Nexus Smart ID

Product deployment strategy

Abstract

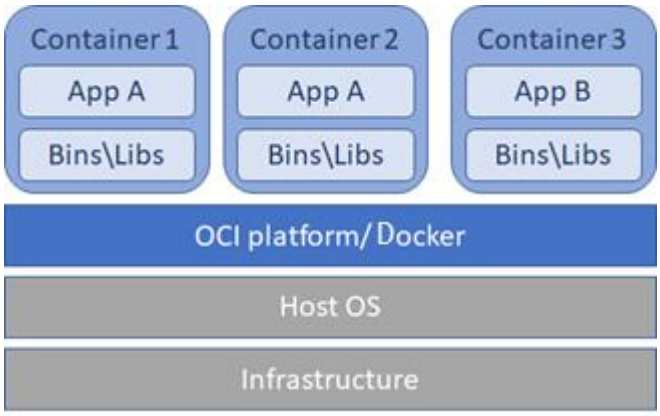
Nexus has decided on a Docker first approach for the Smart ID product family. The container technology will simplify deployment and software updates since all dependencies are packaged within the Docker image.

Customers having challenges with the Docker first approach, are encouraged to address this with Nexus to find a solution for the specific cases.

By introducing Docker, Nexus takes an important step forward in terms of deployment harmonization, automation, and cloud-readiness. This document will describe the background, status, relevant changes and benefits for the customers/partners and further planning as part of the Docker strategy.

Background

The Docker technology is in general based on the “Open Container Initiative” (OCI) (https://opencontainers.org/) and is the next evolution of virtualization. The concept of virtual machines/OS virtualization, based on hypervisor solutions, is a well-established technology and used in almost every IT department today. With Docker/OCI, the virtualization is moving from the OS level to the application level, as the illustration below shows.



The basic approach is to bundle the service or application, including all dependencies (such as web server components, frameworks, JRE etc.), and a minimum OS in one “Container” and run it on a host Linux server or other container infrastructure. Containers will interact with other containers and multiple instances of one app can easily be spined up on the same host.

This setup comes with several advantages, for example flexibility, scalability, performance, and resources consumption.

Docker in Nexus products

Nexus products are moved towards the Docker technology to benefit from these technical advantages, but also to harmonize the deployment methods and system requirements in the historical products. HAG, PRIME, CM, IDC and Hermod have been delivered based on different technologies, with different system requirements and separate setup routines. With Smart ID, based on Docker, Nexus is aligning that by providing all components in one common way.

Benefits of the aligned, Docker-based delivery method of Smart ID:

- System requirements and prerequisites for on-prem installation are aligned, therefore it is easier for customers to provide the corresponding environment.
- For customers running multiple Smart ID components, it is easier and less effort to install and maintain the components when having them on the same platform.

All major OCI implementations that are available today are native Linux implementations. Therefore, Linux is the major platform for Smart ID.

Benefits of Docker

The container technology has several advantages that customers will benefit from when running Smart ID on-premises:

- **Simplified dependency management**:
  One general principal of a Docker container is isolation. Therefore, all dependencies that are necessary to run applications, (for example, Java runtime, application server etc.), are packaged in the Docker image. Customers will no longer need to care about installing and keeping these dependencies up to date – they will be included in the Smart ID delivery.

- **Less interferences due to isolation**:
  Since everything, (including separate minimum OS, network and application), is encapsulated in the Docker container, there are less unwanted interferences with other applications (for example, background services such as virus scanners, backup services, software update etc.).

- **Saving resources**:
  Even though each Docker container runs its own OS instance, the overall footprint and resource consumption is way less in contrast to the “classical approach” – deploying the applications on bare metal or virtual machines on a hypervisor. So, Docker is saving IT resources.

- **Simplified updates:**
  The fact that all dependencies are encapsulated in the Docker image, in combination with the toolset that Docker/Docker Compose provides, will also simplify the procedure of updating the solution. Updating basically means increasing the version number in the central deployment config file and restarting the services. Downloading, deployment, and restarting of the application will be done automatically in one step.

- **Scalability:**
  One other important advantage for customers using Docker is scalability. Comparing with traditional setups, on bare metal or virtual machines, it is simple to scale up a system with docker. Multiple instances of a Docker image can be spined easily on the same Docker platform without additional configuration efforts.

Container security

Docker, by design, is not more secure and not less secure than any other deployment strategy.
The following Docker design principals of container-based solutions help to ensure security:

- Isolation on software- and network level
- Simplified update process to deploy fixes for vulnerabilities faster and more often

3rd party components
One of the Nexus software development principals is to rely on well-established open-source components and libraries where possible. This is a common practice in the software industry and has several advantages.

Firstly, it saves development time. Secondly, it improves security. These components have been developed, evolved, and maintained over years by dedicated teams with focus on the specific functionality. They are used in many software products all over the world. This means they are pen-tested, reviewed, and proven to be secure many times out in the field.

Relying on 3rd party components and libraries is only secure if they are updated on a regular basis, in order to fix potential vulnerabilities that may be detected in the field. Therefore, checking and updating these libraries and components (for example via OWASP scan) is part of the software development process.

Specifically for 3rd party components, like Tomcat, Java, MQ system etc., Docker has advantages for our customers to keep the system up to date.

When using former legacy deployment methods, maintaining these components was not only a significant additional effort for the IT department, but many customers were reluctant with updating

these components for different reasons, and were running outdated 3rd party software components for a long time.

With Docker, Nexus updates these components with each release (major and minor) automatically. Since the 3rd party components (such as Java) are within the Docker image, customers do not even recognize the update, because no additional effort is required to get the components updated with each release.

Nexus Docker Journey

Starting with Smart ID version 20.06, released during summer 2020, Nexus delivers a Smart ID software package that consists of the components Identity Manager, Self-Service, Messaging, Digital Access and Physical Access.

The current Smart ID package (status December 2021) relies on the most basic and well established OCI tools, which is “Docker” and “Docker Compose”. This means, the Smart ID software package can run on any standard Linux distribution that provides these tools according to the specification on https://doc.nexusgroup.com/.

Nexus has decided by purpose to start with this basic Docker/Docker Compose approach for Smart ID for the following reasons:

- With Docker Compose, the prerequisites to the deployment environment at the customer site are very simple. It is basically a standard Linux distribution and a toolset (Docker/Docker Compose) that comes typically with the default repository of most Linux distributions.

- No specific knowledge in Docker is needed on customer side. Not every IT department has experience with Docker yet. With Docker Compose, Nexus provides a solution that can be operated easily by customers without corresponding Docker expertise.

Transition to Smart ID on Docker

When moving to Smart ID from a previous product the following things are important to understand:

- Smart ID bundles all functionalities of the previous products in one solution. But this does not mean that in Smart ID is a completely different software built from scratch. It rather packages the old products in a new way, in multiple Docker containers, that are orchestrated in one solution.

- The packaging of Smart ID allows to still deploy just a subset of the components, for example deploying just the Smart ID Digital Access containers as a replacement for HAG and skip the

rest. In the installation procedure, the necessary containers can be selected, and there is no need to install the full package.

- Currently, the differences between Smart ID components and the old products are mainly on application server level. This means that, for example, user interfaces, database schemas, runtime and configuration data are mainly kept for now. Corresponding data in the databases will be updated automatically by the corresponding component update script when deploying Smart ID. Details are described on https://doc.nexusgroup.com, as part of the Smart ID install and update guides.

Roadmap

There is a clear trend in IT towards container-based virtualization for cloud solutions, but also for on-premises hosted applications. More and more customers are running professional, highly scalable container infrastructures. Therefore, Nexus is working on supporting corresponding enterprise container platforms (such as Kubernetes or OpenShift) for the Smart ID standard as well.

Also, Nexus will continue with the containerization for the rest of the Smart ID components, to get 100% of the components on Docker in a near future.

Over time, Nexus will also align user interfaces, database schemas and further core functionalities cross-component to improve user experience, reuse functionality and reduce redundancy.

Docker on Windows

Historically, many Nexus customers are operating Nexus software on MS Windows Server platforms. Therefore, it is not a surprise that there is a demand for Smart ID on Windows OS.

Even though Windows-based containers exist, all relevant container solutions heavily rely on Linux environments. Major parts of Docker tools are implemented on Linux-native. As a result, the one and only feasible approach as of today is, to have a Linux virtual machine layer between the Docker environment and Windows OS. For test and development environments, for example Windows 10 clients offers the Hyper-V/WSL2 (Windows Subsystem Linux Version 2) features. Since WSL2 is today available on Windows 10/11 client systems only, it is not recommended for production. Windows 10/11 is not considered as a platform for deployment of server components in customers environment, therefore an official support for Docker Windows 10 cannot be expected right now.

Since there is a demand for Smart ID on Windows, Nexus will keep on investigating for Windows Server based Docker solutions, for example, via WSL2 in future Windows releases, or other upcoming Windows-based Docker technologies.

What others say about Docker

The adoption of container technology has been increasing during the last years. Depending on organization size, type of operation and requirements, the container technology can deliver different benefits, from easier deployments and software updates to orchestration and saving resources. Market research companies are unanimous when stating that container technology is here to stay.

Some of the statements:

- “*By 2023, more than 70% of global organizations will be running more than two containerized applications in production, up from less than 20% in 2019.*”
- “*The analyst firm Gartner predicts that by 2023, 70% of organizations will be running three or more containerized applications in production*”
- “*This year’s survey tells a story of unabated growth in containerization with over 87% of respondents stating that they are running container technologies up from only 55% in 2017. Of those running applications in containers, nearly 90% are running them in production, up from 84% last year and 67% in 2017.*”

Top reports:

- https://www.bmc.com/blogs/state-of-containers/
- https://www.stackrox.com/post/2020/03/6-container-adoption-trends-of-2020/
- https://portworx.com/wp-content/uploads/2019/05/2019-container-adoption-survey.pdf

How to contact us

To provide feedback or to suggest product enhancements, please send an email to contact@nexusgroup.com. If you have questions about the product or this bulletin, do not hesitate to contact us. General information is available at: www.nexusgroup.com.