



Clusters

Astra Automation

NetApp
February 12, 2024

Table of Contents

- Clusters 1
 - List the clusters 1
 - Add a cluster using credentials 4
 - List managed clusters 6
 - Manage a cluster 6

Clusters

List the clusters

You can list the available clusters in a specific cloud.

1. Select the cloud

Perform the workflow [List the clouds](#) and select the cloud containing the clusters.

2. List the clusters

Perform the following REST API call to list the clusters in a specific cloud.

HTTP method	Path
GET	/accounts/{account_id}/topology/v1/clouds/{cloud_id}/clusters

Curl example: Return all data for all clusters

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/topology/v1/clouds/<CLOUD_ID>/clusters' --header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

JSON output example

```
{
  "items": [
    {
      "type": "application/astra-cluster",
      "version": "1.1",
      "id": "7ce83fba-6aa1-4e0c-a194-26e714f5eb46",
      "name": "openshift-clstr-ol-07",
      "state": "running",
      "stateUnready": [],
      "managedState": "managed",
      "protectionState": "full",
      "protectionStateDetails": [],
      "restoreTargetSupported": "true",
      "snapshotSupported": "true",
      "managedStateUnready": [],
      "managedTimestamp": "2022-11-03T15:50:59Z",
      "inUse": "true",
      "clusterType": "openshift",
      "accHost": "true",
```

```
"clusterVersion": "1.23",
"clusterVersionString": "v1.23.12+6b34f32",
"namespaces": [
  "default",
  "kube-node-lease",
  "kube-public",
  "kube-system",
  "metallb-system",
  "mysql",
  "mysql-clone1",
  "mysql-clone2",
  "mysql-clone3",
  "mysql-clone4",
  "netapp-acc-operator",
  "netapp-monitoring",
  "openshift",
  "openshift-apiserver",
  "openshift-apiserver-operator",
  "openshift-authentication",
  "openshift-authentication-operator",
  "openshift-cloud-controller-manager",
  "openshift-cloud-controller-manager-operator",
  "openshift-cloud-credential-operator",
  "openshift-cloud-network-config-controller",
  "openshift-cluster-csi-drivers",
  "openshift-cluster-machine-approver",
  "openshift-cluster-node-tuning-operator",
  "openshift-cluster-samples-operator",
  "openshift-cluster-storage-operator",
  "openshift-cluster-version",
  "openshift-config",
  "openshift-config-managed",
  "openshift-config-operator",
  "openshift-console",
  "openshift-console-operator",
  "openshift-console-user-settings",
  "openshift-controller-manager",
  "openshift-controller-manager-operator",
  "openshift-dns",
  "openshift-dns-operator",
  "openshift-etcd",
  "openshift-etcd-operator",
  "openshift-host-network",
  "openshift-image-registry",
  "openshift-infra",
  "openshift-ingress",
```

```

    "openshift-ingress-canary",
    "openshift-ingress-operator",
    "openshift-insights",
    "openshift-kni-infra",
    "openshift-kube-apiserver",
    "openshift-kube-apiserver-operator",
    "openshift-kube-controller-manager",
    "openshift-kube-controller-manager-operator",
    "openshift-kube-scheduler",
    "openshift-kube-scheduler-operator",
    "openshift-kube-storage-version-migrator",
    "openshift-kube-storage-version-migrator-operator",
    "openshift-machine-api",
    "openshift-machine-config-operator",
    "openshift-marketplace",
    "openshift-monitoring",
    "openshift-multus",
    "openshift-network-diagnostics",
    "openshift-network-operator",
    "openshift-node",
    "openshift-oauth-apiserver",
    "openshift-openstack-infra",
    "openshift-operator-lifecycle-manager",
    "openshift-operators",
    "openshift-ovirt-infra",
    "openshift-sdn",
    "openshift-service-ca",
    "openshift-service-ca-operator",
    "openshift-user-workload-monitoring",
    "openshift-vsphere-infra",
    "pcloud",
    "postgresql",
    "trident"
  ],
  "defaultStorageClass": "4bacbb3c-0727-4f58-b13c-3a2a069baf89",
  "cloudID": "4f1e1086-f415-4451-a051-c7299cd672ff",
  "credentialID": "7ffd7354-b6c2-4efa-8e7b-cf64d5598463",
  "isMultizonal": "false",
  "tridentManagedStateAllowed": [
    "unmanaged"
  ],
  "tridentVersion": "22.10.0",
  "apiServiceID": "98df44dc-2baf-40d5-8826-e198b1b40909",
  "metadata": {
    "labels": [
      {

```

```

        "name": "astra.netapp.io/labels/read-
only/cloudName",
        "value": "private"
      }
    ],
    "creationTimestamp": "2022-11-03T15:50:59Z",
    "modificationTimestamp": "2022-11-04T14:42:32Z",
    "createdBy": "00000000-0000-0000-0000-000000000000"
  }
}
]
}

```

Add a cluster using credentials

You can add a cluster so it will be available to be managed by Astra. Beginning with the Astra 22.11 release, you can add a cluster with both Astra Control Center and Astra Control Service.



Adding a cluster is not required when using a Kubernetes service from one of the major cloud providers (AKS, EKS, GKE).

1. Obtain the kubeconfig file

You need to obtain a copy of the **kubeconfig** file from your Kubernetes administrator or service.

2. Prepare the kubeconfig file

Before using the **kubeconfig** file, you should perform the following operations:

Convert file from YAML format to JSON

If you receive the kubeconfig file formatted as YAML, you need to convert it to JSON.

Encode JSON in base64

You must encode the JSON file in base64. For example:

```
yq -o=json ~/.kube/config | base64
```

3. Select the cloud

Perform the workflow [List the clouds](#) and select the cloud where the cluster will be added.



The only cloud you can select is the **private** cloud.

4. Create a credential

Perform the following REST API call to create a credential using the kubeconfig file.

HTTP method	Path
POST	/accounts/{account_id}/core/v1/credentials

JSON input example

```
{
  "type" : "application/astra-credential",
  "version" : "1.1",
  "name" : "Cloud One",
  "keyType" : "kubeconfig",
  "keyStore" : {
    "base64": encoded_kubeconfig
  },
  "valid" : "true"
}
```

Curl example

```
curl --location -i --request POST
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/core/v1/credentials'
--header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>' --data
@JSONinput
```

5. Add the cluster

Perform the following REST API call to add the cluster to the cloud. The value of the `credentialID` input field is obtained from the REST API call in the previous step.

HTTP method	Path
POST	/accounts/{account_id}/topology/v1/clouds/{cloud_id}/clusters

JSON input example

```
{
  "type" : "application/astra-cluster",
  "version" : "1.1",
  "credentialID": credential_id
}
```

Curl example

```
curl --location -i --request POST
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/topology/v1/clouds/<CLOUD_ID>/clusters' --header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>' --data @JSONinput
```

List managed clusters

You can list the Kubernetes clusters currently managed by Astra.

1. List the managed clusters

Perform the following REST API call.

HTTP method	Path
GET	/accounts/{account_id}/topology/v1/managedClusters

Curl example: Return all data for all clusters

```
curl --location -i --request GET
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/topology/v1/managedClusters' --header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'
```

Manage a cluster

You can manage a Kubernetes cluster so that data protection can be performed.

1. Select the cluster to manage

Perform the workflow [List clusters](#) and select the desired cluster. The property `managedState` of the cluster must be `unmanaged`.

2. Optionally select the storage class

Optionally perform the workflow [List storage classes](#) and select the desired storage class.



If you don't provide a storage class on the call to manage the cluster, your default storage class will be used.

3. Manage the cluster

Perform the following REST API call to manage the cluster.

HTTP method	Path
POST	/accounts/{account_id}/topology/v1/managedClusters

JSON input example

```
{  
  "type": "application/astra-managedCluster",  
  "version": "1.0",  
  "id": "d0fdf455-4330-476d-bb5d-4d109714e07d"  
}
```

Curl example

```
curl --location -i --request POST  
'https://astra.netapp.io/accounts/<ACCOUNT_ID>/topology/v1/managedClusters'  
' --header 'Accept: */*' --header 'Authorization: Bearer <API_TOKEN>'  
--data @JSONinput
```

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.