DevOps at Sonatype

Contents

1   DevOps at Sonatype

Lessons Learned from Using Repository Managers and Software Supply Chain Tools

Manfred Moser - @simpligility

• Community Advocate, Author & Trainer

Brian Fox - @brian_fox

• VP of Product Management

Sonatype - @sonatype - www.sonatype.com

2   What Are You Learning Today?

What worked? What caused problems?

→ Apply *our* lessons to *your* situation

3   What does Sonatype actually do?

Manages and develops:

• Central Repository (aka Maven Central)

• OSSRH and related Forges

• Nexus Repository Manager

• Nexus IQ Server

• Nexus IQ Data Services

• Related documentation, websites, blogs, videos,. . .

4   Software Component Warehouse

Nexus Repository Manager

• 70% market share

• > 61K active server installations

• Open Source: Maven2, npm, RubyGems, NuGet, Docker, . . .

• Commercial: Component Information, Staging, Smart Proxy, User Token, . . .

• Nexus 3 - distinct new codebase

5   Software Supply Chain Solutions

Solutions:

- Nexus Firewall

- Nexus Auditor

- Nexus Lifecycle

- Nexus Suite

Include

- Nexus IQ Server

- Integrations with Jenkins, Hudson, Bamboo

- Eclipse IDE/M2e Plugin

- SonarQube integration

- Command-line tool and REST API

All of this is backed by. . .

6   Nexus IQ Data Services

Managed and **curated** data and services for:

- Age

- Popularity

- Security vulnerability data

- License analysis data (observed and declared)

- Multiple component formats

7   Central Repository

aka. Maven Central

- Largest Maven2 format repository

- High performance, global CDN

- > 17 billion download in 2014

- > 1 million GAV coordinates

- Default in Apache Maven and others

And the components come from. . .

8   OSSRH and Forges

Input funnel for Central Repository

- OSSRH - large deployment of Nexus Repository Manager

- Apache, JBoss, … - secondary Nexus instances

- Community support - onboarding and documentation

9   More OSSRH and Central Stats

- currently about 100k projects total

- approx. 3000 new projects each month (GA)

- 10 - 30 project verfied and onbarded per day

- approx. 30.000 new releases each month (GAV)

10   Who Helps at Sonatype

- Internationally distributed

- Multiple-time zones

- Remote work the rule, not the exception

- Roughly 100 people

Tip
Western North America to Eastern Europe

---

images/nexus-team-timezones.png

11   Teams

- Numerous smaller teams

- Different focus of teams

- Cross-team members

- Dynamic grouping around efforts - *task force*

12   Process

In a nutshell - nothing special, no surprises.

images/usual-process.png

13 Process

- Scrum framework
- Kanban inspired
- Backlog refinement
- Regular meetings

→ Differs per team!

> Everyone has their own process. You need to figure out what works for you!

14 Communication

- Good old phone and VOIP
- Atlassian HipChat
- Google Hangouts
- join.me
- PagerDuty

Tip
Using video more has helped avoid misunderstandings.

---

15 Source Control

- GitHub - public and private
- Atlassian Stash - private only

Tip
We are an earlier Git adopter and use it exclusively.

---

16 Track and Plan

- Atlassian JIRA
- Trello
- Basecamp
- Aha.io
- Salesforce

Tool Lessons:

- Different people use different tools
- Overlap is inevitable
- Be prepared to implment integrations
- Tools come and go - be agile

17 Continuous Integration

- Stopped using Hudson long time ago

- Atlassian Bamboo

18 Build

- Apache Maven

- Grunt and NPM for client side

- Shell scripts

19 Maven Tips and Tricks

- Maven wrapper

- Follow best practices

- Organization POM

- Enforcer Plugin

- and lots more

20 (Maven) Project Complexity

Find balance for

- Number vs size of projects

- Multi-module vs multiple projects

- Consider release cycle

- IDE functionality

- Build time

Tip
Example Nexus OSS and Nexus Repository Manager

---

21 Develop

- Feature branches

  - short lived
  - sometimes shared between
  - automatic Bamboo feature branch build creation

- IDE

  - Eclipse IDE
  - IntelliJ IDEA

- Lots of OSX, some Windows & Linux

22 Test

Unit, functional and manual

- Junit

- Geb

- Spock

- Pax Exam

- Selenide

Tip
No tests, no merge!

---

23 Document

Multiple output formats from:

- Atlassian Confluence

- Google Docs

- Asciidoc

- Pelican

Instituting development workflows including

- Git-based versioning

- and branching,

- pull requests and reviews

- and CI builds

is very useful!

24 Continuously Build

- Atlassian Bamboo

- > 100 build plans

- Elastics Bamboo - EC2 instances

- Feature branch builds increases number

- Automated functional test suite runs

- Automated release

- Documentation builds and deployments

25 Build Plan Commonalities

All builds plans:

- Common configuration from base plan - used as shared artifact, managed in git repo

- Global variables - defaults that allow overrides

- *build* task - compile and test code.

- *release* task - publish to Nexus and tag in git

- bundle test artifacts

- Main vs features branches - different config

- Branch builds auto-created

Tip
Consistency helps users and administrators.

---

26 Bamboo Set Up & Tips

- Resource base plan project with tool configuration

- Fresh Maven repo for each build off Nexus

- Build plan notifications into HipChat channels

- Links to GitHub and JIRA

27 More Bamboo Set Up & Tips

- Limited number of standard Amazon Machine Images (AMI)

  - Include standard tools

- Share and store repo and other outputs as build artifacts

  - Stored on Amazon Elastic Block Storage (EBS)

- Static documentation = usable artifact

28 Validate

- SonarQube - integrated in Bamboo and GitHub

- License check with Maven plugin

- Pull requests and code reviews

  - No merges without build passing and code review

- Component policy with Nexus Lifecycle

29   Release

- Workflow and notification with Nexus staging

- Including validation with Nexus Lifecycle

  – Security checks
  – License checks
  – Architecture checks (e.g. component age)

- Usage of release build number - `2.11.4-01`

- Same release stuff on OSSRH

30   Release

images/nexus-bamboo-staging.png

31   Repository Manager

- Component source for consumers

- Component target for producers

images/producers-consumers.png

32   Colocate For Performance

Continuous integration is consumer and producer.

Best practice:

- Get it close together

- And sync to another repository if needed.

images/nexus-bamboo-rso.png

33   Software Supply Chain Management

> We are dogfooding our own tools - Nexus Repository Manager and Nexus Lifecycle

- SNAPSHOT versions of master are deployed to Nexus

- feature branch versions are not deployed

- master = integration branch

- within build cluster

- also used by developers

- target for deployments

- proxy

- host

- staging

- Thousands of users and projects on OSSRH

- smart proxy to Nexus outside cluster

34 Black and White Listing

Wont work .. tbd

35 Golden Repository

wont work

36 Nexus Lifecycle

- Visualize risk through rule-based automation

- Streamlines component selection with real time data

37 Starting Off

- Define risks we care about (internal, external, customer used)

- Open source contributions change out policy (since we contribute it makes sense to use bleeding edge)

- Understand our process and tooling

- limit overhead in our build automation

38 Nexus IQ Server Deployment

images/nexus-iq-server-integration.png

39 Policy

images/sonatype-policy.png

40 Resulting Report

images/nexus-clm-report.png

41   Nexus Lifecycle Lessons

- Surprise how many components are used - so many!

- Blocking a release for policy violations

    - is a big stick
    - but it works

Expect some cleanup of old issues

Socialize the resolution/enforcement process

Low noise and fast results increases usage, adoption

Automate and let the tooling do work (I already have a day job!)

Be responsive (That is my day job!)

42   Perimeter Protection

is Nexus Firewall. Can help

43   Deploy

Ops team:

- RPMs

- Docker images

44   Support

The support team consists of engineers only.

- Write lots of automation and other code

- Atlassian JIRA

- ZenDesk

45   Operations

- SaaS is used whenever possible

- Kanban process

- iDoneThis

Tip
Our Nexus instances vary from hundreds of GB to terabytes of non-proxied context.

---

46   Operations - Service Management

Nexus as component warehouse with Ansible

images/service-management.png

47   Community

- Actively work with vendors

- Including open source projects

- Help upstream to help yourself

  - Report issues
  - Release testing
  - Contributions

- Avoid forking third party libraries

- But do it cleanly when necessary

48   Next?

- Join the Nexus community

- Star using Nexus OSS

- Try Nexus Repository Manager

- Try Nexus Lifecycle

- Come to our booth

49   The End

Questions, Remarks & Discussion

Tip
Slides and examples at http://sonatype.github.io/nexus-presentations/ or email manfred@sonatype.com

---

  i. and we are hiring!

50   Resources

- sonatype.com

- Nexus community

- Central Repository and documentation

- Youtube channel

- Inside Engineering - blog post

- Inside Engineering - videos

- Nexus Tips from the Trenches video series

- 2014 Open Source Software Development Survey Results

- 2015 State of the Software Supply Chain Report

- Sonatype slides

- Repository Management with Nexus

- Java Tools and Technologies Landscape for 2014

- Nexus related slides including this one. . .