Access Control Model for Container based Virtual Environments

Abstract

With rapid development and adoption of virtualization technology, security concerns have become more prominent. Access control is the focal point when it comes to security. Since, it determines if a user can access a system and perform the action they intend to. Containers provide an all or nothing access control mechanism. Where if a host machine user has privileged access then they can access the containers as root user, with all privileges and perform any desired action. All unprivileged users on the host machine are denied access to the container environment. This research focuses on the concept of access control in container environment. It is geared more towards Docker container environment since it is the most widely adopted containerization technology. The study also analyses existing container authorization plugins to determine how they make access decisions. Additionally, this study led to the design and development of an effective access control plugin that makes access decisions to containers based on container users.

References

Index Terms

Computer Science

Information Sciences

Keywords

Virtualization, Container, Docker, Access Control, Authorization