Dell EMC OpenStack Data Protection Extension

Version 19.2

REST API Getting Started Guide

302-005-846
Rev 01
November 2019

DELL EMC

Copyright © 2016-2019 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 **5**

Chapter 1 **Introduction** **9**
OpenStack Data Protection Extension and the REST API 10
OpenStack DPE API specification 10
Authentication, Authorization, and RBAC 10

Chapter 2 **Object Model** **13**
Protection providers 14
Projects 14
Instances 14
Backups 14
Group policies 15
Tasks or jobs 15

Chapter 3 **Swagger Bindings** **17**
Swagger bindings and YAML 18
Generating a set of bindings 18

Chapter 4 **OpenStack DPE API Example Usage** **19**
Examples Overview 20
Administration authentication tokens 20
Obtaining an administration token 20
Obtaining the version of the OpenStack DPE API 21
Provider and project registration 21
Registering a protection provider 21
Registering a project or tenant 22
Instance registration and on-demand backup 23
Adding instances to a tenant 23
Performing an on-demand backup of instance 24
Getting a task object 24
Listing the backups of an instance 24
Policy creation and ad-hoc policy backup 25
Creating a retention object 25
Creating a schedule object 25
Creating a dataset object 26
Creating a policy 26
Adding instances to a policy 27
Performing an on-demand policy backup 28
Instance restore 28
Listing backups of an instance to perform a restore 28
Restoring an instance 29
File-level restoration 29
FLR road map 30
Feature limitations 30
FLR session timers 31
Creating an FLR session 31

Listing the active FLR sessions..... 32
Getting an FLR session..... 32
Browsing and searching for files in the backup.....33
Downloading a file..... 34
Deleting an FLR session..... 35

Appendix Troubleshooting 37
OpenStack DPE API issues..... 38
Backup and restore issues.....38

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 create interfaces to the OpenStack environment using the Dell EMC OpenStack Data Protection Extension and the OpenStack DPE API.

Audience

This document is intended for system administrators and programmers who use the OpenStack environment and the Dell EMC OpenStack DPE API. A high degree of knowledge regarding Avamar and OpenStack administration is required.

Revision history

The following table prevents the revision history of this document.

Revision history

Table 1 Revision history

Revision	Date	Description
01	November 15, 2019	GA release of Avamar 19.2

Related documentation

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

- *OpenStack Data Protection Extension Release Notes*
- *OpenStack Data Protection Extension Installation and User Guide*

Special notice conventions used in this document

These conventions are used for special notices.

DANGER Indicates a hazardous situation which, if not avoided, results in death or serious injury.

WARNING Indicates a hazardous situation which, if not avoided, could result in death or serious injury.

CAUTION Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

NOTICE Addresses practices that are not related to personal injury.

Note: Presents information that is important, but not hazard-related.

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 • 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.

Documentation

The Avamar product documentation provides a comprehensive set of feature overview, operational task, and technical reference information. To supplement the information in product administration and user guides, review the following documents:

- Release notes provide an overview of new features and known limitations for a release.
- Technical notes provide technical details about specific product features, including step-by-step tasks, where necessary.
- White papers provide an in-depth technical perspective of a product or products as applied to critical business issues or requirements.

Knowledgebase

The Knowledgebase contains applicable solutions that you can search for either by solution number (for example, KB000xxxxxx) or by keyword.

To search the Knowledgebase:

1. Go to https://www.dell.com/support/home/us/en/19.
2. Under the **Support** tab, click **Knowledge Base**.
3. Type either the solution number or keywords in the search box. Optionally, you can limit the search to specific products by typing a product name in the search box and then selecting the product from the list that appears.

Online communities

Go to Community Network at http://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 products.

Live chat

To engage Customer Support by using live interactive chat, click **Join Live Chat** on the **Service Center** panel of the Avamar support page.

Service Requests

For in-depth help from Customer Support, submit a service request by clicking **Create Service Requests** on the **Service Center** panel of the Avamar support page.

> **Note:** To open a service request, you must have a valid support agreement. Contact a sales representative for details about obtaining a valid support agreement or with questions about an account.

To review an open service request, click the **Service Center** link on the **Service Center** panel, and then click **View and manage service requests**.

Enhancing support

It is recommended to enable ConnectEMC and Email Home on all Avamar systems:

- ConnectEMC automatically generates service requests for high priority events.
- Email Home sends configuration, capacity, and general system information to Customer Support.

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

Introduction

This chapter contains the following topics:

- OpenStack Data Protection Extension and the REST API 10
- OpenStack DPE API specification 10
- Authentication, Authorization, and RBAC 10

OpenStack Data Protection Extension and the REST API

The OpenStack Data Protection Extension (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 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.

With the OpenStack Data Protection Extension REST API (OpenStack DPE API), backup administrators can create interfaces to authenticate with OpenStack, create projects, instances, and policies, and perform backups and recoveries.

This document provides information and examples for using the OpenStack DPE API.

OpenStack DPE API specification

The OpenStack DPE API reference documentation is provided as online documentation along with the API itself. Both are available on a deployed instance of the OpenStack DPE API qcow2 image.

The URL to access the documentation on a deployed instance of the OpenStack DPE API service is **`https://dpe-api-sever.com:8443/v1/ui`**.

This URL provides an interactive web application based on the Swagger REST API documentation implementation, Swagger UI. The application divides the API into sections, based on the authentication role required to access that section's set of API calls. Each section can be expanded to display the list of API calls supported in that section. Each API can be further expanded to display complete details of the inputs and outputs for that call, as well as the ability to execute that call from the web page itself.

When using the embedded client in the documentation, an example of how to call the same API using 'curl' on the command line is also provided. This is a very simple example of one such call:

```
curl -X GET --header 'Accept: application/json' --header 'X-Auth-Token: 1234...'
'http://host:8443/v1/protectionProviders'
```

This example demonstrates listing all registered protection providers. The response to this call should be a JSON object containing an array of *protectionProvider* objects.

The `X-Auth-Token` header is described below.

Authentication, Authorization, and RBAC

The OpenStack DPE API is integrated with OpenStack's Keystone identity service for authentication and authorization and implements a role-based access control (RBAC) system. To invoke any OpenStack DPE API call other than the basic `getVersions` call, you must first log into keystone and get a token. Keystone returns this token in a header called `X-Subject-Token`. The value of this header must be presented in all OpenStack DPE API calls as the `X-Auth-Token` shown in the example above.

If the token is not provided, or if the token has expired or is in any way invalid, a HTTP status code of 401 will be returned. If the token is valid, but the token does not provide sufficient access to the particular API or objects, a 403 status will be returned.

The OpenStack DPE API is divided into two authorization groups:

- System administrators (members of the admin project with admin role)
- Project administrators (members of a tenant/project with admin role)

Other users will receive a 403 response to any API call. The same user may have both system administration and project administration rights.

System administrators may register and manage protection providers, register and manage projects, and create policies and related objects within each project. Project administrators may manage objects within a project, including registering instances, associating instances with policies and performing backup and restore operations.

Because the API is token-based and stateless, a single client may maintain multiple tokens and intersperse calls with different tokens freely. There is no need to log in and out repeatedly to change roles.

CHAPTER 2

Object Model

This chapter contains the following topics:

- Protection providers 14
- Projects 14
- Instances 14
- Backups 14
- Group policies 15
- Tasks or jobs 15

Protection providers

A protection provider is a reference to a backup appliance which is either a physical Avamar server or an Avamar Virtual Edition (AVE), which may also have an attached Data Domain system.

A protection provider is registered by URL and exists outside of projects. One protection provider may be shared among many projects or may be assigned exclusively to a single project, and a protection provider cannot be removed unless all projects registered to the protection provider have been removed first. A protection provider can be suspended (for example, for maintenance).

Projects

A project represents an OpenStack tenant or project. When a project is registered, at least one protection provider must be associated with it. More than one protection provider may be associated with one project, but the set of associated protection provider cannot be modified after registration. The list of providers may either be shared with other projects, or be exclusive to a single project.

A project contains instances, policies, retentions, schedules and datasets. A project can be suspended similarly to a protection provider. A project can only be removed only after all of its contents have been removed.

If a tenant or project is deleted from OpenStack, it remains registered in the OpenStack DPE API and may be used to restore the contents of the project.

Instances

OpenStack instances are registered under their respective projects. If the OpenStack instance is deleted, the OpenStack DPE API instance remains and can be used to restore the original instance. Instances may be assigned to policies for scheduled backups or they may be used for adhoc backups only.

Backups

A backup object contains volume images as well as metadata that describes the instance at the time the backup was taken. Backup objects are created as a result of a scheduled backup, ad-hoc policy backup, or ad-hoc instance backup. Backups may be restored using the restore API.

Incremental backups

OpenStack DPE supports change block tracking (CBT) for incremental backups by using the Linux Fast Incremental (LFI) feature. CBT requires installation of the `dpe-cbt-agent` and `dpe-cbt-driver` components on all of the compute nodes.

With this feature enabled, the OpenStack DPE proxy uses a manifest of changed blocks from the respective compute node to back up only the differences since the last backup. The protection provider combines the blocks with the previous backup to create a synthetic full backup. To enable CBT for an instance, register that instance with the `cbtEnable` flag set to true.

When a work order is created with the `utilize_changed_block_list` flag set to true, the OpenStack DPE proxy performs an incremental backup of any instances with CBT enabled. For instances where CBT is not enabled, or if the CBT components are unavailable, the OpenStack DPE proxy defaults to a full backup.

Note:

> If the OpenStack DPE proxy performs a full backup because CBT was not enabled for the specific instance, the backup status reports as success without exception.
>
> If you change any volumes on a registered instance, such as attaching a new volume, the best practice is to use the PUT command to re-enable CBT for that instance before completing any backups. The first backup after attaching or detaching a volume from a registered instance will be a full backup.

Group policies

A group policy contains all the information necessary to perform backups of groups of instances.

Group policy objects contain three child objects:

- Schedule - when a scheduled backup is performed.
- Retention policy - how long the backup is stored in the backup appliance
- Dataset - optional backup parameters

Tasks or jobs

Most OpenStack DPE API calls perform whatever function they are assigned and return an immediate success or failure code. However, certain APIs (for example, backup) take long enough to perform that instead of returning an immediate success or failure code, they return a task object. The task object can then be monitored for completion status.

CHAPTER 3

Swagger Bindings

This chapter contains the following topics:

- Swagger bindings and YAML.....18

Swagger bindings and YAML

The OpenStack DPE API is defined by a YAML file following the Open API Specification 2.0 and implemented via Swagger.

The Swagger tool set can be used to generate a set of client bindings in many different programming languages. These bindings provide a nearly complete set of code to allow full operation of the OpenStack DPE API.

Generating a set of bindings

To generate a set of bindings:

Procedure

1. Obtain a copy of the `swagger-codegen` application and build it according to their instructions (for example, using Java and `maven`).
2. Obtain a copy of the YAML file from the OpenStack DPE API server (**`https://`*`dpe-api-server`*`:8443/api-doc/dataprotection.yaml`**).
3. Build the bindings with a command similar to the following:

   ```
   generate python bindings java -jar ./path/to/swagger-codegen-cli.jar
   generate -i ./dataprotection.yaml -l python
   ```

   The Swagger documentation provides further instructions.

After you finish

With this release of OpenStack DPE API, the generated client bindings will work with Python 2.7 and Java 1.8 using Swagger version 2.1.5.

CHAPTER 4

OpenStack DPE API Example Usage

This chapter contains the following topics:

- Examples Overview 20
- Administration authentication tokens 20
- Obtaining the version of the OpenStack DPE API 21
- Provider and project registration 21
- Instance registration and on-demand backup 23
- Policy creation and ad-hoc policy backup 25
- Instance restore 28
- File-level restoration 29

Examples Overview

The examples in this section use `curl` commands to execute POST or GET methods to OpenStack DPE API URLs. The `curl` commands are based on the examples from the OpenStack DPE API server's Swagger UI (displayed by clicking on an API line, then clicking on the **Try it out!** button).

These demonstrate a complete workflow, from registering a new protectionProvider, adding new projects and instances, creating a policy, performing on-demand policy or instances backups, and performing a restore.

Administration authentication tokens

All OpenStack DPE API functions (except for the `get version` API) require an `X-Auth-Token HTTP` request header. The OpenStack DPE API uses the value of the header to verify a user's authorization to perform the API. The token is obtained by sending a request to OpenStack Keystone.

The following command can be used to obtain an administration token from Keystone. The `-i` option in `curl` will display the response headers. To obtain a system administration token, `name` field should be set to `admin` and `password` field set appropriately, as is shown in the below example. To obtain a project administration token, change the `name` and `password` fields to a user with the administrator privilege in a project.

Obtaining an administration token

This example command returns an administration token.

Procedure

1. Use this command to return an administration token.

```
curl -X POST -i --header 'Accept: application/json' -d '{
 "auth": {
    "identity": {
      "methods": ["password"],
      "password": {
        "user": {
          "name": "admin",
          "domain": { "id": "default" },
          "password": "changeme"
        }
      }
    }
  }
}' 'http://keystone.example.com:5000/v3/auth/tokens'
```

Results

Response headers:

```
X-Subject-Token: 6b286f3e56fa4e85bb4f10e6e61a9332
```

Response:

```
Token
```

The value of the `X-Subject-Token` (a GUID) in the response is used as the value of the `X-Auth-Token` header required by OpenStack DPE API.

Obtaining the version of the OpenStack DPE API

The API to get the version of the OpenStack DPE API is the only API that does not require an `X-Auth-Token` header. This command is very useful to test whether the REST API's server application is correctly configured and running and that the network is configured correctly.

Procedure

1. Use the following command to obtain the version of the OpenStack DPE API:

```
curl -X GET --header 'Accept: application/json' 'https://dpe-api-server:8443'
```

Results

Response:

```
{
  "build-version": "{{build}}",
  "api-version": "1.1.0"
}
```

where *{{build}}* is the version of the OpenStack DPE API image file that you deployed.

Provider and project registration

The examples in this section show how to register a protection provider and a project.

The provider and project APIs used in these examples require a system administration privilege. Obtain the system administration token by running the `curl` command shown in Administration authentication tokens on page 20.

Registering a protection provider

Use the following command to register a protection provider (that is, a physical Avamar server or an Avamar Virtual Edition) with the OpenStack DPE API. Supply a user who is configured on the Avamar server or AVE with admin access.

Procedure

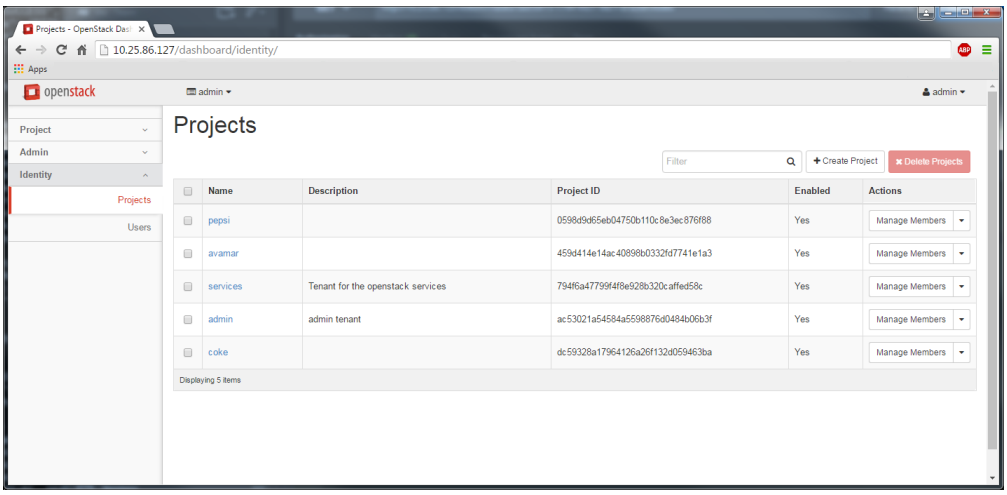
1. Use the following command to register a protection provider:

```
curl -X POST --header 'Content-Type: application/json' --header
'Accept: application/json' \
 --header 'X-Auth-Token: {{token-id}}' -d '{
  "protectionProviders": [
    {
      "name": "Avamar 1",
      "description": "The 1st backup appliance",
      "url": "https://avamar1.example.com:9443",
      "user": "MCUser",
      "password": "MCUser1"
    }
  ]
}' 'https://dpe-api-server:8443/v1/protectionProviders'
```

Registering a project or tenant

Before you begin

To get a list of projects in the OpenStack cloud, use Horizon or the `nova` command line application. The following image shows an example of Horizon's **Projects** page:



The GUID in the **Project ID** column replaces the *{{openstack-project-id}}* string in the example `curl` command below to register a tenant:

Procedure

1. Use the following command to register a project:

```
curl -X POST --header 'Content-Type: application/json' --header
'Accept: application/json' \
 --header 'X-Auth-Token: {{token-id}}' -d '{
  "projects": [
    {
      "id": "{{openstack-project-id}}",
      "name": "Coke",
      "capacityInMB": 0,
      "protectionProviders": [
        {
          "href": "https://dpe-api-server:8443/v1/protectionProviders/
{{provider-id}}",
          "id": "{{provider-id}}",
          "name": "Avamar 1"
        }
      ]
    }
  ]
}' 'https://dpe-api-server:8443/v1/projects'
```

Results

Response:

```
ProtectionProvider
```

The `projects` structure in the message body is a list, allowing for more than one project to be registered with one API call.

Instance registration and on-demand backup

This section demonstrates how to register OpenStack instances with the OpenStack DPE API, initiate a on-demand backup, monitor the backup task, and list backups of an instance.

The APIs used in this section require a project administration authorization token. Obtain the project administration token by running the `curl` command shown in Administration authentication tokens on page 20.

Adding instances to a tenant

Use the following command to register the instances of a project with the OpenStack DPE API. OpenStack instances must be registered with the OpenStack DPE API to be eligible for backup or restore.

Before you begin

The *{{openstack-instance-id}}* is the GUID of an OpenStack instance. As with the project ID shown in Registering a project or tenant on page 22, use either Horizon or the Nova command line to acquire a list of instances for a project or tenant.

Procedure

1. Use the following command to add CBT-enabled instances to a tenant:

```
curl -X POST --header 'Content-Type: application/json' --header
'Accept: application/json' \
 --header 'X-Auth-Token: {{token-id}}' -d '{
  "instances": [
    {
      "name": "Instance 1",
      "id": "{{openstack-instance-id}}",
      "zoneId": "nova",
      "cbtEnable": "true",
      "description": "My first instance"
    }
  ]
}' 'https://dpe-api-server:8443/v1/projects/{{openstack-project-id}}/
instances'
```

Results

Response:

```
Instance
```

The `instances` structure in the message body is a list that allows for more than one instance to be registered with one API call.

Performing an on-demand backup of instance

Use the following command to start an on-demand backup of an instance. The API returns a task object in the response. Use the `href` or `id` in the task object to retrieve the task status, until the task completes.

Procedure

1. Use the following command to perform an on-demand backup of an instance:

```
curl -X POST --header 'Content-Type: application/json' --header
'Accept: application/json' \
 --header 'X-Auth-Token: {{token-id}}' \
 'https://dpe-api-server:8443/v1/instances/{{openstack-instance-id}}/
backups'
```

Results

Response:

```
Task
```

The response from the on-demand backup API is a task object. Use the `id` field from the task object in the `get task` API to retrieve the status of the task, as shown in one of the following examples.

Getting a task object

Make repeated calls to the `get task` API to read the updated status. The task normally begins in the `QUEUED` state, then progresses to `RUNNING`, and finally to `SUCCESS`.

Procedure

1. Use the following command to get a task object:

```
curl -X GET --header 'Accept: application/json' \
 --header 'X-Auth-Token: {{token-id}}' \
 'https://dpe-api-server:8443/v1/tasks/{{task-id}}'
```

Results

Response:

```
Task
```

Listing the backups of an instance

After the task passes to the `SUCCESS` state, the backup appears in the list of backups of the instance. Display that list with the following command.

Procedure

1. Use the following command to list backups of an instance:

```
curl -X GET --header 'Content-Type: application/json' --header 'Accept:
application/json' \
```

```
 --header 'X-Auth-Token: {{token-id}}' \
 'https://dpe-api-server:8443/v1/instances/{{openstack-instance-id}}/
backups'
```

Results

Response:

```
Array of backup objects
```

Policy creation and ad-hoc policy backup

A policy contains references to retention, schedule, and dataset objects, as well as several other fields. The OpenStack DPE API defines a set of interfaces that implement policy driven backup. The interfaces closely correspond to the usage of policies in an Avamar.

Before the policy can be created, the child objects must first exist. The first three `curl` commands in this example create these objects. The `id` and `href` displayed in the responses to these APIs are then required in the `create policy` API, which follows. The final two example commands add instances to a policy and perform an on-demand backup.

Policy creation requires system administration privilege. A system administrator must create these objects on behalf of a project. Administration authentication tokens on page 20 describes how to obtain a system administration token from Keystone.

Creating a retention object

The following command demonstrates how to create a retention object.

Procedure

1. Use the following command to create a retention object:

```
curl -X POST --header 'Content-Type: application/json' --header
'Accept: application/json' --header 'X-Auth-Token: {{token-id}}' \
 -d '{ "description" : "backup retention", "name" : "pepsi_retention",
"retentionDuration" : { "unit" : "months", "duration" : "3" },
"expirationDate" : "1771400345000", "retentionType" : "never", "mode" :
"backup" }' \
 https://dpe-api-server:8443/v1/projects/{{project-id}}/retentions
```

Results

Response:

```
Retention
```

Creating a schedule object

The following command demonstrates how to create a schedule object.

Procedure

1. Use the following command to create a schedule object:

```
curl -X POST --header 'Content-Type: application/json' --header
'Accept: application/json' --header 'X-Auth-Token: {{token-id}}' \
```

```
 -d '{ "description": "Backup schedule for pepsi", "dailySchedule":
{ "maxRunHour": 8, "timeOfDays": [ "12:10:00" ] }, "recurrenceType":
"daily", "timezone": "GMT", "name": "pepsi_schedule" } \
https://dpe-api-server:8443/v1/projects/{{project-id}}/schedules
```

Results

Response:

```
Schedule
```

Creating a dataset object

The following command demonstrates how to create a dataset object.

Procedure

1. Use the following command to create a CBT-enabled dataset object:

```
curl -X POST --header 'Content-Type: application/json' --header
'Accept: application/json' --header 'X-Auth-Token: {{token-id}}' \
   -d '{ "options" : [ {"name": "ddr", "value" : "true"}, {"name": "ddr-
index", "value" : "1"}, {"name": "utilize_changed_block_list","value":
"true"} ], "name" : "dataset-1", "description" : "backup to DDR #1" }' \
   https://dpe-api-server:8443/v1/projects/{{project-id}}/datasets
```

Results

Response:

```
Dataset
```

Creating a policy

The following command uses the IDs returned in the previous three examples to create a policy.

Procedure

1. Use the following command to create a policy:

```
curl -X POST --header 'Content-Type: application/json' --header
'Accept: application/json' --header 'X-Auth-Token: {{token-id}}' \
 -d '{ \
      "description": "policy for pepsi", \
      "name": "policy1", \
      "schedule": { \
          "href": "https://dpe-api-server:8443/v1/schedules/{{schedule-
id}}", \
          "id": "{{schedule-id}}" \
      }, \
      "enabled": true, \
      "dataset": { \
          "href": "https://dpe-api-server:8443/v1/datasets/{{dataset-
id}}", \
          "id": "{{dataset-id}}" \
      }, \
      "overrideSchedule": "notOverridden", \
      "retention": { \
          "href": "https://dpe-api-server:8443/v1/retentions/
{{retention-id}}", \
```

```
            "id": "{{retention-id}}" \
        }, \
        "encryptionType": "high" \
    }' \
https://dpe-api-server:8443/v1/projects/{{project-id}}/policies
```

Results

Response:

```
Policy
```

Adding instances to a policy

The following example command shows how to add three instances to a policy.

Before you begin

A project administrator assigns instances to a policy, removes instances from a policy, and lists instances in a policy. Administration authentication tokens on page 20 describes how to obtain an admin token from Keystone to use with the following commands.

Procedure

1. Use the following command to add instances to a policy:

```
curl -X POST --header 'Content-Type: application/json' --header
'Accept: application/json' --header 'X-Auth-Token: {{token-id}}' \
  -d '{ \
    "instances": [ \
        { \
            "href": "https://dpe-api-server:8443/v1/instances/
{{instance-id-1}}", \
            "id": "{{instance-id-1}}" \
        }, \
        { \
            "href": "https://dpe-api-server:8443/v1/instances/
{{instance-id-2}}", \
            "id": "{{instance-id-2}}" \
        }, \
        { \
            "href": "https://dpe-api-server:8443/v1/instances/
{{instance-id-3}}", \
            "id": "{{instance-id-3}}" \
        } \
    ] \
} \
https://dpe-api-server:8443/v1/policies/{{project-id}}/instances
```

Results

Response:

The list of all instances that are protected by the policy. For example, the example command returned:

```
{
    "instances": [
        {
            "href": "https://dpe-api-server:8443/v1/instances/06e7c9f1-
a41b-4f59-9fa2-ba3189b53eb2",
            "id": "06e7c9f1-a41b-4f59-9fa2-ba3189b53eb2"
```

```
        },
        {
            "href": "https://dpe-api-server:8443/v1/instances/
bb5e7827-76c0-4e94-abf0-74ba321570f7",
            "id": "bb5e7827-76c0-4e94-abf0-74ba321570f7"
        },
        {
            "href": "https://dpe-api-server:8443/v1/instances/0b18544e-
c6ed-4a4d-a771-d6fbd66b8876",
            "id": "0b18544e-c6ed-4a4d-a771-d6fbd66b8876"
        }
    ],
    "href": "https://dpe-api-server:8443/v1/policies/9a1a2f39-7045-4836-
ae30-85674ff27d82/instances"
  }
```

The add, remove, and list policy instances all return the same type of response: the list of all instances that are currently covered by the policy.

Performing an on-demand policy backup

An on-demand policy backup initiates backup tasks for all the instances that are covered by a policy. The following command initiates an on-demand policy backup.

Procedure

1. Use the following command to perform a on-demand backup of all instances covered by a policy:

```
curl -X POST --header 'Content-Type: application/json' --header
'Accept: application/json' --header 'X-Auth-Token: {{token-id}}' \
   https://dpe-api-server:8443/v1/policies/{{policy-id}}/backups
```

Results

Response:

```
Task
```

The response for an on-demand policy backup is a task object that can be polled for task status. Getting a task object on page 24 provides an example of polling for task status.

Instance restore

The restore operation requires a project:admin privilege. Obtain the project:admin token by running the `curl` command shown in Administration authentication tokens on page 20

Listing backups of an instance to perform a restore

This example command lists the backups of an instance so that you can select one to restore.

Procedure

1. Use the following command to list backups of an instance:

```
curl -X GET --header 'Content-Type: application/json' --header 'Accept:
application/json' \
```

```
 --header 'X-Auth-Token: {{token-id}}' \
 'https://dpe-api-server:8443/v1/instances/{{openstack-instance-id}}/
backups'
```

Results

Response:

```
Array of backup objects
```

Restoring an instance

The following command starts a restore operation on an instance by using one of the backup IDs that you obtained from the previous command. The API returns a task object in the response. Use the `href` or `id` in the task object to retrieve the task status, until the task completes.

Procedure

1. Use this command to restore an instance:

```
curl -X POST --header 'Content-Type: application/json' --header
'Accept: application/json' --header 'X-Auth-Token: {{token-id}}' \

   https://dpe-api-server:8443/v1/backups/{{backup-id}}
```

Results

Response:

```
Task
```

The response from the API is a task object. Use the `id` field from the task object in the `get task` API to retrieve the status of the task.

File-level restoration

OpenStack DPE delivers support for file-level restoration (FLR) from instance backups to allow users to retrieve files from a backup without the need to complete a full restore operation. This feature provides the ability to restore specific files from a volume in a particular backup, or browse the files that are contained in the backup volumes.

The FLR service resides on the OpenStack DPE API VM, and controls FLR session management functions and scheduling.

Note: The FLR feature does not support restoring files directly into a running instance. Instead, the OpenStack DPE provides a graphical interface to browse and download files directly from the image backup.

FLR road map

The following road map illustrates a typical sequence of operations for the REST API. The project administrator creates and closes FLR sessions on behalf of the user.

Before you begin

Note: FLR sessions have timeout values that automatically close the session after periods of inactivity. However, anyone who has the objects for an active session may browse and download files from the instance backup.

Procedure

1. On receipt of a request to restore files, the project administrator obtains an administration token from the OpenStack DPE API.

   The *OpenStack Data Protection Extension REST API Getting Started Guide* and Swagger UI provide additional details.

2. The project administrator obtains a list of instances and associated backups from the OpenStack DPE API.
3. The project administrator selects a specific instance backup and then creates an FLR session from the OpenStack DPE API.
4. The OpenStack DPE provides a URL for the new FLR session, along with an FLR session ID and token.
5. The project administrator forwards the FLR session URL, ID, and token to the user.
6. Using the FLR session objects and web interface, the user browses the files and folders that are contained within the instance backup and starts a file restoration operation.
7. The user notifies the project administrator after the FLR session completes.
8. The project administrator uses the FLR session objects to close the session from the OpenStack DPE API.

Feature limitations

Observe the following limitations before using the FLR feature:

- The OpenStack DPE does not track absolute file paths within the instance OS, and is unaware of the mount points for each file system that was mounted within the instance OS. Only relative paths are supported.
- The OpenStack DPE supports a maximum of eight concurrent FLR sessions.
- The selection of individual file systems within an instance backup is not possible. The OpenStack DPE makes all file systems within the instance backup available to browse via the FLR session.
- File system support is limited to the file systems that `libguestfs` supports.
- Authentication and authorization are provided by the FLR session objects. Any user with the FLR session objects, however obtained, can access all of the files within the corresponding instance backup without further challenge.
- By default, OpenStack DPE supports a maximum of approximately 100,000 files in one folder. This is a technical limitation of `libguestfs`.

FLR session timers

Three timers govern the longevity of FLR sessions. The expiration of any of the three timers ends the session.

1. The first-access timer tracks the elapsed time between the creation of the FLR session and the first time that a user opens the FLR session URL or downloads a file. The default value is 2 hours.
2. The inactivity timer tracks the elapsed time between navigation requests via the FLR session URL, or between download requests. The default value is 15 minutes.
3. The end-of-life timer tracks the elapsed time since FLR session creation to establish a maximum session lifetime. Even if the session is active, this timer can end the session after a specified length of time. The default value is 8 hours.

Creating an FLR session

After selecting an instance backup, the project administrator uses the following command to create an FLR session for a user.

Before you begin

Obtain an administration token from the OpenStack DPE API.

Procedure

1. Use the following command to create an FLR session:

```
curl -X POST --header 'Content-Type: application/json'
 --header 'Accept: application/json' --header 'X-Auth-Token:
 {{token-id}}' \
 -d '{ "description" : "FLR session description",
 "firstAccessTimer" : "120", "inactiveTimer" : "15",
 "endOfLifeTimer" : "480" }' \
 https://dpe-api-server:8443/v1/backups/{{backupid}}/flr
```

   Adjust the value of each timer, as necessary, in seconds.

Results

Response:

```
FLR token
```

```
{
  "account": "{{avamar-account-name}}",
  "created": "{{POSIX-time}}",
  "description": "FLR session description",
  "endOfLifeTimerInterval": 480,
  "error": {
    "code": "Error code",
    "message": "Error message"
  },
  "firstAccessTimerInterval": 120,
  "href": "{{href}}",
  "id": "{{flr-session-uuid}}",
  "inactiveTimerInterval": 15,
  "projectId": "{{project-id}}",
  "sequence": "{{backup-sequence-id}}",
  "status": "{{session-status}}",
```

```
  "token": "{{session-token}}",
  "uri" : "https://flr-service-url:worker-port"
}
```

Listing the active FLR sessions

The following command demonstrates how to obtain a list of the active FLR sessions. Use the objects in the response to get the FLR session tokens.

Procedure

1. Use the following command to list the active FLR sessions:

```
curl -X GET --header 'Content-Type: application/json'
 --header 'Accept: application/json' --header 'X-Auth-Token:
 {{token-id}}' \
 https://dpe-api-server:8443/v1/projects/{{project-id}}/flr
```

Results

Response:

```
{
  "href": "{{href}}",
  "sessions": [
   {
    "account": "{{avamar-account-name}}",
    "created": "{{POSIX-time}}",
    "description": "FLR session description",,
    "endOfLifeTimerInterval": 480,
    "error": {
      "code": "Error code",
      "message": "Error message"
    },
    "firstAccessTimerInterval": 120,
    "href": "{{session-href}}",
    "id": "{{flr-session-uuid}}",
    "inactiveTimerInterval": 15,
    "projectId": "{{project-id}}",
    "sequence": "{{backup-sequence-id}}",
    "status": "{{session-status}}",
    "token": "{{session-token}}",
    "uri": "https://flr-service-url:worker-port",
    }
  ]
}
```

The `href` value is unique to each session.

Getting an FLR session

The following command retrieves the details of an active FLR session.

Procedure

1. Use the following command to get an FLR session:

```
curl -X GET --header 'Content-Type: application/json'
 --header 'Accept: application/json' --header 'X-Auth-Token:
```

```
 {{token-id}}' \
 https://dpe-api-server:8443/v1/flr/{{session-id}}
```

Results

Response:

```
{
  "account": "{{avamar-account-name}}",
  "created": "{{POSIX-time}}",
  "description": "FLR session description",
  "endOfLifeTimerInterval": 480,
  "error": {
    "code": "Error code",
    "message": "Error message"
  },
  "firstAccessTimerInterval": 120,
  "href": "{{href}}",
  "id": "{{flr-session-uuid}}",
  "inactiveTimerInterval": 15,
  "projectId": "{{project-id}}",
  "sequence": "{{backup-sequence-id}}",
  "status": "{{session-status}}",
  "token": "{{session-token}}",
  "uri" : "https://flr-service-url:worker-port"
}
```

Browsing and searching for files in the backup

Obtain the full path to the required file before starting the download operation.

Procedure

1. Use the following command to browse or search for files in the backup:

```
curl -X GET --header 'Content-Type: application/json'
 --header 'Accept: application/json' --header 'session-token:
 {{flr-token-id}}' \
 https://dpe-api-server:8443/v1/flr/{{flr-session-id}}/file?
 path={{relative-path}}&searching={{name-keyword}}&
 fields={{fields}}&order={{order}}&start={{start}}&
 limit={{limit}}
```

Parameter	Description
path	Restricts the search to a particular directory inside the file system. • Do not specify absolute paths for this parameter.
searching	Searches the backup for filenames that match the specified keyword.
fields	Filters the information that is returned for each result. • Accepts any of the values `type`, `name`, `permissions`, `uid`, `gid`, `size`, and `modified`. • Separate multiple values with commas. • The default values are `type` and `name`.
order	Controls the sorting order of the results.

Parameter	Description
	• Accepts one of the values `name`, `-name`, `time`, `-time`, `extension`, or `-extension`. • Values that are prefixed with - indicate descending order. • The default value is `name`.
`start`	Provides an offset into the results. • Accepts an integer greater than, or equal to, zero. • The default value is `0`.
`limit`	Limits the number of search results. • Accepts an integer greater than zero. • The default value is unlimited.

To search for files within a backup, combine the use of `searching` and `fields`. For example, use **`searching=doc&fields=name,type`** to search for files with names that contain the string "doc".

To provide paging capabilities, combine the use of `start` and `limit`. For example, use **`start=10&limit=10`** to view the 10th through 19th results.

Results

Response:

```
{
  "href" : "{{href}}",
  "start" : {{start}},
  "limit" : {{limit}},
  "files" : [
    "file" : {
      "href" : "{{file-href}}",
      "type" : "{{filesystem}}/{{folder}}/{{file}}",
      "name" : "{{name}}",
      "permissions": "{{permissions}}",
      "uid" : "{{uid-in-guest-OS}}",
      "gid" : "{{gid-in-guest-OS}}",
      "size" : "{{size}}",
      "modified" : "{{date-time}}"
    }
  ]
}
```

Permissions are returned in `drwx` format.

Downloading a file

After obtaining the information from a file during a browsing session, use the following command to download the file.

Procedure

1. Use the following command to browse files in the backup:

```
curl -X GET --header 'Content-Type: application/json'
 --header 'Accept: application/json' --header 'session-token:
 {{flr-token-id}}' \
```

```
 -d '{ "path" : "/{{file-system-id}}/{{full-path-name-in-file-
 system}}" }' \
 https://dpe-api-server:8443/v1/files/{{flr-session-id}}?
 path={{file-path}}
```

Results

Response:

A file download.

Deleting an FLR session

After retrieving files from an instance backup, the project administrator uses the following command to end a user's FLR session.

Procedure

1. Use the following command to delete an FLR session:

```
curl -X DELETE --header 'Content-Type: application/json'
 --header 'Accept: application/json' --header 'X-Auth-Token:
 {{token-id}}' \
 https://dpe-api-server:8443/v1/flr/{{session-id}}
```

Results

Response:

```
{
  "account": "{{avamar-account-name}}",
  "created": "{{POSIX-time}}",
  "description": "FLR session description",
  "endOfLifeTimerInterval": 480,
  "error": {
    "code": "Error code",
    "message": "Error message"
  },
  "firstAccessTimerInterval": 120,
  "href": "{{href}}",
  "id": "{{flr-session-uuid}}",
  "inactiveTimerInterval": 15,
  "projectId": "{{project-id}}",
  "sequence": "{{backup-sequence-id}}",
  "status": "{{session-status}}",
  "token": "{{session-token}}",
  "uri": "https://flr-service-url:worker-port"
}
```

APPENDIX

Troubleshooting

This appendix includes the following topics:

- OpenStack DPE API issues 38
- Backup and restore issues 38

OpenStack DPE API issues

The following are issues associated with the OpenStack DPE API.

504 error code

If an API requests returns with the error message: `A timeout occurred connecting to the Avamar REST API gateway, please try again later`, this could be because the OpenStack DPE API instance is rebooting. If the problem persists, manually reboot the instance.

500 error code

If an API requests returns with the error message: `No session is found for token` , ensure the OpenStack DPE API instance and Keystone server date and time are correctly synchronized. If the problem persists, reboot the OpenStack DPE API instance.

Modifying protection provider URLs

The `PUT: /protectionProvider/{id}` API allows the protection provider URL to be modified to point to another valid protection provider, but can lead to database issues.

Do not modify the protection provider URL from one protection provider to another valid protection provider. Only modify the protection provider URL when the actual URL of the same protection provider has changed.

Backup and restore issues

The following list describes issues that are related to backing up and restoring.

Restore instance to original fails

The original instance should be powered down before performing a restore to replace the original instance.

Slow backups

Verify that the Cinder drivers have fast clone capabilities and that it is enabled.

Backup task has a status of ERROR

- Review the details of the failed backup job for more information.
- Review the proxy service log, located on the controller node at `/var/dpe/dpe_proxy_service.log`.
- If the job status is partially successful and the `Inspect cbt service failed!` warning appears in the proxy service log, ensure that you have correctly installed the CBT drivers and services and that you have created the API endpoint.
- If you do not use the CBT feature, configure the Avamar server as follows:
  1. SSH to the Avamar server as the root user.
  2. Using a Linux text editor, such as `vi`, edit `/usr/local/avamar/lib/plugins/LINostackimage-1048.xml`.
  3. Locate the node that begins with the following elements:

```
<plugin-entry pid-number="1048" pid="ostackimage" description="Openstack
Image Plugin">
  <version-list>
    <version-reference version="7.4.100"/>
    <version-reference version="7.4.101"/>
    <version-reference version="7.5.100"/>
```

```
  <version-reference version="7.5.101"/>
</version-list>
```

Note: There may be more than one node for the OpenStack image plug-in. Ensure that you locate the node that contains a reference to version **7.5.101**.

4. Inside the OpenStack image plug-in node, locate the following flag:

```
<directives name="snapup">
  <controlgroup  order="1" type="checkwithpulldown" >
    <flag order="1" id="ddr" name="ddr" type="checkbox"
      desc="Store backup on Data Domain system"
      tooltip="Stores the backup on the selected Data Domain
        system instead of the Avamar server"/>
    <flag order="2" id="ddr-index" name="ddr-index"
      type="pulldown" ui-option="5.3.0.0" />
  </controlgroup>
  <flag order="2" id="utilize_changed_block_list"
    name="utilize_changed_block_list" pidnum="1048"
    type="boolean" value="true"
    desc="Use Changed Block Tracking (CBT) to increase
      performance"
    tooltip="Change blocks must be enabled for this to work"/>
</directives>
```

5. Change the value of the **utilize_changed_block_list** flag to **`false`**.
6. Save and close the file.
7. Type the following command:
   `mccli plugin update --force`

Backup job has a status of UNKNOWN

When a backup job has a status of UNKNOWN:

- Verify that the OpenStack DPE proxy instance is powered on and configured properly.
- Verify that the correct ZoneID was used when registering the instances for protection. All backups will fail if an incorrect ZoneID was used. If an incorrect ZoneID was used, the project administrator must unregister all instances and add them again with correct the ZoneID.

Backup job has a status of ERROR

When a backup job has a status of ERROR:

- Verify that the backup_admin user is a member of the Project that is being protected.
- Verify that the backup project (that is, the avamar project) quotas are not exceeded. This can be verified by running command `nova absolute-limits` from the controller node.

After restoring an instance to replace the original instance, subsequent backups fail

When an Instance is restored to replace original, the new instance has a new Instance ID and must be re-registered to the protection provider for future backups.