Red Hat Quay 3.12

概念验证 - 部署 Red Hat Quay

部署 Red Hat Quay

Last Updated: 2024-09-19

Red Hat Quay 3.12 概念验证 - 部署 Red Hat Quay

部署 Red Hat Quay

法律通告

摘要

Red Hat Quay 入门

目录

前言

重要

对于生产目的，以下 *概念验证* 部署方法不受支持。此部署类型使用本地存储。在并行访问 Red Hat Quay 所需的存储 registry 时，无法保证提供所需的读写一致性和数据完整性保证。不要将此部署类型用于生产目的。仅用于测试目的。

Red Hat Quay 是一个企业级的 registry，用于构建、保护和提供容器镜像。本节中的文档详细介绍了如何部署 Red Hat Quay *以概念验证* 或非生产目的。本文档的主要目标包括：

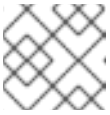
- 如何为基本非生产环境部署 Red Hat Quay。
- 作为 Red Hat Quay 的容器镜像管理，包括如何推送、拉取、标签和组织镜像。
- 探索可用性和可伸缩性。
- 如何使用 SSL/TLS 证书部署高级 Red Hat Quay 概念验证部署。

除了本文档的主要目标之外，可以使用概念验证部署来测试 Red Hat Quay 提供的各种功能，如建立超级用户、设置存储库配额限制、启用 Splunk 进行操作日志存储、启用 Clair 进行漏洞报告等。有关本指南后的一些功能列表，请参阅"下一步"部分。

此概念验证部署步骤可以在一台机器（物理或虚拟）上进行操作。

第 1 章 先决条件

- Red Hat Enterprise Linux (RHEL) 9
  - 要获得 Red Hat Enterprise Linux (RHEL) 9 的最新版本，请参阅 下载 Red Hat Enterprise Linux。
  - 有关安装说明，请参阅 Red Hat Enterprise Linux 9 产品文档 。
- 有效的红帽订阅
- 两个或多个虚拟 CPU
- 4 GB 或更多 RAM
- 测试系统中大约 30 GB 的磁盘空间，可按如下方式划分：
  - Red Hat Enterprise Linux (RHEL)操作系统大约需要 10 GB 磁盘空间。
  - 运行三个容器的 Docker 存储需要大约 10 GB 磁盘空间。
  - Red Hat Quay 本地存储大约需要 10 GB 磁盘空间。



注意

CEPH 或其他本地存储可能需要更多内存。

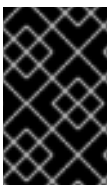
有关大小调整的更多信息，请参阅 Quay 3.x 大小指南。

- Red Hat Quay 支持以下构架：
  - amd64/x86_64
  - s390x
  - ppc64le

1.1. 安装 PODMAN

本文档使用 Podman 来创建和部署容器。

有关 Podman 和相关技术的更多信息，请参阅在 Red Hat Enterprise Linux 9 上构建、运行和管理 Linux 容器。



重要

如果您的系统中没有安装 Podman，可以使用等同的 Docker 命令，但不建议这样做。Docker 尚未通过 Red Hat Quay 3.12 测试，并将在以后的版本中弃用。对于 Red Hat Quay 3.12 的高可用性、生产质量部署，建议使用 podman。

使用以下步骤安装 Podman。

流程

- 输入以下命令安装 Podman：

```
$ sudo yum install -y podman
```

- 另外，您可以安装 **container-tools** 模块，该模块拉取到一组完整的容器软件包：

```
$ sudo yum module install -y container-tools
```

第 2 章 为 RED HAT QUAY 概念验证部署准备 RED HAT ENTERPRISE LINUX

使用以下步骤为 Red Hat Quay 概念验证部署配置 Red Hat Enterprise Linux (RHEL)。

2.1. 安装并注册 RHEL 服务器

使用以下步骤为 Red Hat Quay 概念验证部署配置 Red Hat Enterprise Linux (RHEL)服务器。

流程

1. 安装最新的 RHEL 9 服务器。如果想桌面，您可以执行最小 shell 访问安装，或者 Server 加上 GUI。
2. 注册并订阅您的 RHEL 服务器系统，如 如何使用 Red Hat Subscription-Manager 在红帽客户门户网站中注册和订阅 RHEL 系统
3. 输入以下命令注册您的系统并列出可用的订阅。选择可用的 RHEL 服务器订阅，附加到池 ID，并升级到最新版本：

```
# subscription-manager register --username=<user_name> --password=<password>
# subscription-manager refresh
# subscription-manager list --available
# subscription-manager attach --pool=<pool_id>
# yum update -y
```

2.2. REGISTRY 身份验证

使用以下步骤验证您的 registry 以获取 Red Hat Quay 概念验证。

流程

1. 按照 Red Hat Container Registry Authentication 过程将身份验证设置为 **registry.redhat.io**。通过设置身份验证，您可以拉取 **Quay** 容器。

注意

这与早期版本的 Red Hat Quay 不同，当镜像托管在 Quay.io 上时。

2. 输入以下命令登录到 registry：

```
$ sudo podman login registry.redhat.io
```

您会被会提示输入您的**用户名**和**密码**。

2.3. 防火墙配置

如果您的系统中运行了一个防火墙，您可能需要添加允许访问 Red Hat Quay 的规则。使用以下步骤为概念验证部署配置防火墙。

流程

- 所需的命令取决于您在系统上映射的端口，例如：

```
# firewall-cmd --permanent --add-port=80/tcp \
&& firewall-cmd --permanent --add-port=443/tcp \
&& firewall-cmd --permanent --add-port=5432/tcp \
&& firewall-cmd --permanent --add-port=5433/tcp \
&& firewall-cmd --permanent --add-port=6379/tcp \
&& firewall-cmd --reload
```

2.4. IP 地址和命名服务

在 Red Hat Quay 中配置组件容器有几种方法，以便它们可以相互通信，例如：

- **使用命名服务**。如果您希望部署保留容器重启后（通常是导致更改的 IP 地址），则可以实施命名服务。例如，可以使用 dnsname 插件用于允许容器按名称相互解析。
- **使用主机网络**。您可以使用 **podman run** 命令和-- **net=host** 选项，然后在配置中指定地址时使用主机上的容器端口。当两个容器希望使用相同的端口时，此选项容易出现端口冲突。不建议使用这个方法。
- **配置端口映射**。您可以使用端口映射来公开主机上的端口，然后将这些端口与主机 IP 地址或主机名结合使用。

本文档使用端口映射，并假设您的主机系统的静态 IP 地址。

表 2.1. 概念验证端口映射示例

组件	端口映射	地址
Quy	**-p 80:8080 -p 443:8443**	http://quay-server.example.com
Postgres for Quay	**-p 5432:5432**	quay-server.example.com:5432
Redis	**-p 6379:6379**	quay-server.example.com:6379
postgres 用于 Clair V4	**-p 5433:5432**	quay-server.example.com:5433
Clair V4	**-p 8081:8080**	http://quay-server.example.com:8081

第 3 章 准备您的系统来部署 RED HAT QUAY

对于概念验证 Red Hat Quay 部署，您必须在部署 registry 前配置端口映射、数据库和 Redis。使用以下步骤为您的系统准备部署 Red Hat Quay。

3.1. 为 RED HAT QUAY 配置端口映射

您可以使用端口映射来公开主机上的端口，然后将这些端口与主机 IP 地址或主机名结合使用，以导航到 Red Hat Quay 端点。

流程

1. 输入以下命令为主机系统获取您的静态 IP 地址：

```
$ ip a
```

输出示例

```
---
    link/ether 6c:6a:77:eb:09:f1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.132/24 brd 192.168.1.255 scope global dynamic noprefixroute wlp82s0
---
```

2. 将 IP 地址和本地主机名（例如 **quay-server.example.com** ）添加到 **/etc/hosts** 文件中，该文件将用于访问 Red Hat Quay 端点。您可以输入以下命令确认 IP 地址和主机名已添加到 **/etc/hosts** 文件中：

```
$ cat /etc/hosts
```

输出示例

```
192.168.1.138 quay-server.example.com
```

3.2. 配置数据库

Red Hat Quay 需要一个数据库来存储元数据。PostgreSQL 在整个文档中被使用。对于此部署，使用本地文件系统中的目录来持久保留数据库数据。

使用以下步骤设置 PostgreSQL 数据库。

流程

1. 在安装文件夹中，由 **$QUAY** 变量表示，请输入以下命令为数据库数据创建一个目录：

```
$ mkdir -p $QUAY/postgres-quay
```

2. 输入以下命令设置适当的权限：

```
$ setfacl -m u:26:-wx $QUAY/postgres-quay
```

3. 启动 **Postgres** 容器，使用数据库数据的卷定义指定用户名、密码和数据库名称和端口：

```
$ sudo podman run -d --rm --name postgresql-quay \
  -e POSTGRESQL_USER=quayuser \
  -e POSTGRESQL_PASSWORD=quaypass \
  -e POSTGRESQL_DATABASE=quay \
  -e POSTGRESQL_ADMIN_PASSWORD=adminpass \
  -p 5432:5432 \
  -v $QUAY/postgres-quay:/var/lib/pgsql/data:Z \
  registry.redhat.io/rhel8/postgresql-13:1-109
```

4. 运行以下命令，确保安装了 Postgres **pg_trgm** 模块：

```
$ sudo podman exec -it postgresql-quay /bin/bash -c 'echo "CREATE EXTENSION IF NOT
EXISTS pg_trgm" | psql -d quay -U postgres'
```

注意

Quay 容器需要 **pg_trgm** 模块。

3.3. 配置 REDIS

Redis 是一个键值存储，供 Red Hat Quay 用于实时构建器日志。

使用以下步骤为 Red Hat Quay 概念验证部署 **Redis** 容器。

流程

- 输入以下命令启动 **Redis** 容器，指定端口和密码：

```
$ sudo podman run -d --rm --name redis \
  -p 6379:6379 \
  -e REDIS_PASSWORD=strongpassword \
  registry.redhat.io/rhel8/redis-6:1-110
```

第 4 章 部署 RED HAT QUAY

配置 Red Hat Quay 部署后，您可以按照以下流程部署它。

先决条件

- Red Hat Quay 数据库正在运行。
- Redis 服务器正在运行。

4.1. 创建 YAML 配置文件

使用以下步骤在本地部署 Red Hat Quay。

流程

1. 输入以下命令创建一个用于部署 Red Hat Quay 容器的最小 **config.yaml** 文件：

```
$ touch config.yaml
```

2. 将以下 YAML 配置复制并粘贴到 **config.yaml** 文件中：

```
BUILDLOGS_REDIS:
    host: quay-server.example.com
    password: strongpassword
    port: 6379
CREATE_NAMESPACE_ON_PUSH: true
DATABASE_SECRET_KEY: a8c2744b-7004-4af2-bcee-e417e7bdd235
DB_URI: postgresql://quayuser:quaypass@quay-server.example.com:5432/quay
DISTRIBUTED_STORAGE_CONFIG:
    default:
        - LocalStorage
        - storage_path: /datastorage/registry
DISTRIBUTED_STORAGE_DEFAULT_LOCATIONS: []
DISTRIBUTED_STORAGE_PREFERENCE:
    - default
FEATURE_MAILING: false
SECRET_KEY: e9bd34f4-900c-436a-979e-7530e5d74ac8
SERVER_HOSTNAME: quay-server.example.com
SETUP_COMPLETE: true
USER_EVENTS_REDIS:
    host: quay-server.example.com
    password: strongpassword
    port: 6379
```

3. 创建一个目录来复制 Red Hat Quay 配置捆绑包：

```
$ mkdir $QUAY/config
```

4. 将 Red Hat Quay 配置文件复制到目录中：

```
$ cp -v config.yaml $QUAY/config
```

4.1.1. 配置 Red Hat Quay 超级用户

您可以通过编辑 **config.yaml** 文件来添加超级用户，以添加所需的配置字段。超级用户帐户列表作为数组存储在字段 **SUPER_USERS** 中。超级用户具有以下功能：

- 用户管理
- 机构管理
- 服务密钥管理
- 更改日志透明性
- 使用日志管理
- 全局可见的用户消息创建

流程

1. 将 **SUPER_USERS** 数组添加到 **config.yaml** 文件中：

```
SERVER_HOSTNAME: quay-server.example.com
SETUP_COMPLETE: true
SUPER_USERS:
  - quayadmin (1)
...
```

(1) 如果遵循本指南，请使用 **quayadmin**。

4.2. 为镜像数据准备本地存储

使用以下步骤设置本地文件系统来存储 registry 镜像。

流程

1. 输入以下命令创建一个将存储 registry 镜像的本地目录：

```
$ mkdir $QUAY/storage
```

2. 设置目录以存储 registry 镜像：

```
$ setfacl -m u:1001:-wx $QUAY/storage
```

4.3. 部署 RED HAT QUAY REGISTRY

按照以下步骤部署 **Quay** registry 容器。

流程

1. 输入以下命令启动 **Quay** registry 容器，为配置数据指定适当的卷，并为镜像数据指定本地存储：

```
$ sudo podman run -d --rm -p 80:8080 -p 443:8443  \
```

```
--name=quay \
-v $QUAY/config:/conf/stack:Z \
-v $QUAY/storage:/datastorage:Z \
registry.redhat.io/quay/quay-rhel8:v3.12.2
```

第 5 章 使用 RED HAT QUAY

以下步骤演示了如何使用接口来创建新机构和存储库，以及如何搜索和浏览现有存储库。执行以下步骤 3，您可以使用命令行界面与 registry 交互并推送和拉取镜像。

流程

1. 使用您的浏览器访问位于 **http://quay-server.example.com** 的 Red Hat Quay registry 的用户界面，假设您在 **/etc/hosts** 文件和 **config.yaml** 文件中已将 **quay-server.example.com** 配置为您的主机名。
2. 点 **Create Account** 并添加用户，例如 **quayadmin**，密码为 **password**。
3. 在命令行中登录到 registry：

```
$ sudo podman login --tls-verify=false quay-server.example.com
```

输出示例

```
Username: quayadmin
Password: password
Login Succeeded!
```

5.1. 在 RED HAT QUAY 中推送和拉取镜像

使用以下步骤将镜像推送到 Red Hat Quay registry。

流程

1. 要从 Red Hat Quay registry 中测试推送和拉取镜像，首先从外部 registry 拉取示例镜像：

```
$ sudo podman pull busybox
```

输出示例

```
Trying to pull docker.io/library/busybox...
Getting image source signatures
Copying blob 4c892f00285e done
Copying config 22667f5368 done
Writing manifest to image destination
Storing signatures
22667f53682a2920948d19c7133ab1c9c3f745805c14125859d20cede07f11f9
```

2. 输入以下命令查看镜像的本地副本：

```
$ sudo podman images
```

输出示例

```
REPOSITORY                  TAG      IMAGE ID       CREATED        SIZE
docker.io/library/busybox   latest   22667f53682a   14 hours ago   1.45 MB
```

3. 输入以下命令标记此镜像，这会准备镜像以将其推送到 registry：

```
$ sudo podman tag docker.io/library/busybox quay-
server.example.com/quayadmin/busybox:test
```

4. 将镜像推送到 registry。在这一步后，您可以使用浏览器在存储库中查看标记的镜像。

```
$ sudo podman push --tls-verify=false quay-server.example.com/quayadmin/busybox:test
```

输出示例

```
Getting image source signatures
Copying blob 6b245f040973 done
Copying config 22667f5368 done
Writing manifest to image destination
Storing signatures
```

5. 要从命令行测试对镜像的访问，首先删除镜像的本地副本：

```
$ sudo podman rmi quay-server.example.com/quayadmin/busybox:test
```

输出示例

```
Untagged: quay-server.example.com/quayadmin/busybox:test
```

6. 再次拉取镜像，这次从 Red Hat Quay registry 中拉取镜像：

```
$ sudo podman pull --tls-verify=false quay-server.example.com/quayadmin/busybox:test
```

输出示例

```
Trying to pull quay-server.example.com/quayadmin/busybox:test...
Getting image source signatures
Copying blob 6ef22a7134ba [--------------------------------------] 0.0b / 0.0b
Copying config 22667f5368 done
Writing manifest to image destination
Storing signatures
22667f53682a2920948d19c7133ab1c9c3f745805c14125859d20cede07f11f9
```

5.2. 访问超级用户管理员面板

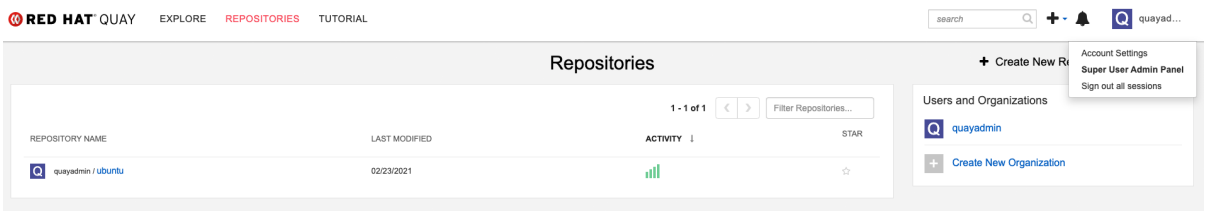
如果您将超级用户添加到 **config.yaml** 文件中，您可以按照以下流程访问 Red Hat Quay UI 上的 **Superuser Admin Panel**。

先决条件

- 您已配置了超级用户。

流程

1. 单击 UI 导航窗格中的当前用户名或 avatar，以访问 Red Hat Quay UI 上的 **Superuser Admin** 面板。然后，单击 **Superuser Admin Panel**。



在本页中，您可以管理用户、您的机构、服务密钥、查看更改日志、查看使用情况日志，并为您的机构创建全局消息。

第 6 章 使用 SSL/TLS 证书进行概念验证部署

使用以下小节配置带有 SSL/TLS 证书的 Red Hat Quay 部署概念验证。

6.1. 使用 SSL/TLS

要使用自签名证书配置 Red Hat Quay，您必须创建一个证书颁发机构(CA)和名为 **ssl.cert** 和 **ssl.key** 的主密钥文件。

6.1.1. 创建证书颁发机构

要使用自签名证书配置 Red Hat Quay，您必须首先创建一个证书颁发机构(CA)。使用以下步骤创建证书颁发机构(CA)。

流程

1. 输入以下命令生成 root CA 密钥：

```
$ openssl genrsa -out rootCA.key 2048
```

2. 输入以下命令生成 root CA 证书：

```
$ openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 1024 -out rootCA.pem
```

3. 输入要合并到证书请求中的信息，包括服务器主机名，例如：

```
Country Name (2 letter code) [XX]:IE
State or Province Name (full name) []:GALWAY
Locality Name (eg, city) [Default City]:GALWAY
Organization Name (eg, company) [Default Company Ltd]:QUAY
Organizational Unit Name (eg, section) []:DOCS
Common Name (eg, your name or your server's hostname) []:quay-server.example.com
```

6.1.1.1. 签署证书

使用以下步骤为证书签名。

流程

1. 输入以下命令生成服务器密钥：

```
$ openssl genrsa -out ssl.key 2048
```

2. 输入以下命令生成签名请求：

```
$ openssl req -new -key ssl.key -out ssl.csr
```

3. 输入要合并到证书请求中的信息，包括服务器主机名，例如：

```
Country Name (2 letter code) [XX]:IE
State or Province Name (full name) []:GALWAY
Locality Name (eg, city) [Default City]:GALWAY
```

```
Organization Name (eg, company) [Default Company Ltd]:QUAY
Organizational Unit Name (eg, section) []:DOCS
Common Name (eg, your name or your server's hostname) []:quay-server.example.com
Email Address []:
```

4. 创建配置文件 **openssl.cnf**，指定服务器主机名，例如：

openssl.cnf

```
[req]
req_extensions = v3_req
distinguished_name = req_distinguished_name
[req_distinguished_name]
[ v3_req ]
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = @alt_names
[alt_names]
DNS.1 = <quay-server.example.com>
IP.1 = 192.168.1.112
```

5. 使用配置文件生成证书 **ssl.cert** ：

```
$ openssl x509 -req -in ssl.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -out
ssl.cert -days 356 -extensions v3_req -extfile openssl.cnf
```

6.2. 配置 SSL/TLS

必须使用命令行界面(CLI)配置 SSL/TLS，并手动更新 **config.yaml** 文件。

6.2.1. 使用命令行界面配置 SSL/TLS

使用以下步骤通过 CLI 配置 SSL/TLS。

先决条件

- 您已创建了证书颁发机构并签署证书。

流程

1. 将证书文件和主密钥文件复制到您的配置目录中，确保它们分别命名为 **ssl.cert** 和 **ssl.key** ：

```
cp ~/ssl.cert ~/ssl.key $QUAY/config
```

2. 输入以下命令进入 **$QUAY/config** 目录：

```
$ cd $QUAY/config
```

3. 编辑 **config.yaml** 文件并指定您希望 Red Hat Quay 处理 TLS/SSL：

config.yaml

```
...
SERVER_HOSTNAME: quay-server.example.com
...
PREFERRED_URL_SCHEME: https
...
```

4. 可选：输入以下命令将 rootCA.pem 文件的内容添加到 ssl.cert 文件的末尾：

```
$ cat rootCA.pem >> ssl.cert
```

5. 输入以下命令停止 **Quay** 容器：

```
$ sudo podman stop quay
```

6. 输入以下命令重启 registry：

```
$ sudo podman run -d --rm -p 80:8080 -p 443:8443 \
  --name=quay \
  -v $QUAY/config:/conf/stack:Z \
  -v $QUAY/storage:/datastorage:Z \
  registry.redhat.io/quay/quay-rhel8:v3.12.2
```

6.3. 测试 SSL/TLS 配置

可以使用命令行界面(CLI)测试您的 SSL/TLS 配置。使用以下步骤测试 SSL/TLS 配置。

6.3.1. 使用 CLI 测试 SSL/TLS 配置

可以使用命令行界面(CLI)测试您的 SSL/TLS 配置。使用以下步骤测试 SSL/TLS 配置。

使用以下步骤通过 CLI 测试 SSL/TLS 配置。

流程

1. 输入以下命令尝试登录到启用了 SSL/TLS 的 Red Hat Quay registry：

```
$ sudo podman login quay-server.example.com
```

输出示例

```
Error: error authenticating creds for "quay-server.example.com": error pinging docker registry
quay-server.example.com: Get "https://quay-server.example.com/v2/": x509: certificate
signed by unknown authority
```

2. 因为 Podman 不信任自签名证书，所以必须使用- **-tls-verify=false** 选项：

```
$ sudo podman login --tls-verify=false quay-server.example.com
```

输出示例

```
Login Succeeded!
```

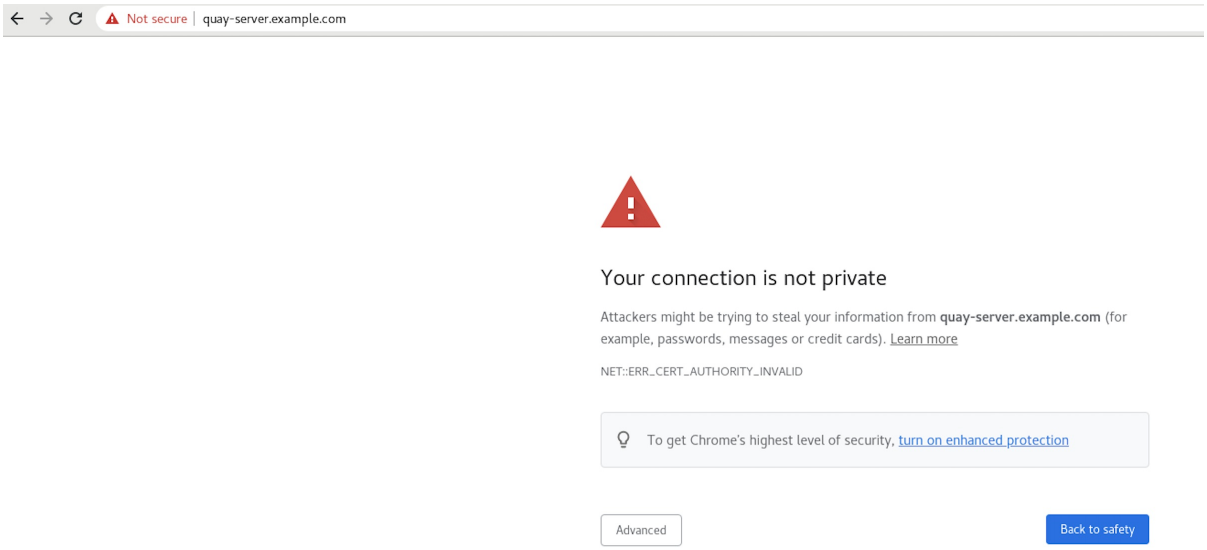
在后面的部分中，您要将 Podman 配置为信任 root 证书颁发机构。

6.3.2. 使用浏览器测试 SSL/TLS 配置

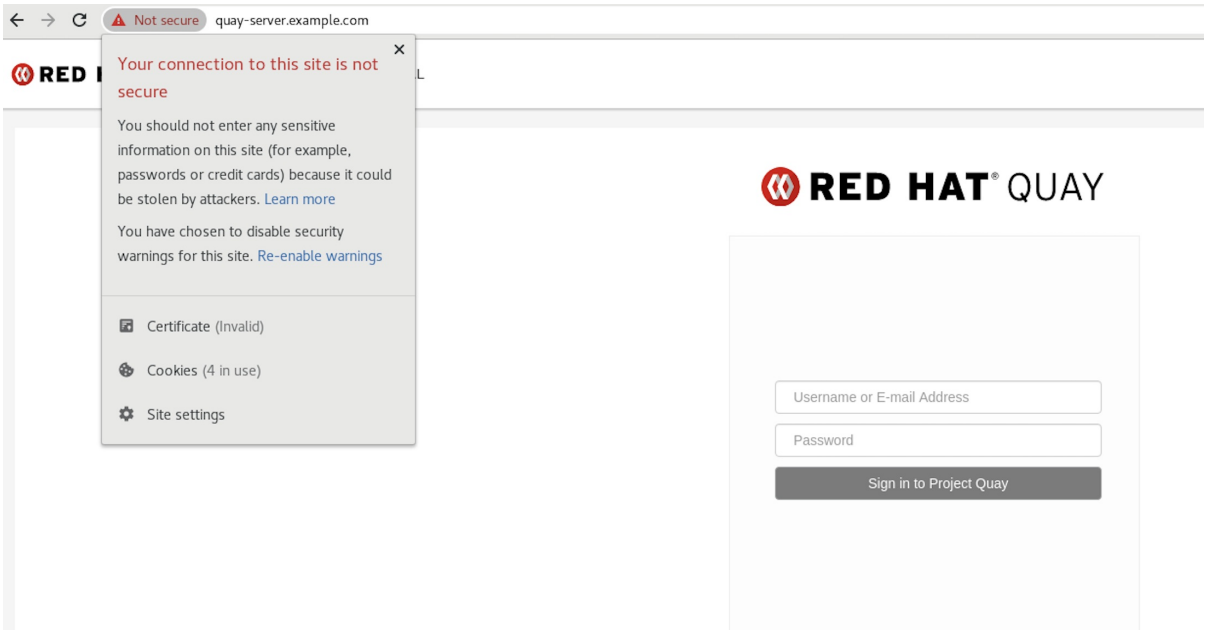
使用以下步骤使用浏览器测试 SSL/TLS 配置。

流程

1. 导航到您的 Red Hat Quay registry 端点，例如 **https://quay-server.example.com**。如果正确配置，浏览器会警告潜在的风险：



2. 继续登录屏幕。浏览器会通知您连接不安全。例如：



在以下部分中，您要将 Podman 配置为信任 root 证书颁发机构。

6.4. 配置 PODMAN 以信任证书颁发机构

Podman 使用两个路径来查找证书颁发机构(CA)文件： **/etc/containers/certs.d/** 和 **/etc/docker/certs.d/**。使用以下步骤将 Podman 配置为信任 CA。

流程

1. 将 root CA 文件复制到 **/etc/containers/certs.d/** 或 **/etc/docker/certs.d/** 之一。使用服务器主机名决定的确切路径，并将文件命名为 **ca.crt** ：

```
$ sudo cp rootCA.pem /etc/containers/certs.d/quay-server.example.com/ca.crt
```

2. 在登录到 Red Hat Quay registry 时，验证您不再需要使用 the **-tls-verify=false** 选项：

```
$ sudo podman login quay-server.example.com
```

输出示例

```
Login Succeeded!
```

6.5. 将系统配置为信任证书颁发机构

使用以下步骤将您的系统配置为信任证书颁发机构。

流程

1. 输入以下命令将 **rootCA.pem** 文件复制到合并的系统范围信任存储中：

```
$ sudo cp rootCA.pem /etc/pki/ca-trust/source/anchors/
```

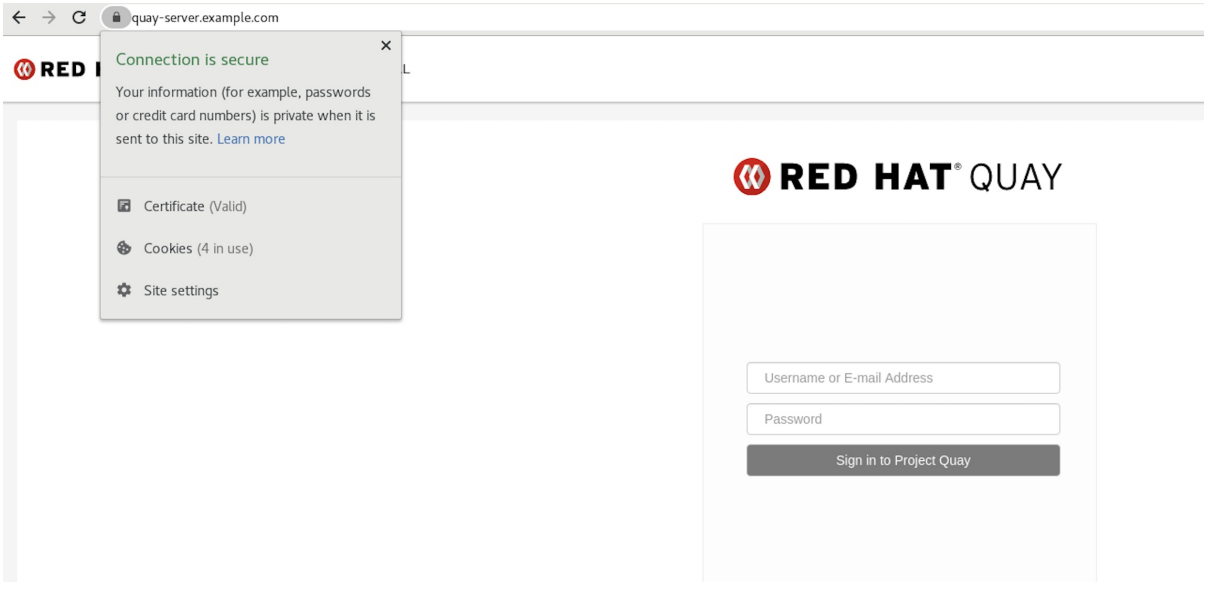
2. 输入以下命令更新系统范围的信任存储配置：

```
$ sudo update-ca-trust extract
```

3. 可选。您可以使用 **trust list** 命令来确保 **Quay** 服务器已配置：

```
$ trust list | grep quay
    label: quay-server.example.com
```

现在，当您通过 **https://quay-server.example.com** 浏览到 registry 时，锁定图标会显示连接安全：



4. 要从系统范围的信任中删除 **rootCA.pem** 文件，请删除该文件并更新配置：

```
$ sudo rm /etc/pki/ca-trust/source/anchors/rootCA.pem
```

```
$ sudo update-ca-trust extract
```

```
$ trust list | grep quay
```

如需更多信息，请参阅 使用共享系统证书的 RHEL 9 文档。

第 7 章 后续步骤

部署 Red Hat Quay 的概念版本后，以下小节可能有用。其中许多流程都可用于概念验证部署，为 Red Hat Quay 的功能提供见解。

- 使用 Red Hat Quay。本指南中的内容解释了以下概念：
  - 添加用户和软件仓库
  - 使用镜像标签
  - 使用构建 worker 构建 Dockerfile
  - 设置构建触发器
  - 为存储库事件添加通知
  - 更多
- 管理 Red Hat Quay.本指南中的内容解释了以下概念：
  - 使用 SSL/TLS
  - 配置操作日志存储
  - 配置 Clair 安全扫描程序
  - 仓库镜像
  - IPv6 和双栈部署
  - 为 Red Hat Quay 配置 OIDC
  - geo-replication
  - 更多