Configure and Manage VMware vSphere Integrated Containers

vSphere Integrated Containers 1.2

vmware

Table of Contents

Configure and Manage vSphere Integrated Containers

Configure and Manage vSphere Integrated Containers provides information about how to use VMware vSphere® Integrated Containers™ as a Cloud administrator.

Product version: 1.2

This documentation applies to all 1.2.x releases.

Intended Audience

This information is intended for Cloud 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. Cloud 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

Logging In to the Management Portal

You can access the Management Portal in a web browser by entering the vSphere Integrated Containers appliance IP address and the port that you specified for the portal during the deployment. By default the port number is *8282*.

If you do not know the port number, you can access the portal by going to http://*vic_appliance_address* and following the **Go to the vSphere Integrated Containers Management Portal** link.

To remove security warnings when you connect to the Getting Started page or management portal, see Obtain the Thumbprints and CA Files of the vSphere Integrated Containers Appliance Certificates and Verify and Trust vSphere Integrated Containers Appliance Certificates.

If you see a certificate error when you attempt to go to http://*vic_appliance_address*, see Browser Rejects Certificates with `ERR_CERT_INVALID` Error.

Default User Access to the Management Portal

The role that has full permissions for vSphere Integrated Containers is the cloud administrator role. By default, the cloud administrator role is assigned to the Administrators group for vCenter Server during the installation of vSphere Integrated Containers. Every user that is a member of that group in the Platform Services Controller can access the Management Portal as cloud administrator. After you log in as a cloud administrator, you can give other users access to vSphere Integrated Containers by assigning them roles in projects.

Optionally, you can log in as one of the example users that were created during the OVA deployment, if you used that option. The example users allow you to see what each type of role can do in vSphere Integrated Containers Management Portal.

For more information about users and roles, see Users and Roles.

Verify and Trust vSphere Integrated Containers Appliance Certificates

You can verify the self-signed certificates and trust the certificate authority (CA) for the vSphere Integrated Containers Getting Started page and the vSphere Integrated Containers Management Portal. Trusting the CA prevents browsers from giving security warnings and potentially locking you out of vSphere Integrated Containers for security reasons.

Prerequisites

To verify and trust the vSphere Integrated Containers appliance certificates, you must obtain the thumbprints and CA files either directly from the appliance, or from the vSphere administrator. For information about how to obtain certificate information, see Obtain the Thumbprints and CA Files of the vSphere Integrated Containers Appliance Certificates.

Procedure

1. In a browser, go to the Getting Started Page at http://*vic_appliance_address*.
2. View the certificate details in the browser and locate the SHA-1 thumbprint.

   How you view the certificate details depends on the type of browser that you use.

3. Compare the SHA-1 thumbprint in the browser to the thumbprint that you or the vSphere administrator obtained from the appliance.

   The thumbprints should be the same.

4. Click the link to the vSphere Integrated Containers Management Portal in the Getting Started page, log in, and repeat the procedure to verify the certificate thumbprint for the management portal.
5. When you have verified both of the thumbprints, import the `ca.crt` files into the root certificate store on your local machine.

   How you import a CA file into the root certificate store depends on the operating system of your local machine.

Result

When you access the Getting Started page and vSphere Integrated Containers Management Portal, your browser shows that the connection is secure.

Configure System Settings

When you first log in to a new vSphere Integrated Containers instance, you can implement certificate verification for image replications, set the period of validity for login sessions, and schedule vulnerability scans.

Procedure

1. Go to http://*vic_appliance_address*, click the link to **Go to the vSphere Integrated Containers Management Portal**, and enter the vCenter Server Single Sign-On credentials.
2. Select **Administration** > **Configuration**, and optionally deselect 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.
3. Modify **Token Expiration (Minutes)** to optionally change the duration of login sessions from the default of 30 minutes.
4. Click **Download** to obtain the root certificate of the vSphere Integrated Containers Registry so that you can distribute it to interested parties. Developers need that certificate to pull an image from the Registry into their Docker client.
5. Under **Vulnerability Scanning**, optionally change the default settings for the scheduled daily vulnerability scanning at 3AM, and click **Save**.

What to Do Next

Add users to the system.

Add Cloud Administrators

You can add any user or group from the Platform Services Controller to the vSphere Integrated Containers Management Portal and assign them the Cloud administrator role.

For more information about working with local users and identity sources in the Platform Services Controller, see the Platform Services Controller Administration Guide in the VMware vSphere documentation.

For more information about users and roles in vSphere Integrated Containers, see Users and Roles.

Procedure

1. Go to http://*vic_appliance_address*, click the link to **Go to the vSphere Integrated Containers Management Portal**, and enter the vCenter Server Single Sign-On credentials.

   Use an account with Cloud administrator privileges.

2. Select **Administration** > **Identity Management**, and click **Users & Groups**.
3. In the search box, enter a group name, user name, email address, or the user's full name and press Enter.

   Wait for the user or group to appear in the table.

4. Select the check box next to the user in the table and click **Assign Admin Role**.

   The user is now a Cloud administrator for vSphere Integrated Containers. You can use the same workflow to unassign the role from a current cloud administrator user or group.

What to Do Next

Create projects and assign the users to those projects.

Add Viewers, Developers, or DevOps Administrators to Projects

You can add any user from the Platform Services Controller to the vSphere Integrated Containers Management Portal and assign them a role.

For more information about working with local users and identity sources in the Platform Services Controller, see the Platform Services Controller Administration Guide in the VMware vSphere documentation.

For more information about users and roles in vSphere Integrated Containers, see Users and Roles.

Procedure

1. Go to http://*vic_appliance_address*, click the link to **Go to the vSphere Integrated Containers Management Portal**, and enter the vCenter Server Single Sign-On credentials.

   Use an account with Cloud administrator or DevOps administrator privileges.

2. Select **Administration** > **Projects**, and click a project to add users to.
3. Click the **Members** tab and click **+ Add** to add a new user to that project.
4. In the Add Users and Groups window configure the user and the access.
   i. In the **ID or email** text box, enter any detail for a desired user and select it from the populated list.
   ii. From the **Role in project** drop-down menu, select a role for that user and click **OK**.

1. (Optional) Change the role of a user that is assigned to the project.
   i. From the table with users, click the three dots next to a user and click **Edit**.
   ii. In the **Edit member role in project** window, select new role for that user and click **OK**.

View and Manage VCHs in vSphere Integrated Containers 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.

- Add Hosts with No TLS Authentication to the Management Portal

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

IMPORTANT: If you have deployed multiple instances of the vSphere Integrated Containers appliance, you can only register a virtual container host (VCH) with one instance of the management portal at a time.

Procedure

1. In the management portal, navigate to **Infrastructure** > **Container Hosts** and click **+New**.
2. On the New Container Host page, configure the host settings.
    i. Enter name for the host.
    ii. Select **VCH** as type.
    iii. Enter the endpoint for the VCH as URL and click **Save**.

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

Result

The VCH appears on the Container 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.

IMPORTANT: If you have deployed multiple instances of the vSphere Integrated Containers appliance, you can only register a virtual container host (VCH) with one instance of the management portal at a time.

Procedure

1. In the management portal, navigate to **Infrastructure** > **Container Hosts** and click **+New**.
2. On the New Container Host page, configure the host settings.
    i. Enter name for the host.
    ii. Select **VCH** as type.
    iii. Enter the endpoint for the VCH as URL.

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

    iv. Do not enter credentials and click **Save**.
    v. If you are prompted to trust the certificate, click **OK**.

Result

The VCH appears on the Container 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.

IMPORTANT: If you have deployed multiple instances of the vSphere Integrated Containers appliance, you can only register a virtual container host (VCH) with one instance of the management portal at a time.

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 **Administration** > **Identity Management** and click **Credentials** to configure the certificates to be used for authentication against the host.
   i. Click **+Credential** to add new entry.
   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.
   v. Click **Save**.
2. Navigate to **Home** > **Infrastructure** > **Container Hosts** and click **+New**.
3. On the New Container Host page, configure the host settings.

   i. Enter name for the host.
   ii. Select **VCH** as Host type.
   iii. Enter the endpoint for the VCH as URL.

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

   iv. As Credentials, select the certificates that you configured for that host and click **Save**.

Result

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

Add Registries to the Management Portal

You can add multiple registries, in addition to the integrated vSphere Integrated Containers Registry 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 Customize the Popular Templates list documentation.

Use registries to store and distribute images. You can configure multiple registries to gain access to both public and private images. JFrog Artifactory is also supported.

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. You cannot use HTTP connections with vSphere Integrated Containers Registry instances.
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 **Administration** > **Registries** > **Source Registries** and click **+Registry**.
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.
    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.

Create a Project in vSphere Integrated Containers

In vSphere Integrated Containers, you create different projects to which you assign users, repositories, and infrastructure. You also set up replication of registries in projects, and configure project-specific settings. When you first deploy vSphere Integrated Containers, a default public project named default-project is created.

Procedure

1. Go to http://*vic_appliance_address*, click the link to **Go to the vSphere Integrated Containers Management Portal**, and enter the vCenter Server Single Sign-On credentials.

   Use an account with Cloud administrator privileges.

2. Navigate to **Administration** > **Projects** and click **+ Project**.
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 **Save**.

Result

The project is added to the list of projects. You can browse existing projects and filter the list by entering text in the search 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.

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. Go to http://*vic_appliance_address*, click the link to **Go to the vSphere Integrated Containers Management Portal**, and enter the vCenter Server Single Sign-On credentials.
2. Select the **Administration** tab and click **Projects**.
3. In the list of projects, click a project.
4. On the Summary page, click **Edit**.
    - If the project is public, deselect the **Public access to project registry** checkbox to change the project state to private.
    - If the project is private, select the **Public access to project registry** checkbox to change the project state to public.
5. To delete a project, on the Projects page, click the three dots next to a project and click **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. Go to http://*vic_appliance_address*, click the link to **Go to the vSphere Integrated Containers Management Portal**, and enter the vCenter Server Single Sign-On credentials.
2. Select the **Administration** tab and click **Logs**.

   In the Logs view you can see system logs as well as logs of the vSphere Integrated Containers Registry.

3. To see a reduced list of operations, enter text in the **Filter Logs** text box.

   For example, enter the name of a repository.

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 Management Portal. 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. Go to http://*vic_appliance_address*, click the link to **Go to the vSphere Integrated Containers Management Portal**, and enter the vCenter Server Single Sign-On credentials.

   Use an account with the system-wide Administrator role, or an account that has the Project Admin role for this project.

2. Select the **Administration** tab, 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 *Install, Deploy, and Maintain the vSphere Integrated Containers Infrastructure*.

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. Areplication 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 System Settings.

Procedure

1. Go to http://*vic_appliance_address*, click the link to **Go to the vSphere Integrated Containers Management Portal**, and enter the vCenter Server Single Sign-On credentials.

   Use an account with Cloud Administrator privileges.

2. Select the **Administration** tab, click **Registries** > **Replication Endpoints** and 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 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. Areplication 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 System Settings.

Procedure

1. Go to http://*vic_appliance_address*, click the link to **Go to the vSphere Integrated Containers Management Portal**, and enter the vCenter Server Single Sign-On credentials.

   Use an account with Cloud Administrator privileges.

2. Select the **Administration** tab, click **Projects** on the left, and click the name of the project to replicate.
3. Click **Registry Replication** and 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, select the **New Endpoint** check box.

     i. Enter a suitable name for the new replication endpoint.
     ii. Optionally select the **Enable** checkbox.

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

     i. Enter the full URL of the vSphere Integrated Containers Registry instance to set up as a replication endpoint.

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

     ii. 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 click **OK**.
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. Go to http://*vic_appliance_address*, click the link to **Go to the vSphere Integrated Containers Management Portal**, and enter the vCenter Server Single Sign-On credentials.

   Use an account with Cloud Administrator privileges.

2. Select the **Administration** tab, click **Registries**, and click **Replication Endpoints**.

   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 Endpoint** or **Delete Endpoint**.
4. To edit, enable or disable, or delete a replication rule, click **Replication Rules**, 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.