Openshift pour sur site

NetApp public and hybrid cloud solutions

NetApp
August 18, 2025

Sommaire

Openshift pour sur site

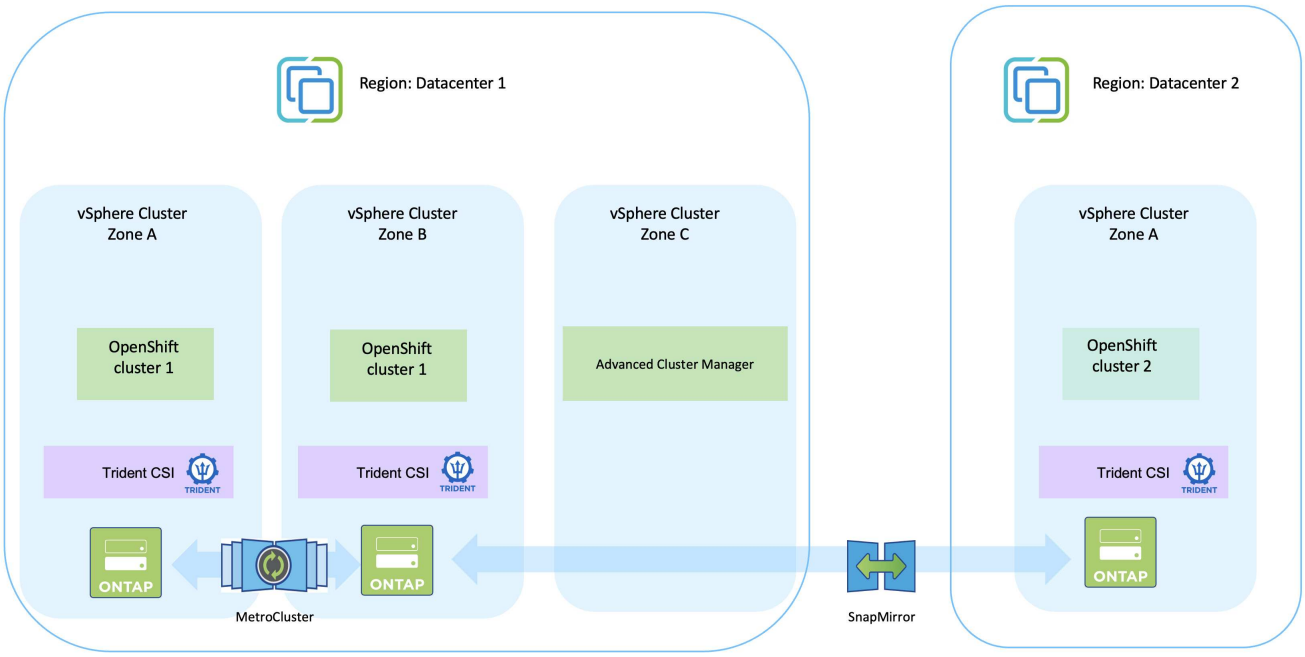
Solution NetApp avec charges de travail de la plateforme de conteneurs Red Hat OpenShift sur VMware

Si les clients ont besoin d'exécuter leurs applications conteneurisées modernes sur l'infrastructure de leurs centres de données privés, ils peuvent le faire. Ils doivent planifier et déployer la plateforme de conteneurs Red Hat OpenShift (OCP) pour un environnement prêt pour la production afin de déployer leurs charges de travail de conteneurs. Leurs clusters OCP peuvent être déployés sur VMware ou sur du bare metal.

Le stockage NetApp ONTAP offre une protection des données, une fiabilité et une flexibilité pour les déploiements de conteneurs. Trident sert de fournisseur de stockage dynamique pour consommer le stockage ONTAP persistant pour les applications avec état des clients. NetApp Trident Protect peut être utilisé pour les nombreuses exigences de gestion des données des applications avec état telles que la protection des données, la migration et la continuité des activités.

Avec VMware vSphere, les outils NetApp ONTAP fournissent un plug-in vCenter qui peut être utilisé pour provisionner des banques de données. Appliquez des balises et utilisez-les avec OpenShift pour stocker la configuration et les données du nœud. Le stockage basé sur NVMe offre une latence plus faible et des performances élevées.

Solution de protection et de migration des données pour les charges de travail OpenShift Container à l'aide de Trident Protect

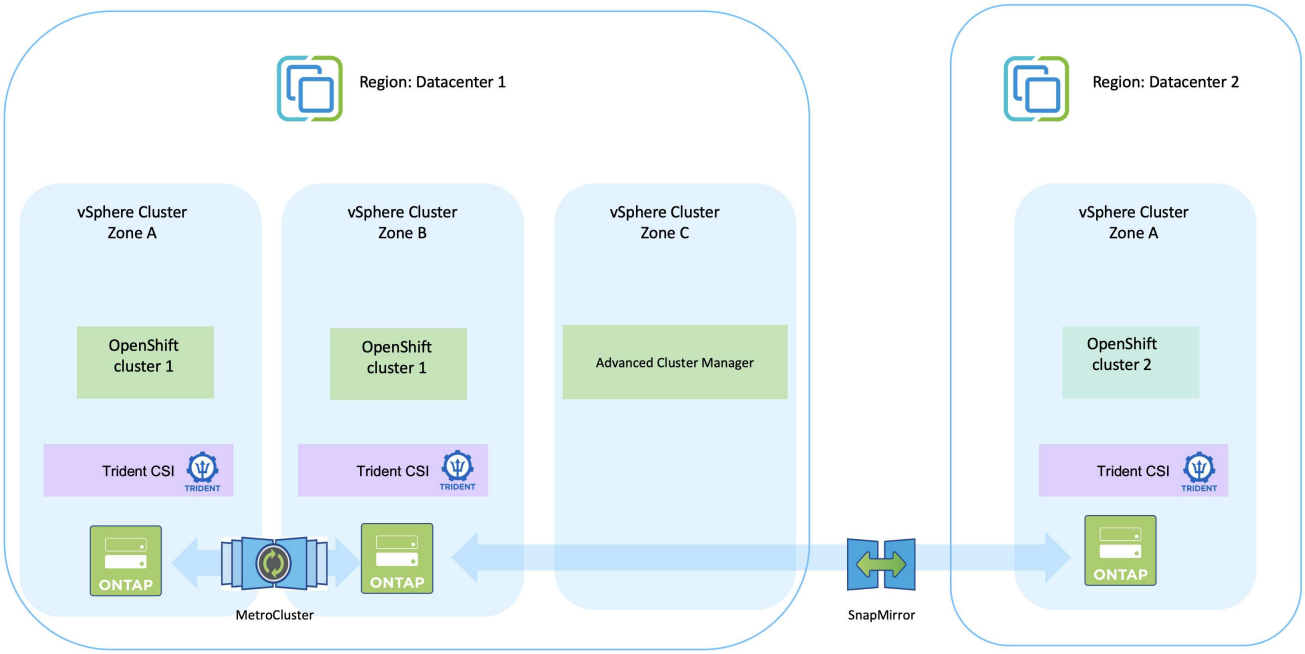


Déployer et configurer la plateforme Red Hat OpenShift Container sur VMware

Cette section décrit un flux de travail de haut niveau sur la façon de configurer et de gérer les clusters OpenShift et de gérer les applications avec état sur eux. Il montre l'utilisation des baies de stockage NetApp ONTAP avec l'aide de Trident pour fournir des volumes persistants.

Il existe plusieurs façons de déployer des clusters de plateforme Red Hat OpenShift Container. Cette description de haut niveau de la configuration fournit des liens de documentation pour la méthode spécifique qui a été utilisée. Vous pouvez vous référer aux autres méthodes dans les liens pertinents fournis dans le"section ressources" .

Voici un diagramme qui illustre les clusters déployés sur VMware dans un centre de données.



Le processus de configuration peut être décomposé selon les étapes suivantes :

Déployer et configurer une machine virtuelle CentOS

- Il est déployé dans l'environnement VMware vSphere.
- Cette machine virtuelle est utilisée pour déployer certains composants tels que NetApp Trident et NetApp Trident Protect pour la solution.
- Un utilisateur root est configuré sur cette machine virtuelle lors de l'installation.

Déployer et configurer un cluster OpenShift Container Platform sur VMware vSphere (Hub Cluster)

Reportez-vous aux instructions pour le"Déploiement assisté" méthode pour déployer un cluster OCP.

N'oubliez pas ce qui suit : - Créez une clé publique et privée SSH à fournir au programme d'installation. Ces clés seront utilisées pour se connecter aux nœuds maître et travailleur si nécessaire. - Téléchargez le programme d'installation à partir de l'installateur assisté. Ce programme est utilisé pour démarrer les machines virtuelles que vous créez dans l'environnement VMware vSphere pour les nœuds maître et travailleur. - Les machines virtuelles doivent avoir les exigences minimales en matière de CPU, de mémoire et de disque dur. (Reportez-vous aux commandes vm create sur"ce" (page pour le maître et les nœuds de travail qui fournissent ces informations) - Le diskUUID doit être activé sur toutes les machines virtuelles. - Créez un minimum de 3 nœuds pour le maître et 3 nœuds pour le travailleur. - Une fois qu'ils sont découverts par le programme d'installation, activez le bouton bascule d'intégration VMware vSphere.

Installer Advanced Cluster Management sur le cluster Hub

Ceci est installé à l'aide de l'opérateur de gestion de cluster avancé sur le cluster Hub. Se référer aux instructions"ici" .

Installer deux clusters OCP supplémentaires (source et destination)

- Les clusters supplémentaires peuvent être déployés à l'aide de l'ACM sur le cluster Hub.
- Se référer aux instructions"ici" .

Configurer le stockage NetApp ONTAP

- Installez un cluster ONTAP avec connectivité aux machines virtuelles OCP dans l'environnement VMWare.
- Créer un SVM.
- Configurez NAS Data Lif pour accéder au stockage dans SVM.

Installer NetApp Trident sur les clusters OCP

- Installez NetApp Trident sur les trois clusters : clusters hub, source et de destination
- Se référer aux instructions"ici" .
- Créez un backend de stockage pour ontap-nas .
- Créez une classe de stockage pour ontap-nas.
- Se référer aux instructions"ici" .

Déployer une application sur le cluster source

Utilisez OpenShift GitOps pour déployer une application. (par exemple Postgres, Ghost)

L'étape suivante consiste à utiliser Trident Protect pour la protection des données et la migration des données du cluster source vers le cluster de destination. Référer"ici" pour les instructions.

Protection des données avec Astra

Cette page présente les options de protection des données pour les applications basées sur Red Hat OpenShift Container exécutées sur VMware vSphere à l'aide de Trident Protect (ACC).

À mesure que les utilisateurs modernisent leurs applications avec Red Hat OpenShift, une stratégie de protection des données doit être mise en place pour les protéger contre toute suppression accidentelle ou toute autre erreur humaine. Souvent, une stratégie de protection est également requise à des fins réglementaires ou de conformité pour protéger leurs données contre une catastrophe.

Les exigences en matière de protection des données varient du retour à une copie ponctuelle au basculement automatique vers un autre domaine de panne sans aucune intervention humaine. De nombreux clients choisissent ONTAP comme plate-forme de stockage préférée pour leurs applications Kubernetes en raison de ses fonctionnalités riches telles que la multilocation, le multiprotocole, les offres de hautes performances et de capacité, la réplication et la mise en cache pour les emplacements multisites, la sécurité et la flexibilité.

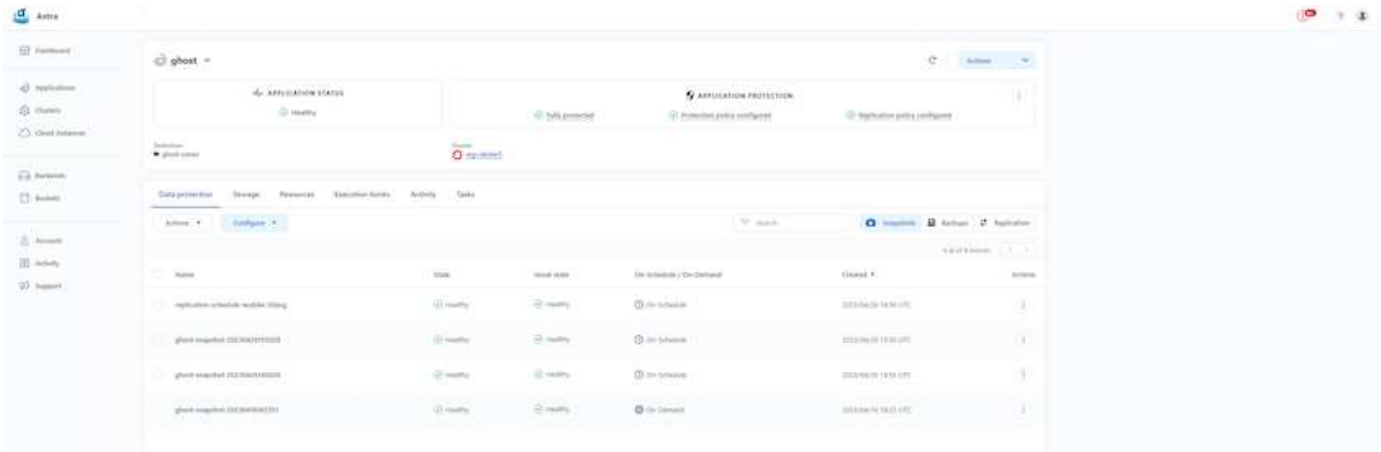
La protection des données dans ONTAP peut être obtenue à l'aide de **Snapshot** ad hoc ou contrôlé par des politiques - **sauvegarde et restauration**

Les copies instantanées et les sauvegardes protègent les types de données suivants : - **Les métadonnées de l'application qui représentent l'état de l'application** - **Tous les volumes de données persistants associés à l'application** - **Tous les artefacts de ressources appartenant à l'application**

Instantané avec ACC

Une copie ponctuelle des données peut être capturée à l'aide de Snapshot avec ACC. La politique de protection définit le nombre de copies Snapshot à conserver. L'option d'horaire minimum disponible est horaire. Des copies instantanées manuelles à la demande peuvent être effectuées à tout moment et à des intervalles plus courts que les copies instantanées planifiées. Les copies instantanées sont stockées sur le même volume provisionné que l'application.

Configuration de Snapshot avec ACC

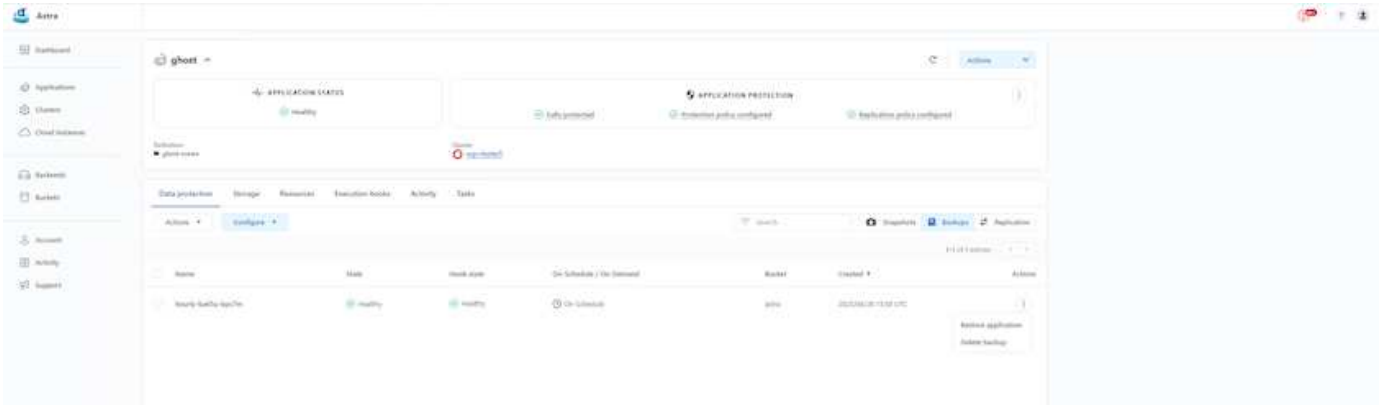


Sauvegarde et restauration avec ACC

Une sauvegarde est basée sur un instantané. Trident Protect peut prendre des copies instantanées à l'aide de CSI et effectuer une sauvegarde à l'aide de la copie instantanée à un moment donné. La sauvegarde est stockée dans un magasin d'objets externe (tout compatible s3, y compris ONTAP S3 à un emplacement différent). La politique de protection peut être configurée pour les sauvegardes planifiées et le nombre de versions de sauvegarde à conserver. Le RPO minimum est d'une heure.

Restauration d'une application à partir d'une sauvegarde à l'aide d'ACC

ACC restaure l'application à partir du compartiment S3 où les sauvegardes sont stockées.



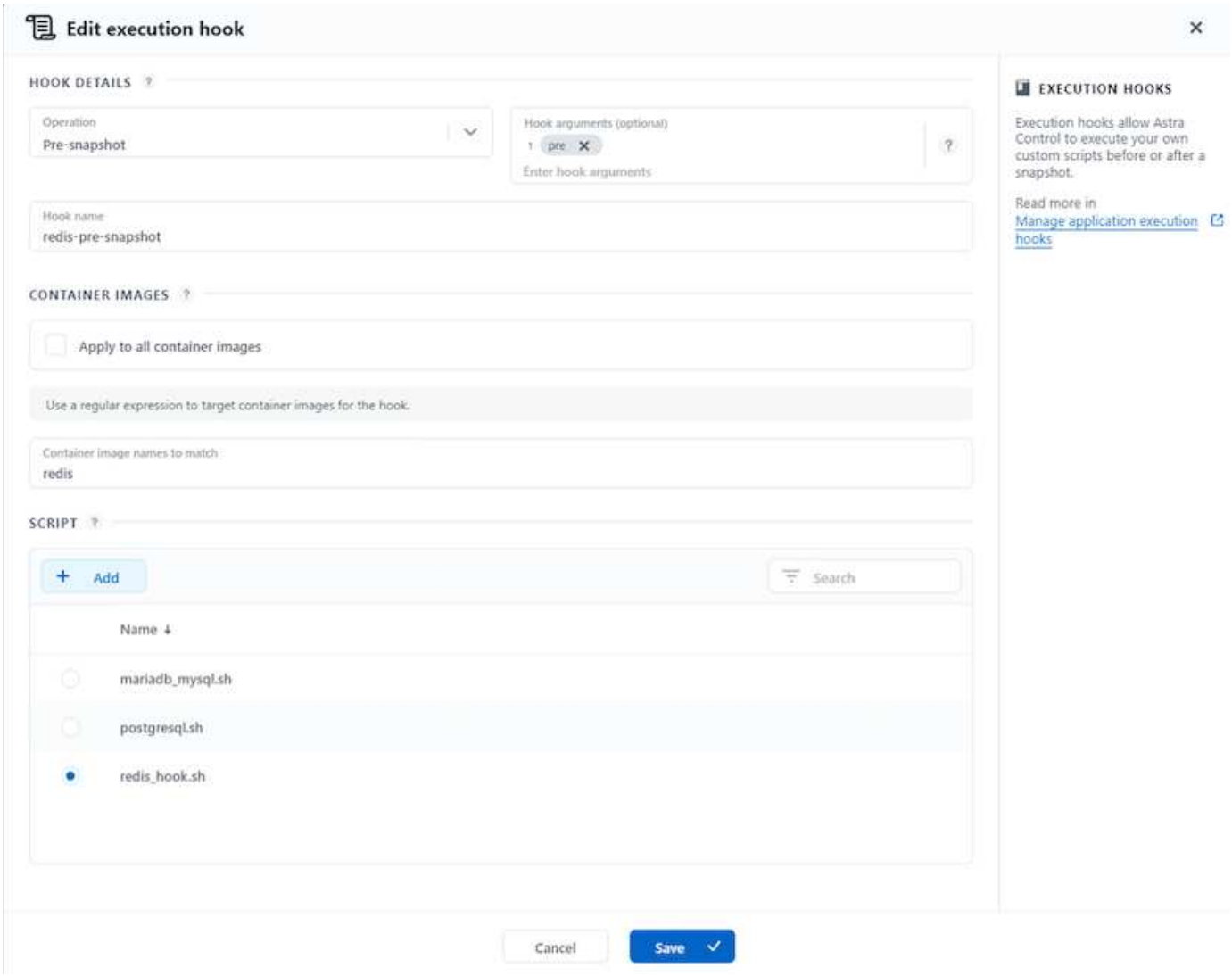
Hooks d'exécution spécifiques à l'application

De plus, les hooks d'exécution peuvent être configurés pour s'exécuter conjointement avec une opération de protection des données d'une application gérée. Même si des fonctionnalités de protection des données au niveau de la baie de stockage sont disponibles, des étapes supplémentaires sont souvent nécessaires pour effectuer des sauvegardes et des restaurations cohérentes avec les applications. Les étapes supplémentaires spécifiques à l'application peuvent être : - avant ou après la création d'une copie instantanée. - avant ou après la création d'une sauvegarde. - après la restauration à partir d'une copie instantanée ou d'une sauvegarde.

Astra Control peut exécuter ces étapes spécifiques à l'application codées sous forme de scripts personnalisés appelés hooks d'exécution.

"Projet GitHub NetApp Verda"fournit des hooks d'exécution pour les applications cloud natives populaires afin de rendre la protection des applications simple, robuste et facile à orchestrer. N'hésitez pas à contribuer à ce projet si vous disposez de suffisamment d'informations pour une application qui ne figure pas dans le référentiel.

Exemple de hook d'exécution pour le pré-snapshot d'une application redis.



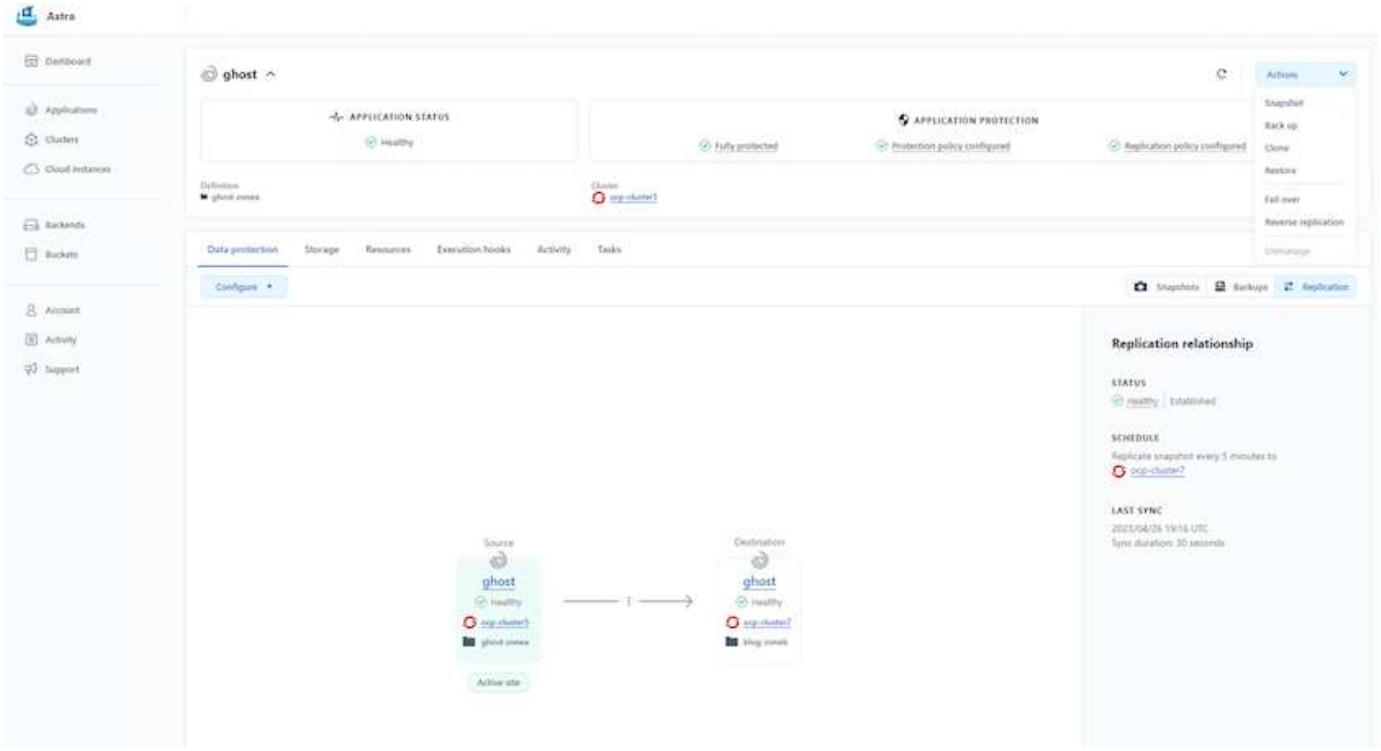
Réplication avec ACC

Pour une protection régionale ou pour une solution RPO et RTO faible, une application peut être répliquée sur une autre instance Kubernetes exécutée sur un site différent, de préférence dans une autre région. Trident Protect utilise ONTAP async SnapMirror avec un RPO aussi bas que 5 minutes. La réplication est effectuée en répliquant vers ONTAP , puis un basculement crée les ressources Kubernetes dans le cluster de destination.

> Notez que la réplication est différente de la sauvegarde et de la restauration où la sauvegarde va vers S3 et la restauration est effectuée à partir de S3. Consultez le lien : https://docs.netapp.com/us-en/astra-control-center/concepts/data-protection.html#replication-to-a-remote-cluster [ici] pour obtenir des détails supplémentaires sur les différences entre les deux types de protection des données.

Référer"ici" pour les instructions de configuration de SnapMirror .

SnapMirror avec ACC



Les pilotes de stockage san-economy et nas-economy ne prennent pas en charge la fonction de réplication. Référer"ici" pour plus de détails.

Vidéo de démonstration :

"Vidéo de démonstration de reprise après sinistre avec Trident Protect"

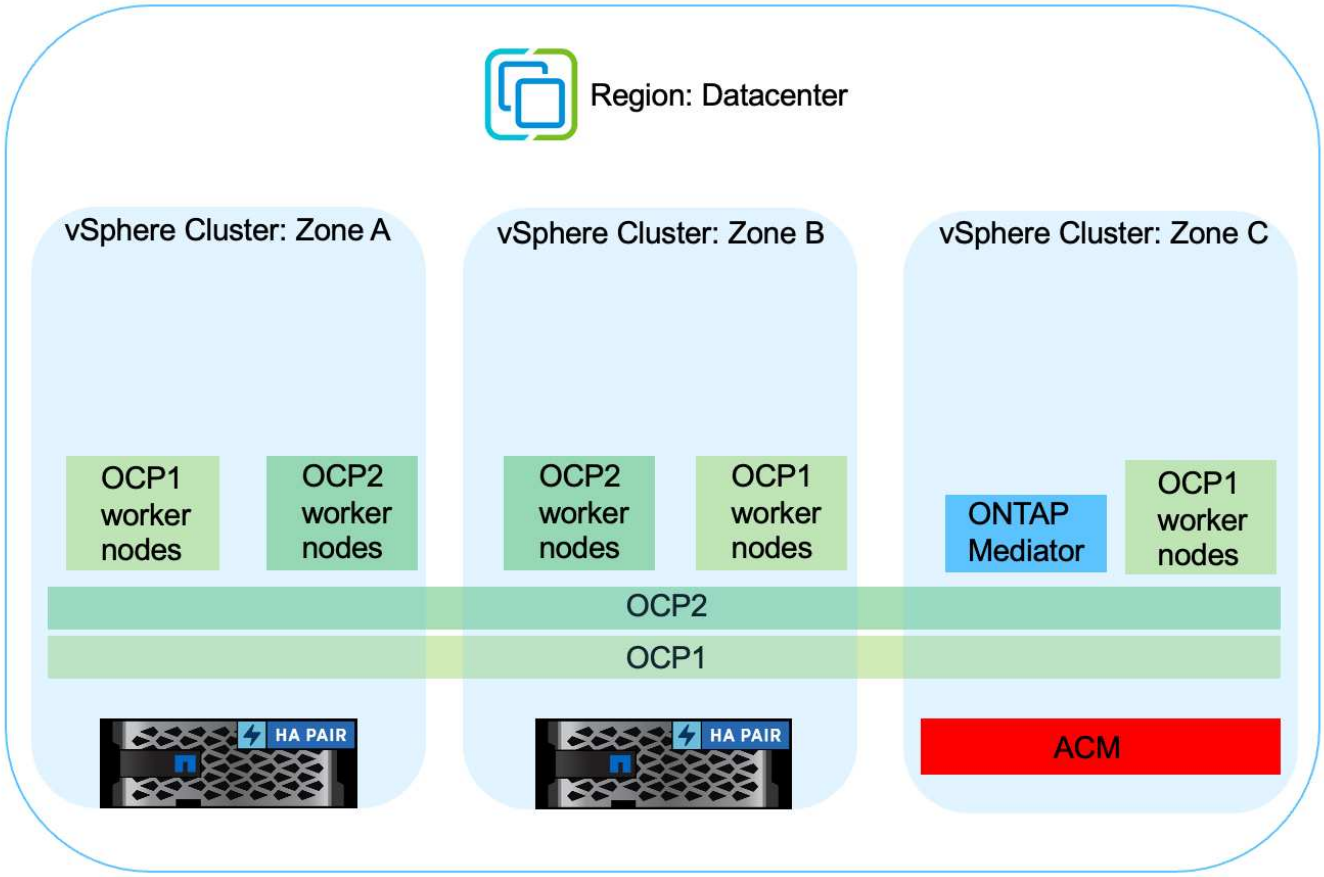
Protection des données avec Trident Protect

Continuité des activités avec MetroCluster

La plupart de nos plateformes matérielles pour ONTAP disposent de fonctionnalités de haute disponibilité pour protéger contre les pannes de périphériques, évitant ainsi la nécessité d'effectuer une récupération après sinistre. Mais pour se protéger des incendies ou de toute autre catastrophe et pour poursuivre l'activité avec un RPO nul et un RTO faible, une solution MetroCluster est souvent utilisée.

Les clients qui disposent actuellement d'un système ONTAP peuvent étendre leur service à MetroCluster en ajoutant des systèmes ONTAP pris en charge dans les limites de distance pour assurer une reprise après sinistre au niveau de la zone. Trident, le CSI (Container Storage Interface) prend en charge NetApp ONTAP, y compris la configuration MetroCluster , ainsi que d'autres options telles que Cloud Volumes ONTAP, Azure NetApp Files, AWS FSx ONTAP, etc. Trident fournit cinq options de pilote de stockage pour ONTAP et toutes sont prises en charge pour la configuration MetroCluster . Référer"ici" pour plus de détails sur les pilotes de stockage ONTAP pris en charge par Trident.

La solution MetroCluster nécessite une extension de réseau de couche 2 ou la capacité d'accéder à la même adresse réseau à partir des deux domaines de pannes. Une fois la configuration de MetroCluster en place, la solution est transparente pour les propriétaires d'applications car tous les volumes du svm MetroCluster sont protégés et bénéficient des avantages de SyncMirror (zéro RPO).



Pour la configuration du backend Trident (TBC), ne spécifiez pas le dataLIF et le SVM lors de l'utilisation de la configuration MetroCluster . Spécifiez l'adresse IP de gestion SVM pour managementLIF et utilisez les informations d'identification du rôle vsadmin.

Des détails sur les fonctionnalités de protection des données de Trident Protect sont disponibles"ici"

Migration de données à l'aide de Trident Protect

Cette page présente les options de migration de données pour les charges de travail de conteneurs sur les clusters Red Hat OpenShift avec Trident Protect.

Les applications Kubernetes doivent souvent être déplacées d'un environnement à un autre. Pour migrer une application avec ses données persistantes, NetApp Trident Protect peut être utilisé.

Migration de données entre différents environnements Kubernetes

ACC prend en charge différentes versions de Kubernetes, notamment Google Anthos, Red Hat OpenShift, Tanzu Kubernetes Grid, Rancher Kubernetes Engine, Upstream Kubernetes, etc. Pour plus de détails, reportez-vous à"ici" .

Pour migrer une application d'un cluster à un autre, vous pouvez utiliser l'une des fonctionnalités suivantes d'ACC :

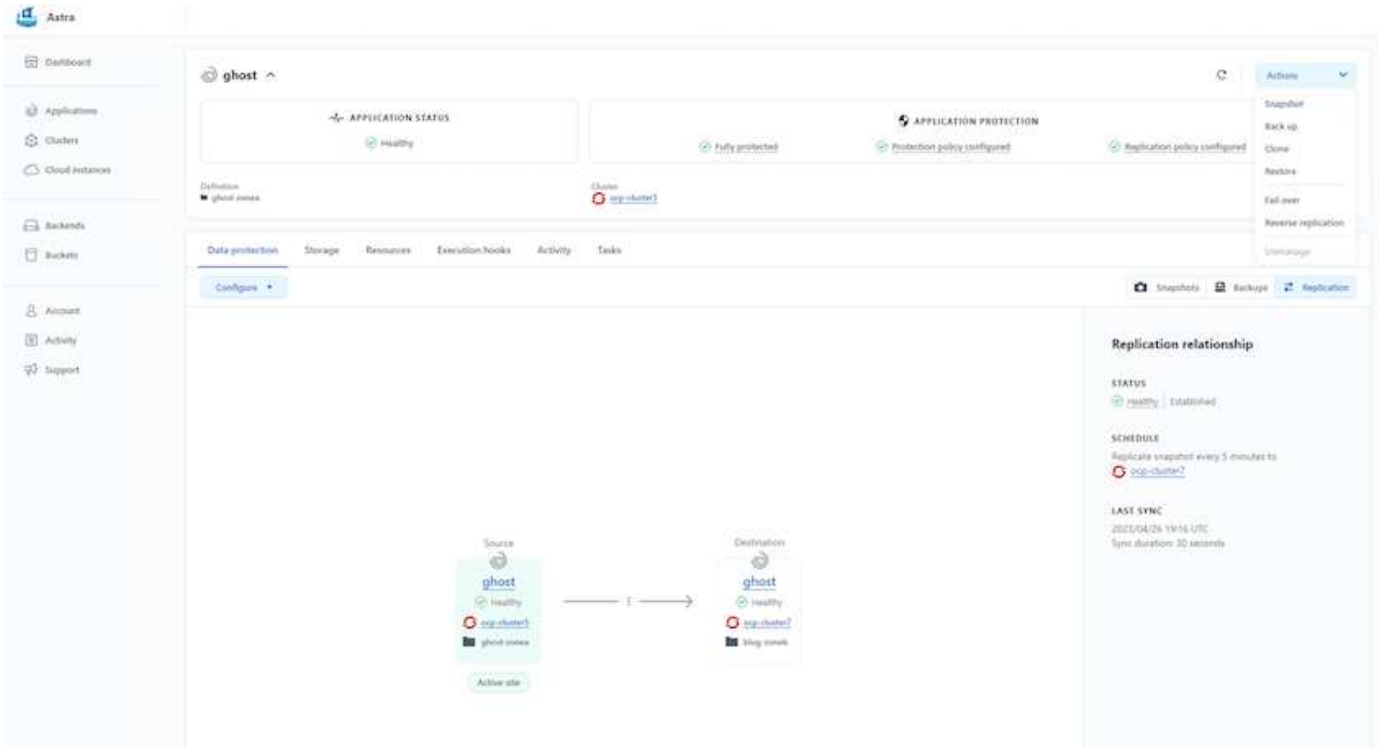
- **réplication**
- **sauvegarde et restauration**

- **clone**

Se référer à la"section protection des données" pour les options **de réplication et de sauvegarde et de restauration**.

Référer"ici" pour plus de détails sur le **clonage**.

Réplication des données à l'aide d'ACC



Informations sur le copyright

Informations sur les marques commerciales