VMware vSphere Integrated Containers Engine for vSphere Administrators

vSphere Integrated Containers Engine 0.7.0

vmware

Table of Contents

Introduction 0

vSphere Integrated Containers Engine Architecture 1

Interoperability of vSphere Integrated Containers Engine with Other VMware Software 2

Virtual Container Host Administration 3

- Obtain vic-machine Version Information 3.1
- Common `vic-machine` Options 3.2
- List Virtual Container Hosts and Obtain Their IDs 3.3
- Obtain Information About a Virtual Container Host 3.4
- Delete a Virtual Container Host 3.5
  - Virtual Container Host Delete Options 3.5.1
- Upgrade a Virtual Container Host 3.6
  - Virtual Container Host Upgrade Options 3.6.1
- Authorize SSH Access to the Virtual Container Host Endpoint VM 3.7
  - Virtual Container Host Debug Options 3.7.1

Find Virtual Container Host Information in the vSphere Web Client 4

Find Container Information in the vSphere Web Client 5

Upgrade the vSphere Integrated Containers Engine Plug-In 6

Access the Administration Portal for a Virtual Container Host 7

- Virtual Container Host Status Reference 7.1

Troubleshooting vSphere Integrated Containers Engine Administration 8

- Access vSphere Integrated Containers Engine Log Bundles 8.1
- Running `vic-machine ls` on an ESXi Host Fails with an Error 8.2
- Deleting or Inspecting a VCH Fails with a Resource Pool Error 8.3
- Connections Fail with Certificate Errors when Using Full TLS Authentication with Trusted Certificates 8.4

vSphere Integrated Containers Engine for vSphere Administrators

vSphere Integrated Containers Engine for vSphere Administrators provides information about how to use VMware vSphere® Integrated Containers™ Engine as a vSphere Administrator.

Product version: 0.7.0

NOTE This book is a work in progress.

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

Intended Audience

This information is intended for vSphere® Administrators who must manage a vSphere Integrated Containers Engine implementation in their vSphere environment. The information is written for experienced vSphere administrators who are familiar with virtual machine technology and datacenter operations. Knowledge of container technology and Docker is assumed.

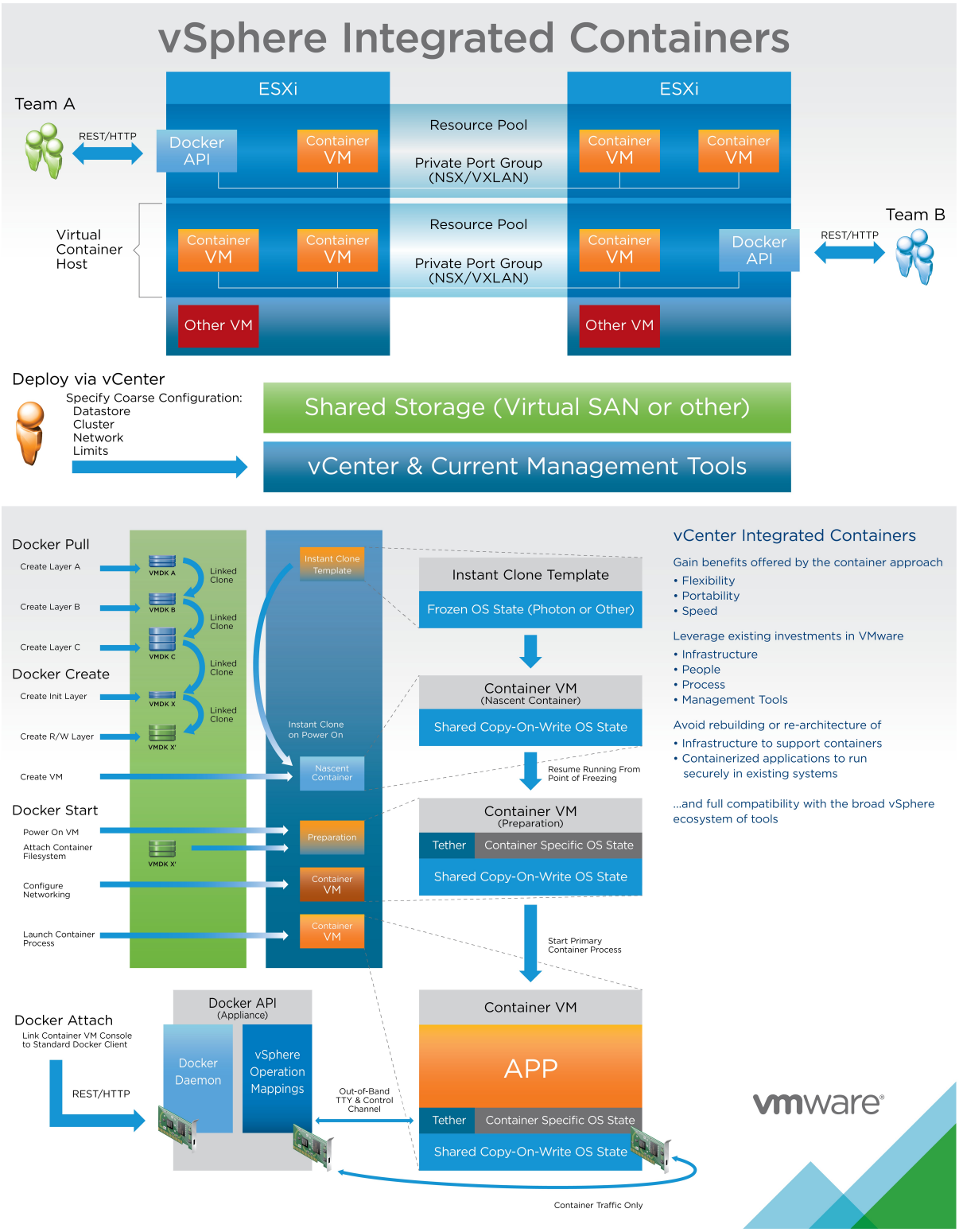
VMware, Inc. 3401 Hillview Ave. Palo Alto, CA94304

www.vmware.com

vSphere Integrated Containers Engine Architecture

vSphere Integrated Containers Engine exists in a vSphere environment, allowing you to manage containers like virtual machines. The architecture consists of these components:

- vCenter Server management tools: Monitor and manage container virtual machines alongside regular virtual machines.
- Trusted networks: Deploy and use vSphere Integrated Containers Engine and create connections between Docker clients and virtual container hosts.
- VMware vSAN™ datastores: Specify vSAN datastores in which to store container images, container VM files, container volumes, and the virtual container host vApp.
- Docker API appliance virtual machine: The vSphere Integrated Containers Engine installer deploys a vApp, referred to as the virtual container host. You point Docker clients to this appliance for use as the Docker endpoint.
- Docker container virtual machines: Using Photon OS technology, you create and provision multiple container virtual machines directly from a template. The Docker daemon runs outside the container virtual machine. The container is a x86 hardware virtualized virtual machine with a process ID, container interfaces and mounts.



Virtual Container Host

The virtual container host appliance is backed by a Photon OS kernel that provides a virtual container endpoint backed by a vSphere vApp that allows you to control and consume container services.

You can access a Docker API endpoint for development and map ports for client connections to run containers as required.

vSphere resource management handles container placement within the virtual container host, so that a virtual container host can be served by an entire vSphere cluster or by a fraction of the same cluster. The only resources consumed by a container host in the cluster are the resources consumed by the container VMs that run in it.

You can reconfigure the virtual container host with no impact to containers running in it. The virtual container host is not limited by the kernel version or by the operating system that the containers are running.

You can deploy multiple virtual container hosts in an environment, depending on your business needs, including allocating separate resources for development, testing, and production.

You can configure virtual container hosts, giving your development team access to a large virtual container host, or sub-allocate smaller virtual container hosts for individual developers.

Each virtual container host maintains a cache of container images, which you download from either the public Docker Hub or a private registry.

The virtual container host maintains filesystem layers inherent in container images by mapping to discrete VMDK files, all of which are housed in vSphere datastores on VSAN, NFS, or local disks.

You deploy a virtual container host using the CLI installer, then access virtual container host endpoints remotely through a Docker command line interface or other API client.

vSphere Web Client Plugin

You can monitor virtual container hosts and container VMs by using the vSphere Integrated Containers Engine plug-in for the vSphere Web Client

Docker Client

Docker clients communicate with the virtual container host, not with each container, so you can see aggregated pools of vSphere resources, including storage and memory allocations.

You can pull standard container images from the Docker hub or from a private registry.

You can create, run, stop, and delete containers using standard docker commands and verify these actions in the vSphere Web Client.

Interoperability of vSphere Integrated Containers Engine with Other VMware Software

IT administrators use vCenter Server to view and manage containers. vSphere Integrated Containers Engine works seamlessly with VMware products.

VMware vRealize® Suite

vRealize Suite is available for health monitoring, performance analysis, and compliance across private and public clouds to move businesses faster.

VMware vSphere vMotion®

IT teams can assure service-level agreements for container workloads with VMware vSphere Distributed Resource Scheduler™ (DRS) as well as reduce planned and unplanned downtime with VMware vSphere vMotion.

You can restart or upgrade the virtual container host without needing to take the containers offline during the process. You do not require a native agent on the ESXi host. The appliance VM does not need to be running for vMotion to occur. Clusters with non-container VMs can also vMotion with fully automated DRS.

VMware vSAN™

The virtual container host maintains filesystem layers inherent in container images by mapping to discrete VMDK files, all of which can be which can be housed in shared vSphere datastores, including vSAN and NFS datastores.

Enhanced Link Mode Environments

You can deploy virtual container hosts in enhanced linked mode environments.

vSphere Features Not Supported in This Release

vSphere Integrated Containers Engine does not currently support the following vSphere features:

- vSphere Storage DRS™: You cannot use datastores in Storage DRS clusters as the target datastores for image stores or volume stores.
- vSphere High Availability: You can deploy virtual container hosts to systems that are configured with High Availability, but you cannot use High Availability to fail over the virtual container hosts themselves.
- vSphere Fault Tolerance: You cannot configure Fault Tolerance on virtual container hosts.
- vSphere Virtual Volumes™: You cannot use Virtual Volumes as the target datastores for image stores or volume stores.
- Snapshots: Creating snapshots of the virtual container host endpoint VM or container VMs can cause vSphere Integrated Containers Engine not to function correctly.
- Powering on, powering off, or deleting the virtual container host endpoint VM or container VMs can cause vSphere Integrated Containers Engine not to function correctly.

Virtual Container Host Administration

The `vic-machine` utility provides commands that allow you to manage existing virtual container hosts.

- Obtain vic-machine Version Information
- Common `vic-machine` Options
- List Virtual Container Hosts and Obtain their IDs
- Obtain Information About a Virtual Container Host
- Delete a Virtual Container Host
- Upgrade a Virtual Container Host
- Authorize SSH Access to the Virtual Container Host Endpoint VM

Obtain `vic-machine` Version Information

You can obtain information about the version of `vic-machine` by using the `vic-machine version` command.

Prerequisites

You have downloaded and unpacked the vSphere Integrated Containers Engine binaries.

Procedure

1. On the system on which you downloaded the binaries, navigate to the directory that contains the `vic-machine` utility.
2. Run the `vic-machine version` command.

   The `vic-machine version` command has no arguments.

   ```
   $ vic-machine-darwin-linux-windows version
   ```

Result

The `vic-machine` utility displays the version of the instance of `vic-machine` that you are using.

```
vic-machine--darwin-linux-windows.exe
version vic_machine_version-vic_machine_build-tag
```

- `vic_machine_version` is the version number of this release of vSphere Integrated Containers Engine.
- `vic_machine_build` is the build number of this release.
- `tag` is the hashtag of this build.

Common `vic-machine` Options

This section describes the options that are common to all `vic-machine` commands. The common options that `vic-machine` requires relate to the vSphere environment in which you deployed the virtual container host, and to the virtual container host itself.

`--target`

Short name: `-t`

The IPv4 address, fully qualified domain name (FQDN), or URL of the ESXi host or vCenter Server instance on which you deployed the virtual container host. This option is always **mandatory**.

- If the target ESXi host is not managed by vCenter Server, provide the address of the host.

  ```
  --target esxi_host_address
  ```

- If the target ESXi host is managed by vCenter Server, or if you deployed the virtual container host to a cluster, provide the address of vCenter Server.

  ```
  --target vcenter_server_address
  ```

- You can include the user name and password in the target URL.

  ```
  --target vcenter_or_esxi_username:password@vcenter_or_esxi_address
  ```

  Wrap the user name or password in single quotes (Linux or Mac OS) or double quotes (Windows) if they include special characters.

  ```
  'vcenter_or_esxi_usern@me':'p@ssword'@vcenter_or_esxi_address
  ```

  If you do not include the user name in the target URL, you must specify the `user` option. If you do not specify the `password` option or include the password in the target URL, `vic-machine` prompts you to enter the password.

- If you deployed the virtual container host on a vCenter Server instance that includes more than one datacenter, include the datacenter name in the target URL. If you include an invalid datacenter name, `vic-machine` fails and suggests the available datacenters that you can specify.

  ```
  --target vcenter_server_address/datacenter_name
  ```

`--user`

Short name: `-u`

The username for the ESXi host or vCenter Server instance on which you deployed the virtual container host. This option is mandatory if you do not specify the username in the `target` option.

```
--user esxi_or_vcenter_server_username
```

Wrap the user name in single quotes (Linux or Mac OS) or double quotes (Windows) if it includes special characters.

```
--user 'esxi_or_vcenter_server_usern@me'
```

`--password`

Short name: `-p`

The password for the user account on the vCenter Server on which you deployed the virtual container host, or the password for the ESXi host if you deployed directly to an ESXi host. If not specified, `vic-machine` prompts you to enter the password.

```
--password esxi_host_or_vcenter_server_password
```

Wrap the password in single quotation marks (') on Mac OS and Linux and in double quotation (") marks on Windows if it includes special characters.

```
--password 'esxi_host_or_vcenter_server_p@ssword'
```

`--thumbprint`

Short name: None

The thumbprint of the vCenter Server or ESXi host certificate. Specify this option if your vSphere environment uses untrusted, self-signed certificates. Alternatively, specifying the `--force` option allows you to omit the `--thumbprint` option. If your vSphere environment uses trusted certificates that are signed by a known Certificate Authority (CA), you do not need to specify the `--thumbprint` option.

To obtain the thumbprint of the vCenter Server or ESXi host certificate, run `vic-machine` without the specifying the `--thumbprint` or `--force` options. The operation fails, but the resulting error message includes the required certificate thumbprint. You can copy the thumbprint from the error message and run `vic-machine` again, including the `thumbprint` option.

```
--thumbprint certificate_thumbprint
```

`--compute-resource`

Short name: `-r`

The relative path to the host, cluster, or resource pool in which you deployed the virtual container host. Specify `--compute-resource` with exactly the same value that you used when you ran `vic-machine create`. You specify the `compute-resource` option in the following circumstances:

- vCenter Server includes multiple instances of standalone hosts or clusters, or a mixture of standalone hosts and clusters.
- The ESXi host includes multiple resource pools.
- You deployed the virtual container host in a specific resource pool in your environment.

If you specify the `id` option, you do not need to specify the `compute-resource` option.

If you do not specify the `compute-resource` or `id` options and multiple possible resources exist, `vic-machine` fails and suggests valid targets for `compute-resource` in the failure message.

- If the virtual container host is in a specific resource pool on an ESXi host, specify the name of the resource pool:

  ```
  --compute-resource  resource_pool_name
  ```

- If the virtual container host is on a vCenter Server instance that has more than one standalone host but no clusters, specify the IPv4 address or fully qualified domain name (FQDN) of the target host:

  ```
  --compute-resource host_address
  ```

- If the virtual container host is on a vCenter Server with more than one cluster, specify the name of the target cluster:

  ```
  --compute-resource cluster_name
  ```

- If the virtual container host is in a specific resource pool on a standalone host that is managed by vCenter Server, specify the IPv4 address or FQDN of the target host and name of the resource pool:

  ```
  --compute-resource host_name/resource_pool_name
  ```

- If the virtual container host is in a specific resource pool in a cluster, specify the names of the target cluster and the resource pool:

  ```
  --compute-resource cluster_name/resource_pool_name
  ```

- Wrap the resource names in single quotes (Linux or Mac OS) or double quotes (Windows) if they include spaces:

  ```
  --compute-resource 'cluster name'/'resource pool name'
  ```

`--name`

Short name: `-n`

The name of the virtual container host. This option is mandatory if the virtual container host has a name other than the default name, `virtual-container-host`, or if you do not use the `id` option. Specify `--name` with exactly the same value that you used when you ran `vic-machine create`. This option is not used by `vic-machine ls`.

```
--name vch_appliance_name
```

Wrap the appliance name in single quotes (Linux or Mac OS) or double quotes (Windows) if it includes spaces.

```
--name 'vch appliance name'
```

`--id`

Short name: None

The vSphere Managed Object Reference, or moref, of the virtual container host, for example `vm-100`. You obtain the ID of a virtual container host by running `vic-machine ls`. If you specify the `id` option, you do not need to specify the `--name` or `--compute-resource` options. This option is not used by `vic-machine ls`.

```
--id vch_id
```

`--timeout`

Short name: none

The timeout period for performing operations on the virtual container host. Specify a value in the format `XmYs` if the default timeout of 3m0s is insufficient.

```
--timeout 5m0s
```

List Virtual Container Hosts and Obtain Their IDs

You can obtain a list of the virtual container hosts that are running in vCenter Server or on an ESXi host by using the `vic-machine ls` command.

The `vic-machine ls` command lists virtual container hosts with their IDs, names, and versions. The `vic-machine ls` command informs you whether upgrades are available for the virtual container hosts.

The `vic-machine ls` command does not include any options in addition to the common options described in Common `vic-machine` Options.

Prerequisites

You have deployed at least one virtual container host.

Procedure

1. On the system on which you run `vic-machine`, navigate to the directory that contains the `vic-machine` utility.
2. Run the `vic-machine ls` command.
   - To obtain a list of all virtual container hosts that are running on an ESXi host or vCenter Server instance, you must provide the address of the target ESXi host or vCenter Server.
   - You must specify the username and optionally the password, either in the `--target` option or separately in the `--user` and `--password` options.
   - If your vSphere environment uses untrusted, self-signed certificates, you must also specify the thumbprint of the vCenter Server instance or ESXi host in the `--thumbprint` option. To obtain the thumbprint of the vCenter Server or ESXi host certificate, run `vic-machine` without the specifying the `--thumbprint` option. The listing of the virtual container hosts fails, but the resulting error message includes the required certificate thumbprint. You can copy the thumbprint from the error message and run `vic-machine` again, including the `--thumbprint` option.

```
$ vic-machine-darwin-linux-windows ls
--target esxi_host_address
--user root
--password esxi_host_password
--thumbprint certificate_thumbprint
```

```
$ vic-machine-darwin-linux-windows ls
--target vcenter_server_username:password@vcenter_server_address
--thumbprint certificate_thumbprint
```

Result

The `vic-machine ls` command lists the virtual container hosts that are running on the ESXi host or vCenter Server instance that you specified.

```
ID         PATH     NAME    VERSION                    UPGRADE STATUS
vm-101     path     vch_1   vch_version-vch_build-tag  Up to date
vm-102     path     vch_2   vch_version-vch_build-tag  Up to date
[...]
vm-n       path     vch_n   vch_version-vch_build-tag  Up to date
```

- The IDs are the vSphere Managed Object References, or morefs, for the virtual container host endpoint VMs. You can use virtual container host IDs when you run the `vic-machine inspect`, `upgrade`, `debug`, and `delete` commands. Using virtual container host IDs reduces the number of options that you need to specify when you run those commands.
- The `PATH` value depends on where the virtual container host is deployed:
  - ESXi host that is not managed by vCenter Server:

    ```
    /ha-datacenter/host/host_name/Resources
    ```

  - Standalone host that is managed by vCenter Server:

    ```
    /datacenter/host/host_address/Resources
    ```

  - vCenter Server cluster:

    ```
    /datacenter/host/cluster_name/Resources
    ```

  - If virtual container hosts are deployed in resource pools on hosts or clusters, the resource pool names appear after `Resources` in the path.
- The `VERSION` value includes the version of `vic-machine` that was used to create the virtual container host, the build number of this version, and a hashtag to identify the build.
- The `UPGRADE STATUS` reflects whether the version of `vic-machine` that you are using is the same as the version of the virtual container host. If the version or build number of the virtual container host does not match that of `vic-machine`, `UPGRADE STATUS` is `Upgradeable to vch_version-vch_build-tag`.

Obtain Information About a Virtual Container Host

You can obtain information about a virtual container host by using the `vic-machine inspect` command.

The `vic-machine inspect` command does not include any options in addition to the common options described in Common `vic-machine` Options.

Prerequisites

You have deployed a virtual container host.

Procedure

1. On the system on which you run `vic-machine`, navigate to the directory that contains the `vic-machine` utility.
2. Run the `vic-machine inspect` command.

   The following example includes the options required to obtain information about a named instance of a virtual container host from a simple vCenter Server environment.

   - You must specify the username and optionally the password, either in the `--target` option or separately in the `--user` and `--password` options.
   - If the virtual container host has a name other than the default name, `virtual-container-host`, you must specify the `--name` or `--id` option.
   - If multiple compute resources exist in the datacenter, you must specify the `--compute-resource` or `--id` option.
   - If your vSphere environment uses untrusted, self-signed certificates, you must also specify the thumbprint of the vCenter Server instance or ESXi host in the `--thumbprint` option. To obtain the thumbprint of the vCenter Server or ESXi host certificate, run `vic-machine` without the specifying the `--thumbprint` option. The inspection of the virtual container host fails, but the resulting error message includes the required certificate thumbprint. You can copy the thumbprint from the error message and run `vic-machine` again, including the `--thumbprint` option.

   ```
   $ vic-machine-darwin-linux-windows inspect
   --target vcenter_server_username:password@vcenter_server_address
   --thumbprint certificate_thumbprint
   --name vch_name
   ```

Result

The `vic-machine inspect` command displays information about the virtual container host:

- The virtual container host ID:

  ```
  VCH ID: VirtualMachine:vm-101
  ```

  The vSphere Managed Object Reference, or moref, of the virtual container host. You can use virtual container host ID when you run the `vic-machine delete`, `upgrade` or `debug` commands. Using a virtual container host ID reduces the number of options that you need to specify when you run those commands.

- The version of the `vic-machine` utility and the version of the virtual container host that you are inspecting.

```
Installer version: vic_machine_version-vic_machine_build-tag
VCH version: vch_version-vch_build-tag
VCH upgrade status:
Installer has same version as VCH
No upgrade available with this installer version
```

If `vic-machine inspect` reports a difference between the version or build number of `vic-machine` and the version or build number of the virtual container host, the upgrade status is `Upgrade available`.

- The address of the VCH Admin portal for the virtual container host.

```
vic-admin portal:
https://vch_address:2378
```

- The address at which the virtual container host publishes ports.

```
vch_address
```

- The Docker environment variables that container developers can use when connecting to this virtual container host.
  - Virtual container host with full TLS authentication with trusted Certificate Authority certificates:

    ```
    DOCKER_TLS_VERIFY=1
    DOCKER_CERT_PATH=path_to_certificates
    DOCKER_HOST=vch_address:2376
    ```

  - Virtual container host with TLS authentication with untrusted self-signed certificates:

    ```
    DOCKER_HOST=vch_address:2376
    ```

  - Virtual container host with no TLS authentication:

    ```
    DOCKER_HOST=vch_address:2375
    ```

- The Docker command to use to connect to the Docker endpoint.
  - Virtual container host with full TLS authentication with trusted Certificate Authority certificates:

    ```
    docker -H vch_address:2376 --tlsverify info
    ```

  - Virtual container host with TLS authentication with untrusted self-signed certificates or no TLS authentication:

    ```
    docker -H vch_address:2376 --tls info
    ```

  - Virtual container host with no TLS authentication:

    ```
    docker -H vch_address:2375 info
    ```

Delete a Virtual Container Host

You delete virtual container hosts by using the `vic-machine delete` command.

For descriptions of the options that `vic-machine delete` includes in addition to the Common `vic-machine` Options , see Virtual Container Host Delete Options.

Prerequisites

You have deployed a virtual container host that you no longer require.

Procedure

1. On the system on which you run `vic-machine` , navigate to the directory that contains the `vic-machine` utility.
2. Run the `vic-machine delete` command.

   The following example includes the options required to remove a virtual container host from a simple vCenter Server environment.

   - You must specify the username and optionally the password, either in the `--target` option or separately in the `--user` and `--password` options.
   - If the virtual container host has a name other than the default name, `virtual-container-host` , you must specify the `--name` or `--id` option.
   - If multiple compute resources exist in the datacenter, you must specify the `--compute-resource` or `--id` option.
   - If your vSphere environment uses untrusted, self-signed certificates, you must also specify the thumbprint of the vCenter Server instance or ESXi host in the `--thumbprint` option. To obtain the thumbprint of the vCenter Server or ESXi host certificate, run `vic-machine` without the specifying the `--thumbprint` or `--force` options. The deletion of the virtual container host fails, but the resulting error message includes the required certificate thumbprint. You can copy the thumbprint from the error message and run `vic-machine` again, including the `--thumbprint` option.

   ```
   $ vic-machine-darwin-linux-windows delete
   --target vcenter_server_username:password@vcenter_server_address
   --thumbprint certificate_thumbprint
   --name vch_name
   ```

3. If the delete operation fails with a message about container VMs that are powered on, run `vic-machine delete` again with the `--force` option.

   CAUTION Running `vic-machine delete` with the `--force` option removes all running container VMs that the virtual container host manages, as well as any associated volumes and volume stores.

   If your vSphere environment uses untrusted, self-signed certificates, running `vic-machine delete` with the `--force` option allows you to omit the `--thumbprint` option.

   ```
   $ vic-machine-darwin-linux-windows delete
   --target vcenter_server_username:password@vcenter_server_address
   --name cluster_name
   --force
   ```

Virtual Container Host Delete Options

The command line utility for vSphere Integrated Containers Engine, `vic-machine`, provides a `delete` command that allows you to cleanly remove virtual container hosts.

The `vic-machine delete` command includes one option in addition to the common options described in Common `vic-machine` Options.

`--force`

Short name: `-f`

Forces `vic-machine delete` to ignore warnings and continue with the deletion of a virtual container host. Any running container VMs and any volume stores associated with the virtual container host are deleted. Errors such as an incorrect compute resource still cause the deletion to fail.

- If you do not specify `--force` and the virtual container host contains running container VMs, the deletion fails with a warning.
- If you do not specify `--force` and the virtual container host has volume stores, the deletion of the virtual container host succeeds without deleting the volume stores. The list of volume stores appears in the `vic-machine delete` success message for reference and optional manual removal.

If your vSphere environment uses untrusted, self-signed certificates, you can use the `--force` option to delete a virtual container host without providing the thumbprint of the vCenter Server or ESXi host in the `--thumbprint` option.

```
--force
```

Upgrade a Virtual Container Host

You upgrade virtual container hosts by downloading a new version of vSphere Integrated Containers Engine and running the `vic-machine upgrade` command.

IMPORTANT: Due to the substantial changes in vSphere Integrated Containers version 0.7, you cannot use `vic-machine upgrade` to upgrade from version 0.6 to version 0.7. You can use `vic-machine upgrade` to upgrade from more recent builds to version 0.7.

For descriptions of the options that `vic-machine upgrade` includes in addition to the Common `vic-machine` Options , see Virtual Container Host Upgrade Options.

Prerequisites

- You deployed one or more virtual container hosts with an older version of the `vic-machine create` command.
- You downloaded a new version of the vSphere Integrated Containers Engine bundle.
- Run the `vic-machine ls` command by using the new version of `vic-machine` to see the upgrade status of all of the virtual container hosts that are running on a vCenter Server instance or ESXi host. For information about running `vic-machine ls` , see List Virtual Container Hosts and Obtain Their IDs.
- Optionally note the IDs of the virtual container hosts.

Procedure

1. On the system on which you run `vic-machine` , navigate to the directory that contains the new version of the `vic-machine` utility.
2. Run the `vic-machine upgrade` command.

   The following example includes the options required to upgrade a virtual container host in a simple vCenter Server environment.

   - You must specify the username and optionally the password, either in the `target` option or separately in the `--user` and `--password` options.
   - If the virtual container host has a name other than the default name, `virtual-container-host` , you must specify the `--name` or `--id` option.
   - If multiple compute resources exist in the datacenter, you must specify the `--compute-resource` or `--id` option.
   - If your vSphere environment uses untrusted, self-signed certificates, you must also specify the thumbprint of the vCenter Server instance or ESXi host in the `--thumbprint` option. To obtain the thumbprint of the vCenter Server or ESXi host certificate, run `vic-machine` without the specifying the `--thumbprint` or `--force` options. The upgrade of the virtual container host fails, but the resulting error message includes the required certificate thumbprint. You can copy the thumbprint from the error message and run `vic-machine` again, including the `--thumbprint` option.

   ```
   $ vic-machine-darwin-linux-windows upgrade
   --target vcenter_server_username:password@vcenter_server_address
   --thumbprint certificate_thumbprint
   --name vch_name
   ```

3. If the upgrade operation fails with error messages, run `vic-machine upgrade` again with the `--force` option.

   If your vSphere environment uses untrusted, self-signed certificates, running `vic-machine upgrade` with the `--force` option allows you to omit the `--thumbprint` option.

```
$ vic-machine-darwin-linux-windows upgrade
--target vcenter_server_username:password@vcenter_server_address
--name cluster_name
--force
```

Result

During the upgrade process, `vic-machine upgrade` performs the following operations:

- Validates whether the configuration of the existing virtual container host is compatible the new version. If not, the upgrade fails.
- Uploads the new versions of the `appliance.iso` and `bootstrap.iso` files to the virtual container host.
- Creates a snapshot of the virtual container host endpoint VM, to use in case the upgrade fails and has to roll back.
- Boots the virtual container host by using the new version of the `appliance.iso` file.
- Deletes the snapshot of the virtual container host endpoint VM once the upgrade has succeeded.
- After you upgrade a virtual container host, any new container VMs will boot from the new version of the `bootstrap.iso` file.

NOTE: Upgrading a virtual container host does not upgrade any existing container VMs that are running in the virtual container host. For container VMs to boot from the latest version of `bootstrap.iso`, container developers must recreate them.

Virtual Container Host Upgrade Options

The command line utility for vSphere Integrated Containers Engine, `vic-machine`, provides an `upgrade` command that allows you to upgrade virtual container hosts to a newer version.

IMPORTANT: Due to the substantial changes in vSphere Integrated Containers version 0.7, you cannot use `vic-machine upgrade` to upgrade from version 0.6 to version 0.7. You can use `vic-machine upgrade` to upgrade from more recent builds to version 0.7.

The `vic-machine upgrade` command includes the following options in addition to the common options described in Common `vic-machine` Options.

`--appliance-iso`

Short name: `--ai`

The path to the new version of the ISO image from which to upgrade the virtual container host appliance. Set this option if you have moved the `appliance.iso` file to a folder that is not the folder that contains the `vic-machine` binary or is not the folder from which you are running `vic-machine`. Include the name of the ISO file in the path.

NOTE: Do not use the `--appliance-iso` option to point `vic-machine` to an `--appliance-iso` file that is of a different version to the version of `vic-machine` that you are running.

```
--appliance-iso path_to_ISO_file/ISO_file_name.iso
```

Wrap the folder names in the path in single quotes (Linux or Mac OS) or double quotes (Windows) if they include spaces.

```
--appliance-iso 'path to ISO file'/appliance.iso
```

`--bootstrap-iso`

Short name: `--bi`

The path to the new version of the ISO image from which to upgrade the container VMs that the virtual container host manages. Set this option if you have moved the `bootstrap.iso` file to a folder that is not the folder that contains the `vic-machine` binary or is not the folder from which you are running `vic-machine`. Include the name of the ISO file in the path.

NOTE: Do not use the `--bootstrap-iso` option to point `vic-machine` to a `--bootstrap-iso` file that is of a different version to the version of `vic-machine` that you are running.

```
--bootstrap-iso path_to_ISO_file/bootstrap.iso
```

Wrap the folder names in the path in single quotes (Linux or Mac OS) or double quotes (Windows) if they include spaces.

```
--bootstrap-iso 'path to ISO file'/ISO_file_name.iso
```

`--force`

Short name: `-f`

Forces `vic-machine upgrade` to ignore warnings and continue with the upgrade of a virtual container host. Errors such as an incorrect compute resource still cause the upgrade to fail.

If your vSphere environment uses untrusted, self-signed certificates, you can use the `--force` option to upgrade a virtual container host without providing the thumbprint of the vCenter Server or ESXi host in the `thumbprint` option.

```
--force
```

Authorize SSH Access to the Virtual Container Host Endpoint VM

By default, SSH access to the virtual container host endpoint VM is disabled. The command line utility for vSphere Integrated Containers Engine, `vic-machine`, provides a `debug` command that allows you to enable SSH access to the virtual container host endpoint VM. The `debug` command also allows you to set a password for the root user account on the endpoint VM. You can also use `debug` to upload a key file for public key authentication when accessing the endpoint VM.

IMPORTANT: If you set a password for the virtual container host endpoint VM, this password does not persist if you reboot the VM. You must run `vic-machine debug` to reset the password each time you reboot the virtual container host endpoint VM.

For descriptions of the options that `vic-machine debug` includes in addition to the Common `vic-machine` Options, see Virtual Container Host Debug Options.

Prerequisites

You have deployed at least one virtual container host.

Procedure

1. On the system on which you run `vic-machine`, navigate to the directory that contains the `vic-machine` utility.
2. Run the `vic-machine debug` command.
    - You must specify the username and optionally the password, either in the `--target` option or separately in the `--user` and `--password` options.
    - If your vSphere environment uses untrusted, self-signed certificates, you must also specify the thumbprint of the vCenter Server instance or ESXi host in the `--thumbprint` option. To obtain the thumbprint of the vCenter Server or ESXi host certificate, run `vic-machine` without the specifying the `--thumbprint` option. The operation fails, but the resulting error message includes the required certificate thumbprint. You can copy the thumbprint from the error message and run `vic-machine` again, including the `--thumbprint` option.
    - Specify the `--enable-ssh` and `--rootpw` options. Wrap the password in single quotes (Linux or Mac OS) or double quotes (Windows) if it includes special characters.
    - Optionally, specify the `--authorized-key` option to upload a public key file to `/root/.ssh/authorized_keys` folder in the endpoint VM. Include the name of the `*.pub` file in the path.

```
$ vic-machine-darwin-linux-windows debug
--target esxi_host_address
--user root
--password esxi_host_password
--thumbprint certificate_thumbprint
--enable-ssh
--rootpw 'new_p@ssword'
--authorized-key path_to_public_key_file/key_file.pub
```

Result

The output of the `vic-machine debug` command includes confirmation that SSH access is enabled:

```
### Configuring VCH for debug ####
[...]
SSH to appliance:
ssh root@vch_address
[...]
Completed successfully
```

Virtual Container Host Debug Options

The command line utility for vSphere Integrated Containers Engine, `vic-machine`, provides a `debug` command that allows you to enable SSH access to the virtual container host endpoint VM, set a password for the root user account, and upload a key file for automatic public key authentication.

If you authorize SSH access to the virtual container host endpoint VM, you can edit system configuration files that you cannot edit by running `vic-machine` commands.

NOTE: Modifications that you make to the configuration of the virtual container host endpoint VM do not persist if you reboot the VM.

The `vic-machine debug` command includes the following options in addition to the common options described in Common `vic-machine` Options.

`--enable-ssh`

Short name: `--ssh`

Enable an SSH server in the virtual container host endpoint VM. The `sshd` service runs until the virtual container host endpoint VM reboots. The `--enable-ssh` takes no arguments.

```
--enable-ssh
```

`--rootpw`

Short name: `--pw`

Set a new password for the root user account on the virtual container host endpoint VM.

IMPORTANT: If you set a password for the virtual container host endpoint VM, this password does not persist if you reboot the VM. You must run vic-machine debug to reset the password each time you reboot the virtual container host endpoint VM.

Wrap the password in single quotes (Linux or Mac OS) or double quotes (Windows) if it includes special characters.

```
--rootpw 'new_p@ssword'
```

`--authorized-key`

Short name: `--key`

Upload a public key file to `/root/.ssh/authorized_keys` folder in the endpoint VM to implement public authentication when accessing the virtual container host endpoint VM. Include the name of the `*.pub` file in the path.

```
--authorized-key path_to_public_key_file/key_file.pub
```

Find Virtual Container Host Information in the vSphere Web Client

After you have installed the vSphere Web Client plug-in for vSphere Integrated Containers Engine, you can find information about virtual container hosts in the vSphere Web Client.

IMPORTANT: Do not use the vSphere Web Client to perform operations on virtual container host appliances or container VMs. Specifically, using the vSphere Web Client to power off, power on, or delete virtual container host appliances or container VMs can cause vSphere Integrated Containers Engine to not function correctly. Always use `vic-machine` to perform operations on virtual container hosts. Always use Docker commands to perform operations on containers.

Prerequisites

- You deployed a virtual container host.
- You installed the vSphere Web Client plug-in for vSphere Integrated Containers Engine.

Procedure

1. In the vSphere Web Client Home page, select **Hosts and Clusters**.
2. Expand the hierarchy of vCenter Server objects to navigate to the virtual container host vApp.
3. Expand the virtual container host vApp and select the virtual container host endpoint VM.
4. Click the **Summary** tab for the virtual container host endpoint VM and scroll down to the Virtual Container Host portlet.

Result

Information about the virtual container host appears in the Virtual Container Host portlet in the **Summary** tab:

- The address of the Docker API endpoint for this virtual container host
- Alink to the vic-admin portal for the virtual container host, from which you can obtain health information and download log bundles for the virtual container host.

Find Container Information in the vSphere Web Client

After you have installed the vSphere Web Client plug-in for vSphere Integrated Containers Engine, you can use the vSphere Web Client to find information about containers that are running in virtual container hosts.

IMPORTANT: Do not use the vSphere Web Client to perform operations on virtual container host appliances or container VMs. Specifically, using the vSphere Web Client to power off, power on, or delete virtual container host appliances or container VMs can cause vSphere Integrated Containers Engine to not function correctly. Always use `vic-machine` to perform operations on virtual container hosts. Always use Docker commands to perform operations on containers.

Prerequisites

- You deployed a virtual container host and pulled and ran at least one container.
- You installed the vSphere Web Client plug-in for vSphere Integrated Containers Engine.

Procedure

1. In the vSphere Web Client Home page, select **Hosts and Clusters**.
2. Expand the hierarchy of vCenter Server objects to navigate to the virtual container host vApp.
3. Expand the virtual container host vApp and select a container VM.
4. Click the **Summary** tab for the container VM and scroll down to the **Container** portlet.

Result

Information about the container appears in the Container portlet in the **Summary** tab:

- The name of the running container. If the container developer used `docker run -name container_name` to run the container, `container_name` appears in the portlet.
- The image from which the container was deployed.
- If the container developer used `docker run -p port` to map a port when running the container, the port number and the protocol appear in the portlet.

Upgrade the vSphere Integrated Containers Engine Plug-In

If you download a new version of vSphere Integrated Containers Engine, upgrade the vSphere Web Client plug-in for vSphere Integrated Containers Engine.

Prerequisites

- You deployed an older version of the vSphere Web Client plug-in for vSphere Integrated Containers Engine.
- You downloaded a new version of vSphere Integrated Containers Engine.

For information about updating the `configs` file and where to copy the `com.vmware.vicui.Vicui-version.zip` file or `com.vmware.vicui.Vicui-version` folder, see the topic that corresponds to your type of deployment in Installing the vSphere Web Client Plug-in for vSphere Integrated Containers Engine in *vSphere Integrated Containers Engine Installation*.

Procedure

1. Copy the new versions of the `com.vmware.vicui.Vicui-version.zip` file or `com.vmware.vicui.Vicui-version` folder to the appropriate location on your Web server or vCenter Server system.
2. Update the new version of the `ui/VCSA/configs` or `ui/vCenterForWindows/configs` file.
3. Run the `ui/VCSA/upgrade.sh` or `ui/vCenterForWindows/upgrade.bat` script.
4. When the upgrade finishes, if you are logged into the vSphere Web Client, log out then log back in again.

Access the Administration Portal for a Virtual Container Host

vSphere Integrated Containers Engine provides a Web-based administration portal for virtual container hosts, called VCH Admin.

Prerequisites

- You deployed a virtual container host.
- Obtain the address of the virtual container host:
  - Copy the address from the output of `vic-machine create` or `vic-machine inspect`.
  - If you deployed the virtual container host to vCenter Server, copy the address from the **Summary** tab for the vSphere Integrated Containers Engine endpoint VM in the vSphere Web Client.
  - If you deployed the virtual container host to an ESXi host, copy the address from the **Summary** tab for the vSphere Integrated Containers Engine endpoint VM in the vSphere Client.
- If you deployed the virtual container host with full TLS authentication with trusted CA certificates, import the `*.pfx` certificate that `vic-machine create` generated into your browser.
  - In the current builds of vSphere Integrated Containers, the certificates do not work in Chrome or Internet Explorer. Use Firefox to access the VCH Admin portal.
  - When you import the certificate into your browser, do not enter a password. Select **Automatically select the certificate store based on the type of certificate**.

Procedure

In a Web browser, go to https://*vch_address*:2378.

Result

The VCH Admin portal displays information about the virtual container host and the environment in which is running:

- Status information about the virtual container host, network, firewall configuration, and license. For information about these statuses and how to remedy error states, see the Virtual Container Host Status Reference.
- The address of the Docker endpoint.
- The remaining capacity of the datastore that you designated as the image store.
- Live logs and log bundles for different aspects of the virtual container host. For information about the logs, see Access vSphere Integrated Containers Engine Log Bundles.

Virtual Container Host Status Reference

The Web-based administration portal for virtual container hosts, VCH Admin, presents status information about a virtual container host.

If the vSphere environment in which you are deploying a virtual container host does not meet the requirements, the deployment does not succeed. However, a successfully deployed virtual container host can stop functioning if the vSphere environment changes after the deployment. If environment changes adversely affect the virtual container host, the status of the affected component changes from green to yellow.

Virtual Container Host (VCH)

VCH Admin checks the status of the processes that the virtual container host runs:

- The port layer server, that presents an API of low-level container primitive operations, and implements those container operations via the vSphere APIs.
- VCH Admin server, that runs the VCH Admin portal.
- The vSphere Integrated Containers Engine initialization service and watchdog service for the other components.
- The Docker engine server, that exposes the Docker API and semantics, translating those composite operations into port layer primitives.

Error

The Virtual Container Host status is yellow.

Cause

One or more of the virtual container host processes is not running correctly.

Solution

1. In the VCH Admin portal for the virtual container host, click the link for the **VCH Admin Server** log.
2. Search the log for references to the different virtual container host processes.

   The different processes are identified in the log by the following names:

   - `port-layer-server`
   - `vicadmin`
   - `vic-init`
   - `docker-engine-server`
3. Identify the process or processes that are not running correctly and attempt to remediate the issues as required.

Network Connectivity

VCH Admin checks external network connectivity by attempting to connect from the virtual container host to docker.io and google.com. VCH Admin only checks the external network connection. It does not check other networks, for example the bridge, management, client, or container networks.

Error

The Network Connectivity status is yellow.

Cause

The external network connection is down.

Solution

1. In the VCH Admin portal for the virtual container host, click the link for the **VCH Admin Server** log.
2. Search the log for references to network issues.
3. In the vSphere Web Client, remediate the network issues as required.

Firewall

VCH Admin checks that the firewall is correctly configured on the ESXi host or the ESXi hosts in the cluster on which the virtual container host is running.

Error

The Firewall status is yellow and shows the error `Firewall must permit 2377/tcp outbound to use VIC`.

Cause

The firewall on the ESXi host on which the virtual container host is running no longer allows outbound connections on port 2377.

- The firewall was switched off when the virtual container host was deployed. The firewall has been switched on since the deployment of the virtual container host.
- A firewall ruleset was applied to the ESXi host to allow outbound connections on port 2377. The ESXi host has been rebooted since the deployment of the virtual container host. Firewall rulesets are not retained when an ESXi host reboots.

Solution

Reconfigure the firewall on the ESXi host or hosts to allow outbound connections on port 2377. For information about how to reconfigure the firewall on ESXi hosts, see VCH Deployment Fails with Firewall Validation Error in *vSphere Integrated Containers Engine Installation*.

Error

The Firewall status is yellow.

Cause

The management network is down, or the virtual container host endpoint VM is unable to connect to vSphere.

Solution

Restore the connection to the management network.

License

VCH Admin checks that the ESXi hosts on which you deploy virtual container hosts have the appropriate licenses.

Error

The License status is yellow and shows the error `License does not meet minimum requirements to use VIC`.

Cause

The license for the ESXi host or for one or more of the hosts in a vCenter Server cluster on which the virtual container host is deployed has been removed, downgraded, or has expired since the deployment of the virtual container host.

Solution

- If the virtual container host is running on an ESXi host that is not managed by vCenter Server, replace the ESXi host license with a valid vSphere Enterprise license.
- If the virtual container host is running on a standalone ESXi host in vCenter Server, replace the ESXi host license with a valid vSphere Enterprise Plus license.
- If the virtual container host is running in a vCenter Server cluster, check that all of the hosts in the cluster have a valid vSphere Enterprise Plus license, and replace any licenses that have been removed, downgraded, or have expired.

Error

The License status is yellow.

Cause

The management network is down, or the virtual container host endpoint VM is unable to connect to vSphere.

Solution

Restore the connection to the management network.

Troubleshooting vSphere Integrated Containers Engine Administration

This information provides solutions for common problems that you might encounter when working with vSphere Integrated Containers Engine.

- Access vSphere Integrated Containers Engine Log Bundles
- Running `vic-machine ls` on an ESXi Host Fails with an Error
- Deleting or Inspecting a VCH Fails with a Resource Pool Error
- Connections Fail with Certificate Errors when Using Full TLS Authentication with Trusted Certificates

Access vSphere Integrated Containers Engine Log Bundles

vSphere Integrated Containers Engine provides log bundles that you can download from the VCH Admin portal for a virtual container host.

- The **Log Bundle** contains logs that relate specifically to the virtual container host that you created.
- The **Log Bundle with container logs** contains the logs for the virtual container host and also includes the logs regarding the containers that the virtual container host manages.
- Live logs (tail files) allow you to view the current status of how components are running.
  - **Docker Personality** is the interface to Docker. When configured with client certificate security, it reports unauthorized access attempts to the Docker server web page.
  - **Port Layer Service** is the interface to vSphere.
  - **Initialization & watchdog** reports network configuration, component launch status for the VCH Admin portal and the port layer, records if they fail, and relaunches them if they do. The binary `vic-init` launches the components and redirects their output to the log files in `/var/log/vic/`. At higher debug levels, the component output is duplicated in that log file, so `init.log` includes a superset of the log data.
  - **Admin Server** includes logs for the admin server, may contain processes that failed, and network issues. When configured with client certificate security, it reports unauthorized access attempts to the admin server web page.

Live logs can help you to see how any current changes you make might affect the logs. For example, when you try to troubleshoot an issue, you can see if your attempt worked or failed by looking at the live logs.

You can share the non-live version of the logs with administrators or VMware Support to help you to solve issues.

Running `vic-machine ls` on an ESXi Host Fails with an Error

When you use `vic-machine ls` to list virtual container hosts and you specify the address of an ESXi host in the `target` option, the operation fails with an error.

Problem

Listing virtual container hosts fails with the error message:

```
Target is managed by vCenter server "vcenter_server_address",
please change --target to vCenter server address or select a standalone ESXi
```

Cause

You set the `target` option to the address of an ESXi host that is managed by a vCenter Server instance.

Solution

Set the `target` option to the address of the vCenter Server instance that manages the ESXi host on which the virtual container hosts are running.

Deleting or Inspecting a VCH Fails with a Resource Pool Error

When you use `vic-machine delete` or `vic-machine inspect` to delete or inspect a virtual container host and you specify the address of an ESXi host in the `target` option, the operation fails with a resource pool error.

Problem

Deleting or inspecting a virtual container host fails with the error message:

```
Failed to get VCH resource pool "/ha-datacenter/host/localhost./Resources/vch_name":
resource pool '/ha-datacenter/host/localhost./Resources/vch_name' not found
```

Cause

You set the `target` option to the address of an ESXi host that is managed by a vCenter Server instance.

Solution

1. Run `vic-machine ls` with the `target` option set to the same ESXi host.

   The `vic-machine ls` operation fails but informs you of the address of the vCenter Server instance that manages the ESXi host.

2. Run `vic-machine delete` or `vic-machine inspect` again, setting the `target` option to the address of the vCenter Server instance that was returned by `vic-machine ls`.

Connections Fail with Certificate Errors when Using Full TLS Authentication with Trusted Certificates

Connections to a virtual container host that uses full TLS authentication with trusted Certificate Authority (CA) certificates fail with certificate errors.

Problem

- `vic-machine` operations on a virtual container host result in a "bad certificate" error:

  ```
  Connection failed with TLS error "bad certificate"
  check for clock skew on the host
  Collecting host-227 hostd.log
  vic-machine-windows.exe failed: tls: bad certificate
  ```

- Connections to the VCH Admin portal for the virtual container host fail with an `ERR_CERT_DATE_INVALID` error.

Cause

There is a clock skew between the virtual container host and the system from which you are connecting to the virtual container host.

Solution

1. Run `vic-machine debug` to enable SSH access to the virtual container host.

   For information about enabling SSH on a virtual container host, see Authorize SSH Access to the Virtual Container Host Endpoint VM.

2. Connect to the virtual container host endpoit VM by using SSH.
3. Use the `date --set` Linux command to set the system clock to the correct date and time.

To prevent this issue recurring on virtual container hosts that you deploy in the future, verify that the host time is correct on the ESXi host on which you deploy virtual container hosts. For information about verifying time synchronization on ESXi hosts, see VMware KB 1003736.