



Überblick über NetApp Storage-Integrationen

NetApp Solutions

NetApp
April 26, 2024

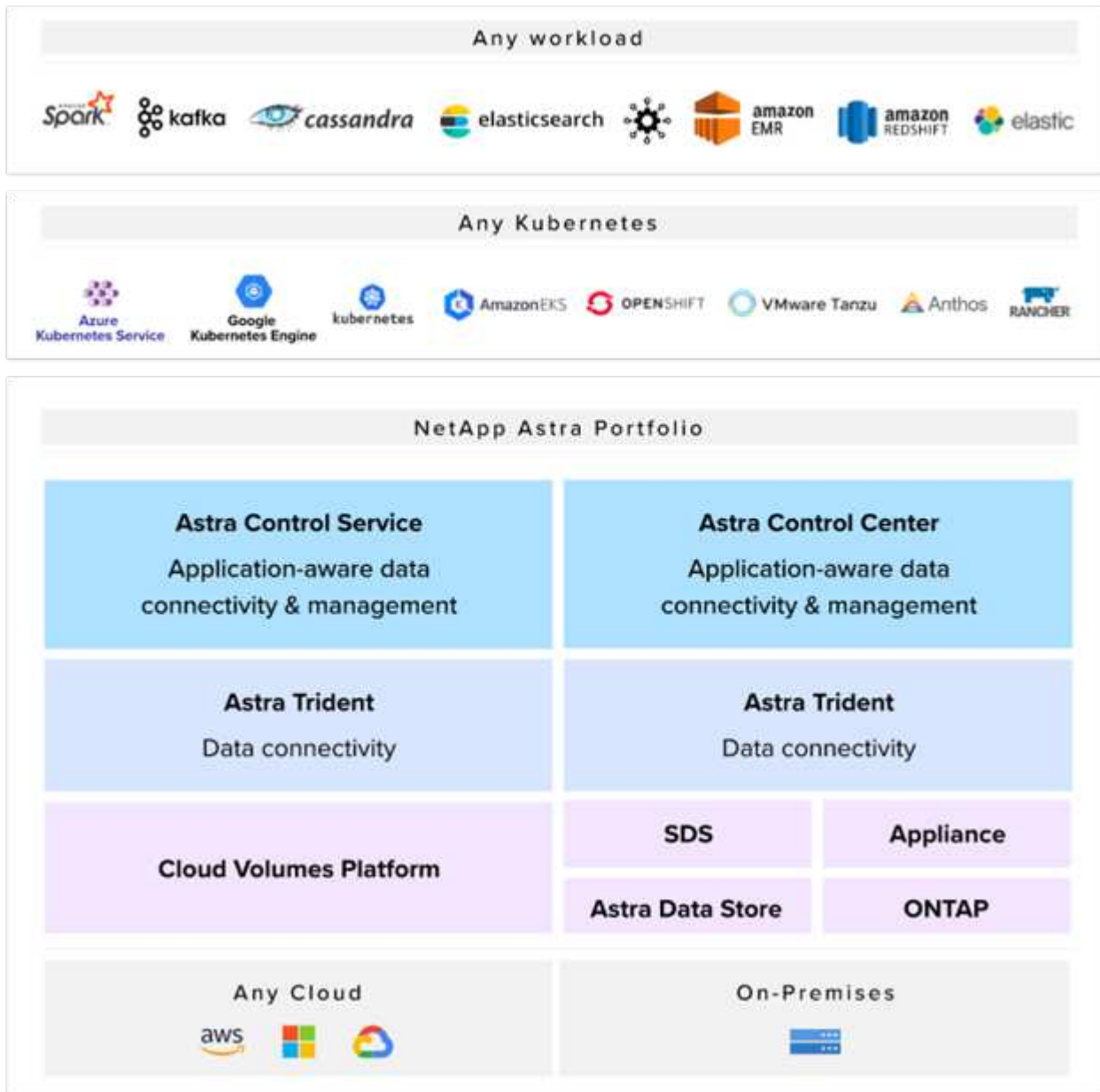
This PDF was generated from https://docs.netapp.com/de-de/netapp-solutions/containers/vtwn_astra_register.html on April 26, 2024. Always check docs.netapp.com for the latest.

Inhalt

- Überblick über die Integration von NetApp Storage..... 1
 - Übersicht über NetApp Astra Control..... 2
 - Astra Trident – Überblick 20

Überblick über die Integration von NetApp Storage

NetApp bietet verschiedene Produkte, die Sie dabei unterstützen, zustandsorientierte Container-Applikationen und ihre Daten zu orchestrieren, zu managen, zu sichern und zu migrieren.



NetApp Astra Control bietet eine umfassende Auswahl an Storage- und applikationsspezifischen Datenmanagement-Services für zustandsorientierte Kubernetes Workloads auf Basis der Datensicherungstechnologie von NetApp. Der Astra Control Service unterstützt statusorientierte Workloads in Cloud-nativen Kubernetes-Implementierungen. Das Astra Control Center unterstützt statusorientierte Workloads in On-Premises-Implementierungen von Kubernetes-Enterprise-Plattformen wie Red Hat OpenShift, Rancher, VMware Tanzu etc. Weitere Informationen finden Sie auf der NetApp Astra Control Website "[Hier](#)".

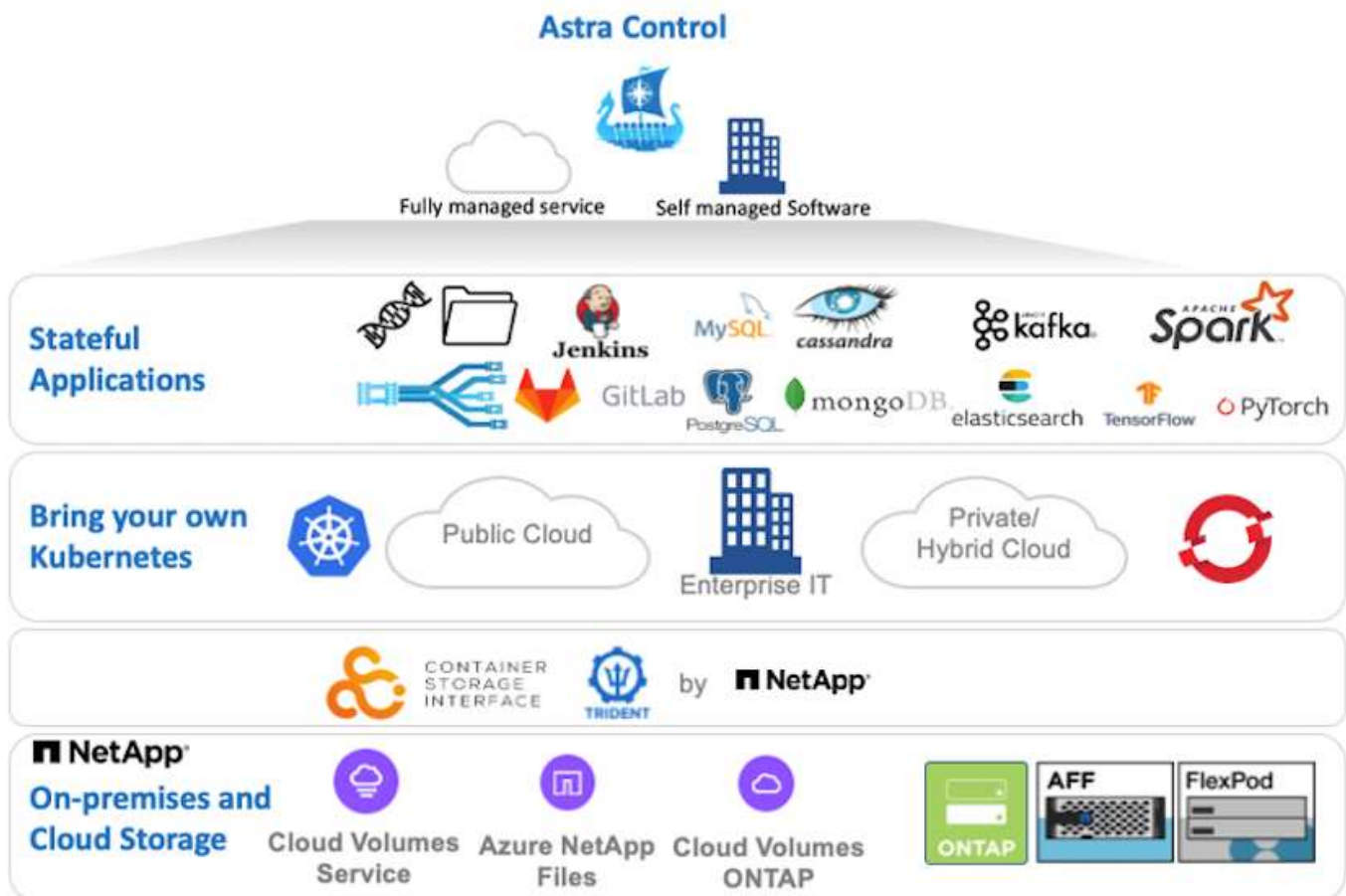
NetApp Astra Trident ist ein Open-Source- und vollständig unterstützter Storage-Orchestrator für Container und Kubernetes-Distributionen wie Red Hat OpenShift, Rancher, VMware Tanzu etc. Weitere Informationen finden Sie auf der Astra Trident Website "[Hier](#)".

Die folgenden Seiten enthalten zusätzliche Informationen zu den NetApp Produkten, die für das Management von Applikationen und persistentem Storage validiert wurden. Sie finden sie in der VMware Tanzu with NetApp Lösung:

- ["NetApp Astra Control Center"](#)
- ["NetApp Astra Trident"](#)

Übersicht über NetApp Astra Control

Das NetApp Astra Control Center bietet umfassende Storage- und applikationsorientierte Datenmanagement-Services für statusorientierte Kubernetes Workloads in einer On-Premises-Umgebung mit NetApp Datensicherungstechnologie.



NetApp Astra Control Center kann auf einem VMware Tanzu Cluster installiert werden. Mit dem Astra Trident Storage-Orchestrator wurde der Server mit Storage-Klassen und Storage-Back-Ends für NetApp ONTAP Storage-Systeme implementiert und konfiguriert.

Weitere Informationen zu Astra Trident finden Sie unter ["Dieses Dokument hier einfügen"](#).

In einer Umgebung mit Cloud-Anbindung sorgt Astra Control Center mithilfe von Cloud Insights für erweitertes Monitoring und Telemetrie. Liegt keine Cloud Insights-Verbindung vor, ist eingeschränktes Monitoring und Telemetrie (sieben Tage mit Kennzahlen) verfügbar und über offene metrische Endpunkte in die nativen Kubernetes-Monitoring-Tools (Prometheus und Grafana) exportiert.

Astra Control Center ist vollständig in das AutoSupport- und Active IQ-Ecosystem von NetApp integriert und bietet damit Support für Benutzer, Hilfestellung bei der Fehlerbehebung und Statistiken zur Anzeige der

Nutzungsstatistik.

Neben der kostenpflichtigen Version des Astra Control Center ist auch eine 90-Tage-Evaluierungslizenz verfügbar. Die Evaluierungsversion wird durch E-Mail und den Slack Community-Kanal unterstützt. Kunden haben Zugriff auf diese Ressourcen, weitere Knowledge-Base-Artikel und Dokumentationen, die über das Produkt-Support-Dashboard verfügbar sind.

Mehr über das Astra Portfolio erfahren Sie auf der ["Astra-Website"](#).

Astra Control Center Automatisierung

Astra Control Center verfügt über eine voll funktionsfähige REST-API für programmatischen Zugriff. Benutzer können jede beliebige Programmiersprache oder ein beliebiges Dienstprogramm verwenden, um mit den ASTRA Control REST-API-Endpunkten zu interagieren. Weitere Informationen zu dieser API finden Sie in der Dokumentation ["Hier"](#).

Wenn Sie nach einem sofort einsatzbereiten Software-Entwicklungskit für die Interaktion mit Astra Control REST-APIs suchen, stellt NetApp ein Toolkit mit dem Astra Control Python SDK bereit, das Sie herunterladen können ["Hier"](#).

Wenn die Programmierung in Ihrer Situation nicht geeignet ist und Sie ein Konfigurationsmanagement-Tool verwenden möchten, können Sie die von NetApp veröffentlichten Ansible-Playbooks klonen und ausführen ["Hier"](#).

Installationsvoraussetzungen für Astra Control Center

Die Installation von Astra Control Center erfordert die folgenden Voraussetzungen:

- Ein oder mehrere Tanzu Kubernetes Cluster, die entweder von einem Management-Cluster oder TKGS oder TKGI gemanagt werden. TKG Workload Cluster 1.4+ und TKGI User Cluster 1.12.2+ werden unterstützt.
- Astra Trident muss bereits auf jedem Tanzu Kubernetes Cluster installiert und konfiguriert sein.
- Mindestens ein NetApp ONTAP Storage-System mit ONTAP 9.5 oder höher



Eine Best Practice für jede Tanzu Kubernetes-Installation an einem Standort ist es, über eine dedizierte SVM für persistenten Storage zu verfügen. Implementierungen an mehreren Standorten erfordern zusätzliche Storage-Systeme.

- Ein Trident Storage-Back-End muss für jeden Tanzu Kubernetes-Cluster mit einer SVM konfiguriert werden, die durch einen ONTAP-Cluster gesichert wird.
- Eine Standard-StorageClass-Konfiguration auf jedem Tanzu Kubernetes Cluster mit Astra Trident als Storage-provisionierung.
- Für jeden Tanzu Kubernetes Cluster muss auf jedem Tanzu Kubernetes ein Load Balancer installiert und konfiguriert werden, um den Lastausgleich zu ermöglichen und Astra Control Center auszusetzen, wenn Sie ingressType verwenden `AccTraefik`.
- Ein Ingress-Controller muss auf jedem Tanzu Kubernetes Cluster installiert und konfiguriert werden, damit Astra Control Center verfügbar ist, wenn Sie ingressType verwenden `Generic`.
- Eine private Image-Registrierung muss konfiguriert sein, um die NetApp Astra Control Center Images zu hosten.
- Sie müssen Zugriff auf den Cluster-Administrator auf das Tanzu Kubernetes Cluster haben, in dem Astra

Control Center installiert wird.

- Sie müssen Administratorzugriff auf NetApp ONTAP Cluster haben.
- Eine RHEL- oder Ubuntu Admin-Workstation.

Installieren Sie Astra Control Center

Diese Lösung beschreibt ein automatisiertes Verfahren für die Installation von Astra Control Center mithilfe von Ansible Playbooks. Wenn Sie nach einem manuellen Verfahren zur Installation des Astra Control Centers suchen, folgen Sie der detaillierten Installations- und Betriebsanleitung ["Hier"](#).

1. Um die Ansible-Playbooks zu verwenden, die Astra Control Center implementieren, benötigen Sie eine Ubuntu/RHEL-Maschine, auf der Ansible installiert ist. Befolgen Sie die Anweisungen ["Hier"](#) Für Ubuntu und RHEL.
2. Klonen Sie das GitHub Repository, das Ansible-Inhalte hostet.

```
git clone https://github.com/NetApp-
Automation/na_astra_control_suite.git
```

3. Melden Sie sich bei der NetApp Support-Website an und laden Sie die neueste Version des NetApp Astra Control Center herunter. Dazu ist eine Lizenz erforderlich, die an Ihr NetApp Konto angehängt ist. Nach dem Download des Tarballs, übertragen Sie es auf die Workstation.



Um mit einer Testlizenz für Astra Control zu beginnen, besuchen Sie die ["Astra: Anmelde-Website"](#).

4. Erstellen oder beziehen Sie die kubeconfig-Datei mit Administratorzugriff auf den Benutzer oder den Workload Tanzu Kubernetes Cluster, auf dem Astra Control Center installiert werden soll.
5. Ändern Sie das Verzeichnis in na_astra_control_suite.

```
cd na_astra_control_suite
```

6. Bearbeiten Sie das vars/vars.yml Datei und füllen Sie die Variablen mit den erforderlichen Informationen aus.

```
#Define whether or not to push the Astra Control Center images to your
private registry [Allowed values: yes, no]
push_images: yes

#The directory hosting the Astra Control Center installer
installer_directory: /home/admin/

#Specify the ingress type. Allowed values - "AccTraefik" or "Generic"
#"AccTraefik" if you want the installer to create a LoadBalancer type
service to access ACC, requires MetalLB or similar.
#"Generic" if you want to create or configure ingress controller
```

```
yourself, installer just creates a ClusterIP service for traefik.
ingress_type: "AccTraefik"

#Name of the Astra Control Center installer (Do not include the
extension, just the name)
astra_tar_ball_name: astra-control-center-22.04.0

#The complete path to the kubeconfig file of the kubernetes/openshift
cluster Astra Control Center needs to be installed to.
hosting_k8s_cluster_kubeconfig_path: /home/admin/cluster-kubeconfig.yml

#Namespace in which Astra Control Center is to be installed
astra_namespace: netapp-astra-cc

#Astra Control Center Resources Scaler. Leave it blank if you want to
accept the Default setting.
astra_resources_scaler: Default

#Storageclass to be used for Astra Control Center PVCs, it must be
created before running the playbook [Leave it blank if you want the PVCs
to use default storageclass]
astra_trident_storageclass: basic

#Reclaim Policy for Astra Control Center Persistent Volumes [Allowed
values: Retain, Delete]
storageclass_reclaim_policy: Retain

#Private Registry Details
astra_registry_name: "docker.io"

#Whether the private registry requires credentials [Allowed values: yes,
no]
require_reg_creds: yes

#If require_reg_creds is yes, then define the container image registry
credentials
#Usually, the registry namespace and usernames are same for individual
users
astra_registry_namespace: "registry-user"
astra_registry_username: "registry-user"
astra_registry_password: "password"

#KubereneTS/OpenShift secret name for Astra Control Center
#This name will be assigned to the K8s secret created by the playbook
astra_registry_secret_name: "astra-registry-credentials"

#Astra Control Center FQDN
```

```
acc_fqdn_address: astra-control-center.cie.netapp.com

#Name of the Astra Control Center instance
acc_account_name: ACC Account Name

#Administrator details for Astra Control Center
admin_email_address: admin@example.com
admin_first_name: Admin
admin_last_name: Admin
```

7. Nutzen Sie das Playbook zur Implementierung des Astra Control Center. Für bestimmte Konfigurationen sind Root-Berechtigungen erforderlich.

Führen Sie den folgenden Befehl aus, um das Playbook auszuführen, wenn der Benutzer, der das Playbook ausführt, root ist oder passwortlose sudo konfiguriert ist.

```
ansible-playbook install_acc_playbook.yml
```

Wenn der Benutzer passwortbasierten sudo-Zugriff konfiguriert hat, führen Sie den folgenden Befehl aus, um das Playbook auszuführen und geben Sie dann das sudo-Passwort ein.

```
ansible-playbook install_acc_playbook.yml -K
```

Schritte Nach Der Installation

1. Die Installation kann einige Minuten dauern. Überprüfen Sie, ob alle Pods und Services im enthalten sind `netapp-astra-cc` Der Namespace ist betriebsbereit.

```
[netapp-user@rhel7 ~]$ kubectl get all -n netapp-astra-cc
```

2. Prüfen Sie die `acc-operator-controller-manager` Protokolle, um sicherzustellen, dass die Installation abgeschlossen ist.

```
[netapp-user@rhel7 ~]$ kubectl logs deploy/acc-operator-controller-  
manager -n netapp-acc-operator -c manager -f
```



Die folgende Meldung zeigt die erfolgreiche Installation des Astra Control Centers an.


```
{"level":"info","ts":1624054318.029971,"logger":"controllers.AstraControlCenter","msg":"Successfully Reconciled AstraControlCenter in [seconds]s","AstraControlCenter":"netapp-astra-cc/astra","ae.Version":"[22.04.0]"}
```

3. Der Benutzername für die Anmeldung beim Astra Control Center ist die E-Mail-Adresse des Administrators in der CRD-Datei und das Passwort ist eine Zeichenfolge ACC- An die Astra Control Center UUID angehängt. Führen Sie den folgenden Befehl aus:

```
[netapp-user@rhel7 ~]$ oc get astracontrolcenters -n netapp-astra-cc
NAME      UUID
astra     345c55a5-bf2e-21f0-84b8-b6f2bce5e95f
```



In diesem Beispiel lautet das Passwort ACC-345c55a5-bf2e-21f0-84b8-b6f2bce5e95f.

4. Holen Sie die Lastausgleichs-IP für den Trafik-Dienst ab, wenn der Typ AccTraefik ist.

```
[netapp-user@rhel7 ~]$ oc get svc -n netapp-astra-cc | egrep
'EXTERNAL|traefik'
```

NAME	EXTERNAL-IP	PORT(S)	TYPE	CLUSTER-IP
traefik	10.61.186.181	80:30343/TCP, 443:30060/TCP	LoadBalancer	172.30.99.142
AGE		16m		

5. Fügen Sie einen Eintrag im DNS-Server hinzu, der auf den in der Astra Control Center CRD-Datei angegebenen FQDN verweist EXTERNAL-IP Des Schleppdienstes.

New Host

Name (uses parent domain name if blank):

astra-control-center

Fully qualified domain name (FQDN):

astra-control-center.cie.netapp.com.

IP address:

10.61.186.181

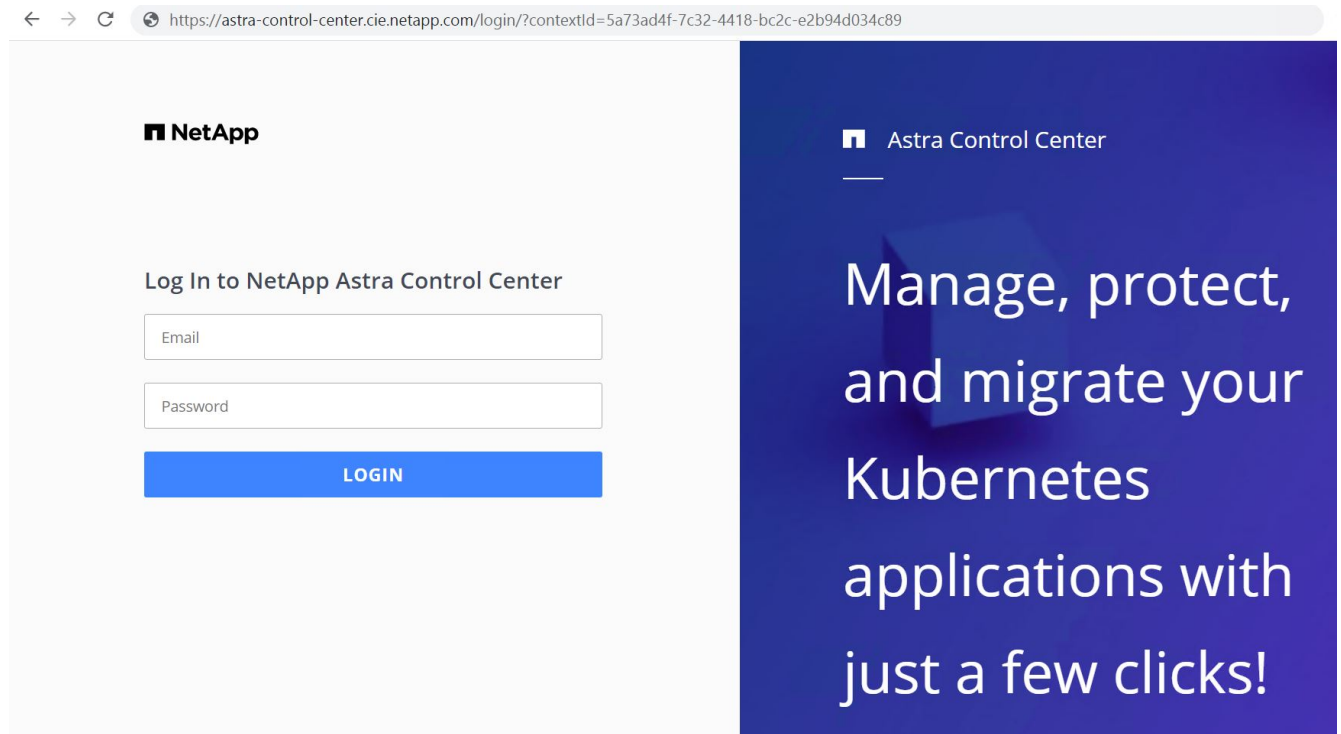
☒ Create associated pointer (PTR) record

☐ Allow any authenticated user to update DNS records with the same owner name

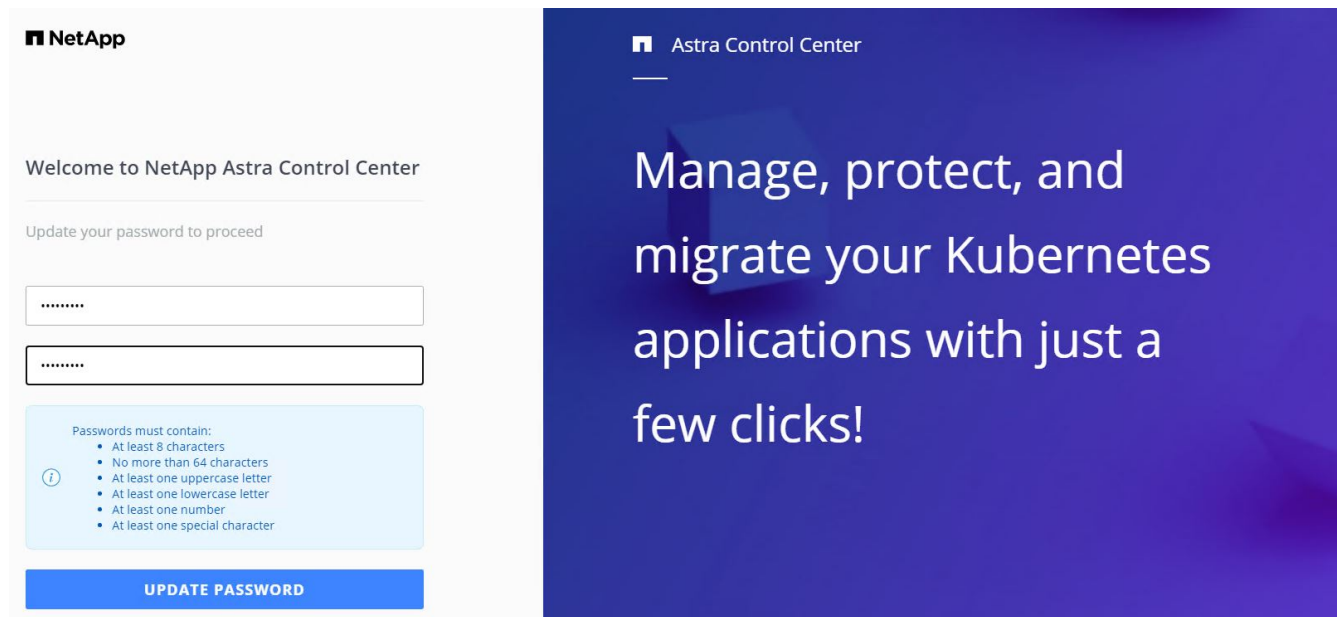
Add Host

Cancel

6. Melden Sie sich bei der Astra Control Center-GUI an, indem Sie den FQDN durchsuchen.



7. Wenn Sie sich zum ersten Mal über die in CRD angegebene Admin-E-Mail-Adresse bei der Benutzeroberfläche des Astra Control Center anmelden, müssen Sie das Passwort ändern.



8. Wenn Sie dem Astra Control Center einen Benutzer hinzufügen möchten, navigieren Sie zu Konto > Benutzer, klicken Sie auf Hinzufügen, geben Sie die Details des Benutzers ein und klicken Sie auf Hinzufügen.

Add user
✕

USER DETAILS

First name

Nikhil

Last name

Kulkarni

Email address

tme_nik@netapp.com

PASSWORD

Temporary password

Confirm temporary password

ⓘ

Passwords must contain:

- At least 8 characters
- No more than 64 characters
- At least one lowercase letter
- At least one uppercase letter
- At least one number
- At least one special character

USER ROLE ⓘ

Role

Owner

Cancel

Add ✓

ADD NEW USER

Add new user

Add a new user to your Astra Control Center account. New users will be prompted to update their password the first time they log in to Astra Control Center. They will also inherit access to account-wide credentials according to their role. Read more in [users](#).

9. Astra Control Center erfordert eine Lizenz für alle Funktionen. Um eine Lizenz hinzuzufügen, navigieren Sie zu Konto > Lizenz, klicken Sie auf Lizenz hinzufügen und laden Sie die Lizenzdatei hoch.

Account

Users

Credentials

Notifications

License

Connections

ASTRA CONTROL CENTER LICENSE

To get started with Astra Control Center, select Add license to manually upload the file.

ADD LICENSE

Select and add a license file.

License file

EvalNLF-AstraControlCenter-480Cores(vCPU)-100000002-ACC60f19...

⬆

✕

Cancel

Add

Bei Problemen mit der Installation oder Konfiguration von NetApp Astra Control Center steht die Wissensdatenbank mit bekannten Problemen zur Verfügung ["Hier"](#).


Registrieren Sie Ihre VMware Tanzu Kubernetes Cluster mit dem Astra Control Center

Damit das Astra Control Center Ihre Workloads managen kann, müssen Sie zuerst Ihre Tanzu Kubernetes-Cluster registrieren.

10

Registrieren Sie VMware Tanzu Kubernetes Cluster

1. Der erste Schritt besteht darin, die Tanzu Kubernetes Cluster zum Astra Control Center hinzuzufügen und zu verwalten. Gehen Sie zu Clusters und klicken Sie auf Cluster hinzufügen, laden Sie die kubeconfig-Datei für den Tanzu Kubernetes-Cluster hoch, und klicken Sie auf Storage auswählen.

 **Add Kubernetes cluster**

STEP 1/3: CREDENTIALS

×

CREDENTIALS

Provide Astra Control access to your Kubernetes and OpenShift clusters by entering a kubeconfig credential.

Follow [instructions](#) on how to create a dedicated admin-role kubeconfig.

[Upload file](#) [Paste from clipboard](#)

Kubeconfig YAML file
tkgi-kubeconfig.txt

↑ ×

Credential name
tkgi-acc

Cancel

Next →


ADDING CLUSTERS

Adding a cluster allows Astra Control to install its storage services, and enable data management operations on your containerized applications.

For more details on required versions or cloud specific setup refer to the documentation.

Read more in [Adding clusters](#).

2. Astra Control Center erkennt geeignete Storage-Klassen. Wählen Sie jetzt aus, wie Storage Volumes mithilfe von Trident durch eine SVM auf NetApp ONTAP bereitgestellt werden, und klicken Sie auf „Review“ (prüfen). Überprüfen Sie im nächsten Teilfenster die Details, und klicken Sie auf Cluster hinzufügen.
3. Wenn der Cluster hinzugefügt wird, wechselt er in den Status Erkennung, während das Astra Control Center den Cluster prüft und die erforderlichen Agenten installiert. Der Cluster-Status ändert sich in **Healthy** Nach der erfolgreichen Registrierung.

 **Clusters**


Actions ▾

+ Add Kubernetes cluster

⌵ Search

1-1 of 1 entries

< >


<input type="checkbox"/>	Name ↓	State	Type	Version	Actions
<input type="checkbox"/>	tkgi-acc	✓ Healthy	 Kubernetes	v1.22.6+vmware.1	<div>⋮</div>



Alle Tanzu Kubernetes Cluster, die von Astra Control Center verwaltet werden sollen, sollten Zugriff auf die Image Registry haben, die für die Installation verwendet wurde, da die auf den verwalteten Clustern installierten Agenten die Bilder aus dieser Registrierung ziehen.

4. Importieren Sie ONTAP-Cluster als Storage-Ressourcen, die vom Astra Control Center als Back-Ends gemanagt werden sollen. Wenn dem Astra Tanzu Kubernetes Cluster hinzugefügt werden und eine Speicheraglass konfiguriert ist, erkennt und inspiziert er den ONTAP Cluster automatisch auf der

Lagerscheinwerfer, importiert ihn aber nicht in das zu verwaltende Astra Control Center.

 **Backends**

+

Add

Search


★

1

1–1 of 1 entries

Name ↓	State	Capacity	Throughput	Type	Cluster	Cloud	Actions
172.21.224.201(trident)	<div><div></div><div>Discovered</div></div>	Not available yet	Not available yet	ONTAP	Not applicable	Not applicable	<div><div></div></div>

5. Um die ONTAP-Cluster zu importieren, navigieren Sie zu Back Ends, klicken Sie auf das Dropdown-Menü und wählen Sie Verwalten neben dem zu verwaltenden ONTAP-Cluster aus. Geben Sie die ONTAP-Cluster-Anmeldeinformationen ein, klicken Sie auf Informationen überprüfen und klicken Sie dann auf Speicher-Backend importieren.

 **Manage ONTAP storage backend**

STEP 1/2: CREDENTIALS

CREDENTIALS

Enter cluster administrator credentials for the ONTAP storage backend you want to manage.

Cluster management IP address

172.21.224.201


User name

admin

Password

Cancel


Next →

 **MANAGING STORAGE BACKENDS**

Storage backends provide storage to your Kubernetes applications.

Managing storage clusters in Astra Control as a storage backend will allow you to get linkages between PVs and the storage backend. You will also see capacity and health details of the storage backend, including performance metrics if Astra Control is connected to Cloud Insights.

Read more in [Storage type](#).

 ONTAP


6. Nach dem Hinzufügen der Back-Ends ändert sich der Status in „verfügbar“. Diese Back-Ends enthalten nun Informationen über die persistenten Volumes im Tanzu Kubernetes Cluster und die entsprechenden Volumes auf dem ONTAP-System.

12

Backends


</

7. Für Backups und Restores in Tanzu Kubernetes Clustern mit Astra Control Center müssen Sie einen Objekt-Storage-Bucket bereitstellen, der das S3-Protokoll unterstützt. Derzeit werden ONTAP S3, StorageGRID, AWS S3 und Microsoft Azure Blob Storage unterstützt. Im Rahmen dieser Installation wird ein AWS S3-Bucket konfiguriert. Wechseln Sie zu Buckets, klicken Sie auf „Bucket hinzufügen“ und wählen Sie „Allgemeines S3“ aus. Geben Sie die Details zum S3-Bucket und die Zugangsdaten ein, um darauf zuzugreifen, klicken Sie auf das Kontrollkästchen „Bucket als Standard-Bucket für die Cloud“ und klicken Sie dann auf „Hinzufügen“.

 **Add bucket**

Enter the access details of your existing object store bucket to allow Astra Control to store your application backups.

Type

 Generic S3

Existing bucket name


na-tanzu-astra/na-astra-tkgi

Description (optional)

S3 server name or IP address

s3.us-east-1.amazonaws.com

☒ Make this bucket the default bucket for this cloud



SELECT CREDENTIALS

Astra Control requires S3 access credentials with the roles necessary to facilitate Kubernetes application data management.


Add

[Use existing](#)

Select credential


AWS Creds

Cancel

Add 

BUCKETS

Astra Control stores backups in your existing object store buckets. The first bucket added for a selected cloud will be designated as the default bucket for backup and clone operations.

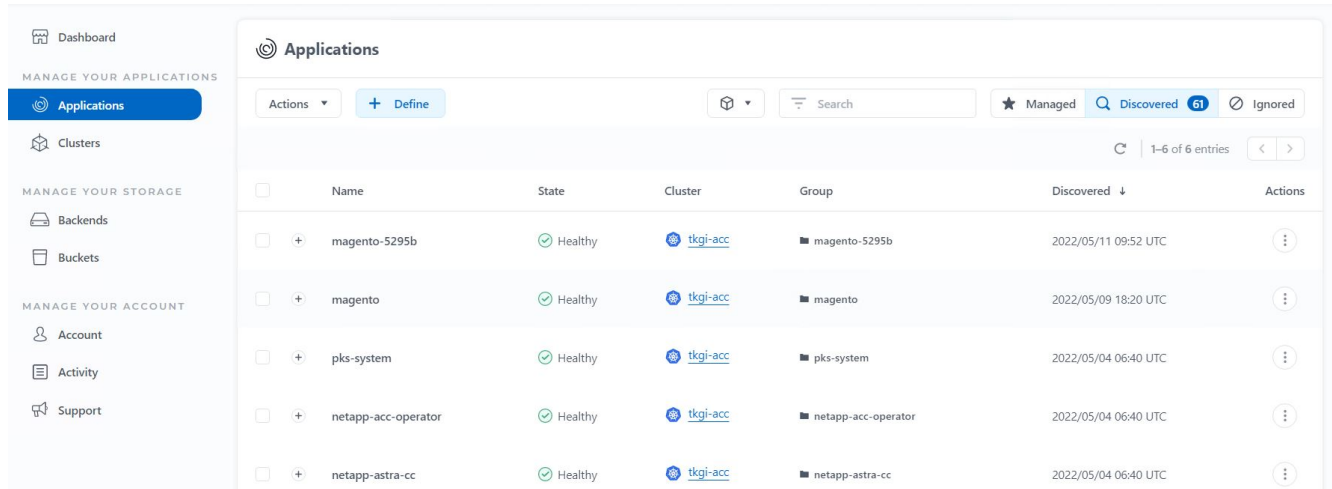
Read more in [Storage buckets](#) .

Wählen Sie die zu schützenden Applikationen aus

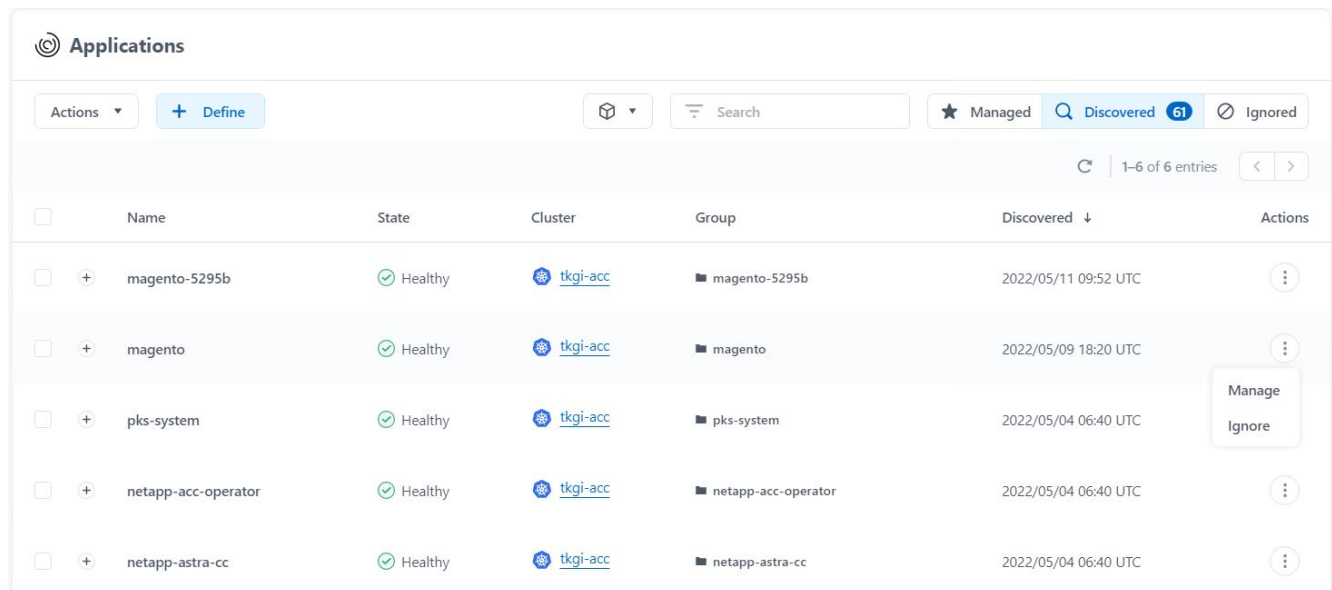
Nachdem Sie Ihre Tanzu Kubernetes Cluster registriert haben, können Sie die Anwendungen ermitteln, die implementiert sind, und sie über das Astra Control Center verwalten.

Management von Applikationen

1. Nachdem die Tanzu Kubernetes-Cluster und ONTAP-Back-Ends beim Astra Control Center registriert wurden, beginnt das Kontrollzentrum automatisch die Anwendungen in allen Namespaces zu erkennen, die die mit dem angegebenen ONTAP-Back-End konfigurierte Speicherageclass verwenden.



2. Navigieren Sie zu Apps > entdeckt, und klicken Sie auf das Dropdown-Menü neben der Anwendung, die Sie mit Astra verwalten möchten. Klicken Sie dann auf Verwalten.



3. Die Anwendung wechselt in den Status „verfügbar“ und kann im Abschnitt „Apps“ unter der Registerkarte „verwaltet“ angezeigt werden.

Applications						
<div> <div>Actions ▾</div> <div>+ Define</div> <div>All clusters ▾</div> <div>Search</div> <div>★ Managed</div> <div>Q Discovered 60</div> <div>Ignored</div> </div>						
<div> <div>1-1 of 1 entries</div> <div>< ></div> </div>						
<input type="checkbox"/>	Name	State	Protection	Cluster	Group	Discovered ↓
<input type="checkbox"/>	magento	Healthy	Unprotected	tkgi-acc	magento	2022/05/09 18:20 UTC

Sichern Sie Ihre Applikationen

Nachdem die Applikations-Workloads vom Astra Control Center gemanagt wurden, können Sie die Sicherungseinstellungen für diese Workloads konfigurieren.

Erstellen Sie einen Anwendungs-Snapshot

Ein Snapshot einer Applikation erstellt eine ONTAP Snapshot Kopie und eine Kopie der Applikationsmetadaten, mit denen Sie die Applikation auf Basis dieser Snapshot Kopie einem bestimmten Zeitpunkt wiederherstellen oder klonen können.

1. Um einen Snapshot der Anwendung zu erstellen, navigieren Sie zur Registerkarte Apps > Managed und klicken Sie auf die Anwendung, von der Sie eine Snapshot Kopie erstellen möchten. Klicken Sie auf das Dropdown-Menü neben dem Anwendungsnamen, und klicken Sie auf Snapshot.

APPLICATION STATUS

Healthy

APPLICATION PROTECTION STATUS

Unprotected

Images

docker.io/bitnami/elasticsearch:6.8.12-debian-10-r61

docker.io/bitnami/magento:2.4.1-debian-10-r14

docker.io/bitnami/mariadb:10.3.24-debian-10-r49

Protection schedule

Disabled

Group

magento

Cluster

tkgi-acc

Actions ▾

Snapshot

Backup

Clone

Restore

Unmanage

2. Geben Sie die Snapshot-Details ein, klicken Sie auf Weiter und klicken Sie dann auf Snapshot. Es dauert etwa eine Minute, um den Snapshot zu erstellen, und der Status wird verfügbar, nachdem der Snapshot erfolgreich erstellt wurde.

Snapshot namespace application

STEP 1/2: DETAILS

✕

SNAPSHOT DETAILS

Name

magento-snapshot-20220516212403

CREATING APPLICATION SNAPSHOTS

Astra Control can take a quick snapshot of your application configuration and persistent storage. Enter a snapshot name to get started.

Read more in [Protect apps](#).

Namespace application
magento

Namespace
magento

Cluster
tkgi-acc

Cancel

Next →

Erstellen eines Applikations-Backups

Ein Backup einer Applikation erfasst den aktiven Status der Applikation und die Konfiguration der Ressourcen des IT-Systems, deckt sie in Dateien ab und speichert sie in einem Remote-Objekt-Storage-Bucket.

- Für die Sicherung und Wiederherstellung von verwalteten Anwendungen im Astra Control Center müssen Sie die Superuser-Einstellungen für die ONTAP-Systeme als Voraussetzung konfigurieren. Geben Sie dazu die folgenden Befehle ein.

```
ONTAP::> export-policy rule modify -vserver ocp-trident -policyname
default -ruleindex 1 -superuser sys
ONTAP::> export-policy rule modify -policyname default -ruleindex 1
-anon 65534 -vserver ocp-trident
```

- Um ein Backup der verwalteten Anwendung im Astra Control Center zu erstellen, navigieren Sie zur Registerkarte Apps > Managed und klicken Sie auf die Anwendung, von der Sie ein Backup durchführen möchten. Klicken Sie auf das Dropdown-Menü neben dem Anwendungsnamen, und klicken Sie auf Backup.

magento

↻

Actions

Snapshot

Backup

Clone

Restore

Unmanage

APPLICATION STATUS

APPLICATION PROTECTION STATUS

Healthy

Unprotected

Images
docker.io/bitnami/elasticsearch:6.8.12-debian-10-r61
docker.io/bitnami/magento:2.4.1-debian-10-r14
docker.io/bitnami/mariadb:10.3.24-debian-10-r49


Protection schedule
Disabled

Group
 magento

Cluster
 tkgi-acc

- Geben Sie die Backup-Details ein, wählen Sie den Objekt-Storage-Bucket aus, der die Backup-Dateien enthält, klicken Sie auf Weiter und klicken Sie nach Überprüfung der Details auf Backup. Abhängig von der

Größe der Applikation und den Daten kann das Backup mehrere Minuten dauern und der Status des Backups wird nach erfolgreichem Abschluss des Backups wieder verfügbar.

 **Back up namespace application**

STEP 1/2: DETAILS

X

BACKUP DETAILS

Name

magento-backup-20220516212622

☐ Back up from an existing snapshot

BACKUP DESTINATION

Bucket

na-tanzu-astra/na-astra-tkgi

Available

Default

CREATING APPLICATION BACKUPS

Astra Control can take a backup of your application configuration and persistent storage. Persistent storage backups are transferred to your object store. Enter a backup name to get started.

Read more in [Application backups](#)

Namespace application

magento

Namespace

magento

Cluster

tkgi-acc


Cancel

Next →

Wiederherstellen einer Anwendung

Auf Knopfdruck können Sie eine Applikation zum Zwecke der Applikationssicherung und Disaster Recovery im selben Cluster oder zu einem Remote-Cluster wiederherstellen, was den Namespace Ursprung im selben Cluster hat.

1. Um eine Anwendung wiederherzustellen, navigieren Sie zur Registerkarte Apps > Managed und klicken Sie auf die betreffende Anwendung. Klicken Sie auf das Dropdown-Menü neben dem Anwendungsnamen, und klicken Sie auf Wiederherstellen.



Actions

APPLICATION STATUS

Healthy

APPLICATION PROTECTION STATUS

Unprotected

Images

docker.io/bitnami/elasticsearch:6.8.12-debian-10-r61

docker.io/bitnami/magento:2.4.1-debian-10-r14

docker.io/bitnami/mariadb:10.3.24-debian-10-r49

Protection schedule

Disabled

Group

magento

Cluster

tkgi-acc

Snapshot

Backup

Clone

Restore

Unmanage

2. Geben Sie den Namen des Restore Namespace ein, wählen Sie den Cluster aus, in dem Sie ihn wiederherstellen möchten, und wählen Sie aus einem vorhandenen Snapshot oder aus einem Backup der Applikation aus, ob Sie ihn wiederherstellen möchten. Klicken Sie Auf Weiter.

Restore namespace application

STEP 1/2: DETAILS

✕

RESTORE DETAILS

Destination cluster

tkgi-acc

Destination namespace

magento

RESTORE SOURCE

Filter

Snapshots

Backups

Application backup	State	On-Schedule/On-Demand	Created ↑
<input type="radio"/> <div>magento-backup-20220516212730</div>	<div>✓</div> <div>Healthy</div>	<div>🕒</div> <div>On-Demand</div>	2022/05/16 21:27 UTC

RESTORING APPLICATIONS

Astra Control can restore your application configuration and persistent storage. Select a source snapshot or backup for the restored application.

🕒 Namespace application

magento

📁 Namespace

magento

🌐 Cluster

tkgi-acc

Cancel

Next →

- Geben Sie im Prüfungsfenster ein `restore` Und klicken Sie auf Wiederherstellen, nachdem Sie die Details geprüft haben.

Restore namespace application

STEP 2/2: SUMMARY

✕

REVIEW RESTORE INFORMATION

⚠️

All existing resources associated with this namespace application will be deleted and replaced with the source backup "magento-backup-20220516212730" taken on 2022/05/16 21:27 UTC. Persistent volumes will be deleted and recreated. External resources with dependencies on this namespace application might be impacted.

We recommend taking a snapshot or a backup of your namespace application before proceeding.

🕒 BACKUP

magento-backup-20220516212730

📁 ORIGINAL GROUP

■ magento

🌐 ORIGINAL CLUSTER

tkgi-acc

🔗 RESOURCE LABELS

Config Maps

app.kubernetes.io/name: elasticsearch +9

Deployments

🕒 RESTORE

magento

📁 DESTINATION GROUP

■ magento

🌐 DESTINATION CLUSTER

tkgi-acc

🔗 RESOURCE LABELS

Config Maps

app.kubernetes.io/name: elasticsearch +9

Deployments

Are you sure you want to restore the namespace application "magento"?

Type restore below to confirm.

Confirm to restore

restore

← Back

Restore ✓

- Die neue Applikation geht in den Status Wiederherstellen, während Astra Control Center die Anwendung auf dem ausgewählten Cluster wiederherstellt. Nachdem alle Ressourcen der Anwendung installiert und von Astra erkannt wurden, geht die Anwendung in den verfügbaren Zustand.

Clone namespace application

STEP 1/2: DETAILS

✕

CLONE DETAILS

Clone namespace
magento-bef7f

Destination cluster
tkgi-acc

☐ Clone from an existing snapshot or backup

Cancel

Next →

CLONING APPLICATIONS

Astra Control can create a clone of your application configuration and persistent storage. Persistent storage backups are transferred from your object store, so choosing a clone from an existing backup will complete the fastest. Enter a clone name to get started.

Not all applications may support cloning.

Read more in [Clone applications](#).

Namespace application
magento

Namespace
magento

Cluster
tkgi-acc

3. Die neue Applikation geht in den Entdeckungszustand, während Astra Control Center die Anwendung im ausgewählten Cluster erstellt. Nachdem alle Ressourcen der Anwendung installiert und von Astra erkannt wurden, geht die Anwendung in den verfügbaren Zustand.

Applications

Actions ▾

+ Define

All clusters ▾

Search

★ Managed

🔍 Discovered 60

🚫 Ignored

1-2 of 2 entries

< >

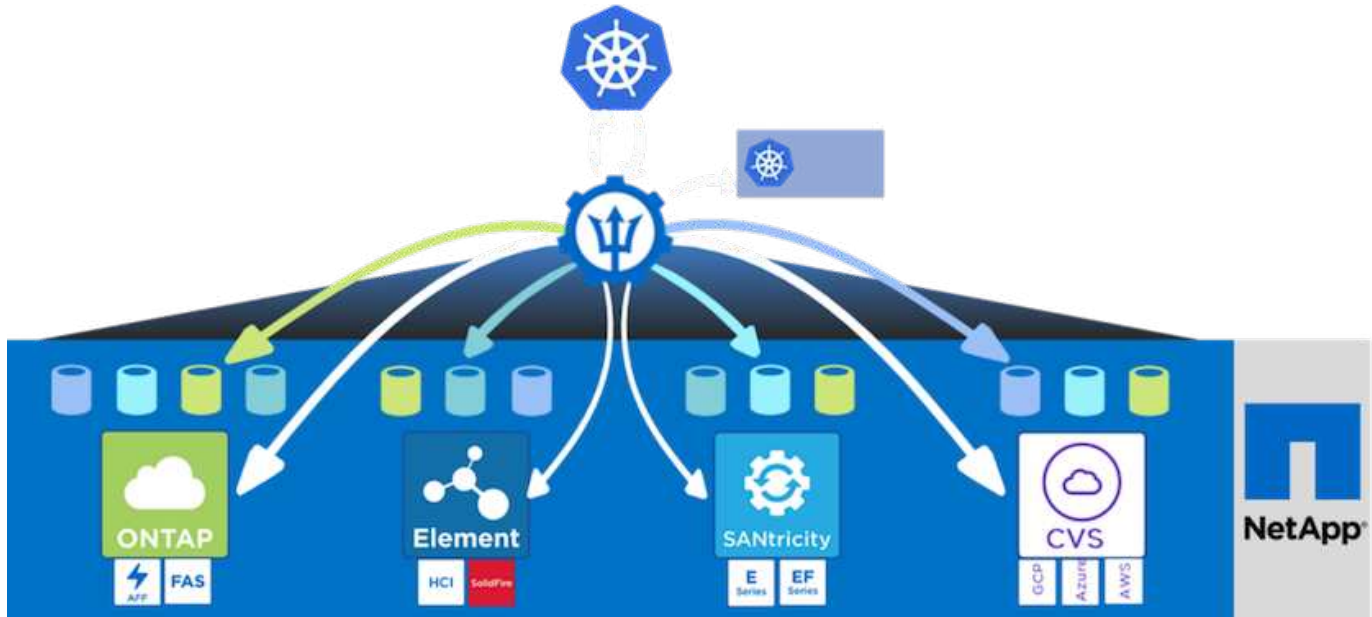
<input type="checkbox"/>	Name	State	Protection	Cluster	Group	Discovered ↓	Actions
<input type="checkbox"/>	magento-bef7f	✓ Healthy	⚠️ Unprotected	tkgi-acc	magento-bef7f	2022/05/16 21:31 UTC	⋮
<input type="checkbox"/>	magento	✓ Healthy	ℹ️ Partially protected	tkgi-acc	magento	2022/05/09 18:20 UTC	⋮

Astra Trident – Überblick

Astra Trident ist ein vollständig unterstützter Open-Source-Storage-Orchestrator für Container und Kubernetes-Distributionen wie Red Hat OpenShift, VMware Tanzu, Anthos by Google Cloud, Rancher etc. Trident kann mit dem gesamten NetApp Storage-Portfolio eingesetzt werden, einschließlich NetApp ONTAP und Element Storage-Systeme. Es unterstützt auch NFS- und iSCSI-Verbindungen. Trident beschleunigt den DevOps-Workflow, da Endbenutzer Storage über ihre NetApp Storage-Systeme bereitstellen und managen können, ohne dass ein Storage-Administrator eingreifen muss.

Ein Administrator kann verschiedene Storage-Back-Ends basierend auf den Projektanforderungen und Storage-Systemmodellen konfigurieren, die erweiterte Storage-Funktionen wie Komprimierung, bestimmte Festplattentypen oder QoS-Level ermöglichen, die eine bestimmte Performance garantieren. Nach ihrer

Definition können diese Back-Ends von Entwicklern in ihren Projekten verwendet werden, um persistente Volume Claims (PVCs) zu erstellen und persistenten Storage nach Bedarf an ihre Container anzubinden.



Astra Trident führt einen schnellen Entwicklungszyklus durch, und, wie Kubernetes, wird viermal im Jahr veröffentlicht.

Die neueste Version von Astra Trident ist 22.04. April 2022. Eine Support-Matrix, in der die Version von Trident getestet wurde, mit der Kubernetes Distribution zu finden ist "[Hier](#)".

Ab Version 20.04 wird die Trident-Einrichtung vom Trident Operator durchgeführt. Der Operator vereinfacht umfangreiche Implementierungen und bietet zusätzlichen Support. Durch die Selbstreparatur für Pods, die im Rahmen der Trident-Installation implementiert werden, wird damit das Selbstreparaturverfahren ermöglicht.

In der Version 21.01 wurde ein Helm Chart zur Erleichterung der Installation des Trident Operators zur Verfügung gestellt.

Trident-Operator mit Helm implementieren

1. Legen Sie zunächst den Speicherort des Benutzer-Clusters fest `kubeconfig` Datei als Umgebungsvariable, damit Sie nicht darauf verweisen müssen, weil Trident keine Option hat, diese Datei zu übergeben.

```
<<<<<<< HEAD
[netapp-user@rhel7]$ export KUBECONFIG=~/.tanzu-install/auth/kubeconfig
=====
[netapp-user@rhel7]$ export KUBECONFIG=~/.Tanzu-install/auth/kubeconfig
>>>>>>> eba1007b77b1ef6011dadd158f1df991acc5299f
```

2. Fügen Sie das NetApp Astra Trident Helm Repository hinzu.

```
[netapp-user@rhel7]$ helm repo add netapp-trident
https://netapp.github.io/trident-helm-chart
"netapp-trident" has been added to your repositories
```

3. Aktualisieren der Helm-Repositorys

```
[netapp-user@rhel7]$ helm repo update
Hang tight while we grab the latest from your chart repositories...
...Successfully got an update from the "netapp-trident" chart repository
...Successfully got an update from the "bitnami" chart repository
Update Complete. ☐Happy Helming!☐
```

4. Erstellen Sie für die Installation von Trident einen neuen Namespace.

```
[netapp-user@rhel7]$ kubectl create ns trident
```

5. Erstellen Sie ein Geheimnis mit den DockerHub-Anmeldeinformationen, um die Astra Trident-Bilder herunterzuladen.

```
[netapp-user@rhel7]$ kubectl create secret docker-registry docker-
registry-cred --docker-server=docker.io --docker-username=netapp
-solutions-tme --docker-password=xxxxxxx -n trident
```

6. Für Benutzer- oder Workload-Cluster, die von TKGS (vSphere mit Tanzu) oder TKG mit Management-Cluster-Implementierungen verwaltet werden, gehen Sie zur Installation von Astra Trident wie folgt vor:

- a. Stellen Sie sicher, dass der angemeldete Benutzer über die Berechtigungen zum Erstellen von Dienstkonten im Dreizack-Namespace verfügt und dass die Dienstkonten im Dreizack-Namespace über die Berechtigung zum Erstellen von Pods verfügen.
- b. Führen Sie den folgenden Helm-Befehl aus, um den Trident Operator im erstellten Namespace zu installieren.

```
[netapp-user@rhel7]$ helm install trident netapp-trident/trident-
operator -n trident --set imagePullSecrets[0]=docker-registry-cred
```

7. Führen Sie für einen Benutzer oder Workload-Cluster, der von TKG-Implementierungen gemanagt wird, den folgenden Helm-Befehl aus, um den Trident Operator in dem erstellten Namespace zu installieren.

```
[netapp-user@rhel7]$ helm install trident netapp-trident/trident-
operator -n trident --set imagePullSecrets[0]=docker-registry-
cred,kubeletDir="/var/vcap/data/kubelet"
```


8. Überprüfen Sie, ob die Trident Pods betriebsbereit sind.

NAME	READY	STATUS	RESTARTS
trident-csi-6vv62	2/2	Running	0
trident-csi-cfd844bcc-sqhcg	6/6	Running	0
trident-csi-dfcmz	2/2	Running	0
trident-csi-pb2n7	2/2	Running	0
trident-csi-qsw6z	2/2	Running	0
trident-operator-67c94c4768-xw978	1/1	Running	0

```
[netapp-user@rhel7]$ ./tridentctl -n trident version
+-----+
| SERVER VERSION | CLIENT VERSION |
+-----+
| 22.04.0        | 22.04.0        |
+-----+
```

Erstellen von Storage-System-Back-Ends

Nach Abschluss der Installation des Astra Trident Operator müssen Sie das Backend für die spezifische NetApp Storage-Plattform konfigurieren, die Sie verwenden. Folgen Sie den Links unten, um mit der Einrichtung und Konfiguration von Astra Trident fortzufahren.

- ["NetApp ONTAP NFS"](#)
- ["NetApp ONTAP iSCSI"](#)

Konfiguration von NetApp ONTAP NFS

Um die Trident Integration mit dem NetApp ONTAP Storage-System über NFS zu aktivieren, müssen Sie ein Backend erstellen, das die Kommunikation zum Storage-System ermöglicht. Wir konfigurieren in dieser Lösung ein Basis-Backend, aber wenn Sie nach mehr angepassten Optionen suchen, besuchen Sie die Dokumentation ["Hier"](#).

Erstellen Sie eine SVM in ONTAP

1. Melden Sie sich beim ONTAP System Manager an, navigieren Sie zu Storage > Storage VMs, und klicken Sie auf Hinzufügen.
2. Geben Sie einen Namen für die SVM ein, aktivieren Sie das NFS-Protokoll, aktivieren Sie das Kontrollkästchen NFS-Client-Zugriff zulassen und fügen Sie die Subnetze hinzu, die Ihre Worker-Nodes in den Exportrichtlinien-Regeln aktiviert sind, damit die Volumes als PVS in Ihren Workload-Clustern

gemountet werden können.

Add Storage VM



STORAGE VM NAME

trident_svm

Access Protocol

☒ SMB/CIFS, NFS, S3

iSCSI

☐ Enable SMB/CIFS

☒ Enable NFS

☒ Allow NFS client access

Add at least one rule to allow NFS clients to access volumes in this storage VM. [?](#)

EXPORT POLICY

Default

RULES

Rule Index	Clients	Access Protocols	Read-Only Rule	Read/Wr
	0.0.0.0/0	Any	Any	Any



Wenn Sie NAT'ed-Bereitstellung von Benutzer-Clustern oder Workload-Clustern mit NSX-T verwenden, müssen Sie das Egress-Subnetz (im Fall von TKGS0 oder das schwimmende IP-Subnetz (im Fall von TKGI) zu den Exportrichtlinien hinzufügen.

3. Geben Sie die Details zu Daten-LIFs sowie die Details für das SVM-Administratorkonto an, und klicken Sie dann auf „Speichern“.

NETWORK INTERFACE

Use multiple network interfaces when client traffic is high.

K8s-Ontap-01

IP ADDRESS

172.21.252.180

SUBNET MASK

24

GATEWAY

172.21.252.1



BROADCAST DOMAIN

Default



Storage VM Administration

☒ Manage administrator account

USER NAME

vsadmin

PASSWORD

.....

CONFIRM PASSWORD

.....

☐ Add a network interface for storage VM management.

4. Weisen Sie die Aggregate einer SVM zu. Navigieren Sie zu Storage > Storage VMs, klicken Sie auf die Auslassungspunkte neben der neu erstellten SVM und klicken Sie dann auf Bearbeiten. Aktivieren Sie das Kontrollkästchen Volume-Erstellung auf bevorzugte lokale Tiers begrenzen und hängen Sie die erforderlichen Aggregate an.

Edit Storage VM



STORAGE VM NAME

trident_svm

DEFAULT LANGUAGE

c.utf_8



DELETED VOLUME RETENTION PERIOD 

12

HOURS

Resource Allocation

☒ Limit volume creation to preferred local tiers

LOCAL TIERS

K8s_Ontap_01_SSD_1 

Cancel

Save

- Bei NAT-gestützten Implementierungen von Benutzer- oder Workload-Clustern, auf denen Trident installiert werden soll, kann die Storage-Mount-Anfrage aufgrund von SNAT von einem nicht standardmäßigen Port stammen. Standardmäßig erlaubt ONTAP nur Volume-Mount-Anfragen, wenn diese vom Root-Port

stammen. Melden Sie sich daher bei der ONTAP CLI an und ändern Sie die Einstellung, um Anfragen von nicht standardmäßigen Ports zu mounten.

```
ontap-01> vserver nfs modify -vserver tanzu_svm -mount-rootonly disabled
```

Back-Ends und StorageClasses erstellen

1. Erstellen Sie für NetApp ONTAP Systeme, die NFS bereitstellen, eine Back-End-Konfigurationsdatei auf dem Jumper Back-End mit BackendName, Management LIF, DatenLIF, svm, Benutzername, Kennwort und weitere Details.

```
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "backendName": "ontap-nas+10.61.181.221",
  "managementLIF": "172.21.224.201",
  "dataLIF": "10.61.181.221",
  "svm": "trident_svm",
  "username": "admin",
  "password": "password"
}
```



Als Best Practice empfiehlt es sich, den benutzerdefinierten BackendName-Wert als Kombination aus storageDriverName und der DatenLIF zu definieren, die NFS bedienen, um die einfache Identifizierung zu erleichtern.

2. Erstellen Sie das Trident-Back-End durch Ausführen des folgenden Befehls.

```
[netapp-user@rhel7]$ ./tridentctl -n trident create backend -f backend-ontap-nas.json
+-----+-----+
+-----+-----+-----+-----+
|          NAME          | STORAGE DRIVER |          UUID          |
| STATE | VOLUMES |          |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| ontap-nas+10.61.181.221 | ontap-nas      | be7a619d-c81d-445c-b80c-5c87a73c5b1e |
| online |          | 0 |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
```

3. Wenn das Back-End erstellt wird, müssen Sie als nächstes eine Storage-Klasse erstellen. Die folgende Beispieldefinition für Speicherklassen zeigt die erforderlichen und grundlegenden Felder an. Der Parameter backendType Sollte den Storage-Treiber aus dem neu erstellten Trident-Back-End widerspiegeln.

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-nfs
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"

```

4. Erstellen Sie die Storage-Klasse, indem Sie den Befehl `kubectl` ausführen.

```

[netapp-user@rhel7 trident-installer]$ kubectl create -f storage-class-nfs.yaml
storageclass.storage.k8s.io/ontap-nfs created

```

5. Nach Erstellung der Storage-Klasse müssen Sie dann die erste Forderung für ein persistentes Volume (PVC) erstellen. Eine PVC-Beispieldefinition ist unten angegeben. Stellen Sie sicher, dass die `storageClassName` Feld stimmt mit dem Namen der gerade erstellten Speicherklasse überein. Die PVC-Definition kann je nach Bedarf weiter angepasst werden, je nach bereitgestelltem Workload.

```

kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: basic
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: ontap-nfs

```

6. Erstellen Sie das PVC mit dem Befehl `kubectl`. Die Erstellung kann je nach Größe des erstellten Sicherungsvolumens einige Zeit in Anspruch nehmen, sodass Sie den Prozess nach Abschluss beobachten können.

```

[netapp-user@rhel7 trident-installer]$ kubectl create -f pvc-basic.yaml
persistentvolumeclaim/basic created

[netapp-user@rhel7 trident-installer]$ kubectl get pvc

```

NAME	STATUS	VOLUME	CAPACITY
ACCESS MODES	STORAGECLASS	AGE	
basic	Bound	pvc-b4370d37-0fa4-4c17-bd86-94f96c94b42d	1Gi
RWO		ontap-nfs	7s

NetApp ONTAP iSCSI-Konfiguration

Zur Integration von NetApp ONTAP Storage-Systemen in VMware Tanzu Kubernetes Cluster für persistente Volumes über iSCSI müssen die Nodes durch Anmeldung bei jedem Knoten vorbereitet und die iSCSI-Dienstprogramme bzw. -Pakete zum Mounten von iSCSI-Volumes konfiguriert werden. Befolgen Sie dazu das in diesem Verfahren beschriebene Verfahren "[Verlinken](#)".



NetApp empfiehlt dieses Verfahren nicht für NAT'ed Implementierungen von VMware Tanzu Kubernetes Clustern.



TKGI verwendet Bosh VMs als Nodes für Tanzu Kubernetes Cluster, auf denen unveränderliche Konfigurations-Images ausgeführt werden. Jegliche manuellen Änderungen von iSCSI-Paketen auf Bosh VMs bleiben auch bei einem Neustart erhalten. NetApp empfiehlt daher den Einsatz von NFS Volumes für persistenten Storage für Tanzu Kubernetes Cluster, die von TKGI implementiert und betrieben werden.

Nachdem die Clusterknoten für iSCSI-Volumes vorbereitet sind, müssen Sie ein Back-End erstellen, das die Kommunikation mit dem Speichersystem ermöglicht. Wir haben in dieser Lösung ein Basis-Backend konfiguriert, aber wenn Sie nach mehr angepassten Optionen suchen, besuchen Sie die Dokumentation "[Hier](#)".

Erstellen Sie eine SVM in ONTAP

Um eine SVM in ONTAP zu erstellen, gehen Sie wie folgt vor:

1. Melden Sie sich beim ONTAP System Manager an, navigieren Sie zu Storage > Storage VMs, und klicken Sie auf Hinzufügen.
2. Geben Sie einen Namen für die SVM ein, aktivieren Sie das iSCSI-Protokoll und geben Sie anschließend Details für die Daten-LIFs ein.

Add Storage VM



STORAGE VM NAME

trident_svm_iscsi

Access Protocol

SMB/CIFS, NFS, S3

iSCSI

☒ Enable iSCSI

NETWORK INTERFACE

K8s-Ontap-01

IP ADDRESS

10.61.181.231

SUBNET MASK

24

GATEWAY

10.61.181.1

BROADCAST DOMAIN

Defa...

☐ Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

IP ADDRESS

10.61.181.232

SUBNET MASK

24

GATEWAY

10.61.181.1

BROADCAST DOMAIN

Defa...

3. Geben Sie die Details für das SVM-Administratorkonto ein, und klicken Sie dann auf Speichern.

Storage VM Administration

☒ Manage administrator account

USER NAME

vsadmin

PASSWORD

.....

CONFIRM PASSWORD

.....

☐ Add a network interface for storage VM management.

Save

Cancel

4. Um die Aggregate der SVM zuzuweisen, wechseln Sie zu Storage > Storage VMs. Klicken Sie auf die Ellipsen neben der neu erstellten SVM und klicken Sie dann auf Bearbeiten. Aktivieren Sie das Kontrollkästchen Volume-Erstellung auf bevorzugte lokale Tiers begrenzen und hängen Sie die erforderlichen Aggregate an.

Edit Storage VM



STORAGE VM NAME

trident_svm_iscsi

DEFAULT LANGUAGE

c.utf_8



DELETED VOLUME RETENTION PERIOD 

12

HOURS

Resource Allocation

☒ Limit volume creation to preferred local tiers

LOCAL TIERS

K8s_Ontap_01_SSD_1 

Cancel

Save

Back-Ends und StorageClasses erstellen

1. Erstellen Sie für NetApp ONTAP Systeme, die NFS bereitstellen, eine Back-End-Konfigurationsdatei auf dem Jumper Back-End mit BackendName, Management LIF, DatenLIF, svm, Benutzername, Kennwort und weitere Details.

```
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "backendName": "ontap-san+10.61.181.231",
  "managementLIF": "172.21.224.201",
  "dataLIF": "10.61.181.231",
  "svm": "trident_svm_iscsi",
  "username": "admin",
  "password": "password"
}
```

2. Erstellen Sie das Trident-Back-End durch Ausführen des folgenden Befehls.

```
[netapp-user@rhel7 trident-installer]$ ./tridentctl -n trident create
backend -f backend-ontap-san.json
+-----+-----+-----+
+-----+-----+-----+-----+
|          NAME          | STORAGE DRIVER |          UUID          |
| STATE | VOLUMES | |          |          |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| ontap-san+10.61.181.231 | ontap-san      | 6788533c-7fea-4a35-b797- |
| fb9bb3322b91 | online |      0 |          |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
```

3. Nachdem Sie ein Backend erstellt haben, müssen Sie zunächst eine Speicherklasse erstellen. Die folgende Beispieldefinition für Speicherklassen zeigt die erforderlichen und grundlegenden Felder an. Der Parameter `backendType` sollte den Storage-Treiber aus dem neu erstellten Trident-Back-End widerspiegeln. Notieren Sie auch den Wert des Namensfelds, auf den in einem späteren Schritt verwiesen werden muss.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-iscsi
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-san"
```



Es gibt ein optionales Feld mit dem Namen `fsType`. Das ist in dieser Datei definiert. In iSCSI-Back-Ends kann dieser Wert auf einen bestimmten Linux-Dateisystem-Typ (XFS, ext4 usw.) gesetzt werden oder kann gelöscht werden, damit Tanzu Kubernetes-Cluster entscheiden können, welches Dateisystem verwendet werden soll.

4. Erstellen Sie die Storage-Klasse, indem Sie den Befehl `kubectl` ausführen.

```
[netapp-user@rhel7 trident-installer]$ kubectl create -f storage-class-iscsi.yaml
storageclass.storage.k8s.io/ontap-iscsi created
```

5. Nach Erstellung der Storage-Klasse müssen Sie dann die erste Forderung für ein persistentes Volume (PVC) erstellen. Eine PVC-Beispieldefinition ist unten angegeben. Stellen Sie sicher, dass die `storageClassName` Feld stimmt mit dem Namen der gerade erstellten Speicherklasse überein. Die PVC-Definition kann je nach Bedarf weiter angepasst werden, je nach bereitgestelltem Workload.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: basic
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: ontap-iscsi
```

6. Erstellen Sie das PVC mit dem Befehl `kubectl`. Die Erstellung kann je nach Größe des erstellten Sicherungsvolumens einige Zeit in Anspruch nehmen, sodass Sie den Prozess nach Abschluss beobachten können.

```
[netapp-user@rhel7 trident-installer]$ kubectl create -f pvc-basic.yaml
persistentvolumeclaim/basic created
```

```
[netapp-user@rhel7 trident-installer]$ kubectl get pvc
```

NAME	STATUS	VOLUME	CAPACITY
basic	Bound	pvc-7ceac1ba-0189-43c7-8f98-094719f7956c	1Gi
ACCESS MODES		STORAGECLASS	AGE
RWO		ontap-iscsi	3s

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.