



Red Hat Quay 3.13

Red Hat Quay Release Notes

Red Hat Quay

Red Hat Quay 3.13 Red Hat Quay Release Notes

Red Hat Quay

Legal Notice

Copyright © 2024 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Abstract

Red Hat Quay Release Notes

Table of Contents

PREFACE	3
CHAPTER 1. RED HAT QUAY RELEASE NOTES	4
1.1. RHBA-2024:9478 - RED HAT QUAY 3.13.1 RELEASE	4
1.2. INFORMATION ABOUT UPGRADING TO 3.13.1	4
1.2.1. Red Hat Quay 3.13.1 enhancements	4
1.2.2. Red Hat Quay 3.13.1 known issues	4
1.2.3. Red Hat Quay 3.13.1 bug fixes	4
1.3. RHBA-2024:8408 - RED HAT QUAY 3.13.0 RELEASE	5
1.4. RED HAT QUAY DOCUMENTATION CHANGES	5
1.5. UPGRADING TO RED HAT QUAY 3.13	5
1.6. RED HAT QUAY NEW FEATURES AND ENHANCEMENTS	6
1.6.1. Red Hat Quay auto-pruning enhancements	6
1.6.1.1. Tag specification patterns in auto-pruning policies	6
1.6.1.2. Multiple auto-pruning policies	6
1.6.2. Keyless authentication with robot accounts	6
1.7. RED HAT QUAY ON OPENSIFT CONTAINER PLATFORM NEW FEATURES AND ENHANCEMENTS	7
1.7.1. Support for certificate-based authentication between Red Hat Quay and PostgreSQL	7
1.7.2. Red Hat Quay v2 UI enhancements	7
1.7.2.1. Robot federation selection	7
1.8. NEW RED HAT QUAY CONFIGURATION FIELDS	7
1.8.1. Disabling pushes to the Red Hat Quay registry configuration field	7
1.9. API ENDPOINT ENHANCEMENTS	8
1.9.1. New autoPrunePolicy endpoints	8
1.9.2. New federated robot token API endpoints	9
1.10. RED HAT QUAY 3.13 NOTABLE TECHNICAL CHANGES	9
1.11. RED HAT QUAY 3.13 KNOWN ISSUES AND LIMITATIONS	9
1.11.1. Clair vulnerability report known issue	9
1.11.2. FIPS mode known issue	9
1.11.3. Registry auto-pruning known issues	9
1.11.3.1. Policy prioritization known issue	9
1.11.3.2. Unrecognizable auto-prune tag patterns	10
1.11.4. Red Hat Quay v2 UI known issues	10
1.12. RED HAT QUAY BUG FIXES	11
1.13. RED HAT QUAY FEATURE TRACKER	12
1.13.1. IBM Power, IBM Z, and IBM® LinuxONE support matrix	13

PREFACE

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](#).

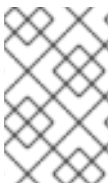


IMPORTANT

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. RED HAT QUAY RELEASE NOTES

The following sections detail y and z stream release information.

1.1. RHBA-2024:9478 - RED HAT QUAY 3.13.1 RELEASE

Issued 2024-11-18

Red Hat Quay release 3.13.1 is now available with Clair 4.8. The bug fixes that are included in the update are listed in the [RHBA-2024:9478](#) advisory.

1.2. INFORMATION ABOUT UPGRADING TO 3.13.1

Previously, when attempting to upgrade to Red Hat Quay 3.13, if FIPS mode was enabled for your OpenShift Container Platform cluster with Clair enabled, Clair would not function in your cluster. This issue was resolved in version 3.13.1. Upgrading to Red Hat Quay 3.13 automatically upgrades users to version 3.13.1 so that this issue is avoided. Additionally, if you are upgrading from 3.13 to 3.13.1 and FIPS was enabled, upgrading to 3.13.1 resolves the issue. ([PROJQUAY-8185](#))

1.2.1. Red Hat Quay 3.13.1 enhancements

With the release of Red Hat Quay 3.13.1, Hitachi Content Platform (HCP) is now supported for use as a storage backend. This allows organizations to leverage HCP for scalable, secure, and reliable object storage within their Red Hat Quay registry deployments.

For more information, see [HCP Object Storage](#).

1.2.2. Red Hat Quay 3.13.1 known issues

When using Hitachi Content Platform for your object storage, attempting to push an image with a large layer to a Red Hat Quay registry results in the following error:

An error occurred (NoSuchUpload) when calling the CompleteMultipartUpload operation: The specified multipart upload does not exist. The upload ID might be invalid, or the multipart upload might have been aborted or completed.

This is a known issue and will be fixed in a future version of Red Hat Quay.

1.2.3. Red Hat Quay 3.13.1 bug fixes

- [PROJQUAY-8185](#). Previously, when attempting to upgrade Red Hat Quay on OpenShift Container Platform to 3.13 with FIPS mode enabled, the upgrade would fail for deploying using Clair. This issue has been resolved. Upgrading to 3.13.1 does not fail for Red Hat Quay on OpenShift Container Platform using Clair with FIPS mode enabled.
- [PROJQUAY-8024](#). Previously, using Hitachi HCP v9.7 as your storage provider would return errors when attempting to pull images. This issue has been resolved.
- [PROJQUAY-5086](#). Previously, Red Hat Quay on OpenShift Container Platform would produce information about horizontal pod autoscalers (HPAs) for some components (for example, **Clair**, **Redis**, **PostgreSQL**, and **ObjectStorage**) when they were unmanaged by the Operator. This issue has been resolved and information about HPAs are not longer reported for unmanaged components.

1.3. RHBA-2024:8408 - RED HAT QUAY 3.13.0 RELEASE

Issued 2024-10-30

Red Hat Quay release 3.13 is now available with Clair 4.8. The bug fixes that are included in the update are listed in the [RHBA-2024:8408](#) advisory. For the most recent compatibility matrix, see [Quay Enterprise 3.x Tested Integrations](#). For information the release cadence of Red Hat Quay, see the [Red Hat Quay Life Cycle Policy](#).

1.4. RED HAT QUAY DOCUMENTATION CHANGES

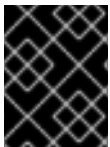
The following documentation changes have been made with the Red Hat Quay 3.13 release:

- The Red Hat Quay *Builders* feature that was originally documented in the [Using Red Hat Quay guide](#) has been moved into a new, dedicated book titled "[Builders and image automation](#)".
- The Red Hat Quay *Builders* feature that was originally documented in the [Red Hat Quay Operator features](#) has been moved into a new, dedicated book titled "[Builders and image automation](#)".
- A new book titled "[Securing Red Hat Quay](#)" has been created. This book covers SSL and TLS for Red Hat Quay, and adding additional certificate authorities (CAs) to your deployment. More content will be added to this book in the future.
- A new book titled "[Managing access and permissions](#)" has been created. This book covers topics related to access controls, repository visibility, and robot accounts by using the UI and the API. More content will be added to this book in the future.

1.5. UPGRADING TO RED HAT QUAY 3.13

With Red Hat Quay 3.13, the **volumeSize** parameter has been implemented for use with the **clairpostgres** component of the **QuayRegistry** custom resource definition (CRD). This replaces the **volumeSize** parameter that was previously used for the **clair** component of the same CRD.

If your Red Hat Quay 3.12 **QuayRegistry** custom resource definition (CRD) implemented a volume override for the **clair** component, you must ensure that the **volumeSize** field is included under the **clairpostgres** component of the **QuayRegistry** CRD.



IMPORTANT

Failure to move **volumeSize** from the **clair** component to the **clairpostgres** component will result in a failed upgrade to version 3.13.

For example:

```
spec:
  components:
  - kind: clair
    managed: true
  - kind: clairpostgres
    managed: true
  overrides:
    volumeSize: <volume_size>
```

For more information, see [Upgrade Red Hat Quay](#).

1.6. RED HAT QUAY NEW FEATURES AND ENHANCEMENTS

The following updates have been made to Red Hat Quay.

1.6.1. Red Hat Quay auto-pruning enhancements

With the release of Red Hat Quay 3.10, a new auto-pruning feature was released. With that feature, Red Hat Quay administrators could set up auto-pruning policies on namespaces for both users and organizations so that image tags were automatically deleted based on specified criteria. In Red Hat Quay 3.11, this feature was enhanced so that auto-pruning policies could be set up on specified repositories.

With Red Hat Quay 3.12, default auto-pruning policies were made to be set up at the registry level on new and existing configurations, which saved Red Hat Quay administrators time, effort, and storage by enforcing registry-wide rules.

With the release of Red Hat Quay 3.13, the following enhancements have been made to the auto-pruning feature.

1.6.1.1. Tag specification patterns in auto-pruning policies

Previously, the Red Hat Quay auto-pruning feature could not target or exclude specific image tags. With the release of Red Hat Quay 3.13, it is now possible to specify a *regular expression*, or *regex* to match a subset of tags for both organization- and repository-level auto-pruning policies. This allows Red Hat Quay administrators more granular auto-pruning policies to target only certain image tags for removal.

For more information, see [Using regular expressions with auto-pruning](#).

1.6.1.2. Multiple auto-pruning policies

Previously, Red Hat Quay only supported a single auto-pruning policy per organization and repository. With the release of Red Hat Quay 3.13, multiple auto-pruning policies can now be applied to an organization or a repository. These auto-pruning policies can be based on different tag naming (regex) patterns to cater for the different life cycles of images in the same repository or organization. This feature provides more flexibility when automating the image life cycle in your repository.

Additional auto-pruning policies can be added on the Red Hat Quay v2 UI by clicking **Add Policy** on the **Auto-Pruning Policies** page. They can also be added by using the API.

For more information about setting auto-prune policies, see [Red Hat Quay auto-pruning overview](#).

1.6.2. Keyless authentication with robot accounts

In previous versions of Red Hat Quay, robot account tokens were valid for the lifetime of the token unless deleted or regenerated. Tokens that do not expire have security implications for users who do not want to store long-term passwords or manage the deletion, or regeneration, or new authentication tokens.

With Red Hat Quay 3.13, Red Hat Quay administrators are provided the ability to exchange Red Hat Quay robot account tokens for an external OIDC token. This allows robot accounts to leverage short-lived, or *ephemeral tokens*, that last one hour. Ephemeral tokens are refreshed regularly and can be used to authenticate individual transactions.

This feature greatly enhances the security of your Red Hat Quay registry by mitigating the possibility of robot token exposure by removing the tokens after one hour.

For more information, see [Keyless authentication with robot accounts](#).

1.7. RED HAT QUAY ON OPENSIFT CONTAINER PLATFORM NEW FEATURES AND ENHANCEMENTS

The following updates have been made to Red Hat Quay on OpenShift Container Platform.

1.7.1. Support for certificate-based authentication between Red Hat Quay and PostgreSQL

With this release, support for certificate-based authentication between Red Hat Quay and PostgreSQL has been added. This allows Red Hat Quay administrators to supply their own SSL/TLS certificates that can be used for client-side authentication with PostgreSQL or CloudSQL. This provides enhanced security and allows for easier automation for your Red Hat Quay registry.

For more information, see [Certificate-based authentication between Red Hat Quay and SQL](#).

1.7.2. Red Hat Quay v2 UI enhancements

The following enhancements have been made to the Red Hat Quay v2 UI.

1.7.2.1. Robot federation selection

A new configuration page, **Set robot federation**, has been added to the Red Hat Quay v2 UI. This can be found by navigating to your organization or repository's robot account, clicking the menu kebab, and then clicking **Set robot federation**. This page is used when configuring keyless authentication with robot accounts, and allows you to add multiple OIDC providers to a single robot account.

For more information, see [Keyless authentication with robot accounts](#).

1.8. NEW RED HAT QUAY CONFIGURATION FIELDS

The following configuration fields have been added to Red Hat Quay 3.13.

1.8.1. Disabling pushes to the Red Hat Quay registry configuration field

In some cases, a read-only option for Red Hat Quay is not possible since it requires inserting a service key and other manual configuration changes. With the release of Red Hat Quay 3.13, a new configuration field has been added: **DISABLE_PUSHES**.

When **DISABLE_PUSHES** is set to **true**, users are unable to push images or image tags to the registry when using the CLI. Most other registry operations continue as normal when this feature is enabled by using the Red Hat Quay UI. For example, changing tags, editing a repository, robot account creation and deletion, user creation, and so on are all possible by using the UI.

When **DISABLE_PUSHES** is set to **true**, the Red Hat Quay garbage collector is disabled. As a result, when **PERMANENTLY_DELETE_TAGS** is enabled, using the Red Hat Quay UI to permanently delete a tag does not result in the immediate deletion of a tag. Instead, the tag stays in the repository until **DISABLE_PUSHES** is set to **false**, which re-enables the garbage collector. Red Hat Quay administrators should be aware of this caveat when using **DISABLE_PUSHES** and **PERMANENTLY_DELETE_TAGS** together.

This field might be useful in some situations such as when Red Hat Quay administrators want to calculate their registry's quota and disable image pushing until after calculation has completed. With this method, administrators can avoid putting the whole registry in **read-only** mode, which affects the database, so that most operations can still be done.

Field	Type	Description
<code>DISABLE_PUSHES</code>	Boolean	Disables pushes of new content to the registry while retaining all other functionality. Differs from read-only mode because database is not set as read-only . Defaults to false .

Example `DISABLE_PUSHES` configuration field

```
# ...
DISABLE_PUSHES: true
# ...
```

1.9. API ENDPOINT ENHANCEMENTS

1.9.1. New `autoPrunePolicy` endpoints

`tagPattern` and `tagPatternMatches` API parameters have been added to the following API endpoints:

- `createOrganizationAutoPrunePolicy`
- `updateOrganizationAutoPrunePolicy`
- `createRepositoryAutoPrunePolicy`
- `updateRepositoryAutoPrunePolicy`
- `createUserAutoPrunePolicy`
- `updateUserAutoPrunePolicy`

These fields enhance the auto-pruning feature by allowing Red Hat Quay administrators more control over what images are pruned. The following table provides descriptions of these fields:

Name	Description	Schema
<code>tagPattern</code> <i>optional</i>	Tags only matching this pattern (regex) will be pruned.	string
<code>tagPatternMatches</code> <i>optional</i>	Determine whether pruned tags should or should not match the <code>tagPattern</code> .	boolean

For example API commands, see [Red Hat Quay auto-pruning overview](#).

1.9.2. New federated robot token API endpoints

The following API endpoints have been added for the keyless authentication with robot accounts feature:

- **GET `oauth2/federation/robot/token`**. Use this API endpoint to return an expiring robot token using the robot identity federation mechanism.
- **POST `/api/v1/organization/{orgname}/robots/{robot_shortname}/federation`**. Use this API endpoint to create a federation configuration for the specified organization robot.

1.10. RED HAT QUAY 3.13 NOTABLE TECHNICAL CHANGES

Clair now requires its PostgreSQL database to be version 15. For standalone Red Hat Quay deployments, administrators must manually migrate their database over from PostgreSQL version 13 to version 15. For more information about this procedure, see [Upgrading the Clair PostgreSQL database](#).

For Red Hat Quay on OpenShift Container Platform deployments, this update is automatically handled by the Operator so long as your Clair PostgreSQL database is currently using version 13.

1.11. RED HAT QUAY 3.13 KNOWN ISSUES AND LIMITATIONS

The following sections note known issues and limitations for Red Hat Quay 3.13.

1.11.1. Clair vulnerability report known issue

When pushing Suse Enterprise Linux Images with **HIGH** image vulnerabilities, Clair 4.8.0 does not report these vulnerabilities. This is a known issue and will be fixed in a future version of Red Hat Quay.

1.11.2. FIPS mode known issue

If FIPS mode is enabled for your OpenShift Container Platform cluster and you use Clair, you must not upgrade the Red Hat Quay Operator to version 3.13. If you upgrade, Clair will not function in your cluster. ([PROJQUAY-8185](#))

1.11.3. Registry auto-pruning known issues

The following known issues apply to the auto-pruning feature.

1.11.3.1. Policy prioritization known issue

Currently, the auto-pruning feature prioritizes the following order when configured:

1. Method: **creation_date** + **organization wide**
2. Method: **creation_date** + **repository wide**
3. Method: **number_of_tags** + **organization wide**
4. Method: **number_of_tags** + **repository wide**

This means that the auto-pruner first prioritizes, for example, an organization-wide policy set to expire tags by their creation date before it prunes images by the number of tags that it has.

There is a known issue when configuring a registry-wide auto-pruning policy. If Red Hat Quay administrators configure a **number_of_tags** policy before a **creation_date** policy, it is possible to prune more than the intended set for the **number_of_tags** policy. This might lead to situations where a repository removes certain image tags unexpectedly.

This is not an issue for organization or repository-wide auto-prune policies. This known issue only exists at the registry level. It will be fixed in a future version of Red Hat Quay.

1.11.3.2. Unrecognizable auto-prune tag patterns

When creating an auto-prune policy, the pruner cannot recognize `\b` and `\B` patterns. This is a common behavior with regular expression patterns, wherein `\b` and `\B` match empty strings. Red Hat Quay administrators should avoid using *regex* patterns that use `\B` and `\b` to avoid this issue. ([PROJQUAY-8089](#))

1.11.4. Red Hat Quay v2 UI known issues

The Red Hat Quay team is aware of the following known issues on the v2 UI:

- [PROJQUAY-6910](#). The new UI can't group and stack the chart on usage logs
- [PROJQUAY-6909](#). The new UI can't toggle the visibility of the chart on usage log
- [PROJQUAY-6904](#). "Permanently delete" tag should not be restored on new UI
- [PROJQUAY-6899](#). The normal user can not delete organization in new UI when enable `FEATURE_SUPERUSERS_FULL_ACCESS`
- [PROJQUAY-6892](#). The new UI should not invoke not required stripe and status page
- [PROJQUAY-6884](#). The new UI should show the tip of slack Webhook URL when creating slack notification
- [PROJQUAY-6882](#). The new UI global readonly super user can't see all organizations and image repos
- [PROJQUAY-6881](#). The new UI can't show all operation types in the logs chart
- [PROJQUAY-6861](#). The new UI "Last Modified" of organization always show N/A after target organization's setting is updated
- [PROJQUAY-6860](#). The new UI update the time machine configuration of organization show NULL in usage logs
- [PROJQUAY-6859](#). The new UI remove image repo permission show "undefined" for organization name in audit logs
- [PROJQUAY-6852](#). "Tag manifest with the branch or tag name" option in build trigger setup wizard should be checked by default.
- [PROJQUAY-6832](#). The new UI should validate the OIDC group name when enable OIDC Directory Sync
- [PROJQUAY-6830](#). The new UI should show the sync icon when the team is configured sync team members from OIDC Group

- [PROJQUAY-6829](#). The new UI team member added to team sync from OIDC group should be audited in Organization logs page
- [PROJQUAY-6825](#). Build cancel operation log can not be displayed correctly in new UI
- [PROJQUAY-6812](#). The new UI the "performer by" is NULL of build image in logs page
- [PROJQUAY-6810](#). The new UI should highlight the tag name with tag icon in logs page
- [PROJQUAY-6808](#). The new UI can't click the robot account to show credentials in logs page
- [PROJQUAY-6807](#). The new UI can't see the operations types in log page when quay is in dark mode
- [PROJQUAY-6770](#). The new UI build image by uploading Docker file should support .tar.gz or .zip
- [PROJQUAY-6769](#). The new UI should not display message "Trigger setup has already been completed" after build trigger setup completed
- [PROJQUAY-6768](#). The new UI can't navigate back to current image repo from image build
- [PROJQUAY-6767](#). The new UI can't download build logs
- [PROJQUAY-6758](#). The new UI should display correct operation number when hover over different operation type
- [PROJQUAY-6757](#). The new UI usage log should display the tag expiration time as date format

1.12. RED HAT QUAY BUG FIXES

The following issues were fixed with Red Hat Quay 3.13:

- [PROJQUAY-5681](#). Previously, when configuring an image repository with **Events and Notifications** to receive a Slack notification for **Push to Repository** and **Package Vulnerability Found**, no notification was returned of **new critical image vulnerability found**. This issue has been resolved.
- [PROJQUAY-7244](#). Previously, it was not possible to filter for repositories under specific organizations. This issue has been resolved, and you can now filter for repositories under specific organizations.
- [PROJQUAY-7388](#). Previously, when Red Hat Quay was configured with OIDC authentication using Microsoft Azure Entra ID and team sync was enabled, removing the team sync resulted in the usage logs chart displaying **Undefined**. This issue has been resolved.
- [PROJQUAY-7430](#). Some public container image registries, for example, Google Cloud Registry, generate longer passwords for the login. When this happens, Red Hat Quay could not mirror images from those registries because the password length exceeded the maximum allowed in the Red Hat Quay database.
The actual length limit imposed by the encryption mechanism is lower than **9000**. This implies that while the database can hold up to **9000** characters, the effective limit during encryption is actually **6000**, and be calculated as follows: $\{\text{Max Password Length}\} = \{\text{field_max_length}\} - \{\text{_RESERVED_FIELD_SPACE}\}$. A password length of **6000** ensures compatibility with AWS ECR and most registries.

- [PROJQUAY-7599](#). Previously, attempting to delete a manifest using a tag name and the Red Hat Quay v2 API resulted in a 405 error code. This was because there was no **delete_manifest_by_tagname** operation in the API. This issue has been resolved.
- [PROJQUAY-7606](#). Users can now create a new team using the dashes (-) via the v2 UI. Previously, this could only be done using the API.
- [PROJQUAY-7686](#). Previously, the vulnerability page showed vertical scroll bars when provided URLs in the advisories were too big, which caused difficulties in reading information from the page. This issue has been resolved.
- [PROJQUAY-7982](#). There was a bug in the console service when using Quay.io for the first time. When attempting to create a user correlated with the console's user, clicking **Confirm username** refreshed the page and opened the same modal. This issue has been resolved.

1.13. 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 1.1. New features tracker

Feature	Quay 3.13	Quay 3.12	Quay 3.11
Keyless authentication with robot accounts	General Availability	-	-
Certificate-based authentication between Red Hat Quay and SQL	General Availability	-	-
Splunk HTTP Event Collector (HEC) support	General Availability	General Availability	-
Open Container Initiative 1.1 support	General Availability	General Availability	-
Reassigning an OAuth access token	General Availability	General Availability	-
Creating an image expiration notification	General Availability	General Availability	-
Team synchronization for Red Hat Quay OIDC deployments	General Availability	General Availability	General Availability

Feature	Quay 3.13	Quay 3.12	Quay 3.11
Configuring resources for managed components on OpenShift Container Platform	General Availability	General Availability	General Availability
Configuring AWS STS for Red Hat Quay, Configuring AWS STS for Red Hat Quay on OpenShift Container Platform	General Availability	General Availability	General Availability
Red Hat Quay repository auto-pruning	General Availability	General Availability	General Availability
FEATURE_UI_V2	Technology Preview	Technology Preview	Technology Preview

1.13.1. IBM Power, IBM Z, and IBM® LinuxONE support matrix

Table 1.2. list of supported and unsupported features

Feature	IBM Power	IBM Z and IBM® LinuxONE
Allow team synchronization via OIDC on Azure	Not Supported	Not Supported
Backing up and restoring on a standalone deployment	Supported	Supported
Clair Disconnected	Supported	Supported
Geo-Replication (Standalone)	Supported	Supported
Geo-Replication (Operator)	Supported	Not Supported
IPv6	Not Supported	Not Supported
Migrating a standalone to operator deployment	Supported	Supported
Mirror registry	Supported	Supported
PostgreSQL connection pooling via pgBouncer	Supported	Supported
Quay config editor - mirror, OIDC	Supported	Supported
Quay config editor - MAG, Kinesis, Keystone, GitHub Enterprise	Not Supported	Not Supported
Quay config editor - Red Hat Quay V2 User Interface	Supported	Supported
Quay Disconnected	Supported	Supported

Feature	IBM Power	IBM Z and IBM® LinuxONE
Repo Mirroring	Supported	Supported