



# Install using Trident operator

Trident

NetApp  
June 30, 2026

# Table of Contents

- Install using Trident operator ..... 1
  - Manually deploy the Trident operator (Standard mode) ..... 1
    - Critical information about Trident 26.02 ..... 1
    - Manually deploy the Trident operator and install Trident ..... 1
    - Verify the installation ..... 4
  - Manually deploy the Trident operator (Offline mode) ..... 6
    - Critical information about Trident ..... 6
    - Manually deploy the Trident operator and install Trident ..... 6
    - Verify the installation ..... 11
- Deploy Trident operator using Helm (Standard mode) ..... 12
  - Critical information about Trident 25.10 ..... 12
  - Deploy the Trident operator and install Trident using Helm ..... 12
  - Pass configuration data during install ..... 13
  - Configuration options ..... 13
- Deploy Trident operator using Helm (Offline mode) ..... 20
  - Critical information about Trident 26.02 ..... 20
  - Deploy the Trident operator and install Trident using Helm ..... 20
  - Pass configuration data during install ..... 21
  - Configuration options ..... 22
- Customize Trident operator installation ..... 28
  - Understanding controller pods and node pods ..... 28
  - Configuration options ..... 28
  - Sample configurations ..... 32

# Install using Trident operator

## Manually deploy the Trident operator (Standard mode)

You can manually deploy the Trident operator to install Trident. This process applies to installations where the container images required by Trident are not stored in a private registry. If you do have a private image registry, use the [process for offline deployment](#).

### Critical information about Trident 26.02

You must read the following critical information about Trident.

#### Critical information about Trident

- Kubernetes 1.35 is now supported in Trident. Upgrade Trident prior to upgrading Kubernetes.
- Trident strictly enforces the use of multipathing configuration in SAN environments, with a recommended value of `find_multipaths: no` in `multipath.conf` file.

Use of non-multipathing configuration or use of `find_multipaths: yes` or `find_multipaths: smart` value in `multipath.conf` file will result in mount failures. Trident has recommended the use of `find_multipaths: no` since the 21.07 release.

## Manually deploy the Trident operator and install Trident

Review [the installation overview](#) to ensure you've met installation prerequisites and selected the correct installation option for your environment.

### Before you begin

Before you begin installation, log in to the Linux host and verify it is managing a working, [supported Kubernetes cluster](#) and that you have the necessary privileges.



With OpenShift, use `oc` instead of `kubectl` in all of the examples that follow, and log in as **system:admin** first by running `oc login -u system:admin` or `oc login -u kube-admin`.

1. Verify your Kubernetes version:

```
kubectl version
```

2. Verify cluster administrator privileges:

```
kubectl auth can-i '*' '*' --all-namespaces
```

3. Verify you can launch a pod that uses an image from Docker Hub and reach your storage system over the pod network:

```
kubectl run -i --tty ping --image=busybox --restart=Never --rm -- \
ping <management IP>
```

### Step 1: Download the Trident installer package

The Trident installer package contains everything you need to deploy the Trident operator and install Trident. Download and extract the latest version of the Trident installer from [the Assets section on GitHub](#).

```
wget https://github.com/NetApp/trident/releases/download/v26.02.0/trident-
installer-26.02.0.tar.gz
tar -xf trident-installer-26.02.0.tar.gz
cd trident-installer
```

### Step 2: Create the `TridentOrchestrator` CRD

Create the `TridentOrchestrator` Custom Resource Definition (CRD). You will create a `TridentOrchestrator` Custom Resource later. Use the appropriate CRD YAML version in `deploy/crds` to create the `TridentOrchestrator` CRD.

```
kubectl create -f
deploy/crds/trident.netapp.io_tridentorchestrators_crd_post1.16.yaml
```

### Step 3: Deploy the Trident operator

The Trident installer provides a bundle file that can be used to install the operator and create associated objects. The bundle file is an easy way to deploy the operator and install Trident using a default configuration.

- For clusters running Kubernetes 1.24, use `bundle_pre_1_25.yaml`.
- For clusters running Kubernetes 1.25 or later, use `bundle_post_1_25.yaml`.

## Before you begin

- By default, the Trident installer deploys the operator in the `trident` namespace. If the `trident` namespace does not exist, create it using:

```
kubectl apply -f deploy/namespace.yaml
```

- To deploy the operator in a namespace other than the `trident` namespace, update `serviceaccount.yaml`, `clusterrolebinding.yaml` and `operator.yaml` and generate your bundle file using the `kustomization.yaml`.

1. Create the `kustomization.yaml` using the following command where `<bundle.yaml>` is `bundle_pre_1_25.yaml` or `bundle_post_1_25.yaml` based on your Kubernetes version.

```
cp deploy/kustomization_<bundle.yaml> deploy/kustomization.yaml
```

2. Compile the bundle using using the following command where `<bundle.yaml>` is `bundle_pre_1_25.yaml` or `bundle_post_1_25.yaml` based on your Kubernetes version.

```
kubectl kustomize deploy/ > deploy/<bundle.yaml>
```

## Steps

1. Create the resources and deploy the operator:

```
kubectl create -f deploy/<bundle.yaml>
```

2. Verify the operator, deployment, and replicaset were created.

```
kubectl get all -n <operator-namespace>
```



There should only be **one instance** of the operator in a Kubernetes cluster. Do not create multiple deployments of the Trident operator.

## Step 4: Create the `TridentOrchestrator` and install Trident

You can now create the `TridentOrchestrator` and install Trident. Optionally, you can [customize your Trident installation](#) using the attributes in the `TridentOrchestrator` spec.

```

kubect1 create -f deploy/crds/tridentorchestrator_cr.yaml
tridentorchestrator.trident.netapp.io/trident created

kubect1 describe torc trident

Name:          trident
Namespace:
Labels:        <none>
Annotations:   <none>
API Version:   trident.netapp.io/v1
Kind:          TridentOrchestrator
...
Spec:
  Debug:       true
  Namespace:   trident
  nodePrep:
    - iscsi
Status:
  Current Installation Params:
    IPv6:                false
    Autosupport Hostname:
    Autosupport Image:   netapp/trident-autosupport:26.02
    Autosupport Proxy:
    Autosupport Serial Number:
    Debug:                true
    Image Pull Secrets:
    Image Registry:
    k8sTimeout:          30
    Kubelet Dir:         /var/lib/kubelet
    Log Format:           text
    Silence Autosupport: false
    Trident Image:       netapp/trident:26.02.0
  Message:              Trident installed Namespace:
trident
  Status:                Installed
  Version:               v26.02.0
Events:
  Type Reason Age From Message ---- -
  Installing 74s trident-operator.netapp.io Installing Trident Normal
  Installed 67s trident-operator.netapp.io Trident installed

```

## Verify the installation

There are several ways to verify your installation.

## Using `TridentOrchestrator` status

The status of `TridentOrchestrator` indicates if the installation was successful and displays the version of Trident installed. During the installation, the status of `TridentOrchestrator` changes from `Installing` to `Installed`. If you observe the `Failed` status and the operator is unable to recover by itself, [check the logs](#).

Status	Description
Installing	The operator is installing Trident using this <code>TridentOrchestrator</code> CR.
Installed	Trident has successfully installed.
Uninstalling	The operator is uninstalling Trident, because <code>spec.uninstall=true</code> .
Uninstalled	Trident is uninstalled.
Failed	The operator could not install, patch, update or uninstall Trident; the operator will automatically try to recover from this state. If this state persists you will require troubleshooting.
Updating	The operator is updating an existing installation.
Error	The <code>TridentOrchestrator</code> is not used. Another one already exists.

## Using pod creation status

You can confirm if the Trident installation completed by reviewing the status of the created pods:

```
kubectl get pods -n trident
```

NAME	READY	STATUS	RESTARTS
trident-controller-7d466bf5c7-v4cpw 1m	6/6	Running	0
trident-node-linux-mr6zc 1m	2/2	Running	0
trident-node-linux-xrp7w 1m	2/2	Running	0
trident-node-linux-zh2jt 1m	2/2	Running	0
trident-operator-766f7b8658-ldzsv 3m	1/1	Running	0

## Using `tridentctl`

You can use `tridentctl` to check the version of Trident installed.

```
./tridentctl -n trident version
```

```
+-----+-----+
| SERVER VERSION | CLIENT VERSION |
+-----+-----+
| 26.02.0        | 26.02.0        |
+-----+-----+
```

## Manually deploy the Trident operator (Offline mode)

You can manually deploy the Trident operator to install Trident. This process applies to installations where the container images required by Trident are stored in a private registry. If you do not have a private image registry, use the [process for standard deployment](#).

### Critical information about Trident

You must read the following critical information about Trident.

#### Critical information about Trident

- Kubernetes 1.35 is now supported in Trident. Upgrade Trident prior to upgrading Kubernetes.
- Trident strictly enforces the use of multipathing configuration in SAN environments, with a recommended value of `find_multipaths: no` in `multipath.conf` file.

Use of non-multipathing configuration or use of `find_multipaths: yes` or `find_multipaths: smart` value in `multipath.conf` file will result in mount failures. Trident has recommended the use of `find_multipaths: no` since the 21.07 release.

## Manually deploy the Trident operator and install Trident

Review [the installation overview](#) to ensure you've met installation prerequisites and selected the correct installation option for your environment.

### Before you begin

Log in to the Linux host and verify it is managing a working and [supported Kubernetes cluster](#) and that you have the necessary privileges.



With OpenShift, use `oc` instead of `kubectl` in all of the examples that follow, and log in as **system:admin** first by running `oc login -u system:admin` or `oc login -u kube-admin`.

1. Verify your Kubernetes version:

```
kubectl version
```

2. Verify cluster administrator privileges:

```
kubectl auth can-i '*' '*' --all-namespaces
```

3. Verify you can launch a pod that uses an image from Docker Hub and reach your storage system over the pod network:

```
kubectl run -i --tty ping --image=busybox --restart=Never --rm -- \
ping <management IP>
```

### Step 1: Download the Trident installer package

The Trident installer package contains everything you need to deploy the Trident operator and install Trident. Download and extract the latest version of the Trident installer from [the Assets section on GitHub](#).

```
wget https://github.com/NetApp/trident/releases/download/v6.0/trident-
installer-26.02.0.tar.gz
tar -xf trident-installer-26.02.0.tar.gz
cd trident-installer
```

### Step 2: Create the `TridentOrchestrator` CRD

Create the `TridentOrchestrator` Custom Resource Definition (CRD). You will create a `TridentOrchestrator` Custom Resources later. Use the appropriate CRD YAML version in `deploy/crds` to create the `TridentOrchestrator` CRD:

```
kubectl create -f deploy/crds/<VERSION>.yaml
```

### Step 3: Update the registry location in the operator

In `/deploy/operator.yaml`, update `image: docker.io/netapp/trident-operator:26.02.0` to reflect the location of your image registry. Your [Trident and CSI images](#) can be located in one registry or different registries, but all CSI images must be located in the same registry. For example:

- `image: <your-registry>/trident-operator:26.02.0` if your images are all located in one registry.
- `image: <your-registry>/netapp/trident-operator:26.02.0` if your Trident image is located in

a different registry from your CSI images.

#### Step 4: Deploy the Trident operator

The Trident installer provides a bundle file that can be used to install the operator and create associated objects. The bundle file is an easy way to deploy the operator and install Trident using a default configuration.

- For clusters running Kubernetes 1.24, use `bundle_pre_1_25.yaml`.
- For clusters running Kubernetes 1.25 or later, use `bundle_post_1_25.yaml`.

#### Before you begin

- By default, the Trident installer deploys the operator in the `trident` namespace. If the `trident` namespace does not exist, create it using:

```
kubectl apply -f deploy/namespace.yaml
```

- To deploy the operator in a namespace other than the `trident` namespace, update `serviceaccount.yaml`, `clusterrolebinding.yaml` and `operator.yaml` and generate your bundle file using the `kustomization.yaml`.
  1. Create the `kustomization.yaml` using the following command where `<bundle.yaml>` is `bundle_pre_1_25.yaml` or `bundle_post_1_25.yaml` based on your Kubernetes version.

```
cp deploy/kustomization_<bundle.yaml> deploy/kustomization.yaml
```

2. Compile the bundle using using the following command where `<bundle.yaml>` is `bundle_pre_1_25.yaml` or `bundle_post_1_25.yaml` based on your Kubernetes version.

```
kubectl kustomize deploy/ > deploy/<bundle.yaml>
```

#### Steps

1. Create the resources and deploy the operator:

```
kubectl create -f deploy/<bundle.yaml>
```

2. Verify the operator, deployment, and replicaset were created.

```
kubectl get all -n <operator-namespace>
```



There should only be **one instance** of the operator in a Kubernetes cluster. Do not create multiple deployments of the Trident operator.

## Step 5: Update the image registry location in the `TridentOrchestrator`

Your [Trident and CSI images](#) can be located in one registry or different registries, but all CSI images must be located in the same registry. Update `deploy/crds/tridentorchestrator_cr.yaml` to add the additional location specs based on your registry configuration.

### Images in one registry

```
imageRegistry: "<your-registry>"
autosupportImage: "<your-registry>/trident-autosupport:26.02"
tridentImage: "<your-registry>/trident:26.02.0"
```

### Images in different registries

```
imageRegistry: "<your-registry>"
autosupportImage: "<your-registry>/trident-autosupport:26.02"
tridentImage: "<your-registry>/trident:26.02.0"
```

## Step 6: Create the `TridentOrchestrator` and install Trident

You can now create the `TridentOrchestrator` and install Trident. Optionally, you can further [customize your Trident installation](#) using the attributes in the `TridentOrchestrator` spec. The following example shows an installation where Trident and CSI images are located in different registries.

```

kubect1 create -f deploy/crds/tridentorchestrator_cr.yaml
tridentorchestrator.trident.netapp.io/trident created

kubect1 describe torc trident

Name:          trident
Namespace:
Labels:        <none>
Annotations:   <none>
API Version:   trident.netapp.io/v1
Kind:          TridentOrchestrator
...
Spec:
  Autosupport Image: <your-registry>/trident-autosupport:26.02
  Debug:              true
  Image Registry:    <your-registry>
  Namespace:         trident
  Trident Image:     <your-registry>/trident:26.02.0
Status:
  Current Installation Params:
    IPv6:              false
    Autosupport Hostname:
    Autosupport Image: <your-registry>/trident-autosupport:26.02
    Autosupport Proxy:
    Autosupport Serial Number:
    Debug:              true
    Http Request Timeout: 90s
    Image Pull Secrets:
    Image Registry:    <your-registry>
    k8sTimeout:        30
    Kubelet Dir:       /var/lib/kubelet
    Log Format:         text
    Probe Port:        17546
    Silence Autosupport: false
    Trident Image:     <your-registry>/trident:26.02.0
  Message:             Trident installed
  Namespace:           trident
  Status:               Installed
  Version:              v26.02.0
Events:
  Type Reason Age From Message -----Normal
  Installing 74s trident-operator.netapp.io Installing Trident Normal
  Installed 67s trident-operator.netapp.io Trident installed

```

## Verify the installation

There are several ways to verify your installation.

### Using `TridentOrchestrator` status

The status of `TridentOrchestrator` indicates if the installation was successful and displays the version of Trident installed. During the installation, the status of `TridentOrchestrator` changes from `Installing` to `Installed`. If you observe the `Failed` status and the operator is unable to recover by itself, [check the logs](#).

Status	Description
Installing	The operator is installing Trident using this <code>TridentOrchestrator</code> CR.
Installed	Trident has successfully installed.
Uninstalling	The operator is uninstalling Trident, because <code>spec.uninstall=true</code> .
Uninstalled	Trident is uninstalled.
Failed	The operator could not install, patch, update or uninstall Trident; the operator will automatically try to recover from this state. If this state persists you will require troubleshooting.
Updating	The operator is updating an existing installation.
Error	The <code>TridentOrchestrator</code> is not used. Another one already exists.

### Using pod creation status

You can confirm if the Trident installation completed by reviewing the status of the created pods:

```
kubectl get pods -n trident
```

```
NAME                                READY   STATUS    RESTARTS
AGE
trident-controller-7d466bf5c7-v4cpw 6/6     Running  0
1m
trident-node-linux-mr6zc            2/2     Running  0
1m
trident-node-linux-xrp7w            2/2     Running  0
1m
trident-node-linux-zh2jt            2/2     Running  0
1m
trident-operator-766f7b8658-ldzsv  1/1     Running  0
3m
```

## Using `tridentctl`

You can use `tridentctl` to check the version of Trident installed.

```
./tridentctl -n trident version

+-----+-----+
| SERVER VERSION | CLIENT VERSION |
+-----+-----+
| 26.02.0       | 26.02.0       |
+-----+-----+
```

## Deploy Trident operator using Helm (Standard mode)

You can deploy the Trident operator and install Trident using Helm. This process applies to installations where the container images required by Trident are not stored in a private registry. If you do have a private image registry, use the [process for offline deployment](#).

### Critical information about Trident 25.10

You must read the following critical information about Trident.

#### Critical information about Trident

- Kubernetes 1.35 is now supported in Trident. Upgrade Trident prior to upgrading Kubernetes.
- Trident strictly enforces the use of multipathing configuration in SAN environments, with a recommended value of `find_multipaths: no` in `multipath.conf` file.

Use of non-multipathing configuration or use of `find_multipaths: yes` or `find_multipaths: smart` value in `multipath.conf` file will result in mount failures. Trident has recommended the use of `find_multipaths: no` since the 21.07 release.

## Deploy the Trident operator and install Trident using Helm

Using the Trident [Helm Chart](#) you can deploy the Trident operator and install Trident in one step.

Review [the installation overview](#) to ensure you've met installation prerequisites and selected the correct installation option for your environment.

### Before you begin

In addition to the [deployment prerequisites](#) you need [Helm version 3](#).

### Steps

1. Add the Trident Helm repository:

```
helm repo add netapp-trident https://netapp.github.io/trident-helm-chart
```

2. Use `helm install` and specify a name for your deployment as in the following example where `100..0` is the version of Trident you are installing.

```
helm install <name> netapp-trident/trident-operator --version 100.2602.0  
--create-namespace --namespace <trident-namespace>
```



If you already created a namespace for Trident, the `--create-namespace` parameter will not create an additional namespace.

You can use `helm list` to review installation details such as name, namespace, chart, status, app version, and revision number.

## Pass configuration data during install

There are two ways to pass configuration data during the install:

Option	Description
<code>--values</code> (or <code>-f</code> )	Specify a YAML file with overrides. This can be specified multiple times and the rightmost file will take precedence.
<code>--set</code>	Specify overrides on the command line.


For example, to change the default value of `debug`, run the following command where `100.2602.0` is the version of Trident you are installing:

```
helm install <name> netapp-trident/trident-operator --version 100.2602.0  
--create-namespace --namespace trident --set tridentDebug=true
```

## Configuration options

This table and the `values.yaml` file, which is part of the Helm chart, provide the list of keys and their default values.


Option	Description	Default
<code>nodeSelector</code>	Node labels for pod assignment	
<code>podAnnotations</code>	Pod annotations	
<code>deploymentAnnotations</code>	Deployment annotations	



Option	Description	Default
tolerations	Tolerations for pod assignment	
affinity	Affinity for pod assignment	<pre> affinity:   nodeAffinity:  requiredDuringSchedulingIgnoredDuringExecution:   nodeSelectorTerms:     - matchExpressions:       - key: kubernetes.io/arch         operator: In         values:       - arm64       - amd64       - key: kubernetes.io/os         operator: In         values:       - linux </pre> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>Do not remove the default affinity from the values.yaml file. When you want to provide a custom affinity, extend the default affinity.</p> </div>
tridentControllerPluginNodeSelector	Additional node selectors for pods. Refer to <a href="#">Understanding controller pods and node pods</a> for details.	
tridentControllerPluginTolerations	Overrides Kubernetes tolerations for pods. Refer to <a href="#">Understanding controller pods and node pods</a> for details.	
tridentNodePluginNodeSelector	Additional node selectors for pods. Refer to <a href="#">Understanding controller pods and node pods</a> for details.	
tridentNodePluginTolerations	Overrides Kubernetes tolerations for pods. Refer to <a href="#">Understanding controller pods and node pods</a> for details.	

Option	Description	Default
imageRegistry	Identifies the registry for the <code>trident-operator</code> , <code>trident</code> , and other images. Leave empty to accept the default.  IMPORTANT: When installing Trident in a private repository, if you are using the <code>imageRegistry</code> switch to specify the repository location, do not use <code>/netapp/</code> in the repository path.	""
imagePullPolicy	Sets the image pull policy for the <code>trident-operator</code> .	IfNotPresent
imagePullSecrets	Sets the image pull secrets for the <code>trident-operator</code> , <code>trident</code> , and other images.	
kubeletDir	Allows overriding the host location of kubelet's internal state.	"/var/lib/kubelet"
operatorLogLevel	Allows the log level of the Trident operator to be set to: <code>trace</code> , <code>debug</code> , <code>info</code> , <code>warn</code> , <code>error</code> , or <code>fatal</code> .	"info"
operatorDebug	Allows the log level of the Trident operator to be set to debug.	true
operatorImage	Allows the complete override of the image for <code>trident-operator</code> .	""
operatorImageTag	Allows overriding the tag of the <code>trident-operator</code> image.	""
tridentIPv6	Allows enabling Trident to work in IPv6 clusters.	false
tridentK8sTimeout	Overrides the default 30-second timeout for most Kubernetes API operations (if non-zero, in seconds).	0
tridentHttpRequestTimeout	Overrides the default 90-second timeout for the HTTP requests, with 0s being an infinite duration for the timeout. Negative values are not allowed.	"90s"
tridentSilenceAutosupport	Allows disabling Trident periodic AutoSupport reporting.	false

Option	Description	Default
tridentAutosupportImageTag	Allows overriding the tag of the image for Trident AutoSupport container.	<version>
tridentAutosupportProxy	Enables Trident AutoSupport container to phone home via an HTTP proxy.	""
tridentLogFormat	Sets the Trident logging format (text or json).	"text"
tridentDisableAuditLog	Disables Trident audit logger.	true
tridentLogLevel	Allows the log level of Trident to be set to: trace, debug, info, warn, error, or fatal.	"info"
tridentDebug	Allows the log level of Trident to be set to debug. You can automate the force-detach process through integration with node health check (NHC) operator. For information, see <a href="#">Automating the failover of stateful applications with Trident</a> .	false
tridentLogWorkflows	Allows specific Trident workflows to be enabled for trace logging or log suppression.	""
tridentLogLayers	Allows specific Trident layers to be enabled for trace logging or log suppression.	""
tridentImage	Allows the complete override of the image for Trident.	""
tridentImageTag	Allows overriding the tag of the image for Trident.	""
tridentProbePort	Allows overriding the default port used for Kubernetes liveness/readiness probes.	""
windows	Enables Trident to be installed on Windows worker node.	false
enableForceDetach	Allows enabling the force detach feature.	false
excludePodSecurityPolicy	Excludes the operator pod security policy from creation.	false

Option	Description	Default
cloudProvider	Set to "Azure" when using managed identities or a cloud identity on an AKS cluster. Set to "AWS" when using a cloud identity on an EKS cluster.	""
cloudIdentity	Set to workload identity ("azure.workload.identity/client-id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx") when using cloud identity on an AKS cluster. Set to AWS IAM role ("eks.amazonaws.com/role-arn: arn:aws:iam::123456:role/trident-role") when using cloud identity on an EKS cluster.	""
iscsiSelfHealingInterval	The interval at which the iSCSI self-healing is invoked.	5m0s
iscsiSelfHealingWaitTime	The duration after which iSCSI self-healing initiates an attempt to resolve a stale session by performing a logout and subsequent login.	7m0s
nodePrep	Enables Trident to prepare the nodes of the Kubernetes cluster to manage volumes using the specified data storage protocol. <b>Currently, iSCSI is the only value supported.</b> NOTE: Beginning with OpenShift 4.19, the minimum Trident version supported for this feature is 25.06.1.	

Option	Description	Default
enableConcurrency	<p>Enables concurrent Trident controller operations for improved throughput.</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;">  <p><b>Tech Preview:</b> This feature is experimental and currently supports limited parallel workflows with the ONTAP-NAS (NFS only) and ONTAP-SAN (NVMe for unified ONTAP 9) drivers, in addition to the existing tech preview for the ONTAP-SAN driver (iSCSI and FCP protocols in unified ONTAP 9).</p> </div>	false
k8sAPIQPS	The queries per second (QPS) limit used by the controller while communicating with the Kubernetes API server. The Burst value is set automatically based on the QPS value.	100; optional

Option	Description	Default
resources	<p>Sets Kubernetes resource limits and requests for the Trident controller, node, and operator pods. You can configure CPU and memory for each container and sidecar to manage resource allocation in Kubernetes.</p> <p>For more information about configuring resource requests and limits, refer to <a href="#">Resource Management for Pods and Containers</a>.</p> <div style="display: flex; justify-content: space-between;"> <div style="width: 20%; text-align: center;">  </div> <div style="width: 75%;"> <ul style="list-style-type: none"> <li>• DO NOT change the names of any containers or fields.</li> <li>• DO NOT change the indentation - YAML indentation is critical for proper parsing.</li> </ul> </div> </div> <div style="display: flex; justify-content: space-between; margin-top: 20px;"> <div style="width: 20%; text-align: center;">  </div> <div style="width: 75%;"> <ul style="list-style-type: none"> <li>• No limits are applied by default - only requests have default values and are automatically applied if not specified.</li> <li>• Container names are listed as they appear in the pod specifications.</li> <li>• Sidecars are listed under each main container.</li> <li>• Check the TORC's <code>CurrentInstallationParams</code> field to view the values currently applied.</li> </ul> </div> </div>	<pre>resources:   controller:     trident-main:       requests:         cpu: 10m         memory: 80Mi       limits:         cpu:         memory:     csi-provisioner:       requests:         cpu: 2m         memory: 20Mi       limits:         cpu:         memory:     csi-attacher:       requests:         cpu: 2m         memory: 20Mi       limits:         cpu:         memory:     csi-resizer:       requests:         cpu: 3m         memory: 20Mi       limits:         cpu:         memory:     csi-snapshotter:       requests:         cpu: 2m         memory: 20Mi       limits:         cpu:         memory:     trident-autosupport:       requests:         cpu: 1m         memory: 30Mi       limits:         cpu:         memory:   node:     linux:       trident-main:</pre>

Option	Description	Default
httpsMetrics	Enable HTTPS for Prometheus metrics endpoint.	false
hostNetwork	Enables host networking for the Trident controller. This is useful when you want to separate the frontend and backend traffic in a multi-home network.	false

### Understanding controller pods and node pods

Trident runs as a single controller pod, plus a node pod on each worker node in the cluster. The node pod must be running on any host where you want to potentially mount a Trident volume.

Kubernetes [node selectors](#) and [tolerations and taints](#) are used to constrain a pod to run on a specific or preferred node. Using the `ControllerPlugin` and NodePlugin, you can specify constraints and overrides.`

- The controller plugin handles volume provisioning and management, such as snapshots and resizing.
- The node plugin handles attaching the storage to the node.

## Deploy Trident operator using Helm (Offline mode)

You can deploy the Trident operator and install Trident using Helm. This process applies to installations where the container images required by Trident are stored in a private registry. If you do not have a private image registry, use the [process for standard deployment](#).

### Critical information about Trident 26.02

You must read the following critical information about Trident.

#### Critical information about Trident

- Kubernetes 1.35 is now supported in Trident. Upgrade Trident prior to upgrading Kubernetes.
- Trident strictly enforces the use of multipathing configuration in SAN environments, with a recommended value of `find_multipaths: no` in `multipath.conf` file.

Use of non-multipathing configuration or use of `find_multipaths: yes` or `find_multipaths: smart` value in `multipath.conf` file will result in mount failures. Trident has recommended the use of `find_multipaths: no` since the 21.07 release.

## Deploy the Trident operator and install Trident using Helm

Using the Trident [Helm Chart](#) you can deploy the Trident operator and install Trident in one step.

```

requests:
  cpu: 1m
  memory: 10Mi
node-driver-registrar:
  requests:
    cpu: 6m
    memory: 40Mi
limits:
  cpu:
  memory:
liveness-probe:
requests:

```

```

cpu:
memory:

```

Review [the installation overview](#) to ensure you've met installation prerequisites and selected the correct installation option for your environment.

### Before you begin

In addition to the [deployment prerequisites](#) you need [Helm version 3](#).



When installing Trident in a private repository, if you are using the `imageRegistry` switch to specify the repository location, do not use `/netapp/` in the repository path.

### Steps

1. Add the Trident Helm repository:

```
helm repo add netapp-trident https://netapp.github.io/trident-helm-chart
```

2. Use `helm install` and specify a name for your deployment and image registry location. Your [Trident and CSI images](#) can be located in one registry or different registries, but all CSI images must be located in the same registry. In the examples, `100.2602.0` is the version of Trident you are installing.

#### Images in one registry

```
helm install <name> netapp-trident/trident-operator --version  
100.2602.0 --set imageRegistry=<your-registry> --create-namespace  
--namespace <trident-namespace> --set nodePrep={iscsi}
```

#### Images in different registries

```
helm install <name> netapp-trident/trident-operator --version  
100.2602.0 --set imageRegistry=<your-registry> --set operatorImage  
=<your-registry>/trident-operator:26.02.0 --set  
tridentAutosupportImage=<your-registry>/trident-autosupport:26.02  
--set tridentImage=<your-registry>/trident:26.02.0 --create  
-namespace --namespace <trident-namespace> --set nodePrep={iscsi}
```



If you already created a namespace for Trident, the `--create-namespace` parameter will not create an additional namespace.

You can use `helm list` to review installation details such as name, namespace, chart, status, app version, and revision number.

## Pass configuration data during install

There are two ways to pass configuration data during the install:

Option	Description
<code>--values (or -f)</code>	Specify a YAML file with overrides. This can be specified multiple times and the rightmost file will take precedence.
<code>--set</code>	Specify overrides on the command line.

For example, to change the default value of `debug`, run the following command where `100.2602.0` is the version of Trident you are installing:

```
helm install <name> netapp-trident/trident-operator --version 100.2602.0
--create-namespace --namespace trident --set tridentDebug=true
```

To add the `nodePrep` value, run the following command:

```
helm install <name> netapp-trident/trident-operator --version 100.2602.0
--create-namespace --namespace trident --set nodePrep={iscsi}
```


## Configuration options


This table and the `values.yaml` file, which is part of the Helm chart, provide the list of keys and their default values.




Do not remove the default affinity from the `values.yaml` file. When you want to provide a custom affinity, extend the default affinity.

Option	Description	Default
<code>nodeSelector</code>	Node labels for pod assignment	
<code>podAnnotations</code>	Pod annotations	
<code>deploymentAnnotations</code>	Deployment annotations	
<code>tolerations</code>	Tolerations for pod assignment	

Option	Description	Default
affinity	Affinity for pod assignment	<pre> affinity:   nodeAffinity:      requiredDuringSchedulingIgnoredDuringExecution:        nodeSelectorTerms:         -           matchExpressions:             - key:               kubernetes.io/arch                operator: In                 values:                   - arm64                   - amd64             - key:               kubernetes.io/os                operator: In                 values:                   - linux </pre> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>Do not remove the default affinity from the values.yaml file. When you want to provide a custom affinity, extend the default affinity.</p> </div>
tridentControllerPluginNodeSelector	Additional node selectors for pods. Refer to <a href="#">Understanding controller pods and node pods</a> for details.	
tridentControllerPluginTolerations	Overrides Kubernetes tolerations for pods. Refer to <a href="#">Understanding controller pods and node pods</a> for details.	
tridentNodePluginNodeSelector	Additional node selectors for pods. Refer to <a href="#">Understanding controller pods and node pods</a> for details.	

Option	Description	Default
<code>tridentNodePluginTolerations</code>	Overrides Kubernetes tolerations for pods. Refer to <a href="#">Understanding controller pods and node pods</a> for details.	
<code>imageRegistry</code>	Identifies the registry for the <code>trident-operator</code> , <code>trident</code> , and other images. Leave empty to accept the default.  IMPORTANT: When installing Trident in a private repository, if you are using the <code>imageRegistry</code> switch to specify the repository location, do not use <code>/netapp/</code> in the repository path.	""
<code>imagePullPolicy</code>	Sets the image pull policy for the <code>trident-operator</code> .	<code>IfNotPresent</code>
<code>imagePullSecrets</code>	Sets the image pull secrets for the <code>trident-operator</code> , <code>trident</code> , and other images.	
<code>kubeletDir</code>	Allows overriding the host location of kubelet's internal state.	<code>"/var/lib/kubelet"</code>
<code>operatorLogLevel</code>	Allows the log level of the Trident operator to be set to: <code>trace</code> , <code>debug</code> , <code>info</code> , <code>warn</code> , <code>error</code> , or <code>fatal</code> .	<code>"info"</code>
<code>operatorDebug</code>	Allows the log level of the Trident operator to be set to debug.	<code>true</code>
<code>operatorImage</code>	Allows the complete override of the image for <code>trident-operator</code> .	""
<code>operatorImageTag</code>	Allows overriding the tag of the <code>trident-operator</code> image.	""
<code>tridentIPv6</code>	Allows enabling Trident to work in IPv6 clusters.	<code>false</code>
<code>tridentK8sTimeout</code>	Overrides the default 180-second timeout for most Kubernetes API operations (if non-zero, in seconds).  <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-left: 20px;">  The <code>tridentK8sTimeout</code> parameter is applicable only for Trident installation. </div>	180

Option	Description	Default
tridentHttpRequestTimeout	Overrides the default 90-second timeout for the HTTP requests, with 0s being an infinite duration for the timeout. Negative values are not allowed.	"90s"
tridentSilenceAutosupport	Allows disabling Trident periodic AutoSupport reporting.	false
tridentAutosupportImageTag	Allows overriding the tag of the image for Trident AutoSupport container.	<version>
tridentAutosupportProxy	Enables Trident AutoSupport container to phone home via an HTTP proxy.	""
tridentLogFormat	Sets the Trident logging format (text or json).	"text"
tridentDisableAuditLog	Disables Trident audit logger.	true
tridentLogLevel	Allows the log level of Trident to be set to: trace, debug, info, warn, error, or fatal.	"info"
tridentDebug	Allows the log level of Trident to be set to debug.	false
tridentLogWorkflows	Allows specific Trident workflows to be enabled for trace logging or log suppression.	""
tridentLogLayers	Allows specific Trident layers to be enabled for trace logging or log suppression.	""
tridentImage	Allows the complete override of the image for Trident.	""
tridentImageTag	Allows overriding the tag of the image for Trident.	""
tridentProbePort	Allows overriding the default port used for Kubernetes liveness/readiness probes.	""
windows	Enables Trident to be installed on Windows worker node.	false
enableForceDetach	Allows enabling the force detach feature. You can automate the force-detach process through integration with node health check (NHC) operator. For information, see <a href="#">Automating the failover of stateful applications with Trident</a> .	false

Option	Description	Default
excludePodSecurityPolicy	Excludes the operator pod security policy from creation.	false
nodePrep	<p>Enables Trident to prepare the nodes of the Kubernetes cluster to manage volumes using the specified data storage protocol. <b>Currently, <code>iscsi</code> is the only value supported.</b></p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-left: 20px;">  <p>Beginning with OpenShift 4.19, the minimum Trident version supported for this feature is 25.06.1.</p> </div>	

Option	Description	Default
resources	<p>Sets Kubernetes resource limits and requests for the Trident controller, node, and operator pods. You can configure CPU and memory for each container and sidecar to manage resource allocation in Kubernetes.</p> <p>For more information about configuring resource requests and limits, refer to <a href="#">Resource Management for Pods and Containers</a>.</p> <ul style="list-style-type: none"> <li>• DO NOT change the names of any containers or fields.</li> <li>• DO NOT change the indentation - YAML indentation is critical for proper parsing.</li> <li>• No limits are applied by default - only requests have default values.</li> <li>• Container names are listed as they appear in the pod specifications.</li> <li>• Sidecars are listed under each main container.</li> <li>• Check the TORC's <code>status.CurrentInstallationParams</code> field to view the values currently applied.</li> </ul>	<pre>resources:   controller:     trident-main:       requests:         cpu: 10m         memory: 80Mi       limits:         cpu:         memory:     csi-provisioner:       requests:         cpu: 2m         memory: 20Mi       limits:         cpu:         memory:     csi-attacher:       requests:         cpu: 2m         memory: 20Mi       limits:         cpu:         memory:     csi-resizer:       requests:         cpu: 3m         memory: 20Mi       limits:         cpu:         memory:     csi-snapshotter:       requests:         cpu: 2m         memory: 20Mi       limits:         cpu:         memory:   trident-   autosupport:     requests:       cpu: 1m       memory: 30Mi     limits:       cpu:       memory: node:   linux:</pre>

# Customize Trident operator installation

The Trident operator allows you to customize Trident installation using the attributes in the `TridentOrchestrator` spec. If you want to customize the installation beyond what `TridentOrchestrator` arguments allow, consider using `tridentctl` to generate custom YAML manifests to modify as needed.

## Understanding controller pods and node pods

Trident runs as a single controller pod and a node pod on each worker node in the cluster. The node pod must be running on any host where you want to potentially mount a Trident volume.

Kubernetes [node selectors](#) and [tolerations and taints](#) are used to constrain a pod to run on a specific or preferred node. Using the `ControllerPlugin` and `NodePlugin`, you can specify constraints and overrides.

- The controller plugin handles volume provisioning and management, such as snapshots and resizing.
- The node plugin handles attaching the storage to the node.

## Configuration options



`spec.namespace` is specified in `TridentOrchestrator` to signify the namespace where Trident is installed. This parameter **cannot be updated after Trident is installed**. Attempting to do so causes the `TridentOrchestrator` status to change to `Failed`. Trident is not intended to be migrated across namespaces.

This table details `TridentOrchestrator` attributes.

Parameter	Description	Default
<code>namespace</code>	Namespace to install Trident in	"default"
<code>debug</code>	Enable debugging for Trident	false
<code>enableForceDetach</code>	<p><code>ontap-san</code>, <code>ontap-san-economy</code>, <code>ontap-nas</code>, and <code>ontap-nas-economy</code> only.</p> <p>Works with Kubernetes Non-Graceful Node Shutdown (NGNS) to grant cluster administrators ability to safely migrate workloads with mounted volumes to new nodes should a node become unhealthy.</p> <p>For information, see <a href="#">Automating the failover of stateful applications with Trident</a>.</p>	false
<code>windows</code>	Setting to <code>true</code> enables installation on Windows worker nodes.	false

```


trident-main:
  requests:
    cpu: 10m
    memory:
      60Mi
  limits:
    cpu:
    memory:
node-driver-
  registrar:
    requests:
    cpu: 1m
    memory:
      10Mi
  limits:
    cpu:
    memory:
windows:
trident-main:
  requests:
    cpu: 6m
    memory:
      40Mi
  limits:



```

```

  limits:
    cpu:
    memory:
operator:
  requests:
    cpu: 10m
    memory: 40Mi
  limits:

```

Parameter	Description	Default
cloudProvider	Set to "Azure" when using managed identities or a cloud identity on an AKS cluster. Set to "AWS" when using a cloud identity on an EKS cluster. Set to "GCP" when using a cloud identity on a GKE cluster.	""
cloudIdentity	Set to workload identity ("azure.workload.identity/client-id: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx") when using cloud identity on an AKS cluster. Set to AWS IAM role ("eks.amazonaws.com/role-arn: arn:aws:iam::123456:role/trident-role") when using cloud identity on an EKS cluster. Set to cloud identity ("iam.gke.io/gcp-service-account: xxx@mygcpproject.iam.gserviceaccount.com") when using cloud identity on a GKE cluster.	""
IPv6	Install Trident over IPv6	false
k8sTimeout	Timeout for Kubernetes operations.  <div style="display: flex; align-items: center;">  <p>The k8sTimeout parameter is applicable only for Trident installation.</p> </div>	180sec
silenceAutosupport	Don't send autosupport bundles to NetApp automatically	false
autosupportImage	The container image for Autosupport Telemetry	"netapp/trident-autosupport10"
autosupportProxy	The address/port of a proxy for sending Autosupport Telemetry	"http://proxy.example.com:8888"
uninstall	A flag used to uninstall Trident	false
logFormat	Trident logging format to be used [text,json]	"text"
tridentImage	Trident image to install	"netapp/trident:26.02"
imageRegistry	Path to internal registry, of the format <registry FQDN>[:port][/subpath]	"registry.k8s.io"
kubeletDir	Path to the kubelet directory on the host	"/var/lib/kubelet"
wipeout	A list of resources to delete to perform a complete removal of Trident	
imagePullSecrets	Secrets to pull images from an internal registry	

Parameter	Description	Default
imagePullPolicy	<p>Sets the image pull policy for the the Trident operator. Valid values are:</p> <p>Always to always pull the image.</p> <p>IfNotPresent to pull the image only if it does not already exist on the node.</p> <p>Never to never pull the image.</p>	IfNotPresent
controllerPluginNodeSelector	Additional node selectors for pods. Follows same format as <code>pod.spec.nodeSelector</code> .	No default; optional
controllerPluginTolerations	Overrides Kubernetes tolerations for pods. Follows the same format as <code>pod.spec.Tolerations</code> .	No default; optional
nodePluginNodeSelector	Additional node selectors for pods. Follows same format as <code>pod.spec.nodeSelector</code> .	No default; optional
nodePluginTolerations	Overrides Kubernetes tolerations for pods. Follows the same format as <code>pod.spec.Tolerations</code> .	No default; optional
nodePrep	<p>Enables Trident to prepare the nodes of the Kubernetes cluster to manage volumes using the specified data storage protocol.</p> <p><b>Currently, <code>iscsi</code> is the only value supported.</b></p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;">  Beginning with OpenShift 4.19, the minimum Trident version supported for this feature is 25.06.1. </div>	
k8sAPIQPS	The queries per second (QPS) limit used by the controller while communicating with the Kubernetes API server. The Burst value is set automatically based on the QPS value.	100; optional
enableConcurrency	<p>Enables concurrent Trident controller operations for improved throughput.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin-top: 10px;">  <b>Tech Preview:</b> This feature is experimental and currently supports limited parallel workflows with the ONTAP-NAS (NFS only) and ONTAP-SAN (NVMe for unified ONTAP 9) drivers, in addition to the existing tech preview for the ONTAP-SAN driver (iSCSI and FCP protocols in unified ONTAP 9). </div>	false

Parameter	Description	Default
resources	<p>Sets Kubernetes resource limits and requests for the Trident controller and node pods. You can configure CPU and memory for each container and sidecar to manage resource allocation in Kubernetes.</p> <p>For more information about configuring resource requests and limits, refer to <a href="#">Resource Management for Pods and Containers</a>.</p> <ul style="list-style-type: none"> <li>• DO NOT change the names of any containers or fields.</li> <li>• DO NOT change the indentation - YAML indentation is critical for proper parsing.</li> <li>• No limits are applied by default - only requests have default values and are applied automatically if not specified.</li> <li>• Container names are listed as they appear in the pod specifications.</li> <li>• Sidecars are listed under each main container.</li> <li>• Check the TORC's <code>status.CurrentInstallation.Params</code> field to view the values currently applied.</li> </ul>	<pre>resources:   controller:     trident-   main:     requests:       cpu:         10m       memory:         80Mi     limits:       cpu:  memory:   csi-   provisioner:     requests:       cpu: 2m       memory:         20Mi     limits:       cpu:       memory:   csi-   attacher:     requests:       cpu: 2m       memory:         20Mi     limits:       cpu:       memory:   csi-   resizer:     requests:       cpu: 3m       memory:         20Mi     limits:       cpu:       memory:   csi-   snapshotter:     requests:       cpu: 2m       memory:         20Mi     limits:</pre>

Parameter	Description	Default
httpsMetrics	Enable HTTPS for Prometheus metrics endpoint.	false
hostNetwork	Enables host networking for the Trident controller. This is useful when you want to separate the frontend and backend traffic in a multi-home network.	false



For more information on formatting pod parameters, refer to [Assigning Pods to Nodes](#)

## Sample configurations

You can use the attributes in [Configuration options](#) when defining `TridentOrchestrator` to customize your installation.

### Basic custom configuration

This example, created after running the `cat deploy/crds/tridentorchestrator_cr_imagepullsecrets.yaml` command, represents a basic custom installation:

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  imagePullSecrets:
  - thisisasecret
```

```
requests:
  cpu:
    1m

memory: 10Mi
limits:
  cpu:

memory:
  windows:
    trident-
main:

requests:
  cpu:
    6m

memory: 40Mi
limits:
```

## Node selectors

This example installs Trident with node selectors.

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  controllerPluginNodeSelector:
    nodetype: master
  nodePluginNodeSelector:
    storage: netapp
```

```
memory:
liveness-
```

## Windows worker nodes

This example, created after running the `cat deploy/crds/tridentorchestrator_cr.yaml` command, installs Trident on a Windows worker node.

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  windows: true
```

## Managed identities on an AKS cluster

This example installs Trident to enable managed identities on an AKS cluster.

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  cloudProvider: "Azure"
```

## Cloud identity on an AKS cluster

This example installs Trident for use with a cloud identity on an AKS cluster.

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  cloudProvider: "Azure"
  cloudIdentity: 'azure.workload.identity/client-id: xxxxxxxx-xxxx-
xxxx-xxxx-xxxxxxxxxxxxx'
```

## Cloud identity on an EKS cluster

This example installs Trident for use with a cloud identity on an AKS cluster.

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  cloudProvider: "AWS"
  cloudIdentity: "'eks.amazonaws.com/role-arn:
arn:aws:iam::123456:role/trident-role'"
```

## Cloud identity for GKE

This example installs Trident for use with a cloud identity on a GKE cluster.

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-gcp-gcnv
spec:
  version: 1
  storageDriverName: google-cloud-netapp-volumes
  projectNumber: '012345678901'
  network: gcnv-network
  location: us-west2
  serviceLevel: Premium
  storagePool: pool-premium1
```

## Kubernetes resource requests and limits configuration for Trident controller and Trident Linux node pods

This example configures Kubernetes resource requests and limits for Trident controller and Trident Linux node pods.



**Disclaimer:** The request and limit values provided in this example are for demonstration purposes only. Adjust these values based on your environment and workload requirements.

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  imagePullSecrets:
  - thisisasecret
  resources:
    controller:
      trident-main:
        requests:
          cpu: 10m
          memory: 80Mi
        limits:
          cpu: 200m
          memory: 256Mi
    # sidecars
    csi-provisioner:
      requests:
        cpu: 2m
        memory: 20Mi
      limits:
        cpu: 100m
        memory: 64Mi
    csi-attacher:
      requests:
        cpu: 2m
        memory: 20Mi
      limits:
        cpu: 100m
        memory: 64Mi
    csi-resizer:
      requests:
        cpu: 3m
        memory: 20Mi
```

```
limits:
  cpu: 100m
  memory: 64Mi
csi-snapshotter:
  requests:
    cpu: 2m
    memory: 20Mi
  limits:
    cpu: 100m
    memory: 64Mi
trident-autosupport:
  requests:
    cpu: 1m
    memory: 30Mi
  limits:
    cpu: 50m
    memory: 128Mi
node:
  linux:
    trident-main:
      requests:
        cpu: 10m
        memory: 60Mi
      limits:
        cpu: 200m
        memory: 256Mi
    # sidecars
    node-driver-registrar:
      requests:
        cpu: 1m
        memory: 10Mi
      limits:
        cpu: 50m
        memory: 32Mi
```

## Kubernetes resource requests and limits configuration for Trident controller and Trident Windows and Linux node pods

This example configures Kubernetes resource requests and limits for Trident controller and Trident Windows and Linux node pods.



**Disclaimer:** The request and limit values provided in this example are for demonstration purposes only. Adjust these values based on your environment and workload requirements.

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  imagePullSecrets:
  - thisisasecret
  windows: true
  resources:
    controller:
      trident-main:
        requests:
          cpu: 10m
          memory: 80Mi
        limits:
          cpu: 200m
          memory: 256Mi
      # sidecars
      csi-provisioner:
        requests:
          cpu: 2m
          memory: 20Mi
        limits:
          cpu: 100m
          memory: 64Mi
      csi-attacher:
        requests:
          cpu: 2m
          memory: 20Mi
        limits:
          cpu: 100m
          memory: 64Mi
      csi-resizer:
        requests:
```

```
    cpu: 3m
    memory: 20Mi
  limits:
    cpu: 100m
    memory: 64Mi
csi-snapshotter:
  requests:
    cpu: 2m
    memory: 20Mi
  limits:
    cpu: 100m
    memory: 64Mi
trident-autosupport:
  requests:
    cpu: 1m
    memory: 30Mi
  limits:
    cpu: 50m
    memory: 128Mi
node:
  linux:
    trident-main:
      requests:
        cpu: 10m
        memory: 60Mi
      limits:
        cpu: 200m
        memory: 256Mi
    # sidecars
    node-driver-registrar:
      requests:
        cpu: 1m
        memory: 10Mi
      limits:
        cpu: 50m
        memory: 32Mi
  windows:
    trident-main:
      requests:
        cpu: 6m
        memory: 40Mi
      limits:
        cpu: 200m
        memory: 128Mi
    # sidecars
    node-driver-registrar:
```

```
requests:
  cpu: 6m
  memory: 40Mi
limits:
  cpu: 100m
  memory: 128Mi
liveness-probe:
  requests:
    cpu: 2m
    memory: 40Mi
  limits:
    cpu: 50m
    memory: 64Mi
```

## Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.