

DevOps at Sonatype

Contents

| | | |
|-----------|--|----------|
| 1 | DevOps at Sonatype | 1 |
| 2 | What Are You Learning Today? | 1 |
| 3 | What does Sonatype actually do? | 1 |
| 4 | Software Component Warehouse | 1 |
| 5 | Software Supply Chain Solutions | 2 |
| 6 | Nexus IQ Data Services | 2 |
| 7 | Central Repository | 2 |
| 8 | OSSRH and Forges | 3 |
| 9 | More OSSRH and Central Stats | 3 |
| 10 | Who Helps at Sonatype | 3 |
| 11 | Teams | 3 |
| 12 | Process | 3 |
| 13 | Process | 4 |
| 14 | Communication | 4 |
| 15 | Source Control | 4 |
| 16 | Track and Plan | 4 |
| 17 | Continuous Integration | 5 |
| 18 | Build | 5 |
| 19 | Maven Tips and Tricks | 5 |
| 20 | (Maven) Project Complexity | 5 |
| 21 | Develop | 5 |
| 22 | Test | 6 |
| 23 | Document | 6 |

| | | |
|-----------|--|-----------|
| 24 | Continuously Build | 6 |
| 25 | Bamboo Tips | 7 |
| 26 | More Bamboo Tips | 7 |
| 27 | Build Plan Commonalities | 7 |
| 28 | Repository Manager | 7 |
| 29 | Co-Locate For Performance | 8 |
| 30 | Validate | 8 |
| 31 | Release | 8 |
| 32 | Manage Components | 8 |
| 33 | Black and White Listing | 9 |
| 34 | Golden Repository | 9 |
| 35 | Nexus Lifecycle | 9 |
| 36 | Starting Off | 9 |
| 37 | Nexus IQ Server Deployment | 9 |
| 38 | Policy | 9 |
| 39 | Resulting Report | 9 |
| 40 | Nexus Lifecycle Lessons | 10 |
| 41 | Perimeter Protection | 10 |
| 42 | Deploy | 10 |
| 43 | Support | 10 |
| 44 | Operations | 10 |
| 45 | Operations - Service Management | 11 |
| 46 | Community | 11 |
| 47 | Next? | 11 |
| 48 | The End | 11 |
| 49 | Resources | 12 |

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 verified 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

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 implement 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 Bamboo Tips

- Resource project
- Fresh Maven repo for each build off Nexus
- Build plan notifications into HipChat channels
- Links to GitHub and JIRA

26 More Bamboo Tips

- Share and store repo and other outputs as build artifacts
- Static documentation = usable artifact
- Limited number of standard Amazon Machine Images (AMI)
- Include standard tools
- Build artifacts stored on Amazon Elastic Block Storage (EBS)
- Base build plan with tool configuration

27 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

28 Repository Manager

- component source for consumers
- component target for producers

images/producers-consumers.png

29 Co-Locate 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

30 Validate

- SonarQube - integrated in Bamboo and GitHub
- License check with Maven plugin
- No merges without build passing and code review
- Component policy with Nexus Lifecycle

31 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

images/nexus-bamboo-staging.png

32 Manage Components

Nexus Repository Manager and Nexus Lifecycle

Nexus Repository Manager

- 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

33 Black and White Listing

Wont work .. tbd

34 Golden Repository

wont work

35 Nexus Lifecycle

- Visualize risk through rule-based automation
- Streamlines component selection with real time data

36 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

37 Nexus IQ Server Deployment

images/nexus-iq-server-integration.png

38 Policy

images/sonatype-policy.png

39 Resulting Report

images/nexus-clm-report.png

40 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!)

41 Perimeter Protection

is Nexus Firewall. Can help

42 Deploy

Ops team:

- RPMs
- Docker images

43 Support

The support team consists of engineers only.

- Write lots of automation and other code
- Atlassian JIRA
- ZenDesk

44 Operations

- SaaS is used whenever possible
- Kanban process
- iDoneThis

Tip

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

45 Operations - Service Management

Nexus as component warehouse with Ansible

images/service-management.png

46 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

47 Next?

- Join the [Nexus community](#)
- Star using Nexus OSS
- Try Nexus Repository Manager
- Try Nexus Lifecycle
- Come to our booth

48 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!

49 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...](#)