





# VMware Tanzu and Entrust CloudControl

Integration Guide

2024-12-20

© 2025 Entrust Corporation. All rights reserved.

# Table of Contents

1. Introduction
1.1. Product configurations
1.2. Requirements
2. Procedures
2.1. Download the CloudControl software
2.2. Deploy the CloudControl VM from the OVA
2.3. Power on the appliance
2.4. Configure the CloudControl virtual appliance
2.5. Set up the CloudControl GUI
2.6. VMware Tanzu prerequisites
2.7. VMware Tanzu setup
2.8. On-board the Tanzu clusters
2.9. View VMware Tanzu Kubernetes cluster inventory
2.10. Transfer root access control to CloudControl
2.11. Create a Trust Manifest Access Control Policy
2.12. Image registries
2.13. Image Deployment Control Policy
2.14. Configuration hardening
3. Additional resources and related products
3.1. CloudControl
3.2. Entrust products
3.3. nShield product documentation

# Chapter 1. Introduction

This guide describes how to integrate VMware Tanzu Kubernetes clusters with Entrust CloudControl. Entrust CloudControl organizes a cluster inventory into categories relating to the Tanzu deployment. Entrust CloudControl uses role and asset-based access control to help the user define who can do what to which cluster objects. It also uses image deployment control policies that can be applied to a cluster infrastructure. This ensures ongoing compliance with your organization security policies.

# 1.1. Product configurations

Entrust has successfully tested the integration of Entrust CloudControl with VMware Tanzu in the following configurations:

System	Version
VMware vCenter	7.0.1 U1 (build-16858589)
Kubernetes Version	v1.18.19+vmware.1
Entrust CloudControl	6.6.0

# 1.2. Requirements

Before starting the integration process, familiarize yourself with:

- The documentation and setup process for VMware Tanzu.
- The documentation and setup process for Entrust CloudControl. The online documentation contains everything needed to successfully install and deploy CloudControl.



Entrust recommends that you allow only unprivileged connections unless you are performing administrative tasks.

# **Chapter 2. Procedures**

This guide uses a standalone CloudControl deployment and does not use Active Directory. All users are local to the system. CloudControl supports a cluster environment. For more information refer to the Entrust CloudControl Installation Guide in the online documentation.

# 2.1. Download the CloudControl software

- 1. Go to https://my.hytrust.com/s/software-downloads.
- 2. Log in and select HyTrust CloudControl.
- 3. Open the folder HTCC\_6.6.0\_2023-02-241. This folder contains version 6.5.0 that was used in this guide.
- 4. Select the Entrust-CloudControl-6.6.0.660934.zip link to download the file.

fi i	Cases	Knowledge Base 🗸	Product Documentation	Licenses	Software Downloads	Upgrade Center	Videos				
	Sofware Downloads Folders and Files										
	/ Hytrus	t CloudControl									
		Folder Name									
		HTCC_MoveRPVTool_2020-10-	15								
		HTCC_Migration_Tool_2021-05-	19								
	-	HTCC_6.6.0_2023-02-24									
		Action Name						Size			
		Entrust_CloudControl_F	Release_Notes_v6.6.pdf					0.19 MB			
		Entrust-CloudControl-6.	6.0.660934.zip					6399.99 MB			
	~	Entrust-CloudControl-6.	6.0.660934.zip.sha256sum.txt					104 Bytes			
	~	Entrust-CloudControl-6.	6.0.660934.zip.sha384sum.txt					136 Bytes			
		Entrust-CloudControl-6.	6.0.660934_upgrade.zip					3788.62 MB			
		Entrust-CloudControl-6.	6.0.660934_upgrade.zip.sha256s	um.txt				112 Bytes			
		Entrust-CloudControl-6.	6.0.660934_upgrade.zip.sha384si	um.txt				144 Bytes			

5. After the file has been downloaded, open the ZIP file to access to the OVA file.

# 2.2. Deploy the CloudControl VM from the OVA

- 1. Log in to vCenter.
- 2. Select the cluster to create the CloudControl VM in.
- 3. From the Actions menu, select Deploy OVF template.

Deploy OVF Template	Select an OVF template	$\times$
1 Select an OVF template	Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer such as a local hard drive a network share or a CD/DVD drive.	
2 Select a name and folder	OURL	
3 Select a compute resource	http://remoteserver-address/filetodeploy.ovf   .ova	
4 Review details	Local file	
5 Select storage	UPLOAD FILES No files selected.	
6 Ready to complete	Select a template to deploy. Use multiple selection to select all the files associated with an OVF template (ovr, vmdk, etc.)	×

- 4. Select Local File and upload the CloudControl OVA file.
- 5. Select Next

Follow the instructions during the deployment as needed.



For more information refer to Installing CloudControl from an OVA in the online documentation.

# 2.3. Power on the appliance

- 1. Log in to the vSphere Client.
- 2. Locate the Entrust CloudControl virtual machine in the inventory.
- 3. Right-click the CloudControl virtual machine and select **Power > Power On**.

# 2.4. Configure the CloudControl virtual appliance

This guide uses a Standalone Node setup. For more information refer to Creating a Standalone Node in the online documentation.

# 2.5. Set up the CloudControl GUI

After the standalone node has been configured, finish the setup using the GUI. For more information refer to Setting Up the CloudControl GUI in the online documentation.

# 2.6. VMware Tanzu prerequisites

CloudControl has some prerequisites for VMware Tanzu that must be put in place.

For more information refer to VMware Tanzu Prerequisites in the online documentation.

# 2.7. VMware Tanzu setup

This guide does not describe the deployment of a VMware Tanzu cluster. Refer to the VMware documentation for details.

When the VMware Tanzu cluster is set up, use the cluster kubeconfig file to onboard the cluster into CloudControl. A client machine with kubectl installed is required to run commands specified in this guide.

The examples in this guide use a CentOS 8 virtual machine which will be referred to as the kubectl node from now on.

- 1. Log in to the kubectl node client machine.
- 2. On the kubectl node log into the VMware Tanzu Management/Supervisor cluster:

```
% kubectl vsphere login --vsphere-username administrator@vsphere.local --server=https://xx.xxx.xx
--insecure-skip-tls-verify
```

When this command has executed successfully, use the \$HOME/.kube/config file for onboarding. This will be the config file to onboard the Management/Supervisor cluster. Save this file in the \$HOME directory and name it management.kubeconfig.txt.

```
% cp $HOME/.kube/config $HOME/management.kubeconfig.txt
```

3. To get the Tanzu Kubernetes cluster config file, log into the Tanzu Kubernetes cluster:

```
% kubectl vsphere login --vsphere-username administrator@vsphere.local --server=https://xx.xxx.xxx
--insecure-skip-tls-verify --tanzu-kubernetes-cluster-namespace qanamespace --tanzu-kubernetes-cluster-name
qa-tkg-cluster-01
```

In this example, the namespace for our cluster is **qanamespace** and the cluster name is **qa-tkg-cluster-01**. These are just examples. Enter the names that apply to the environment in use.

When this command has executed successfully, use the \$HOME/.kube/config file for on-boarding. This will be the config file to onboard the Tanzu Kubernetes cluster. Save this file the \$HOME directory and name it tanzucluster.kubeconfig.txt.

```
% cp $HOME/.kube/config $HOME/tanzucluster.kubeconfig.txt
```

- \$HOME/.kube/config is the file needed to onboard the clusters in CloudControl. For Tanzu, use the following files:
  - a. management.kubeconfig.txt for the Management/Supervisor cluster.
  - b. tanzucluster.kubeconfig.txt for the Tanzu Kubernetes cluster.

Both clusters will have to be on-boarded into CloudControl.

Now add the Tanzu clusters into CloudControl, see On-board the Tanzu clusters.

## 2.8. On-board the Tanzu clusters

On-boarding is the process of adding the Tanzu Kubernetes clusters into CloudControl. For more information refer to Adding a VMware Tanzu Cluster in the online documentation. For Tanzu, import the Tanzu Management cluster and at least a Tanzu Kubernetes cluster.

## 2.8.1. On-boarding the Tanzu Management cluster

1. From the Home tab, select Inventory > Kubernetes Clusters.

ENTRUST	CloudControl				<b>:</b> ( )
	Inventory	, S	ecurity	System	
	AWS Accounts Kuberne	tes Clusters NSX-T	VSphere	VCF	III III Image Registics

2. On the **Clusters** page, select **Actions > Add Kubernetes Cluster**.

If there are no clusters in the system, **Add Kubernetes Cluster** is also available on the **Kubernetes Clusters** page.

- 3. On the Add Kubernetes Cluster Import tab, choose one of the following:
  - ° Select Import File, then select Browse and choose the kubeconfig file to import.
  - ° Select Enter Text, then paste the contents of the kubeconfig file as plain text.

A kubeconfig file is a configuration file written in YAML that describes the cluster.

To import the Management cluster, use the Management cluster config file produced earlier, management.kubeconfig.txt.



4. Select **Enter Text**, then paste the contents on the Management cluster config file as plain text.

- 5. Select Continue.
- 6. On the **Clusters** tab, select the Tanzu Management cluster to add and select **Continue**.

Only one cluster can be selected. Select the Tanzu Management cluster IP address or FQDN.



- 7. On the **About** tab, enter the following:
  - ° Friendly Name: Enter the user-facing name for the cluster.
  - **Password**: Enter the password for the user selected who has access to the cluster. In this example, that is the same password used by administrator@vsphere.local.

🐇 🔊 Log Analysis 🗙 🎯 Kubernetes Clusters 🗙 🕂 Add Kubernetes Clus 🗴	
Add Kubernetes Cluster 🛞 Management Cluster	
1: Import 🖌 — 2: Clusters 🖌 — 3: About — 4: Details — 5: Master Nodes	
Vendor Type © Tanzu Management Cluster	
Friendly Name	
Management Cluster	
User wcp: :administrator@vsphere.local	
Password *	
Back	

For the **Vendor Type**, CloudControl detects that this is a Tanzu Management cluster.

- 8. Select Continue.
- 9. On the **Details** tab, monitor the process.

Add Kubernetes Cluster	
1: Import 🗸 — 2: Clusters 🖌 — 3: About 🖌 — 4: Details	5: Master Nodes
Connecting to Tanzu Management Cluster	
Discovering Nodes	6 Found
Discovering Namespaces	19 Found
<ul> <li>Discovering Deployments</li> </ul>	26 Found
✓ Discovering Pods	183 Found
<ul> <li>Discovering Containers</li> </ul>	136 Found
Discovering Services	28 Found
	Continue

- 10. Select Continue.
- 11. On the **Master Nodes** tab, a list of nodes will be displayed with their name, IP, and hostname information.
- 12. Select Continue.
- 13. After the cluster has been imported into CloudControl the cluster dashboard is shown.

ENTRUS	T CloudControl				<b>= 4</b> ?
🐔 🚁 Log Analys	sis 🛛 🗶 💿 Kubernetes Clusters 🗶	*			
Cluster					Views   Actions
○ Node: 6	s 🗖 Namespaces	© Deployments	<sup>⊕ Pods</sup> 166	<ul><li>Containers</li><li>154</li></ul>	∞° Services
	Details	د مرتبع Configuration Hard	ening Summary	Container De	ployment Control
Type IP Address API Server Port Master Nodes	Container Orchestrator 6443 3	Assessments	Remediations	í	ĩí
SSH Port API Version Platform Build Date	22 v1.18.2-6+38ac483e736488 linux/amd64 Jul 7, 2020, 8:51:34 AM	Currently no asset	ssment policies licy now		
	Configuration Hardening Tre	nding	All containers (active and particular) 1.	Container Runtime Violation	1 <b>S</b> 2 <sup>2</sup>

## 2.8.2. On-boarding the Tanzu Kubernetes cluster

After the Tanzu Management cluster has been on-boarded, import a Tanzu Kubernetes cluster.

1. From the Home tab, select Inventory > Kubernetes Clusters.



- 2. On the Clusters page, select Actions > Add Kubernetes Cluster.
- On the Add Kubernetes Cluster Import tab, select Enter Text, then paste the contents of the kubeconfig file as plain text.

To import the Tanzu Kubernetes cluster, use the Tanzu cluster config file tanzucluster.kubeconfig.txt.



- 4. Select **Enter Text**, then paste the contents on the Tanzu Kubernetes cluster config file as plain text.
- 5. Select Continue.
- 6. On the **Clusters** tab, select the Tanzu Kubernetes cluster to add and select **Continue**.

Only one cluster can be selected. Select the Tanzu Kubernetes cluster IP address or FQDN.



- 7. On the **About** tab, enter the following:
  - ° Friendly Name: Enter the user-facing name for the cluster.
  - **Password**: Enter the password for the user who has access to the cluster. In this example, that is the same password used by administrator@vsphere.local.

🐇 🔊 Log Analysis 🗙 🌀 Kubernetes Clusters 🗶 🕇 Add Kubernetes Cl	×
Add Kubernetes Cluster 🛞 Kubernetes Cluster	
1: Import 🗸 — 2: Clusters 🖌 — 3: About — 4: Details — 5: Master Nodes	
Vendor Type O Tanzu Kubernetes Cluster	
Friendly Name	
Kubernetes Cluster	
U <b>ser</b> wop: :administrator@vsphere.local	
Password *	
Back	Continue

For the **Vendor Type**, CloudControl detects that this is a Tanzu Kubernetes cluster.

- 8. Select Continue.
- 9. On the **Details** tab, monitor the process.



- 10. Select Continue.
- 11. On the **Master Nodes** tab, a list of nodes will be displayed with their name, IP, and hostname information.
- 12. Select Continue.
- 13. In the Enable Access Control dialog, either:
  - a. Select Enable Access Control to enable the ROOT Access Control Trust Manifest. CloudControl will take control of managing access to the cluster. Create a Trust Manifest Access Control Policy to be able to create and manage objects in the cluster.

- b. Select **No, not now** to wait until later. This feature can be enabled after the cluster has been onboarded.
- 14. After the cluster has been imported into CloudControl the cluster dashboard is shown.



# 2.9. View VMware Tanzu Kubernetes cluster inventory

From the **Home** page, select **Inventory > Kubernetes Clusters** to view the **Kubernetes Clusters** page. From here, in depth information of all of the objects in that cluster can be viewed, as well as any tags or policies related to those objects. This information is included in a dashboard or a resource page.

For more information refer to Viewing Kubernetes Inventory in the online documentation.

Also refer to Navigating Kubernetes Inventory View Pages in the online documentation.

# 2.10. Transfer root access control to CloudControl

When root access control is enabled in the Kubernetes cluster, access control of the Tanzu Kubernetes cluster is transferred to CloudControl. This means that management of objects in the cluster will be controlled by CloudControl rules. These rules must be created and defined in CloudControl for the user to be able to create, edit, and delete objects in the cluster.

#### 2.10.1. Before root access control is enabled

During the on-boarding process, root access was not enabled for the imported cluster. As a result, the user can still create objects at the Tanzu level.

For example, the user could create a pod. The pod.yaml file is below:

```
apiVersion: v1
kind: Pod
metadata:
    name: tutum-centos3
spec:
    containers:
        name: tutum-ssh-server3
        image: tutum/centos
```

#### To create the pod:



The pod is created successfully. This process will fail if root access control is enabled using default HyTrust Global Access Control Policy, which denies all operations. See Enable root access control.

To delete the pod:

```
% kubectl get pods
NAME READY STATUS RESTARTS AGE
tutum-centos3 1/1 Running 0 3m57s
% kubectl delete pod tutum-centos3
pod "tutum-centos3" deleted
```

The pod is deleted successfully. This process will fail if root access control is enabled using default HyTrust Global Access Control Policy, which denies all operations. See Enable root access control.

## 2.10.2. Enable root access control

When root access control is enabled for the Kubernetes cluster, access control of the Tanzu Kubernetes cluster is transferred to CloudControl.

To enable root access control:

1. From the Home tab, select Inventory > Kubernetes Clusters.

ENTRUST	CloudControl						<b>:</b> • ?
	Inv	rentory	Sec	urity	Syste	∯ ∯ em	
	AWS Accounts	Kubernetes Clusters	NSX-T	vSphere	VCF	Image Registries	

- 2. Select Management to view the clusters.
- 3. Select the Tanzu Kubernetes Cluster Name link.

This action will display the details about the selected cluster.

ENTRUS	T CloudControl				<b>∷ ∆</b> ?
🐇 🔊 Log Analy	sis 🗙 🔘 Kubernetes Clusters 🗶	s · · · · · · · · · · · · · · · · · · ·			
Cluster	71				🖾 Views 🛛 👻 Actions 🖡
⊙ Node 4	s Namespaces	Deployments	⊕ Pods 43	<ul><li>Containers</li><li>54</li></ul>	∞ Services
	Details "	Configuration Harde	ening Summary 🖉	" Container De	ployment Control
Type IP Address API Server Port Master Nodes	Container Orchestrator 4 6443 1	Assessments R	emediations		Ш
API Version Platform Build Date	22 v1.18.19+vmware.1 linux/amd64 May 14, 2021, 1:26:15 PM	Currently no asses Create a pol	sment policies icy now		
	Configuration Hardening Trend	ling		Container Runtime Violation	15 g <sup>2</sup>
			✓ All containers (active and 1	paused) comply with the policy.	

The Details section of the page shows that Access Control is Disabled.

4. Select the **Disable** link to **Enable Root Access Control**.



#### 5. In the Access Control dialog, set Status to Enabled and select Apply.

After root access is enabled, it is not possible to work with objects directly. For example, the user could create a pod:

```
% kubectl create -f pod.yaml
Error from server (Forbidden): error when creating "pod.yaml": admission webhook "accesscontrol.hytrust.com"
denied the request: Permission Denied by HyTrust Security Policy.
```

In this example, it is not possible to create the pod, as CloudControl now controls permissions on the cluster. To perform these actions, user permissions must be granted through a policy, see Create a Trust Manifest Access Control Policy.

# 2.11. Create a Trust Manifest Access Control Policy

After root access control is enabled in the cluster, the user is unable to create objects in the cluster. This is because cluster permissions are then managed by CloudControl.

This section describes the process to create a Trust Manifest Access Control policy, so a user can manage objects in the cluster.

## 2.11.1. Log analysis

Use the logs in the system to check why access has been denied for a request. From this, create a Trust Manifest Access Control Policy to allow the user to perform the request successfully. For more information refer to Log Analysis in the online documentation.

1. Go to the Home tab, select Security > Log Analysis.

2. Select the record that shows the **Deny** status to see the reason for the denial.

Look for an entry similar to the following:

Authorization d needs to be at le	enied due to no rules applying to the user via the configured a east one direct role association by way of user name or group(	ccess control pol s)	icy for the resource(s) with name(s) '['  '. There
Privileges	Compute.ContainerNamespace.Create	Date	Mar 24, 2022, 9:52:42 AM
Resources	(TanzuKubernetesCluster)	Priority	A WARN
Source	cchytrustvcf.local ( )	Status	Deny
Destination	cchytrustvcf.local ( )	User	kubernetes-admin
Protocol	RESTAPI	Groups	
Policy	Enforced	Roles	
Msg ID	AUZ0001	Action	Compute.ContainerNamespace.Create
Category	AUZ	Vendor Action	Compute.ContainerNamespace.Create
		Trust Manifest	HyTrust Global Trust Manifest for Access Control

In this example, a request to create a pod was denied.

Now create a Trust Manifest Access Control Policy to allow the user to create the pod.

### 2.11.2. Create the Access Control Policy

This section describes how to use an Access Control Policy to allow users to create pods in the Tanzu cluster.

In the example below, the Access Control Policy will allow the kubernetes: admin user to create pods in the cluster. Any other user in the system will be denied access.

For details of how to create an Access Control Policy, refer to Creating an Access Control Trust Manifest from the CloudControl GUI in the online documentation.

- 1. From the Home tab, select Security > Trust Manifests.
- On the Manage Trust Manifests page, select Create Trust Manifest. This is the plus sign in the GUI.
- On the Details tab of the Create Trust Manifest page, enter the Name and optional Description for the Trust Manifest.
- 4. For Policy Type, select Access Control.
- 5. In the Access Control Policy section, enter the name of the rule. That is, ACP.
- 6. For Rule Type, select Allow.
- 7. For Role, select ASC\_ContainerInfraAdmin.

This is the role that controls all operation related to creating objects in cluster.

- 8. Under Subjects:
  - a. For Type, select Kubernetes.
  - b. For Group or User, add:
    - k8s::user:kubernetes:admin

#### k8s::user:sso:administrator@vsphere.local

- 9. Select **Validate** to validate the policy.
- 10. Select **Save** to save the policy.
- 11. Select **Publish** to publish the policy.

When the policy is published, it prompts the user to assign resources to the policy. Select the Tanzu Kubernetes cluster and select **Assign**.

12. Select Close.

## 2.11.3. Test the Access Control Policy

To test if the Access Control policy is working, create the pod:

```
% kubectl create -f pod.yaml
pod/tutum-centos3 created
```

The request is successful.

To test the deletion of a pod:

% kubectl delete pod tutum-centos3

Error from server (Forbidden): admission webhook "accesscontrol.hytrust.com" denied the request: Permission Denied by HyTrust Security Policy, Resource not found.

In this example, the resource is not found in CloudControl. This is because the CloudControl has not updated its cluster inventory yet. When a cluster is onboarded, it creates an internal job that runs every 5 minutes to update the cluster inventory. This means that the only way to delete the pod in this case is to:

- Wait for the cluster inventory job to complete.
- Manually sync the inventory.

To manually sync the inventory:

- 1. In the Cluster Detail tab, select Actions > Sync Inventory.
- 2. Select Initiate Sync.

After the sync completes, delete the pod. For example:

% kubectl delete pod tutum-centos3

pod "tutum-centos3" deleted

The pod deletes successfully.

## 2.12. Image registries

An image registry is a service that stores repositories and images. Each repository contains one or more version of the same image. All images in a repository must have the same name, and be differentiated by tags. The tag name corresponds to the version of the image. The most recent image is also tagged as 'latest'.

Image registries are not protected by CloudControl, but adding a registry allows CloudControl to discover valuable information about the registry, such as the number of images and their specific vulnerabilities.

This allows more detailed rules when creating an Image Deployment Control Policy which will be discussed later in this guide. Entrust strongly suggests adding private image registries to CloudControl for better control during image deployment in Kubernetes.

Add the private registry to CloudControl: xxxx.yyyy.zzz

 In the Home tab, Select Inventory > Image Registries to view the registries that have been added to CloudControl.



2. On the Image Registries page, select Actions > Add Registry.

If there are no registries in the system, select the **Add Registry** link on the **Image Registries** page.

- 3. On the Add Registry page, in the About tab enter the following information:
  - a. Name Name of the registry
  - b. IP/FQDN Enter the IP Address or FQDN for the registry.
  - c. Port Enter the registry port used in configuration of the local registry.
  - d. **Authorization Schema** Choose one of the following to use for authorization: **BASIC** or **OAUTH**.

- e. User Enter the username for the registry.
- f. Password Enter the password for this user.
- g. Description Enter an optional description.
- 4. Select Continue.

Add Registry	×
Add Registry	
1: About 2: Details	
Name*	
registry.	
Description	
Docker registry used by	
P/FQDN *	
registry.	
Port*	
443	
Authorization Scheme	
BASIC	<b>v</b>
Jser Name *	
course and a second s	
Password *	

If certificate authority has not already been added, the system prompts the user to add one.

- 1. In the Missing Certificate Authority window, select Install Certificate Authority Now.
- 2. On the Install Certificates page, do one of the following:
  - a. Select Import and then select Browse to locate the certificate file.
  - b. Select **Enter Text**, then paste the contents of the certificate as plain text into **Certificate Data**.
- 3. Select Continue.
- 4. On the **Details** page, monitor the process.
- 5. Select **Continue** to view the dashboard for the newly added registry.

() EN	ITRUST	CloudCo	ontrol									4	?
* 8	Image Registries	×	🔛 registry. 🗙 🗙										
Actions										•			
Name ID Resourc Platform	Details Name registry. ID 1541798b-fd54-f60-addd Resource Type ContainerRegistry Platform None detected								Tags No tags are curre Assign M	ntly assigned			
						lmag	jes						
Filter											Acti	ions	•
	Name	-	Image ID	0	Image Tag 🜼	Vulnerab	ilities	Signature 0	Containers	Create Time			
	aw-centos7nshiel	dibm	sha256:4b4b5a4726d3b4	÷.	latest	Not assses	sed	true	0	Jun 2, 2021, 9:25:10 AM		» O	*
	aw-nshieldproxy		sha256:b7d6c622e3972f6		latest	Not assses	sed	true	0	Jan 12, 2021, 5:35:17 PM	-	<b>0</b> ♦	
	aw-rh8nshieldibm		sha256:d5e8cd3b1d86ccf		withTouch	Not assses	sed	true	0	Jun 8, 2021, 1:14:37 PM	-	<b>0</b> ♦	
	aw-rh8nshieldibm		sha256:fb0627e7c24ba07		testing	Not assses	sed	true	0	Jun 17, 2021, 5:31:04 PM	-	<b>0</b> ♦	
	aw-rh8nshieldibm		sha256:eb9035c83f8fbbdf		latest	Not assses	sed	true	0	Jun 15, 2021, 9:42:19 AM	-	<b>0</b> ♦	
	busybox		sha256:2131f09e4044327		latest	Not assses	sed	true	0	Jun 29, 2020, 4:21:41 PM	-	» O	
	cv-12.71-nshield-	ар	sha256:6dedb82d073382		latest	Not assses	sed	true	0	Sep 16, 2021, 9:52:37 AM	-	<b>0</b> ♦	
Showing	cv-12.71-nshield- g 1 to 8 of 47 records	hw (0 Selec	sha256:df9ee225b06a90e		latest	Not assses	sed	true	0	Sep 16, 2021, 9:51:44 AM	*	<b>0</b>	*

Now create an Image Deployment Control Policy, see Image Deployment Control Policy.

# 2.13. Image Deployment Control Policy

The Image Deployment Control Policy controls how images are deployed in the Tanzu Kubernetes cluster managed by CloudControl. As part of a Trust Manifest, it allows the user to determine what images from a registry are safe to be added to protected clusters.

CloudControl enforces image security using Image Deployment Control Policies, which are comprised of one or more deployment rules:

#### 2.13.1. Private registry rules

Private Registries

Allows the user to enter a list of private registries, either onboarded or not, to be evaluated with the trust manifest. Only the images from registries listed in the **Allowed Registries** section are evaluated to see if they can be deployed. Images from all other registries will be denied.

Signature Rule

Allows the user to deny images that do not have an associated digital signature.

• Attributes Rule

Allows the user to deny or deploy images based on their image ID or image name.

Vulnerabilities Rule

Allows the user to deny or deploy images based on CVSS scores or specific CVEs.

## 2.13.2. Public registry rules

A public registry rule enables images from public registries to be deployed in the environment without any evaluation.



Entrust strongly recommends leaving the public registry rule set to ENABLED and not allowing public registries to be deployed. If a public registry must be used, then leave the rule set to ENABLED and enter that specific registry into the allowed registries. This will allow only that specific registry image to be deployed, and will prevent all other public registry images from deployment.

## 2.13.3. Other considerations

Rules can either have a True or False value and can also include a 'stop processing' clause. Deployment rules in a policy are evaluated in the following order:

- If False, the image will not be deployed, and no further rules are evaluated.
- If True, AND there is a 'stop processing' clause, the image is allowed to be deployed and no further rules are evaluated.
- If True, the next rule in the policy is evaluated. If this is the only rule, then the image is allowed to be deployed.
- If all rules are True, then the image is allowed to be deployed.



Entrust recommends always using the image SHA as it is a unique identifier for the images. Pods can be created by using either an image name with tag, or an image name with SHA, and in many cases images with the same SHA could have been tagged with different tags. For example, a single image named **TestImage** could have different tags, **TestImage:3**, **TestImage:4**, and **TestImage:5**, but all these images will have the same SHA because the underlying image is the same for all three of them.

When any Image Deployment Control Policy rule is created, use the image name with SHA to ensure that the intended image is evaluated no matter what tags are there. When an image name with tag is used, such as **TestImage:3**, then only the image that matches that specific tag will be selected. The other images, TestImage:4 and TestImage:5 will not be

evaluated.

## 2.13.4. Create an Image Deployment Control Policy

This section will show how an Image Deployment Control Policy is used to control which images are allowed/denied in the deployment.

For more information refer to Creating a Deployment Control Trust Manifest from the CloudControl GUI in the online documentation.

- 1. From the Home tab, select Security > Trust Manifests.
- 2. On the Manage Trust Manifests page, select Actions > Create Trust Manifest.
- On the Details tab of the Create Trust Manifest page, enter the Name and optional Description for the trust manifest.
- 4. For Policy Type, select Deployment Control.
- 5. In the Deployment Control Rules: Private registries section:
  - a. For Allowed Registries, enter the registries to allow. That is:
    - Enter the registry that was onboarded: **xxxxx.yyyy.zzz**.
    - Registries can be existing onboarded registries or registries that will be onboarded later.
    - Registries that have not been onboarded are depicted with a yellow warning icon.
- 6. In the Deployment Control Rules: Rules section:
  - a. For **Signature Rule**, select either **Enabled** or **Disabled**. This determines whether to deny an image when no signature is present.
- 7. In the Deployment Control Rules: Rules section:
  - a. For **Attribute Rule**, select **Enabled** or **Disabled** to determine whether to evaluate using attributes, and then complete the following:
    - i. **Name** Enter the name of the rule. The name cannot contain any special characters.
    - ii. Exemption List Deploy on Match

Select **ENABLED** or **DISABLED** to determine whether to use this when evaluating.

If **ENABLED**, use the + and - symbols to add the following criteria:

- Image ID Enter the image ID in SHA format to match.
- Image Name Enter the Name and Tag Regex to match.

If there is a match, the image will immediately be deployed, and no other deployment policy rules will be evaluated.

If there is no match, continue to the next enabled step.

If there are no other steps, continue to the next rule in the deployment policy.

iii. Whitelist - Deny on No Match

Select **ENABLED** or **DISABLED** to determine whether to use this when evaluating.

If **ENABLED**, use the + and - symbols to add the following criteria:

- Image ID Enter the image ID in SHA format to match.
- Image Name Enter the Name and Tag Regex to match.

If there is no match, the image will immediately be denied, and no other deployment policy rules will be evaluated.

If there is a match, continue to the next enabled step.

If there are no other steps, continue to the next rule in the deployment policy.

iv. Blacklist - Deny on Match

Select **ENABLED** or **DISABLED** to determine whether to use this when evaluating.

If **ENABLED**, use the + and - symbols to add the following criteria:

- Image ID Enter the image ID in SHA format to match.
- Image Name Enter the Name and Tag Regex to match.

If there is a match, the image will immediately be denied, and no other deployment policy rules will be evaluated.

If there is no match, continue to the next rule in the deployment policy.

b. Optional. In the **Public Registries** section, add public registries to be deployed without any evaluation.

Entrust recommends leaving this section enabled, but not entering any values for **Allowed Registries**.

- 8. Select one of the following:
  - Validate Validate the draft or existing trust manifest.

- ° **Save** Save the trust manifest as a draft.
- **Publish** Publish the trust manifest.

## 2.13.5. Image Deployment Control Policy examples

In this example, an Image Deployment Control Policy is created. It will only allow images that are in the private registry that was onboarded earlier. Any other image that is not in the private registry will be blocked and will not run.

To be able to publish the policy:

- The Restrict Public Registry rule will be enabled.
- A fake registry name **abc** will be added to the exception list. This will force the policy to only allow images in the private registry.

Private Registries	
Allowed Registries *	
圈 registry. :443 ×	
Rules Evaluation will happen in the following order:	Expand All   Collap
🗸 Signature Rule	
mages without a valid signature will be denied.	LI SABL
> Attributes Rule	LI SAEL
> Vulnerabilities Rule	
	USAH
Public Registries	UNXE
Public Registries	U TANK
Public Registries <ul> <li>Restrict Public Registry Rule</li> <li>Adding public registries will allow all images in these registries to be deployed without any further</li> </ul>	user sweet
Public Registries ✓ Restrict Public Registry Rule ▲ Adding public registries will allow all images in these registries to be deployed without any further This is against recommended best practice.	ursea Escer
Public Registries         Public Registry Rule         Adding public registries will allow all images in these registries to be deployed without any further         This is against recommended best practice.         Allowed Registries	uner
Public Registries	uner Prove revaluation.
Public Registries	revaluation.
Public Registries ✓ Restrict Public Registry Rule Adding public registries will allow all images in these registries to be deployed without any further This is against recommended best practice. Allowed Registries abo ×	revaluation.

After this policy is published, it is possible to deploy an image that is not in the registry.

For example, using the **pod.yaml** file again:

apiVersion: v1
kind: Pod
metadata:
name: tutum-centos3
spec:
containers:
- name: tutum-ssh-server3
image: tutum/centos



The YAML file is not using an image from the private registry.

```
% kubectl create -f pod.yaml
Error from server (Forbidden): error when creating "pod.yaml": admission webhook "deploymentcontrol.hytrust.com"
denied the request: Permission Denied by HyTrust Security Policy.
```

In this example, the pod was not deployed because it uses an image from the **tutum** registry.

To use an image from a private registry using a different YAML file. For example, podinternal-registry.yaml with the following content:

```
apiVersion: v1
kind: Pod
metadata:
    name: internal-registry-centos
spec:
    imagePullSecrets:
    - name: regcred
    containers:
    - name: internal-registry-centos
    image: xxxxxx.yyyy.zzz/cv-centos:latest
```

Assuming the ImagePullSecret **regcred** which has the credentials to access the private registry has been created, create the pod:

```
% kubectl create -f pod-internal-registry.yaml
pod/internal-registry-centos created
```

The deployment is successful, because the Image Deployment Control Policy allows images from the private registry.

Add the **tutum** external registry to the external registry exception list, so an external image can also be deployed. For example:

Deployment Control Rules

red Registries *	
registry. 443 ×	
tion will happen in the following order:	Expand All   Co
Signature Rule Images without a valid signature will be denied.	LA S
Attributes Rule	Ins
Vulnerabilities Rule	US
2 Registries Restrict Public Registry Rule	
A Adding public registries will allow all images in these registries to be deployed without any further evaluation. This is against recommended best practice.	on.
Allowed Registries	
	registrices         registry       443 >         tion will happen in the following order:       Inages without a valid signature will be denied.         Signature Rule       Images without a valid signature will be denied.         Attributes Rule       Images without a valid signature will be denied.         Signatures       Registries Rule         Autributes Rule       Images without a valid signature will be denied.         Attributes Rule       Images without a valid signature will be denied.         Autributes Rule       Images without a valid signature will be denied.         Autributes Rule       Images without a valid signature will be denied.         Autributes Rule       Images without a valid signature will be denied.         Autributes Rule       Images without a valid signature will be denied.         Autributes Rule       Images without a valid signature will be denied.         Statistics       Registries         Adding public registries will allow all images in these registries to be deployed without any further evaluation.         This is against recommended best practice.         Allowed Registries

Create the pod using **pod.yaml** file again:

% kubectl create -f pod.yaml
pod/tutum-centos3 created

The deployment policy is working as designed.

Expand the policy by further restricting what images can be deployed from the private registry.

To determine what images are in the private registry:

1. In the **Home** tab, Select **Inventory > Image Registries** and select the private registry that was onboarded.

		loudControl										
	Image Registries	× 🗄 r	registry. 🗙									
reç	gistry.	-									Acti	on
			Details						T	lags		
ne	re	egistry.							_			
souri	te Type C	5dff98b-fd54 ontainerReg	-4503-addd iistry									
tform	1 N	one detected	d						No tags are c	urrently assigned		
									Assi	ign Now		
						lma	iges					
lter											Action	s
ter	Name	▲ Ima	age ID	0	lmage Tag ≎	Vulnera	bilities	Signature 0	Containers	Create Time	Action	S
ter	Name aw-centos7nshieldi	<mark>▲ Im</mark> a ibm sha	<b>age ID</b> 1256:4b4b5a4726d3b4	0	Image Tag $\diamond$ latest	Vulnera Not asse	bilities	Signature 0	Containers 0	Create Time Jun 2, 2021, 9:25:10 AM	Action	S
ter	Name aw-centos7nshieldi aw-nshieldproxy	▲ Im; ibm sha sha	age ID 1256:4b4b5a4726d3b4( 1256:b7d6c622e3972f6	0	Image Tag ≎ latest latest	Vulnera Not assse	bilities Issed	Signature 0 true true	Containers 0 0	Create Time           Jun 2, 2021, 9:25:10 AM           Jan 12, 2021, 5:35:17 PM	Action © 0 © 0	S
	Name aw-centos7nshieldi aw-nshieldproxy aw-rh8nshieldibm	▲ Ima ibm sha sha sha	age ID 256-454554726d3b4( 256-67d6c622e3972f6 2266-d5682cd3b1d86ccf	0	Image Tag $\diamond$ latest latest withTouch	Vulnera Not asse Not asse	bilities Issed Issed	Signature ¢ true true true	Containers 0 0 0	Create Time Jun 2, 2021, 9:25:10 AM Jan 12, 2021, 5:35:17 PM Jun 8, 2021, 1:14:37 PM	Action:	S
	Name aw-centos7nshieldi aw-nshieldproxy aw-rh8nshieldibm aw-rh8nshieldibm	▲ Ima ibm sha sha sha sha	age ID 256:4b4b5a4726d3b4( 256:b7d6c622e3972f6 256:d5e8cd3b1d86ccf 256:b0627e7c24ba07	0	Image Tag o latest latest withTouch testing	Vulnera Not asse Not asse Not asse	bilities issed issed issed issed	Signature true true true true true	Containers 0 0 0 0	Create Time Jun 2, 2021, 9:25:10 AM Jan 12, 2021, 5:35:17 PM Jun 8, 2021, 1:14:37 PM Jun 17, 2021, 5:31:04 PM	Action	S
	Name aw-centos7nshieldi aw-nshieldproxy aw-rh8nshieldibm aw-rh8nshieldibm	▲ Ima ibm sha sha sha sha	age ID 256:4b4b5a4726d3b4( 256:b7d6c522e3972f6 256:d5e8cd3b1d86ccf 2256:bb0627e7c24ba07 256:eb9035c83f8bbd(	0	Image Tag latest latest withTouch testing latest	Vulnera Not assse Not assse Not assse Not assse	bilities issed issed issed issed issed issed	Signature o true true true true true true	Containers 0 0 0 0 0 0 0	Create Time Jun 2, 2021, 9:25:10 AM Jan 12, 2021, 5:35:17 PM Jun 8, 2021, 1:14:37 PM Jun 17, 2021, 5:31:04 PM Jun 15, 2021, 9:42:19 AM	Action	S
	Name aw-centos7nshieldi aw-nshieldproxy aw-rh8nshieldibm aw-rh8nshieldibm aw-rh8nshieldibm busybox	▲ Im: ibm sha sha sha sha sha sha sha	age ID 2256:4b4b5a4726d3b4( 2256:b7d6c622e3972f6 2256:d5e8cd3b1d86ccf 2256:b0627e7c24ba07 2256:eb9035c83f8fbbdf 2256:2131f09e4044327	0	Image Tag ○ latest latest withTouch testing latest latest	Vulnera Not assee Not assee Not assee Not assee Not assee	bilities issed issed issed issed issed issed	Signature 🗘	Containers 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	<ul> <li>Create Time</li> <li>Jun 2, 2021, 9:25:10 AM</li> <li>Jan 12, 2021, 5:35:17 PM</li> <li>Jun 8, 2021, 1:14:37 PM</li> <li>Jun 17, 2021, 5:31:04 PM</li> <li>Jun 15, 2021, 9:42:19 AM</li> <li>Jun 29, 2020, 4:21:41 PM</li> </ul>	Action:	S
	Name aw-centos7nshieldi aw-nshieldproxy aw-nb8nshieldbm aw-nb8nshieldbm aw-nb8nshieldbm busybox cv-12.71-nshield-ap	<ul> <li>Im.</li> <li>ibm sha</li> <li>sha</li> <li>sha</li> <li>sha</li> <li>sha</li> <li>sha</li> <li>sha</li> <li>sha</li> <li>sha</li> <li>sha</li> </ul>	age ID 2256:4b4b5a4726d3b4( 2256:b7d6c622e3972f6 2256:d5e8cd3b1d86ccf 2256:tb0627e7c24ba07 2256:eb0035c83f8fbbdf 2256:2131f09e4044327 2256:66dedb82d073382:	0	Image Tag 0 latest 2 with Touch 2 latest 2 latest 2 latest 2 latest 2	Vulnera Not asse Not asse Not asse Not asse Not asse Not asse	bilities issed issed issed issed issed issed issed	Signature  Signature True True True True True True True T	Containers 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	<ul> <li>Create Time</li> <li>Jun 2, 2021, 9:25:10 AM</li> <li>Jan 12, 2021, 5:35:17 PM</li> <li>Jun 8, 2021, 1:14:37 PM</li> <li>Jun 17, 2021, 5:31:04 PM</li> <li>Jun 15, 2021, 9:42:19 AM</li> <li>Jun 29, 2020, 4:21:41 PM</li> <li>Sep 16, 2021, 9:52:37 AM</li> </ul>	Action (0) (0) (0) (0) (0) (0) (0) (0) (0) (0)	S

2. Look at the images that are available in the registry.

Change the deployment policy to only allow images with name **cv-centos** and with the **latest** tag. Any other image in the private registry that does not match this requirement in the name will be blocked.

To do this, add an **Attribute Rule** to the deployment policy. For example:

Name *				
CV Images Only				
Evaluation will happen in the follow	ing order:			
Step 1. Exemption List				
Deploy on Match				
If any of the following criteria mate to the next enabled step.	ches, <u>deploy</u> the image and	stop processing the De	ployment Policy. If no criter	ia matches, <u>co</u>
Criteria *				
Image Name 🗙 👻 Name F	Regex * cv-centos	Tag Regex *	latest	00
Deny on No Match				
Deny on No Match If none of the following criteria mator the next enabled step.	tches, <u>deny</u> the image and	stop processing the De	ployment Policy. If any criter	ria matches, <u>co</u>
Deny on No Match If none of the following criteria mato the next enabled step. Criteria *	tches, <u>deny</u> the image and	stop processing the De	ployment Policy. If any crite	ria matches, <u>co</u>
Deny on No Match If none of the following criteria ma to the next enabled step. Criteria * Image Name X * Name F	tches, <u>deny</u> the image and Regex *	stop processing the De Tag Regex *	ployment Policy. If any criter	ria matches, <u>co</u>
Criteria * Market Step 3. Blacklist Contact	tches, <u>deny</u> the image and Regex * <u>cv-*</u> ches, <u>deny</u> the image and st	Tag Regex *	loyment Policy. If any criter latest	ria matches, <u>co</u>
Criteria Deny on No Match If none of the following criteria me to the next enabled step. Criteria * Mame F Step 3. Blacklist Deny on Match If any of the following criteria mati- next rule. Criteria	tches, <u>deny</u> the image and cegex * $cv-*$	Tag Regex *	latest ent Policy. If any criter	ria matches, <u>co</u>
Criteria Beny on No Match If none of the following criteria me to the next enabled step. Criteria * Image Name X * Name F Step 3. Blacklist Deny on Match If any of the following criteria met next rule. Criteria Select Criteria *	ttches, <u>deny</u> the image and Regex * cv-* ches, <u>deny</u> the image and st	Tag Regex *	ployment Policy. If any criter latest nent Policy. If no criteria mat	ria matches, <u>co</u>

Now try to deploy the **busybox** image in the private registry. To do this, create a file called **pod-internal-busybox.yaml** with the following content:

```
apiVersion: v1
kind: Pod
metadata:
    name: internalregistry-busybox
spec:
    imagePullSecrets:
        name: regcred
        containers:
            name: internalregistry-busybox-test
            image: xxxxxx.yyyy.zzz/busybox
```

When this is deployed, it should fail and deny the deployment. For example:

% kubectl create -f pod-internal-busybox.yaml

Error from server (Forbidden): error when creating "pod-internal-busybox.yaml": admission webhook "deploymentcontrol.hytrust.com" denied the request: Permission Denied by HyTrust Security Policy.

Now deploy the **cv-centos** image in the private registry. To do this, use the **pod-internal-registry.yaml** file again.

```
% kubectl create -f pod-internal-registry.yaml
```

pod/internal-registry-centos created

The deployment is successful.

This demonstrates how to harden the Image Deployment Control Policy.

## 2.13.6. Image Deployment Control Policy based on vulnerabilities

When onboarding a private registry into CloudControl, the system checks the number of vulnerabilities in each image in the registry. Below is an example of a private registry when it was onboarded.

Name	•	Image ID	0	Image 🗘	Vulnerabilities	Signature 0	Contain	c		
ojw-ab5		sha256:7d2badb2abefa86b79515671f3581cb9f44895ac		latest	0	true	0	N	<b>&gt; 0</b>	•
ojw-ckst		sha256:365215cb7643101318e37b590519fd0e5173972		ocs1	0	true	0	N	<b>&gt; 0</b>	
ojw-ckst-kmdl		sha256:f03e3350c05abd4335a38e71baea030942fd4aa		setr	0	true	0	N	<b>&gt; 0</b>	
ojw-httpd		sha256:6e26c808ef1f055a2d82d8951c0feb94c5c6585c		latest	<mark>69</mark> 101	true	0	N	≫ 0	
ojw-httpd-ast		sha256:71c5d377ecfc3fe8276a4b235cef8e22f9d08107a		latest	69 101	true	0	N	<b>&gt; 0</b>	II.
ojw-httpd-err		sha256:3e319d6460418325a5ed1545bf514dc328f003b		latest	69 101	true	0	N	<b>&gt; 0</b>	
oiw-httpd-nsc		sha256:d2857a6b2afc24622d96e1562f57acfe557fc7cc		latest	69 101	true	0	N	<b>&gt; 0</b>	*

For each image, CloudControl collects the number of vulnerabilities and their types. Select a link in the **Vulnerabilities** column to view a pop-up with tabs that include the details.

iage 🖾 ojw-httpd (Last	Details V	ulnerabilities Containers
Severity = LOW >	Severity = NEGLIGIBLE >	3 ×
/ulnerability	≎ <u>Severity</u>	≎ Description
VE-2020-29363	NEGLIGIBLE	An issue was discovered in p11-kit 0.23.6 through 0.2
VE-2018-6829	NEGLIGIBLE	cipher/elgamal.c in Libgcrypt through 1.8.2, when use
VE-2021-20193	NEGLIGIBLE	A flaw was found in the src/list.c of tar 1.33 and earlier
VE-2019-9923	NEGLIGIBLE	pax_decode_header in sparse.c in GNU Tar before 1
VE-2005-2541	NEGLIGIBLE	Tar 1.15.1 does not properly warn the user when extra
VE-2018-1000654	NEGLIGIBLE	GNU Libtasn1-4.13 libtasn1-4.13 version libtasn1-4.13
VE-2019-17543	LOW	LZ4 before 1.9.2 has a heap-based buffer overflow in
VE-2011-3374	NEGLIGIBLE	It was found that apt-key in apt, all versions, do not co
VE-2019-18276	NEGLIGIBLE	An issue was discovered in disable_priv_mode in shell

The **Vulnerabilities** tab lists each vulnerability with their CVE, severity, and description. Select the CVE link to view details about the CVE. For example:

Image 🖬 ojw-ht	Vulnerability	Details		×		×
Filter Severity Vulnerability CVE-2020-29363 CVE-2018-6829 CVE-2021-20193 CVE-2021-20193	Name Severity Fixed By CVE Link Description	CVE-2019-17543 COW Attps://security-tracker.de Z4 before 1.9.2 has a hea Z4_write32 (related to L2 applications that call L24 This issue can also lead I rendor states "only a few API are at risk."	bian.org/tracker/CVE-2019-17543 p-based buffer overflow in 4_compress_destSize), affecting compress_fast with a large input o data corruption.) NOTE: the specific / uncommon usages of the Close	C∕ª he	rough 0.2 when use and earlier before 1	*
CVE-2005-2541	NEG	IGIBLE Tar 1	.15.1 does not properly warn the	user v	vhen extra	

With this information on hand, create/modify the Image Deployment Control Policy to allow/deny deployments based on the number of vulnerabilities an image contain.

For example, modify the current Image Deployment Control Policy to allow any image from the private registry, but only if it has no vulnerabilities. This requires the use of two images from the private registry:

- cv-centos which has no vulnerability.
- ojw-httpd which has some vulnerabilities.

#### 2.13.6.1. Modify the Image Deployment Control Policy

Modify the policy by disabling the **Attributes Rule** and enabling the **Vulnerabilities Rule**. The default thresholds will be appropriate for testing.

- 1. From the **Home** tab, select **Security > Trust Manifests**.
- 2. On the **Manage Trust Manifests** page, select the deployment control policy created earlier.

- 3. Select Edit.
- 4. Disable the Attribute Rule section under Rules, under Private Registries.
- 5. Enable the Vulnerability Rule section.
  - a. Give a name for the rule, for example **My Vulnerability Rule**.
  - b. Take the defaults for the **Deny deployment thresholds** values.

The **ojw-httpd** image has more than 30 low severity vulnerabilities.

6. Select Validate and the select Apply.

Priva	ite Reç	listries	
Allov	ved Red	jistries *	ENA
E	registry	. :443 ×	
	-		
Evalu	s ation wil	I happen in the following order:	Expand All   Collaps
~	Signat	ure Rule	
	Imaga	a without a walid airpature will be denied	DIBABLEC
	inage	s without a valid signature will be defried.	
	A 44	des Duls	
	Attribu		DIBABLED
<u> </u>	Vulner	akilijina Dula	
~	vumer		ENABLED
	Name	*	
	My \	/ulnerability Rule	
	Deny	deployment if thresholds exceed:	
	0	or more defcon1 and critical severity vulnerabilities	
	1	or more high severity vulnerabilities	
	5	or more medium severity vulnerabilities	
	0	of more medium severity vulnerabilities	
	30	or more low and negligible severity vulnerabilities	
	Whitelist		
	Ignoro	DIMBLED	
	ignore	anesholds for the following valuerabilities.	

Test the policy, see Test the policy.

#### 2.13.6.2. Test the policy

To test the policy, attempt to deploy the **cv-centos** image. Use the same **pod-internal-registry.yaml** file again.

```
% kubectl create -f pod-internal-registry.yaml
pod/internal-registry-centos created
```

The deployment succeeds.

Now attempt to deploy the **ojw-httpd** image. To do this, create a file called **pod-internalcve.yaml** with the following content:

```
apiVersion: v1
kind: Pod
metadata:
    name: internalregistry-ojw-httpd
spec:
    imagePullSecrets:
        - name: regcred
        containers:
            - name: internalregistry-ojw-httpd
            image: xxxxxx.yyyy.zzz/ojw-httpd:latest
```

It should fail and be denied.

```
% kubectl create -f pod-internal-cve.yaml
Error from server (Forbidden): error when creating "pod-internal-cve.yaml": admission webhook
"deploymentcontrol.hytrust.com" denied the request: Permission Denied by HyTrust Security Policy.
```

Examine the logs to see the denial.

- 1. Go to the Home tab, select Security > Log Analysis.
- 2. Select the record that shows the **Deny** status to see the reason for the denial.
- 3. Look for something like this:

Container Imag (latest)` has Vul	e `registry. :443/ojw-httpd@sha256:6e26c808ef1f0 nerabilities that exceed the threshold.	155a2d82d8951c	0feb94c5c6585c9c5cef90ad7f394dd09290b5 tag:
Privileges		Date	Mar 16, 2023, 2:03:49 PM
Resources	(ContainerOrchestrator)	Priority	A WARN
Source	cchytrust.local ( )	Status	Deny
Destination	cchytrust.local ( )	User	sso:Administrator@vsphere.local
Protocol	RESTAPI	Groups	
Policy	unknown	Roles	
Msg ID	K8S0004	Action	Deploying Image
Category	POL	Vendor Action	Deploying Image

This feature from CloudControl allows the user to put in place image deployment control policies that can harden the organization deployment requirements and tailor this capability according to the organization needs.

# 2.14. Configuration hardening

Configuration hardening allows the user to improve the security posture of Kubernetes environments by hardening the configuration to meet the company's specific security policy and industry best practices. By automating the hardening process, the user can reduce the operational burden during a compliance audit.

With CloudControl, the user can:

- · Create and customize templates to use in configuration hardening checks.
- Assess and remediate your environments against the configuration hardening checks

• Review dashboards, reports and alerts to monitor the results of assessments and remediations.

## 2.14.1. About templates

CloudControl uses templates to support all configuration hardening activities. CloudControl supports the following types of templates:

- **Catalog templates** Read-only collection of hardening operations. There is a Kubernetes operations catalog of templates that can be used.
- **System templates** Read-only collection of operations derived from a catalog template for a given compliance standard
- **Custom templates** Templates created by users. In most cases, they are copied or cloned from existing system or catalog templates. Custom templates can be modified and used in configuration hardening policies.



CloudControl also includes sample custom templates that can immediately be used in a policy.

Templates can contain both assessment and remediation hardening operations. Review all operations in the template to ensure that any parameter values are set appropriately for the infrastructure requirements.

## 2.14.2. About policies

Configuration hardening policies are used to run custom templates. Each policy associates a template with one or more resources or tag-based resource configurations and can be run manually or as a scheduled activity. Policies can either assess or remediate a resource but cannot do both.

## 2.14.3. More information

Consult the online documentation for more information on Configuration Hardening.

## 2.14.4. Creating a configuration hardening policy example

For this guide a configuration hardening policy will be created based on one of the templates available.

- 1. From the Home tab, select Security > Configuration Hardening.
- 2. On the Configuration Hardening Management page, select the Policies tab.
- 3. Select the Create (+) button.
- 4. In the **Create Policy** wizard on the **Select Type** page, select the type of policy that you want to create. This can be one of the following:
  - Assess Only Runs operations on the host to compare the parameter values specified in the template with the actual values on the host.
  - Remediate Only Modifies the parameter values on the host in order to match the values specified in the templates.
- 5. Select Assess Only.

Create Policy 👳	×							
1: Select Type = 2: Details = 3: Templates = 4: Resources = 5: Schedule								
Assess Only Assessment is the process of running operations, or tests, on the resource to compare the parameter value specified in the template with the actual value configured on the resource.								
Remediate Remediation modifies parameter values on the resources based on the desired values defined in templates. Will only run remediation on operations that are selected for remediation.								
Cancel Con	ntinue							

- 6. Select **Continue**.
- 7. On the **Details** page, enter the name and optional description of the policy, and specify whether the policy is enabled.

Create Policy S My Configuration Hardening Policy									
1: Select Type 🖌 – 2: Details – 3: Templates – 4: Resources – 5: Schedule									
Name *									
My Configuration Hardening Policy									
Status LIVELED									
Description 219 Charact	ters								
Test configuration hardening policy									
Back	Cancel Continue								

- 8. Select Continue.
- 9. On the **Templates** page, select the **resource type** for the policy. This can be one of the following:
  - AWS Account Runs AWS-related templates against your AWS environment.
  - ° ESXi Runs vSphere related templates against your ESXi hosts.
  - Kubernetes Runs Kubernetes related templates against your Kubernetes environment.

- NSXDataCenter Runs NSX-T related templates against your NSX-T environment.
- 10. Select Kubernetes as the template to run against your environment.
- 11. The template list displays the name, description and type of operations Select a template that contains the type of operations that you selected for the policy.
- 12. Select **Kubernetes HyTrust Best Practice with HyTrust default values** template. This template is used in the example.

Creat	reate Policy 🛞 My Configuration Hardening Policy										
1: Sel	lect Type 🗸	2: Details 🗸	H	3: Templates	4: Resources	-	5: Schedule				
Resou	гсе Туре										
Kube	rnetes									Ŧ	
Selec The and	t a Template following is a used in this p	E Kubernete: list of templates olicy.	s - H for t	lyTrust Best Prac he selected resc	tice with HyTrust burce type. If a sys	defa sterr	ault values h template is sele	cted, :	a clone of the template will be creat	ed	
	Template N	lame	٥	Description	ı 0	, -	Туре	0	Operations		
	Kubernetes -	HyTrust Best Pr		This template i	is based on Hy	(	Custom		53 Assess, 5 Remediate		
	Kubernetes -	HyTrust Best Pr		This is a refere	ence template	ę	System 53 Assess, 5 Remediate				
	Kubernetes 1	.23.0 - CIS Kub.		This is a refere	ence template	ę	Bystem		53 Assess, 5 Remediate		
Showing Back	g 1 to 3 of <b>3</b> reco	rds (1 Selected)							Cancel Continu	e	



See the online documentation for more information on Creating a Custom Template.

- 13. Select Continue.
- 14. On the **Assignments** page, select one of the following and choose the resources to apply the policy to:
  - Tags Select the Tags radio button and then choose a tag or tags assigned to the resource. Select the + icon to assign more tags to the resource. If there are no tags assigned, select the Assign Tags Now link.
  - ° Resources Select Specific Resources and then choose one or more resources.
- 15. Select **Resources** for the resources to apply the policy to.
- 16. Select the Kubernetes cluster that has been onboarded.

Creat	Create Policy S My Configuration Hardening Policy									
1: Sel	lect Type 🗸	2: Details 🗸	3: Templates 🗸	4: Resources	5: Schedule					
Assign this policy to one or more K8s Clusters based on tags or by direct assignment. For now, only Master Nodes are hardened.										
ך 2	Fags Apply this policy	to K8s Clusters that H	nave the following tags	Res Identif	Resources Identify K8s Clusters that this policy should be applied to					
Filter										
	Resource			▲ Mar	agement Sy	stem		٥		
	qa-tkg-cluste	r-01		qa-tk	g-cluster-01					

1 records		1 Selected
Back	Cancel	Continue

- 17. Select Continue.
- 18. On the **Schedule** page, enable a recurring schedule if required.

If enabled, select the type of schedule to use to run the policy and specify the start date. This can be one of the following:

- **Daily** The policy will run every day at the specified time.
- **Hourly** The policy will run periodically throughout the day, based on the defined schedule.
- <sup>°</sup> Weekly The policy will run on every day that you select at the specified time.

Create Policy   My Configuration Hardening Policy										
1: Select Type 🖌 — 2: Details 🖌 — 3: Templates 🖌 — 4: Resources 🖌 — 5: Schedule										
Recurring Schedule										
Status ENGLA										
Frequency										
Daily 👻										
Every day at 09 : 00 AM										
Start Date										
Today 🛍										
Back Cancel Cre	ate									

- 19. Select Create.
- 20. The new policy appears on the **Policies** tab.

* 5	Configuration Hardeni ×													
Configuration Hardening Management Policies Templates								Global Compliance Threshold: 100% (change)			(ohange)			
Filter												/ + 0	Action	ns   -
													Colu	mns •
	Name	•	Description	0	Template	٥	Resource Type	0	Schedule	:	0	Last Event $\circ$	Status	0
	My Configuration Hardening P	olicy	Test configuration hardening poli	icy.	Kubernetes - HyTrust Best Practic		Kubernetes		Daily at 09:00 A	M			ENABLED	

## 2.14.5. Adding credentials to Tanzu master nodes

This is required to be able to run the configuration hardening policy. Follow the instructions, as described here, on how to SSH to Tanzu Kubernetes Cluster Nodes as the System User Using a Password.

After obtaining the password, save it. This password is used to store the credentials of the master nodes in CloudControl. For example:

Credentials : vmware-system-user / zeaIHcnKYYINzqF6TQ6D3c4gSuVUtJizl35uxKZ+Ks8=

- 1. Navigate to the Tanzu cluster.
- 2. From the Home tab, select Inventory > Kubernetes Cluster.
- 3. Select the link for the Tanzu cluster. In this case the **qa-tkg-cluster-01**.
- On the qa-tkg-cluster-01 page, select the Nodes tab. Add any missing credentials to the master nodes.

(Guster	-cluster-01						🖪 Views 🛛 🕶	Actions -
		O Nodes (6)	) Namespaces (9)	Deployments (5)     Pods (48)	✤ Containers (64) ✿ Services (4)			×
Filter								Actions 🛛 👻
	Name 🔺	Vendor Type	0 IP Address	O Hostname	Credentials			
	qa-tkg-cluster-01-control-pl	TanzuMasterNode	100000000000000000000000000000000000000		✓ Valid	<b>%</b> 1		
	qa-tkg-cluster-01-control-pl	TanzuMasterNode	100000000000000000000000000000000000000		× Missing	<b>%</b> 1		
	qa-tkg-cluster-01-control-pl	TanzuMasterNode	100.000.000		× Missing	<b>%</b> 1		
	ga-tkg-cluster-01-workers	TanzuWorkerNode			Not applicable	<b>%</b> 1		
	qa-tkg-cluster-01-workers	TanzuWorkerNode	100.000		Not applicable	<b>%</b> 1		
	qa-tkg-cluster-01-workers	TanzuWorkerNode	100.000		Not applicable	<b>%</b> 1		

5. Select the master node and then from the **Actions** Menu select **Update SSH Access Credentials**.

		O Nodes (6)	Namespaces (9)	Deployments (5)	💬 Pods (48)	🗢 Containers (64)	OG Services (4)		×
Filter									Actions -
	Name 🔺 Ven	idor Type	0 IP Address	0 Ho:	stname	Cre	dentials		Update SSH Access Credentials
	qa-tkg-cluster-01-control-p Tanz	ruMasterNode				<b>√</b> Va	alid	<b>%</b> 1	Assign Tags
	qa-tkg-cluster-01-control-p Tanz	ruMasterNode	102.008.071			× Mi	ssing	<b>%</b> 1	Unassign tags
	qa-tkg-cluster-01-control-p Tanz	ruMasterNode	100.000.000			× Mi	ssing	<b>%</b> 1	
	qa-tkg-cluster-01-workers Tanz	tuWorkerNode				Not	applicable	<b>%</b> 1	
	qa-tkg-cluster-01-workers Tanz	tuWorkerNode	$(-\infty)_{i}=(-\infty)_{i}=(-\infty)_{i}$			Nota	applicable	<b>%</b> 1	
	qa-tkg-cluster-01-workers Tanz	tuWorkerNode				Not	applicable	<b>%</b> 1	

6. In the Add SSH Credentials window, enter the User Name and Password saved earlier.

Add SSH Access Credentials					
User Name/Password User Name/SSH Key					
User Name *					
vmware-system-user					
Password *					
SSH Port					
22					
Cancel Sav	/e				

- 7. Select Save.
- 8. Do this for all the master nodes in the cluster.

## 2.14.6. Run the new configuration hardening policy

When running a remediation policy, the assessment policy automatically runs immediately following its completion. This ensures that the compliance score is updated with the new percentage.

- 1. From the Home tab, select Security > Configuration Hardening.
- 2. On the Configuration Hardening Management page, select the Policies tab.
- 3. Select the policy that you want to run.
- 4. Select Actions > Run Now.
- 5. You can view the results by selecting the link in the **Last Event** column after the configuration hardening policy finishes running.
- 6. Select View Full Results.

Configu	ration Hardening Manage	ment	Policies	Templates			Global Complian	e Threshold: 100	1% (change
Filter							- +	a Acti	ions   -
								Col	lumns -
	Name 🔺	Description 0	Template 0	Resource Type	Schedule	0 L	.ast Event	<ul> <li>Status</li> </ul>	0
0	My Configuration Hardening P	Test configuration hardening	Kubernetes - HyTrust Best Pr	Kubernetes	Daily at 09:00 AM	M	4ar 30, 2023, 9:03:08 Al	enabled	
						Last Event Su 1 Completely so Policy Template Resource Type Elapsed Time View Full Resource	ammary canned 0 Not scanned My Configuration Ha Policy Kubernetes - Hy Trust Values Kubernetes 00:03:08 alts	i e² ¥ rdening Best default	



When viewing the full results, if you see a warning message indicating that it "Failed to Assess one or more resource(s)", make sure you have added the credentials to all Tanzu master nodes to perform compliance. See Adding credentials to Tanzu master nodes for more details.

#### 7. In the Last Event Summary Tab, select Resource.

🛛 🔞 Last Event Summai	Resource	rce Results			x		×
Policy My Co Template Kuber Resource Type Kuber Total Resources (1) 1 Completely scanned 0 Nor Filter c	Resource Policy Template Elapsed Time Time <b>Operations (</b> Passed 40 (75%)	My Configuration Hardening Policy Kubernetes - HyTrust Best Practice with HyTrust default values 1 minute 10 seconds Mar 30, 2023, 10:12:54 AM 53 Total) Faled 13 (25%) Skipped 0 (0%)	Score () Policy Type Template Revision Compliance Threshold Vendor Resource Type	0 75% Assess 1 100% TanzuKubernetesCluster		AM ] Status	0
	Filter 3/3 Failed Catego Resour Operat	re that the —anonymous-auth argume ASC Dr. ASC-Kilvernetes-0008 Assessment T ry: Ad Server Elapsed Time: 1 seconds ce Type: KulvernetesMesterNode Version: Kul t to Jon has failed on one or more resources (More of	nt is set to false ime: Mar 30, 2023, 10:12:45 bernetes 1.23.0 Ketails) (Remediation Steps)	Sort by Operation Name	↔ GH		
	Passed Ensui Passed ID: 30 Catego Resour	re that the —audit-log-maxage argume ppriate ASCID: ASC-Kubernetes-0030 Assessment T ry: Api Server Elapsed Time: +1 second ce Tune: KubernetesMesterNode Version: Kub	ent is set to 30 or as Time: Mar 30, 2023, 10:12:45 bernetes 1 23 0	HI 5 AM	GH		

8. Check the results to see whether each test in the policy **Passed** or **Failed**. Select the **More details** link to get details on the result for each of the master nodes in the cluster. For **Failed** tests, select the **Remediation Steps** link to get information on how to remediate the problem.

# Chapter 3. Additional resources and related products

- 3.1. CloudControl
- 3.2. Entrust products
- 3.3. nShield product documentation