Configure and Manage vSphere Integrated Containers

VMware vSphere Integrated Containers 1.4.x

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: 1.4

This documentation applies to all 1.4.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

Initial Configuration of the Management Portal

You must prepare the vSphere Integrated Container Management Portal and Registry for use, before you create your first projects and add more users.

The members of the vSphere Administrators group are the default Cloud administrators that can log in, configure the management portal, and add new Cloud administrators.

- Logging In to the Management Portal
- Configure System Settings
- Add Cloud Administrators

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 CAFiles of the vSphere Integrated Containers Appliance Certificates and Verify and Trust vSphere Integrated Containers Appliance Certificates.

Troubleshooting

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.

If you are unable to log in to vSphere Integrated Containers Management Portal, see Troubleshoot Post-Deployment Operation.

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 vSphere Integrated Containers Roles and Personas.

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 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**.
3. Under System Settings, 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.

   You must distribute the certificate to the interested parties:

   - vSphere administrators need the certificate so that they can deploy VCHs that connect to the Registry.
   - Developers need the certificate so that they can pull images 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 vSphere Integrated Containers Roles and Personas.

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.

Working with Projects

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.

- Create a Project in vSphere Integrated Containers
- Manage Projects
- Access and Search Project Logs
- Manage Internal Repositories in vSphere Integrated Containers Registry
- Assign Viewers, Developers, or DevOps Administrators to a Project
- Assign Projects to a User
- Add VCHs in vSphere Integrated Containers Management Portal

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 as well as turning security options on and off. 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. Navigate to **Administration** > **Projects** > **Your_project**.
3. Click the **Configuration** tab to change the project settings.
    i. If you want to make all repositories of that project public, select the **Public** check box.
    ii. If you want to prevent unsigned images from the project repositories from being run, select the **Enable content trust** check box.
    iii. If you want to prevent vulnerable images from your project repository from running, select the **Prevent vulnerable images from running** check box.
    iv. (Optional) Change the severity level of vulnerabilities found that prevents an image from running.

        Images cannot be run if their level equals the currently selected level or higher.

    v. If you want to activate an immediate vulnerability scan on new images that are pushed to the project registry, select the **Automatically scan images on push** check box.
4. 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 Internal Repositories in vSphere Integrated Containers Registry

You can access the list of internal 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. In the management portal, navigate to **Administration** > **Projects** > **Your_project**.

   Use an account with the Cloud Administrator role, or an account that has the DevOps Admin role for this project.

2. Click the **Internal Repositories** tab to 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, select the check box next to a repository name and click **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*.

Assign Viewers, Developers, or DevOps Administrators to a Project

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

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 vSphere Integrated Containers Roles and Personas.

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 or group 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**.
5. (Optional) Change the role of a user that is assigned to the project.
   i. From the table with users, select the check box 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**.

Assign Projects to a User

You can assign one or more projects to any user from the Platform Services Controller to the vSphere Integrated Containers Management Portal. You assign the same user different roles in different projects.

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 vSphere Integrated Containers Roles and Personas.

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** > **Identity Management** > **Users & Groups**.
3. In the search box, enter all or part of a user name, email address, or user group name and press Enter.
4. Select the check box for a user, and click **Assign Project Roles**.
5. From the left hand drop-down menu, select a project to which to assign the user or group.
6. From the right-hand drop-down menu, select a role for the user or group in that project.
7. (Optional) Click the plus (**+**) symbol to assign more projects to the same user.

   You can assign multiple projects to the same user. The user can have a different role in each project.

8. Click **OK**.

Result

The projects that you assigned to the user are listed in the **Projects** column.

What to Do Next

You can remove a user from a project by selecting the user, clicking **Assign Project Roles**, and clicking the minus (**-**) symbol for a project.

Add VCHs in vSphere Integrated Containers Management Portal

You can provision containers, view live stats, and manage the hosts in your environment after you add existing Docker hosts or vSphere Integrated Containers virtual container hosts (VCHs) to projects. You can add the same VCH to multiple projects.

NOTE: vSphere Integrated Containers Management Portal allows you to provision containers from the registries that are included in the lists of global registries that the cloud administrator configures, or project registries that the DevOps administrator configures. However, if the vSphere administrator deployed a VCH with whitelist mode enabled, and if the whitelist on the VCH is more restrictive than the global and project registry lists, you can only provision containers from the registries that the VCH permits in its whitelist, even if the VCH is included in a project that permits other registries. For more information, see VCH Whitelists and Registry Lists in vSphere Integrated Containers Management Portal in *Install, Deploy, and Maintain the vSphere Integrated Containers Infrastructure*.

You add VCHs to projects according to the security flavor that you deployed the host with.

- Add Virtual Container Hosts with Full TLS Authentication to the Management Portal
- Add Virtual Container Hosts with Server-Side TLS Authentication to the Management Portal
- Add Virtual Container Hosts with No TLS Authentication to the Management Portal

Add Virtual Container Hosts with Full TLS Authentication to the Management Portal

If the vSphere administrator deployed a virtual container host (VCH) that implements verification of both server and client certificates, you must provide the details of the client certificate when you add the VCH to a project in the management portal. Connections to the VCH use HTTPS.

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 the VCH from the vSphere administrator.

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. Go to the **Home** view, click the **Project** drop-down menu, and select the project to which to add the VCH.
3. Navigate to **Infrastructure** > **Container Hosts** and click **+Host**.
4. 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 for the selected project. You can also see the VCHs that you added to a project by navigating to **Administration** > **Projects** > *project* > **Infrastructure**.

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

If the vSphere administrator deployed a virtual container host (VCH) with server-side authentication but without implementing verification of client certificates, you do not provide a certificate when you add the VCH to a project in the management portal. Connections to the VCH use HTTPS.

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

Procedure

1. In the **Home** view of the management portal, click the **Project** drop-down menu and select the project to which to add the VCH.
2. Navigate to **Infrastructure** > **Container Hosts** and click **+Host**.
3. 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 for the selected project. You can also see the VCHs that you added to a project by navigating to **Administration** > **Projects** > *project* > **Infrastructure**.

Add Virtual Container Hosts with No TLS Authentication to the Management Portal

If the vSphere administrator deployed a virtual container host (VCH) without implementing any TLS authentication, you do not provide a certificate when you add the VCH to a project in the management portal. Connections to the VCH use HTTP.

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 **Home** view of the management portal, click the **Project** drop-down menu and select the project to which to add the VCH.
2. Navigate to **Infrastructure** > **Container Hosts** and click **+Host**.
3. 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 for the selected project. You can also see the VCHs that you added to a project by navigating to **Administration** > **Projects** > *project* > **Infrastructure**.

Working with Registries

You use registries to store and distribute images. 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. You can add global registries, that are visible to all projects, as well as project registries, that are available only to the project to which they are added. All users can only search and provision images and templates from registries that are available to their projects. When you disable a registry, searching for templates and images in that registry is also disabled.

Even if you disable the default https://registry.hub.docker.com registry, you can still see the popular templates under **Library** > **Repositories**.

Starting with vSphere Integrated Containers 1.4, you can configure namespaces for the registries that you add. If you add a new registry and configure a namespace for it, users cannot search, browse, or deploy images that are outside of that namespace. You can add a registry multiple times to allow users to reach different namespaces in that registry.

vSphere Integrated Containers supports JFrog Artifactory and 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.

- Add Global Registries
- Add Project Specific Registries

Add Global Registries

You can add multiple global registries that are added by the cloud admin and are available to all users of the management portal. Global registries that are allowed by the cloud admin cannot be disabled or removed by other users.

Procedure

1. In the management portal, navigate to **Administration** > **Global Registries** > **Source Registries** and click **+Registry**.
2. In the dialog box that opens, configure the registry settings.
    i. As address, enter the IP or hostname of the registry, the port, and optionally a namespace.

    For example: `https://registry.hub.docker.com:443/vmware`

    ii. Enter a name for the registry.
    iii. Optionally, select the login credentials to access the registry.
    iv. Click **Verify** and if prompted to trust the registry certificate, click **OK**.
    v. After successful verification, click **Save**.

Result

The registry appears on the Global Registries page and all users can access the images stored in that registry.

Add Project Specific Registries

In addition to the integrated vSphere Integrated Containers Registry and the global registries added by the Cloud administrator, DevOps administrators can add project specific registries. From the Project registries view, DevOps administrators can add, update, and delete project specific registries and also see the available global registries but cannot remove them.

Starting with vSphere Integrated Containers 1.4, you can also configure namespaces for the registries that you add. If you add a new registry and configure a namespace for it, developers cannot search, browse, or deploy images that are outside of that namespace. You can add a registry multiple times to allow developers to reach different namespaces in that registry.

Procedure

1. In the management portal, navigate to **Administration** > **Projects** and click your project.
2. On the Project Registries tab, click **+ New Project Registry**.
3. On the Add Project Registry page, configure your new registry.
    i. As address, enter the IP or hostname of the registry, the port, and optionally a namespace.

    For example: `https://registry.hub.docker.com:443/library`

    ii. Enter a name for the registry.
    iii. Optionally, select the login credentials to access the registry.
    iv. Click **Verify** and if prompted to trust the registry certificate, click **OK**.
    v. After successful verification, click **Save**.

Result

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

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.

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 **Global Registries** > **Replication Endpoints** and click the **+ New 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. Optionally, select the **Verify Remote Cert** check box. Deselect if the remote registry uses a self-signed or untrusted certificate.
7. Click **Test Connection**.
8. 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, the selected 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.
- You configured the target registry as a replication endpoint.

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** > **Global Registries**, and click **New Replication Rule**.
3. In the New Replication Rule dialog box, configure the new rule.

   i. Enter a suitable name for the new replication rule and optionally add a description.
   ii. Enter the name of the project that uses the images you want to replicate.
   iii. If you want to limit the repositories or tags for replication, select in the Source images filter field.
   iv. Select an endpoint registry.
   v. From the **Trigger Mode** drop down menu, select your desired method for pushing to the endpoint.

      You can manually push, automatically replicate and delete images in the endpoint registry by selecting immeadiate and the respective options, or configure scheduled replication per your preference.

   vi. Click **Save**.

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 **Global Registries**, and click **Replication Endpoints**.

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

3. To edit or delete an endpoint, select the check box next to an endpoint name and click **Edit** or **Delete**.
4. To edit or delete a replication rule, click **Replication Rules**, select the check box next to a rule name and click **Edit** 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.

Vulnerability Scanning

vSphere Integrated Containers uses the open source project Clair to scan images for known vulnerabilities. Cloud administrators and DevOps administrators can set threshold values that restrict vulnerable images that exceed the threshold from being run on a per-project level. Once an image is uploaded into the registry, Clair checks the various layers of the image against known vulnerability databases and reports issues to the administrators.

Prerequisites

You must allow firewall access from your vSphere Integrated Containers instance to the following URLs so that Clair can sync its database.

Item	Database URL
Ubuntu	https://launchpad.net/ubuntu-cve-tracker
Red Hat Enterprise Linux	https://www.redhat.com/security
Oracle	https://linux.oracle.com/oval
Debian	https://security-tracker.debian.org
Alpine	https://git.alpinelinux.org
National Vulnerability Database	http://static.nvd.nist.gov
CVE information	https://cve.mitre.org/

- Configure Scheduled Vulnerability Scan on All Images
- Configure Vulnerability Scanning on a Per-Project Level
- Perform a Vulnerability Scan on a Single Image

Configure Scheduled Vulnerability Scan on All Images

You can set daily vulnerability scan on all images or disable that functionality.

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 under **Vulnerability Scanning**, verify that the database was updated recently.
3. Optionally, change the default settings for the scheduled daily vulnerability scanning and click **Save**.

   You can schedule a full scan for all images once a day or disable the automated full scan.

4. (Optional) Click **Scan Now** to manually start a full scan for all images.

   You can start a manual scan only once in two hours as the procedure is resource intensive.

5. To verify the scan results, navigate to **Administration** > **Projects** > **Your_project** > **Repositories**, expand an image repository, and hover over the report under **vulnerability**.

Configure Vulnerability Scanning on a Per-Project Level

Cloud administrators and DevOps administrators can set threshold values that prevent vulnerable images that exceed the threshold from being run. An automated scan on new images that are pushed to the project registry is also available.

Procedure

1. In the Management Portal, navigate to **Administration** > **Projects** > **Your_project** > **Configuration**.
2. To prevent vulnerable images from your project repository to run, select the **Prevent vulnerable images from running** check box.
3. (Optional) Change the severity level of vulnerabilities found that prevents an image to run.

   Images cannot be run if their level equals the currently selected level or higher.

4. To activate an immediate vulnerability scan on new images that are pushed to the project registry, select the **Automatically scan images on push** check box.
5. To verify the scan results, click the **Repositories** tab, expand the image repository and hover over the report under **vulnerability**.

Perform a Vulnerability Scan on a Single Image

Cloud administrators and DevOps administrators can perform a manual scan on a single image.

Procedure

1. In the Management Portal, navigate to **Administration** > **Projects** > **Your_project** > **Internal Repositories**.
2. Click an image repository.
3. Select the check box next to an image and click **Scan**.

The results of the scan appear for each scanned image, under the **vulnerability** column.