Хранилища контейнеров и артефактов поставки, инфраструктура для контроля безопасности артефактов

Не забудь включить запись!

План

- Жизненный цикл артефакта
- Хранение артефактов
- Registry
- Security
- DEMO

Жизненный цикл артефакта

Артефакт

- это любой созданный искусственно элемент программной системы

Жизненный цикл артефакта

- Создание
- Тестирование
- Различного рода проверки
- Эксплуатация
- Обновление
- Удаление

Артефакты и CI/CD

Нужно ли проводить проверки безопасности в пайплайне?

Артефакты и CI/CD

В каком именно месте расположить проверки безопасности?

Типы образов

- Образы готовые для развертывания в production окружении
- Образы с различными debug инструментами

Хранение артефактов

- "Боевые" сервера
- Файл сервера
- Флэшки ^_^
- Специализированные хранилища

Хранение артефактов

Хранение артефактов

Google Container Registry

Хранение артефактов: GCR

- Безопасное, приватное Docker registry
- Сборка и развертывание в автоматическом режиме
- Встроенное сканирование уязвимостей
- Блокировка потенциально опасных образов
- Нативная поддержка докера
- Быстрый и высокодоступный
- Поддержка триггеров
- API сканирования уязвимостей

Хранение артефактов: GCR

Resource	Monthly Free Usage Limits
Standard Storage	5 GB-months
Class A Operations	5,000
Class B Operations	50,000
Network Egress	1 GB from North America to each GCP egress destination (Australia and China excluded)

Monthly Usage	Egress to Worldwide Destinations (excluding Asia & Australia) (per GB)	Egress to Asia Destinations (excluding China, but including Hong Kong) (per GB)	Egress to China Destinations (excluding Hong Kong) (per GB)	Egress to Australia Destinations (per GB)	Ingress
0-1 TB	$0.12	$0.12	$0.23	$0.19	Free
1-10 TB	$0.11	$0.11	$0.22	$0.18	Free
10+ TB	$0.08	$0.08	$0.20	$0.15	Free

Хранение артефактов: GCR

Storage Class[1]	Class A operations (per 10,000 operations)	Class B operations (per 10,000 operations)	Free operations
Standard Storage	$0.05	$0.004	Free
Nearline Storage and **Durable Reduced Availability (DRA) Storage**	$0.10	$0.01	Free
Coldline Storage	$0.10	$0.05	Free

	Nearline Storage	Coldline Storage
Data retrieval	$0.01 per GB	$0.05 per GB
Minimum storage duration	30 days	90 days

Хранение артефактов: GCR

API or Feature	Class A Operations	Class B Operations	Free Operations
JSON API	storage.*.insert[1] storage.*.patch storage.*.update storage.*.setIamPolicy storage.buckets.list storage.buckets.lockRetentionPolicy storage.notifications.delete storage.objects.compose storage.objects.copy storage.objects.list storage.objects.rewrite storage.objects.watchAll storage.projects.hmacKeys.create storage.projects.hmacKeys.list storage.*AccessControls.delete	storage.*.get storage.*.getIamPolicy storage.*.testIamPermissions storage.*AccessControls.list storage.notifications.list Each object notification	storage.channels.stop storage.buckets.delete storage.objects.delete storage.projects.hmacKeys.delete
XML API	GET Service GET Bucket (when listing objects in a bucket) PUT POST	GET Bucket (when retrieving bucket configuration) GET Object HEAD	DELETE

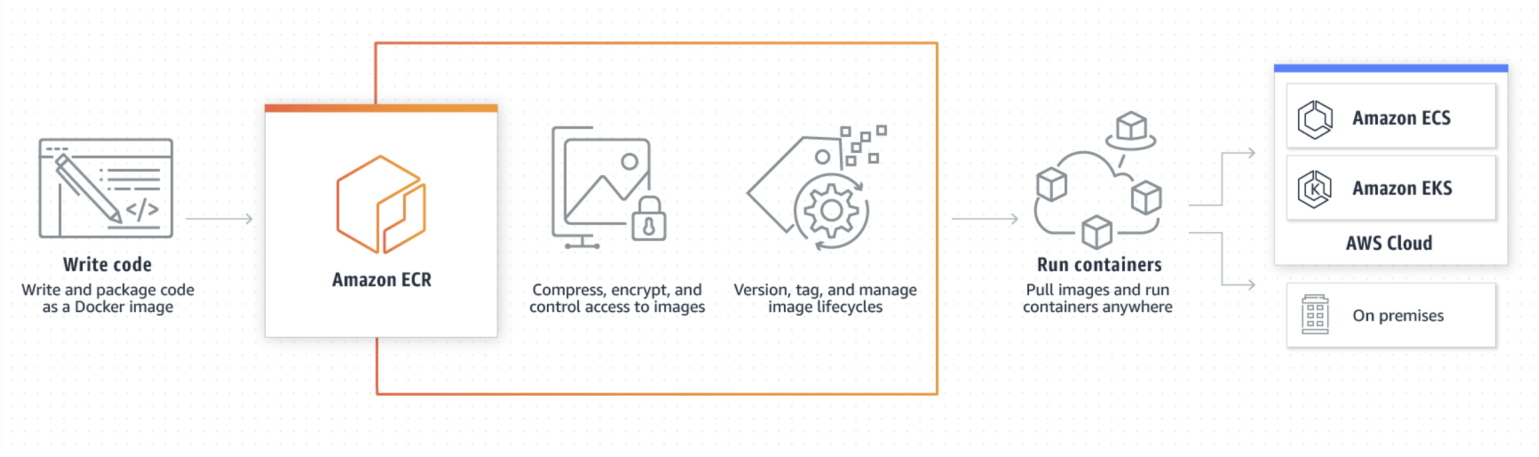
Хранение артефактов

Amazon Elastic Container Registry

Amazon ECR

Хранение артефактов: ECR

- Полностью управляемое хранилище
- Высокая доступность
- Безопасность



Хранение артефактов: ECR

```
Amazon ECR offers new customers 500MB-month of storage for one year.
```

Storage:

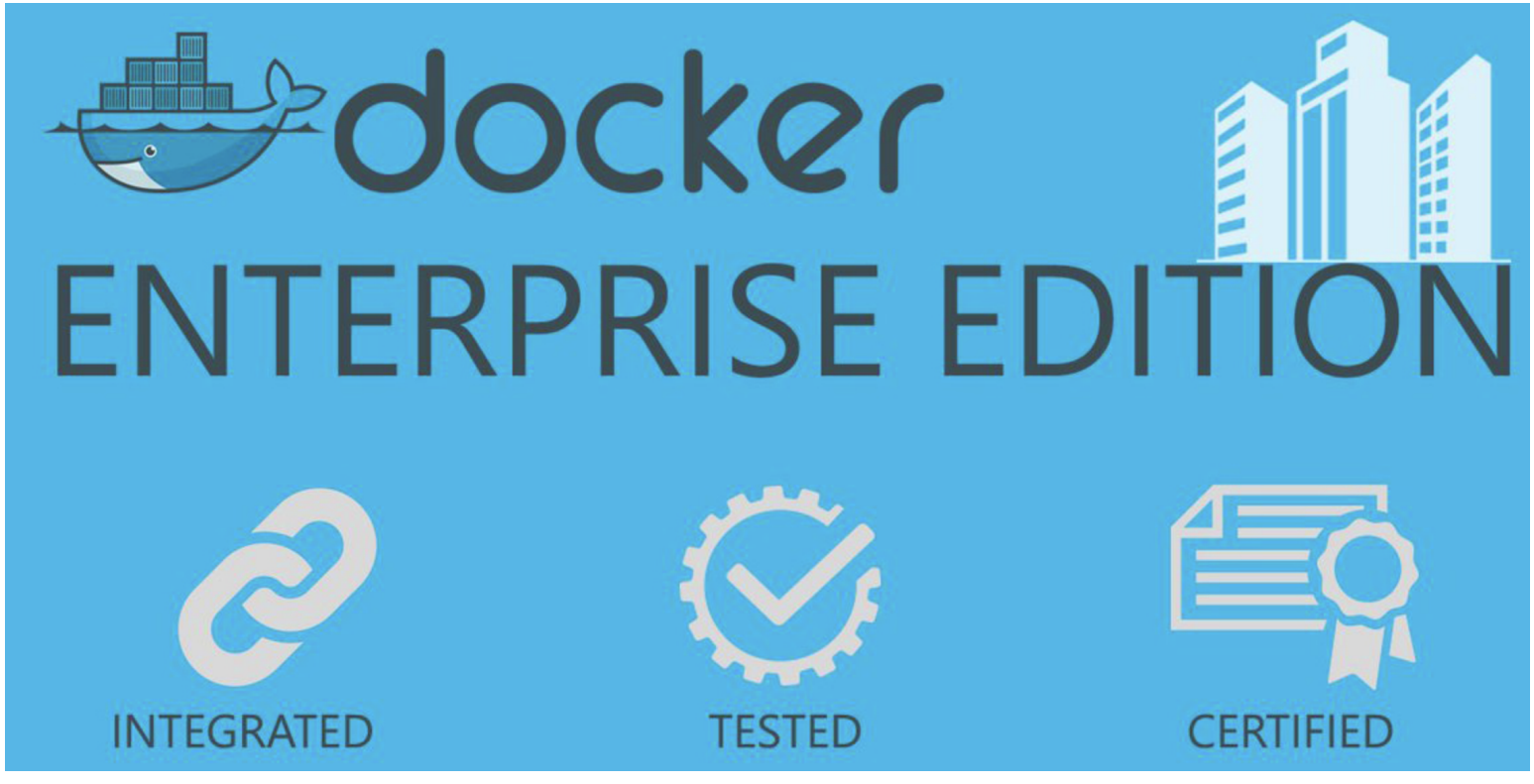
- Storage is $0.10 per GB-month

Data transfer: **

Region: EU (Frankfurt)

	Pricing
Data Transfer IN	
All data transfer in	$0.00 per GB
Data Transfer OUT* **	
Up to 1 GB / Month	$0.00 per GB
Next 9.999 TB / Month	$0.09 per GB
Next 40 TB / Month	$0.085 per GB
Next 100 TB / Month	$0.07 per GB
Greater than 150 TB / Month	$0.05 per GB

Хранение артефактов: Docker Enterprise



Хранение артефактов: Docker Enterprise

Компоненты входящие в поставку

- Docker Desktop Enterprise
- Docker Application
- Docker Kubernetes Service (DKS)
- Lifecycle Automation Tools

Хранение артефактов: Quay

Хранение артефактов: Quay

- Автоматические билды
- Сканирование безопасности
- Геораспределенная репликация
- Security vulnerability detection integration
- Continuous garbage collection
- Torrent distribution ^_^
- Поддержка манифестов для различных архитектур

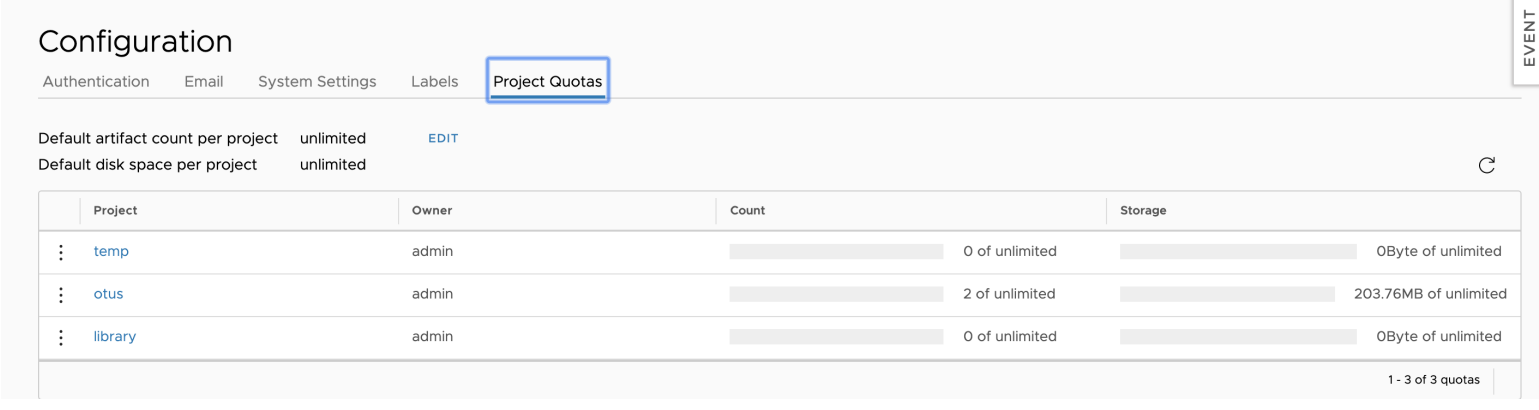
Хранение артефактов: Harbor

Хранение артефактов: Harbor

- Multi-tenant
- Расширенный API и Web UI
- Репликация образов между инстансами Harbor
- RBAC
- Анализ безопасности и уязвимостей
- Подпись образов и проверка

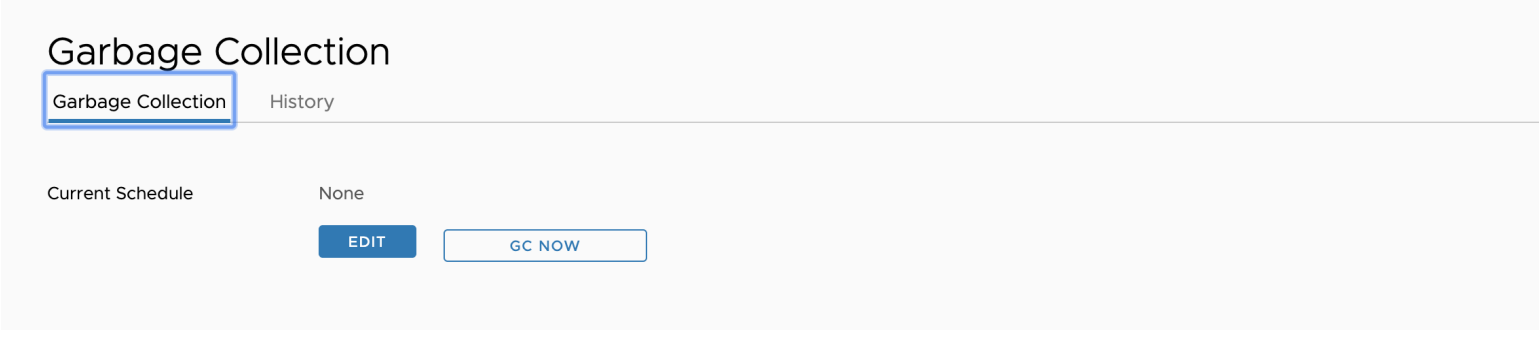
Хранение артефактов: Harbor

Квоты для проектов



Хранение артефактов: Harbor

Очистка мусора



Хранение артефактов: Harbor

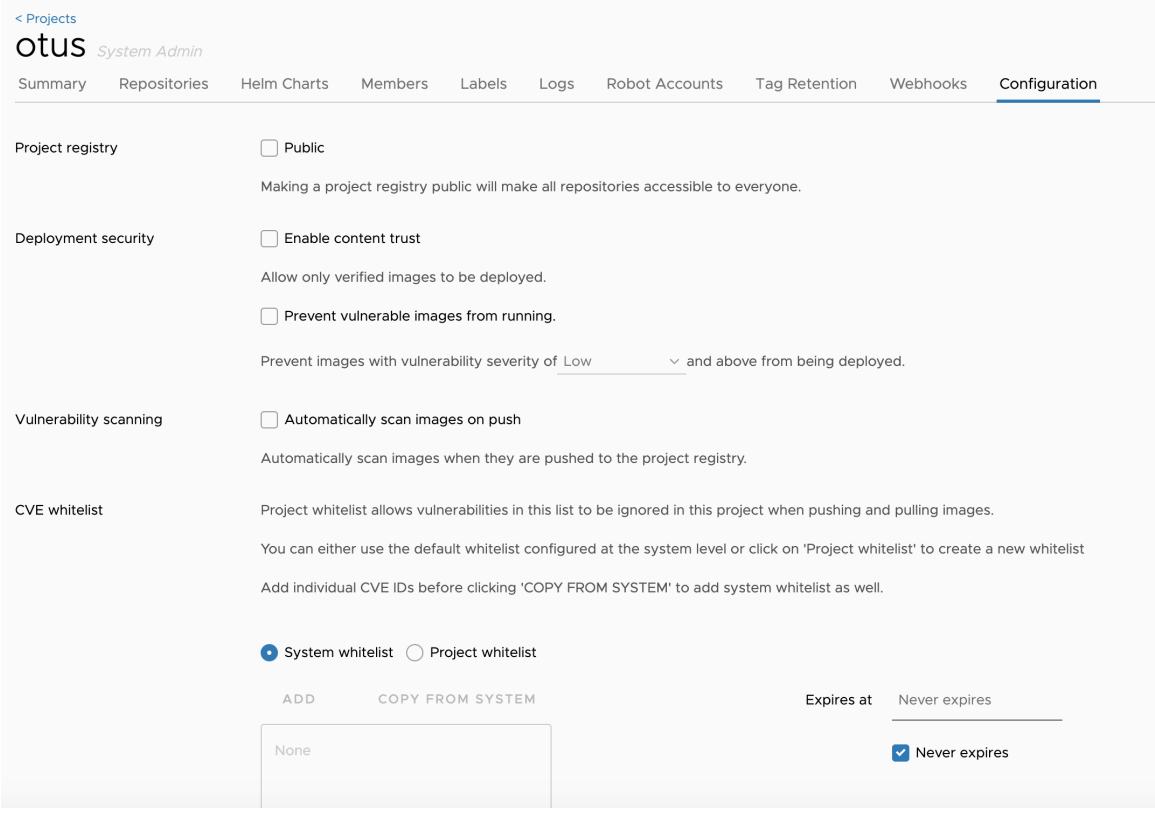
Создание правил репликации

Хранение артефактов: Harbor

Создание entrypoint

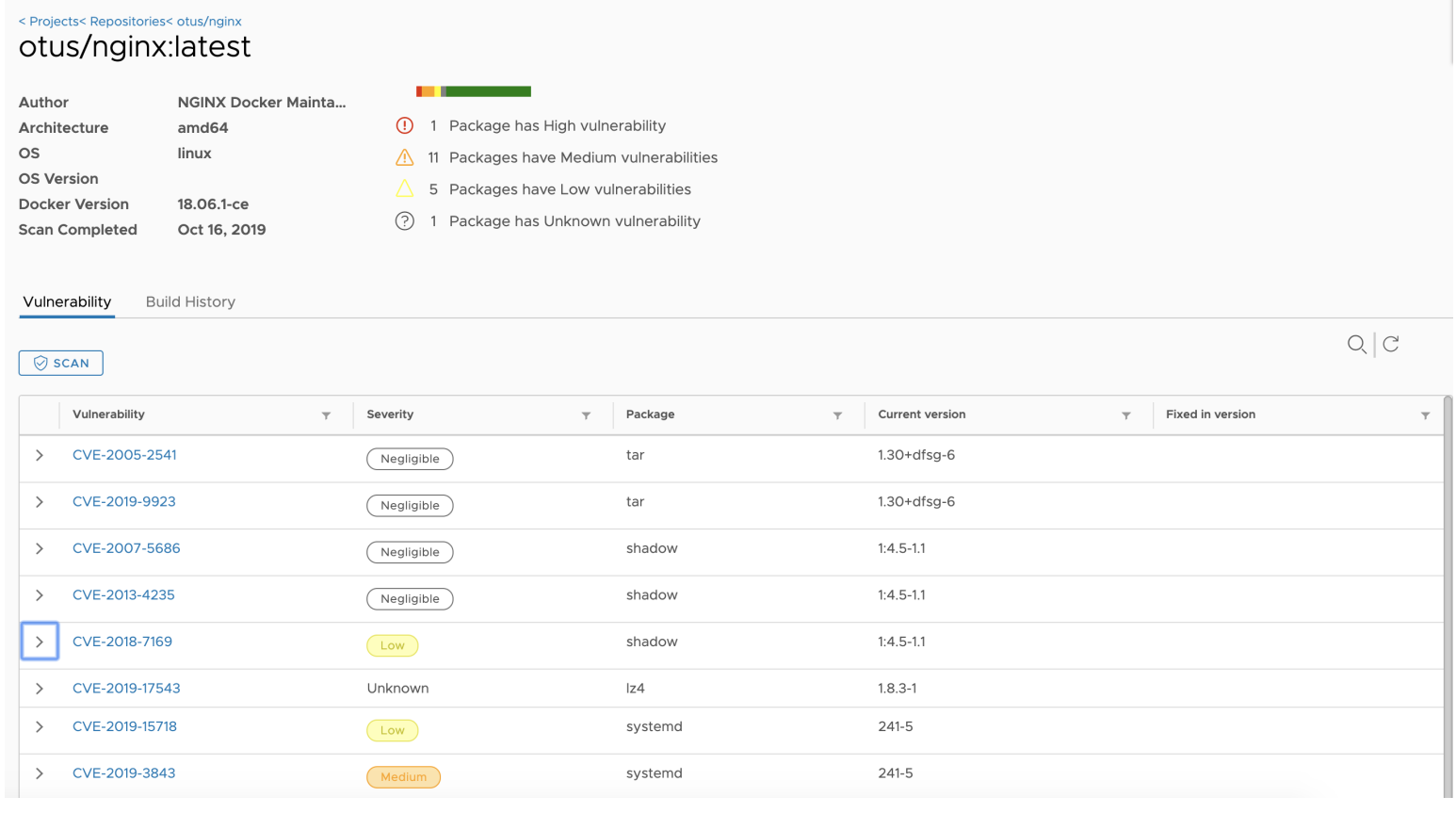
Хранение артефактов: Harbor

Настройка проектов



Хранение артефактов: Harbor

Результаты сканирования образа



Хранение артефактов: Harbor

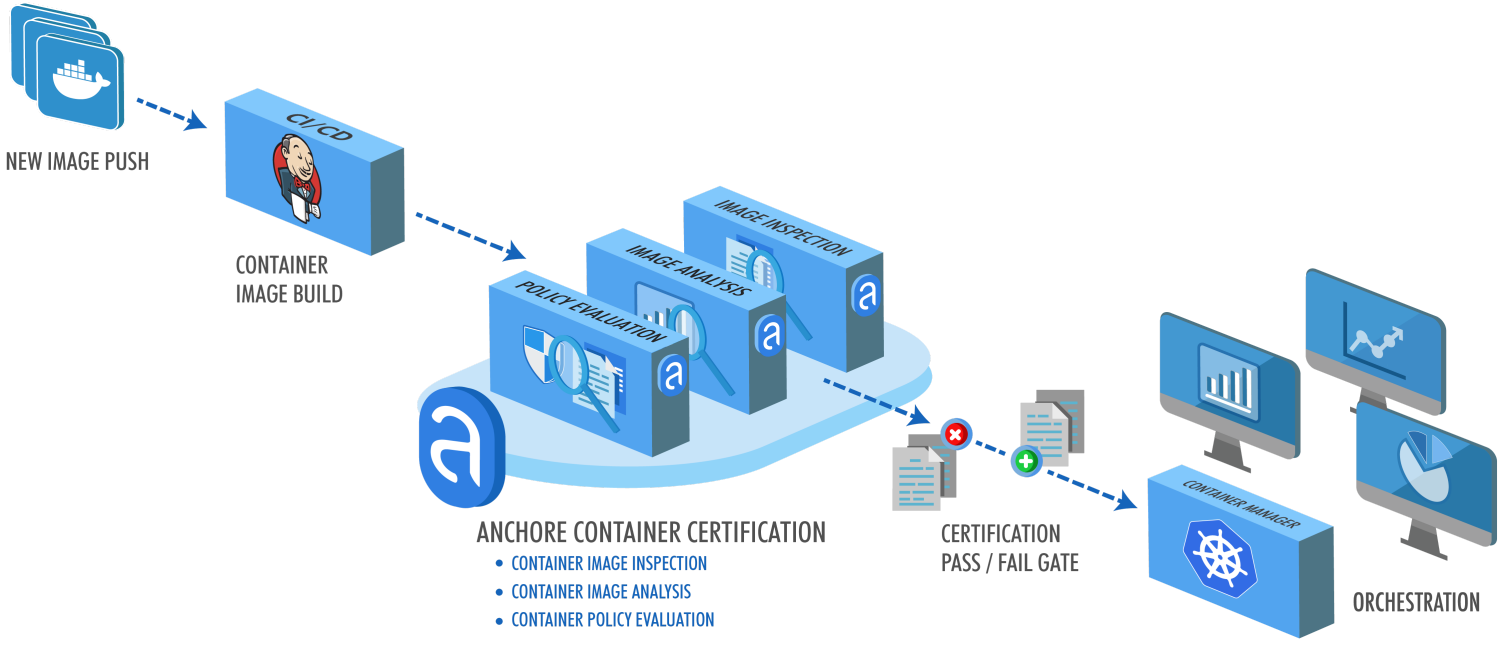
Результаты сканирования образа

Vulnerability | Build History

Create on	Commands
7/10/19, 12:22 AM	ADD file:71ac26257198ecf6a4ea05f45e522de961543a965486dd49a86bd6aca8342026 in /
7/10/19, 12:22 AM	CMD ["bash"]
7/23/19, 10:58 PM	LABEL maintainer=NGINX Docker Maintainers <docker-maint@nginx.com>
7/23/19, 10:58 PM	ENV NGINX_VERSION=1.17.2
7/23/19, 10:58 PM	ENV NJS_VERSION=0.3.3
7/23/19, 10:58 PM	ENV PKG_RELEASE=1~buster
7/23/19, 10:59 PM	RUN set -x && addgroup --system --gid 101 nginx && adduser --system --disabled-login --ingroup nginx --no-create-home --home /nonexistent --gecos "nginx user" --shell /bin/false --uid 101 nginx && apt-get update && apt-get install --no-install-recommends --no-install-suggests -y gnupg1 ca-certificates && NGINX_GPGKEY=573BFD6B3D8FBC641079A6ABABF5BD827BD9BF62; found=''; for server in ha.pool.sks-keyservers.net hkp://keyserver.ubuntu.com:80 hkp://p80.pool.sks-keyservers.net:80 pgp.mit.edu ; do echo "Fetching GPG key $NGINX_GPGKEY from $server"; apt-key adv --keyserver "$server" --keyserver-options timeout=10 --recv-keys "$NGINX_GPGKEY" && found=yes && break; done; test -z "$found" && echo >&2 "error: failed to fetch GPG key $NGINX_GPGKEY" && exit 1; apt-get remove --purge --auto-remove -y gnupg1 && rm -rf /var/lib/apt/lists/* && dpkgArch="$(dpkg --print-architecture)" && nginxPackages=" nginx=${NGINX_VERSION}-${PKG_RELEASE} nginx-module-xslt=${NGINX_VERSION}-${PKG_RELEASE} nginx-module-geoip=${NGINX_VERSION}-${PKG_RELEASE} nginx-module-image-filter=${NGINX_VERSION}-${PKG_RELEASE} nginx-module-njs=${NGINX_VERSION}.${NJS_VERSION}-${PKG_RELEASE} " && case "$dpkgArch" in amd64|i386) echo "deb https://nginx.org/packages/mainline/debian/ buster nginx" >> /etc/apt/sources.list.d/nginx.list && apt-get update ;; *) echo "deb-src https://nginx.org/packages/mainline/debian/ buster nginx" >> /etc/apt/sources.list.d/nginx.list && tempDir="$(mktemp -d)" && chmod 777 "$tempDir" && savedAptMark="$(apt-mark showmanual)" && apt-get update && apt-get build-dep -y $nginxPackages && (cd "$tempDir" && DEB_BUILD_OPTIONS="nocheck parallel=$(nproc)" apt-get source --compile $nginxPackages) && apt-mark showmanual \| xargs apt-mark auto > /dev/null && { [-z "$savedAptMark"] || apt-mark manual $savedAptMark; } && ls -lAFh "$tempDir" && (cd "$tempDir" && dpkg-scanpackages . > Packages) && grep '^Package: ' "$tempDir/Packages" && echo "deb [trusted=yes] file://$tempDir ./" > /etc/apt/sources.list.d/temp.list && apt-get -o Acquire::GzipIndexes=false update ;; esac && apt-get install --no-install-recommends --no-install-suggests -y $nginxPackages gettext-base && apt-get remove --purge --auto-remove -y ca-certificates && rm -rf /var/lib/apt/lists/* /etc/apt/sources.list.d/nginx.list && if [-n "$tempDir"]; then apt-get purge -y --auto-remove && rm -rf "$tempDir" /etc/apt/sources.list.d/temp.list; fi
7/23/19, 10:59 PM	RUN ln -sf /dev/stdout /var/log/nginx/access.log && ln -sf /dev/stderr /var/log/nginx/error.log
7/23/19, 10:59 PM	EXPOSE 80
7/23/19, 10:59 PM	STOPSIGNAL SIGTERM
7/23/19, 10:59 PM	CMD ["nginx" "-g" "daemon off;"]

11 commands

Хранение артефактов: Anchore



Хранение артефактов: Anchore

- Анализ образов
- Управление на основе политик
- Оповещения
- Интеграция с системами CI/CD
- Высокая кастомизация
- Оркестрация

Хранение артефактов: Anchore

- Сканирование уязвимостей
- Сканирование на наличие чувствительных данных
- Выявление всех известных пакетов ОС
- Сканирование 3d-party libraries
- Whitelist
- Blacklist
- Проверка Dockerfile
- Другие проверки ^_^

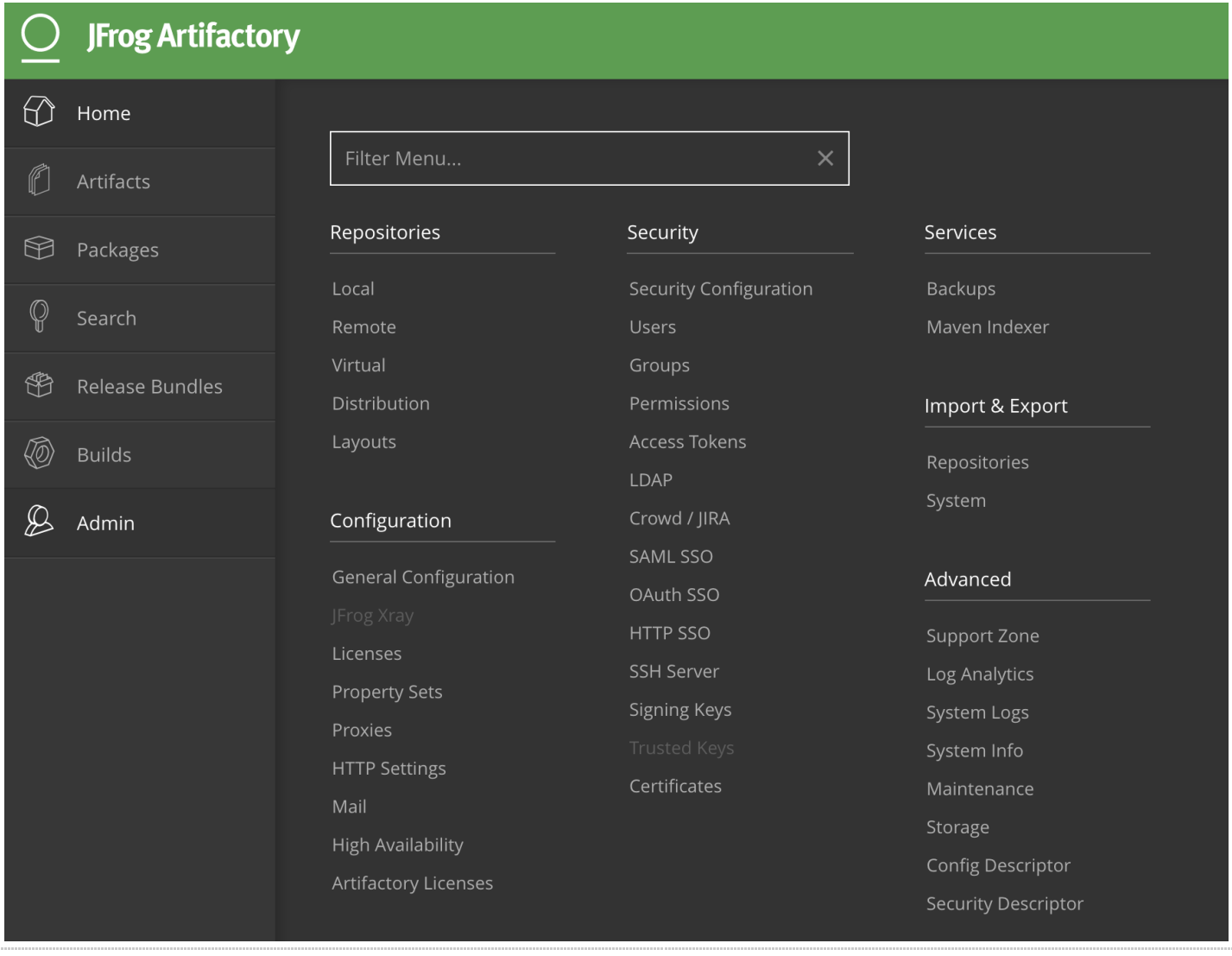
Хранение артефактов: Artifactory

JFrog Artifactory

Хранение артефактов: Artifactory

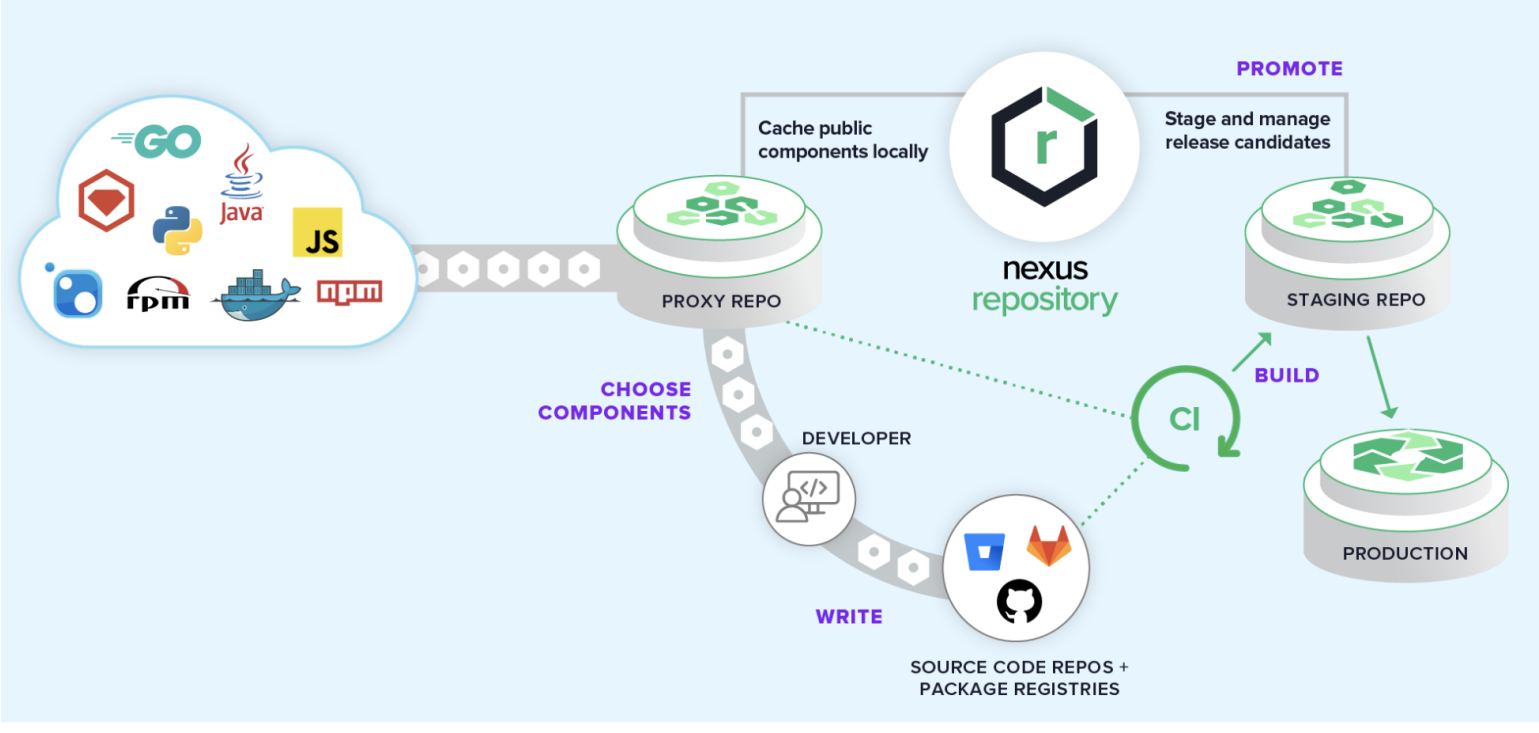
- Автоматизация и интеграция с большинством систем CI
- Высокая доступность
- Репликация
- Восстановление в случае аварии
- Расширяемость
- Внешнии хранилища (Filestore Sharding, Checksum-based Storage, Hybrid, Redundancy)
- Поддержка

Хранение артефактов: Artifactory



Хранение артефактов: Nexus Repository

Хранение артефактов: Nexus Repository



Хранение артефактов: Nexus Repository

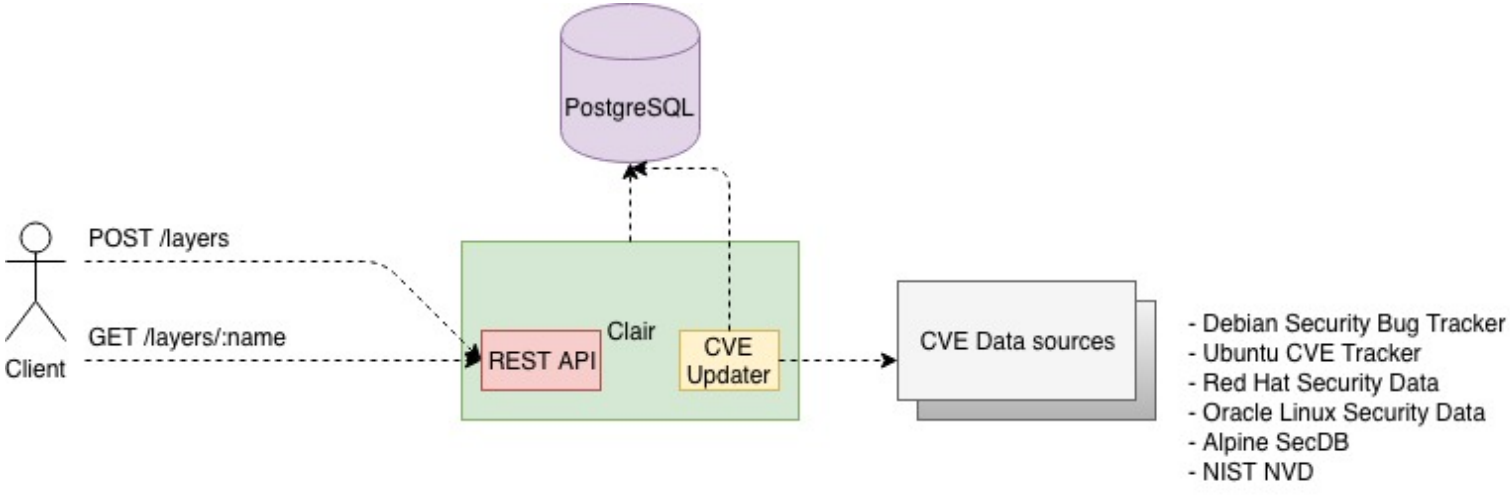
- Поддержка всех популярных форматов
- Расширенная поддержка Java (JVM)
- Поддержка доплнительных инструментов (Ansible, Docker, Chef, etc.)
- Безопасность
- Repository Health Check (RHC)
- Сканирование на безопасность и лицензионную чистоту
- Интеграция с LDAP, Atlassian Crowd, etc.

Security: Clair

Security: Clair

- REST API
- Статический анализ на уязвимости
- HTML отчеты

Security: Clair

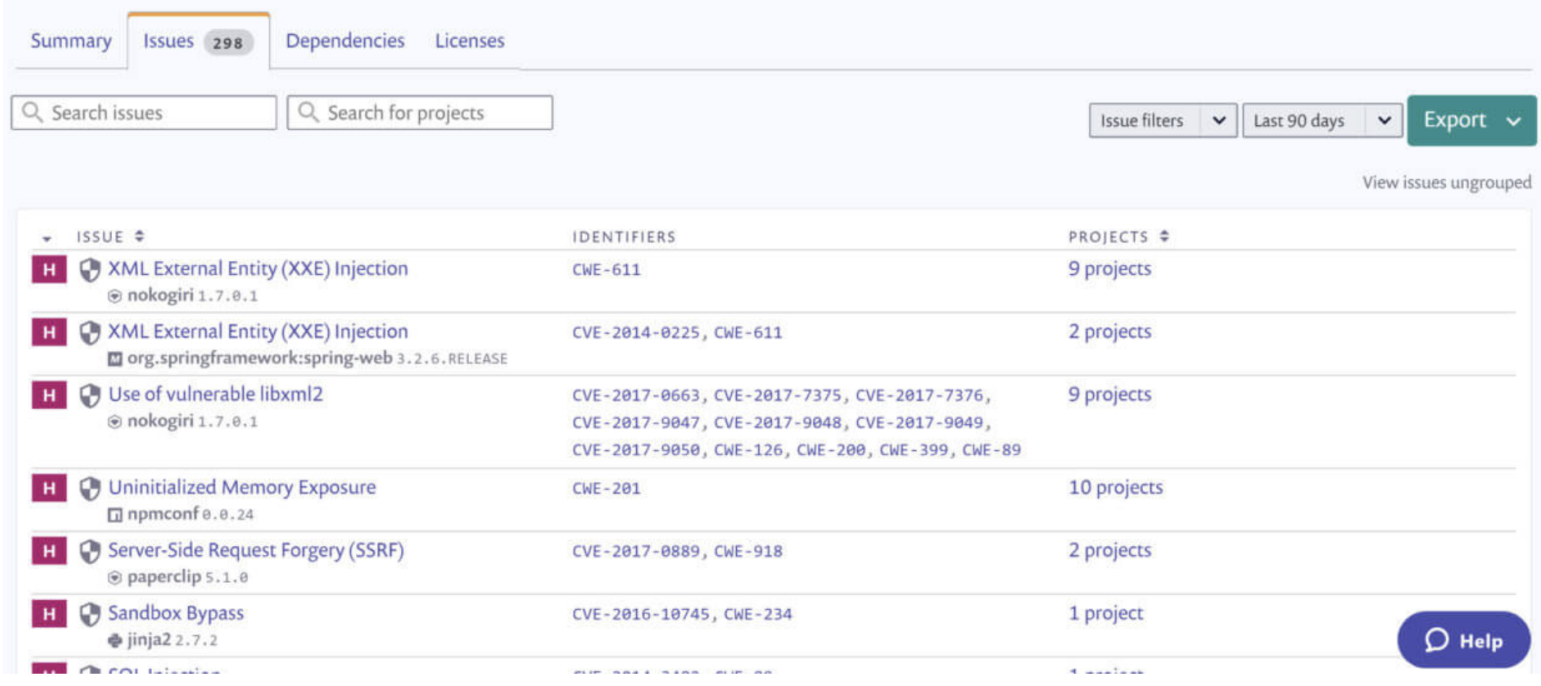


Security: Snyk

Security: Snyk

- Интеграция с Git
- Ингтеграция с инструментами CI/CD
- Сканирование в удаленных реджестри (Scan image stored in ECR, Artifactory)
- BOM report
- Copyright info
- Поддерживаемые языки (Java, Python, Net, Ruby, JS)

Security: Snyk



[Ссылка]

Security: Snyk

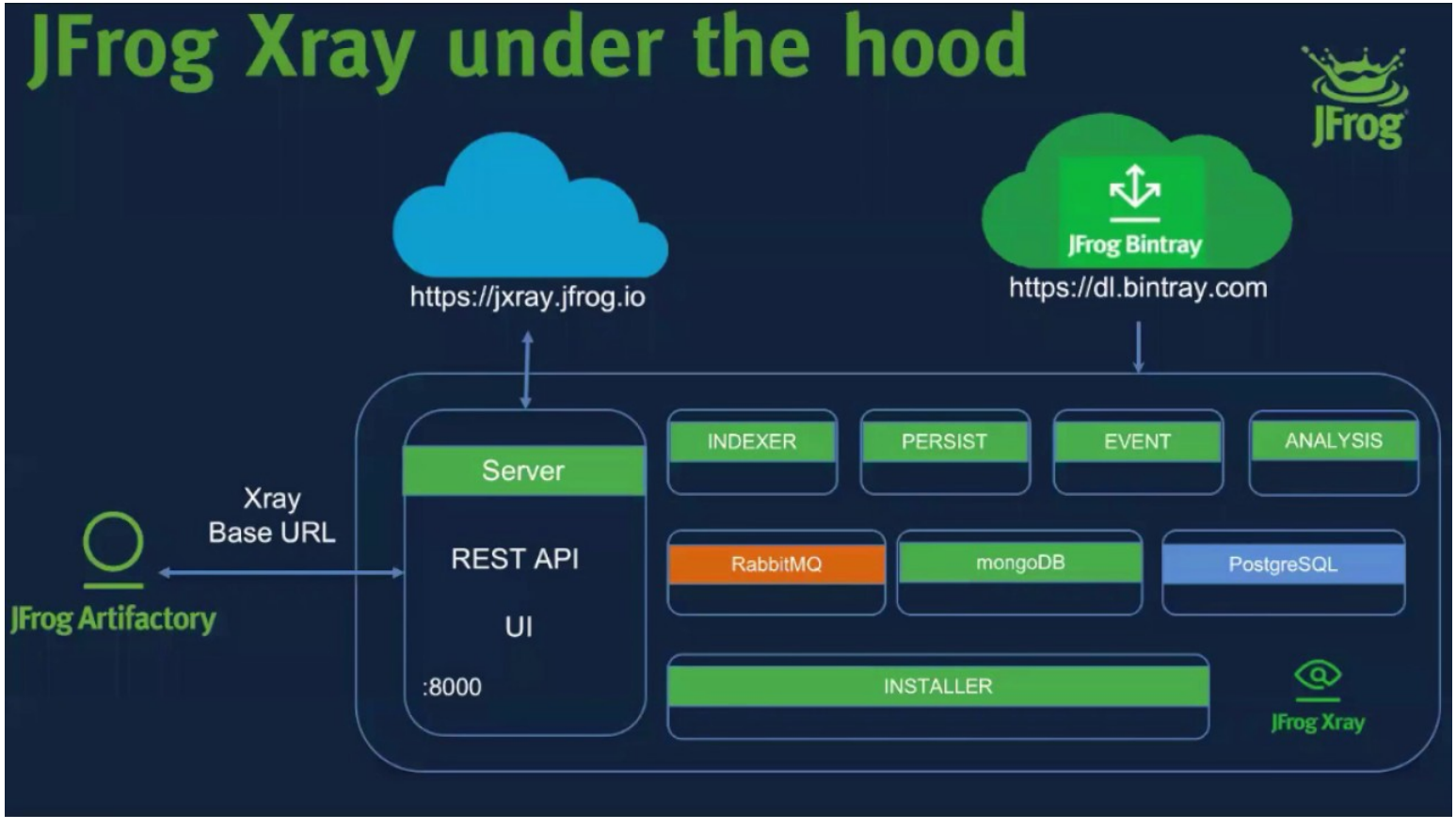
```
 dependancy_scanning:
  image: node:latest
  stage: test
  script:
 # Install npm, snyk, and snyk-to-html
 - npm install -g npm@latest
 - npm install -g snyk
 - npm install snyk-to-html -g
 # Run snyk help, snyk auth, snyk monitor, snyk test to break build and out report
 - snyk --help
 - snyk auth $SNYK_TOKEN
 - snyk monitor --project-name=goof-gitlab
 - snyk test --json | snyk-to-html -o snyk_results.html

  # Output report
  artifacts:
 when: always
 paths:

- snyk_results.html
```

Security: Xray

Security: Xray

- Универсальных инструмент для различных артефактов
- Высокая расширяемость
- Нативная поддержка Artifactory
- Готовая цепочка поставки артефактов
- Платная поддержка

Security: Xray



Security: Trivy

Security: Trivy

- Обнаружение комплексных уязвимостей
- Простота использования и простота установки
- Высокая точность
- DevSecOps ^_^

Security: Trivy

2. bash

```
bash-3.2$ trivy knqyf263/test-image:1.2.3
2019-05-13T15:19:03.912+0900    INFO    Updating vulnerability database...
2019-05-13T15:19:05.983+0900    INFO    Detecting Alpine vulnerabilities...
2019-05-13T15:19:05.987+0900    INFO    Updating npm Security DB...
2019-05-13T15:19:07.048+0900    INFO    Detecting npm vulnerabilities...
2019-05-13T15:19:07.048+0900    INFO    Updating pipenv Security DB...
2019-05-13T15:19:08.507+0900    INFO    Detecting pipenv vulnerabilities...
2019-05-13T15:19:08.508+0900    INFO    Updating bundler Security DB...
2019-05-13T15:19:09.574+0900    INFO    Detecting bundler vulnerabilities...
2019-05-13T15:19:09.575+0900    INFO    Updating cargo Security DB...
2019-05-13T15:19:10.441+0900    INFO    Detecting cargo vulnerabilities...
2019-05-13T15:19:10.441+0900    INFO    Updating composer Security DB...
2019-05-13T15:19:11.649+0900    INFO    Detecting composer vulnerabilities...

knqyf263/test-image:1.2.3 (alpine 3.7.1)
========================================
Total: 26 (UNKNOWN: 0, LOW: 3, MEDIUM: 16, HIGH: 5, CRITICAL: 2)

+---------+------------------+----------+-------------------+---------------+---------------------------------+
| LIBRARY | VULNERABILITY ID | SEVERITY | INSTALLED VERSION | FIXED VERSION |              TITLE              |
+---------+------------------+----------+-------------------+---------------+---------------------------------+
| curl    | CVE-2018-14618   | CRITICAL | 7.61.0-r0         | 7.61.1-r0     | curl: NTLM password overflow    |
|         |                  |          |                   |               | via integer overflow            |
+         +------------------+----------+                   +---------------+---------------------------------+
|         | CVE-2018-16839   | HIGH     |                   | 7.61.1-r1     | curl: Integer overflow leading  |
|         |                  |          |                   |               | to heap-based buffer overflow in|
|         |                  |          |                   |               | Curl_sasl_create_plain_message()|
+         +------------------+          +                   +---------------+---------------------------------+
|         | CVE-2019-3822    |          |                   | 7.61.1-r2     | curl: NTLMv2 type-3 header      |
|         |                  |          |                   |               | stack buffer overflow           |
+         +------------------+          +                   +---------------+---------------------------------+
|         | CVE-2018-16840   |          |                   | 7.61.1-r1     | curl: Use-after-free when       |
|         |                  |          |                   |               | closing "easy" handle in        |
|         |                  |          |                   |               | Curl_close()                    |
+         +------------------+----------+                   +---------------+---------------------------------+
|         | CVE-2018-16890   | MEDIUM   |                   | 7.61.1-r2     | curl: NTLM type-2 heap          |
|         |                  |          |                   |               | out-of-bounds buffer read       |
+         +------------------+          +                   +               +---------------------------------+
|         | CVE-2019-3823    |          |                   |               | curl: SMTP end-of-response      |
|         |                  |          |                   |               | out-of-bounds read              |
+         +------------------+          +                   +---------------+---------------------------------+
|         | CVE-2018-16842   |          |                   | 7.61.1-r1     | curl: Heap-based buffer         |
|         |                  |          |                   |               | over-read in the curl tool      |
|         |                  |          |                   |               | warning formatting              |
+---------+------------------+----------+-------------------+---------------+---------------------------------+
| git     | CVE-2018-19486   | HIGH     | 2.15.2-r0         | 2.15.3-r0     | git: Improper handling of       |
|         |                  |          |                   |               | PATH allows for commands to be  |
|         |                  |          |                   |               | executed from...                |
+         +------------------+----------+                   +               +---------------------------------+
```

Security: Sonarqube

Security: Sonarqube

- Поддержка языков (Kotlin, Scala, Ruby, Golang, etc.)
- Code Reliability
- Technical Debt
- Безопасность

Security: Notary

Security: TUF

Security: Portieris

Security: Portieris

- IBM Cloud Container Registry
- Quay.io
- Docker Hub

Security: Portieris

```
apiVersion: securityenforcement.admission.cloud.ibm.com/v1beta1
kind: ImagePolicy
metadata:
  name: allow-custom
spec:
   repositories:
    - name: "icr.io/*"
      policy:
        trust:
          enabled: true
          trustServer: "https://icr.io:4443" # Optional, custom trust server for
repository
```

Security: Binary Authorization for GKE