VMware™

Tanzu Application Catalog™

Bitnami Open Source Software for Enterprise

To truly harness the power of cloud native applications, every organization must leverage open source technology. Yet, there is a disconnect between developers who use open source software to innovate and operators who must enforce IT policy for software running in production environments. Tanzu Application Catalog bridges that gap between developer productivity and IT governance—it gives developers a private self-service registry of Bitnami open source containers that are continuously maintained to meet the IT governance needs of operators in each organization.

The challenge with open source software

Bitnami, acquired by VMware in 2019, is a leading publisher of pre-packaged open source software. Millions of developers trust Bitnami’s library of containers and cloud images because they are consistently kept up-to-date, packaged using best practices, and quickly patched in the event of a vulnerability. Despite this goodwill among the developer community, many organizations still cannot run Bitnami’s free containers in production.

To reduce the threat of critical application outages or security breaches posed by open source software, enterprises must have full transparency and auditability for the apps and components they deploy in production environments. Until now, the only way to meet this demand has been for developers to tediously maintain open source software “by hand.” Organizations face multiple layers of complexity in managing hundreds or thousands of apps built by various teams, each using different mixes of self-maintained open source components with different binaries, libraries, and software licenses in every stack. Clearly, a new approach to sourcing and managing open source software is needed.

One solution that meets the needs of developers and operators

Tanzu Application Catalog is designed to combine the convenience of public container registries and marketplaces with the transparency and trust of maintaining open source software by hand. It delivers a set of pre-packaged container images and Helm charts from the Bitnami collection, chosen and curated by the customer, that are built on each customer’s unique security-hardened base operating system images (“golden images”) and deposited into private container repositories. Each container is continuously updated and comes with metadata proving the trustworthiness of the software within. With Tanzu Application Catalog, developers can focus on building their applications while operators maintain full accountability for the open source software running in their environments.
Curate a custom catalog of open source containers, packaged for Kubernetes and delivered to your repository

Tanzu Application Catalog is a customizable selection of open source software from the Bitnami collection that is continuously maintained and verifiably tested for use in production environments. It gives developers the productivity and agility of pre-packaged apps and components, while enabling operators to meet the stringent security and transparency requirements of enterprise IT.

Keep Open Source Containers Patched and Current

Standardize open source software across your organization on a catalog that’s consistently updated by known and trusted sources.

Transform DevOps Into DevSecOps

Bring developers, security, and operations together to automate critical processes and controls.

Improve Developer Productivity

Enable developers to focus on innovation by automating patches, upgrades, and dependency management.

Loved by Developers, Trusted by Ops

Tanzu Application Catalog brings the power of open source into the Enterprise, significantly benefiting IT operators and software developers alike.

For Operators:

Operators use Tanzu Application Catalog to provide pre-packaged, production-ready open source containers and Helm charts for developers to use in their custom applications. This can increase overall productivity by giving developers on-demand, self-service application components, while retaining the same level of compliance with IT security and auditability governance that came with maintaining them in-house.

InfoSec teams and platform operators access container metadata through the UI or API. Vital compliance and audit details are available, including:

• A history of updates to each container and Helm chart
• A manifest of libraries, binaries, and software licenses in every container
• Results of tests run in every environment relevant to the customer for every update
• Proof of open source security and virus scans
• Links to the upstream source of libraries and binaries included in every container

FEATURES:

• Pre-packaged applications and application components delivered as Docker containers and Helm charts
• Customer-curated; selection can be updated as needed
• Containers can be built on your “golden” OS image, or you can select one maintained with best practices by VMware
• Containers are kept up-to-date automatically; any change to upstream code or base OS triggers rebuild and retesting
• Each container comes with documented metadata
• Continuously updated Helm charts for container orchestration included
• Push or pull: containers and charts are either pushed to your private repository, or we store them for you to pull
SOLUTION OVERVIEW

**Top Apps & Components Available for Your Catalog:**

**Language Runtimes**
- Nodejs
- Python
- Ruby
- Java

**Databases**
- MySQL
- PostgreSQL
- MariaDB
- MongoDB

**App Components**
- Kafka
- RabbitMQ
- NATS
- TensorFlow
- ElasticSearch
- FluentD

**Developer Tooling**
- Harbor
- Artifactory
- Jenkins
- Git
- Redmine
- Zookeeper
- Prometheus

**By Developers:**

Developers have long used pre-packaged containers and Helm charts from public repositories and marketplaces to develop custom applications. For production workloads, however, developers must separately build and maintain their own containers that conform to IT security and auditability standards. They build the container images they need either manually or with configuration management tools. These images are then stored in private repositories, to be fed into existing DevOps workflows.

Developers who use Tanzu Application Catalog simply replace the containers and Helm charts they were maintaining for production workloads with IT-approved containers and charts built and maintained by VMware. These can be downloaded for local development, or they can be used in production. For development teams that rely on hand-built containers, Tanzu App Catalog is a huge leap forward in efficiency, compliance, and better security.

**How it works**

Streamline development with a continuously maintained catalog of open source components and applications.

**Choose Your Software**

Choose open source software from the Bitnami library that you want to use in production: from components like runtimes and databases to turnkey apps like content management and developer productivity tools.

**Specify Your Operating System**

Tanzu Application Catalog supports golden images with your preferred specifications, agents, and settings. Upload your standard OS image, and Tanzu Application Catalog will build and test your containers on top of it. Don’t have a golden image? No problem—choose a base OS image maintained with best practices by VMware.

**Deploy With Confidence**

Let Bitnami automation continuously update your catalog with the latest security patches, app or component version updates, and base operating system changes. This way, you’re always deploying the most performant and secure stack. Easily audit what is in the stack, code provenance, licenses, test results, and security scans for the open source libraries and binaries in your catalog.

Learn more at [https://cloud.vmware.com/tanzu-application-catalog](https://cloud.vmware.com/tanzu-application-catalog).