Docker + Device Authority's KeyScaler Platform

Overview

What is Containerization?

Containerization is a technique used to abstract applications from the environments that they run on. Docker containers wrap up software and its dependencies into a standardized unit for software development that includes everything it needs to run: code, runtime, system tools and libraries.

What is Docker?

Docker is an open source, industry standard platform which can run these images, providing a clean separation of concerns.

Why is Docker important for Device Authority's KeyScaler platform?

KeyScaler™ with Docker support allows deployment of the KeyScaler system into a containerized environment, allowing operations teams to focus on deployment without bothering with application details such as specific KeyScaler versions and configurations. Development teams can work with the available KeyScaler API and EPIC systems while remaining free to choose the tooling that best suits themselves, dramatically reducing IT costs, both capital expense and operational efficiencies, while improving developer productivity.

Benefits of Docker

The abstractions given by the Docker container platform can reduce IT costs by 50% while accelerating your time to market by 3X.

KeyScaler supports any device, any IoT platform, any certificate and any network. A Docker based deployment expands this agnostic approach to technology to the hosting infrastructure, allowing:

- Any programming language
- Any application framework
- Any operating system
- Any infrastructure: bare metal, virtual machine, or public cloud

Docker can also be ran using managed services such as Azure Kubernetes Service (AKS), Amazon Elastic Container Service (Amazon ECS) and Google Kubernetes Engine (GKE)

Developers of solutions are given the freedom to select the best tools, programming languages, and application frameworks for any project.

With the enormous and dynamic scale of the IoT where new devices are continually being provisioned, the ability for infrastructure to respond dynamically to load requirements is critical, and highly available configurations using containerization allows KeyScaler to load balance only the aspects of the system coming under load, seamlessly catering for the real world impact, while minimizing impact on server resource and thus cost.

Docker for Security

As an enterprise solution, Docker provides default configurations that offer greater protection for applications running on top of Docker Engine. The platform establishes strong secure defaults, while still leaving the controls with the admin to change configurations and policies as needed.

Out-of-the-box security defaults include:

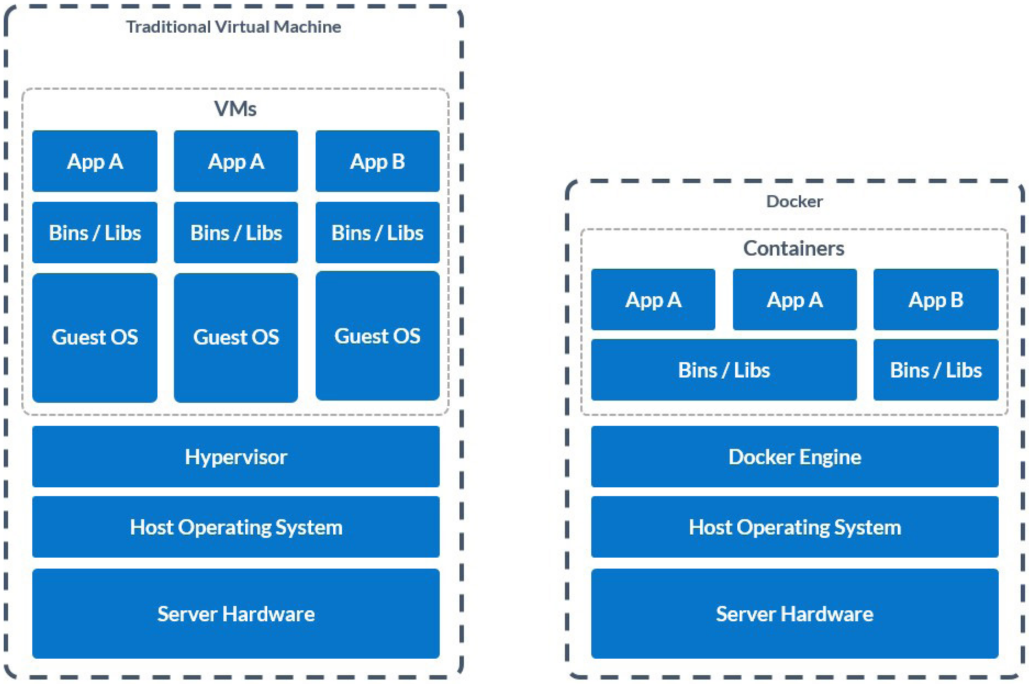
- **System-level mutual TLS authentication and cryptographic node identity** ensure that communications stay inside the cluster, and foreign nodes stay outside, preventing data leakage and attacks.

- **Application-level isolation with authentication/authorization** lets you share resources without sacrificing security because you must explicitly open network communications to an application for any application or person to see or access it.

- **FIPS 140-2 validated cryptographic modules ensure that Docker Engine** - Enterprise meets the standards required by the US Federal government and other regulated industries by delivering on the fundamental confidentiality, integrity and availability objectives of information security.

How does it work?

Traditional virtual machine hosting looks like the left side of the diagram below, with the server hardware at the bottom, the host operating system above that and then a hypervisor layer such as VirtualBox or VMware, which consumes the computing power of the server to provide virtual hardware, which is then consumed by a guest operating system. That guest operating system is where the dependencies for your application and the application itself is installed. This is great for isolation but results in redundant operating systems.



With Docker, the stack is much shorter (as per the right diagram above): we still have the hardware and host operating system on the bottom, but the hypervisor layer is replaced with the Docker engine. The docker engine creates software containers which are smart enough to leverage items of the host operating system to create what looks like a fully isolated guest operating system for the applications you run inside, while being able to leverage shared dependencies across containers.

Using Docker as a foundation for KeyScaler deployments, you get an integrated security framework for delivering safer applications and improving policy automation without sacrificing performance. Docker adds an extra layer of protection that travels with your applications in a secure supply chain that traverses any infrastructure and across both application and device lifecycle.

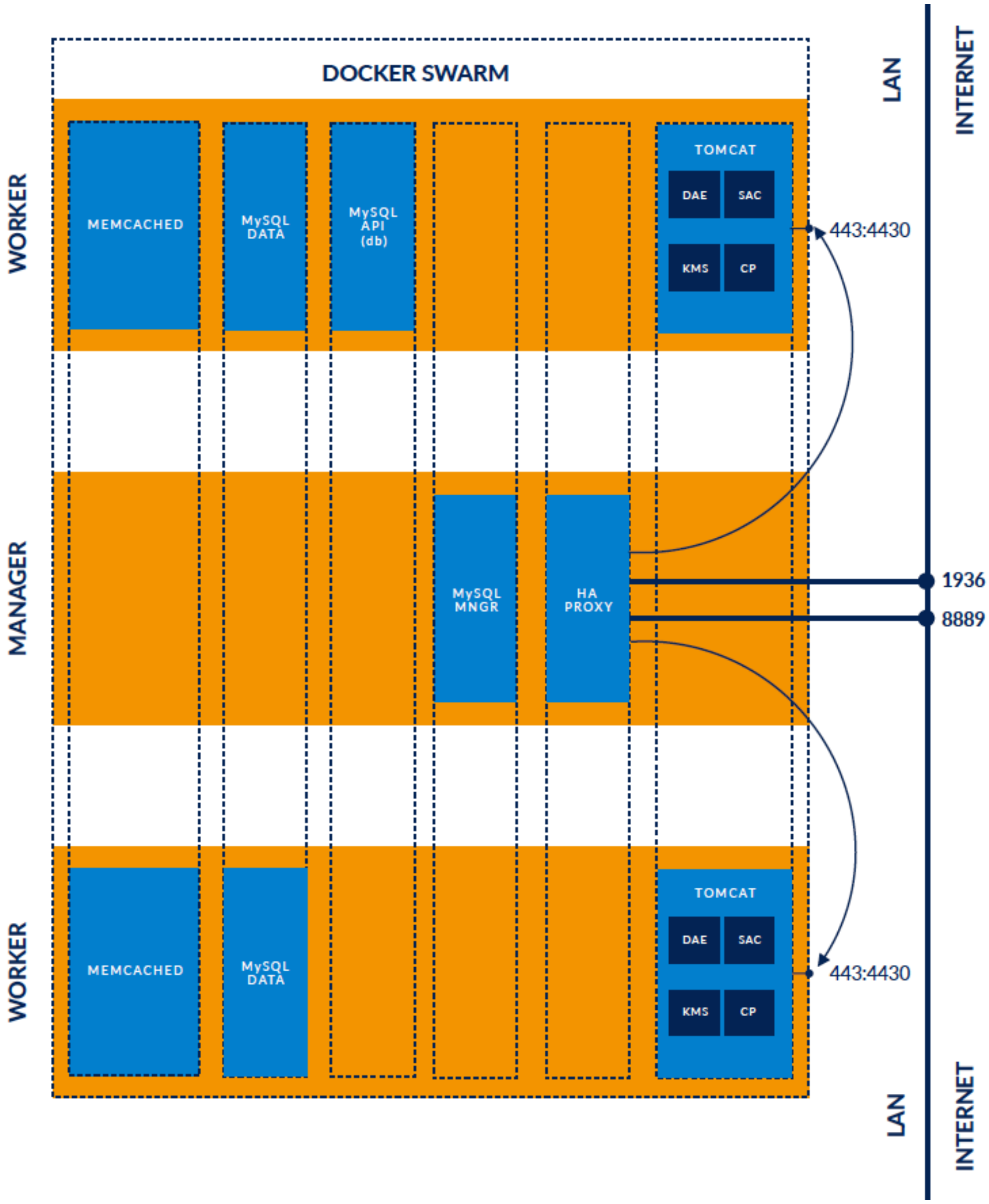
And with a single interface and centrally-managed content, you get a seamless workflow that improves governance and ensures compliance across your whole organization.

KeyScaler on Docker

Device Authority's KeyScaler is a purpose-built device centric IoT IAM platform. KeyScaler provides automated device provisioning, authentication and credential management. KeyScaler addresses the challenges of provisioning devices with unique certificates at IoT scale without human intervention. Secure credential management directly integrates with leading Certificate Authorities to securely automate certificate provisioning, revocation and renewal processes. Most importantly, our solution creates a direct, authenticated, policy-enforced binding between devices and the certificates that are assigned to them.

KeyScaler running on Docker benefits greatly from the speed to deployment and scaling architecture. Installing from supplied images to a fully configured, highly available system is a matter of minutes.

Further Technical Detail



Six Docker services: memcached, MySQL data, MySQL API (db), MySQL manager, HAProxy and tomcat.

Tomcat, memcached and MySQL data services are replicated once in each worker VM; the MySQL API service deploys one container on a random VM; HAProxy and MySQL manager services deploy one container on the manager VM. The tomcat containers each contain one instance of DAE, SAC, KMS and SAC, which communicate

internally to each container (localhost). All services communicate with each other inside the ksdocker_ha network in the Swarm, with the exception of Tomcat which publishes a port on the host itself so that HAProxy is able to differentiate between the two instances of the tomcat service and can load-balance them independently of Docker. The installation is reachable externally by the two ports that HAProxy publishes in the ingress network, one for HAProxy status page and the other for KeyScaler.

Who We Are

Device Authority is a global leader in Identity and Access Management (IAM) for the Internet of Things (IoT); focused on medical / healthcare, industrial and smart connected devices. Our KeyScaler™ platform provides trust for IoT devices and the IoT ecosystem, to address the challenges of securing the Internet of Things. KeyScaler uses breakthrough technology including Dynamic Device Key Generation (DDKG) and PKI Signature+ that delivers unrivalled simplicity and trust to IoT devices. This solution delivers automated device provisioning, authentication, credential management and policy based end-to-end data security/ encryption.

With offices in Fremont, California and Reading, UK, Device Authority partners with the leading IoT ecosystem providers, including AWS, DigiCert, Gemalto, HID Global, Microsoft, nCipher Security, PTC, Sectigo, Thales, Wipro and more.

Keep updated by visiting www.deviceauthority.com, following @DeviceAuthority and subscribing to our BrightTALK channel.

sales@deviceauthority.com
www.deviceauthority.com

DEVICE AUTHORITY™