Sonatype

Nexus Pro CLM Edition

Enhanced Repository Management: Automated Policy Governance for Agile Development Efforts

Analysis shows that greater than 80% of a typical application is comprised of components, most of which are open source and originate from hundreds of projects outside the enterprise. While component-based development improves productivity and speed, organizations must gain control over the ever-changing security, licensing and quality risks. In response, Sonatype has brought an innovative platform to market called Component Lifecycle Management (CLM). CLM supports the entire software lifecycle while Nexus Pro CLM Edition governs component usage both within and through the Nexus repository manager. Nexus Pro CLM Edition provides security, licensing and other critical information about the components in your repository and generates a complete Bill of Materials for all of the applications released via Nexus Pro staging. Using automated security, licensing and architecture policies, you can manage the release process to ensure that only applications with trusted components are promoted.

Nexus Pro CLM Edition

Nexus Pro CLM Edition improves the visibility and control of your component-based development by analyzing the content of your application builds and automatically controlling the release process using security, licensing and quality criteria. Security, licensing and architecture policies codify your organization standards and applications with different security profiles. These policies are automatically enforced during the build promotion and staging process to ensure that only trusted applications are promoted through to production.

Nexus Pro CLM Edition is the first repository-based component management solution to provide:

Efficiency: Enable development teams to enjoy the benefits of agile development in a streamlined and structured environment.

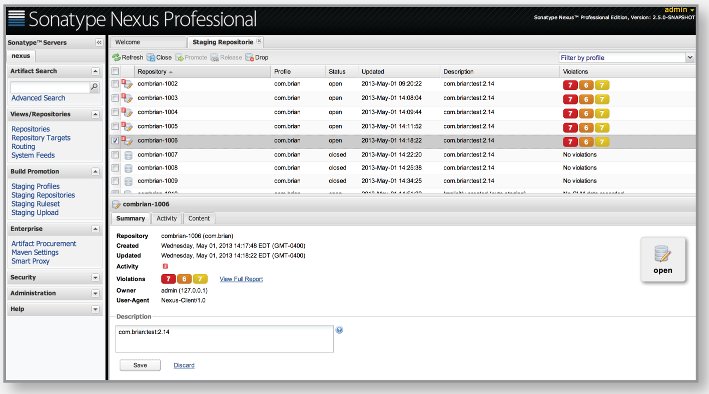
- Nexus Pro reduces build times & improves collaboration between all developer constituents and teams.
- Nexus Pro CLM Edition extends Nexus Pro by providing the ability to govern the build release process.

Component Intelligence: Provide reporting on the health of all components by delivering complete component intelligence, analyzing both the security and licensing state of all components used in your applications.

- Security, licensing and popularity data for all components and dependencies provided as part of the build process.
- Visibility into internally developed components and components downloaded from public repositories allow you to analyze repository health.

Enable the enterprise: Builds on the leading enterprise repository management solution that ensures components are always available for sharing, and delivered securely.

- Advanced repository features like HA, advanced security, repository health check, 24x7 expert support makes your repository platform ready for the enterprise.
- The repository manager improves developer efficiency by enabling faster and more reliable builds, and improving collaboration and sharing between developers.



Repository	Profile	Status	Updated	Description	Violations
combrian-1002	com.brian	open	2013-May-01 09:20:22	com.brian:test:2.14	7 6 7
combrian-1003	com.brian	open	2013-May-01 14:08:04	com.brian:test:2.14	7 6 7
combrian-1004	com.brian	open	2013-May-01 14:09:44	com.brian:test:2.14	7 6 7
combrian-1005	com.brian	open	2013-May-01 14:11:52	com.brian:test:2.14	7 6 7
☑ combrian-1006	com.brian	open	2013-May-01 14:18:22	com.brian:test:2.14	7 6 7
combrian-1007	com.brian	closed	2013-May-01 14:22:20	com.brian:test:2.14	No violations
combrian-1008	com.brian	closed	2013-May-01 14:25:38	com.brian:test:2.14	No violations
combrian-1009	com.brian	closed	2013-May-01 14:34:25	com.brian:test:2.14	No violations
combrian-1010	com.brian	open	2013-May-01 14:51:22	Implicitly created (auto staging)	No CLM data recorded

combrian-1006

Summary | Activity | Content

Repository combrian-1006 (com.brian)
Created Wednesday, May 01, 2013 14:17:48 EDT (GMT-0400)
Updated Wednesday, May 01, 2013 14:18:22 EDT (GMT-0400)
Activity
Violations 7 6 7 View Full Report
Owner admin (127.0.0.1)
User-Agent Nexus-Client/1.0

open

Description

com.brian:test:2.14

Save Discard

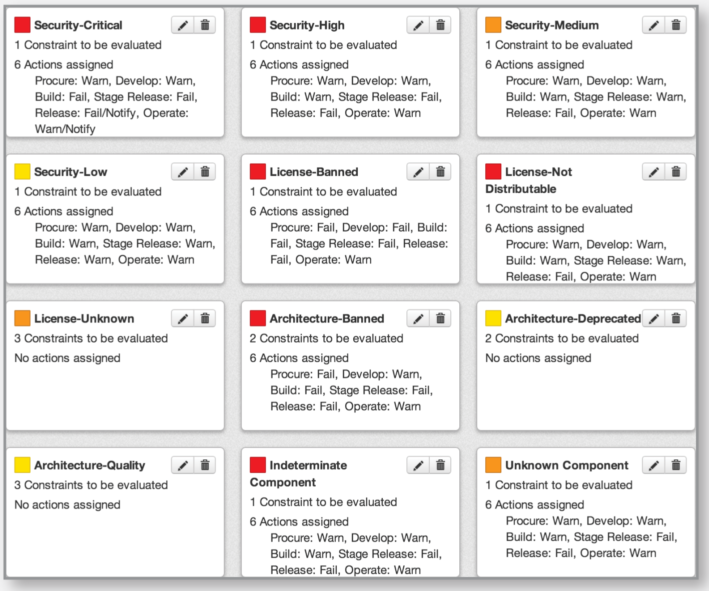
▲ Nexus Pro provides visibility into the components that violate your security, licensing and architecture policies.

Improved Security: Apply security licensing and architecture policies to ensure trusted applications are promoted and staged as part of the build release process.

- Automatically validate components based on up to date component intelligence provided by Sonatype ensures the releases you produce meet your security, licensing and architecture standards.
- Ensure that any whitelists or black lists you maintain are enforced using notifications or by automatically stopping the staging process.

Path to Full CLM: Repository-based visibility and control provides a natural path to component lifecycle management for the entire software development lifecycle (SDLC).

- Organizations can leverage their repository manager and release process to improve visibility and control without impacting the development process.
- Extending your repository-based policies to support the entire lifecycle, including IDE integration and continuous production monitoring is easily achieved.



🟥 **Security-Critical**
1 Constraint to be evaluated
6 Actions assigned
Procure: Warn, Develop: Warn, Build: Fail, Stage Release: Fail, Release: Fail/Notify, Operate: Warn/Notify

🟥 **Security-High**
1 Constraint to be evaluated
6 Actions assigned
Procure: Warn, Develop: Warn, Build: Warn, Stage Release: Fail, Release: Fail, Operate: Warn

🟧 **Security-Medium**
1 Constraint to be evaluated
6 Actions assigned
Procure: Warn, Develop: Warn, Build: Warn, Stage Release: Warn, Release: Fail, Operate: Warn

🟨 **Security-Low**
1 Constraint to be evaluated
6 Actions assigned
Procure: Warn, Develop: Warn, Build: Warn, Stage Release: Warn, Release: Warn, Operate: Warn

🟥 **License-Banned**
1 Constraint to be evaluated
6 Actions assigned
Procure: Fail, Develop: Fail, Build: Fail, Stage Release: Fail, Release: Fail, Operate: Warn

🟥 **License-Not Distributable**
1 Constraint to be evaluated
6 Actions assigned
Procure: Warn, Develop: Warn, Build: Warn, Stage Release: Warn, Release: Fail, Operate: Warn

🟧 **License-Unknown**
3 Constraints to be evaluated
No actions assigned

🟥 **Architecture-Banned**
2 Constraints to be evaluated
6 Actions assigned
Procure: Fail, Develop: Warn, Build: Fail, Stage Release: Fail, Release: Fail, Operate: Warn

🟨 **Architecture-Deprecated**
2 Constraints to be evaluated
No actions assigned

🟨 **Architecture-Quality**
3 Constraints to be evaluated
No actions assigned

🟥 **Indeterminate Component**
1 Constraint to be evaluated
6 Actions assigned
Procure: Warn, Develop: Warn, Build: Warn, Stage Release: Fail, Release: Fail, Operate: Warn

🟧 **Unknown Component**
1 Constraint to be evaluated
6 Actions assigned
Procure: Warn, Develop: Warn, Build: Warn, Stage Release: Fail, Release: Fail, Operate: Warn

▲ Security, licensing and architecture policies are easily defined and enforced during build promotion and staging using Nexus Pro CLM Edition.

What Makes Sonatype Different

As the stewards of the Central Repository, the creators of the Apache Maven project and the distributors of the Nexus repository manager, Sonatype has pioneered the tooling that delivers components to over 10 million developers and their millions of applications. Sonatype dramatically alters the traditional security equation by fixing at-risk components. This reduces the need for specialized and expensive security experts required by post-development, "problem discovery" approaches. By providing developers with the information needed to make applications as secure as possible, they become the frontline defense against vulnerabilities, delivering the broadest and least costly mode of securing applications. Because Sonatype continuously monitors your application inventory for newly reported vulnerabilities, CLM creates a platform for sustainability and ongoing trust.

Sonatype CLM is the only software platform specifically designed for the modern, component-based software supply chain. Sonatype's solution extends to the entire software supply chain by not only supporting FOSS but also internally developed and third party components. This modern approach to software assurance makes it possible to both identify and reduce risk and ensure compliance without impeding development velocity. This enables developers to deliver applications at the pace business demands.

Nexus Pro CLM Edition is the only solution that extends the industry leading repository manager with policy support to ensure that trusted applications are promoted for production consideration. Nexus Pro CLM Edition provides the visibility and control you need at the build release stage to ensure your agile, component-based development efforts deliver trusted solutions. This repository-based management approach is a natural starting point for complete lifecycle management.

On a global scale, Sonatype enables organizations to "Go Fast and Be Secure".

About Sonatype

Sonatype has been on the forefront of creating tools to manage, organize, and better secure components since the inception of the Central Repository and Maven in 2001. Today, over 70,000 companies download over 8 billion components every year from the Central Repository, demonstrating the explosive growth in component-based development. Today's software ecosystem has created a level of complexity that is increasingly hard to manage. Partnering with application developers, security professionals and the open source community, Sonatype has introduced a way to keep pace with modern software development without sacrificing security. We call it Component Lifecycle Management (CLM), the new platform for securing the modern software supply chain.

We believe that to achieve application security, the approach has to be simple to use, integrated throughout the lifecycle and ensure sustaining trust. With CLM we're improving the visibility, management and security of component-based development across the entire lifecycle. Together with our customers, we're ushering in a new era of application security.

Sonatype
12501 Prosperity Drive • Suite 350
Silver Spring, MD 20904
877.866.2836 • www.sonatype.com