Axway API Gateway 7.6.2 Release Notes

Document version: 14 July 2020

Summary

API Gateway is available as a software installation or a virtualized deployment in Docker containers.

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 Gateway 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 Gateway 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*.

Daily rollover and purging of traffic monitoring data

Traffic monitor settings have been enhanced to include new transaction file management settings including daily rollover and purging options. For more information, see the *API Gateway Administrator Guide*.

Support for /tmp directory mounted with noexec

Support has been added for installing or running API Gateway on a Linux system which has the `/tmp` directory mounted with `noexec`. For more information, see the *API Gateway Installation Guide*.

Visual Mapper support for multiple schema inputs

API Gateway Visual Mapper now includes support for multiple schema inputs:

- The **Create Map** dialog has been updated to enable selection of multiple source schemas. The Visual Mapper **Data Map Editor** has been updated to allow designing a map relationship with multiple input schemas. For more details, see the *API Gateway Visual Mapper User Guide*.
- The **Execute Data Map** filter has been updated to support visual maps with multiple schema inputs. This provides for the mapping of message attributes to the inputs defined by the visual map. Previously, only the content body of a message was provided to the visual map for conversion. For more details, see the *API Gateway Policy Developer Filter Reference*.

kpsadmin diagnostics

A new `diagnostics` option has been added to the `kpsadmin` command to help diagnose common KPS and Apache Cassandra configuration issues. For more details, run `kpsadmin --help` or see the *API Gateway Key Property Store User Guide*.

OAuth configuration in Policy Studio

Use Policy Studio to easily configure API Gateway as an OAuth authorization server and OAuth resource server instead of using the `deployOAuthConfig` script. For more details, see "Deploy OAuth configuration" in the *API Gateway OAuth User Guide*.

Smooth rate limiting

The enhanced **Throttling** filter strictly enforces high volume over short interval rate limits with near zero error rate even under extremely high volumes.

- Use the new smoothing rate limiting algorithm with elastic topology deployment where the number of API Gateway instances handling requests can scale in and out very quickly.
- Match the rate limits with your load balancing strategy, and distribute them among the running instances equally (round robin).

For more details, see "Configure rate limiting" in the *API Gateway Policy Developer Guide* and "Throttling" in the *API Gateway Policy Developer Filter Reference*.

Axway AMPLIFY menu

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

Improved threat reporting

When ModSecurity blocks incoming requests, the threat report is saved in a message attribute that can, for example, be forwarded to third-party monitoring systems. For more details, see "Manage API firewalling" in the *API Gateway Administrator Guide*.

Policy Studio filter enhancements

This release contains several other filter enhancements:

- The **OCSP Client** filter has been enhanced to use improved time validation logic when validating OCSP responses.
- The **Connect to URL** filter has been enhanced with new fields that allow reading the response message body into API Gateway memory and releasing previously opened connections.

For more details, see the *API Gateway Policy Developer Filter Reference*.

Third-party library updates

The following third-party libraries have been updated:

- Apache Cassandra has been upgraded to version 2.2.12
- Log4j has been upgraded to version 2.8.2.
- Jython has been upgraded to version 2.7.1.

New documentation

This release contains the following new documentation.

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 Apache Cassandra Administrator Guide

- This is a new guide that describes how to set up and use the Apache Cassandra database for API Gateway 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 Gateway instances and services, remote hosts, and clients.

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 Gateway 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 Gateway 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 Gateway on Windows servers. Only the following developer tools are available on Windows:
    - Policy Studio
    - Configuration Studio
    - Package and Deployment Tools

The following capabilities have also been removed:

- The `ConnectToUrlFilter.removePreviousConnections=true` system property is no longer available. However, you can still configure this feature by enabling the **Release previously opened connection** option on each **Connect to URL** filter that requires this behavior.

Known issues

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

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.

Team development - Conflicts when adding dependencies between template projects

In Policy Studio, if you create a new common project from the Common Project template and a new API project from the API Project template and you try to add the API project as a dependent project of the common project, a conflict occurs.

This is due to an issue with the Axway PassPort repositories containing conflicting (randomly generated) password fields in the common and API projects.

As a workaround, use the Entity Explorer tool to set the value of the field `FIELD_KEYSTORE_PASSWORD` to the same value in both the common and API projects. For more information on using the Entity Explorer, see the *API Gateway Developer Guide*.

Related issues: RDAPI-11159

Upgrade - Changes in order of execution of database statements

If you are upgrading your API Gateway installation, and you are using a **Retrieve from or write to database** filter with multiple database statements in your old installation, you must review the ordering of the database statements after you upgrade.

In earlier versions of API Gateway multiple database statements were not executed in the order they were listed in the filter. Now, database statements are executed in the order they are listed in the filter. After upgrading you must ensure that multiple database statements are listed in the order they should be executed.

Related issues: RDAPI-11455

TLS for non-default JRE

If you select an alternative JRE instead of the default JRE during the installation and want to enable Cassandra to use TLS, you must install Java Cryptographic Extension (JCE) Unlimited Strength Jurisdiction policies for your JRE.

Save to File filter

The **Save to File** filter may cause up to 2% of the transactions to fail with the following error:

```
 java.lang.RuntimeException: No such file or directory. cannot remove
file '/path/to/filename'
```

This happens in the following cases:

- The **Save to File** filter is pointing to a directory where the number of files has already reached the set **Maximum number of files** limit.
- The **Save to File** filter is part of a policy that is under heavy concurrent load.

If this happens, it is recommended to use a periodic job scheduled at an appropriate frequency for the "housekeeping" of the directory, and not to rely on the **Save To File** filter to do this.

Related issues: RDAPI-7619

WebSocket protocol

- If you use `%h` in the Access Log initial string and your DNS configuration is not correct (for example, a name server configured on `/etc/resolv.conf` is not reachable), the HTTP Long Polling connections have a time delay at the API Gateway. WebSocket connections are not affected.
- Adding the same URL for a WebSocket path and a HTTP path is not supported. You get an error message if you try this in Policy Studio.

JWT filters

When you operate in FIPS mode, the implementation from the default, non-FIPS provider is invoked, if any of the following algorithms is selected in the **JWT Signing** filter:

- RSASSA-PSS using SHA-256 and MGF1 with SHA-256
- RSASSA-PSS using SHA-384 and MGF1 with SHA-384
- RSASSA-PSS using SHA-512 and MGF1 with SHA-512

To avoid this, disable the Bouncy Castle Crypto Provider in the `/system/conf/jvm.xml` file. When the JWT Signing filter with one of the above algorithms selected is called, the filter fails with the following error:

```
ERROR 18/Apr/2016:16:24:39.275 [4a48:17e014570200451f205ec316] java
exception:
com.vordel.circuit.jwt.JWTException: com.nimbusds.jose.JOSEException:
Unsupported RSASSA algorithm: SHA512withRSAandMGF1 Signature not
available
```

For more details, see the *API Gateway Policy Developer Guide*.

Related issues: RDAPI-3041

Add JSON Node filter displays redacted data in trace

When the **Add JSON Node** filter is used in an API Gateway policy, and redaction of JSON message content has been configured, sensitive redacted data in the JSON body is still displayed in the API Gateway trace log file. Regardless of the trace level, the redacted data should be hidden in the trace log when the message body has been processed by API Gateway.

Related issues: RDAPI-8227

Tips and tricks

Upgrade

- If you are upgrading your API Gateway installation, and you are using a **Scripting Language** filter in your old installation with the **Language** field set to `JavaScript (Rhino engine JRE7 and earlier)`, you must change the **Language** of the filter to `JavaScript` and ensure that the JavaScript syntax in the script conforms with Nashorn engine syntax. If you do not make these changes, the script continues to work in your new installation, but with a severe drop in performance. It is recommended to use Nashorn for all new development.
- After upgrading your API Gateway installation, it is recommended that you clear your browser cache before using any of the web UIs. See the documentation for your browser for information on how to clear the cache.

High availability

For more information and best practices when setting up a highly available (HA) API Gateway deployment, see the *API Gateway Apache Cassandra Administrator Guide*.

Multiple datacenters

- You must add external load balancer hosts to the Node Manager whitelist to ensure that they are accepted in each datacenter.
- You may need to increase the Node Manager timeout for longer API Gateway startup times in a multi-datacenter environment.
- You may need to increase the maximum received bytes per transaction to optimize performance in a multi-datacenter environment.

For more details, see "Configure API Management in multiple datacenters" in the *API Gateway Installation Guide*.

Performance

For best performance, we recommend:

- Always install the latest release and service packs to benefit from new improvements and features.
- Use HTTP 1.1 instead of 1.0 whenever possible to enable persistent connections.
- Use persistent connections throughout the entire stack, and overwrite the connection type with `keep-alive` whenever possible to avoid creating and dropping connections for each individual request.

- In a classic deployment, use Ehcache instead of KPS whenever possible, because data held in process memory is quicker to access. Note that Ehcache is not supported in a container deployment.
- Keep thread count reasonable. A good starting point to use as a rule of thumb is `initial latency (ms)* expected throughput (count) / 1000 ms = the number of threads (count)`. In HA deployment, you may want to account failure in one node. Note that the ratio of thread count and CPU cores impacts the latency. You may also want to consider horizontal scaling instead of vertical scaling.

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 39 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 Gateway fixed issues

API Gateway 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 Gateway 7.6.2 fixed security vulnerabilities

Internal ID	Case ID	CVE Identifier	Description
RDAPI-10496	—	CVE-2014-3566	**Issue**: API Gateway included IBM MQ JARs version 7.5.0.2 that are vulnerable to POODLE CVE-2014-3566. **Resolution**: API Gateway now includes version 7.5.0.8 of the IBM MQ JARs and is no longer vulnerable.
RDAPI-11728	00928470	CWE-538	**Issue**: It was possible to view Client Application Registry resource files (e.g. compressed JS files) without being logged in. **Resolution**: These files cannot be viewed without being logged in.
RDAPI-12332	—	CVE-2017-5645	**Issue**: Security vulnerability CVE-2017-5645 in Apache Log4j 2.8.1. **Resolution**: Log4j has been upgraded to 2.8.2 to mitigate the vulnerability.
RDAPI-12779	00963339	CVE-2018-7489	**Issue**: FasterXML jackson-databind component security vulnerability CVE-2018-7489 **Resolution**: This component has been updated to v2.9.5 to mitigate the vulnerability.
RDAPI-13175	00972709	CVE-2018-0739	**Issue**: OpenSSL security vulnerability CVE-2018-0739. **Resolution**: OpenSSL has been upgraded to v1.0.2.o to mitigate the vulnerability.

Internal ID	Case ID	CVE Identifier	Description
RDAPI-13700	—	CVE-2018-2938; CVE-2018-2964; CVE-2018-2941; CVE-2018-2942; CVE-2018-2972; CVE-2018-2973; CVE-2018-2940; CVE-2018-2952	**Issue**: API Gateway used a Java version that contained security vulnerabilities. **Resolution**: Java version has been updated to 8u181, which fixes the vulnerabilities.

API Gateway 7.6.1 fixed security vulnerabilities

Internal ID	Case ID	CVE Identifier	Description
RDAPI-11625	00929871	CVE-2017-5645	**Issue**: Log4j issue with serialized log events. **Resolution**: Previously, API Gateway used log4j v1.2 (EOL). Now, API Gateway uses log4j2 v2.8 only.
RDAPI-11687	00930798	CVE-2017-3735; CVE-2017-3736	**Issue**: OpenSSL 1.0.2k-fips. **Resolution**: Previously, API Gateway used OpenSSL 1.0.2k-fips. Now, API Gateway uses OpenSSL v1.0.2m-AXWAY-1.
RDAPI-12174	00943503	CWE-923	**Issue**: Oracle Critical Patch Update, January 2018. **Resolution**: Previously, API Gateway did not include Oracle Critical Patch Update, 16 January 2018. Now, API Gateway includes this update from Oracle.

API Gateway 7.6.0 fixed security vulnerabilities

Internal ID	Case ID	CVE Identifier	Description
RDAPI-8813	00888175	CVE-2017-3241	**Issue**: Security vulnerability in JRE version. **Resolution**: Previously, API Gateway used JRE version that included a security vulnerability. Now, the JRE version has been updated to v8u131 that fixes this vulnerability.
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 that is susceptible to a security vulnerability. Now, JQuery has been upgraded to JQuery 2.2.4 that is not susceptible to this security vulnerability.
RDAPI-9272	—	CVE-2017-5645	**Issue**: Security vulnerability in Apache Log4j. **Resolution**: Previously with Apache Log4j 2.8.1, if the TCP or UDP socket server received serialized log events from another application, it was possible to send a specially crafted binary payload that, when deserialized, could execute arbitrary code. Now, the Log4j dependency in API Gateway has been updated from v2.8.1 to v2.8.2 to fix this vulnerability.
RDAPI-9279	—	CVE-2016-7051	**Issue**: Security vulnerability in Jackson XML dataformat component. **Resolution**: Previously, the `XmlMapper` in the Jackson XML dataformat component allowed remote attackers to conduct server-side request forgery (SSRF) attacks using vectors related to a document type definition (DTD). Now, the `com.fasterxml.jackson.dataformat` has been updated to v2.7.8 to fix this vulnerability.

Internal ID	Case ID	CVE Identifier	Description
RDAPI-11215	00921329	CVE-2017-12972, CVE-2017-12973, CVE-2017-12974	**Issue**: Security vulnerabilities in the JWT library. **Resolution**: Previously, API Gateway used the Nimbus JOSE+JWT library v4.27 that contained security vulnerabilities. Now, the version of the library has been upgraded to v4.41.2 that fixes these vulnerabilities.
RDAPI-11267	—	CVE-2017-9801	**Issue**: Security vulnerability in `commons-email-1.2.jar`. **Resolution**: Previously, API Gateway used `commons-email-1.2.jar` that contains a security vulnerability. When a call-site passed a subject for an email containing line-breaks, the caller could add arbitrary SMTP headers. Now, API Gateway uses `commons-email-1.5.jar` instead to fix this issue.

Internal ID	Case ID	CVE Identifier	Description
RDAPI-11319	00925133	CVE-2017-10346, CVE-2017-10285, CVE-2017-10388, CVE-2017-10309, CVE-2017-10274, CVE-2017-10356, CVE-2017-10293, CVE-2017-10342, CVE-2017-10350, CVE-2017-10349, CVE-2017-10348, CVE-2017-10357, CVE-2016-9841, CVE-2016-10165, CVE-2017-10355, CVE-2017-10281, CVE-2017-10347, CVE-2017-10386, CVE-2017-10380, CVE-2017-10295, CVE-2017-10341, CVE-2017-10345	**Issue**: Security vulnerabilities in JRE. **Resolution**: Previously, API Gateway used JRE version 1.8.0_141-b15 that contained several security vulnerabilities. Now, JRE has been upgraded to v1.8u152 that fixes these vulnerabilities.

Internal ID	Case ID	CVE Identifier	Description
RDAPI-11781	—	CVE-2015-6420	**Issue**: Security vulnerability in Apache `commons-collections.jar`. **Resolution**: Previously, API Gateway used Apache `commons-collections.jar` v3.2.1 that has known vulnerabilities. Now, the `commons-collections.jar` has been updated to v3.2.2 that addresses the known vulnerabilities.

Other fixed issues

API Gateway 7.6.2 other fixed issues

Internal ID	Case ID	Description
RDAPI-9462	00900505	**Issue**: Cannot change trace level dynamically using API Gateway Manager if you have multiple HTTP interfaces listening on the same port but with different IP addresses. **Resolution**: API Gateway Manager now stores port and IP address to differentiate interfaces listening on the same port.
RDAPI-11038	00915537	**Issue**: API Gateway Manager shows only the last 50 events by default, and this could not be increased. **Resolution**: The default has been increased to 100 events, and you can change that default using the environment settings property env.METRICS.EVENTS.MAX.
RDAPI-11052	00883448	**Issue**: Directory Scanner exhausting system resources by triggering too many policies at the same time. **Resolution**: Directory Scanner settings have been improved to control the maximum of simultaneous workers and the maximum number of files processed on each scan.
RDAPI-11235	00921670	**Issue**: Missing information on storage and encryption of API Manager user passwords. **Resolution**: The Security Guide has been updated to include information on how API Manager user passwords are stored and encrypted.

Internal ID	Case ID	Description
RDAPI-11657	00948214, 00949201, 00930447	**Issue**: API Gateway using ModSecurity 2.8. **Resolution**: ModSecurity has been upgraded to version 2.9.2.
RDAPI-12211	00941727	**Issue**: LDAP sample policies in Policy Studio not using SSL only or HTTP only options. **Resolution**: The sample policy (Node Manager > Protect Management Interfaces (LDAP) policy > Create Session filter) now uses the 'Session sent over SSL only' and 'HTTP Only cookie' options.
RDAPI-12218	00946105	**Issue**: Some user actions were being written to the audit log with N/A instead of the user name. **Resolution**: The user actions are now displayed in the audit log with the user name that performed the action.
RDAPI-12236	00945954	**Issue**: Help text for the deploy_fragment script was incomplete. **Resolution**: Help text for the deploy_fragment script has been updated to inform the user that an <addOrReplace> tag can be used to overwrite existing configuration.
RDAPI-12242	00928619	**Issue**: Visual Mapper conversion of XML with an array to a JSON array produced a blank JSON array. **Resolution**: Visual Mapper conversion of XML with an array to a JSON array produces a correct JSON array.
RDAPI-12294	00949329	**Issue**: Incorrect location of venv script in Administrator Guide. **Resolution**: The Administrator Guide has been updated with the correct location of the venv script in posix/lib.
RDAPI-12337	00926083	**Issue**: Trace level logging not appearing for WebSocket server to client communication. **Resolution**: Trace level logging now works as expected for Websocket server to client communication.
RDAPI-12343	00929972, 00924335, 00926504	**Issue**: The documentation on configuring Cassandra HA advised running the setup_apimanager script after the HA steps, which caused synchronization errors. **Resolution**: The documentation has been updated to remove this advice.

Internal ID	Case ID	Description
RDAPI-12351	00949828	**Issue**: Archiving metrics tables using the dbpurger script sometimes resulted in a concurrency error. **Resolution**: The script has been updated and the concurrency error no longer occurs.
RDAPI-12352	00951489	**Issue**: License generator cannot generate 7.6.x licenses. **Resolution**: The license generator has been updated to generate 7.6.x licenses.
RDAPI-12370	00942279	**Issue**: Some selectors did not work when used in the username and password fields in the Configure Database Connection dialog in Policy Studio. **Resolution**: Any valid selector can now be used in this dialog.
RDAPI-12394	00946452	**Issue**: The first message to be processed by a Data Map takes too long. **Resolution**: Removed the URL resolving when initializing a Data Map so that initialization of the Data Map is much quicker.
RDAPI-12408	00951136, 00952492	**Issue**: API Gateway server crash when an empty transaction stream is viewed from API Gateway Manager. **Resolution**: Updated the REST API to return an empty response, and the crash no longer occurs.
RDAPI-12436	00949082	**Issue**: Not possible to use general selectors when specifying custom attributes to include in the transaction event log. **Resolution**: You can now use any selector value when specifying custom attributes to include in the transaction event log.
RDAPI-12452	00930133	**Issue**: When extracting attributes from a SAML assertion, attributes could be mistakenly read from a second assertion nested underneath the first. **Resolution**: Attributes are always read from the correct SAML assertion.
RDAPI-12462	00950159	**Issue**: Updating KPS records containing encrypted strings longer than 56 characters corrupts the record. **Resolution**: Updating KPS records containing encrypted strings longer than 56 characters now works as expected.
RDAPI-12516	00945351	**Issue**: XACML PEP filter inserts duplicate SOAPAction and Content-Type headers in each XACML request. **Resolution**: The filter now inserts only one header of each type.

Internal ID	Case ID	Description
RDAPI-12520	—	**Issue**: Two separate installations of same API Gateway version can create library conflicts and the vshell process could crash. **Resolution**: The vshell binary now checks for possible conflicts between its runtime directory and possible extern installation path contained in its own RPATH attribute, and exits with an error if a conflict is detected.
RDAPI-12522	00955307	**Issue**: Documentation for integrating Oracle (OAM and OES) with API Gateway was not published. **Resolution**: This documentation is now published in the Authentication and Authorization Integration Guide.
RDAPI-12538	00950845	**Issue**: Remote hosts were deleted but not removed from the internal search subnet search tree, which could result in a segmentation fault when redeploying a configuration using Remote Hosts configured to cover subnet. **Resolution**: Deleted entries are correctly removed from the internal search tree.
RDAPI-12553	00970764, 00958733, 00955055	**Issue**: Crash occurring with XML redaction when an XML tag attribute has an empty value. **Resolution**: Empty attribute values (either '' or "") are now correctly handled and the crash does not occur.
RDAPI-12577	00948561	**Issue**: Memory leak in API Gateway native code when running load test. **Resolution**: The cause of the memory leak was a temporary buffer that was not released. The temporary buffer is now released and the memory leak does not occur.
RDAPI-12676	00955133	**Issue**: Message Size filter did not allow selectors to be used for minimum or maximum size, and did not allow you to specify sizes greater than 2 GB. **Resolution**: You can now use selectors for minimum or maximum size, and you can specify sizes greater than 2 GB.
RDAPI-12703	00953858	**Issue**: When API Gateway was shutting down or a new configuration was deployed, a Java exception was sometimes logged from Directory Scanner. **Resolution**: This exception no longer occurs when deploying a configuration containing a Directory Scanner.

Internal ID	Case ID	Description
RDAPI-12761	00894028	**Issue**: Incorrect timestamps in file names of scheduled reports from API Gateway Analytics. **Resolution**: Timestamps in file names are set correctly to the report generation time.
RDAPI-12771	00920016, 00922717	**Issue**: When setting up API Gateway Analytics with LDAP the browser authentication dialog appears twice. **Resolution**: The error that triggered the second authentication dialog is no longer returned and the second dialog does not appear.
RDAPI-12797	00955335	**Issue**: Documentation did not make it clear that application quotas are not enforced when pass through inbound authentication is used. **Resolution**: Documentation has been updated to clarify this.
RDAPI-12800	00960972	**Issue**: API Manager alert policies cannot be environmentalized in Policy Studio. **Resolution**: Alert policies can be environmentalized and Environment Settings includes the environmentalized fields.
RDAPI-12809	00957296	**Issue**: Cannot enable zero downtime deployment (ZDD) in Policy Studio projects with dependencies. **Resolution**: You can now successfully update ZDD settings in projects with dependencies.
RDAPI-12818	00965142	**Issue**: Documentation did not state that the metrics database must have transaction isolation set to READ COMMITTED. **Resolution**: Documentation has been updated to state that this setting is required for all supported third-party databases.
RDAPI-12873	00956525	**Issue**: Throttling filter sometimes failed to return the HTTP headers showing the remaining limit. **Resolution**: The headers showing the remaining limit are always returned if the option to include them is selected.
RDAPI-12877	00967786	**Issue**: Broken SOAP web service link in documentation. **Resolution**: Documentation has been updated to remove the broken link and to advise users to adapt the example.
RDAPI-12905	00968545	**Issue**: Unnecessary log file velocity.log generated when emails were sent from API Manager. **Resolution**: This unnecessary file is no longer generated.

Internal ID	Case ID	Description
RDAPI-12983	00950692	**Issue**: Configuration deploy breaks distributed Ehcache operations. **Resolution**: A delay is introduced between recreating the Ehcache manager and the caches to resolve this issue. The default value of the delay is 5 seconds, and you can configure it using the system property: distributed.ehcache.cache.reload.pause.secs.
RDAPI-13064	00956041	**Issue**: Audit log events not logged correctly for some CRUD events (remote host, application, back-end API, front-end API). **Resolution**: Audit log events are logged correctly for all CRUD events.
RDAPI-13156	00969873	**Issue**: Threat protection properties did not allow you to implement OWASP Modsecurity CRS version 3.x rules without using a workaround, as the configuration files needed to be loaded in a specific order. **Resolution**: The ModSecurity implementation in API Gateway now loads the files in the order specified by the OWASP documentation.
RDAPI-13216	00964592	**Issue**: JSON Add Node filter with replace options throwing exception when applied to a document root ($). **Resolution**: The specified content is successfully applied to root and the exception does not occur.
RDAPI-13272	00976475	**Issue**: JWT Verify filter does not support JWK-Sets with multiple certificates. **Resolution**: Support has been added to the JWT Verify filter.
RDAPI-13283	00977414, 00972585	**Issue**: managedomain -v reports errors with patch file jars not found in ext/lib due to extra whitespace in files. Reolution: managedomain -v is more tolerant of extra spaces in ID files and does not report errors.
RDAPI-13294	00966762	**Issue**: Cannot change the trace level on Node Manager or API Gateway Analytics configurations using Policy Studio. **Resolution**: The trace level can now be modified.
RDAPI-13350	00979267	**Issue**: API Gateway did not check if the Cassandra keyspaces were already configured before trying to create them. **Resolution**: Pre-existing keyspaces are now detected correctly, which allows the use of a non-superuser Cassandra user.

Internal ID	Case ID	Description
RDAPI-13386	00972252	**Issue**: WebSocket traffic is not logged to Transaction Access Log even when enabled. **Resolution**: WebSocket traffic is correctly logged to the Transaction Access Log, and WebSocket traces are printed at level DEBUG instead of INFO.
RDAPI-13426	00980017	**Issue**: Open traffic log maximum disk space was limited to 2047 MiB even if a higher value was specified. **Resolution**: Maximum disk space is no longer limited and the specified value is used.

API Gateway 7.6.1 other fixed issues

Internal ID	Case ID	Description
RDAPI-9088	00896467	**Issue**: Add details on Cassandra debug logging to documentation. **Resolution**: Previously, the *API Gateway Installation Guide* did not include details on how to enable Apache Cassandra debug logging. Now, the Installation Guide is updated to include a new section on Cassandra debug logging.
RDAPI-11071	00909499	**Issue**: Connect to URL filter returns 500 Internal Server Error instead of 504 Gateway Timeout. **Resolution**: Previously, when the Connect to URL filter timed out, it returned an HTTP code 500 General Server Error to the client. Now, it returns a 504 Gateway Timeout error code.
RDAPI-11161	00917233	**Issue**: Default limits for transaction and trace file size are too low. **Resolution**: Previously, the default limits for API Gateway transaction size and trace file size were too low. Now, the default value for `maxRequestMemory` have increased to 26 MiB, and the default values for `maxInputLen` and `maxOutputLen` have increased to 20 MiB.

Internal ID	Case ID	Description
RDAPI-11522	00923675	**Issue**: :Policy Studio very slow to load or modify exported policy. **Resolution**: Previously, loading a policy containing a large number of filters and multiple paths to several filters might take a long time. Now, you can use a hidden Java property to speed up the policy loading at the cost of a potentially inaccurate list of filter attributes. You can add the `-DfastCoverage=true` property to the `policystudio.ini` file to skip revisiting filter success or failure paths.
RDAPI-11705	000929803	**Issue**: KPS Cassandra consistency level not working correctly in API Gateway Manager. **Resolution**: Previously, consistency levels specified in Policy Studio for Apache Cassandra were ignored. Now, consistency levels are considered for rate limiting, KPS, and quota on a per table basis.
RDAPI-11755	00931396	**Issue**: Attribute highlighting on Policy Studio canvas incorrectly shows kps attributes as missing. **Resolution**: Previously, attribute highlighting did not work correctly for `${kps.` attributes. Now, attribute highlighting works as expected.
RDAPI-11849	00933271	**Issue**: API Gateway crash occurs during redaction of XML content. **Resolution**: Previously, a crash might occur when executing multiple XML redactions simultaneously. Now, multi-threading operations are fully supported by XML redaction.
RDAPI-11954	00906226	**Issue**: JSON Path filter out attributes do not refresh when using Show all Attributes. **Resolution**: Previously, the JSON path filter's out attributes were not shown when using **Show All Attributes**. Now, the attributes are shown when **Show All Attributes** is enabled.
RDAPI-11957	00933410	**Issue**: Environmentalized fields in Policy Studio not migrated. **Resolution**: Previously, you could environmentalize a field with no values in Policy Studio, or set no values for an environmentalized field. Now, you cannot environmentalize a field with no values, or set no values for an environmentalized field (the field's default values are set when available).

Internal ID	Case ID	Description
RDAPI-11963	00929436	**Issue**: API Gateway freeze during startup. **Resolution**: Previously, during startup, instantiation of several JMS sessions and JMS consumers at the same time could cause deadlock. Now, locks used by JMS sessions have been removed.
RDAPI-12008	00934883	**Issue**: XML Signature Generation filter not compliant with WS-I Basic Security Profile 1.0. **Resolution**: Previously, the X.509 TokenType was not set in the `SecurityTokenReference` tag. Now, the X.509 TokenType is set if requested.
RDAPI-12029	00910357	**Issue**: Secure WebSocket communication may freeze when transferring large payload. **Resolution**: Previously, API Gateway could stop reading a large payload over WebSockets when SSL security was used. Now, the WebSocket layer no longer directly relies on socket events when receiving payload data.
RDAPI-12031	00940228	**Issue**: Documentation for all fields in the transaction event logs. **Resolution**: Previously, the documentation did not fully describe the fields in transaction event log entries. Now, the documentation describes these fields.
RDAPI-12056	00941806, 00942881	**Issue**: init.d scripts may not reliably start API Gateway under load. **Resolution**: Previously, `init.d` scripts were exiting without verifying if the API Gateway process was stopped and used ports were free. Now, they wait until the process is killed and ports are free.

RDAPI-12078	00941719	**Issue**: managedomain command-line help not intuitive for metrics_enabled command
		Resolution: Previously, the `managedomain` command help displayed:
		`--metrics_enabled=METRICS_ENABLED Controls whether metrics data collection is enabled or not.`
		Now, the command help is more intuitive:
		`--metrics_enabled=METRICS_ENABLED Specifies whether writing of metrics data is enabled. Enter y or n.`

Internal ID	Case ID	Description
RDAPI-12211	00941727	**Issue**: Modification needed in LDAP Sample Policies\Protect Management Interfaces (LDAP). **Resolution**: Previously, in Policy Studio under **Node Manager** > **Protect Management Interfaces (LDAP)** policy > **Create Session** filter, the **Session sent over SSL only** and **HTTP Only cookie** check boxes were not selected. Now, both of these check boxes are selected.
RDAPI-12225	00942441	**Issue**: API Management support for Python 2.7.5 with Cassandra on CentOS. **Resolution**: Previously, the *API Gateway Installation Guide* incorrectly stated that Python 2.7.10 was required for Apache Cassandra. Now, this guide has been updated to state that 2.7.x is required (up to 2.7.10 for Cassandra 2.2.5, and up to the latest 2.7 version for Cassandra 2.2.8).

API Gateway 7.6.0 other fixed issues

Internal ID	Case ID	Description
RDAPI-5937	00860502	**Issue**: Base64 encoder script issue and non-standard Java classes. **Resolution**: Previously, the Base64 encoder script in Policy Studio made an RFC 1521 or MIME legal result by adding line breaks every 76 characters. This was not compatible with URL encoding, because URL decoder script could not handle the line breaks correctly. In addition, the Base64 encoder and decoder scripts were using non-standard Java classes. Now, the Base64 encoder script does not add the line breaks anymore, and the Base64 encoder and decoder scripts use standard Java classes.
RDAPI-7282	00874107	**Issue**: HTTP status code missing from access logs. **Resolution**: Previously, if you enabled the transaction access logging for a policy where you had set the status code option, the status code was not shown in the access log file. Now, the status code is correctly shown in the access log file.

Internal ID	Case ID	Description
RDAPI-7620	00881441	**Issue**: The Analytics Reports API returns stack trace in the response body. **Resolution**: Previously, responses to certain bad requests (for example, invalid JSON) contained stack trace information. Now, the stack trace information has been replaced with a more generic response.
RDAPI-8481, RDAPI-9414	00888407	**Issue**: Policy references incorrect after copying a policy container. **Resolution**: Previously in Policy Studio, when you copied a policy container that referenced other policies in the same container, the policy references in the **Policy Shortcut** and **Policy Shortcut Chain** filters were not updated to point to the new copy of the container. Instead, the policy references continued to point to the original container. Now, the original behavior has been restored. When you copy a policy container, the policy references are updated to point to the new container, not the original container.
RDAPI-8507	00895453	**Issue**: `Sysupgrade export` and `apply` commands fail if the Admin Node Manager is not listening on address "`*`". **Resolution**: Previously, the `sysupgrade` script failed if the Admin Node Manager was listening on a specific IP address. Now, `sysupgrade` succeeds even if the Admin Node Manager is listening on a specific IP address. **Note** Ensure the following entry is not included in `/etc/hosts` file: `127.0.1.1 hostname`
RDAPI-8559	00868410	**Issue**: Request fails when the HTTP body has an unknown `Content-Transfer-Encoding` mechanism. **Resolution**: Previously, API Gateway threw a `java.lang.Error` exception when writing the body of a request that contained an unhandled `Content-Transfer-Encoding` value. Now, API Gateway ignores unknown `Content-Transfer-Encoding` and treats the value as `binary`.
RDAPI-8572	00884739	**Issue**: OAuth tokens stored in cleartext when using a database-backed OAuth store. **Resolution**: Previously, the OAuth refresh tokens not encrypted with a system passphrase contained sensitive data in serialized blobs. Now, the data has been redacted, so the plain text blobs are safe.

Internal ID	Case ID	Description
RDAPI-8617	00876429	**Issue**: Cannot use a selector in the **Read from JMS** filter. **Resolution**: Previously, you could not use a selector in the **Read timeout(ms)** field in the **Read from JMS**filter, the deployment failed if you tried to do this. Now, you can use a selector in the **Read timeout(ms)** field of the **Read from JMS** filter, and deployment succeeds.
RDAPI-8630	00883283	**Issue**: The filter **Validate REST Filter** does not handle URL encoded path parameters correctly. **Resolution**: Previously, the filter **Validate REST Filter** did not handle URL encoded path parameters correctly and failed if a path parameter contained, for example, URL encoded slash character. Now, the filter can be configured to handle URL encoded path parameters correctly. For more details, see *API Gateway Policy Developer Filter Reference*.
RDAPI-8745	00888804	**Issue**: Enabling threat protection on an interface prevents API Gateway from serving static files. **Resolution**: Previously, when you enabled threat protection on an interface, API Gateway could not access static content. Now, the threat protection mechanism correctly parses requests to static content and responses are sent back to API Gateway.
RDAPI-8795	00889541	**Issue**: HTTP responses containing intermediary `HTTP 100 Continue` responses not displayed correctly in the Traffic Monitor log. **Resolution**: Previously, if a received response contained `HTTP 100 Continue`, you did not see any response headers in the **Response** column in Traffic Monitor. Now, API Gateway Manager skips all `HTTP 100 Continue` responses, and you can see the final response headers in Traffic Monitor.
RDAPI-8943	00893117	**Issue**: Upgrade with Key Property Store (KPS) overrides fails. **Resolution**: Previously, if you tried to upgrade from an older configuration that contained KPS tables overriding the default Cassandra datasource, the upgrade process failed. Now, the upgrade completes and the datasource references are updated correctly.

Internal ID	Case ID	Description
RDAPI-8958	00876470	**Issue**: Client certificate fails when CA certificates have the same name. **Resolution**: Previously, you could not use several CA certificates with the same Subject Distinguished Name (DName) but different Subject Key Identifiers. API Gateway was unable to build the correct certificate chain, and mutual authentication failed. Now, API Gateway can verify certificates against CA certificates with the same Subject DName but different the Subject Key Identifiers, and mutual authentication succeeds.
RDAPI-8959	00893563	**Issue**: A Groovy scripting filter fails. **Resolution**: Previously in Policy Studio, if you tried to use the `com.vordel.mime.XMLBody` class in a Groovy script, the scripting filter threw a `ClassNotFoundException` error. Now the filter behaves as expected, no error is thrown, and the script is persisted.
RDAPI-8997	00892824	**Issue**: Unnecessary legacy file. **Resolution**: Previously, API Gateway shipped with the `system/conf/truststore.xml` file. Now the file has been removed because API Gateway does not use it anymore.
RDAPI-9125	00891076	**Issue**: Error in the dialogs of relative path types. **Resolution**: Previously, when you added a relative path attribute, the environmentalization action was erroneously shown as enabled in the **Static Content Provider**, **Static File Provider** and **Servlet Application** dialogs. Now, the dialogs have been fixed and the environmentalization action is disabled.
RDAPI-9187	00889639	**Issue**: `REMOTE_ADDR` has incorrect value when Apache ModSecurity rules are evaluated. **Resolution**: Previously, API Gateway was not always setting correct remote IP address for Apache ModSecurity, and the threat protection rules with `REMOTE_ADDR` did not work as expected. Now, API Gateway sets the correct remote IP address for ModSecurity, and the threat protection rules work as expected.
RDAPI-9193	00897169	**Issue**: Payload data that Open Traffic Event Log records can get corrupted. **Resolution**: Previously, the Open Traffic Event Log used asynchronous file write operation including buffers that could get corrupted or overwritten. Now, file write operations are performed synchronously so that the buffers do not get corrupted.

Internal ID	Case ID	Description
RDAPI-9228	00891478	**Issue**: Encoding issue with the **Connect to URL** filter and Amazon Web Services (AWS) V4 signing. **Resolution**: Previously, when encoding parameters for AWS V4 signing, certain values were being incorrectly encoded. Now, encoding has been updated to ensure it complies with the AWS requirements.
RDAPI-9231	00813372	**Issue**: The `dbpurger` script fails with a `NullPointerException` error when used with the `dbname` parameter. **Resolution**: Previously, the `dbpurger` script was incorrectly trying to use the parameter `dburl` instead of the provided parameter `dbname`. Now, the `dbpurger` script correctly handles the parameter `dbname` and searches the configuration for the corresponding URL to use.
RDAPI-9237	00893615	**Issue**: Failures in the **Set Attribute** filter not handled correctly. **Resolution**: Previously, if the **Set Attribute** filter referenced an attribute but the attribute's value was `null` because of a non-existent KPS table, a `NullPointerException` error was logged in the API Gateway trace and the policy execution was aborted. Now, there is no `NullPointerException` error and the policy execution proceeds.
RDAPI-9253	00890176	**Issue**: Environmentalized passwords not saved when project has a passphrase. **Resolution**: Previously in Policy Studio and Configuration Studio, if a project had a passphrase, the environmentalized values of the encrypted fields, like passwords, were not saved. Now, the values of these fields are saved and the correct password cipher retained.
RDAPI-9367	00896183	**Issue**: Not enough information in the trace log on OpenSSL remote host connection failure. **Resolution**: Previously, if you were using OpenSSL to connect to a remote host and your DH key was too short, the connection failed, and the API Gateway trace log did not contain enough information to understand why the connection to a remote host was failing. Now, the API Gateway trace log contains more information on this connection error to help troubleshoot this.

Internal ID	Case ID	Description
RDAPI-9505	00900981	**Issue**: The **XML to JSON** filter fails when XML encoding is set to `utf-8`. **Resolution**: Previously, the **XML to JSON** filter failed if the XML encoding in the XML body was lowercase `utf-8` instead of the uppercase `UTF-8`. This was caused by `sjsxp-1.0.jar` in the libraries. Now, the `sjsxp-1.0.jar` has been removed, and the lowercase XML encoding `utf-8` no longer causes the**XML to JSON** filter to fail.
RDAPI-9692	00901696	**Issue**: Parameters path attribute cannot be use as a stylesheet parameter in the **XSLT Transformation** filter. **Resolution**: Previously, if you used a `params.path.XXX` attribute as a stylesheet parameter in the **XSLT Transformation** filter, it caused a `java.lang.IllegalArgumentException`. Now, the attribute evaluation has been updated to support non-string object types.
RDAPI-10159	00901619	**Issue**: Large query strings cause API Gateway to crash. **Resolution**: Previously, the OpsDB component in API Gateway caused the API Gateway to crash if an HTTP request contained excessively long query string. Now, all attempts to write any type of data of any size to the OpsDB component that *previously* led to the crash or unexpected behavior in API Gateway are prevented. This also prevents data corruption and improves error handling when reading JSON data from the OpsDB.
RDAPI-10202	00901498	**Issue**: No error when retrieving content exceeding the maximum transaction size. **Resolution**: Previously, if the **Connect To URL** filter tried to retrieve content exceeding the maximum transaction size you had defined, API Gateway did not fail the policy or report an error. Instead it truncated data after the maximum received bytes was reached. Now, if the server returns the `Content-Length` header to API Gateway, API Gateway checks for the returned size. If the size exceeds the configured value, API Gateway reports an error.
RDAPI-10239	00904360	**Issue**: Unnecessary legacy menu item. **Resolution**: Previously, API Gateway Manager had a menu item **Push Deployment to Group** that pushed the configuration from one server to the rest of servers in the same group. Now, this menu item is no longer available.

Internal ID	Case ID	Description
RDAPI-10353	00902178	**Issue**: Long timeout for Cassandra connections. **Resolution**: Previously, if the machine hosting a Cassandra instance crashed or had a network failure, the Cassandra-dependent traffic in API Gateway was almost completely blocked for up to 15 minutes. Now, the Datastax driver in API Gateway has been updated to the latest version. API Gateway correctly detects the failure, the outage window of the Cassandra traffic has been reduced to ~40 seconds, and API Gateway only rejects 33% of the Cassandra-dependent traffic.
RDAPI-10408	00901959	**Issue**: Monitoring in API Gateway Manager not displaying memory or CPU. **Resolution**: Previously, when API Gateway Manager sent a `GET` request to `/api/monitoring/metrics/timeline` to get the minimum, maximum, or average values for a metric (in this example `memoryUsed`) and the query string was `metricType=<memoryUsedMin or memoryUsedMax or memoryUsedAvg>`, an error response with a status code `HTTP 503 Service Unavailable` was returned. Now, the status code of the response is `HTTP 200`, and the response body contains the values for the requested metric for valid values.
RDAPI-10417	00905276	**Issue**: Problem with license file in unattended installation. **Resolution**: Previously, if you installed API Gateway in the unattended mode, the license file was not copied to the `conf/licenses` directory and API Gateway could not start properly. Now, the license file is copied to the right directory, and the product starts normally.
RDAPI-10433	00905427	**Issue**: `NullPointerException` when a JMS message has no body. **Resolution**: Previously, when API Gateway consumed a JMS message containing only properties and no body from the JMS queue, API Gateway threw a `NullPointerException`, because traffic monitoring tried to log the JMS message body that did not exist. Now, traffic monitoring in API Gateway has been updated, and API Gateway can consume JMS messages that do not contain a body as per usual.

Internal ID	Case ID	Description
RDAPI-10436	00907041	**Issue**: OpenID request shown as `Unknown type flow` in API Gateway Manager. **Resolution**: Previously, when you requested an OpenID token, API Gateway Manager logged the request with type `token_id token` as `Unknown type flow` type on the **Traffic** tab. Now, the OpenID request with type `token_id token` is logged as `OpenIDConnect ID Token and Token Request`.
RDAPI-10506	00907700	**Issue**: Security vulnerabilities with the Java version. **Resolution**: Previously, API Gateway used a Java version with security vulnerabilities. Now, API Gateway uses JRE 8u141 that fixes these vulnerabilities.
RDAPI-10663	0896155	**Issue**: Errors with special characters in KPS tables. **Resolution**: Previously in API Gateway Manager, if you entered a string containing a \ character in the **Primary Key** field in a KPS table, API Gateway Manager displayed an error. Now, API Gateway Manager displays the KPS table correctly even when the **Primary Key** field contains special characters.
RDAPI-10664	00917255, 00902613	**Issue**: Installing API Gateway as a Linux system service can cause a library conflict. **Resolution**: Previously, if you installed API Gateway as a Linux system service, you had to add installation paths to global system configuration (`ldconfig`) which could cause library version conflict. Now, the `vshell` binary is pre-configured with default library paths under `/opt/Axway/apigateway`, and the changes to global system configuration are no longer required. You can change the default paths using tools like `chrpathor patchelf`.
RDAPI-10681	00907790	**Issue**: Schema validation done at different phases depending on the selected schema validation option. **Resolution**: Previously, if you used both a default and a custom schema validation option, the schema validation was done in different phases of processing a request. The default schema validation was done *before* the policy for a given operation. The custom validation was done *after* the policy for a given operation, which might cause problems in validation. Now, you can also configure the custom validation to take place before further processing the request.

Internal ID	Case ID	Description
RDAPI-10694	00907281	**Issue**: The API Gateway RADIUS client is a single-threaded. **Resolution**: Previously, the API Gateway RADIUS client could not process user authentication asynchronously. For example, when a RADIUS server required a two-way authentication, the RADIUS client could process the second authentication only after completing the first authentication. Now, API Gateway RADIUS client can process user authentication asynchronously.
RDAPI-10697	00904790	**Issue**: Validating SAML assertion fails if there is no statement in the assertion. **Resolution**: Previously, the **Retrieve from SAML Attribute Assertion** filter failed if the SAML assertion did not contain a statement. Now, this no longer happens, and the SAML assertion can be validated.
RDAPI-10702	00907036	**Issue**: Nonce claim not part of the generated OpenID token. **Resolution**: Previously, when an OpenID token was generated for the OpenID implicit grant type or the Authorization code grant type (if one was specified in the authentication request), the generated ID Token did not contain a nonce. Now, the ID Token contains a nonce claim.
RDAPI-10714	00907286	**Issue**: Attributes from RADIUS authentication request not parsed correctly. **Resolution**: Previously, when you send an authentication request to RADIUS, some of the returned RADIUS attributes were not setup correctly. Now, all of the returned RADIUS attributes contain the correct values.
RDAPI-10751	00910246	**Issue**: Unable to add Cassandra entries in a `.fed` file using a script. **Resolution**: Previously, you could not use the `updateCassandraSettings.py` script to add several Cassandra `host:port` entries in a `.fed` file, because the script could not change user names and passwords in the Cassandra instances. Now, the script has been improved to accommodate this using the following new parameters: • Cassandra user name • Cassandra password • Cassandra keyspace • `.fed` file passphrase

Internal ID	Case ID	Description
RDAPI-10871	00911830	**Issue**: Deployment in high availability (HA) environment fails when any of the Admin Node Manager is down. **Resolution**: Previously, if you tried to deploy a configuration to a HA environment, the deployment failed if any of the Admin Node Managers was down. Now, the deployment succeeds as long as one of the Admin Node Managers is running.
RDAPI-10873	00912679	**Issue**: Unimplemented function `compareDocumentPosition` triggered on some XSLT transformation. **Resolution**: Previously, some XSLT transformations that used to work in API Gateway 7.3.1 could not be used in v7.5.3 or later because of a missing function that the new version of XSLT layer uses. Now, the missing function has been implemented in XML layer.
RDAPI-10929	00912469	**Issue**: Certificates generated in Policy Studio signed using a SHA1 algorithm. **Resolution**: Previously, if you generated certificates in Policy Studio, they were signed using the algorithm `SHA1withRSA` that was considered to be a weak algorithm. Now, the algorithm has been updated, and certificates generated in Policy Studio are signed using the algorithm `SHA256withRSA`.
RDAPI-10949	00915509, 00911895	**Issue**: Runtime exceptions not captured by fault handlers. **Resolution**: Previously, when a filter threw a runtime exception, the exception skipped all fault handlers and was propagated to the client. Now, all runtime exceptions are caught and logged to trace. If you include a specific fault handler in the policy, API Gateway calls that fault handler, otherwise the generic fault handler is used.
RDAPI-10952	00907784	**Issue**: The **SMIME Decrypt** filter fails with error. **Resolution**: Previously, if you were using the **SMIME Decrypt** filter and it did not directly follow the **SMIME Encrypt** filter, the decrypt filter failed with the error `Cannot decrypt message of content type application/pkcs7-mime`. Now, the **SMIME Decrypt** filter no longer has to directly follow the **SMIME Encrypt** filter.

Internal ID	Case ID	Description
RDAPI-10960	00916136	**Issue**: Missing script in the Package and Deployment Tools installer. **Resolution**: Previously, the Package and Deployment Tools installer did not contain the `apimanager-promote` script. Now, the script is included in the installer on Linux.
RDAPI-10961	00913118	**Issue**: Policy errors showing up in deployment error log. **Resolution**: Previously, if you were deploying a configuration from Policy Studio and at the same time something (for example, a misconfigured load balancer) was causing high number of errors in your environment, the policy deployment error log in Policy Studio might contain traces of these other errors that were completely unrelated to the your configuration update. Now, the deployment error log no longer contains traces unrelated to your configuration update.
RDAPI-10968	00913251	**Issue**: When calling many filters, Traffic Monitor crashes when logging the `Circuit Path` used by policies. **Resolution**: Previously, if the `Circuit Path` string exceeded 524 KB (OpsDB page size), it could cause Traffic Monitor to crash. Now, API Gateway chunks the `Circuit Path` string into blocks that do not exceed 524 KB.
RDAPI-11015	00879231	**Issue**: Missing JSON exception message. **Resolution**: Previously, the **JSON Error** filter sometimes did not include the failure reason in the response message. Now, if you select the option **Show detailed explanation of error**, the failure reason is always included in the response error message.
RDAPI-11080	00916969	**Issue**: KPS property name causes error. **Resolution**: Previously, the *API Gateway Key Property Store User Guide* did not mention that using `key` as the name for a property in a KPS table causes a deployment error. Now, a note on this has been added to the guide.
RDAPI-11108	0892900	**Issue**: Path defined on virtual hosts not in the **Used by** list of a global policy. **Resolution**: Previously in Policy Studio, if you used a global request or response policy to expose a relative path on a virtual host, the path was not displayed in the **Used by** list in the global policy edit dialog. Now, the **Used by** list of policy also includes the relative paths exposed on a virtual host.

Internal ID	Case ID	Description
RDAPI-11115	00906638	**Issue**: Unable to import a SOAP service into API Manager. **Resolution**: Previously, you could not import a WSDL with invalid schema into API Manager or Policy Studio. Now, you can import a WSDL with invalid schema when you set the Java system property `wsdlImport.suppressSchemaValidationErrors` to `true`.
RDAPI-11185	00905063	**Issue**: The **JSON Path** filter does not work as documented. **Resolution**: Previously, the **JSON Path** filter could not be used with some legacy filters, like **Insert SAML Attribute Assertion**, because the **JSON Path** filter did not extract the attributes in the format the legacy filters expected. Now, you can extract all the attributes from the root JSON message and save them in an `attribute.lookup.list` element if you do not add any attributes on the **JSON Path** filter configuration.
RDAPI-11201	00921196	**Issue**: Setting up Cassandra on a remote node with encryption fails with errors. **Resolution**: Previously, when you ran the `setup-cassandra` script on a remote node that had the flags `--enable-server-encryption` and `--enable-client-encryption`, the script failed with errors and did not show the instructions for keystore and truststore management. Now, the script on the remote node succeeds and shows the management instructions.
RDAPI-11231	00921748	**Issue**: Importing broken reference breaks the environment settings. **Resolution**: Previously when importing data to Policy Studio, if you imported a broken reference that removed entities with environmentalized fields, it corrupted the environment settings of a project. Now, you see an error during the import operation if the import requires deleting entities with environmentalized fields.

Internal ID	Case ID	Description
RDAPI-11287	00904604	**Issue**: Incorrect character encoding in API Gateway Manager. **Resolution**: Previously, if a HTTP transaction containing `UTF-8` characters in both the headers and message body was stored in the traffic monitor database, and you later viewed that transaction in API Gateway Manager, the `UTF-8` characters in the message body were incorrectly encoded and displayed. Now, both headers and message bodies containing `UTF-8` characters are displayed correctly in API Gateway Manager.
RDAPI-11309	00923314	**Issue**: Domain audit log does not log all events selected in its configuration. **Resolution**: Previously, the user events for updating or deleting a user and updating a password were not included in the domain audit log even if you had enabled logging them in the log settings. Now, all selected user events are correctly reported in the domain audit log.
RDAPI-11412	00924785	**Issue**: The **Remove All** button in the virtual host paths does not remove all the paths. **Resolution**: Previously in Policy Studio, you tried to remove the virtual host paths under **Environment Configuration > Listeners** using the **Remove All** button, not all paths were removed. Now, all the paths are removed.
RDAPI-11438	00918713	**Issue**: Invalid request in the **OCSP Client** filter. **Resolution**: Previously, the **OCSP Client** filter generated an invalid request if the OCSP Responder URL did not have a slash after the host name. Now, the **OCSP Client** filter ensures that the OCSP Responder URL has the slash after the host name to ensure the `POST` request line is valid.
RDAPI-11499	00922129	**Issue**: Errors in Visual Mapper. **Resolution**: Previously, when you tried opening a `.fed` file that had been saved in a particular state, Visual Mapper would give the error `Could not open the editor: Index: 1, Size: 1`, and you could not view the map. Now, the map can be viewed.

Internal ID	Case ID	Description
RDAPI-11518	00926945	**Issue**: The HTTP method is not correctly checked when using a CORS profile on an API listener. **Resolution**: Previously, if you set a CORS profile to an API listener, the HTTP method was not checked against the value you had configured in the API listener. Now, the HTTP method is checked against the value you configure in the API listener both with and without the CORS profile.

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 Gateway *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 Gateway 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 Gateway 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.