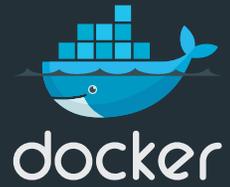


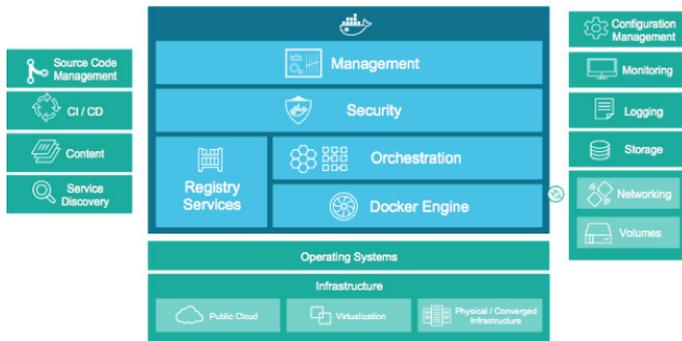
Docker Universal Control Plane

Deploy and Manage On-Premises, Your Dockerized Distributed Applications



As application teams deploy their Dockerized applications into production environments, IT operations teams require the ability to secure and manage applications to ensure reliability, performance and availability against committed customer service levels. Docker enables organizations to build, ship and run distributed applications anywhere. The key elements within “run” includes the ability to deploy, manage and secure the infrastructure and applications at any scale.

Docker Universal Control Plane (UCP) is an enterprise on-premise solution that enables IT operations teams to deploy and manage their Dockerized applications in production, while giving developers the agility and portability they need, all from within the enterprise firewall. A part of the Docker Containers-As-A-Service Platform, an end to end IT managed framework giving developers and IT operations teams agility, portability and control, Universal Control Plane and Trusted Registry comprise our on-premise offering for enterprises that need to host their content and management plan on-premises or in a VPC.



Key Benefits

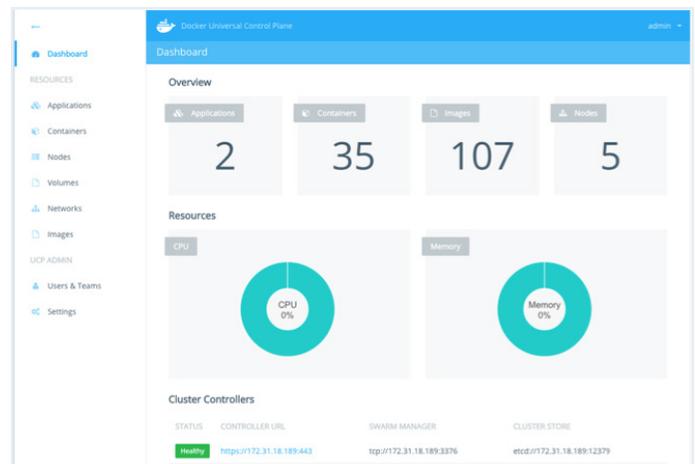
- **User Management:** SSO with DTR, Role-based access control
- **Resource Management:** Management for clusters, app, containers, images, networks, volumes. Monitoring and logging capabilities
- **Security and Compliance:** On-prem deployment, LDAP/AD authentication, audit logs, Out of the box High availability, TLS

Docker Universal Control Plane is a solution designed to deploy, manage and scale Dockerized applications and infrastructure. As a Docker native solution, full support for the Docker API ensures seamless transition of your app from development to test to production - no code changes required, support for the

Docker toolset and compatibility with the Docker ecosystem. From infrastructure clustering and container scheduling with the embedded Docker Swarm to multi-container application definition with Docker Compose and image management with Trusted Registry. Universal Control Plane simplifies the process of managing infrastructure, deploying, managing applications and monitoring their activity, with a mix of graphical dashboards and Docker command line driven user interface.

Enterprise grade user access is controlled with integrations with your existing LDAP/AD, ability to create teams and orgs and granular RBAC policies to UCP managed objects like containers. The integration of Docker Trusted Registry and Docker Content Trust allows enterprises to ensure a secure content lifecycle with enforced image signing and verification. Universal Control Plane is the only tool on the market that comes with Docker Content Trust directly out of the box. With these integrations Universal Control Plane gives enterprise IT security teams the necessary control over what content can be used and deployed in their environment.

Universal Control Plane can be deployed to any private infrastructure and public cloud including Microsoft Azure, Digital Ocean, Amazon Web Services, and SoftLayer. Once deployed, UCP uses Docker Swarm to create and manage clusters, tested up to 1,000 nodes deployed in any private data center or public cloud provider.



Feature Note: This is the main admin dashboard to Docker Universal Control Plane. The dashboard displays information about the applications, containers, images and nodes running in your cluster. It also provides insight into resources being used, as well as information about your Swarm master, backups and node clusters. Also, on the left hand side you can see all of the other objects that you can manage from UCP.

Docker Native Deployment and Management

Docker Universal Control Plane supports the Docker API allowing for a seamless experience with Docker CLI, Compose, Swarm and Trusted Registry. For example, you can integrate all of your repos within Docker Trusted Registry, pull them into Universal Control Plane and then deploy into your Swarm cluster with just a few clicks within the UI. With a simple “docker-compose up,” IT teams can deploy Docker Compose-based applications to the Swarm cluster directly from CLI and Universal Control Plane will discover and manage the applications.

```

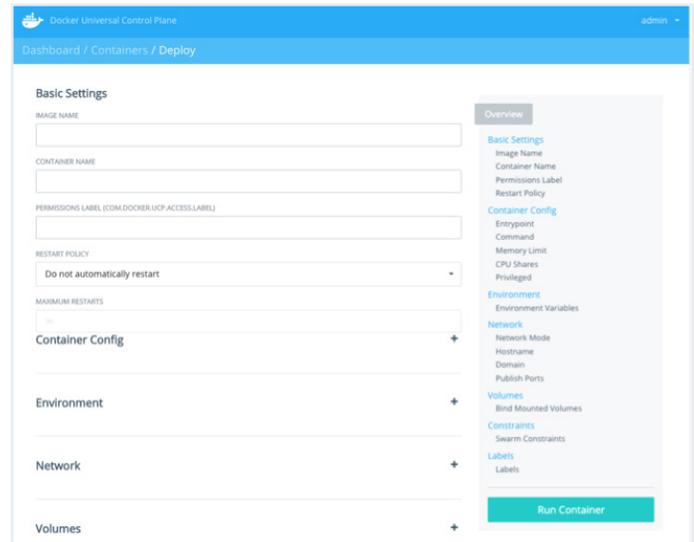
root@docker:~# docker ps
CONTAINER ID   IMAGE                                COMMAND                  CREATED          STATUS          PORTS          NAMES
30a225e4e8b0   nginx:alpine                               nginx                    7 minutes ago   Up 7 minutes   80/tcp         btan1

root@docker:~# docker inspect

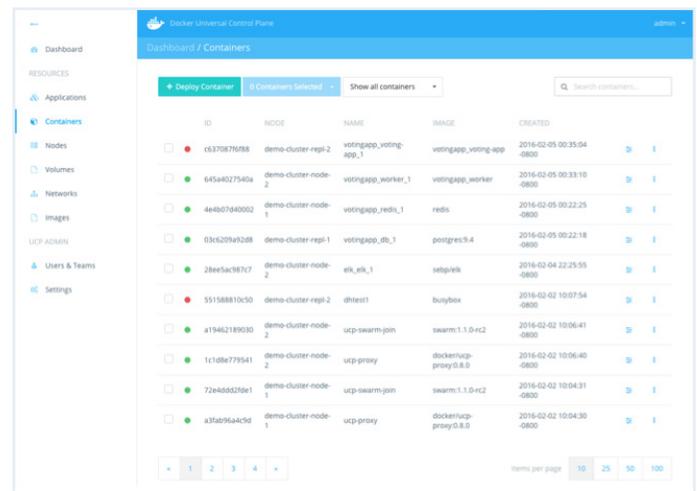
```

By pointing your Docker host to your UCP instance you are able to perform all the normal operations that you are used to for a completely native Docker experience i.e Docker-ps, Docker inspect, view Docker images etc. Since UCP i supports the Docker API, you get the benefit of the Docker ecosystem and choice of partner solution to integrate into your environment. Universal Control Plane supports a high availability configuration and TLS out of the box providing you added security and reliability of your management environment.

Universal Control Plane works natively with Docker Compose defined applications. No changes to the application code are required to go from building your application locally with Compose to moving through QA and then shipping to production. Deploy applications or containers into the UCP managed node cluster with Compose or launch containers on the fly using the Docker CLI. You can specify the image, restart policies, configurations like entry point, commands, reservations information, environment variables specify default networking setting to expose ports, and use scheduling constraints.



Feature Note: This is the UI for deploying a Docker container into a Swarm cluster. After setting your specifications for your container you simply click the green “Run Container” button to deploy to your cluster.

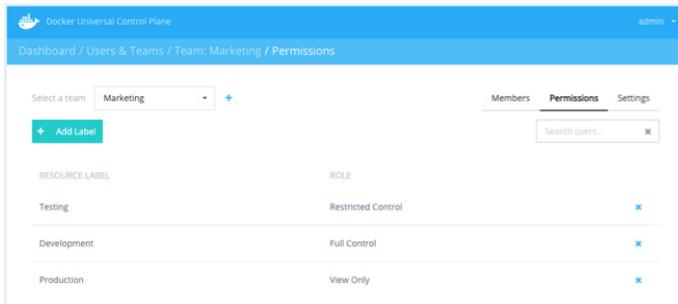


Feature Note: In this screenshot you can see that when you click into “Containers” from the main drop-down menu you have the ability to search for containers. You also have the ability to search for images, applications or nodes once you click into each operation type. The tool allows IT teams to drill into a cluster and search by ID, image and name. If you want to inspect container to correlate to CLI, you can click into the image in “details” to see the status, configs, which imaged was use, add resource limits, look at volumes use, ports and the process table.

Built in Security and Control

Security is top of mind for many enterprise IT operations teams. Ops teams need to be able to secure and manage their environment to meet compliance requirements. The ability for Docker UCP to integrate with existing tools like LDAP/AD for user authentication and its integration with Docker Trusted Registry, enables enterprises to build, ship and run their applications securely. Within Docker UCP, you can set up granular role-based access controls for your container resources or you can do centralized authentication by linking UCP with your LDAP or Active Directory. For role-based access control, within UCP you can assign user accounts to teams and provide pre-defined sets of permissions (“roles”) to container resources. This granularity allows you to control who can access certain containers, which dramatically reduces organizational risk within enterprises.

The integration with Docker Trusted Registry also means that you can use Docker Content Trust, to sign your images and verify that only trusted content is deployed into your environment, providing a secure content lifecycle. This means that you can pull images from Docker Trusted Registry into Docker UCP and not have to worry about their security.



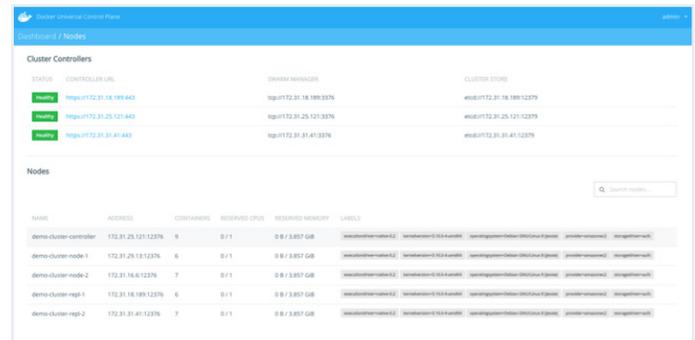
Feature Note: Within UCP you have the ability to assign users to specific teams, and then assign specific roles to that team (e.g. “Full Control, “View Only”) via labels to specific container resources. You can also integrate with your existing LDAP/AD for authentication. This makes it very easy to automatically assign the appropriate levels of access to teams within your org.

Monitor and Manage at Any Scale

Having visibility into your infrastructure and applications is crucial. With Docker UCP’s dashboard you can see exactly what’s running in your environment, and can even be alerted of any odd behavior that may be taking place. View and monitor all of your deployed Docker Compose applications or running container from the dashboard. From there, you can dive into specific applications or containers to debug them, check logs and view real time stats. Simply scale up or down applications and services from the UI or command line interface as needed.



Feature Note: Within Docker UCP, you have the ability to monitor stats like the CPU and Memory used for the deployed applications. As well as drill down into the individual containers that make up the application.



The screenshot shows the 'Nodes' page. It has two main sections: 'Cluster Controllers' and 'Nodes'. The 'Cluster Controllers' section shows three controllers with their status, URLs, and IP addresses. The 'Nodes' section shows a table of nodes with columns for Name, Address, Containers, Reserved CPU, Reserved Memory, and Labels.

NAME	ADDRESS	CONTAINERS	RESERVED CPU	RESERVED MEMORY	LABELS
demo-cluster-controller	172.31.25.12112276	9	0/1	0.8 / 3.857 GB	demo-cluster-controller-01, demo-cluster-controller-02, demo-cluster-controller-03, demo-cluster-controller-04, demo-cluster-controller-05, demo-cluster-controller-06, demo-cluster-controller-07, demo-cluster-controller-08, demo-cluster-controller-09
demo-cluster-node-1	172.31.29.1312276	6	0/1	0.8 / 3.857 GB	demo-cluster-node-01, demo-cluster-node-02, demo-cluster-node-03, demo-cluster-node-04, demo-cluster-node-05, demo-cluster-node-06
demo-cluster-node-2	172.31.16.612276	7	0/1	0.8 / 3.857 GB	demo-cluster-node-01, demo-cluster-node-02, demo-cluster-node-03, demo-cluster-node-04, demo-cluster-node-05, demo-cluster-node-06, demo-cluster-node-07
demo-cluster-ntp-1	172.31.18.18912276	6	0/1	0.8 / 3.857 GB	demo-cluster-ntp-01, demo-cluster-ntp-02, demo-cluster-ntp-03, demo-cluster-ntp-04, demo-cluster-ntp-05, demo-cluster-ntp-06
demo-cluster-ntp-2	172.31.31.4112276	7	0/1	0.8 / 3.857 GB	demo-cluster-ntp-01, demo-cluster-ntp-02, demo-cluster-ntp-03, demo-cluster-ntp-04, demo-cluster-ntp-05, demo-cluster-ntp-06, demo-cluster-ntp-07

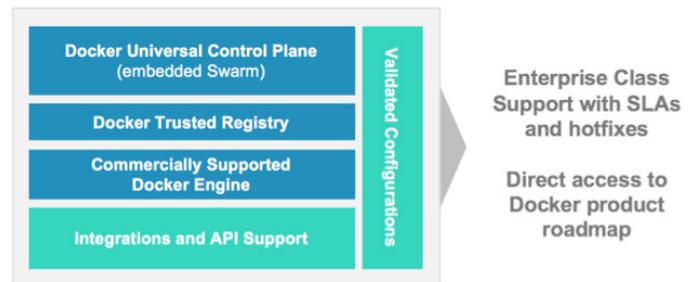
Feature Note: High availability for UCP controller and Swarm is another benefit of Docker UCP. You can designate Swarm “master” nodes and “replica nodes” within UCP. If a Master node goes down, it automatically fails over to a replica node and makes it the new master. This allows for high availability of your master nodes. In the screenshot above you can see that there is a master node, two replicas and two slave nodes. The scheduler, security settings and accounts are all preserved as a result of this.

Name	Docker Universal Control Plane	Docker Trusted Registry	Commercial Support
Description	Enterprise-grade on-premises service for managing and deploying dockerized distributed applications in any on-premises or virtual cloud environments. It's built in security features like LDAP/AD integration and role-based access control (RBAC) allow IT teams to be in compliance with industry security regulations.	Enterprise-ready on-premises service for storing, distributing and securing images. The registry gives enterprises the ability to ensure secure collaboration between developers and sysadmins to build, ship and run applications.	Subscribers receive commercial support for their Docker engines. We call the "CS" engine. The CS Engine is made up of the same Core Engine as the open source engine, but has added support from the Docker team as well.
Features	<ul style="list-style-type: none"> • GUI management for apps, containers, nodes networks, images and volumes • Monitoring and logging of UCP users and events • Out of the box HA • LDAP/AD integration • Role-based-access control for teams. • SSO and push/pull images for Docker Trusted registry • Out of the box TLS • Docker native stack with Swarm, Compose, CS engine and DTR • Full Docker API compatible 	<ul style="list-style-type: none"> • Web UI for administrators and users LDAP/AD integration • Role-based access control • Docker Content Trust image signing and verification • Garbage collection for saving memory space • User audit logs 	<ul style="list-style-type: none"> • Direct support contact • Bug fixes, patches • Hot fixes, patches • Predictable cadence (Docker owns Docker Roadmap) • Longer supported versions • Defect fixes • Validations for configurations

The Docker Datacenter Subscription

The Docker Datacenter subscription enables enterprises to leverage a platform built by Docker, for Docker. The Docker native tools are integrated to create an on premises CaaS platform, allowing organizations to save time and seamlessly take applications built in dev to production.

Docker Datacenter is an integrated solution including open source software, commercial software, the integrations between them, full Docker API support, validated configurations and commercial support for your Docker Datacenter environment. A pluggable architecture allows flexibility in compute, networking and storage providers used in your CaaS infrastructure without disrupting the application code. Leverage existing technology investments with Docker Datacenter. The open APIs allow your Docker Datacenter CaaS to easily integrate into your existing systems like LDAP/AD, monitoring, logging and more.



Support From the Source

With a Docker Datacenter subscription, enterprises receive technical support directly from Docker engineering, not an open source forum. This team are the primary contributors and maintainers of the upstream Docker projects. With Datacenter Subscription, customers receive support that is:

Responsive - The subscription comes with a direct support contact giving subscribers access to private communications channels with the support team at dedicated SLAs (see below). The Docker support team will also provide fixes for any breakages or bugs found so that enterprises can rest assured that their environment achieves peak uptime.

Secure - The Docker team validates and tests will address any security vulnerabilities found within IT environments and issue necessary patches, hot fixes as well as validation for configurations.

Stable - The Docker team provides: a predictable release cadence as they own the Docker product roadmap, longer supported versions, defect fixes, validations for operating systems and full Docker API support.

Get Started Today

The Docker Datacenter subscription is available with two different support coverage windows. You can choose from Business Day Support which provides 12 hour cover during the business week or Business Critical Support for 24 hours by 7 days a week and 365 days a year.



The Docker Datacenter subscription provides a fully supported end-to-end CaaS platform for your on-premises or virtual private cloud, getting you access to the world-class expertise of the Docker support and product teams that enterprises rely on.

Interested in learning more about the Docker Datacenter subscription or in signing up for a free 30-day trial? Contact our Sales team at www.docker.com/contact or visit our website <https://www.docker.com/pricing>.

www.docker.com

