

Technical Disclosure Commons

Defensive Publications Series

November 08, 2018

UPGRADING A MULTI-HOST PLATFORM-AS-A-SERVICE INFRASTRUCTURE END-TO-END USING CONTAINER IMAGES HOSTED IN THE CLOUD

Prabhakar Palanivel

Follow this and additional works at: https://www.tdcommons.org/dpubs_series

Recommended Citation

Palanivel, Prabhakar, "UPGRADING A MULTI-HOST PLATFORM-AS-A-SERVICE INFRASTRUCTURE END-TO-END USING CONTAINER IMAGES HOSTED IN THE CLOUD", Technical Disclosure Commons, (November 08, 2018)
https://www.tdcommons.org/dpubs_series/1633



This work is licensed under a [Creative Commons Attribution 4.0 License](https://creativecommons.org/licenses/by/4.0/).

This Article is brought to you for free and open access by Technical Disclosure Commons. It has been accepted for inclusion in Defensive Publications Series by an authorized administrator of Technical Disclosure Commons.

UPGRADING A MULTI-HOST PLATFORM-AS-A-SERVICE INFRASTRUCTURE END-TO-END USING CONTAINER IMAGES HOSTED IN THE CLOUD

AUTHORS:
Prabhakar Palanivel

ABSTRACT

Techniques are provided for updating all the components of a Platform-as-a-Service (“PaaS”) infrastructure, including the host kernel, the PaaS infrastructure, host daemons, and the utilities. The update may occur using the container images uploaded into the cloud container registry.

DETAILED DESCRIPTION

A Platform-as-a-Service (“PaaS”) infrastructure consists of multiple nodes, each of which has various software components which need to be updated periodically. The components include a host kernel, PaaS software and its associated infrastructure (e.g., distributed key-value store, Domain Name System (DNS) services, etc.), host software components (e.g., command-line-utilities, host daemons, etc.), and infrastructure services running inside the PaaS to support hosting the actual applications (e.g., catalog servers, platform User Interface (UI) services, etc.).

The administrator would not want to access the individual nodes or to update the components manually. The complete infrastructure should be updated remotely, for instance, by invoking a Representational State Transfer (REST) Application Programming Interface (API) which is handled by a service running inside the PaaS infrastructure. Considering that the software components evolve continuously, it should be possible to upgrade the upgrade-infrastructure as well before processing an actual software upgrade.

Techniques are described herein to update all the PaaS components using the container images hosted in the cloud registry, without any manual intervention by the administrator, while accounting for the intricacies of updating the aforementioned components. The update orchestrator which drives the whole update process may be yet another service running inside the PaaS, so that it can be updated in the same way the rest of the infrastructure services are updated.

These techniques enable updating the complete PaaS infrastructure components using a set of container images distributed through the container registries hosted on the cloud. Updating the infrastructure services running inside the PaaS is a well-known process whereby a user configures these services to use certain container images and the images are automatically downloaded and used for running these services. The techniques described herein to extend this approach and use the container images for updating the host components including the kernel, system daemons, PaaS infrastructure components, and command line utilities that run on the host.

In the following description, the terms “node” and “host” are used interchangeably and refer to the individual server in the PaaS cluster which is essentially a cluster of servers working together to provide PaaS functionality.

Figure 1 below illustrates a workflow for host updates.

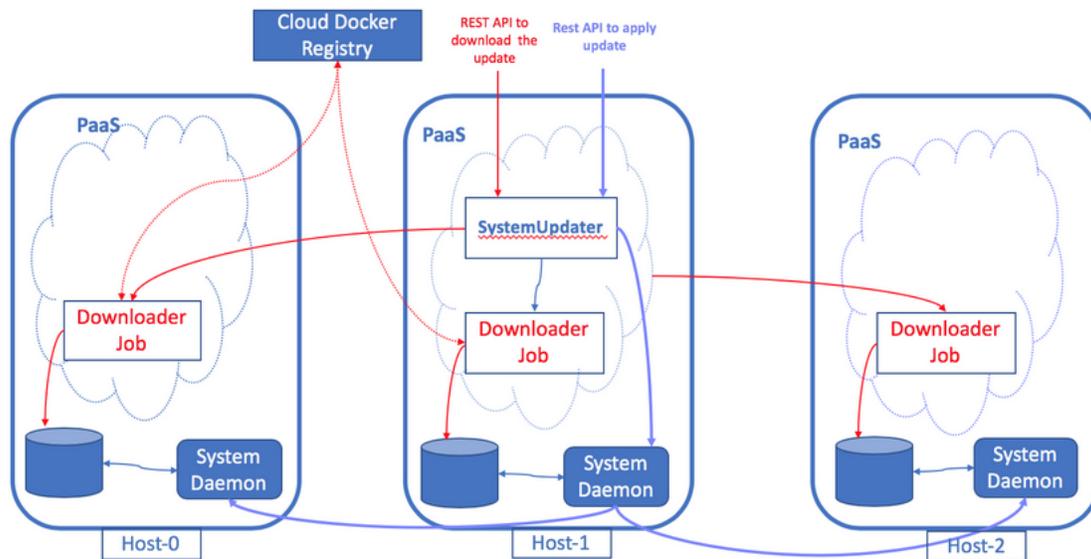


Figure 1

At the download phase of the host updates, the host update packages are packaged as a container image and this image is posted into the cloud image registry along with the rest of the images relevant to the specific software version. The administrator initiates the update process to upgrade the PaaS infrastructure to a specific version. As part of processing this request, downloading of the host updates is triggered.

The System-updater service (shown in Figure 1) is the orchestrator which handles the whole update process. In each host in the PaaS cluster, the System-updater launches a

run-to-completion container (referred to as Downloader Job in Figure 1) using this container image. The Downloader Job has appropriate locations of the host filesystem mounted (“bind-mounted”) into its filesystem.

Using these mounts, the Downloader Job copies the host-update packages into the individual hosts at a predefined locations in the host filesystem. In addition to copying the update packages, an updater-daemon is inserted into each host using the mounts mentioned above. The Downloader Job also starts the updater-daemon using the operating system specific mechanism. The updater-daemon waits for notifications from the System-updater service by watching a key in the distributed key-value database.

At the install phase of the host updates, the System-updater service triggers the host-updates by notifying the updater-daemons running in the hosts, one host at a time. Alternatively, the System-updater can notify one host and the hosts can be updated in a daisy chained manner. The updater-daemon, upon receiving the notification, starts deploying the host updates. Once the updates have been deployed, the updater-daemon notifies the System-updater service using the same distributed key-value database. The System-updater service then proceeds with updating the next host in the cluster.

All the components used for upgrade may themselves be upgraded during the upgrade process. When performing the host updates, the PaaS infrastructure may not be relied upon, as the infrastructure may itself be updated as part of the process.

In summary, techniques are provided for updating all the components of a PaaS infrastructure, including the host kernel, the PaaS infrastructure, host daemons, and the utilities. The update may occur using the container images uploaded into the cloud container registry.