



Set up Microsoft Azure

Astra

Ben Cammett
June 11, 2021

Table of Contents

- Set up Microsoft Azure 1
 - Quick start for setting up Azure 1
 - AKS cluster requirements 1
 - Register for Azure NetApp Files 4
 - Create a NetApp account 4
 - Set up a capacity pool 4
 - Delegate a subnet to Azure NetApp Files 5
 - Create an Azure service principal 5

Set up Microsoft Azure

A few steps are required to prepare your Microsoft Azure subscription before you can manage Azure Kubernetes Service clusters with Astra Control Service.

Quick start for setting up Azure

Get started quickly by following these steps or scroll down to the remaining sections for full details.



Review Astra Control Service requirements for Azure Kubernetes Service

Ensure that clusters are healthy and running Kubernetes version 1.17 or later, that node pools are online and running **Linux**, and more. [Learn more about this step.](#)



Register for Azure NetApp Files

Request access to the Azure NetApp Files service and then register the NetApp Resource Provider. [Learn more about this step.](#)



Create a NetApp account

In the Azure portal, go to Azure NetApp Files and create a NetApp account. [Learn more about this step.](#)



Set up capacity pools

Set up one or more capacity pools for your persistent volumes. [Learn more about this step.](#)



Delegate a subnet to Azure NetApp Files

Delegate a subnet to Azure NetApp Files so that Astra Control Service can create persistent volumes in that subnet. [Learn more about this step.](#)



Create an Azure service principal

Create an Azure service principal that has the Contributor role. [Read step-by-step instructions.](#)

AKS cluster requirements

A Kubernetes cluster must meet the following requirements so you can discover and manage it from Astra Control Service.

Kubernetes version

Clusters must be running Kubernetes version 1.17 or later.

Image type

The image type for all node pools must be Linux.

Cluster state

Clusters must be running in a healthy state and have at least one online worker node with no worker nodes in a failed state.

Azure region

Clusters must reside in a region where Azure NetApp Files is available. [View Azure products by region.](#)

Subscription

Clusters must reside in a subscription where Azure NetApp Files is enabled. You'll choose a subscription when you [register for Azure NetApp Files](#).

VNet

- Clusters must reside in a VNet that has direct access to an Azure NetApp Files delegated subnet. [Learn how to set up a delegated subnet.](#)
- If your Kubernetes clusters are in a VNet that's peered to the Azure NetApp Files delegated subnet that's in another VNet, then both sides of the peering connection must be online.
- Be aware that the default limit for the number of IPs used in a VNet (including immediately peered VNets) with Azure NetApp Files is 1,000. [View Azure NetApp Files resource limits.](#)

If you're close to the limit, you have two options:

- You can [submit a request for a limit increase](#). Contact your NetApp representative if you need help.
- When creating a new AKS cluster, specify a new network for the cluster. Once the new network is created, provision a new subnet and delegate the subnet to Azure NetApp Files.

Private networking

Private networking must not be enabled on a cluster.

External volume snapshot controller

Clusters must have a CSI volume snapshot controller installed. This controller is installed by default starting with K8s version 1.21, but you'll need to check on clusters running versions 1.17, 1.18, 1.19, or 1.20. [Learn more about an external snapshot controller for on-demand volume snapshots.](#)

Install a CSI volume snapshot controller

As noted in the list of requirements, Kubernetes clusters must have a CSI volume snapshot controller installed. Follow these steps to install the controller on your clusters.

Steps for K8s versions 1.17, 1.18, and 1.19

1. Install volume snapshot CRDs.

```
kubectl apply -f https://raw.githubusercontent.com/kubernetes-csi/external-snapshotter/release-3.0/client/config/crd/snapshot.storage.k8s.io_volumesnapshotclasses.yaml
kubectl apply -f https://raw.githubusercontent.com/kubernetes-csi/external-snapshotter/release-3.0/client/config/crd/snapshot.storage.k8s.io_volumesnapshotcontents.yaml
kubectl apply -f https://raw.githubusercontent.com/kubernetes-csi/external-snapshotter/release-3.0/client/config/crd/snapshot.storage.k8s.io_volumesnapshots.yaml
```

2. Create the snapshot controller.

If you want the snapshot controller in a specific namespace, download and edit the following files before you apply them.

```
kubectl apply -f https://raw.githubusercontent.com/kubernetes-csi/external-snapshotter/release-3.0/deploy/kubernetes/snapshot-controller/rbac-snapshot-controller.yaml
kubectl apply -f https://raw.githubusercontent.com/kubernetes-csi/external-snapshotter/release-3.0/deploy/kubernetes/snapshot-controller/setup-snapshot-controller.yaml
```

Steps for K8s version 1.20

1. Install volume snapshot CRDs.

```
kubectl apply -f https://raw.githubusercontent.com/kubernetes-csi/external-snapshotter/v4.0.0/client/config/crd/snapshot.storage.k8s.io_volumesnapshotclasses.yaml
kubectl apply -f https://raw.githubusercontent.com/kubernetes-csi/external-snapshotter/v4.0.0/client/config/crd/snapshot.storage.k8s.io_volumesnapshotcontents.yaml
kubectl apply -f https://raw.githubusercontent.com/kubernetes-csi/external-snapshotter/v4.0.0/client/config/crd/snapshot.storage.k8s.io_volumesnapshots.yaml
```

2. Create the snapshot controller.

If you want the snapshot controller in a specific namespace, download and edit the following files before you apply them.

```
kubectl apply -f https://raw.githubusercontent.com/kubernetes-csi/external-snapshotter/v4.0.0/deploy/kubernetes/snapshot-controller/rbac-snapshot-controller.yaml
kubectl apply -f https://raw.githubusercontent.com/kubernetes-csi/external-snapshotter/v4.0.0/deploy/kubernetes/snapshot-controller/setup-snapshot-controller.yaml
```

Register for Azure NetApp Files

Get access to Azure NetApp Files by submitting a waitlist request. After you're approved, you'll need to register the NetApp Resource Provider.

Steps

1. [Submit a waitlist request to access Azure NetApp Files.](#)
2. Wait for a confirmation email from the Azure NetApp Files team.
3. [Follow Azure NetApp Files documentation to register the NetApp Resource Provider.](#)

Create a NetApp account

After you've been granted access, create a NetApp account in Azure NetApp Files.

Step

1. [Follow Azure NetApp Files documentation to create a NetApp account from the Azure portal.](#)

Set up a capacity pool

One or more capacity pools are required so that Astra Control Service can provision persistent volumes in a capacity pool. Astra Control Service doesn't create capacity pools for you.

Take the following into consideration as you set up capacity pools for your Kubernetes apps:

- A capacity pool can have an Ultra, Premium, or Standard service level. Each of these service levels are designed for different performance needs. Astra Control Service supports all three.

You need to set up a capacity pool for each service level that you want to use with your Kubernetes clusters.

[Learn more about service levels for Azure NetApp Files.](#)

- Before you create a capacity pool for the apps that you intend to protect with Astra Control Service, choose the required performance and capacity for those apps.

Provisioning the right amount of capacity ensures that users can create persistent volumes as they are needed. If capacity isn't available, then the persistent volumes can't be provisioned.

- An Azure NetApp Files capacity pool can use the manual or auto QoS type. Astra Control Service supports auto QoS capacity pools. Manual QoS capacity pools aren't supported.

Step

1. [Follow Azure NetApp Files documentation to set up an auto QoS capacity pool.](#)

Delegate a subnet to Azure NetApp Files

You need to delegate a subnet to Azure NetApp Files so that Astra Control Service can create persistent volumes in that subnet. Note that Azure NetApp Files enables you to have only one delegated subnet in a VNet.

If you're using peered VNets, then both sides of the peering connection must be online: the VNet where your Kubernetes clusters reside and the VNet that has the Azure NetApp Files delegated subnet.

Step

1. [Follow the Azure NetApp Files documentation to delegate a subnet to Azure NetApp Files.](#)

After you're done

Wait about 10 minutes before discovering the compute running in the delegated subnet.

Create an Azure service principal

Astra Control Service requires a Azure service principal that is assigned the Contributor role. Astra Control Service uses this service principal to facilitate Kubernetes application data management on your behalf.

A service principal is an identity created specifically for use with applications, services, and tools. Assigning a role to the service principal restricts access to specific Azure resources.

Follow the steps below to create a service principal using the Azure CLI. You'll need to save the output in a JSON file and provide it to Astra Control Service later on. [Refer to Azure documentation for more details about using the CLI.](#)

The following steps assume that you have permission to create a service principal and that you have the Microsoft Azure SDK (az command) installed on your machine.

Requirements

- The service principal must use regular authentication. Certificates aren't supported.
- The service principal must be granted Contributor or Owner access to your Azure subscription.
- The Azure subscription must contain the AKS clusters and your Azure NetApp Files account.

Steps

1. Identify the subscription and tenant ID where your AKS clusters reside (these are the clusters that you want to manage in Astra Control Service).

```
az configure --list-defaults
az account list --output table
```

2. Create the service principal, assign the Contributor role, and specify the scope to the entire subscription where the clusters reside.

```
az ad sp create-for-rbac --name http://sp-astra-service-principal --role contributor --scopes /subscriptions/SUBSCRIPTION-ID
```

3. Store the resulting Azure CLI output as a JSON file.

You'll need to provide this file so that Astra Control Service can discover your AKS clusters and manage Kubernetes data management operations. [Learn about managing credentials in Astra Control Service.](#)

4. Optional: Add the subscription ID to the JSON file so that Astra Control Service automatically populates the ID when you select the file.

Otherwise, you'll need to enter the subscription ID in Astra Control Service when prompted.

Example

```
{
  "appId": "0db3929a-bfb0-4c93-baee-aaf8",
  "displayName": "sp-example-dev-sandbox",
  "name": "http://sp-example-dev-sandbox",
  "password": "mypassword",
  "tenant": "011cdf6c-7512-4805-aaf8-7721afd8ca37",
  "subscriptionId": "99ce999a-8c99-99d9-a9d9-99cce99f99ad"
}
```

5. Optional: Test your service principal.

```
az login --service-principal --username APP-ID-SERVICEPRINCIPAL
--password PASSWORD --tenant TENANT-ID
az group list --subscription SUBSCRIPTION-ID
az aks list --subscription SUBSCRIPTION-ID
az storage container list --subscription SUBSCRIPTION-ID
```


Copyright Information

Copyright © 2021 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.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

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.