Use Astra Data Store with VMware

Astra Data Store

NetApp
June 01, 2022

Table of Contents

Use Astra Data Store with VMware

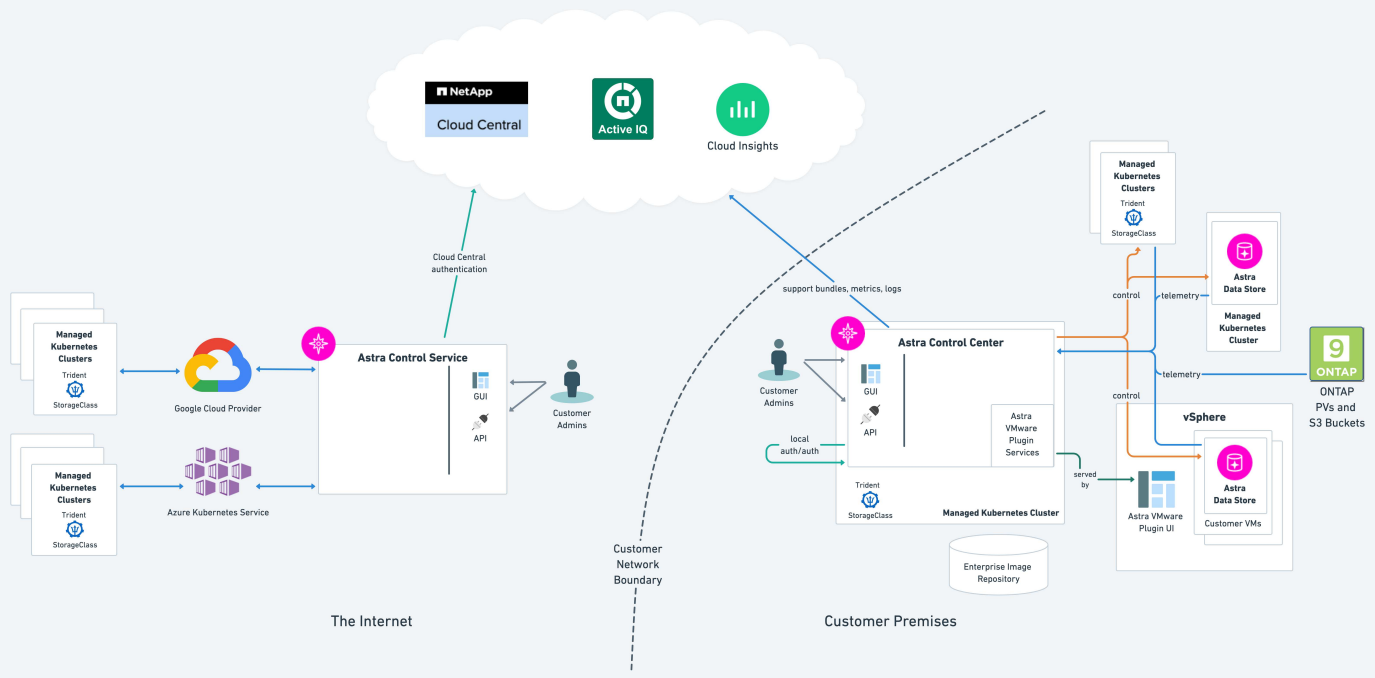
Learn about Astra Data Store with VMware

Astra Data Store supports both containerized and virtualized workloads. Integrations with vVols and storage policy-based management enable vSphere administrators to apply a storage quality of service. The NetApp Astra Plugin for VMware vSphere provides a familiar management and monitoring experience, eliminating cumbersome storage tasks.

The Astra Plugin for VMware vSphere offers the following benefits:

- VM granular storage provisioning with full vVols and VASA integrations
- Storage policy-based management integration
- vCenter plugin for vSphere native management

The following image shows the Astra family ecosystem with VMware.



For more information

- Astra Control Center documentation
- Astra family introduction

Astra Data Store with VMware requirements

After you verify that your environment meets general Astra Data Store requirements, you should verify that your environment also meets minimum requirements for VMware components such as the VMware VASA provider and the NetApp Astra Plugin for VMware vSphere.

VMWare vSphere requirements

Astra Data Store uses the VMWare VASA Provider as an API interface to communicate with storage. Make sure your environment meets the basic VASA Provider requirements as well as the following additional requirements:

- VMware vSphere 7.0 (Update 1 through Update 3 supported)
- One unassigned IP address for ingress traffic

- NetApp Astra Plugin for VMware vSphere does not support vSphere 7.0 Update 3c; use vSphere 7.0 Update 3d instead.
- NetApp Astra Plugin for VMware vSphere does not support Linked Mode vCenter servers.

NetApp Astra Plugin for VMware vSphere requirements

The NetApp Astra Plugin for VMware vSphere has the following requirements:

- An Astra Control Center instance running on a Kubernetes cluster
- A licensed Astra Data Store instance running on a Kubernetes cluster

Supported web browsers

The NetApp Astra Plugin for VMware vSphere supports the latest versions of the following web browsers:

- Mozilla Firefox
- Microsoft Edge (Chromium-based)
- Google Chrome

For more information

- Astra Control Center documentation
- Astra family introduction
- Astra Data Store requirements

Set up Astra Data Store with VMware

You can set up Astra Data Store as a storage backend and manage it using the NetApp Astra Plugin for VMware vSphere.

Setting up Astra Data Store with VMware involves the following tasks:

- Activate VMware vSphere services using Astra Control Center.
- Add a vCenter using Astra Control Center.
- Create a custom SCC (if using OpenShift)
- Use an existing storage backend in the Astra Plugin for VMware vSphere.
- Create a datastore using the Astra Plugin for VMware vSphere.
- Generate VM storage policies.

What you'll need

Before you set up Astra Data Store with VMware, you'll need to ensure the following:

- Astra Control Center is installed and set up.
- Astra Data Store is licensed and deployed. See Install Astra Data Store.

> For the Astra Data Store Early Access Program (EAP) release, Astra Control Center and Astra Data Store must be deployed in two different Kubernetes clusters.

- The Kubernetes clusters that were used to deploy Astra Control Center and Astra Data Store must already be managed by Astra Control Center.
- You have uploaded your Astra Control Center and VASA provider packages before adding a vCenter. See Manage software packages.

Activate VMware vSphere services using Astra Control Center

Begin setting up Astra Data Store with VMware by activating vSphere services on Astra Control Center.

> VMware vSphere services in Astra Control Center are not enabled by default.

1. Log in to Astra Control Center.
2. From the left navigation, select **Clusters**.

   The banner displays a message that VMware vSphere services are not yet enabled.

3. Select **Enable VMware vSphere services**.

   This action might take a while. After the services are enabled, the **Add vCenter** button is enabled.

Add a vCenter using Astra Control Center

Add your first vCenter, which registers the Astra Plugin for VMware vSphere.

You must have administrative privileges to add the vCenter to Astra Control Center.

> After the plugin is registered with VMware vSphere, the Astra Plugin for VMware vSphere icon appears in the VMware Shortcuts page.

1. Log in to Astra Control Center.
2. From the left navigation, select **Clusters**.
3. Select **Add vCenter**.
4. Enter the vCenter server details, vCenter port, and administrative user name and password to provide them to Astra Control Center.

   > This enables deployment of the Astra Plugin for this vCenter in the VMware vSphere client.

5. Select **Add**.

   The vCenter appears on the Clusters page and the total number of managed vCenters is updated on the

Astra Control Dashboard. This also initiates the Astra Plugin for VMware vSphere deployment.

Verify the vCenter addition

The newly added vCenter appears on the Clusters page and on the Dashboard.

Both vCenters and Kubernetes clusters appear on the Astra Control Center Dashboard.

1. Access Astra Control Center.
2. From the left navigation, select **Clusters**.
3. Verify that the newly managed vCenter appears on the Clusters page.
4. From the left navigation, select **Dashboard**.
5. From the Astra Control Center Dashboard, note the new managed vCenter cluster as part of the **Managed** count.

   The Managed Clusters count includes both vCenters and Kubernetes clusters.

6. To view cluster details, click the **Managed** count.

   The Clusters page appears.

Create a custom SCC (if using OpenShift)

If you are using OpenShift, you can optionally assign security context constraints (SCC) that control the actions that a pod can perform and control what the pod can access.

By default, the execution of any container will be granted the restricted SCC and only the capabilities defined by that SCC. Restricted SCC does not provide permissions required by VASA provider pods. Use this procedure to provide the required higher privileges (listed in the sample) to the service accounts used by VASA provider deployments.

Assign a custom SCC to various default service accounts for the Astra Data Store 'ntv-system' namespace, which is a hybrid of privileged and node-exporter SCCs.

The following steps are needed only for deployment on the Red Hat OpenShift Container Platform (OCP).

1. Create a custom SCC called `vp_backend_privileged_scc.yaml`:

   ```
   kubectl create -f vp_backend_privileged_scc.yaml
   ```

   Sample: vp_backend_privileged_scc.yaml

   ```
   allowHostDirVolumePlugin: true
   allowHostIPC: false
   allowHostNetwork: true
   allowHostPID: false
   allowHostPorts: true
   ```

```
allowPrivilegeEscalation: true
allowPrivilegedContainer: true
allowedCapabilities:
  - '*'
allowedUnsafeSysctls:
  - '*'
apiVersion: security.openshift.io/v1
defaultAddCapabilities: null
fsGroup:
  type: RunAsAny
groups: []
kind: SecurityContextConstraints
metadata:
  name: vpbackend-privileged
priority: null
readOnlyRootFilesystem: false
requiredDropCapabilities: null
runAsUser:
  type: RunAsAny
seLinuxContext:
  type: RunAsAny
seccompProfiles:
  - '*'
supplementalGroups:
  type: RunAsAny
users:
  - system:serviceaccount:ntv-system:default
  - system:serviceaccount:ntv-system:ntv-auth-svc
  - system:serviceaccount:ntv-system:ntv-autosupport
  - system:serviceaccount:ntv-system:ntv-compliance-svc
  - system:serviceaccount:ntv-system:ntv-datastore-svc
  - system:serviceaccount:ntv-system:ntv-metallb-controller
  - system:serviceaccount:ntv-system:ntv-metallb-speaker
  - system:serviceaccount:ntv-system:ntv-mongodb
  - system:serviceaccount:ntv-system:ntv-nfs-svc
  - system:serviceaccount:ntv-system:ntv-rabbitmq-svc
  - system:serviceaccount:ntv-system:ntv-storage-svc
  - system:serviceaccount:ntv-system:ntv-vault
  - system:serviceaccount:ntv-system:ntv-vault-admin
  - system:serviceaccount:ntv-system:ntv-vault-agent-injector
  - system:serviceaccount:ntv-system:ntv-vault-controller
  - system:serviceaccount:ntv-system:ntv-vault-initializer
  - system:serviceaccount:ntv-system:ntv-vcenter-svc
  - system:serviceaccount:ntv-system:ntv-vm-management-svc
  - system:serviceaccount:ntv-system:ntv-watcher-svc
  - system:serviceaccount:ntv-system:ntv-vault-sa-vault-tls
```

```
  - system:serviceaccount:ntv-system:ntv-gateway-svc
  - system:serviceaccount:ntv-system:ntv-jobmanager-svc
  - system:serviceaccount:ntv-system:ntv-vasa-svc
volumes:
  - '*'
```

2. Display the newly added SCC using the `oc get scc` command:

```
oc get scc vpbackend-privileged
```

Response:

```
NAME                  PRIV  CAPS  SELINUX  RUNASUSER FSGROUP  SUPGROUP
PRIORITY   READONLYROOTFS VOLUMES
vpbackend-privileged true ["*"]  RunAsAny RunAsAny  RunAsAny RunAsAny
<no value> false          ["*"]
```

Use an existing storage backend in the Astra Plugin for VMware vSphere

After adding a vCenter by using the Astra Control Center UI, add the Astra Data Store storage backend using the Astra Plugin for VMware vSphere.

This process completes the following actions:

- Adds an existing storage backend to the selected vCenter.
- Registers the VASA provider with the selected vCenter. The VASA provider provides communication between VMware and Astra Data Store.
- Adds a VASA provider self-signed certificate to the storage backend.

It can sometimes take 10 minutes for the vCenter you added to appear in the storage backend wizard.

Astra Data Store should not be shared with multiple vCenters.

Steps

1. Access the NetApp Astra Plugin for VMware vSphere.
2. From the left navigation, select **Astra Plugin for VMware vSphere** or from the Shortcuts page, select the **Astra Plugin for VMware vSphere** icon.
3. From the Astra Plugin for VMware vSphere Overview page, select **Use existing storage backend**. Or, from the left navigation, select **Storage Backends** > **Add**, and select **Use existing storage backend**.
4. Select the existing Astra Data Store as the storage backend and select **Next**.
5. On the VASA provider page, enter the VASA provider name, IP address (if using a load balancer), user name, and password.

For the user name, you can use alphanumeric characters and the underscore. Do not enter any special characters. The first letter of the user name must begin with an alphabet character.

6. Indicate whether you want to deploy a load balancer and enter the IP address, which will be used to access the VASA provider. The IP needs to be an additional routable free IP separate from the node IPs. When the load balancer is enabled, Metallb is deployed in the Astra Data Store Kubernetes cluster and configured to allocate the free IP.

   If you are using a Google Anthos cluster for deployment, choose not to deploy a load balancer as Anthos already runs metallb as a load balancer. The metallb deploy flag should be set to false in VASA provider CR (v1beta1_vasaprovider.yaml).

   If you choose not to deploy a load balancer, it is assumed that the load balancer has already been deployed and configured to allocate IPs for the Kubernetes service of type **Load Balancer**.

   At this point in the deployment, the VASA provider is not yet deployed.

7. Select **Next**.
8. On the Certificate page, review the certificate information for the self-signed certificate.
9. Select **Next**.
10. Review summary information.
11. Select **Add**.

    This deploys the VASA provider.

Verify the storage backend in the Astra Plugin for VMware vSphere

After the Astra Data Store storage backend is registered, it appears in the Astra Plugin for VMware vSphere storage backends list.

You can determine the storage backend status and the VASA provider status. You can also see the used capacity of each storage backend.

After selecting a storage backend, you can also view used and available capacity, data reduction ratio, and internal network management IP address.

Steps

1. In the NetApp Astra Plugin for VMware vSphere, from the left navigation, select **Storage Backends**.
2. Select the Astra Data Store storage backend to see the Summary tab.
3. Review used and available capacity, data reduction ratio, and status of the VASA provider.
4. Select the other tabs to see information about VMs, datastores, hosts, and storage nodes.

Create a datastore using the Astra Plugin for VMware vSphere

After adding the storage backend and registering the Astra Plugin for VMware vSphere, you can create a datastore in VMware.

You can add the datastore to a datacenter, compute, or a host cluster.

You cannot use the same storage backend to create multiple datastores under same datacenter.

You can add a vVol datastore type using an NFS protocol.

Steps

1. Access the Astra Plugin for VMware vSphere.
2. From the plugin menu, select **Create Datastore**.
3. Enter the new datastore name, type (vVol), and protocol (NFS).
4. Select **Next**.
5. From the Storage page, select the Astra Data Store storage backend that you just created.

   You cannot use a storage backend that has an existing datastore.

6. Select **Next**.
7. From the Summary page, review the information.
8. Select **Create**.

   If you encounter an error related to a failed scan or general system error, rescan/synchronize your storage provider on vCenter then try to create the datastore again.

Generate VM storage policies

After you create a datastore and before you create VMs, you should generate predesigned VM storage policies by using `/virtualization/api/v1/vcenters/vm-storage-policies` in the REST API UI.

Steps

1. Access the REST API UI page by going to `https://<ads_gateway_ip>:8443`.
2. Go to the API `POST /virtualization/api/auth/login` and provide the username, password and vCenter hostname.

   Response:

```
{
  "vmware-api-session-id": "212f4d6447b05586ab1509a76c6e7da56d29cc5b",
  "vcenter-guid": "8e475060-b3c8-4267-bf0f-9d472d592d39"
}
```

3. Go to the API `GET /virtualization/api/auth/validate-session` and complete the following steps:
   a. Use the `vmware-api-session-id` and `vcenter-guid` generated above as headers.
   b. Select **Try it now**.

   Response: (authentication truncated below):

```
authorization: eyJhbGciOiJSUzI1NiIsInR...9h15DYYvClT3oA  connection:
keep-alive  content-type: application/json  date: Wed,18 May 2022
13:31:18 GMT  server: nginx  transfer-encoding: chunked
```

4. Go to the API `/virtualization/api/v1/vcenters/vm-storage-policies` and add the bearer token generated in the previous response as 'authorization'.

   A "200" response appears and three VM storage policies are generated.

5. Verify the new VM storage policies (named Bronze, Silver, and Gold) on the VCenter Storage Policy page.
6. Continue by creating VMs.

What's next

Next, you might want to do the following tasks:

- Create VMs.
- Mount the datastore. See Mount a datastore.

For more information

- Astra Control Center documentation
- Astra family introduction

Monitor components of your VMware installation

You can use the NetApp Astra Plugin for VMware vSphere to monitor components of your Astra Data Store installation. You can monitor the health of your system including the storage backends, VASA providers, VMs, and vVols. You can also view capacity and vCenter information.

Monitor the health of your system using the Astra Plugin for VMware vSphere Dashboard

Managing your Astra Data Store with VMware environment involves monitoring the overall health of storage backends and VASA providers.

Using the NetApp Astra Plugin for VMware vSphere Dashboard, you can see the following information:

- Physical used and available capacity of all storage backends in this vCenter. You can hover over information and see more details.
- Healthy and unhealthy storage backends and VASA providers
- Latency, IOPS, throughput and capacity utilization for the top 10 VMs.

From the Dashboard, you can perform several additional tasks:

- Monitor capacity
- Use an existing storage backend. See Set up storage backends.
- Access the product documentation

Steps to review the Dashboard

1. Access the Astra Plugin for VMware vSphere.
2. From the Overview page, review the following sections:
   a. **Storage backends** section: You can click on the states of both the storage backends and VASA providers to see details about their status. You can also click to view all storage backends.
   b. **Storage Backend Capacity** section: Review the total physical used and available capacity for the storage backends in the selected vCenter. To change the vCenter server, click the vCenter Server option in the upper right.
   c. **Virtual Machines** section: Review virtual machines having the top 10 capacity utilization.

You can instead show what you want, for example, the top 10 VMs with high latency, by clicking on the table heading.

Steps to monitor Astra Data Store in other views

1. Access the following views to monitor Astra Data Store components:
   - **Virtual Machines** tab: Lists all the VMs that are managed by Astra Data Store compared to the Dashboard, which lists only the top 10 VMs.
   - **Storage** drill down: Displays hosts, virtual machines and datastores that are associated with the storage system.
   - **VM Storage** view: Provides details of vVols that are created by the VASA provider.

Review storage backend threshold settings

Storage backend capacity threshold settings govern when alert notifications appear on all datastores in the storage backend.

The following default thresholds are set when you deploy or add a storage backend by using the Astra Plugin for VMware vSphere:

- 90% full generates a red alert
- 80% full generates a yellow alert

You can view the level at which the system generates an alert in VMware.

For the Astra Data Store Early Access Program, if the same storage container is used across multiple datacenters, you might see an incorrect alarm for datastores.

Steps

1. Access the NetApp Astra Plugin for VMware vSphere.
2. From the left navigation, select **Settings**.
3. Review the settings thresholds.

For more information

- Astra Control Center documentation
- Astra family introduction

Manage Astra Data Store components of your VMware installation

You can manage the following Astra Data Store components in your vSphere environment and from Astra Control Center:

- Work with managed vCenters
- Manage VMs from vSphere
- Manage the storage backend
- Manage datastores

Work with managed vCenters

You can work with the managed vCenters in the following ways:

- View vCenter details in Astra Control Center
- View vCenter details in Astra Control Center
- Unmanage a vCenter in Astra Control Center

View vCenter details in Astra Control Center

You can determine all the vCenters associated with a cluster.

Steps

1. From the Astra Control Center left navigation, select **Clusters**.
2. View the list of vCenters.
3. Select **Save**.

View vCenter details in Astra Control Center

You might want to view the health of your system and clusters. You can determine how many clusters are managed by looking at the Astra Control Center Dashboard.

Steps

1. From the Astra Control Center left navigation, select **Clusters**.
2. Select the vCenter.
3. View the information.

Unmanage a vCenter in Astra Control Center

If you no longer want Astra Control Center to manage the vCenter, you can unmanage it. This removes and unregisters the vCenter from Astra Control Center.

Clusters, storage backends and VMs associated with this vCenter must be removed from the Astra Plugin for VMware vSphere first.

Steps

1. From the Astra Control Center left navigation, select **Clusters**.

2. From the Clusters page, select the vCenter.

   Or, select multiple vCenters and select **Unmanage all**.

3. Right-click the **Actions** menu and select **Unmanage**.
4. In the Unmanage vCenter page, type "unmanage".
5. Select **Yes, unmanage vCenter**.

Manage VMs from vSphere

You can manage VMs associated with Astra Data Store using native vSphere operations.

- Delete VM
- Rename VM
- Resize VM

For this release, you can only resize one VM disk at a time. Attempts to resize multiple disks will fail.

- Power VM on or off
- Suspend VM
- Reset VM

The following snapshot workflows are available for the Astra Data Store using native vCenter operations:

- Take snapshot of Astra Data Store
- Revert a snapshot
- Delete a snapshot

Snapshot operations might occasionally fail with a vVol runtime error. If this happens, retry the operation.

Manage the storage backend

You can remove the storage backend. Removing a storage backend does not destroy it and does not delete the Astra Data Store product itself; it just unregisters the VASA provider from VMware and unlinks the storage backend for that vCenter.

If the VASA provider is enabled and deployed outside of the vCenter, you can only remove Astra Data Store. If the storage backend is being used as part of a provisioning datastores process, you won't be able to remove the storage backend.

If Astra Data Store is not being linked with more than one vCenter, when you remove it, the VASA provider will be unregistered and uninstalled.

Steps

1. Access the Astra Plugin for VMware vSphere.

2. From the left navigation, select **Storage Backends**.
3. On the Storage Backends page, click on the storage backend Actions menu and select **Remove**.
4. Enter the VASA provider user name and password.
5. Select **Remove**.

Manage datastores

You can manage Astra Data Store in your vSphere environment using native vCenter operations to manage VMs and Astra Plugin extensions to manage datastores:

- Create a datastore
- Mount a datastore
- Delete a datastore

Mount a datastore

Using the Astra Plugin for VMware vSphere, you can mount the datastore on one or more additional hosts.

Steps

1. Select the datastore for Astra Data Store from your data center inventory in vCenter.
2. Right-click the datastore and select **Astra Plugin for VMware vSphere** > **Mount Datastore**.
3. From the Mount datastore on hosts page, select the hosts on which you want to mount the datastore.

   If you want to mount the datastore on all hosts, check **Mount on all hosts**.

4. Select **Mount**.

After you initiate the operation, you can follow progress in the Recent Tasks panel in the vSphere Client.

If you encounter an error related to a failed scan or general system error, rescan/synchronize your storage provider on vCenter then try to create the datastore again.

Delete a datastore

Using the Astra Plugin for VMware vSphere, you can delete a datastore.

To delete the datastore, all VMs on the datastore must first be removed.

Steps

1. Select the datastore from your data center inventory in vCenter.
2. Right-click the datastore and select **Astra Plugin** > **Delete Datastore**.
3. In the Delete Datastore page, confirm the information or take additional suggested actions so that the datastore can be deleted.
4. Select **Delete**.

For more information

- Astra Control Center documentation
- Astra family introduction

Uninstall Astra Data Store from a VMware-integrated environment

You can uninstall Astra Data Store and its related components from your vSphere environment.

See these instructions on uninstalling Astra Data Store.

For more information

- Astra Control Center documentation
- Astra family introduction