# Amazon FSx for NetApp ONTAP

Astra Trident

NetApp
May 08, 2024

# Table of Contents

# 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.

### Overview

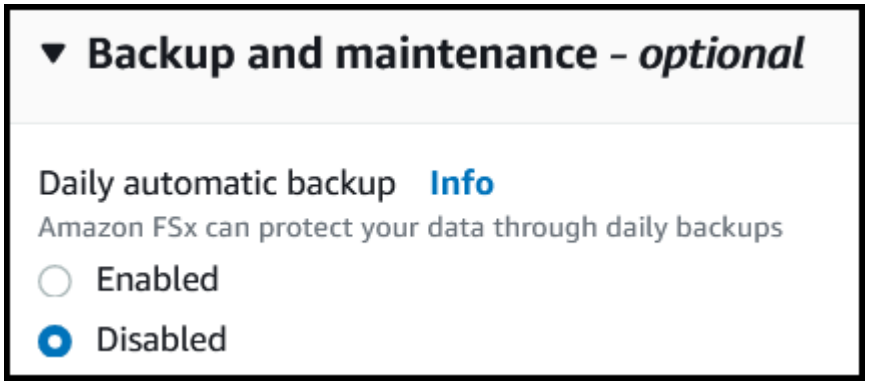
A file system is the primary resource in Amazon FSx, analogous to an ONTAP cluster on premises. Within each SVM you can create one or multiple volumes, which are data containers that store the files and folders in your file system. With Amazon FSx for NetApp ONTAP, Data ONTAP will be provided as a managed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



### FSx for ONTAP driver details

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 NAS drivers and SAN 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.

## Requirements

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.

- Astra Trident supports SMB volumes mounted to pods running on Windows nodes only. Refer to Prepare to provision SMB volumes for details.

## 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:

**YAML**

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

**JSON**

```
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "backendName": "customBackendName",
  "managementLIF": "svm-XXXXXXXXXXXXXXXXX.fs-
XXXXXXXXXXXXXXXXX.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

## 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.

#### Before you begin

Before you can provision SMB volumes using the `ontap-nas` driver, you must have the following.

- 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='password'
```

- 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.

**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` | You can specify one of the following: the name of an SMB share created using the Microsoft Management Console or ONTAP CLI or a name to allow Astra Trident to create the SMB share.<br><br>This parameter is required for Amazon FSx for ONTAP backends. | `smb-share` |
| `nasType` | **Must set to `smb`.** If null, defaults to `nfs`. | `smb` |

| Parameter | Description | Example |
| --- | --- | --- |
| `securityStyle` | Security style for new volumes.<br><br>**Must be set to `ntfs` or `mixed` for SMB volumes.** | `ntfs` or `mixed` for SMB volumes |
| `unixPermissions` | Mode for new volumes. **Must be left empty for SMB volumes.** | "" |

# 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 |
| `managementLIF` | IP address of a cluster or SVM management LIF<br><br>A fully-qualified domain name (FQDN) can be specified.<br><br>Can be set to use IPv6 addresses if Astra Trident was installed using the IPv6 flag. IPv6 addresses must be defined in square brackets, such as [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]. | "10.0.0.1", "[2001:1234:abcd::fefe]" |

| Parameter | Description | Example |
| --- | --- | --- |
| `dataLIF` | IP address of protocol LIF.<br><br>**ONTAP NAS drivers**: 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 Update `dataLIF` after initial configuration.<br><br>**ONTAP SAN drivers**: Do not specify for iSCSI. Astra Trident uses ONTAP Selective LUN Map to discover the iSCI LIFs needed to establish a multi path session. A warning is generated if dataLIF is explicitly defined.<br><br>Can be set to use IPv6 addresses if Astra Trident was installed using the IPv6 flag. IPv6 addresses must be defined in square brackets, such as [28e8:d9fb:a825:b7bf:69a8:d02f:9e7b:3555]. | |
| `autoExportPolicy` | Enable automatic export policy creation and updating [Boolean].<br><br>Using the `autoExportPolicy` and `autoExportCIDRs` options, Astra Trident can manage export policies automatically. | `false` |
| `autoExportCIDRs` | List of CIDRs to filter Kubernetes' node IPs against when `autoExportPolicy` is enabled.<br><br>Using the `autoExportPolicy` and `autoExportCIDRs` options, Astra Trident can manage export policies automatically. | "[“0.0.0.0/0”, “::/0”]" |
| `labels` | Set of arbitrary JSON-formatted labels to apply on volumes | "" |

| Parameter | Description | Example |
| --- | --- | --- |
| `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. |
| `storagePrefix` | Prefix used when provisioning new volumes in the SVM.<br><br>Cannot be modified after creation. To update this parameter, you will need to create a new backend. | `trident` |
| `limitAggregateUsage` | **Do not specify for Amazon FSx for NetApp ONTAP.**<br><br>The provided `fsxadmin` and `vsadmin` do not contain the permissions required to retrieve aggregate usage and limit it using Astra Trident. | Do not use. |
| `limitVolumeSize` | Fail provisioning if requested volume size is above this value.<br><br>Also restricts the maximum size of the volumes it manages for qtrees and LUNs, and the `qtreesPerFlexvol` option allows customizing the maximum number of qtrees per FlexVol. | “” (not enforced by default) |
| `lunsPerFlexvol` | Maximum LUNs per Flexvol, must be in range [50, 200].<br><br>SAN only. | `100` |

| Parameter | Description | Example |
| --- | --- | --- |
| `debugTraceFlags` | Debug flags to use when troubleshooting. Example, {“api”:false, “method”:true}<br><br>Do not use `debugTraceFlags` unless you are troubleshooting and require a detailed log dump. | null |
| `nfsMountOptions` | Comma-separated list of NFS mount options.<br><br>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.<br><br>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. | "" |
| `nasType` | Configure NFS or SMB volumes creation.<br><br>Options are `nfs`, `smb`, or null.<br><br>**Must set to `smb` for SMB volumes.** Setting to null defaults to NFS volumes. | `nfs` |
| `qtreesPerFlexvol` | Maximum Qtrees per FlexVol, must be in range [50, 300] | `200` |
| `smbShare` | You can specify one of the following: the name of an SMB share created using the Microsoft Management Console or ONTAP CLI or a name to allow Astra Trident to create the SMB share.<br><br>This parameter is required for Amazon FSx for ONTAP backends. | `smb-share` |

| Parameter | Description | Example |
| --- | --- | --- |
| `useREST` | Boolean parameter to use ONTAP REST APIs. **Tech preview**<br><br>`useREST` is provided as a **tech preview** that is recommended for test environments and not for production workloads. When set to `true`, Astra Trident will use ONTAP REST APIs to communicate with the backend.<br><br>This feature requires ONTAP 9.11.1 and later. In addition, the ONTAP login role used must have access to the `ontap` application. This is satisfied by the pre-defined `vsadmin` and `cluster-admin` roles. | `false` |

**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 to 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 |
| --- | --- | --- |
| `spaceAllocation` | Space-allocation for LUNs | `true` |
| `spaceReserve` | Space reservation mode; “none” (thin) or “volume” (thick) | `none` |
| `snapshotPolicy` | Snapshot policy to use | `none` |

| Parameter | Description | Default |
| --- | --- | --- |
| `qosPolicy` | QoS policy group to assign for volumes created. Choose one of qosPolicy or adaptiveQosPolicy per storage pool or backend.<br><br>Using QoS policy groups with Astra Trident requires ONTAP 9.8 or later.<br><br>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. | “” |
| `adaptiveQosPolicy` | Adaptive QoS policy group to assign for volumes created. Choose one of qosPolicy or adaptiveQosPolicy per storage pool or backend.<br><br>Not supported by ontap-nas-economy. | “” |
| `snapshotReserve` | Percentage of volume reserved for snapshots “0” | If `snapshotPolicy` is `none`, `else` “” |
| `splitOnClone` | Split a clone from its parent upon creation | `false` |
| `encryption` | Enable NetApp Volume Encryption (NVE) on the new volume; defaults to `false`. NVE must be licensed and enabled on the cluster to use this option.<br><br>If NAE is enabled on the backend, any volume provisioned in Astra Trident will be NAE enabled.<br><br>For more information, refer to: How Astra Trident works with NVE and NAE. | `false` |
| `luksEncryption` | Enable LUKS encryption. Refer to Use Linux Unified Key Setup (LUKS).<br><br>SAN only. | "" |
| `tieringPolicy` | Tiering policy to use `none` | `snapshot-only` for pre-ONTAP 9.5 SVM-DR configuration |

| Parameter | Description | Default |
| --- | --- | --- |
| `unixPermissions` | Mode for new volumes.<br><br>**Leave empty for SMB volumes.** | “” |
| `securityStyle` | Security style for new volumes.<br><br>NFS supports `mixed` and `unix` security styles.<br><br>SMB supports `mixed` and `ntfs` security styles. | NFS default is `unix`.<br><br>SMB default is `ntfs`. |

### 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"
```

## Configure the Astra Trident EKS add-on version 23.10 on EKS cluster

Astra Trident streamlines Amazon FSx for NetApp ONTAP storage management in Kubernetes to enable your developers and administrators focus on application deployment. The Astra Trident EKS add-on includes the latest security patches, bug fixes, and is validated by AWS to work with Amazon EKS. The EKS add-on enables you to consistently ensure that your Amazon EKS clusters are secure and stable and reduce the amount of work that you need to do in order to install, configure, and update add-ons.

### Prerequisites

Ensure that you have the following before configuring the Astra Trident add-on for AWS EKS:

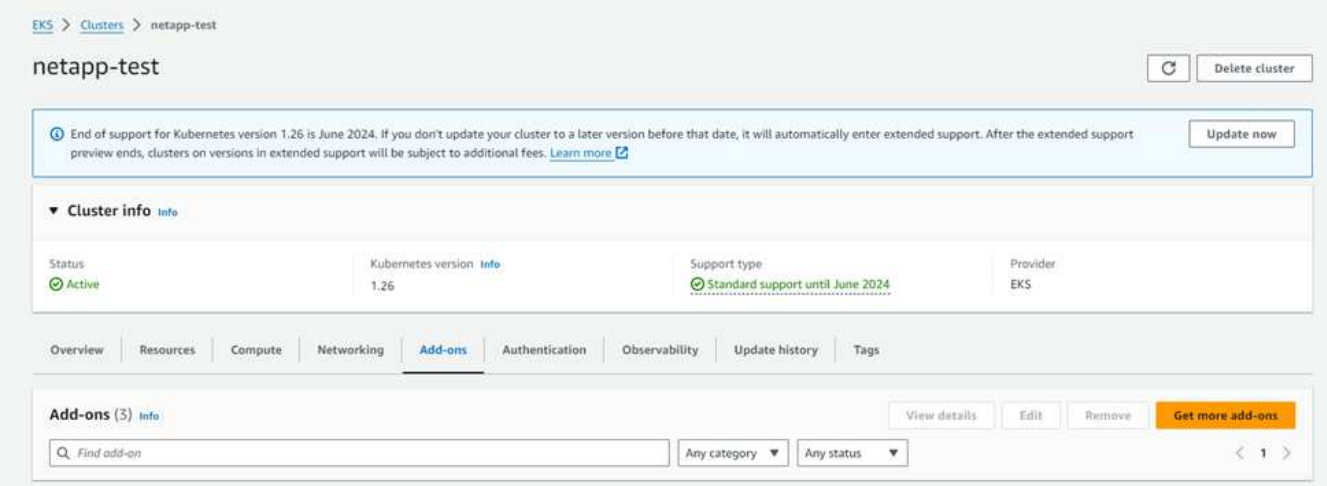
- An Amazon EKS cluster account with add-on subscription
- AWS permissions to the AWS marketplace:

```
"aws-marketplace:ViewSubscriptions",
"aws-marketplace:Subscribe",
"aws-marketplace:Unsubscribe
```

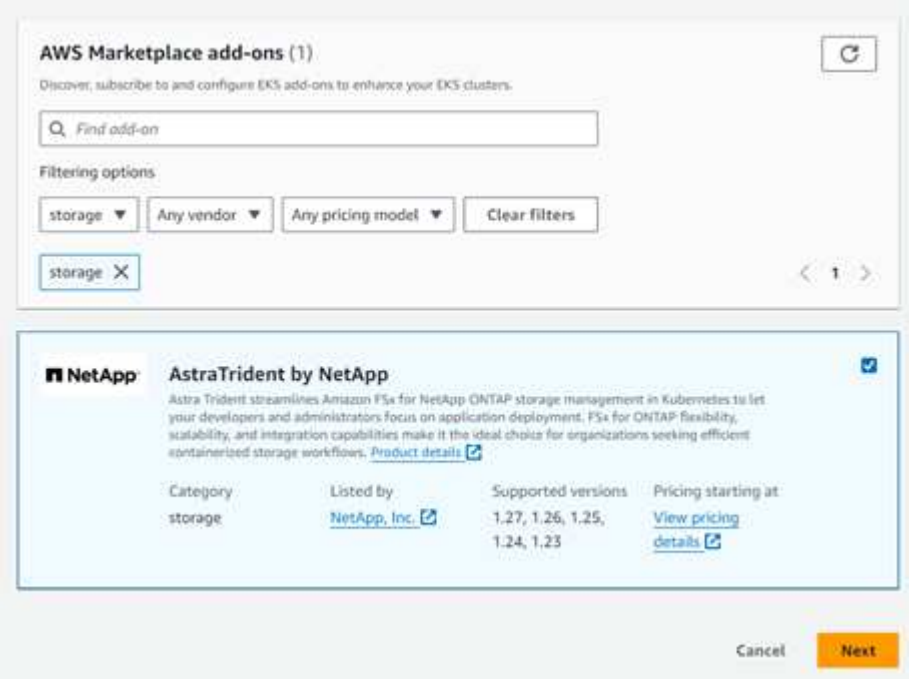
- AMI type: Amazon Linux 2 (AL2_x86_64) or Amazon Linux 2 Arm(AL2_ARM_64)
- Node type: AMD or ARM
- An existing Amazon FSx for NetApp ONTAP file system

## Steps

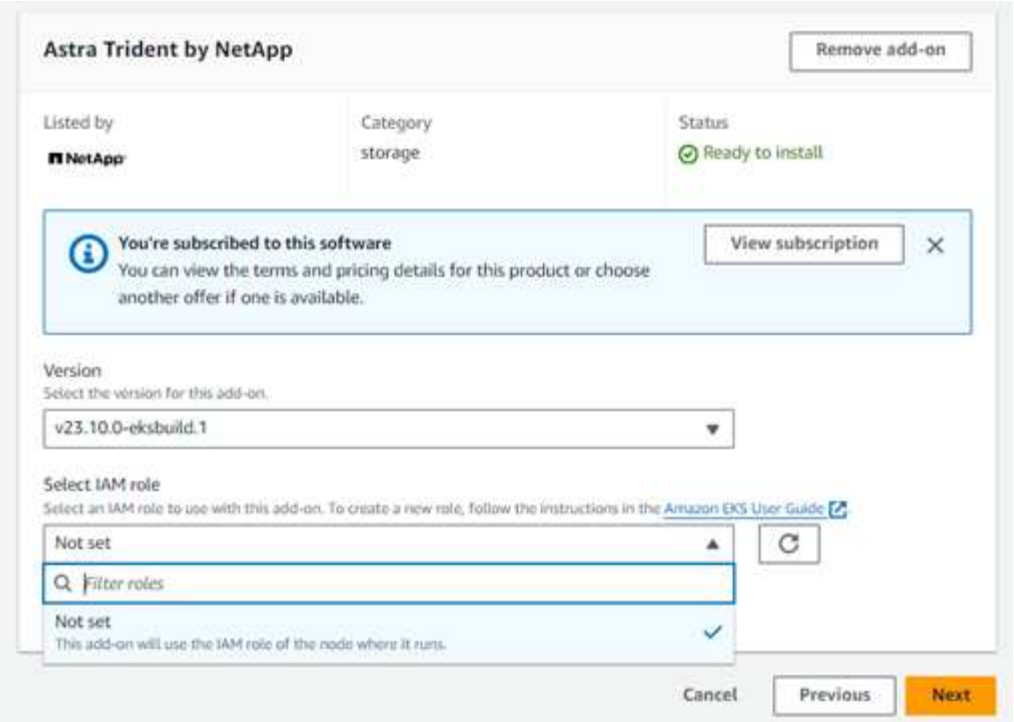
1. On your your EKS Kubernetes cluster, navigate to the **Add-ons** tab.



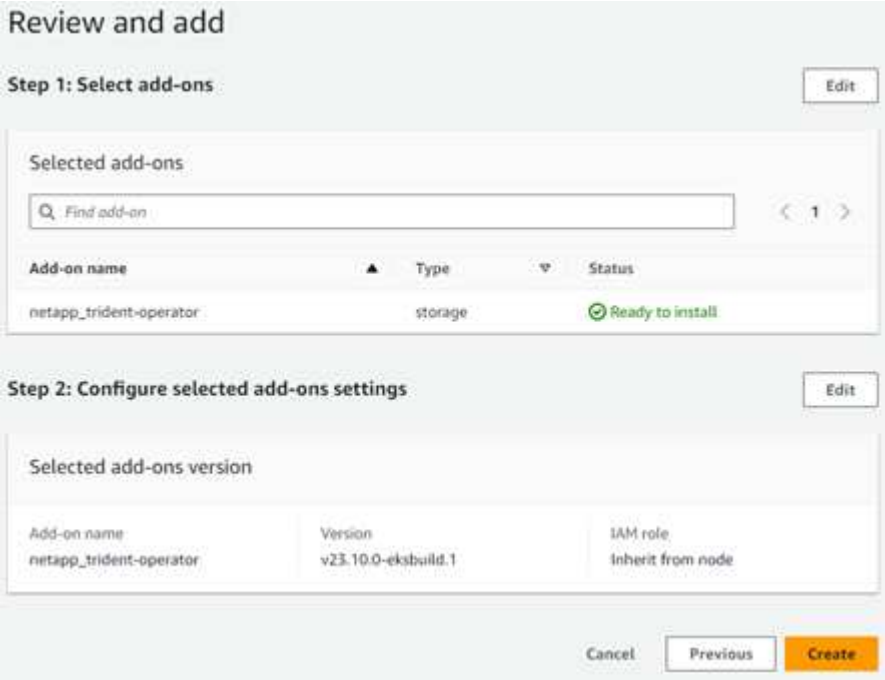

2. Go to **AWS Marketplace add-ons** and choose the *storage* category.




3. Locate **AstraTrident by NetApp** and select the checkbox for the Astra Trident add-on.
4. Choose the desired version of the add-on.




5. Select the IAM role option to inherit from the node.
6. Configure any optional settings as required and select **Next**.




7. Select **Create**.
8. Verify that the status of the add-on is *Active*.


## Install/uninstall the Astra Trident EKS add-on using CLI

**Install the Astra Trident EKS add-on using CLI:**

The following example commands install the Astra Trident EKS add-on:
`eksctl create addon --cluster K8s-arm --name netapp_trident-operator --version v23.10.0-eksbuild.`
`eksctl create addon --cluster K8s-arm --name netapp_trident-operator --version v23.10.0-eksbuild.1` (with a dedicated version)

**Uninstall the Astra Trident EKS add-on using CLI:**

The following command uninstalls the Astra Trident EKS add-on:
`eksctl delete addon --cluster K8s-arm --name netapp_trident-operator`