



# **Amazon FSx for NetApp ONTAP**

## **Astra Trident**

NetApp  
March 17, 2023

# Table of Contents

- Amazon FSx for NetApp ONTAP ..... 1
  - Use Astra Trident with Amazon FSx for NetApp ONTAP ..... 1
  - Integrate Amazon FSx for NetApp ONTAP ..... 2
  - FSx for ONTAP configuration options and examples ..... 5

# Amazon FSx for NetApp ONTAP

## Use Astra Trident with Amazon FSx for NetApp ONTAP

[Amazon FSx for NetApp ONTAP](#) is a fully managed AWS service that enables customers to launch and run file systems powered by the NetApp ONTAP storage operating system. FSx for ONTAP enables you to leverage NetApp features, performance, and administrative capabilities you are familiar with, while taking advantage of the simplicity, agility, security, and scalability of storing data on AWS. FSx for ONTAP supports ONTAP file system features and administration APIs.

A file system is the primary resource in Amazon FSx, analogous to an ONTAP cluster on premises. Within each SVM you can create one or multiple volumes, which are data containers that store the files and folders in your file system. With Amazon FSx for NetApp ONTAP, Data ONTAP will be provided as a managed file system in the cloud. The new file system type is called **NetApp ONTAP**.

Using Astra Trident with Amazon FSx for NetApp ONTAP, you can ensure Kubernetes clusters running in Amazon Elastic Kubernetes Service (EKS) can provision block and file persistent volumes backed by ONTAP.

Amazon FSx for NetApp ONTAP uses [FabricPool](#) to manage storage tiers. It enables you to store data in a tier, based on whether the data is frequently accessed.

### Considerations

- SMB volumes:
  - SMB volumes are supported using the `ontap-nas` driver only.
  - Astra Trident supports SMB volumes mounted to pods running on Windows nodes only.
  - Astra Trident does not support Windows ARM architecture.
- Volumes created on Amazon FSx file systems that have automatic backups enabled cannot be deleted by Trident. To delete PVCs, you need to manually delete the PV and the FSx for ONTAP volume. To prevent this issue:
  - Do not use **Quick create** to create the FSx for ONTAP file system. The quick create workflow enables automatic backups and does not provide an opt-out option.
  - When using **Standard create**, disable automatic backup. Disabling automatic backups allows Trident to successfully delete a volume without further manual intervention.

▼ **Backup and maintenance - *optional***

---

Daily automatic backup [Info](#)

Amazon FSx can protect your data through daily backups

☐ Enabled

☒ Disabled

## Drivers

You can integrate Astra Trident with Amazon FSx for NetApp ONTAP using the following drivers:

- `ontap-san`: Each PV provisioned is a LUN within its own Amazon FSx for NetApp ONTAP volume.
- `ontap-san-economy`: Each PV provisioned is a LUN with a configurable number of LUNs per Amazon FSx for NetApp ONTAP volume.
- `ontap-nas`: Each PV provisioned is a full Amazon FSx for NetApp ONTAP volume.
- `ontap-nas-economy`: Each PV provisioned is a qtree, with a configurable number of qtrees per Amazon FSx for NetApp ONTAP volume.
- `ontap-nas-flexgroup`: Each PV provisioned is a full Amazon FSx for NetApp ONTAP FlexGroup volume.

For driver details, see [ONTAP drivers](#).

## Authentication

Astra Trident offers two modes of authentication.

- **Certificate-based**: Astra Trident will communicate with the SVM on your FSx file system using a certificate installed on your SVM.
- **Credential-based**: You can use the `fsxadmin` user for your file system or the `vsadmin` user configured for your SVM.



Astra Trident expects to be run as a `vsadmin` SVM user or as a user with a different name that has the same role. Amazon FSx for NetApp ONTAP has an `fsxadmin` user that is a limited replacement of the ONTAP `admin` cluster user. We strongly recommend using `vsadmin` with Astra Trident.

You can update backends to move between credential-based and certificate-based methods. However, if you attempt to provide **credentials and certificates**, backend creation will fail. To switch to a different authentication method, you must remove the existing method from the backend configuration.

For details on enabling authentication, refer to the authentication for your driver type:

- [ONTAP NAS authentication](#)
- [ONTAP SAN authentication](#)

## Find more information

- [Amazon FSx for NetApp ONTAP documentation](#)
- [Blog post on Amazon FSx for NetApp ONTAP](#)

## Integrate Amazon FSx for NetApp ONTAP

You can integrate your Amazon FSx for NetApp ONTAP file system with Astra Trident to ensure Kubernetes clusters running in Amazon Elastic Kubernetes Service (EKS) can provision block and file persistent volumes backed by ONTAP.

## Before you begin

In addition to [Astra Trident requirements](#), to integrate FSx for ONTAP with Astra Trident, you need:

- An existing Amazon EKS cluster or self-managed Kubernetes cluster with `kubectl` installed.
- An existing Amazon FSx for NetApp ONTAP file system and storage virtual machine (SVM) that is reachable from your cluster's worker nodes.
- Worker nodes that are prepared for [NFS or iSCSI](#).



Ensure you follow the node preparation steps required for Amazon Linux and Ubuntu [Amazon Machine Images](#) (AMIs) depending on your EKS AMI type.

## Additional requirements for SMB volumes

- A Kubernetes cluster with a Linux controller node and at least one Windows worker node running Windows Server 2019. Astra Trident supports SMB volumes mounted to pods running on Windows nodes only.
- At least one Astra Trident secret containing your Active Directory credentials. To generate secret `smbcreds`:

```
kubectl create secret generic smbcreds --from-literal username=user
--from-literal password='pw'
```

- A CSI proxy configured as a Windows service. To configure a `csi-proxy`, refer to [GitHub: CSI Proxy](#) or [GitHub: CSI Proxy for Windows](#) for Kubernetes nodes running on Windows.

## ONTAP SAN and NAS driver integration



If you are configuring for SMB volumes, you must read [Prepare to provision SMB volumes](#) before creating the backend.

### Steps

1. Deploy Astra Trident using one of the [deployment methods](#).
2. Collect your SVM management LIF DNS name. For example, using the AWS CLI, find the `DNSName` entry under `Endpoints` → `Management` after running the following command:

```
aws fsx describe-storage-virtual-machines --region <file system region>
```

3. Create and install certificates for [NAS backend authentication](#) or [SAN backend authentication](#).



You can log in to your file system (for example to install certificates) using SSH from anywhere that can reach your file system. Use the `fsxadmin` user, the password you configured when you created your file system, and the management DNS name from `aws fsx describe-file-systems`.

4. Create a backend file using your certificates and the DNS name of your management LIF, as shown in the sample below:

```
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "backendName": "customBackendName",
  "managementLIF": "svm-XXXXXXXXXXXXXXXXXXXX.fs-XXXXXXXXXXXXXXXXXXXX.fsx.us-east-2.aws.internal",
  "svm": "svm01",
  "clientCertificate": "ZXR0ZXJwYXB...ICMgJ3BhcGVyc2",
  "clientPrivateKey": "vciwKIyAgZG...0cnksIGRlc2NyaX",
  "trustedCACertificate": "zcyBbaG...b3Igb3duIGNsYXNz",
}
```

For information about creating backends, see these links:

- [Configure a backend with ONTAP NAS drivers](#)
- [Configure a backend with ONTAP SAN drivers](#)

## Results

After deployment, you can create a [storage class](#), [provision a volume](#), and [mount the volume in a pod](#).

## Prepare to provision SMB volumes

You can provision SMB volumes using the `ontap-nas` driver. Before you complete [ONTAP SAN and NAS driver integration](#) complete the following steps.

### Steps

1. Create SMB shares. You can create the SMB admin shares in one of two ways either using the [Microsoft Management Console](#) Shared Folders snap-in or using the ONTAP CLI. To create the SMB shares using the ONTAP CLI:
  - a. If necessary, create the directory path structure for the share.

The `vserver cifs share create` command checks the path specified in the `-path` option during share creation. If the specified path does not exist, the command fails.

- b. Create an SMB share associated with the specified SVM:

```
vserver cifs share create -vserver vserver_name -share-name
share_name -path path [-share-properties share_properties,...]
[other_attributes] [-comment text]
```

- c. Verify that the share was created:

```
vserver cifs share show -share-name share_name
```



Refer to [Create an SMB share](#) for full details.

2. When creating the backend, you must configure the following to specify SMB volumes. For all FSx for ONTAP backend configuration options, refer to [FSx for ONTAP configuration options and examples](#).

| Parameter       | Description  | Example                       |
|-----------------|--|-------------------------------|
| smbShare        | Name of the SMB share created using Shared Folder Microsoft Management Console. For example "smb-share".<br><br><b>Required for SMB volumes.</b> | smb-share                     |
| nasType         | <b>Must set to smb.</b> If null, defaults to nfs.  | smb                           |
| securityStyle   | Security style for new volumes.<br><br><b>Must be set to ntfs or mixed for SMB volumes.</b>  | ntfs or mixed for SMB volumes |
| unixPermissions | Mode for new volumes. <b>Must be left empty for SMB volumes.</b>   | ""                            |

## FSx for ONTAP configuration options and examples

Learn about backend configuration options for Amazon FSx for ONTAP. This section provides backend configuration examples.

### Backend configuration options

See the following table for the backend configuration options:

| Parameter         | Description                        | Example   |
|-------------------|------------------------------------|---|
| version           |                                    | Always 1  |
| storageDriverName | Name of the storage driver         | "ontap-nas", "ontap-nas-economy", "ontap-nas-flexgroup", "ontap-san", "ontap-san-economy" |
| backendName       | Custom name or the storage backend | Driver name + "_" + dataLIF   |

| Parameter     | Description   | Example                              |
|---------------|---|--------------------------------------|
| managementLIF | <p>IP address of a cluster or SVM management LIF</p> <p>For seamless MetroCluster switchover, you must specify an SVM management LIF.</p> <p>A fully-qualified domain name (FQDN) can be specified.</p> <p>Can be set to use IPv6 addresses if Astra Trident was installed using the <code>--use-ipv6</code> flag. IPv6 addresses must be defined in square brackets, such as [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555].</p>  | "10.0.0.1", "[2001:1234:abcd::fefe]" |
| dataLIF       | <p>IP address of protocol LIF.</p> <p><b>ONTAP NAS drivers:</b> We recommend specifying dataLIF. If not provided, Astra Trident fetches data LIFs from the SVM. You can specify a fully-qualified domain name (FQDN) to be used for the NFS mount operations, allowing you to create a round-robin DNS to load-balance across multiple data LIFs. Can be changed after initial setting. Refer to <a href="#">Update dataLIF after initial configuration</a>.</p> <p><b>ONTAP SAN drivers:</b> Do not specify for iSCSI. Astra Trident uses ONTAP Selective LUN Map to discover the iSCSI LIFs needed to establish a multi path session. A warning is generated if dataLIF is explicitly defined.</p> <p>Can be set to use IPv6 addresses if Astra Trident was installed using the <code>--use-ipv6</code> flag. IPv6 addresses must be defined in square brackets, such as [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555].</p> |                                      |



| Parameter            | Description  | Example                                       |
|----------------------|--|---|
| autoExportPolicy     | <p>Enable automatic export policy creation and updating [Boolean].</p> <p>Using the autoExportPolicy and autoExportCIDRs options, Astra Trident can manage export policies automatically.</p>                        | "false"                                       |
| autoExportCIDRs      | <p>List of CIDRs to filter Kubernetes' node IPs against when autoExportPolicy is enabled.</p> <p>Using the autoExportPolicy and autoExportCIDRs options, Astra Trident can manage export policies automatically.</p> | "["0.0.0.0/0", "::/0"]"                       |
| labels               | Set of arbitrary JSON-formatted labels to apply on volumes   | ""  |
| clientCertificate    | Base64-encoded value of client certificate. Used for certificate-based auth  | ""  |
| clientPrivateKey     | Base64-encoded value of client private key. Used for certificate-based auth  | ""  |
| trustedCACertificate | Base64-encoded value of trusted CA certificate. Optional. Used for certificate-based authentication.   | ""  |
| username             | Username to connect to the cluster or SVM. Used for credential-based authentication. For example, vsadmin.   |   |
| password             | Password to connect to the cluster or SVM. Used for credential-based authentication.   |   |
| svm                  | Storage virtual machine to use   | Derived if an SVM managementLIF is specified. |
| igroupName           | Name of the igroup for SAN volumes to use. Refer to <a href="#">Details about igroupName</a> .   | "trident-<backend-UUID>"                      |
| storagePrefix        | <p>Prefix used when provisioning new volumes in the SVM.</p> <p>Cannot be modified after creation. To update this parameter, you will need to create a new backend.</p>  | "trident"                                     |

| Parameter           | Description  | Example                      |
|---------------------|--|------------------------------|
| limitAggregateUsage | <p><b>Do not specify for Amazon FSx for NetApp ONTAP.</b></p> <p>The provided <code>fsxadmin</code> and <code>vsadmin</code> do not contain the permissions required to retrieve aggregate usage and limit it using Astra Trident.</p>   | Do not use.                  |
| limitVolumeSize     | <p>Fail provisioning if requested volume size is above this value.</p> <p>Also restricts the maximum size of the volumes it manages for qtrees and LUNs, and the <code>qtreesPerFlexvol</code> option allows customizing the maximum number of qtrees per FlexVol.</p>   | "" (not enforced by default) |
| lunsPerFlexvol      | <p>Maximum LUNs per Flexvol, must be in range [50, 200].</p> <p>SAN only.</p>  | "100"                        |
| debugTraceFlags     | <p>Debug flags to use when troubleshooting. Example, <code>{"api":false, "method":true}</code></p> <p>Do not use <code>debugTraceFlags</code> unless you are troubleshooting and require a detailed log dump.</p>  | null                         |
| nfsMountOptions     | <p>Comma-separated list of NFS mount options.</p> <p>The mount options for Kubernetes-persistent volumes are normally specified in storage classes, but if no mount options are specified in a storage class, Astra Trident will fall back to using the mount options specified in the storage backend's configuration file.</p> <p>If no mount options are specified in the storage class or the configuration file, Astra Trident will not set any mount options on an associated persistent volume.</p> | ""                           |

| Parameter        | Description  | Example     |
|------------------|--|-------------|
| nasType          | <p>Configure NFS or SMB volumes creation.</p> <p>Options are <code>nfs</code>, <code>smb</code>, or <code>null</code>.</p> <p><b>Must set to <code>smb</code> for SMB volumes.</b> Setting to <code>null</code> defaults to NFS volumes.</p>   | "nfs"       |
| qtreesPerFlexvol | Maximum Qtrees per FlexVol, must be in range [50, 300]   | "200"       |
| smbShare         | <p>Name of the SMB share created using Shared Folder Microsoft Management Console.</p> <p><b>Required for SMB volumes.</b></p>   | "smb-share" |
| useREST          | <p>Boolean parameter to use ONTAP REST APIs. <b>Tech preview</b></p> <p><code>useREST</code> is provided as a <b>tech preview</b> that is recommended for test environments and not for production workloads. When set to <code>true</code>, Astra Trident will use ONTAP REST APIs to communicate with the backend.</p> <p>This feature requires ONTAP 9.11.1 and later. In addition, the ONTAP login role used must have access to the <code>ontap</code> application. This is satisfied by the pre-defined <code>vsadmin</code> and <code>cluster-admin</code> roles.</p> | "false"     |

### Details about `igroupName`

`igroupName` can be set to an `igroup` that is already created on the ONTAP cluster. If unspecified, Astra Trident automatically creates an `igroup` named `trident-<backend-UUID>`.

If providing a pre-defined `igroupName`, we recommend using one `igroup` per Kubernetes cluster, if the SVM is to be shared between environments. This is necessary for Astra Trident to automatically maintain IQN additions and deletions.

- `igroupName` can be updated to point to a new `igroup` that is created and managed on the SVM outside of Astra Trident.
- `igroupName` can be omitted. In this case, Astra Trident will create and manage an `igroup` named `trident-<backend-UUID>` automatically.

In both cases, volume attachments will continue to be accessible. Future volume attachments will use the

updated igroup. This update does not disrupt access to volumes present on the backend.

### Update dataLIF after initial configuration

You can change the data LIF after initial configuration by running the following command to provide the new backend JSON file with updated data LIF.

```
tridentctl update backend <backend-name> -f <path-to-backend-json-file-with-updated-dataLIF>
```



If PVCs are attached to one or multiple pods, you must bring down all corresponding pods and then bring them back up in order for the new data LIF to take effect.

### Backend configuration options for provisioning volumes

You can control default provisioning using these options in the `defaults` section of the configuration. For an example, see the configuration examples below.

| Parameter                      | Description  | Default             |
|--------------------------------|--|---------------------|
| <code>spaceAllocation</code>   | Space-allocation for LUNs  | <code>"true"</code> |
| <code>spaceReserve</code>      | Space reservation mode; <code>"none"</code> (thin) or <code>"volume"</code> (thick)  | <code>"none"</code> |
| <code>snapshotPolicy</code>    | Snapshot policy to use   | <code>"none"</code> |
| <code>qosPolicy</code>         | <p>QoS policy group to assign for volumes created. Choose one of <code>qosPolicy</code> or <code>adaptiveQosPolicy</code> per storage pool or backend.</p> <p>Using QoS policy groups with Astra Trident requires ONTAP 9.8 or later.</p> <p>We recommend using a non-shared QoS policy group and ensuring the policy group is applied to each constituent individually. A shared QoS policy group will enforce the ceiling for the total throughput of all workloads.</p> | <code>""</code>     |
| <code>adaptiveQosPolicy</code> | <p>Adaptive QoS policy group to assign for volumes created. Choose one of <code>qosPolicy</code> or <code>adaptiveQosPolicy</code> per storage pool or backend.</p> <p>Not supported by <code>ontap-nas-economy</code>.</p>  | <code>""</code>     |

| Parameter       | Description  | Default   |
|-----------------|--|---|
| snapshotReserve | Percentage of volume reserved for snapshots "0"  | If snapshotPolicy is "none", else ""  |
| splitOnClone    | Split a clone from its parent upon creation  | "false"   |
| encryption      | <p>Enable NetApp Volume Encryption (NVE) on the new volume; defaults to <code>false</code>. NVE must be licensed and enabled on the cluster to use this option.</p> <p>If NAE is enabled on the backend, any volume provisioned in Astra Trident will be NAE enabled.</p> <p>For more information, refer to: <a href="#">How Astra Trident works with NVE and NAE</a>.</p> | "false"   |
| luksEncryption  | <p>Enable LUKS encryption. Refer to <a href="#">Use Linux Unified Key Setup (LUKS)</a>.</p> <p>SAN only.</p>   | ""  |
| tieringPolicy   | Tiering policy to use "none"   | "snapshot-only" for pre-ONTAP 9.5 SVM-DR configuration                            |
| unixPermissions | <p>Mode for new volumes.</p> <p><b>Leave empty for SMB volumes.</b></p>  | ""  |
| securityStyle   | <p>Security style for new volumes.</p> <p>NFS supports <code>mixed</code> and <code>unix</code> security styles.</p> <p>SMB supports <code>mixed</code> and <code>ntfs</code> security styles.</p>   | <p>NFS default is <code>unix</code>.</p> <p>SMB default is <code>ntfs</code>.</p> |

## Example

Using `nasType`, `node-stage-secret-name`, and `node-stage-secret-namespace`, you can specify an SMB volume and provide the required Active Directory credentials. SMB volumes are supported using the `ontap-nas` driver only.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: nas-smb-sc
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
  trident.netapp.io/nasType: "smb"
  csi.storage.k8s.io/node-stage-secret-name: "smbcreds"
  csi.storage.k8s.io/node-stage-secret-namespace: "default"
```

## Copyright information

Copyright © 2023 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.