully qualified domain names for the nodes.
- Configure DNS records for all vCenters that are configured in vCloud Director and configure all vCenters to use DNS.

Avamar prerequisites

Complete the following Avamar prerequisites before you install the software:

- Register the management and resource vCenters with the Avamar servers by using fully qualified domain names.
- Install or deploy Avamar or AVE servers and any corresponding Data Domain systems are installed, with supported software versions.
- Deploy image proxies within the resource vCenters that are compliant with the Avamar server software version.
- Register the image proxies with the associated Avamar servers.

Before you install the vCD DPE, perform the following steps:

1. Log in to the Avamar server as admin.
2. Using a Linux text editor, such as `vi`, open `/usr/local/avamar/var/mc/server_data/prefs/mcserver.xml`.
3. Change the following line:

   ```
   <entry key="allow_duplicate_client_names" value="false" />
   ```

   to:

   ```
   <entry key="allow_duplicate_client_names" value="true" />
   ```
4. Restart the Avamar MCS by typing the following commands:

```
dpnctl stop mcs
dpnctl start mcs
```

Security prerequisites

Complete the following security prerequisites before you install the software:

- Configure vCloud Director for SSL.
- Ensure that the CN field in the SSL certificates points to the fully qualified domain name of the server.

  The CN should correspond to the vCloud Director public address, which is also the fully qualified domain name of the load balancer.

Monitoring prerequisites

The vCD DPE provides JMX monitoring for the backup gateway and the cells. To monitor the system, configure a JMX client.

Different types of JMX clients can connect to a JMX agent (MBean server). For example, a simple JMX client such as `jconsole`, which is part of the Java SDK, or a full featured management application, such as Hyperic. Typically, operations personnel use a remote full featured JMX compliant management application to create alerts or notifications that are based on reading MBean attributes from the backup gateway and the cells.

CHAPTER 2

vCD DPE Architecture

This chapter includes the following topics:

- Architecture 16
- vSphere configuration requirements 18
- Licensing requirements 19
- Supported node operating systems 19
- Supported databases 19
- Supported Java versions 19
- Supported TLS and SSL protocol versions and cipher suites 19
- DNS and time sync requirements 19
- Network security recommendations 19
- Network connection and port usage summary 20
- Cell network usage overview 22
- Backup gateway network usage overview 23
- Deployment example with network segregation 23

Architecture

The vCD DPE consists of one or more cell nodes. These nodes share a common database, and are linked to a single vCloud, and an arbitrary number of vCenter servers, ESXi host clusters, and backup appliances.

A typical installation creates a group of nodes. Each node in the group runs a collection of services. All members of the group share a single database. Each cell in the group connects to the VMware vCloud Director through a common RabbitMQ server. The RabbitMQ message queue acts as a load balancer, holding requests for a scale out "farm" of cells. The available throughput is expandable by adding cells and backup appliances.

List of components

Table 6 List of components

Component	Description	Source
vCloud Director	Implements service to provision and manages software defined virtual data centers as part of a public, private, or hybrid cloud solution. Incorporates vSphere vCenters and ESXi clusters.	VMware
vCD DPE UI plug-in extension	Helps you manage data protection from the vCloud Director web page.	Dell EMC
vPA	Maintains the configuration of other nodes through the open source Puppet tool.	Dell EMC
Utility node	Hosts instances of the RabbitMQ server and PostgreSQL database server.	Dell EMC
RabbitMQ server	Implements a scalable message bus service to provide publish/subscribe event notification and data delivery.	Installation deploys an instance on the utility node.
PostgreSQL database server	Implements the SQL database that holds backup policies and backup policy mapping to vCloud objects. Also implements the SQL database which stores notification messages that are persisted by the reporting server.	Installation deploys an instance on the utility node.
Cell nodes	Implements an embedded extension to the vCloud Director REST API to provide policy-based backup service for virtual data centers and vApps.	Dell EMC
Avamar server	Initiates scheduled backups and maintains a catalog of retained backups. Also manages ad-hoc backup and restore requests. An Avamar server is vSphere-aware, but maintains no awareness or connections to the vCloud.	Dell EMC
Backup gateway	Implements a "façade" web service which adds cloud awareness to an Avamar server. Resides on the same VM as the vApp proxy.	Dell EMC
Data Domain system	Provides scalable storage for backups, with features that include source data deduplication and replication.	Dell EMC
VM image proxy	Conducts a VM backup or restore when triggered by an Avamar server.	Dell EMC
vApp proxy	Conducts a vCloud vApp backup or restore when triggered by an Avamar server with a backup gateway. Resides on the same VM as the backup gateway.	Dell EMC
UI server	This component provides a user interface for basic backup and restore configuration and operations.	Dell EMC

Table 6 List of components (continued)

Component	Description	Source
Reporting server	This optional component listens for RabbitMQ event messages, as described in the *vCloud Director Data Protection Extension Message Bus Specification Reference Guide*. Remaps and persists the event messages into a dedicated PostgreSQL relational database for purposes of report generation and chargeback.	Dell EMC
FLR UI server	This optional component provides a user interface for file level restore operations.	Dell EMC

Component deployment summary

Table 7 Component deployment summary

Component	Where installed (management or tenant environment)	Number deployed (min–max)
vCloud Director	Components straddle both	1–1
vCD DPE UI plug-in extension	Tenant	1–1
vPA	Management	1 per physical site
Utility node	Management	1–1
RabbitMQ server	Management	1–1
PostgreSQL database server	Management	1–1
Cell nodes	Management	1–n, 2 min for production, typically 1+# of Avamar servers
Avamar server	Management	1–n, 1 typical
Backup gateway with vApp proxy server	Management	1 per Avamar server
Data Domain system	Management	0–n, 1 typical
VM image proxy	Tenant	1–n, 1 per resource cluster is minimum and typical
UI server	Management	1–1
Reporting server	Management	0–1 (optional)
FLR UI server	Management	0–1 (optional)

All components are hosted on VMs except for the Avamar server and Data Domain system, which are also available in physical options for very large clouds.

Hardware and software requirements

Each vCD DPE node must meet certain hardware and software requirements.

A supported database must be accessible to all members of the group. The vCD DPE typically deploys a RabbitMQ server and a PostgreSQL database during installation.

The vCD DPE requires access to vCloud Director and one or more Dell EMC backup appliances.

Resource requirements

AVE and DDVE instances have their own separate resource requirements that depend, in part, on licensed capacity. The *Avamar Virtual Edition Installation and Upgrade Guide* and *Data Domain Virtual Edition Installation and Administration Guide* provide more information.

All components use the SLES 12 SP4 operating system.

Table 8 Resource requirements

Node	Virtual CPUs	Virtual disk	Virtual RAM
vPA	2	20 GB thin	2 GB
Backup gateway with vApp proxy server	4	20 GB	6 GB
Utility node with RabbitMQ server and PostgreSQL database server	2 per node	20 GB per node	2 GB per node
Cell nodes			
UI server			
Reporting server			
FLR UI server			

vSphere configuration requirements

Servers and hosts that are intended for use with the vCD DPE must meet specific configuration requirements.

A vCloud Director installation should segregate management VMs into a management vCenter, and resource clusters running tenant workloads into a second resource vCenter.

- Deploy Avamar VM image proxies in the resource vCenter, with one (or optionally more) per ESX host cluster. Deploy these proxies from vCenter, and not from vCloud Director.
- Deploy all other vCD DPE nodes in the management vCenter.
- Register the resource vCenter with the Avamar server that protects vApps running on the vCenter.
- The best practice is to create a dedicated vSphere account for use by the Avamar server, so that activities that the Avamar server initiates can be identified in vSphere events and logs.
- Register the management vCenter that hosts a backup gateway with the Avamar server that is associated with the backup gateway.
- Configure and verify operation of forward and reverse DNS for all nodes with a hostname.

Licensing requirements

Licensing is installed and managed at the backup appliance level. The vCD DPE does not require license configuration.

Supported node operating systems

The vCD DPE deploys nodes as complete VMs with pre-installed operating systems.

Dell EMC does not support replacement of the standard operation system distribution or version, or extraction of RPMs and redeployment to a custom customer-configured VM.

Supported databases

The vCD DPE requires a PostgreSQL database. Versions 9.1 through 9.6 are supported. PostgreSQL 10.*x* is not supported.

The optional reporting server also requires a PostgreSQL database. The vFabric PostgreSQL database meets this requirement. The version included in SLES 11.3 also meets this requirement.

Supported Java versions

Some nodes must have Java Runtime Environment (JRE) 1.8 or later installed and enabled. The preflight tool also requires JRE 1.8 or later. Only the 64-bit version of JRE is supported.

Supported TLS and SSL protocol versions and cipher suites

The vCD DPE requires clients to use TLS 1.2. Supported cipher suites include those with ECDHE key exchange algorithm, RSA signatures and AES-128 or AES-256 ciphers.

DNS and time sync requirements

Secure, reliable operation depends on a secure, reliable network that supports forward and reverse lookup of hostnames, a network time service, and other services. Your network must meet these requirements before you begin the installation.

Network security recommendations

Secure operation requires a secure network environment. Configure and test this network environment before you begin the installation.

About this task

Connect all nodes to a network that is secured and monitored.

vCD DPE network connections have several additional requirements:

- Do not connect the vCD DPE directly to the public Internet. Always protect vCD DPE network connections with a firewall.
  - Open to incoming connections only the ports that are documented in the port usage table.

  - Open port 22 (SSH) for incoming connections, if needed.
  - The firewall must reject all other incoming traffic from a public network.
- Change the default passwords and use strong passwords.
- Route traffic between nodes over a dedicated private network, if possible.
- Virtual switches and distributed virtual switches that support provider networks must be isolated from each other. They cannot share the same level 2 physical network segment.

Network connection and port usage summary

Table 9 Network connection and port usage summary

Initiator	Target	Protocol	Port	Notes
Cells	vCloud Director	TCP (HTTPS)	443	vCloud REST API
Cells	RabbitMQ server	AMQP (TLS)	5671[a]	Message queue
Cells	PostgreSQL database server	TCP (SSL)	5432	PostgreSQL frontend/backend protocol v3.0
Cells	Backup gateway	TCP (HTTPS)	8443	Backup gateway REST API
JMX client	Cells	TCP (RMI SSL)	7010[b]	MBean server
JMX client	Cells	TCP (RMI SSL)	7011[b]	MBean server client RMI port
Backup gateway	vCenter(s)	TCP (HTTPS)	443	vSphere SOAP API
Backup gateway	vCloud Director	TCP (HTTPS)	443	vCloud REST API
Backup gateway	RabbitMQ server	AMQP (TLS)	5671[a]	Message queue
JMX client	Backup gateway	TCP (RMI SSL)	7010[b]	Avamar MBean server
JMX client	Backup gateway	TCP (RMI SSL)	7011[b]	Avamar MBean server client RMI port
JMX client	Backup gateway	TCP (RMI SSL)	7020[b]	Plugin MBean server
JMX client	Backup gateway	TCP (RMI SSL)	7021[b]	Plugin MBean server client RMI port
Avamar server	Data Domain (optional)	TCP (NFS)	2049	`nfsd`
Avamar server	Data Domain (optional)	TCP (NFS)	2052	`mountd`
Avamar server	Data Domain (optional)	TCP (NFS)	111	`portmapper`
Avamar server	Data Domain (optional)	ICMP (ping)	7	
Avamar server	Data Domain (optional)	UDP	161	SNMP
VM image proxies	vCenter	TCP (HTTPS)	443	Vmfs datastore browse. Upload and download
VM image proxies	AVE	TCP	28001	Avamar management protocol
Backup gateway	AVE	TCP	28001	Avamar management protocol
Avamar server	VM image proxies	TCP	28002-28033	Avamar management protocol
Avamar server	Backup gateway	TCP	28002-28033	Avamar management protocol
VM image proxies	Avamar server	TCP	27000, 29000	Avamar storage protocol

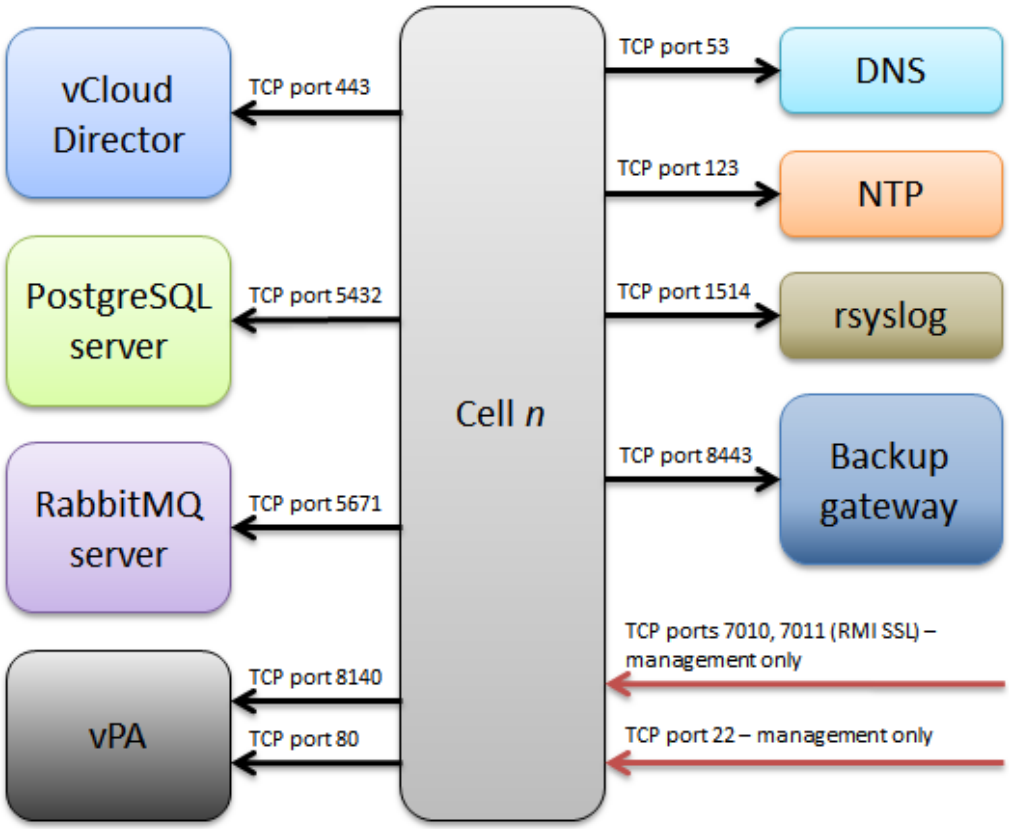
Table 9 Network connection and port usage summary (continued)

Initiator	Target	Protocol	Port	Notes
Backup gateway	Avamar server	TCP	27000, 29000	Avamar storage protocol
Backup gateway	Avamar server	TCP (HTTPS)	9443	Avamar SOAP web service
VM image proxies	Data Domain	TCP	111	DDBoost-NFS protocol: RPC `portmapper`
VM image proxies	Data Domain	TCP	2049	DDBoost, NFS protocol
VM image proxies	Data Domain	TCP	2052[b]	DDBoost-NFS protocol: `mountd`
Newly deployed Backup gateway and cells	vPA	TCP (HTTPS)	8140	Puppet API
Newly deployed Backup gateway and cells	vPA	TCP (HTTP)	80	Yum repository
vPA	vCenter(s)	TCP (HTTPS)	443	vSphere SOAP API
Reporting server	RabbitMQ server	AMQP (TLS)	5671[b]	Message queue.
Reporting PostgreSQL database server	PostgreSQL database server	TCP (SSL)	5432	PostgreSQL frontend/backend protocol v3.0.
Web browser	FLR UI server	TCP (HTTPS)	5481	
FLR UI server	vCloud Director	TCP (HTTPS)	443	vCloud REST API
Web browser	UI server	TCP (HTTPS)	443	
UI server	vCloud Director	TCP (HTTPS)	443	vCloud REST API

a. Assuming use of TLS, unencrypted AMQP (not recommended) uses 5672 instead.
b. Default, can be reconfigured.

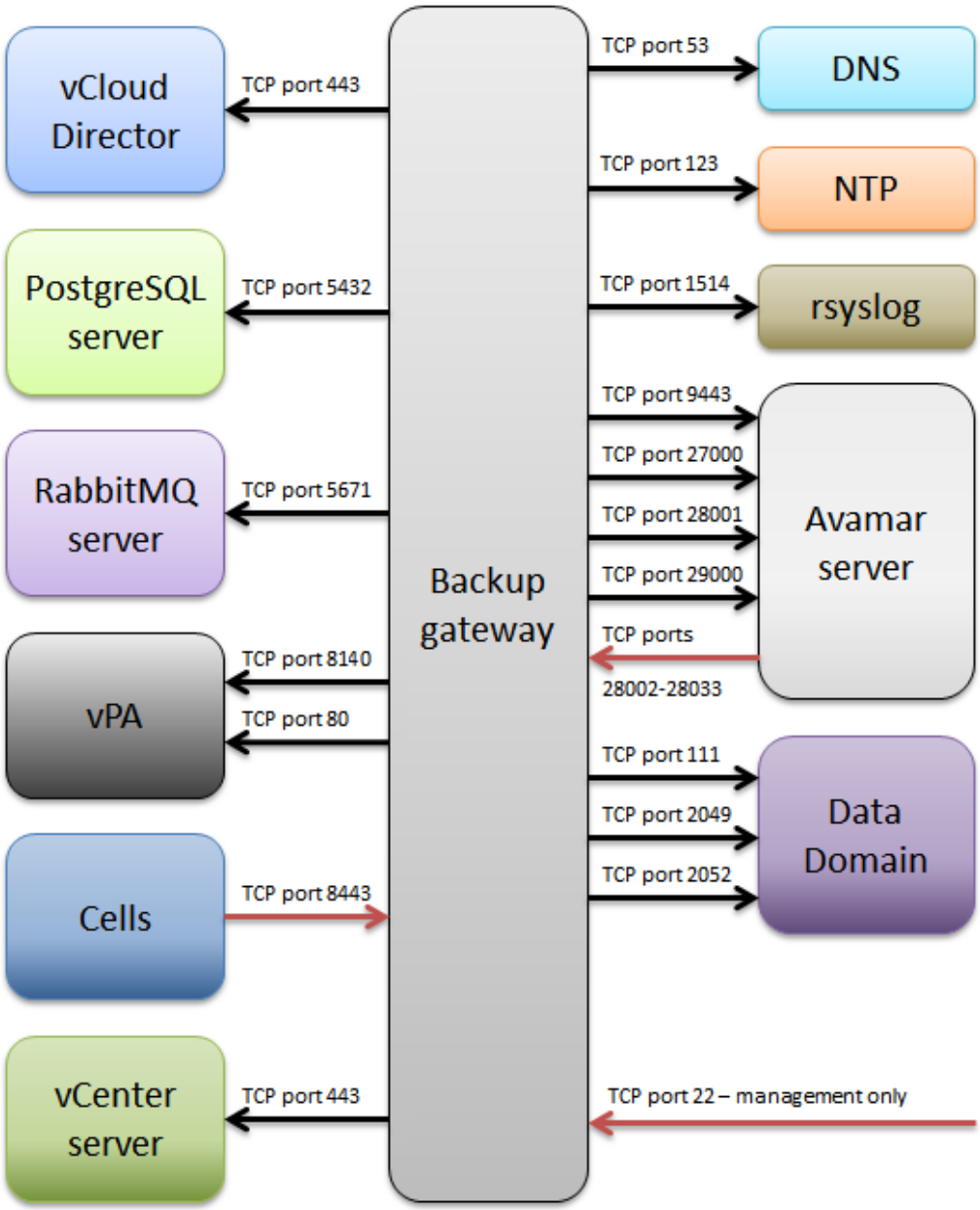
Cell network usage overview

Figure 1 Cell network usage overview



Backup gateway network usage overview

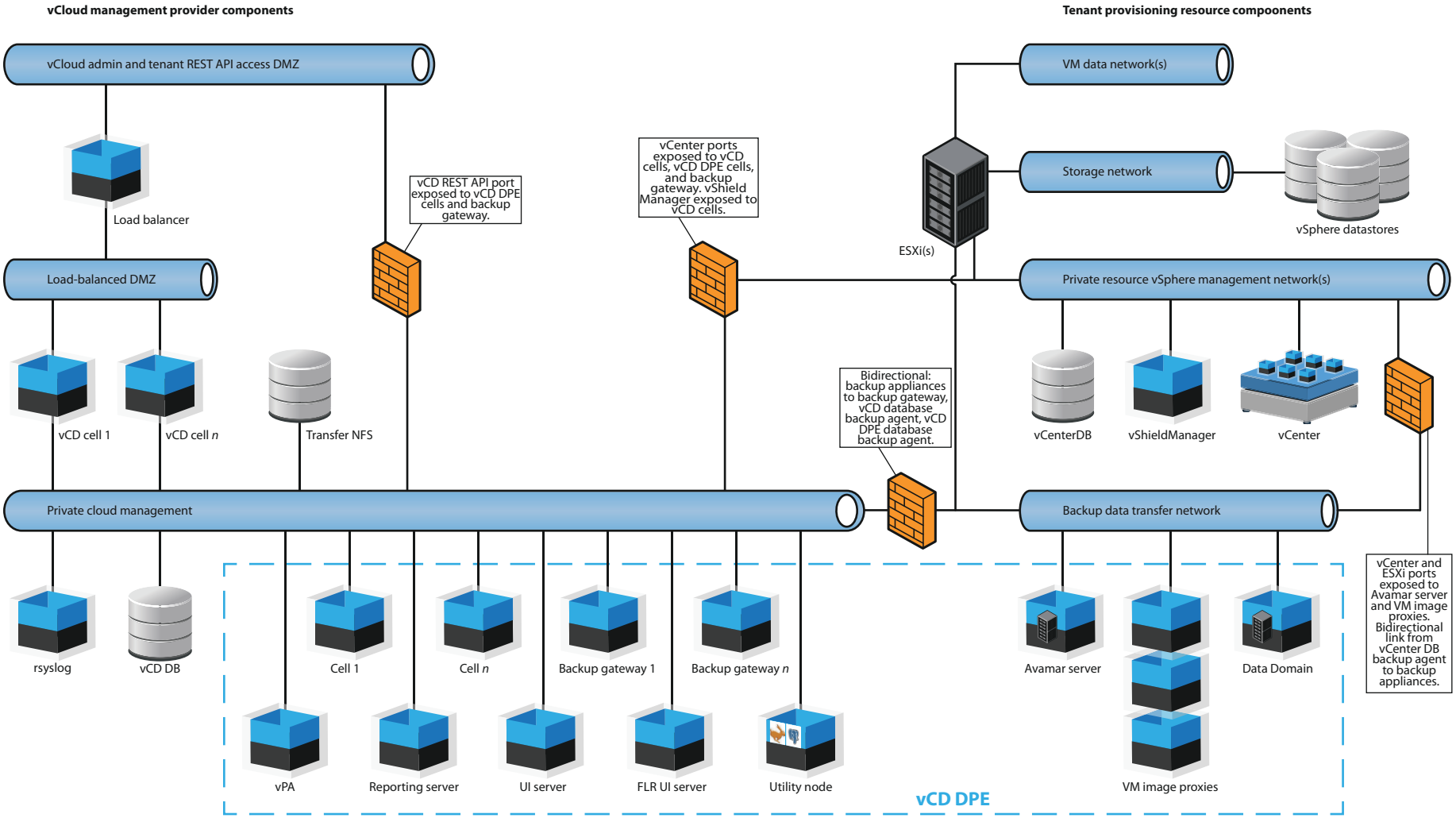
Figure 2 Backup gateway network usage overview



Deployment example with network segregation

In a service provider environment, network segregation for security and congestion control is typical. The following diagram is one example of how a service provider might choose to segregate a network. The diagram shows the placement of both vCloud Director and vCD DPE components. The degree to which a network is segregated is flexible and need not match the suggested configuration.

Figure 3 Network segregation



CHAPTER 3

Prepare the vPA

This chapter includes the following topics:

- Deploy the vPA on the management vCenter 26
- Install VMware components 26
- About the deployment plan 27

Deploy the vPA on the management vCenter

Before you begin

Deployment requires the following network settings for the vPA:

- The fully qualified domain name.
- The IP address.
- The default gateway.
- The network mask.
- The DNS server IP address.
- The vSphere network ID.

Procedure

1. Use the installation prerequisites and the vSphere Web Client deployment wizard to deploy the vPA in the management vCenter.

   Ensure that the network settings are correct. All nodes copy network settings from the vPA during deployment.

2. During the vPA deployment, the vCD DPE presents the End User License Agreement (EULA). Read and accept the EULA.

   When you accept the EULA, the vPA deployment proceeds. Wait for the vPA to complete.

3. After vPA deployment completes, log in to the vPA as the root user.
4. Check the network settings by typing the following command:

   ```
   hostname
   ```

   This command prints the hostname.

5. Verify that the hostname is the same as the fully qualified domain name.

   If the hostname is not the same as the fully qualified domain name, the network settings are incorrect. Check the network settings and redeploy the vPA.

Install VMware components

After you deploy the vPA, install the VMware OVF tool and the VMware vSphere CLI on the vPA.

Before you begin

The following packages can be found in the `/root` directory on the vPA:

- `VMware-ovftool-4.3.0-12320924-lin.x86_64.bundle`
- `VMware-vSphere-CLI-6.7.0-8156551.x86_64.tar.gz`

Procedure

1. Log in to the vPA as the root user.
2. Change directory by typing the following command:

   ```
   cd /root
   ```

3. Install the VMware OVF tool by typing the following command:

   ```
   ./VMware-ovftool-4.3.0-12320924-lin.x86_64.bundle
   ```

   Review and accept the terms in the EULA for the VMware OVF tool.

4. Install the VMware vSphere CLI:
   a. Extract the tar file:
      ```
      tar -xzvf VMware-vSphere-CLI-6.7.0-8156551.x86_64.tar.gz
      ```
   b. Change directory by typing the following command:
      ```
      cd vmware-vsphere-cli-distrib
      ```
   c. Start the installer by typing the following command:
      ```
      ./vmware-install.pl
      ```
   d. Review and accept the terms in the EULA for the VMware vSphere CLI.

About the deployment plan

`deploy_plan.conf` is a configuration file that contains information about the vCloud Director backup environment, including credentials for vCloud Director, vCenter, vCD DPE nodes, and other components.

The management tool uses these credentials to generate the property files, truststores, and SSL certificates for deployment. Complete the deployment plan before deploying VMs.

The reporting server and the FLR UI server nodes are optional. If you do not plan to deploy these nodes, comment out the corresponding sections in the deployment plan. Prepare the deployment plan on page 30 provides more information.

Deployment plan parameters

The following table describes the fields in `deploy_plan.conf`. This topic also contains general rules for most password fields.

Table 10 Deployment plan parameters

Section	Parameter	Description
`Vcenter`	`fqdn`	Required. The FQDN that corresponds to the management vCenter.
	`admin`	Required. The admin role account that corresponds to the management vCenter.
	`vct_password`	Required. The password for the admin role account.
`Vcloud`	`fqdn`	Required. The FQDN that corresponds to vCloud Director.
	`user`	Required. A vCloud Director administrative account to be used for backup related activities. The account must be in the form of *username*@*SYSTEM*.
	`vcd_password`	Required. The password for the vCloud Director administrative account.
`Credentials`	`truststore_password`[a]	A password for the truststore that holds SSL certificates. The value for this field follows the general password rules.
	`lockbox_password`[a]	The value for this field follows the general password rules.
	`vm_password`	Required. The root password for all nodes.

Table 10 Deployment plan parameters (continued)

Section	Parameter	Description
		The value for this field follows the general password rules.
	shared_secret	A shared 256 bit, Base64-encoded secret key to be set to the same value for all cells within a vCloud. The shared secret value encrypts elements in the PostgreSQL database for cells. For new deployments, the shared secret key is optional[a]. For upgrades, the shared secret key is required. Supply the shared secret key that was configured during deployment. Upgrade prerequisites on page 44 provides more information.
Postgresql	ip	Required. The IP address and FQDN for the utility node. For new deployments, you must deploy PostgreSQL and RabbitMQ on the same node.
	fqdn	
	user	Required. The user account for PostgreSQL.
	db_password	Required. The password for the PostgreSQL user account. The value for this field follows the general password rules.
	vm_user[b]	The user account and password for the VM that hosts the PostgreSQL node.
	vm_password[b]	
Rabbitmq	ip	Required. The IP address and FQDN for the utility node. For new deployments, you must deploy PostgreSQL and RabbitMQ on the same node.
	fqdn	
	user	Required. The user account for RabbitMQ.
	mq_password	Required. The password for the RabbitMQ user account. The value for this field follows the general password rules.
	vm_user[b]	The user account and password for the VM that hosts the RabbitMQ node.
	vm_password[b]	
Vcpcell-*x*[c]	ip[d]	Required. The IP address and FQDN for the cell.
	fqdn[d]	
	db_name	Required. The database name for the cell. The database name must be the same among cells.
	db_user[b]	The database user account for the cell.
	db_password[b]	The database user password for the cell.
Vcpbg-*x*[c]	ip[d]	Required. The IP address and FQDN for the backup gateway.
	fqdn[d]	
	ave_addr	Required. The FQDN of the Avamar server.
	ave_user	Required. The administrative account on the Avamar server.
	ave_password	Required. The password for the administrative account on the Avamar server.
Vcprpt[e]	ip[d]	Required. The IP address and FQDN for the reporting server.

Table 10 Deployment plan parameters (continued)

Section	Parameter	Description
	fqdn[d]	
	db_name	Required. The database name for the reporting server.
	db_user[b]	The database user account for the reporting server.
	db_password[b]	The database user password of the reporting server.
Vcpui	ip[d]	Required. The IP address and FQDN for the UI server.
	fqdn[d]	
Vcpflr[e]	ip[d]	Required. The IP address and FQDN for the FLR UI server.
	fqdn[d]	
Advanced[f]	vm_cluster[g]	The cluster within the management vCenter which contains the backup gateway VM.
	vm_datacenter[g]	The datacenter within the management vCenter which contains the backup gateway VM.
	vm_datastore[g]	The datastore that holds virtual disks that are associated with the backup gateway VM.
	vm_resourcepool[g]	The resource pool within the Cluster which contains the backup gateway VM.
	vm_DNS[g]	The DNS server address.
	vm_network[g]	The label on the vSphere network to connect to the cell VM.
	vm_netmask[g]	The cell VM subnet mask.
	vm_gateway[g]	The cell VM gateway.
	vm_diskmode[g]	The disk provisioning type. For example, thin provisioning.
	vm_folder[g]	The folder that stores vCD DPE nodes.
	gateway.port.jmx_port_1	These fields are required for Java JMX monitoring. **Note:** Only advanced users should modify these fields.
	gateway.port.jmx_rmi_port_1	
	gateway.port.jmx_port_2	
	gateway.port.jmx_rmi_port_2	
	vcpcell.port.jmx_port_1	
	vcpcell.port.jmx_rmi_port_1	

a. If this value is not set, the management tool automatically generates it. Dell EMC recommends that you do not set this value.
b. This field is only required for upgrades from versions before 18.2, when RabbitMQ and PostgreSQL reside on different VMs and have separate credentials.

Table 10 Deployment plan parameters (continued)

c. *x* is a placeholder that represents the component number (for example, *Vcpcell-1* or *Vcpbg-1*).
d. The IP address and FQDN must match the DNS record.
e. This node is optional.
f. The fields in the `Advanced` section of the configuration file are optional, however, you cannot remove or omit this section.
g. If you do not set this value, the management tool uses the corresponding value from the vPA VM.

General password rules

Passwords must meet the following requirements:

- Be at least 8 characters long
- Contain at least one numeric character
- Contain at least one uppercase alphabetic character
- Contain at least one lowercase alphabetic character
- Contain at least one of the following non-alphanumeric characters:

  !@#%&*_-=+~

The password cannot contain characters such as a period (.) or a space, and cannot start with `@vcp@`.

Prepare the deployment plan

The vPA contains a sample deployment plan for you to copy and complete. The sample deployment plan contains sections that correspond to a default deployment, but some nodes are optional.

Before you begin

Note:
In general, do not modify or delete the `deploy_plan.conf.sample` file. However, if you plan to deploy the optional reporting server or FLR UI server nodes in the future, you must also uncomment the corresponding sections in the sample deployment plan.

Procedure

1. Log in to the vPA as the root user.
2. Change directory by typing the following command:

   ```
   cd /root/deploy_plan/
   ```

3. Make a copy of the sample deployment plan by typing the following command:

   ```
   cp deploy_plan.conf.sample deploy_plan.conf
   ```

4. Provide write access to the deployment plan by typing the following command:

   ```
   chmod a+w deploy_plan.conf
   ```

5. Using a Linux text editor, such as `vi`, open the deployment plan and provide configuration values for all required fields.

   Deployment plan parameters on page 27 provides additional information about parameter values.

6. If you want to deploy the optional reporting server or FLR UI server nodes, uncomment all lines in the `[Vcprpt]` or `[Vcpflr]` sections by removing # from the beginning of each line in the section.

   For example:

```
[Vcpflr]
ip=
fqdn=
```

The management tool does not deploy nodes that are commented out.

7. Save and close the deployment plan.

After you finish

The deployment plan contains plain-text credentials. To protect these credentials, encrypt the deployment plan.

Encrypt and decrypt the deployment plan

After you complete the deployment plan, protect the stored credentials by encrypting the deployment plan.

About this task

Two management tool parameters control encryption and decryption: `--encrypt` and `--show-pwd`.

Procedure

1. To encrypt the `deploy_plan.conf` file:
   a. Log in to the vPA as the root user.
   b. Change directory to `/root/deploy_plan/`.
   c. Type the following command:

      `vcp-management-tool --encrypt`

      The management tool prompts you for a master password to protect the deployment plan. The management tool encrypts all passwords in the deployment plan with this master password.
2. To decrypt the `deploy_plan.conf` file:
   a. Log in to the vPA as the root user.
   b. Change directory to `/root/deploy_plan/`.
   c. Type the following command:

      `vcp-management-tool --show-pwd`

      The management tool decrypts all passwords in the configuration file.

      Note: Ensure that you keep the master password secure.

Reset the password fields in the deployment plan

After you encrypt the `deploy_plan.conf` file, the passwords in the configuration file appear as encoded text. You can change the password by replacing the encoded text with the new password.

About this task

To reset the password fields, complete the following steps:

Procedure

1. Use a Linux text editor to open the `deploy_plan.conf` file, which is located in the `/root/deploy_plan/` directory.

2. In the password field that you want to change, replace the value with the new password:

   For example:

   `vct_password=`*MyNewPassword*

   where:

   MyNewPassword is the new password for the management vCenter admin role account.

3. Save and close the configuration file.

After you finish

To protect these credentials, encrypt the configuration file.

Reset the master password for the deployment plan

About this task

To reset the `deploy_plan.conf` master password, complete the following steps.

Procedure

1. Use a Linux text editor to open the `deploy_plan.conf` file, which is located in the `/root/deploy_plan/` directory.
2. Replace all encoded passwords in the `deploy_plan.conf` file by typing each password value in clear text.
3. To reset the master password, encrypt the configuration file:
   a. Type the following command:

      ```
      vcp-management-tool --encrypt
      ```

      The management tool prompts you to specify a master password to protect the `deploy_plan.conf` file.

   b. Type a password value for the master password.
4. Save and close the configuration file.

CHAPTER 4

Deployment

This chapter includes the following topics:

- About deployment 34
- Perform an all-in-one deployment 34
- Deploy a single node 35
- Install the UI plug-in on vCloud Director 36
- Deployment scenarios 36

About deployment

This chapter explains how to deploy vCD DPE nodes in your environment. Before deploying nodes, verify the configuration fields in the deployment plan.

The management tool (`vcp-management-tool`) enables you to deploy multiple VMs (all-in-one deployment) or a single VM (single-node deployment) based on the requirements of your backup environment.

An all-in-one deployment provides a simple and integrated way to deploy all vCD DPE nodes.

A single-node deployment provides a flexible method to deploy one node in scenarios such as:

- Scaling-out a cell.
- Scaling-out a backup gateway.
- Redeploying a VM after a failure.

Perform an all-in-one deployment

All-in-one deployment enables you to deploy all vCD DPE nodes together.

Before you begin

The management tool deploys the RabbitMQ and PostgreSQL servers on the same VM. Ensure that the deployment plan contains the same IP address and fully qualified domain name for the RabbitMQ and PostgreSQL servers.

About this task

By default, the all-in-one deployment process targets installation of the following vCD DPE nodes:

- Cell
- Backup gateway
- Utility node (RabbitMQ and PostgreSQL)
- UI server

The reporting server and FLR UI server nodes are optional. If you do not want to deploy either of these nodes, Prepare the deployment plan on page 30 provides more information.

The management tool deploys the VMs sequentially. If deployment of a single VM fails, the entire deployment process terminates. In this case, to re-deploy the VMs, delete all deployed vCD DPE VMs in the vCenter.

Procedure

1. Log in to the vPA as the root user.
2. To start the deployment process, type the following command:

   ```
   vcp-management-tool --deploy
   ```

   The management tool encrypts the configuration file to protect your credentials. When you run the management tool for the first time, set a master password. This password is required for performing other operations, such as upgrading the software.

   After deploying each VM, the management tool displays the path to the deployment log file.
3. Configure the AMQP settings for the RabbitMQ server in the vCloud Director UI:

   a. In the vCloud Director UI, browse to **System** > **Administration** > **System Settings** > **Extensibility**.

b. Configure the AMQP settings.

To use an existing AMQP configuration, see Deploy nodes with an existing RabbitMQ (AMQP) configuration on page 36.

4. Restart the services:

   a. Log in to the cell node as the root user.

   b. Type the following commands:

```
systemctl stop vcpsrv
systemctl start vcpsrv
```

   c. Log in to the UI server node as the root user.

   d. Type the following commands:

```
systemctl stop vcpui
systemctl start vcpui
```

Results

The deployment process creates a folder with the name `truststore` within the `/root/deploy_plan` directory. Do not delete this folder or any files within this folder.

The all-in-one deployment method automatically installs the vCD DPE UI plug-in on vCloud Director.

Deploy a single node

Perform these steps to deploy a single node from the deployment plan. For example, when you need to scale-out a cell or backup gateway, or when you need to re-deploy a node because of a failure.

Before you begin

Complete the following prerequisites:

- Deploy the utility node (RabbitMQ and PostgreSQL) first.
- Fully configure the node, including the fully qualified domain name, in the deployment plan.

Procedure

1. Log in to the vPA as the root user.
2. To start the deployment process, type the following command:

```
vcp-management-tool --deploy --vm=host.mydomain.com
```

   where *host.mydomain.com* is the fully qualified domain name of the node to deploy.

   After deploying the node, the management tool displays the path to the deployment log file.

   Note: The management tool encrypts the deployment plan to protect your credentials. When you run the management tool for the first time, set a master password. This password is required for performing other operations, such as upgrading the software.

Results

The deployment process creates a folder with the name `truststore` within the `/root/deploy_plan` directory. Do not delete this folder or any files within this folder.

After you finish

For single-node deployment, the management tool does not automatically install the vCD DPE UI plug-in. To manually install the UI plug-in, see Install the UI plug-in on vCloud Director on page 36.

Install the UI plug-in on vCloud Director

The vCD DPE UI plug-in helps you manage data protection from the vCloud Director web page. Use the following steps to install the UI plug-in if you deployed the vCD DPE nodes by using the single-node deployment method.

About this task

Note: The all-in-one deployment method automatically installs the UI plug-in.

Procedure

1. Log in to the vPA as the root user.
2. Install the UI plug-in by typing the following command:

   ```
   vcp-management-tool --deploy --vcdui-plugin
   ```

Results

After installation completes, **Data Protection** appears as an additional item in the vCloud Director navigation panel.

The installation process creates a log file on the vPA in `/root/deploy_plan/log/`.

Deployment scenarios

Consider the following scenarios when deploying nodes in your environment.

Deploy nodes with an existing RabbitMQ (AMQP) configuration

vCloud Director supports various extensions. The presence of another extension means that there is an existing RabbitMQ instance. In this case, deploy the vCD DPE and then change the deployment plan to reference the existing RabbitMQ configuration.

Before you begin

- Ensure that the deployment plan contains the same IP address and fully qualified domain name for new RabbitMQ and PostgreSQL servers.
- Ensure that SSL certificates are installed for your existing RabbitMQ instance.

About this task

The all-in-one deployment installs a new instance of RabbitMQ, but the remainder of this task reconfigures the vCD DPE to use the existing RabbitMQ configuration.

Although the all-in-one deployment installs RabbitMQ on the utility node, you cannot use this node for RabbitMQ. Only use the utility node for PostgreSQL.

Procedure

1. Perform an all-in-one deployment to deploy all nodes.

   The management tool deploys new RabbitMQ and PostgreSQL servers on the same VM.
2. Log in to the vPA as the root user.

3. Change directory by typing the following command:

   cd /root/deploy_plan

4. Using a Linux text editor, such as `vi`, open `deploy_plan.conf`.
5. In the **Rabbitmq** section, edit the following fields to reflect the settings for the existing RabbitMQ instance:

Field	Description
ip[a]	Specifies the IP address of the RabbitMQ instance.
fqdn[a]	Specifies the fully qualified domain name of the RabbitMQ instance.
user	Specifies the username of the RabbitMQ instance.
mq_password	Specifies the password of the RabbitMQ instance.
vm_user	Specifies the username of the VM that hosts the RabbitMQ instance.
vm_password	Specifies the password of the VM that hosts the RabbitMQ instance.

   a. Supply the IP address and fully qualified domain name of the VM that hosts the RabbitMQ server, not those of the load balancer.

   For example:

```
[Rabbitmq]
ip=1.2.3.4
fqdn=vcdrabbitmq1.vcd.example.com
user=vcdmq
mq_password=P@ssw0rd1
vm_user=root
vm_password=P@ssw0rd2
```

6. Save and close the deployment plan.
7. Upgrade all nodes by typing the following command:

   vcp-management-tool --upgrade

   You must upgrade the nodes to establish the RabbitMQ SSL certificate.

Scale out the cell or backup gateway

Depending on the environment, you might be required to deploy more than one cell or backup gateway. Use the single-node deployment method to fulfill this requirement.

Scale out the cell

Perform these steps to configure and deploy an additional cell.

Procedure

1. Log in to the vPA as the root user.
2. Change directory by typing the following command:

   cd /root/deploy_plan

3. Using a Linux text editor, such as `vi`, open `deploy_plan.conf`.
4. Locate the `Vcpcell-1` section.

5. Create a section for the new cell.
6. In the following fields, provide configuration values for the new cell:

Field	Description
ip	Specifies the IP address of the cell.
fqdn	Specifies the fully qualified domain name of the cell.
db_name	Specifies the database name for the cell.
db_user	Specifies the database user account for the cell.
db_password	Specifies the database user account password for the cell.

For example:

```
[Vcpcell-1]
ip=1.2.3.4
fqdn=vcpcell1.vcd.example.com
db_name=vcpsrv
db_user=vcpsrv
db_password=P@ssw0rd

[Vcpcell-2]
ip=1.2.3.5
fqdn=vcpcell2.vcd.example.com
db_name=vcpsrv
db_user=vcpsrv
db_password=P@ssw0rd
```

Note:
The `db_user` and `db_password` fields are optional. Specify these values if you manage PostgreSQL and have your own credentials. This occurs when you upgrade from a version of vCD DPE earlier than 18.2, where you deployed your own instance of PostgreSQL.

Ensure that the database credentials (`db_name`, `db_user`, `db_password`) are the same credentials that were configured for `Vcpcell-1`.

7. Save and close the deployment plan.
8. To deploy the new cell, type the following command:

   `vcp-management-tool --deploy --vm=`*`vcpcell2.vcd.example.com`*

   where *vcpcell2.vcd.example.com* is the fully qualified domain name of the cell that you configured as `Vcpcell-2`.

Scale out the backup gateway

Perform these steps to configure and deploy an additional backup gateway.

Procedure

1. Log in to the vPA as the root user.
2. Change directory by typing the following command:

   `cd /root/deploy_plan`

3. Using a Linux text editor, such as `vi`, open `deploy_plan.conf`.
4. Locate the `Vcpbg-1` section.
5. Create a section for the new backup gateway.

6. In the following fields, provide configuration values for the backup gateway:

Field	Description
ip	Specifies the IP address of the backup gateway.
fqdn	Specifies the fully qualified domain name of the backup gateway.
ave_addr	Specifies the IP address of the Avamar server.
ave_user	Specifies the administrative user account on the Avamar server.
ave_password	Specifies the password for the administrative user account on the Avamar server.

For example:

```
[Vcpbg-1]
ip=1.2.3.4
fqdn=backupgateway1.vcd.example.com
ave_addr=ave1.vcd.example.com
ave_user=MCUser
ave_password=P@ssw0rd

[Vcpbg-2]
ip=1.2.3.5
fqdn=backupgateway2.vcd.example.com
ave_addr=ave2.vcd.example.com
ave_user=MCUser
ave_password=P@ssw0rd2
```

Note: Ensure that the Avamar server information is different for each backup gateway.

7. Save and close the deployment plan.
8. To deploy the new backup gateway, type the following command:

   `vcp-management-tool --deploy --vm=`*`backupgateway2.vcd.example.com`*

   where *backupgateway2.vcd.example.com* is the fully qualified domain name of the backup gateway that you configured as `Vcpbg-2`.

Deploy the UI server and FLR UI server with a user-provided certificate

To increase security and prevent browser warnings, you can use your own certificate to deploy the UI server or FLR UI server web service. Before deployment, import the private key into a truststore.

Before you begin

- Create a truststore in the `/root/deploy_plan/truststore` directory. Create this directory if it does not exist.

  The truststore name must be in the format *`fqdn`*`.truststore` with alias name `tomcat`.

  where *fqdn* is the fully qualified domain name of the UI server or FLR UI server.

  For example: `xyz.mydomain.com.truststore`
- Ensure that the password for *`fqdn`*`.truststore` matches the password value for `truststore_password` in the deployment plan.
- The steps in this procedure are for new deployments. If you need to update the certificates for an existing UI server or FLR UI server, complete the following tasks:

  1. Remove the truststore for the UI server or FLR UI server.

2. To recreate the truststore, perform steps 1-4 in the following procedure.
3. Perform an all-in-one upgrade.

   Perform an all-in-one upgrade on page 45 provides more information.

Procedure

1. If the private key is encrypted, complete the following substeps:
   a. Log in to the vPA as the root user.
   b. Change directory by typing the following command:

      ```
      cd /root/deploy_plan/truststore
      ```

   c. To import *privatekey.key* into the truststore, type the following command on one line:

      ```
      openssl pkcs12 -passin pass:private.key.password -passout
      pass:truststore.password -inkey privatekey.key -in publiccert.cer -
      export -out fqdn.truststore -name tomcat
      ```

      where:

      - *private.key.password* is the password of the private key.
      - *truststore.password* is the password of the truststore.
      - *fqdn* is the fully qualified domain name of the UI server or FLR UI server.
      - *privatekey.key* represents the private key.
      - *publiccert.cer* represents the public certificate.

2. If the private key is not encrypted, complete the following substeps:
   a. Log in to the vPA as the root user.
   b. Change directory by typing the following command:

      ```
      cd /root/deploy_plan/truststore
      ```

   c. To import *privatekey.key* into the truststore, type the following command on one line:

      ```
      openssl pkcs12 -passout pass:truststore.password -inkey privatekey.key -
      in publiccert.cer -export -out fqdn.truststore -name tomcat
      ```

      where:

      - *truststore.password* is the password of the truststore.
      - *fqdn* is the fully qualified domain name of the UI server or FLR UI server.
      - *privatekey.key* represents the private key.
      - *publiccert.cer* represents the public certificate.

3. Verify the contents of the truststore by using the `keytool` utility:

   ```
   keytool -list -v -keystore fqdn.truststore -alias tomcat -storepass
   truststore.password
   ```

   where:

   - *truststore.password* is the password of the truststore.
   - *fqdn* is the fully qualified domain name of theUI server.

4. Ensure that the private key and certificate information is correct.
5. Perform an all-in-one deployment.

Perform an all-in-one deployment on page 34 provides more information.

CHAPTER 5

Upgrade

This chapter includes the following topics:

- Introduction 44
- Prepare for upgrade 44
- Upgrade the vPA 44
- Perform an all-in-one upgrade 45
- Upgrade using the existing PostgreSQL database and RabbitMQ server 46
- Migrate the existing PostgreSQL databases to the utility node 47
- Perform an upgrade on a single node 51
- Verify completion of the upgrade 51
- Log in to the vCD DPE 54

Introduction

This chapter describes how to upgrade the vCD DPE.

Before starting the upgrade, back up the vCD DPE PostgreSQL database. Dell EMC also recommends that you back up the individual vCD DPE VMs, or take vSphere snapshots, so that you can roll them back in the event of an error.

Note: Upgrades from/to specific versions may have specific detailed additional steps. This chapter defines the basic process and the minimum necessary steps.

The upgrade preserves the contents of the vCD DPE database and all objects that are defined therein.

Best practice

Reserve a portion of each day, week, or month as a maintenance window during which scheduled backups are not run. Perform the upgrade during this maintenance window.

Upgrade prerequisites

Consider the following important prerequisites before upgrading from a previous release:

- The upgrade procedure supports vCD DPE releases 18.2.0 and later.
- Ensure that you have a copy of the sample deployment plan file (`deploy_plan.conf.sample`) and a copy of the deployment plan (`deploy_plan.conf`) in `/root/deploy_plan/` on the vPA.
- Ensure that the deployment plan contains all required fields.
- Complete the `shared_secret` field in the `Credentials` section of the deployment plan.

  The `shared_secret` field represents a secret value that encrypts elements in the PostgreSQL database for cells. Ensure that the shared secret is the same as the secret that you used for the previous release.

Prepare for upgrade

From vCD DPE 19.2, the base OS is upgrade to SLES12SP4 and vCD DPE does not support OS upgrade in place. So, follow the below given steps:

1. Deploy a new vPA 19.2, refer Deploy the vPA.
2. Copy the `deploy_plan.conf` from previous vPA.
3. Back up all vCP DPE nodes, power off and rename.
4. Perform all-in-one deployment, refer Perform an all-in-one deployment.

Follow below steps to continue the upgrade process.

Upgrade the vPA

This task upgrades the vPA, including all the Puppet scripts, RPMs, and associated files and processes. The vPA drives upgrades to the other nodes.

About this task

This upgrade scenario is for hotfix releases.

For all of the following steps, *build* represents the build number that is associated with the release.

Procedure

1. Log in to the vPA as the root user.
2. Stop the Puppet master and the Apache `httpd` services by typing the following commands:

   ```
   systemctl stop puppetmaster
   systemctl stop apache2
   ```

3. Ensure that the vPA has at least 5 GB of free space available.
4. Using a secure file transfer tool such as `scp`, copy the vPA upgrade RPM (`emcvpa-build.rpm`) to the vPA.
5. Install the vPA upgrade RPM by typing the following command:

   ```
   rpm -Uvh --force emcvpa-build.rpm
   ```

   This step might install new Puppet files.

6. If you chose to deploy the reporting server or FLR UI server, complete the following substeps:
   a. Using a Linux text editor, such as `vi`, open the deployment plan.
   b. Uncomment all lines in the `[Vcprpt]` or `[Vcpflr]` sections by removing # from the beginning of each line in the section.

      For example:

      ```
      [Vcpflr]
      ip=
      fqdn=
      ```

      The management tool does not upgrade nodes that are commented out.

   c. Save and close the deployment plan.
   d. Using a Linux text editor, such as `vi`, open the sample deployment plan.
   e. Uncomment the same lines in the `[Vcprpt]` or `[Vcpflr]` sections that you uncommented in the deployment plan by removing # from the beginning of each line in the section.

      For example:

      ```
      [Vcpflr]
      ip=
      fqdn=
      ```

   f. Save and close the sample deployment plan.
7. Start the Puppet master and the Apache `httpd` services by typing the following commands:

   ```
   systemctl start apache2
   systemctl start puppetmaster
   ```

Perform an all-in-one upgrade

Perform this task to upgrade all vCD DPE nodes together (cells, backup gateway, utility node, UI server, reporting server, and FLR UI server). The management tool upgrades each node in turn.

Before you begin

- Complete all upgrade prerequisites.

- The reporting server and FLR UI server nodes are optional. The deployment plan may not contain these nodes. Prepare the deployment plan on page 30 provides more information.

Procedure

1. Log in to the vPA as the root user.
2. Launch the management tool to deploy the nodes by typing the following command:

   ```
   vcp-management-tool --deploy
   ```

   When prompted, type the master password that you set during deployment.
3. Choose one of the following upgrade paths:
   - To use the existing (separate) PostgreSQL database server and RabbitMQ server, complete the steps in Upgrade using the existing PostgreSQL database and RabbitMQ server on page 46.
   - To use the PostgreSQL server and RabbitMQ service on the utility node, complete the tasks in Migrate the existing PostgreSQL databases to the utility node on page 47.

Upgrade using the existing PostgreSQL database and RabbitMQ server

This task contains preparatory steps for PostgreSQL 9.4. The initial steps upgrade the cipher configuration of the existing database, while subsequent steps configure the deployment plan.

Procedure

1. Establish an SSH connection to the existing PostgreSQL database server.
2. Change user by typing the following command:

   ```
   su - postgres
   ```
3. Change directory by typing the following command:

   ```
   cd $PGDATA
   ```
4. Using a Linux text editor, such as `vi`, open `postgresql.conf`.
5. Change the `ssl_ciphers` value to `'RSA:MEDIUM:-DH:!aNULL'`.
6. Save and close `postgresql.conf`.
7. Restart PostgreSQL by typing the following command:

   ```
   service postgresql restart
   ```
8. Establish an SSH connection to the vPA.
9. Update the deployment plan configuration fields for PostgreSQL and RabbitMQ.

Table 11 Deployment plan parameters

Section	Parameter	Description
`Postgresql`	`ip`	Required. The IP address and FQDN for the PostgreSQL server.
	`fqdn`	
	`user`	Required. The user account for PostgreSQL database.

Table 11 Deployment plan parameters (continued)

Section	Parameter	Description
	db_password	Required. The password for the PostgreSQL database user account.
	vm_user	The user account and password for the VM that hosts the PostgreSQL server.
	vm_password	
Rabbitmq	ip	Required. The IP address and FQDN for the RabbitMQ server.
	fqdn	
	user	Required. The user account for the RabbitMQ service.
	mq_password	Required. The password for the RabbitMQ service.
	vm_user	The user account and password for the VM that hosts the RabbitMQ service.
	vm_password	
Vcpcell-*x*[a]	db_name	Required. The database name for the PostgreSQL cell database.
	db_user	The database user account for the PostgreSQL cell database.
	db_password	The database user password for the PostgreSQL cell database.
Vcprpt[b]	db_name	Required. The database name for the PostgreSQL reporting server database.
	db_user	The database user account for the PostgreSQL reporting server database.
	db_password	The database user password of the PostgreSQL reporting server database.

a. *x* is a placeholder that represents the component number (for example, *Vcpcell-1* or *Vcpbg-1*).
b. This node is optional.

10. Launch the management tool to push the updated configuration by typing the following command:

    ```
    vcp-management-tool --upgrade
    ```

    When prompted, type the master password that you set during deployment.

Migrate the existing PostgreSQL databases to the utility node

This section contains steps for PostgreSQL 9.4. For other versions of PostgreSQL, refer to the PostgreSQL documentation for that version.

The utility node runs the SLES 12 SP4 operating system and PostgreSQL 9.6.

Dump the existing PostgreSQL databases

This task exports the existing data from the PostgreSQL server.

Procedure

1. Establish an SSH connection to the existing PostgreSQL database server.
2. Change user by typing the following command:

   ```
   su - postgres
   ```

3. Connect to the PostgreSQL database by typing the following command:

   ```
   psql
   ```

4. List the PostgreSQL databases by typing the following command:

   ```
   \list
   ```

   Note the name of the vCD DPE cell and reporting server databases. The reporting server is optional.
5. Close the connection to the PostgreSQL database by typing the following command:

   ```
   \q
   ```

6. Dump the vCD DPE cell database by typing the following command:

   ```
   pg_dump --no-owner CellDBName > vcdsrv.sql
   ```

   where *CellDBName* is the cell database name that you noted.

   Repeat this step for each cell database that you noted, using a different output filename.
7. If deployed, dump the vCD DPE reporting server database by typing the following command:

   ```
   pg_dump --no-owner RptDBName > vcdrpt.sql
   ```

   where *RptDBName* is the reporting server database name that you noted.
8. Copy the dump files locally for later import to the utility node.

Prepare the utility node

This task removes the existing databases that were created as part of the vCD DPE 19.2 utility node deployment.

Procedure

1. Stop the vCD DPE services by repeating the following substeps for each cell:
   a. Open an SSH connection to the cell node.
   b. Stop the vCD DPE service for that node by typing the following command:

      ```
      systemctl stop vcpsrv
      ```

2. If deployed, stop the reporting server service:
   a. Open an SSH connection to the reporting server node.
   b. Stop the reporting server service by typing the following command:

      ```
      systemctl stop vcprpt
      ```

3. Open an SSH connection to the utility node.

4. Transfer the dump files from the previous task to the `/root` directory on the utility node.
5. Transfer the cell dump file to the PostgreSQL directory by typing the following command:

   ```
   cp vcdsrv.sql $PGDATA
   ```

6. If deployed, transfer the reporting server dump file to the PostgreSQL directory by typing the following command:

   ```
   cp vcdrpt.sql $PGDATA
   ```

7. Change user by typing the following command:

   ```
   su - postgres
   ```

8. Connect to the PostgreSQL database by typing the following command:

   ```
   psql
   ```

9. List the newly-deployed PostgreSQL databases by typing the following command:

   ```
   \list
   ```

   Note the name of the new vCD DPE cell and reporting server databases. The reporting server is optional.

10. Check for connections to the PostgreSQL cell database by typing the following commands, each on one line:

    ```
    revoke CONNECT ON DATABASE CellDBName FROM PUBLIC ;
    select pid, pg_terminate_backend(pid) from pg_stat_activity where
    datname='CellDBName' and pid <> pg_backend_pid();
    ```

    where *CellDBName* is the cell database name that you noted.

    If the SQL output is not empty, open connections to the database still exist. Ensure that you have stopped all of the vCD DPE services and then repeat this step.

    Repeat this step for each PostgreSQL cell database that you noted.

11. If deployed, check for connections to the PostgreSQL reporting server database by typing the following commands, each on one line:

    ```
    revoke CONNECT ON DATABASE RptDBName FROM PUBLIC ;
    select pid, pg_terminate_backend(pid) from pg_stat_activity where
    datname='RptDBName' and pid <> pg_backend_pid();
    ```

    where *RptDBName* is the reporting server database name that you noted.

    If the SQL output is not empty, open connections to the database still exist. Ensure that you have stopped the reporting server service and then repeat this step.

12. Drop the new PostgreSQL cell database by typing the following command:

    ```
    drop database CellDBName;
    ```

    where *CellDBName* is the cell database name that you noted.

    Repeat this step for each PostgreSQL cell database that you noted.

13. If deployed, drop the new PostgreSQL reporting server database by typing the following command:

    ```
    drop database RptDBName;
    ```

where *RptDBName* is the reporting server database name that you noted.

Import the existing PostgreSQL databases

This task imports the dumped PostgreSQL databases into new databases on the vCD DPE 19.2 utility node.

Procedure

1. Create a PostgreSQL cell database by typing the following command:

   ```
   create database CellDBName owner PostgreSQLUser;
   ```

   where:

   - *CellDBName* is the cell database name that you noted and that corresponds to the value that you supplied in the deployment plan.
   - *PostgreSQLUser* is the PostgreSQL cell user account that you supplied in the deployment plan.

   Repeat this step for each PostgreSQL cell database that you noted.

2. If deployed, create a PostgreSQL reporting server database by typing the following command:

   ```
   create database RptDBName owner PostgreSQLUser;
   ```

   where:

   - *RptDBName* is the reporting server database name that you noted.
   - *PostgreSQLUser* is the PostgreSQL reporting server user account that you supplied in the deployment plan.

3. Close the connection to the PostgreSQL database by typing the following command:

   ```
   \q
   ```

4. Import the dumped PostgreSQL cell database by typing the following command:

   ```
   psql -d CellDBName -f vcdsrv.sql
   ```

   where *CellDBName* is the cell database name that you noted and that corresponds to the value that you supplied in the deployment plan.

   Repeat this step for each PostgreSQL cell database that you dumped and substitute the dump filename accordingly.

5. If deployed, import the dumped PostgreSQL reporting server database by typing the following command:

   ```
   psql -d RptDBName -f vcdrpt.sql
   ```

   where *RptDBName* is the reporting server database name that you noted.

6. Start the vCD DPE services by repeating the following substeps for each cell:

   a. Open an SSH connection to the cell node.

   b. Start the vCD DPE service for that node by typing the following command:

   ```
   systemctl start vcpsrv
   ```

7. If deployed, start the reporting server service:

   a. Open an SSH connection to the reporting server node.

b. Start the reporting server service by typing the following command:

```
systemctl start vcprpt
```

Perform an upgrade on a single node

Perform this task to upgrade a single node that you have configured in the deployment plan. For example, when you need to upgrade nodes one at a time, or when you need to upgrade a single node because of a failure condition.

Before you begin

Upgrade the utility node before you upgrade any other nodes.

> **Note:**
> If you specify the utility node and the management tool deployed RabbitMQ and PostgreSQL on the same VM, the management tool upgrades the utility node. Otherwise, if you specify the utility node, the management tool returns an error and does not upgrade the utility node.

Procedure

1. Log in to the vPA as the root user.
2. Change directory by typing the following command:

   ```
   cd /root/deploy_plan
   ```

3. Launch the management tool by typing the following command:

   ```
   vcp-management-tool --upgrade --vm=host.mydomain.com
   ```

   where *host.mydomain.com* is the fully qualified domain name of the node to upgrade. The node must be configured in the deployment plan.

   When prompted, type the master password that you set during deployment.

Verify completion of the upgrade

Verification of a successful upgrade ensures that the vCD DPE software was installed on the backup gateway, the cell, the reporting server, the UI server, and the FLR UI server. Verification also ensures that the services are running.

Verify the backup gateway upgrade

On the backup gateway node, verify the successful installation of the vCD DPE backup gateway and Avamar software, that the backup gateway service is running, and that the backup gateway can connect to Avamar.

Procedure

1. Establish an SSH connection to the backup gateway node.
2. Verify the presence of the backup gateway software by typing the following command:

   ```
   rpm -qa | grep vcp
   ```

   The console displays output similar to the following:

   ```
   vcp-backup-gateway-build
   ```

   where *build* represents the current release.

3. Verify the presence of the Avamar software by typing the following command:

   ```
   rpm -qa | grep Avamar
   ```

The console displays output similar to the following:

```
AvamarVMwareCombined-vApp-build
```

where *build* represents the current release.

4. Verify that the `vcpbg` service has started by typing the following command:

   `systemctl status vcpbg`

   The console displays output similar to the following:

   ```
   vcpbg.service - vcp backup gateway service
      Loaded: loaded (/usr/lib/systemd/system/vcpbg.service; enabled; vendor
   preset: disabled)
      Active: active (running)
   ```

5. Review the log file at `/var/log/vcp/vcpbg.log` and verify that the log does not contain any failure messages.
6. Check the log file for indications of a successful connection.

   If the backup gateway can establish a connection with Avamar, the log file contains the following message:

   ```
   Open connection: 1 connections
   ```

Verify the cell upgrade

On the cell, verify the successful installation of the vCD DPE software, and that the service is running.

Procedure

1. Establish an SSH connection to the cell.
2. Verify the presence of the cell software by typing the following command:

   `rpm -qa | grep vcp`

   The console displays output similar to the following:

   ```
   vcp-server-build
   ```

   where *build* represents the current release.

3. Verify that the `vcpsrv` service has started by typing the following command:

   `systemctl status vcpsrv`

   The console displays output similar to the following:

   ```
   vcpsrv.service - vcp service
      Loaded: loaded (/usr/lib/systemd/system/vcpsrv.service; enabled;
   vendor preset: disabled)
      Active: active (running)
   ```

4. Review the log file at `/var/log/vcp/vcpserver.log` and verify that the log does not contain any failure messages.

Verify the reporting server upgrade

On the reporting server node, verify the successful installation of the reporting server software, and that the service is running.

Procedure

1. Establish an SSH connection to the reporting server node.
2. Verify the presence of the reporting server software by typing the following command:

   `rpm -qa | grep vcp`

The console displays output similar to the following:

```
vcprpt-build
```

where *build* represents the current release.

3. Verify that the `vcprpt` service has started by typing the following command:

   `systemctl status vcprpt`

   The console displays output similar to the following:

```
vcprpt.service - vcp report service
   Loaded: loaded (/usr/lib/systemd/system/vcprpt.service; enabled;
vendor preset: disabled)
   Active: active (running)
```

4. Review the log file at `/var/log/vcp/vcpreporting.log` and verify that the log does not contain any failure messages.

Verify the UI server upgrade

On the UI server node, verify the successful installation of the UI server software, and that the service is running.

Procedure

1. Establish an SSH connection to the UI server node.
2. Verify the presence of the UI server software by typing the following command:

   `rpm –qa | grep vcp`

   The console displays output similar to the following:

```
vcp-ui-server-build
```

   where *build* represents the current release.

3. Verify that the `vcpsrv` service has started by typing the following command:

   `systemctl status vcpui`

   The console displays output similar to the following:

```
vcpui.service - vcp ui service
   Loaded: loaded (/usr/lib/systemd/system/vcpui.service; enabled; vendor
preset: disabled)
   Active: active (running)
```

4. Review the log file at `/var/log/vcp/vcpui.log` and verify that the log does not contain any failure messages.

Verify the FLR UI server upgrade

On the FLR UI server node, verify the successful installation of the FLR UI server software, and that the service is running.

Procedure

1. Establish an SSH connection to the FLR UI server node.
2. Verify the presence of the FLR UI server software by typing the following command:

   `rpm –qa | grep vcp`

   The console displays output similar to the following:

```
vcp-flr-ui-server-build
```

   where *build* represents the current release.

3. Verify that the `vcpsrv` service has started by typing the following command:

   `systemctl status flrui`

   The console displays output similar to the following:

   ```
   flrui.service - vcp file level restore ui service
      Loaded: loaded (/usr/lib/systemd/system/flrui.service; enabled; vendor
   preset: disabled)
      Active: active (running)
   ```

4. Review the log file at `/var/log/vcp/flrui.log` and verify that the log does not contain any failure messages.

Log in to the vCD DPE

About this task

After you verify completion of the upgrade, log in to the UI server and continue using the vCD DPE as described in the *vCloud Director Data Protection Extension Administration and User Guide*.

Procedure

1. Open a web browser and type the following URL:

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

   where *UI_server* is the IP address or fully qualified domain name of the UI server.

2. Log in using a system or Org administrator credential.

   Logging in as a user other than the system administrator only displays the information that is relevant for that user. For example, one Org administrator cannot see vApps from another Org.

CHAPTER 6

Troubleshooting

This chapter includes the following topics:

- Logfile locations 56
- Partial updates to the deployment plan 56
- Master password encryption and decryption errors 56
- Deployment plan validation errors 56
- Shared secret errors 57
- Property file errors 57
- Unable to obtain vCenter information from the vPA 57
- Verify that all services are running 58
- SSL certificate errors 61
- Partial updates to the bootstrap.properties file 62
- Cannot add a private key for a node 64
- Nodes do not successfully upgrade 64
- Cannot log in using plaintext authentication 64
- The vPA OVA template certificate has expired 65

Logfile locations

Logs from the management tool reside on the vPA at `/root/deploy_plan/log/` and use the naming convention *`node-FQDN.timestamp`*`.log`.

For example, `vcpcell1.vcd.example.com.2018-12-31-12_00_00.log`.

Review the logfiles for detailed error information and correct any problems with the deployment plan.

Partial updates to the deployment plan

The vCD DPE supports partial updates to the deployment plan, even after encryption.

After you encrypt the deployment plan, add additional fields as necessary. The next time that you run the management tool, the management tool checks the deployment plan, prompts for the previous master password, and then encrypts the entire deployment plan.

Master password encryption and decryption errors

The vCD DPE uses a master password to encrypt the credentials in the deployment plan. Store the master password in a secure manner.

If a deployment or upgrade fails with the message `Decrypt With MasterPassword fail`, the most likely cause is that the supplied master password was incorrect. Verify that you correctly typed the master password.

Encrypt and decrypt the deployment plan on page 31 provides more information about encryption and decryption, including how to decrypt the deployment plan to verify credentials.

Deployment plan validation errors

The management tool performs several checks on the deployment plan to verify the information inside.

The most common causes of validation errors are:

- An IP address or fully qualified domain name does not match the DNS records.
- An IP address or fully qualified domain name is already occupied by an existing VM in the vCenter.
- For new deployments, the IP address or fully qualified domain name of the RabbitMQ service must match that of the PostgreSQL service. (These services must reside on the same VM.)
- A password does not obey the general rules for passwords. Deployment plan parameters on page 27 provides more information.
- Incorrect information exists in one of the following fields:

Table 12 Common sources of validation errors

Section	Field	Required?
Credentials	`truststore_password`	Optional
	`lockbox_password`	Optional

Table 12 Common sources of validation errors (continued)

Section	Field	Required?
	`vm_password`	Required
RabbitMQ	`mq_password`	Required
PostgreSQL	`db_password`	Required

Shared secret errors

For new deployments, the management tool automatically generates a shared secret to populate the `shared_secret` field in the `Credentials` section of the deployment plan. Specifying a value for deployment is optional.

For upgrades, completion of the `shared_secret` field in the `Credentials` section of the deployment plan is mandatory.

If you receive the error `This field is mandatory`, verify that the `shared_secret` value matches the shared secret that was generated or specified during deployment.

Property file errors

The message `Cannot find property file` means that a temporary file was deleted while the management tool was active.

The most likely cause is that two instances of the management tool are active at the same time. When the management tool starts, it deletes any temporary files that may exist from the previous operation. If one management tool instance deletes the temporary files that belong to another instance, the result is property file errors.

Run only one instance of the management tool at a time, and wait for the operation to complete before starting another.

Unable to obtain vCenter information from the vPA

Some circumstances prevent the management tool from obtaining the necessary vCenter information from the vPA. One or more of the following mandatory fields in the `Advanced` section of the deployment plan may be empty:

- `vm_cluster`
- `vm_datacenter`
- `vm_datastore`
- `vm_resourcepool`
- `vm_network`
- `vm_diskmode`
- `vm_folder`

If these mandatory fields are empty, all management tool operations fail.

Perform the following corrective actions:

- Verify the vCenter credentials in the deployment plan and retry the operation.

- Manually type values in the empty fields.

Verify that all services are running

Continue troubleshooting by verifying that the vCD DPE services are running on all nodes:

Verify the UI server

If you deployed a UI server, perform the following steps.

Procedure

1. Open a web browser and type the following URL:

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

   where *UI_server* is the IP address or fully qualified domain name of the UI server.

   If the UI is running, accept the self-signed certificate.
2. Log in with the vCloud Director administrator credentials.
3. Create a backup appliance for each gateway or Avamar server that you deployed.

   The *vCloud Director Data Protection Extension Administration and User Guide* provides detailed information.

After you finish

If you encounter problems, perform the following tasks to confirm the correct operation of the other nodes, and to resolve any issues.

Verify the FLR UI server

If you deployed an FLR UI server, perform the following steps.

Procedure

1. Open a web browser and type the following URL:

   https://*FLR_UI_server*:5481/vcp-flr-ui

   where *FLR_UI_server* is the IP address or fully qualified domain name of the FLR UI server.

   If the UI is running, accept the self-signed certificate.
2. Log in by using the vCloud Director administrator credentials.

Verify the cells

The cells implement an extension to the vCloud Director REST API. If the cells are operating correctly, log in to the vCD REST API and call the vCD DPE with the `curl` utility or a REST client application.

Procedure

1. Log in to the vCD REST API and obtain an authorization token with the following command:

```
curl -k -f -c cookie.txt \
 -H "Accept: application/*+xml;version=5.5" \
 --user administrator@system:vmware \
 -X GET https://vcloud.example.com/api/login
```

The vCD REST API returns an XML object that contains all of the organizations in the vCloud instance.

2. Using the authorization token, issue a request to retrieve the `EmcBackupService` with the following command:

```
curl -k -b cookie.txt \
 -H "Accept: application/*+xml;version=5.5" \
 -X GET https://vcloud.example.com/api/admin/extension/EmcBackupService
```

The vCD REST API returns an XML object that identifies the `EmcBackupService` as enabled. For example:

```
<BackupServiceReferences>
<BackupService type="application/vnd.emc.vcp.backupService+xml"
cloudUUID="78d2734f-0f95-4f82-95b1-d00ba8a16c95" id="1234dead-5678-
beaf-0cde-34567890abcd">
<IsEnabled>true</IsEnabled>
<Link href="https://vcloud.example.com/api/admin/extension/
EmcBackupService/backupAppliances" rel="down" type="application/
vnd.emc.vcp.backupAppliance+xml" />
<Link href="https://vcloud.example.com/api/admin/extension/
EmcBackupService/orgRegistrations" rel="down" type="application/
vnd.emc.vcp.orgRegistration+xml" />
<Link href="https://vcloud.example.com/api/admin/extension/
EmcBackupService/backupPolicyTemplateCatalogs" rel="down"
type="application/vnd.emc.vcp.backupPolicyTemplateCatalog+xml" />
<Link href="https://vcloud.example.com/api/admin/extension/
EmcBackupService/backupSchedules" rel="down" type="application/
vnd.emc.vcp.backupSchedule+xml" />
<Link href="https://vcloud.example.com/api/admin/extension/
EmcBackupService/backupRetentions" rel="down" type="application/
vnd.emc.vcp.backupRetention+xml" />
<Link href="https://vcloud.example.com/api/admin/extension/
EmcBackupService/backupOptionSets" rel="down" type="application/
vnd.emc.vcp." />
<Link href="https://vcloud.example.com/api/admin/extension/
EmcBackupService/backupPolicyTemplates" rel="down" type="application/
vnd.emc.vcp.backupPolicyTemplate+xml" />
<Product>vCloud Director Data Protection Extension
         - Backup Service</Product>
<Version>build</Version>
</BackupService>
</BackupServiceReferences>
```

3. In the output from the previous command, verify that the value for *build* matches the expected value.
4. If the REST API command fails, establish an SSH connection to the cell.
5. Verify the presence of the cell software by typing the following command:

```
rpm -qa | grep vcp
```

The console displays output similar to the following:

```
vcp-server-build
```

where *build* represents the current release.

6. Verify that the `vcpsrv` service has started by typing the following command:

```
systemctl status vcpsrv
```

The console displays output similar to the following:

```
vcpsrv.service - vcp service
   Loaded: loaded (/usr/lib/systemd/system/vcpsrv.service; enabled;
```

```
vendor preset: disabled)
   Active: active (running)
```

7. If the service is not running, or the cell software is not installed, perform the following substeps:
   a. Run **`puppet agent --test`** and determine if any there are any failed tasks.
   b. Review the logfile at `/var/log/message` and verify that the log does not contain any Puppet or installation error messages.
   c. Review the logfiles at `/var/log/vcp/vcpserver.log` and `/var/log/vcp/vcpsrv.log`. Verify that the logs do not contain any failure or error messages.
8. Verify that the cell can be monitored.

   The *vCloud Director Data Protection Extension Administration and User Guide* provides more information.

Verify the backup gateway

The backup gateway has a REST API, but it is not part of vCloud Director's REST API. You can perform a basic check on a backup gateway by using a browser.

Procedure

1. Open a web browser and type the following URL:

   `https://`*`backup_gateway`*`:8443/vcp-ba-ads-ws/login`

   where *backup_gateway* is the IP address or fully qualified domain name of the backup gateway.

2. Log in with the Avamar credentials from the gateway properties file.

   The UI lists the Avamar and backup gateway software versions, and the Avamar and Data Domain back-end storage units.
3. If the UI login fails, establish an SSH connection to the backup gateway.
4. Verify the presence of the backup gateway software by typing the following command:

   `rpm -qa | grep vcp`

   The console displays output similar to the following:

   ```
   vcp-backup-gateway-build
   ```

   where *build* represents the current release.
5. Verify that the `vcpbg` service has started by typing the following command:

   `systemctl status vcpbg`

   The console displays output similar to the following:

   ```
   vcpbg.service - vcp backup gateway service
      Loaded: loaded (/usr/lib/systemd/system/vcpbg.service; enabled; vendor
   preset: disabled)
      Active: active (running)
   ```
6. If the service is not running, or the backup gateway software is not installed, perform the following substeps:
   a. Run **`puppet agent --test`** and determine if any there are any failed tasks.
   b. Review the logfile at `/var/log/message` and verify that the log does not contain any Puppet or installation error messages.

c. Review the logfiles at `/var/log/vcp/vcpbg.log` and `/var/log/vcp/vcpbg-plugin.log`. Verify that the logs do not contain any failure or error messages.

7. Verify that the cell can be monitored.

   The *vCloud Director Data Protection Extension Administration and User Guide* provides more information.

Verify the reporting server

Procedure

1. Establish an SSH connection to the reporting server.
2. Verify the presence of the reporting server software by typing the following command:

   `rpm -qa | grep vcp`

   The console displays output similar to the following:

   ```
   vcprpt-build
   ```

   where *build* represents the current release.
3. Verify that the `vcprpt` service has started by typing the following command:

   `systemctl status vcprpt`

   The console displays output similar to the following:

   ```
   vcprpt.service - vcp report service
      Loaded: loaded (/usr/lib/systemd/system/vcprpt.service; enabled;
   vendor preset: disabled)
      Active: active (running)
   ```
4. If the service is not running, or the reporting server software is not installed, perform the following substeps:

   a. Run **`puppet agent --test`** and determine if any there are any failed tasks.

   b. Review the logfile at `/var/log/message` and verify that the log does not contain any Puppet or installation error messages.

   c. Review the log file at `/var/log/vcp/vcpreporting.log` and verify that the log does not contain any failure messages.

SSL certificate errors

If the error `peer not authenticated` appears in the logs, then the server's public certificate cannot be authenticated.

About this task

For example:

`GET https://`*`vcp.example.com`*`:8443/vcp-ba-ads-ws/BackupServer`

The command returns output similar to the following:

```
Jun 20 22:20:03 vcp.example.com 2014-06-20 22:20:03,864 ERROR [service-
worker-3] ( com.emc.vcp.ads.client.RestTemplateFactory: 228) - SSL Error:
org.springframework.web.client.ResourceAccessException: I/O error: peer not
authenticated; nested exception is javax.net.ssl.SSLPeerUnverifiedException:
peer not authenticated
Jun 20 22:20:03 vcp.example.com 2014-06-20 22:20:03,865 ERROR [service-
worker-3] ( com.emc.vcp.service.appliance.ApplianceAdmService: 196) - Create
Backup Appliance
Jun 20 22:20:03 vcp.example.com
```

```
com.emc.vcp.service.exceptions.AdsClientException: 01105: SSL Error - peer not authenticated
```

Procedure

1. Verify that the client's truststore contains a copy of the server's public certificate.
2. Verify that the CN field in the certificate matches the fully qualified domain name of the server.

Partial updates to the bootstrap.properties file

Nodes such as the backup gateway, the cell, and the reporting server use the `/etc/vcp/bootstrap.properties` file for initial configuration. Normally, the deployment generates a `bootstrap.properties` file with all of the required information and you do not need to edit the file.

On startup, the service reads the contents of `bootstrap.properties` and stores them in a secure file that is called a lockbox. The service erases the original contents of `bootstrap.properties` because the file might contain security-sensitive information, such as usernames and passwords.

To modify the contents of the lockbox after initial deployment, for example, if you made a mistake or changed a password, it is not necessary to re-create the entire contents of `bootstrap.properties`. You can create a subset of the full file that contains only the updated information. When the service restarts, it reads the partial data and overwrites or adds to the lockbox contents. The original contents of `bootstrap.properties` are again erased for security reasons.

Composing a partial bootstrap.properties file

There are three types of entries in the `bootstrap.properties` file:

1. Directives such as `cst.*` entries, `component.keys`, and `hide.keys`. These directives affect the operation of `bootstrap.properties` for lockbox processing.
2. Credential keys that are referenced by the `component.keys` directive.

   These keys are always in three parts:

   - `.username`
   - `.password`
   - `.url`
3. Independent keys, which are not part of `component.keys`, but may be referenced by the `hide.keys` directive.

`cst.*` directives

There are several keys that start with `cst.` that control the lockbox itself. These keys are:

```
cst.overWrite  #set to true to trigger update of lockbox.
cst.pw         #the current password of the lockbox.
cst.changePw   #the new password for the lockbox.
cst.resetLb    #reset the lockbox if the VM configuration changes w.r.to CPU,
memory
```

Generally, only `cst.overWrite` is required. To have the service read and process the contents of `bootstrap.properties`, and update the lockbox, you must add the following directive to the partial `bootstrap.properties`:

```
cst.overWrite=true
```

`component.keys` directive

The `component.keys` directive indicates which keys are part of a credential and should be processed as such. These keys are always removed from `bootstrap.properties` for security reasons.

If a `component.keys` directive refers to a set of keys that do not exist in `bootstrap.properties`. These keys are erased from the lockbox when the service starts. Therefore the partial `bootstrap.properties` should only reference the credentials that are being updated.

For example, the standard `component.keys` directive for a cell is:

```
component.keys=db,vcloud,rabbitmq,avamar,trust
```

If you compose a partial `bootstrap.properties` to update only the vCloud credentials, use the following `component.keys` directive:

```
component.keys=vcloud
```

`hide.keys` directive

The `hide.keys` directive indicates which independent, non-credential keys should be removed from `bootstrap.properties` on startup of the service. If you update these independent keys and they are sensitive in nature, such as a password, ensure that `hide.keys` contains these keys.

Credentials

Any set of keys that are referenced by `component.keys` must be entered as a set of up to three keys. Any keys that are not present are erased from the lockbox when the service starts.

For example, to update the vCloud credentials you would compose a `bootstrap.properties` file that contains the following:

```
cst.overWrite=true
component.keys=vcloud
vcloud.username=administrator@system
vcloud.password=changeme
vcloud.url=https://www.mycloud.com
```

Independent keys

Some keys in `bootstrap.properties` are independent and not part of a credential set. These values may be referenced in the `hide.keys` directive, but a reference is not necessary if the keys are not sensitive in nature.

The following example `bootstrap.properties` overwrites only the independent key `SharedVcpNode256BitKey`:

```
cst.overWrite=true
hide.keys=SharedVcpNode256BitKey
SharedVcpNode256BitKey=WJG1tSLV3whtD/CxEPvZ0hu0/HFjrzTQgoai6Eb2vgM=
```

Reset the lockbox

Conditions such as the following may prevent reading of the lockbox:

- Using VMware vSphere vMotion to move a VM onto another host with different original host characteristics. For example, a different CPU type.
- Cloning a VM and changing the VM configuration. For example, changing the CPU type and memory allocation.
- Changes to the operating system values. For example, the hostname.

Workaround

Note: Resetting the lockbox requires the original passphrase.

1. Modify `bootstrap.properties` by providing the following two key/value pairs:
   - **`cst.pw=`*`ORIGINAL_PASSPHRASE`***
   - **`cst.resetLb=true`**
2. Save and close `bootstrap.properties`.
3. Restart the application.

Cannot add a private key for a node

The vCD DPE displays a message such as `addprivatekey for [fqdn] failed` during deployment or upgrade.

The most likely cause is that the value of the `truststore_password` field in the deployment plan does not match the password that is set for the truststore file in `/root/deploy_plan/truststore`.

The corrective action is to test and, if necessary, change the password on the truststore file, or correct the password in the deployment plan.

Nodes do not successfully upgrade

The most likely cause is that the Puppet versions on the vPA and the nodes do not match.

Verify the version of the Puppet master software on the vPA and the Puppet client software on each node.

To check the Puppet version on a node, establish an SSH connection to that node and type the following command:

```
puppet --version
```

A version mismatch may cause Puppet to fail to execute some tasks. This typically happens if the OS security patch rollup is installed on some nodes but not others, as the OS security patch rollup may upgrade the Puppet software.

Cannot log in using plaintext authentication

The vCD DPE error logs contain the message `Login was refused using authentication mechanism PLAIN` when you log in to a cell or the UI server.

Node type	Log location
UI server	`/var/log/vcp/vcpui.log`
Cell	`/var/log/vcp/vcpserver.log`

The most likely cause is that the RabbitMQ credentials are incorrect. Verify the credentials in the deployment plan and make any necessary changes. If you change the credentials, perform an upgrade on the cell and UI server. Perform an upgrade on a single node on page 51 provides more information.

To restart the RabbitMQ service after the upgrade, log in to each node and restart the corresponding service by typing one of the following commands:

Node type	Command
UI server	`systemctl restart vcpui`
Cell	`systemctl restart vcpsrv`

The vPA OVA template certificate has expired

If the vPA OVA template certificate has expired, you receive a certificate error during vPA deployment.

The corrective action is to deploy the vPA without the security certificate and then ignore the certificate error. The following steps provide more information:

1. Download the vPA OVA template file.
2. Use an archive utility, such as `7-Zip`, to unzip the contents of the OVA template file.

   The contents include the following files:

   - The VM disk (VMDK) file
   - The manifest file
   - The OVF virtual appliance file
   - The certificate file
3. Using the vSphere web client, deploy the OVA template from the unzipped files.

   Select only the VMDK file, the manifest file, and the OVF file. Exclude the certificate file.
4. When vSphere prompts with a certificate warning, ignore the warning and continue.

APPENDIX

RabbitMQ Server

This appendix includes the following topics:

- Generate public/private key pairs for SSL servers 68
- Installing and configuring a RabbitMQ server 71

Generate public/private key pairs for SSL servers

This task creates a private CA, and then issues and signs a set of certificates for a server and a client. These certificates can be used for the backup gateway, the UI server, the FLR UI server, RabbitMQ, PostgreSQL, or any other server that requires SSL support.

About this task

This task creates the following files:

- `cacert.pem` (the root CA certificate)
- `server/cert.pem` (the server public certificate)
- `server/key.pem` (the server private key)
- `client/cert.pem` (the client public certificate)
- `client/key.pem` (the client private key)

Procedure

1. Log in to a suitable Linux host.

   You can use the vPA, but almost any Linux system is acceptable.

2. Set up the environment by typing the following commands:

   ```
   mkdir testca
   cd testca
   mkdir certs private
   chmod 700 private
   echo 01 > serial
   touch index.txt
   ```

3. Within the new `testca` directory, create a file named `openssl.cnf`.

   Paste the following text into the file:

   ```
   [ca]
   default_ca = testca

   [testca]
   dir = .
   certificate = $dir/cacert.pem
   database = $dir/index.txt
   new_certs_dir = $dir/certs
   private_key = $dir/private/cakey.pem
   serial = $dir/serial

   default_crl_days = 7
   default_days = 365
   default_md = sha256

   policy = testca_policy
   x509_extensions = certificate_extensions

   [testca_policy]
   commonName = supplied
   stateOrProvinceName = optional
   countryName = optional
   emailAddress = optional
   organizationName = optional
   organizationalUnitName = optional
   ```

```
[certificate_extensions]
basicConstraints = CA:false

[req]
default_bits = 2048
default_keyfile = ./private/cakey.pem
default_md = sha256
prompt = yes
distinguished_name = root_ca_distinguished_name
x509_extensions = root_ca_extensions

[root_ca_distinguished_name]
commonName = hostname

[root_ca_extensions]
basicConstraints = CA:true
keyUsage = keyCertSign, cRLSign

[client_ca_extensions]
basicConstraints = CA:false
keyUsage = digitalSignature
extendedKeyUsage = 1.3.6.1.5.5.7.3.2

[server_ca_extensions]
basicConstraints = CA:false
keyUsage = keyEncipherment
extendedKeyUsage = 1.3.6.1.5.5.7.3.1
```

4. Generate a Certificate Authority (CA) certificate by typing the following command on one line:

   openssl req -x509 -config openssl.cnf -newkey rsa:2048 -days 365 -out cacert.pem -outform PEM -subj /CN=*MyTestCA*/ -nodes

   where *MyTestCA* is the name of the CA that you want to use. This value does not need to be the fully qualified domain name of a server.

   Note: You can specify more than 365 days.

5. Transform the certificate by typing the following command:

   openssl x509 -in cacert.pem -out cacert.cer -outform DER

   The files `testca/cacert.pem` and `testca/cacert.cer` now contain the root certificate, but in different formats.

6. Generate a key and certificate for the server by performing the following substeps:

   a. Create a directory for the server key and certificate by typing the following command:

      mkdir server

   b. Change directory by typing the following command:

      cd server

   c. Generate a server key by typing the following command:

      openssl genrsa -out key.pem 2048

   d. Generate a signing request by typing the following command on one line:

      openssl req -new -key key.pem -out req.pem -outform PEM -subj / CN=*FQDN*/O=*Your-Organization*/ -nodes

      where:

      - *FQDN* is the fully qualified domain name of the server for which you are generating the key and certificate.

- *Your-Organization* is the name of your organization.

e. Change directory by typing the following command:

```
cd ..
```

f. Sign the request with the CA certificate by typing the following command on one line:

```
openssl ca -config openssl.cnf -in server/req.pem -out server/cert.pem -
notext -batch -extensions server_ca_extensions
```

g. Change directory by typing the following command:

```
cd server
```

h. Generate a server certificate by typing the following command on one line:

```
openssl pkcs12 -export -out keycert.p12 -in cert.pem -inkey key.pem -
passout pass:MySecretPassword
```

7. Change directory by typing the following command:

```
cd ..
```

8. Generate a key and certificate for the client by performing the following substeps:

Note: The process for creating server and client certificates is very similar. The differences are the `keyUsage` and `extendedKeyUsage` fields in the SSL configuration file.

a. Create a directory for the client key and certificate by typing the following command:

```
mkdir client
```

b. Change directory by typing the following command:

```
cd client
```

c. Generate a client key by typing the following command:

```
openssl genrsa -out key.pem 2048
```

d. Generate a signing request by typing the following command on one line:

```
openssl req -new -key key.pem -out req.pem -outform PEM -subj /
CN=FQDN/O=Your-Organization/ -nodes
```

where:

- *FQDN* is the fully qualified domain name of the client for which you are generating the key and certificate.
- *Your-Organization* is the name of your organization.

e. Change directory by typing the following command:

```
cd ..
```

f. Sign the request with the CA certificate by typing the following command on one line:

```
openssl ca -config openssl.cnf -in client/req.pem -out client/cert.pem -
notext -batch -extensions client_ca_extensions
```

g. Change directory by typing the following command:

```
cd client
```

h. Generate a client certificate by typing the following command on one line:

```
openssl pkcs12 -export -out keycert.p12 -in cert.pem -inkey key.pem -
passout pass:MySecretPassword
```

Results

The server and client keys and certificates reside in the `server/` and `client/` directories, respectively.

Installing and configuring a RabbitMQ server

The Advanced Message Queuing Protocol (AMQP) is an open standard for message queuing that supports flexible messaging for enterprise systems. RabbitMQ is a message bus product that implements AMQP.

vCloud Director can be configured to use a RabbitMQ message broker to provide event and chargeback notifications. The message broker is also a mandatory interface mechanism for REST API extensions.

The vCD DPE requires the installation and configuration of a RabbitMQ server, with specific exchange and queue configuration settings in both vCloud Director and the RabbitMQ server.

Deploying RabbitMQ

Install the RabbitMQ server as described in the vCloud Director documentation. You do this while logged on as a system administrator, by going to **Administration** > **System Settings** > **Blocking Tasks**, and then enabling notifications.

When this setting is enabled, vCloud Director publishes notification messages on the configured RabbitMQ (AMQP) message bus. These messages are published into a single exchange that is shared by all consumers of these notifications. Each consumer must create and bind a QUEUE to the exchange. You can apply a filter between the connection between the exchange and the queue to limit this queue to only to certain classes of notifications.

vCloud Director publishes notifications on a specific exchange. vCloud Director itself does not create this exchange, it must be created as part of the setup of RabbitMQ. The default exchange name is called `systemExchange`. Configure the exchange as `type=Topic` and `Durable=true`. Refer to the RabbitMQ server documentation for instructions.

Note:
For informational purposes, there is an additional exchange that is called `vcd.notifications20`, which also receives notifications. There are two observed differences between this exchange and `systemExchange`. First, the payload of the notifications is in JSON format, rather than XML. Second, this exchange contains notifications which are generated by extensions while the `systemExchange` only appears to receive system-generated notifications.

Notifications of system events are sent to the AMQP message broker that you configured in the system AMQP settings.

Notifications are always generated in two formats:

- An XML document, which is sent to the AMQP exchange specified in the system `AmqpSettings`.
- A JSON object, which is sent to an AMQP exchange whose name has the form *prefix*`.notifications20`, where *prefix* is the value of the `AmqpPrefix` element in the system `AmqpSettings`.

During the RabbitMQ installation, note the values that you must supply when configuring the vCD DPE to work with the RabbitMQ installation:

- The fully qualified domain name of the RabbitMQ server host. For example: *amqp.example.com*.
- A username and password that are valid for authenticating with RabbitMQ.
- The port at which the broker listens for messages. The default is 5672.
- The RabbitMQ virtual host. The default is `/`. If a single RabbitMQ server supports multiple extensions, or other workloads, a virtual host can be deployed with an alternate name such as *emc.vcp.129*.

Monitor RabbitMQ

About this task

The RabbitMQ server is a critical component of the vCD DPE and the vCloud Director notification mechanism. The REST API backup extension cannot operate without a functional RabbitMQ server.

In a production environment, you should consider various high availability options, such as running a cluster, for the RabbitMQ deployment.

RabbitMQ logs abrupt TCP connection failures, timeouts, protocol version mismatches. If you are running RabbitMQ, the logfile location depends on the operating systems and installation method. Often, the log is found in the `/var/log/rabbitmq` directory.

`rabbitmqctl` is the standard integrated management and monitoring tool. Refer to the RabbitMQ documentation for details.

RabbitMQ can run an optional web browser UI based monitor. See http://www.rabbitmq.com/management.html

A RabbitMQ server can throttle message rates or suspend publication of new messages, based on memory consumption and low disk space. These aspects of the RabbitMQ server should be periodically monitored.

RabbitMQ message publication latencies greater than about 5 s are likely to cause issues with the vCloud Director REST API extension mechanism. There is a mechanism for increasing this timeout in vCloud Director, but you should investigate and correct the root cause of high latencies, rather than increasing the vCloud Director timeout setting.

Procedure

1. Generate a server status report for support purposes by typing the following command:

   ```
   rabbitmqctl report > server_report.txt
   ```

2. Display message broker status information by typing the following command:

   ```
   rabbitmqctl status
   ```

3. List vhosts to determine if RabbitMQ server is supporting multiple applications by typing the following command:

   ```
   rabbitmqctl list_vhosts
   ```

4. List queues by typing the following command:

   ```
   rabbitmqctl list_queues -p / name messages memory consumers
   ```

5. List exchanges by typing the following command:

   ```
   rabbitmqctl list_exchanges -p / name type
   ```

6. List bindings of exchanges to queues by typing the following command:

   ```
   rabbitmqctl list_bindings -p /
   ```

Install an SSL certificate on a RabbitMQ server

Procedure

1. Generate a set of server SSL certificates for the RabbitMQ server.

   Generate public/private key pairs for SSL servers on page 68 provides more information.

2. Copy the following three files to the `/tmp` directory on the RabbitMQ server:
   - `cacert.pem`
   - `cert.pem`
   - `key.pem`
3. Establish an SSH connection to the RabbitMQ server.
4. Change directory by typing the following command:

   `cd /tmp`

Publish an SSL certificate on a RabbitMQ server

If you installed the Pivotal version of RabbitMQ, it creates a group that is called `pivotal`. If you are using a different version, use the group that is associated with RabbitMQ.

Procedure

1. Create a directory for the SSL certificates by typing the following command:

   `mkdir -p /etc/rabbitmq/ssl`

2. Copy the SSL certificates and key to the new directory by typing the following command:

   `cp *.pem /etc/rabbitmq/ssl`

3. Change directory by typing the following command:

   `cd /etc/rabbitmq`

4. Change the ownership of the new folder by typing the following command:

   `chown -R rabbitmq:pivotal ssl`

5. List the contents of the RabbitMQ directory by typing the following command:

   `ls -lR`

6. Using a Linux text editor, such as `vi`, edit `rabbitmq.config`.
7. Update the path names for the SSL certificates and key.

   The contents of the file are similar to the following:

```
[
  {rabbit, [
     {ssl_listeners, [5671]},
     {ssl_options, [{cacertfile,"/etc/rabbitmq/ssl/cacert.pem"},
                    {certfile,"/etc/rabbitmq/ssl/cert.pem"},
                    {keyfile,"/etc/rabbitmq/ssl/key.pem"},
                    {verify,verify_peer},
                    {fail_if_no_peer_cert,false}]}
   ]}
].
```

   Note: The trailing `.` (period) is required.

8. Restart the RabbitMQ service by typing the following command:

```
service rabbitmq-server restart
```