Axway API Manager 7.6.2 Release Notes

Document version: 28 May 2019

Summary

API Manager is a licensed product running on top of API Gateway, and has the same deployment options as API Gateway: software installation, or virtualized deployment in Docker containers. For more information on API Gateway, see the *API Gateway Release Notes*.

The software installation is available on Linux. For more details on supported platforms for software installation, see "System requirements" in the *API Gateway Installation Guide*.

Docker deployment is supported on Linux. For a summary of the system requirements for a Docker deployment, see "System requirements" in the *API Gateway Installation Guide*, and for more details see "What you need before you start" in the *API Gateway Container Deployment Guide*.

New features and enhancements

The following new features and enhancements are available in this release.

Elastic topology container deployment

The new elastic topology container deployment architecture brings flexibility to capacity planning.

- Deploy API Manager in Docker containers and use Kubernetes for container orchestration.
- Easily scale the capacity of your environment up or down to respond to changes in load.
- Auto healing to quickly start a new instance in case of a failure.

- Choose the deployment architecture best suited to your needs: in addition to elastic topology, API Gateway7.6.2 also supports the classic deployment architecture that uses Node Managers.
- Deploy configuration changes directly from Policy Studio to API Manager containers for development testing (supported in development environments only).
- Redirect the trace and traffic logs to `stdout` instead of to separate files. This allows the logs to be read directly from each container by an external logging service.
- Use Apache Cassandra as a distributed data store.

For more details, see the *API Gateway Container Deployment Guide*.

Global policy enforcement

This feature allows organizations and their governance teams to apply mandatory security, compliance, and governance policies, which are executed as part of every API call across their entire API portfolio. For more details, see "Advanced API administration tasks" in the *API Manager User Guide*.

Custom properties for APIs

API Manager has been enhanced to enable you to define custom properties for APIs, in the same way as you can define custom properties for applications, organizations, and users. For more information, see the *API Manager User Guide*.

Application credential alerts

The application credential alerts feature enables you to trigger alerts for any change to the credentials (API keys, OAuth credentials, or external credentials) associated with an application. For more information, see the *API Manager User Guide*.

Fault handling policies

This feature allows organizations and their governance teams to apply a fault handler policy at the global, API, and API method levels, so that it is executed when an error or exception occurs during runtime API invocation. For more information, see the *API Manager User Guide*.

API Manager configuration in Policy Studio

Use Policy Studio to easily configure API Manager instead of using the `setup-apimanager` script. For more details, see "Enable API Manager" in the *API Manager User Guide*.

Query-string based API versioning

In addition to the existing URL path based API versioning, API Manager now supports query string-based API versioning, giving flexibility in exposing API versions to API consumers.

- Protect client applications invoking APIs from being impacted by minor and patch changes.
- Use a global setting to define the query string variable name that specifies the API version that an application invokes.

For more details, see "Advanced API administration tasks" in the *API Manager User Guide*.

Method-level authorization

Method-level authorization increases the granularity in the access control for client applications.

- Control which client application can access which method.
- Restrict the number of applications authorized for write methods while still enabling the rest to access the read methods.

For more details, see "Advanced API administration tasks" in the *API Manager User Guide*.

Axway AMPLIFY menu

You can now connect to Axway services and Axway AMPLIFY platform straight from the API Manager UI. For more details, see Axway AMPLIFY™ Platform.

Limitations of this release

This release has the following limitations.

Elastic topology container deployment

When using an elastic container deployment:

- Traffic monitor data for a specific API Manager instance does not persist in the event of that instance container stopping. However, you can redirect the trace and traffic logs to `stdout` instead of to separate files, which allows the logs to be read directly from each container by an external logging service.
- Distributed Ehcache is not supported. However, you can use Apache Cassandra as a distributed data store.
- To upgrade from an earlier version to 7.6.2, you must first upgrade to a 7.6.2 classic deployment and then migrate to an elastic container deployment.

For more details, see the *API Gateway Container Deployment Guide*.

Other deployment options

This release is not available as a virtual appliance, or as a managed service on Axway Cloud.

Removed features

In our efforts to continually upgrade our products in response to the needs of our customers' IT environments, Axway occasionally discontinues support for some capabilities. API Manager 7.5.3 is the last release that includes the following capabilities, which have been removed from the 7.6.2 release:

- Axway physical appliance deployment option.
- API Manager on Windows servers. Only the following developer tools are available on Windows:
    - Policy Studio
    - Configuration Studio
    - Package and Deployment Tools

Fixed issues

API Manager 7.6.2 includes all fixes for 7.5.3 Service Packs up to and including 7.5.3 SP 7. For details of all the Service Pack fixes included in 7.6.2, see the corresponding *SP Readme* attached to each Service Pack on Axway Support at https://support.axway.com.

Known issues

The following are known issues for this release of API Manager.

Documentation might contain references to removed features

Documentation might contain references to removed features (for example, hardware or virtual appliances, or Windows support). This does not mean that the removed features are still supported, and the references should be ignored.

Cassandra synchronization in multi-datacenter environments

In multi-datacenter environments with Cassandra read/write consistency set to local quorum, there is a small risk of configuration corruption if the event triggering API Manager to load a configuration change happens before the configuration replication to the other datacenter is complete. Changing the polling time as described in "Configure API Management in multiple datacenters" in the *API Gateway Installation Guide* reduces this risk, but does not remove it completely.

This issue results in outdated configuration data being used for the affected API until API Gateway is restarted. For example, as a result of this, valid traffic may be rejected if a new API has been added and not updated, or wrong traffic may be accepted if an API has been deprecated and not updated. The workaround requires a restart of all API Gateway instances in the affected datacenter.

Axway is working on a product change that will avoid restarting API Gateway in such situations, and recommends to:

- Wait for the resolution before going live with multiple datacenters and local quorum consistency.
- If this is not possible, monitor your production environment closely for this error, and restart API Gateway if the error is encountered.

RAML import does not support references to external files

Importing RAML version 0.8 or RAML version 1.0 files that include references to external files is currently not supported.

Related issues: RDAPI-10356

Upgrade from API Manager 7.3.0 not supported

Upgrading API Manager version 7.3.0 to version 7.6.2 is not supported.

Related issues: RDAPI-5136, RDAPI-8237

API Manager users cannot complete registration after upgrading from 7.3.1

New users that were registered in API Manager 7.3.1 before an upgrade, but who did not complete registration by activating their account with the link provided in email, cannot complete registration after the upgrade. The link in the email references the API Manager API v1.1 that is no longer available. For example:

```
https://<API Gateway IP
address>/api/portal/v1.1/users/validateuser?email=s@s.com&validator=9a5addcb-
e10c-499b-bf0a-0c70915f3862
```

The workaround is that the user copies the link address, pastes it to the address bar, and changes the API version `v1.1` to `v1.2` or `v1.3`. After this, the activation link works, and the user can complete registration.

This issue does not occur when upgrading from API Manager 7.4.0 or later.

Related issues: RDAPI-3417

API Manager removes trailing slashes from the paths of APIs created from a Swagger definition file

When a back-end API is created from a Swagger definition file that contains trailing slashes in the path, API Manager removes the trailing slashes from the paths. Furthermore, when a request comes in with a trailing slash, API Manager returns HTTP error `403 bad request` because it does not match the requested path.

To preserve the trailing forward slashes, edit the `jvm.xml` file and set the `com.vordel.apimanager.uri.path.trailingSlash.preserve` system property to `true`. After updating the file, restart the API Manager instance to enable the changes to be applied.

For example:

```
<VMArg name="-Dcom.vordel.apimanager.uri.path.trailingSlash.preserve=true"/>
```

The default value of the property is `false`.

Related issues: RDAPI-9243

Unsupported Swagger 2.0 elements

When registering a back-end API from a Swagger 2.0 definition, API Manager does not support the following elements and does not import them into the API Catalog:

- `title`
- `termsOfService`
- `contact`
- `license`
- `tags`
- `securityDefinitions`
- `externalDocs`

For each path/API method:

- `tags`
- `security`

  For each parameter:

  - `default`
  - `maximum`
  - `exclusiveMaximum`
  - `minimum`
  - `exclusiveMinimum`
  - `maxLength`
  - `minLength`
  - `pattern`
  - `allowEmptyValue`
  - `collectionFormat`
  - `maxItems`
  - `minItems`
  - `uniqueItems`
  - `enum`
  - `multipleOf`

  For each response code:

  - `headers`

Note Some of these elements are also used in the model definitions section in the Swagger 2.0 specification, and API Manager imports these elements when contained in that section. API Manager supports all elements in the Swagger model definitions section.

Supported Swagger 2.0 elements

The following elements are supported and imported into the API Catalog:

- `description`
- `version`
- `host`
- `schemes`
- `basePath`

- Global `parameter`
- `produces`
- Model definitions

For each path/API:

- Path
- HTTP method
- Path `parameter` and reference to global `parameter`

  For each method:

  - `operationId`
  - `summary`
  - `description`
  - `consumes`
  - `produces`

  For each parameter:

  - `name`
  - `in`
  - `description`
  - `required`
  - `type`
  - `schema`
  - `format`
  - Reference to global or path `parameter`

  For each response code:

  - Response code
  - `description`
  - `schema`

Documentation

You can find the latest information and up-to-date user guides at the Axway Documentation portal at https://docs.axway.com.

This section describes documentation enhancements and related documentation.

Documentation enhancements

See *What's new in documentation* on page 24 for a summary of the documentation changes in this release.

Related documentation

The AMPLIFY API Management solution enables you to create, publish, promote, and manage Application Programming Interfaces (APIs) in a secure and scalable environment. For more information, see the *AMPLIFY API Management Getting Started Guide*.

The following reference documents are also available on the Axway Documentation portal at https://docs.axway.com:

- *Supported Platforms*

  Lists the different operating systems, databases, browsers, and thick client platforms supported by each Axway product.

- *Interoperability Matrix*

  Provides product version and interoperability information for Axway products.

Support services

The Axway Global Support team provides worldwide 24 x 7 support for customers with active support agreements.

Email support@axway.com or visit Axway Support at https://support.axway.com.

See "Get help with API Gateway" in the *API Gateway Administrator Guide* for the information that you should be prepared to provide when you contact Axway Support.

API Manager fixed issues

API Manager 7.6.2 includes all fixes for 7.5.3 Service Packs up to and including 7.5.3 SP 7. For details of all the Service Pack fixes included in 7.6.2, see the corresponding *SP Readme* attached to each Service Pack on Axway Support at https://support.axway.com.

Fixed security vulnerabilities

API Manager 7.6.2 fixed security vulnerabilities

Internal ID	Case ID	CVE Identifier	Description
RDAPI-11491	00925293	CWE-298	**Issue**: API Manager email registration links did not expire. **Resolution**: The email registration link is now only valid for 48 hours. An attempt to access the link after 48 hours will fail.
RDAPI-11678	00926874	CWE-319	**Issue**: API Manager static files such as registration-failed, request-forgotten-pw-failed, and so on, were accessible with all HTTP methods, which was reported as insecure during vulnerability testing. **Resolution**: The security vulnerabilities are no longer present when the system is upgraded or newly created.
RDAPI-12407	00917113	CWE-256	**Issue**: API collections exported from API Manager contain plain text credentials as they were exported as a plain text file by default. **Resolution**: When exporting API collections, the file is encrypted by default and you must supply a password.

API Manager 7.6.1 fixed security vulnerabilities

Internal ID	Case ID	CVE Identifier	Description

Internal ID	Case ID	CVE Identifier	Description
RDAPI-9120	00895727	CVE-2016-7103, CWE-79	**Issue**: Security vulnerability in JQuery. **Resolution**: Previously, API Gateway Manager and API Manager used JQuery 1.1.7, which is susceptible to a security vulnerability. Now, JQuery has been upgraded to JQuery 2.2.4, which is not susceptible to this security vulnerability.
RDAPI-10527	00906442	CWE-93	**Issue**: CRLF Injection in /api/portal/v1.3/discovery/ on the filename parameter. **Resolution**: Previously, the API Manager API allowed a CRLF Injection in `/api/portal/v1.3/discovery/` on the `filename` parameter. Now, there is no CRLF Injection allowed on the `filename` parameter in `/api/portal/v1.3/discovery/`.

API Manager 7.6.0 fixed security vulnerabilities

Internal ID	Case ID	CVE Identifier	Description
RDAPI-10444	00906442	CWE-209	**Issue**: Security vulnerability when creating an application. **Resolution**: Previously, error handling exposed information if you issued a `POST` request with invalid data to create an application in API Manager. Now, if you attempt to create an application using invalid data, API Manager shows you the correct error message and no information is exposed.

Internal ID	Case ID	CVE Identifier	Description
RDAPI-10525	00906442	CWE-384	**Issue**: Fixed user sessions in API Manager. **Resolution**: Previously in API Manager, it was possible to fix a user's session and once the user had logged in to API Manager use the predefined session to impersonate that user. Now, this is no longer possible, because API Manager regenerates the session ID for a user after the user logs in.
RDAPI-10563	00901852	CWE-913	**Issue**: API Manager static content files accessible without authentication. **Resolution**: Previously, the static content files on API Manager web UI could be accessed without user authentication. Now, the static content on all API Manager pages except the login page is fully protected in all *new* API Manager configurations. To protect non-login static content in *existing*API Manager configuration, you must run the `posix/bin/update-apimanager` script for each group in your topology to apply the protection configuration. It is recommended to back up your configuration before running the script.
RDAPI-10749	00906442	CWE-209	**Issue**: Security vulnerability when updating the `advisorybanner` API. **Resolution**: Previously, error handling exposed information if you issued a `PUT` request with invalid data in the request body to the `advisorybanner` API. Now, if you try to update the `advisorybanner` using invalid data, API Manager shows you the correct error message and no information is exposed.

Internal ID	Case ID	CVE Identifier	Description
RDAPI-10806	—	CVE-2017-1000048	**Issue**: Security vulnerability in the SDK generator. **Resolution**: Previously, the SDK generator in API Manager used the Node.js module `qs` v6.2.1 that contained a security vulnerability. Now, the Node.js version has been updated, and the security vulnerability is no longer present.
RDAPI-11424	00925709	CWE-79	**Issue**: Cross-site scripting (XSS) vulnerability in API Manager quota. **Resolution**: Previously, APIs in API Manager that exceeded their quotas reflected the original message body back to the client, causing a reflected XSS vulnerability. Now, when the API quota is exceeded, APIs do not send the message body back to the client. In addition, previously API Gateway was sending a `HTTP 403` response code when a resource path was not found. Now, API Gateway correctly sends a `HTTP 404` response code.

Other fixed issues

API Manager 7.6.2 other fixed issues

Internal ID	Case ID	Description
RDAPI-11801	00922991	**Issue**: API Version and State attributes not displayed in the APIs list on the Applications page in API Manager. **Resolution**: These attributes are now displayed in the APIs list on the Application page.

Internal ID	Case ID	Description
RDAPI-11895	00930929	**Issue**: API Manager user documentation did not state that unpublished APIs are only displayed to the owner's organization, and not to other organizations. **Resolution**: The documentation has been updated to clarify this.
RDAPI-11932	00927783	**Issue**: Korean characters (UTF-8) appearing as series of question marks (???) in API Manager registration emails. **Resolution**: All UTF-8 characters are correctly rendered in the registration email, provided the mail.mime.charset system property is set to "utf-8" using a jvm.xml file.
RDAPI-12016	00895802	**Issue**: API Manager did not return 400 Bad Request in the HTTP response status if JSON validation failed. **Resolution**: 400 Bad Request is returned in the HTTP response status if JSON validation fails.
RDAPI-12047	—	**Issue**: API Gateway less responsive when system entropy level is low. **Resolution**: API Gateway now makes fewer random number generation calls for path resolving per request, and responsiveness is improved. To further improve responsiveness, your Linux system administrator should resolve the low system entropy level.
RDAPI-12064	00926473	**Issue**: In a multi-node deployment, after registering a WSDL to API Manager the Download WSDL link only works for the first server, and the other servers must be restarted. **Resolution**: Download WSDL link works for all servers in a multi-node deployment without restarting.
RDAPI-12207	00944673	**Issue**: API Manager user documentation only explained how to customize password validation for the change password feature. **Resolution**: The documentation now also explains how to to customize password validation for the user registration feature.
RDAPI-12214	00912805, 00911974	**Issue**: Some sorting and filtering options did not work correctly in API Manager. **Resolution**: Issues with sorting and filtering have been fixed and you can now sort application developers and applications by organization and display all users and applications for a specific organization. Also, the link to the respective organization from the Application Developers and Applications pages now works correctly, and you can enable case-insensitive table sorting (sorting is case-sensitive by default).

Internal ID	Case ID	Description
RDAPI-12253	00940071	**Issue**: API outbound custom routing policies had to use a custom script to access authentication profiles to configure a Connection filter. **Resolution**: Authentication profile configurations are enabled for the Connection filter in API outbound custom routing policies.
RDAPI-12282	00941934	**Issue**: Failure reimporting an API collection that included APIs that were previously cloned and modified (methods deleted). **Resolution**: You can now successfully export and reimport an API collection that includes APIs that were previously cloned and modified.
RDAPI-12299	00924527	**Issue**: For a front-end API with an outbound authentication profile set up for SSL Client Certificate, where the certificate was malformed or corrupted, a MalformedURLException exception appeared in the API Gateway trace, but the corresponding front-end API was not listed in API Manager. **Resolution**: An exception appears in the API Gateway trace, and the corresponding front-end API name, organization name, and version are now listed in API Manager.
RDAPI-12375	00950002	**Issue**: If an API Manager session cookie was deleted, API Manager continuously looped on the login page. **Resolution**: If the session cookie is deleted, the server ensures that associated cookies are also deleted, and the user can log in successfully.
RDAPI-12399	00939103, 00948780, 00942725	**Issue**: Incorrect encoding of SOAP endpoint URI if the SOAP endpoint contained query parameters. **Resolution**: SOAP endpoints containing query parameters are encoded correctly.
RDAPI-12400	00948674	**Issue**: Outbound back-end service URL not displayed correctly in API Manager. **Resolution**: Outbound back-end service URL is now encoded correctly and displays correctly in API Manager.
RDAPI-12419	00934697	**Issue**: API method description containing special characters not displayed correctly in API Catalog. **Resolution**: Special characters are displayed correctly.

Internal ID	Case ID	Description
RDAPI-12441	00932805	**Issue**: API Manager reflected the request body in the response for 4xx errors. **Resolution**: API Manager no longer reflects the request body in the response.
RDAPI-12760	—	**Issue**: Back-end service URL contained a double slash if the base path ended in a single slash. **Resolution**: Back-end service URL no longer shows a double slash.
RDAPI-12842	00964971, 00964501	**Issue**: API Manager configuration settings accidentally overwritten with default settings when the process failed to read them. **Resolution**: API Manager reports an error when it fails to read configuration settings and the settings are not overridden.
RDAPI-12858	00962369, 00956154	**Issue**: Cannot edit front-end API per-method override if back-end API method contains multiple body parameters. **Resolution**: You can now edit the front-end API per-method override for methods with multiple body parameters. However, only the first body parameter is displayed, along with a warning message.
RDAPI-12906	00954793	**Issue**: Logo appeared in API developer registration email after being removed from email template. **Resolution**: The logo no longer appears in the email if it is removed from the template.
RDAPI-13124	00930932	**Issue**: Default response codes were added during import, even if they already existed, resulting in duplicate response codes. **Resolution**: Default response codes are only added during import if the response code does not currently exist for the method.
RDAPI-13132	00967330	**Issue**: Exception when API Manager tried to process a request that contained a JSON payload when an API method body parameter was optional. **Resolution**: API Manager correctly processes JSON payloads when an API method body parameter is optional.
RDAPI-13230	00967883, 00949233, 00950615	**Issue**: 64 bit integer path parameters were incorrectly validated as 32 bit integers and rejected. **Resolution**: 64 bit integer path parameters are correctly validated and passed through to the back-end.

Internal ID	Case ID	Description
RDAPI-13382	00959616	**Issue**: API Manager crashed when deleting a remote host that was created using another instance in the group. **Resolution**: Debug traces are logged when remote hosts are not found and API Manager no longer crashes.
RDAPI-13384	00971103	**Issue**: Downloading Swagger for different APIs with the same name resulted in the same file being downloaded (one of which was incorrect). **Resolution**: The correct Swagger file is downloaded for each API.
RDAPI-13689	00915348, 00931270	**Issue**: 'StatusCode 0' error occurred when using Try Method in API Manager for an API-key protected front-end API where no Javascript origins were configured. **Resolution**: When using Try Method for an API-key protected front-end API, you are now prompted to select an application and corresponding API key, which is validated before testing the API. If no JavaScript origin is configured, you cannot invoke the API, and the error does not occur.

API Manager 7.6.1 other fixed issues

Internal ID	Case ID	Description
RDAPI-10428	00901780	**Issue**: API key field name selector for two-way SSL inbound security in API Manager does not work. **Resolution**: Previously, when virtualizing a front-end API protected by two-way SSL, the selector configured in API Manager used to obtain the API key from the client certificate was ignored by the runtime, always defaulting to `${certificate.subject.CN}`. Now, the selector entered in API Manager is correctly picked up by the runtime. The selector support has also been expanded to include the client certificate Subject Alternative Name (SAN). The supported selectors are: `${certificate.san.othername}`, `${certificate.san.dns}`, `${certificate.san.email}`, `${certificate.san.rfc822name}`, `${certificate.san.dname.CN}`, and `${certificate.san.rid}`.

Internal ID	Case ID	Description
RDAPI-11255	00919428	**Issue**: API Manager HTTP error codes and messages. **Resolution**: Previously, the API Manager documentation did not describe the HTTP error responses. Now, the documentation includes this information.
RDAPI-11712	00930827	**Issue**: API Manager application image compression. **Resolution**: Previously, after importing an application, API, or image in API Manager, the image became blurred. Now, after importing in API Manager, these images are no longer blurred.
RDAPI-11976	00903673	**Issue**: Cannot unpublish an API with pending API access in API Manager. **Resolution**: Previously, in API Manager you could not unpublish an API that had pending API access against an application. Now, you can unpublish an API with pending API access against an application.
RDAPI-12019	00922245	**Issue**: API Manager behaves differently depending on whether a request sends an uppercase or lowercase O in the origin header. **Resolution**: Previously, CORS headers were forwarded to back-end APIs by API Manager if an uppercase O was used in the origin header, and were not forwarded if a lowercase O was used. Now, API Manager always removes CORS headers and does not send them to back-end APIs regardless of the case used in the origin header.
RDAPI-12183	00908268	**Issue**: API Manager application image disappears after edit. **Resolution**: Previously, after creating an application and adding an image, the image disappeared when you edited the application. Now, the image no longer disappears when you edit the application.

API Manager 7.6.0 other fixed issues

Internal ID	Case ID	Description
RDAPI-7218	00877344	**Issue**: Swagger file import causes error on the next deployment. **Resolution**: Previously, API Manager did not include mime type validation when you imported Swagger 2.0 files. This might result in importing invalid mime type that caused errors when the configuration was deployed to the API Manager group. Now, API Manager has mime type validation for Swagger 2.0 files to prevent importing invalid Swagger definitions.
RDAPI-7884	00882567	**Issue**: Problem with the back-end URL if the address location in WSDL ends with `/`. **Resolution**: Previously, if you imported a WSDL API that contained an address location ending with `/` character, the base path for the API was set incorrectly. Now, the base path is set correctly even when the address ends with `/`.
RDAPI-8407	00885591	**Issue**: `REQUIRED` fields return `HTTP 500` and no detailed error message. **Resolution**: Previously in API Gateway, if you called an API that had `REQUIRED` fields validated by an API Manager instance that did not exist, API Gateway returned `HTTP 500 Internal Server Error`. Now, API Gateway correctly returns `HTTP 400 Bad Request` indicating that the request was incorrect.
RDAPI-8778	00889273	**Issue**: Incorrect Swagger documentation. **Resolution**: Previously, the Swagger documentation for the API Manager REST API method `DELETE` did not correctly reflect the functionality of the method. Now, the Swagger documentation has been updated to better reflect the actual functionality of the `DELETE` method.
RDAPI-8815	00888306	**Issue**: Error messages from API promotion policy do not contain meaningful information. **Resolution**: Previously, when you used the API promotion policy to promote APIs, you did not get a meaningful error message in API Manager if the policy failed. Now, if you include the filter **Set Attribute** filter in the policy, you can use the attribute `errorMessage` to set a meaningful error message that is displayed in API Manager if the API promotion policy fails.

Internal ID	Case ID	Description
RDAPI-8921	00879346	**Issue**: API Manager ignores the query parameter string on SOAP endpoints. **Resolution**: Previously, when you imported an API web service definition into API Manager, API Manager ignored a query parameter in the `soap:address location` field, so the routing to the back-end URL was wrong. Now, the query parameter in the `soap:address location` field is retained on import, and the routing to the back-end URL remains correct.
RDAPI-8947	00895146, 00887470	**Issue**: No version number on an imported API. **Resolution**: Previously, when you re-imported an API collection that contained versioned APIs, API Manager did not correctly reflect the versioning after the re-import. Now, the correct API version is shown after the re-import.
RDAPI-8965	00894145	**Issue**: Wrong error code when calling a non-existent API. **Resolution**: Previously, API Gateway returned `HTTP 500 Internal Server Error` when calling an API that did not exist on API Manager. Now, API Gateway correctly returns `HTTP 404 Not Found`.
RDAPI-10063	00894818	**Issue**: The `setup-apimanager` script ignores the `--adminName` option. **Resolution**: Previously, you could not use the `--adminName` option in the `setup-apimanager` script to change the default user name of the API Manager administrator account when creating the account. Now, the `setup-apimanager` script handles the `--adminName` and `--adminPass` options correctly, and you can create the administrator user account with the credentials you want.
RDAPI-10209	00901367	**Issue**: Unable to use multiple values in a REST request query string parameter. **Resolution**: Previously in API Manager, you could not use multiple values in the query string parameter when sending a REST request to a virtualized API, because only one value was sent to the back-end service. Now, all query string values are sent to the back-end service, so you can use multi-value query string parameters.

Internal ID	Case ID	Description
RDAPI-10248	00884582	**Issue**: Mails on new user registrations not working as expected. **Resolution**: Previously, the approver mail on new users was not working as expected if both **Auto-approve user registration** and **Delegate user management** were switched off. The approver email was sent to the email address of the organization, and the approver was redirected to API Portal, or to API Manager if there was no API Portal. Now, if both **Auto-approve user registration** and **Delegate user management** are switched off, the approver email is sent to the email address of the API administrator, and the approver is redirected to API Manager. If **Delegate user management** is `ON`, the mail is sent to the email address of the organization.
RDAPI-10560	00930069, 00901347	**Issue**: Java exception when sending a `PATCH` request containing a JSON array. **Resolution**: Previously, when API Manager tried to process a request that contained JSON payload with a root array element, API Manager threw a `JSONException` and logged an error in the trace file. Now, API Manager correctly processes JSON payloads that contain a root array element.
RDAPI-10786	00905760, 00911323	**Issue**: Problem publishing two APIs with the same resource path. **Resolution**: Previously in API Manager, if you tried to create a front-end API duplicating a resource path already in use, API Manager displayed an error on invalid message and you could not save the front-end API. Now, you can save a front-end API with a duplicated resource path.
RDAPI-10809	00902220	**Issue**: API Manager Swagger files are inaccurate. **Resolution**: Previously, the query parameters that specific API Manager API endpoints accepted were not documented in the Swagger files. In addition, the Client Application Registry API was documented as part of the API Manager APIs. Now, the missing query parameters have been added to the Swagger files, and the Client Application Registry API is documented in its own Swagger file.
RDAPI-10992	00915443	**Issue**: Swagger APIs using regular expressions in paths fail after upgrading API Manager. **Resolution**: Previously, after you upgraded from API Manager 7.3.1 to v7.5.3 or later, requests to virtualized APIs were not correctly matched with the back-end API if the back-end API path contained regular expressions or multiple template variables. Now, API Manager correctly matches the requests with the back-end API.

Internal ID	Case ID	Description
RDAPI-11094	00908896	**Issue**: Application `state` marked optional, but is mandatory. **Resolution**: Previously in API Manager 7.5.3, if you tried to update an application and did not include the `state` information (marked optional) in the request, the updating the application failed. Now, the `state` field has been updated to be optional, and you can update an application without filling the field.
RDAPI-11186	00870827	**Issue**: API Manager removes forward-slashes from requests. **Resolution**: Previously, if you created a back-end API from a Swagger definition file that contained trailing forward-slashes (for example, because the back-end service expected them in the request), API Manager automatically trimmed the trailing forward-slashes from the requests to back-end services. Now, you can preserve the trailing forward-slashes by setting the following system property: `<VMArg name="-Dcom.vordel.apimanager.uri.path.trailingSlash.preserve=true"/>`
RDAPI-11257	00919374	**Issue**: Error in the Swagger documentation. **Resolution**: Previously, the Swagger documentation incorrectly stated that the type of the `appIds` parameters for `migrate/applications/export` endpoints is `query`. Now, the Swagger documentation correctly states that the type is `formData`.
RDAPI-11441	00912158	**Issue**: Application override quota not shown in API Manager. **Resolution**: Previously, if you had configured API Manager to use a multi-node Cassandra cluster and you tried to add a new quota to an application, the quota was not always created correctly. Now, the new quota is created correctly and is visible in API Manager.
RDAPI-11457	00918072	**Issue**: Internal server error when creating a front-end API. **Resolution**: Previously, when you created a front-end API from an imported Swagger definition that did not have the host and base path set, API Manager displayed an internal server error, and the created API was only visible after a refresh. Now, there is no internal server error and the front-end API is visible in API Manager right away.

Internal ID	Case ID	Description
RDAPI-11495	00908256	**Issue**: API administrator not notified on an unreachable email address in self-registration. **Resolution**: Previously, if a new user entered an unreachable email address when self-registering to API Manager or API Portal, the API administrator was not notified on the failed registration email. Now, the API administrator receives a notification if sending the registration email to the newly registered user fails.
RDAPI-11498	00918621	**Issue**: The `POST` method in API Manager REST API ignores the user type. **Resolution**: Previously, when you invoked the `POST` method in API Manager REST API to call to `/api/portal/v1.3/users/`, the method ignored the user type (`internal` or `external`) you specified and set the type to `internal`. Now, the `POST` method correctly sets the user type as you specify. The default user type is `internal`.
RDAPI-11509	00921767	**Issue**: Unable to upgrade an API using API Manager REST API. **Resolution**: Previously, if you tried to upgrade an API using the API Manager REST API, the code comments in the REST API to generate the API description incorrectly indicated that the *back-end* API ID should be used in the upgrade. Now, the code comments have been updated and correctly indicate that the *front-end* API ID should be used for the upgrade operation.

What's new in documentation

This topic describes the documentation changes in this release.

API Gateway

API Gateway Concepts Guide

- Restructured the API Gateway Analytics information and added links to the new *API Gateway Analytics User Guide*.

API Gateway Installation Guide

- Moved the Apache Cassandra administration topics to a new guide.
- Moved the Apache Cassandra installation topic into the API Manager *Installation* section.
- Updated the prerequisites and installation instructions for Apache Cassandra to state that 2.2.12 is the supported version.
- Updated the prerequisites with additional steps you must complete before installing or running API Gateway if your Linux system has the `/tmp` directory mounted with `noexec`.
- Restructured the API Gateway Analytics information and added links to the new *API Gateway Analytics User Guide*.

API Gateway Container Deployment Guide

- This is a new guide that describes how to deploy and run API Gateway and API Manager in containers and elastically scale the capacity up or down as required.

API Gateway Upgrade Guide

- Updated the topic on upgrading Apache Cassandra to describe how to upgrade from version 2.2.8 to 2.2.12.

- Restructured the API Gateway Analytics information and added links to the new *API Gateway Analytics User Guide*.

API Gateway Policy Developer Guide

- Updated the topic on configuring a JMS service to describe a new field that enables you to specify the maximum number of JMS sessions.
- Updated the topic on configuring a directory scanner to describe enhancements to the file processing settings.
- Restructured the API Gateway Analytics information and added links to the new *API Gateway Analytics User Guide*.

API Gateway Policy Developer Filter Reference

- Updated the topic on configuring an OCSP client filter to describe new options for time validation.
- Added information on how to insert an XML node containing a `namespace`.
- Restructured the API Gateway Analytics information and added links to the new *API Gateway Analytics User Guide*.
- Updated the topic on the Generic Error filter to describe new options for customized generic errors.
- Updated information on the Smooth Rate Limiting algorithm options.

API Gateway Administrator Guide

- Renamed the topic on running API Gateway as non-root to "Run API Gateway on privileged ports", and updated the topic to describe alternative options for adding API Gateway library paths to the system path.
- Updated the topic on Embedded ActiveMQ settings to describe new fields that enable you to specify the maximum memory and disk usage for ActiveMQ messages and to enable reporting of memory and disk usage.
- Updated the topic on traffic monitoring settings to describe new and updated fields that enable you to configure transaction file management.
- Added an appendix describing the open logging schema.
- Restructured the API Gateway Analytics information and added links to the new *API Gateway Analytics User Guide*.

API Gateway Apache Cassandra Administrator Guide

- This is a new guide that describes how to set up and use the Apache Cassandra database for API Manager and API Manager. It includes information on best practices and tuning, setting up high availability, and backup and restore.

API Gateway Analytics User Guide

- This is a new guide that describes how to set up and use API Gateway Analytics to monitor and report on message traffic between API Manager instances and services, remote hosts, and clients.

API Gateway OAuth User Guide

- Added information on deploying OAuth in Policy Studio. This replaces the `deployOauthConfig` script that was used in earlier versions.

API Gateway DevOps Deployment Guide

- Removed references to API Gateway server-side support for Windows.

API Gateway Developer Guide

- Restructured the API Gateway Analytics information and added links to the new *API Gateway Analytics User Guide*.

API Gateway Authentication and Authorization Integration Guide

- Added sections on Oracle Access Manager (OAM) integration and Oracle Entitlements Server (OES) integration

API Gateway Kerberos Integration Guide

- Added information on how to configure a delegation in Kerberos service principal.

API Gateway Key Property Store User Guide

- Added information on using the KPS scripting API.
- Added information on the `kpsadmin diagnostics` command, which you can use to help diagnose common KPS and Apache Cassandra configuration issues.

API Manager

API Manager User Guide

- Rewrote and restructured the information on API Manager single sign-on (SSO) to address user feedback and make the steps easier to follow. Added more detail on the mapping of SSO user roles to API Manager roles and organizations.
- Added a new topic on how to enforce API Manager global policies (for example, mandatory security, compliance, or governance policies).
- Added a new topic on how to add a fault handler policy at the global, API, and API method level.
- Added a new topic on how to create custom routing policies with API key, OAuth, and SSL outbound authentication.
- Restructured the guide and added a new section on advanced API administration use cases.
- Updated the topic on customizing API Manager with a new section on adding custom properties for APIs.
- Added information on application credential alerts.
- Updated the topic on registering REST APIs with clarification on unsupported web services features and more information on creating a REST API data model.