Add a provider-managed cluster

Astra Control Service

NetApp
July 29, 2024

This PDF was generated from https://docs.netapp.com/us-en/astra-control-service/get-started/add-public-provider-managed-cluster.html on July 29, 2024. Always check docs.netapp.com for the latest.

Table of Contents

Add a provider-managed cluster

Add a public provider-managed cluster to Astra Control Service

After you set up your cloud environment, you're ready to create a Kubernetes cluster and then add it to Astra Control Service.

- Create a Kubernetes cluster
- Add the cluster to Astra Control Service
- Change the default storage class

Create a Kubernetes cluster

If you don't have a cluster yet, you can create one that meets the requirements of one of the following providers:

- Astra Control Service requirements for Azure Kubernetes Service (AKS) with Azure NetApp Files
- Astra Control Service requirements for Azure Kubernetes Service (AKS) with Azure managed disks
- Astra Control Service requirements for Google Kubernetes Engine (GKE)
- Astra Control Service requirements for Amazon Elastic Kubernetes Service (EKS)

Astra Control Service supports AKS clusters that use Azure Active Directory (Azure AD) for authentication and identity management. When you create the cluster, follow the instructions in the official documentation to configure the cluster to use Azure AD. You'll need to make sure your clusters meet the requirements for AKS-managed Azure AD integration.

Add the cluster to Astra Control Service

After you log in to Astra Control Service, your first step is to start managing your clusters. Before you add a cluster to Astra Control Service, you'll need to perform specific tasks and make sure the cluster meets certain requirements.

When you manage Azure Kubernetes Service and Google Kubernetes Engine clusters, note that you have two options for Astra Control Provisioner installation and lifecycle management:

- You can use Astra Control Service to automatically manage the lifecycle of Astra Control Provisioner. To do this, make sure that Astra Trident is not installed and Astra Control Provisioner is not enabled on the cluster that you want to manage with Astra Control Service. In this case, Astra Control Service automatically enables Astra Control Provisioner when you begin managing the cluster, and Astra Control Provisioner upgrades are handled automatically.
- You can manage the lifecycle of Astra Control Provisioner yourself. To do this, enable Astra Control Provisioner on the cluster before managing the cluster with Astra Control Service. In this case, Astra Control Service detects that Astra Control Provisioner is already enabled and does not reinstall it or manage Astra Control Provisioner upgrades. Refer to Enable Astra Control Provisioner for steps enable Astra Control Provisioner.

When you manage Amazon Web Services clusters with Astra Control Service, if you need storage backends that can only be used with Astra Control Provisioner, you need to enable Astra Control Provisioner manually on

the cluster before you manage it with Astra Control Service. Refer to Enable Astra Control Provisioner for steps to enable Astra Control Provisioner.

Before you begin

Amazon Web Services

- You should have the JSON file containing the credentials of the IAM user that created the cluster. Learn how to create an IAM user.
- Astra Control Provisioner is required for Amazon FSx for NetApp ONTAP. If you plan to use Amazon FSx for NetApp ONTAP as a storage backend for your EKS cluster, refer to the Astra Control Provisioner information in the EKS cluster requirements.
- (Optional) If you need to provide provide `kubectl` command access for a cluster to other IAM users that are not the cluster's creator, refer to the instructions in How do I provide access to other IAM users and roles after cluster creation in Amazon EKS?.
- If you plan to use NetApp Cloud Volumes ONTAP as a storage backend, you need to configure Cloud Volumes ONTAP to work with Amazon Web Services. Refer to the Cloud Volumes ONTAP setup documentation.

Microsoft Azure

- You should have the JSON file that contains the output from the Azure CLI when you created the service principal. Learn how to set up a service principal.

  You'll also need your Azure subscription ID, if you didn't add it to the JSON file.

- If you plan to use NetApp Cloud Volumes ONTAP as a storage backend, you need to configure Cloud Volumes ONTAP to work with Microsoft Azure. Refer to the Cloud Volumes ONTAP setup documentation.

Google Cloud

- You should have the service account key file for a service account that has the required permissions. Learn how to set up a service account.
- If you plan to use NetApp Cloud Volumes ONTAP as a storage backend, you need to configure Cloud Volumes ONTAP to work with Google Cloud. Refer to the Cloud Volumes ONTAP setup documentation.

Steps

1. (Optional) If you are adding an Amazon EKS cluster or want to manage the installation and upgrades of Astra Control Provisioner yourself, enable Astra Control Provisioner on the cluster. Refer to Enable Astra Control Provisioner for enablement steps.
2. Open the Astra Control Service web UI in a browser.
3. On the Dashboard, select **Manage Kubernetes cluster**.

   Follow the prompts to add the cluster.

4. **Provider**: Select your cloud provider and then either provide the required credentials to create a new cloud instance, or select an existing cloud instance to use.
   a. **Amazon Web Services**: Provide details about your Amazon Web Services IAM user account by uploading a JSON file or by pasting the contents of that JSON file from your clipboard.

      The JSON file should contain the credentials of the IAM user that created the cluster.

b. **Microsoft Azure**: Provide details about your Azure service principal by uploading a JSON file or by pasting the contents of that JSON file from your clipboard.

   The JSON file should contain the output from the Azure CLI when you created the service principal. It can also include your subscription ID so it's automatically added to Astra. Otherwise, you need to manually enter the ID after providing the JSON.

c. **Google Cloud Platform**: Provide the service account key file either by uploading the file or by pasting the contents from your clipboard.

   Astra Control Service uses the service account to discover clusters running in Google Kubernetes Engine.

d. **Other**: This tab is for use with self-managed clusters only.

5. **Cloud instance name**: Provide a name for the new cloud instance that will be created when you add this cluster. Learn more about cloud instances.
6. Select **Next**.

   Astra Control Service displays a list of clusters that you can choose from.

7. **Cluster**: Select a cluster from the list to add to Astra Control Service.

   When you are selecting from the list of clusters, pay careful attention to the **Eligiblity** column. If a cluster is "Ineligible" or "Partially eligible", hover over the status to determine if there's an issue with the cluster. For example, it might identify that the cluster doesn't have a worker node.

8. Select **Next**.
9. (Optional) **Storage**: Optionally, select the storage class that you'd like Kubernetes applications deployed to this cluster to use by default.
   a. To select a new default storage class for the cluster, enable the **Assign a new default storage class** check box.
   b. Select a new default storage class from the list.

   Each cloud provider storage service displays the following price, performance, and resilience information:

   - Cloud Volumes Service for Google Cloud: Price, performance, and resilience information
   - Google Persistent Disk: No price, performance, or resilience information available
   - Azure NetApp Files: Performance and resilience information
   - Azure Managed disks: No price, performance, or resilience information available
   - Amazon Elastic Block Store: No price, performance, or resilience information available
   - Amazon FSx for NetApp ONTAP: No price, performance, or resilience information available
   - NetApp Cloud Volumes ONTAP: No price, performance, or resilience information available

Each storage class can utilize one of the following services:

- Cloud Volumes Service for Google Cloud
- Google Persistent Disk
- Azure NetApp Files
- Azure managed disks
- Amazon Elastic Block Store
- Amazon FSx for NetApp ONTAP
- NetApp Cloud Volumes ONTAP

  Learn more about storage classes for Amazon Web Services clusters, storage classes for GKE clusters, and storage classes for AKS clusters.

10. Select **Next**.
11. **Review & Approve**: Review the configuration details.
12. Select **Add** to add the cluster to Astra Control Service.

Result

If this is the first cluster that you have added for this cloud provider, Astra Control Service creates an object store for the cloud provider for backups of applications running on eligible clusters. (When you add subsequent clusters for this cloud provider, no further object stores are created.) If you specified a default storage class, Astra Control Service sets the default storage class that you specified. For clusters managed in Amazon Web Services or Google Cloud Platform, Astra Control Service also creates an admin account on the cluster. These actions can take several minutes.

Change the default storage class

You can change the default storage class for a cluster.

Change the default storage class using Astra Control

You can change the default storage class for a cluster from within Astra Control. If your cluster uses a previously installed storage backend service, you might not be able to use this method to change the default storage class (the **Set as default** action is not selectable). In this case, you can Change the default storage class using the command line.

Steps

1. In the Astra Control Service UI, select **Clusters**.
2. On the **Clusters** page, select the cluster that you want to change.
3. Select the **Storage** tab.
4. Select the **Storage classes** category.
5. Select the **Actions** menu for the storage class that you want to set as default.
6. Select **Set as default**.

Change the default storage class using the command line

You can change the default storage class for a cluster using Kubernetes commands. This method works regardless of your cluster's configuration.

Steps

1. Log in to your Kubernetes cluster.
2. List the storage classes in your cluster:

```
kubectl get storageclass
```

3. Remove the default designation from the default storage class. Replace <SC_NAME> with the name of the storage class:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-
class":"false"}}}'
```

4. Mark a different storage class as default. Replace <SC_NAME> with the name of the storage class:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'
```

5. Confirm the new default storage class:

```
kubectl get storageclass
```

Add a private provider-managed cluster to Astra Control Service

You can use Astra Control Service to manage the following types of private provider-managed clusters:

- Amazon Elastic Kubernetes Service (EKS)
- Azure Kubernetes Service (AKS)
- Google Kubernetes Engine (GKE)
- Red Hat OpenShift Service on AWS (ROSA)
- ROSA with AWS PrivateLink

These instructions assume that you have already created a private cluster and prepared a secure method to remotely access it; for more information about creating and accessing private clusters, refer to the following documentation:

- Azure documentation for private AKS clusters
- Azure documentation for private OpenShift clusters
- Amazon EKS documentation

- Google Kubernetes Engine (GKE) documentation
- Red Hat OpenShift Service on AWS (ROSA) documentation

You need to perform the following tasks to add your private cluster to Astra Control Service:

1. Install Astra Connector
2. Set up persistent storage
3. Add the private provider-managed cluster to Astra Control Service

Install Astra Connector

Before you add a private cluster, you need to install Astra Connector on the cluster so that Astra Control can communicate with it. Refer to Install the previous version of Astra Connector for private clusters managed with non-Kubernetes-native workflows for instructions.

Set up persistent storage

Configure persistent storage for the cluster. Refer to the Get Started documentation for more information about configuring persistent storage:

- Set up Microsoft Azure with Azure NetApp Files
- Set up Microsoft Azure with Azure managed disks
- Set up Amazon Web Services
- Set up Google Cloud

Add the private provider-managed cluster to Astra Control Service

You can now add the private cluster to Astra Control Service.

When you manage Azure Kubernetes Service and Google Kubernetes Engine clusters, note that you have two options for Astra Control Provisioner installation and lifecycle management:

- You can use Astra Control Service to automatically manage the lifecycle of Astra Control Provisioner. To do this, make sure that Astra Trident is not installed and Astra Control Provisioner is not enabled on the cluster that you want to manage with Astra Control Service. In this case, Astra Control Service automatically enables Astra Control Provisioner when you begin managing the cluster, and Astra Control Provisioner upgrades are handled automatically.
- You can manage the lifecycle of Astra Control Provisioner yourself. To do this, enable Astra Control Provisioner on the cluster before managing the cluster with Astra Control Service. In this case, Astra Control Service detects that Astra Control Provisioner is already enabled and does not reinstall it or manage Astra Control Provisioner upgrades. Refer to Enable Astra Control Provisioner for steps enable Astra Control Provisioner.

When you manage Amazon Web Services clusters with Astra Control Service, if you need storage backends that can only be used with Astra Control Provisioner, you need to enable Astra Control Provisioner manually on the cluster before you manage it with Astra Control Service. Refer to Enable Astra Control Provisioner for steps to enable Astra Control Provisioner.

Before you begin

Amazon Web Services

- You should have the JSON file containing the credentials of the IAM user that created the cluster. Learn how to create an IAM user.
- Astra Control Provisioner is required for Amazon FSx for NetApp ONTAP. If you plan to use Amazon FSx for NetApp ONTAP as a storage backend for your EKS cluster, refer to the Astra Control Provisioner information in the EKS cluster requirements.
- (Optional) If you need to provide provide `kubectl` command access for a cluster to other IAM users that are not the cluster's creator, refer to the instructions in How do I provide access to other IAM users and roles after cluster creation in Amazon EKS?.
- If you plan to use NetApp Cloud Volumes ONTAP as a storage backend, you need to configure Cloud Volumes ONTAP to work with Amazon Web Services. Refer to the Cloud Volumes ONTAP setup documentation.

Microsoft Azure

- You should have the JSON file that contains the output from the Azure CLI when you created the service principal. Learn how to set up a service principal.

  You'll also need your Azure subscription ID, if you didn't add it to the JSON file.

- If you plan to use NetApp Cloud Volumes ONTAP as a storage backend, you need to configure Cloud Volumes ONTAP to work with Microsoft Azure. Refer to the Cloud Volumes ONTAP setup documentation.

Google Cloud

- You should have the service account key file for a service account that has the required permissions. Learn how to set up a service account.
- If the cluster is private, the authorized networks must allow the Astra Control Service IP address:

  52.188.218.166/32

- If you plan to use NetApp Cloud Volumes ONTAP as a storage backend, you need to configure Cloud Volumes ONTAP to work with Google Cloud. Refer to the Cloud Volumes ONTAP setup documentation.

Steps

1. (Optional) If you are adding an Amazon EKS cluster or want to manage the installation and upgrades of Astra Control Provisioner yourself, enable Astra Control Provisioner on the cluster. Refer to Enable Astra Control Provisioner for enablement steps.
2. Open the Astra Control Service web UI in a browser.
3. On the Dashboard, select **Manage Kubernetes cluster**.

   Follow the prompts to add the cluster.

4. **Provider**: Select your cloud provider and then either provide the required credentials to create a new cloud instance, or select an existing cloud instance to use.
   a. **Amazon Web Services**: Provide details about your Amazon Web Services IAM user account by uploading a JSON file or by pasting the contents of that JSON file from your clipboard.

The JSON file should contain the credentials of the IAM user that created the cluster.

b. **Microsoft Azure**: Provide details about your Azure service principal by uploading a JSON file or by pasting the contents of that JSON file from your clipboard.

   The JSON file should contain the output from the Azure CLI when you created the service principal. It can also include your subscription ID so it's automatically added to Astra. Otherwise, you need to manually enter the ID after providing the JSON.

c. **Google Cloud Platform**: Provide the service account key file either by uploading the file or by pasting the contents from your clipboard.

   Astra Control Service uses the service account to discover clusters running in Google Kubernetes Engine.

d. **Other**: This tab is for use with self-managed clusters only.

5. **Cloud instance name**: Provide a name for the new cloud instance that will be created when you add this cluster. Learn more about cloud instances.
6. Select **Next**.

   Astra Control Service displays a list of clusters that you can choose from.

7. **Cluster**: Select a cluster from the list to add to Astra Control Service.

   When you are selecting from the list of clusters, pay careful attention to the **Eligiblity** column. If a cluster is "Ineligible" or "Partially eligible", hover over the status to determine if there's an issue with the cluster. For example, it might identify that the cluster doesn't have a worker node.

1. Select **Next**.
2. (Optional) **Storage**: Optionally, select the storage class that you'd like Kubernetes applications deployed to this cluster to use by default.
   a. To select a new default storage class for the cluster, enable the **Assign a new default storage class** check box.
   b. Select a new default storage class from the list.

Each cloud provider storage service displays the following price, performance, and resilience information:

- Cloud Volumes Service for Google Cloud: Price, performance, and resilience information
- Google Persistent Disk: No price, performance, or resilience information available
- Azure NetApp Files: Performance and resilience information
- Azure Managed disks: No price, performance, or resilience information available
- Amazon Elastic Block Store: No price, performance, or resilience information available
- Amazon FSx for NetApp ONTAP: No price, performance, or resilience information available
- NetApp Cloud Volumes ONTAP: No price, performance, or resilience information available

Each storage class can utilize one of the following services:

- Cloud Volumes Service for Google Cloud
- Google Persistent Disk
- Azure NetApp Files
- Azure managed disks
- Amazon Elastic Block Store
- Amazon FSx for NetApp ONTAP
- NetApp Cloud Volumes ONTAP

Learn more about storage classes for Amazon Web Services clusters, storage classes for GKE clusters, and storage classes for AKS clusters.

3. Select **Next**.
4. **Review & Approve**: Review the configuration details.
5. Select **Add** to add the cluster to Astra Control Service.

Result

If this is the first cluster that you have added for this cloud provider, Astra Control Service creates an object store for the cloud provider for backups of applications running on eligible clusters. (When you add subsequent clusters for this cloud provider, no further object stores are created.) If you specified a default storage class, Astra Control Service sets the default storage class that you specified. For clusters managed in Amazon Web Services or Google Cloud Platform, Astra Control Service also creates an admin account on the cluster. These actions can take several minutes.

Change the default storage class

You can change the default storage class for a cluster.

Change the default storage class using Astra Control

You can change the default storage class for a cluster from within Astra Control. If your cluster uses a

previously installed storage backend service, you might not be able to use this method to change the default storage class (the **Set as default** action is not selectable). In this case, you can Change the default storage class using the command line.

Steps

1. In the Astra Control Service UI, select **Clusters**.
2. On the **Clusters** page, select the cluster that you want to change.
3. Select the **Storage** tab.
4. Select the **Storage classes** category.
5. Select the **Actions** menu for the storage class that you want to set as default.
6. Select **Set as default**.

Change the default storage class using the command line

You can change the default storage class for a cluster using Kubernetes commands. This method works regardless of your cluster's configuration.

Steps

1. Log in to your Kubernetes cluster.
2. List the storage classes in your cluster:

```
kubectl get storageclass
```

3. Remove the default designation from the default storage class. Replace <SC_NAME> with the name of the storage class:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-
class":"false"}}}'
```

4. Mark a different storage class as default. Replace <SC_NAME> with the name of the storage class:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'
```

5. Confirm the new default storage class:

```
kubectl get storageclass
```

Copyright information

Copyright © 2024 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.