Sonatype

USE CASE

# NEXUS REPOSITORY MANAGEMENT AND NEXUS LIFECYCLE

## FOR OPERATIONS

Let’s start with you. Chances are, you are part of the operations team at your organization... responsible for all the production servers and the applications running on them. Keeping them up and running and humming away nicely is your job. Maybe you also look after the servers for your testing environments as well as the infrastructure for your developers like the continuous integration servers, the version control system and so on. How about automation in support of continuous and DevOps goals? And maybe you already run the repository manager Sonatype Nexus on one of these servers. If you are, that’s great. We can hopefully show you how to get even more value from Nexus. And if you’re not, we hope you’ll be eager to try Nexus in your environment.

## KEY BENEFITS

### Streamlining your ‘Software Supply Chain’

What happens when a new vulnerability is identified in an open source component leveraged by your developers? How long will it take for you to find and fix any and all implementations?

One important aspect of effectively supporting applications running in production, is understanding their requirements as well as their composition. With today’s component-based development, you have a software supply chain around each of your applications. What components (parts) are built into your applications? Do you have an accurate inventory, or ‘bill of materials’, for each release to enable you to quickly target your response to the inevitable vulnerability?

There are several proven principles that leading IT organizations implement to optimize this software supply chain: Use fewer and better suppliers (i.e. open source projects), use the highest quality parts from those suppliers (i.e. components, libraries, frameworks), and ensure complete traceability across the software development life cycle. The Nexus platform of software supply chain solutions allows you to apply these principles to eliminate complexity so you can deliver faster, improve efficiency and maintain optimal quality.

With this software supply chain approach, you control and understand all parts involved in creating your application from the source of your supplier to the usage within an application in production. From an operations perspective this means that you understand what is used in detail and can initiate necessary product upgrades or recalls. These component parts need to be managed in some central storage system - a repository manager.

## What is Repository Management?

The Nexus line of repository managers are servers specifically designed to help you manage binary libraries and packages that development teams use to create their applications. These components come in many different forms - some of which are open source - and are the building blocks for creating powerful applications, which in turn are considered to be components on a larger scale. They come as Java archives, Java web archives and others in a Maven repository; NuGet packages in a NuGet repository; or JavaScript libraries in a NPM repository. Nexus allows you to manage all the different components found in the different repositories and expose them to a large variety of tools ranging from simple bash scripts using curl or wget to complex build setups with Maven, Grunt or some other build tool or custom integrations.

In the same way that Git or Subversion is used for version control for your source code, a Nexus repository manager is a critical part of your software development infrastructure that allows you to manage all binary components, build outputs and their versions.

## Nexus Lifecycle

Once you store and manage your components and build outputs in a repository manager and everything is in one location, it is far easier to understand and control your component usage. Nexus Lifecycle is designed for that purpose. It includes features such as up-to-date component intelligence, policy creation and enforcement, as well as detailed reporting. Nexus Lifecycle has integration points for the Nexus repository manager, integrated development environments, continuous integration servers, build tools and other tools. With a rich web application for administration and configuration as well as reporting, Nexus Lifecycle can expose and control component usage throughout your software development life cycle. You can optimize your software supply chain and automate any enforcements to ensure only the highest quality component parts - especially those without known vulnerabilities - make it into your production applications.

## Using Nexus to Support Dev and QA

With the Nexus Repository Manager and Nexus Lifecycle, you can bring numerous benefits to your development and operations teams:

- By proxying external repositories like the Central Repository or NuGet.org and the resulting caching of components in Nexus, you can avoid repeated downloads of component and therefore save bandwidth and time for each build and developer.
- Components that are not available in external repositories can be made available throughout your organization by simply uploading them to Nexus and hosting them there. This greatly simplifies their usage and avoids the need for yet another infrastructure to host them and another access method to use them.
- Up-to-date component intelligence including known security vulnerabilities, license details, age and popularity helps your entire organization choose the latest and highest quality component. In turn you can avoid legal issues, usage of suboptimal components or even security breaches due to wrong component choices.
- Control component usage by enforcing the repository manager as the only source. This allows you to improve build times for everyone, as well as ensure that architecture standards are followed.
- Fulfill regulatory requirements to control component usage for process audits, software escrow and similar tracking needs by controlling Nexus and its management and storage.
- Release process tooling in Nexus includes validation, email notifications and dedicated security access. You will benefit from the improved visibility and control and in turn create better releases with more confidence.
- Nexus Lifecycle can further enhance your component release processes by adding policy validation

at any stage of the software development life cycle. The policies allow you to ensure release component quality following the criteria of your choice.

- Policy validation and inspection from Nexus Lifecycle can be accessed and automated with the numerous tool integrations. You can completely integrate these tools in your development lifecycle and expose component intelligence and insight in the tools you use every day - no matter if you are a developer, work on QA or are purely doing operational work.

## Ops Supporting Ops with Nexus

Beyond the use cases above, a number of operations specific use cases allow you take advantage of both the Nexus Repository Manager and Nexus Lifecycle.

- Components produced by the development team, and hosted in Nexus, can be consumed for deployments to your testing and production infrastructure. This removes the need to maintain another infrastructure and process for handling these components.
- Ops tooling like installer and package creation tools can use the components in the repositories to create downstream components required by operations deployment e.g. RPM archive exposed via a yum repo from a Java-based WAR files in a Maven repository or similar with other formats like NuGet, NPM and others. Again, this keeps your infrastructure simple to maintain and easy to understand for your users. All components are in one place.
- Repositories in Nexus (e.g. the yum format) can be used to allow operations to provision production environments.
- Any binary components required by the operations teams, including third-party application installers and others, can be stored and managed in Nexus.
- Deployment and provisioning tools like Puppet, Chef or simply scripts can access Nexus as a source for components to deploy.
- Nexus repositories can be monitored to determine availability of new internally produced components. The improved visibility simplifies internal communication and reduces the need for other setup and procedures.
- Nexus release process improvements can be configured to include enforcement of operations requirements from a legal, security as well as architectural viewpoint resulting in higher quality releases in these aspects.
- Operations team can be included in the release process automation and notification as a critical stakeholder and potentially a final recipient for component deployment.
- The 'bill of materials' reports created by Nexus Lifecycle for deployment components allows the operations team to easily supply an inventory of components and any known security or license concerns to security, legal and management teams as requested. This process takes only a click of a button and saves an immense amount of time over other manual options.
- Bill of material component monitoring can alert the operations team regarding new security vulnerabilities for components in currently deployed applications. This allows you to react to new vulnerabilities as soon as they are known, without any research or monitoring efforts on your side, and enables you to prevent security breaches in your applications running in production.
- Components deployed to Nexus can easily be made available for download externally with advanced privilege management, eliminating the need to maintain another infrastructure for finished products.

## Conclusion

While the usage of the Nexus Repository Manager and Nexus Lifecycle-based policy management are a well understood development practice with numerous benefits, your operations team can use these same tools for a wide variety of operations purposes. Visit www.sonatype.com/nexus-platform for more information.

## References

*Details about components, repositories and related concepts: http://books.sonatype.com/nexus-book/reference/concepts.html*

*Comprehensive documentation for Sonatype Nexus - Repository Management with Sonatype Nexus - http://books.sonatype.com/nexus-book/*

*Nexus Lifecycle documentation - http://books.sonatype.com/sonatype-clm-book/html/*

Sonatype helps organizations build better software, even faster. Like a traditional supply chain, software applications are built by assembling open source and third party components streaming in from a wide variety of public and internal sources. While re-use is far faster than custom code, the flow of components into and through an organization remains complex and inefficient. Sonatype's Nexus platform applies proven supply chain principles to increase speed, efficiency and quality by optimizing the component supply chain. Sonatype has been on the forefront of creating tools to to improve developer efficiency and quality since the inception of the Central Repository and Apache Maven in 2001, and the company continues to serve as the steward of the Central Repository serving 17.2 Billion component download requests in 2014 alone. Sonatype is privately held with investments from New Enterprise Associates (NEA), Accel Partners, Bay Partners, Hummer Winblad Venture Partners and Morgenthaler Ventures. Visit: www.sonatype.com

Sonatype Inc. • 8161 Maple Lawn Blvd, Suite 250 • Fulton, MD 20759 • 1.877.866.2836 • www.sonatype.com