VMware vSphere Integrated Containers Engine for vSphere Administrators

vSphere Integrated Containers Engine 0.8

vmware

Table of Contents

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: 0.8

Intended Audience

This information is intended for vSphere® Administrators who 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 useful.

For an introduction to vSphere Integrated Containers Engine 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
- Submit a doc issue in Github

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

www.vmware.com

Interoperability of vSphere Integrated Containers Engine with Other VMware Software

vSphere Administrators can use vSphere to view and manage virtual container hosts (VCHs) and container VMs. vSphere Integrated Containers Engine works with the following vSphere features and VMware products.

Performing Operations on VCHs and Container VMs in vSphere

- If you restart a VCH endpoint VM, it comes back up in the same state that it was in when it shut down.
- If you shut down the VCH vApp, the VCH endpoint VM and all of the container VMs that it manages are shut down.
- If you use DHCP on the client network, the IP address of the VCH endpoint VM might change after a restart. Use `vic-machine inspect` to obtain the new IP address.
- Do not manually delete a VCH vApp or VCH endpoint VM. Use `vic-machine delete` to delete VCHs.
- Manually powering off container VMs can result in incorrect end-times for container opeations. Do not manually delete a contaienr VM. Use Docker commands to perform operations on container VMs.

VMware vRealize® Suite

You can use VMware vRealize Automation to provide a self-provisioning service for VCHs, by using the vRealize Automation interface or APIs to request VCHs. At the end of such a provisioning process, vRealize Automation can communicate the VCH endpoint VM address to the requester.

VMware vSphere vMotion®

You can use vMotion to move VCHs without needing to take the container VMs offline. The VCH endpoint VM does not need to be running for vMotion to occur on the container VMs. Clusters with a mix of container VMs and non-container VMs can use vMotion with fully automated DRS.

Maintenance Mode

Hosts with container VMs can enter maintenance mode without manual intervention, with these exceptions:

- For a standalone ESXi host, you must power down VCHs and any container VMs before entering maintenance mode.
- In a clustered vSphere environment with DRS set to automatic, DRS migrates VCHs to another host in the cluster before the host enters maintenance mode.
- For a host with running container VMs, DRS migrates the container VMs to another host in the cluster before the host enters maintenance mode.

VMware vSAN™

VCHs maintain filesystem layers inherent in container images by mapping to discrete VMDK files, all of which can be housed in shared vSphere datastores, including vSAN, NFS, and iSCSI datastores.

vCenter Linked Mode Environments

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

VCH Administration

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

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-operating_system version
   ```

Result

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

```
vic-machine-operating_system
version vic_machine_version-vic_machine_build-git_commit
```

- `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 short `git commit` checksum for the latest commit for 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 (VCH), and to the VCH 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 VCH. 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 VCH 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 VCH 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 VCH. 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 VCH, 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. If you obtain the thumbprint by other means, use upper-case letters and colon delimitation rather than space delimitation when you specify `--thumbprint`.

```
--thumbprint certificate_thumbprint
```

--compute-resource

Short name: `-r`

The relative path to the host, cluster, or resource pool in which you deployed the VCH. 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.
- You deployed the VCH 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 VCH is in a specific resource pool on an ESXi host, specify the name of the resource pool:

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

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

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

- If the VCH 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 VCH 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 VCH. This option is mandatory if the VCH 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 VCH, for example `vm-100`. You obtain the ID of a VCH 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 create` or `vic-machine version`.

```
--id vch_id
```

`--timeout`

Short name: none

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

```
--timeout 5m0s
```

List VCHs and Obtain Their IDs

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

The `vic-machine ls` command lists VCHs with their IDs, names, and versions. 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 a VCH. If you have not deployed a VCH, `vic-machine ls` returns an empty list.

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 VCHs 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 VCHs 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-operating_system ls
--target esxi_host_address
--user root
--password esxi_host_password
--thumbprint certificate_thumbprint
```

```
$ vic-machine-operating_system ls
--target vcenter_server_username:password@vcenter_server_address
--thumbprint certificate_thumbprint
```

Result

The `vic-machine ls` command lists the VCHs 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-git_commit   Up to date
vm-102     path     vch_2   vch_version-vch_build-git_commit   Up to date
[...]
vm-n       path     vch_n   vch_version-vch_build-git_commit   Up to date
```

-->

```
ID         PATH     NAME    VERSION
vm-101     path     vch_1   vch_version-vch_build-git_commit
vm-102     path     vch_2   vch_version-vch_build-git_commit
[...]
vm-n       path     vch_n   vch_version-vch_build-git_commit
```

- The IDs are the vSphere Managed Object References, or morefs, for the VCH endpoint VMs. You can use VCH IDs when you run the `vic-machine inspect`, `debug`, and `delete` commands. Using VCH IDs reduces the number of options that you need to specify when you run those commands.
- The `PATH` value depends on where the VCH 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 VCHs are deployed in resource pools on hosts or clusters, the resource pool names appear after `Resources` in the path. You can use the information in `PATH` in the `--compute-resource` option of `vic-machine` commands.
- The `VERSION` value shows the version of `vic-machine` that was used to create the VCH. It includes the release version, the build number and the short Git commit checksum.

Obtain Information About a VCH

You can obtain information about a virtual container host (VCH) 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 VCH.

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 VCH 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 VCH 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 VCH 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-operating_system 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 VCH:

- The VCH ID:

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

  The vSphere Managed Object Reference, or moref, of the VCH. You can use VCH ID when you run the `vic-machine delete` or `debug` commands. Using a VCH 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 VCH that you are inspecting.

  ```
  Installer version: vic_machine_version-vic_machine_build-git_commit
  VCH version: vch_version-vch_build-git_commit
  ```

- The address of the VCH Admin portal for the VCH.

```
VCH Admin Portal:
https://vch_address:2378
```

- The address at which the VCH publishes ports.

```
vch_address
```

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

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

  - VCH with TLS authentication with untrusted self-signed certificates:

```
DOCKER_HOST=vch_address:2376
```

  - VCH with no TLS authentication:

```
DOCKER_HOST=vch_address:2375
```

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

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

  - VCH with TLS authentication with untrusted self-signed certificates:

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

  - VCH with no TLS authentication:

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

Delete a VCH

You delete virtual container hosts (VCHs) 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 VCH Delete Options.

When you delete a VCH that uses TLS authentication with trusted Certificate Authority (CA) certificates, `vic-machine delete` does not delete the certificates or the certificate folder, even if you specify the `--force` option. Because `vic-machine delete` does not delete the certificates, you can delete VCHs and create new ones that reuse the same certificates. This is useful if you have already distributed the client certificates for VCHs that you need to recreate.

Prerequisites

You have deployed a VCH 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 VCH 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 VCH 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 VCH 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-operating_system 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 `docker stop` on the containers and run `vic-machine delete` . Alternatively, run `vic-machine delete` with the `--force` option.

   CAUTION Running `vic-machine delete` with the `--force` option removes all running container VMs that the VCH manages, as well as any associated volumes and volume stores. It is not recommended to use the `--force` option to remove running containers.

   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-operating_system delete
--target vcenter_server_username:password@vcenter_server_address
--name vch_name
--force
```

VCH 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 (VCHs).

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 VCH. Any running container VMs and any volume stores associated with the VCH are deleted. Errors such as an incorrect compute resource still cause the deletion to fail.

- If you do not specify `--force` and the VCH contains running container VMs, the deletion fails with a warning.
- If you do not specify `--force` and the VCH has volume stores, the deletion of the VCH 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 VCH without providing the thumbprint of the vCenter Server or ESXi host in the `--thumbprint` option.

```
--force
```

Find VCH 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 (VCHs) in the vSphere Web Client.

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

Prerequisites

- You deployed a VCH.
- You installed the vSphere Web Client plug-in for vSphere Integrated Containers Engine.
- If you deployed the VCH to a vCenter Server 6.5 instance, use the Flash-based vSphere Web Client to view the vSphere Web Client plug-in for vSphere Integrated Containers Engine. vSphere Integrated Containers Engine does not currently provide a plug-in for the new HTML5 vSphere Client.

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 VCH vApp.
3. Expand the VCH vApp and select the VCH endpoint VM.
4. Click the **Summary** tab for the VCH endpoint VM and scroll down to the VCH portlet.

Result

Information about the VCH appears in the VCH portlet in the **Summary** tab:

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

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 (VCHs).

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

Prerequisites

- You deployed a VCH and pulled and ran at least one container.
- You installed the vSphere Web Client plug-in for vSphere Integrated Containers Engine.
- If you deployed the VCH to a vCenter Server 6.5 instance, use the Flash-based vSphere Web Client to view the vSphere Web Client plug-in for vSphere Integrated Containers Engine. vSphere Integrated Containers Engine does not currently provide a plug-in for the new HTML5 vSphere Client.

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 VCH vApp.
3. Expand the VCH 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.

Access the Administration Portal for a VCH

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

If you deployed the VCH with `--no-tls` or `--no-tlsverify`, you can only log in to VCH Admin by specifying the username and password of the ESXi host or vCenter Server on which you deployed the VCH. If you deployed the VCH with client and server authentication by using `--tls-cname` or by specifying a static IP address on the client network, you can use the generated `*.pfx` certificate to authenticate with the VCH Admin portal. For information about using the `*.pfx` certificate to log into VCH admin, see Browser-Based Certificate Login and Command Line Certificate Login.

Prerequisites

- You deployed a VCH.
- Obtain the address of the VCH:
  - Copy the address from the output of `vic-machine create` or `vic-machine inspect`.
  - If you deployed the VCH 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 VCH to an ESXi host, copy the address from the **Summary** tab for the vSphere Integrated Containers Engine endpoint VM in the desktop vSphere Client.

Procedure

1. Go to https://*vch_address*:2378.

   If prompted about an insecure or not private connection, click Advanced and follow the prompts to proceed to the portal.

2. Enter the username and password for the vCenter Server instance or ESXi host.

Result

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

- Status information about the VCH, registry and Internet connections, firewall configuration, and license. For information about these statuses and how to remedy error states, see the VCH Status Reference.
- The address of the Docker endpoint.
- The system time of the VCH. This is useful to know because clock skews between VCHs and client systems can cause TLS authentication to fail. For information about clock skews, see Connections Fail with Certificate Errors when Using Full TLS Authentication with Trusted Certificates.
- The remaining capacity of the datastore that you designated as the image store. If the VCH is unable to connect to vSphere, the datastore information is not displayed.
- Live logs and log bundles for different aspects of the VCH. For information about the logs, see Access vSphere Integrated Containers Engine Log Bundles.

Browser-Based Certificate Login

If you deployed the VCH with client and server authentication by using `--tls-cname` or by specifying a static IP address on the client network, you can use browser-based certificate authentication to access the VCH Admin Portal. In this way, you do not need to provide the vSphere credentials each time that you log in to VCH Admin.

Prerequisites

- You deployed a VCH with `--tls-cname` or a static IP address for the VCH on the client network.
- Use Firefox. Currently, this feature is only supported with Firefox.
- Locate the file named `cert.pfx` on the system on which you ran `vic-machine create`. The `cert.pfx` is located in either of the following locations:
  - In the folder with the same name as the VCH, in the directory from which you ran `vic-machine create`.
  - In a folder that you specified in the `vic-machine create --cert-path` option.

Procedure

1. In Firefox, select `Tools` > `Options` and select `Advanced`.
2. Click `View Certificates`.
3. Click `Import`.
4. Browse to the `cert.pfx` file and click `Open`.
5. Click `OK`.

   Do not enter a password when prompted.

Result

You see a message stating that the certificate was successfully installed. With the VCH certificate installed in your browser, you can navigate to https://*vch_address*:2378/ or to one of the log pages without having to enter the vSphere credentials.

Command Line Certificate Login

You can use certificate-based authentication with tools such as `curl` or `wget` to access the VCH Admin log server.

With TLS Client Authentication

If you deployed the VCH with client authentication by using `--tls-cname` or by specifying a static IP address on the client network, you can point `curl` to the `cert.pem` and `key.pem` files for the VCH. The following example authenticates connections to the `port-layer.log` file.

```
curl https://vch_address:2378/logs/port-layer.log
--key ./cert_folder/key.pem
--certificate ./cert_folder/cert.pem
```

NOTE: If your certificates are self-signed, you might also need to specify the `curl -k` flag.

In the example above, *cert_folder* is either of the following locations:

- The folder with the same name as the VCH, in the directory from which you ran `vic-machine create`.
- A folder that you specified in the `vic-machine create --cert-path` option.

Without Client Authentication

If you deployed the VCH without client authentication by using either of `--no-tls` or `--no-tlsverify`, you can use curl to access the logs but you must first authenticate connections to VCH Admin by using the vSphere username and password.

1. Log in to VCH Admin to gather an authentication cookie for subsequent access:

   ```
   curl -sk https://vch_address:2378/authentication
   -XPOST -F username=vsphere_username
   -F password=vsphere_password
   -D cookies_file
   ```

2. Use the cookie from Step 1 in a `curl` command to access the logs.

   ```
   curl -sk https://vch_address:2378/logs/port-layer.log
   -b cookies_file
   ```

VCH Admin Status Reference

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

If the vSphere environment in which you are deploying a VCH does not meet the requirements, the deployment does not succeed. However, a successfully deployed VCH can stop functioning if the vSphere environment changes after the deployment. If environment changes adversely affect the VCH, 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 VCH 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 **VCH** status is yellow.
- The **VCH** status is yellow and an error message informs you that the VCH cannot connect to vSphere.

Cause

- One or more of the VCH processes is not running correctly, or the VCH is unable to connect to vSphere.
- The management network connection is down and the VCH endpoint VM cannot connect to vSphere.

Solution

1. (Optional) If you see the error that the VCH is unable to connect to vSphere, check the VCH management network.
2. In the VCH Admin portal for the VCH, click the link for the **VCH Admin Server** log.
3. Search the log for references to the different VCH processes.

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

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

Registry and Internet Connectivity

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

Error

The **Registry and Internet Connectivity** status is yellow.

Cause

The public network connection is down.

Solution

Check the **VCH Admin Server** log for references to network issues. Use the vSphere Web Client to remediate the management network issues as required.

Firewall

VCH Admin checks that the firewall is correctly configured on an ESXi host on which the VCH is running. If the VCH is running in a cluster, VCH Admin checks the firewall configuration on all of the hosts in the cluster.

Error

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

Cause

- The management network connection is down and the VCH endpoint VM cannot connect to vSphere.
- The firewall on the ESXi host on which the VCH is running no longer allows outbound connections on port 2377.
  - The firewall was switched off when the VCH was deployed. The firewall has been switched on since the deployment of the VCH.
  - 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 VCH. Firewall rulesets are not retained when an ESXi host reboots.

Solution

- If the **Firewall** status is unavailable:
  - Check the **VCH Admin Server** log for references to network issues.
  - Use the vSphere Web Client to remediate the management network issues as required.
- If you see the error about port 2377, 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*.

License

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

Error

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

Cause

- The license for the ESXi host or for one or more of the hosts in a vCenter Server cluster on which the VCH is deployed has been removed, downgraded, or has expired since the deployment of the VCH.
- The management network is down, or the VCH endpoint VM is unable to connect to vSphere.

Solution

- If the license does not meet the requirements:
  - If the VCH 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 VCH is running on a standalone ESXi host in vCenter Server, replace the ESXi host license with a valid vSphere Enterprise Plus license.
  - If the VCH 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.
- If the **License** status is unavailable:
  - Check the **VCH Admin Server** log for references to network issues.
  - Use the vSphere Web Client to remediate the management network issues as required.

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

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

If the VCH is unable to connect to vSphere, logs that require a vSphere connection are disabled, and you see an error message. You can download the log bundle to troubleshoot the error.

- The **Log Bundle** contains logs that relate specifically to the VCH that you created.
- The **Log Bundle with container logs** contains the logs for the VCH and also includes the logs regarding the containers that the VCH 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 other components
      - Reports component failures and restart counts
      ```

      At higher debug levels, the component output is duplicated in the log files for those components, so `init.log` includes a superset of the log data.

      Note: This log file is duplicated on the datastore in a file in the endpoint VM folder named `tether.debug`, to allow the debugging of early stage initialization and network configuration issues.

    - **Admin Server** includes logs for the VCH 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 information about current commands and changes as you make them. For example, when you are troubleshooting an issue, you can see whether your command 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 resolve issues.

Logs also include vic-machine commands used during VCH installation to help you resolve issues.

Collecting Logs Manually

If the VCH Admin portal is offline, use `vic-machine debug` to enable SSH on the VCH and use `scp -r` to capture the logs from `/var/log/vic/`.

Setting the Log Size Cap

The log size cap is set at 20MB. If the size exceeds 20 MB, then vSphere Integrated Containers Engine compresses the files and saves a history of the last two rotations. These files are rotated:

`/var/log/vic/port-layer.log`

`/var/log/vic/init.log`

`/var/log/vic/docker-personality.log`

`/var/log/vic/vicadmin.log`

Debugging the VCH

By default, all shell access to the virtual container host (VCH) endpoint VM is disabled. Login shells for all users are set to `/bin/false`. The command line utility for vSphere Integrated Containers Engine, `vic-machine`, provides a `debug` command that allows you to enable shell access to the virtual container host (VCH) endpoint VM, either by using the VM console or via SSH.

Do not confuse the `vic-machine debug` command with the `vic-machine create --debug` option. The `vic-machine debug` command allows you to log into and debug a VCH endpoint VM that you have already deployed. The `vic-machine create --debug` option deploys a new VCH that has increased levels of logging and other modifications, to allow you to debug the environment in which you deploy VCHs. For information about the `vic-machine create --debug` option, see the section on `--debug` in VCH Deployment Options in *vSphere Integrated Containers Engine Installation*.

- Enable Shell Access to the VCH Endpoint VM
- Authorize SSH Access to the VCH Endpoint VM
- VCH Debug Options

Enable shell access to the VCH Endpoint VM

You can use the `vic-machine debug` command to enable shell access to a VCH endpoint VM by setting a root password on the VM. Setting a root password enables access to the VCH endpoint VM via the VM console only. If you require SSH access to the VCH endoint VM, rather than just shell access, see Authorize SSH Access to the VCH Endpoint VM.

IMPORTANT: Any changes that you make to a VCH by using `vic-machine debug` are non-persistent and are discarded if the VCH endpoint VM reboots.

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

Prerequisites

You deployed a VCH.

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.
   - Specify the vSphere target and its credentials, either in the `--target` option or separately in the `--user` and `--password` options.

     The credentials that you provide must have the following privilege on the endpoint VM:

     ```
     Virtual machine.Guest Operations.Guest Operation Program Execution
     ```

   - Specify the ID or name of the VCH to debug.
   - Potentially provide the thumbprint of the vCenter Server or ESXi host certificate.
   - Provide a password for the root user on the VCH endpoint VM by specifying the `--rootpw` option. Wrap the password in single quotes (Linux or Mac OS) or double quotes (Windows) if it includes shell characters such as `$` , `!` or `%` .

     ```
     $ vic-machine-operating_system debug
     --target vcenter_server_or_esxi_host_address
     --user vcenter_server_or_esxi_host_username
     --password vcenter_server_or_esxi_host_password
     --id vch_id
     --thumbprint certificate_thumbprint
     --rootpw 'new_p@ssword'
     ```

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
```

Authorize SSH Access to the VCH Endpoint VM

You can use the `vic-machine debug` command to enable shell access to a VCH endpoint VM by setting a root password on the VM. Setting a root password enables access to the VCH endpoint VM via the VM console. You can also use `debug` to authorize SSH access to the VCH endpoint VM. You can optionally upload a key file for public key authentication when accessing the endpoint VM by using SSH.

IMPORTANT: Any changes that you make to a VCH by using `vic-machine debug` are non-persistent and are discarded if the VCH endpoint VM reboots.

Prerequisites

You deployed a VCH.

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.
   - Specify the vSphere target and its credentials, either in the `--target` option or separately in the `--user` and `--password` options.

     The credentials that you provide must have the following privilege on the endpoint VM:

     ```
     Virtual machine.Guest Operations.Guest Operation Program Execution
     ```

     - Specify the ID or name of the VCH to debug.
     - Potentially provide the thumbprint of the vCenter Server or ESXi host certificate.
     - Specify the `--rootpw` option. Wrap the password in single quotes (Linux or Mac OS) or double quotes (Windows) if it includes shell characters such as `$`, `!` or `%`.
     - Authorize SSH access by specifying `--enable-ssh`.
     - 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-operating_system debug
     --target vcenter_server_or_esxi_host_address
     --user vcenter_server_or_esxi_host_username
     --password vcenter_server_or_esxi_host_password
     --id vch_id
     --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
```

VCH 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 (VCH) 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 VCH 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 VCH 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 VCH endpoint VM. The `sshd` service runs until the VCH 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 VCH endpoint VM.

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

Wrap the password in single quotes (Linux or Mac OS) or double quotes (Windows) if it includes shell characters such as `$`, `!` or `%`.

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

`--authorized-key`

Short name: `--key`

Upload a public key file to `/root/.ssh/authorized_keys` to enable SSH key authentication for the `root` user. Include the name of the `*.pub` file in the path.

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

Deleting or Inspecting a VCH Fails with a Not a VCH or Resource Pool Not Found Error

When you use `vic-machine delete` or `vic-machine inspect` to delete or inspect a virtual container host (VCH) and you specify the address of an ESXi host in the `target` option, the operation fails with "an error stating that the target is not a VCH or that the resource pool cannot be found".

Problem

Deleting or inspecting a VCH fails with one of the following error messages:

```
### Inspecting VCH ####
Not a VCH
Failed to get Virtual Container Host vch_name
Not a VCH
--------------------
vic-machine-os failed: inspect failed
```

```
### Inspecting VCH ####
Failed to get VCH resource pool "path_to_resource_pool":
resource pool 'path_to_resource_pool' not found
Failed to get Virtual Container Host vch_name
resource pool 'path_to_resource_pool' not found
--------------------
vic-machine-os failed: inspect failed
```

```
### Removing VCH ####
Not a VCH
Failed to get Virtual Container Host vch_name
Not a VCH
--------------------
vic-machine-os failed: delete failed
```

```
### Removing VCH ####
Failed to get VCH resource pool "path_to_resource_pool":
resource pool 'path_to_resource_pool' not found
Failed to get Virtual Container Host vch_name
resource pool 'path_to_resource_pool' not found
--------------------
vic-machine-os failed: delete failed
```

Cause

You set the `target` option to the address of an ESXi host that is managed by a vCenter Server instance. If there are multiple ESXi hosts in a cluster, the error that you see depends on the host that you specify in the `target` option.

- If you set the `target` option to the ESXi host on which the VCH is running, you see the error `Not a VCH, Failed to get Virtual Container Host`.
- If you set the `target` option to an ESXi host in the cluster that is not the one on which the VCH is running, you see the error `Not a VCH, Failed to get VCH resource pool`.

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 (VCH) that uses full TLS authentication with trusted Certificate Authority (CA) certificates fail with certificate errors.

Problem

- `vic-machine` operations on a VCH 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
  ```

  NOTE: `vic-machine` tolerates a 1 day skew. A skew of 1 day might result in a different certificate error than time skew.
- Connections to the VCH Admin portal for the VCH fail with an `ERR_CERT_DATE_INVALID` error.
- Connections to the VCH from Docker clients fail with a `bad certificate` error.

Cause

There is potentially a clock skew between the VCH and the system from which you are connecting to the VCH.

Solution

1. Go to the VCH Admin portal for the VCH at https://*vch_address*:2378 and check the System Time under **VCH Info**.
2. If the system time of the VCH is wrong, run `vic-machine debug` to enable SSH access to the VCH.

   For information about enabling SSH on a VCH, see Authorize SSH Access to the VCH Endpoint VM.
3. Connect to the VCH endpoit VM by using SSH.
4. Use the `date --set` Linux command to set the system clock to the correct date and time.

   The two most common date formats are the following:

   - Unix Time Stamp: `date --set='@1480969133'`
   - `YYYYMMDD HH:MM` format: `date --set="20161205 14:31"`

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

Send Documentation Feedback

Help us to improve the vSphere Integrated Containers documentation.

- Send doc feedback to VMware
- Submit a doc issue in Github