Présentation des intégrations de stockage NetApp

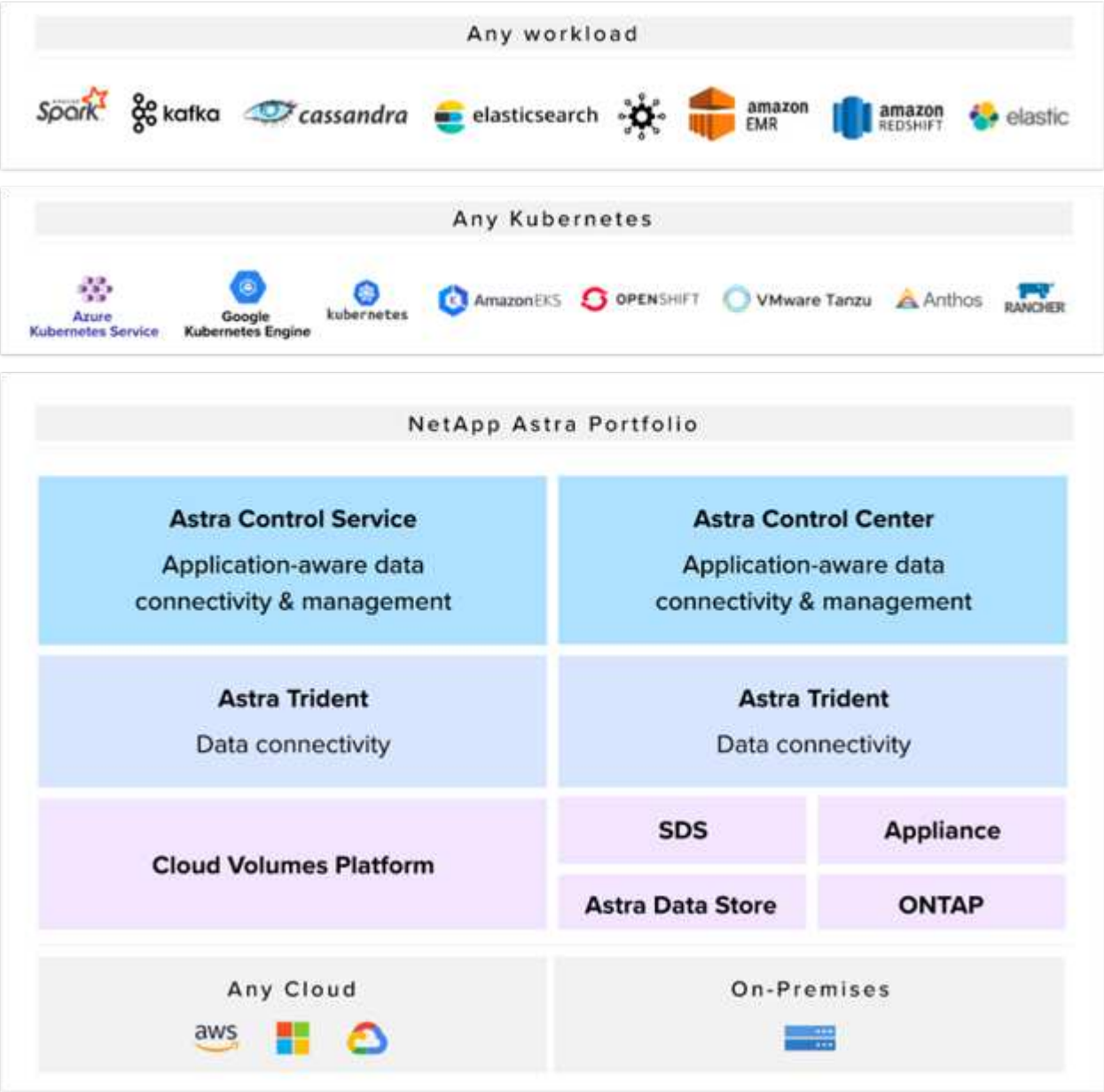
NetApp Solutions

NetApp
April 26, 2024

Sommaire

Présentation de l'intégration du stockage NetApp

NetApp propose plusieurs produits pour orchestrer, gérer, protéger et migrer les applications conteneurisées avec état et leurs données.



NetApp Astra Control propose un ensemble complet de services de gestion du stockage et des données respectueuse des applications pour les workloads Kubernetes avec état optimisés par la technologie de protection des données NetApp. Astra Control Service est disponible pour la prise en charge des workloads avec état dans les déploiements Kubernetes cloud natifs. Le centre de contrôle Astra permet de prendre en charge les workloads avec état dans les déploiements sur site de plateformes Kubernetes d'entreprise telles que Red Hat OpenShift, Rancher, VMware Tanzu etc. Pour en savoir plus, rendez-vous sur le site Web NetApp Astra Control "ici".

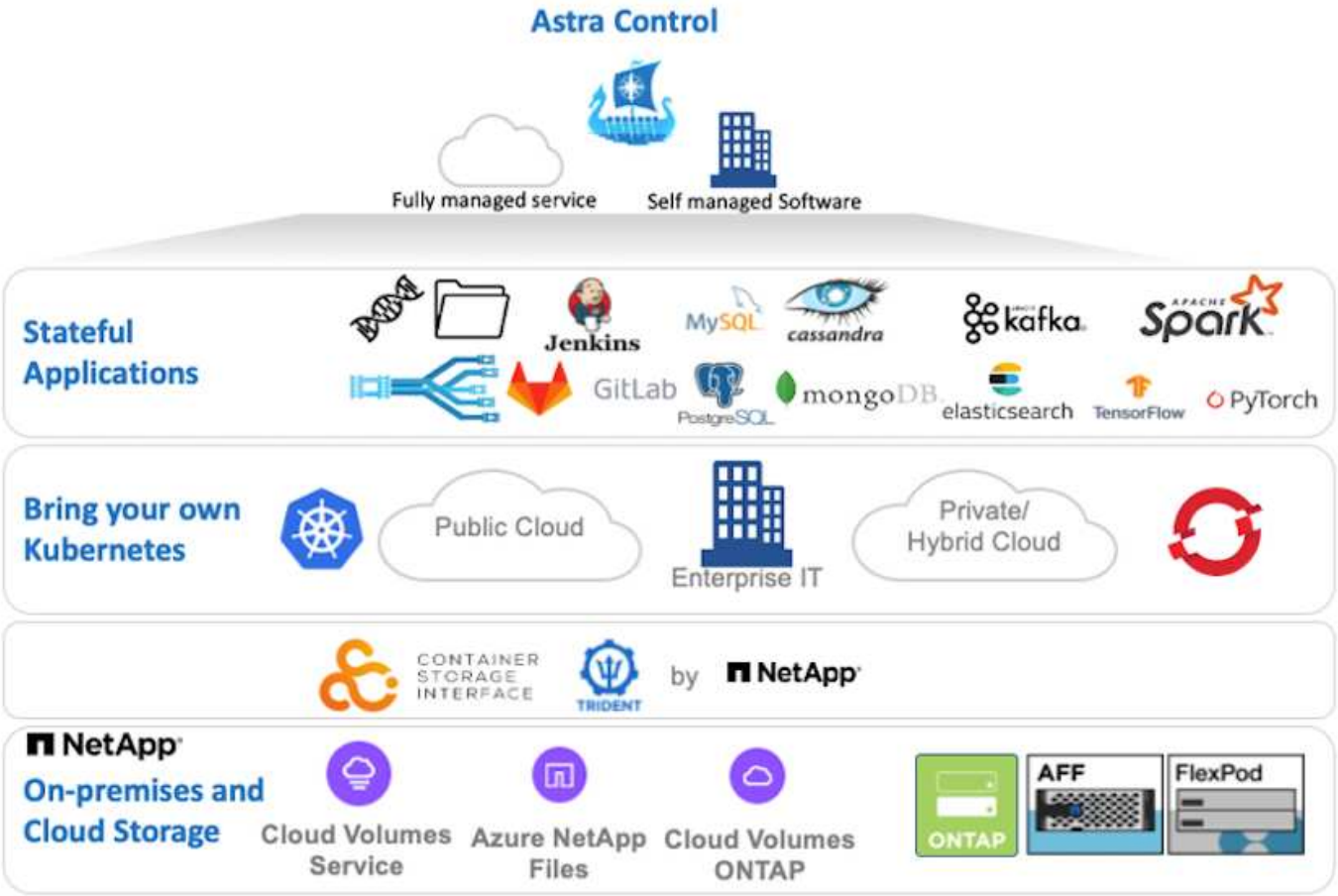
NetApp Astra Trident est un orchestrateur de stockage open source entièrement pris en charge pour les conteneurs et les distributions Kubernetes telles que Red Hat OpenShift, Rancher, VMware Tanzu etc. Pour en savoir plus, rendez-vous sur le site Web Astra Trident "ici".

Les pages suivantes présentent des informations supplémentaires sur les produits NetApp validés pour les applications et la gestion du stockage persistant dans la solution VMware Tanzu with NetApp :

- "NetApp Astra Control Center"
- "NetApp Astra Trident"

Présentation de NetApp Astra Control

NetApp Astra Control Center propose un ensemble complet de services de gestion du stockage et des données respectueuse des applications pour les workloads Kubernetes avec état, déployés dans un environnement sur site et optimisé par les technologies NetApp de protection des données.



Le centre de contrôle NetApp Astra peut être installé sur un cluster VMware Tanzu sur lequel l'orchestrateur de stockage Astra Trident est déployé et configuré avec des classes de stockage et des systèmes back-end de stockage vers des systèmes de stockage NetApp ONTAP.

Pour en savoir plus sur Astra Trident, rendez-vous sur "ce document ici".

Dans un environnement connecté au cloud, Astra Control Center utilise Cloud Insights pour fournir des fonctionnalités avancées de surveillance et de télémétrie. En l'absence de connexion Cloud Insights, un contrôle limité et une télémétrie (sept jours de metrics) sont disponibles et exportés vers les outils de contrôle natifs Kubernetes (Prometheus et Grafana) via des terminaux ouverts.

Le centre de contrôle Astra est entièrement intégré à l'écosystème NetApp AutoSupport et Active IQ qui fournit un soutien aux utilisateurs, fournit des conseils pour la résolution de problèmes et affiche des statistiques d'utilisation.

En plus de la version payante d'Astra Control Center, une licence d'évaluation de 90 jours est également disponible. La version d'évaluation est prise en charge par e-mail et dans le Channel Slack de la communauté. Les clients ont accès à ces ressources, à d'autres articles de la base de connaissances et à de la documentation disponibles dans le tableau de bord de support des produits.

Pour en savoir plus sur la gamme Astra, consultez le "Site Web d'Astra".

Automatisation du centre de contrôle Astra

Astra Control Center est doté d'une API REST entièrement fonctionnelle pour l'accès par programmation. Les utilisateurs peuvent utiliser n'importe quel langage ou utilitaire de programmation pour interagir avec les terminaux API REST Astra Control. Pour plus d'informations sur cette API, reportez-vous à la documentation "ici".

Si vous recherchez un kit de développement logiciel prêt à l'emploi pour interagir avec les API REST Astra Control, NetApp propose un kit avec le kit de développement Python Astra Control que vous pouvez télécharger "ici".

Si la programmation n'est pas adaptée à votre situation et si vous souhaitez utiliser un outil de gestion de la configuration, vous pouvez cloner et exécuter les playbooks Ansible publiés par NetApp "ici".

Conditions préalables à l'installation d'Astra Control Center

L'installation d'Astra Control Center requiert les conditions préalables suivantes :

- Un ou plusieurs clusters Kubernetes tanzu gérés soit par un cluster de gestion, soit par TKGS ou TKGI. Les clusters de charges de travail TKG 1.4+ et les clusters utilisateur TKGI 1.12.2+ sont pris en charge.
- Astra Trident doit déjà être installé et configuré sur chacun des clusters Kubernetes de Tanzanie.
- Un ou plusieurs systèmes de stockage NetApp ONTAP exécutant ONTAP 9.5 ou version ultérieure.

> C'est une bonne pratique pour chaque installation de Kubernetes de tanzu sur un site qui dispose d'un SVM dédié pour le stockage persistant. Les déploiements multisites requièrent des systèmes de stockage supplémentaires.

- Un système back-end de stockage Trident doit être configuré sur chaque cluster Kubernetes tanzu avec une SVM sauvegardée par un cluster ONTAP.
- Classe de stockage par défaut configurée sur chaque cluster Kubernetes tanzu avec Astra Trident comme mécanisme de provisionnement du stockage.
- Un équilibreur de charge doit être installé et configuré sur chaque cluster Kubernetes tanzu pour équilibrer la charge et exposer Astra Control Center si vous utilisez ingressType `AccTraefik`.
- Un contrôleur d'entrée doit être installé et configuré sur chaque cluster Kubernetes tanzu pour exposer Astra Control Center si vous utilisez ingressType `Generic`.
- Un registre d'images privées doit être configuré pour héberger les images du NetApp Astra Control Center.
- Vous devez disposer d'un accès administrateur de cluster au cluster Kubernetes tanzu sur lequel Astra Control Center est installé.
- Vous devez disposer d'un accès d'administration aux clusters NetApp ONTAP.
- Un poste de travail d'administration RHEL ou Ubuntu.

Poser le centre de contrôle Astra

Cette solution décrit une procédure automatisée pour installer Astra Control Center à l'aide d'un playbooks Ansible. Si vous recherchez une procédure manuelle pour installer le centre de contrôle Astra, suivez le guide d'installation et d'exploitation détaillé "ici".

1. Pour déployer Astra Control Center, vous devez disposer d'un ordinateur Ubuntu/RHEL avec Ansible. Suivre les procédures "ici" Pour Ubuntu et RHEL.
2. Clonez le référentiel GitHub qui héberge le contenu Ansible.

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

3. Connectez-vous au site de support NetApp et téléchargez la dernière version de NetApp Astra Control Center. Une licence associée à votre compte NetApp est requise. Après avoir téléchargé le tarball, transférez-le sur le poste de travail.

> Pour commencer avec une licence d'essai d'Astra Control, visitez le "Site d'inscription à Astra".

4. Créez ou obtenez le fichier kubeconfig avec un accès administrateur au cluster Kubernetes de l'utilisateur ou de la charge de travail Tanzu sur lequel Astra Control Center doit être installé.
5. Définissez le répertoire sur `na_astra_control_suite`.

```
cd na_astra_control_suite
```

6. Modifiez le `vars/vars.yml` classez les variables et remplissez-les avec les informations requises.

```
#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. Utilisez le PlayBook pour déployer le centre de contrôle Astra. Le PlayBook requiert des privilèges root pour certaines configurations.

   Exécutez la commande suivante pour exécuter le PlayBook si l'utilisateur exécutant le PlayBook est root ou a configuré un sudo sans mot de passe.

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

   Si l'accès sudo basé sur un mot de passe est configuré, exécutez la commande suivante pour exécuter le PlayBook, puis saisissez le mot de passe sudo.

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

Après l'installation

1. L'installation peut prendre plusieurs minutes. Vérifier que tous les pods et services dans le `netapp-astra-cc` les espaces de noms sont opérationnels.

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

2. Vérifier le `acc-operator-controller-manager` journaux pour vérifier que l'installation est terminée.

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

   Le message suivant indique que le centre de contrôle Astra a été installé avec succès.

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

3. Le nom d'utilisateur pour la connexion à Astra Control Center est l'adresse électronique de l'administrateur fournie dans le fichier CRD et le mot de passe est une chaîne `ACC-` Joint à l'UUID du centre de contrôle Astra. Exécutez la commande suivante :

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

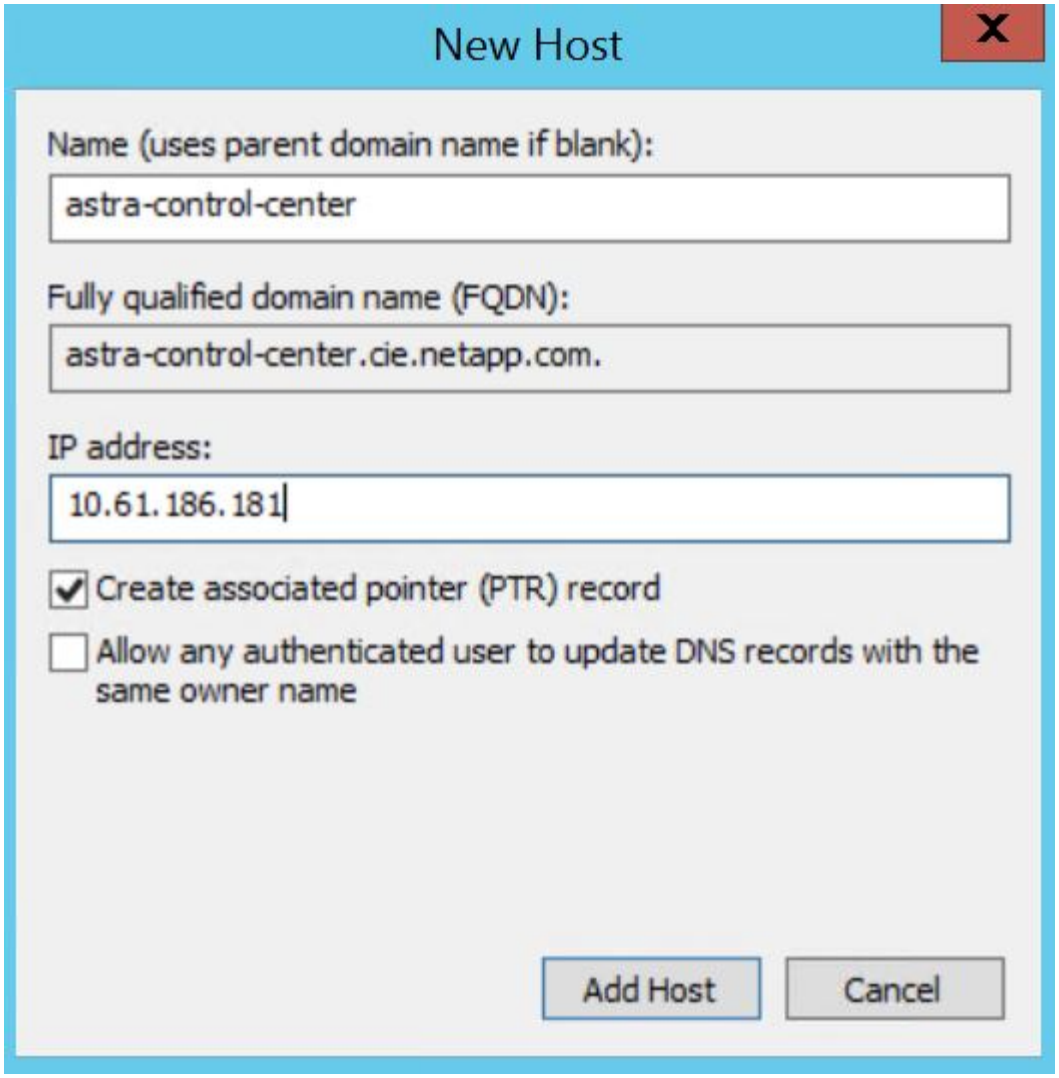
> Dans cet exemple, le mot de passe est `ACC-345c55a5-bf2e-21f0-84b8-b6f2bce5e95f`.

4. Obtenez l'IP de l'équilibreur de charge du service traefik si ingressType est AccTraefik.

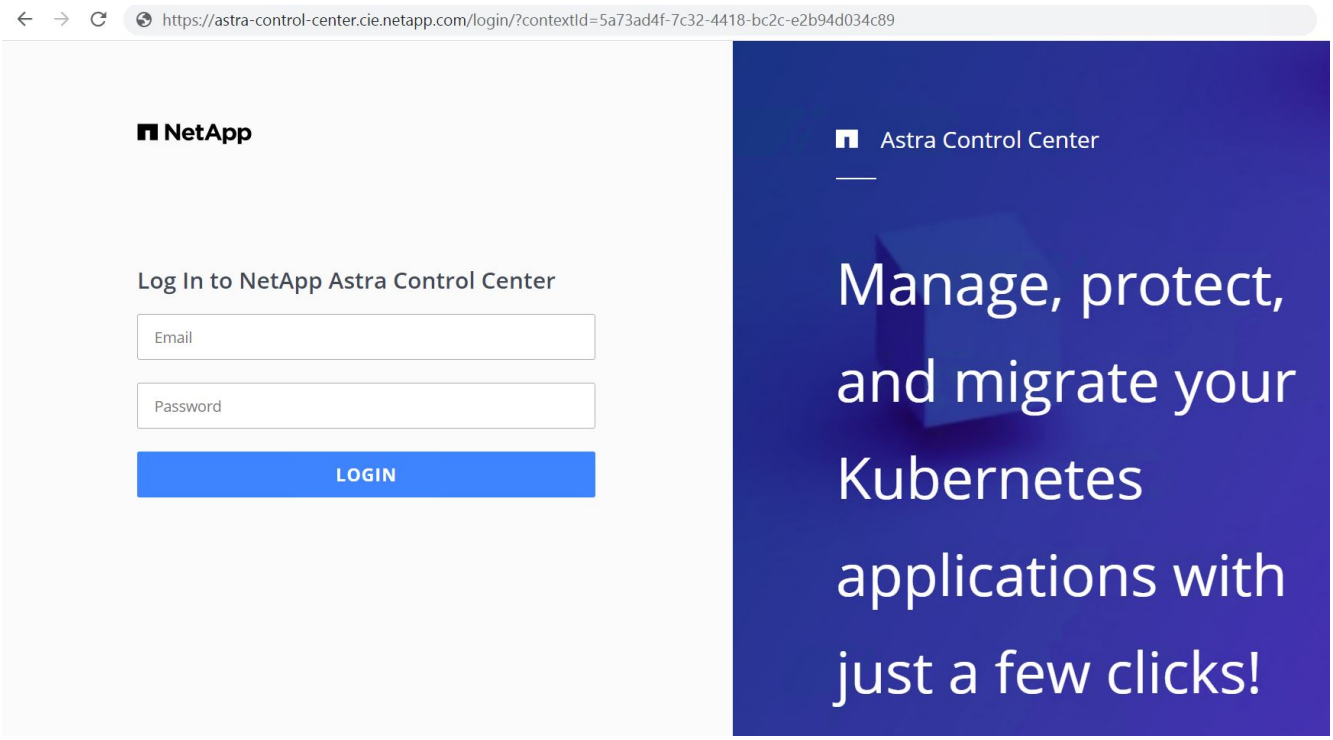
```
[netapp-user@rhel7 ~]$ oc get svc -n netapp-astra-cc | egrep
'EXTERNAL|traefik'

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

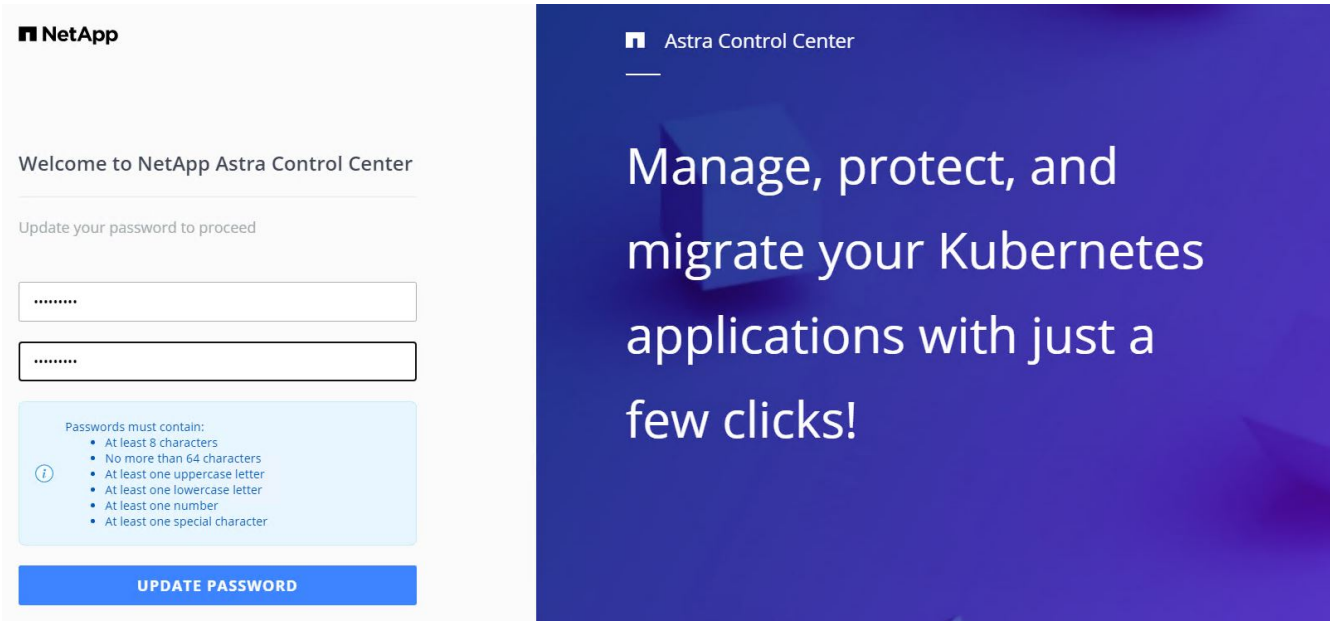
5. Ajoutez une entrée dans le serveur DNS pointant le FQDN fourni dans le fichier CRD Astra Control Center vers le `EXTERNAL-IP` du service de trafik.



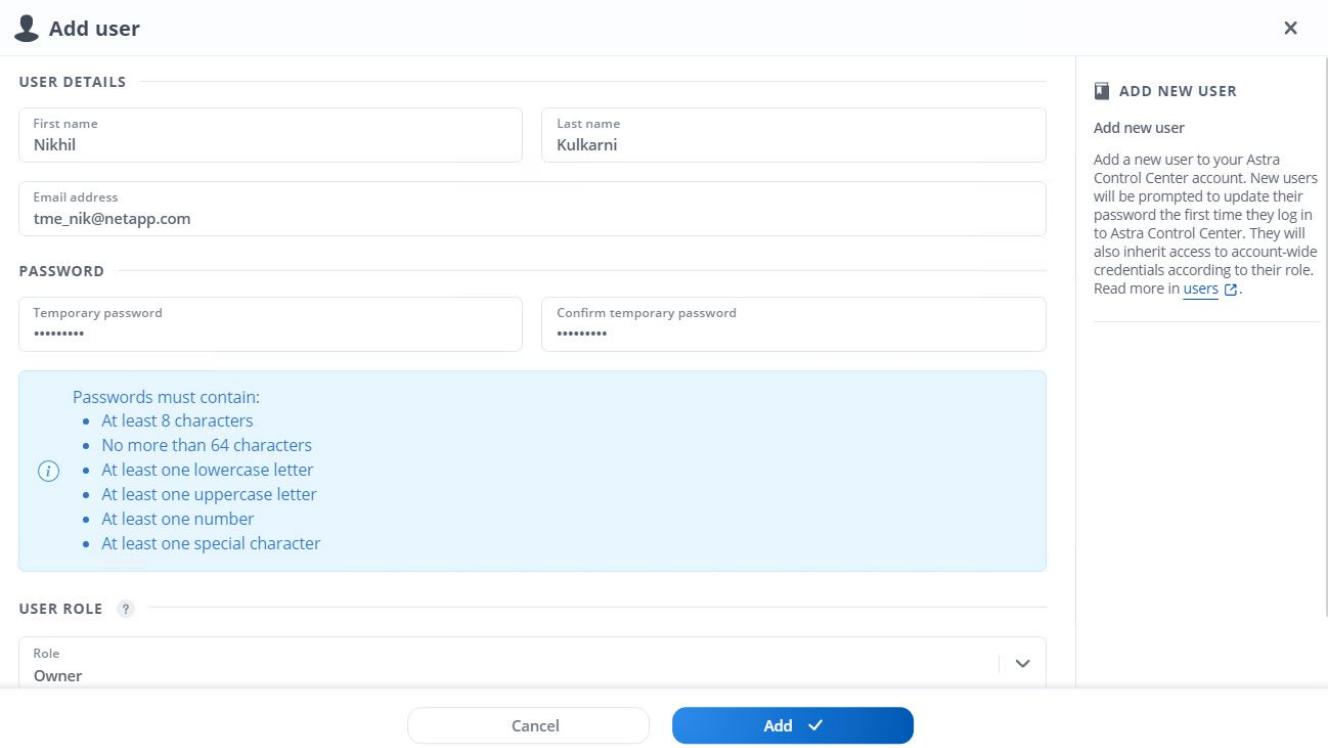
6. Connectez-vous à l'interface graphique d'Astra Control Center en parcourant son FQDN.



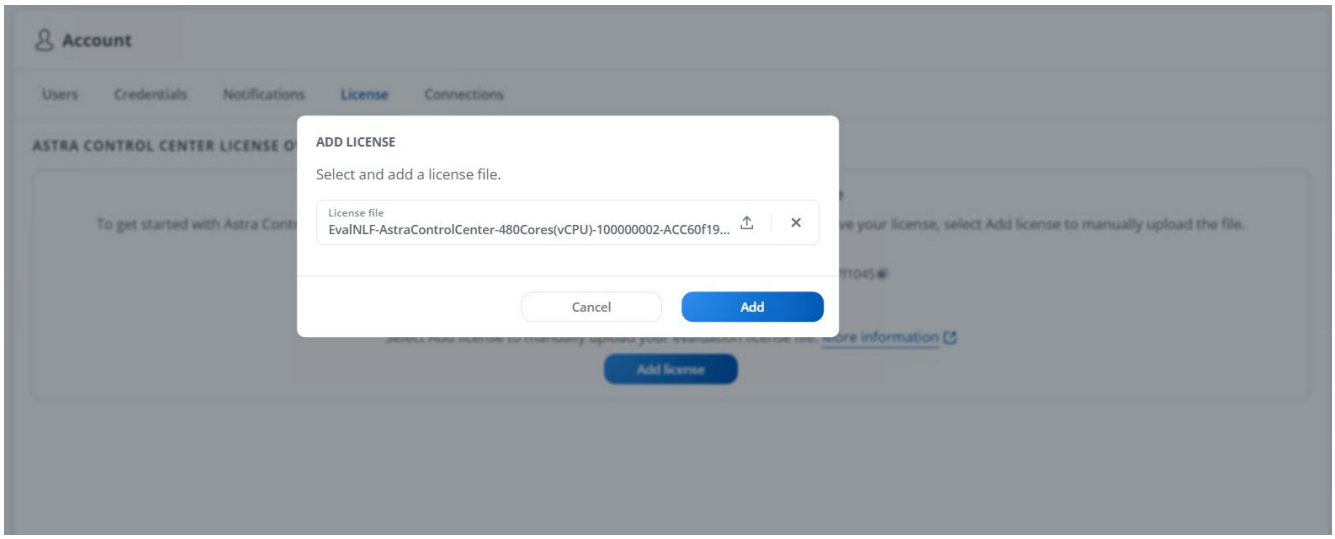
7. Lorsque vous vous connectez à l'interface graphique d'Astra Control Center pour la première fois à l'aide de l'adresse e-mail d'administration fournie dans CRD, vous devez modifier le mot de passe.



8. Si vous souhaitez ajouter un utilisateur au Centre de contrôle Astra, accédez à compte > utilisateurs, cliquez sur Ajouter, entrez les détails de l'utilisateur et cliquez sur Ajouter.



9. Astra Control Center requiert une licence pour toutes ses fonctionnalités. Pour ajouter une licence, accédez à compte > Licence, cliquez sur Ajouter une licence et téléchargez le fichier de licence.



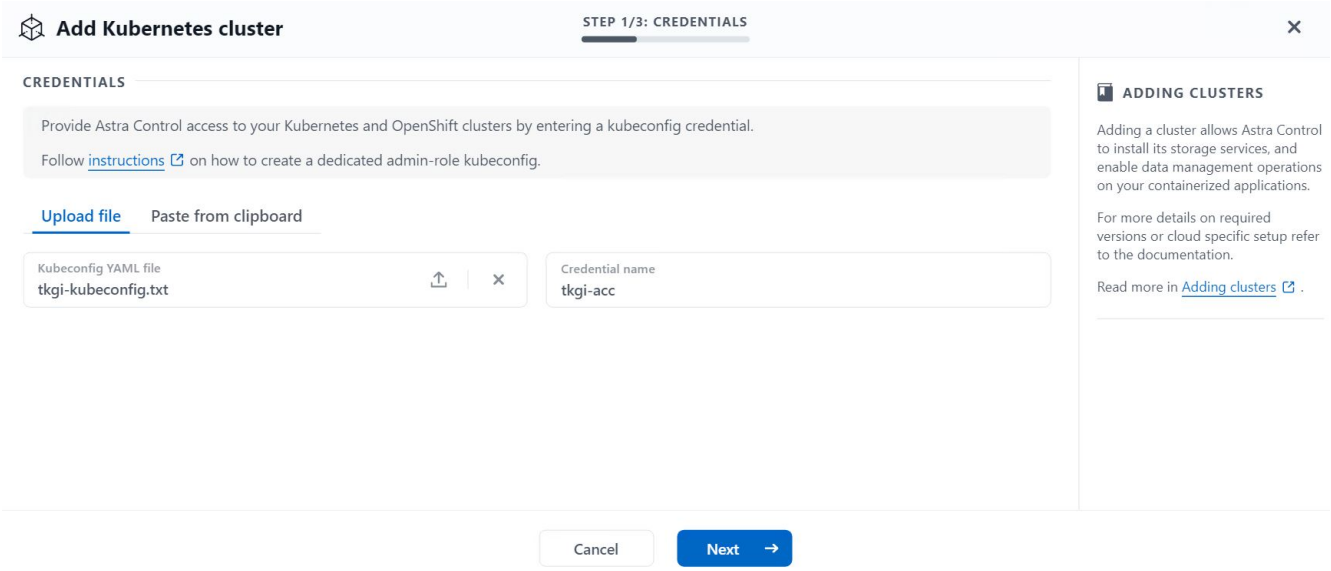
En cas de problème avec l'installation ou la configuration de NetApp Astra Control Center, la base de connaissances des problèmes connus est disponible "ici".

Enregistrez vos clusters Kubernetes VMware Tanzu avec le Centre de contrôle Astra

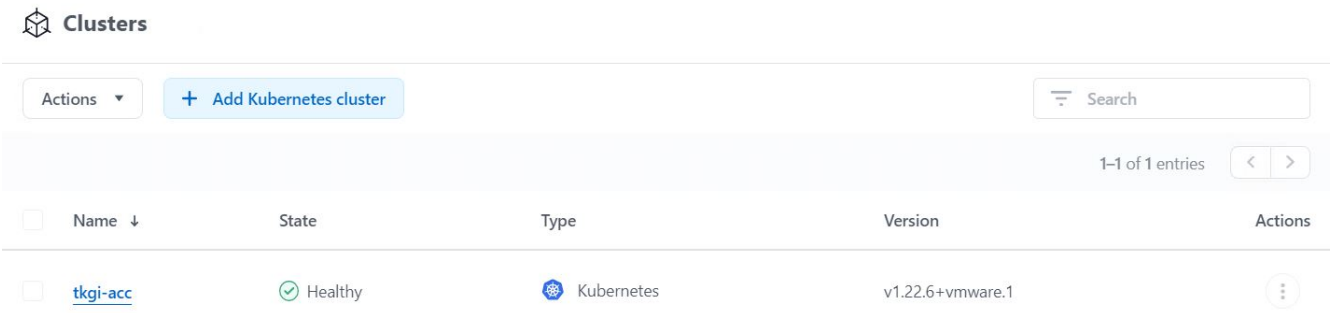
Pour permettre au Centre de contrôle Astra de gérer vos charges de travail, vous devez d'abord enregistrer vos clusters Kubernetes Tanzu.

Enregistrez les clusters VMware Tanzu Kubernetes

1. La première étape consiste à ajouter les clusters Kubernetes tanzu au Centre de contrôle Astra et à les gérer. Accédez à clusters et cliquez sur Ajouter un cluster, téléchargez le fichier kubeconfig pour le cluster Kubernetes de Tanzanie, puis cliquez sur Sélectionner un stockage.

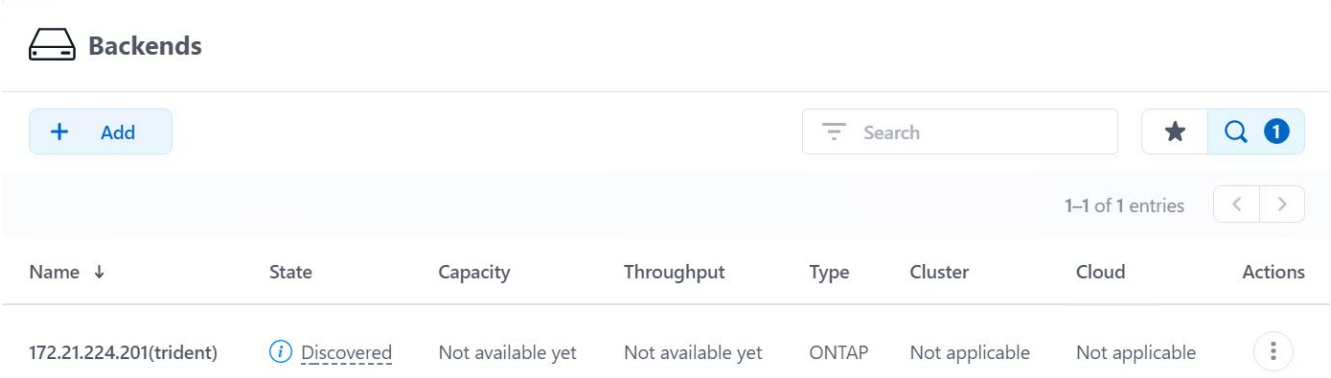


2. Astra Control Center détecte les classes de stockage admissibles. Maintenant, sélectionnez la façon dont storageclass provisionne les volumes en utilisant Trident sauvegardé par un SVM sur NetApp ONTAP et Click Review. Dans le volet suivant, vérifiez les détails et cliquez sur Ajouter un cluster.
3. Lorsque le cluster est ajouté, il passe à l'état découverte pendant qu'Astra Control Center l'inspecte et installe les agents nécessaires. L'état du cluster est modifié en `Healthy` une fois l'enregistrement terminé.

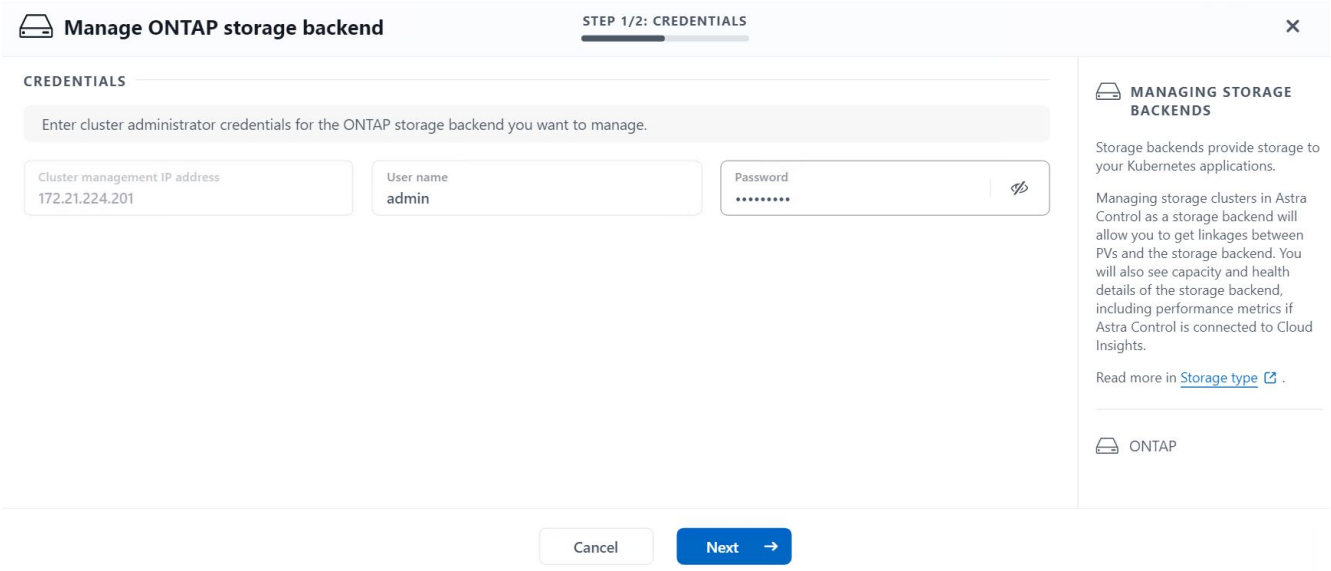


> Tous les clusters Kubernetes tanzu à gérer par Astra Control Center doivent avoir accès au registre d'images utilisé pour son installation, car les agents installés sur les clusters gérés extraient les images de ce registre.

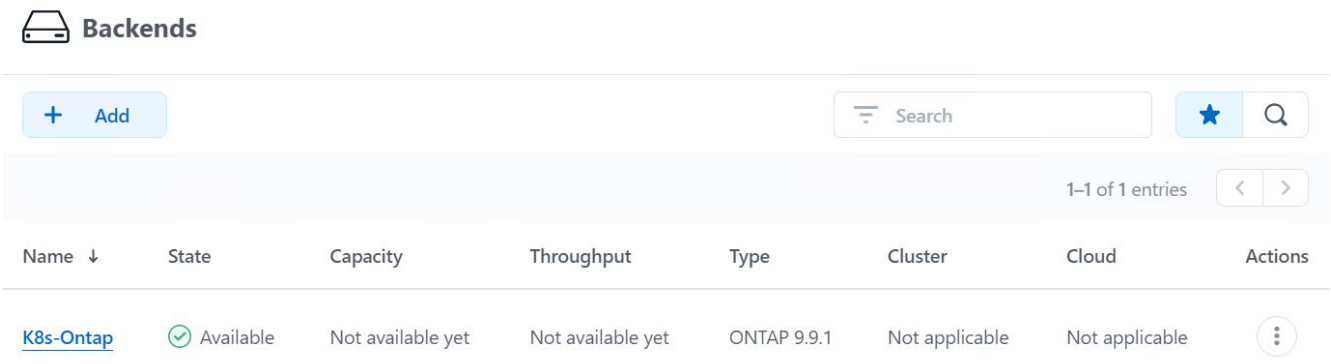
4. Importation de clusters ONTAP comme ressources de stockage à gérer en tant que système back-end par Astra Control Center. Lorsque des clusters Kubernetes tanzu sont ajoutés à Astra et qu'un storageclass est configuré, il détecte et inspecte automatiquement le cluster ONTAP qui soutient le storageclass, mais ne l'importe pas dans le Control Center Astra à gérer.



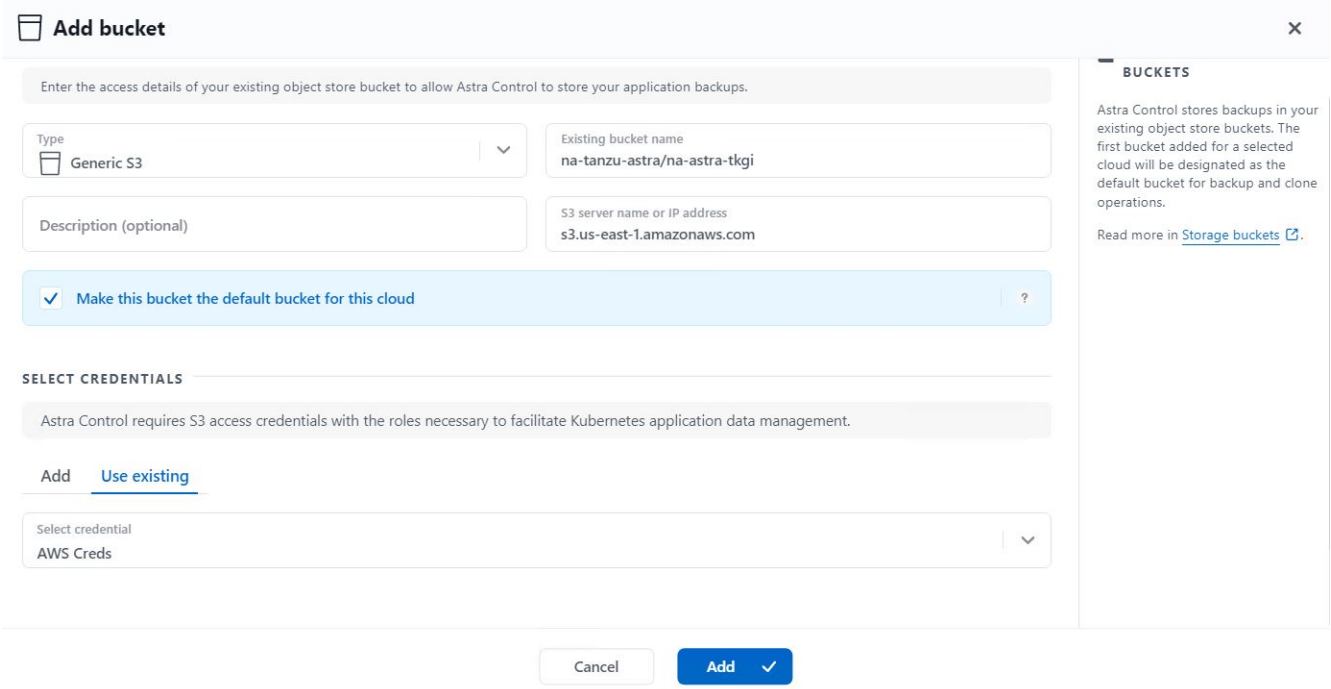
5. Pour importer les clusters ONTAP, accédez aux systèmes back-end, cliquez sur la liste déroulante et sélectionnez gérer en regard du cluster ONTAP à gérer. Entrez les informations d'identification du cluster ONTAP, cliquez sur vérifier les informations, puis sur Importer le stockage back-end.



6. Une fois que le système back-end est ajouté, le statut devient disponible. Ces systèmes back-end disposent désormais d'informations sur les volumes persistants dans le cluster Kubernetes tanzu et sur les volumes correspondants sur le système ONTAP.



7. Pour la sauvegarde et la restauration entre des clusters Kubernetes tanzu à l'aide d'Astra Control Center, vous devez provisionner un compartiment de stockage objet qui prend en charge le protocole S3. Les options actuellement prises en charge sont ONTAP S3, StorageGRID, AWS S3 et le stockage Microsoft Azure Blob Storage. Pour les besoins de cette installation, nous allons configurer un compartiment AWS S3. Accédez à godets, cliquez sur Ajouter un compartiment et sélectionnez Generic S3. Entrez les informations d'identification du compartiment S3 et des informations d'identification pour y accéder, cliquez sur la case à cocher définir ce compartiment comme compartiment par défaut pour le cloud, puis cliquez sur Ajouter.

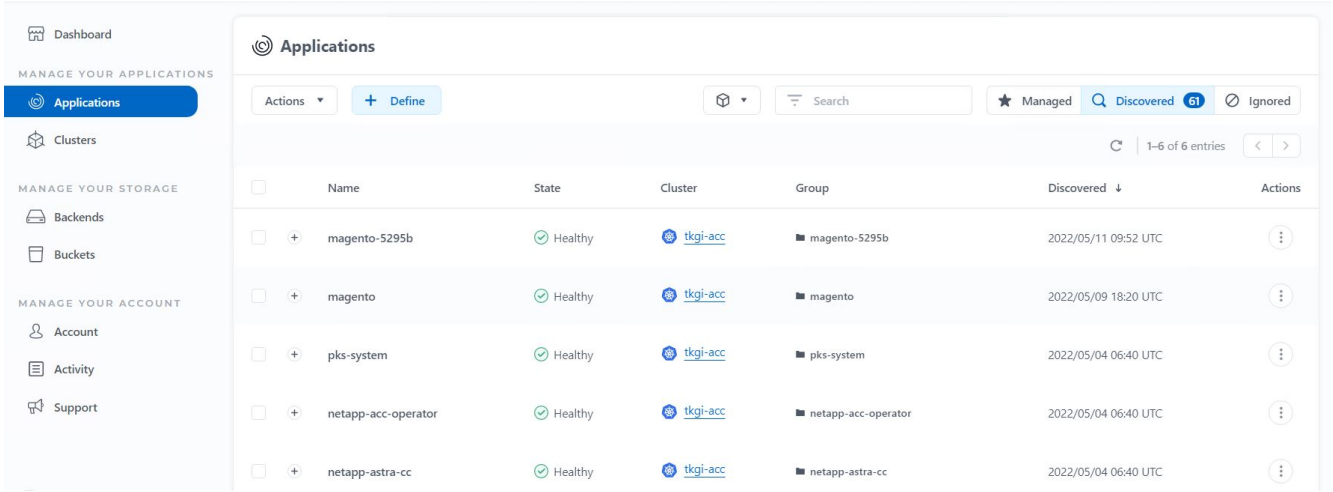


Choisissez les applications à protéger

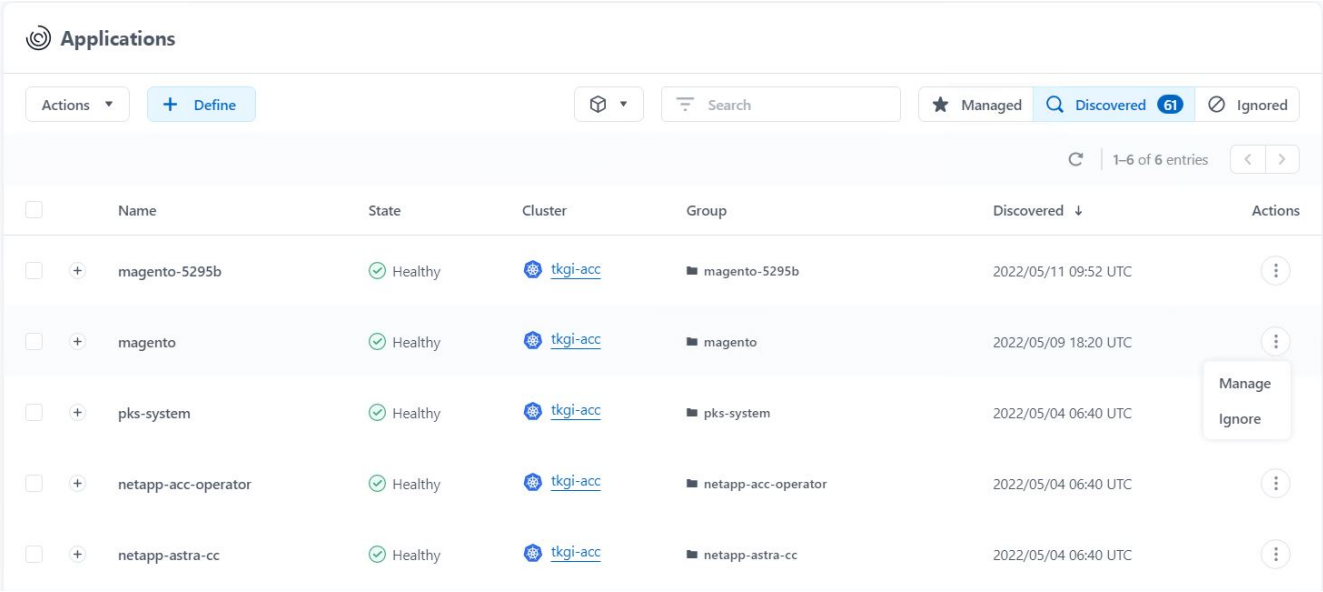
Une fois que vous avez enregistré vos clusters Kubernetes Tanzu, vous pouvez découvrir les applications qui sont déployées et les gérer via le Centre de contrôle Astra.

Gestion des applications

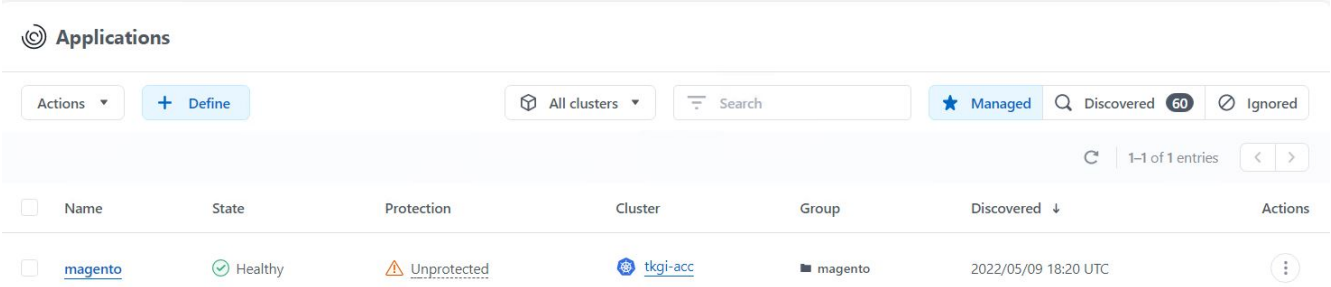
1. Une fois que les clusters Kubernetes tanzu et les systèmes back-end ONTAP sont enregistrés auprès du Centre de contrôle Astra, le centre de contrôle commence automatiquement à découvrir les applications dans tous les espaces de noms qui utilisent le storageclass configuré avec le back-end ONTAP spécifié.



2. Accédez à applications > découverte et cliquez sur le menu déroulant en regard de l'application que vous souhaitez gérer à l'aide d'Astra. Cliquez ensuite sur gérer.



3. L'application passe à l'état disponible et peut être affichée sous l'onglet géré de la section applications.



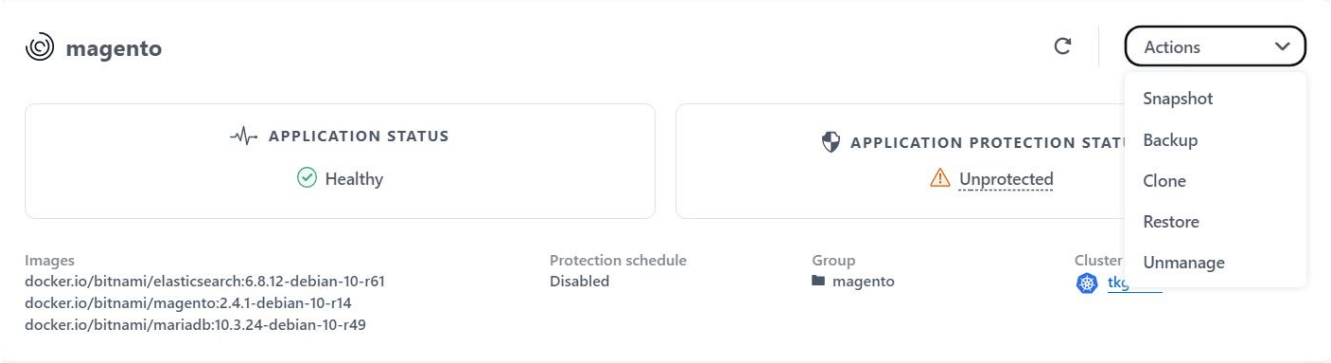
Protégez vos applications

Une fois les charges de travail applicatives gérées par Astra Control Center, vous pouvez configurer les paramètres de protection pour ces charges de travail.

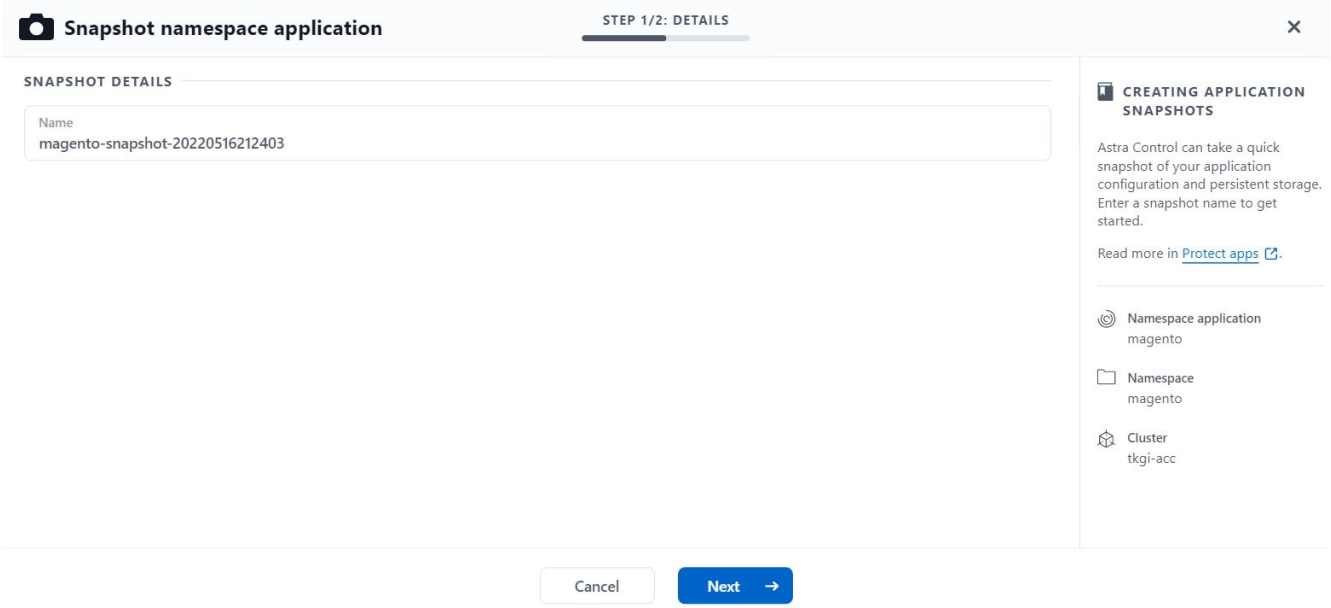
Créer un instantané d'application

Un snapshot d'une application crée une copie ONTAP Snapshot et une copie des métadonnées d'application qui peuvent être utilisées pour restaurer ou cloner l'application à un point dans le temps spécifique en fonction de cette copie Snapshot.

1. Pour prendre un instantané de l'application, accédez à l'onglet applications > gestion, puis cliquez sur l'application dont vous souhaitez effectuer une copie Snapshot. Cliquez sur le menu déroulant en regard du nom de l'application et cliquez sur instantané.



2. Entrez les détails du snapshot, cliquez sur Suivant, puis sur instantané. La création du Snapshot prend environ une minute et son état est disponible une fois celui-ci créé.



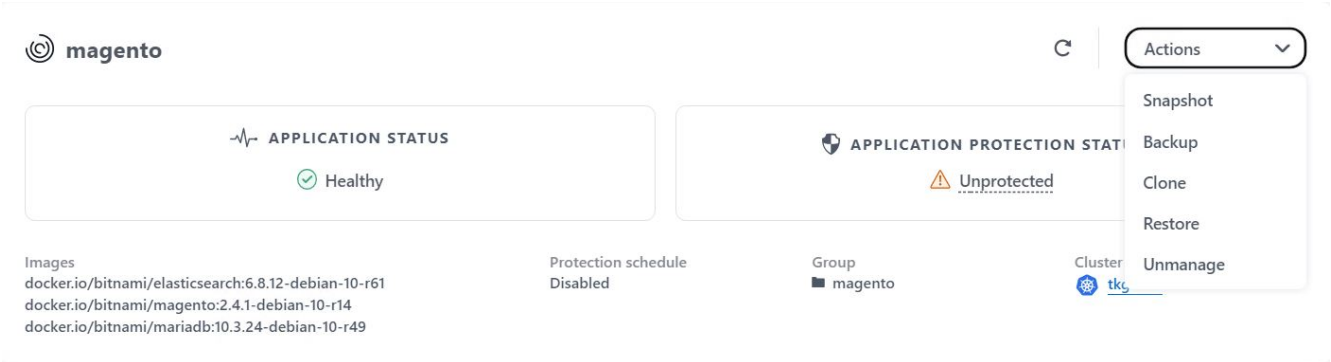
Création d'une sauvegarde d'application

Une sauvegarde d'une application capture l'état actif de l'application et la configuration des ressources informatiques, les analyse en fichiers et les stocke dans un compartiment de stockage objet distant.

1. Pour la sauvegarde et la restauration des applications gérées dans le Centre de contrôle Astra, vous devez configurer les paramètres de superutilisateur des systèmes ONTAP de secours au préalable. Pour ce faire, entrez les commandes suivantes.

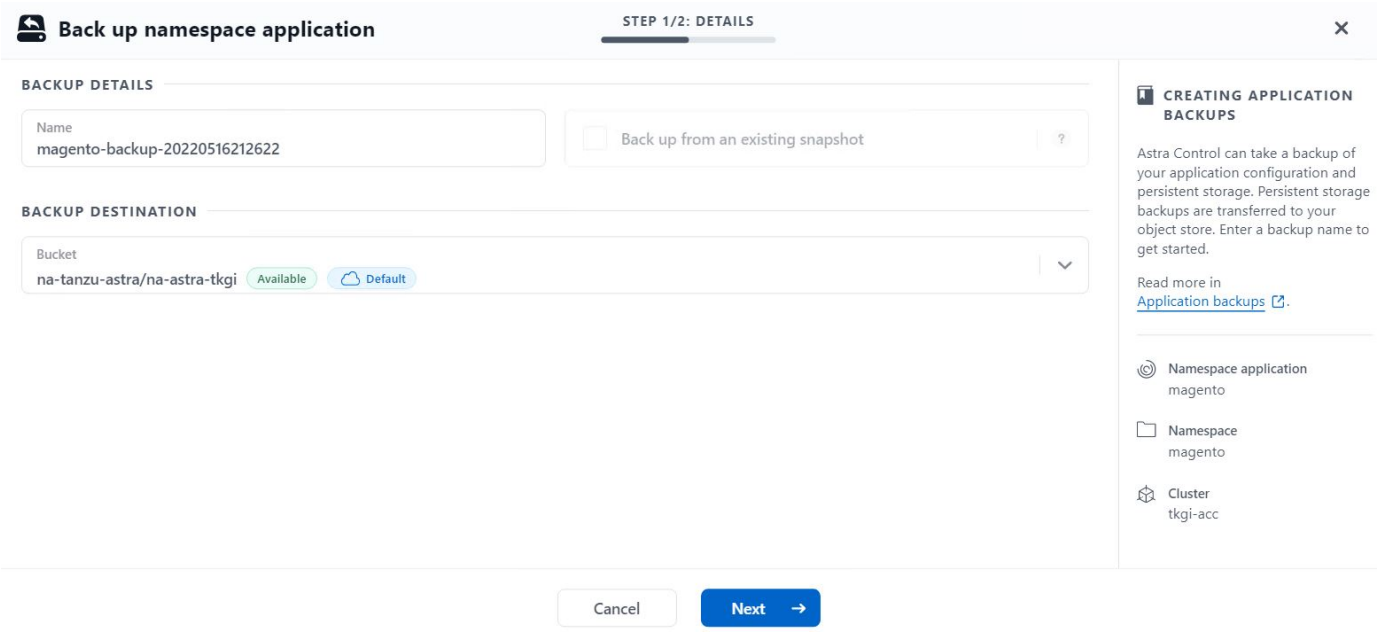
```
ONTAP::> export-policy rule modify -vserver ocp-trident -policyname
default -ruleindex 1 -superuser sys
ONTAP::> export-policy rule modify -policyname default -ruleindex 1
-anon 65534 -vserver ocp-trident
```

2. Pour créer une sauvegarde de l'application gérée dans Astra Control Center, accédez à l'onglet applications > géré et cliquez sur l'application dont vous souhaitez effectuer une sauvegarde. Cliquez sur le menu déroulant en regard du nom de l'application et cliquez sur Sauvegarder.



3. Entrez les détails de la sauvegarde, sélectionnez le compartiment de stockage objet pour contenir les fichiers de sauvegarde, cliquez sur Next (Suivant) et, après avoir vérifié les détails, cliquez sur Backup (Sauvegarder). Selon la taille de l'application et des données, la sauvegarde peut prendre plusieurs

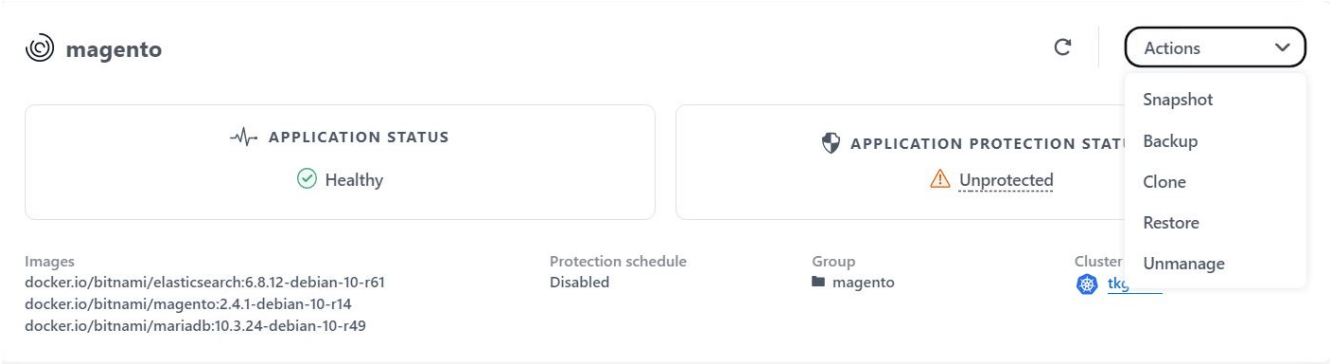
minutes, et l'état de la sauvegarde est disponible une fois la sauvegarde terminée.



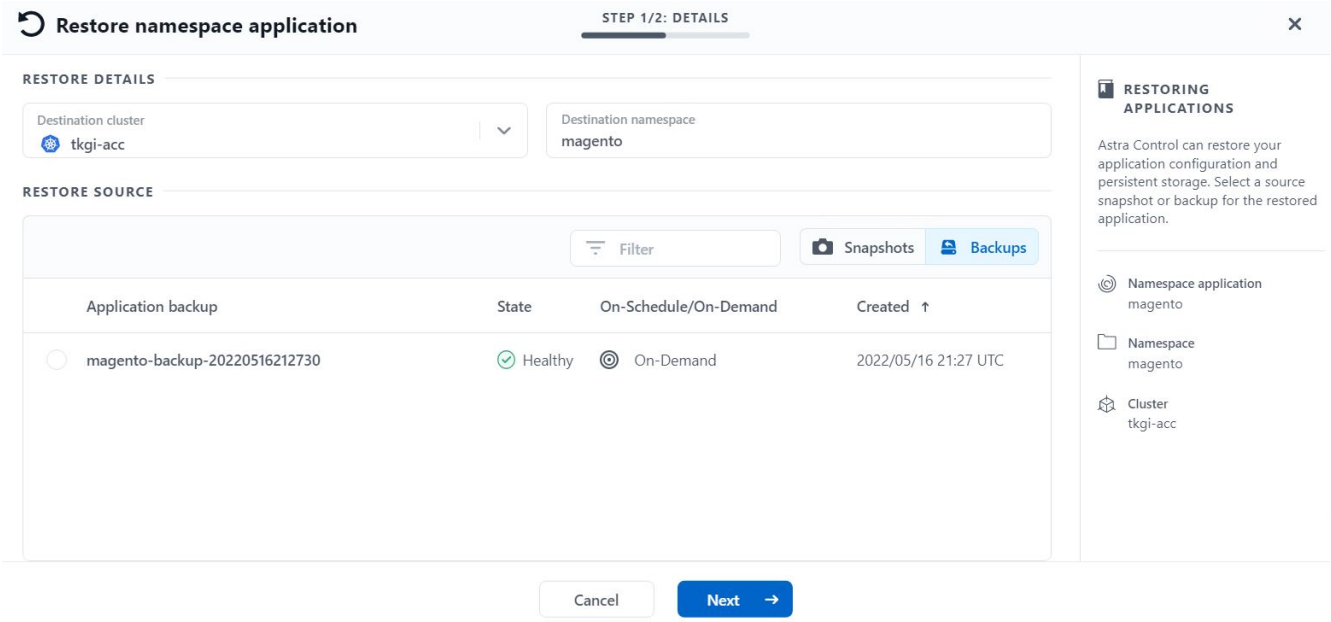
Restauration d'une application

En appuyant sur un bouton, vous pouvez restaurer une application sur l'espace de noms d'origine dans le même cluster ou sur un cluster distant afin d'assurer la protection des applications et la reprise sur incident.

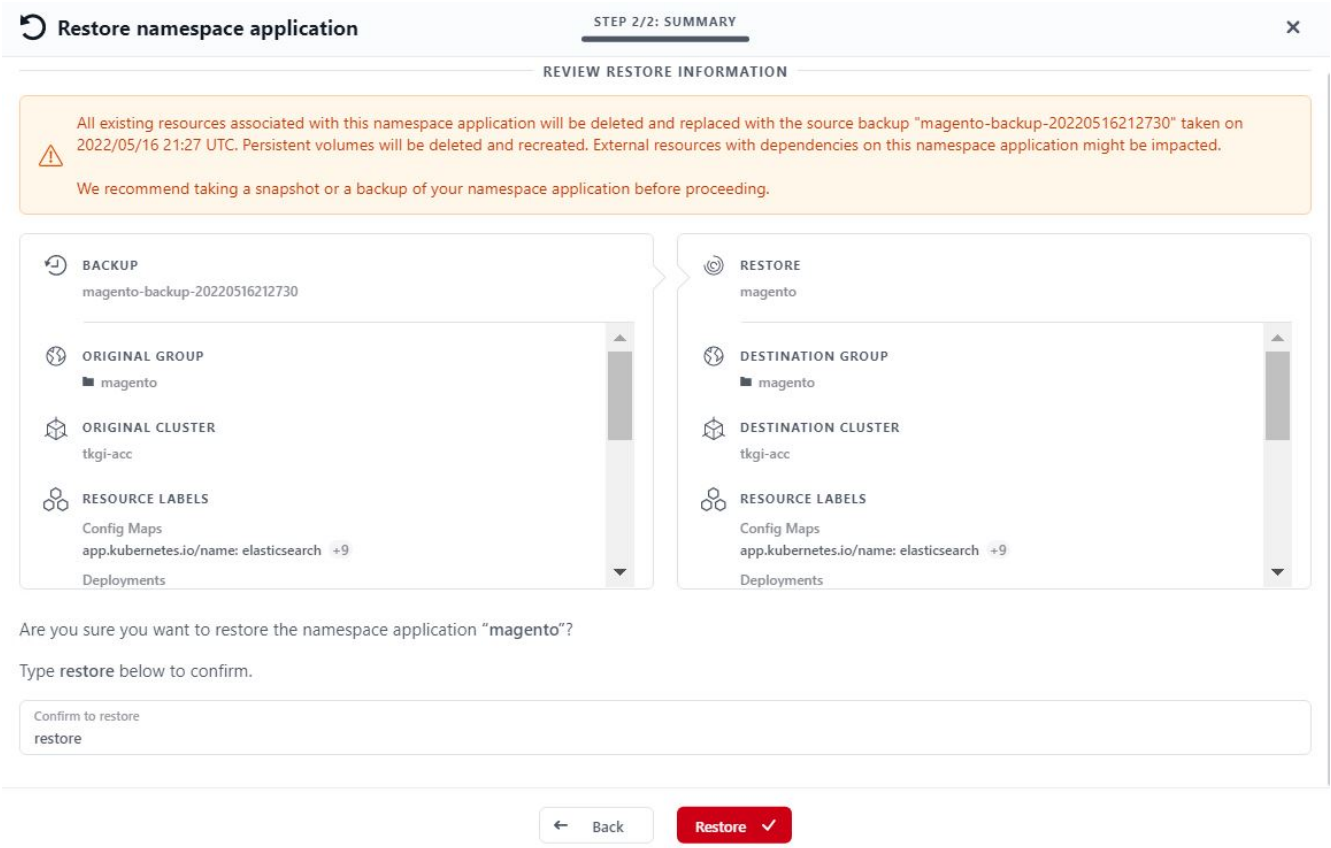
1. Pour restaurer une application, accédez à l'onglet applications > gestion et cliquez sur l'application en question. Cliquez sur le menu déroulant en regard du nom de l'application et cliquez sur Restaurer.



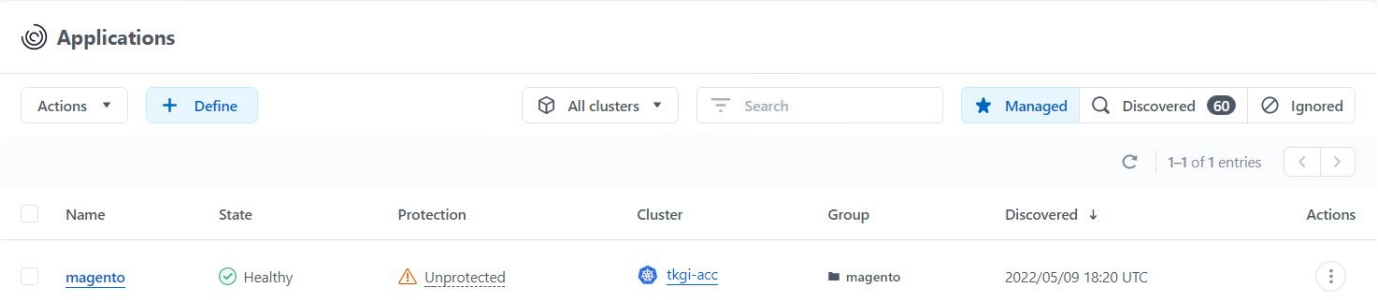
2. Entrez le nom de l'espace de noms de restauration, sélectionnez le cluster vers lequel vous souhaitez le restaurer et choisissez si vous souhaitez le restaurer à partir d'un snapshot existant ou à partir d'une sauvegarde de l'application. Cliquez sur Suivant.



3. Dans le volet de révision, entrez `restore` Puis cliquez sur Restaurer une fois que vous avez examiné les détails.



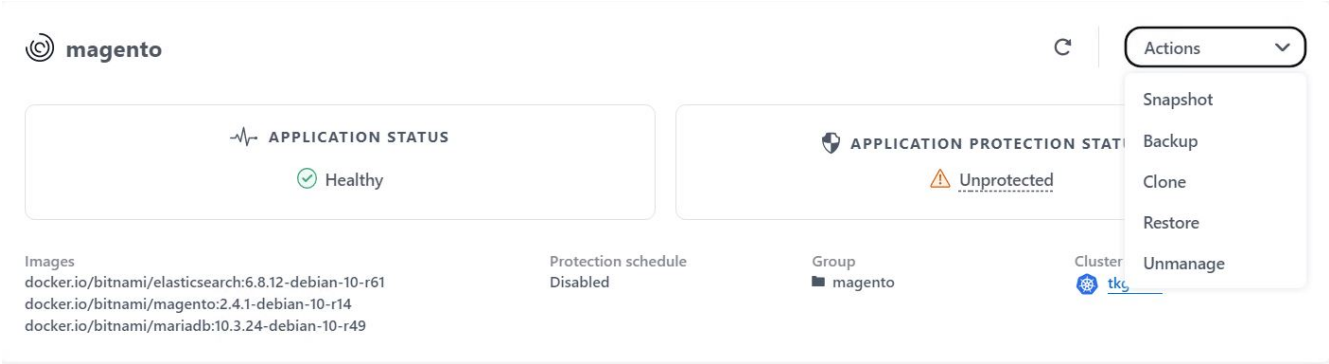
4. La nouvelle application passe à l'état de restauration tandis qu'Astra Control Center restaure l'application sur le cluster sélectionné. Une fois que toutes les ressources de l'application sont installées et détectées par Astra, l'application passe à l'état disponible.



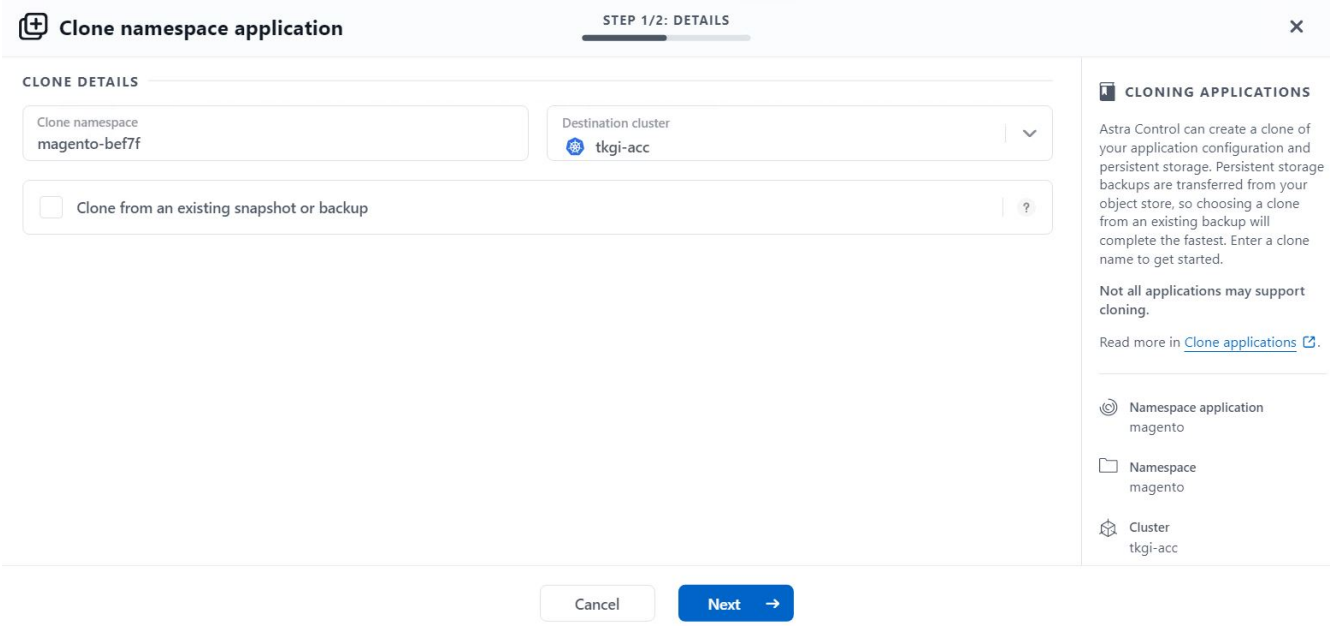
Clonage d'une application

Vous pouvez cloner une application sur le cluster d'origine ou sur un cluster distant à des fins de développement/test ou de protection des applications et de reprise sur incident. Le clonage d'une application au sein d'un même cluster sur le même système back-end utilise la technologie NetApp FlexClone, qui clonez instantanément les demandes de volume persistant et économise de l'espace de stockage.

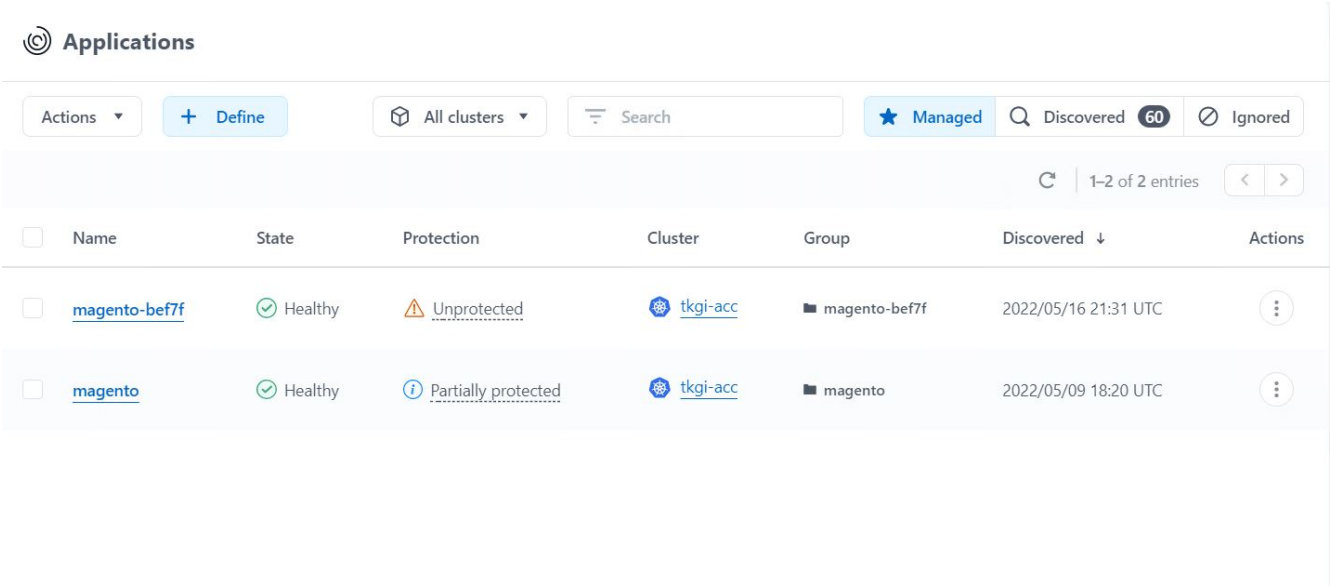
1. Pour cloner une application, accédez à l'onglet applications > gestion et cliquez sur l'application en question. Cliquez sur le menu déroulant en regard du nom de l'application, puis cliquez sur Cloner.



2. Entrez les détails du nouvel espace de noms, sélectionnez le cluster vers lequel vous souhaitez le cloner à partir d'un snapshot existant, puis choisissez si vous souhaitez le cloner à partir d'une sauvegarde ou à partir de l'état actuel de l'application. Cliquez sur Suivant, puis sur Cloner dans le volet de révision une fois que vous avez passé en revue les détails.



3. La nouvelle application passe à l'état découverte tandis que Astra Control Center crée l'application sur le cluster sélectionné. Une fois que toutes les ressources de l'application sont installées et détectées par Astra, l'application passe à l'état disponible.

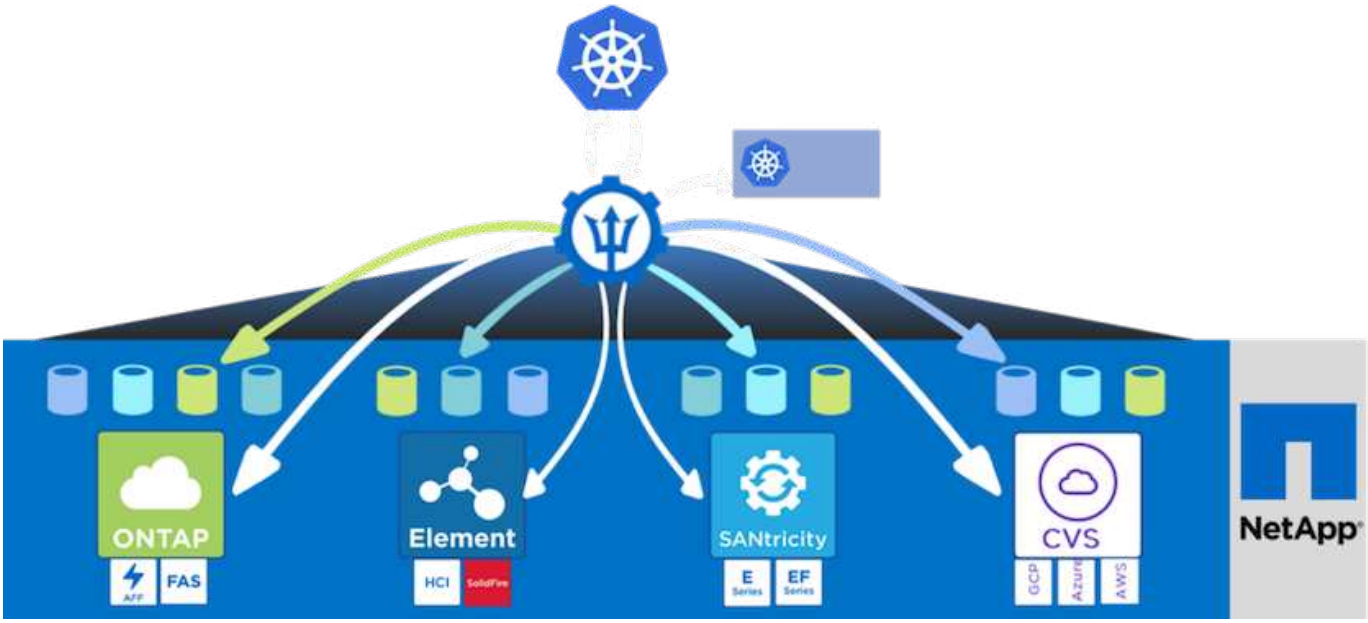


Présentation d'Astra Trident

Astra Trident est un orchestrateur de stockage open source entièrement pris en charge pour les conteneurs et les distributions Kubernetes telles que Red Hat OpenShift, VMware Tanzu, Anthos by Google Cloud, Rancher etc. Trident fonctionne avec l'ensemble de la gamme de solutions de stockage NetApp, notamment les systèmes de stockage NetApp ONTAP et Element, et prend également en charge les connexions NFS et iSCSI. Trident accélère le workflow DevOps en permettant aux utilisateurs d'approvisionner et de gérer le stockage à partir de leurs systèmes de stockage NetApp, sans intervention de l'administrateur de stockage.

Un administrateur peut configurer plusieurs systèmes de stockage back-end en fonction des besoins des projets et des modèles de système de stockage. Ces fonctionnalités permettent notamment la compression, des types de disques spécifiques ou des niveaux de QoS garantissant un certain niveau de performance. Une

fois définis, ces systèmes back-end peuvent être utilisés par les développeurs dans leurs projets pour créer des demandes de volume persistant et connecter le stockage persistant à la demande dans leurs conteneurs.



Astra Trident a un cycle de développement rapide et, comme Kubernetes, est lancé quatre fois par an.

La dernière version d'Astra Trident est disponible en avril 22.04, en avril 2022. Une matrice de prise en charge pour quelle version de Trident a été testée avec laquelle une distribution Kubernetes est disponible "ici".

Depuis la version 20.04, l'opérateur Trident effectue la configuration de Trident. L'opérateur facilite les déploiements à grande échelle et offre un support supplémentaire, notamment l'auto-rétablissement des pods déployés dans le cadre de l'installation de Trident.

Avec la version 21.01, un graphique Helm a été disponible pour faciliter l'installation de l'opérateur Trident.

Déploiement de l'opérateur Trident à l'aide de Helm

1. Définissez tout d'abord l'emplacement du cluster utilisateur `kubeconfig` Fichier en tant que variable d'environnement pour que vous n'ayez pas à le référencer, car Trident n'a pas d'option pour transmettre ce fichier.

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

2. Ajoutez le référentiel NetApp Astra Trident Helm.

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

3. Mettre à jour les référentiels Helm.

```
[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. Créez un nouvel espace de nom pour l'installation de Trident.

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

5. Créez un secret avec les informations d'identification DockerHub pour télécharger les images Astra Trident.

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

6. Pour les clusters utilisateur ou de charge de travail gérés par TKGS (vSphere avec Tanzu) ou TKG avec des déploiements de clusters de gestion, procédez comme suit pour installer Astra Trident :
   a. Assurez-vous que l'utilisateur connecté dispose des autorisations nécessaires pour créer des comptes de service dans l'espace de noms trident et que les comptes de service dans l'espace de noms trident disposent des autorisations de créer des pods.
   b. Exécutez la commande ci-dessous Helm pour installer l'opérateur Trident dans l'espace de noms créé.

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

7. Pour un cluster utilisateur ou de charge de travail géré par des déploiements TKGI, exécutez la commande Helm suivante pour installer l'opérateur Trident dans l'espace de noms créé.

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

8. Vérifiez que les modules Trident sont opérationnels.

```
NAME                                READY   STATUS    RESTARTS
AGE
trident-csi-6vv62                   2/2     Running   0
14m
trident-csi-cfd844bcc-sqhcg         6/6     Running   0
12m
trident-csi-dfcmz                   2/2     Running   0
14m
trident-csi-pb2n7                   2/2     Running   0
14m
trident-csi-qsw6z                   2/2     Running   0
14m
trident-operator-67c94c4768-xw978   1/1     Running   0
14m

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

Création de systèmes back-end de stockage

Une fois l'installation d'Astra Trident Operator, vous devez configurer le système back-end pour la plateforme de stockage NetApp spécifique que vous utilisez. Suivez les liens ci-dessous pour poursuivre l'installation et la configuration d'Astra Trident.

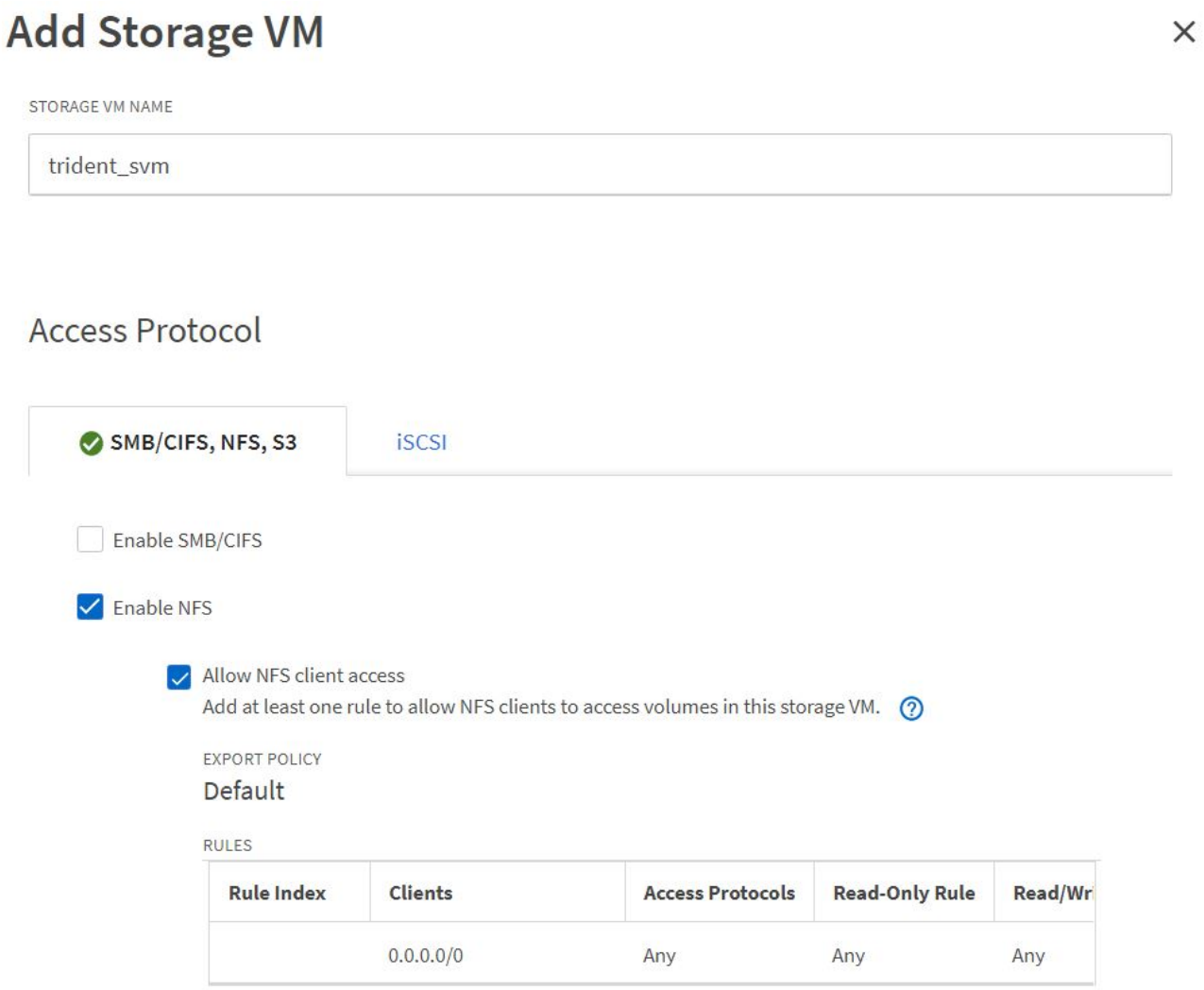
- "NetApp ONTAP NFS"
- "ISCSI NetApp ONTAP"

Configuration NetApp ONTAP NFS

Pour activer l'intégration de Trident avec le système de stockage NetApp ONTAP via NFS, vous devez créer un système back-end permettant la communication avec le système de stockage. Nous configurons un back-end de base dans cette solution, mais si vous cherchez des options plus personnalisées, consultez la documentation "ici".

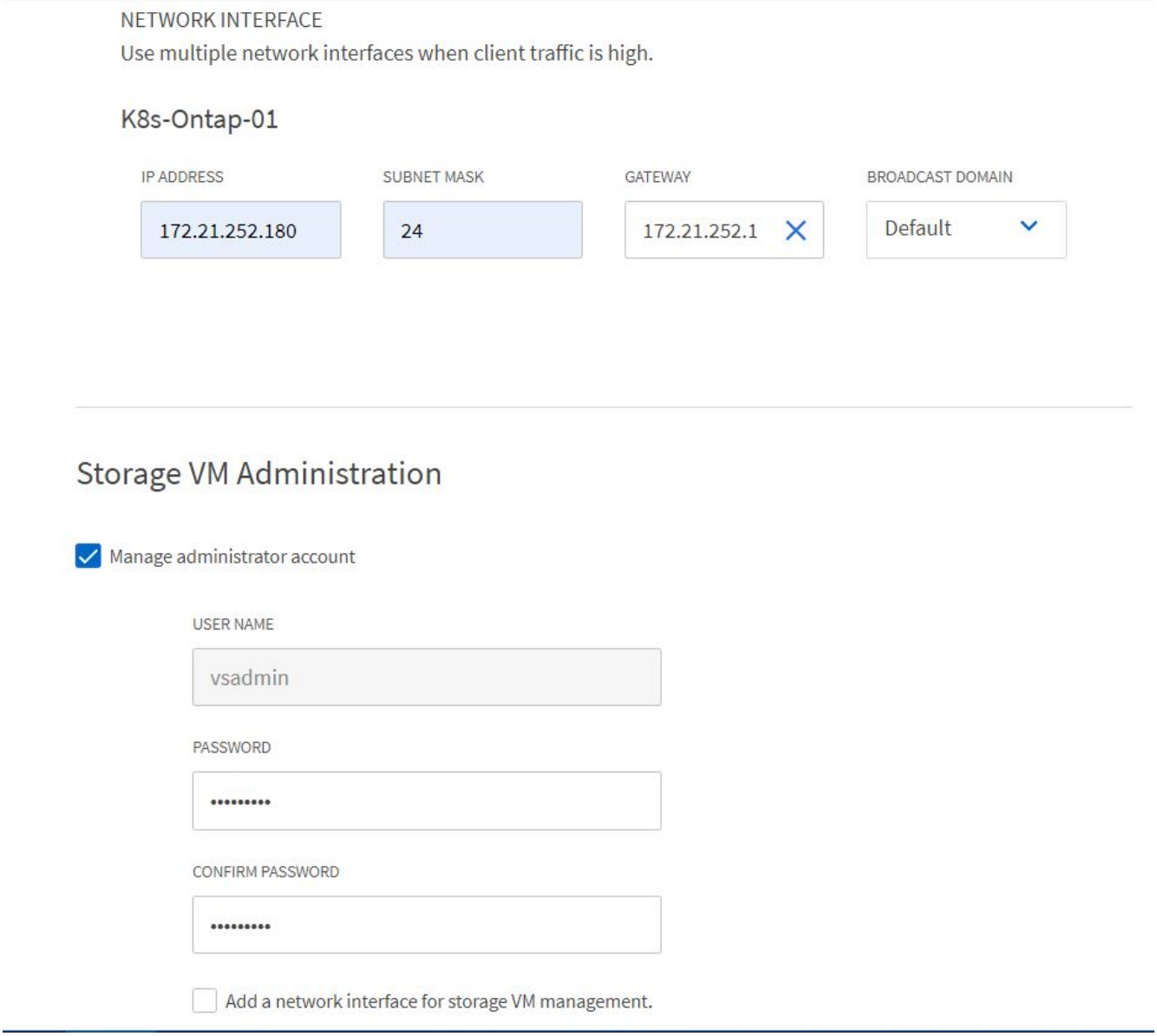
Créer un SVM en ONTAP

1. Connectez-vous à ONTAP System Manager, accédez à Storage > Storage VM, puis cliquez sur Add.
2. Entrez un nom pour la SVM, activez le protocole NFS, cochez la case Autoriser NFS client Access et ajoutez les sous-réseaux sur lesquels sont situés les nœuds workers dans les règles d'export pour que les volumes soient montés en tant que PV dans les clusters de vos charges de travail.

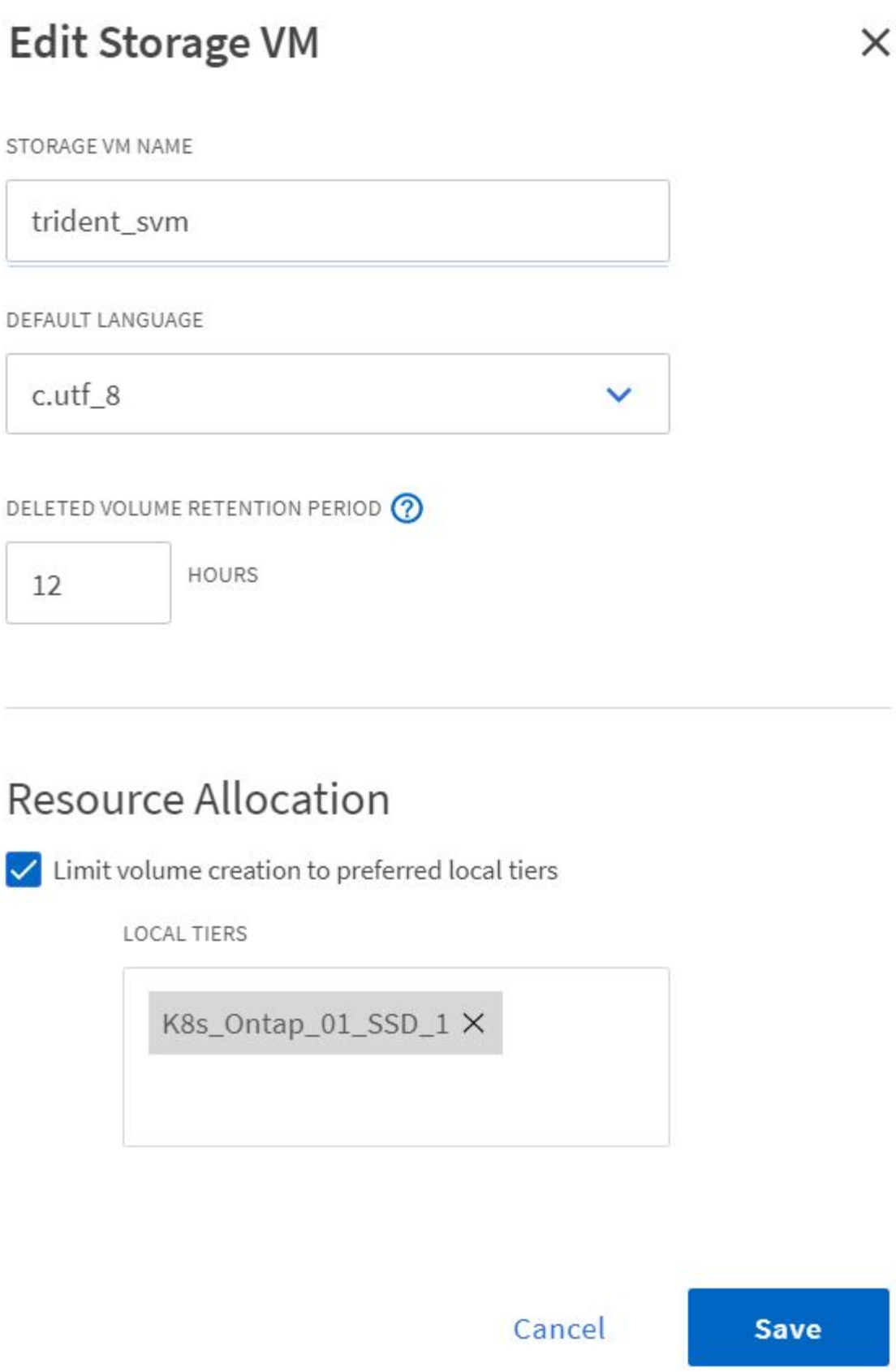


> Si vous utilisez le déploiement NAT'ed de clusters utilisateur ou de clusters de charge de travail avec NSX-T, vous devez ajouter le sous-réseau Egress (dans le cas de GSTK0 ou du sous-réseau IP flottant (dans le cas de TKGI) aux règles de politique d'exportation.

3. Fournir le détail des LIFs de données et les détails du compte d'administration des SVM, puis cliquer sur Save.



4. Assigner les agrégats à un SVM. Accédez à Storage > Storage VM, cliquez sur les points de suspension situés à côté du SVM qui vient d'être créé, puis cliquez sur Modifier. Cochez la case limiter la création de volume aux niveaux locaux préférés et joignez les agrégats requis à ceux-ci.



5. Dans le cas de déploiements NAT de clusters d'utilisateurs ou de workloads sur lesquels Trident doit être installé, la demande de montage du stockage peut arriver à partir d'un port non standard du fait de SNAT. Par défaut, ONTAP autorise uniquement les demandes de montage de volume quand provient du port

racine. Ainsi, connectez-vous à l'interface de ligne de commandes de ONTAP et modifiez le paramètre pour autoriser les demandes de montage à partir de ports non standard.

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

Création de systèmes back-end et de classes de stockage

1. Pour les systèmes NetApp ONTAP qui utilisent NFS, créez un fichier de configuration interne sur le jump avec la postname, degestion LIF, dataLIF, svm, nom d'utilisateur, mot de passe et autres détails.

```
{
    "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"
}
```

> Il est recommandé de définir la valeur backendName personnalisée comme combinaison du storageDriverName et de la dataLIF qui sert NFS pour une identification facile.

2. Créez le back-end Trident en exécutant la commande suivante.

```
[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. Lorsque le back-end est créé, vous devez ensuite créer une classe de stockage. L'exemple de définition de classe de stockage suivant met en évidence les champs requis et de base. Le paramètre `backendType` Doit refléter le pilote de stockage du nouveau système back-end Trident créé.

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

4. Créez la classe de stockage en exécutant la commande kubectl.

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

5. Une fois la classe de stockage créée, vous devez ensuite créer la première demande de volume persistant. Un exemple de définition de PVC est donné ci-dessous. Assurez-vous que le `storageClassName` le champ correspond au nom de la classe de stockage que vous venez de créer. La définition du volume persistant peut être personnalisée davantage selon les besoins, en fonction de la charge de travail à provisionner.

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

6. Créez la demande de volume persistant en exécutant la commande kubectl. La création peut prendre un certain temps en fonction de la taille du volume de sauvegarde en cours de création, de sorte que vous pouvez regarder le processus au fur et à mesure qu'il se termine.

```
[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
```

Configuration ONTAP iSCSI de NetApp

Pour intégrer le système de stockage NetApp ONTAP avec des clusters Kubernetes VMware Tanzu pour les volumes persistants via iSCSI, la première étape consiste à préparer les nœuds en vous connectant à chaque nœud et en configurant les utilitaires ou packages iSCSI pour le montage des volumes iSCSI. Pour ce faire, suivre la procédure décrite dans ce document "lien".

> NetApp ne recommande pas cette procédure pour les déploiements NAT des clusters VMware Tanzu Kubernetes.

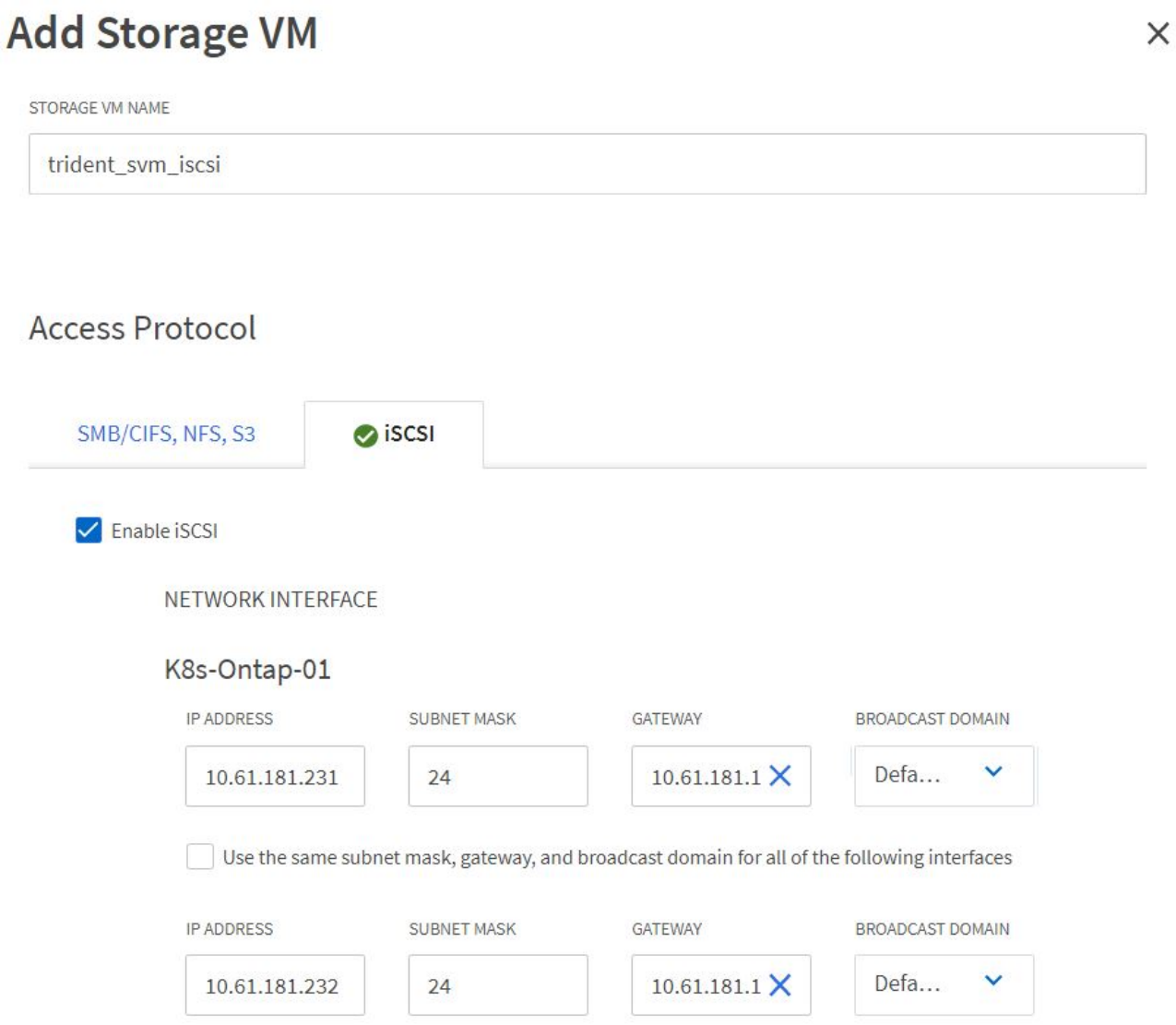
> TKGI utilise les machines virtuelles Bosh comme nœuds pour les clusters Kubernetes tanzu qui exécutent des images de configuration immuables, et toute modification manuelle des packages iSCSI sur les machines virtuelles Bosh n'est pas conservée d'un redémarrage à l'autre. Par conséquent, NetApp recommande d'utiliser des volumes NFS pour le stockage persistant des clusters Kubernetes tanzu déployés et gérés par TKGI.

Une fois les nœuds de cluster prêts pour les volumes iSCSI, vous devez créer un back-end permettant la communication avec le système de stockage. Nous avons configuré un back-end de base dans cette solution, mais si vous cherchez des options plus personnalisées, consultez la documentation "ici".

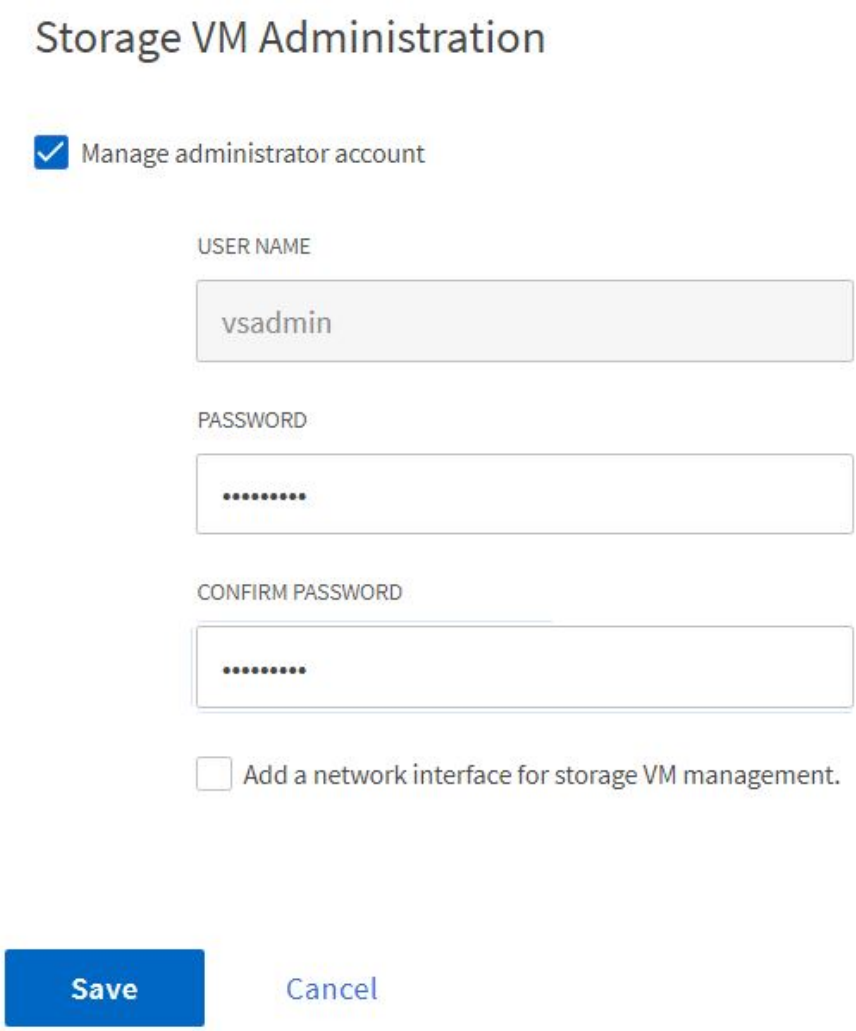
Créer un SVM en ONTAP

Pour créer un SVM dans ONTAP, effectuez la procédure suivante :

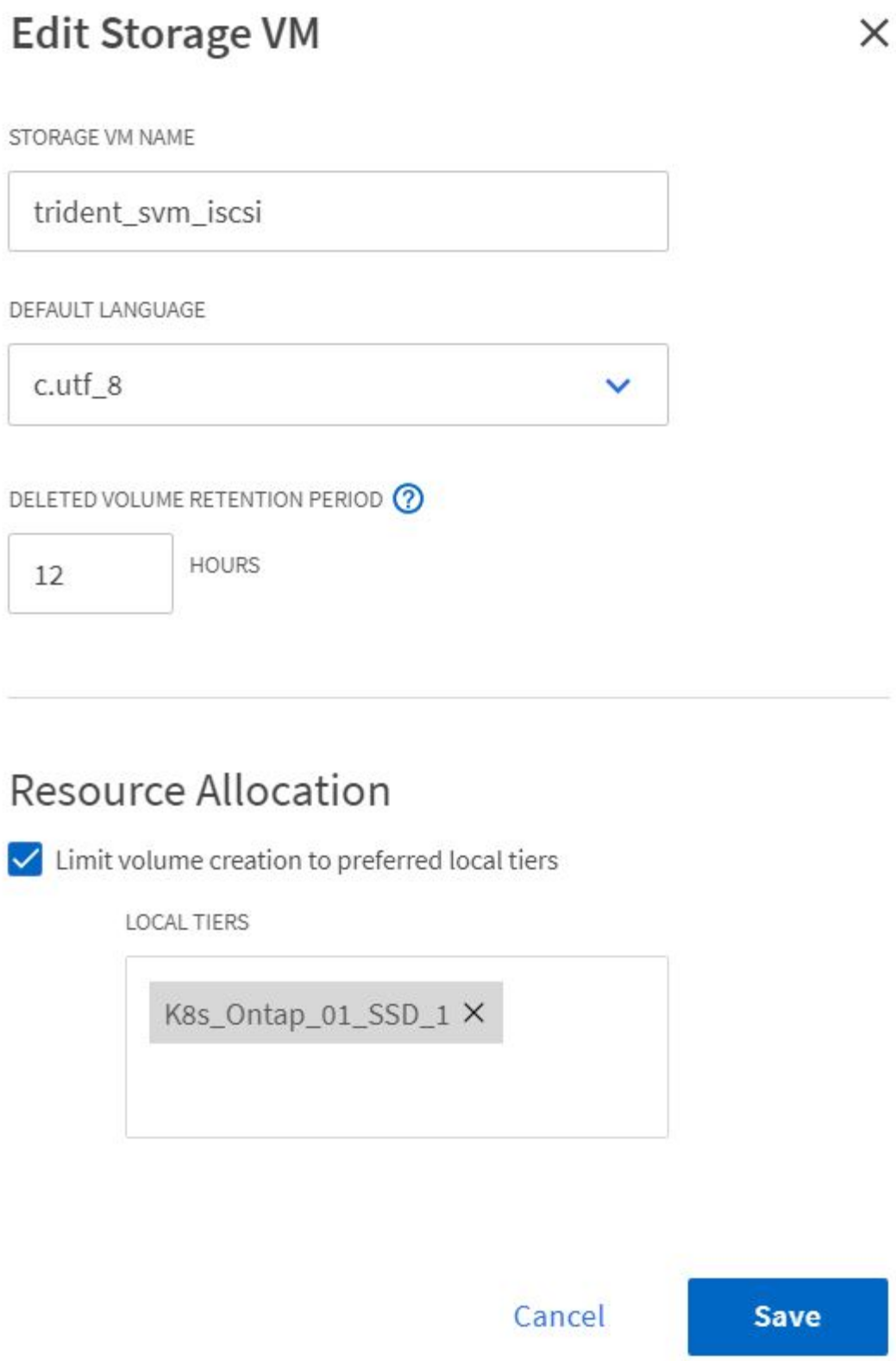
1. Connectez-vous à ONTAP System Manager, accédez à Storage > Storage VM, puis cliquez sur Add.
2. Entrer un nom pour le SVM, activer le protocole iSCSI, puis fournir le détail des LIFs de données.



3. Entrez les détails du compte d'administration du SVM, puis cliquez sur Save.



4. Pour attribuer les agrégats au SVM, accédez à Storage > Storage VM, puis cliquez sur les points de suspension situés à côté du SVM qui vient d'être créé, puis cliquez sur Modifier. Cochez la case limiter la création de volume aux niveaux locaux préférés et joignez les agrégats requis à ceux-ci.



Création de systèmes back-end et de classes de stockage

1. Pour les systèmes NetApp ONTAP qui utilisent NFS, créez un fichier de configuration interne sur le jump avec la postname, degestion LIF, dataLIF, svm, nom d'utilisateur, mot de passe et autres détails.

```
{
  "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. Créez le back-end Trident en exécutant la commande suivante.

```
[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. Une fois que vous avez créé un back-end, vous devez ensuite créer une classe de stockage. L'exemple de définition de classe de stockage suivant met en évidence les champs requis et de base. Le paramètre `backendType` Doit refléter le pilote de stockage du nouveau système back-end Trident créé. Notez également la valeur nom-champ, qui doit être référencée ultérieurement.

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

> Il y a un champ facultatif appelé `fsType` qui est défini dans ce fichier. Dans les systèmes back-end iSCSI, cette valeur peut être définie sur un type de système de fichiers Linux spécifique (XFS, ext4, etc.) ou peut être supprimée pour permettre aux clusters Kubernetes tanzu de décider du système de fichiers à utiliser.

4. Créez la classe de stockage en exécutant la commande kubectl.

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

5. Une fois la classe de stockage créée, vous devez ensuite créer la première demande de volume persistant. Un exemple de définition de PVC est donné ci-dessous. Assurez-vous que le `storageClassName` le champ correspond au nom de la classe de stockage que vous venez de créer. La définition du volume persistant peut être personnalisée davantage selon les besoins, en fonction de la charge de travail à provisionner.

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

6. Créez la demande de volume persistant en exécutant la commande kubectl. La création peut prendre un certain temps en fonction de la taille du volume de sauvegarde en cours de création, de sorte que vous pouvez regarder le processus au fur et à mesure qu'il se termine.

```
[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-7ceac1ba-0189-43c7-8f98-094719f7956c   1Gi
RWO            ontap-iscsi      3s
```