VMware vSphere Integrated Containers for Dev Ops Administrators

vSphere Integrated Containers 1.1

vmware

Table of Contents

DevOps Administrators

vSphere Integrated Containers for DevOps Administrators

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

Product version: 1.1

Intended Audience

This information is intended for DevOps administrators who want to use vSphere Integrated Containers Registry to create and manage development projects, assign developers to projects, set up access to virtual container hosts (VCHs), and manage registries of container images. DevOps administrators use vSphere Integrated Containers Management Portal to provision and manage containers and to manage the lifecycle of VCHs. Knowledge of container technology and Docker is useful.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304

www.vmware.com

Overview of vSphere Integrated Containers For DevOps Administrators

vSphere Integrated Containers integrates of all the packaging and runtime benefits of containers with the enterprise capabilities of a vSphere environment. As a DevOps admin, you use vSphere Integrated Containers Registry to manage container images and you use vSphere Integrated Containers Management Portal to deploy and managing container-based applications.

- vSphere Integrated Containers Registry is an enterprise-class registry server that you can use to store and distribute container images. vSphere Integrated Containers Registry allows DevOps administrators to organize image repositories in projects, and to set up role-based access control to those projects to define which users can access which repositories. vSphere Integrated Containers Registry also provides rule-based replication of images between registries, implements Docker Content Trust, and provides detailed logging for project and user auditing.
- vSphere Integrated Containers Management Portal is a highly scalable and very lightweight container management platform for deploying and managing container based applications. It is designed to have a small footprint and boot extremely quickly. vSphere Integrated Containers Management Portal is intended to provide DevOps administrators with automated deployment and lifecycle management of containers, including the following services:
    - Rule-based resource management, allowing DevOps administrators to set deployment preferences which let vSphere Integrated Containers Management Portal manage container placement.
    - Live state updates that provide a live view of the container system.
    - Multi-container template management, that enables logical multi-container application deployments.

The information in this topic is intended for DevOps administrators. For an extended version of this information, see Overview of vSphere Integrated Containers for vSphere Administrators in *vSphere Integrated Containers for vSphere Administrators*.

Differences Between vSphere Integrated Containers and a Classic Container Environment

The main differences between vSphere Integrated Containers and a classic container environment are the following:

- vSphere, not Linux, is the container host:
    - Containers are spun up *as* VMs, not *in* VMs.
    - Every container is fully isolated from the host and from the other containers.
    - vSphere provides per-tenant dynamic resource limits within a vCenter Server cluster
- vSphere, not Linux, is the infrastructure:
    - You can select vSphere networks that appear in the Docker client as container networks.
    - Images, volumes, and container state are provisioned directly to VMFS.
- vSphere is the control plane:
    - Use the Docker client to directly control selected elements of vSphere infrastructure.
    - Acontainer endpoint Service-as-a-Service presents as a service abstraction, not as IaaS

What Does vSphere Integrated Containers Do?

vSphere Integrated Containers allows a DevOps administrator or the vSphere administrator to easily make the vSphere infrastructure accessible to container application developers, so that you can provision container workloads into production.

Scenario 1: A Classic Container Environment

In a classic container environment:

- A user raise a ticket and say, "I need Docker".
- The vSphere administrator provisions a large Linux VM and sends you the IP address.
- You install Docker, patch the OS, configure in-guest network and storage virtualization, secure the guest, isolate the containers, package the containers efficiently, and manage upgrades and downtime.

In this scenario, what the vSphere administrator has given you is similar to a nested hypervisor that you have to manage and which is opaque to them.

Scenario 2: vSphere Integrated Containers

With vSphere Integrated Containers:

- A user raises a ticket and say, "I need Docker".
- The vSphere administrator identifies datastores, networking, and compute on a cluster that they can use in the Docker environment.
- The vSphere administrator uses a utility called `vic-machine` to install a small appliance, called a virtual container host (VCH). The VCH represents an authorization for users to use the infrastructure that the vSphere administrator has identified, into which they can self-provision container workloads.
- The appliance runs a secure remote Docker API, that is the only access that users have to the vSphere infrastructure.
- Instead of sending the users a Linux VM, the vSphere administrator sends them the IP address of the appliance, the port of the remote Docker API, and a certificate for secure access.

What Is vSphere Integrated Containers Engine?

The objective of vSphere Integrated Containers Engine is to take as much of vSphere as possible and layer whatever Docker capabilities are missing on top, reusing as much of Docker's own code as possible. The result should not sacrifice the portability of the Docker image format and should be completely transparent to a Docker client. The following sections describe key concepts and components that make this possible.

Container VMs

The container VMs that vSphere Integrated Containers Engine creates have all of the characteristics of software containers:

- An ephemeral storage layer with optionally attached persistent volumes.
- A custom Linux guest OS that is designed to be "just a kernel" and that needs images to be functional.
- A mechanism for persisting and attaching read-only binary image layers.
- A PID 1 guest agent *tether* extends the control plane into the container VM.
- Various well-defined methods of configuration and state ingress and egress
- Automatically configured to various network topologies.

The provisioned container VM does not contain any OS container abstraction.

- The container VM boots from an ISO that contains the Photon Linux kernel. Note that container VMs do not run the full Photon OS.
- The container VM is configured with a container image that is mounted as a disk.
- Container image layers are represented as a read-only VMDK snapshot hierarchy on a vSphere datastore. At the top of this hierarchy is a read-write snapshot that stores ephemeral state.
- Container volumes are formatted VMDKs that are attached as disks and indexed on a datastore.
- Networks are distributed port groups that are attached as vNICs.

Virtual Container Hosts

A virtual container host (VCH) is the functional equivalent of a Linux VM that runs Docker, but with some significant benefits. A VCH represents the following elements:

- A clustered pool of resource into which to provision container VMs.
- A single-tenant container namespace.
- A secure API endpoint.
- Authorization to use and configure pre-approved virtual infrastructure.

AVCH is functionally distinct from a traditional container host in the following ways:

- It naturally encapsulates clustering and dynamic scheduling by provisioning to vSphere targets.
- The resource constraints are dynamically configurable with no impact on the containers.
- Containers do not share a kernel.
- There is no local image cache. This is kept on a datastore in the cluster that the vSphere administrator specified when they deployed a VCH.
- There is no read-write shared storage

Managing Images, Projects, and Users with vSphere Integrated Containers Registry

vSphere Integrated Containers Registry is an enterprise-class registry server that you can use to store and distribute container images. vSphere Integrated Containers Registry extends the open source Docker Distribution project by adding the features that enterprise users require, such as user management, access control, and activity auditing. You can improve image transfer efficiency by deploying vSphere Integrated Containers Registry alongside vSphere Integrated Containers Engine, so that your registry is located close to the build and run environment.

The sections below present the key features of vSphere Integrated Containers Registry.

- Projects and Role-Based Access Control
- User Authentication
- Rule-Based Image Replication
- Docker Content Trust
- Garbage Collection
- Logging

Projects and Role-Based Access Control

In vSphere Integrated Containers Registry, you organize repositories in projects. "Repository" is Docker terminology for a collection of container images that have the same name but that have different tags. You assign users to the projects and you assign roles with different permissions to the users in each project. There are two types of project in vSphere Integrated Containers Registry:

- **Public projects**: All users can pull images from the project. Users must be members of a project and have the appropriate privileges to push images to the project.
- **Private projects**: Only members of the project can pull images from private private projects. Members must have the appropriate privileges to be able to push images to the project.

When you first deploy vSphere Integrated Containers Registry, a default public project named `library` is created. You can toggle projects from public to private, or the reverse, at any moment.

For information about projects, see Create a Project, Assign Users to a Project, Manage Project Members, and Manage Projects.

User Authentication

You can configure vSphere Integrated Containers Registry to use an existing LDAP or Active Domain service, or use local user management to authenticate and manage users.

Local User Management

You create user and manage user accounts locally in vSphere Integrated Containers Registry. User information is stored in a database that is embedded in vSphere Integrated Containers Registry. When you first deploy vSphere Integrated Containers Registry, the registry uses local user management by default. For information about creating local user accounts, see Create Users.

LDAP Authentication

Immediately after you deploy vSphere Integrated Containers Registry, can you configure the registry to use an external LDAP or Active Directory server to authenticate users. If you implement LDAP authentication, users whose credentials are stored by the external LDAP or Active Directory server can log in to vSphere Integrated Containers Registry directly. In this case, you do not need to create user accounts locally.

IMPORTANT: The option to switch from local user management to LDAP authentication is only available while the local database is empty. If you start to populate the database with users and projects, the option to switch to LDAP authentication is disabled. If you want to implement LDAP authentication, you must enable this option when you first log in to a new registry instance.

For information about enabling LDAP authentication, see Configure a Registry.

Rule Based Image Replication

You can set up multiple registries and replicate images between registry instances. Replicating images between registries helps with load balancing and high availability, and allows you to create multi-datacenter, hybrid, and multi-cloud setups. For information about image replication, see Replicating Images.

Docker Content Trust

vSphere Integrated Containers Registry provides a Docker Notary server that allows you to implement Docker Content Trust by signing and verifying the images in the registry. For information about Docker Notary, see Content trust in Docker in the Docker documentation.

The Notary server runs by default. For information about how container developers use Docker Content Trust with vSphere Integrated Containers Registry, see Configure the Docker Client for Use with vSphere Integrated Containers in *Developing Container Applications with vSphere Integrated Containers*.

Garbage Collection

You can configure vSphere Integrated Containers Registry to perform garbage collection whenever you restart the registry service. If you implement garbage collection, the registry recycles the storage space that is consumed by images that you have deleted. For more information about garbage collection, see Manage Repositories. See also Garbage Collection in the Docker documentation.

Logging

vSphere Integrated Containers Registry keeps a log of every operation that users perform in a project. The logs are fully searchable, to assist you with activity auditing. For information about project logs, see Access Project Logs.

Configure a Registry

When you first log in to a new vSphere Integrated Containers Registry instance, you can optionally configure the registry to implement authentication of users by using an LDAP or Active Directory service. You can define who can create projects or register as users, implement certificate verification for image replications, set up a mail server, and set the period of validity for login sessions.

IMPORTANT: The option to switch from local user management that uses a database to LDAP authentication is only available while the local database is empty. If you start to populate the database with users and projects, the option to switch to LDAP authentication is disabled. If you want to implement LDAP authentication, you must enable this option when you first log in to a new registry instance, before you create any projects or users.

With the exception of changing the authentication mode after you have already created projects or users, you can change any of the other settings at any time after the initial configuration.

Prerequisites

The vSphere administrator enabled vSphere Integrated Containers Registry when they deployed the vSphere Integrated Containers appliance.

Procedure

1. Log in as `admin` user to the vSphere Integrated Containers Registry interface at https://*vic_appliance_address*:443.

   If you configured the vSphere Integrated Containers appliance to use a different port for vSphere Integrated Containers Registry, replace 443 with the appropriate port.

2. Expand **Administration** on the left, select **Configuration** > **Authentication**, and set the **Auth Mode**.

   - To use local user management, leave **Auth Mode** set to **Database**.
   - To implement LDAP or Active Directory authentication, select **LDAP**.

3. If you selected LDAP authentication, fill in the details of your LDAP or Active Directory service, click **Test LDAP Server**, and click **Save** if the test is successful.

4. Use the **Project Creation** drop-down menu to set which users can create projects.

   - Select **Everyone** to allow all users to create projects
   - Select **Admin Only** to allow only users with the Administrator role to create projects

5. If you selected **Database** authentication, optionally uncheck the **Allow Self-Registration** checkbox.

   This option is not available if you use LDAP authentication. If you leave this option enabled, a link that allows unregistered users to sign up for an account appears on the vSphere Integrated Containers Registry login page. When self-registration is disabled, the link does not appear on the login page, and only users with the Administrator role can register new users.

6. Click **Save** to save the authentication settings.

7. Click **Replication**, and optionally uncheck the **Verify Remote Cert** checkbox to disable verification of replication endpoint certificates.

   You must disable certificate verification if the remote registry uses a self-signed or an untrusted certificate. For example, disable certificate verification if the registry uses the default auto-generated certificates that vSphere Integrated Containers Registry created during the deployment of the vSphere Integrated Containers appliance.

8. Click **Email** to set up a mail server, test the settings, and click **Save**.

   The mail server is used to send responses to users who request to reset their password.

9. Click **System Settings** to change the length of login sessions from the default of 30 minutes, and click **Save**.

What to Do Next

If you use local user management, create users. If you use either LDAP authentication or local user management, create projects and assign users to those projects.

Create Users in vSphere Integrated Containers Registry

If you configured vSphere Integrated Containers Registry to use local user management rather than LDAP authentication, you must create user accounts before you can assign users to projects.

If the registry uses LDAP authentication, you cannot create or register new users in the registry. The LDAP server manages users externally. However, users must log in at least once with their LDAP credentials in order to be added to the registry account system. After a user has logged in once, you can assign that user to projects.

Procedure

1. Log in to the vSphere Integrated Containers Registry interface at https://*vic_appliance_address*:443.

   Use the `admin` account, or an account with Administrator privileges. If the vSphere Integrated Containers appliance uses a different port for vSphere Integrated Containers Registry, replace 443 with the appropriate port.

2. Expand **Administration** on the left, click **Users**, then click the **+ Users** button.
3. Enter a user name, email address, and the user's full name.

   The user name and email address must be unique in this registry instance. The email address and the user's full name are for use in email responses to password reset requests.

4. Enter and confirm a password for the user.

   The password must contain at least 8 characters, with 1 lower case letter, 1 upper case letter, and 1 numeric character. Special characters are not currently permitted. If the passwords do not match or if they do not meet the password criteria, the **OK** button remains deactivated.

5. When you have completed all of the required fields correctly, click **OK**.

What to Do Next

Create projects and assign the users to those projects.

Assign the System-Wide Administrator Role to Users

You can assign the system-wide administrator role to any user. Users with the administrator role have extra permissions in addition to their project-specific privileges.

- Browse and manage all projects
- Register new users
- Assign the administrator role to other users
- Delete users
- Manage replication rules in a project
- Perform system-wide configuration

The administrator role owns the default public project named `library`.

Prerequisites

You have created at least one user.

Procedure

1. Log in to the vSphere Integrated Containers Registry interface at https://*vic_appliance_address*:443.

   Use the `admin` account, or an account with Administrator privileges. If the vSphere Integrated Containers appliance uses a different port for vSphere Integrated Containers Registry, replace 443 with the appropriate port.

2. Expand **Administration** on the left, and click **Users**.
3. In the list of users, click the 3 vertical dots next to a user name and select **Set as Administrator**.
4. To remove the administrator role from a user, click the 3 vertical dots next to a user name and select **Revoke Administrator**.

Create a Project in vSphere Integrated Containers Registry

In vSphere Integrated Containers Registry, you group container image repositories in projects. A project contains all of the repositories that an application requires. You cannot push images to vSphere Integrated Containers Registry until you have created a project.

NOTE: The current version of vSphere Integrated Containers Engine does not support `docker push`. To push images to vSphere Integrated Containers Registry, use a regular Docker client. You can then pull the images from the registry to a vSphere Integrated Containers Engine virtual container host (VCH).

Procedure

1. Log in to the vSphere Integrated Containers Registry interface at https://*vic_appliance_address*:443.

   If the registry is configured so that only administrators can create projects, use the `admin` account, or an account with Administrator privileges. If the vSphere Integrated Containers appliance uses a different port for vSphere Integrated Containers Registry, replace 443 with the appropriate port.

2. Click **Projects** on the left, then click the **+ Project** button.
3. Provide a name for the project.
4. (Optional) Check the **Public** check box to make the project public.

   If you set the project to **Public**, any user can pull images from this project. If you leave the project set to **Private**, only users who are members of the project can pull images. You can toggle projects from public to private, or the reverse, at any moment after you create the project.

5. Click **OK**.

Result

When you create a new project, you are automatically assigned the Project Admin role for that project.

The project is added to the list of projects. You can browse existing projects by limiting the list to only display public projects, or filter the list by entering text in the **Filter** text box.

What to Do Next

You can add users to the project, push images to the project, browse the repositories that the project contains, view the project logs, and set up image replication.

Assign Users to a Project

To be able to pull images from a private vSphere Integrated Containers Registry project, a user must be a member of that project. In the case of public projects, any user can pull images from the project, but only members of the project with at least Developer privileges can push images to the project.

Prerequisites

You have a created project. If the registry uses local user management, there must be at least one user in the system in addition to the user who created the project.

Procedure

1. Log in to the vSphere Integrated Containers Registry interface at https://*vic_appliance_address*:443.

   Use the `admin` account, an account with the system-wide Administrator role, or an account that has the Project Admin role for this project. If the vSphere Integrated Containers appliance uses a different port for vSphere Integrated Containers Registry, replace 443 with the appropriate port.

2. Click **Projects** on the left and click the name of a project in the project list.
3. Click **Members**, then click the **+ Member** button to add users to the project.
4. Enter the user name for an existing user account, and select a role for the user in this project.
   - **Project Admin**: Read and write privileges for the project, with management privileges such as adding and removing members.
   - **Developer**: Can pull images from and push images to the project.
   - **Guest**: Can pull images from the project, but cannot push images to the project.
5. Click **OK**.

Manage Project Members

After you have added members to a project, you can change existing project members' roles or remove members from the project.

Prerequisites

You have a created project and assigned users to it.

Procedure

1. Log in to the vSphere Integrated Containers Registry interface at https://*vic_appliance_address*:443.

   Use the `admin` account, an account with the system-wide Administrator role, or an account that has the Project Admin role for this project. If the vSphere Integrated Containers appliance uses a different port for vSphere Integrated Containers Registry, replace 443 with the appropriate port.

2. Click **Projects** on the left, click a project name, and click **Members**.
3. In the list of project members, click the 3 vertical dots next to a user name and select an option.
   - To assign the member to a different role in the project, select **Project Admin**, **Developer**, or **Guest**.
   - To remove the member from the project, select **Delete**.

Manage Projects

After you have created a project, you can toggle the project between the public and private states. When you no longer require a project, you can delete it.

Prerequisites

You have a created project.

Procedure

1. Log in to the vSphere Integrated Containers Registry interface at https://*vic_appliance_address*:443.

   Use the `admin` account, an account with the system-wide Administrator role, or an account that has the Project Admin role for this project. If the vSphere Integrated Containers appliance uses a different port for vSphere Integrated Containers Registry, replace 443 with the appropriate port.

2. Click **Projects** on the left.
3. In the list of projects, click the 3 vertical dots next to a project name and select an option.
   - If the project is public, select **Make private** to change the project state to private.
   - If the project is private, select **Make public** to change the project state to public.
   - To delete the project, select **Delete**.

Access and Search Project Logs

vSphere Integrated Containers keeps a log of all of the operations that users perform in a project. You can apply filters to help you to search the logs.

Prerequisites

You have a created project.

Procedure

1. Log in to the vSphere Integrated Containers Registry interface at https://*vic_appliance_address*:443.
2. Click **Projects** on the left, click a project name, and click **Logs**.

   The Logs view lists all of the operations that users have performed on this project.
3. To see a reduced list of operations, enter text in the **Filter Logs** text box.

   For example, enter the name of a user, repository, or image tag.
4. To filter by the type of operation, click **Advanced** > **Operations** and select or deselect operation types.
5. To filter by date, enter start and end dates in the format `m/d/yyyy`.

Manage Repositories in vSphere Integrated Containers Registry

You can access the list of repositories that users have pushed to a project. You can browse repositories to see the different tags applied to images in the repository. You can also delete a repository or a tag in a repository.

Deleting a repository involves two steps. First, you delete a repository in vSphere Integrated Containers Registry interface. This is known as soft deletion. You can delete the entire repository or just one tag in the repository. After a soft deletion, the registry no longer manages the repository. However, the repository files remain in the registry storage until you run garbage collection by restarting the registry.

Prerequisites

You have created a project and pushed at least one repository to the project.

Procedure

1. Log in to the vSphere Integrated Containers Registry interface at https://*vic_appliance_address*:443.

   Use the `admin` account, an account with the system-wide Administrator role, or an account that has the Project Admin role for this project. If the vSphere Integrated Containers appliance uses a different port for vSphere Integrated Containers Registry, replace 443 with the appropriate port.

2. Click **Projects** on the left and click the name of a project in the project list.

   All of the repositories for this project appear under Repositories. You can see the number of tags that the repository contains, and how many times that users have pulled the repository.

3. (Optional) To delete a repository, click the 3 vertical dots next to a repository name and select **Delete**.

   CAUTION: If two tags refer to the same image, if you delete one tag, the other tag is also deleted.

4. Click a repository name to view its contents.

What to Do Next

If you deleted respositories, and if the registry is configured with garbage collection enabled, restart the registry. vSphere Integrated Containers Registry will perform garbage collection when it reboots. For information about restarting the registry, see Restart the vSphere Integrated Containers Services in *vSphere Integrated Containers for vSphere Administrators*.

Replicating Images with vSphere Integrated Containers Registry

You can replicate images between vSphere Integrated Containers Registry instances. You can use image replication to transfer images from one data center to another, or to transfer them from an on-premises registry to a registry instance in the cloud.

To set up image replication between registry instances, you create replication endpoints and replication rules. vSphere Integrated Containers Registry performs image replication at the project level. When you set a replication rule on a project, all of the image repositories in that project replicate to the remote replication endpoint that you designate in the rule. vSphere Integrated Containers Registry schedules a replication job for each repository.

IMPORTANT: vSphere Integrated Containers Registry only replicates image repositories. It does not replicate users, roles, replication rules, or any other information that does not relate to images. Each vSphere Integrated Containers Registry instance manages its own user, role, and rule information.

- Create Replication Endpoints
- Create Replication Rules
- Manage Replication Endpoints and Rules

Create Replication Endpoints

To replicate image repositories from one instance of vSphere Integrated Containers Registry to another, you first create replication endpoints. A replication endpoint is a remote registry to which you replicate the images that a project contains.

You can create replication endpoints independently of projects, or you can create new endpoints when you create replication rule for a project. This procedure describes how to create endpoints independently of projects.

Prerequisites

- You deployed at least two instances of vSphere Integrated Containers Registry.
- If the remote registry that you intend to use as the endpoint uses a self-signed or an untrusted certificate, you must disable certificate verification on the registry from which you are replicating. For example, disable certificate verification if the endpoint registry uses the default auto-generated certificates that vSphere Integrated Containers Registry created during the deployment of the vSphere Integrated Containers appliance. For information about disabling certificate verification, see Configure a Registry.

Procedure

1. Log in to the vSphere Integrated Containers Registry instance to use as the source registry for replications.

   Log in at https://*vic_appliance_address*:443. Use the `admin` account, or an account with Administrator privileges. If the vSphere Integrated Containers appliance uses a different port for vSphere Integrated Containers Registry, replace 443 with the appropriate port.

2. Expand **Administration** on the left, click **Replication**, then click the **+ Endpoint** button.
3. Enter a suitable name for the new replication endpoint.
4. Enter the full URL of the vSphere Integrated Containers Registry instance to set up as a replication endpoint.

   For example, https://*registry_address*:443.

5. Enter the user name and password for the endpoint registry instance.

   Use the `admin` account for that vSphere Integrated Containers Registry instance, an account with Administrator privileges on that instance, or an account that has write permission on the corresponding project in the endpoint registry.

6. Click **Test Connection**.
7. When you have successfully tested the connection, click **OK**.

Result

The endpoint registry that you created is available for selection when you create replication rules for projects.

What to Do Next

Create a replication rule for a project.

Create Replication Rules

You replicate image repositories between vSphere Integrated Containers Registry instances by creating replication rules for projects. A replication rule identifies an endpoint registry to which to replicate images.

- When you first enable a replication rule, all of the images in the project replicate to the endpoint registry.
- If the project does not already exist on the remote registry, the rule creates a new project automatically.
- After the initial synchronization between the registries, images that users push to the project on the source registry replicate incrementally to the endpoint registry.
- If users delete images from the source registry, the replication rule deletes the image from the endpoint registry.
- Replication rules are unidirectional. To establish two-way replication, so that users can push images to either project and keep the projects in sync, you must create replication rules in both registry instances.

Prerequisites

- You have two vSphere Integrated Containers Registry instances, one that contains the images to replicate and one to act as the replication endpoint registry.
- You created at least one project, and pushed at least one image to that project.
- If the remote registry that you intend to use as the endpoint uses a self-signed or an untrusted certificate, you must disable certificate verification on the registry from which you are replicating. For example, disable certificate verification if the endpoint registry uses the default auto-generated certificates that vSphere Integrated Containers Registry created during the deployment of the vSphere Integrated Containers appliance. For information about disabling certificate verification, see Configure a Registry.

Procedure

1. Log in to the vSphere Integrated Containers Registry instance that contains the images to replicate.

   Log in at https://*vic_appliance_address*:443. Use the `admin` account, or an account with Administrator privileges. If the vSphere Integrated Containers appliance uses a different port for vSphere Integrated Containers Registry, replace 443 with the appropriate port.

2. Click **Projects** on the left and click the name of the project to replicate.
3. Click **Replication**, then click the **+ Replication Rule** button.
4. Enter a suitable name for the new replication rule and optionally add a description.
5. Select or create an endpoint registry.
   - To select an existing endpoint registry, select an endpoint from the **Endpoint Name** drop-down menu.

     When you select an existing endpoint registry, the URL, user name and password are filled in automatically. If only one endpoint registry exists in the system, it is selected automatically.

   - To create a new endpoint, check the **New Endpoint** check box.

     i. Enter a suitable name for the new replication endpoint.
     ii. Enter the full URL of the vSphere Integrated Containers Registry instance to set up as a replication endpoint.

     For example, https://*registry_address*:443.

     iii. Enter the user name and password for the endpoint registry instance.

     Use the `admin` account for that vSphere Integrated Containers Registry instance, an account with Administrator privileges on that instance, or an account that has write permission on the corresponding project in the endpoint registry. If the project already exists and the replication user that you configure in the rule does not have write privileges in the target project, the replication fails.

6. Click **Test Connection**.
7. When you have successfully tested the connection, optionally check the **Enable** checkbox, and click **OK**.

   If you select **Enable**, replication starts immediately. You can track the progress of the replication in the list of **Replication Jobs**.

8. Click the icon in the **Logs** column for the replication job to check that replication succeeded without errors.

Result

Depending on the size of the images and the speed of the network connection, replication might take some time to complete. An image is not available in the endpoint registry until all of its layers have been synchronized from the source registry. If a replication job fails due to a network issue, vSphere Integrated Containers Registry reschedules the job to retry it a few minutes later.

Manage Replication Endpoints and Rules

You can list, add, edit and delete replication endpoints and replication rules, depending on certain circumstances.

- You cannot edit or delete replication endpoints that are the targets for replication rules.
- You cannot edit replication rules that are enabled.
- You cannot delete replication rules that have running jobs. If a rule is disabled, the running jobs under it will be stopped.

Prerequisites

- You deployed at least two instances of vSphere Integrated Containers Registry.
- You created at least one replication endpoint.
- You created at least one replication rule.

Procedure

1. Log in to the vSphere Integrated Containers Registry instance to use as the source registry for replications.

   Log in at https://*vic_appliance_address*:443. Use the `admin` account, or an account with Administrator privileges. If the vSphere Integrated Containers appliance uses a different port for vSphere Integrated Containers Registry, replace 443 with the appropriate port.

2. Expand **Administration** on the left, click **Replication**

   Existing endpoints appear in the **Endpoints** view.

3. To edit or delete an endpoint, click the 3 vertical dots next to an endpoint name and select **Edit** or **Delete**.
4. To edit, enable or disable, or delete a replication rule, click **Replication Rule**, then click the 3 vertical dots next to a rule name and select **Edit**, **Enable** or **Disable**, or **Delete**.

Result

- If you enabled a rule, replication starts immediately.
- If you disabled a rule, vSphere Integrated Containers Registry attempts to stop all running jobs. It can take some time for all jobs to finish.

View and Manage VCHs, Add Registries, and Provision Containers Through the Management Portal

You can view live stats and manage the hosts in your environment after you add your existing VCHs to the management portal. Connect each VCH by using an authentication method and protocol, per the security flavor that you deployed the host with.

- For hosts with no TLS authentication, connect over HTTP with no credentials.
- For hosts with only server-side TLS authentication, connect over HTTPS with no credentials.
- For hosts with full TLS authentication, connect over HTTPS by using a client certificate.

Use registries to store and distribute images. You can configure multiple registries to gain access to both public and private images. You must manually add Harbor as a registry. JFrog Artifactory is also supported.

- Add Hosts with Server-Side TLS Authentication to the Management Portal
- Add Hosts with Full TLS Authentication to the Management Portal
- Add Registries to the Management Portal
- Provision Container VMs in the vSphere Integrated Containers Management Portal

Add Hosts with No TLS Authentication to the Management Portal

Connect hosts that do not require TLS authentication over HTTP with no credentials.

Procedure

1. In the management portal, navigate to **Resources** > **Hosts** and click **Add a host**.
2. On the Add Host page, configure the host settings.
    i. Enter the endpoint for the VCH as Address.

    For example, *http://*hostname*:2375*.

    ii. Select **VCH** as Host type.
    iii. Do not enter credentials and click **Verify**.
3. After successful verification, click **Add**.

Result

The VCH appears on the Hosts page and can be managed.

Add Hosts with Server-Side TLS Authentication to the Management Portal

Connect hosts that require server-side TLS authentication only over HTTP with no credentials.

Procedure

1. In the management portal, navigate to **Resources** > **Hosts** and click **Add a host**.
2. On the Add Host page, configure the host settings.
    i. Enter the endpoint for the VCH as Address.

    For example, *https://*hostname*:2376*.

    ii. Select **VCH** as Host type.
    iii. Do not enter credentials and click **Verify**.
3. After successful verification, click **Add**.

Result

The VCH appears on the Hosts page and can be managed.

Add Hosts with Full TLS Authentication to the Management Portal

Connect hosts that require full TLS authentication over HTTPS by using certificate to authenticate against the host.

Prerequisite

Obtain the client private key (*key.pem*) and client public key (*cert.pem*) for authentication against the VCH.

Procedure

1. In the management portal, navigate to **Resources** > **Hosts** and click **Add a host**.
2. On the Add Host page, configure the certificates to be used for authentication against the host.
   i. On the right, click **Credentials** and click **Add**.
   ii. In the **New Credential** dialog box, enter name and click the **Certificate** radio button.
   iii. In the **Public certificate** text box, enter the content of the *cert.pem* file.
   iv. In the **Private certificate** text box, enter the content of the *key.pem* file.
3. On the Add Host page, configure the host settings.
   i. Enter the endpoint for the VCH as Address.

      For example, *https://*hostname*:2376*.

   ii. Select **VCH** as Host type.
   iii. As Login credential, select the certificates that you configured for that host and click **Verify**.
4. After successful verification, click **Add**.

Result

The VCH appears on the Hosts page and can be managed.

Create and Manage Container Placements

You can use placements and placement settings to limit and reserve resources. You can also set a priority to the reserved amount of CPU or memory. Select a project for your placement and provision templates to that project to use the placement resourcing.

Prerequisite

Verify that at least one host is configured and available.

Procedure

1. In the management portal, navigate to **Policies** > **Placements** and click **Add**.
2. In the Add Placement dialog box, configure the new placement settings and click **Save**.

Setting	Description
Name	Enter a name for your placement.
Project	Assign the placement to a project. When you provision new templates to that project, you utilize the placement configuration.
Placement Zone	Select a placement zone from the list to assign the placement to a host.
Priority	(Optional) Enter a priority value for the placement. Higher value results in higher prioritized resourcing of the provisioned containers in the placement zone.
Instances	(Optional) Enter a number to limit the count of provisioned instances up to that number. For unlimited count, leave empty.
Memory Limit	(Optional) Limits the maximum amount of memory that the placement uses. For unlimited usage, leave empty.

Result

The placement appears on the Placements page and you can provision templates to that placement by selecting the assigned project.

Create New Networks for Provisioning Containers

You can create, modify, and attach network configurations to containers and container templates.

Procedure

1. In the management portal, navigate to **Deployments** > **Networks** and click **Create Network**.
2. On the Create Network page, select the **Advanced** check box to access all available settings.
3. Configure the new network settings and click **Create**.

Setting	Description
Name	Enter a name for the network.
IPAM config	Enter subnet, IP range, and gateway values that are unique to this network configuration. They must not overlap with any other networks on the same container host.
Custom Properties	(Optional) Specify custom properties for the new network configuration. `containers.ipam.driver` - for use with containers only. Specifies the IPAM driver to be used when adding a network component. The supported values depend on the drivers that are installed in the container host environment in which they are used. For example, a supported value might be infoblox or calico depending on the IPAM plug-ins that are installed on the container host. This property name and value are case-sensitive. The property value is not validated when you add it. If the specified driver does not exist on the container host at provisioning time, an error message is returned and provisioning fails. `containers.network.driver` - for use with containers only. Specifies the network driver to be used when adding a network component. The supported values depend on the drivers that are installed in the container host environment in which they are used. By default, Docker-supplied network drivers include bridge, overlay, and macvlan, while VCH-supplied network drivers include the bridge driver. Third-party network drivers such as weave and calico might also be available, depending on what networking plug-ins are installed on the container host. This property name and value are case-sensitive. The property value is not validated when you add it. If the specified driver does not exist on the container host at provisioning time, an error message is returned and provisioning fails.
Hosts	Select the hosts to use the new network.

Result

New network is created and you can provision containers on it.

Add Registries to the Management Portal

You can add multiple registries to gain access to both public and private images. You can enable and disable the registries that you added. When you disable a registry, searching for templates and images in that registry is disabled. Even if you disable the default https://registry.hub.docker.com registry, you can still access the popular templates. To customize your popular templates, see the https://github.com/vmware/admiral/wiki/Configuration-guide#customize-the-popular-templates-list instruction.

vSphere Integrated Containers can interact with both Docker Registry HTTP API V1 and V2 in the following manner:

Protocol	Description
V1 over HTTP (unsecured, plain HTTP registry)	You can freely search this kind of registry, but you must manually configure each Docker host with the `--insecure-registry` flag to provision containers based on images from insecure registries. You must restart the Docker daemon after setting the property.
V1 over HTTPS	Use behind a reverse proxy, such as NGINX. The standard implementation is available through open source at https://github.com/docker/docker-registry.
V2 over HTTPS	The standard implementation is open sourced at https://github.com/docker/distribution.
V2 over HTTPS with basic authentication	The standard implementation is open sourced at https://github.com/docker/distribution.
V2 over HTTPS with authentication through a central service	You can run a Docker registry in standalone mode, in which there are no authorization checks.

Procedure

1. In the management portal, navigate to **Templates** > **Registries** and click **Add**.
2. In the Add Registry dialog box, configure the registry settings.
    i. As address, enter the IP or hostname of the registry and the port.

    If you add Harbor, enter https://*hostname*:443.

    ii. Enter name for the registry.
    iii. Select the login credential and click **Verify**.
    iv. If prompted to trust the registry certificate, click **OK**.
    v. After successful verification, click **Save**.

Result

The registry appears on the Registries page and you can access the images stored in that registry.

Provisioning Container VMs in the Management Portal

You can provision container VMs from the management portal. You can quick-provision containers by using default settings or you can customize your deployment by using the available settings. You can either provision or save as a template your configured container.

You can provision containers, templates, or images.

- To provision a single container, go to **Deployments** > **Containers** and click **Create container**.
- To provision an image with additional settings, go to **Templates** > **Templates**, filter by images, and under **Provision** click **Enter additional info**.
- To provision a template, go to **Templates** > **Templates**, filter by templates, and click **Provision**.

When you create containers from the Containers page in the management portal, you can configure the following settings:

- Basic configuration
  - Image to be used
  - Name of the container
  - Custom commands
  - Links
- Network configuration
  - Port bindings and ports publishing
  - Hostname
  - Network mode
- Storage configuration
  - Select volumes
  - Configure a working directory
- Policy configuration
  - Define clusters
  - Resource allocation
  - Anti-affinity rules
- Custom environment variables
- Health checks
- Logging

Related topics

- Configuring Links
- Configuring Health Checks
- Configuring Cluster Size and Scale

Configuring Links

You configure links to templates or images. You can use links to enable communication between multiple services in your application. Links in vSphere Integrated Containers are similar to Docker links, but connect containers across hosts. Alink consists of two parts: a service name and an alias. The service name is the name of the service or template being called. The alias is the hostname that you use to communicate with that service.

For example, if you have an application that contains a Web and database service and you define a link in the Web service to the database service by using an alias of *my-db*, the Web service application opens a TCP connection to *my-db:{PORT_OF_DB}*. The *PORT_OF_DB* is the port that the database listens to, regardless of the public port that is assigned to the host by the container settings. If MySQL is checking for updates on its default *3306* port, and the published port for the container host is *32799*, the Web application accesses the database at *my-db:3306*.

You can use networks instead of links. Links are a legacy Docker feature with significant limitations when linking container clusters, including:

- Docker does not support multiple links with the same alias.
- You cannot update the links of a container runtime. When scaling up or down a linked cluster, the dependent container's links will not be updated.

Configuring Health Checks

You can configure a health check method to update the status of a container based on custom criteria.

You can use HTTP or TCP protocols when executing a command on the container. You can also specify a health check method. The available health configuration modes are described below.

Mode	Description
None	Default. No health checks are configured.
HTTP	If you select HTTP, you must provide an API to access and an HTTP method and version to use. The API is relative and you do not need to enter the address of the container. You can also specify a timeout period for the operation and set health thresholds. For example, a healthy threshold of 2 means that two consecutive successful calls must occur for the container to be considered healthy and in the RUNNING status. An unhealthy threshold of 2 means that two unsuccessful calls must occur for the container to be considered unhealthy and in the ERROR status. For all the states in between the healthy and unhealthy thresholds, the container status is DEGRADED.
TCP connection	If you select TCP connection, you must only enter a port for the container. The health check attempts to establish a TCP connection with the container on the provided port. You can also specify a timeout value for the operation and set healthy or unhealthy thresholds as with HTTP.
Command	If you select Command, you must enter a command to be run on the container. The success of the health check is determined by the exit status of the command.

Configuring Cluster Size and Scale

You can create container clusters by using Containers placement settings to specify cluster size.

When you configure a cluster, a specified number of containers is provisioned. Requests are load balanced among all containers in the cluster. You can modify the cluster size on a provisioned container or application to increase or decrease the size of the cluster by one. When you modify the cluster size at runtime, all affinity filters and placement rules are considered.