OpenManage Integration for VMware vCenter Version 5.2

API Guide

October 2020
Rev. A00

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

1

Overview

OpenManage Integration for VMware vCenter (OMIVV) provides RESTful APIs to enable automation. The support for RESTful API is available from version 5.2.0. The APIs are compliant with OpenAPI Specification (OAS) 3.0.0.

This document is intended for a vCenter Administrator. It is assumed that the reader is familiar with REST APIs and programmatic interaction with REST APIs. Any programming language can be used to create applications that interface with these APIs. You can run the APIs using an API Client such as Curl or Postman.

This document describes the set of APIs that can be used to automate the catalog-based host and cluster level firmware updates and firmware drift management.

OMIVV sample API scripts are available at https://github.com/dell/omivv.

Topics:

Supported APIs

- Start an OMIVV session
- Get vCenter details
- Set vCenter context
- Get datacenters, clusters, and hosts details
- Get cluster and cluster health details
- Get cluster profile details
- Get repository profile details
- Get firmware repository inventory details
- Create host and cluster level firmware inventory report
- Create host and cluster level firmware update job
- Get host firmware update job details
- Get firmware drift report
- End an OMIVV session

Prerequisites

Before using the OMIVV APIs:

- Create all the profiles (Host Credential Profile, Cluster Profile, System Profile, Repository Profile) in OMIVV User Interface (UI) and use the profiles as required.
- The hosts must be management-complaint. For more information, see the Management Compliance topic in User's Guide.

Base URI

The base URI for any OMIVV RESTful API request must be in the following format:

```
https://{OMIVV Address}/Spectre/api/rest/v1/Services/
```

OMIVV Address: IPv4 address or Fully Qualified Domain Name (FQDN).

NOTE: All the URIs and query parameters are case-sensitive.

Request headers

The request header represents headers in the client HTTPS request that are used to communicate client preferences to the service end-point. The bearer token is the request header.

Sequence of API for firmware update

To perform the firmware update, run the following APIs in the given order:

1. `AuthenticationService/login`—Start an OMIVV session using OMIVV credentials. You will receive an access token.

   All subsequent APIs must include this token as a bearer token as part of request header.
2. `ConsoleService/Consoles`—Get all registered vCenters information
3. `ConsoleService/Consoles/{id}`—Get the vCenter tree view of all the datacenters, clusters, and hosts of the given vCenter ID.
4. `ConsoleService/OperationalContext`—Set the vCenter which is the context of the API operation
5. `ConsoleService/Clusters/{id}`—Get cluster details
6. `ConsoleService/Clusters/{id}/Details`—Verify cluster health status on OMIVV context.
7. `PluginProfileService/ClusterProfiles`—Get the list of all cluster profiles.
8. `PluginProfileService/ClusterProfiles/{id}`—Get the details of a given cluster profile ID.
9. `PluginProfileService/RepositoryProfiles`—Get the list of repository profile details.
10. `PluginProfileService/RepositoryProfiles/{id}`—Retrieve content of specified repository.
11. `RepositoryManagementService/RepositoryData?repoProfileID={repoProfileID}&bundleId={bundleId}&systemId={systemId}`—Get the firmware repository inventory report.
12. `UpdateService/FWReport`—Create firmware inventory report of the individual or clustered host based on the specified repository
13. `Services/UpdateService/Jobs`—Create firmware update job.
14. `UpdateService/Jobs`—Get all firmware update jobs
15. `UpdateService/Jobs/{id}`—Get the firmware update job details
16. `AuthenticationService/logoff`—End an OMIVV session

2

Security

The authentication and authorization flows are prerequisites to any API invocation. The request is forwarded to the CXF server defined for the REST API after the invocation.

If there is authorization and authentication failure, an appropriate error code with message is sent to the API client.

On success, the request is forwarded to the appropriate REST service endpoint (API) defined on the CXF servlet.

Topics:

OMIVV authentication

OMIVV web server handles incoming web requests and routes them to the REST endpoints.

- Authentication server performs the following:
  - Accepts login requests and provide the bearer token. This token is generated using the JWT scheme that includes a header, body, and footer.
  - Accepts log out requests which closes the session
- API server: Service all defined REST endpoints except endpoints that are related to authentication.

API clients establish a session with the API server using the endpoint: `/Services/AuthenticationService/login`.

OMIVV user credentials are required to authenticate a client of the RESTful API. Only the admin user is allowed to successfully log in as an API user. Other users (fo example, the read-only user) are not allowed to use the API.

Bearer Token

Each session that is created using an authentication service contains a bearer token that is generated using the JWT scheme.

Expiration period for bearer token is 60 minutes. If you are using the token after 60 minutes, an appropriate error code with message is sent to the API client.

The account lockout duration is one minute. If an account lockout happens after creating the Bearer token, bearer token can not be used during lockout duration (one minute). After an account lockout duration, same Bearer token can be used until it expires.

Rate limit

At a given time, only three unique client IPs can be active and can create total ten sessions. From an active session, you can send only 100 API requests in one minute (which excludes logoff API call).

If there are more than ten sessions, an appropriate error code with message is sent to the API Client.

The total number of failure login attempts that is allowed is six (count includes failed login attempts in administration console or REST API or use of invalid token for REST API access). After six failed login attempts, the account gets locked.

The account lockout duration is one minute.

You cannot start a new session when the account is locked. But, current active session remains active.

During the lockout period, any REST API call will not work except logoff API. An appropriate error message is displayed.

vCenter authorization

Authorization flow validates the following:

- Session token
- vCenter user credentials for the required permissions to run the API

Validate session token

OMIVV validates the token that is received from the API client against the following:

- Tampering
- Session validity

Validate vCenter user credentials

APIs are authorized against the vCenter user credentials, when required. Set an operational context which indicates the vCenter and the associated user credentials.

An operation context is required to ensure the permissions available to the user. You can set an operation context by invoking the corresponding API.

This context is unique to an OMIVV user session, and only a single context can be active for a session at a time. The different OMIVV user sessions can invoke APIs that use a different vCenter context.

3

Session management

Topics:

Start an OMIVV session

Description: Starts an OMIVV session for the given OMIVV IP. The OMIVV session is valid for 60 minutes. Only the admin user is allowed to successfully log in as an API user.

The bearer token received from this API must be used for other APIs as a header parameter.

Command or URL: `/Services/AuthenticationService/login`

Method: POST

Request body:

```
{
        "apiUserCredential" : {
            "username":"{OMIV username (admin)}",
            "domain" : "",
            "password" : "{OMIVV password}"
        }
    }
```

For more information about request body parameters, see Request body on page 36.

Parameters: None

vCenter Privileges required: None

HTTP response code:

Table 1. HTTP response codes

Code	Description
200	OK
400	Invalid parameters
429	Too many requests
500	Internal Server error / timeout
503	Client limit exhausted.

For OMIVV-Specific error codes, see OMIVV-Specific error codes on page 47.

Example Response:

```
{
    "accessToken": "{token ID}",
    "tokenType": "{token type}",
    "expiresAt": "{token expire date and time}"
}
```

For more information, see Response body on page 39.

End an OMIVV session

Description: Logs out from the OMIVV session. This API internally invalidate the bearer token.

Command or URL: `/Services/AuthenticationService/logoff`

Method: POST

Authorization: Bearer authentication

Parameters: None

vCenter privileges required: None

HTTP response code:

Table 2. HTTP response codes

Code	Description
200	Logged off successfully
401	Authorization failure
429	Too many requests
500	Internal Server error / timeout

For OMIVV-Specific error codes, see OMIVV-Specific error codes on page 47.

Example Response: `Logged off successfully.`

4

Console management

Topics:

Get list of registered vCenters

Description: Gets the list of all the registered vCenters for the given OMIVV.

Command or URL: `/Services/ConsoleService/Consoles`

Method: GET

Parameters: None

Authorization: Bearer authentication

vCenter privileges required: None

HTTP response code:

Table 3. HTTP response code

Code	Description
200	OK
401	Authorization failure
429	Too many requests
500	Internal Server error / timeout

For OMIVV-Specific error codes, see OMIVV-Specific error codes on page 47.

Example Response:

```
[
    {
        "id": "{vCenter ID}",
        "href": "https://{OMIVVIP}/Spectre/api/rest/v1/Services/ConsoleService/Consoles/
{vCenter ID}",
        "objectType": "ConsoleMetadata",
        "hostname": "{vCenter hostname or FQDN}",
        "ip": "{vCenter IP}"
    }
]
```

For more information, see Response body on page 39.

Get vCenter tree view of data center

Description: Gets the vCenter tree view of all the data centers, clusters, and hosts of the given vCenter ID.

This API helps you to get the host and cluster details for operations like firmware update.

All Dell EMC and OEM managed or unmanaged hosts are listed.

Command or URL: `/Services/ConsoleService/Consoles/{id}`

Method: GET

Authorization: Bearer authentication

Parameters:

Table 4. Parameters

Parameter	Value	Description	Default value	Parameter type	Data type
id	(required)	Resource ID. Use the vCenter ID received from the **Get list of registered vCenters** API. For more information, see Get list of registered vCenters on page 11.	N/A	Path	String

For OMIVV-Specific error codes, see OMIVV-Specific error codes on page 47.

vCenter privileges required: None

HTTP response code:

Table 5. HTTP response code

Code	Description
200	OK
401	Authorization failure
404	Resource not found
429	Too many requests
500	Internal Server error / timeout

Example Response:

```
{
     "id": "{vCenter ID}",
     "href": "https://{OMIVV IP}/Spectre/api/rest/v1/Services/ConsoleService/Consoles/
{vCenterID}",
     "objectType": "Console",
     "ip": "{vCenter IP}",
     "hostname": "{vCenter hostname or FQDN}",
    "datacenters": [
          {
             "id": "{Datacenter ID}",
             "href": "",
             "objectType": "Datacenter",
             "name": "{Datacenter name}",
             "clusters": [
                {
                   "id": "{cluster ID}",
                   "href": "https://{OMIVVIP}/Spectre/api/rest/v1/Services/
ConsoleService/Clusters/{clusterID}",
                   "objectType": "ClusterMetadata",
                   "name": "{cluster name}"
                },
                {
                   "id": "{cluster id}",
                    "href": "https://{OMIVVIP}/Spectre/api/rest/v1/Services/
ConsoleService/Clusters/{clusterID}",
                    "objectType": "ClusterMetadata",
                     "name": "{Cluster name}"
                }
                ],
    "hosts": ": [
```

```
            {
               "id": "{Host ID}",
                "href": "",
                "objectType": "Host",
                "hostip": "{Host IP}",
                "hostName": "{Hostname or FQDN}",
                "managementIP": "{iDRAC IP}",
                "serviceTag": "{Host Service Tag}",
                "model": "{Server Model Name}",
                "systemId": "{System ID}"
            }
  ]
  }
,
```

For more information, see Response body on page 39.

Set vCenter context

Description: Sets the vCenter context on which user want to perform any operation.

Enter the vCenter ID received from `/Services/ConsoleService/Consoles` API.

The required vCenter user privilege for all other APIs are verified when you trigger the API.

Command or URL: `/Services/ConsoleService/OperationalContext`

Method: POST

Request Body:

```
{
            "consoleId": "{vCenterID}",
            "consoleUserCredential":
          {
                "username": "{vCenter username}",
                "domain": "{domain}",
                "password": "{vCenter password}"
            }
        }
```

For more information about request body parameters, see Request body on page 36.

Parameters: None

vCenter privileges required: None

HTTP response code:

Table 6. HTTP response code

Code	Description
204	OK
400	Invalid parameters
401	Authorization failure
403	Failed to login to vCenter
429	Too many requests
500	Internal Server error / timeout

For OMIVV-Specific error codes, see OMIVV-Specific error codes on page 47.

Example Response: No content

Get cluster details

Description: Gets the cluster details of the given cluster ID. You can view all the hosts belong to the cluster. The vSAN and vSphere cluster details are displayed.

Command or URL: `/Services/ConsoleService/Clusters/{cluster-id}`

Method: GET

Authorization: Bearer authentication

Parameters:

Table 7. Parameters

Parameter	Value	Description	Default value	Parameter type	Data type
id	(required)	Resource ID. Use the cluster ID received from the **Get vCenter tree view of datacenter** API. For more information, see Get vCenter tree view of data center on page 11.	N/A	Path	String

vCenter privileges required: None

HTTP response code:

Table 8. HTTP response code

Code	Description
200	OK
400	Operational context not set
401	Authorization failure
404	Resource not found
429	Too many requests
500	Internal Server error / timeout

For OMIVV-Specific error codes, see OMIVV-Specific error codes on page 47.

Example response:

```
{
      "id": "{Cluster ID}",
      "href": "https://{OMIVVIP}/Spectre/api/rest/v1/Services/ConsoleService/Clusters/
{cluster ID}",
      "objectType": "Cluster",
      "name": "{Cluster name}",
      "consoleID": {Console ID},
      "clusterType": "{Cluster Type (vSAN or vSphere)}",
      "hosts": [
         {
            "id": "{Host ID}",
            "href": "",
            "objectType": "Host",
            "hostip": "{host IP}",
            "hostName": "{Hostname}",
            "managementIP": "{iDRAC IP}",
            "serviceTag": "{Service Tag}",
            "model": "{Server model name}",
            "systemId": "{System ID}"
         }
    ]
}
```

For more information, see Response body on page 39.

Get cluster health

Description: Gets the health (DRS and vSAN cluster health) of the given cluster ID. The health data is used for assessing the firmware update.

The data that is displayed here is real-time health information.

Command or URL: `/Services/ConsoleService/Clusters/{cluster_id}/Details`

Method: GET

Authorization: Bearer authentication

Parameters:

Table 9. Parameters

Parameter	Value	Description	Default value	Parameter type	Data type
id	(required)	Resource ID. Use the cluster ID received from the **Get vCenter tree view of datacenter** API. For more information, see Get vCenter tree view of data center on page 11.	N/A	Path	String

vCenter privileges required: None

HTTP response code:

Table 10. HTTP response code

Code	Description
200	OK
400	Operational context is not set.
401	Authorization failure
404	Resource not found
429	Too many requests
500	Internal Server error / timeout

For OMIVV-Specific error codes, see OMIVV-Specific error codes on page 47.

Example Response:

```
{
    "clusterId": "{cluster ID}",
    "drsState": "{DRS status}",
    "vsanObjectHealth": "{vSAN object health status}"
}
```

For more information, see Response body on page 39.

5

Repository profile management

Topics:

Get list of repository profiles

Description: Gets the list of all repository profiles that are created in OMIVV UI.

Command or URL: `/Services/PluginProfileService/RepositoryProfiles`

Method: GET

Authorization: Bearer authentication

Parameters: None

vCenter privileges required: Dell.Inventory.Configure Inventory

HTTP response code:

Table 11. HTTP response code

Code	Description
200	OK
400	Operational Context not set
401	Authorization failure
403	vCenter permission denied
429	Too many requests
500	Internal Server error / timeout

For OMIVV-Specific error codes, see OMIVV-Specific error codes on page 47.

Example Response:

```
[
     {
        "id": "{Repository profile ID}",
        "href": "https://{OMIVVIP}/Spectre/api/rest/v1/Services/PluginProfileService/
RepositoryProfiles/{vCenterID}",
        "objectType": "BaseProfileMetadata",
        "profileName": "{Repository profile name}",
        "description": "{Profile description}"
},
]
```

For more information, see Response body on page 39.

Get repository profile details

Description: Gets the details of the given repository profile ID. You can view the firmware and driver repository details. Also, you can view factory-created and user-created repository details.

Command or URL: `/Services/PluginProfileService/RepositoryProfiles/{id}`

Method: GET

Authorization: Bearer authentication

Parameters:

Table 12. Parameters

Parameter	Value	Description	Default value	Parameter type	Data type
id	(required)	Resource ID. Use the repository profile ID received from the **Get list of repository profiles** API. For more information, see Get list of repository profiles on page 16	N/A	Path	String

vCenter privileges required: Dell.Inventory.Configure Inventory

HTTP response code:

Table 13. HTTP response code

Code	Description
200	OK
400	Operational Context is not set
401	Authorization failure
403	vCenter permission denied
429	Too many requests
500	Internal Server error / timeout

For OMIVV-Specific error codes, see OMIVV-Specific error codes on page 47.

Example Response:

```
{
    "id": "{Repository profile ID}",
    "href": "https://{OMIVVIP}/Spectre/api/rest/v1/Services/PluginProfileService/
RepositoryProfiles/{Repository profile ID}",
    "objectType": "RepositoryProfile",
    "data":
       {
          "name": "{Profile Name}",
          "description": "{Repository Profile description}",
          "globalDefault": {Dell default repository profile},
          "repoType": "{Repository type}",
          "protocolType": "{Protocol type}",
          "uri": "{Catalog location}",
          "credential":
       {
          "username": "{Repository profile username}",
          "domain": "{domain name}",
          "password": "{Profile password}"
        },
           "synchronizeRepository": {Synchronize with current repository location}
 }
}
```

For more information, see Response body on page 39.

6

Cluster profile management

Topics:

Get list of cluster profiles

Description: Gets the list of all cluster profiles that are created in OMIVV UI.

Command or URL: `/Services/PluginProfileService/ClusterProfiles`

Method: GET

Authorization: Bearer authentication

Parameters: None

vCenter privileges required: Dell.Inventory.Configure Inventory

HTTP response code:

Table 14. HTTP response code

Code	Description
200	OK
400	Operation context is not set
401	Authorization failure
403	vCenter permission denied
429	Too many requests
500	Internal Server error / timeout

For OMIVV-Specific error codes, see OMIVV-Specific error codes on page 47.

Example Response:

```
[
    {
        "id": "{Cluster Profile ID}",
        "href": "https://{OMIVVIP}/Spectre/api/rest/v1/Services/PluginProfileService/
ClusterProfiles/{Cluster profile ID}",
        "objectType": "BaseProfileMetadata",
        "profileName": "{Cluster profile name}",
        "description": "{Cluster profile description}"
    }
]
```

For more information, see Response body on page 39.

Get details of cluster profiles

Description: Gets the details of a given cluster profile. You can view the associated system profile, driver repository profile, firmware repository profile, and associated cluster details.

Command or URL: `/Services/PluginProfileService/ClusterProfiles/{id}`

Method: GET

Authorization: Bearer authentication

Parameters:

Table 15. Parameters

Parameter	Value	Description	Default value	Parameter type	Data type
id	(required)	Resource ID. Use the cluster profile ID received from the **Get list of cluster profiles** API. For more information, see Get list of cluster profiles on page 18	N/A	Path	String

vCenter Privileges required: Dell.Inventory.Configure Inventory

HTTP response code:

Table 16. HTTP response code

Code	Description
200	OK
400	Operational Context not set
401	Authorization failure
403	VCenter permission denied
404	Resource not found
429	Too many requests
500	Internal Server error / timeout

For OMIVV-Specific error codes, see OMIVV-Specific error codes on page 47.

Example Response:

```
{
    "id": "{Cluster profie ID}",
    "href": "https://{OMIVVIP}/Spectre/api/rest/v1/Services/PluginProfileService/
ClusterProfiles/{Cluster profile ID}",
    "objectType": "ClusterProfile",
    "data": {
        "profileName": "{Cluster profile name}",
        "description": "{Cluster profile description}",
        "clusters": [
            {
                "id": "{Cluster ID}",
                "href": "https://{OMIVVIP}/Spectre/api/rest/v1/Services/ConsoleService/
Clusters/{Cluster ID}",
                "objectType": "ClusterMetadata",
                "name": "{Cluster name}"
            }
        ],
        "repo": [
            {
                "id": "{Repostory profile ID}",
                "href": "https://{OMIVVIP}/Spectre/api/rest/v1/Services/
PluginProfileService/RepositoryProfiles/{Repository profile ID}",
                "objectType": "BaseProfileMetadata",
                "profileName": "{Repository profile name}",
                "repoType": "{Repository profile type (Firmware or Driver}",
                "description": "{Profile description}"
            }
        ],
        "systemProfile": {
            "id": "{System profileID}",
            "href": "https://{OMIVVIP}/Spectre/api/rest/v1/Services/PluginProfileService/
RepositoryProfiles/{System profile ID}",",
```

```
            "objectType": "BaseProfileMetadata",
            "profileName": "{System profile name}",
            "description": "{System profile description}"
        }
    }
}
```

For more information, see Response body on page 39.

7

Firmware repository inventory management

Topics:

- Get firmware repository inventory details

Get firmware repository inventory details

Description: Gets the details of firmware repository inventory. Ensure that the repository is successfully downloaded.

The driver repository inventory is not supported.

You can view the details like bundle ID, list of components of the particular bundle ID for the specific server model.

Command or URL: `/Services/RepositoryManagementService/RepositoryData?repoProfileID={repoProfileID}&bundleId={bundleId} &systemId={systemId}`

Mandatory query parameter: repoProfileID

Optional query parameter: bundleId, systemId

Method: GET

Authorization: Bearer authentication

Parameters:

Table 17. Parameters

Parameter	Value	Description	Parameter type	Data type
repoProfileID	(required)	Related firmware repository profile ID. Use the repository profile ID received from the **Get list of repository profiles** API. For more information, see Get list of repository profiles on page 16	query	String
systemId	Optional	SystemID of the server to filter the bundles. To get the system ID, run `/Services/ConsoleService/Consoles/{id}` or `/Services/ConsoleService/Clusters/{cluster-id}`. For more information, see Get vCenter tree view of data center on page 11 and Get cluster details on page 14.	query	String
bundleId	Optional	Bundle ID to retrieve software components. To get the bundle ID, run `/Services/RepositoryManagementService/RepositoryData?repoProfileID={repoProfileID}&bundleId={bundleId}`. It is mandatory to enter bundleId to get the component list.	query	String

vCenter privileges required: Dell.Configuration.Firmware Update

HTTP response code:

Table 18. HTTP response code

Code	Description
200	OK
400	Invalid parameters
401	Authorization failure
403	Failed to log in to vCenter

Table 18. HTTP response code

Code	Description
429	Too many requests
500	Internal Server error / timeout

For OMIVV-Specific error codes, see OMIVV-Specific error codes on page 47.

Example Response:

```
{
    "repoProfileID": "{Repository profile ID}",
     "bundleID": "{Bundle ID}",
     "bundles": [
        {
          "bundleID": "{Bundle ID}",
          "name": "{Bundle name}",
          "description": "{Bundle description}",
          "model": "{Server model name}",
          "targetOS": "{Target host OS name}",
          "systemId": "{Server unique ID}"
         }
 ],
"components": [
   {
      "packageID": "{Component unique package ID}",
      "rebootRequired":"{host reboot required (True or False)}",
      "releaseDate": "{Component release date and month}",
      "name": "{Component name}",
      "description": "{Component description}",
      "supportedHWComponents": [
          {
             "componentID": "{Component ID}",
             "pcieVariants": [
                {
                   "deviceID": "{Device ID}",
                   "subDeviceID": "{Sub device ID}",
                   "subVendorID": "{Sub vendor ID}",
                   "vendorID": "{Vendor ID}"
                 }
              ]
           },
        ]
   }],
            "revisionHistory": "{Revison history}",
            "vendorVersion": "{Vendor Version}",
            "criticality": "{importance of component update}"
        },
```

NOTE: After you upgrade OMIVV to 5.2 (RPM Upgrade or backup and restore), the value of model, revisionHistory, and description are displayed as null until firmware repository is refreshed. To refresh the repository profile, on the repository profile page, click **Edit** and complete the wizard without doing any modification.

For more information, see Response body on page 39.

8

Firmware inventory management

Topics:

Create host level firmware inventory report

Description: Creates the host level firmware inventory report. You can view the host component details that is associated to the given bundle ID before performing firmware update.

Ensure that the host is managed by OMIVV and management complaint.

Use the bundle ID received from the `/Services/RepositoryManagementService/RepositoryData?repoProfileID={repoProfileID}&systemId={systemId}&bundleId={bundleId}` API.

Use the system ID received from the `/Services/ConsoleService/Clusters/{cluster-id}` API.

For hosts that are managed at data center level, use the system ID received from the /Services/ConsoleService/Consoles/{id} API.

Command or URL: `/Services/UpdateService/FWReport`

Method: POST

Authorization: Bearer authentication

Request Body:

```
{
   "reportType":"HOST",
  "hostID":"{host ID}",
  "repoProfileID":"{Repository profile ID}"
   "bundleAssociation":[
      {
           "systemId":"{system ID}",
         "bundleID":"{Bundle ID}"
      }
   ],

 }
```

For more information about request body parameters, see Request body on page 36.

Parameters: None

vCenter privileges required: Dell.Configuration.Firmware Update

HTTP response code:

Table 19. HTTP response code

Code	Description
200	OK
400	Invalid parameters
401	Authorization failure
403	Failed to login to vCenter
429	Too many requests

Table 19. HTTP response code

Code	Description
500	Internal Server error / timeout

For OMIVV-Specific error codes, see OMIVV-Specific error codes on page 47.

Example Response:

```
{
   "reportType": "HOST",
    "clusterReport":NULL,
    "hostReports":
                {
                    "host": {
                        "id": "{Host ID}",
                         "href": "",
                         "objectType": "Host",
                          "hostip": "{Host IPv4 or FQDN}",
                          "hostName": "",
                          "managementIP": "{iDRAC IP}",
                          "serviceTag": "{Host Service Tag}",
                          "model": "{Server model name}",
                          "systemId": "{System ID}"
                 },
                 "applicableComponents": [
                     {
                        "componentType": "{Component Type}",
                        "packageId": "{Package ID}",
                        "component": "{Component Name}",
                        "currentVersion": "{Current installed componet verson}",
                        "availableVersion": "{Available component version}",
                        "criticality": "{Importance of component update}",
                        "updateAction": "{Component update status}",
                        "scheduled": {Component update job scheduled},
                        "rebootRequired": {Host reboot required (True or False)},
                        "releaseDate": "{Component release date and month}"
                       },
             ]
  }
}
```

For more information, see Response body on page 39.

Create cluster level firmware inventory report

Description: Creates the cluster-level firmware inventory report. You can create vSAN and vSphere cluster level firmware inventory reports.

Use the bundle ID received from the `/Services/RepositoryManagementService/RepositoryData?repoProfileID={repoProfileID}&systemId={systemId}&bundleId={bundleId}` API.

Use the system ID received from the `/Services/ConsoleService/Clusters/{cluster-id}` API.

Command or URL: `/Services/UpdateService/FWReport`

Method: POST

Authorization: Bearer authentication

Request Body:

```
 {
   "reportType":"{CLUSTER}",
   "clusterID":"{Cluster ID}",

   "bundleAssociation":[
      {
         "systemId":"{System ID}",
```

```
            "bundleID":"{Bundle ID}"
        },
        {
            "systemId":"{System ID}",
            "bundleID":"{Bundle ID}"
        }


    ],
    "repoProfileID":"{Repository profile ID}"
}
```

For more information about request body parameters, see Request body on page 36.

Parameters: None

vCenter privileges required: Dell.Configuration.Firmware Update

HTTP response code:

Table 20. HTTP response code

Code	Description
200	OK
400	Invalid parameters
401	Authorization failure
403	Failed to login to vCenter
429	Too many requests
500	Internal Server error / timeout

For OMIVV-Specific error codes, see OMIVV-Specific error codes on page 47.

Example Response:

```
{
     "reportType": "{CLUSTER}",
     "clusterReport": {
         "cluster": {
            "id": "{Cluster ID}",
            "href": "https://{OMIVVIP}/Spectre/api/rest/v1/Services/ConsoleService/
Clusters/{Cluster ID}",
            "objectType": "clusterMetadata",
            "name": "{Cluster name}"
          },
         "hostReports": [
            {
              "host": {
                 "id": "{Host ID}",
                  "href": "",
                  "objectType": "Host",
                  "hostip": "{Host IP}",
                  "hostName": "",
                  "managementIP": "{iDRAC IP}",
                  "serviceTag": "{Host Service Tag}",
                  "model": "{Server model name}",
                  "systemId": "{System ID}"
           },
          "applicableComponents": [
              {
                 "componentType": "{Componenet Type}",
                 "packageId": "{Package ID}",
                 "component": "{Component Name}",
                 "currentVersion": "{Currently installed component version}",
                 "availableVersion": "{Available component version}",
                 "criticality": "{Importance of component update}",
                 "updateAction": "{Component update status}",
                 "scheduled": {Component update job scheduled},
```

```
                    "rebootRequired": {Host reboot required},
                    "releaseDate": "{Component release date and month}"
                },
            ]
        }
    ]
  },
   "hostReport": null
}
```

For more information, see Response body on page 39.

9

Firmware update management

Topics:

Create host level firmware update jobs

Description: Creates the firmware update job for a host managed by OMIVV. You can update both vSAN and vSphere host.

Driver update is not supported.

Chassis and single DUP firmware updates are not supported.

It may take few seconds to create firmware update job for large number of hosts.

Command or URL: `Services/UpdateService/Jobs`

Method: POST

Request body:

```
{
   "jobname":"{Firmware update job name}",
   "jobdesc":"{Job description}",
   "updateType":"{Update type (FIRMWARE)}",
   "updateTargetType":"HOST",
   "schedule":{
               "runLater":{Scheduled to run at a specified time (true or false)},
               "dateTime":"{Firmware update job schedule (date and time format:YYYY-MM-
DDTHH:MM:SSZ, 24 hour UTC time}"
               "runNow":{Run firmware update job now (true or false)},

  },
   "firmwareRepoProfileID":"{Firmware repository profile ID}",
   "rebootOptions":"{Reboot options}",
   "preCheck":{Check prerequisites before upate(true or false)},
   "firmwareUpdateTargets":[
               {
                              "hostId":"{Host ID}",
                              "bundleId":"{Bundle ID}",
                              "packageIDs":["Package ID1", "Package ID2"]
               }],
      "jobSpecificCustomConfiguration":{
               "exitMaintenanceMode":{true or false},
               "migratePoweredOffAndSuspendedVMs":{true or false},
               "resetIDracAndDeleteJobs":{true or false},
               "enterMaintenanceModetimeout":60,
               "enterMaintenanceModeOption": "{Enter maintenance mode option}"

      }
}
```

For more information about request body parameters, see Request body on page 36.

Authorization: Bearer authentication

Parameters: None

vCenter privileges required: Dell.Configuration.Firmware Update

HTTP response code:

Table 21. HTTP response code

Code	Description
202	OK
400	Operational Context not set
401	Authorization failure
403	VCenter permission denied
429	Too many requests
500	Internal Server error / timeout

For OMIVV-Specific error codes, see OMIVV-Specific error codes on page 47.

Example Response:

```
{
    "id": "{JOB ID}",
    "href": "https://{OMIVVIP}/Spectre/api/rest/v1/Services/UpdateService/Jobs/{job ID}",
    "objectType": "Job",
    "status": "{Job status}"
}
```

For more information, see Response body on page 39.

Create cluster level firmware update jobs

Description: Creates the firmware update job for a cluster managed by OMIVV. You can update both vSAN and vSphere clusters.

Driver update is not supported.

It may take few seconds to create the firmware update job for large number of hosts.

Command or URL: `Services/UpdateService/Jobs`

Method: POST

Request body:

```
{
   "jobname":"{job name}",
   "jobdesc":"{job description}",
   "updateType":"{Update type (firmware)}",
   "updateTargetType":"CLUSTER",
   "schedule":{
              "runLater":{Scheduled to run at a specified time (true or false),
              "dateTime":"{Firmware update job schedule (Firmware update job schedule
(date and time format:YYYY-MM-DDTHH:MM:SSZ, 24 hour UTC time)}"
              "runNow":{Run firmware update job now (true or false)},

  },
   "firmwareRepoProfileID":"{Firmware repository profile ID}",
   "rebootOptions":"{Reboot options}",
   "preCheck":{Check prerequisites before upate(true or false),
   "firmwareUpdateTargets":[
              {
                           "hostId":"{Host ID}",
                           "clusterId":"{Cluster ID, only for cluster update}",
                           "bundleId":"{Bundle ID}",
                           "packageIDs":["Package ID1", "Package ID2"]
              }],
         "jobSpecificCustomConfiguration":{
              "exitMaintenanceMode":{true or false},
              "migratePoweredOffAndSuspendedVMs":{true or false},
```

```
                "resetIDracAndDeleteJobs":{true or false},
                "enterMaintenanceModetimeout":60,
                "enterMaintenanceModeOption": "{enter maintenance mode option}"

        }
}
```

For more information about request body parameters, see Request body on page 36.

Authorization: Bearer authentication

Parameters: None

vCenter privileges required: Dell.Configuration.Firmware Update

HTTP response code:

Table 22. HTTP response code

Code	Description
202	OK
400	Operational Context not set
401	Authorization failure
403	VCenter permission denied
429	Too many requests
500	Internal Server error / timeout

For OMIVV-Specific error codes, see OMIVV-Specific error codes on page 47.

Example Response:

```
{
    "id": "{JOB ID}",
    "href": "https://{OMIVVIP}/Spectre/api/rest/v1/Services/UpdateService/Jobs/{job ID}",
    "objectType": "Job",
    "status": "Scheduled"
}
```

For more information, see Response body on page 39.

Get list of firmware update jobs (Host and Cluster)

Description: Gets all the host and cluster firmware update jobs.

Command or URL: `/Services/UpdateService/Jobs`

Method: GET

Authorization: Bearer authentication

Parameters: None

vCenter privileges required: Dell.Configuration.Firmware Update

HTTP response code:

Table 23. HTTP response code

Code	Description
200	OK
400	Operational Context not set

Table 23. HTTP response code

Code	Description
401	Authorization failure
403	VCenter permission denied
429	Too many requests
500	Internal Server error / timeout

For OMIVV-Specific error codes, see OMIVV-Specific error codes on page 47.

Example Response:

```
[
    {
        "id": "{Firmware update job ID}",
        "href": "https://{OMIVVIP}/Spectre/api/rest/v1Services/UpdateService/Jobs/
{firmware update job ID}",
        "objectType": "JOB",
        "status": "{job status}"
    }
]
```

For more information, see Response body on page 39.

Get firmware update job details (Host or Cluster)

Description: Gets the details of the given host firmware update job ID.

Command or URL: `/Services/UpdateService/Jobs/{id}`

Method: GET

Authorization: Bearer authentication

Parameters:

Table 24. Parameters

Parameter	Value	Description	Default value	Parameter type	Data type
id	(required)	Resource ID. Use the firmware update job ID received from the **Get list of host firmware update jobs** API. For more information, see Get list of firmware update jobs (Host and Cluster) on page 29.	N/A	Path	String

vCenter privileges required: Dell.Configuration.Firmware Update

HTTP response code:

Table 25. HTTP response code

Code	Description
200	OK
400	Operational Context is not set
401	Authorization failure
403	vCenter permission denied
404	Resource not found
429	Too many requests
500	Internal Server error / timeout

For OMIVV-Specific error codes, see OMIVV-Specific error codes on page 47.

Example Response:

```
{
    "id": "{Job ID}",
    "href": "https://{OMIVVIP}/Spectre/api/rest/v1/Services/UpdateService/Jobs/{job ID}",
    "objectType": "UpdateJob",
    "status": "{job status}",
    "data": {
        "jobname": "{Job name}",
        "jobdesc": "{Job description}",
        "updateType": "{Update type}",
        "schedule": {
            "runNow": false,
            "runLater": true,
            "dateTime": "{Update job schedule date and time}"
        },
        "repoProfileID": "{Repository profile ID}",
        "associatedEntities": [
            {
                "host": {
                    "id": "{Host ID}",
                    "href": "",
                    "objectType": "Host",
                    "hostip": "{Host IP}",
                    "hostName": "{Hostname}",
                    "managementIP": "{iDRAC IP}",
                    "serviceTag": "{Host Service Tag}",
                    "model": "{Server model name}",
                    "systemId": "{System ID}"
                },
                "bundleId": null,
                "packageIDs": [
                    "{Package ID1}",
                    "{Package ID2}"
                ]
            }
        ],
        "rebootOptions": "{reboot options}",
         "jobSpecificCustomConfiguration": {
            "exitMaintenanceMode":{true or false},
              "migratePoweredOffAndSuspendedVMs":{true or false},
              "resetIDracAndDeleteJobs":{true or false},
              "enterMaintenanceModetimeout":60,
              "enterMaintenanceModeOption": "{Enter maintenance mode option}"
        }
    }
}
```

For more information, see Response body on page 39.

10

System profile management

Topics:

Get list of system profiles

Description: Gets the list of all system profiles that are created in OMIVV UI.

Command or URL: `/Services/PluginProfileService/SystemProfiles`

Method: GET

Authorization: Bearer authentication

Parameters: None

vCenter privileges required: None

HTTP response code:

Table 26. HTTP response code

Code	Description
200	OK
400	Operation context is not set
401	Authorization failure
403	vCenter permission denied
429	Too many requests
500	Internal Server error / timeout

For OMIVV-Specific error codes, see OMIVV-Specific error codes on page 47.

Example Response:

```
[
    {
        "id": "{System profile ID}",
        "href": "https://{OMIVVIP}/Spectre/api/rest/v1/Services/PluginProfileService/
SystemProfiles/{System profile ID}",
        "objectType": "BaseProfileMetadata",
        "profileName": "{System profile name}",
        "description": "{system profile description}"
    }
]
```

For more information, see Response body on page 39.

Get system profile details

Description: Gets the details of the given system profile ID.

You can use only 12G and later PowerEdge servers and bare-metal servers as a reference server.

Command or URL: `/Services/PluginProfileService/SystemProfiles`

Method: GET

Authorization: Bearer authentication

Parameters: None

vCenter privileges required: None

HTTP response code:

Table 27. HTTP response code

Code	Description
200	OK
400	Operation context is not set
401	Authorization failure
403	vCenter permission denied
429	Too many requests
500	Internal Server error / timeout

For OMIVV-Specific error codes, see OMIVV-Specific error codes on page 47.

Example Response:

```
{
    "id": "{System profile ID}",
    "href": "https://{OMIVVIP}/Spectre/api/rest/v1/Services/PluginProfileService/
SystemProfiles/{System profile ID}",
    "objectType": "SystemProfile",
    "data": {
        "name": "{System profile name}",
        "description": "{Profile description}",
        "referenceServerIP": "{reference server IP}"
    }
}
```

For more information, see Response body on page 39.

11

Drift management

Topics:

- Get firmware drift report

Get firmware drift report

Description: Gets the firmware drift report for specific cluster.

This API helps you to get the drifted components details before running firmware update.

Command or URL: `/Services/DriftDetectionService/DriftReport/{id}/FwDriftDetails`

Method: GET

Authorization: Bearer authentication

Parameters:

Table 28. Parameters

Parameter	Value	Description	Default value	Parameter type	Data type
id	(required)	Resource ID. Use the cluster ID retrieved from `/Services/ConsoleService/Consoles/{id}`.	N/A	Path	String

vCenter privileges required: Dell.Inventory.Configure Inventory

HTTP response code:

Table 29. HTTP response code

Code	Description
200	OK
401	Authorization failure
404	Resource not found
429	Too many requests
500	Internal Server error / timeout

For OMIVV-Specific error codes, see OMIVV-Specific error codes on page 47.

Example Response:

```
[
    {
        "host": {
            "id": "{Host ID}",
            "href": "",
            "objectType": "Host",
            "hostip": "{Host IP}",
            "hostName": "{Hostname}",
            "managementIP": "{iDRAC IP}",
            "serviceTag": "{Service tag}",
            "model": "{Server Model name}",
            "systemId": "{System ID}"
        },
```

```
        "overallSummary": {
            "compliantStatus": "{Compliance Status}",
            "nonCompliantType": "{Non-compliant Type}",
            "noncompliantTypeDescription": "{Firmware version is different for N number
of component (s)}"
        },
        "componentDriftList": [
            {
                "componentDetails": {
                    "componentID": "{Component ID}",
                    "packageID": "{Package ID}",
                    "bundleID": "{Bundle ID}",
                    "instanceID": "{Instance ID}",
                    "componentName": "{Component Name}",
                    "componentType": "{Component Type}",
                    "componentTypeDisplay": "{Component Type Display}",
                    "upgrade": "Component Update required True or False",
                    "criticality": "{Importance of component update}",
                    "rebootRequired": "Host reboot required (True or False)",
                    "pciDeviceInfo": {
                        "deviceID": "{PCI device ID}",
                        "subDeviceID": "{PCI sub device ID}",
                        "subVendorID": "{PCI sub vendor ID}",
                        "vendorID": "{PCI vendor ID}"
                    }
                },
                "complianceSummary": {
                    "compliantStatus": "{Compliance Status}",
                    "nonCompliantType": "{non-compliance type}",
                    "noncompliantTypeDescription": "{Reason for non-compliance}"
                },
                "complianceDetails": {
                    "driftedVersionInfo": "{Component Version in Host}",
                    "baselineVersionInfo": "{Component version in Repository}"
                }
            }


        ]
    }
]
```

NOTE: After you upgrade OMIVV to 5.2 (RPM Upgrade or backup and restore), the value of model, revisionHistory, and description are displayed as null until firmware repository is refreshed. To refresh the repository profile, on the repository profile page, click **Edit** and complete the wizard without doing any modification. After repository profile is updated, update the associated cluster profile. Drift detection job runs after you update the cluster profile.

For more information, see Response body on page 39.

A

Request body

Start an OMIVV session

Table 30. Start an OMIVV session API

Parameter	Description
username	OMIVV username. Only admin user is allowed to login to API.
password	OMIVV password

Set vCenter context

Table 31. Set vCenter context API

Parameter	Description
consoleId	vCenter ID
username	vCenter username
domain	vCenter domain
password	vCenter password

Create host or cluster level firmware inventory report

Table 32. Host or cluster level firmware inventory report

Parameter	Description
reportType	Inventory report type (Host or Cluster)
hostID	Host ID
clusterID	Cluster ID
repoProfieID	Repository profile ID
systemId	System ID
bundleID	Bundle ID

Create cluster or host level firmware update job

Table 33. Cluster or host level firmware update job (continued)

Parameter	Description
jobname	Firmware update job name
jobdesc	Firmware update job description
updateType	Update type (FIRMWARE).

Table 33. Cluster or host level firmware update job (continued)

Parameter	Description
	The value for update type is case-sensitive. Enter the value in upper case. OMIVV supports only FIRMWARE update type.
updateTartgetType	Update Target Type (host or cluster). Host—used to update single host Cluster—used to update the hosts under cluster
runLater	Scheduled to run at a specified time (true or false)
runNow	Run firmware update job now (true or false)
dateTime	Firmware update job schedule (date and time format: YYYY-MM-DDTHH:MM:SSZ) for runLater. Enter date and time in 24 hour UTC format.
firmwareRepoProfileID	Repository profile ID. To get the repository profile details, run `/Services/PluginProfileService/RepositoryProfiles`.
rebootOptions	Reboot options. Safe reboot: Apply Updates and Reboot after entering Maintenance mode. Applicable for cluster level, vSphere, vSAN, and datacenter host level. Next reboot: Apply updates on next reboot. Applicable for vSphere, datacenter, and vSAN host level. Force reboot: Apply updates and force reboot without entering maintenance mode. Applicable for vSphere and datacenter host level. **NOTE:** If you select the Next reboot or Force reboot options, the following parameters are not applicable: exitMaintenanceMode, migratePoweredOffAndSuspendedVMs, enterMaintenanceModetimeout, enterMaintenanceModeOption
preCheck	Prerequisites check before firmware update. Ensure that prerequisites checks are met in your environment: For vSAN host and cluster: DRS is enabled Host is not already in maintenance mode vSAN data objects are healthy For vSphere host and cluster: DRS is enabled. The possible input value is true or false. Default value is true if the required value is not entered. For cluster-level firmware update, the only allowed value is true.
hostId	Host ID. You can update only 64 hosts. To get the host ID, run `/Services/ConsoleService/Consoles/{id}`

Table 33. Cluster or host level firmware update job

Parameter	Description
clusterId	Cluster ID. To get the cluster ID, run `/Services/ConsoleService/Consoles/{id}`.
bundleId	Bundle ID. To get the bundle ID, run `/Services/RepositoryManagementService/RepositoryData?bundleId={bundleId}`
packageIDs	package ID. To get the package ID, run `/Services/UpdateService/FWReport`. Package ID of the up-to-date components are not supported and firmware update job fails.
exitMaintenanceMode	Exit maintenance mode after firmware update completes. If you disable this option, host remains in maintenance mode.
migratePoweredOffAndSuspendedVMs	Move powered-off and suspended virtual machines to other hosts in cluster. Disabling this option disconnects VM until the host device is online.
resetIDracAndDeleteJobs	Clears all the iDRAC jobs present in the Job Queue followed by iDRAC reset before updating firmware on the host. If you do not mention any value while running API, OMIVV considers the settings configured on the **Settings** > **Firmware Update Settings** on the User Interface.
enterMaintenanceModetimeout	Enter the Maintenance Mode timeout value between 60–1440 minutes. If the wait time goes beyond the specified time, the update jobs fail and enter maintenance task will be canceled or timed out. However, the components may get updated automatically when the host is restarted.
enterMaintenanceModeOption	Enter maintenance mode option. This option is applicable for vSAN host and cluster. Supported options are: Ensure accessibility Full Data migration No data migration

B

Response body

This topic describes each parameter in the example response.

Start an OMIVV session

Table 34. Response body

Field	Type	Description
accessToken	String	Token ID
tokenType	String	Token type
expiresAt	Integer and string	Expiry date and time for token ID.

Get list of registered vCenters

Table 35. Response body

Field	Type	Description
id	String	vCenter ID
hostname	String	vCenter Hostname or FQDN
ip	String	vCenter IP

Get vCenter tree view of datacenter

Table 36. Response body

Field	Type	Description
id	String	vCenter ID or datacenter ID or cluster ID or Host ID
hostname	String	vCenter hostname or FQDN. The hostname value is displayed in the response only if the hostname is configured properly using DNS. Otherwise, hostname value displayed as null or blank.
ip	String	vCenter IP
name	String	Datacenter name or cluster name

Get cluster details

Table 37. Response body

Table 37. Response body

Field	Type	Description
id	String	Cluster ID or host ID
name	String	Cluster name
cluster type	String	Cluster type (vSAN or vSphere)
hostip	String	Host IPv4
managementIP	String	iDRAC IP
hostname	String	vCenter host name
serviceTag	String	Service Tag of the server
model	String	Server model name
systemId	String	System ID

Get cluster health

Table 38. Response body

Field	Type	Description
clusterId	String	Cluster ID
drsState	String	DRS state (Enabled or Disabled)
vsanObjectHealth	String	vSAN object health status (Healthy, Unhealthy, or N/A)

Get list of cluster profiles

Table 39. Response body

Field	Type	Description
id	String	Cluster profile ID
profileName	String	Cluster profile name
description	String	Cluster profile description

Get details of cluster profiles

Table 40. Response body

Field	Type	Description
id	String	Cluster ID or cluster profile ID or repository profile ID or system profile ID
profileName	String	Cluster profile name or repository profile name or system profile name
description	String	Cluster profile description or repository profile description or System profile description
name	String	Cluster name

Table 40. Response body

Field	Type	Description
repoType	String	Repository profile type (Driver or Firmware)

Get list of repository profiles

Table 41. Response body

Field	Type	Description
id	String	vCenter ID
profileName	String	Repository profile name

Get repository profile details

Table 42. Response body

Field	Type	Description
id	String	Repository profile ID
name	String	Repository profile name
description	String	Repository profile description.
globalDefault	Boolean	Dell EMC default catalog repository profile (True). Factory-created firmware repository profile.
repoType	String	Repository Type (Firmware or Driver)
protocolType	String	Protocol Type (NFS, CIFS, FTP, HTTP, HTTPS)
uri	String	Catalog location
synchronzeRepository	Boolean	Synchronize with currently repository location (Enabled or Disabled)
username	String	Repository profile username
domain	String	domain name
password	String	Profile password

Get firmware repository inventory details

Table 43. Response body

Field	Type	Description
repoProfileID	String	Repository profile ID
bundleID	String	Bundle ID
name	String	Bundle name
description	String	Bundle description
model	String	Server Model

Table 43. Response body

Field	Type	Description
targetOS	String	Target host OS name. Windows target OS used for firmware update using iDRAC.
systemId	String	System ID
packageID	String	Component unique package ID
rebootRequired	Boolean	Host reboot required (True or False)
releaseDate	Integer and string	Component release date and month
componentID	String	Supported hardware component ID
deviceID	String	Supported hardware device ID
subDeviceID	String	Supported hardware sub device ID
subVendorID	String	Supported hardware sub vendor ID
vendorID	String	Supported hardware sub vendor ID

Create host level firmware inventory report

Table 44. Response body

Field	Type	Description
reportType	String	Inventory report type
id	String	Host ID
hostip	String	Host IPv4 or FQDN
hostName	String	Hostname
managementIP	String	iDRAC IP
serviceTag	String	Host Service Tag
model	String	Server model
systemId	String	System ID
componentType	String	Component type
packageId	String	Component unique package ID
component	String	Component name
currentVersion	String	Current installed component version
availableVersion	String	Available component version
criticality	String	Importance of component update (Urgent, Recommended, Optional, Security, Performance)
updateAction	String	Component update status (Up to date, downgrade, upgrade)
scheduled	String	Component update job scheduled
rebootRequired	Boolean	Host reboot required (True or False)
releaseDate	Integer and String	Component release date and month

Create cluster level firmware inventory report

Table 45. Response body

Field	Type	Description
reportType	String	Inventory report type
id	String	Host ID or cluster ID
hostip	String	Host IPv4 or FQDN
hostName	String	Hostname
managementIP	String	iDRAC IP
serviceTag	String	Host Service Tag
model	String	Server model
systemId	String	System ID
componentType	String	Component type
packageId	String	Component unique package ID
component	String	Component name
currentVersion	String	Current installed component version
availableVersion	String	Available component version
criticality	String	Importance of component update (Urgent, Recommended, Optional, Security, Performance)
updateAction	String	Component update status (up to date, downgrade, upgrade)
scheduled	String	Component update job scheduled
rebootRequired	Boolean	Host reboot required (True or False)
releaseDate	Integer and String	Component release date and month

Create host or cluster level firmware update job

Table 46. Create host or cluster level firmware update job

Field	Type	Description
id	String	Firmware update job ID
Status	String	Firmware update job status.

Get list of host firmware update jobs

Table 47. Response body

Field	Type	Description
id	String	Firmware update job ID
status	String	Status of the firmware update job (Scheduled, Cancelled, Staging, Success, and Failed)

Get host or cluster firmware update job details

Table 48. Response body

Field	Type	Description
id	String	Firmware update job ID or host ID
status	String	Status of the firmware update job
jobname	String	Firmware update job name
jobdesc	String	Firmware update job description
updateType	String	Update type
runNow	Boolean	Run update job now
runLater	Boolean	Run update job later
dateTime	Integer and String	Update job schedule date and time
repoProfileID	String	Firmware repository profile ID
hostip	String	Host IPv4 or FQDN
hostName	String	Hostname
managementIP	String	IDRAC IP
serviceTag	String	Host Service Tag
model	String	Server Model
systemId	String	System ID
bundleId	String	Bundle ID
packageIDs	String	Component unique package ID
rebootOptions	String	Reboot options. Safe reboot: Apply Updates and Reboot after entering Maintenance mode. Applicable for cluster level, vSphere, vSAN, and datacenter host level. Next reboot: Apply updates on next reboot. Applicable for vSphere, datacenter, and vSAN host level. Force reboot: Apply updates and force reboot without entering maintenance mode. Applicable for vSphere and datacenter host level.
precheck	Boolean	Prerequisites check before firmware update. Ensure that prerequisites checks are met in your environment: For vSAN host and cluster: DRS is enabled Host is not already in maintenance mode vSAN data objects are healthy For vSphere host and cluster: DRS is enabled

Table 48. Response body

Field	Type	Description
migratePoweredOffAndSuspendedVMs	Boolean	Move powered-off and suspended virtual machines to other hosts in cluster. Disabling this option disconnects VM until the host device is online.
resetiDracAndDeleteJobs	Boolean	Clears all the iDRAC jobs present in the Job Queue followed by iDRAC reset before updating firmware on the host. If you do not mention any value while running API, OMIVV considers the settings configured on the **Settings** > **Firmware Update Settings** on the User Interface.
enterMaintenanceModetimeout	String	Enter the Maintenance Mode timeout value between 60–1440 minutes. If the wait time goes beyond the specified time, the update jobs fail and enter maintenance task will be canceled or timed out. However, the components may get updated automatically when the host is restarted
enterMaintenanceModeOption	String	Enter maintenance mode option. This option is applicable for vSAN host and cluster. Supported options are: Ensure accessibility Full Data migration No data migration

Get firmware drift report

Table 49. Get firmware drift report (continued)

Field	Type	Description
id	String	Host ID
hostip	String	Host IP
hostname	String	Hostname
managementIP	String	iDRAC IP
Service Tag	String	Service Tag of the host
model	String	Server Model Name
systemID	String	System ID
complianceStatus	String	Compliance Status. You may get any of the following values for compliant status: VERSION_MISMATCH NEW COMPONENT

Table 49. Get firmware drift report

Field	Type	Description
		COMPONENT MISSING/ATTRIBUTE_MISMATCH NOT_APPLICABLE
nonCompliantType	String	Reason for non-compliance
noncompliantTypeDescription	String	Detailed description for non-compliance
componentID	String	Component ID
packageID	String	Package ID
bundleID	String	Bundle ID
instanceID	String	FQDD
componentName	String	Component Name
componentType	String	Component Type
componentTypeDisplay	String	Component Type Display. For example, firmware is displayed as FRMW.
upgrade	Boolean	Component Upgrade required (True or False)
criticality	String	Importance of component update
rebootRequired	Boolean	Host reboot required (true or false)
deviceID	String	Device ID
subDeviceID	String	Sub device ID
subVendorID	String	Sub Vendor ID
vendorID	String	Vendor ID
driftedVersionInfo	String	Component version in host
baselineVersionInfo"	String	component version in repository

C

OMIVV-Specific error codes

Table 50. OMIVV-specific error codes

Code	Description
11501	Number of active sessions limit exceeded.
11502	Number of active client limit exceeded.
11503	Input user data is not valid to process the login request.
11504	Exception occurred in token generation.
11505	User is not authorized to process the login request.
11506	Not a valid API Action specified.
11507	Account is locked.
11508	Request limit per minute exceeded.
11509	Empty Action request. Connection refused.
11510	User is not authorized to process the login request. Account Locked.
11601	Invalid Token
11602	Invalid path
11603	Internal Server Error
11604	Public key not found
11605	Token has already expired
10001	vCenter is not registered with appliance.
10101	Invalid console id {0}
10102	No vCenter is registered with appliance for the given id {0}
10103	vCenter tree is empty for id {0}
10201	Invalid http header does not contain authorization token.
10202	Invalid http header is empty.
10203	Invalid Parameters. vCenter context request parameters is not proper.
10205	Failed to login to vCenter. Make sure vCenter is running and credentials are valid.
10206	Invalid Parameters. No vCenter is registered with the appliance.
10301	Cluster does not exist.
10302	The cluster with name {0} and id {1} has been deleted or has zero hosts.
10303	The cluster with name {0} and id {1} has been deleted or has zero OMIVV managed hosts.
10304	The cluster with name {0} and id {1} is not associated with Cluster Profile.

Table 50. OMIVV-specific error codes

Code	Description
10401	The requestinfo is null or request does not contain serverIP details.
10402	Unable to find the cluster details because cluster is not part of the selected vCenter: {0}
10601	Repository profile does not exist.
10901	Cluster profile is not created.
11001	Cluster profile does not exist.
10701	Invalid repository profile {0}.
10702	The repository {0} is not downloaded or refreshed.
10703	An exception occurred while loading the repository {0} : {1}.
10704	Invalid bundleId {0}.
10705	Invalid systemId {0}.
10706	Driver repository profiles {0} are not supported.
10802	For vSAN-enabled cluster, the cluster or host level firmware inventory is not supported for Dell Default Catalog and Validated MX Stack Catalog firmware repository profiles.
10804	Unable to find the cluster details: {0}.
10808	Firmware inventory report at host level does not allow empty or null hostId value.
10809	System BundleID does not allow empty or null value.
10810	vCenter with id {0} not found in registered list.
10812	Unable to find the cluster details using: {0}.
10814	The host is not compliant because the Hypervisor status is non- compliant.
10815	Only HOST/CLUSTER firmware inventoryType is allowed.
10816	Firmware inventory report does not allow empty or null BundleAssociations value.
10817	SystemId does not allow empty or null value.
10818	Unable to find the applicable files components using BundleAssociations.
10820	Unable to find the HostName using hostAddress {0}.
10821	Firmware inventory report at cluster level does not allow empty or null clusterId.
10822	Unable to retrieved vcenter tree using vCenterAddress {0}.
10823	The host is not compliant because the host is not associated to Host Credential Profile.
10824	The host is not compliant because the CSIOR status is non-compliant.
10825	Unable to find the Host managementIP using hostAddress {0}.
11301	preCheck is not applicable for rebootOptions with values FORCEREBOOT or NEXTREBOOT.

Table 50. OMIVV-specific error codes

Code	Description
11302	enterMaintenanceModeOption, exitMaintenanceMode, migratePoweredOffAndSuspendedVMs, and enterMaintenanceModetimeout are not applicable for rebootOptions with values FORCEREBOOT or NEXTREBOOT.
11303	firmwareUpdateTargets cannot be null or empty.
11304	More than one firmwareUpdateTargets is not supported for HOST firmware update.
11305	Invalid job schedule.
11306	Invalid jobSpecificCustomConfiguration details : {0}.
11307	rebootOptions cannot be null or empty.
11308	Invalid jobSpecificCustomConfiguration details. Enter the enterMaintenanceModetimeout value between 60 to 1440 minutes.
11309	Invalid input. The value for preCheck should be true for cluster update.
11310	exitMaintenanceMode value should be true for cluster update.
11312	Invalid enterMaintenanceModeOption.
11313	enterMaintenanceModeOption is not applicable for non-vSAN host or cluster.
11315	packageIDs cannot be null or empty.
11316	Unsupported jobSpecificCustomConfigurations. Only 5 job specific configurations are supported.
11317	Duplicate Host id : {0}.
11318	Component is up to date with package id: {0}.
11319	Invalid packageId {0}.
11320	Invalid packageId.
11321	Invalid input preCheck is applicable only for host managed under cluster.
11322	Unable to find the host details in inventory for host : {0}.
11323	The host with id {0} is not associated to credential profile.
11324	The host is not compliant {0}.
11325	The following firmware update jobs are currently scheduled {0} for host/cluster {1}.
11326	Invalid dateTime: {0}.
11327	An exception occurred while setting date and time schedule : {0}.
11328	Empty or null value is not allowed for job name.
11329	The job name is too long. Job name allows only 255 characters.
11330	The entered job name already exists {0}.
11331	The job Description is too long. Job Description allows only 2000 characters.

Table 50. OMIVV-specific error codes

Code	Description
11332	Do not enter true or false or null values for both the runNow and runLater job schedules at a time.
11333	Schedule the job at least 30 minutes after the UTC current time: {0}.
11334	The dateTime values for job schedular should not be null or empty.
11335	The dateTime used for job schedular is invalid.
11336	The dateTime format for job schedular should be : yyyy-MM-dd'T'HH:mm:ssZ.
11337	Host {0} is not part of the cluster.
11338	All hosts in the cluster are non-compliant.
11339	The host is not compliant {0}.
11340	rebootOptions with NEXTREBOOT is not applicable for runLater.
11341	rebootOptions with NEXTREBOOT is applicable only for HOST level Update Job.
11342	rebootOptions with FORCEREBOOT is not applicable for runLater.
11343	rebootOptions with FORCEREBOOT is applicable only for HOST level Update Job.
11344	rebootOptions with FORCEREBOOT is applicable only for non-vSAN HOST level Update Job.
11345	Driver updates are not supported.
11346	bundleId cannot be null or empty.
11347	hostId cannot be null or empty.
11349	clusterId cannot be null or empty.
11350	Invalid clusterId {0}.
11351	For vSAN-enabled cluster, the cluster or host level update job is not supported for Dell Default Catalog and Validated MX Stack Catalog firmware repository profiles.
11451	Firmware update job is not present.
11452	Invalid Job id.
11453	Job id {0} not found.
11701	Exception occured while retrieving firmware drift details.
11702	Exception occured while retrieving configuration drift details
11703	Exception occured while retrieving driver drift details
11704	Firmware drift is not calculated for cluster {0}. Ensure drift detection job is completed successfully.
0	Unknown exception occured.
12501	Input request is not valid.
12502	Operational Context not set.
12503	Invalid path parameter.

Table 50. OMIVV-specific error codes

Code	Description
12504	Invalid Parameters.
12505	vCenter for which the Operational Context was set got unregistered with the appliance.
12506	Could not find the request header information.
12507	Could not find the Bearer Authorization token.
12508	Invalid Server Context.
12509	Error in connecting to vCenter.
12510	vCenter User is not authorized to access this URI.
12511	URI not supported by OMIVV.
12512	vCenter ID {0} is not available in the registered list.
12001	Internal Server Error/Timeout occurred: {0}.
12002	Unable to schedule the firmware update job.
12003	Unable to get applicable files.
12004	Unable to get the applicable software files.
12005	Unable to get the applicable software bundles.
12006	An exception occurred while finding the vSAN cluster details.
12007	Unable to process.
12008	vCenter id {0} is not is not registered with appliance.
12009	Invalid vCenter details.
12010	An unknown exception was recorded in the logs.