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

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
- Default in Apache Maven and others

And the components come from… OSSRH and Forges

- OSSRH - large deployment of Nexus Repository Manager
- Apache, JBoss, java.net … - secondary Nexus instances
- Community support - on-boarding and documentation

8 More OSSRH and Central Stats

- > 17 billion download in 2014
- > 1 million GAV coordinates
- 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)

9 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

10 Teams

- Numerous smaller teams
- Different focus of teams
- Cross-team members
- Dynamic grouping around efforts - *task force*

11 Process

In a nutshell - nothing special, no surprises.

images/usual-process.png

12 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!

13 Product Owner Team

Multi-disciplinary team:

- Security
- Development
- Architecture
- User experience
- Documentation

14 Communication

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

> **Tip**
> Using video more has helped avoid misunderstandings.

15 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

16 (Maven) Project Complexity

Find balance for

- Number vs size of projects
- Multi-module vs multiple projects
- Consider release cycle
- Branching, Git and CI integration
- IDE functionality
- Build time

> **Tip**
> Example Nexus OSS and Nexus Pro

17 Develop

- Feature branches
  - short lived
  - sometimes shared between
  - automatic Bamboo feature branch build creation
  - feature flags for longer lived efforts
- IDE
  - Eclipse IDE
  - IntelliJ IDEA
- Lots of OSX, some Windows & Linux

18 Test

Unit, functional and manual

- Junit
- Geb
- Spock
- Pax Exam
- Selenide

> **Tip**
> No tests, no merge!

19 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!

20 Continuously Build

- Atlassian Bamboo with Elastic Bamboo
- > 100 build plans
- Feature branch builds increases number
- Automated test, release and deployment
- Base plan build with shared artifact
- All plans same setup
- Share outputs as artifacts

Tip
Consistency helps users and administrators.

21 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

22 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.

23 Software Supply Chain Management

> We are dogfooding our own tools

- Nexus Repository Manager
- Nexus Lifecycle

including Bamboo integration and IDE integration.

24 Nexus Repository Manager

- Component source for consumers
- Component target for producers

images/producers-consumers.png

25 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

26 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

27 Nexus IQ Server Deployment

images/nexus-iq-server-integration.png

28 Policy Configuration

Simplified version:

images/sonatype-policy.png

29 Resulting Report

Overview section in notification:

images/nexus-clm-report.png

30 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

31 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.

32 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*!

33 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.

34 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!

35 Operations - Service Management

Nexus as component warehouse with Ansible

images/service-management.png

36 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

37 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.

38 The End

Want to help us → we are hiring!

Questions, remarks & discussion

Slides

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

39 Resources

- sonatype.com
- Nexus community
- Central Repository and documentation
- Inside Engineering - blog post
- Inside Engineering - videos
- Nexus Tips from the Trenches video series
- 2015 State of the Software Supply Chain Report
- Repository Management with Nexus
- Java Tools and Technologies Landscape for 2014
- Nexus related slides including this one. . .