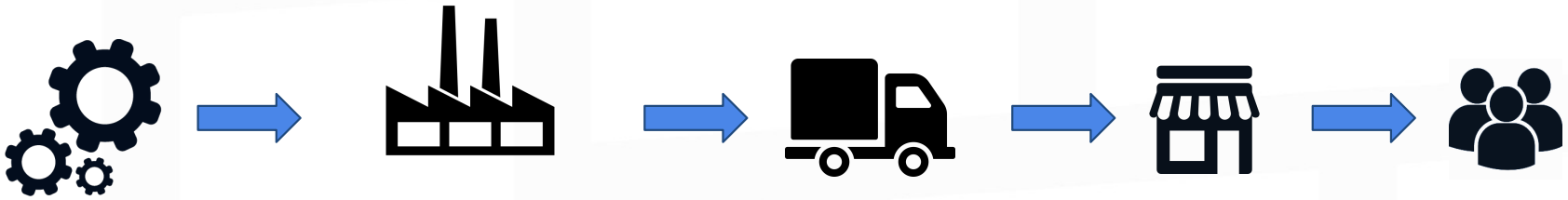
Securing your software supply chain

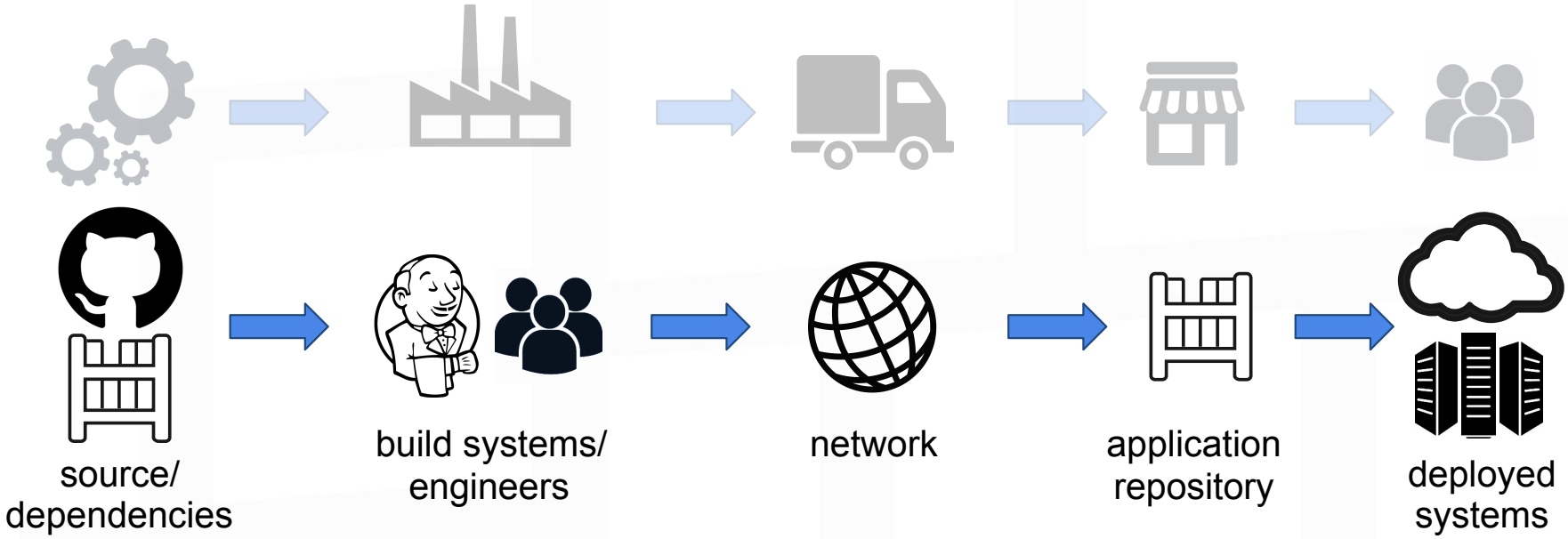
David Lawrence
Ying Li
Security Engineers

dockercon 16

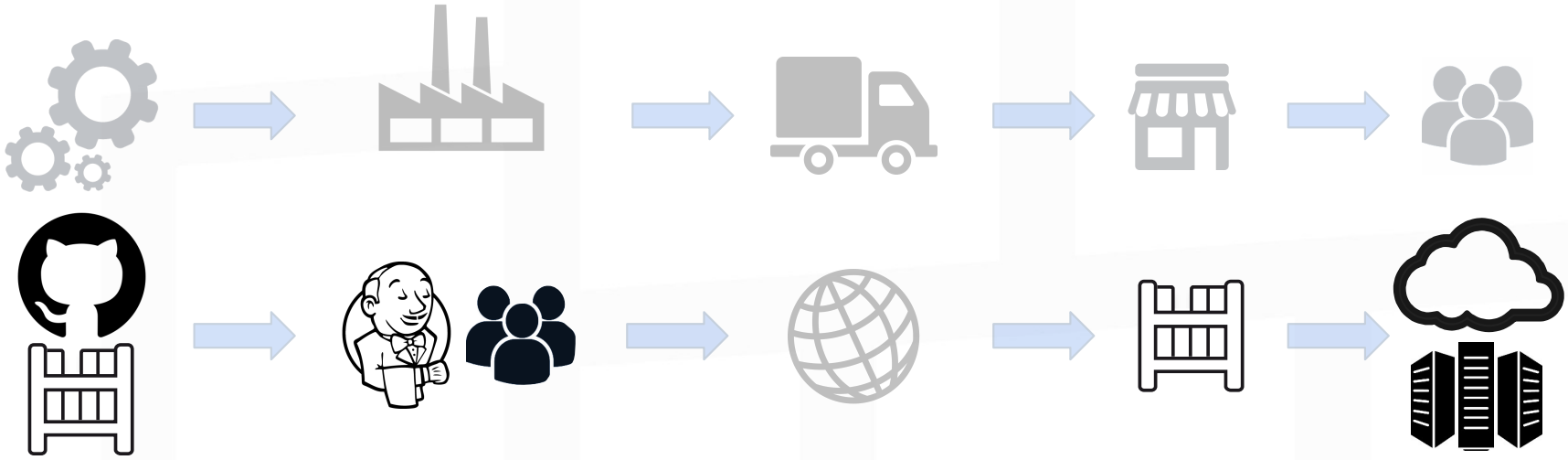
Cat Laser/Cam™ Supply Chain



Software Supply Chain



Identity



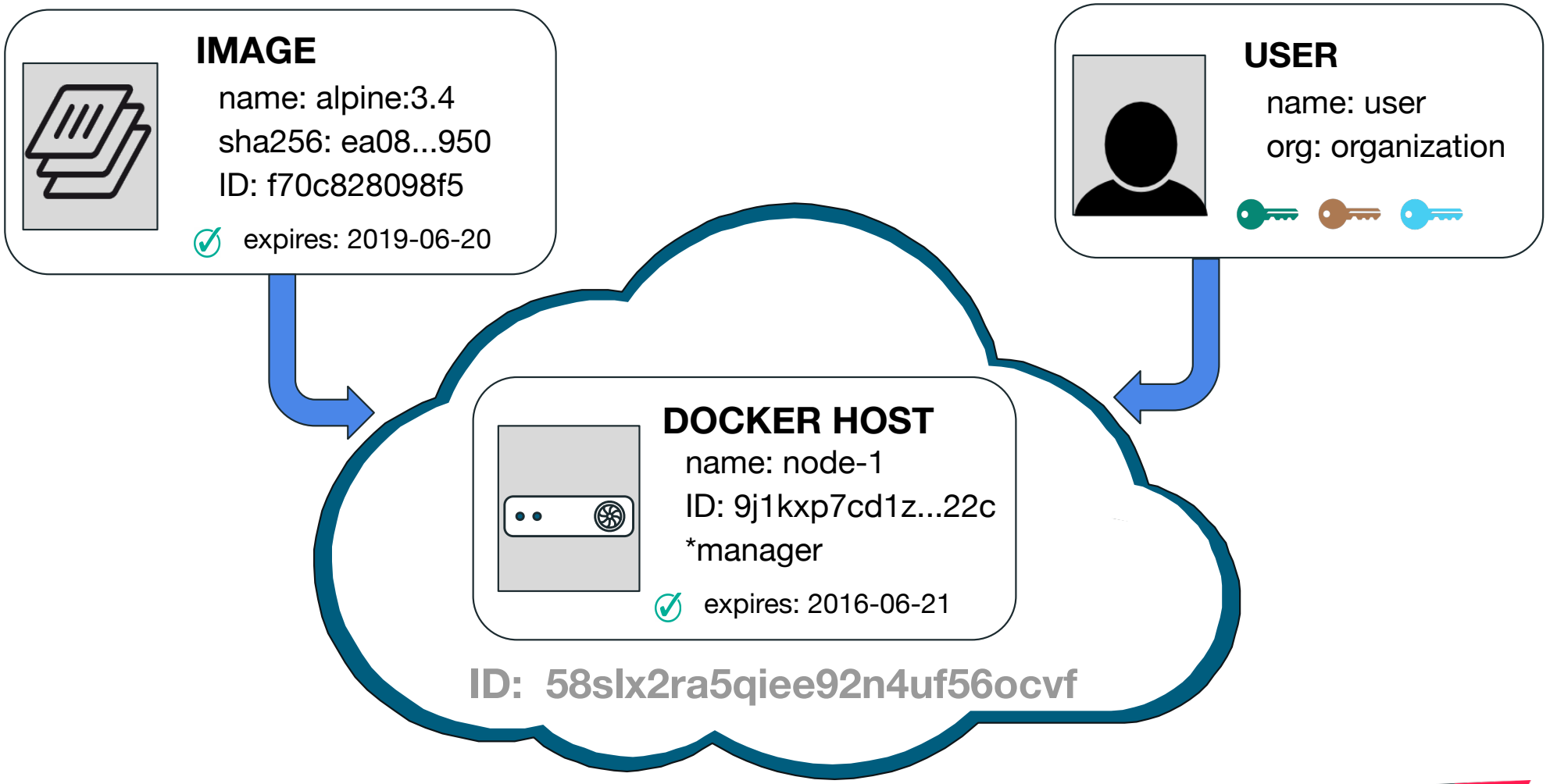


IMAGE
name: alpine:3.4
sha256: ea08...950
ID: f70c828098f5
expires: 2019-06-20
USER
name: user
org: organization
DOCKER HOST
name: node-1
ID: 9j1kxp7cd1z...22c
*manager
expires: 2016-06-21
ID: 58slx2ra5qiee92n4uf56ocvf

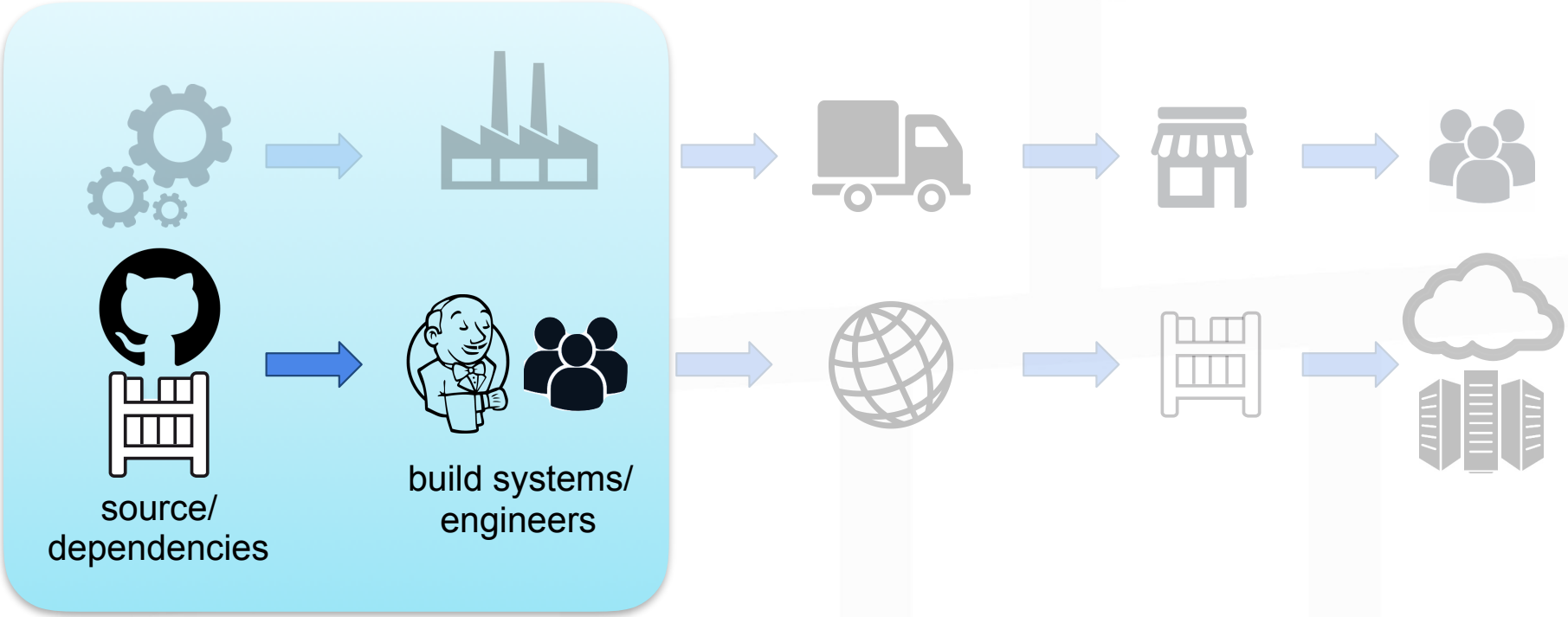
```
$ docker login docker.io
Username (user): user
Password:
Login Succeeded


$ notary -d ~/.docker/trust key list
    ROLE          GUN                      KEY ID                  LOCATION
-------------------------------------------------------------------------------
  root                          5f8ec4acd0a9ca301ef84ac...587       file (...)
  targets      user/myrepo       71662d563fc1dfd0a83c5b3...9ce       file (...)
  user                          d73b1075076e39a0c3ed638...05e       file (...)
```

```
$ swarmctl node ls

ID                         Name    Membership  Status  Availability  Manager Status
--                         ----    ----------  ------  ------------  --------------
3w8pfmhn6janhhzg7pu7ktxd2  node-3  ACCEPTED    READY   ACTIVE
9dva02k3khzbrgyok9dqwvv2m  node-2  ACCEPTED    READY   ACTIVE
9j1kxp7cd1zs7a2njgyz6q22c  node-1  ACCEPTED    READY   ACTIVE       REACHABLE *
```

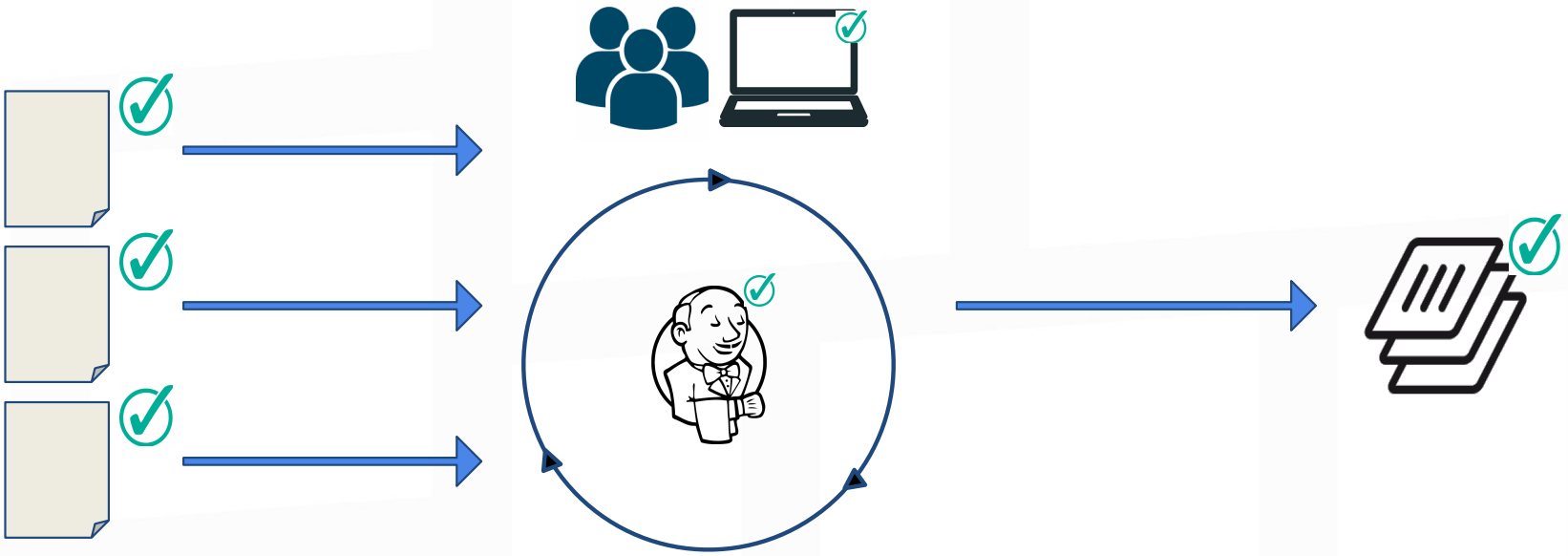
```
$ openssl x509 -in node-3/certificates/swarm-node.crt -text
Certificate:
    ...
    Issuer: CN=swarm-ca
    Validity
      Not Before: Jun 17 20:30:00 2016 GMT
      Not After : Sep 15 20:30:00 2016 GMT
    Subject: O=58slx2ra5qiee92n4uf..., OU=swarm-worker, CN=3w8pfmhn6janhhzg7pu7ktxd2
    ...
    X509v3 extensions:
      ...
      X509v3 Subject Alternative Name:
        DNS:swarm-worker
...
-----BEGIN CERTIFICATE-----
...
```

```
$ docker images --digests
REPOSITORY     TAG       DIGEST                         IMAGE ID       CREATED...
debian         latest    sha256:e7d38b3517548a1c...0aa   f50f9524513f   8 weeks...
busybox        latest    sha256:4a731fb46adc5cef...a92   47bcc53f74dc   11 days...
user/myrepo    latest    sha256:ea0d1389812f43e4...950   f9858dea7747   6 hours...


$ notary -d ~/.docker/trust list docker.io/user/myrepo
  NAME                  DIGEST                                SIZE (BYTES)    ROLE
------------------------------------------------------------------------------------
 latest   ea0d1389812f43e474c50155ec4914e1b48792...950    1360          targets
```

Consistent Builds



Good Input → Good Output



$ cat dependency_checklist.txt

* quality
* authenticity
* integrity
* freshness
* consistency

```
1 FROM ubuntu:16.04
```

- Use official images
  - * TLS/DCT → authenticity
  - * TLS/DCT → integrity
  - * DCT → freshness
- Pin image version

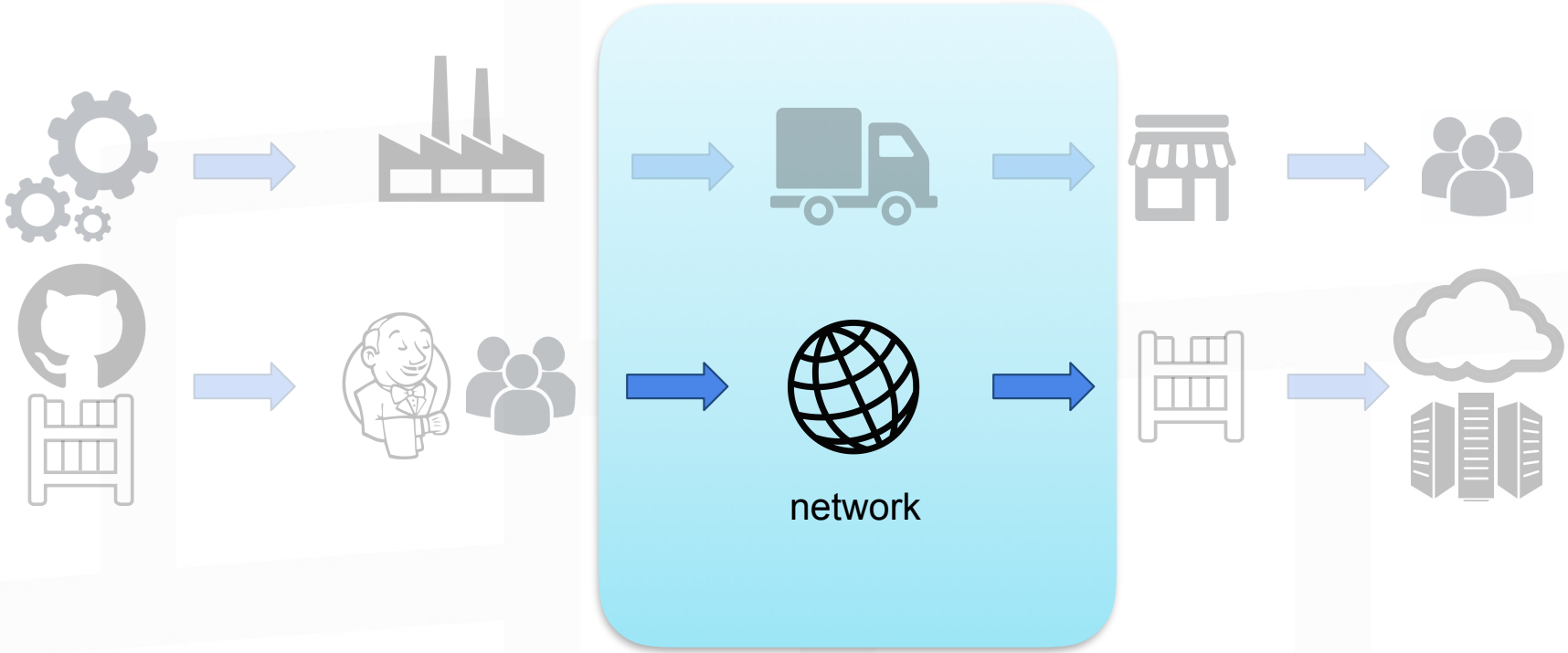
```
1 FROM ubuntu:16.04
2 RUN wget https://<mysite.io>/apt.key \
    && echo "<checksum> apt.key" \
    | shasum -a 256 -c
```

- Use HTTPS
  - * TLS → authenticity
  - * TLS → integrity
- Validate content

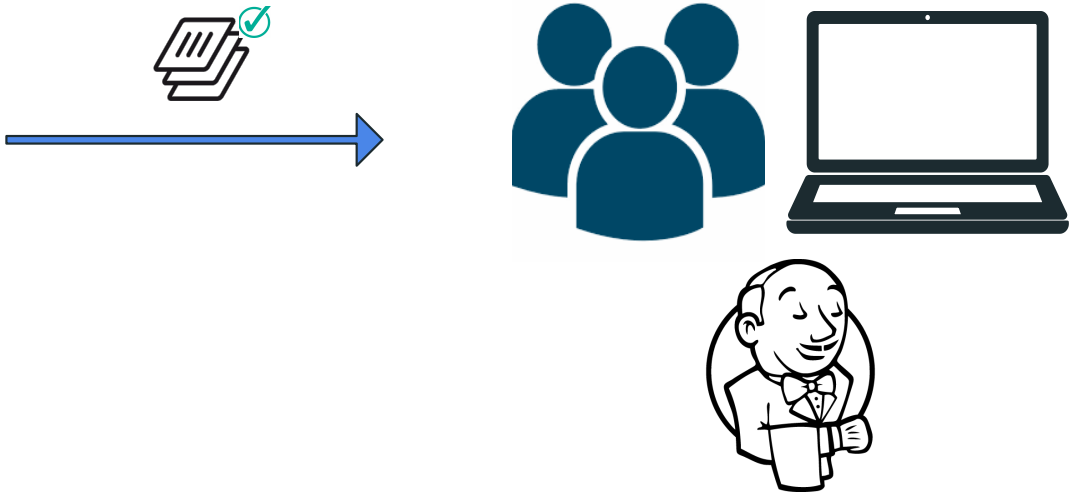
```
3 RUN apt-key add apt.key \
    && add-apt-repository ppa:<mysite.io> \
    && apt-get update \
    && apt-get install mypackage
```

Validate signatures
GPG → integrity
GPG → authenticity

Application Signing



Developer
or CI



```
$ # enable docker content trust

$ export DOCKER_CONTENT_TRUST=1
```

```
$ # protects against untrusted images

$ head -n 1 Dockerfile
FROM user/repo:unsigned

$ docker build -t user/myrailsbase .
No trust data for unsigned
```

$ # protects against maliciously signed images

$ head -n 1 Dockerfile
FROM user/repo:fakesigned

$ docker build -t user/myrailsbase .

Warning: potential malicious behavior - trust data has insufficient signatures for remote repository docker.io/user/repo: valid signatures did not meet threshold

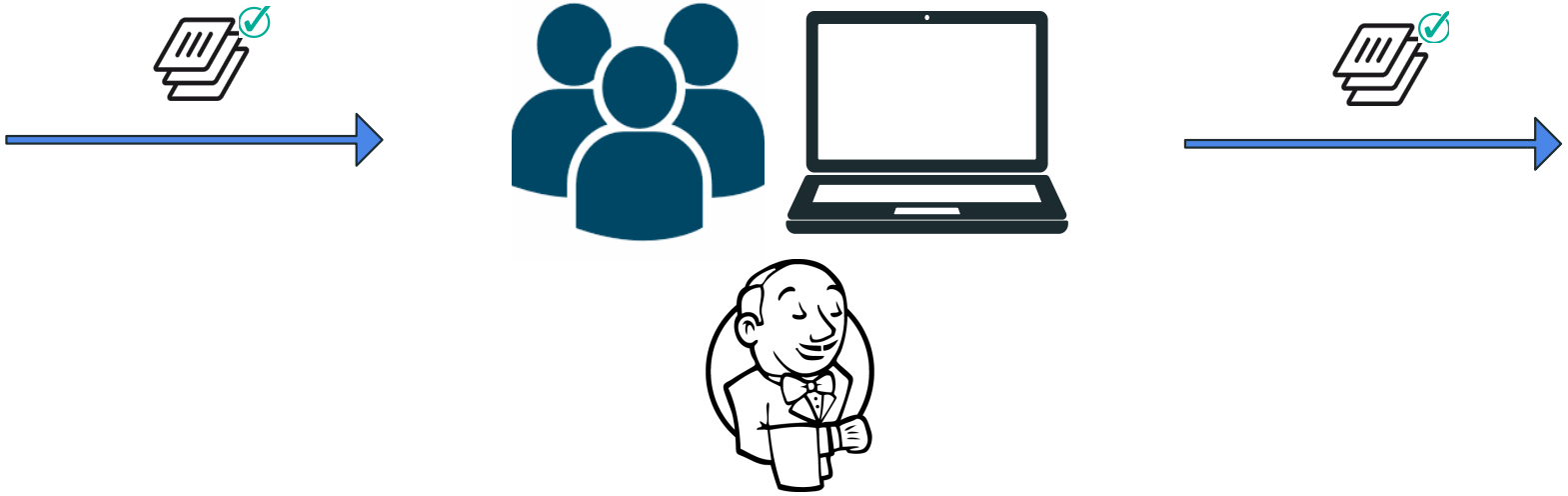
$ # protects against stale images

$ head -n 1 Dockerfile
FROM user/repo:reallyold

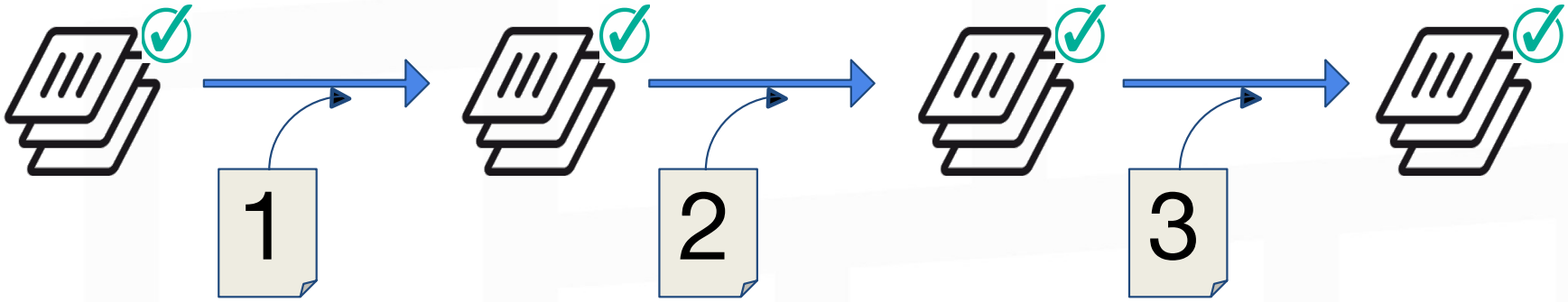
$ docker build -t user/myrailsbase .

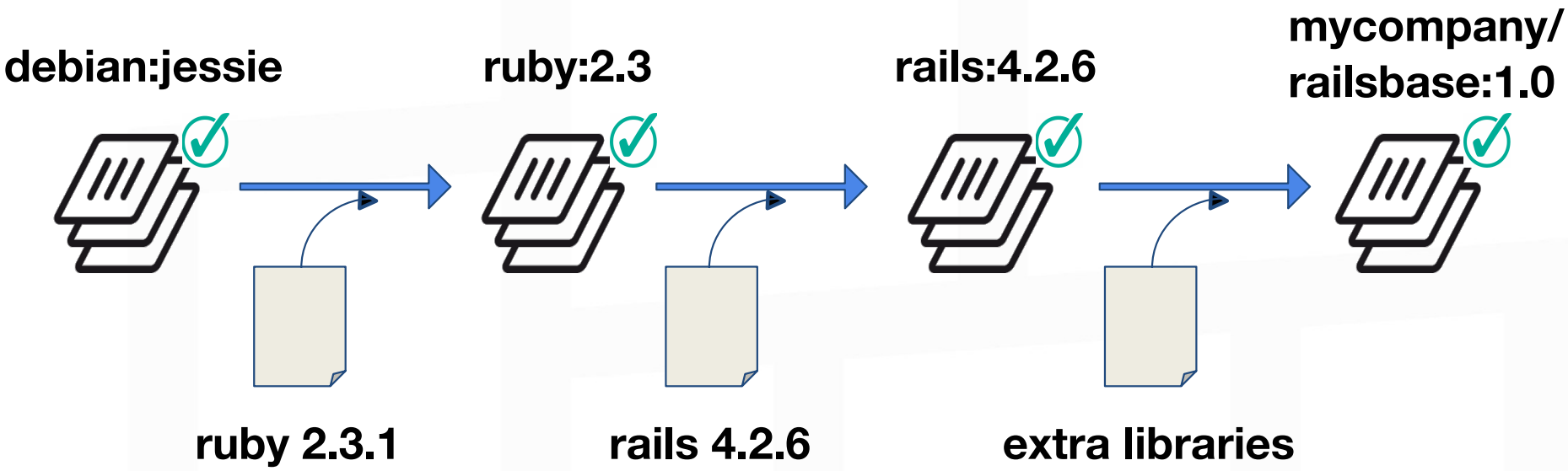
Error: remote repository docker.io/user/repo out-of-date: targets expired at Thu Jun 16 10:47:43 PDT 2016

Developer
or CI

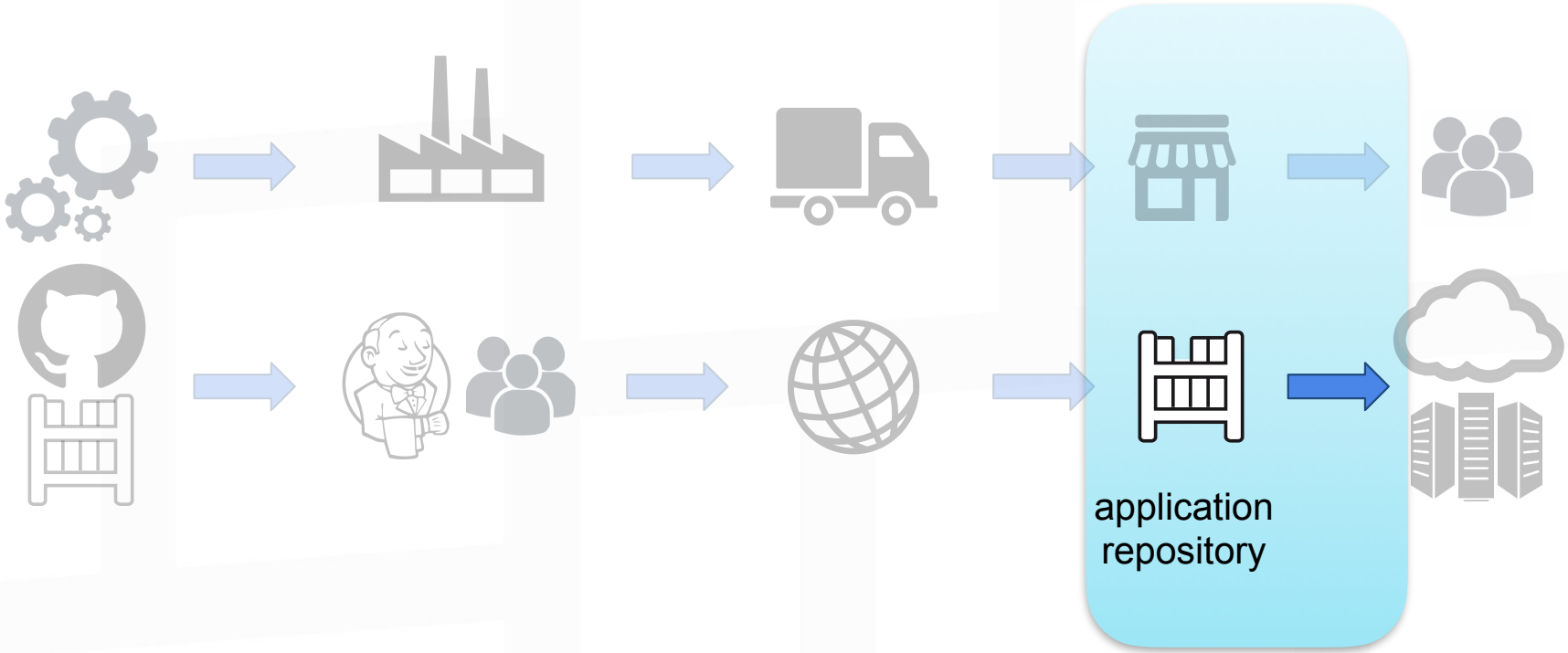


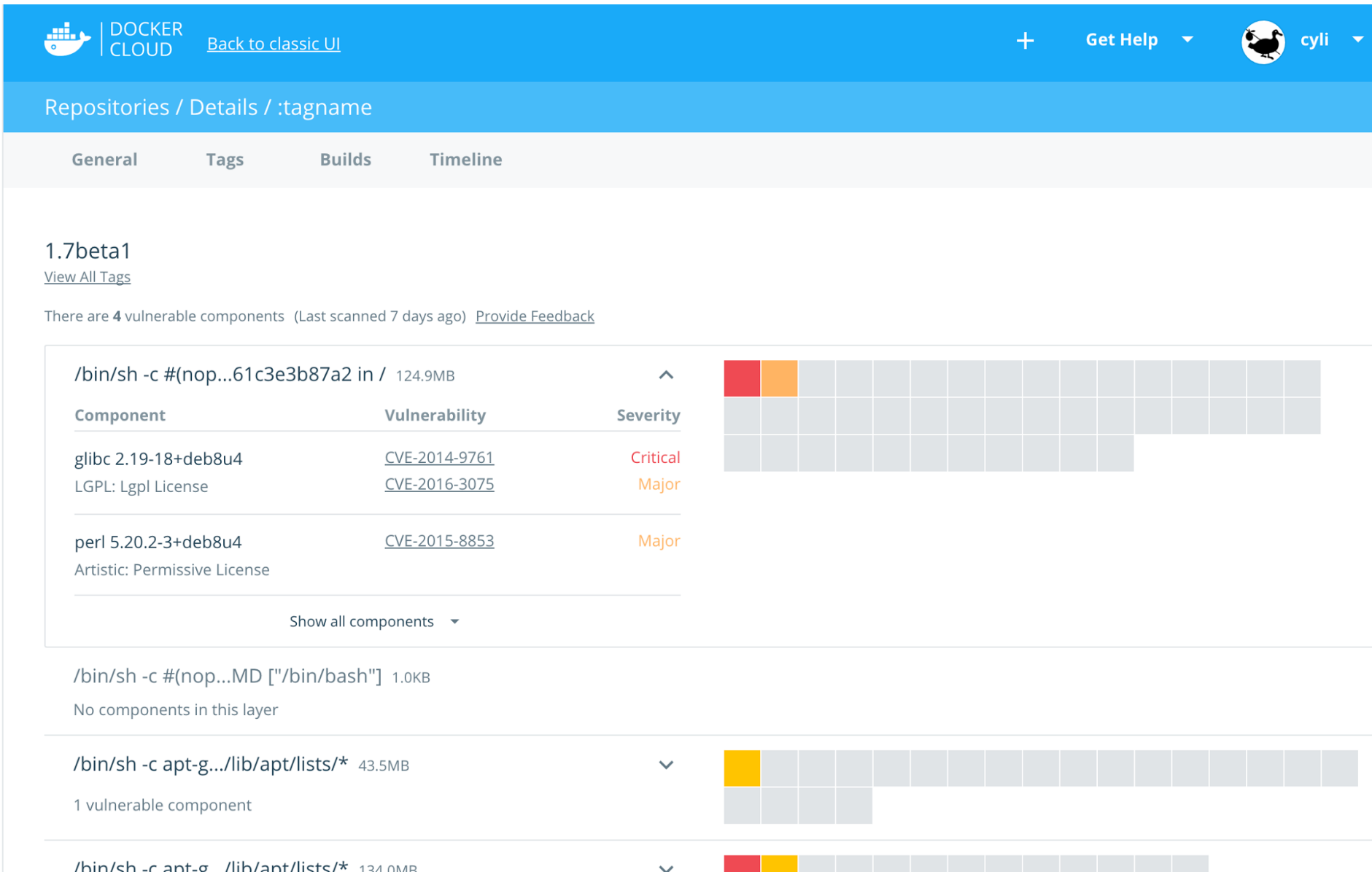
Trusted Image Chaining

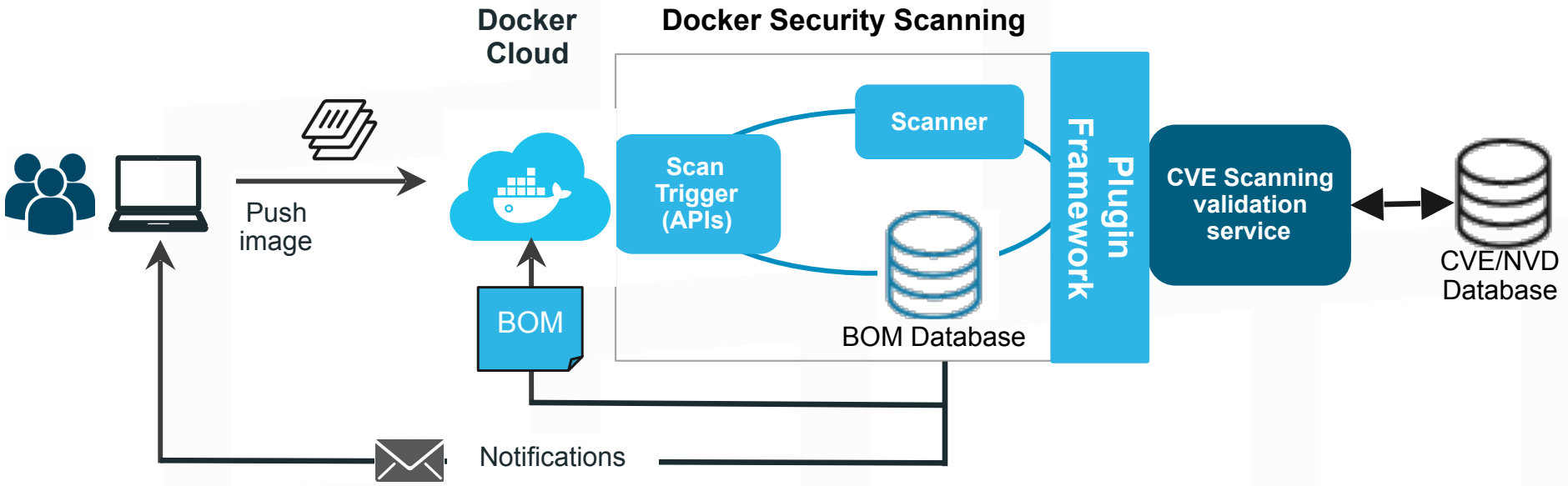


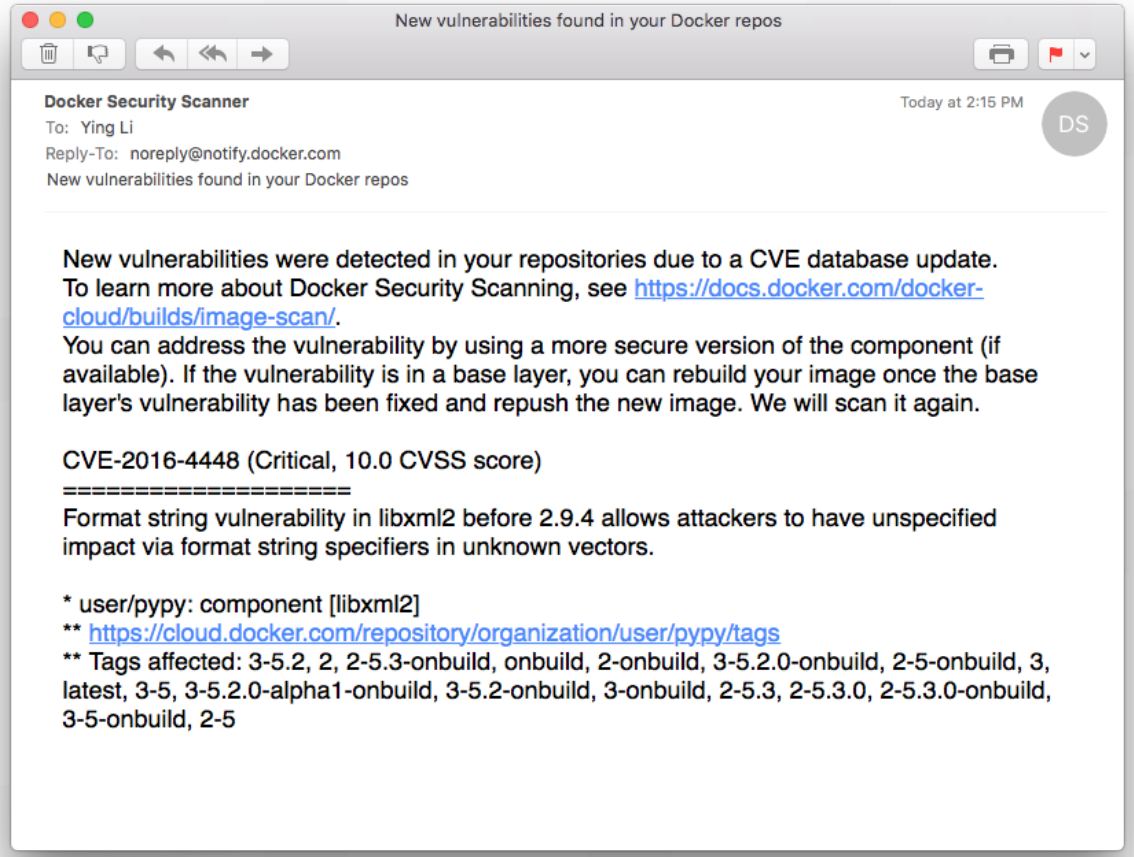

debian:jessie
ruby:2.3
rails:4.2.6
mycompany/
railsbase:1.0
ruby 2.3.1
rails 4.2.6
extra libraries

Security Scanning + Gating

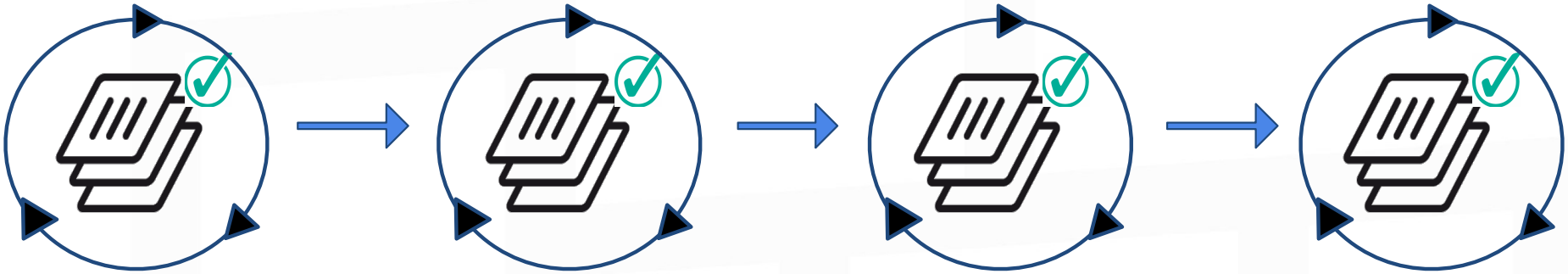


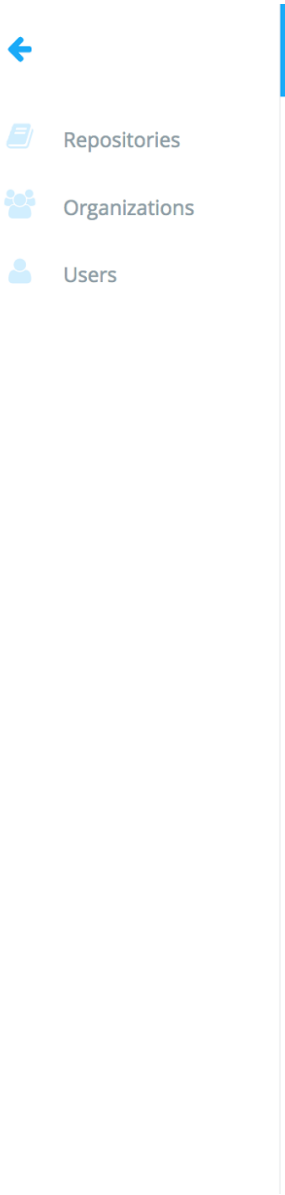

DOCKER CLOUD
Back to classic UI
Get Help
cyli
Repositories / Details / :tagname
General
Tags
Builds
Timeline
1.7beta1
View All Tags
There are 4 vulnerable components (Last scanned 7 days ago) Provide Feedback
/bin/sh -c #(nop...61c3e3b87a2 in / 124.9MB
Component
Vulnerability
Severity
glibc 2.19-18+deb8u4
LGPL: Lgpl License
CVE-2014-9761
CVE-2016-3075
Critical
Major
perl 5.20.2-3+deb8u4
Artistic: Permissive License
CVE-2015-8853
Major
Show all components
/bin/sh -c #(nop...MD ["/bin/bash"] 1.0KB
No components in this layer
/bin/sh -c apt-g.../lib/apt/lists/* 43.5MB
1 vulnerable component


Docker Cloud
Docker Security Scanning
Push image
Scan Trigger (APIs)
Scanner
Plugin Framework
CVE Scanning validation service
CVE/NVD Database
BOM
BOM Database
Notifications


New vulnerabilities found in your Docker repos
Docker Security Scanner
To: Ying Li
Reply-To: noreply@notify.docker.com
New vulnerabilities found in your Docker repos
Today at 2:15 PM
DS
New vulnerabilities were detected in your repositories due to a CVE database update.
To learn more about Docker Security Scanning, see https://docs.docker.com/docker-cloud/builds/image-scan/.
You can address the vulnerability by using a more secure version of the component (if available). If the vulnerability is in a base layer, you can rebuild your image once the base layer's vulnerability has been fixed and repush the new image. We will scan it again.
CVE-2016-4448 (Critical, 10.0 CVSS score)
==========
Format string vulnerability in libxml2 before 2.9.4 allows attackers to have unspecified impact via format string specifiers in unknown vectors.
* user/pypy: component [libxml2]
** https://cloud.docker.com/repository/organization/user/pypy/tags
** Tags affected: 3-5.2, 2, 2-5.3-onbuild, onbuild, 2-onbuild, 3-5.2.0-onbuild, 2-5-onbuild, 3, latest, 3-5, 3-5.2.0-alpha1-onbuild, 3-5.2-onbuild, 3-onbuild, 2-5.3, 2-5.3.0, 2-5.3.0-onbuild, 3-5-onbuild, 2-5

Auto-Chained Remediation





TRUSTED REGISTRY

Search Trusted Registry

user

← Back to repositories

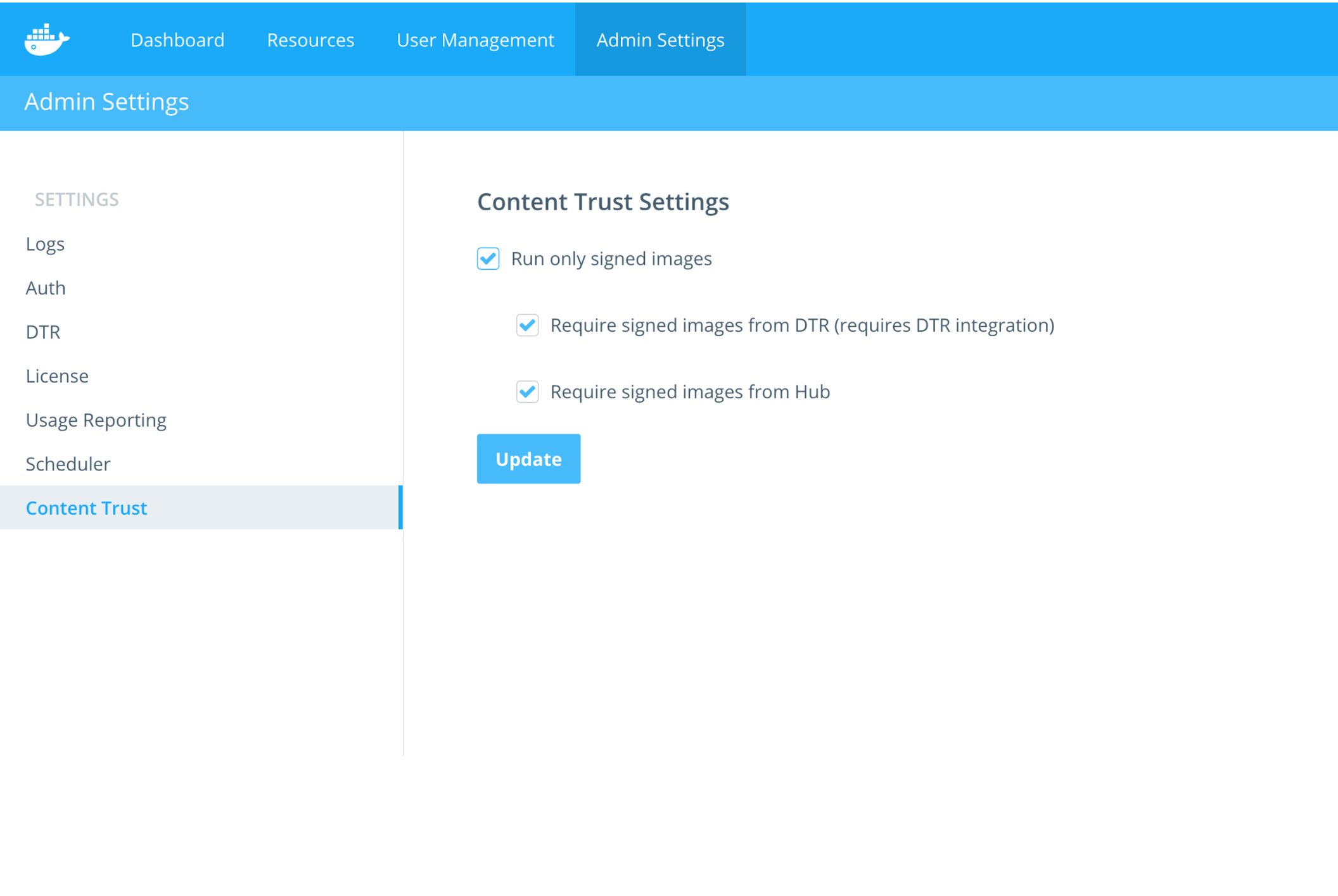
user / myrailsbase

Rails base image with pagination, clearance (auth), and formtastic plugins

INFO | TAGS | SETTINGS

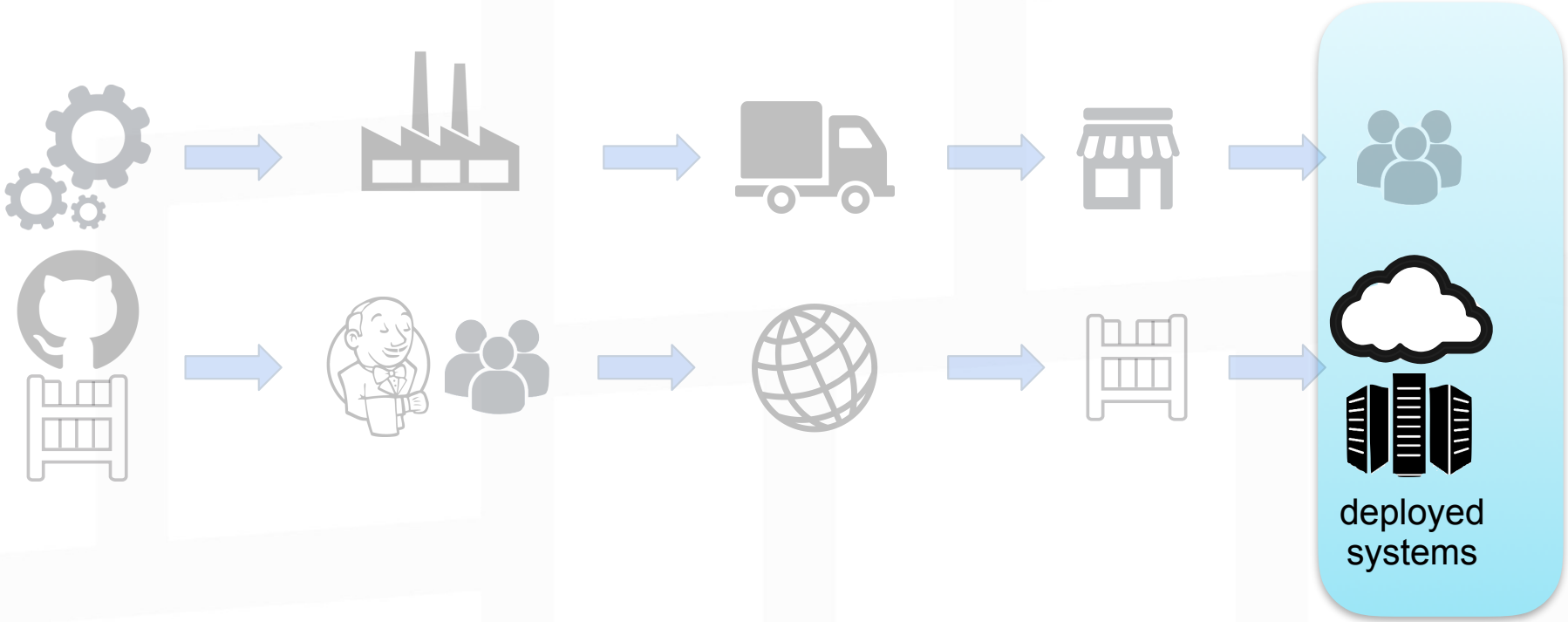
Select all

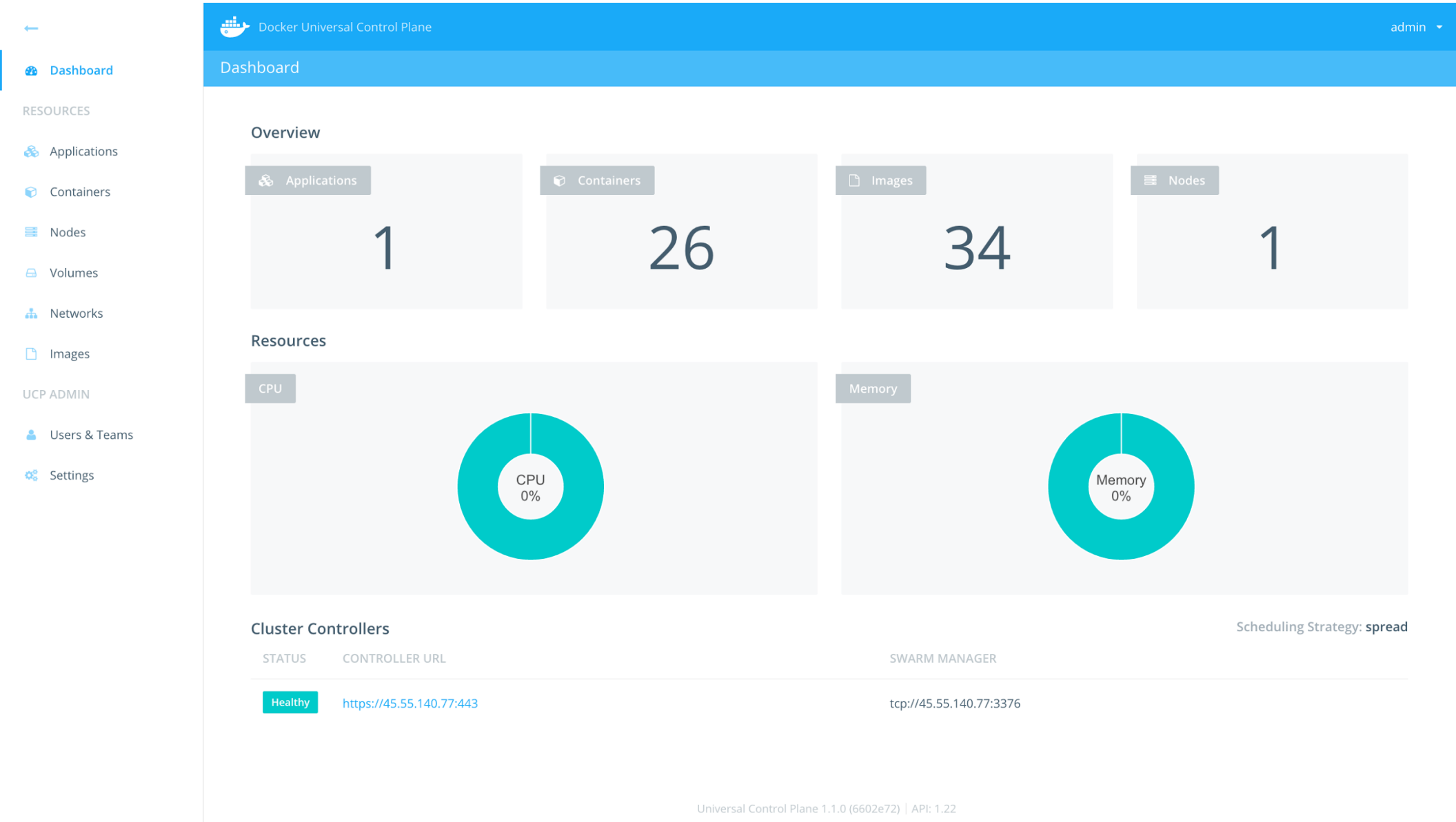
TAGS	
3.4	✔ signed
3.3	✔ signed
3.2	✔ signed
3.1	! outdated
latest	✔ signed
3.0	


Dashboard
Resources
User Management
Admin Settings
Admin Settings
SETTINGS
Logs
Auth
DTR
License
Usage Reporting
Scheduler
Content Trust
Content Trust Settings
Run only signed images
Require signed images from DTR (requires DTR integration)
Require signed images from Hub
Update

```
$ docker ps --format “table {{.ID}}\t{{.Image}}\t{{.Created}}” \
      -f ancestor=user/pypy:3-5.2 \
      -f ancestor=user/pypy:2-5.3

CONTAINER ID    IMAGE              CREATED     COMMAND
bf8966f2dc59    user/django:pypy    2 weeks     "python manage.py run"
263158cab9f0    twisted_web         2 hours     "twistd -n web --path"
005c98e79459    user/pypy:3-5.2     1 hours     “scrapy crawl dmoz"
005c98e79459    user/pypy:2-5.3     1 hours     “youtube-dl ‘http://w"
```

Orchestration

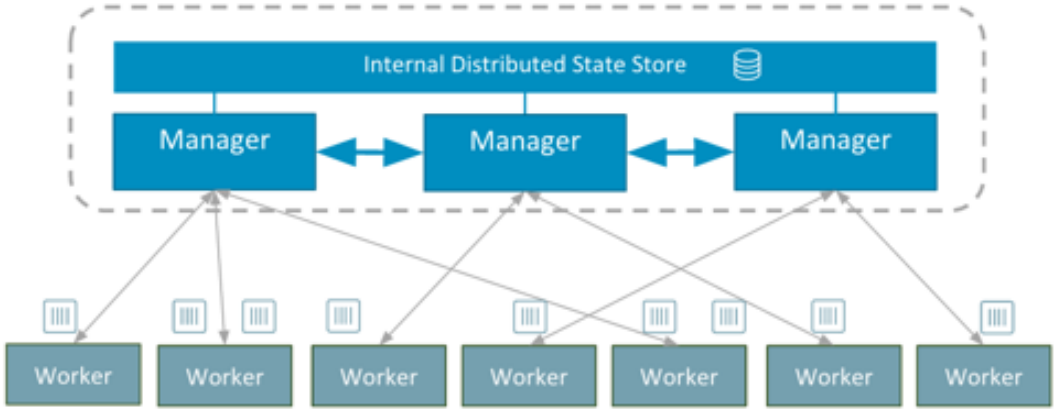



Docker Universal Control Plane
admin
Dashboard
Dashboard
RESOURCES
Applications
Containers
Nodes
Volumes
Networks
Images
UCP ADMIN
Users & Teams
Settings
Overview
Applications
1
Containers
26
Images
34
Nodes
1
Resources
CPU
CPU
0%
Memory
Memory
0%
Cluster Controllers
Scheduling Strategy: spread
STATUS
CONTROLLER URL
SWARM MANAGER
Healthy
https://45.55.140.77:443
tcp://45.55.140.77:3376
Universal Control Plane 1.1.0 (6602e72) | API: 1.22

```
$ docker run -it --net host --pid host --cap-add audit_control ... docker/docker-bench-security

[INFO] 1 - Host Configuration
[WARN] 1.1  - Create a separate partition for containers
[PASS] 1.2  - Use an updated Linux Kernel
[PASS] 1.4  - Remove all non-essential services from the host - Network
[PASS] 1.5  - Keep Docker up to date
[INFO]       * Using 1.11.2 which is current as of 2016-06-02
[INFO]       * Check with your operating system vendor for support and security maintenance for docker
[INFO] 1.6  - Only allow trusted users to control Docker daemon
[INFO]       * docker:x:999:docker
[WARN] 1.7  - Failed to inspect: auditctl command not found.
[WARN] 1.8  - Failed to inspect: auditctl command not found.
[WARN] 1.9  - Failed to inspect: auditctl command not found.
[INFO] 1.10 - Audit Docker files and directories - docker.service
[INFO]       * File not found
[INFO] 1.11 - Audit Docker files and directories - docker.socket
[INFO]       * File not found
...
```

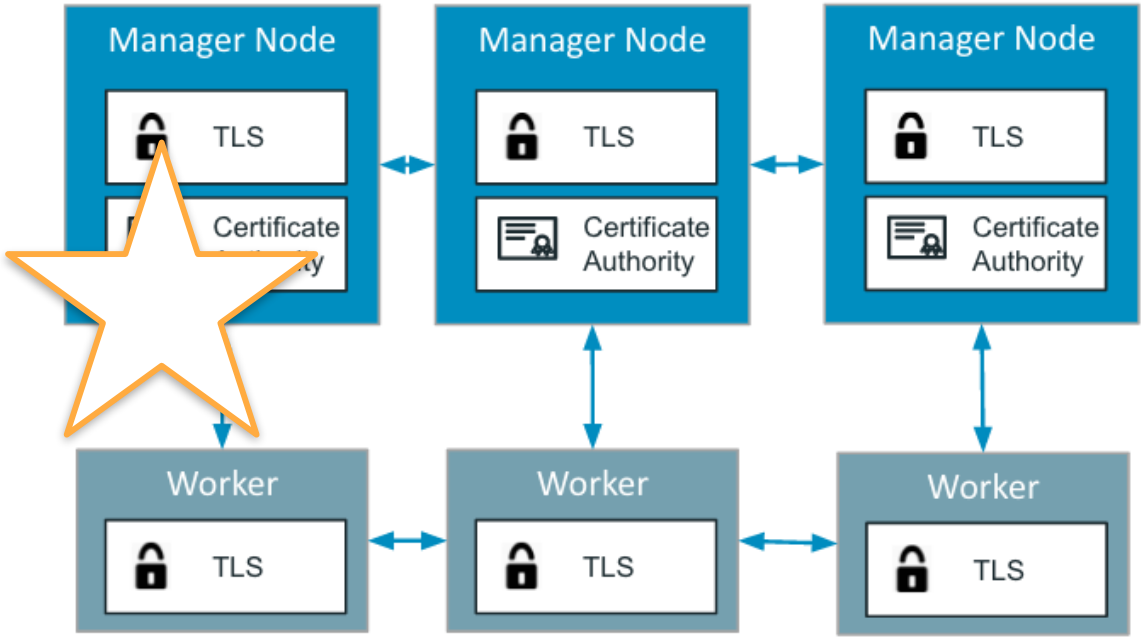
Secure Cluster Management

- Docker 1.12 integrates swarm.
- Strong default swarm security.



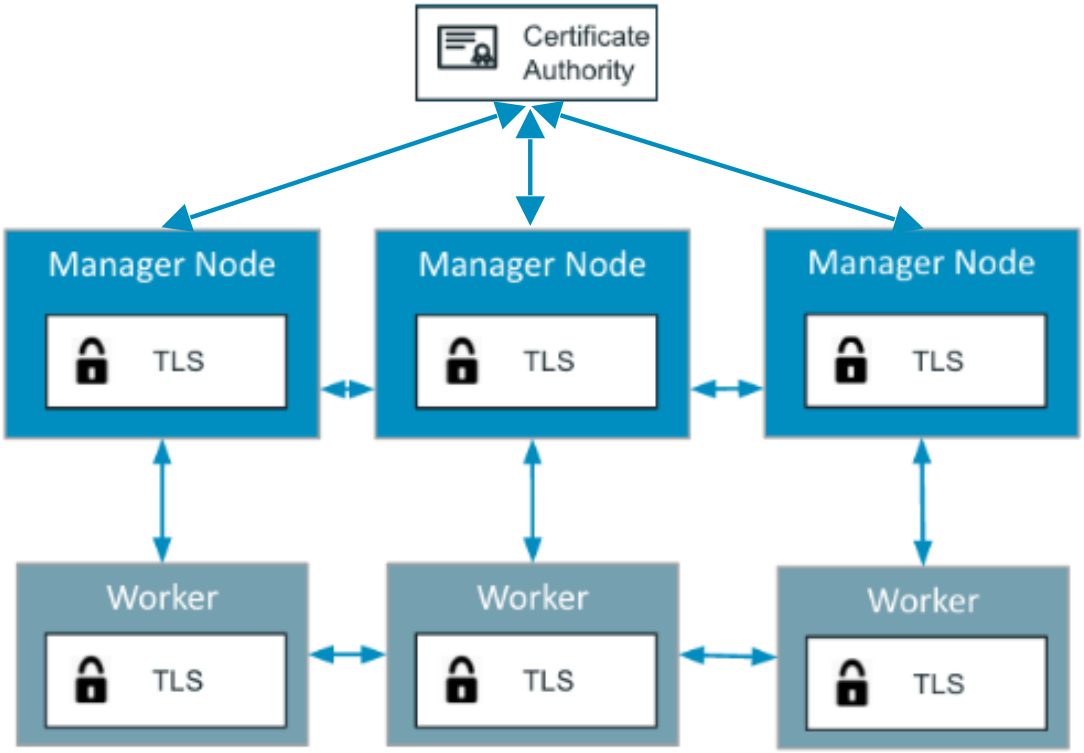
Mutual TLS by default

- Leader acts as CA.
- Any Manager can be promoted to leader.
- Workers and managers identified by their certificate.
- Communications secured with Mutual TLS.



Support for External CAs

- Managers support BYO CA.
- Forwards CSRs to external CA.



Automatic Certificate Rotation

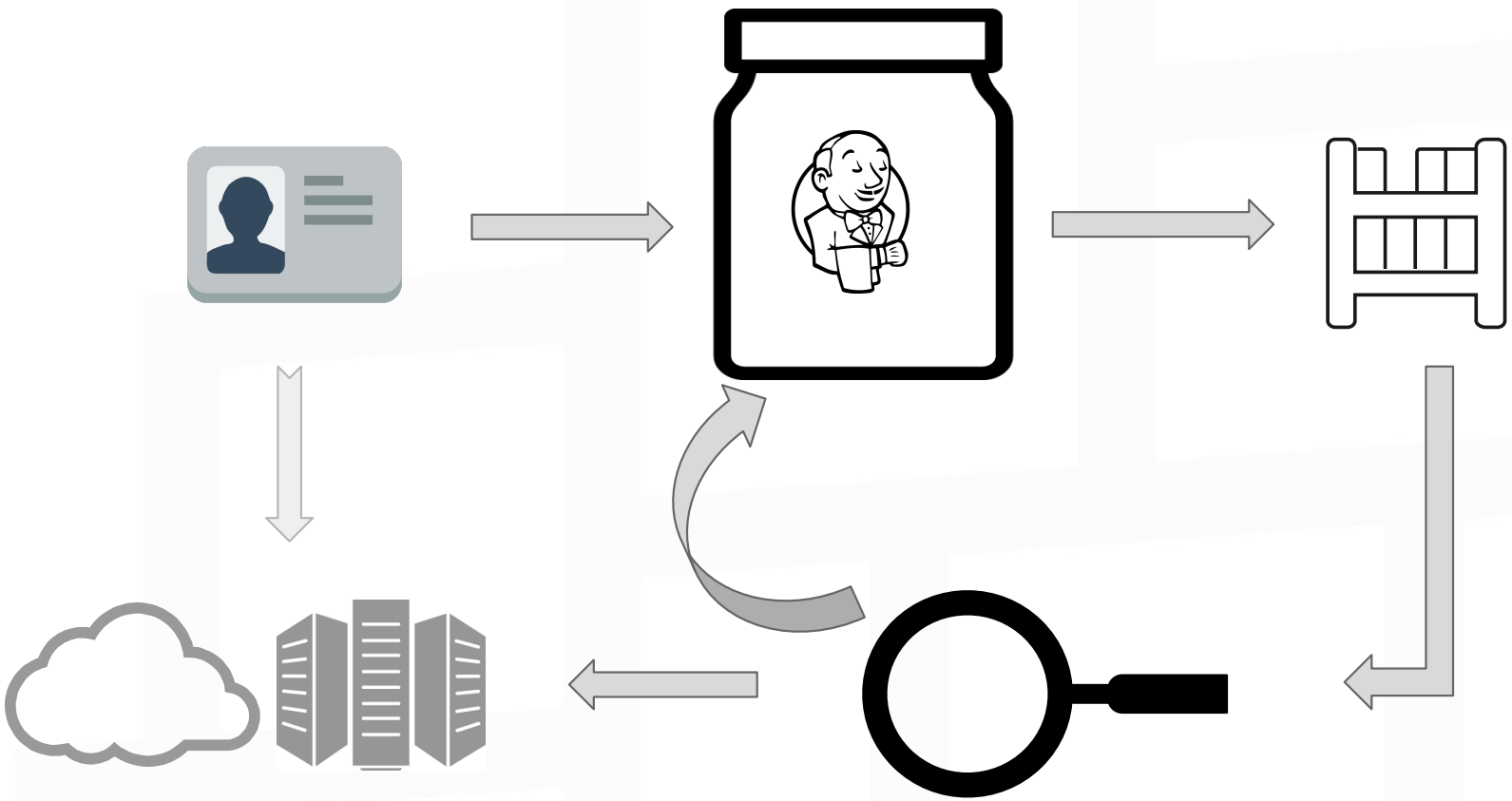
- Customizable certificate rotation periods.
- Occurs automatically.
- Ensures potentially compromised or leaked certificates are rotated out of use.
- Whitelist of currently valid certificates.

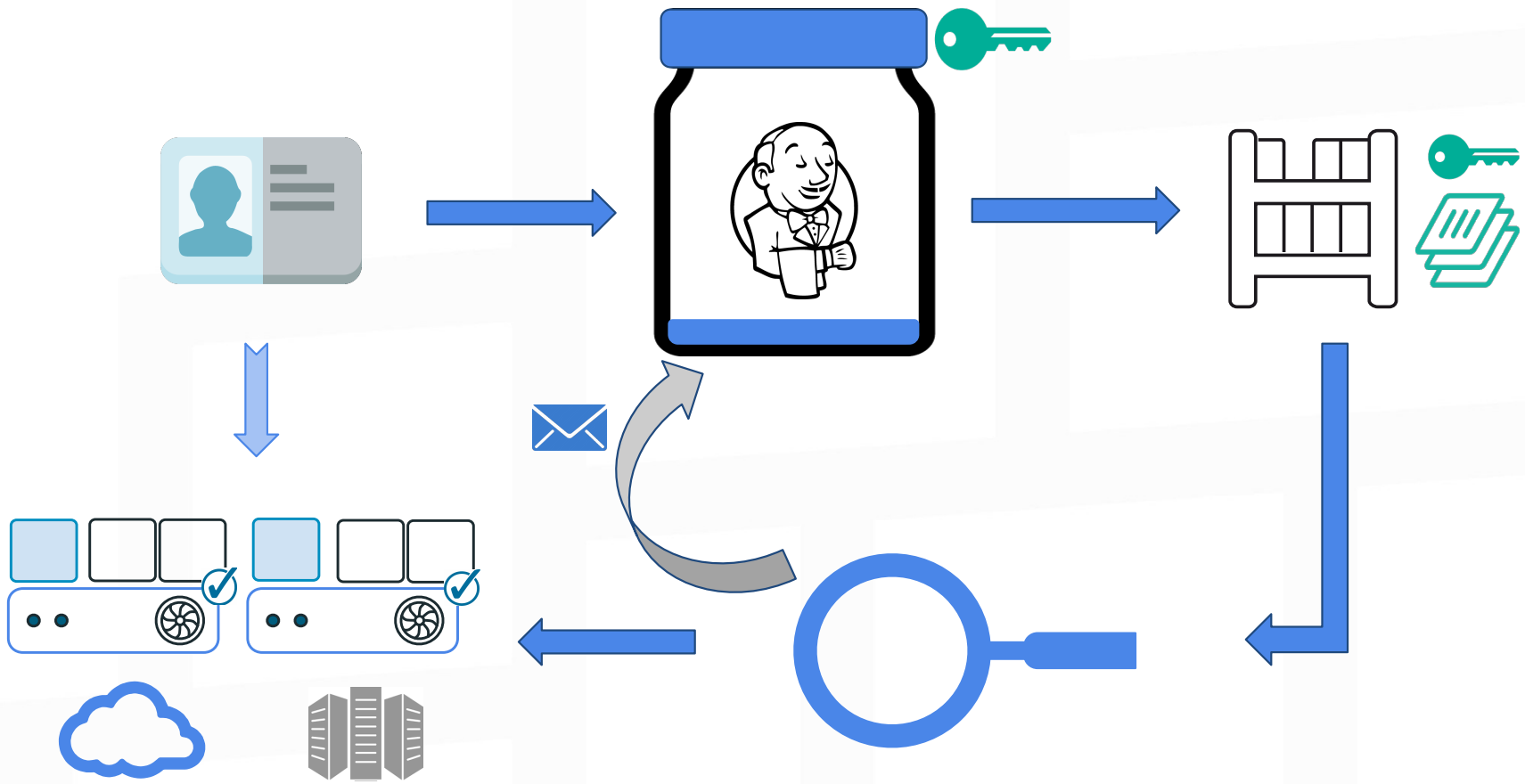
Secure Addition of Nodes

Three ways to approve addition of a node to the cluster:

- Automatic acceptance.
- Secret token.
- Manual approval.

DEMO





Thank you!