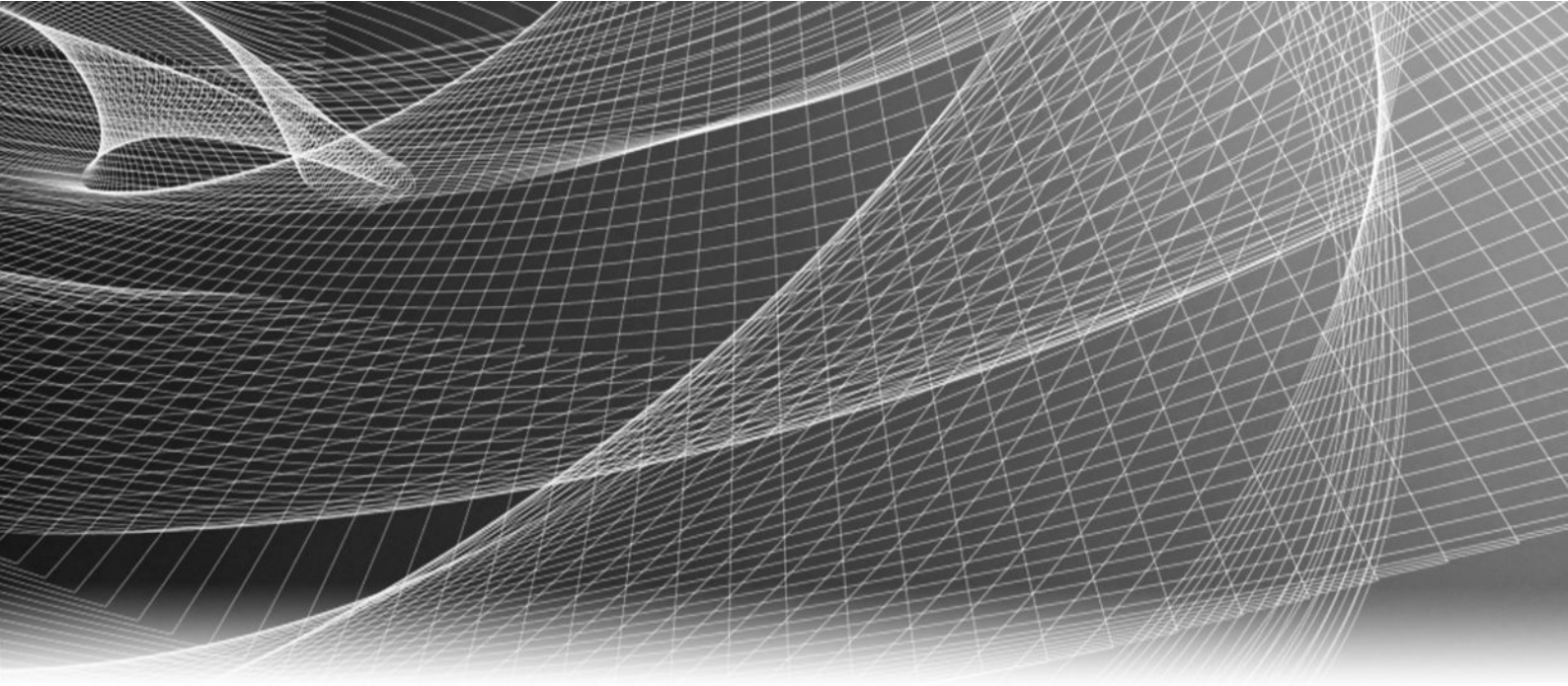

EMC® OpenStack Data Protection Extension®

Version 7.3

Installation Guide

302-003-022

REV 02

EMC²

Published June 2016

EMC 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. EMC Corporation 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 EMC software described in this publication requires an applicable software license.

For the most up-to-date regulatory document for your product line, go to EMC Online Support (https://support.emc.com).

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

CONTENTS

TABLES

PREFACE

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

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

Note

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

Purpose

This document describes how to install, configure, and use the EMC OpenStack Data Protection Extension.

Audience

This document is intended for system administrators and programmers who will be installing the EMC OpenStack Data Protection Extension and the EMC OpenStack DPE API. A high degree of knowledge regarding EMC Avamar and OpenStack administration is required.

Revision history

The following table prevents the revision history of this document.

Table 1 Revision history

Revision	Date	Description
02	September 27, 2016	Typo fix in footer.
01	June 23, 2016	First release of this document.

Related documentation

The following EMC publications available at https://support.emc.com provide additional information:

- *EMC OpenStack Data Protection Extension Release Notes*
- *EMC OpenStack Data Protection Extension REST API Getting Started Guide*

Typographical conventions

EMC uses the following type style conventions in this document:

Table 2 Style conventions

Bold	Used for names of interface elements, such as names of buttons, fields, tab 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:

Table 2 Style conventions (continued)

	• System code • System output, such as an error message or script • Pathnames, file names, 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 non-essential information that is omitted from the example

Where to get help

EMC support, product, and licensing information can be obtained as follows:

Product information

For documentation, release notes, software updates, or information about EMC products, go to EMC Online Support at https://support.emc.com.

Technical support

Go to EMC Online Support and click Service Center. Several options for contacting EMC Technical Support appear on the site. Note that to open a service request, you must have a valid support agreement. Contact your EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

Online communities

Go to EMC Community Network at https://community.emc.com for peer contacts, conversations, and content on product support and solutions. Interactively engage online with customers, partners, and certified professionals for all EMC products.

Your comments

Your suggestions help to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to DPAD.Doc.Feedback@emc.com.

CHAPTER 1

Introduction

This chapter includes the following topics:

EMC OpenStack Data Protection Extension

The EMC OpenStack Data Protection Extension (EMC OpenStack DPE) allows backup administrators to manage backup and restore operations for projects in an OpenStack cloud infrastructure. The backup administrator role is performed by an OpenStack administrator who has access rights to projects and associated instances that need to be backed up or restored. The backup administrator can manage the protection provider (currently an Avamar server), all projects that will be protected by the protection providers, and configure backup policies for scheduling backups of a particular project. The backup administrator also manages the backup proxies that are deployed in the OpenStack cloud and are used to perform backup and restore operations.

The EMC OpenStack DPE provides project administrators the ability to manage instances they want to be protected, and browse the backup inventory of a protected instance. The project administrator can then select a backup and restore it to replace the original instance, or restore it to a new location. Progress of the backup or restore operation can be monitored. Project administrators can also add instances to a backup policy created by the backup administrator for scheduled backups.

Proxy instances

Instance backups and restores require deployment of proxy instances within the OpenStack compute nodes. A EMC OpenStack DPE proxy instance is also referred to as `dpe-avamar-proxy`. Proxies run Avamar software inside a Linux instance, and are deployed using a qcow2 image file.

Once deployed, each proxy provides these capabilities:

- Backup of instances and associated volumes attached to the instances
- Restore of instances and associated volumes attached to the instances

Each proxy is capable of performing one single backup or restore operation at a time.

Proxy deployment considerations

The follow factors should be taken into account by a backup administrator when deploying proxies. The number of proxies to deploy in an OpenStack environment depends on the following:

- The number of availability zones and compute nodes in the protected OpenStack environment.
- The number of projects to be protected
- The number of instances within each project to be protected
- The size of the instances and associated volumes to be protected

Guidelines for proxy deployments

The following guidelines should be followed when deploying proxies:

- There must be at least one proxy per availability zone (for zones that have any instances that should be backed up).
- For optimal performance, as many as one proxy can be installed per nova-compute physical host. Fewer proxies are required if less performance is needed.
- Distribute proxies across physical hosts to optimize network load.

- Each proxy can backup multiple projects. However, suggested practice is to deploy one or more proxy to protect a single project.
- One proxy is capable of performing a single backup.
- One proxy can backup approximately 180GB of data per hour. Proxy performance on page 34 contains further information.
- For scaled environments, multiple proxies should be deployed to ensure that all backups are completed within the backup window of the Avamar server, as defined when creating a scheduled backup policy for a particular Project.

ZoneIDs

When a proxy is deployed and configured, the backup administrator must define a ZoneID for each proxy. The ZoneID allows a proxy to be associated to an OpenStack availability zone. OpenStack availability zones on page 34 contains more information. The following items should be considered when creating ZoneIDs with EMC OpenStack DPE:

- If the OpenStack cloud contains multiple availability zones, a proxy must be deployed for each zone.
- The backup administrator is responsible for managing the ZoneID of all deployed proxies.
- All proxies defined by a ZoneID can service all the projects and instances in the availability zone of the ZoneID.
- When an instance is added for protection, the project administrator must specify a valid ZoneID.
- An Instance can only be associated to a single ZoneID.
- The default ZoneID is named **nova**.
- The ZoneID name is case sensitive.

Examples of ZoneID usage:

- A backup admin must define a single ZoneID (for example, **nova**) and deploy all proxies with the same ZoneID. This means all instances, regardless of which project they are is in, have access to all proxies in **nova**.
- A backup admin can define a ZoneID for each OpenStack availability zone, and associate one or more proxies per ZoneID. This allows the backup administrator to group all instances in an availability zone that use a particular set of proxies.
- A backup admin can define a ZoneID for each project to be protected, and associate one or more proxies for each ZoneID. This allows the backup administrator to define a group of proxies at the project level.

Volume copies

The backup process requires temporary creation of an volume copy. These volume copies are managed by the cinder drivers of the particular storage array in which the instances and associated volumes are created. The backup performance can be greatly impacted depending on the cinder driver's feature that accelerates the process for creating a copied volume (for example, VNX Snap Copy). Drivers that do not support some form of accelerated copied volume will do a full data copy when creating the volume from a snapshot or cloning a volume, which is time-consuming, especially for large volumes.

Cinder drivers on page 34 contains more information.

Architecture and system requirements

This section details the components of the EMC OpenStack DPE product and system requirements.

Components of the EMC OpenStack DPE product

The following table lists the components of the EMC OpenStack DPE product.

Table 3 Components of the EMC OpenStack DPE product

Component	Description	Publisher
Avamar server	Also referred to as the Protection Provider.	EMC
Data Domain	Provides scalable storage for backups, with features including source data deduplication.	EMC
EMC OpenStack DPE API	Management API for EMC OpenStack DPE, provided as a qcow2 image. Includes the API reference documentation via the Swagger UI.	EMC
EMC OpenStack DPE proxy (`dpe-avamar-proxy`)	An Avamar proxy or worker, provided as a qcow2 image and registered to the Avamar server.	EMC
EMC OpenStack DPE service (`dpe-proxy-service`)	Integrates with OpenStack controller nodes for Keystone authentication and logging. Provided as an RPM package for RHEL distributions and as a DEB package for Ubuntu.	EMC

Resource requirements

The following components should meet these resource requirements:

Table 4 Resrouces requirements for components of the EMC OpenStack DPE system

Component	Virtual CPUs	Virtual disk size	Virtual RAM
EMC OpenStack DPE proxy	2	16 GB	2 GB
EMC OpenStack DPE API	2	16 GB	3 GB

DNS and Time Sync Requirements

Secure, reliable operation of EMC OpenStack DPE depends on a network that is also secure and reliable, and that supports forward and reverse lookup of hostnames, network time service, and various other services. Your network must meet these requirements before you begin installing EMC OpenStack DPE.

Network Connection and Port Usage

The following table provides a summary of the ports that are required by the EMC OpenStack DPE.

Table 5 EMC OpenStack DPE port requirements

Initiator	Target	Protocol	Port	Notes
Avamar server	Proxy instance	TCP	28000-30109	Various port required for communication between Avamar server and dpe-avamar-proxy service. See the *EMC Avamar Product Security Guide* for details.
EMC OpenStack DPE proxy	`dpe-proxy-service`	TCP	1947	default binding port
EMC OpenStack DPE service	EMC OpenStack DPE API (`dpe-api`)	TCP	8080	default binding port
Proxy (`avagent`)	Avamar server	TCP	28001	

CHAPTER 2

Installation

This chapter includes the following topics:

Overview

This section provides an overview of the installation of the EMC OpenStack DPE product.

EMC OpenStack DPE requires the deployment of three components in the OpenStack cloud infrastructure.

- EMC OpenStack DPE service (`dpe-proxy-service`), provided as an rpm for RHEL or deb for Ubuntu installation file.
- EMC OpenStack DPE proxy (`dpe-avamar-proxy`), provided as a qcow2 image.
- EMC OpenStack DPE API (`dpe-api`), provided as a qcow2 image.

Overview of the installation:

1. A backup-service project and backup administrator user must be created for hosting the EMC OpenStack DPE components.
2. The EMC OpenStack DPE service must be installed and configured on each of the OpenStack controller nodes (multiple nodes for High Availability support)
3. Within the avamar project, one or more EMC OpenStack DPE proxy instances must be deployed and configured.
4. Within the avamar project, a EMC OpenStack DPE API instance (REST API) must be deployed and configured.

Overview of configuration:

Note

Refer to the *EMC OpenStack Data Protection Extension REST API Getting Started Guide* for more details on configuring the EMC OpenStack DPE API.

---

1. After installation is complete, the EMC OpenStack DPE API can be used to register an Avamar server as a protection provider
2. OpenStack projects are registered and associated with one protection provider.
3. Instances within those projects are registered for protection.
4. Policies may also be created for scheduled backups.

Installation Prerequisites

Prior to beginning the installation of the EMC OpenStack DPE, validate that all prerequisites have been met.

OpenStack prerequisites

The EMC OpenStack DPE was designed to work with multiple OpenStack distributions and is currently certified against the reference architectures for the OpenStack releases named Kilo and Liberty. The supported distributions include Mirantis and Red Hat.

metadata_host

The EMC OpenStack DPE service looks for `metadata_host` to discover instances. This flag must be added to `/etc/nova/nova.conf` file on the controller node that has EMC

OpenStack DPE service installed. If the `metadata_host` entry does not exist, execute the following command to add the flag:

```
openstack-config --set /etc/nova/nova.conf DEFAULT metadata_host
<controller-node-ip>
```

cloud-init

`cloud-init` must be properly configured, or deployment of EMC OpenStack DPE components will fail. By default, certain settings are not enabled which are required for `cloud-init` to function. Ensure the following settings are set to 'true' in the `/etc/neutron/dhcp_agent.ini` file on the controller node and run the following commands to set the flags:

```
openstack-config --set /etc/neutron/dhcp_agent.ini DEFAULT
enable_isolated_metadata True
openstack-config --set /etc/neutron/dhcp_agent.ini DEFAULT
enable_metadata_network True
```

After changing these settings, restart neutron services.

Backup-service project and user

A backup-service project and backup administrator user account must be created for hosting the EMC OpenStack DPE components. The following guidelines should be followed when creating this project and user account:

- Create a backup-service project solely for use by the backup service. The suggested name for this project is **avamar**, for clarity purposes.
  - The backup-service project name will go into the backup-service configuration.
  - Proxy instances will run within the backup-service project.
  - You cannot perform backups of instances within the backup-service project.
  - Temporary volumes and snapshots for backup and restore operations will be attached to the backup-service project.
  - Quotas for the backup-service project should be fairly large.
    - The number of volumes quota should be greater than the maximum number volumes in all active backups and restores. Only one backup or restore can be active for each proxy instance. Queued (but not active) backup or restore jobs do not count against this limit.
    - The total size of the volumes quota should be greater than the total size of all volumes in all active backups and restores. Queued jobs do not count against this limit.
- The suggested name for the user is backup_admin, for clarity purposes. Do not use an existing user.
  - The username and password will go into the backup-service configuration file.
  - The user must have the admin role for the backup-service project.
  - The user must have the member role of all projects with instances you wish to back up.

Example backup-service project and user configuration

The following task describes how to confgure an example backup-service project named **avamar** and user named **backup_admin**.

Before you begin

In the root user home directory of the tack controller node , there should be a `keystonerc_admin` or `openrc` file (or a similar file for various different distributions) containing the environment variables needed by the OpenStack CLI tools. Contents should look like:

```
# unset OS_SERVICE_TOKEN
# export OS_USERNAME=admin
# export OS_PASSWORD=yourpassword
# export OS_AUTH_URL=http://yourhost:5000/v2.0
# export PS1='[\u@\h \W(keystone_admin)]\$ '
# export OS_TENANT_NAME=admin
# export OS_REGION_NAME=RegionOne
```

These environment variables must be exported using the shell's `source` command:

```
# source keystonerc_admin
```

Procedure

1. Create a backup-service project by performing the following steps:

   a. Enter the following command at the command prompt to create a backup service tenant:

   ```
   # openstack project create avamar
   +-------------+----------------------------------+
   | Field       | Value                            |
   +-------------+----------------------------------+
   | description | None                             |
   | enabled     | True                             |
   | id          | f1210c6bc95043e8acbe10b2c29675ac |
   | name        | avamar                           |
   +-------------+----------------------------------+
   ```

   b. Determine the volume quotas:

   ```
   # cinder quota-show avamar
   +------------------+-------+
   |     Property     | Value |
   +------------------+-------+
   | backup_gigabytes |  1000 |
   |     backups      |   10  |
   |    gigabytes     |  1000 |
   | gigabytes_iscsi  |   -1  |
   |    snapshots     |   10  |
   | snapshots_iscsi  |   -1  |
   |     volumes      |   10  |
   |  volumes_iscsi   |   -1  |
   +------------------+-------+
   ```

   The EMC OpenStack DPE requires enough quotas for the volume number and size to allow for the largest possible number and size of concurrent backups that will be executed. For example, the next command will change the number of volumes to 100 and the volume size to 1000 GB.

c. Set the necessary volume number and size:

```
# cinder quota-update --volumes 100 --gigabytes 1000 avamar
+------------------+-------+
|     Property     | Value |
+------------------+-------+
| backup_gigabytes |  1000 |
|     backups      |   10  |
|    gigabytes     |  1000 |
| gigabytes_iscsi  |   -1  |
|    snapshots     |   10  |
| snapshots_iscsi  |   -1  |
|     volumes      |  100  |
|  volumes_iscsi   |   -1  |
+------------------+-------+
```

Note

backup_gigabytes and backups quotas are not related to EMC OpenStack DPE requirements.

2. Add roles to the backup-admin user by performing the following steps:

a. List the available projects:

```
# openstack project list
+----------------------------------+--------------------+
| ID                               | Name               |
+----------------------------------+--------------------+
| 15e3219df829442790495ba17d8cef37 | services           |
| d224c02464c147dfa8e86f6c1209a814 | admin              |
| daf2ec458c4548e6be18f4aff3d01948 | project-ABC        |
| ec0ad980acb64dfa98966d1fb899ed23 | project-XYZ        |
| f1210c6bc95043e8acbe10b2c29675ac | avamar             |
+----------------------------------+--------------------+
```

b. List the available roles:

```
# openstack role list
+----------------------------------+---------------+
| ID                               | Name          |
+----------------------------------+---------------+
| 6b9489f52a364dceb81ef5e957097b3c | admin         |
| 773822c030ef4dff93997e92e56ab2c2 | ResellerAdmin |
| 9fe2ff9ee4384b1894a90878d3e92bab | _member_      |
| da2f7af3bcf042459294156a9e4d12fe | SwiftOperator |
+----------------------------------+---------------+
```

c. Add the backup_admin user as an admin to the avamar project:

```
# openstack role add --project avamar --user backup_admin admin
+-------+----------------------------------+
| Field | Value                            |
+-------+----------------------------------+
| id    | 6b9489f52a364dceb81ef5e957097b3c |
| name  | admin                            |
+-------+----------------------------------+
```

d. Add the backup_admin user as an member to other projects:

```
# openstack role add --project project-ABC --user backup_admin
_member_
```

```
+-------+----------------------------------+
| Field | Value                            |
+-------+----------------------------------+
| id    | 9fe2ff9ee4384b1894a90878d3e92bab |
| name  | _member_                         |
+-------+----------------------------------+
```

```
# openstack role add --project project-XYZ --user backup_admin
_member_
+-------+----------------------------------+
| Field | Value                            |
+-------+----------------------------------+
| id    | 9fe2ff9ee4384b1894a90878d3e92bab |
| name  | _member_                         |
+-------+----------------------------------+
```

Networking prerequisites

The following prerequisites apply to networking issues with the EMC OpenStack DPE:

- EMC OpenStack DPE supports Neutron Configuration for FLAT, VLAN, GRE, & VXLAN segmentation.
- This documentation may refer to a flat network (which may also be referred to as a provider network) for the **avamar** project to use.
- If deploying proxies through NAT/Floating IP configuration, the IP assigned to the proxy instances must be registered to your DNS (that is, the fully-qualified domain name must be resolvable to an IP based on nslookup).
- The proxy instance must be able to connect to the Avamar server and the EMC OpenStack DPE service running on the controller node.
- The Avamar server must be able to connect to the proxy instance.
- The EMC OpenStack DPE API must be able to connect to the Avamar server.
- The EMC OpenStack DPE service and the EMC OpenStack DPE API must be able to connect to OpenStack.

Avamar prerequisites

The following Avamar prerequisites apply to installations of EMC OpenStack DPE:

- Avamar servers must be installed and must be at version 7.3.0.226.
- Data Domain can be used as backend storage and must be configured from within the Avamar Administrator GUI.
  - Data Domain version must be a version supported by Avamar 7.3 (currently, Data Domain versions 5.6 and 5.7 are supported).

Installation Checklist

The following is a checklist for installation activities of the various components of EMC OpenStack DPE.

- EMC OpenStack DPE service installation checklist
  - The EMC OpenStack DPE service requires the following packages to be installed onto the OpenStack controller node:
    - **python-suds** version 0.4 or greater

  - **python-requests** version 2.7.0 or greater
  - **python-bottle** version 0.12.6 or greater
- The EMC OpenStack DPE proxy will connect to the EMC OpenStack DPE service on a single port using TCP and any firewall must be configured to allow for communications on this port. The default port number is 1947.

- EMC OpenStack DPE proxy installation checklist
  - Configure the avamar project according to instructions in Example backup-service project and user configuration on page 18.
  - Configure a flat or VLAN external network for the **avamar** project to use.
  - Configure keystone environment variables for admin access to the **avamar** project by adding the following to the `/root/keystonerc_backup_admin` file on the OpenStack controller node:

```
unset OS_SERVICE_TOKEN
export OS_USERNAME=backup_admin
export OS_PASSWORD=changeme
export OS_AUTH_URL=http://keystone.example.com:5000/v2.0
export PS1='[\u@\h \W(keystone_avamar)]\$ '
export OS_TENANT_NAME=avamar
export OS_REGION_NAME=RegionOne
```

- The EMC OpenStack DPE API installation checklist
  - Configure the avamar project according to instructions in Example backup-service project and user configuration on page 18.
  - The EMC OpenStack DPE API instance can use either the same flat network that the EMC OpenStack DPE proxy uses, or it can use a Floating IP on a private network.
  - The EMC OpenStack DPE API will connect to the EMC OpenStack DPE service on a single port using TCP and any firewall must be configured to allow for communications on this port. The default port number is 8080.

Unpacking the EMC OpenStack DPE installation files

Procedure

1. From the EMC Online Support website (http://support.EMC.com), obtain a copy of the EMC OpenStack DPE installation zip file (`EMC_OpenStack_DPE_`*`version`*`.zip`).

   Where *version* is the version of the EMC OpenStack DPE.

2. Use a standard unzip program to unpack the installation files to a temporary location.

Results

The following files will be unzipped from the EMC OpenStack DPE installation zip file:

- The EMC OpenStack DPE service installation package for Ubuntu (`dpe-proxy-service-`*`version`*`.deb`).
- The EMC OpenStack DPE service installation package for RedHat (`dpe-proxy-service-`*`version`*`.rpm`).
- The EMC OpenStack DPE proxy image file (`dpe-avamar-proxy.`*`version`*`.qcow2`).
- The EMC OpenStack DPE API image file (`dpe-api.`*`version`*`.qcow2`).

The following sections detail how to install and configure EMC OpenStack DPE components by using these files.

Installing the EMC OpenStack DPE service

This section provides information about installing and configuring the EMC OpenStack DPE service.

Procedure

1. Install the EMC OpenStack DPE service rpm or deb file from the temporary location where they were unpacked as described in Unpacking the EMC OpenStack DPE installation files on page 21:
   - On RHEL, install the rpm using the following command:

     ```
     # yum localinstall dpe-proxy-service-version.rpm
     ```

   - On Ubuntu, install the deb using the following command:

     ```
     # dpkg -i dpe-proxy-service-version.deb
     ```

   Where *version* is the version of the EMC OpenStack DPE.

Configuring the proxy service configuration file

The proxy service configuration (`/etc/avamar/proxy-service1.conf`) contains configurable settings related to the proxy service. All of these settings have default values, and therefore the `proxy-service1.conf` file can be empty or have all values commented out.

The following is a description of each setting in the `proxy-service1.conf` file:

- [Service] settings:
  - `bind`: The network interface to which the proxy service binds. Default is `0.0.0.0` (which is usually the correct setting).
  - `port`: The port to which the proxy service binds. Default is `1947`.
  - `server`: The type of Python server implementation to use. Default is `paste`.
  - `ssl_pem`: The path to an SSL pem file (or "*" to accept all). Required to use SSL, otherwise not required. Default is `null`.
  - `debug`: Enables debug output from the server. Default is `false`.
- [Setting] (common) settings:
  - `interface`: Selects which set of OpenStack endpoints are expected on the same network as the proxy service. Depending on the network topology, only public or internal endpoints may be visible. On highly secure customer sites, the EMC OpenStack DPE will most likely be installed on the internal network. For most other configurations, the public endpoints are appropriate. Defaults to `public`.
  - `timeout_volume_clone`: The maximum time (in seconds) that the proxy service will wait for a volume clone operation to complete. Default is `7200` (two hours).
  - `timeout_volume_create`: The maximum time (in seconds) that the proxy service will wait for a volume create operation to complete. Default is `3600` (one hour).

  - `timeout_volume_detach`: The maximum time (in seconds) that the proxy service will wait for a volume detach operation to complete. Default is `3600` (one hour).
  - `timeout_proxy_request`: The maximum time (in seconds) that the proxy plug0in will wait for a response from the proxy service. Default is `7200` (two hours).
- [Watchdog] settings
  - `interval_poll`: The interval (in seconds) between when the watchdog wakes. Default is `3`.
  - `interval_inspect`: The interval (in seconds) between when the watchdog inspects tenants and volumes for stray volumes. Default is `3600` (one hour).
  - `volume_expiration`: Determines how old (in seconds) a volume must be before it is considered for cleanup. Default is `86400` (24 hours).

Procedure

1. Use a text editor to edit the `proxy-service1.conf` file as appropriate to change the values of the settings in the file.

   For any value that you set in the file, remember to uncomment (remove the `#` character) at the beginning of the line.

   Note

   There is no enforcement mechanism for reasonable values in the `proxy-service1.conf` file. The defaults are generally reasonable. Choose over-rides carefully.

Example 1 Example `proxy-service1.conf` file

```
[Service]
# How should the proxy-service appear as a web-service.

# Specify if you want the proxy-service bound to a particular
interface.
#bind=0.0.0.0

# If running more than one proxy-service, each bind/port must be
unique.
#port=1947

# The default WSGI server to use for the proxy-service.
#server=paste

# Must specify if use of SSL is wanted between proxy-instance and
proxy-service.
#ssl_pem=

# Primarily for development (or debugging).
#debug=False

[Settings]
# Control over aspects of the proxy-service behavior.

# Which OpenStack API interfaces should we use?
#interface=public

# Allow time needed for large volumes and slow/dumb storage.
#timeout_volume_clone=7200

# Allow time needed for slow storage.
#timeout_volume_create=3600

# Primarily a workaround for the Kilo (and prior) bug with
multipathed storage.
#timeout_volume_detach=3600

# How long should the proxy-instance wait for the processing of a
request by the proxy-service?
#timeout_proxy_request=7200

[Watchdog]
# Control over the background watchdog that (eventually) cleans up
volumes not processed properly.

# How often should the watchdog wake (in seconds)?
#interval_poll=3

# How often should the watchdog inspect tenants/volumes (in seconds)?
#interval_inspect=3600

# How old a disused/marked volume must be before forced deletion?
#volume_expiration=86400
```

Configuring the proxy service for SSL

This section describes how to configure the service for SSL. This is an optional task.

Procedure

1. If SSL will be used with the `dpe-proxy-service`, use a text editor to edit the `proxy-service1.conf` file and change the values of these two settings:

- `[Service] server`: Set to `paste`. This is the wsgi server that is used in OpenStack and should be available if the proxy service is installed on the OpenStack controller node. Otherwise it needs to be installed on the system the proxy service is running on.
- `[Service] ssl_pem`: Set to the location of a valid PEM file (for example, set this to ssl_pem="/etc/avamar/host.pem"). This file can be created by executing the following commands:

```
openssl genrsa 1024 > host.key
chmod 400 host.key
openssl req -new -x509 -nodes -sha1 -days 365  \
              -key host.key > host.cert
cat host.cert host.key > host.pem
chmod 400 host.pem
chown avamar:avamar host.pem
```

Configuring the `proxy-owner1.conf` file

The `proxy-owner1.conf` specifies the owner of proxy instances and working quota for use by the proxy service.

The following is a description of each setting in the `proxy-owner1.conf` file:

- [Keystone] settings:
  - `href`: Required. The URL to your OpenStack Keystone implementation. From this URL, the EMC OpenStack DPE is able to discover all otehr OpenStack services.
  - `username`: Required. The OpenStack user login used for both client registration and the proxy service. This should be the backup_admin user, as described in Backup-service project and user on page 17.
  - `password`: Required. The password for the backup_admin user.
  - `ssl_verify`: Determines whether to verify the ssl-certificate and host of the OpenStack Keystone implementation. Setting this to false disables verification; otherwise should be set to the path of a valid ssl-certificate for the Keystone host.
- [Tenant] setting
  - `name`: Required. The name of the backup service project used to contain proxies and working volume quotas.

Procedure

1. Use a text editor to edit the `proxy-owner1.conf` file as appropriate to change the values of the settings in the file.

   For any value that you set in the file, remember to uncomment (remove the # character) at the beginning of the line.

Example 2 Example `proxy-owner1.conf` file

```
[Keystone]
#href=http://localhost:5000/
#username=backup_admin
#password=secret
#ssl_verify=/path/to/sslcert.pem

[Tenant]
#name=avamar
```

Starting the EMC OpenStack DPE service

Once the EMC OpenStack DPE service has been installed and configured, use this procedure to start it.

Procedure

1. Execute the following commands to start the EMC OpenStack DPE service:
   - RHEL:

     ```
     # systemctl enable dpe-proxy-service
     # systemctl start dpe-proxy-service
     ```

   - Ubuntu:

     ```
     # initctl start dpe-proxy-service
     ```

Installing the EMC OpenStack DPE proxy

This section provides information about installing and configuring the EMC OpenStack DPE proxy.

Procedure

1. Create a new image in the **avamar** project of your OpenStack cloud using the EMC OpenStack DPE proxy image file found in the temporary location where they were unpacked as described in Unpacking the EMC OpenStack DPE installation files on page 21. You can use Horizon or execute the following command at the command prompt:

   ```
   openstack image create --disk-format qcow2 --file dpe-avamar-
   proxy.version.qcow2 --min-disk 16 --min-ram 2048 --private avamar-
   proxy
   ```

   Where *version* is the version of the EMC OpenStack DPE.

2. Create a flavor for the **avamar** proxies. Log into Keystone as the backup_admin user and run the following command at the command prompt:

   ```
   openstack flavor create --disk 16 --ram 2048 --vcpus 2 --swap 0 --
   ephemeral 0 --public avamar-proxy
   ```

3. Use one of the following commands to create or import a keypair for ssh access:

Note

You can also use the same keypair as the EMC OpenStack DPE API image.

- To import a keypair:

```
openstack keypair create --public-key ~/.ssh/idrsa.pub avamar_kp
```

- To create a keypair:

```
openstack keypair create keypair_name > private_key.pem
```

4. Create the security group and rules to define the access that is permitted by the proxy instance to the network. The following uses the proxy-security group name:

```
SECURITY_GROUP_NAME=proxy-security
openstack security group create $SECURITY_GROUP_NAME
openstack security group rule create --proto icmp   --src-ip
0.0.0.0/0                          #SECURITY_GROUP_NAME
openstack security group rule create --proto tcp    --src-ip
0.0.0.0/0 --dst-port 22:22         #SECURITY_GROUP_NAME
openstack security group rule create --proto tcp    --src-ip
0.0.0.0/0 --dst-port 28000:30100   #SECURITY_GROUP_NAME
```

5. Use the following script to deploy an instance of the EMC OpenStack DPE API inside the avamar project using the image created in step 1 on page 26, above, as the boot source. Do not create a volume from the image. Replace all variables in the script with valid parameter values.

```
USERNAME_PROXY=backup-admin       #username of 'avamar' project
PASSWORD_PROXY=changeme           #password of backup admin of
'avamar' project
HOSTNAME_CONTROLLER=10.25.64.xx   #IP or FQDN of controller node
HOSTNAME_AVAMAR=10.25.95.xx       #IP or FQDN of Avamar server
ZONEID=nova                       #default is 'nova'.  Set
according to the Guidelines defined in the Proxy section

URL_PROXY_SERVICE="http://$USERNAME_PROXY:$PASSWORD_PROXY@
$HOSTNAME_CONTROLLER:1947"

PROXY_FLAVOR=avamar-proxy
PROXY_NAME=proxy-1
PROXY_CONFIG_FILE=/tmp/user-data
IMAGE_PROXY=avamar-proxy

KEYPAIR_NAME=avamar_kp
SECURITY_GROUP_NAME=proxy-security
cat > $PROXY_CONFIG_FILE <<XXXX
#cloud-config
bootcmd:
 - service avagent register $HOSTNAME_AVAMAR /clients/$ZONEID
"$URL_PROXY_SERVICE"
XXXX

openstack server create \
    --image $IMAGE_PROXY \
    --key-name $KEYPAIR_NAME \
    --flavor $PROXY_FLAVOR \
    --security-group $SECURITY_GROUP_NAME \
    --user-data $PROXY_CONFIG_FILE \
    $PROXY_NAME
```

Note

The ZoneID `nova` in the above command must match the ZoneID field used to register instances via the EMC OpenStack DPE API. If the instance and proxy are not in the same availability zone, backup/restore operations will fail. The default zoneID is `nova`.

Installing the EMC OpenStack DPE API

This section provides information about installing and configuring the EMC OpenStack DPE API.

Procedure

1. Using the EMC OpenStack DPE image file found in the temporary location where they were unpacked as described in Unpacking the EMC OpenStack DPE installation files on page 21, create a new image of the EMC OpenStack DPE API in the **avamar** project of your OpenStack cloud by executing the following command at the command prompt:

   ```
   openstack image create --disk-format qcow2 --file dpe-
   api.version.qcow2 --min-disk 16 --min-ram 3072 --public avamar-api
   ```

   Where *version* is the version of the EMC OpenStack DPE.

2. Create a flavor for the **avamar** management service. Log into Keystone as the backup_admin user and run the following command at the command prompt:

   ```
   openstack flavor create --disk 16 --ram 3072 --vcpus 2 --swap 0 --
   ephemeral 0 --private avamar-api
   ```

3. Use one of the following commands to create or import a keypair for ssh access:

   Note

   You can also use the same keypair as the proxy image.

   - To import a keypair:

     ```
     openstack keypair create --public-key ~/.ssh/idrsa.pub avamar_kp
     ```

   - To create a keypair:

     ```
     openstack keypair create --public-key > keypair.pem avamar_kp
     ```

4. Create the security group and rules to define the access that is permitted by the proxy instance to the network. The following uses the avamar-api-security group name:

   ```
   SECURITY_GROUP_NAME=avamar-api-security
   openstack security group create $SECURITY_GROUP_NAME
   openstack security group rule create --proto icmp   --src-ip
   0.0.0.0/0                          #SECURITY_GROUP_NAME
   openstack security group rule create --proto tcp    --src-ip
   0.0.0.0/0 --dst-port 22:22         #SECURITY_GROUP_NAME
   openstack security group rule create --proto tcp    --src-ip
   0.0.0.0/0 --dst-port 8080          #SECURITY_GROUP_NAME
   ```

5. Use the following script to deploy an instance of the EMC OpenStack DPE API inside the avamar project using the image created in step 1 on page 28, above, as the boot

source. Do not create a volume from the image. The username and password must be for a keystone user in the admin project with the admin privilege. Replace all variables in script with valid parameter values.

```
USERNAME=admin
PASSWORD_=password
KEYSTONE="http://keystone.example.com:5000"

IMAGE=avamar-api
FLAVOR=avamar-api
INSTANCE_NAME=avamar-api
CONFIG_FILE=/tmp/user-data
KEYPAIR=avamar_kp
SECURITY_GROUP_NAME=avamar-api-security

cat > $CONFIG_FILE <<XXXX
#cloud-config
bootcmd:
 - /tmp/postconfig.sh $USERNAME $PASSWORD "$KEYSTONE"
XXXX

OpenStack server create \
    --image $IMAGE \
    --key-name $KEYPAIR \
    --security-group $SECURITY_GROUP_NAME \
    --flavor $FLAVOR \
    --user-data $CONFIG_FILE \
    $INSTANCE_NAME
```

6. Optional. If SSL is being used, follow these steps to configure SSL:

   a. Generate a private key and server certificate for the EMC OpenStack DPE API by logging into the management instance via `ssh`, changing to the `/etc/avamar` directory, and executing the following commands:

   ```
   openssl genrsa 1024 > /tmp/host.key
   chmod 400 /tmp/host.key
   openssl req -new -x509 -nodes -sha1 -days 3650 -key /tmp/
   host.key > /tmp/host.cert
   cat /tmp/host.cert /tmp/host.key > /etc/avamar/host.pem
   chmod 400 /etc/avamar/host.pem
   chown avamar /etc/avamar/host.pem
   ```

   b. If `ssl_verify` in the `/etc/avamar/mgmt-config.json` file is set to a `.pem` file, use the following command to validate the SSL public certificate for Keystone. If the certificate does not need to be verified, set `ssl_verify` to `false` and do not perform this step.

   ```
   openssl s_client -showcerts -connect host:port /null | openssl
   x509 -outform PEM > keystone.pem
   ```

   c. Edit the `/etc/avamar/mgmt-config.json` file:

   - In the [authentication] section, set the `href` setting to the URL of the Keystone instance; if the SSL public certificate should be validated, set the `ssl_verify` to the `.pem` file.
   - In the [mgmtApi] section, set `ssl_pem` to the host.pem file created in step 6.a on page 29.

   ```
   {
    "authentication": {
   ```

```
 "href": "https://keystone.example.com:5000",
 "username": "admin",
 "password": "changeme",
 "interface": "public",
 "ssl_verify": "/etc/avamar/keystone.pem"
 },
 "mgmtApi": {
 "host": "0.0.0.0",
 "port": 8080,
 "ssl_pem": "/etc/avamar/host.pem"
 },
 "providerApi": {
 "url": "http://localhost:8580/rest-api",
 "username": "admin",
 "password": "changeme",
 "ssl_verify": false
 },
 "resourceShareCapacityMB": 10000
}
```

7. Restart the management service:

```
systemctl restart dpe-api.service
```

Postinstallation checklist

Use the following checklist to ensure that the systems is working properly after installation.

Verify that the services are running.

- The EMC OpenStack DPE service
  - On RHEL:

    ```
    systemctl status dpe-proxy-service
    ```

  - On Ubuntu:

    ```
    initctl status dpe-proxy-service
    ```

  These commands should return a status of `active (running)`.
- The EMC OpenStack DPE API service
  Perform an ssh into the EMC OpenStack DPE API instance and execute the following at the command prompt:

  ```
  systemctl status dpe-api
  ```

  This command should return a status of `active (running)`.
- The EMC OpenStack DPE proxy
  Perform an ssh into the EMC OpenStack DPE proxy instances and execute the following at the command prompt:
  - On RHEL:

    ```
    service avagent status
    ```

  This command should return a status of `Client Agent is running` and `Client activated`.

Verify component communication:

- Avamar server can ping FQDN of all deployed `dpe-avamar-proxy` instances
- EMC OpenStack DPE proxy instances can ping the Avamar server.
- EMC OpenStack DPE proxy instances can ping thr Controller node (the EMC OpenStack DPE service) .
- The EMC OpenStack DPE API instance can ping Keystone.
- The EMC OpenStack DPE API instance can ping the Avamar server.EMC OpenStack DPE service node can ping the EMC OpenStack DPE proxy instances.

Verify communication ports:

- ssh to the EMC OpenStack DPE proxy instance
- Run following command to check communication port of EMC OpenStack DPE proxy instance:

  ```
  curl http://dpe-proxy-service-IP:1947
  ```

  This should not return a `couldn't connect to host` error.
- From the controller node, run following command to check the communication port of the EMC OpenStack DPE API instance:

  ```
  curl http://dpe-api-service-IP:8080
  ```

  This should not return a `couldn't connect to host` error.

APPENDIX A

Additional Information

This appendix includes the following topics:

Proxy performance

In an optimized OpenStack cloud infrastructure, the EMC OpenStack DPE proxy is capable of backing up approximately 180GB of data per hour.

OpenStack availability zones

OpenStack availability zones enable the cloud administrator to arrange OpenStack compute hosts into logical groups, and provides a form of physical isolation and redundancy from other availability zones, such as by using a separate power supply or separate network equipment.

The cloud administrator defines the availability zone in which a specified compute host resides locally on each server. An availability zone is commonly used to identify a set of servers that have a common attribute. For instance, if some of the racks in your data center are on a separate power source, you can put servers in those racks in their own availability zone. Availability zones can also help separate different classes of hardware.

When users provision resources, they can specify from which availability zone they want their instance to be built. This allows cloud consumers to ensure that their application resources are spread across disparate machines to achieve high availability in the event of hardware failure.

Cinder drivers

The EMC OpenStack DPE supports all storage arrays.

VNX snap copy

The VNX driver supports snap copy, which dramatically accelerates the process for creating a copied volume. By default, the driver will do full data copy when creating a volume from a snapshot or when cloning a volume, which is time-consuming especially for large volumes. When snap copy is used, the driver will simply create a snapshot and mount it as a volume when creating or when cloning a volume, which will be instantaneous even for large volumes.

To enable this functionality, include the `--metadata snapcopy=True` option when creating cloned volume or creating volume from a snapshot:

```
cinder create --source-volid <source-void> --name "cloned_volume" --
metadata snapcopy=True
```

or

```
cinder create --snapshot-id <snapshot-id> --name "vol_from_snapshot"
--metadata snapcopy=True
```

The newly created volume will actually be a snap copy rather than a full copy. If a full copy is needed, retype or migration can be used to convert the snap-copy volume to a full-copy volume, which may be time-consuming.

Determine whether the volume is a snap-copy volume a full-copy volume by showing its metadata:

```
cinder metadata-show volume
```

If the `snapcopy` entry in the metadata is `true`, the volume is a snap-copy volume. Otherwise, it is a full-copy volume.

APPENDIX B

Troubleshooting

This appendix includes the following topics:

OpenStack cloud infrastructure issues

This section addresses issues related to OpenStack infrastructure

The `metadata_host` parameter in the nova configuration file

The EMC OpenStack DPE service looks for the `metadata_host` paramater in the `etc/nova/nova.conf` file to discover instances. This flag must be present in the `nova.conf` file on the controller node on which the EMC OpenStack DPE service is installed. Execute the following command to add the this parameter to the file:

```
openstack-config --set /etc/nova/nova.conf DEFAULT metadata_host
controller-node-ip
```

`cloud-init` not configured

By default, certain settings are not enabled which is required for `cloud-init` to function. Ensure the following settings are set to **`true`** in the `/etc/neutron/dhcp_agent.ini` file on the controller node. Run the following commands to set the flags:

```
openstack-config --set /etc/neutron/dhcp_agent.ini DEFAULT
enable_isolated_metadata True
openstack-config --set /etc/neutron/dhcp_agent.ini DEFAULT
enable_metadata_network True
```

After changing settings, restart neutron services.

Note

If `cloud-init` is not configured properly, deployment of the EMC OpenStack DPE components will fail to run the proper post-configuration tasks and will the installation will not successfully complete.

Networking issues

This section describes networking issues that may occur with the EMC OpenStack DPE .

Ports for EMC OpenStack DPE component communication

The EMC OpenStack DPE proxy instance will connect to the EMC OpenStack DPE service on a single port using TCP. This port is configurable and defaults to 1947. The EMC OpenStack DPE API instance will connect to the EMC OpenStack DPE service on a single port using TCP. That port is configurable and defaults to 8080.

These port must be configured at the firewall to allow for communication. Execute the following commands on the controller node where the EMC OpenStack DPE service and EMC OpenStack DPE service are installed to add the ports to iptable:

```
iptables -I INPUT -p tcp --dport 1947 -j ACCEPT
iptables -I OUTPUT -p tcp --dport 1947 -j ACCEPT
iptables -I INPUT -p tcp --dport 8080 -j ACCEPT
iptables -I OUTPUT -p tcp --dport 8080 -j ACCEPT
```

Confirm that the ports are properly confirmed:

1. ssh to the EMC OpenStack DPE proxy instance.

2. Execute the following commands at the command line:

```
curl http://dpe-proxy-service-IP:1947
curl http://dpe-proxy-service-IP:8080
```

This should indicate successful communication and not return errors similar to `couldn't connect to host`.

Hostname resolution

The EMC OpenStack DPE requires proper hostname resolution for backup and restore operations. In certain Openstack network configurations, the proxy instance may not have a resolvable hostname. For example, deploying the EMC OpenStack DPE proxy instance on a private subnet with a Floating IP will require hostname resolution. The Avamar server communicates with the proxy through hostname.

To ensure proper operation of the EMC OpenStack DPE, hostname resolution using the `/etc/hosts` file may be required:

1. Log into the Avamar server.
2. Attempt to ping the hostname of the deployed EMC OpenStack DPE proxy instance.
3. If it is not pingable, modify the `/etc/hosts` file by adding and entry for the EMC OpenStack DPE proxy instance. One entry must be added per deployed proxy instance.
4. ssh into the EMC OpenStack DPE proxy.
5. Attempt to ping the hostname of the Avamar server.
6. If it is not pingable, modify the `/etc/hosts` file by adding entry for the Avamar server. This must be done for all deployed proxy instances.
7. If Avamar server is configured with a Data Domain, attempt to ping the hostname of the Data Domain system.
8. If it is not pingable, modify the `/etc/hosts` file by adding entry for the Data Domain system. This must be done for all deployed proxy instances.

EMC OpenStack DPE instances cannot ping the OpenStack controller node

The following requirements apply to communication between the EMC OpenStack DPE system and the OpenStack controller node:

- The EMC OpenStack DPE proxy must be able to communicate with the EMC OpenStack DPE service running on the OpenStack controller node.
- The EMC OpenStack DPE API must be able to communicate with the Keystone services running on the OpenStack controller node.

The EMC OpenStack DPE proxy instance (and optionally, the EMC OpenStack DPE API instance) run in a flat network on an OpenStack cloud. The controller node is a multi-homed host with access to the flat network as well as the admin network (and possibly the storage network and other networks). This may present issues if the controller node is not reachable from the EMC OpenStack DPE instances given default network settings in effect on the controller node. If the controller node is running RHEL6 or newer, default settings may need to be changed to fix this problem. This might also be an issue on other flavors and versions of Linux.

Note

If a EMC OpenStack DPE instance is unable to ping the OpenStack controller node, installation will complete but backup and restore operations will fail.

To resolve this issue:

1. Edit file `/etc/sysctl.conf` and set the following values:

```
net.ipv4.conf.default.rp_filter = 2
net.ipv4.conf.all.rp_filter = 2
```

   - net.ipv4.conf.default.rp_filter = 2
   - net.ipv4.conf.all.rp_filter = 2

2. Execute the following command to make the new values premanent:

```
sysctl -p
```

   Instances on the OpenStack flat network should now be able to ping the controller node. Verify the resolution to this issue by pinging the controller node from the EMC OpenStack DPE proxy instance.

Installation troubleshooting

This section provides troubleshooting steps for issues related to installation.

The EMC OpenStack DPE proxy instance fails to register to the protection provider

After deploying the EMC OpenStack DPE proxy instance, the `service avagent status` command returns the status:

```
avagent Info: Client Agent is not running.
```

To resolve this issue:

1. Enable cloud-init on OpenStack as described in OpenStack prerequisites on page 16.
2. Redeploy the EMC OpenStack DPE proxy instance.

If the problem persists, use the following procedure to manually register the proxy instance:

1. ssh to the EMC OpenStack DPE proxy instance.
2. Run the following command:

```
service avagent register Avamar_IP /clients/ZoneID http://
username:password@dpe-proxy-service-IP:port
```

   Where:

   - *Avamar IP* is the IP address of the Avamar server.
   - *ZoneID* is the ZoneID of the instance being registered.
   - http://*username*:*password*@*dpe-proxy-service-IP*:*port* represents the URL and login information for the EMC OpenStack DPE service (`dpe-proxy-service`).

The EMC OpenStack DPE API instance did not install completely

After deploying the EMC OpenStack DPE API instance, the `systemctl status dpe-api` command returns the status:

```
dpe-api.service
   Loaded: not-found (Reason: No such file or directory)
   Active: inactive (dead)
```

To resolve this issue:

1. Enable cloud-init on OpenStack as described in OpenStack prerequisites on page 16.

2. Redeploy the EMC OpenStack DPE API instance.

If the problem persists, use the following procedure to manually complete the EMC OpenStack DPE API installation:

1. ssh to the EMC OpenStack DPE API instance.
2. Run the following command:

   ```
   ./tmp/postconifig.sh username password http://Keystone-IP:5000
   ```

   Where:

   - *username* and *password* are the OpenStack Keystone admin login information.
   - *Keystone-IP* is the IP address of the Keystone server.