Red Hat Quay

Red Hat Quay
Abstract

Red Hat Quay Release Notes
Table of Contents

PREFACE ........................................................................................................... 3

CHAPTER 1. CLAIR CRDA ENDPOINTS DISABLED ............................................. 4

CHAPTER 2. RHBA-2024:0251 - RED HAT QUAY 3.8.15 BUG FIX UPDATE .......... 5
  2.1. BUG FIXES ................................................................................. 5


CHAPTER 4. RHBA-2023:5686 - RED HAT QUAY 3.8.13 BUG FIX UPDATE .......... 7

CHAPTER 5. RHBA-2023:5099 - RED HAT QUAY 3.8.12 BUG FIX UPDATE .......... 8
  5.1. BUG FIXES ............................................................................. 8

CHAPTER 6. RHBA-2023:4275 - RED HAT QUAY 3.8.11 BUG FIX UPDATE .......... 9

CHAPTER 7. RHBA-2023:3891 - RED HAT QUAY 3.8.10 BUG FIX UPDATE .......... 10
  7.1. BUG FIXES ........................................................................... 10

CHAPTER 8. RHBA-2023:3681 - RED HAT QUAY 3.8.9 BUG FIX UPDATE ............ 11
  8.1. BUG FIXES ........................................................................... 11

CHAPTER 9. RHBA-2023:3181 - RED HAT QUAY 3.8.8 BUG FIX UPDATE ............ 12
  9.1. BUG FIXES .......................................................................... 12

CHAPTER 10. RHBA-2023:2087 - RED HAT QUAY 3.8.7 BUG FIX UPDATE .......... 13
  10.1. BUG FIXES ....................................................................... 13

CHAPTER 11. RHBA-2023:1874 - RED HAT QUAY 3.8.6 BUG FIX UPDATE .......... 14
  11.1. BUG FIXES ....................................................................... 14

CHAPTER 12. RHBA-2023:1498 - RED HAT QUAY 3.8.5 BUG FIX UPDATE .......... 15
  12.1. BUG FIXES ....................................................................... 15

CHAPTER 13. RHBA-2023:1188 - RED HAT QUAY 3.8.4 BUG FIX UPDATE .......... 16
  13.1. BUG FIXES ....................................................................... 16

CHAPTER 14. RHBA-2023:0906 - RED HAT QUAY 3.8.3 BUG FIX UPDATE .......... 17
  14.1. BUG FIXES ....................................................................... 17

CHAPTER 15. RHBA-2023:0789 - RED HAT QUAY 3.8.2 BUG FIX UPDATE .......... 18
  15.1. BUG FIXES ....................................................................... 18

CHAPTER 16. RHBA-2023:0044 - RED HAT QUAY 3.8.1 BUG FIX UPDATE .......... 19
  16.1. BUG FIXES ....................................................................... 19

CHAPTER 17. RHBA-2022:6976 - RED HAT QUAY 3.8.0 RELEASE ....................... 20
  17.1. RED HAT QUAY, CLAIR, AND QUAY BUILDER NEW FEATURES AND ENHANCEMENTS ................................................................. 20
  17.2. NEW RED HAT QUAY CONFIGURATION FIELDS ................................ 21
  17.3. RED HAT QUAY OPERATOR ..................................................... 22
  17.4. RED HAT QUAY 3.8 KNOWN ISSUES AND LIMITATIONS .................. 23
  17.4.1. Known issues: .................................................................. 23
  17.4.2. IPv6 and dual-stack limitations and known issues: ....................... 25
  17.5. RED HAT QUAY BUG FIXES ................................................... 26
  17.6. RED HAT QUAY FEATURE TRACKER ...................................... 26
  17.6.1. Deprecated features ......................................................... 27
Red Hat Quay container registry platform provides secure storage, distribution, and governance of containers and cloud-native artifacts on any infrastructure. It is available as a standalone component or as an Operator on OpenShift Container Platform. Red Hat Quay includes the following features and benefits:

- Granular security management
- Fast and robust at any scale
- High velocity CI/CD
- Automated installation and updates
- Enterprise authentication and team-based access control
- OpenShift Container Platform integration

Red Hat Quay is regularly released, containing new features, bug fixes, and software updates. To upgrade Red Hat Quay for both standalone and OpenShift Container Platform deployments, see Upgrade Red Hat Quay.

**IMPORTANT**

Red Hat Quay only supports rolling back, or downgrading, to previous z-stream versions, for example, 3.7.2 → 3.7.1. Rolling back to previous y-stream versions (3.7.0 → 3.6.0) is not supported. This is because Red Hat Quay updates might contain database schema upgrades that are applied when upgrading to a new version of Red Hat Quay. Database schema upgrades are not considered backwards compatible.

Downgrading to previous z-streams is neither recommended nor supported by either Operator based deployments or virtual machine based deployments. Downgrading should only be done in extreme circumstances. The decision to rollback your Red Hat Quay deployment must be made in conjunction with the Red Hat Quay support and development teams. For more information, contact Red Hat Quay support.

Documentation for Red Hat Quay is versioned with each release. The latest Red Hat Quay documentation is available from the Red Hat Quay Documentation page. Currently, version 3 is the latest major version.

**NOTE**

Prior to version 2.9.2, Red Hat Quay was called Quay Enterprise. Documentation for 2.9.2 and prior versions are archived on the Product Documentation for Red Hat Quay 2.9 page.
CHAPTER 1. CLAIR CRDA ENDPOINTS DISABLED

As of September 25, 2023, the Code Ready Dependency Analytics Service for Java vulnerability matching is no longer usable with Clair. The service's API moved to a different endpoint and there are no plans to update Clair to support this new endpoint. Instead, users should upgrade to Red Hat Quay 3.9 in order to keep getting CVE reports on Java Maven packages indexed by Clair from container images stored in Red Hat Quay, with the additional benefit of offline support and without the need for separate API keys.
CHAPTER 2. RHBA-2024:0251 - RED HAT QUAY 3.8.15 BUG FIX UPDATE

Issued 2024-02-01

Red Hat Quay release 3.8.15 is now available. The bug fixes that are included in the update are listed in the RHBA-2024:0251 advisory.

2.1. BUG FIXES

- **PROJQUAY-6588**: Use config editor secret password as credential for reconfigure request
CHAPTER 3. RHBA-2023:6820 - RED HAT QUAY 3.8.14 BUG FIX UPDATE

Issued 2023-11-08

Red Hat Quay release 3.8.14 is now available. The bug fixes that are included in the update are listed in the RHBA-2023:6820 advisory.
CHAPTER 4. RHBA-2023:5686 - RED HAT QUAY 3.8.13 BUG FIX UPDATE

Issued 2023-10-17

Red Hat Quay release 3.8.13 is now available. The bug fixes that are included in the update are listed in the RHBA-2023:5686 advisory.
CHAPTER 5. RHBA-2023:5099 - RED HAT QUAY 3.8.12 BUG FIX UPDATE

Issued 2023-9-12

Red Hat Quay release 3.8.12 is now available. The bug fixes that are included in the update are listed in the RHBA-2023:5099 advisory.

5.1. BUG FIXES

- PROJQUAY-6005. Quay Operator doesn’t trust internal service CA when it is rotated.
CHAPTER 6. RHBA-2023:4275 - RED HAT QUAY 3.8.11 BUG FIX UPDATE

Issued 2023-8-10

Red Hat Quay release 3.8.11 is now available. The bug fixes that are included in the update are listed in the RHBA-2023:4275 advisory.
CHAPTER 7. RHBA-2023:3891 - RED HAT QUAY 3.8.10 BUG FIX UPDATE

Issued 2023-7-12

Red Hat Quay release 3.8.10 is now available. The bug fixes that are included in the update are listed in the RHBA-2023:3891 advisory.

7.1. BUG FIXES

CHAPTER 8. RHBA-2023:3681 - RED HAT QUAY 3.8.9 BUG FIX UPDATE

Issued 2023-6-20

Red Hat Quay release 3.8.9 is now available. The bug fixes that are included in the update are listed in the RHBA-2023:3681 advisory.

8.1. BUG FIXES

- **PROJQUAY-4297.** Enabling quota management in Red Hat Quay significantly slows down opening of the superuser panel.

- **PROJQUAY-5079.** Red Hat Quay Operator pod can not deploy Quay pods when setting the horizontalpodautoscaler parameter as managed in OpenShift Container Platform 4.13.

- **PROJQUAY-5273.** Proxy configuration does not allow anonymous pulls from upstream.
CHAPTER 9. RHBA-2023:3181 - RED HAT QUAY 3.8.8 BUG FIX
UPDATE

Issued 2023-5-24

Red Hat Quay release 3.8.8 is now available. The bug fixes that are included in the update are listed in the RHBA-2023:3181 advisory.

9.1. BUG FIXES

- PROJQUAY-4739. Storage replication errors out with a strange exception.
Red Hat Quay release 3.8.7 is now available. The bug fixes that are included in the update are listed in the RHBA-2023:2087 advisory.

10.1. BUG FIXES

- PROJQUAY-5140. Improving FEATURE_PROXY_STORAGE to remove failures when having complex infrastructure configuration.
CHAPTER 11. RHBA-2023:1874 - RED HAT QUAY 3.8.6 BUG FIX UPDATE

Issued 2023-4-20

Red Hat Quay release 3.8.6 is now available. The bug fixes that are included in the update are listed in the RHBA-2023:1874 advisory.

11.1. BUG FIXES

- PROJQUAY-4972. Allow storage replication worker to continue functioning on certain exceptions.
CHAPTER 12. RHBA-2023:1498 - RED HAT QUAY 3.8.5 BUG FIX UPDATE

Issued 2023-3-28

Red Hat Quay release 3.8.5 is now available. The bug fixes that are included in the update are listed in the RHBA-2023:1498 advisory.

12.1. BUG FIXES

- PROJQUAY-4845. Quay web interface should not divulge user existence and password mismatch.
CHAPTER 13. RHBA-2023:1188 - RED HAT QUAY 3.8.4 BUG FIX UPDATE

Issued 2023-3-14

Red Hat Quay release 3.8.4 is now available. The bug fixes that are included in the update are listed in the RHBA-2023:1188 advisory.

13.1. BUG FIXES

- **PROJQUAY-5074.** Health checks should check storage engines.
- **PROJQUAY-5117.** Quay calls LDAP on robot account login.
CHAPTER 14. RHBA-2023:0906 - RED HAT QUAY 3.8.3 BUG FIX UPDATE

Issued 2023-2-27

Red Hat Quay release 3.8.3 is now available. The bug fixes that are included in the update are listed in the RHBA-2023:0906 advisory.

14.1. BUG FIXES

- PROJQUAY-3643. CVE-2022-24863 quay-registry-container: http-swagger: a denial of service attack consisting of memory exhaustion on the host system [quay-3.7]
Red Hat Quay 3.8 Red Hat Quay Release Notes

CHAPTER 15. RHBA-2023:0789 - RED HAT QUAY 3.8.2 BUG FIX UPDATE

Issued 2023-2-15

Red Hat Quay release 3.8.2 is now available with Clair 4.6.0. The bug fixes that are included in the update are listed in the RHBA-2023:0789 advisory.

15.1. BUG FIXES

- PROJQUAY-4395. Default value of false for CLEAN_BLOB_UPLOAD_FOLDER does not make sense.

- PROJQUAY-4726. No audit logs when superuser trigger and cancel build under normal user’s namespace with superuser full access enabled.

- PROJQUAY-4992. Cleanup deprecated appr code.
CHAPTER 16. RHBA-2023:0044 - RED HAT QUAY 3.8.1 BUG FIX UPDATE

Issued 2023-1-24

Red Hat Quay release 3.8.1 is now available. The bug fixes that are included in the update are listed in the RHBA-2023:0044 advisory.

16.1. BUG FIXES

- **PROJQUAY-2146.** Combined URLs in security scan report (pointing to errata URL).
- **PROJQUAY-3632.** Web UI - viewing account results in error.
- **PROJQUAY-4800.** Add PUT method to CORS method list.
- **PROJQUAY-4857.** Add tracking and cookie content when domain contains Quay.io.
- **PROJQUAY-4527.** New UI toggle cannot switch back from new UI to current UI on Apple Safari.
- **PROJQUAY-4663.** Pagination for delete repository modal not showing correct values.
- **PROJQUAY-4765.** Quay 3.8.0 superuser does not have permission to add new team member to normal user’s team when enabled superuser full access.
CHAPTER 17. RHBA-2022:6976 - RED HAT QUAY 3.8.0 RELEASE

Issued 2022-12-6

Red Hat Quay release 3.8.0 is now available with Clair 4.5.1. The bug fixes that are included in the update are listed in the RHBA-2022:6976 advisory.

17.1. RED HAT QUAY, CLAIR, AND QUAY BUILDER NEW FEATURES AND ENHANCEMENTS

The following updates have been made to Red Hat Quay, Clair, and Quay Builders:

- Previously, Red Hat Quay only supported the IPv4 protocol family. IPv6 support is now available in Red Hat Quay 3.8 standalone deployments. Additionally, dual-stack (IPv4/IPv6) support is available.

Table 17.1. Network protocol support

<table>
<thead>
<tr>
<th>Protocol family</th>
<th>Red Hat Quay 3.7</th>
<th>Red Hat Quay 3.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IPv6</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Dual-stack (IPv4/IPv6)</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

For more information, see PROJQUAY-272.

For a list of known limitations, see IPv6 and dual-stack limitations.

- Previously, Red Hat Quay did not require self-signed certificates to use Subject Alternative Names (SANs). Red Hat Quay users could temporarily enable Common Name matching with GODEBUG=x509ignoreCN=0 to bypass the required certificate.

With Red Hat Quay 3.8, Red Hat Quay has been upgraded to use Go version 1.17. As a result, setting GODEBUG=x509ignoreCN=0 no longer works. Users must include self-signed certificates to use SAN.

For more information, see PROJQUAY-1605.

- The following enhancements have been made to the Red Hat Quay proxy cache feature:

  - Previously, the cache of a proxy organization with quota management enabled could reach full capacity. As a result, pulls for new images could be prevented until an administrator cleaned up the cached images.

    With this update, Red Hat Quay administrators can now use the storage quota of an organization to limit the cache size. Limiting the cache size ensures that backend storage consumption remains predictable by discarding images from the cache according to the pull frequency or overall usage of an image. As a result, the storage size allotted by quota management always stays within its limits.

    For more information, see Leveraging storage quota limits in proxy organizations.
Previously, when mirroring a repository, an image with the latest tag must have existed in the remote repository. This requirement has been removed. Now, an image with the latest tag is no longer required, and you do not need to specify an existing tag explicitly. For more information on this update, see PROJQUAY-2179.

For more information on tag patterns, see Mirroring tag patterns.

- Red Hat Quay 3.8 now includes support for the following Open Container Initiative (OCI) image media types:
  - Software Packadage Data Exchange (SPDX)
  - Syft
  - CycloneDX
    These can be configured by the users in their config.yaml file, for example:

    ```yaml
    ... 
    ALLOWED_OCI_ARTIFACT_TYPES:
        application/vnd.syft+json
        application/vnd.cyclonedx
        application/vnd.cyclonedx+xml
        application/vnd.cyclonedx+json
        application/vnd.in-toto+json
    ... 
    
    NOTE
    When adding OCI media types that are not configured by default, users will also need to manually add support for cosign and Helm if desired. The ztsd compression scheme is supported by default, so users will not need to add that OCI media type to their config.yaml to enable support.

17.2. NEW RED HAT QUAY CONFIGURATION FIELDS

- The following configuration field has been added to test Red Hat Quay's new user interface:
  - FEATURE_UI_V2: With this configuration field, users can test the beta UI environment. Default: False
    For more information, see v2 user interface configuration.

- The following configuration fields have been added to enhance the Red Hat Quay registry:
  - FEATURE_LISTEN_IP_VERSION: This configuration field allows users to set the protocol family to IPv4, IPv6, or dual-stack. This configuration field must be properly set, otherwise Red Hat Quay fails to start. Default: IPv4
    Additional configurations: IPv6, dual-stack
    For more information, see IPv6 configuration field.
The following configuration fields have been added to enhance Lightweight Directory Access Protocol (LDAP) deployments:

- **LDAP_SUPERUSER_FILTER**: This configuration field is a subset of the **LDAP_USER_FILTER** configuration field. It allows Red Hat Quay administrators the ability to configure Lightweight Directory Access Protocol (LDAP) users as superusers when Red Hat Quay users select LDAP as their authentication provider. With this field, administrators can add or remove superusers without having to update the Red Hat Quay configuration file and restart their deployment.

  This field requires that your **AUTHENTICATION_TYPE** is set to **LDAP**.

  For more information, see LDAP superuser configuration reference.

- **LDAP_RESTRICTED_USER_FILTER**: This configuration field is a subset of the **LDAP_USER_FILTER** configuration field. When configured, allows Red Hat Quay administrators the ability to configure Lightweight Directory Access Protocol (LDAP) users as restricted users when Red Hat Quay uses LDAP as its authentication provider.

  This field requires that your **AUTHENTICATION_TYPE** is set to **LDAP**.

  For more information, see LDAP restricted user configuration.

The following configuration fields have been added to enhance the superuser role:

- **FEATURE_SUPERUSERS_FULL_ACCESS**: This configuration field grants superusers the ability to read, write, and delete content from other repositories in namespaces that they do not own or have explicit permissions for.

  For more information, see FEATURE_SUPERUSERS_FULL_ACCESS configuration reference.

- **GLOBAL_READONLY_SUPER_USERS**: This configuration field grants users of this list read access to all repositories, regardless of whether they are public repositories.

  For more information, see GLOBAL_READONLY_SUPER_USERS configuration reference.

  **NOTE**

  In its current state, this feature only allows designated users to pull content from all repositories. Administrative restrictions will be added in a future version of Red Hat Quay.

The following configuration fields have been added to enhance user permissions:

- **FEATURE_RESTRICTED_USERS**: When set with **RESTRICTED_USERS_WHITELIST**, restricted users cannot create organizations or content in their own namespace. Normal permissions apply for an organization’s membership, for example, a restricted user will still have normal permissions in organizations based on the teams that they are members of.

  For more information, see FEATURE_RESTRICTED_USERS configuration reference.

- **RESTRICTED_USERS_WHITELIST**: When set with **FEATURE_RESTRICTED_USERS**: true, administrators can exclude users from the **FEATURE_RESTRICTED_USERS** setting.

  For more information, see RESTRICTED_USERS_WHITELIST configuration reference.

### 17.3. RED HAT QUAY OPERATOR

The following updates have been made to the Red Hat Quay Operator:
Previously, the Red Hat Quay Operator only supported the IPv4 protocol family. IPv6 support is now available in Red Hat Quay 3.8 Operator deployments.

Table 17.2. Network protocol support

<table>
<thead>
<tr>
<th>Protocol family</th>
<th>Red Hat Quay 3.7 Operator</th>
<th>Red Hat Quay 3.8 Operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IPv6</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Dual-stack (IPv4/IPv6)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For more information, see PROJQUAY-272.

For a list of known limitations, see IPv6 and dual-stack limitations.

17.4. RED HAT QUAY 3.8 KNOWN ISSUES AND LIMITATIONS

17.4.1. Known issues:

- The `metadata_json` column in the `logentry3` table on MySQL deployments has a limited size of `TEXT`. Currently, the default size of the column set to be `TEXT` is 65535 bytes. 65535 bytes is not big enough for some mirror logs when debugging is turned off. When a statement containing `TEXT` larger than 65535 bytes is sent to MySQL, the data sent is truncated to fit into the 65535 boundary. Consequently, this creates issues when the `metadata_json` object is decoded, and the decode fails because the string is not terminated properly. As a result, Red Hat Quay returns a 500 error.
  There is currently no workaround for this issue, and it will be addressed in a future version of Red Hat Quay. For more information, see PROJQUAY-4305.

- There is a known issue when using the `--sign-by-sigstore-private-key` flag with some versions of Podman v4.y.z or greater. When the flag is used, the following error is returned: `Error: writing signatures: writing sigstore attachments is disabled by configuration`. To use this flag with Podman v4, your version must be v4.2.1; versions prior to 4.2.1 return the aforementioned error.
  There is currently no workaround for this issue, and it will be addressed in a future version of Podman.

- Currently, when pushing images with the Cosign private key `sigstore` with Podman 4, the following error is returned: `Error: received unexpected HTTP status: 500 Internal Server Error`. This is a known issue and will be fixed in a future version of Podman.
  For more information, see PROJQUAY-4588.

- There is a known issue when using the `FEATURE_SUPERUSERS_FULL_ACCESS` configuration field with the Red Hat Quay UI v2. When this field is set, all superuser actions on tenant content should be audited. Currently, when a superuser deletes an existing organization that is owned by a normal user, there is no way to audit that operation. This will be fixed in a future version of Red Hat Quay.

- There is a known issue when using the `FEATURE_SUPERUSERS_FULL_ACCESS` configuration field with the Red Hat Quay UI v2. When setting this field to `true` in your `config.yaml` file, Red Hat Quay superusers can view organizations created by normal users, but
cannot see the image repository. As a temporary workaround, superusers can view those repositories by navigating to them from the Organizations page. This will be fixed in a future version of Red Hat Quay.

- When setting the FEATURE_SUPERUSERS_FULL_ACCESS configuration field to true, superusers do not have permission to create a new image repository under a normal user’s organization. This is a known issue and will be fixed in a future version of Red Hat Quay.

- When running Red Hat Quay in the old UI, timed-out sessions would require that a superuser input their password again in the pop-up window. With the new UI, superusers are returned to the main page and required to input their username and password credentials. This is a known issue and will be fixed in a future version of the new UI.

- When FEATURE_RESTRICTED_USERS is set to true, superusers are unable to create new organizations. This is a known issue and will be fixed in a future version of Red Hat Quay.

- If FEATURE_RESTRICTED_USERS or LDAP_RESTRICTED_USER_FILTER are set with a user, for example, user1, and the same user is also a superuser, they will not be able to create new organizations. This is a known issue. The superuser configuration field should take precedence over the restricted user configuration, however this is also an invalid configuration. Red Hat Quay administrators should not set the same user as both a restricted user and a superuser. This will be fixed in a future version of Red Hat Quay so that the superuser configuration field takes precedence over the restricted user field.

- After selecting Enable Storage Replication in the Red Hat Quay configuration editor and reconfiguring your Red Hat Quay deployment, the new Quay and Mirror pods fail to start. This error occurs because the Quay and Mirror pods rely on the QUAY_DISTRIBUTED_STORAGE_PREFERENCE environment variable, which is now unsupported in Red Hat Quay 3.8. As a temporary workaround, you must update the QuayRegistry config.yaml file manually to include the QUAY_DISTRIBUTED_STORAGE_PREFERENCE environment variable, for example:

```yaml
spec:
  components:
    - kind: clair
      managed: true
    - kind: postgres
      managed: true
    - kind: objectstorage
      managed: false
    - kind: redis
      managed: true
    - kind: horizontalpodautoscaler
      managed: true
    - kind: route
      managed: true
    - kind: mirror
      managed: true
    overrides:
      env:
        - name: QUAY_DISTRIBUTED_STORAGE_PREFERENCE
          value: local_us
        - kind: monitoring
          managed: false
        - kind: tls
```
This is a known issue and will be fixed in a future version of Red Hat Quay.

- When configuring Red Hat Quay AWS S3 Cloudfront, a new parameter, `s3_region` is required. Currently, the Red Hat Quay config editor does not include this field. As a temporary workaround, you must manually insert the `s3_region` parameter in your `config.yaml` file, for example:

```
DISTRIBUTED_STORAGE_CONFIG:
  default:
    - CloudFrontedS3Storage
    - cloudfront_distribution_domain: <domain_name>
    cloudfront_distribution_org_overrides: {}
    cloudfront_key_id: <cloudfront_key_id>
    cloudfront_privatekey_filename: default_cloudfront_signing_key.pem
    host: s3.us-east-2.amazonaws.com
    s3_access_key: ***
    s3_bucket: ***
    s3_secret_key: ***
    storage_path: /cloudfronts3/quayregistry
    s3_region: us-east-2
```

17.4.2. IPv6 and dual-stack limitations and known issues:

- Currently, attempting to configure your Red Hat Quay deployment with the common Azure Blob Storage configuration will not work on IPv6 single stack environments. Because the endpoint of Azure Blob Storage does not support IPv6, there is no workaround in place for this issue. For more information, see PROJQUAY-4433.

- Currently, attempting to configure your Red Hat Quay deployment with Amazon S3 CloudFront will not work on IPv6 single stack environments. Because the endpoint of Amazon S3 CloudFront does not support IPv6, there is no workaround in place for this issue. For more information, see PROJQUAY-4470.

- Currently, dual-stack (IPv4 and IPv6) support does not work on Red Hat Quay OpenShift Container Platform deployments. When Red Hat Quay 3.8 is deployed on OpenShift Container Platform with dual-stack support enabled, the Quay route generated by the Red Hat Quay Operator only generates an IPv4 address, and not an IPv6 address. As a result, clients with an IPv6 address cannot access the Red Hat Quay application on OpenShift Container Platform. This limitation will be lifted upon the release of OpenShift Container Platform 4.12.

- Currently, Github and `api.github.com` do not support IPv6. When Red Hat Quay is deployed on OpenShift Container Platform with IPv6 enabled, the config editor cannot be configured to use Github authentication.
Currently, Gitlab does not support IPv6.

There is a known issue when `FEATURE_LISTEN_IP_VERSION` is set to IPv6, and you have selected Red Hat Quay handles TLS in the configuration editor and uploaded self-signed certificates. If these conditions have been met, and you update any one configuration in the configuration editor (for example, adding a new superuser), when reconfiguring Red Hat Quay again, the mirror pod crashes and returns the following error: `Init:CrashLoopBackOff`. If Red Hat Quay handles TLS is selected in your deployment, you must set `FEATURE_LISTEN_IP_VERSION` to IPv4. This will be fixed in a future version of Red Hat Quay.

17.5. RED HAT QUAY BUG FIXES

- **PROJQUAY-4431**. Proxy cache failed to validate Azure Container Registry (ACR).

17.6. RED HAT QUAY FEATURE TRACKER

New features have been added to Red Hat Quay, some of which are currently in Technology Preview. Technology Preview features are experimental features and are not intended for production use.

Some features available in previous releases have been deprecated or removed. Deprecated functionality is still included in Red Hat Quay, but is planned for removal in a future release and is not recommended for new deployments. For the most recent list of deprecated and removed functionality in Red Hat Quay, refer to Table 1.1. Additional details for more fine-grained functionality that has been deprecated and removed are listed after the table.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Quay 3.8</th>
<th>Quay 3.7</th>
<th>Quay 3.6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Docker v1 support</td>
<td>Deprecated</td>
<td>General Availability</td>
<td>General Availability</td>
</tr>
<tr>
<td>FEATURE_UI_V2</td>
<td>Technology Preview</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>FEATURE_LISTEN_IP_VERSION</td>
<td>General Availability</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>LDAP_SUPERUSER_FILTER</td>
<td>General Availability</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>LDAP_RESTRICTED_USER_FILTER</td>
<td>General Availability</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>FEATURE_SUPERUSERS_FULL_ACCESS</td>
<td>General Availability</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>GLOBAL_READONLY_SUPER_USERS</td>
<td>General Availability</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Feature</td>
<td>Quay 3.8</td>
<td>Quay 3.7</td>
<td>Quay 3.6</td>
</tr>
<tr>
<td>--------------------------------------------------------------</td>
<td>--------------------</td>
<td>--------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>FEATURE_RESTRICTED_USERS</td>
<td>General Availability</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>RESTRICTED_USERS_WHITELIST</td>
<td>General Availability</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Quota management and enforcement</td>
<td>General Availability</td>
<td>General Availability</td>
<td>-</td>
</tr>
<tr>
<td>Red Hat Quay build enhancements</td>
<td>General Availability</td>
<td>General Availability</td>
<td>-</td>
</tr>
<tr>
<td>Red Hat Quay as proxy cache for upstream registries</td>
<td>General Availability</td>
<td>Technology Preview</td>
<td>-</td>
</tr>
<tr>
<td>Geo-replication - Red Hat Quay Operator</td>
<td>General Availability</td>
<td>General Availability</td>
<td>-</td>
</tr>
<tr>
<td>Advanced Clair configuration</td>
<td>General Availability</td>
<td>General Availability</td>
<td>-</td>
</tr>
<tr>
<td>Support for Microsoft Azure Government (MAG)</td>
<td>General Availability</td>
<td>General Availability</td>
<td>-</td>
</tr>
<tr>
<td>FEATURE_HELM_OCI_SUPPORT</td>
<td>Deprecated</td>
<td>Deprecated</td>
<td>Deprecated</td>
</tr>
<tr>
<td>MySQL and MariaDB database support</td>
<td>Deprecated</td>
<td>Deprecated</td>
<td>Deprecated</td>
</tr>
<tr>
<td>Open Container Initiative (OCI) Media types</td>
<td>General Availability</td>
<td>General Availability</td>
<td>General Availability</td>
</tr>
<tr>
<td>Java scanning with Clair</td>
<td>Technology Preview</td>
<td>Technology Preview</td>
<td>Technology Preview</td>
</tr>
<tr>
<td>Image APIs</td>
<td>Deprecated</td>
<td>Deprecated</td>
<td>General Availability</td>
</tr>
</tbody>
</table>

### 17.6.1. Deprecated features

- Support for Docker v1 is now deprecated and will be removed in a future release of Red Hat Quay. Users must now opt-in to enable Docker v1 support. Users should migrate any stored images in Docker v1 format to the OCI image format to avoid potential loss of data.