Signup Login

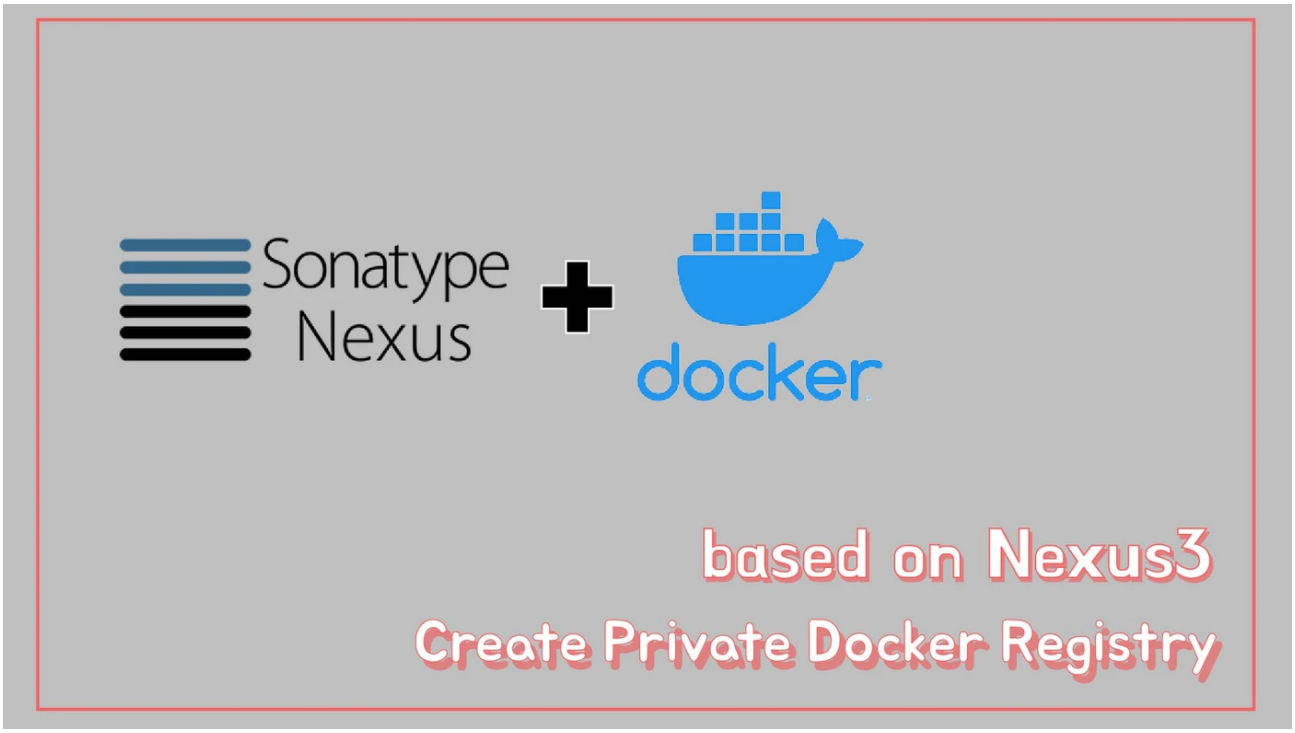
日立がマテリアルズ・インフォマティクスで実現するDX 詳しくはこちら

⚠ **More than 1 year has passed since last update.**

@leechungkyu updated at 2020-02-07

Create Private Docker Registry (base on Nexus3)

Docker, Registry, Nexus, docker-registry, Sonatype



> I will share how to create an Private Docker Registry with Nexus3.x.
> It's built on Nexus and provides GUI environment.

LGTM 1 1

Demo Environment

- Ubuntu 18.04
- Docker version 18.09.1
  - Docker requires at least > v1.8
- Nexus 3.20.1

Install Nexus3 and create Private Docker Registry

> Nexus ip is 182.252.133.70.
>
> ```
> $ ssh root@182.252.133.70
> ```

1) Create Host <-> Nexus container permanent volume

```
$ mkdir /nexus-data
```

2) Create Nexus container

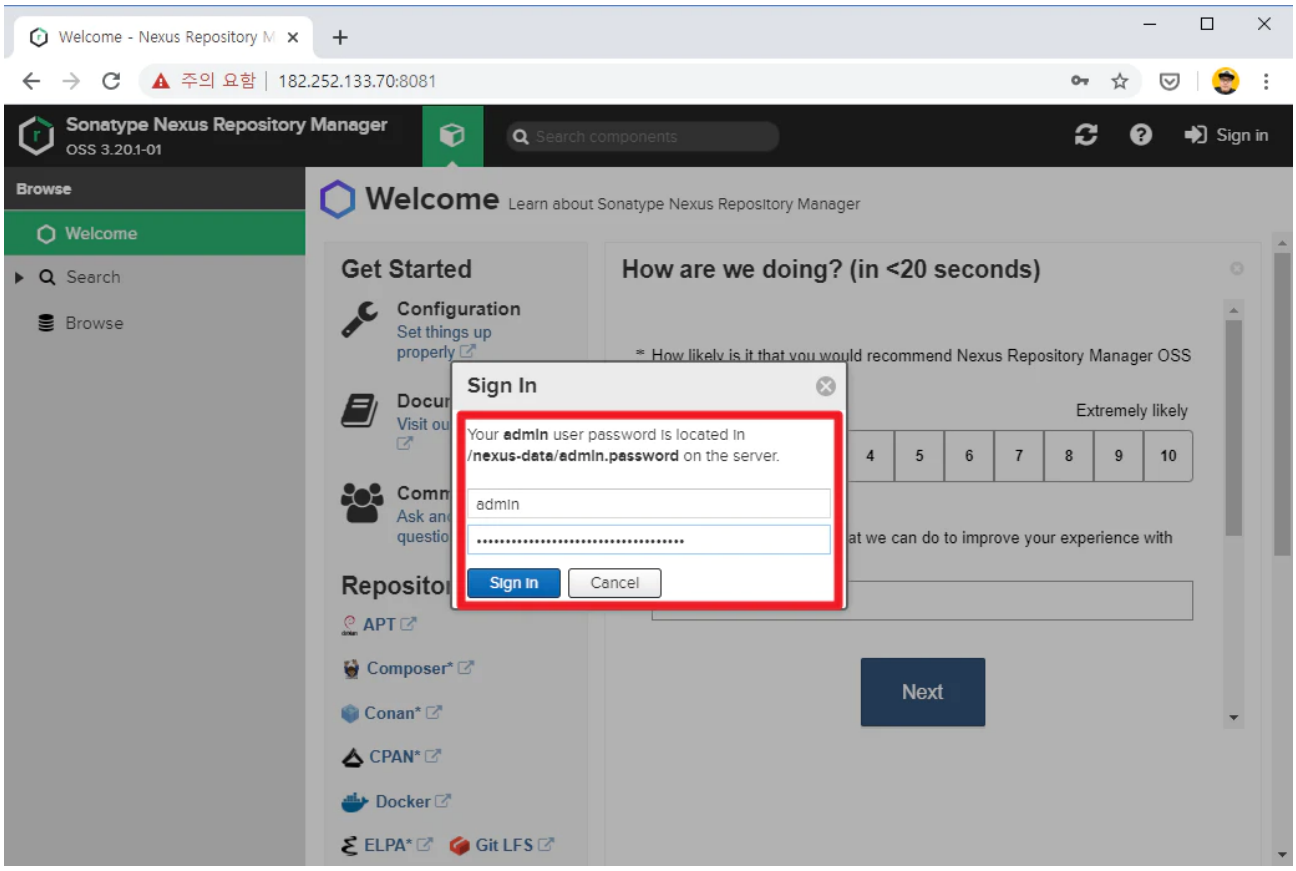
```
$ docker run --name nexus -d -p 5000:5000 -p 8081:8081 -v /nexus-data:/nexus-data -
```

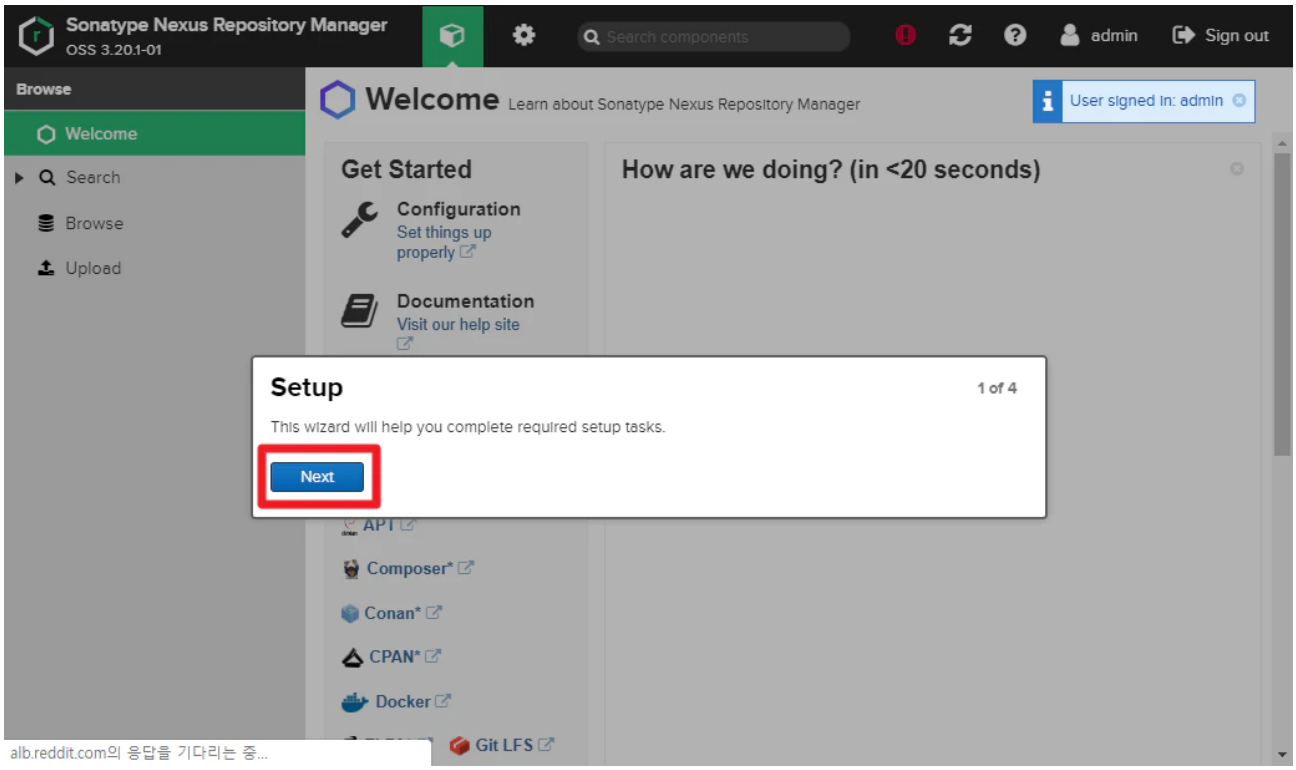
3) Connect to Nexus web http://182.252.133.70:8081

First time, login admin account is required.

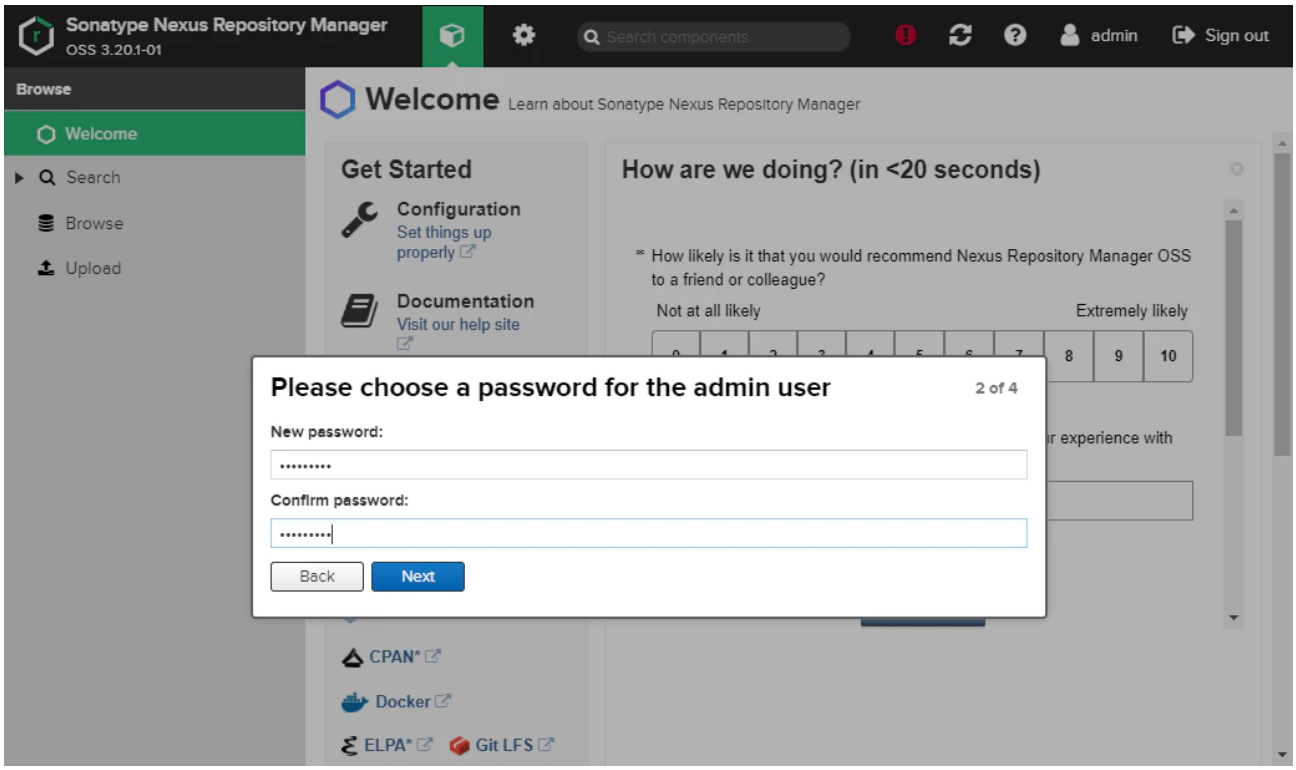
admin password find `/nexus-data/admin.password`

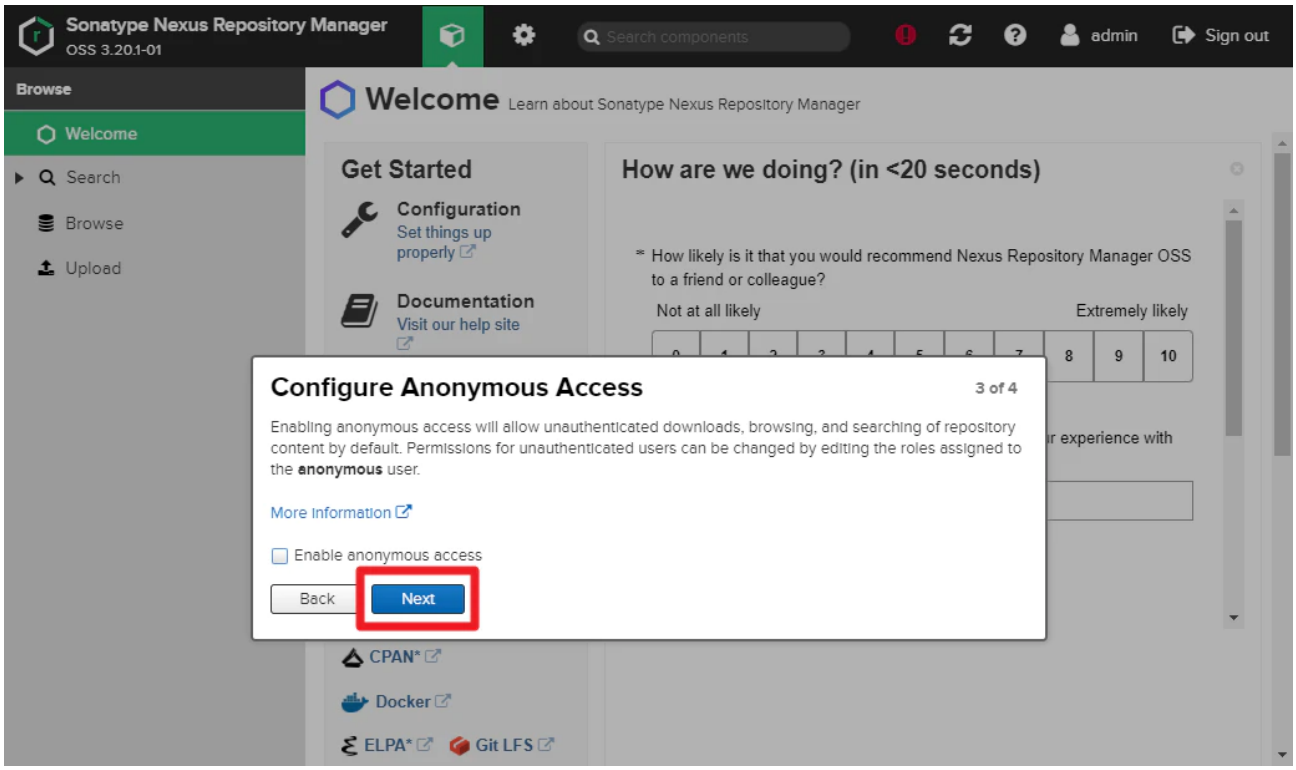
```
$ cat /nexus-data/admin.password
6f471aea-1d52-4e4b-9988-1714e9bf849d # admin's password
```

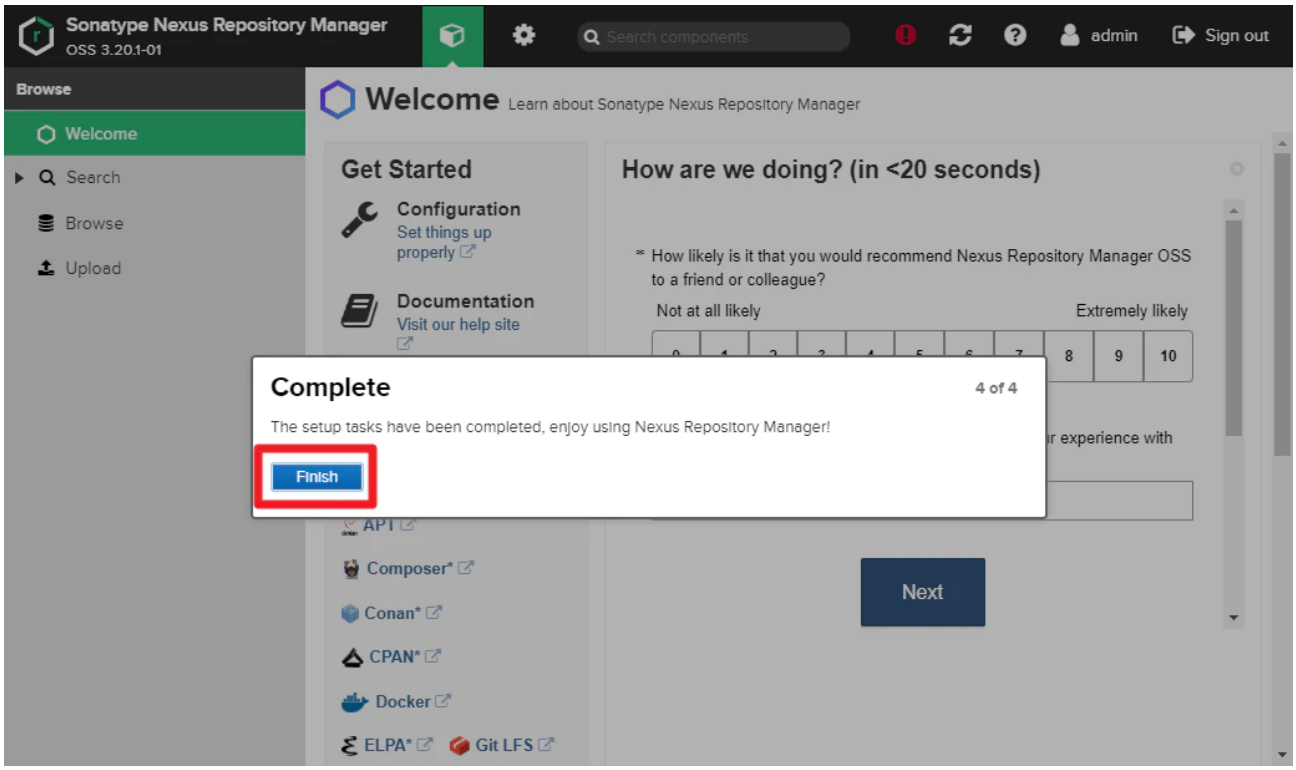




Enter a new admin password.


Sonatype Nexus Repository Manager
OSS 3.20.1-01
Search components
admin
Sign out
Browse
Welcome
Search
Browse
Upload
Welcome
Learn about Sonatype Nexus Repository Manager
Get Started
Configuration
Set things up properly
Documentation
Visit our help site
How are we doing? (in <20 seconds)
* How likely is it that you would recommend Nexus Repository Manager OSS to a friend or colleague?
Not at all likely
Extremely likely
0 1 2 3 4 5 6 7 8 9 10
Please choose a password for the admin user
2 of 4
New password:
Confirm password:
Back
Next
CPAN*
Docker
ELPA*
Git LFS

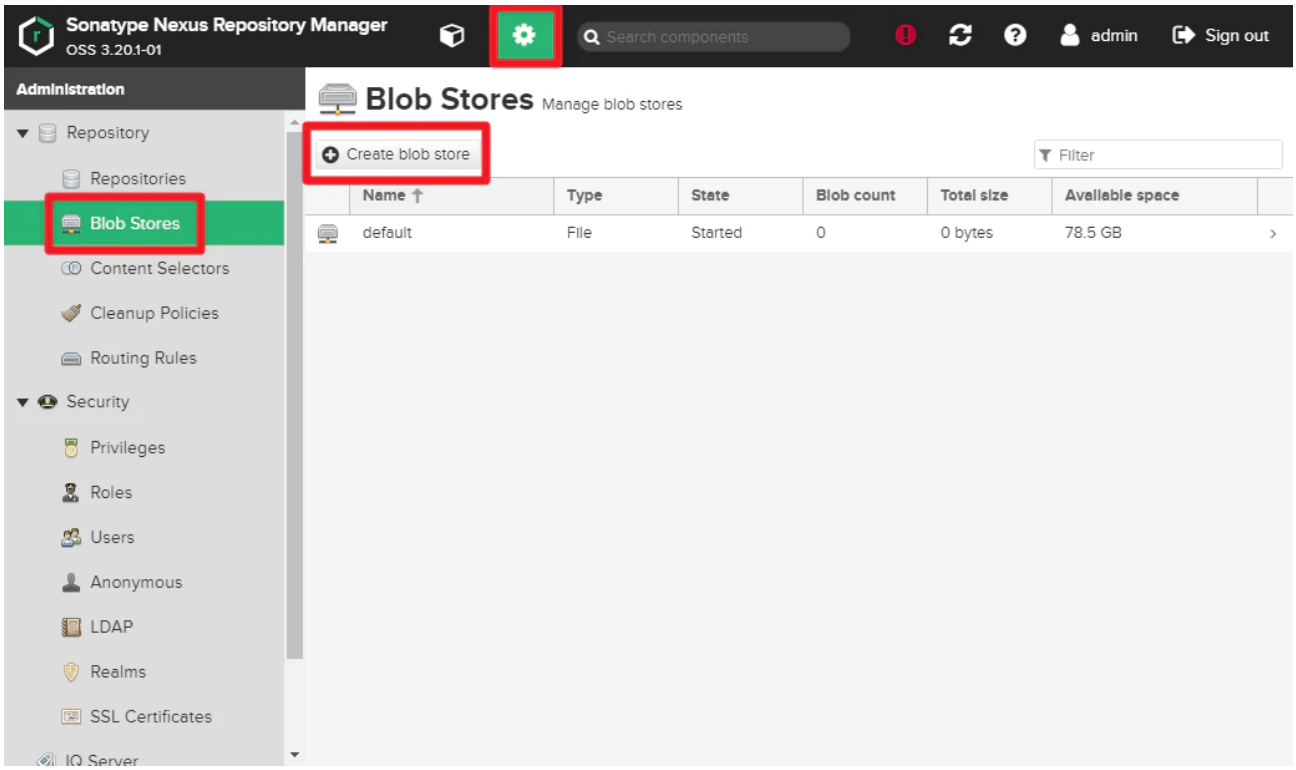

Sonatype Nexus Repository Manager
OSS 3.20.1-01
Search components
admin
Sign out
Browse
Welcome
Search
Browse
Upload
Welcome
Learn about Sonatype Nexus Repository Manager
Get Started
Configuration
Set things up properly
Documentation
Visit our help site
How are we doing? (in <20 seconds)
* How likely is it that you would recommend Nexus Repository Manager OSS to a friend or colleague?
Not at all likely
Extremely likely
0 1 2 3 4 5 6 7 8 9 10
Configure Anonymous Access
3 of 4
Enabling anonymous access will allow unauthenticated downloads, browsing, and searching of repository content by default. Permissions for unauthenticated users can be changed by editing the roles assigned to the anonymous user.
More information
Enable anonymous access
Back
Next
CPAN*
Docker
ELPA*
Git LFS



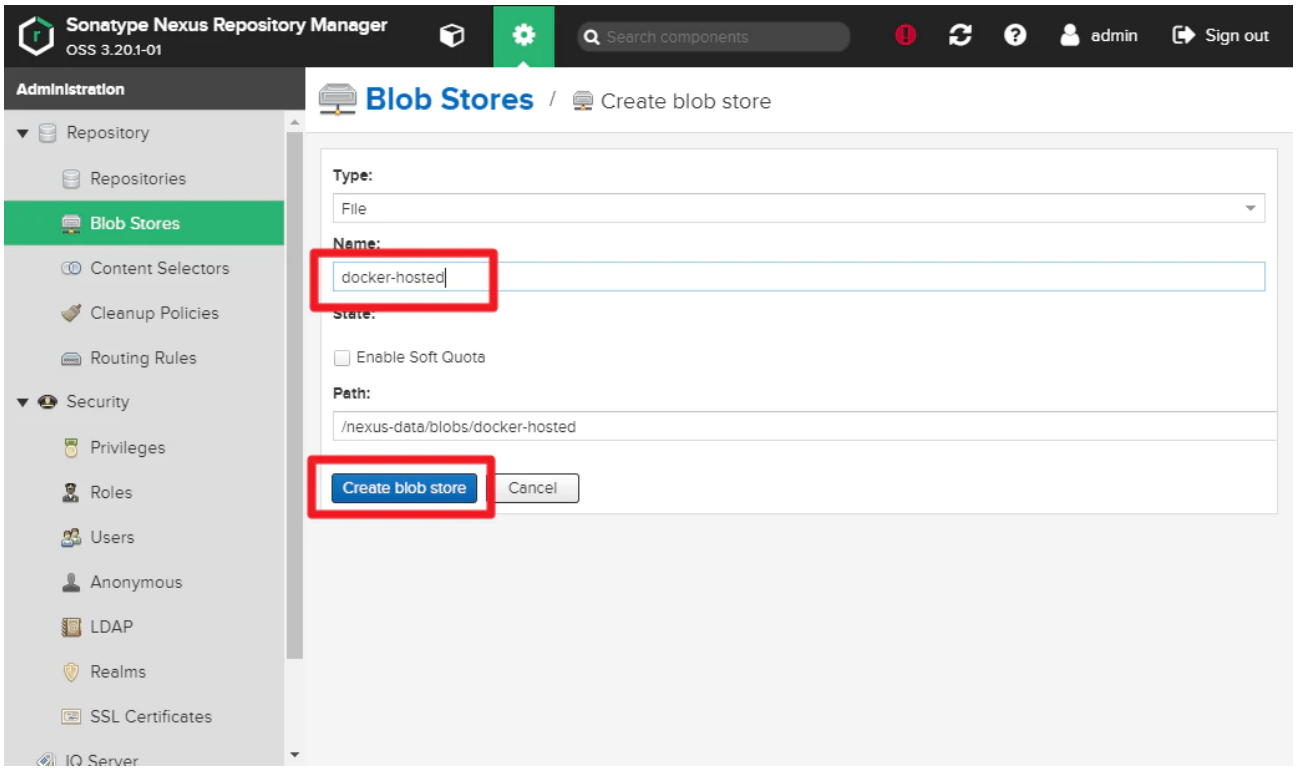
4) Create `docker-hosted` and `docker-proxy` Blob on Nexus

Gear > Repository > Blob Stores > Create blob store

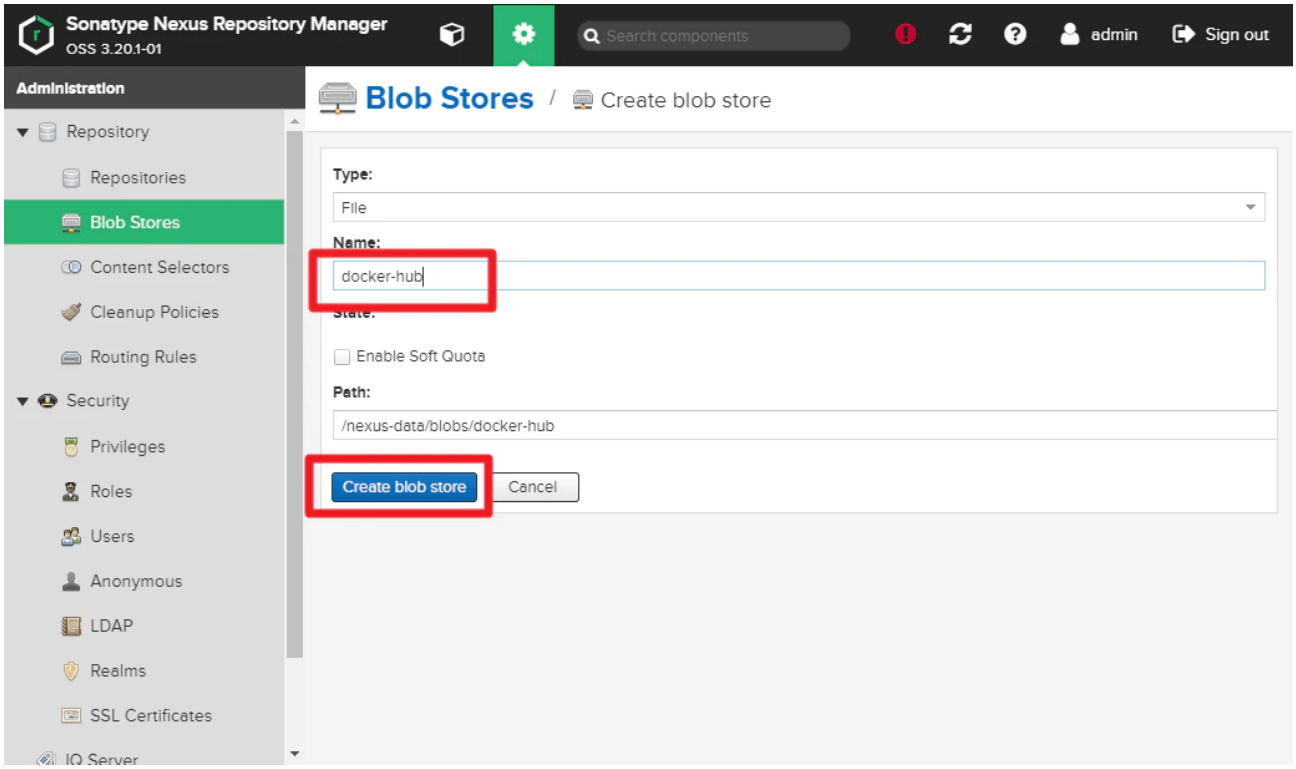
You need to create `docker-hosted` and `docker-hub` .



Name : docker-hosted



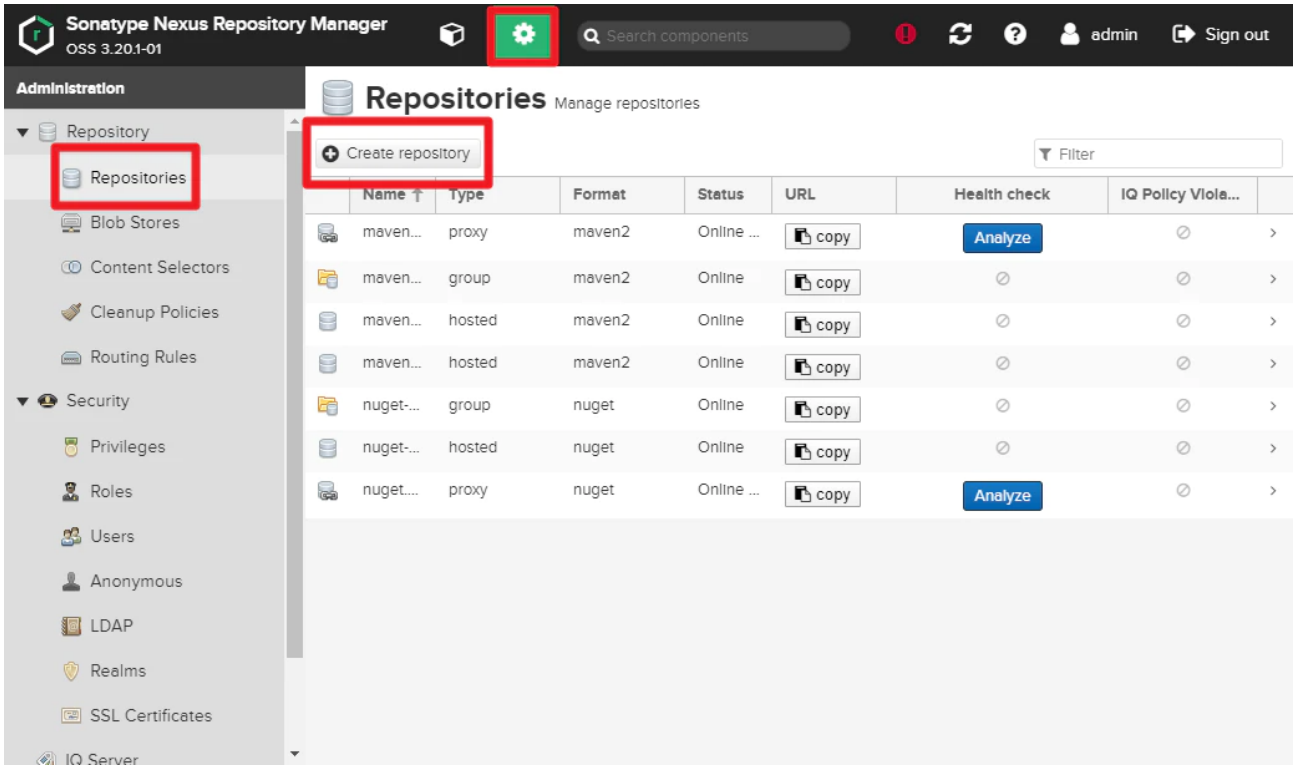
Name : docker-hub



5) Create `docker-hosted` and `docker-proxy` Repository on Nexus

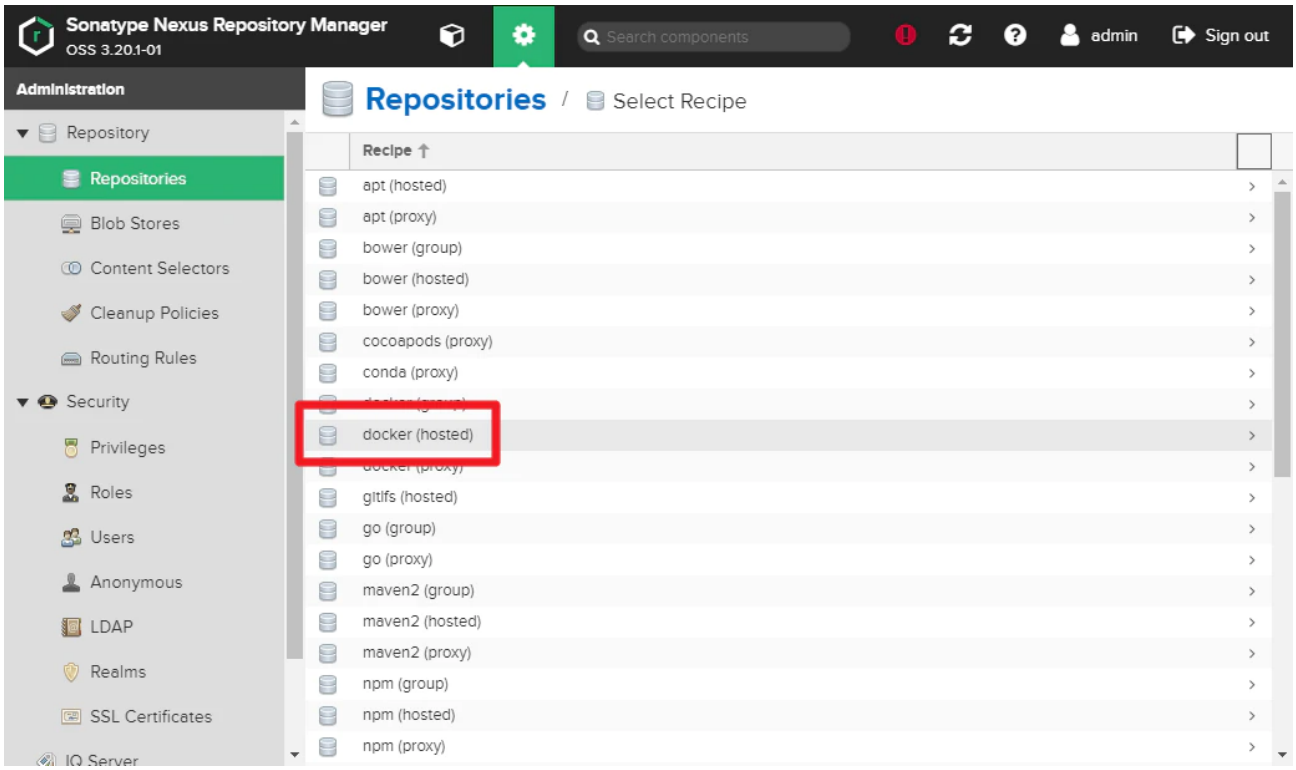
Gear > Repository > Repositories > Create repository

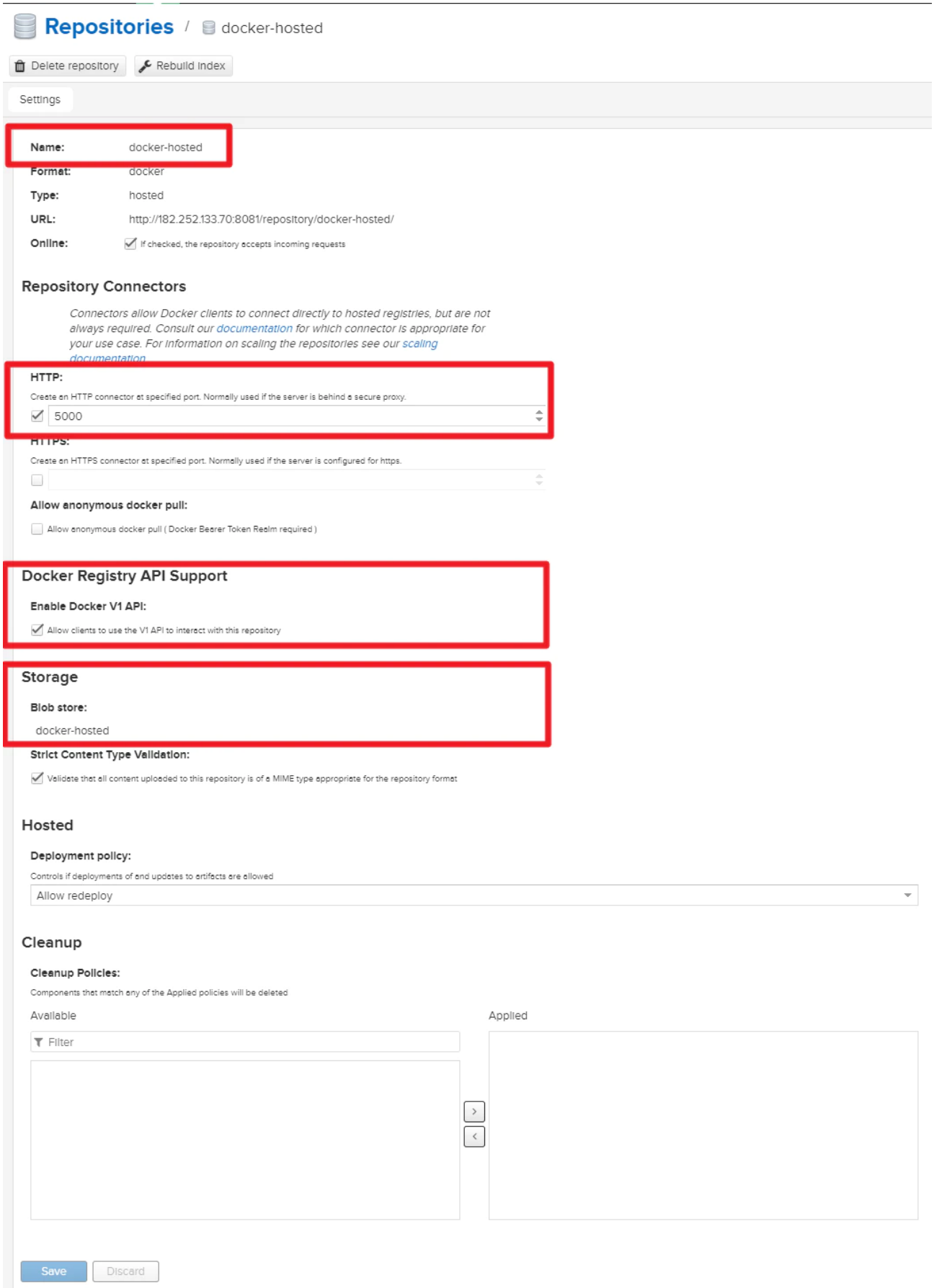
You need to create `docker-hosted` and `docker-hub` .



Select `docker (hosted)`

- Name : `docker-hosted`
- Check HTTP and input 5000
- Check Enable Docker V1 API
- Select Blob store docker-hosted


Sonatype Nexus Repository Manager
OSS 3.20.1-01
Search components
admin
Sign out
Administration
Repository
Repositories
Blob Stores
Content Selectors
Cleanup Policies
Routing Rules
Security
Privileges
Roles
Users
Anonymous
LDAP
Realms
SSL Certificates
IQ Server
Repositories / Select Recipe
Recipe
apt (hosted)
apt (proxy)
bower (group)
bower (hosted)
bower (proxy)
cocoapods (proxy)
conda (proxy)
docker (hosted)
gitlfs (hosted)
go (group)
go (proxy)
maven2 (group)
maven2 (hosted)
maven2 (proxy)
npm (group)
npm (hosted)
npm (proxy)


Repositories / docker-hosted
Delete repository
Rebuild index
Settings
Name: docker-hosted
Format: docker
Type: hosted
URL: http://182.252.133.70:8081/repository/docker-hosted/
Online: If checked, the repository accepts incoming requests
Repository Connectors
Connectors allow Docker clients to connect directly to hosted registries, but are not always required. Consult our documentation for which connector is appropriate for your use case. For information on scaling the repositories see our scaling documentation
HTTP:
Create an HTTP connector at specified port. Normally used if the server is behind a secure proxy.
5000
HTTPS:
Create an HTTPS connector at specified port. Normally used if the server is configured for https.
Allow anonymous docker pull:
Allow anonymous docker pull (Docker Bearer Token Realm required)
Docker Registry API Support
Enable Docker V1 API:
Allow clients to use the V1 API to interact with this repository
Storage
Blob store:
docker-hosted
Strict Content Type Validation:
Validate that all content uploaded to this repository is of a MIME type appropriate for the repository format
Hosted
Deployment policy:
Controls if deployments of and updates to artifacts are allowed
Allow redeploy
Cleanup
Cleanup Policies:
Components that match any of the Applied policies will be deleted
Available
Filter
Applied
Save
Discard

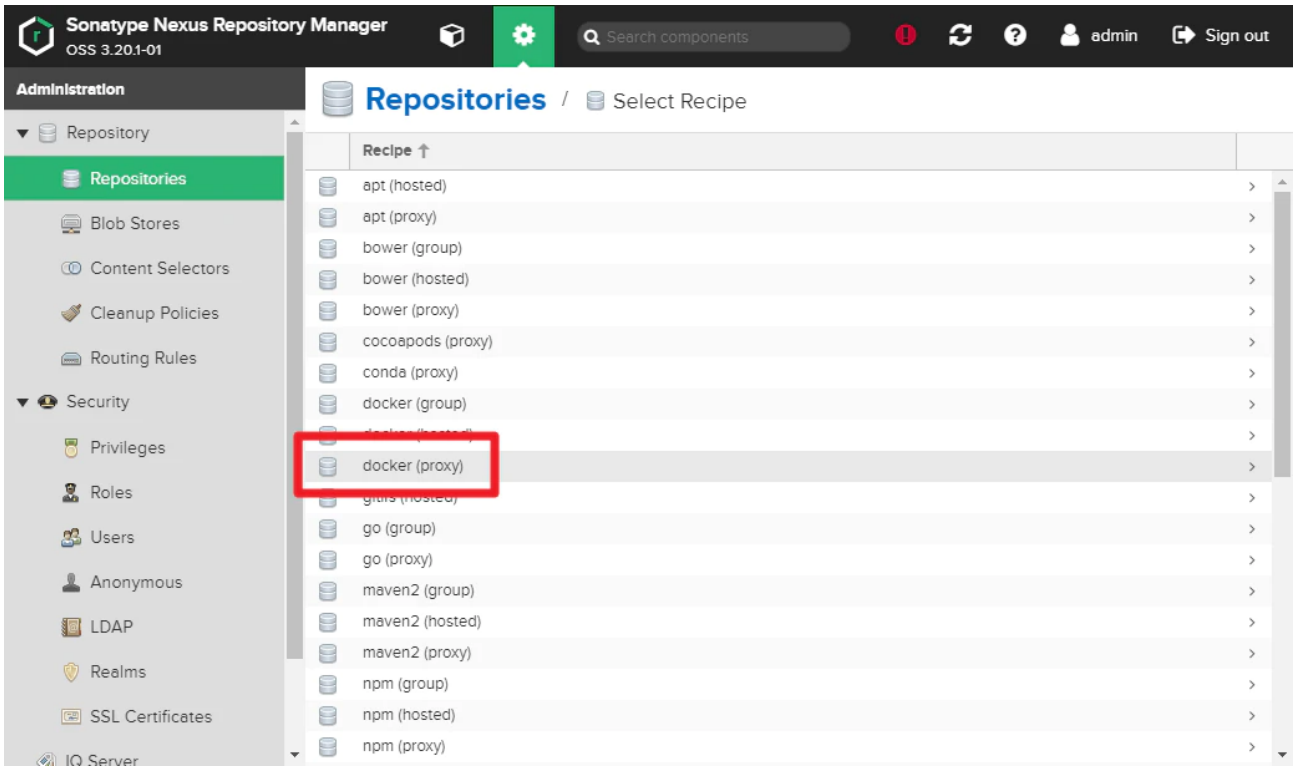
Select `docker (proxy)`

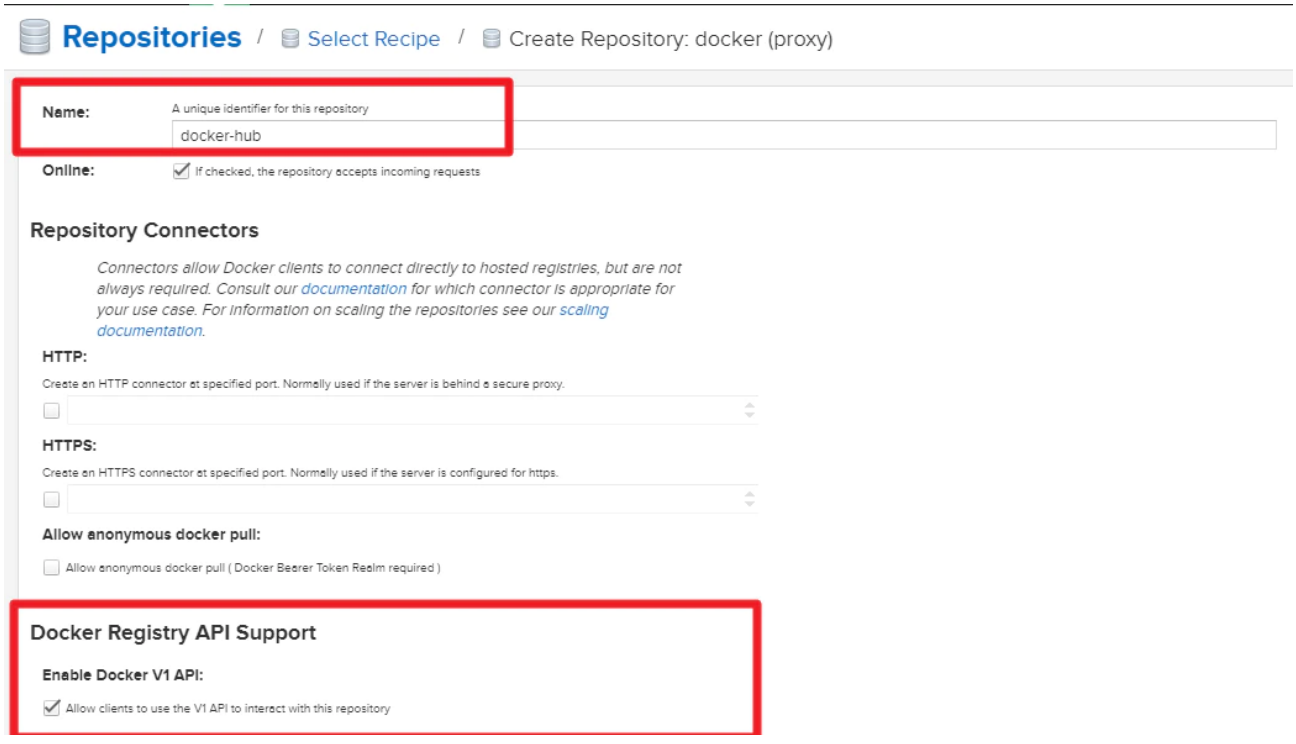
- Name : `docker-hub`

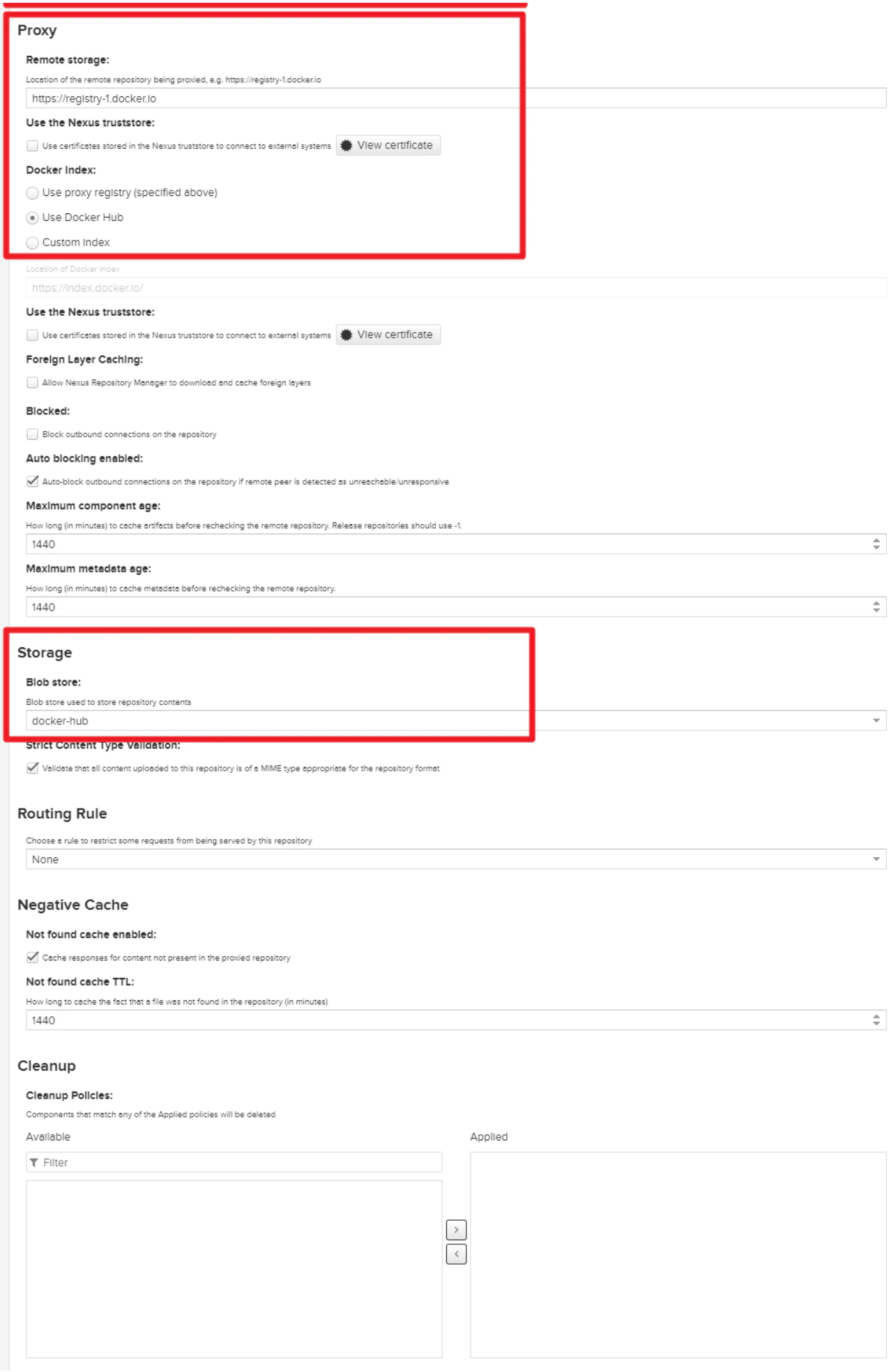
- Check Enable Docker V1 API

- Input `https://registry-1.docker.io` in Remote storage

- Select Use Docker Hub

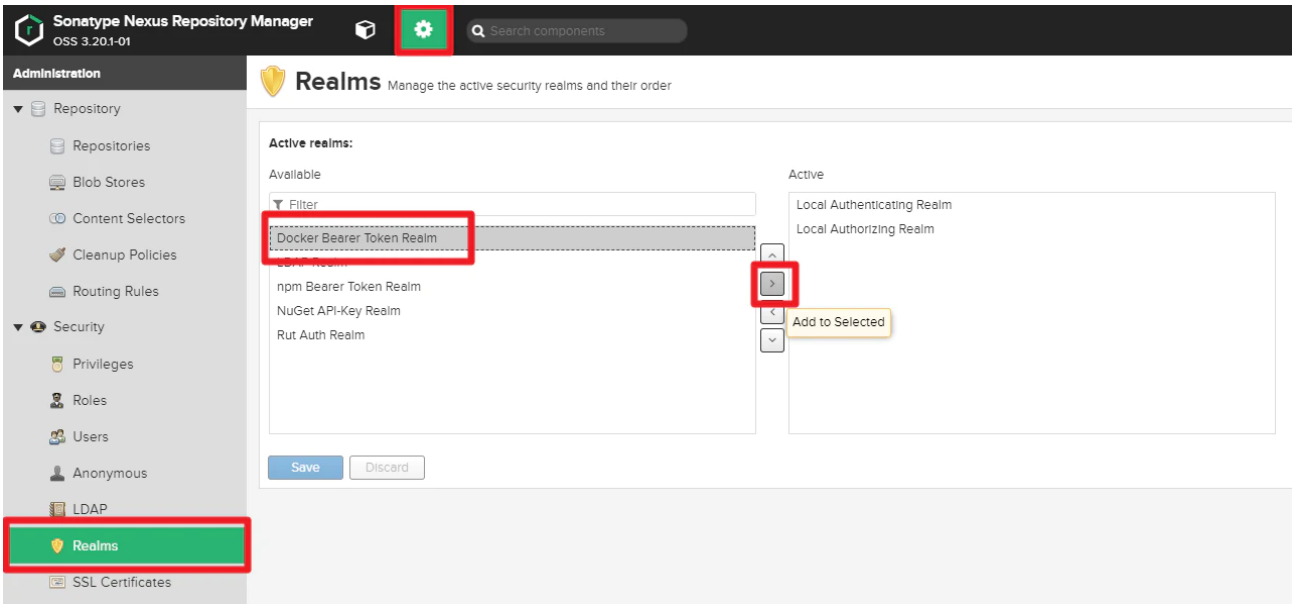


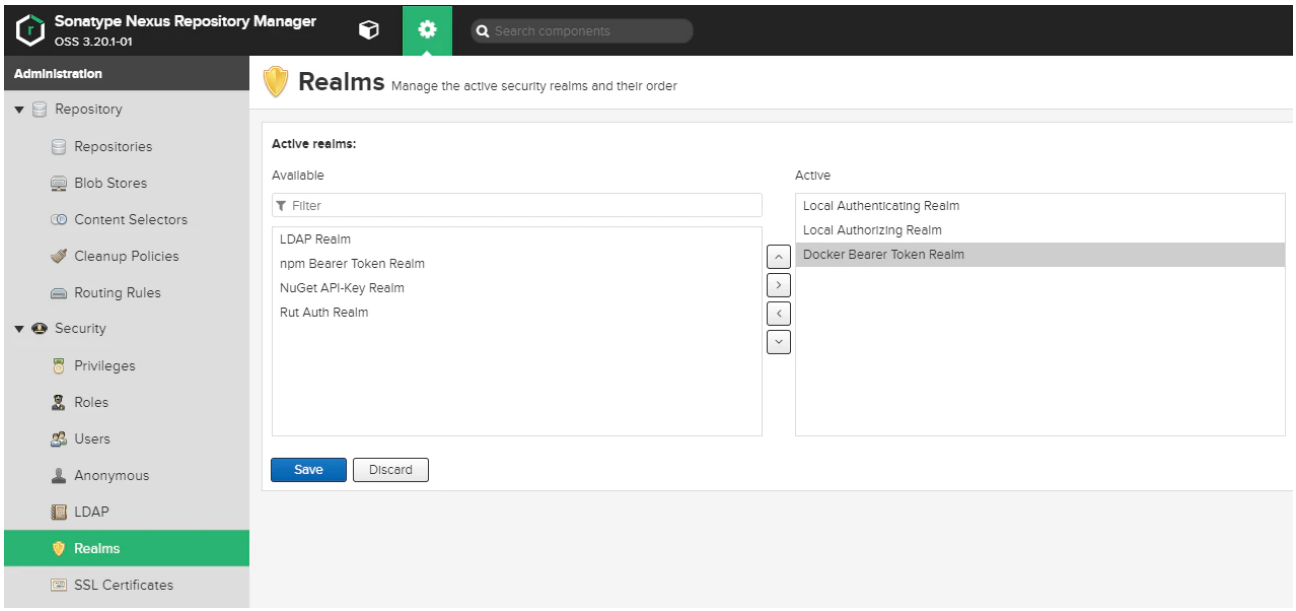



Proxy
Remote storage:
Location of the remote repository being proxied, e.g. https://registry-1.docker.io
https://registry-1.docker.io
Use the Nexus truststore:
Use certificates stored in the Nexus truststore to connect to external systems
View certificate
Docker Index:
Use proxy registry (specified above)
Use Docker Hub
Custom index
Location of Docker index
https://index.docker.io/
Use the Nexus truststore:
Use certificates stored in the Nexus truststore to connect to external systems
View certificate
Foreign Layer Caching:
Allow Nexus Repository Manager to download and cache foreign layers
Blocked:
Block outbound connections on the repository
Auto blocking enabled:
Auto-block outbound connections on the repository if remote peer is detected as unreachable/unresponsive
Maximum component age:
How long (in minutes) to cache artifacts before rechecking the remote repository. Release repositories should use -1.
1440
Maximum metadata age:
How long (in minutes) to cache metadata before rechecking the remote repository.
1440
Storage
Blob store:
Blob store used to store repository contents
docker-hub
Strict Content Type Validation:
Validate that all content uploaded to this repository is of a MIME type appropriate for the repository format
Routing Rule
Choose a rule to restrict some requests from being served by this repository
None
Negative Cache
Not found cache enabled:
Cache responses for content not present in the proxied repository
Not found cache TTL:
How long to cache the fact that a file was not found in the repository (in minutes)
1440
Cleanup
Cleanup Policies:
Components that match any of the Applied policies will be deleted
Available
Filter
Applied

6) Set Realms on Nexus

Gear > Realms > Move `Docker Bearer Token Realm` to active > Save





7) Set docker command http enabled (v1)

Create file `/etc/docker/daemon.json`

✔️ If the file does not exist, you must create it.

```
$ cat /etc/docker/daemon.json
```

```
{
        "insecure-registries" : ["182.252.133.70:5000"]
}
```

Restart docker daemon

```
$ service docker restart
```

Restart Nexus container

```
$ docker restart nexus
```

Push image from external client to Private Docker Registry

> Client ip is 182.252.133.71.
>
> ```
> $ ssh root@182.252.133.71
> ```

1) Set docker command http enabled (v1)

Create file `/etc/docker/daemon.json`

✔️ If the file does not exist, you must create it.

💥 All clients **must** be setting.

```
$ cat /etc/docker/daemon.json
```

```
{
        "insecure-registries" : ["182.252.133.70:5000"]
}
```

Restart docker daemon

```
$ service docker restart
```

2) Login Private Docker Registry

```
$ docker login 182.252.133.70:5000
```

```
Username: admin
Password:
WARNING! Your password will be stored unencrypted in /root/.docker/config.json.
Configure a credential helper to remove this warning. See
https://docs.docker.com/engine/reference/commandline/login/#credentials-store

Login Succeeded
```

3) docker pull and push Private Docker Registry

docker pull busybox image (from https://hub.docker.com/_/busybox)

```
$ docker pull busybox # docker pull from hub.docker.com
bdbbaa22dec6: Pull complete
Digest: sha256:6915be4043561d64e0ab0f8f098dc2ac48e077fe23f488ac24b665166898115a
Status: Downloaded newer image for busybox:latest
docker.io/library/busybox:latest
```

Check busybox image

```
$ docker images -a
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZ
busybox             latest              6d5fcfe5ff17        5 weeks ago         1.2
```

tag

```
$ docker tag 6d5fcfe5ff17 182.252.133.70:5000/busybox:v20200205
```

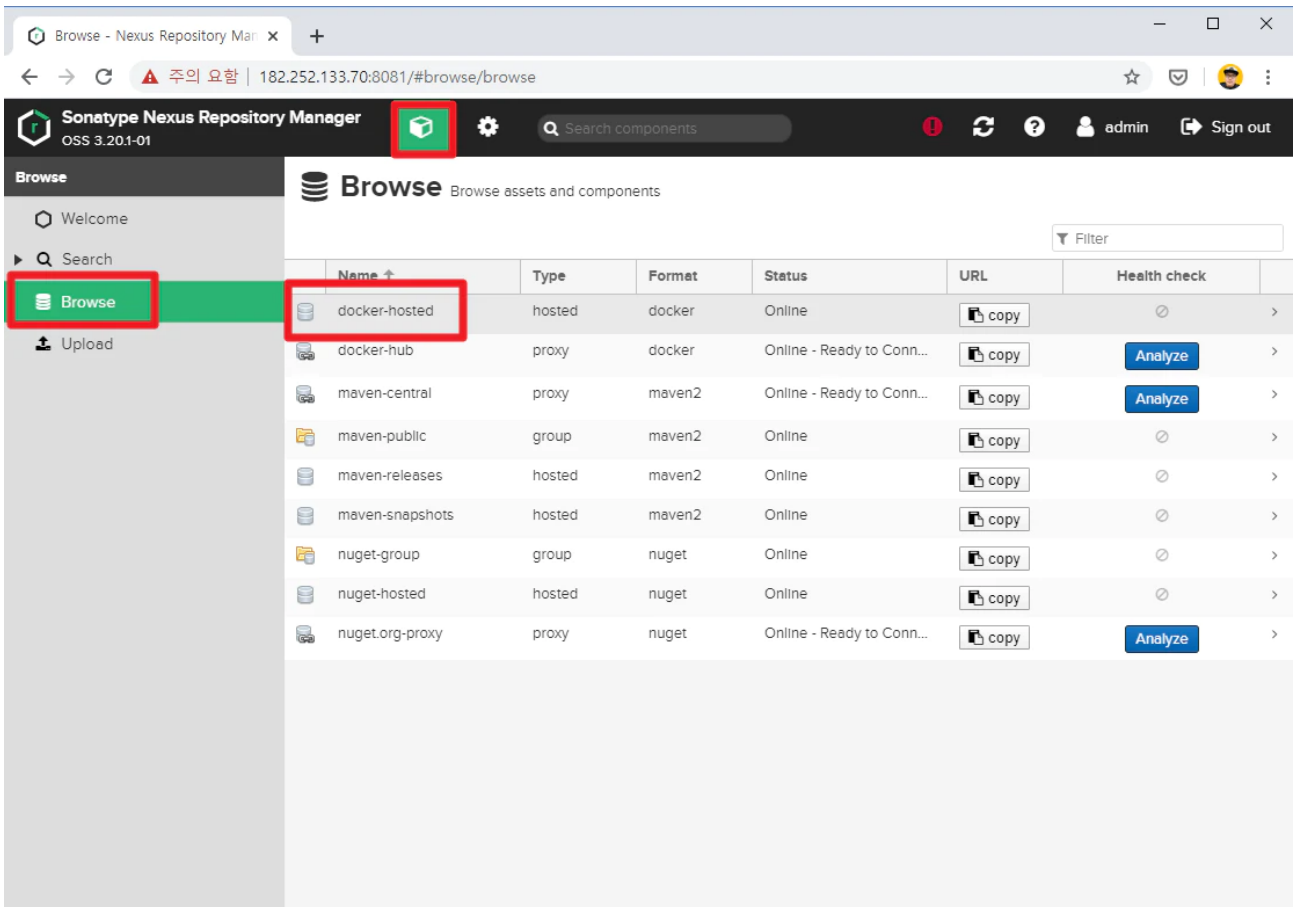
push Private Docker Registry

```
$ docker push 182.252.133.70:5000/busybox:v20200205
The push refers to repository [182.252.133.70:5000/busybox]
195be5f8be1d: Pushed
v20200205: digest: sha256:edafc0a0fb057813850d1ba44014914ca02d671ae247107ca70c94db6
```

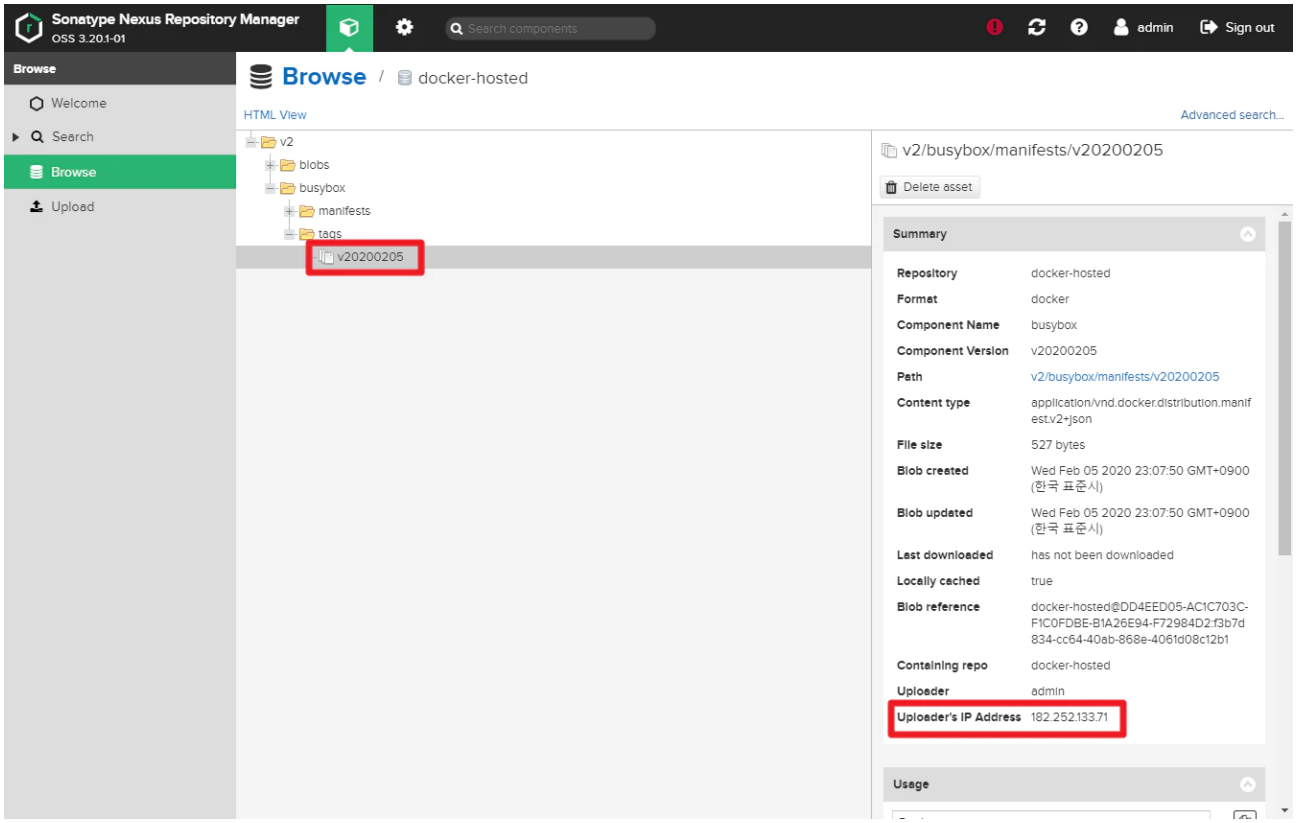
Check image in Private Docker Registry

1) Connect to Nexus web http://182.252.133.70:8081

Browse > docker-hosted



tag



Pull in Private Docker Registry

```
$ docker pull 182.252.133.70:5000/busybox:v20200205
bdbbaa22dec6: Pull complete
Digest: sha256:edafc0a0fb057813850d1ba44014914ca02d671ae247107ca70c94db686e7de6
Status: Downloaded newer image for 182.252.133.70:5000/busybox:v20200205
182.252.133.70:5000/busybox:v20200205
```

```
$ docker images -a
REPOSITORY                          TAG                 IMAGE ID            CREATED
182.252.133.70:5000/busybox         v20200205           6d5fcfe5ff17        5 weeks ago
```

More to do

> 443 port, need adding SSL

SSL should be applied.

After that, creating file `/etc/docker/daemon.json` can be omiited.

💡 I'll write this next posting.

Why not register and get more from Qiita?

Sign up

Login

ChungKyu Lee

@leechungkyu

I like Qiita.

Follow