MOPV031

THE DEPLOYMENT TECHNOLOGY OF EPICS APPLICATION SOFTWARE BASED ON DOCKER

R. Wang†, Y.H. Guo, B.J. Wang, N. Xie, IMP, LAN Zhou 730000, P.R. China

ICALEPCS 2021

- EPICS+StreamDevice

StreamDevice, as a gene ral-purpose string interface d evice's Epics driver, has been widely used in the control of devices with network and seri al ports in CAFe equipment.

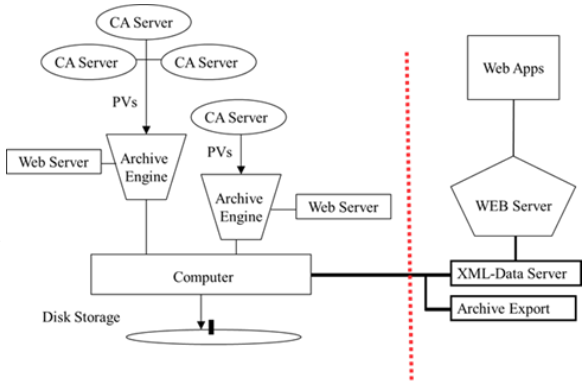

Fig.1 StreamDevice used for webpages

- Docker

Docker, a lightweight application container deploy-ment framework, can package, publish, and run any application.

Docker is considered an Internet container and will be the future standard for PaaS

- The security of Docker container

a) Images security restrictions

b) Container resource security mechanism

c) Container network security mechanism

- Performance

a) Image testing

b) Mirror access authentication test

c) Resource limit testing

d) Network communication testing

THE DEPLOYMENT TECHNOLOGY OF EPICS APPLICATION SOFTWARE BASED ON DOCKER

R. Wang†, Y.H. Guo, B.J. Wang, N. Xie, IMP, LAN Zhou 730000, P.R. China

- EPICS+StreamDevice

CAFe equipment, the CiADS superconducting linear accelerator prototype, was built in 2018 to validate the superconducting linear acc elerator for CiADS with 10 mA continuous beam current. The equipment consists of the ion source, low-energy transmission section, RFQ, medium-energy transmission section, superconducting linear accelerator, high-energy transmission section, and beam terminal collector. The equipment layout is shown in figure. The overall parameters of the equipment include beam intensity of 10mA, beam energy of 25-40MeV, RF frequency of 162.5MHz, and temperature of 4.5k.

StreamDevice can analyze web pages by regular expres-sions, and read this important information in real time in the web control interfa ce to learn whether the archiving system is running. After setting PV, CA Server performs data archiving by Archive Engine. And these data should be submitted by Achieve Export to browse. Finally, the information is displayed in the human-machine interface on Web Apps

An asynchronous drive module (ASYN) interface was integrated with Strea mDevice, which supports serial ports (RS485, RS232), IEEE-488 (GPIB or HP-IB), and Ethernet interfaces. It can realize the communication between serial por ts and Gaussian power supply. The communication rules are specified by writing protocol files, and PV information is defined by DB files

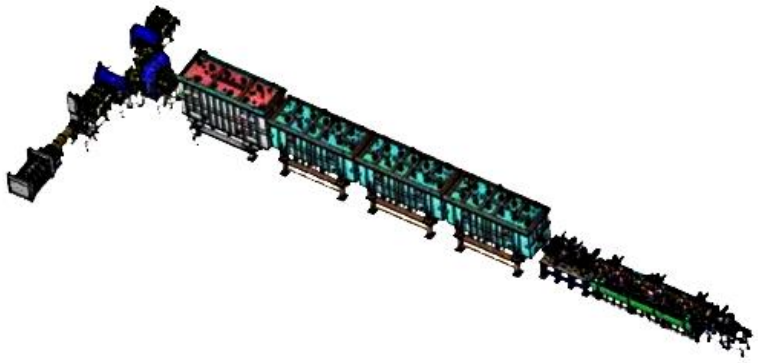

Fig.2 Layout of CAFe superconducting proton linear accelerator

THE DEPLOYMENT TECHNOLOGY OF EPICS APPLICATION SOFTWARE BASED ON DOCKER

R. Wang†, Y.H. Guo, B.J. Wang, N. Xie, IMP, LAN Zhou 730000, P.R. China

- Docker

Docker, a lightweight application container deployment framework, can package, publish, and run any application. Application migratio n can be realized by firstly packaging EPICS+StreamDevice with Docker, secondly building images and sending them to the remote registry (docker hub), finally pulling and running images on deployed servers..

Before using Docker to package EPICS + StreamDevice, if the server is updated or the server is abnormally collapsed, these applica tions need to be redeployed. The deployment process is complex an d may encounter un-known problems, which takes a lot of manpowe r and time. Packaging all effective loads through Docker enables con sensus migration between almost any server, which greatly simplifie s deployment and maintenance. The official Ubuntu 18.04 is used as the basic image. The container should be constructed from the image, which installs EPICS + StreamDevice in the container. After all, the container will be committed as a new image.

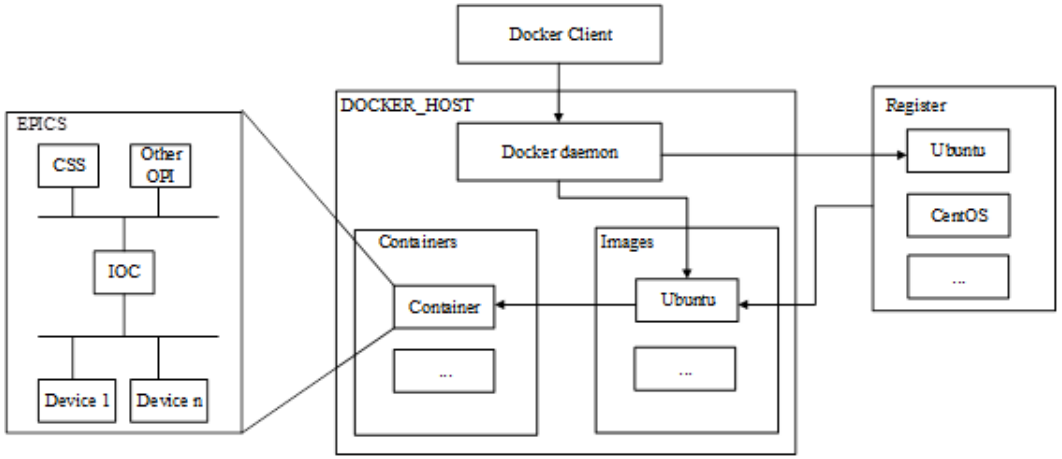

Fig.3 The overall framework of the system

Application migration can be realized by firstly packaging EPICS+StreamDevice with Docker, secondly building images and sending t hem to the remote registry (docker hub), finally pulling and running images on deployed servers.

THE DEPLOYMENT TECHNOLOGY OF EPICS APPLICATION SOFTWARE BASED ON DOCKER

R. Wang†, Y.H. Guo, B.J. Wang, N. Xie, IMP, LAN Zhou 730000, P.R. China

- The security of Docker container

1.Images security restrictions

The official image registry allows all Docker hub users to visit. All the application projects on it are open source.

The private image stowage was built through Aliyun to increase the authentication mechanism when attempting to pull the image. This method can limit the pull permissions, and ensure the security of the image.

2.Container resource security mechanism

Since the Docker container shares the operating system kernel with the host, there is a risk that the container is controlled by the attacke r to obtain the access rights of the host file. Or the attacker obtains the root permission by illegal means to control the host and other contain ers on the host. It will result in the escape of the container, or even that the Docker container exhausts the host to make the host or other cont ainers pause or die.

3.Container network security mechanism

Since the Docker container shares the operating system kernel with the host, there is a risk that the container is controlled by the attacke r to obtain the access rights of the host file. Or the attacker obtains the root permission by illegal means to control the host and other contain ers on the host. It will result in the escape of the container, or even that the Docker container exhausts the host to make the host or other cont ainers pause or die.

It is necessary to prohibit communication between containers, which can be achieved by setting the parameter dockerd-icc.

THE DEPLOYMENT TECHNOLOGY OF EPICS APPLICATION SOFTWARE BASED ON DOCKER

R. Wang†, Y.H. Guo, B.J. Wang, N. Xie, IMP, LAN Zhou 730000, P.R. China

- Performance

1.Images test

Official image of Ubuntu 18.04.
EPICS is installed and then Asyn and StreamDevice are deployed.

2.Mirror access authentication test

First Aliyun account should be logged in to establish an image stow age and create a namespace. Then the image Tag that needs to be uploade d should be changed on the host running docker.

3.Resource limit testing

Cgroups can limit resource items such as CPU, memory, and disk I/ O speed of the Docker container to avoid a single container running out o f hardware resources on the host.

4.Resource limit testing

The EPICS + StreamDevice container used in this paper provides se rvices separately, so it should be forbidden to communicate with other co ntainers running on the host computer. In the test environment, the IP of t he EPICS + StreamDevice container is 172.17.0.2, and that of the Ubunt u container is 172.17.0.3. It is necessary to set dockerd-icc = false to pro hibit communication between them

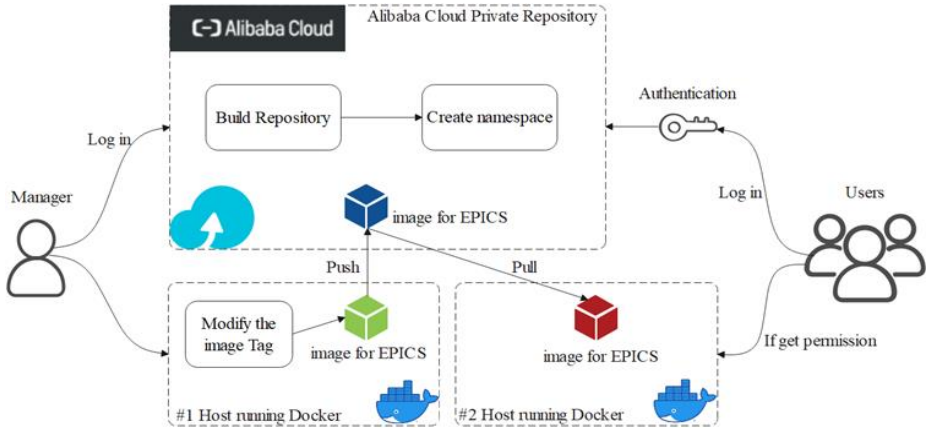

Fig.4 Aliyun private repository image access authentication

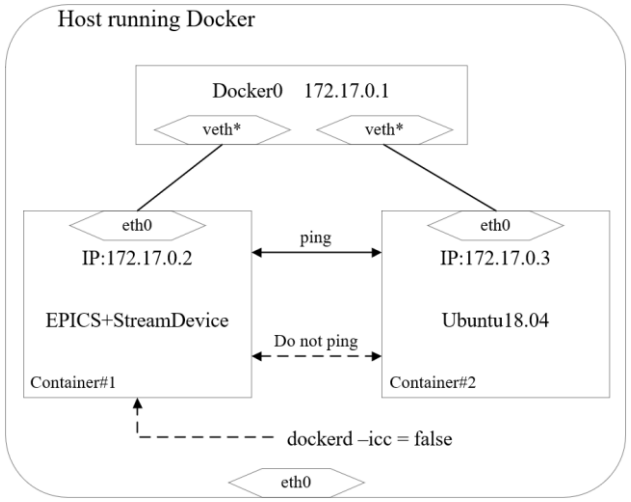

Fig.5 Docker internal network structure