

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	6
22	Test	6
23	Document	6

24	Continuously Build	7
25	Build Plan Commonalities	7
26	Bamboo Set Up & Tips	7
27	More Bamboo Set Up & Tips	7
28	Validate	8
29	Release	8
30	Release	8
31	Software Supply Chain Management	8
32	Nexus Repository Manager	8
33	Colocate For Performance	9
34	Nexus Lifecycle	9
35	Nexus IQ Server Deployment	9
36	Policy Configuration	9
37	Resulting Report	9
38	Nexus Repository Manager Tips	10
39	Black Listing and White Listing	10
40	Golden Repository	10
41	Perimeter Protection	11
42	Nexus Lifecycle Lessons	11
43	Deploy	11
44	Operations	11
45	Operations - Service Management	12
46	Support	12
47	Community	12
48	What's Next?	12

49 The End	13
50 Resources	13

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

Data and services for:

- Age
- Popularity
- Security vulnerabilities
- License information
- Multiple component formats

→ Constantly updated, curated and accurate data.

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
- 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 early 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

**Important**

CI infrastructure is an invaluable workhorse!

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

- Base plan for resources like tool configuration
- Fresh Maven repo for each build off Nexus
- Build plan notifications into HipChat channels
- Linked to GitHub branch and PR
- Linked to JIRA issue

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

Tip

No matter what you do .. there is always a chance something goes wrong.

30 Release

images/nexus-bamboo-staging.png

31 Software Supply Chain Management

We are dogfooding our own tools

- Nexus Repository Manager
- Nexus Lifecycle

including Bamboo integration and IDE integration.

32 Nexus Repository Manager

- Component source for consumers
- Component target for producers

images/producers-consumers.png

33 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

34 Nexus Lifecycle

- Define risks we care about
- Open source contributions change our policy
- Understand our process and tooling
- Limit overhead in our build automation

We gain

- Visualized risk through rule-based automation
- Streamlined component selection based on real time data

35 Nexus IQ Server Deployment

images/nexus-iq-server-integration.png

36 Policy Configuration

Simplified version:

images/sonatype-policy.png

37 Resulting Report

Overview section in notification:

images/nexus-clm-report.png

38 Nexus Repository Manager Tips

Here are a few things that work for us

- Versioning and component deployment
 - Only SNAPSHOT versions of *master* are deployed
 - Feature branch versions are *not* deployed
- Multiple server installations
 - In different networks
 - Smart proxy between them
- Release with Staging
 - Dogfooding ourselves
 - Thousands of users and projects on OSSRH

39 Black Listing and White Listing

Define

- Which components are okay to be used?
- Which components are *not* okay to be used?

Problem

- Too many criteria
- Complex and labor intensive to figure out criteria and values
- Usage influences criteria
- Different usage for different projects



Important

It just doesn't work! Too slow. Not scalable.

40 Golden Repository

Only the good components can be in the repository.

Problems:

- Components age like milk, not wine!
- A golden repository per project?
- Does not scale



Important

On the surface it looks easy. It's *not*!

41 Perimeter Protection

Nexus Firewall

- Requires up to date and accurate information
 - As provided by Nexus IQ Data Services
- Tremendous help to reduce influx
- But does not control usage

Tip

Helps, but is not the full solution. Just like a network firewall. Its not enough.

42 Nexus Lifecycle Lessons

Once we had Nexus Lifecycle and started using it. . .

- Surprised how many components are used
- Blocking a release for policy violations
 - is a big stick
 - but it works
- Shared ownership helps - socialize the resolution/enforcement process
- Initial introduction forced some cleanup of old issues
- Ongoing low noise and fast results increases usage, adoption

→ Without the automation this would be not achievable!

43 Deploy

Ops team:

- RPMs
- Docker images
- Manual tweaks
- Ansible

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 Support

The support team consists of engineers only.

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

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
 - And send back upstream

48 What's Next?

- Join the Nexus community at <http://www.sonatype.org/nexus>
- Start using Nexus OSS
- Try Nexus Repository Manager
- Try Nexus Lifecycle

Tip

Come to our booth for demos, T-shirts and more.

49 The End

Want to help us → we are hiring!

Questions, remarks & discussion

Slides

- <http://sonatype.github.io/nexus-presentations/>
- or email manfred@sonatype.com

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...](#)
-