VMware vSphere Integrated Containers Engine Security

vSphere Integrated Containers Engine 0.8

vmware

Table of Contents

vSphere Integrated Containers Engine Security

vSphere Integrated Containers Engine Security provides security-related information about VMware vSphere® Integrated Containers™ Engine.

For the full vSphere Integrated Containers Engine documentation set, go to https://vmware.github.io/vic-product/#getting-started.

Product version: **0.8**

This document was last updated on **2017-02-23**.

Intended Audience

This information is intended for VMware vSphere® administrators who deploy vSphere Integrated Containers Engine in a secure environment.

For an introduction to vSphere Integrated Containers and descriptions of its main components, see Overview of vSphere Integrated Containers Engine for vSphere Administrators in *vSphere Integrated Containers Engine Installation*.

Send Documentation Feedback

Help us to improve the vSphere Integrated Containers documentation.

- Send doc feedback to VMware by email
- Submit an issue in Github
- Send us a message on https://vmwarecode.slack.com/messages/vic-doc

---

VMware, Inc. 3401 Hillview Ave. Palo Alto, CA94304

www.vmware.com

vSphere Integrated Containers Engine Security Reference

Use the Security Reference to learn about the security features of vSphere Integrated Containers Engine.

Network Security

VMware highly recommends using a secure management network for vSphere Integrated Containers Engine. The container VMs communicate with the endpoint VM over the management network when an interactive shell is required. While the communication is encrypted, the public keys are not validated, which leaves scope for man-in-the-middle attacks. This connection is only used for the interactive console when enabled (stdin/out/err), and not for any other purpose.

External Interfaces, Ports, and Services

The following ports must be open on the VCH appliance.

Endpoint VM

Client interface:

- 2375 insecure port for Docker API access if deployed with `--no-tls`
- 2376 for TLS secured port for Docker API access
- 22 SSH when enabled with `vic-machine debug`
- 2378 VIC admin server health and log access (HTTPS)
- 6060 pprof debug data when enabled with --debug levels

Management interface:

- 2377 incoming connections from container VMs
- 443 outgoing connections established to vSphere target
- 443 outgoing connections established to ESX hosts

Bridge interface:

- 53 DNS server for container name resolution

Public interface:

- any port not listed as used elsewhere can be forwarded to a container VM

Container VM

- 6060 pprof debug data when enabled with --debug levels
- vSphere Integrated Containers Engine does not use ports when not configured for debug

Service Accounts and Privileges

vSphere Integrated Containers Engine does not create service accounts and does not assign privileges. The `--ops-user` and `--ops-password` options allow a VCH to operate with less-privileged credentials than those that are required for deploying a new VCH. For information about the `--ops-user` option and the permissions that it requires, see the descriptions of `--ops-user` in

VCH Deployment Options and Advanced Examples of Deploying a VCH, and the section Use Different User Accounts for VCH Deployment and Operation in *vSphere Integrated Containers Engine Installation*.

Apply Security Updates and Patches

Download a new version of vSphere Integrated Containers Engine and upgrade your existing VCHs.

Security Related Log Messages

Security-related information for vSphere Integrated Containers Engine appears in `docker-personality.log` and `vicadmin.log`, that you can access from the VCH Admin portal for a VCH.

Sensitive Data

The VMX file of the VCH endpoint VM stores vSphere Integrated Containers Engine configuration information, which allows most of the configuration to be read-only by the guest. The container VMs might hold sensitive application data, such as environment variables for processes, command arguments, and so on.

Send Documentation Feedback

Help us to improve the vSphere Integrated Containers documentation.

- Send doc feedback to VMware by email
- Submit an issue in Github
- Send us a message on https://vmwarecode.slack.com/messages/vic-doc