Cloud hybride

FlexPod

NetApp
March 25, 2024

Sommaire

Cloud hybride

Cloud hybride FlexPod avec Cloud Volumes ONTAP pour Epic

Tr-4960 : cloud hybride FlexPod avec Cloud Volumes ONTAP pour Epic

En partenariat avec :

Kamini Singh, NetApp

Pour réussir sa transformation digitale, il suffit d'en faire plus avec la donnée. Les hôpitaux génèrent et requièrent d'importants volumes de données pour gérer leur entreprise et servir leurs patients de manière efficace. Les informations sont collectées et traitées lors du traitement des patients et de la gestion des horaires du personnel et des ressources médicales.

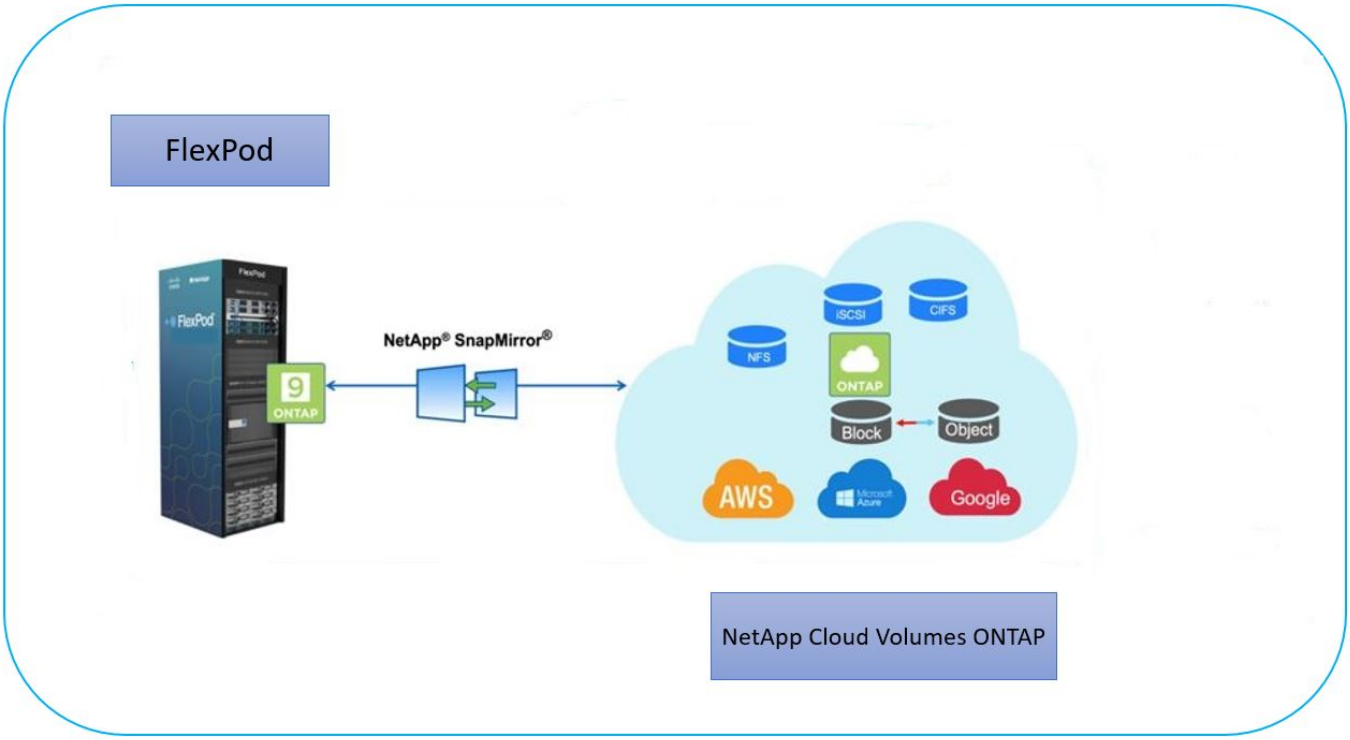
Face à la taille croissante des données de santé et aux informations exploitables qu'elles peuvent fournir, les services de données de santé et la protection des données sont deux aspects à la fois essentiels et complexes. Premièrement, les données de santé doivent être à la fois disponibles et protégées pour répondre aux exigences de restauration des données, de continuité de l'activité médicale et de conformité.

Deuxièmement, les données sur les soins de santé doivent être facilement accessibles pour analyse. Cette analyse utilise souvent des approches basées sur l'intelligence artificielle (IA) et le machine learning (ML) pour aider les entreprises du secteur médical à améliorer leurs solutions et à créer de la valeur commerciale.

Troisièmement, les infrastructures de services de données et les méthodologies de protection des données doivent prendre en charge la croissance des données de santé à mesure que le business médical se développe. De plus, la mobilité des données devient stratégique, car il est nécessaire de déplacer les données de la périphérie au cœur et jusqu'au cloud pour utiliser les ressources disponibles à des fins d'analyse ou d'archivage.

NetApp propose une solution unique de gestion des données pour les applications d'entreprise, y compris le secteur de la santé, et nous pouvons guider les hôpitaux tout au long de leur transition vers la transformation digitale. NetApp Cloud Volumes ONTAP propose une solution de gestion des données de santé dans laquelle les données peuvent être efficacement répliquées à partir d'un data Center FlexPod vers Cloud Volumes ONTAP déployé sur un cloud public tel qu'AWS.

En exploitant des ressources de cloud public sécurisées et économiques, Cloud Volumes ONTAP améliore la reprise après incident dans le cloud grâce à une réplication des données ultra-efficace, des fonctionnalités d'efficacité du stockage intégrées et des tests de reprise d'activité simples. La gestion de ces systèmes se fait par un contrôle unifié et la simplicité de la glisser-déposer. Vous bénéficiez ainsi d'une protection à toute épreuve, peu importe le type d'erreur, de défaillance ou d'incident. Cloud Volumes ONTAP propose la technologie NetApp SnapMirror comme solution de réplication des données de niveau bloc qui assure l'actualisation du volume de destination grâce à des mises à jour incrémentielles.



Public

Ce document est destiné aux ingénieurs solutions partenaires et NetApp, ainsi qu'aux équipes des services professionnels. NetApp suppose que le lecteur possède les connaissances de base suivantes :

- Une solide compréhension des concepts SAN et NAS
- Connaissance technique des systèmes de stockage ONTAP de NetApp
- Connaissance technique de la configuration et de l'administration du logiciel ONTAP

Avantages de la solution

Le data Center FlexPod intégré à NetApp Cloud Volumes ONTAP offre les avantages suivants pour les charges de travail du secteur de la santé :

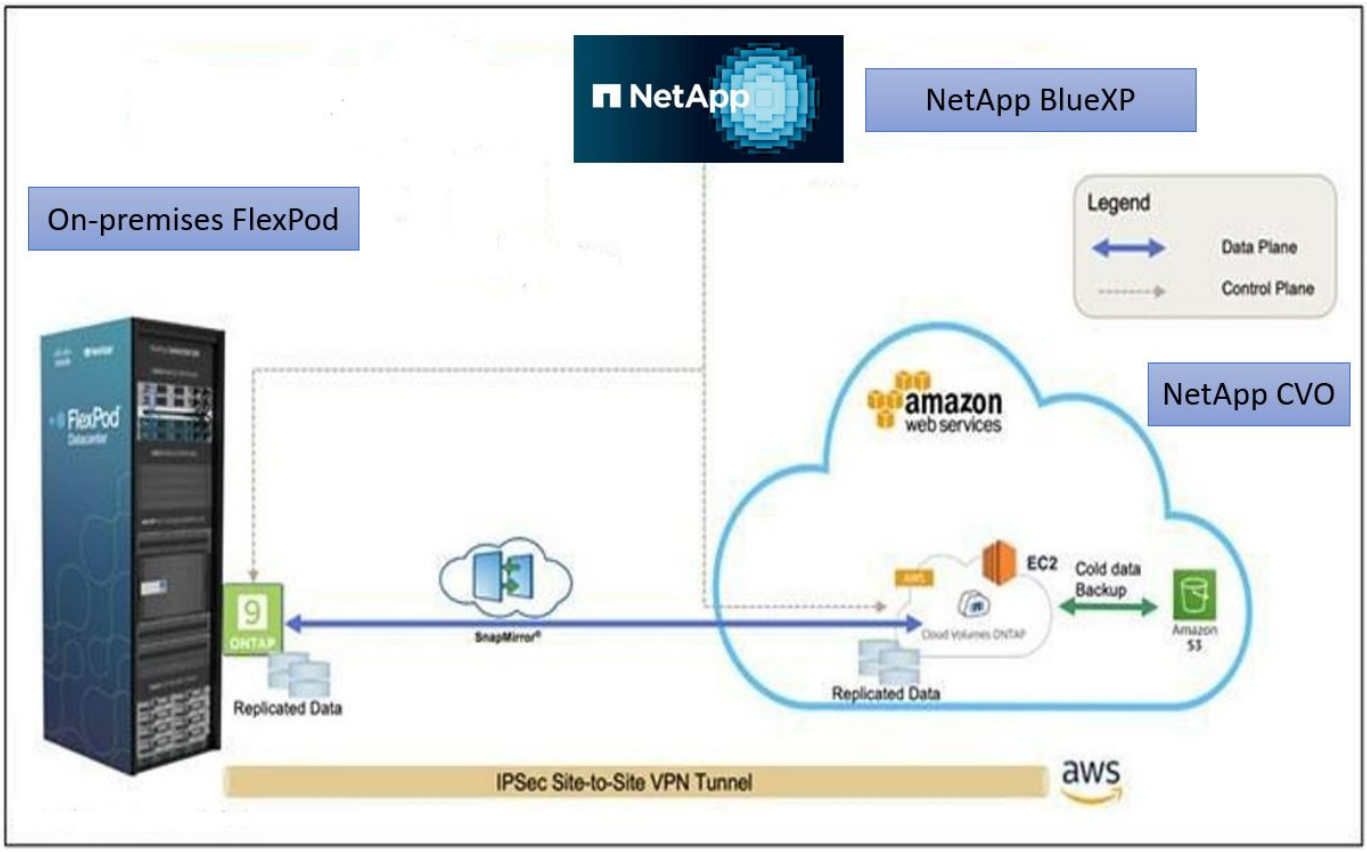
- **Protection personnalisée.** Cloud Volumes ONTAP assure la réplication des données au niveau des blocs de ONTAP vers le cloud afin de maintenir la destination à jour grâce à des mises à jour incrémentielles. Les utilisateurs peuvent spécifier une planification de synchronisation pour déterminer quand les modifications à la source sont transférées. Cela procure une protection personnalisée pour tous les types de données de santé.
- **Basculement et retour arrière.** en cas d'incident, les administrateurs du stockage peuvent rapidement définir le basculement vers les volumes cloud. Une fois le site primaire restauré, les nouvelles données créées dans l'environnement de reprise sont synchronisées avec les volumes source, ce qui permet de rétablir la réplication des données secondaires. Ainsi, les données de santé peuvent être facilement restaurées sans interrompre l'activité.
- **Efficacité.** l'espace de stockage et les coûts de la copie cloud secondaire sont optimisés grâce à la compression des données, au provisionnement fin et à la déduplication. Les données de santé sont transférées au niveau des blocs sous forme compressée et dédupliquée, ce qui accélère les transferts. Ainsi, les données sont automatiquement transférées vers un stockage objet à faible coût et sont transférées vers un stockage haute performance uniquement lors des accès, comme dans un scénario de

reprise après incident. Ceci réduit considérablement les coûts réguliers de stockage.

- **Protection contre les ransomware** la protection NetApp BlueXP analyse les sources de données dans les environnements sur site et cloud, détecte les vulnérabilités de sécurité, et fournit leur état de sécurité actuel et l'évaluation des risques. Il fournit ensuite des recommandations exploitables que vous pouvez approfondir l'investigation et le suivi pour remédier à ces problèmes. Ainsi, vous pouvez protéger vos données de santé stratégiques contre les attaques par ransomware.

Topologie de la solution

Cette section décrit la topologie logique de la solution. La figure suivante représente la topologie de la solution composée de l'environnement sur site FlexPod, de NetApp Cloud Volumes ONTAP (CVO) exécuté sur Amazon Web Services (AWS) et de la plateforme SaaS NetApp BlueXP.



Les plans de contrôle et les plans de données sont clairement indiqués entre les points d'extrémité. Le plan de données s'exécute entre l'instance ONTAP s'exécutant sur un système FAS 100 % Flash dans FlexPod et l'instance NetApp CVO dans AWS grâce à une connexion VPN sécurisée de site à site. La réplication des données de charge de travail liée au secteur de la santé depuis le data Center FlexPod sur site vers NetApp Cloud Volumes ONTAP est gérée par NetApp SnapMirror. Cette solution prend également en charge une sauvegarde et un Tiering facultatifs des données inactives résidant dans l'instance NetApp CVO vers AWS S3.

"Ensuite, les composants de la solution."

Composants de la solution

"Précédent : présentation de la solution."

FlexPod

FlexPod est un ensemble défini de matériels et de logiciels qui constitue une base intégrée pour les solutions virtualisées et non virtualisées. FlexPod inclut le stockage NetApp ONTAP, la mise en réseau Cisco Nexus, la mise en réseau de stockage Cisco MDS et Cisco Unified Computing System (Cisco UCS).

Les établissements de santé recherchent une solution pour faciliter leur transformation digitale et améliorer l'expérience et les résultats des patients. Avec FlexPod, vous bénéficiez d'une plateforme sécurisée et évolutive qui améliore l'efficacité et permet à votre personnel de prendre plus rapidement des décisions avisées afin de meilleurs soins aux patients.

FlexPod est la plateforme idéale pour répondre aux besoins des workloads dans le domaine de la santé, car elle offre les avantages suivants :

- Optimisation des opérations pour obtenir plus rapidement des informations et améliorer la qualité des soins
- Rationalisation des applications d'imagerie grâce à une infrastructure évolutive et fiable.
- Déploiement rapide et efficace, avec une approche éprouvée pour les applications dédiées au domaine de la santé telles que les DME.

EHR

Electronic Health Records (DSE) est un logiciel destiné aux moyennes et grandes organisations médicales, aux hôpitaux et aux organismes de santé intégrés. Les clients comprennent également des hôpitaux communautaires, des établissements universitaires, des organisations pour enfants, des fournisseurs de filet de sécurité et des systèmes multi-hospitaliers. Les logiciels intégrés aux DME couvrent les fonctions cliniques, d'accès et de revenus, et s'étendent à la maison.

Les prestataires de soins de santé restent sous pression pour maximiser les avantages de leurs investissements substantiels dans les systèmes de santé électroniques de pointe. Lorsque les clients conçoivent leurs data centers pour des solutions EHR et des applications stratégiques, ils identifient souvent les objectifs suivants pour l'architecture de leur data Center :

- Haute disponibilité des applications EHR
- Hautes performances
- Facilité de mise en œuvre de dossiers médicaux électroniques dans le data Center
- Agilité et évolutivité pour soutenir la croissance avec de nouvelles versions ou applications de dossiers médicaux électroniques
- Aspect économique
- Facilité de gestion, stabilité et support
- Protection robuste des données, sauvegarde, restauration et continuité de l'activité

FlexPod est validé pour les DME et prend en charge une plateforme contenant Cisco UCS avec processeurs Intel Xeon, Red Hat Enterprise Linux (RHEL) et la virtualisation avec VMware ESXi. Cette plateforme, associée au classement « High Comfort » de EHR pour le stockage NetApp exécutant ONTAP, permet aux clients d'exécuter leurs applications de santé en toute confiance dans un cloud privé entièrement géré via FlexPod, qui peut également être connecté à n'importe quel fournisseur de cloud public.

NetApp BlueXP

BlueXP (anciennement NetApp Cloud Manager) est une plateforme de gestion SaaS haute performance qui permet aux experts IT et aux architectes cloud de gérer de manière centralisée leur infrastructure multicloud

hybride à l'aide des solutions cloud NetApp. Cette solution offre un système centralisé pour afficher et gérer vos environnements de stockage sur site et cloud, prenant en charge des environnements de cloud hybride de plusieurs fournisseurs et comptes. Pour plus d'informations, voir "BlueXP".

Connecteur

Une instance de connecteur permet à BlueXP de gérer les ressources et les processus dans un environnement de cloud public. Le connecteur est requis pour la plupart des fonctionnalités fournies par BlueXP, et peut être déployé dans le cloud ou sur le réseau sur site.

Le connecteur est pris en charge aux emplacements suivants :

- Amazon Web Services
- Microsoft Azure
- Google Cloud
- Sur site

Pour en savoir plus sur le connecteur, reportez-vous au "Page connecteur".

NetApp Cloud Volumes ONTAP

NetApp Cloud Volumes ONTAP est une offre de stockage Software-defined qui exécute le logiciel de gestion des données ONTAP dans le cloud afin d'optimiser la gestion des données pour les workloads en mode bloc ou fichier. Avec Cloud Volumes ONTAP, vous pouvez optimiser vos coûts de stockage cloud et augmenter les performances de vos applications tout en améliorant la protection des données, la sécurité et la conformité.

Principaux avantages :

- **Efficacité du stockage.** tirer parti de la déduplication intégrée des données, de la compression des données, du provisionnement fin et du clonage instantané pour réduire les coûts de stockage.
- **Haute disponibilité.** assurer la fiabilité et la continuité de l'activité en cas de défaillances dans votre environnement cloud.
- **Protection des données.** Cloud Volumes ONTAP utilise SnapMirror, la technologie de réplication leader du secteur NetApp, pour répliquer les données sur site vers le cloud afin de disposer facilement de copies secondaires pour de multiples utilisations. Cloud Volumes ONTAP s'intègre également à Cloud Backup pour fournir des fonctionnalités de sauvegarde et de restauration pour la protection et l'archivage à long terme de vos données cloud.
- **Tiering des données.** basculer entre des pools de stockage hautes et basses performances à la demande sans mettre les applications hors ligne.
- **Cohérence des applications.** fournir la cohérence des copies NetApp Snapshot avec la technologie NetApp SnapCenter.
- **Sécurité des données.** Cloud Volumes ONTAP prend en charge le chiffrement des données et offre une protection contre les virus et les ransomware.
- **Contrôles de conformité en matière de confidentialité.** l'intégration à Cloud Data Sense vous aide à comprendre le contexte des données et à identifier les données sensibles.

Pour plus d'informations, reportez-vous à la section "Cloud Volumes ONTAP".

NetApp Active IQ Unified Manager

NetApp Active IQ Unified Manager permet de surveiller vos clusters de stockage ONTAP à partir d'une interface unique, remaniée et intuitive qui fournit des informations exploitables au savoir de la communauté et à l'analytique IA. Il fournit des informations opérationnelles, performantes et proactives sur l'environnement de stockage et les machines virtuelles qui s'exécutent dessus. Lorsqu'un problème se produit avec l'infrastructure de stockage, Unified Manager vous informe des détails du problème pour vous aider à identifier la cause première. Le tableau de bord des machines virtuelles vous offre un aperçu des statistiques de performances de la machine virtuelle. Vous pouvez ainsi examiner l'ensemble du chemin d'E/S depuis l'hôte vSphere vers le réseau, et enfin vers le stockage.

Certains événements fournissent également des mesures correctives qui peuvent être prises pour corriger le problème. Vous pouvez configurer des alertes personnalisées en cas d'événements afin que, lorsque des problèmes se produisent, vous soyez averti par e-mail et des interruptions SNMP. Active IQ Unified Manager vous permet de planifier les besoins en stockage de vos utilisateurs en prévoyant la capacité et les tendances d'utilisation afin d'anticiper les problèmes et d'éviter les décisions réactives à court terme susceptibles d'engendrer d'autres problèmes à long terme.

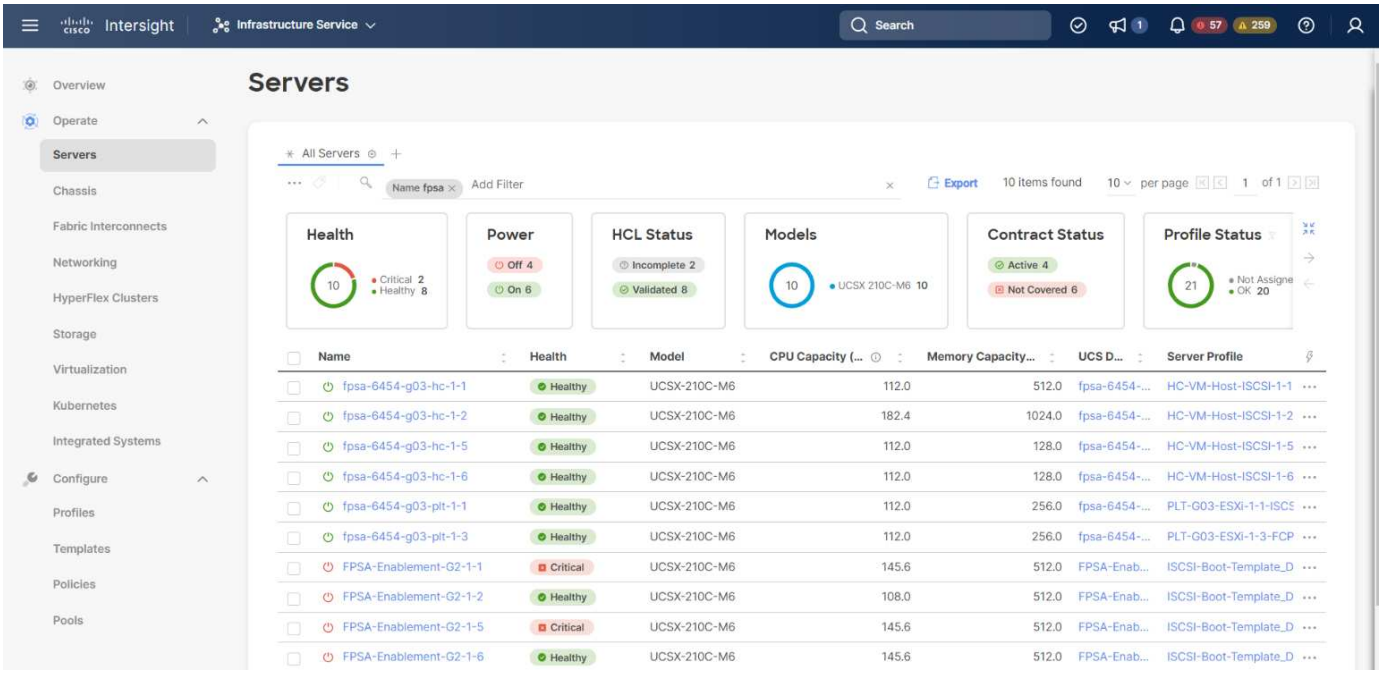
Pour plus d'informations, voir "Active IQ Unified Manager".

Cisco Intersight

Cisco Intersight est une plateforme SaaS qui assure une automatisation, une observabilité et une optimisation intelligentes pour les applications et l'infrastructure classiques et cloud. La plateforme permet de stimuler les évolutions avec les équipes IT et propose un modèle d'exploitation conçu pour le cloud hybride. Cisco Intersight offre les avantages suivants :

- **Livraison plus rapide.** Intersight est fourni en tant que service à partir du cloud ou dans le data Center du client avec des mises à jour fréquentes et une innovation continue grâce à un modèle de développement logiciel agile. Ainsi, le client peut se concentrer sur la prise en charge des besoins stratégiques de l'entreprise.
- **Opérations simplifiées.** Intersight simplifie les opérations en utilisant un outil SaaS unique et sécurisé avec un inventaire, une authentification et des API communs pour fonctionner sur l'ensemble de la pile et sur tous les emplacements, éliminant ainsi les silos entre les équipes. Vous pouvez ainsi gérer les serveurs physiques et les hyperviseurs sur site, sur les machines virtuelles, K8s, sans serveur, l'automatisation, d'optimisation et de contrôle des coûts à la fois sur site et dans les clouds publics.
- **Optimisation continue.** vous pouvez optimiser en continu votre environnement en utilisant l'intelligence fournie par Cisco Intersight sur toutes les couches, ainsi que par Cisco TAC. Ces informations sont converties en actions recommandées et automatisables, qui vous permettent de vous adapter en temps réel à toutes les modifications, allant du déplacement des workloads au contrôle de l'état des serveurs physiques en passant par des recommandations de réduction des coûts pour les clouds publics avec lesquels vous travaillez.

Il existe deux modes d'opérations de gestion possibles avec Cisco Intersight : Umm (UCSM Managed mode) et IMM (Intersight Managed mode). Vous pouvez sélectionner le mode UCSM géré natif (UMM) ou le mode géré Intersight pour les systèmes FAS Cisco UCS lors de la configuration initiale des interconnexions de fabric. Dans cette solution, l'IMM native est utilisé. La figure suivante présente le tableau de bord de Cisco Intersight.



VMware vSphere 7.0

VMware vSphere est une plateforme de virtualisation qui permet de gérer de manière globale de vastes ensembles d'infrastructures (notamment les processeurs, le stockage et la mise en réseau) dans un environnement d'exploitation transparent, polyvalent et dynamique. Contrairement aux systèmes d'exploitation classiques qui gèrent une machine individuelle, VMware vSphere agrège l'infrastructure d'un datacenter entier afin de créer une centrale unique avec des ressources qui peuvent être allouées rapidement et dynamiquement à n'importe quelle application dans le besoin.

Pour plus d'informations sur VMware vSphere et ses composants, voir "VMware vSphere".

Serveur VMware vCenter

VMware vCenter Server assure une gestion unifiée de tous les hôtes et machines virtuelles depuis une console unique et rassemble le contrôle des performances des clusters, des hôtes et des machines virtuelles. VMware vCenter Server offre aux administrateurs des informations détaillées sur l'état et la configuration des clusters de calcul, des hôtes, des VM, du stockage, du système d'exploitation invité, et autres composants essentiels d'une infrastructure virtuelle. VMware vCenter gère la richesse des fonctionnalités disponibles dans un environnement VMware vSphere.

Pour plus d'informations, reportez-vous à la section "VMware vCenter".

Révisions matérielles et logicielles

Cette solution de cloud hybride peut être étendue à tout environnement FlexPod exécutant les versions logicielles, matérielles et firmware prises en charge, comme défini dans le "Matrice d'interopérabilité NetApp", "Compatibilité matérielle et logicielle UCS", et "Guide de compatibilité VMware".

Le tableau suivant présente les révisions matérielles et logicielles FlexPod sur site.

Composant	Solution NetApp	Version
Calcul	Cisco UCS X210c M6	5.0(1b)

Composant	Solution NetApp	Version
	Cisco UCS Fabric Interconnect 6454	4.2(2a)
Le réseau	Cisco Nexus 9336C-FX2 NX-OS	9.3(9)
Stockage	NetApp AFF A400	ONTAP 9.11.1P2
	Outils NetApp ONTAP pour VMware vSphere	9.11
	Plug-in NetApp NFS pour VMware VAAI	2.0
	NetApp Active IQ Unified Manager	9.11P1
Logiciel	VMware vSphere	7.0(U3)
	Pilote Ethernet nenic VMware ESXi	1.0.35.0
	Appliance VMware vCenter	7.0.3
	Appliance virtuelle Cisco InterSight Assist	1.0.9-342

Le tableau suivant présente les versions de NetApp BlueXP et Cloud Volumes ONTAP.

Fournisseur	Solution NetApp	Version
NetApp	BlueXP	3.9.24
	Cloud Volumes ONTAP	ONTAP 9.11

"Suivant : installation et configuration."

Installation et configuration

"Précédent : composants de la solution."

Déploiement de NetApp Cloud Volumes ONTAP

Pour configurer votre instance Cloud Volumes ONTAP, procédez comme suit :

1. Préparez l'environnement du fournisseur de services clouds publics.

   Pour la configuration de la solution, vous devez capturer les détails de l'environnement de votre fournisseur de services de cloud public. Par exemple, pour la préparation de l'environnement Amazon Web Services (AWS), vous avez besoin de la clé d'accès AWS, de la clé secrète AWS et d'autres détails du réseau tels que la région, le VPC, le sous-réseau, etc.

2. Configurez la passerelle de point de terminaison VPC.

   Une passerelle de terminal VPC est nécessaire pour activer la connexion entre le VPC et le service AWS S3. Elle permet d'activer la sauvegarde sur CVO, un terminal de type passerelle.

3. Accédez à NetApp BlueXP.

   Pour accéder à NetApp BlueXP et à d'autres services cloud, vous devez vous inscrire sur "NetApp

BlueXP". Pour configurer des espaces de travail et des utilisateurs dans le compte BlueXP, cliquez sur "ici". Vous avez besoin d'un compte autorisé à déployer le connecteur dans votre fournisseur cloud directement à partir de BlueXP. Vous pouvez télécharger la règle BlueXP depuis le site "ici".

4. Déployez le connecteur.

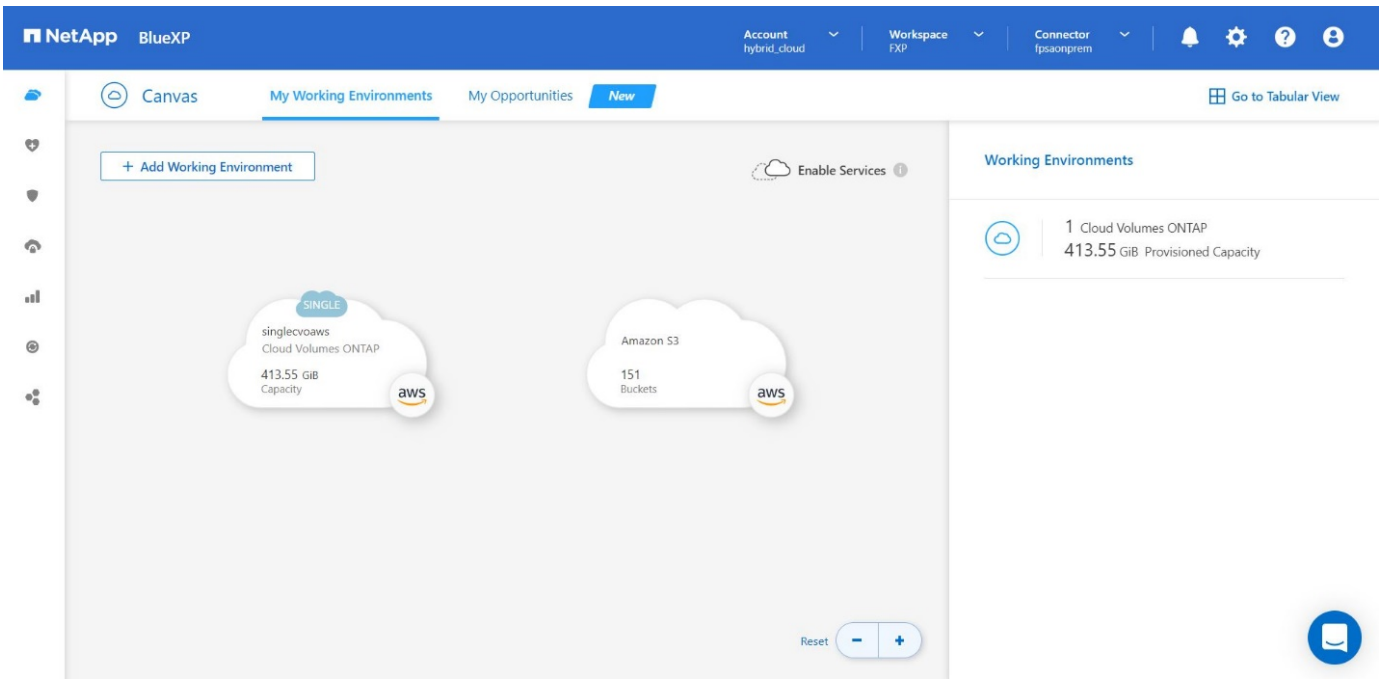
   Avant d'ajouter un environnement de travail Cloud volumes ONTAP, vous devez déployer Connector. BlueXP vous invite si vous essayez de créer votre premier environnement de travail Cloud Volumes ONTAP sans connecteur. Pour déployer Connector dans AWS à partir de BlueXP, consultez cette page "lien".

5. Lancez Cloud Volumes ONTAP dans AWS.

   Vous pouvez lancer Cloud Volumes ONTAP dans une configuration à système unique ou en tant que paire haute disponibilité dans AWS. "Lisez les instructions détaillées".

   Pour plus d'informations sur ces étapes, reportez-vous au "Guide de démarrage rapide de Cloud Volumes ONTAP dans AWS".

   Dans cette solution, nous avons déployé un système Cloud Volumes ONTAP à un seul nœud dans AWS. La figure suivante présente le tableau de bord NetApp BlueXP avec une instance CVO à un seul nœud.



Déploiement FlexPod sur site

Pour en savoir plus sur la conception de FlexPod avec UCS X-Series, VMware et NetApp ONTAP, consultez le "FlexPod Datacenter avec Cisco UCS X-Series" guide de conception. Ce document fournit des conseils de conception pour l'intégration de la plateforme UCS X-Series gérée par Cisco Intersight à l'infrastructure FlexPod Datacenter.

Pour déployer l'instance FlexPod sur site, reportez-vous à la section "ce guide de déploiement".

Ce document apporte des conseils de déploiement pour intégrer la plateforme UCS X-Series gérée par Cisco Intersight à une infrastructure FlexPod Datacenter. Il aborde à la fois les configurations et les meilleures pratiques pour un déploiement réussi.

FlexPod peut être déployé en mode géré UCS et en mode géré Cisco Intersight (IMM). Si vous déployez FlexPod en mode géré UCS, reportez-vous à cette section "guide de conception" et ceci "guide de déploiement".

Le déploiement de FlexPod peut être automatisé avec une infrastructure basée sur le code grâce à Ansible. Vous trouverez ci-dessous des liens vers les référentiels GitHub pour un déploiement FlexPod de bout en bout :

- Vous pouvez voir la configuration Ansible d'FlexPod avec Cisco UCS en mode géré, NetApp ONTAP et VMware vSphere "ici".
- Vous pouvez voir la configuration Ansible d'FlexPod avec Cisco UCS dans IMM, NetApp ONTAP et VMware vSphere "ici".

Configuration du stockage ONTAP sur site

Cette section décrit certaines des importantes étapes de configuration de ONTAP spécifiques à cette solution.

1. Configurez un SVM avec le service iSCSI en cours d'exécution.

```
1. vserver create –vserver Healthcare_SVM –rootvolume
Healthcare_SVM_root –aggregate aggr1_A400_G0312_01 –rootvolume-security-
style unix
2. vserver add-protocols -vserver Healthcare_SVM -protocols iscsi
3. vserver iscsi create -vserver Healthcare_SVM

   To verify:

   A400-G0312::> vserver iscsi show -vserver Healthcare_SVM
   Vserver: Healthcare_SVM
   Target Name:
   iqn.1992-08.com.netapp:sn.1fbf00f438c111ed866cd039ea91fb56:vs.3
   Target Alias: Healthcare_SVM
   Administrative Status: up
```

   Si la licence iSCSI n'a pas été installée lors de la configuration du cluster, assurez-vous d'installer la licence avant de créer le service iSCSI.

2. Créer un volume FlexVol.

```
1. volume create -vserver Healthcare_SVM -volume hc_iscsi_vol -aggregate
aggr1_A400_G0312_01 -size 500GB -state online -policy default -space
guarantee none
```

3. Ajoutez des interfaces pour l'accès iSCSI.

```
1. network interface create -vserver Healthcare_SVM -lif iscsi-lif-01a
-service-policy default-data-iscsi -home-node <st-node01> -home-port
a0a-<infra-iscsi-a-vlan-id> -address <st-node01-infra-iscsi-a-ip>
-netmask <infra-iscsi-a-mask> -status-admin up
2. network interface create -vserver Healthcare_SVM -lif iscsi-lif-01b
-service-policy default-data-iscsi -home-node <st-node01> -home-port
a0a-<infra-iscsi-b-vlan-id> -address <st-node01-infra-iscsi-b-ip>
-netmask <infra-iscsi-b-mask> –status-admin up
3. network interface create -vserver Healthcare_SVM -lif iscsi-lif-02a
-service-policy default-data-iscsi -home-node <st-node02> -home-port
a0a-<infra-iscsi-a-vlan-id> -address <st-node02-infra-iscsi-a-ip>
-netmask <infra-iscsi-a-mask> –status-admin up
4. network interface create -vserver Healthcare_SVM -lif iscsi-lif-02b
-service-policy default-data-iscsi -home-node <st-node02> -home-port
a0a-<infra-iscsi-b-vlan-id> -address <st-node02-infra-iscsi-b-ip>
-netmask <infra-iscsi-b-mask> –status-admin up
```

Dans cette solution, nous avons créé quatre interfaces logiques iSCSI, deux sur chaque nœud.

Une fois l'instance FlexPod opérationnelle avec vCenter déployée et tous les hôtes ESXi ajoutés, nous devons déployer une VM Linux qui agit comme un serveur qui se connecte au stockage NetApp ONTAP et y accède. Dans cette solution, nous avons installé une instance CentOS 8 dans vCenter.

4. Créer une LUN.

```
1. lun create -vserver Healthcare_SVM -path /vol/hc_iscsi_vol/iscsi_lun1
-size 200GB -ostype linux -space-reserve disabled
```

Pour une base de données opérationnelle EHR (ODB), un journal et des charges de travail applicatives, EHR recommande de présenter le stockage aux serveurs comme des LUN iSCSI. NetApp prend également en charge l'utilisation de FCP et NVMe/FC si certaines versions d'AIX et de systèmes d'exploitation RHEL sont compatibles, ce qui améliore les performances. FCP et NVMe/FC peuvent coexister sur la même structure.

5. Créer un groupe initiateur.

```
1. igroup create –vserver Healthcare_SVM –igroup ehr –protocol iscsi
–ostype linux –initiator iqn.1994-05.com.redhat:8e91e9769336
```

Les iGroups permettent au serveur d'accéder aux LUN, Pour l'hôte Linux, l'IQN du serveur se trouve dans le fichier `/etc/iscsi/initiatorname.iscsi`.

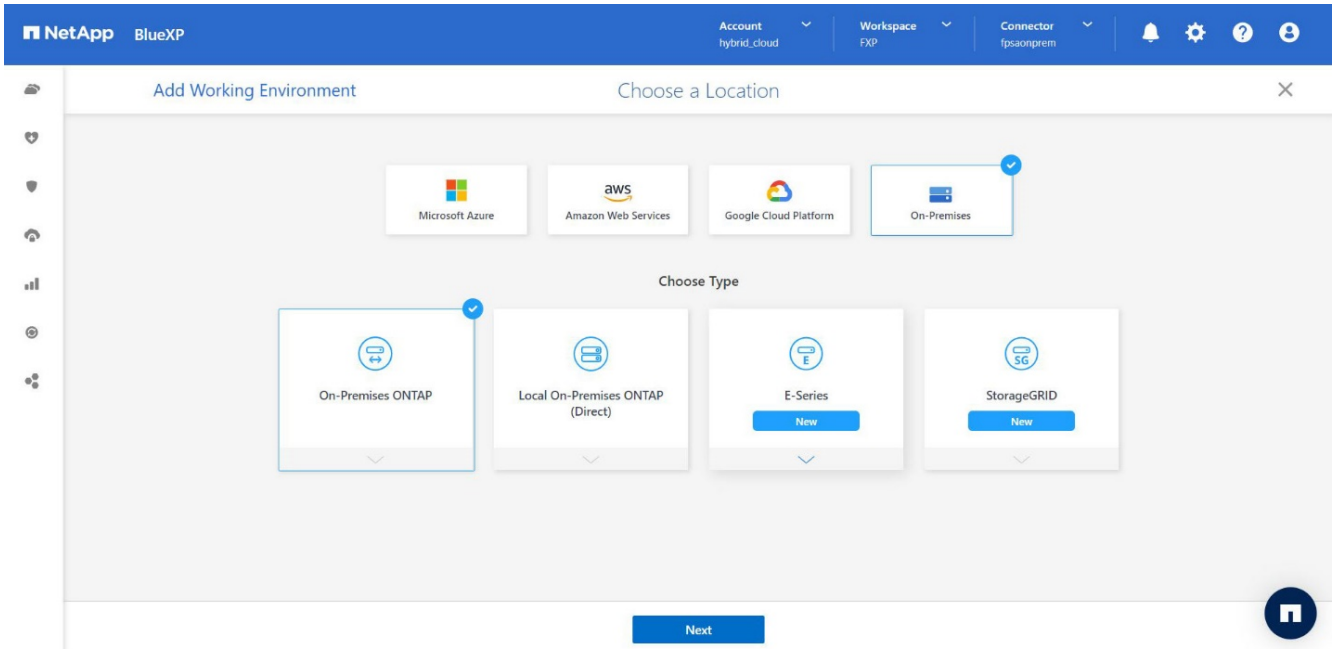
6. Mappez la LUN sur le groupe initiateur.

```
1. lun mapping create -vserver Healthcare_SVM -path
/vol/hc_iscsi_vol/iscsi_lun1 -igroup ehr -lun-id 0
```

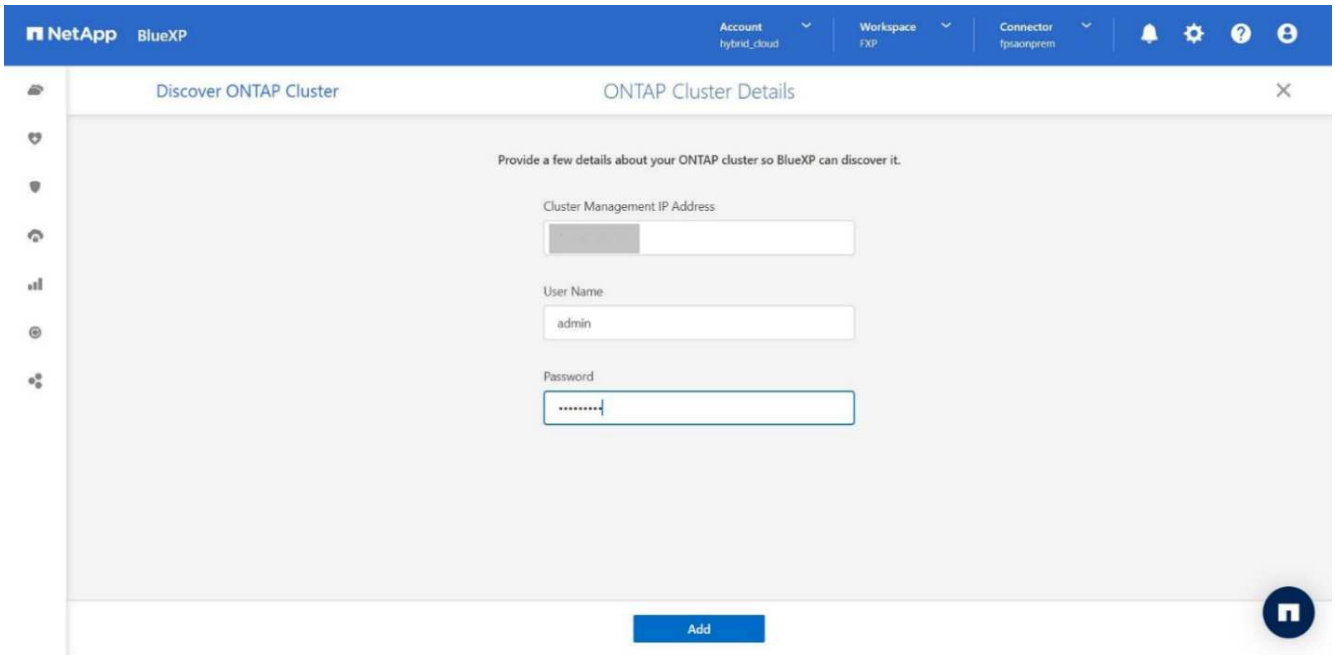
Ajoutez le stockage FlexPod sur site à BlueXP

Procédez comme suit pour ajouter votre stockage FlexPod à l'environnement de travail à l'aide de NetApp BlueXP.

1. Dans le menu de navigation, sélectionnez **stockage** > **Canvas**.
2. Sur la page Canevas, cliquez sur **Ajouter un environnement de travail** et sélectionnez **sur site**.
3. Sélectionnez **ONTAP sur site**. Cliquez sur **Suivant**.

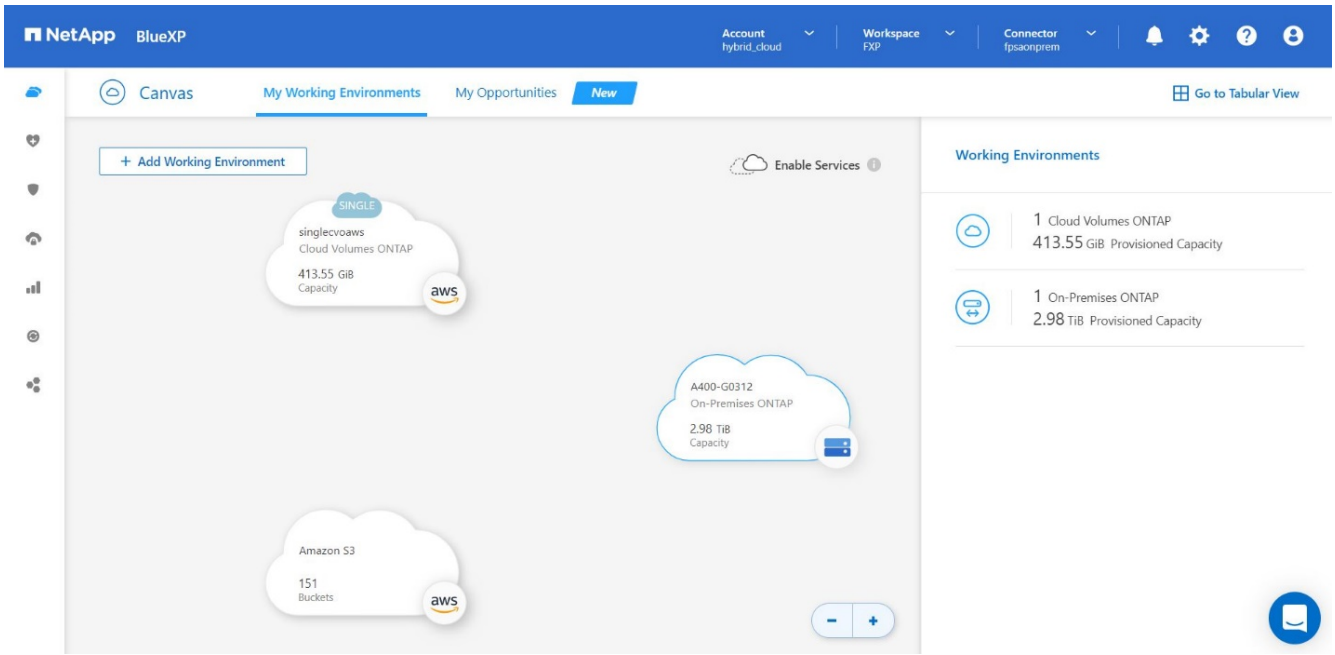


4. Sur la page ONTAP Cluster Details (Détails du cluster ONTAP), entrez l'adresse IP de gestion du cluster et le mot de passe du compte d'utilisateur admin. Cliquez ensuite sur **Ajouter**.



5. Sur la page Détails et informations d'identification, entrez un nom et une description pour l'environnement de travail, puis cliquez sur **Go**.

   BlueXP découvre le cluster ONTAP et l'ajoute en tant qu'environnement de travail sur la zone de travail.



Pour plus d'informations, reportez-vous à la page "Découvrez les clusters ONTAP sur site".

"Ensuite : configuration SAN."

Configuration SAN

"Précédent : installation et configuration."

Cette section décrit la configuration côté hôte requise par le dossier EHR pour permettre

au logiciel d'intégrer au mieux le stockage NetApp. Dans ce segment, nous discutons plus particulièrement de l'intégration de l'hôte pour les systèmes d'exploitation Linux. Utilisez le "Matrice d'interopérabilité NetApp (IMT)" pour valider toutes les versions des logiciels et des firmwares.

> Les étapes de configuration suivantes sont spécifiques à l'hôte CentOS 8 qui a été utilisé dans cette solution.

Kit d'utilitaire hôte NetApp

NetApp recommande d'installer NetApp Host Utility Kit (Host Utilities Kit) sur les systèmes d'exploitation d'hôtes connectés aux systèmes de stockage NetApp et accédant à ces derniers. Les E/S multichemins Microsoft natives (MPIO) sont prises en charge. Le système d'exploitation doit être compatible ALUA (Asymmetric Logical Unit Access) pour les chemins d'accès multiples. L'installation des utilitaires d'hôtes configure les paramètres de l'adaptateur de bus hôte (HBA) pour le stockage NetApp.

Les utilitaires d'hôte NetApp peuvent être téléchargés "ici". Dans cette solution, nous avons installé Linux Host Utilities 7.1 sur l'hôte.

```
[root@hc-cloud-secure-1 ~]# rpm -ivh netapp_linux_unified_host_utilities-
7-1.x86_64.rpm
```

Découvrez le stockage ONTAP

Assurez-vous que le service iSCSI est en cours d'exécution lorsque les connexions sont supposées se produire. Pour définir le mode de connexion pour un portail spécifique sur une cible ou pour tous les portails sur une cible, utilisez le `iscsiadm` commande.

```
[root@hc-cloud-secure-1 ~]# rescan-scsi-bus.sh
[root@hc-cloud-secure-1 ~]# iscsiadm -m discovery -t sendtargets -p
<iscsi-lif-ip>
[root@hc-cloud-secure-1 ~]# iscsiadm -m node -L all
```

Vous pouvez maintenant utiliser `sanlun` Pour afficher des informations sur les LUN connectées à l'hôte. Assurez-vous d'être connecté en tant que root sur l'hôte.

```
[root@hc-cloud-secure-1 ~]# sanlun lun show
controller(7mode/E-Series)/
                                     device    host             lun
vserver(cDOT/FlashRay) lun-pathname filename  adapter protocol size
product
------------------------------------------------------------------------
---
Healthcare_SVM                        /dev/sdb host33  iSCSI    200g
cDOT
                       /vol/hc_iscsi_vol/iscsi_lun1

Healthcare_SVM                        /dev/sdc host34  iSCSI    200g
cDOT
                       /vol/hc_iscsi_vol/iscsi_lun1
```

Configurer les chemins d'accès multiples

Device Mapper Multipathing (DM-Multipath) est un utilitaire natif de multipathing sous Linux. Il peut être utilisé pour la redondance et pour améliorer les performances. Elle agrège ou combine les chemins d'E/S multiples entre les serveurs et le stockage, afin de créer un périphérique unique au niveau du système d'exploitation.

1. Avant de configurer DM-Multipath sur votre système, assurez-vous que votre système a été mis à jour et inclut le `device-mapper-multipath` création de package.

   ```
   [root@hc-cloud-secure-1 ~]# rpm -qa|grep multipath
   device-mapper-multipath-libs-0.8.4-31.el8.x86_64
   device-mapper-multipath-0.8.4-31.el8.x86_64
   ```

2. Le fichier de configuration est le `/etc/multipath.conf` fichier. Mettez à jour le fichier de configuration comme indiqué ci-dessous.

   ```
   [root@hc-cloud-secure-1 ~]# cat /etc/multipath.conf
   defaults {
      path_checker      readsector0
      no_path_retry      fail
   }
   devices {
      device {
         vendor         "NETAPP  "
         product         "LUN.*"
         no_path_retry     queue
         path_checker      tur
      }
   }
   ```

3. Activez et démarrez les services multivoies.

```
[root@hc-cloud-secure-1 ~]# systemctl enable multipathd.service
[root@hc-cloud-secure-1 ~]# systemctl start  multipathd.service
```

4. Ajoutez le module noyau chargeable `dm-multipath` et redémarrez le service multivoie. Enfin, vérifiez l'état des chemins d'accès multiples.

```
[root@hc-cloud-secure-1 ~]# modprobe -v dm-multipath
insmod /lib/modules/4.18.0-408.el8.x86_64/kernel/drivers/md/dm-
multipath.ko.xz

[root@hc-cloud-secure-1 ~]# systemctl restart multipathd.service

[root@hc-cloud-secure-1 ~]# multipath -ll
3600a09803831494c372b545a4d786278 dm-2 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| `- 33:0:0:0 sdb 8:16 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
`- 34:0:0:0 sdc 8:32 active ready running
```

Pour plus d'informations sur ces étapes, reportez-vous à la section "ici".

Créer un volume physique

Utilisez le `pvcreate` commande permettant d'initialiser un périphérique de bloc à utiliser comme volume physique. L'initialisation est similaire au formatage d'un système de fichiers.

```
[root@hc-cloud-secure-1 ~]# pvcreate /dev/sdb
Physical volume "/dev/sdb" successfully created.
```

Créer un groupe de volumes

Pour créer un groupe de volumes à partir d'un ou de plusieurs volumes physiques, utilisez `vgcreate` commande. Cette commande crée un nouveau groupe de volumes par son nom et y ajoute au moins un volume physique.

```
[root@hc-cloud-secure-1 ~]# vgcreate datavg /dev/sdb
Volume group "datavg" successfully created.
```

Le `vgdisplay` peut être utilisé pour afficher les propriétés des groupes de volumes (taille, extensions, nombre

de volumes physiques, etc.) dans un format fixe.

```
[root@hc-cloud-secure-1 ~]# vgdisplay datavg
  --- Volume group ---
  VG Name               datavg
  System ID
  Format                lvm2
  Metadata Areas        1
  Metadata Sequence No  1
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                0
  Open LV               0
  Max PV                0
  Cur PV                1
  Act PV                1
  VG Size               <200.00 GiB
  PE Size               4.00 MiB
  Total PE              51199
  Alloc PE / Size       0 / 0
  Free  PE / Size       51199 / <200.00 GiB
  VG UUID               C7jmI0-J0SS-Cq91-t6b4-A9xw-nTfi-RXcy28
```

Créer un volume logique

Lorsque vous créez un volume logique, le volume logique est découpé dans un groupe de volumes à l'aide des extensions libres sur les volumes physiques qui composent le groupe de volumes.

```
[root@hc-cloud-secure-1 ~]# lvcreate - l 100%FREE -n datalv datavg
Logical volume "datalv" created.
```

Cette commande crée un volume logique appelé `datalv` qui utilise tout l'espace non alloué dans le groupe de volumes `datavg`.

Créer un système de fichiers

```
[root@hc-cloud-secure-1 ~]# mkfs.xfs -K /dev/datavg/datalv
meta-data=/dev/datavg/datalv     isize=512    agcount=4, agsize=13106944
blks
         =                       sectsz=4096  attr=2, projid32bit=1
         =                       crc=1        finobt=1, sparse=1, rmapbt=0
         =                       reflink=1    bigtime=0 inobtcount=0
data     =                       bsize=4096   blocks=52427776, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0, ftype=1
log      =internal log           bsize=4096   blocks=25599, version=2
         =                       sectsz=4096  sunit=1 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
```

Créer un dossier à monter

```
[root@hc-cloud-secure-1 ~]# mkdir /file1
```

Montez le système de fichiers

```
[root@hc-cloud-secure-1 ~]# mount -t xfs /dev/datavg/datalv /file1

[root@hc-cloud-secure-1 ~]# df -k
Filesystem                 1K-blocks    Used Available Use% Mounted on
devtmpfs                     8072804       0   8072804   0% /dev
tmpfs                        8103272       0   8103272   0% /dev/shm
tmpfs                        8103272    9404   8093868   1% /run
tmpfs                        8103272       0   8103272   0% /sys/fs/cgroup
/dev/mapper/cs-root         45496624 5642104  39854520  13% /
/dev/sda2                    1038336  258712    779624  25% /boot
/dev/sda1                     613184    7416    605768   2% /boot/efi
tmpfs                        1620652      12   1620640   1% /run/user/42
tmpfs                        1620652       0   1620652   0% /run/user/0
/dev/mapper/datavg-datalv 209608708 1494520 208114188   1% /file1
```

Pour plus d'informations sur ces tâches, reportez-vous à la page "Administration LVM avec commandes CLI".

Génération de données

```
`Dgen.pl` Est un générateur de données de script perl pour le simulateur
d'E/S de EHR (GenerateIO). Les données contenues dans les LUN sont
générées avec le DME `Dgen.pl` script. Le script est conçu pour créer des
données similaires à celles qui se trouvent dans une base de données EHR.
```

```
[root@hc-cloud-secure-1 ~]# cd GenerateIO-1.17.3/

[root@hc-cloud-secure-1 GenerateIO-1.17.3]# ./dgen.pl --directory /file1
--jobs 80

[root@hc-cloud-secure-1 ~]# cd /file1/
[root@hc-cloud-secure-1 file1]# ls
dir01  dir05  dir09  dir13  dir17  dir21  dir25  dir29  dir33  dir37
dir41  dir45  dir49  dir53  dir57  dir61  dir65  dir69  dir73  dir77
dir02  dir06  dir10  dir14  dir18  dir22  dir26  dir30  dir34  dir38
dir42  dir46  dir50  dir54  dir58  dir62  dir66  dir70  dir74  dir78
dir03  dir07  dir11  dir15  dir19  dir23  dir27  dir31  dir35  dir39
dir43  dir47  dir51  dir55  dir59  dir63  dir67  dir71  dir75  dir79
dir04  dir08  dir12  dir16  dir20  dir24  dir28  dir32  dir36  dir40
dir44  dir48  dir52  dir56  dir60  dir64  dir68  dir72  dir76  dir80

[root@hc-cloud-secure-1 file1]# df -k .
Filesystem                 1K-blocks  Used       Available  Use%  Mounted
on
/dev/mapper/datavg-datalv  209608708  178167156  31441552   85%   /file1
```

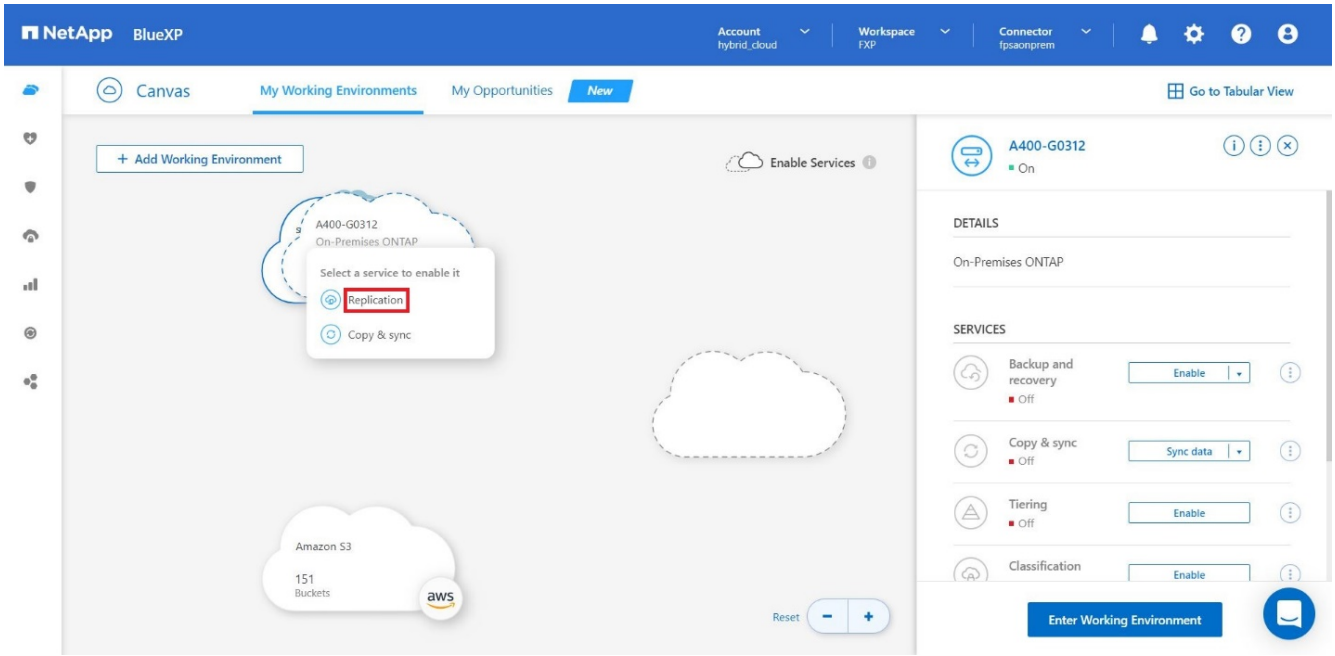
En cours d'exécution, le `Dgen.pl` script utilise 85 % du système de fichiers pour la génération de données par défaut.

Configurez la réplication SnapMirror entre ONTAP et Cloud Volumes ONTAP sur site

NetApp SnapMirror réplique les données à des vitesses élevées sur un réseau LAN ou WAN, vous garantissant ainsi une haute disponibilité et une réplication rapide des données dans les environnements traditionnels et virtualisés. En répliquant vos données sur des systèmes de stockage NetApp, puis en les mettant régulièrement à jour, vous disposez de données actualisées et accessibles dès que vous en avez besoin. Aucun serveur de réplication externe n'est requis.

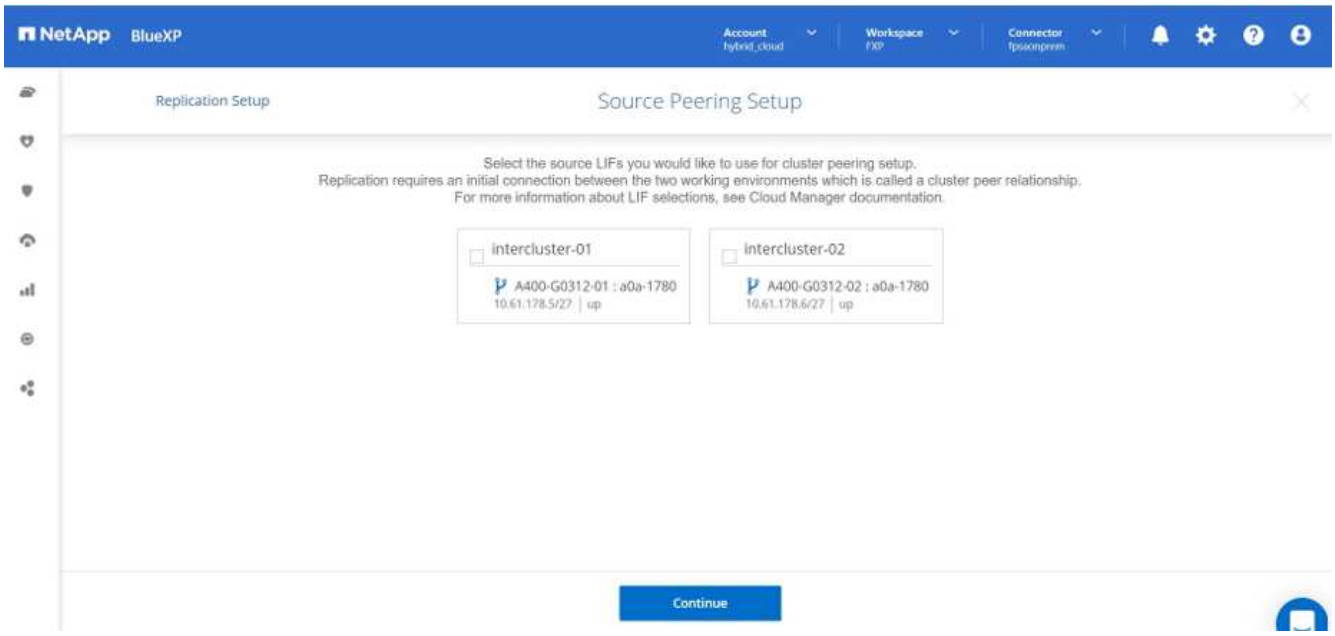
Effectuez les étapes suivantes pour configurer la réplication SnapMirror entre votre système ONTAP sur site et CVO.

1. Dans le menu de navigation, sélectionnez **stockage** > **Canvas**.
2. Dans Canvas, sélectionnez l'environnement de travail qui contient le volume source, faites-le glisser vers l'environnement de travail vers lequel vous souhaitez répliquer le volume, puis sélectionnez **Replication**.

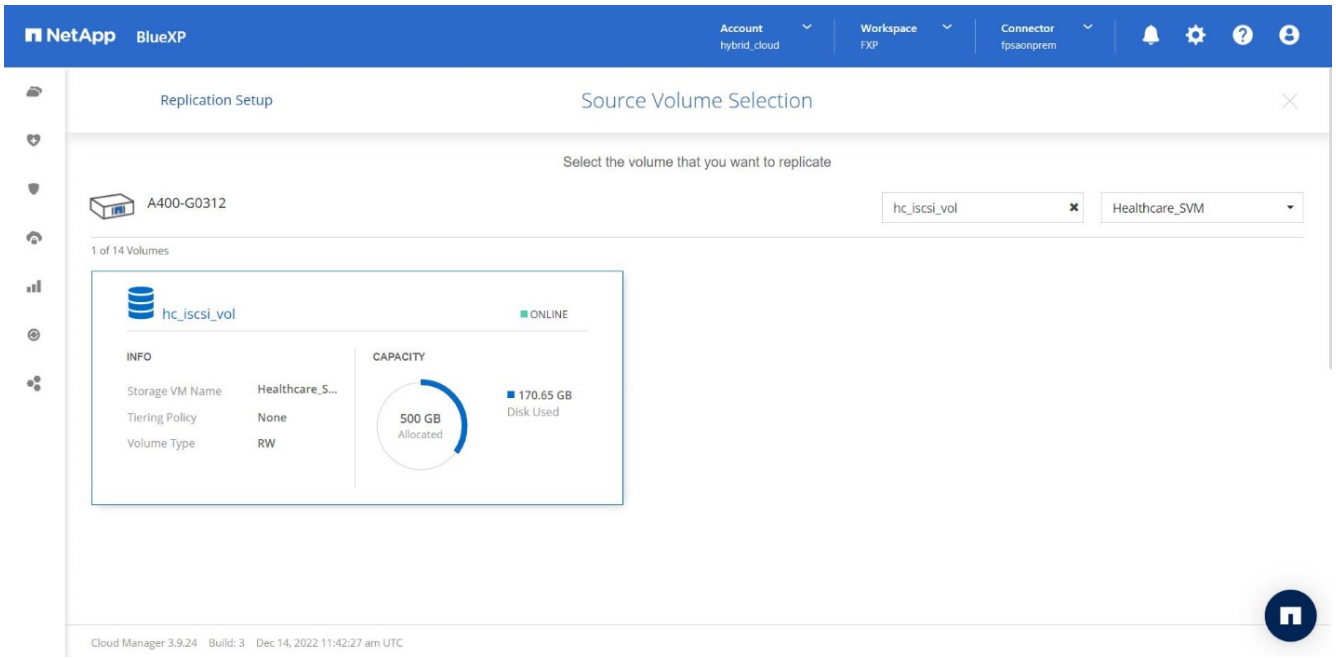


Les autres étapes expliquent comment créer une relation synchrone entre Cloud Volumes ONTAP et les clusters ONTAP sur site.

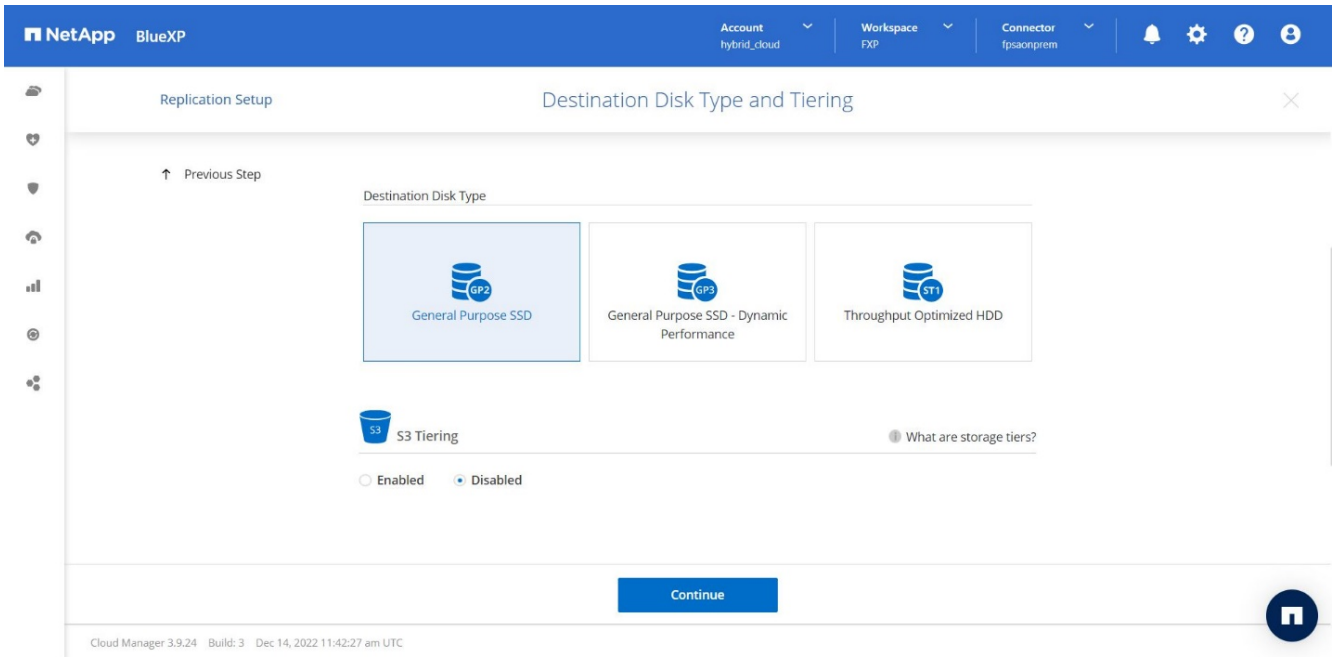
3. **Configuration du peering source et destination.** si cette page s'affiche, sélectionnez toutes les LIFs intercluster pour la relation entre pairs de cluster.



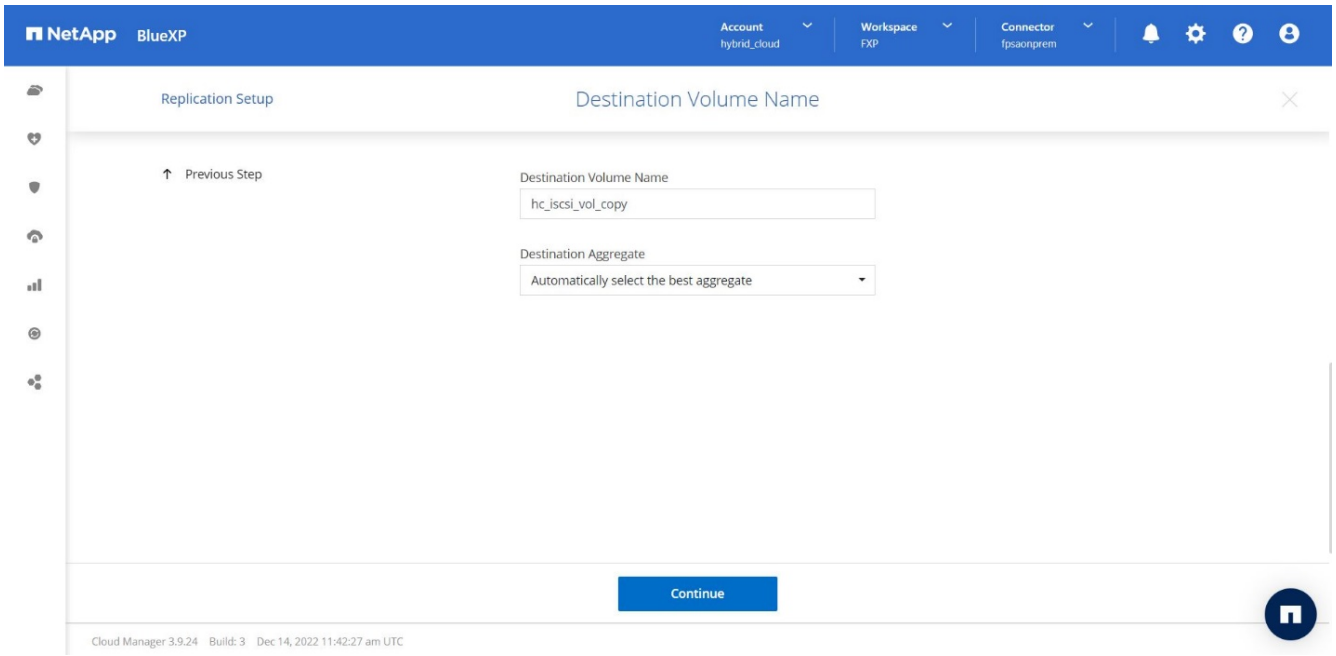
4. **Sélection du volume source.** sélectionnez le volume que vous souhaitez répliquer.



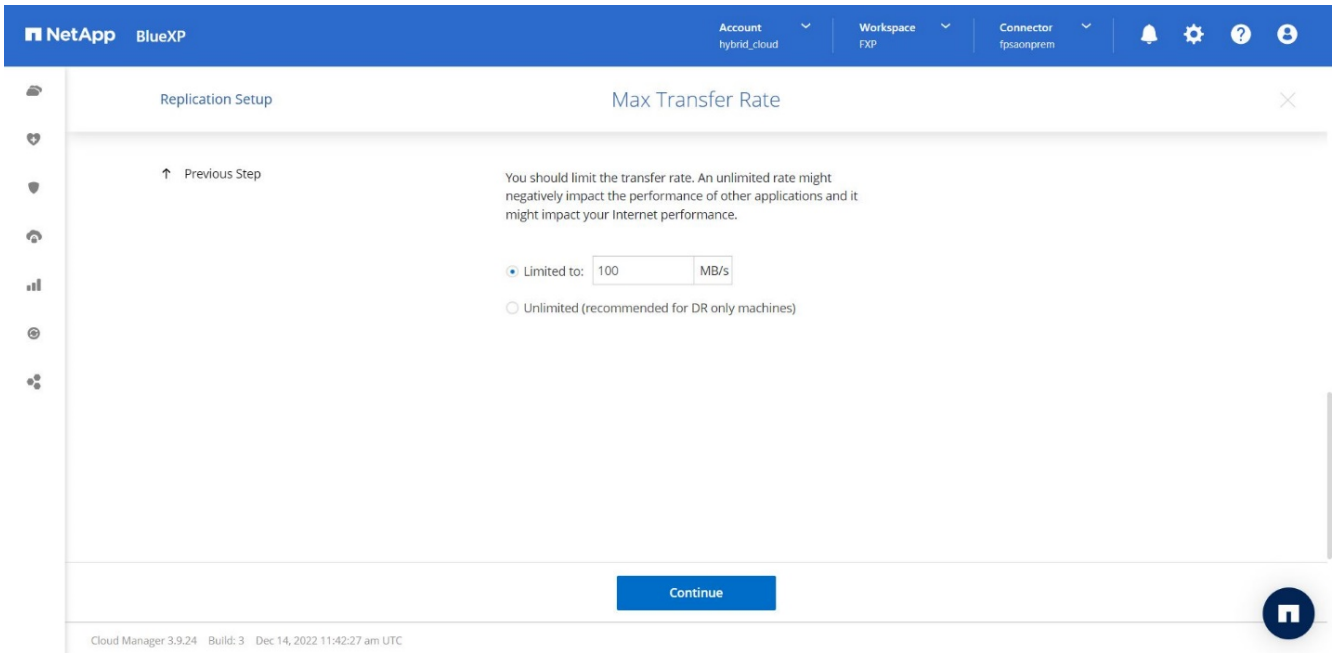
5. **Type de disque de destination et hiérarchisation.** si la cible est un système Cloud Volumes ONTAP, sélectionnez le type de disque de destination et choisissez si vous souhaitez activer la hiérarchisation des données.



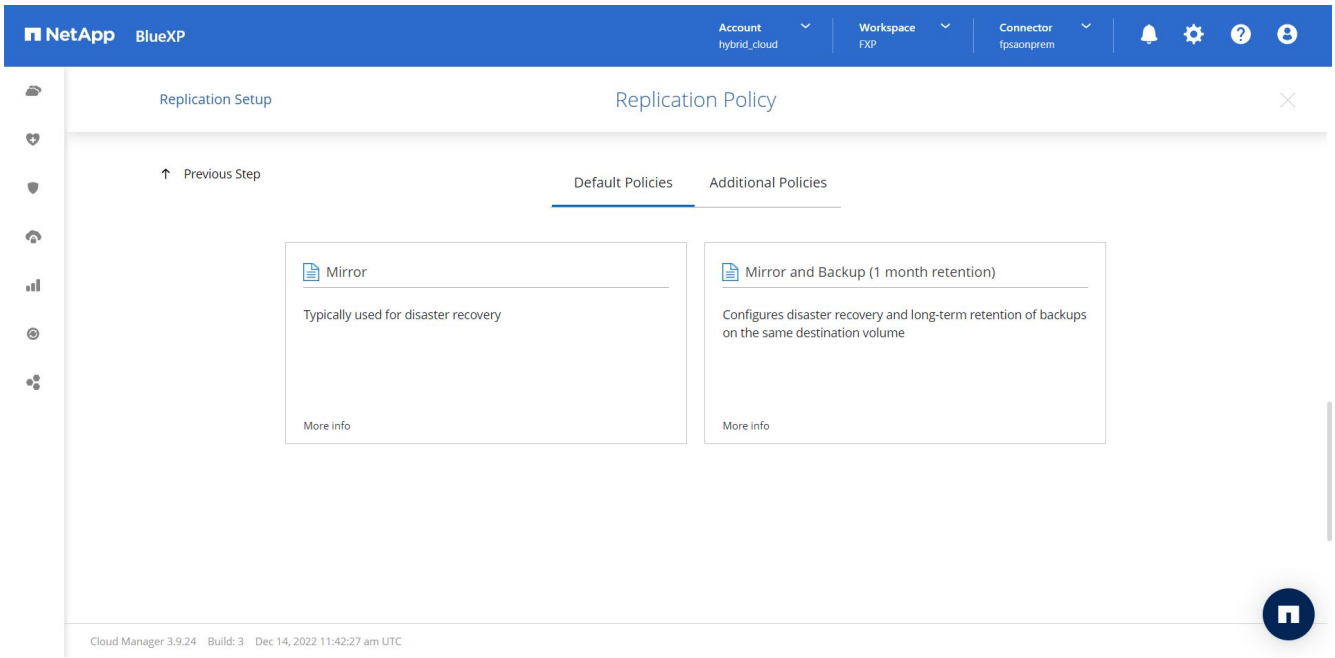
6. **Nom du volume de destination :** Indiquez le nom du volume de destination et choisissez l'agrégat de destination. Si la destination est un cluster ONTAP, vous devez également spécifier la VM de stockage de destination.



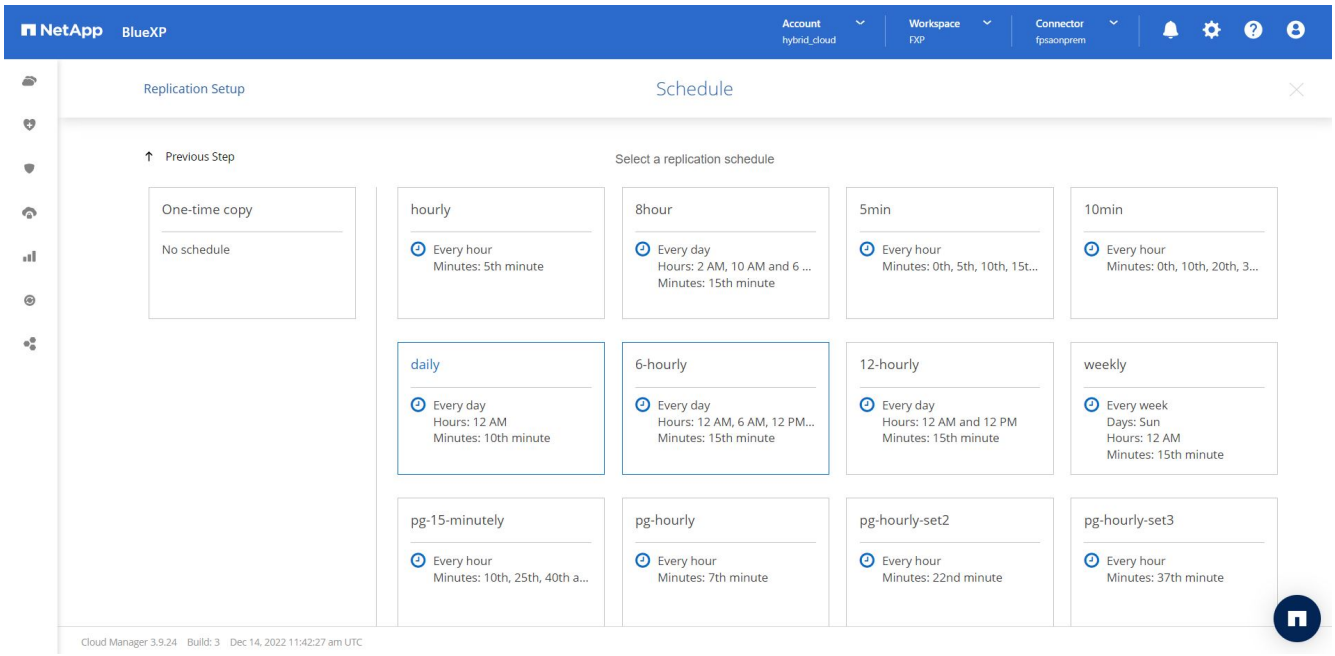
7. **Taux de transfert max.** Indiquez le taux maximal (en mégaoctets par seconde) auquel les données peuvent être transférées.



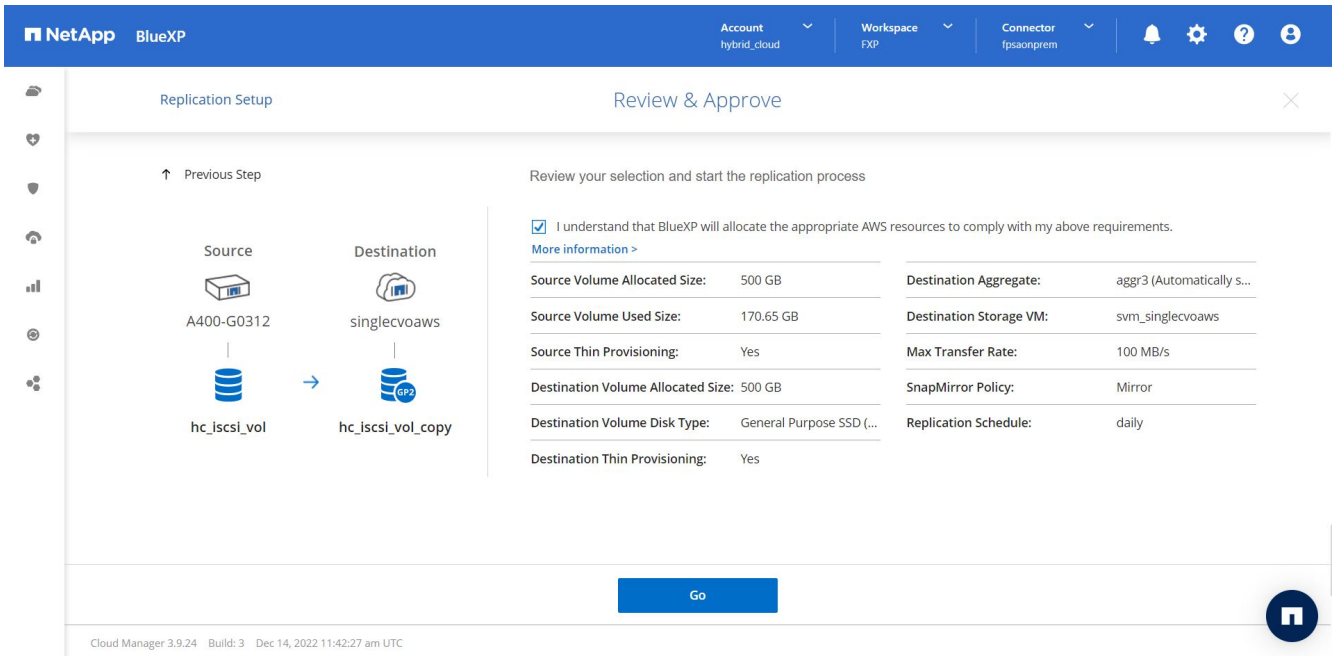
8. **Règle de réplication.** Choisissez une stratégie par défaut ou cliquez sur **règles supplémentaires**, puis sélectionnez l'une des stratégies avancées. Pour obtenir de l'aide, "en savoir plus sur les règles de réplication".



9. **Horaire.** Choisissez une copie ponctuelle ou un horaire récurrent. Plusieurs plannings par défaut sont disponibles. Si vous voulez un autre planning, vous devez créer un nouveau planning sur le `destination cluster` Utiliser System Manager.

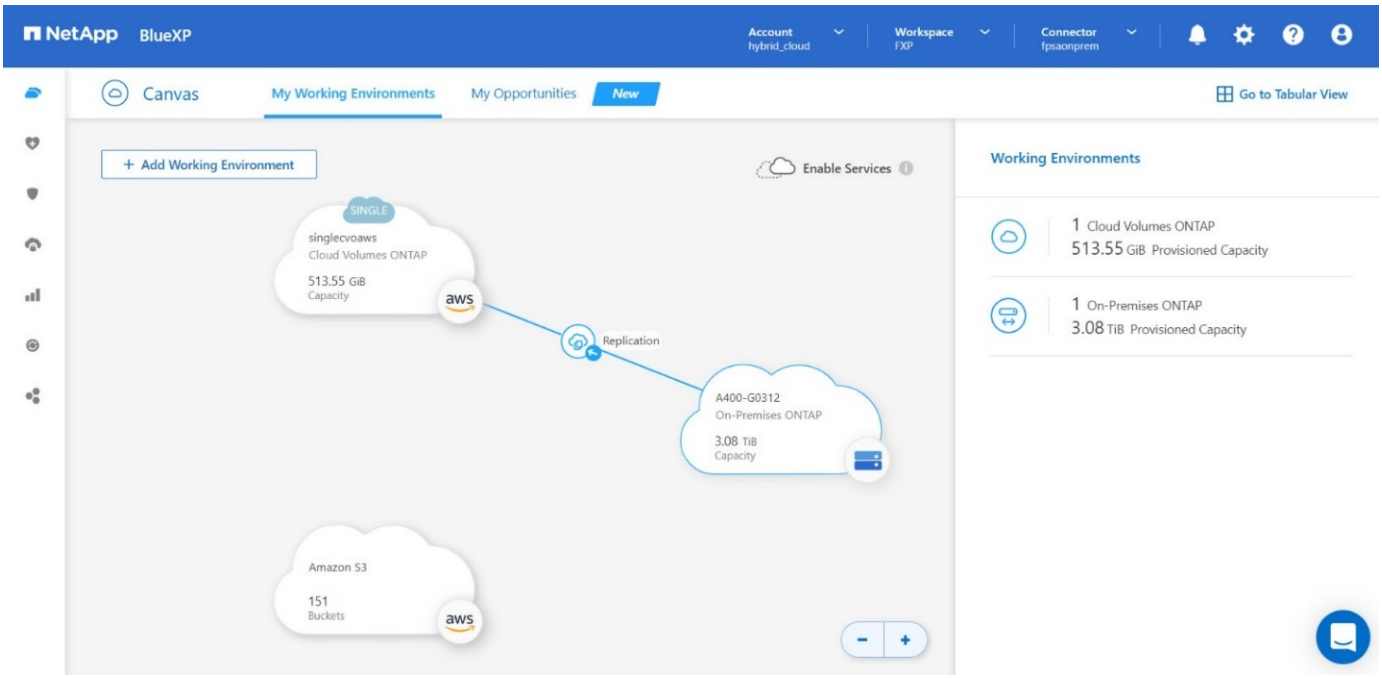


10. **Revoir.** revoir vos sélections et cliquer sur **aller**.

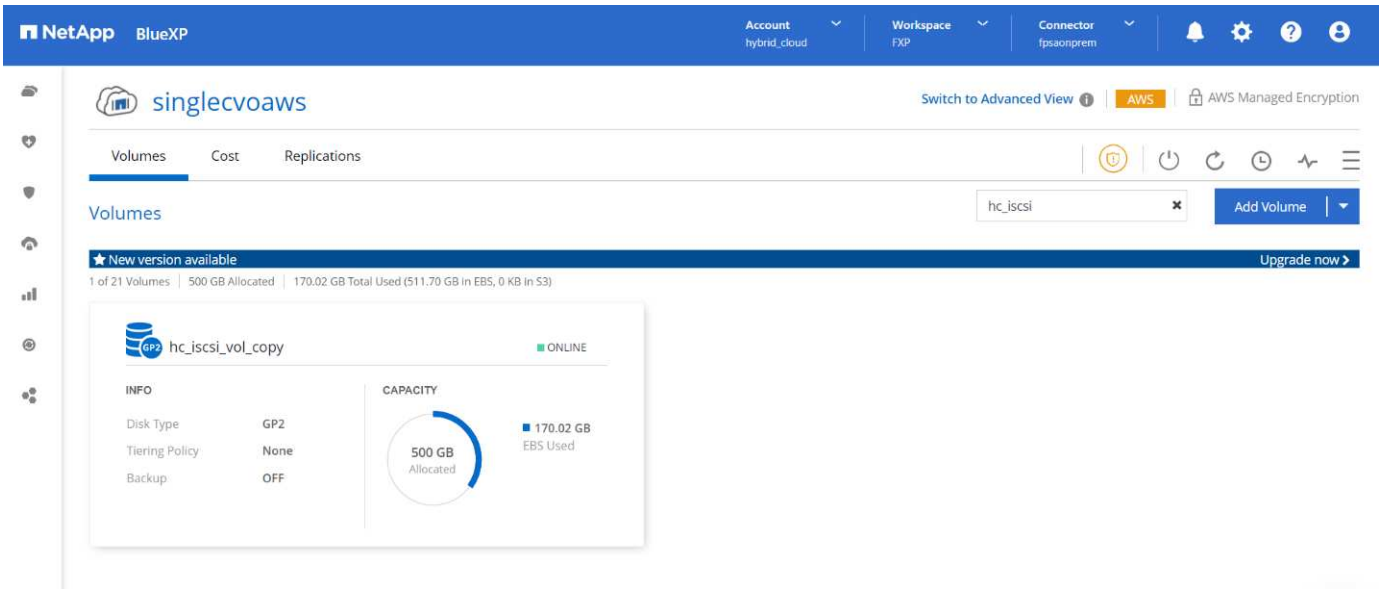


Pour plus d'informations sur ces étapes de configuration, reportez-vous à la section "ici".

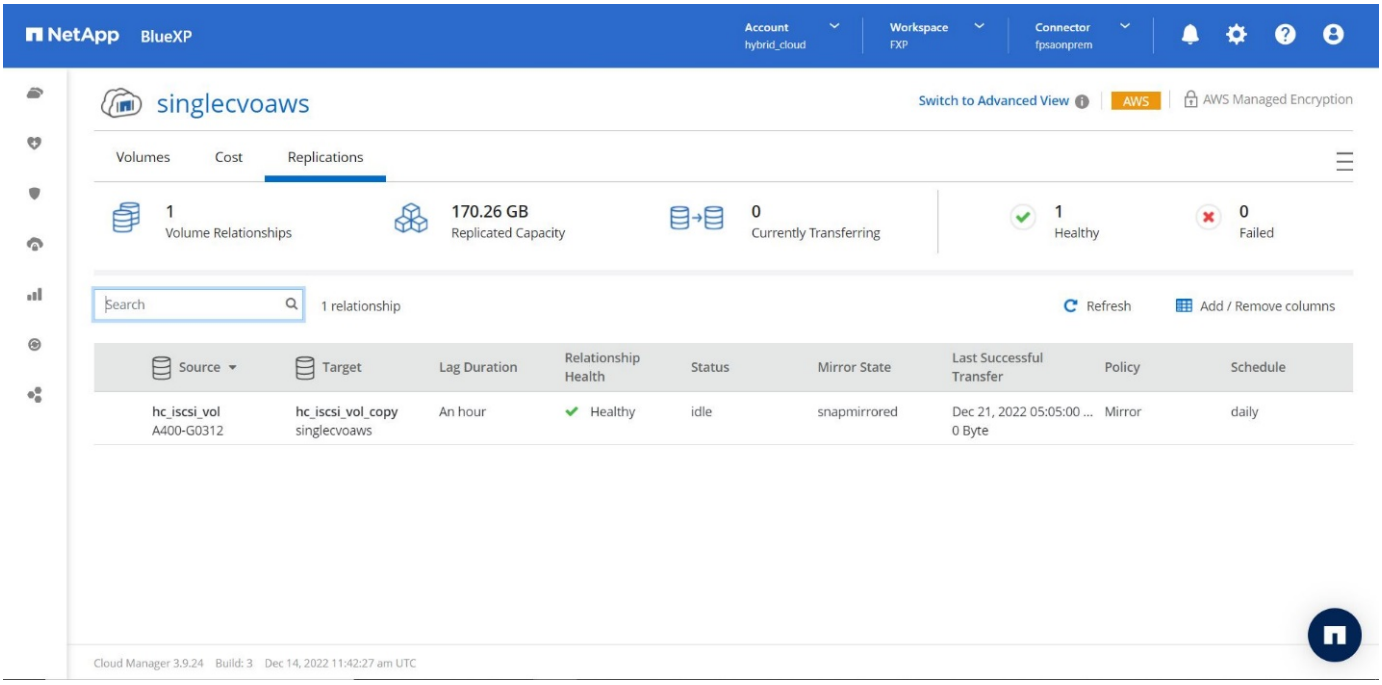
BlueXP démarre le processus de réplication des données. Maintenant, vous pouvez voir le service **Replication** qui a été établi entre votre système ONTAP sur site et Cloud Volumes ONTAP.



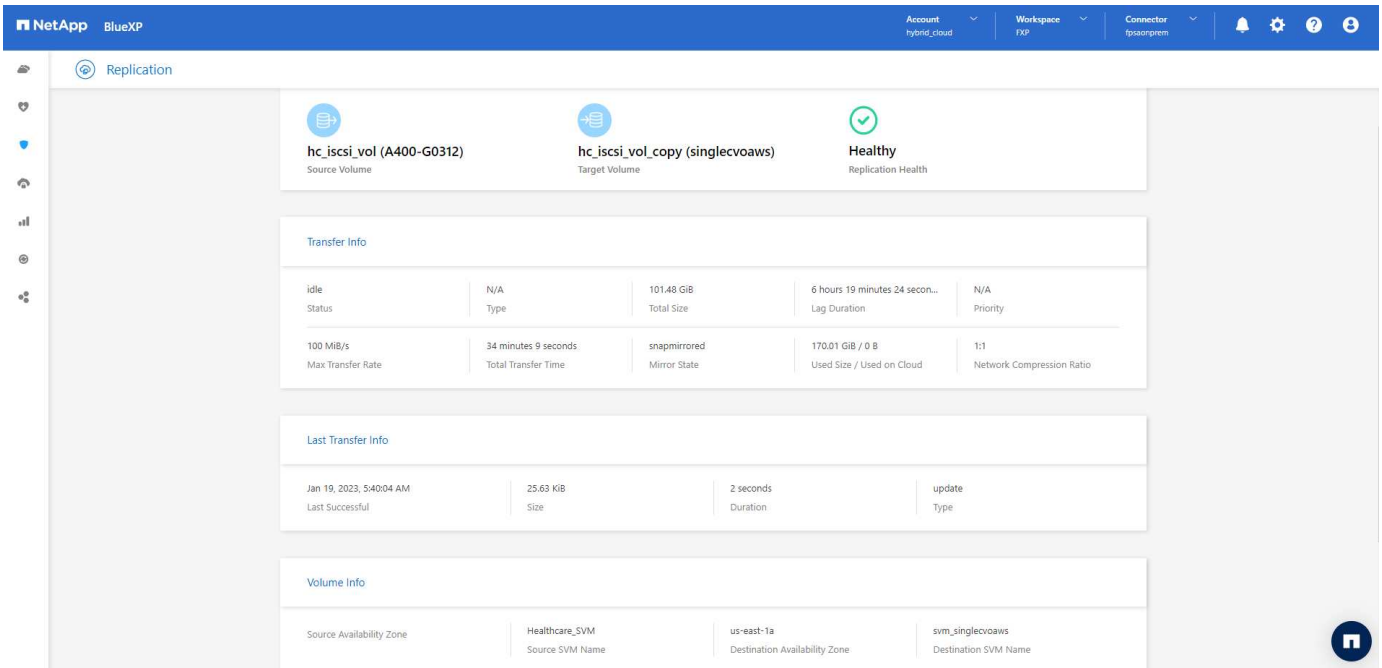
Dans le cluster Cloud Volumes ONTAP, vous pouvez afficher le volume qui vient d'être créé.



Vous pouvez également vérifier que la relation SnapMirror est établie entre le volume sur site et le volume cloud.



Pour plus d'informations sur la tâche de réplication, reportez-vous à l'onglet **Replication**.



"Ensuite, validation de la solution."

Validation des solutions

"Précédent : configuration SAN."

Cette section présente quelques cas d'utilisation de solutions.

- L'une des principales utilisations de SnapMirror est la sauvegarde des données. SnapMirror peut être utilisé en tant qu'outil de sauvegarde principal en répliquant les données au sein d'un même cluster ou vers des cibles distantes.
- Utilisation de l'environnement de reprise d'activité pour exécuter des tests de développement d'applications (développement/test)
- Reprise sur incident en cas d'incident en production.
- Distribution des données et accès aux données à distance.

Toutefois, les rares cas d'utilisation validés dans cette solution ne représentent pas l'intégralité des fonctionnalités de réplication SnapMirror.

Développement et test d'applications (développement/test)

Pour accélérer le développement d'applications, vous pouvez cloner rapidement les données répliquées au niveau du site de reprise après incident et les utiliser pour développer et tester des applications. La colocation des environnements de reprise après incident et de test et développement peut considérablement améliorer l'utilisation des installations de sauvegarde ou de reprise après incident. Les clones à la demande de test et développement fournissent autant de copies que nécessaire pour passer plus rapidement en production.

La technologie NetApp FlexClone permet de créer rapidement une copie en lecture-écriture d'un volume FlexVol de destination SnapMirror si vous souhaitez disposer d'un accès en lecture-écriture à la copie secondaire pour vérifier si toutes les données de production sont disponibles.

Procédez comme suit pour utiliser l'environnement de reprise sur incident afin d'effectuer des opérations de développement/test d'applications :

1. Faire une copie des données de production. Pour ce faire, créez une copie Snapshot d'application d'un volume sur site. La création de snapshots d'applications s'effectue en trois étapes : `Lock`, `Snap`, et `Unlock`.

   a. Mettez le système de fichiers en veille afin que les E/S soient suspendues et que les applications conservent leur cohérence. Toute application qui exécute le système de fichiers reste à l'état d'attente jusqu'à ce que la commande unquiesce soit émise à l'étape c. Les étapes a, b et c sont exécutées via un processus ou un workflow transparent qui n'affecte pas le SLA de l'application.

   ```
   [root@hc-cloud-secure-1 ~]# fsfreeze -f /file1
   ```

   Cette option demande que le système de fichiers spécifié soit bloqué à partir de nouvelles modifications. Tout processus tentant d'écrire dans le système de fichiers gelé est bloqué jusqu'à ce que le système de fichiers soit débloqué.

   b. Créez une copie Snapshot du volume sur site.

   ```
   A400-G0312::> snapshot create -vserver Healthcare_SVM -volume
   hc_iscsi_vol -snapshot kamini
   ```

   c. Annulez la mise en veille du système de fichiers pour redémarrer les E/S.

   ```
   [root@hc-cloud-secure-1 ~]# fsfreeze -u /file1
   ```

   Cette option est utilisée pour annuler le gel du système de fichiers et permettre aux opérations de continuer. Toutes les modifications du système de fichiers bloquées par le gel sont débloqués et autorisées à se terminer.

   Les copies Snapshot cohérentes au niveau des applications peuvent également être effectuées à l'aide de NetApp SnapCenter, qui dispose de l'orchestration complète du flux de travail décrit ci-dessus dans le cadre de SnapCenter. Pour plus d'informations, reportez-vous à la section "ici".

2. Effectuez une opération de mise à jour de SnapMirror pour maintenir la synchronisation des systèmes de production et de reprise après incident.

   ```
   singlecvoaws::> snapmirror update -destination-path
   svm_singlecvoaws:hc_iscsi_vol_copy -source-path
   Healthcare_SVM:hc_iscsi_vol

   Operation is queued: snapmirror update of destination
   "svm_singlecvoaws:hc_iscsi_vol_copy".
   ```

   Une mise à jour de SnapMirror peut également être effectuée via l'interface graphique BlueXP sous l'onglet **Replication**.

3. Créez une instance FlexClone à partir du snapshot d'application pris précédemment.

```
singlecvoaws::> volume clone create -flexclone kamini_clone -type RW
-parent-vserver svm_singlecvoaws -parent-volume hc_iscsi_vol_copy
-junction-active true -foreground true -parent-snapshot kamini

[Job 996] Job succeeded: Successful
```

Pour la tâche précédente, un nouvel instantané peut également être créé, mais vous devez suivre les mêmes étapes que ci-dessus pour assurer la cohérence des applications.

4. Activez un volume FlexClone pour afficher l'instance EHR dans le cloud.

```
singlecvoaws::> lun mapping create –vserver svm_singlecvoaws –path
/vol/kamini_clone/iscsi_lun1 -igroup ehr-igroup –lun-id 0

singlecvoaws::> lun mapping show
Vserver     Path                                  Igroup    LUN ID
Protocol
---------- -------------- --------------- -----  --------   ------
---------
svm_singlecvoaws
                 /vol/kamini_clone/iscsi_lun1    ehr-igroup   0    iscsi
```

5. Exécuter les commandes suivantes sur l'instance EHR dans le cloud pour accéder aux données ou au système de fichiers.
   a. Découvrez le stockage ONTAP. Vérifiez l'état des chemins d'accès multiples.

```
sudo rescan-scsi-bus.sh
sudo iscsiadm -m discovery -t sendtargets -p <iscsi-lif-ip>
sudo iscsiadm -m node -L all
sudo sanlun lun show

Output:
controller(7mode/E-Series)/         device    host             lun
vserver(cDOT/FlashRay) lun-pathname filename  adapter protocol size
product
------------------------------------------------------------------------
--------
svm_singlecvoaws                    /dev/sda  host2   iSCSI    200g
cDOT
                    /vol/kamini_clone/iscsi_lun1
sudo multipath -ll

Output:
3600a09806631755a452b543041313053 dm-0 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50'
hwhandler='1 alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
`- 2:0:0:0 sda 8:0 active ready running
```

b. Activer le groupe de volumes.

```
sudo vgchange -ay datavg
Output:
1 logical volume(s) in volume group "datavg" now active
```

c. Montez le système de fichiers et affichez le résumé des informations du système de fichiers.

```
sudo mount -t xfs /dev/datavg/datalv /file1

cd /file1
df -k .
Output:
Filesystem                 1K-blocks  Used     Available  Use%
Mounted on
/dev/mapper/datavg-datalv  209608708 183987096  25621612  88%
/file1
```

L'environnement de reprise d'activité est valide pour le développement et les tests d'applications. Les opérations de développement/test d'applications sur votre système de stockage de reprise après incident vous permettent d'exploiter davantage les ressources qui restent inactives la plupart du temps.

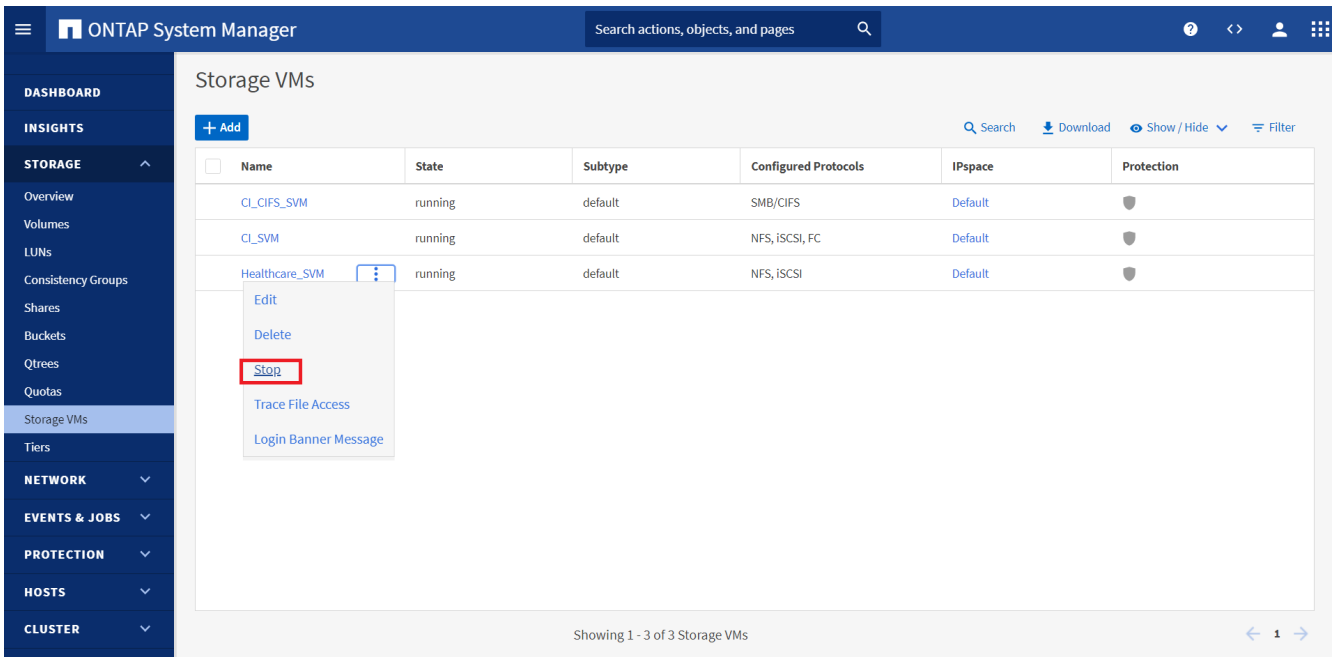
Reprise après incident

La technologie SnapMirror est également utilisée dans le cadre des plans de reprise d'activité. Si les données stratégiques sont répliquées vers un autre emplacement physique, un incident grave n'est pas nécessairement à l'origine de périodes prolongées d'indisponibilité des données pour les applications stratégiques. Les clients peuvent accéder aux données répliquées sur le réseau jusqu'à ce que le site de production soit corrompu, supprimé accidentellement, endommagé, etc.

En cas de restauration sur le site primaire, SnapMirror constitue un moyen efficace de resynchroniser le site de reprise d'activité avec le site primaire, en transférant uniquement les données nouvelles ou modifiées vers le site primaire à partir du site de reprise d'activité, simplement en inversant la relation SnapMirror. Une fois que le site de production principal a repris les opérations normales de l'application, SnapMirror poursuit le transfert vers le site de reprise après incident sans nécessiter un autre transfert de base.

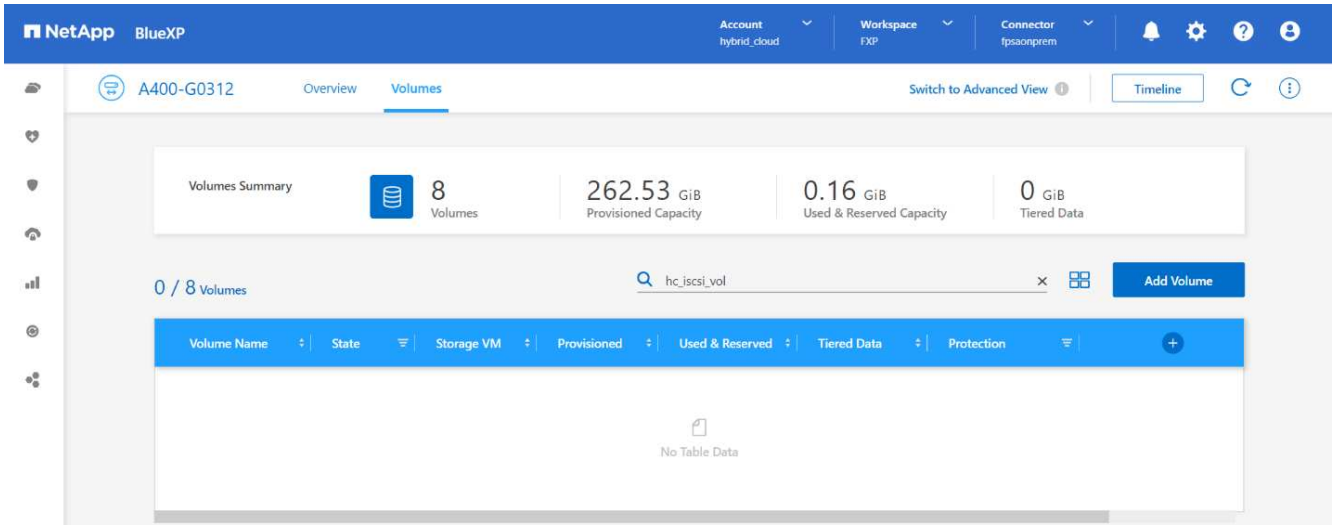
Pour effectuer la validation d'un scénario DR réussi, procédez comme suit :

1. Simuler un incident côté source (production) en arrêtant le SVM qui héberge le volume ONTAP sur site (`hc_iscsi_vol`).



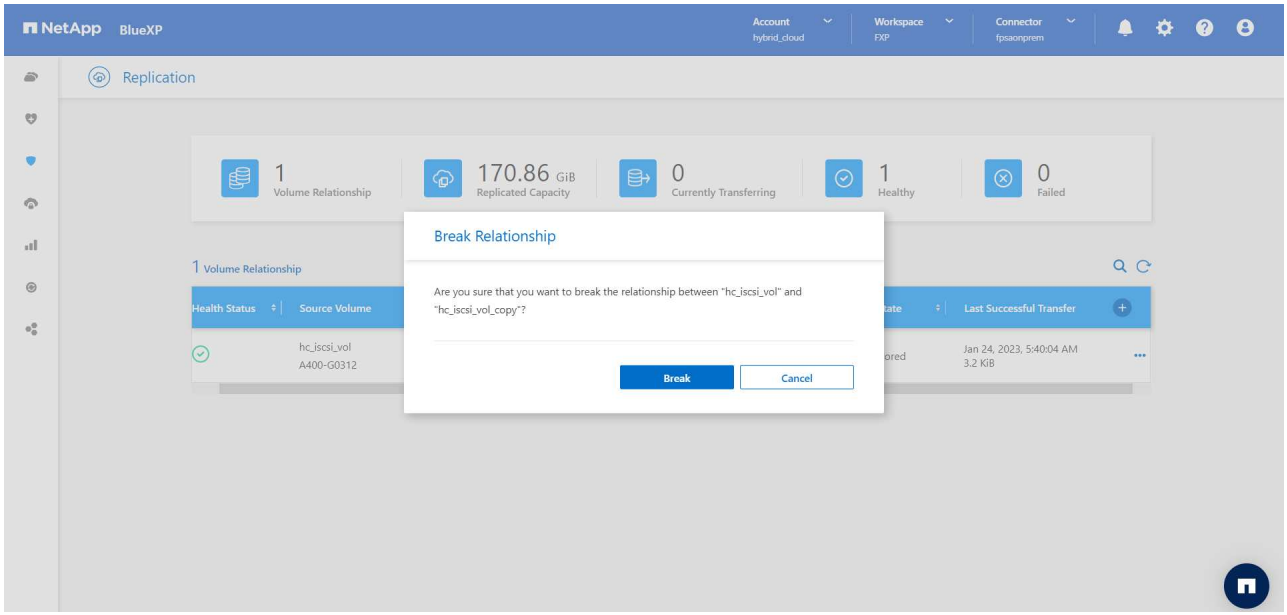
   Assurez-vous que la réplication SnapMirror est déjà configurée entre l'ONTAP sur site dans l'instance FlexPod et Cloud Volumes ONTAP dans AWS, afin de pouvoir créer fréquemment des copies Snapshot d'application.

   Après l'arrêt du SVM, le `hc_iscsi_vol` Le volume n'est pas visible dans BlueXP.



2. Activer la reprise sur incident dans CVO.

   a. Rompez la relation de réplication SnapMirror entre ONTAP sur site et Cloud Volumes ONTAP et gérez le volume de destination CVO (`hc_iscsi_vol_copy`) à la production.



   Une fois la relation SnapMirror rompue, le type de volume de destination passe de la protection des données (DP) à la lecture/écriture (RW).

```
singlecvoaws::> volume show -volume hc_iscsi_vol_copy -fields typev
server          volume             type
--------------- ----------------- ----
svm_singlecvoaws hc_iscsi_vol_copy RW
```

   b. Activez le volume de destination dans Cloud Volumes ONTAP pour afficher l'instance EHR sur une instance EC2 dans le cloud.

```
singlecvoaws::> lun mapping create –vserver svm_singlecvoaws –path
/vol/hc_iscsi_vol_copy/iscsi_lun1 -igroup ehr-igroup –lun-id 0

singlecvoaws::> lun mapping show
Vserver     Path                                Igroup   LUN ID
Protocol
---------- ----------------------------------  --------  ------
---------
svm_singlecvoaws
            /vol/hc_iscsi_vol_copy/iscsi_lun1  ehr-igroup  0    iscsi
```

c. Pour accéder aux données et au système de fichiers sur l'instance EHR dans le cloud, commencez par découvrir le stockage ONTAP et vérifiez l'état des chemins d'accès multiples.

```
sudo rescan-scsi-bus.sh
sudo iscsiadm -m discovery -t sendtargets -p <iscsi-lif-ip>
sudo iscsiadm -m node -L all
sudo sanlun lun show
Output:
controller(7mode/E-Series)/         device    host             lun
vserver(cDOT/FlashRay) lun-pathname filename  adapter protocol size
product
---------------------------------------------------------------------
--------
svm_singlecvoaws                    /dev/sda  host2   iSCSI    200g
cDOT
                  /vol/hc_iscsi_vol_copy/iscsi_lun1
sudo multipath -ll
Output:
3600a09806631755a452b543041313051 dm-0 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50'
hwhandler='1 alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
`- 2:0:0:0 sda 8:0 active ready running
```

d. Activez ensuite le groupe de volumes.

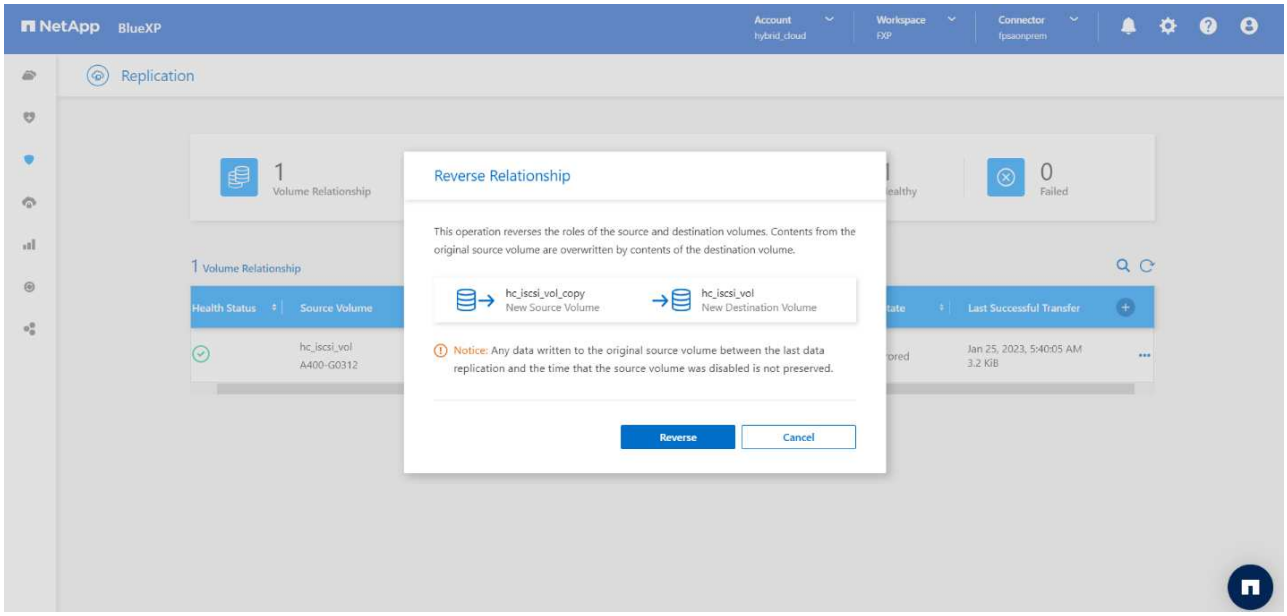
```
sudo vgchange -ay datavg
Output:
1 logical volume(s) in volume group "datavg" now active
```

e. Enfin, montez le système de fichiers et affichez les informations sur le système de fichiers.

```
sudo mount -t xfs /dev/datavg/datalv /file1

cd /file1
df -k .
Output:
Filesystem                  1K-blocks  Used      Available  Use%
Mounted on
/dev/mapper/datavg-datalv  209608708  183987096  25621612  88%
/file1
```

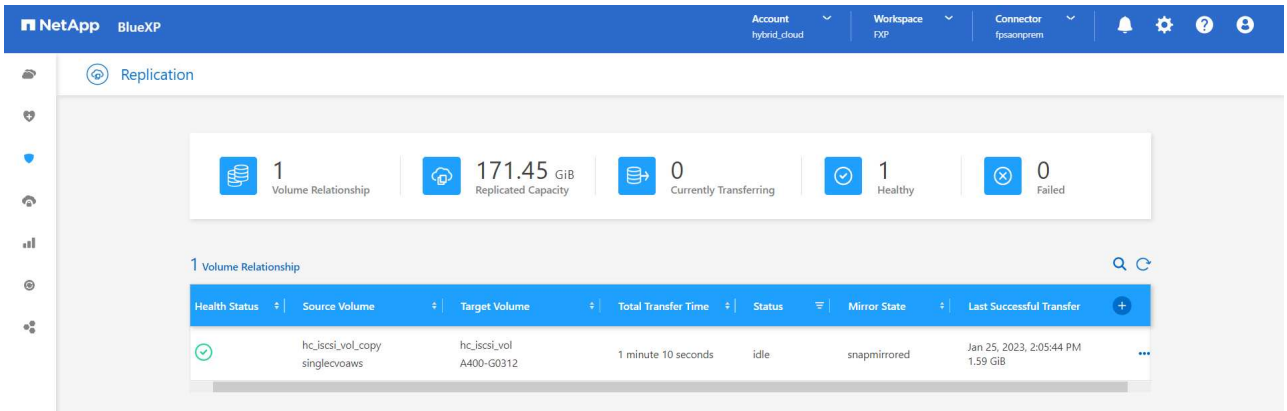
Ce résultat indique que les utilisateurs peuvent accéder aux données répliquées sur le réseau jusqu'à ce que le site de production soit récupéré après sinistre.

f. Inverser la relation SnapMirror. Cette opération inverse les rôles des volumes source et de destination.



Lorsque cette opération est effectuée, le contenu du volume source d'origine est écrasé par le contenu du volume de destination. Ceci est utile lorsque vous souhaitez réactiver un volume source hors ligne.

Désormais, le volume CVO (`hc_iscsi_vol_copy`) devient le volume source et le volume sur site (`hc_iscsi_vol`) devient le volume de destination.



Toutes les données écrites sur le volume source d'origine entre la dernière réplication de données et l'heure à laquelle le volume source a été désactivé ne sont pas conservées.

a. Pour vérifier l'accès en écriture au volume CVO, créez un nouveau fichier sur l'instance EHR dans le cloud.

```
cd /file1/
sudo touch newfile
```

Lorsque le site de production est en panne, les clients peuvent toujours accéder aux données et effectuer des écritures sur le volume Cloud Volumes ONTAP, qui est désormais le volume source.

En cas de restauration sur le site primaire, SnapMirror constitue un moyen efficace de resynchroniser le site de reprise d'activité avec le site primaire, en transférant uniquement les données nouvelles ou modifiées vers le site primaire à partir du site de reprise d'activité, simplement en inversant la relation SnapMirror. Une fois que le site de production principal a repris les opérations normales de l'application, SnapMirror poursuit le transfert vers le site de reprise après incident sans nécessiter un autre transfert de base.

Cette section illustre la résolution d'un scénario de reprise après incident lorsque le site de production est touché par un incident. Les données peuvent désormais être consommées en toute sécurité par des applications qui peuvent désormais servir les clients pendant que le site source effectue une restauration.

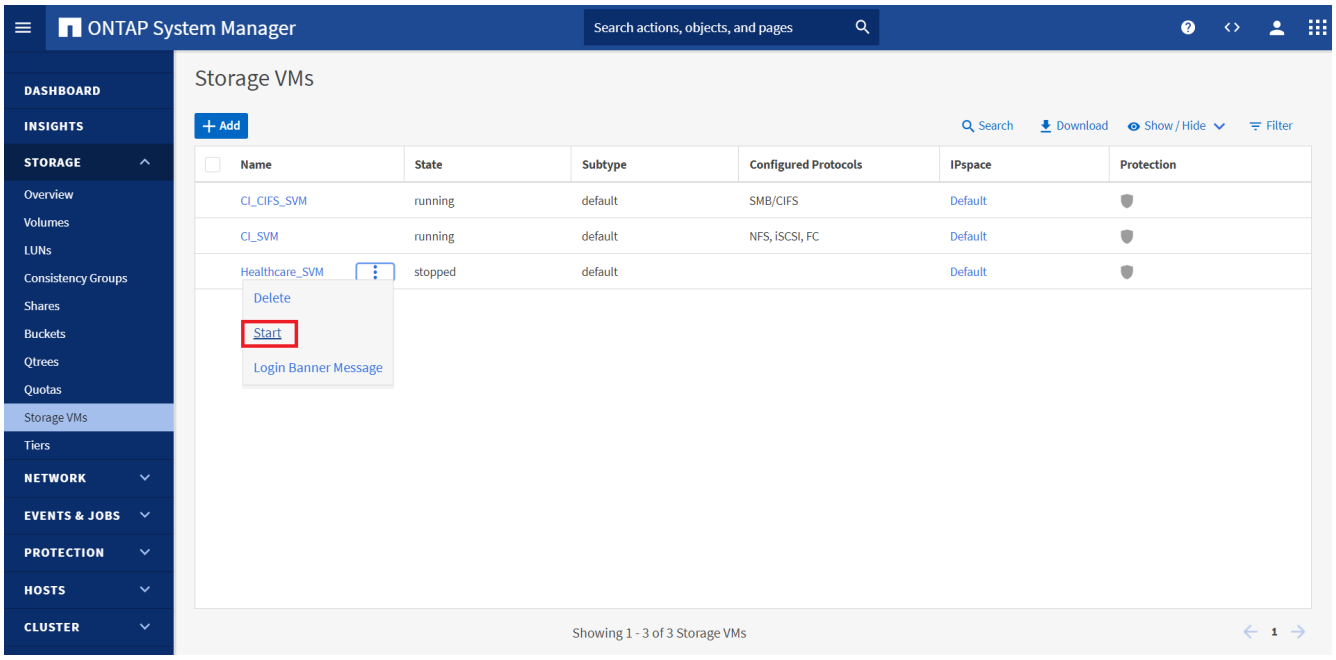
Vérification des données sur le site de production

Une fois le site de production restauré, vous devez vous assurer que la configuration d'origine est restaurée et que les clients peuvent accéder aux données à partir du site source.

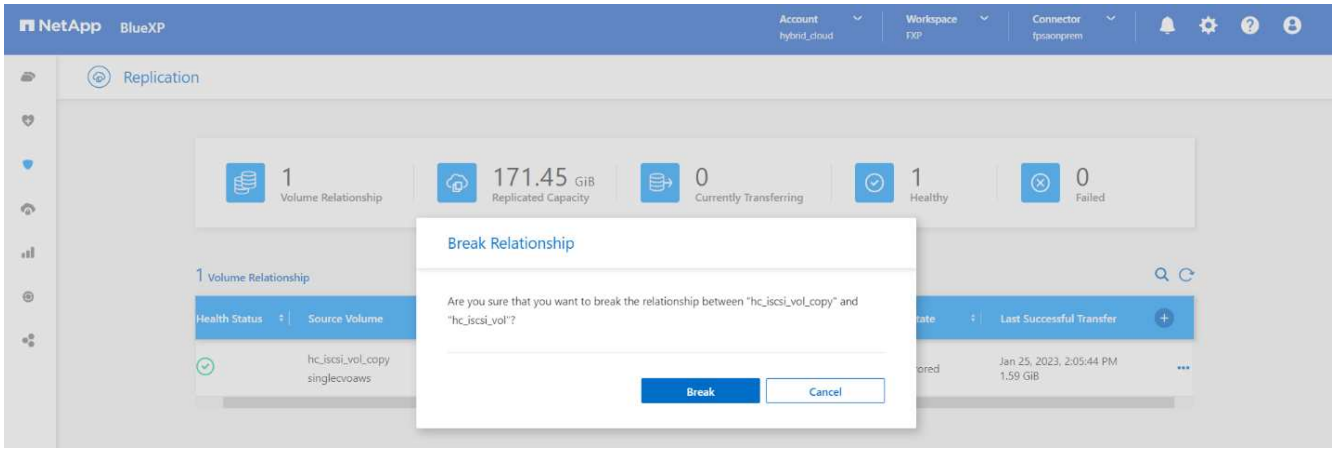
Dans cette section, nous abordons l'accès au site source et la restauration de la relation SnapMirror entre ONTAP sur site et Cloud Volumes ONTAP, puis nous avons enfin effectué un contrôle d'intégrité des données à l'extrémité source

La procédure suivante peut être utilisée pour la vérification des données sur le site de production :

1. Assurez-vous que le site source est maintenant en service. Pour ce faire, démarrer le SVM qui héberge le volume ONTAP sur site (`hc_iscsi_vol`).



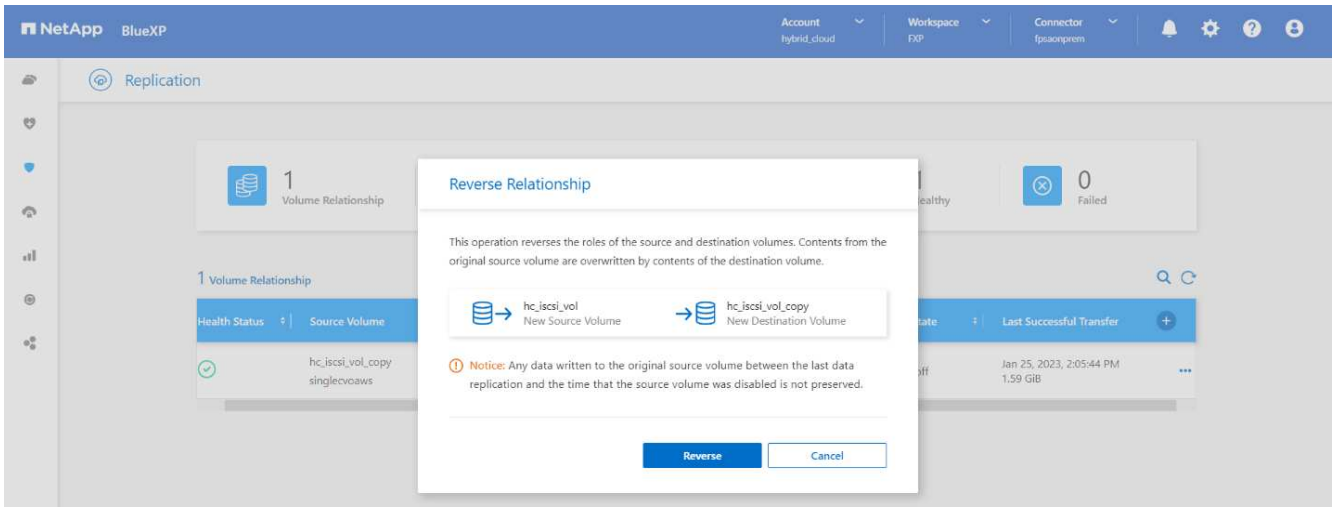
2. Rompre la relation de réplication SnapMirror entre Cloud Volumes ONTAP et ONTAP sur site et promouvoir le volume sur site (`hc_iscsi_vol`) de retour à la production.



Une fois la relation SnapMirror rompue, le type de volume sur site passe de la protection des données (DP) à la lecture/écriture (RW).

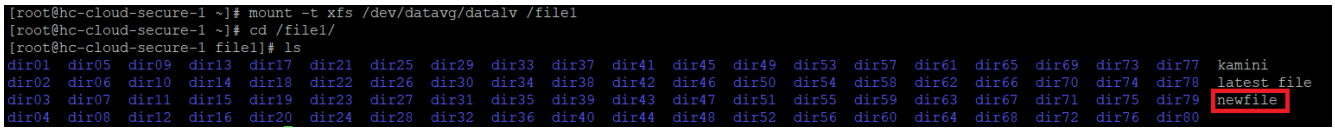
```
A400-G0312::> volume show -volume hc_iscsi_vol -fields type
vserver         volume       type
-------------- ------------ ----
Healthcare_SVM hc_iscsi_vol RW
```

3. Inverser la relation SnapMirror. Désormais, le volume ONTAP sur site (`hc_iscsi_vol`) Devient le volume source tel qu'il était précédemment, et le volume Cloud Volumes ONTAP (`hc_iscsi_vol_copy`) devient le volume de destination.



En suivant ces étapes, nous avons réussi à restaurer la configuration d'origine.

4. Redémarrez l'instance EHR sur site. Montez le système de fichiers et vérifiez que `newfile` Que vous avez créé sur l'instance EHR dans le cloud lorsque la production a été hors service existe également dans ce domaine.



Nous pouvons déduire que la réplication des données de la source vers la destination a été effectuée avec succès et que l'intégrité des données a été préservée. La vérification des données sur le site de production est terminée.

"Suivant: Conclusion."

Conclusion

"Précédent : validation de la solution."

La création d'un cloud hybride est un objectif pour la plupart des établissements de santé : garantir la disponibilité des données à tout moment. Dans cette solution, nous avons mis en œuvre une solution de cloud hybride FlexPod avec Cloud Volumes ONTAP, en utilisant la technologie de réplication NetApp SnapMirror pour valider certains cas d'utilisation afin de sauvegarder et de restaurer les applications et les charges de travail de santé.

FlexPod, une infrastructure convergée rigoureusement testée et prévalidée issue d'un partenariat stratégique entre Cisco et NetApp, est conçue pour fournir des performances système prévisibles à faible latence et une haute disponibilité. Cette approche se traduit par des niveaux de confort élevés pour les DME et, à terme, par le meilleur temps de réponse pour les utilisateurs du système EHR.

Avec NetApp, vous pouvez exécuter des opérations de production EHR, de reprise d'activité, de sauvegarde ou de Tiering dans le cloud, comme si vous exécutiez des fonctionnalités de stockage NetApp dans un data Center sur site. Avec NetApp Cloud Volumes ONTAP, NetApp fournit les fonctionnalités de grande qualité et les performances requises pour exécuter efficacement les dossiers EHR dans le cloud. Options cloud de

NetApp pour l'utilisation de blocs sur iSCSI et de fichiers sur NFS ou SMB.

Cette solution répond aux besoins des établissements de santé et leur permet de franchir le pas vers leur transformation digitale. Il peut également les aider à gérer efficacement leurs applications et leurs charges de travail.

"Suivant : où trouver des informations supplémentaires ?"

Où trouver des informations complémentaires

"Précédent: Conclusion."

Pour en savoir plus sur les informations données dans ce livre blanc, consultez ces documents et/ou sites web :

- Page d'accueil de FlexPod

  "https://www.flexpod.com"

- Guides de conception et de déploiement validés par Cisco pour FlexPod

  "https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html"

- NetApp BlueXP

  "https://bluexp.netapp.com/"

- NetApp Cloud Volumes ONTAP

  "https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/concept-overview-cvo.html"

- Démarrage rapide de Cloud Volumes ONTAP dans AWS

  "https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/task-getting-started-aws.html"

- Réplication SnapMirror

  "https://docs.netapp.com/us-en/cloud-manager-replication/concept-replication.html"

- Tr-3928 : meilleures pratiques NetApp pour Epic

  https://www.netapp.com/pdf.html?item=/media/17137-tr3928pdf.pdf

- Tr-4693 : Guide de déploiement du data Center FlexPod pour les DME EPIC

  "https://www.netapp.com/media/10658-tr-4693.pdf"

- FlexPod pour Epic

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_vmw_epic.html"

- Matrice d'interopérabilité NetApp

"http://support.netapp.com/matrix/"

- Outil d'interopérabilité matérielle et logicielle Cisco UCS

  "http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"

- Guide de compatibilité VMware

  "http://www.vmware.com/resources/compatibility/search.php"

Historique des versions

Version	Date	Historique des versions du document
Version 1.0	Mars 2023	Version initiale

FlexPod Cloud hybride pour Google Cloud Platform avec NetApp Cloud Volumes ONTAP et Cisco Intersight

Tr-4939 : Cloud hybride FlexPod pour Google Cloud Platform avec NetApp Cloud Volumes ONTAP et Cisco Intersight

Ruchika Lahoti, NetApp

Introduction

L'objectif de protection des données avec reprise après incident est essentiel à la continuité de l'activité. La reprise d'activité permet aux entreprises de basculer leurs opérations sur un emplacement secondaire, puis de restaurer et de rétablir leur fonctionnement vers le site primaire de manière efficace et fiable. Le développement d'une stratégie de reprise après incident est une priorité IT si l'on persiste avec plusieurs problèmes tels que les catastrophes naturelles, les défaillances réseau, les vulnérabilités logicielles et les erreurs humaines.

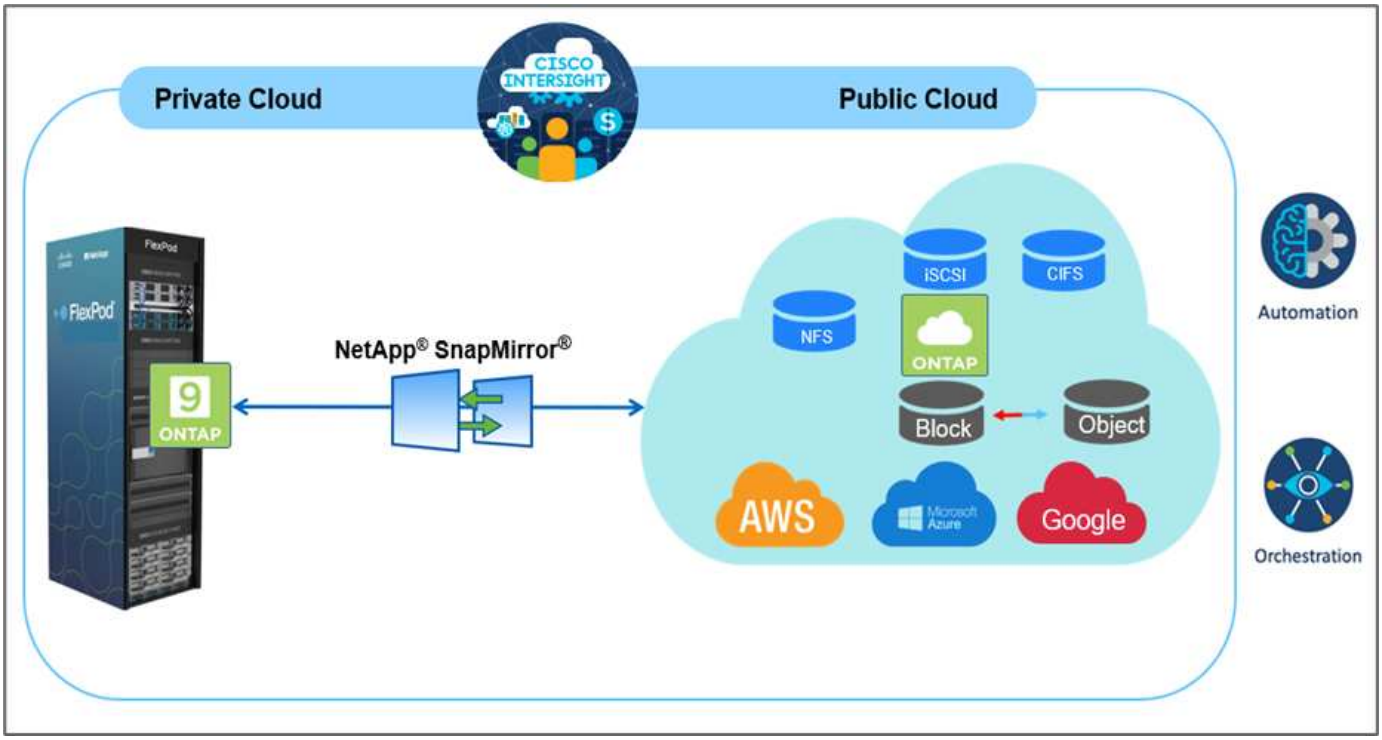
Pour la reprise après incident, toutes les charges de travail exécutées sur le site primaire doivent être fidèlement reproduites sur le site de DR. Une entreprise doit également disposer d'une copie à jour de toutes les données d'entreprise, y compris la base de données, les services de fichiers, le stockage NFS et iSCSI, etc. Comme les données de l'environnement de production sont constamment mises à jour, les modifications doivent être régulièrement transférées vers le site de reprise.

Néanmoins, pour la plupart des entreprises, déployer de tels environnements de reprise est difficile à concilier avec les exigences d'indépendance de l'infrastructure et du site. Le nombre de ressources requises et les coûts de configuration, de test et de maintenance d'un data Center secondaire peuvent être très élevés, ce qui approche généralement du coût de l'ensemble de l'environnement de production. Il est difficile de minimiser l'empreinte des données avec une protection adéquate, tout en synchronisant les données en continu et en établissant des basculements et des rétablissements transparents. Une fois le site de reprise créé, un autre défi se présente : répliquer les données depuis l'environnement de production et les synchroniser dans la suite.

Ce rapport technique rassemble la solution d'infrastructure convergée FlexPod, NetApp Cloud Volumes ONTAP sur Google Cloud et Cisco Intersight pour former un data Center dans le cloud hybride pour la reprise après incident. Dans cette solution, nous abordons la conception et l'exécution d'un workflow ONTAP sur site à l'aide de Cisco Intersight Cloud Orchestrator. Nous discutons également du déploiement de NetApp Cloud

Volumes ONTAP et de l'orchestration et l'automatisation de la réplication et de la reprise après incident des données entre FlexPod et Cloud Volumes ONTAP à l'aide du service Cisco Intersight pour HashiCorp Terraform.

Le schéma suivant fournit une présentation de la solution.



Cette solution offre de nombreux avantages, notamment :

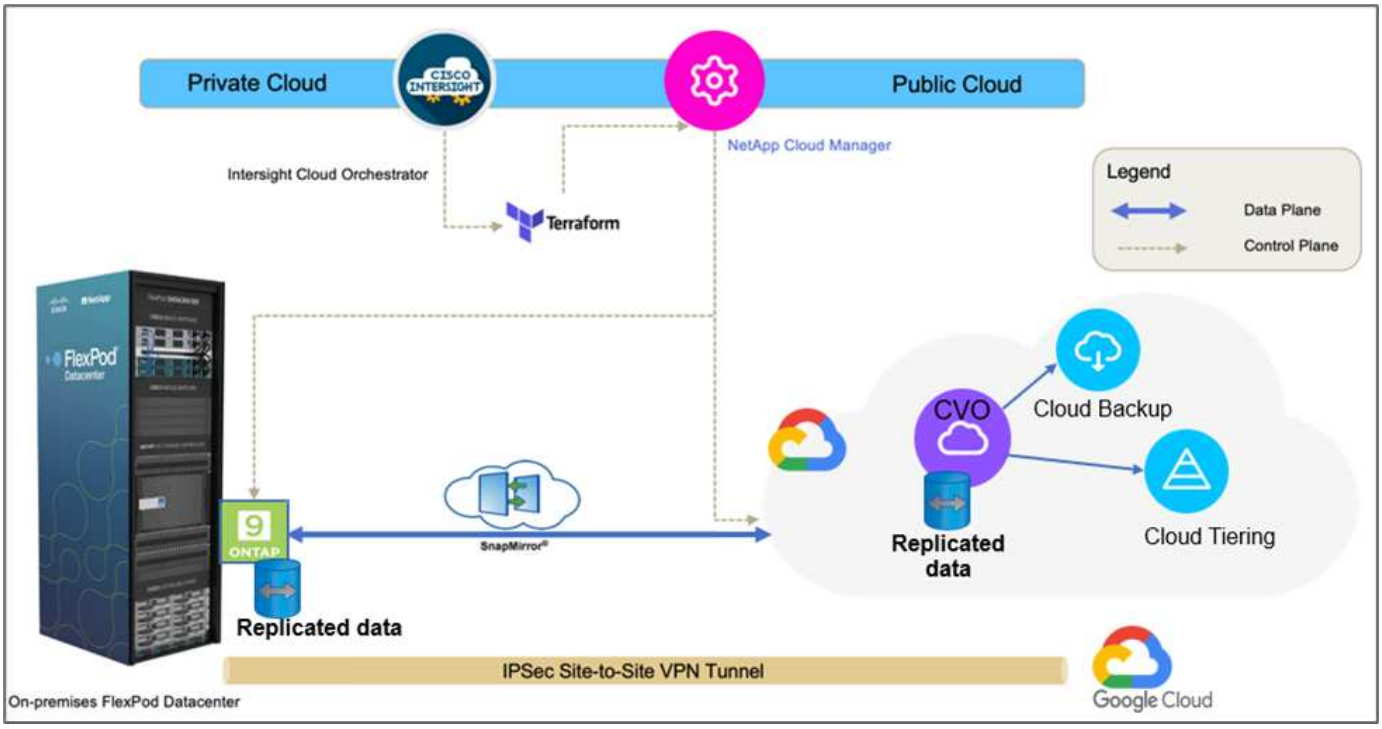
- **Orchestration et automatisation.** Cisco Intersight simplifie les opérations quotidiennes de l'infrastructure de cloud hybride FlexPod en fournissant des frameworks d'orchestration cohérents qui sont proposés via l'automatisation.
- **Protection personnalisée.** Cloud Volumes ONTAP assure la réplication des données au niveau des blocs depuis ONTAP vers le cloud afin de maintenir la destination à jour grâce à des mises à jour incrémentielles. Les utilisateurs peuvent spécifier une planification de synchronisation toutes les 5 minutes ou toutes les heures, par exemple, en fonction des modifications de la source qui sont transférées.
- **Basculement et retour arrière transparents** en cas d'incident, les administrateurs du stockage peuvent rapidement basculer vers les volumes cloud. Lorsque le site primaire est restauré, les nouvelles données créées dans l'environnement de reprise sont resynchronisées sur les volumes source et re-établissent la réplication secondaire.
- **Efficacité :** l'espace de stockage et les coûts pour la copie cloud secondaire sont optimisés grâce à la compression des données, au provisionnement fin et à la déduplication. Les données sont transférées au niveau du bloc sous forme compressée et dédupliquée, ce qui accélère le transfert. Ainsi, les données sont automatiquement transférées vers un stockage objet à faible coût et sont transférées vers un stockage haute performance uniquement lors des accès, comme dans un scénario de reprise après incident. Ceci réduit considérablement les coûts réguliers de stockage.
- * Augmentation de la productivité INFORMATIQUE.* l'utilisation d'Intersight comme plate-forme d'entreprise unique et sécurisée pour la gestion du cycle de vie de l'infrastructure et des applications simplifie la gestion de la configuration et l'automatisation des tâches manuelles à grande échelle pour la solution.

Public

Le public visé peut inclure, sans s'y limiter, les ingénieurs commerciaux, les consultants sur le terrain, les services professionnels, les responsables INFORMATIQUES, Ingénieurs partenaires, ingénieurs de fiabilité des sites, architectes cloud, ingénieurs cloud et clients qui souhaitent exploiter une infrastructure conçue pour optimiser l'efficacité IT et favoriser l'innovation IT.

Topologie de la solution

Cette section décrit la topologie logique de la solution. La figure ci-dessous illustre la topologie de la solution de l'environnement FlexPod sur site, de NetApp Cloud Volumes ONTAP exécuté sur Google Cloud, Cisco Intersight et NetApp Cloud Manager.



Les plans de contrôle et les plans de données sont clairement indiqués entre les points d'extrémité. Le plan de données utilise une connexion VPN site à site sécurisée pour connecter l'instance ONTAP exécutée sur FlexPod FAS 100 % Flash à l'instance NetApp Cloud Volumes ONTAP sur Google Cloud.

La réplication des données de charge de travail de FlexPod vers NetApp Cloud Volumes ONTAP est gérée par NetApp SnapMirror. Le processus global est orchestré à l'aide de Cisco Intersight Cloud Orchestrator pour les environnements sur site et cloud. Cisco Intersight Cloud Orchestrator utilise les fournisseurs de ressources Terraform pour NetApp Cloud Manager pour effectuer des opérations liées au déploiement de NetApp Cloud Volumes ONTAP et établir des relations de réplication des données.

> Cette solution prend également en charge la sauvegarde et le Tiering des données inactives résidant dans l'instance NetApp Cloud Volumes ONTAP vers Google Cloud Storage.

"Ensuite, les composants de la solution."

Composants de la solution

"Précédent : présentation de la solution."

FlexPod

FlexPod est un ensemble défini de matériels et de logiciels qui constitue une base intégrée pour les solutions virtualisées et non virtualisées. FlexPod inclut le stockage NetApp ONTAP, les réseaux Cisco Nexus, les réseaux de stockage Cisco MDS et Cisco Unified Computing System (Cisco UCS). La conception est suffisamment flexible pour que le réseau, le calcul et le stockage puissent s'intégrer dans un seul rack de data Center ou être déployés selon la conception du centre de données du client. La densité des ports permet aux composants réseau de prendre en charge plusieurs configurations.

Cisco Intersight

Cisco Intersight est une plateforme SaaS qui assure une automatisation, une observabilité et une optimisation intelligentes pour les applications et l'infrastructure classiques et cloud. La plateforme permet de stimuler les évolutions avec les équipes IT et propose un modèle d'exploitation conçu pour le cloud hybride. Cisco Intersight offre les avantages suivants :

- **Livraison plus rapide.** livraison en tant que service depuis le cloud ou dans le centre de données du client avec des mises à jour fréquentes et une innovation continue, grâce à un modèle de développement logiciel agile. Le client peut ainsi se concentrer sur l'accélération de la livraison pour le secteur d'activité.
- **Opérations simplifiées.** simplifier les opérations en utilisant un seul outil SaaS sécurisé avec inventaire, authentification et API communs pour travailler sur l'ensemble de la pile et tous les emplacements, éliminant ainsi les silos entre les équipes. De la gestion des serveurs physiques et des hyperviseurs sur site aux machines virtuelles, K8s, sans serveur, automatisation, l'optimisation et le contrôle des coûts à la fois sur site et dans les clouds publics.
- **Optimisation continue.** optimisation continue de votre environnement en utilisant l'intelligence fournie par Cisco Intersight sur chaque couche, ainsi que Cisco TAC. Cette intelligence est convertie en actions recommandées et automatisés, qui vous permettent de vous adapter en temps réel à chaque changement : du déplacement des charges de travail et du contrôle de l'état des serveurs physiques aux recommandations de réduction des coûts des clouds publics avec lesquels vous travaillez.

Il existe deux modes d'opérations de gestion possibles avec Cisco Intersight : Umm (UCSM Managed mode) et IMM (Intersight Managed mode). Vous pouvez sélectionner UMM natif ou IMM pour les systèmes Cisco UCS rattachés au fabric lors de la configuration initiale des interconnexions de fabric. Dans cette solution, l'IMM native est utilisé.

Licences Cisco Intersight

Cisco Intersight utilise une licence basée sur un abonnement avec plusieurs niveaux.

Les niveaux de licence Cisco Intersight sont les suivants :

- **Cisco Intersight Essentials.** inclut toutes les fonctionnalités de base ainsi que les fonctionnalités suivantes :
  - Cisco UCS Central
  - Droit Cisco IMC Supervisor
  - Configuration basée sur des règles avec profils de serveur
  - Gestion du firmware
  - Évaluation de la compatibilité avec la liste de compatibilité matérielle (HCL)
- **Cisco Intersight Advantage.** comprend les fonctionnalités du niveau Essentials ainsi que les fonctionnalités suivantes :
  - Widgets, inventaire, capacité, fonctionnalités d'utilisation et corrélation des inventaires interdomaines

sur l'ensemble des ressources de calcul physique, réseau, stockage, virtualisation VMware et cloud public AWS.
    - Service de conseil de sécurité Cisco où les clients peuvent recevoir d'importantes alertes de sécurité et des notifications sur site sur les périphériques de point final affectés.
- **Cisco Intersight Premier.** en plus des capacités offertes par le niveau avantage, Cisco Intersight Premier propose les éléments suivants :
    - Intersight Cloud Orchestrator (ICO) pour les ressources de calcul, de réseau, de stockage, de systèmes intégrés, de virtualisation, des plateformes de conteneur et de cloud public
    - Droit d'abonnement complet pour Cisco UCS Director sans frais supplémentaires.

Vous trouverez plus d'informations sur les licences Intersight et les fonctionnalités prises en charge dans chaque licence "ici".

> Dans cette solution, nous utilisons Intersight Cloud Orchestrator et Intersight Service pour HashiCorp Terraform. Ces fonctionnalités sont disponibles pour les utilisateurs disposant de la licence Intersight Premier. Par conséquent, ce niveau de licence doit être activé.

Intégration du cloud Terraform avec ICO

Vous pouvez utiliser Cisco Intersight Cloud Orchestrator (ICO) pour créer et exécuter des workflows qui appellent les API Terraform Cloud (TFC). La tâche Invoke Web API Request prend en charge Terraform Cloud comme cible et peut être configurée avec les API Terraform Cloud via des méthodes HTTP. Le workflow peut donc avoir une combinaison de tâches qui appellent plusieurs API Terraform Cloud à l'aide de tâches API génériques et d'autres opérations. Vous devez disposer d'une licence Premier pour utiliser la fonction ICO.

Assistance Cisco Intersight

Cisco Intersight aide à ajouter des périphériques de terminaison à Cisco Intersight. Un centre de données peut avoir plusieurs périphériques qui ne se connectent pas directement à Cisco Intersight. Tout périphérique pris en charge par Cisco Intersight mais qui ne se connecte pas directement à celui-ci nécessite un mécanisme de connexion. Cisco Intersight fournit ce mécanisme de connexion et vous aide à ajouter des périphériques à Cisco Intersight.

Cisco Intersight Assist est disponible au sein de Cisco Intersight Virtual Appliance, qui est distribué sous la forme d'une machine virtuelle déployable contenue dans un format de fichier OVA (Open Virtual Appliance). Vous pouvez installer l'appliance sur un serveur ESXi. Pour plus d'informations, reportez-vous à la section "Guide de mise en route de Cisco Intersight Virtual Appliance".

Après avoir réclamé Intersight Assist dans Intersight, vous pouvez demander des périphériques de terminaison à l'aide de l'option réclamation via Intersight Assist. Pour plus d'informations, voir "Mise en route".

NetApp Cloud Volumes ONTAP

- Exploitation de la déduplication intégrée et de la compression des données, du provisionnement fin et du clonage pour réduire les coûts de stockage.
- Nous garantissons une fiabilité exceptionnelle et la continuité de l'activité en cas de défaillances dans votre environnement cloud.
- Cloud Volumes ONTAP utilise la technologie de réplication leader de NetApp SnapMirror pour répliquer les données sur site vers le cloud. Les copies secondaires sont ainsi disponibles dans différents cas d'utilisation.
- Cloud Volumes ONTAP s'intègre également avec Cloud Backup Service pour fournir des fonctionnalités de

sauvegarde et de restauration pour une protection et un archivage à long terme de vos données cloud.

- Basculer à la demande entre des pools de stockage hautes performances et faibles performances, sans mettre les applications hors ligne.
- Cohérence des copies Snapshot avec NetApp SnapCenter.
- Cloud Volumes ONTAP prend en charge le cryptage des données et protège contre les virus et les attaques par ransomware.
- L'intégration avec Cloud Data SENSE vous aide à comprendre le contexte des données et à identifier les données sensibles.

Cloud Central

Cloud Central est une plateforme centralisée qui permet d'accéder aux services de données cloud NetApp et de les gérer. Ces services vous permettent d'exécuter des applications stratégiques dans le cloud, de créer des sites de reprise après incident automatisés, de sauvegarder vos données SaaS et de migrer et contrôler efficacement les données sur plusieurs clouds. Pour plus d'informations, voir "Cloud Central".

Le gestionnaire Cloud

Cloud Manager est une plateforme de gestion SaaS de grande qualité qui permet aux experts IT et aux architectes cloud de gérer de manière centralisée leur infrastructure multicloud hybride à l'aide des solutions cloud NetApp. Elle offre un système centralisé pour afficher et gérer vos ressources de stockage sur site et cloud afin de prendre en charge plusieurs fournisseurs et comptes de cloud hybride. Pour plus d'informations, voir "Le gestionnaire Cloud".

Connecteur

Connector permet à Cloud Manager de gérer les ressources et les processus dans un environnement de cloud public. Une instance de connecteur est requise pour utiliser de nombreuses fonctionnalités fournies par Cloud Manager et peut être déployée dans le réseau dans le cloud ou sur site. Le connecteur est pris en charge aux emplacements suivants :

- AWS
- Microsoft Azure
- Google Cloud
- Sur site

NetApp Active IQ Unified Manager

Avec NetApp Active IQ Unified Manager, vous pouvez contrôler vos clusters de stockage ONTAP à partir d'une interface intuitive unique, reconçue pour l'intelligence artificielle et les connaissances de la communauté. Il offre des informations complètes sur les opérations, les performances et le mode proactif de l'environnement de stockage et des machines virtuelles qui s'exécutent sur celui-ci. Lorsqu'un problème se produit avec l'infrastructure de stockage, Unified Manager vous informe des détails du problème pour vous aider à identifier la cause première. Le tableau de bord des machines virtuelles vous offre un aperçu des statistiques de performances de la machine virtuelle. Vous pouvez ainsi examiner l'ensemble du chemin d'E/S depuis l'hôte vSphere vers le réseau, et enfin vers le stockage.

Certains événements fournissent également des mesures correctives que vous pouvez prendre pour corriger le problème. Vous pouvez configurer des alertes personnalisées en cas d'événements afin que, lorsque des problèmes se produisent, vous soyez averti par e-mail et des interruptions SNMP. Active IQ Unified Manager vous permet de planifier les besoins en stockage de vos utilisateurs en anticipant les besoins en stockage et

en vous permettant d'anticiper les problèmes, ce qui évite de prendre des décisions réactives à court terme et même d'engendrer des problèmes supplémentaires à long terme.

VMware vSphere

VMware vSphere est une plateforme de virtualisation qui permet de gérer de manière holistique de vastes ensembles d'infrastructures (ressources notamment les processeurs, le stockage et le réseau), sous la forme d'un environnement d'exploitation transparent, polyvalent et dynamique. Contrairement aux systèmes d'exploitation traditionnels qui gèrent une machine individuelle, VMware vSphere agrège l'infrastructure d'un data Center dans son ensemble pour créer une seule puissance avec des ressources qui peuvent être allouées rapidement et dynamiquement à n'importe quelle application, selon les besoins.

Pour plus d'informations sur VMware vSphere, veuillez suivre "ce lien".

VMware vSphere vCenter

VMware vCenter Server assure une gestion unifiée de tous les hôtes et machines virtuelles depuis une console unique et rassemble le contrôle des performances des clusters, des hôtes et des machines virtuelles. VMware vCenter Server offre aux administrateurs des informations détaillées sur l'état et la configuration des clusters de calcul, des hôtes, des VM, du stockage, du système d'exploitation invité, et autres composants essentiels d'une infrastructure virtuelle. VMware vCenter gère la richesse des fonctionnalités disponibles dans un environnement VMware vSphere.

Versions matérielles et logicielles

Cette solution de cloud hybride peut être étendue à tout environnement FlexPod qui exécute des versions logicielles, matérielles et de firmware prises en charge telles que définies dans la matrice d'interopérabilité NetApp et dans la liste de compatibilité matérielle Cisco UCS.

La solution FlexPod utilisée comme plateforme de base dans notre environnement sur site a été déployée selon les instructions et les spécifications décrites "ici".

Le réseau au sein de cet environnement est basé sur l'ACI. Pour plus d'informations, voir "ici".

- Consultez les liens suivants pour plus d'informations :
- "Matrice d'interopérabilité NetApp"
- "Guide de compatibilité VMware"
- "Outil d'interopérabilité matérielle et logicielle Cisco UCS"

Le tableau suivant présente les révisions matérielles et logicielles de FlexPod.

Composant	Solution NetApp	Version
Calcul	CISCO UCS X210C-M6	5.0(1b)
	Cisco UCS Fabric Interconnect 6454	4.2(2a)
Le réseau	Cisco Nexus 9332C (Rachis)	14.2(7)
	Cisco Nexus 9336C-FX2 (feuille)	14.2(7)
	ACI Cisco	4.2(7)
Stockage	Avec AFF A220	9.11.1

Composant	Solution NetApp	Version
	Outils NetApp ONTAP pour VMware vSphere	9.10
	Plug-in NetApp NFS pour VMware VAAI	2.0-15
	Active IQ Unified Manager	9.11
Logiciel	VSphere ESXi	7.0(U3)
	Appliance VMware vCenter	7.0.3
	Appliance virtuelle Cisco InterSight Assist	1.0.11-306

L'exécution des configurations Terraform s'effectue sur le compte Terraform Cloud for Business. La configuration Terraform utilise le fournisseur Terraform pour NetApp Cloud Manager.

Le tableau suivant répertorie les fournisseurs, les produits et les versions.

Composant	Solution NetApp	Version
HashiCorp	Terraform	1.2.7

Le tableau suivant présente les versions de Cloud Manager et de Cloud Volumes ONTAP.

Composant	Solution NetApp	Version
NetApp	Cloud Volumes ONTAP	9.11
	Le gestionnaire Cloud	3.9.21

"Suivant : installation et configuration - déployer FlexPod."

Installation et configuration

Déployez FlexPod

"Précédent : composants de la solution."

Pour comprendre les détails de la conception et du déploiement de FlexPod, notamment la configuration de différents éléments de la conception et des meilleures pratiques associées, consultez la section "Conceptions validées par Cisco pour FlexPod".

FlexPod peut être déployé à la fois en mode géré UCS et en mode géré Cisco InterSight. Si vous déployez FlexPod en mode géré UCS, vous trouverez la dernière conception validée Cisco "ici".

Cisco Unified Computing System (Cisco UCS) X-Series est un tout nouveau système de calcul modulaire, configuré et géré à partir du cloud. Elle est conçue pour répondre aux besoins des applications modernes et pour améliorer l'efficacité opérationnelle, l'agilité et l'évolutivité au travers d'un design modulaire, adaptable et prêt pour le futur. Vous trouverez des conseils de conception concernant l'intégration de la plateforme UCS X-Series gérée par Cisco Intersight dans l'infrastructure FlexPod "ici".

FlexPod avec Cisco ACI est disponible "ici".

"Suivant : configuration Cisco Intersight."

Configuration Cisco Intersight

"Précédent : déployer FlexPod."

Pour configurer Cisco Intersight et Intersight, consultez les conceptions validées par Cisco pour FlexPod trouvées "ici".

"Suivant : intégration du cloud Terraform avec la condition préalable d'ICO."

Terraform intégration au cloud avec une condition préalable de l'ICO

"Précédent : configuration Cisco Intersight."

Procédure 1 : connecter Cisco Intersight et Terraform Cloud

1. Faites une demande de remboursement ou créez une cible cloud Terraform en fournissant les informations pertinentes sur le compte Terraform Cloud.
2. Créez une cible Terraform Cloud Agent pour les clouds privés afin que les clients puissent installer l'agent dans le data Center et activer la communication avec Terraform Cloud.

   Pour plus d'informations, veuillez consulter la section "ce lien".

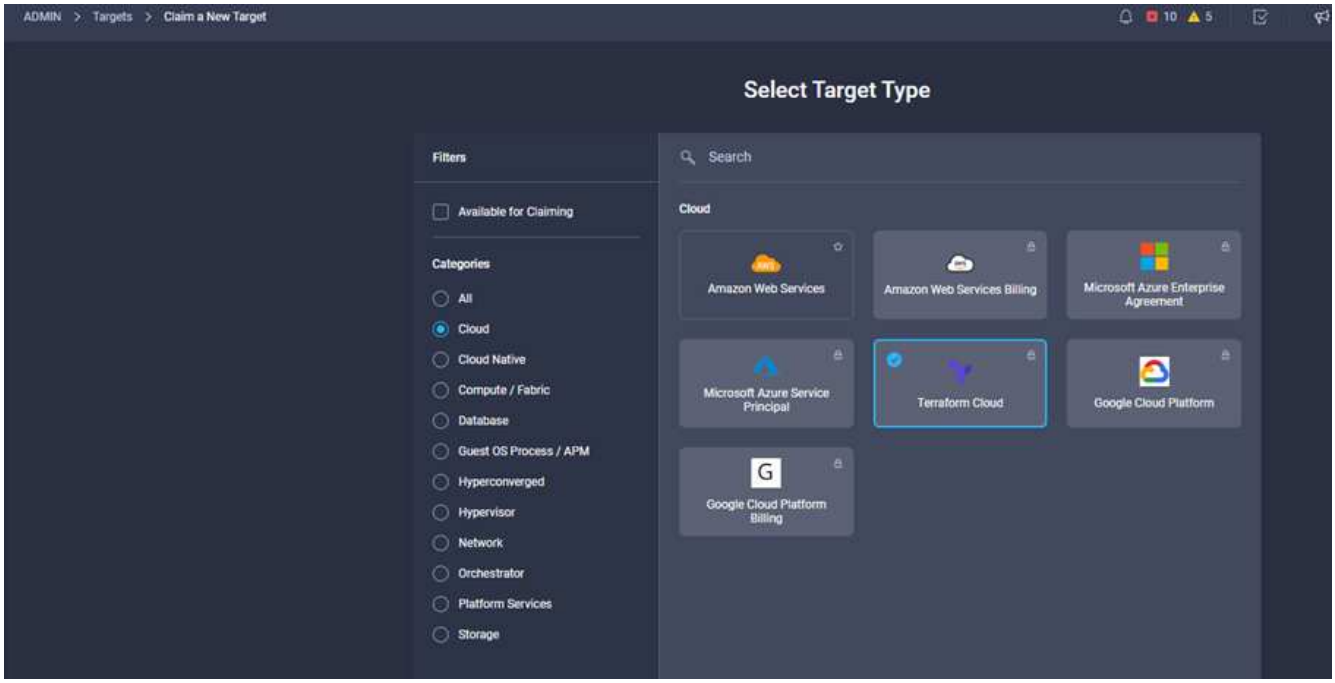
Procédure 2 : générer un jeton utilisateur

Dans le cadre de l'ajout d'une cible pour Terraform Cloud, vous devez fournir le nom d'utilisateur et le jeton d'API à partir de la page des paramètres Terraform Cloud.

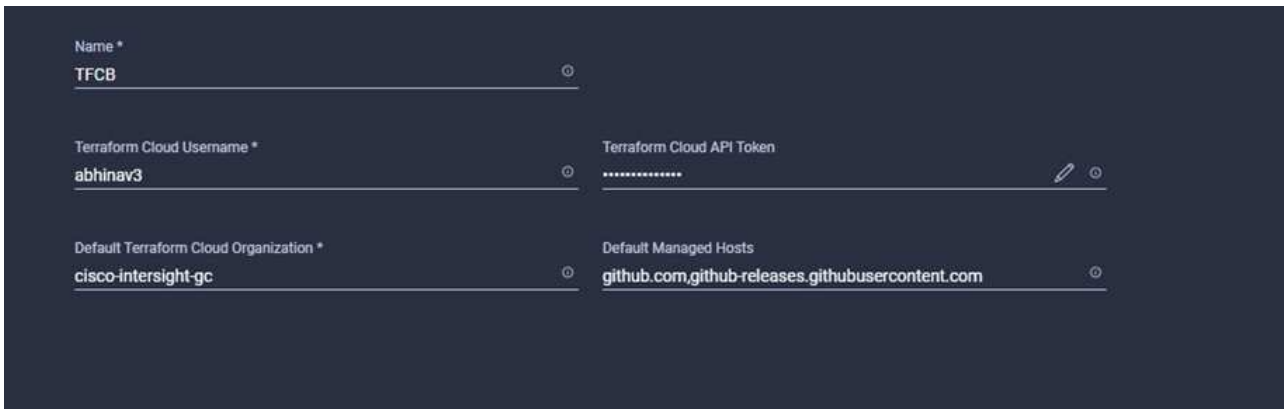
1. Connectez-vous à Terraform Cloud et accédez à **User Tokens** : "https://app.terraform.io/app/settings/tokens".
2. Cliquez sur **Créer un nouveau jeton API**.
3. Attribuez un nom à mémoriser et enregistrez le token dans un endroit sécurisé.

Procédure 3 : cible de cloud de demande Terraform

1. Connectez-vous à Intersight avec les privilèges Administrateur de compte, Administrateur de périphérique ou technicien de périphérique.
2. Accédez à **ADMIN > Targets > Claim a New Target**.
3. Dans **Categories**, cliquez sur **Cloud**.
4. Cliquez sur **Terraform Cloud** et cliquez sur **Start**.



5. Entrez un nom pour la cible, votre nom d'utilisateur pour le Terraform Cloud, le jeton API et une organisation par défaut dans Terraform Cloud comme indiqué dans l'image suivante.
6. Dans le champ **Default Managed Hosts**, assurez-vous d'ajouter les liens suivants avec d'autres hôtes gérés :
   - github.com
   - github-releases.githubusercontent.com



Si tout est correctement saisi, votre cible Terraform Cloud s'affiche dans la section **cibles Intersight**.

Procédure 4 : ajouter des agents Terraform Cloud

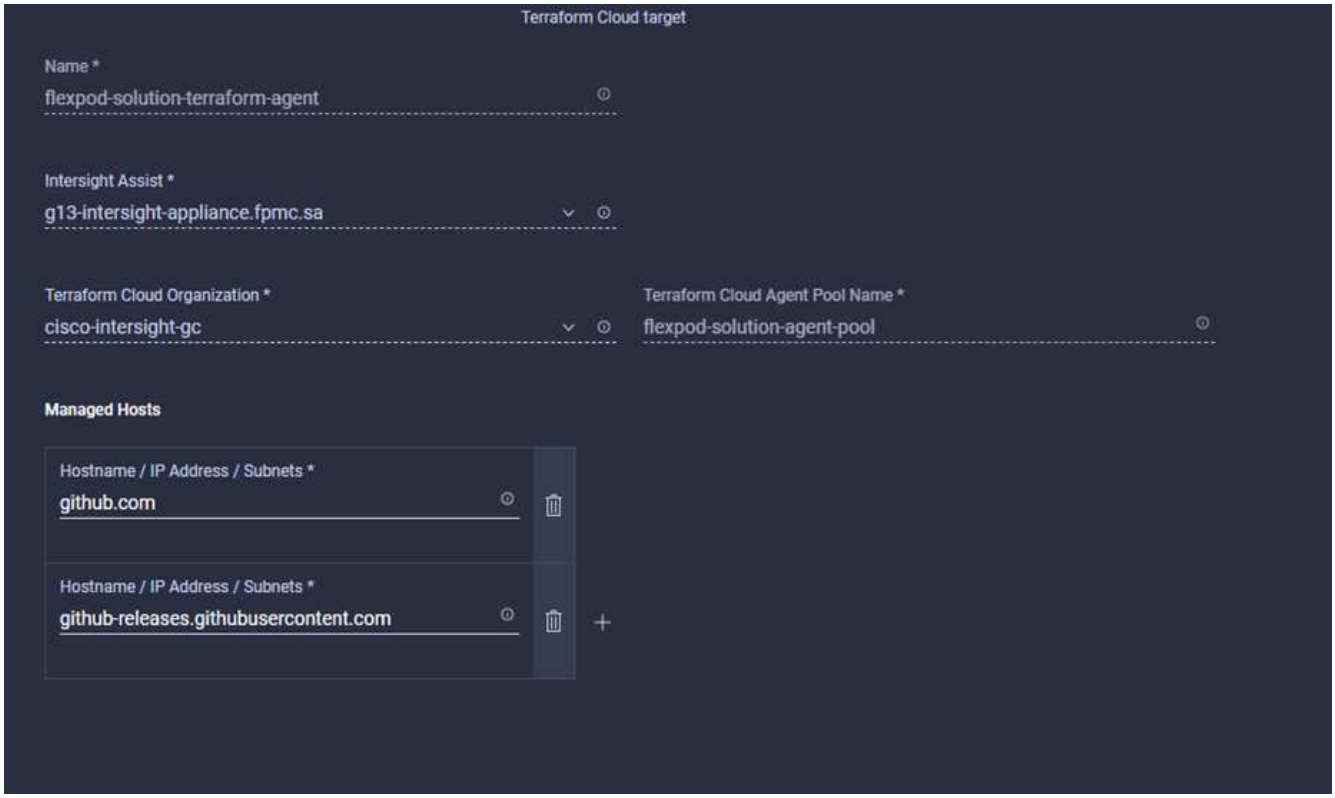
Prérequis :

- Cible Terraform Cloud.
- Demande d'assistance Intersight dans Intersight avant de déployer l'agent Cloud Terraform.

> Vous ne pouvez demander que cinq agents pour chaque assistance.

Après avoir créé la connexion à Terraform, vous devez faire tourner un agent Terraform pour exécuter le code Terraform.

1. Cliquez sur **Claim Terraform Cloud Agent** dans la liste déroulante de votre cible Terraform Cloud.
2. Entrez les détails de l'agent Terraform Cloud. La capture d'écran suivante montre les détails de configuration de l'agent Terraform.



Vous pouvez mettre à jour n'importe quelle propriété Terraform Agent. Si la cible est à l'état **non connecté** et n'a jamais été à l'état **connecté**, alors aucun jeton n'a été généré pour l'agent Terraform.

Une fois la validation de l'agent réussie et qu'un jeton d'agent est généré, vous ne pouvez pas reconfigurer l'organisation et/ou le pool d'agents. Le déploiement réussi d'un agent Terraform est indiqué par l'état **Connected**.

Après avoir activé et demandé l'intégration Terraform Cloud, vous pouvez déployer un ou plusieurs agents Terraform Cloud dans Cisco InterSight Assist. L'agent Terraform Cloud est modélisé comme cible enfant de la cible Terraform Cloud. Lorsque vous demandez la cible de l'agent, un message s'affiche pour indiquer que la demande cible est en cours.

Au bout de quelques secondes, la cible est déplacée à l'état **Connected** et la plateforme Intersight achemine les paquets HTTPS de l'agent vers la passerelle Terraform Cloud.

Votre agent Terraform doit être correctement réclamé et s'afficher sous cibles comme **connecté**.

"Configuration du fournisseur de services clouds publics"

Configurez le fournisseur de services clouds publics

"Précédent : intégration du cloud Terraform avec la condition préalable d'ICO."

Procédure 1 : accéder à NetApp Cloud Manager

Pour accéder à NetApp Cloud Manager et aux autres services cloud, vous devez vous inscrire "NetApp Cloud Central".

> Pour configurer des espaces de travail et des utilisateurs sur le compte Cloud Central, cliquez sur "ici".

Procédure 2 : déployer le connecteur

Pour déployer Connector dans Google Cloud, rendez-vous ici "lien".

"Ensuite, déploiement automatisé du stockage NetApp dans le cloud hybride."

Déploiement automatisé du stockage de cloud hybride NetApp

"Précédent : configuration du fournisseur de services clouds publics."

Google Cloud

Vous devez d'abord activer des API et créer un compte de service qui fournit à Cloud Manager des autorisations pour déployer et gérer des systèmes Cloud Volumes ONTAP dans le même projet que celui du connecteur ou dans des projets différents.

Avant de déployer un connecteur dans un projet Google Cloud, vérifiez que ce connecteur ne s'exécute pas sur vos sites ou dans un autre fournisseur cloud.

Deux ensembles d'autorisations doivent être en place avant de déployer un connecteur directement depuis Cloud Manager :

- Vous devez déployer Connector à l'aide d'un compte Google qui dispose d'autorisations pour lancer l'instance de VM Connector à partir de Cloud Manager.
- Lors du déploiement de Connector, vous êtes invité à sélectionner l'instance de VM. Cloud Manager obtient les autorisations du compte de service pour créer et gérer les systèmes Cloud Volumes ONTAP en votre nom. Les autorisations sont fournies en ajoutant un rôle personnalisé au compte de service.vous devez configurer deux fichiers YAML qui incluent les autorisations requises pour l'utilisateur et le compte de service. Découvrez comment utiliser "Les fichiers YAML pour configurer les autorisations" ici.

Voir "cette vidéo détaillée" pour tous les prérequis requis.

Architecture et modes de déploiement Cloud Volumes ONTAP

Cloud Volumes ONTAP est disponible dans Google Cloud sous forme de système à un seul nœud et en tant que paire de nœuds à haute disponibilité. En fonction de ces exigences, nous pouvons choisir le mode de déploiement Cloud Volumes ONTAP. La mise à niveau d'un système à un seul nœud vers une paire haute disponibilité n'est pas prise en charge. Si vous souhaitez passer d'un système à un seul nœud à une paire HA, vous devez déployer un nouveau système et répliquer les données du système existant vers le nouveau.

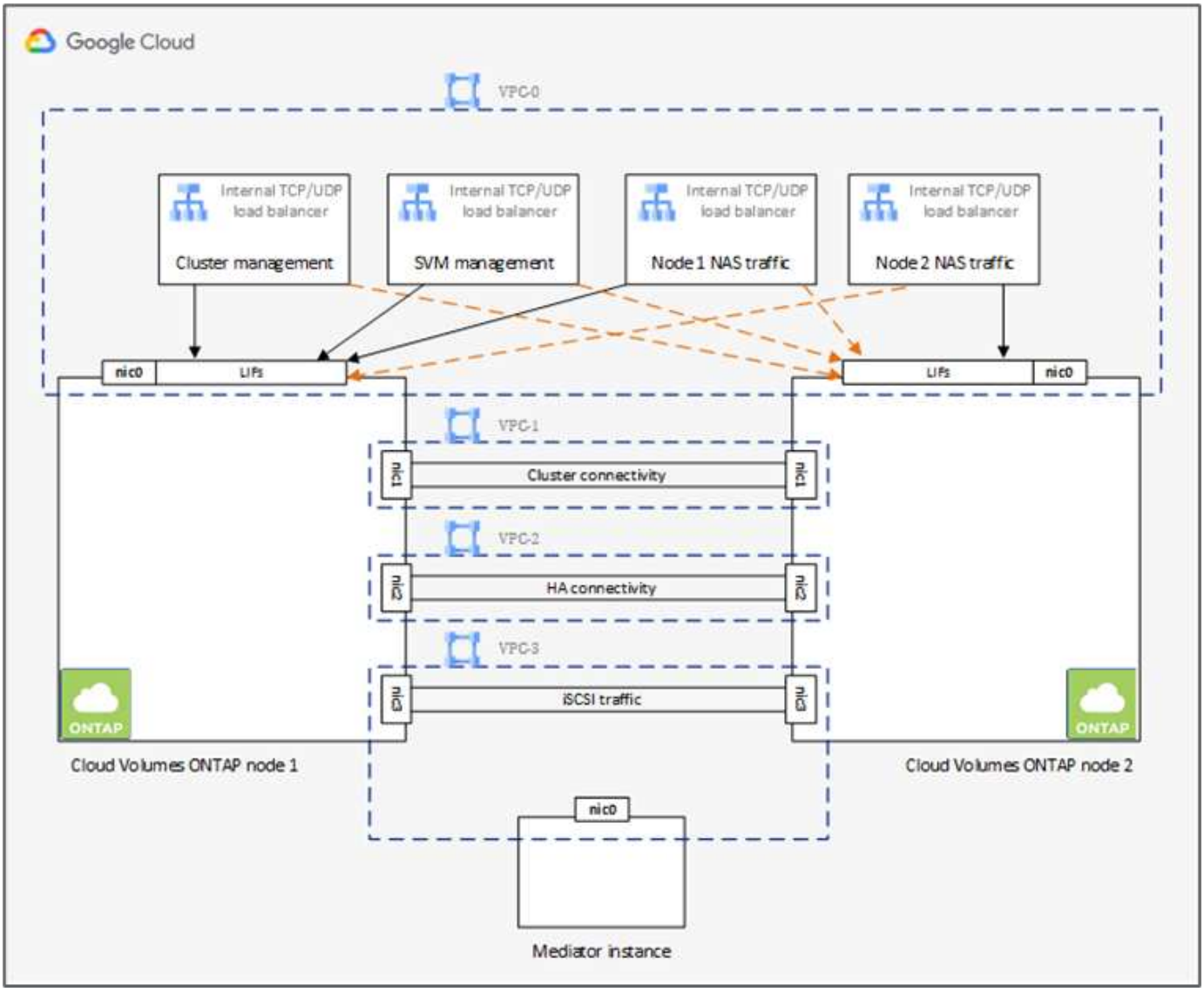
Haute disponibilité de Cloud Volumes ONTAP dans Google Cloud

Google Cloud prend en charge le déploiement de ressources dans plusieurs régions géographiques et zones géographiques. Le déploiement HA comprend deux nœuds ONTAP qui utilisent de puissants types de machines standard n1 ou n2 disponibles dans Google Cloud. Les données sont répliquées de manière synchrone entre les deux nœuds Cloud Volumes ONTAP afin d'assurer la disponibilité en cas de défaillance. Le déploiement HAUTE DISPONIBILITÉ de Cloud Volumes ONTAP requiert quatre VPC et un sous-réseau privé dans chaque VPC. Les sous-réseaux des quatre VPC doivent être configurés avec des plages CIDR non chevauchantes.

Les quatre VPC sont utilisés à des fins suivantes :

- VPC 0 permet la communication entrante aux nœuds de données et Cloud Volumes ONTAP.
- VPC 1 assure la connectivité du cluster entre les nœuds Cloud Volumes ONTAP.
- VPC 2 permet la réplication des RAM non volatiles (NVRAM) entre les nœuds.
- VPC 3 est utilisé pour la connectivité à l'instance de médiateur HA et au trafic de réplication de disque pour les reconstructions de nœuds.

L'image suivante montre un Cloud Volumes ONTAP hautement disponible dans Goggle Cloud.



Pour plus de détails, voir "ce lien".

Pour connaître les exigences de mise en réseau pour Cloud Volumes ONTAP dans Google Cloud, consultez "ce lien".

Pour plus d'informations sur le Tiering des données, voir "ce lien".

Configurez les conditions préalables à l'environnement

La création automatisée de clusters Cloud Volumes ONTAP, la configuration SnapMirror entre un volume sur site et un volume cloud, la création d'un volume cloud, etc., s'effectue à l'aide de la configuration Terraform. Ces configurations Terraform sont hébergées sur un compte Terraform Cloud for Business. Avec Intersight Cloud Orchestrator, vous orchestrez des tâches telles que la création d'un espace de travail dans un compte Terraform Cloud for Business, l'ajout de toutes les variables requises à l'espace de travail, l'exécution d'un plan Terraform, etc.

Pour ces tâches d'automatisation et d'orchestration, quelques exigences et données sont nécessaires, comme décrit dans les sections suivantes.

Référentiel GitHub

Vous avez besoin d'un compte GitHub pour héberger votre code Terraform. Intersight Orchestrator crée un nouvel espace de travail dans le compte Terraform Cloud for Business. Cet espace de travail est configuré avec un workflow de contrôle de version. À cette fin, vous devez conserver la configuration Terraform dans un référentiel GitHub et la fournir comme entrée lors de la création de l'espace de travail.

"Lien GitHub" Fournit la configuration Terraform avec diverses ressources. Vous pouvez forer ce référentiel et en faire une copie dans votre compte GitHub.

Dans ce référentiel, `provider.tf` A la définition du fournisseur Terraform requis. Le fournisseur Terraform pour NetApp Cloud Manager est utilisé.

`variables.tf` dispose de toutes les déclarations de variables. La valeur de ces variables est entrée en tant qu'entrée de workflow d'Intersight Cloud Orchestrator. Cela permet de transmettre des valeurs à un espace de travail et d'exécuter la configuration Terraform.

`resources.tf` Définit les diverses ressources nécessaires pour ajouter un système ONTAP sur site à l'environnement de travail, créer un cluster Cloud Volumes ONTAP à nœud unique sur Google Cloud, établir une relation SnapMirror entre l'infrastructure sur site et Cloud Volumes ONTAP, créer un volume cloud sur Cloud Volumes ONTAP, etc.

Dans ce référentiel :

- `provider.tf` Définit NetApp Cloud Manager comme fournisseur Terraform requis.
- `variables.tf` Dispose des déclarations de variables utilisées comme entrée pour le workflow Intersight Cloud Orchestrator. Cela permet de transmettre des valeurs à l'espace de travail et d'exécuter la configuration Terraform.
- `resources.tf` Définit diverses ressources pour ajouter une ONTAP sur site à l'environnement de travail, créer un cluster Cloud Volumes ONTAP à un seul nœud sur Google Cloud, établir une relation SnapMirror entre l'infrastructure sur site et Cloud Volumes ONTAP, créer un volume cloud sur Cloud Volumes ONTAP, etc.

Vous pouvez ajouter un bloc de ressources supplémentaire pour créer plusieurs volumes sur Cloud Volumes ONTAP, ou utiliser count ou `for_each` Constructions Terraform.

Pour connecter des espaces de travail Terraform, des modules et des jeux de règles aux référentiels git contenant des configurations Terraform, Terraform Cloud doit accéder à votre GitHub repo.

Ajoutez un client et l'ID Token OAuth du client est utilisé comme l'une des entrées de workflow d'InterSight Cloud Orchestrator.

1. Connectez-vous à votre compte Terraform Cloud for Business. Accédez à **Paramètres > fournisseurs**.
2. Cliquez sur **Ajouter un fournisseur VCS**.
3. Sélectionnez votre version.
4. Suivez les étapes de la section **configurer fournisseur**.
5. Vous voyez le client ajouté dans **VCS Providers**. Notez l'ID du token OAuth.

Jeton d'actualisation pour les opérations de l'API NetApp Cloud Manager

En plus de l'interface du navigateur Web, Cloud Manager dispose d'une API REST qui permet aux développeurs de logiciels d'accéder directement à la fonctionnalité Cloud Manager via l'interface SaaS. Le service Cloud Manager comprend plusieurs composants distincts qui forment collectivement une plateforme de développement extensible. Le jeton d'actualisation vous permet de générer des jetons d'accès que vous ajoutez à l'en-tête autorisation pour chaque appel d'API.

Sans appeler directement une API, le fournisseur netapp-cloudManager utilise un jeton d'actualisation et convertit les ressources Terraform en appels d'API correspondants. Vous devez générer un jeton d'actualisation pour les opérations de l'API NetApp Cloud Manager à partir de "NetApp Cloud Central".

Vous devez disposer de l'ID client du connecteur Cloud Manager pour créer des ressources dans Cloud Manager, par exemple pour créer un cluster Cloud Volumes ONTAP, configurer SnapMirror, etc.

1. Connectez-vous à Cloud Manager : "https://cloudmanager.netapp.com/".
2. Cliquez sur **connecteur**.
3. Cliquez sur **gérer les connecteurs**.
4. Cliquez sur les points de suspension et copiez l'ID du connecteur.

Développez le workflow Cisco Intersight Cloud Orchestrator

Cisco Intersight Cloud Orchestrator est disponible dans Cisco Intersight si :

- Vous avez installé la licence InterSight Premier.
- Vous êtes administrateur de compte, administrateur de stockage, administrateur de virtualisation ou administrateur de serveurs et avez au moins un serveur qui vous est attribué.

Concepteur de flux de travail

Le concepteur de flux de travail vous aide à créer de nouveaux flux de travail (ainsi que des tâches et des types de données) et à modifier des flux de travail existants pour gérer des cibles dans Cisco Intersight.

Pour lancer Workflow Designer, accédez à **orchestration > workflows**. Un tableau de bord affiche les détails suivants sous les onglets **Mes workflows**, **modèles de flux de travail** et **tous les workflows** :

- État de validation
- Statut de la dernière exécution

- Flux de travail par nombre d'exécution
- Principales catégories de flux de travail
- Nombre de flux de travail définis par le système
- Principaux flux de travail par cible

Le tableau de bord vous permet de créer, modifier, cloner ou supprimer un onglet. Pour créer votre propre onglet de vue personnalisée, cliquez sur **+**, spécifiez un nom, puis sélectionnez les paramètres requis à afficher dans les colonnes, les colonnes de balises et les widgets. Vous pouvez renommer un onglet s'il ne possède pas d'icône **Lock**.

Sous le tableau de bord, vous trouverez une liste tabulaire des flux de production affichant les informations suivantes :

- Afficher le nom
- Description
- Défini par le système
- Version par défaut
- Exécutions
- Statut de la dernière exécution
- État de validation
- Dernière mise à jour
- Entreprise

La colonne actions vous permet d'effectuer les actions suivantes :

- **Exécuter.** exécute le flux de travail.
- **Historique.** affiche l'historique d'exécution du flux de travail.
- **Gérer les versions.** Créer et gérer des versions pour les flux de travail.
- **Supprimer.** Supprimer un flux de travail.
- **Réessayer.** Réessayer un flux de travail échoué.

Flux de travail

Créer un flux de travail composé des étapes suivantes :

- **Définition d'un flux de travail.** spécifier le nom d'affichage, la description et d'autres attributs importants.
- **Définir les entrées de flux de travail et les sorties de flux de travail.** spécifier les paramètres d'entrée obligatoires pour l'exécution du flux de travail et les sorties générées lors de l'exécution réussie
- **Ajouter des tâches de flux de travail.** Ajouter une ou plusieurs tâches de flux de travail dans le concepteur de flux de travail qui sont nécessaires pour que le flux de travail puisse exécuter sa fonction.
- *Valider le flux de travail. *Valider un flux de travail pour s'assurer qu'il n'y a pas d'erreurs dans la connexion des entrées et sorties de tâche.

Créez des workflows de stockage FlexPod sur site

Pour configurer un workflow pour le stockage FlexPod sur site, reportez-vous à la section "ce lien".

"Suivant : workflow de reprise après incident."

Workflow de reprise d'activité

"Précédent : déploiement automatisé du stockage NetApp dans le cloud hybride."

Les étapes sont les suivantes :

1. Définir le flux de travail.
   - Créez un nom court et convivial pour le flux de travail, tel que Disaster Recovery Workflow.
2. Définissez l'entrée du flux de travail. Nous utilisons les données d'entrée suivantes pour ce flux de travail :
   - Options de volume (nom du volume, chemin de montage)
   - Capacité du volume
   - Data Center associé au nouveau datastore
   - Cluster sur lequel le datastore est hébergé
   - Nom du nouveau datastore à créer dans vCenter
   - Type et version du nouveau datastore
   - Nom de l'organisation Terraform
   - Espace de travail Terraform
   - Description de l'espace de travail Terraform
   - Variables (sensibles et non sensibles) requises pour exécuter la configuration Terraform
   - Motif du démarrage du plan
3. Ajoutez les tâches du flux de travail.

   Les tâches liées aux opérations dans FlexPod incluent les tâches suivantes :

   - Création de volumes dans FlexPod.
   - Ajout de l'export policy de stockage au volume créé
   - Mappez le nouveau volume sur un datastore dans VMware vCenter.

     Tâches liées à la création d'un cluster Cloud Volumes ONTAP :

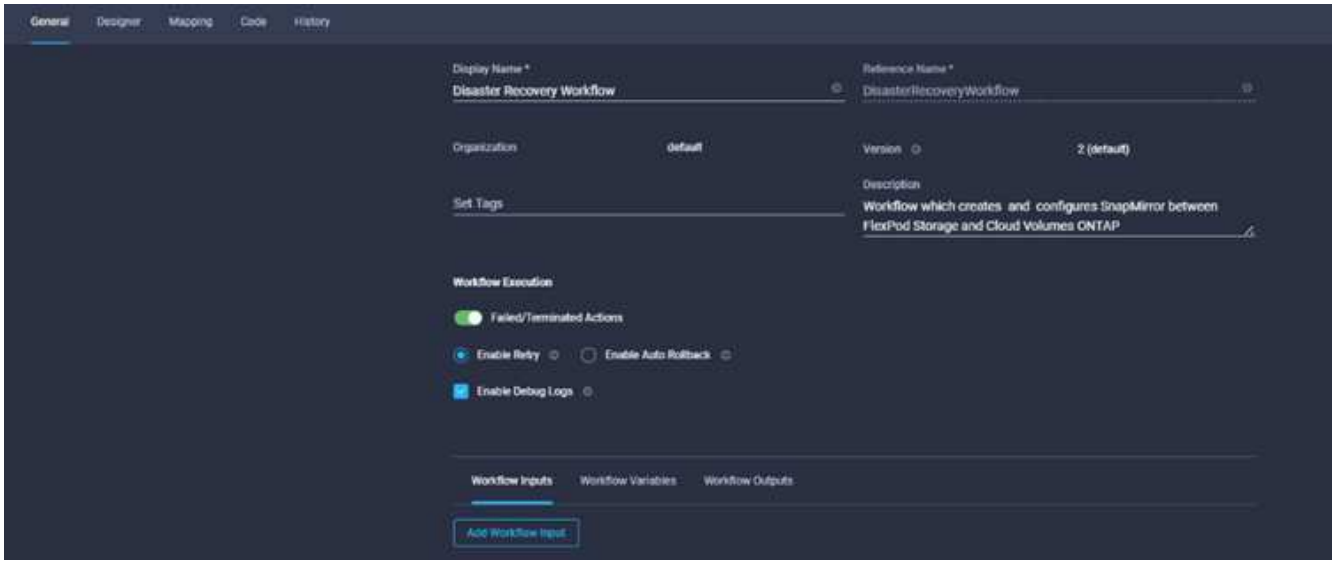
   - Ajouter un espace de travail Terraform
   - Ajouter des variables Terraform
   - Ajoutez des variables sensibles à Terraform
   - Démarrez un nouveau plan Terraform
   - Confirmez l'exécution de Terraform
4. Validation du flux de travail

Procédure 1 : créez le flux de travail

1. Cliquez sur **orchestration** dans le volet de navigation de gauche et cliquez sur **Créer un flux de travail**.
2. Dans l'onglet **général** :
   a. Indiquez le nom d'affichage (flux de travail de reprise après sinistre).

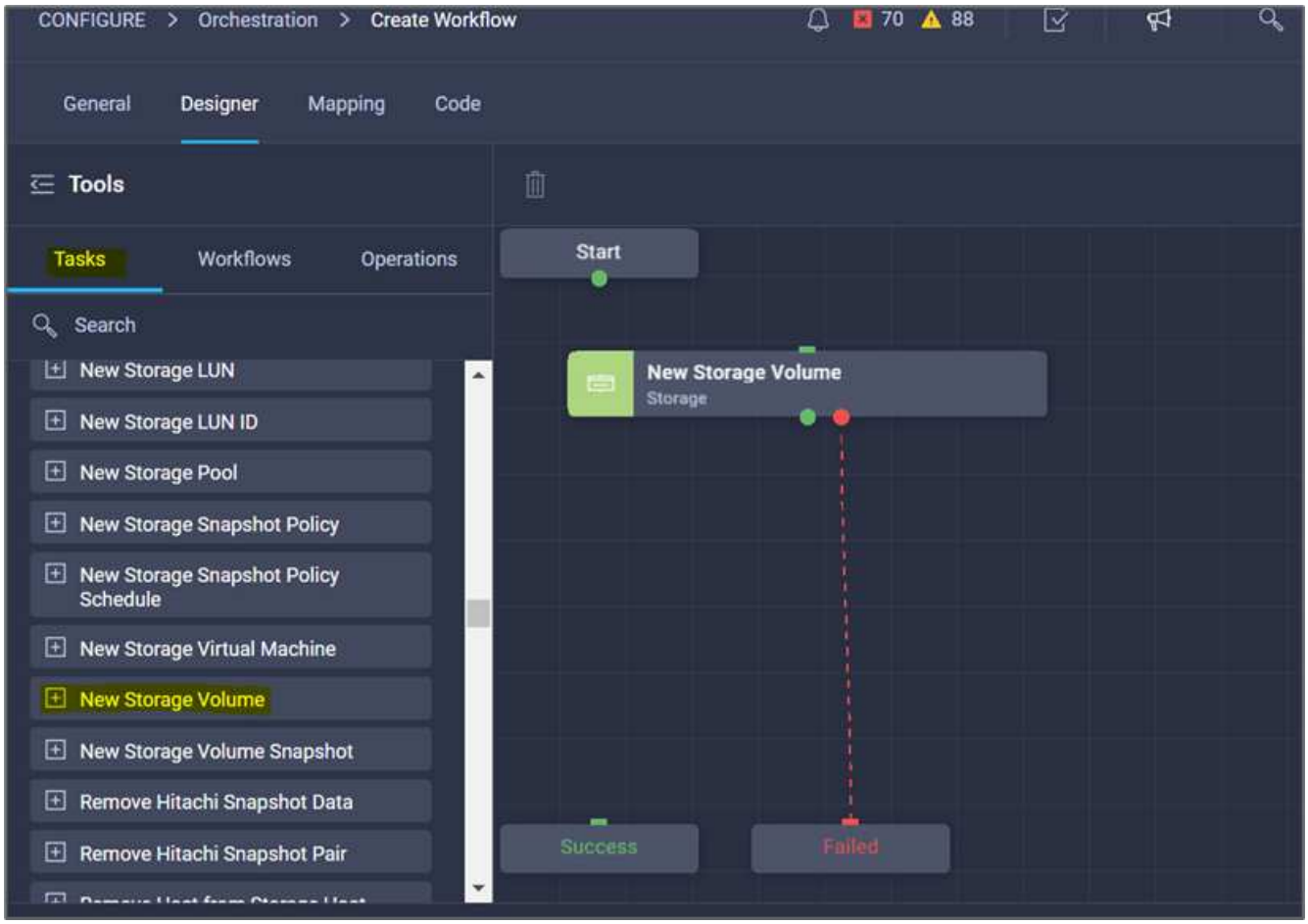
b. Sélectionnez l’organisation, définissez les balises et fournissez une description.

3. Cliquez sur Enregistrer.

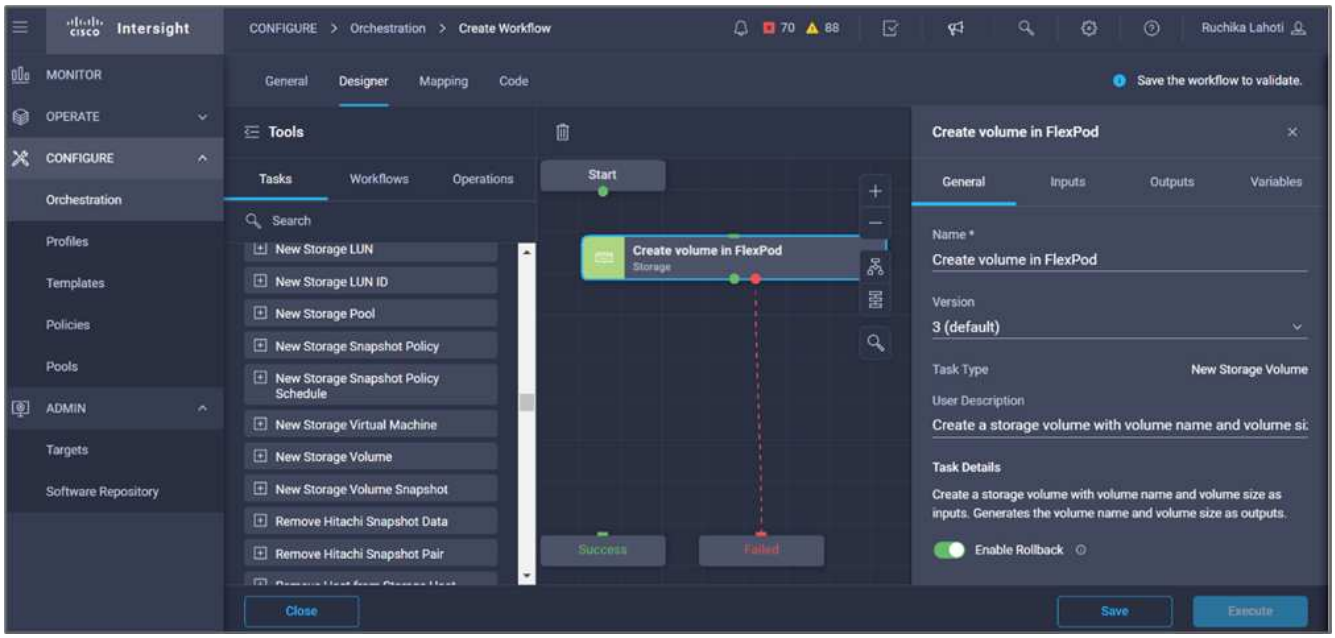


Procédure 2. Créer un nouveau volume dans FlexPod

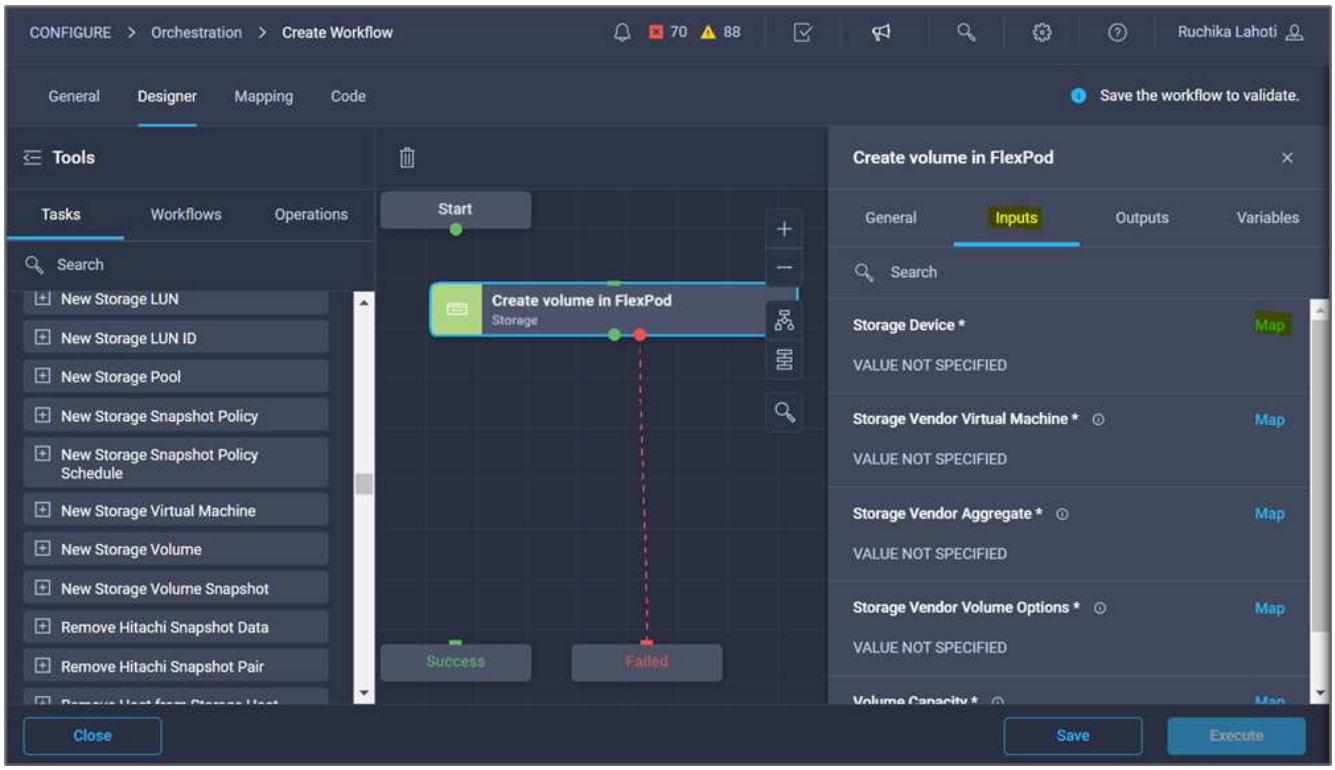
1. Accédez à l’onglet **Designer** et cliquez sur **tâches** dans la section **Outils**.
2. Faites glisser et déposez la tâche **stockage > Nouveau volume de stockage** de la section **Outils** dans la zone **Design**.
3. Cliquez sur **Nouveau volume de stockage**.



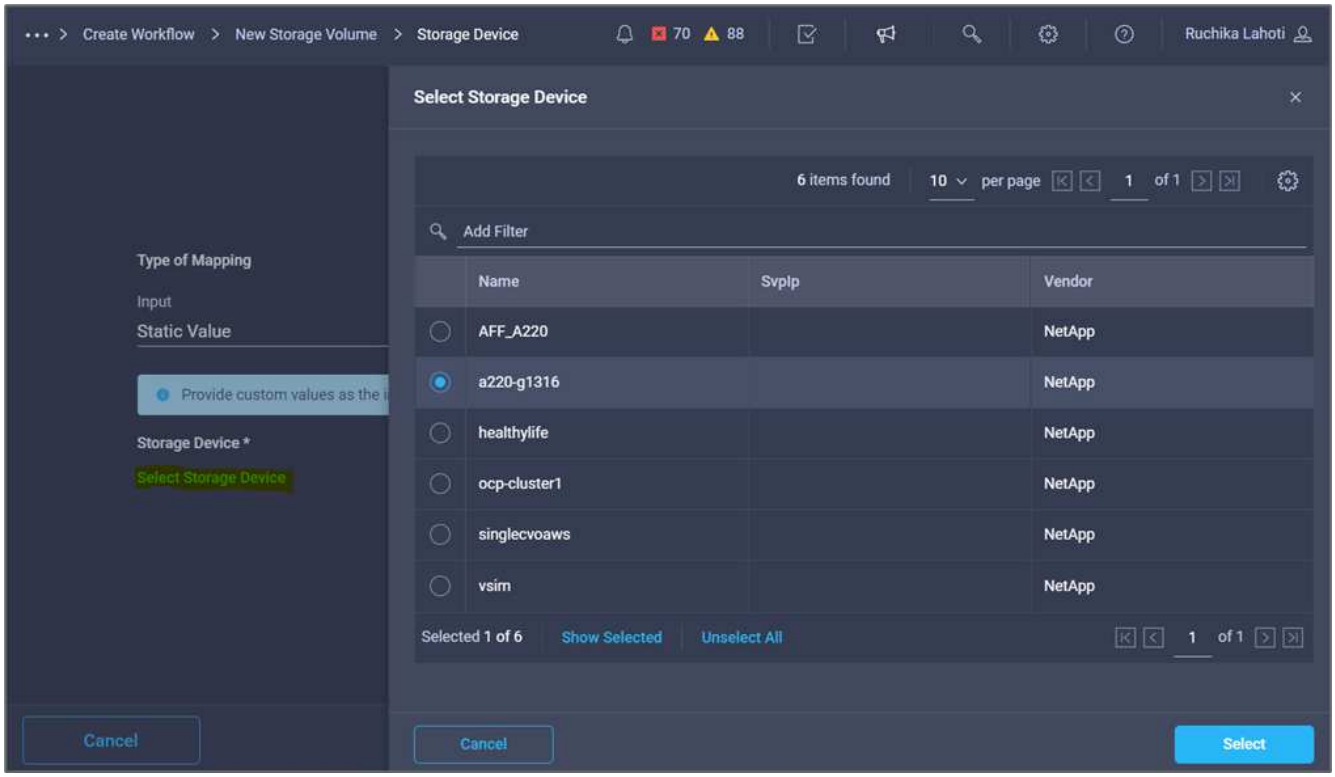
4. Dans la zone **Propriétés de tâche**, cliquez sur l'onglet **général**. Vous pouvez également modifier le nom et la description de cette tâche. Dans cet exemple, le nom de la tâche est **Créer un volume dans FlexPod**.



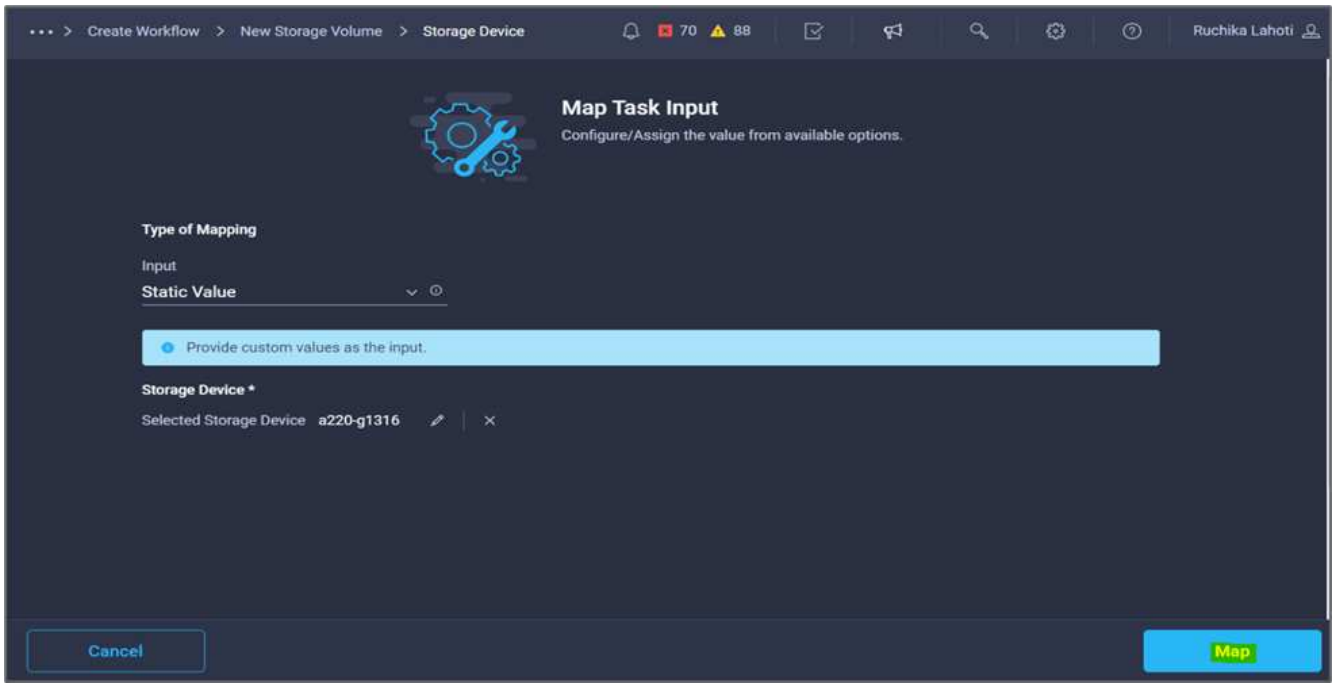
5. Dans la zone **Propriétés de tâche**, cliquez sur **entrées**.
6. Cliquez sur **Map** dans le champ **Storage Device**.



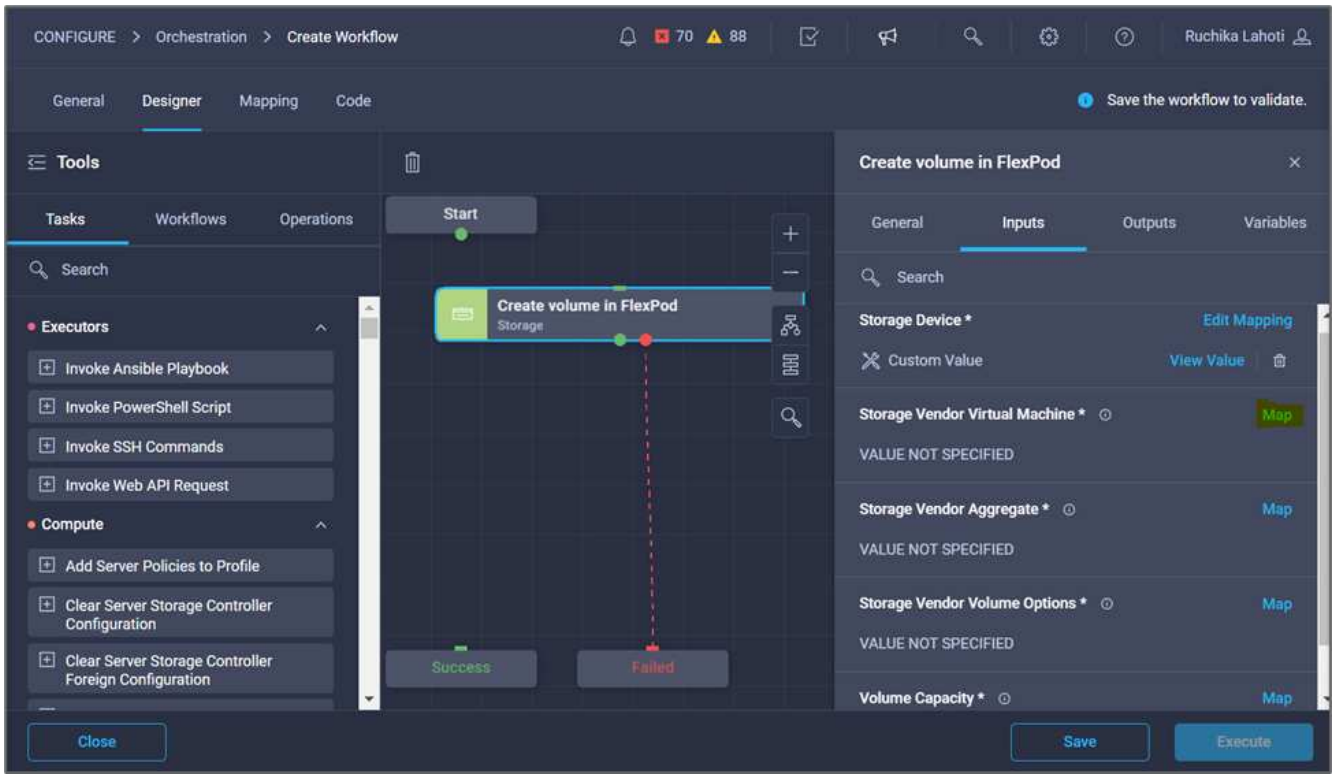
7. Choisissez **valeur statique** et cliquez sur **Sélectionner le périphérique de stockage**.
8. Cliquez sur la cible de stockage ajoutée et cliquez sur **Sélectionner**.



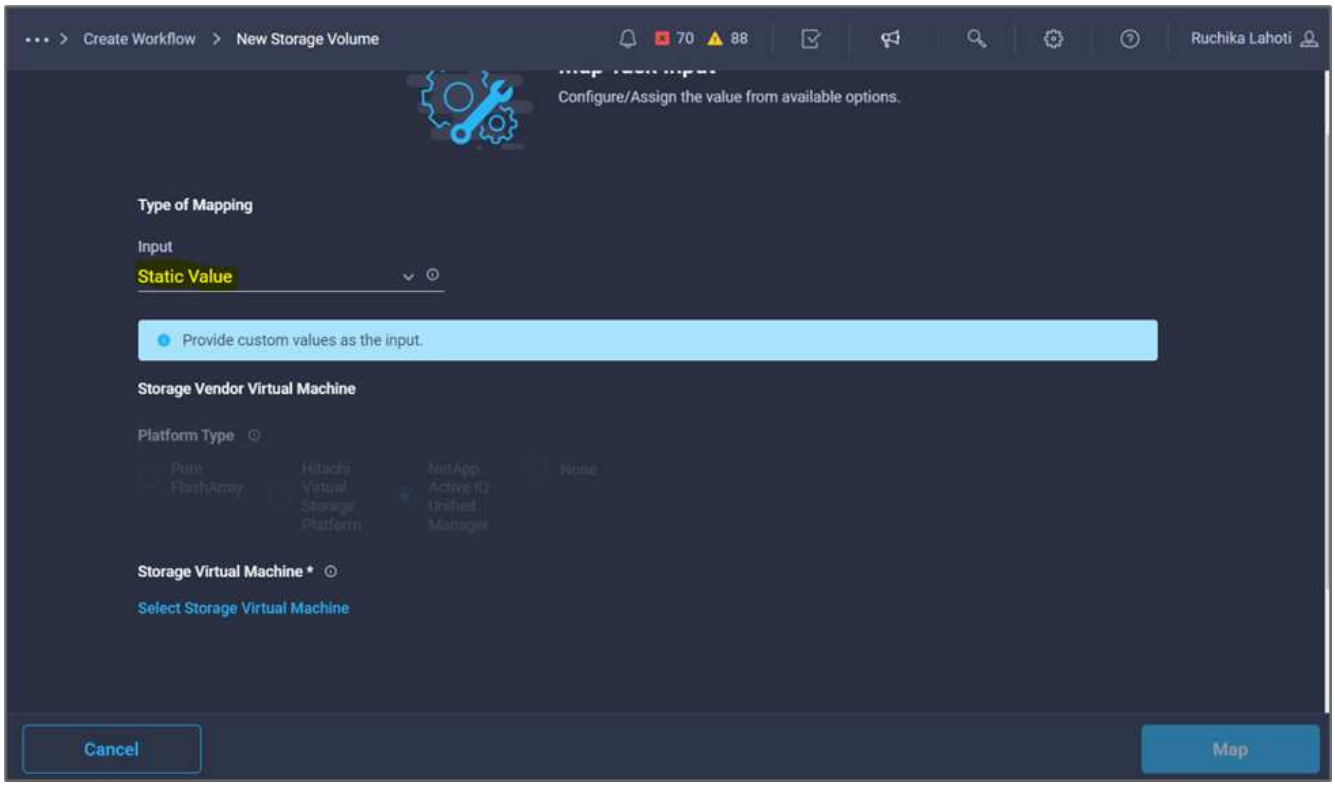
9. Cliquez sur **carte**.



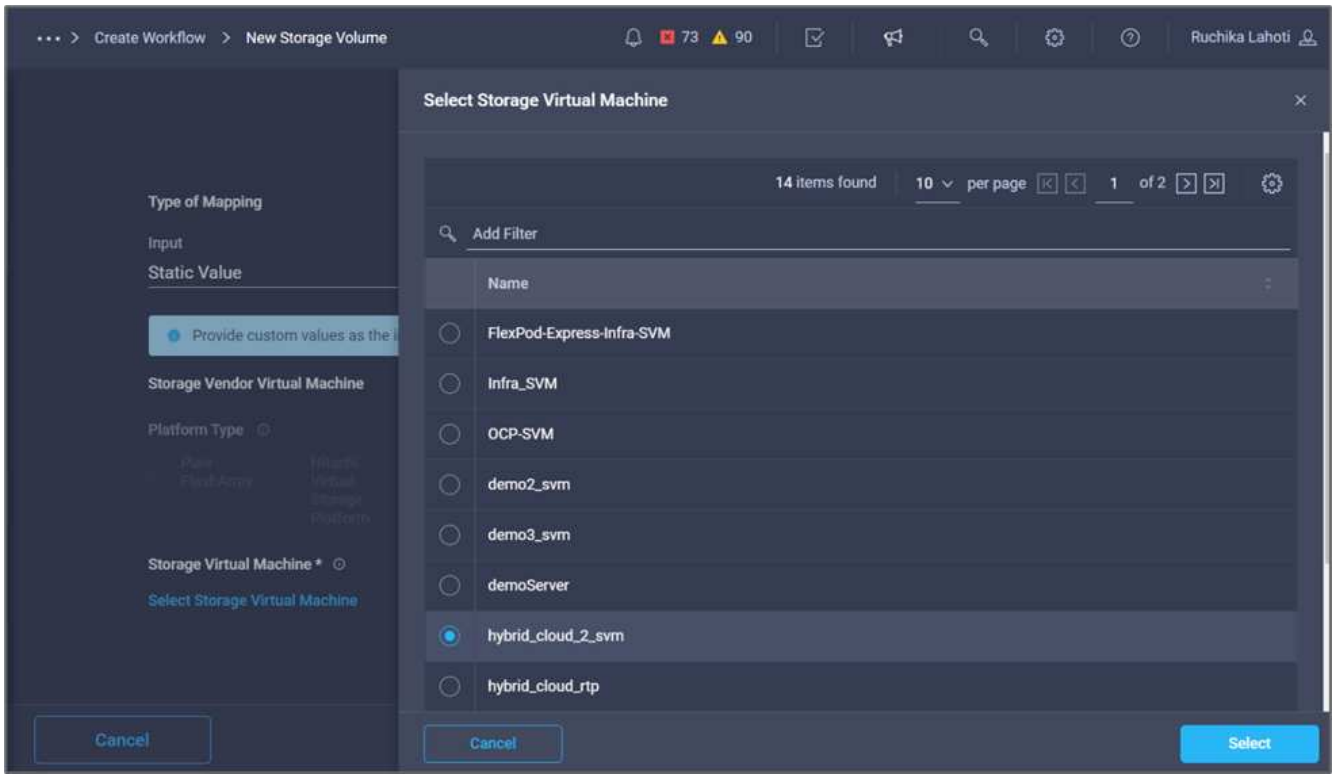
10. Cliquez sur **Map** dans le champ **Storage Vendor Virtual machine**.



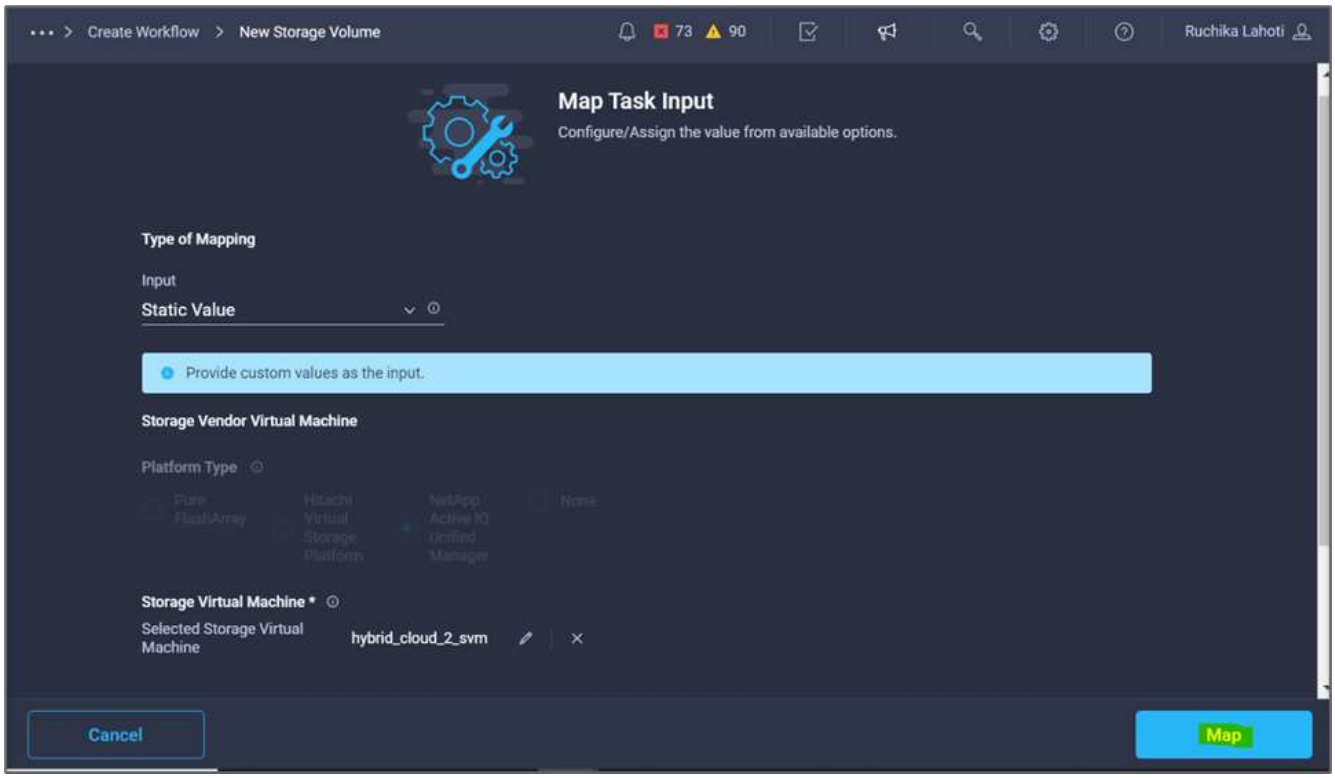
11. Choisissez **valeur statique** et cliquez sur **Sélectionner Storage Virtual machine**.



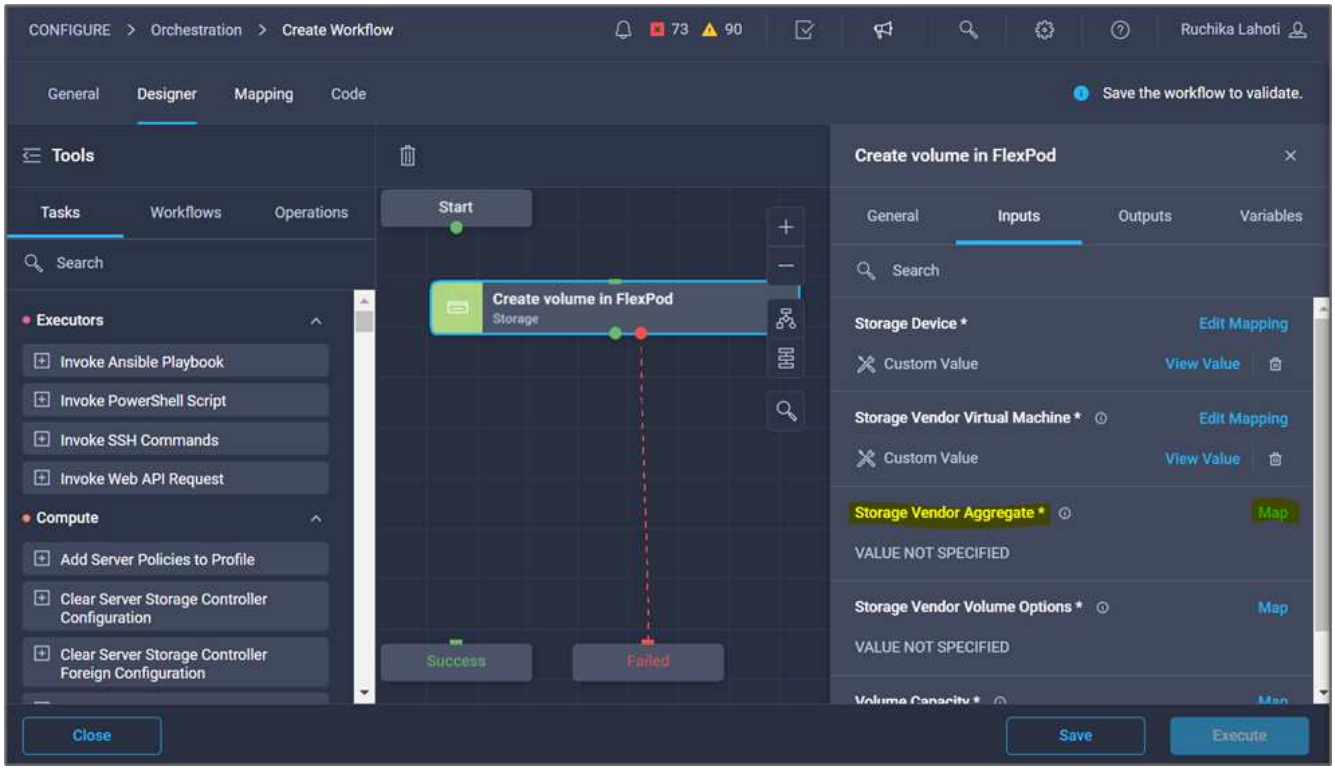
12. Sélectionnez la machine virtuelle de stockage sur laquelle le volume doit être créé et cliquez sur **Sélectionner**.



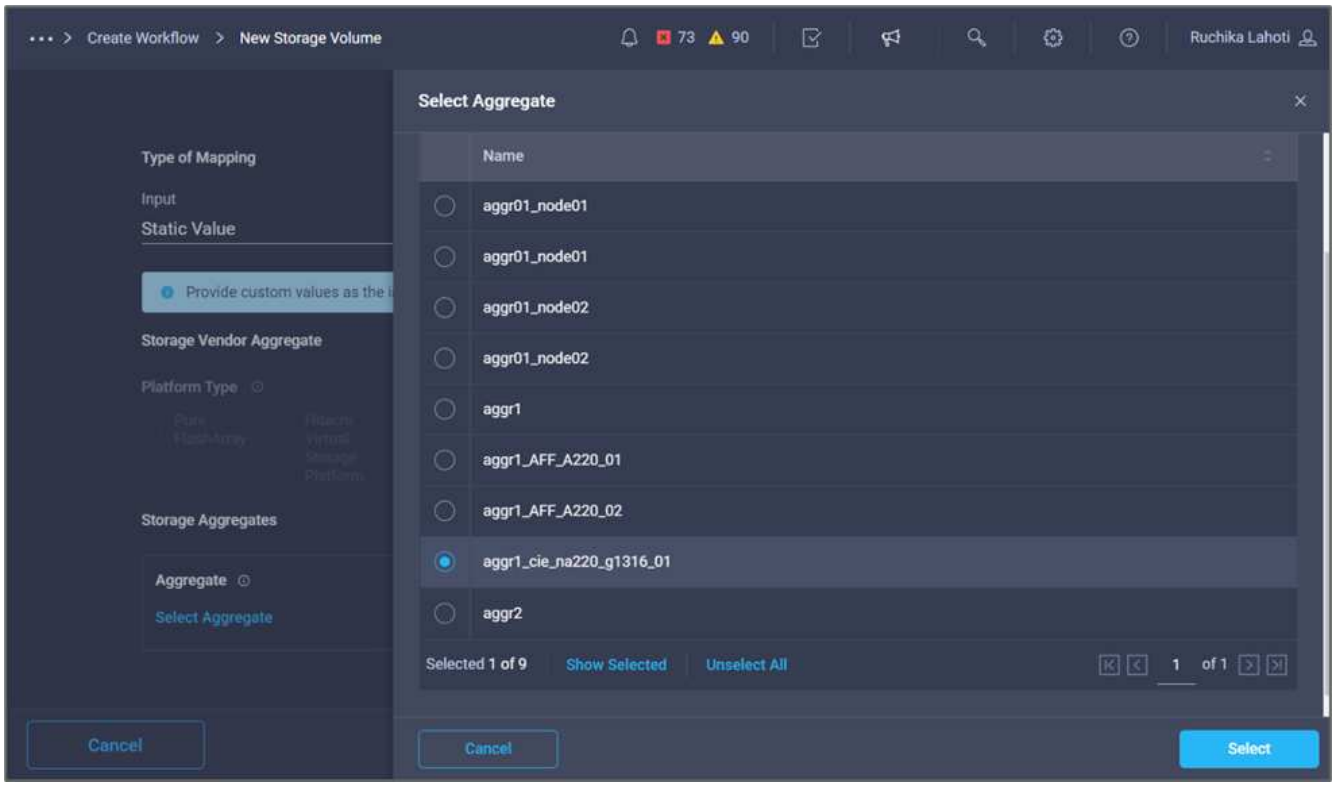
13. Cliquez sur **carte**.



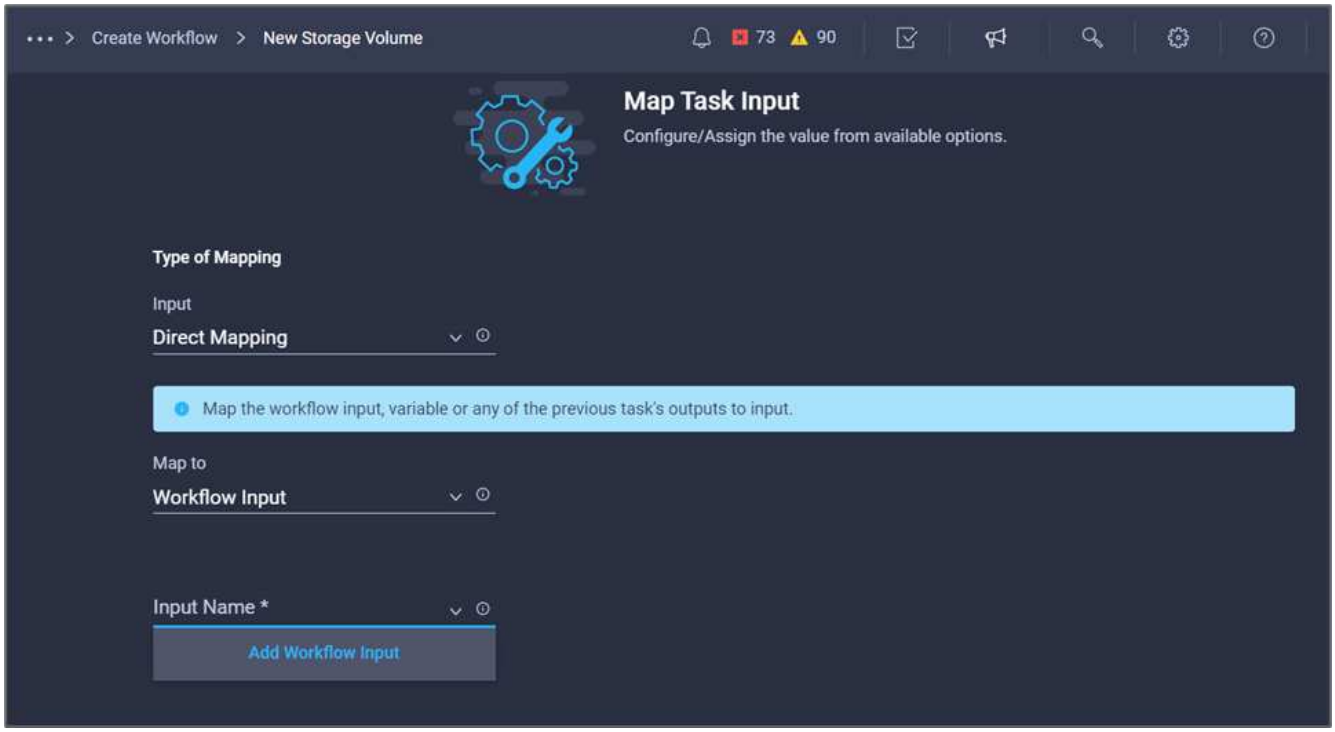
14. Cliquez sur **Map** dans le champ **Storage Vendor Aggregate**.



15. Choisissez **valeur statique** et cliquez sur **Sélectionner l'agrégat de stockage**. Choisissez l'agrégat et cliquez sur **Select**.



16. Cliquez sur **carte**.
17. Cliquez sur **Map** dans le champ **Storage Vendor Volume Options**.
18. Choisissez **mappage direct** et cliquez sur **entrée de flux de travail**.



19. Dans l'assistant Ajouter une entrée, procédez comme suit :
    a. Indiquez un nom d'affichage et un nom de référence (facultatif).
    b. Assurez-vous que **Storage Vendor Volume Options** est sélectionné pour **Type**.

c. Cliquez sur **définir la valeur par défaut et remplacer**.

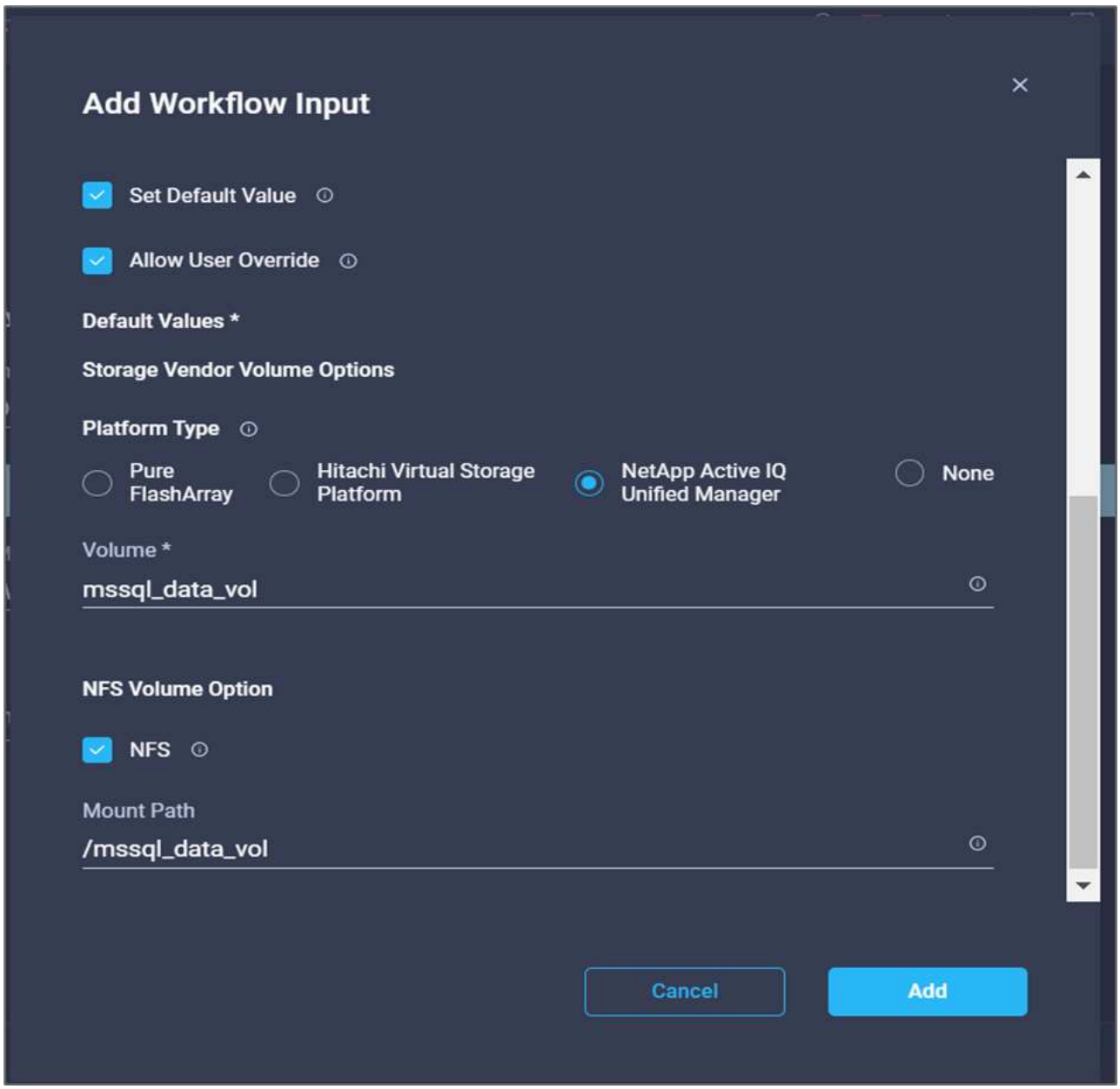
d. Cliquez sur **requis**.

e. Définissez **Type de plateforme** sur **NetApp Active IQ Unified Manager**.

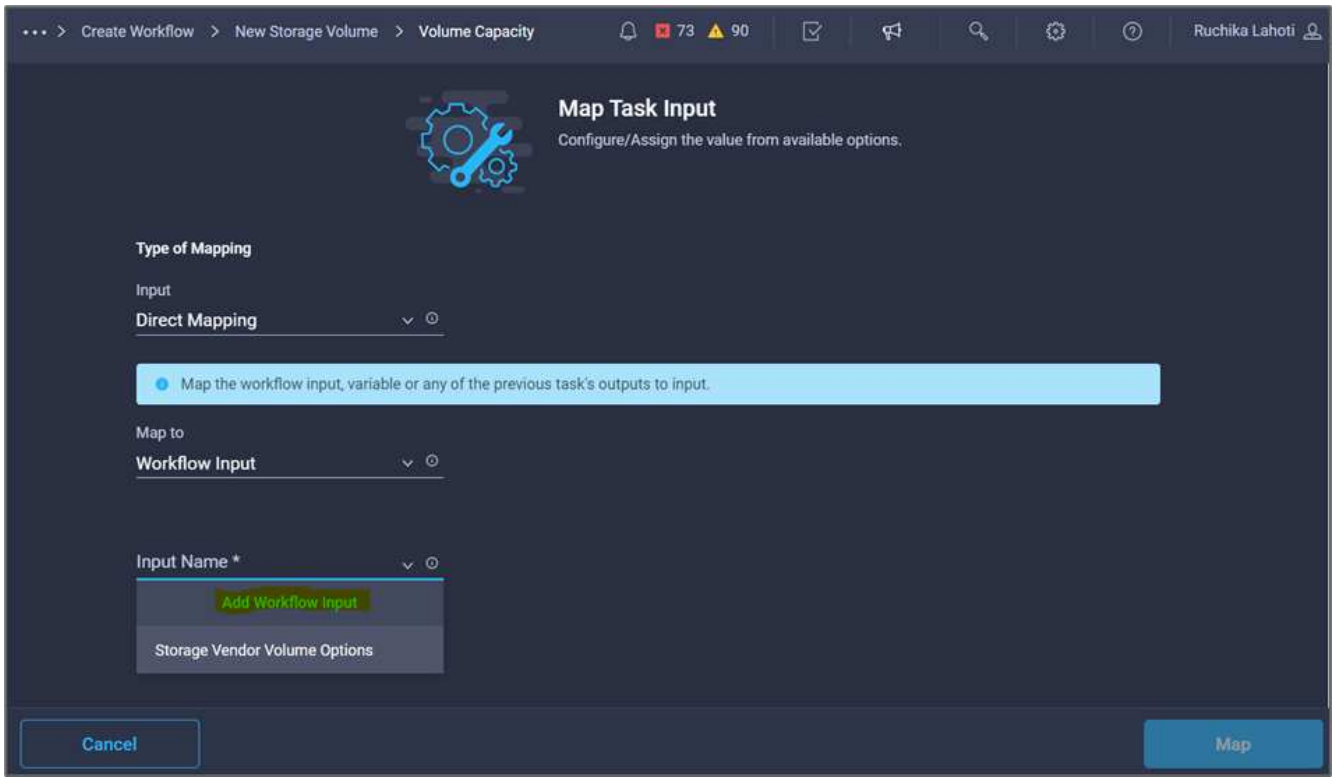
f. Indiquez une valeur par défaut pour le volume créé sous **Volume**.

g. Cliquez sur **NFS**. Si NFS est défini, un volume NFS est créé. Si cette valeur est définie sur FALSE, un volume SAN est créé.

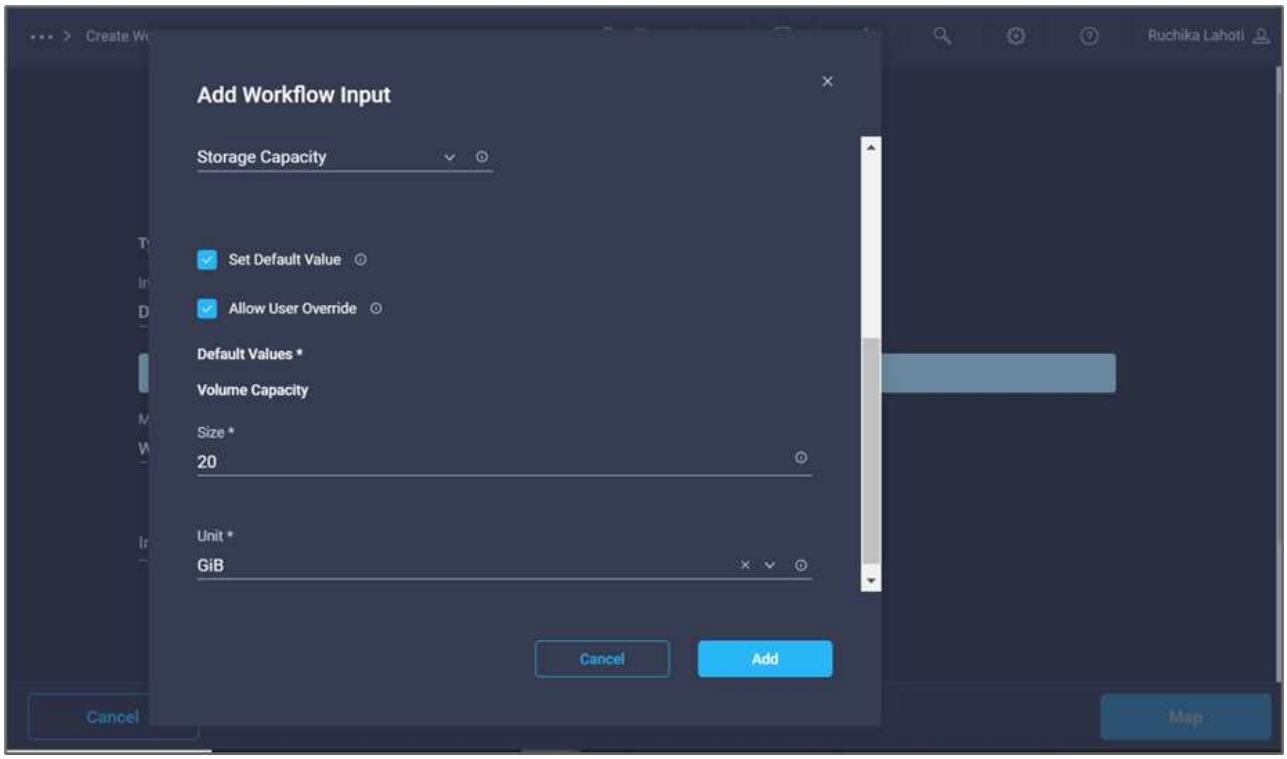
h. Indiquez un chemin de montage et cliquez sur **Ajouter**.



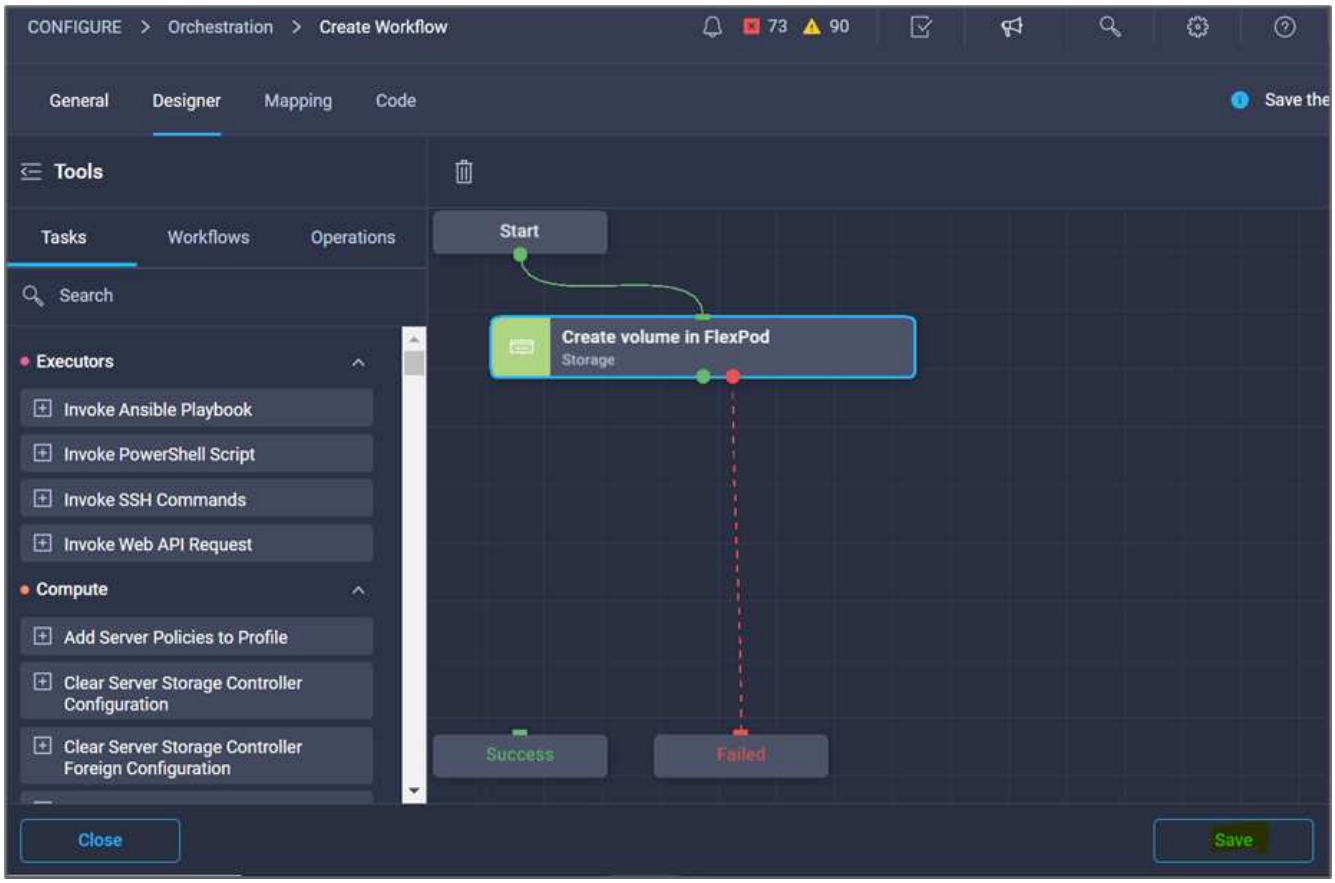
20. Cliquez sur **carte**.
21. Cliquez sur **Map** dans le champ **Volume Capacity**.
22. Choisissez **mappage direct** et cliquez sur **entrée de flux de travail**.
23. Cliquez sur **Nom d'entrée** et **Créer une entrée de flux de travail**.



24. Dans l'assistant Ajouter une entrée :
    a. Indiquez un nom d'affichage et un nom de référence (facultatif).
    b. Cliquez sur **requis**.
    c. Pour **Type**, sélectionnez **capacité de stockage**.
    d. Cliquez sur **définir la valeur par défaut et remplacer**.
    e. Indiquez une valeur par défaut pour la taille du volume et l'unité.
    f. Cliquez sur **Ajouter**.



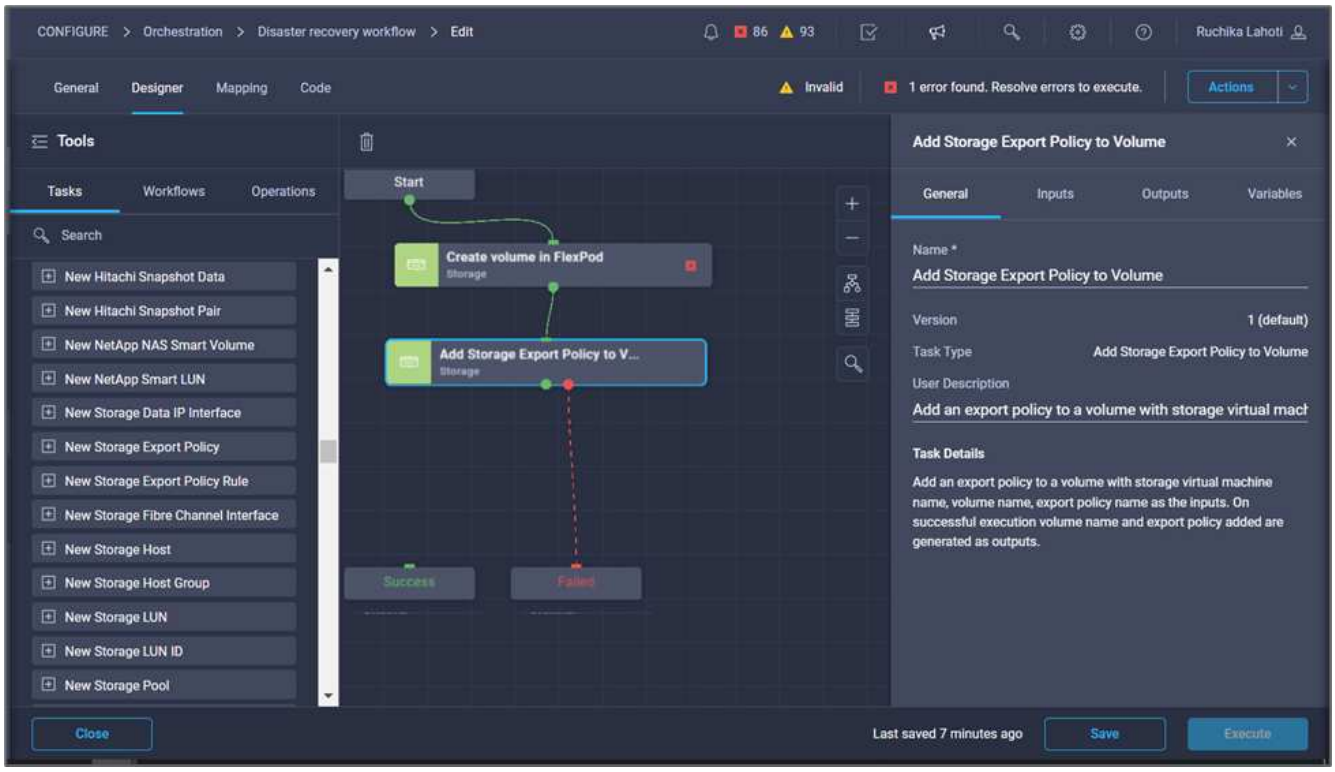
25. Cliquez sur **carte**.
26. Avec Connector, créez une connexion entre les tâches **Démarrer** et **Créer un volume dans FlexPod**, puis cliquez sur **Enregistrer**.



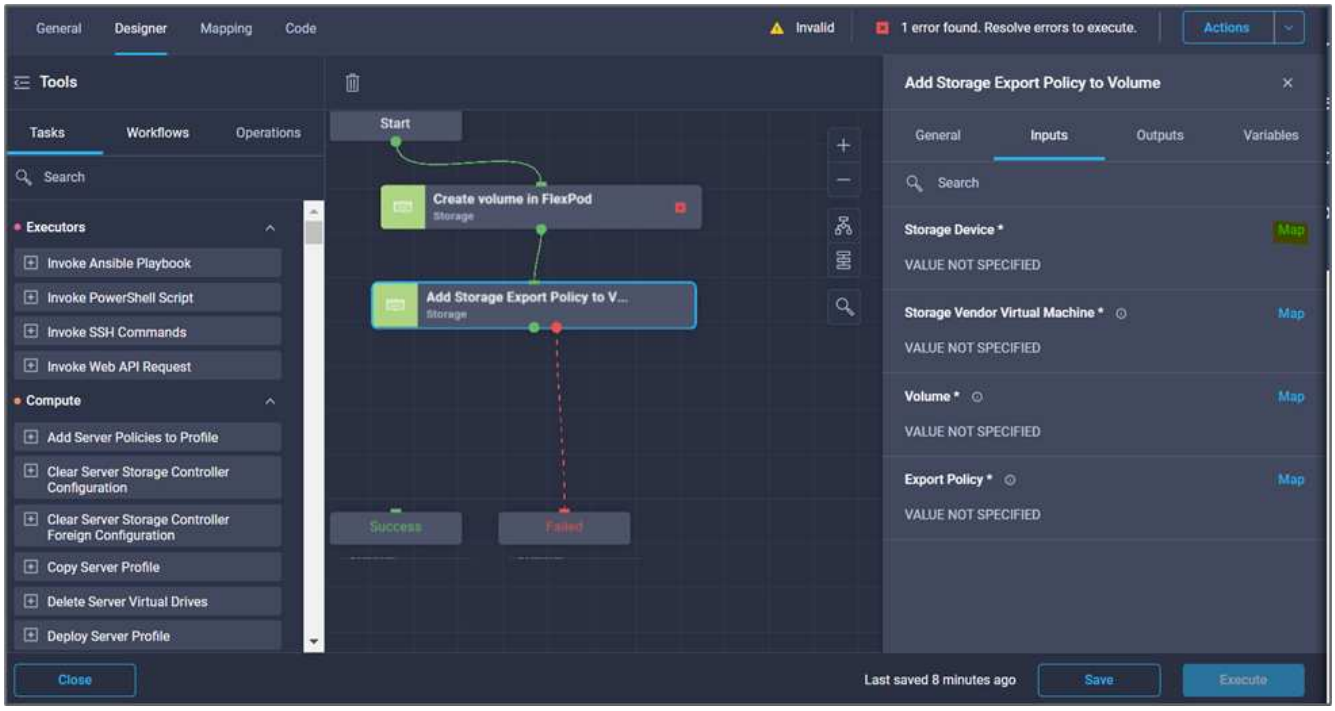
Ignorer l'erreur pour l'instant. Cette erreur s'affiche car il n'y a pas de connectivité entre les tâches **Créer un volume dans FlexPod** et **succès** qui est nécessaire pour spécifier la transition réussie.

Procédure 3 : ajout d'une règle d'exportation de stockage

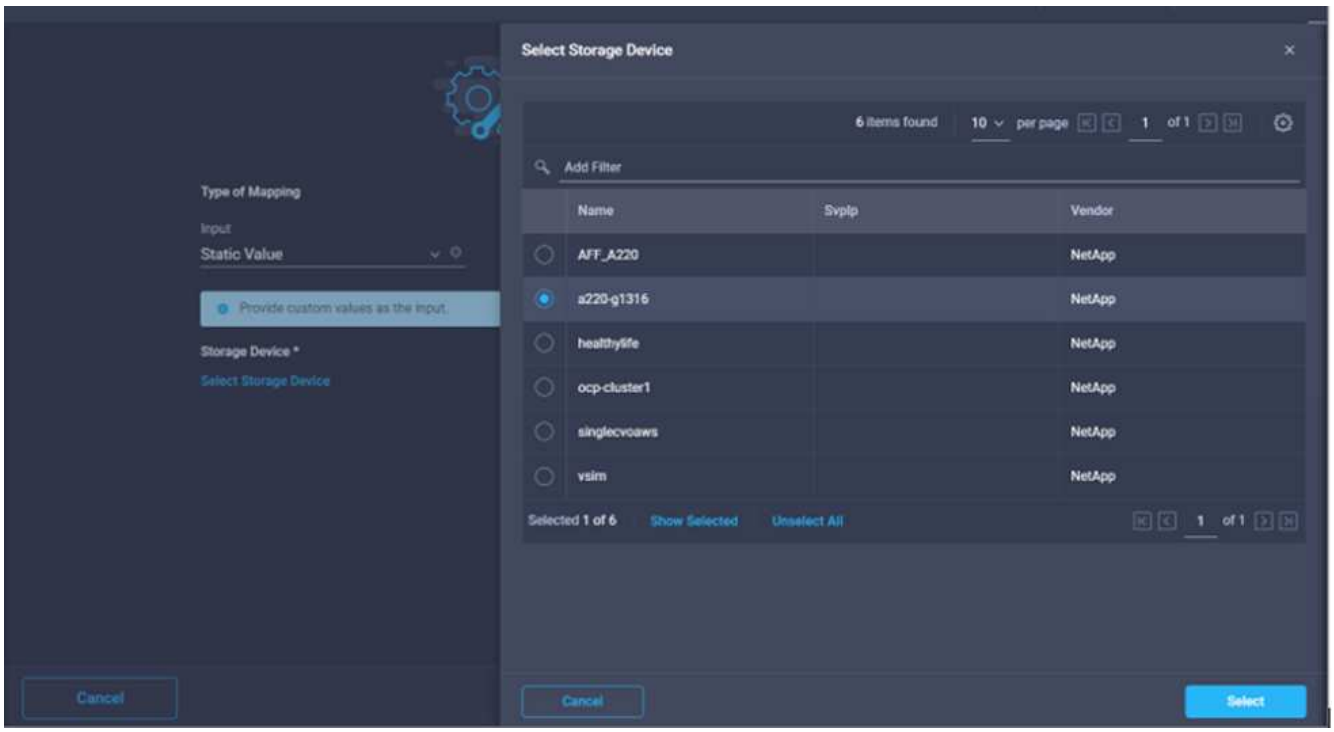
1. Accédez à l'onglet **Designer** et cliquez sur **tâches** dans la section **Outils**.
2. Faites glisser et déposez la tâche **stockage > Ajouter une stratégie d'exportation de stockage au volume** à partir de la section **Outils** de la zone **Design**.
3. Cliquez sur **Ajouter une stratégie d'exportation de stockage au volume**. Dans la zone **Propriétés de tâche**, cliquez sur l'onglet **général**. Vous pouvez également modifier le nom et la description de cette tâche. Dans cet exemple, le nom de la tâche est Ajouter une stratégie d'exportation de stockage.
4. Utilisez Connector pour établir une connexion entre les tâches **Créer un volume dans FlexPod** et **Ajouter une stratégie d'exportation de stockage**. Cliquez sur **Enregistrer**.



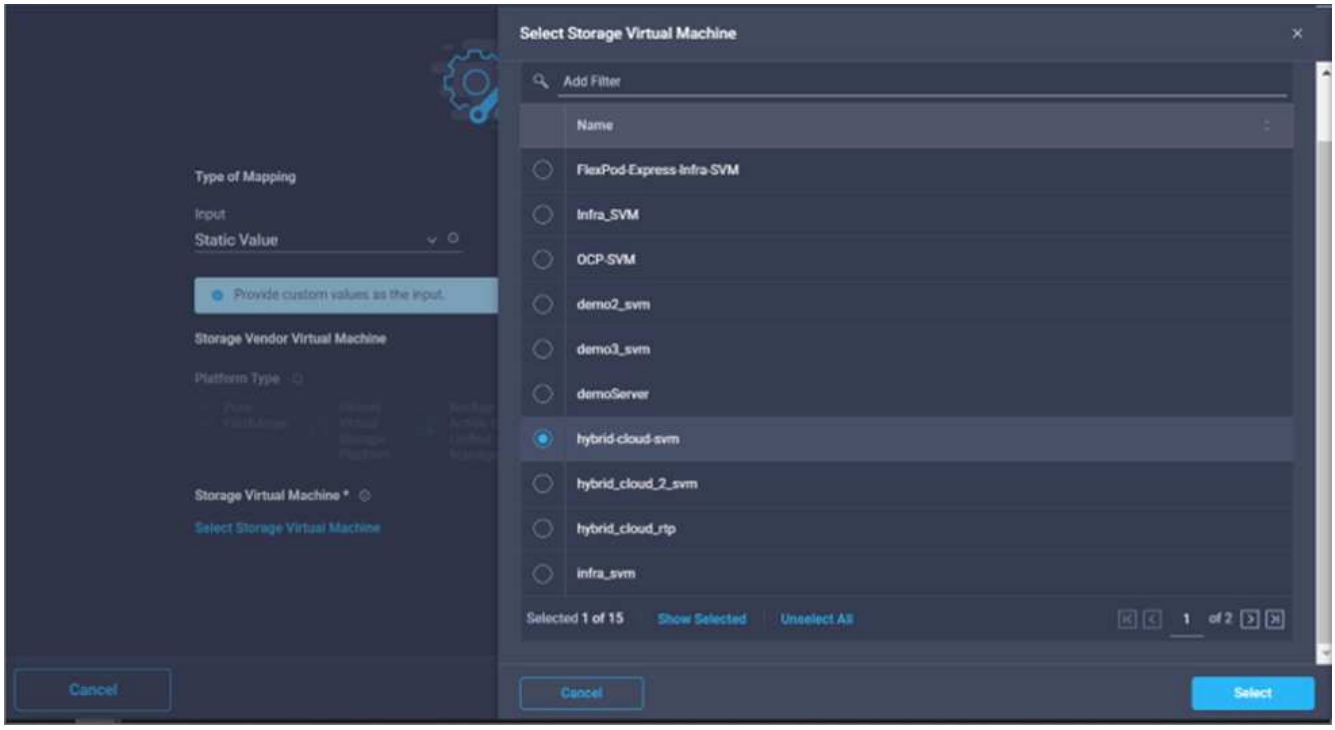
5. Dans la zone **Propriétés de tâche**, cliquez sur **entrées**.
6. Cliquez sur **Map** dans le champ **Storage Device**.



7. Choisissez **valeur statique** et cliquez sur **Sélectionner le périphérique de stockage**. Sélectionnez la même cible de stockage ajoutée lors de la création de la tâche précédente de création d'un volume de stockage.
8. Cliquez sur **carte**.

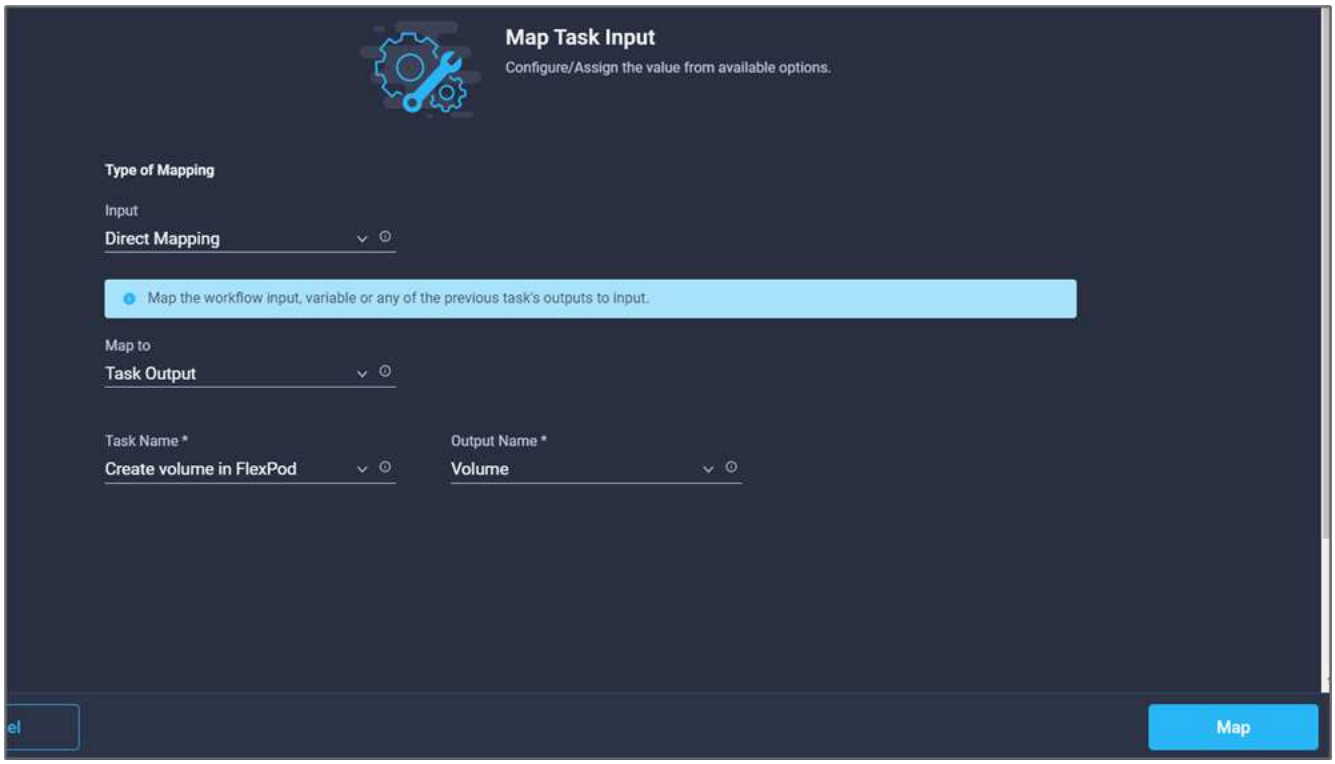


9. Cliquez sur **Map** dans le champ **Storage Vendor Virtual machine**.
10. Choisissez **valeur statique** et cliquez sur **Sélectionner Storage Virtual machine**. Sélectionnez la même machine virtuelle de stockage ajoutée lors de la création de la précédente tâche de création d'un volume de stockage.

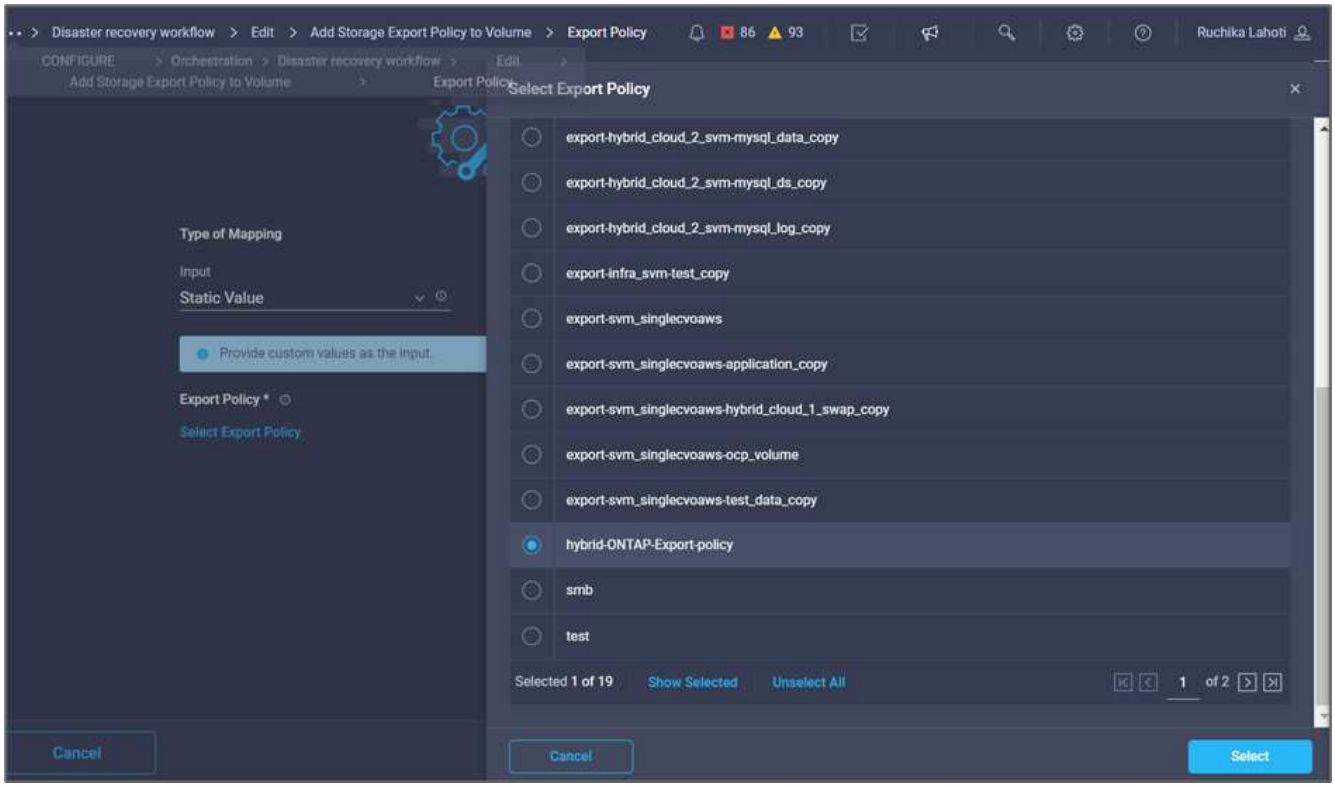


11. Cliquez sur **carte**.
12. Cliquez sur **Map** dans le champ **Volume**.
13. Cliquez sur **Nom de la tâche**, puis sur **Créer un volume dans FlexPod**. Cliquez sur **Nom de sortie**, puis sur **Volume**.

> Dans Cisco Intersight Cloud Orchestrator, vous pouvez fournir la sortie d'une tâche précédente comme entrée pour une nouvelle tâche. Dans cet exemple, les détails **Volume** ont été fournis à partir de la tâche **Créer un volume dans FlexPod** sous forme d'entrée pour la tâche **Ajouter une stratégie d'exportation de stockage**.



14. Cliquez sur **carte**.
15. Cliquez sur **carte** dans le champ **politique d'exportation**.
16. Choisissez **valeur statique** et cliquez sur **Sélectionner stratégie d'exportation**. Sélectionner la export policy créée.

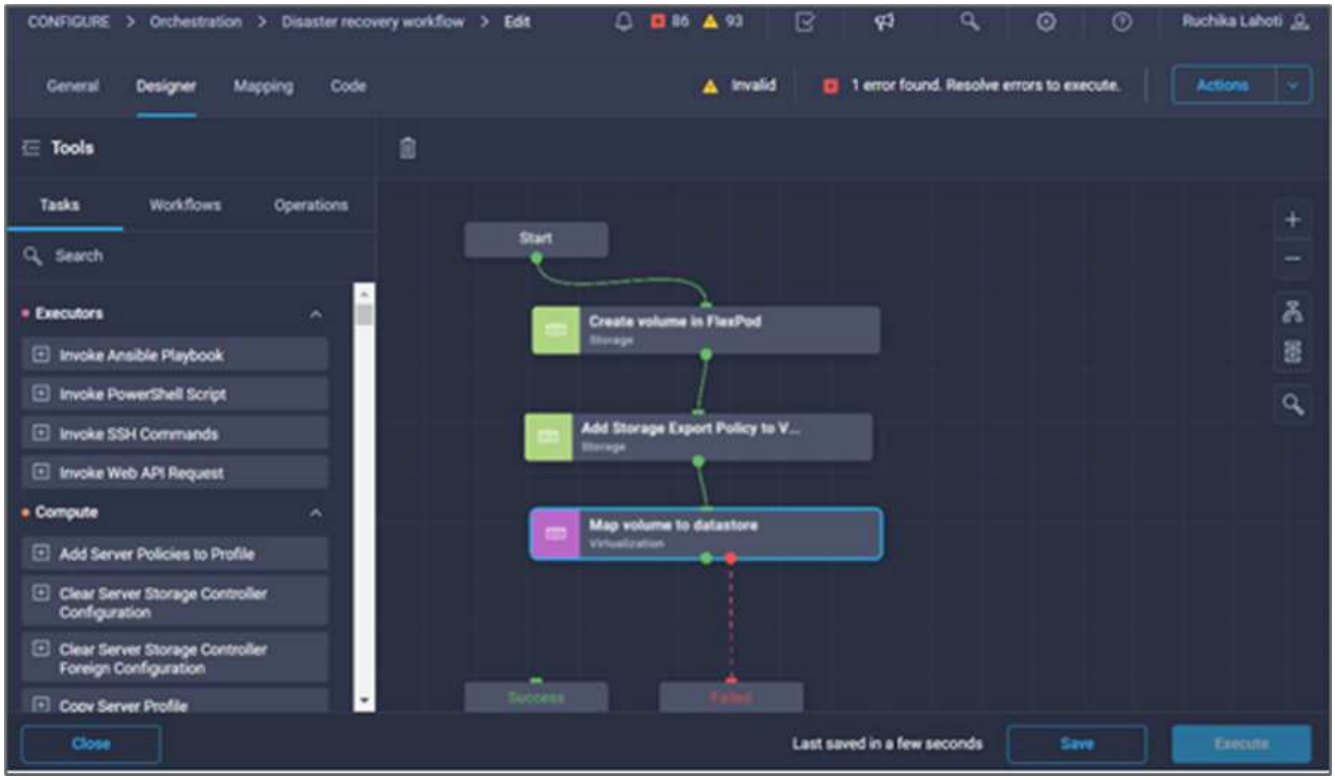


17. Cliquez sur **carte**, puis sur **Enregistrer**.

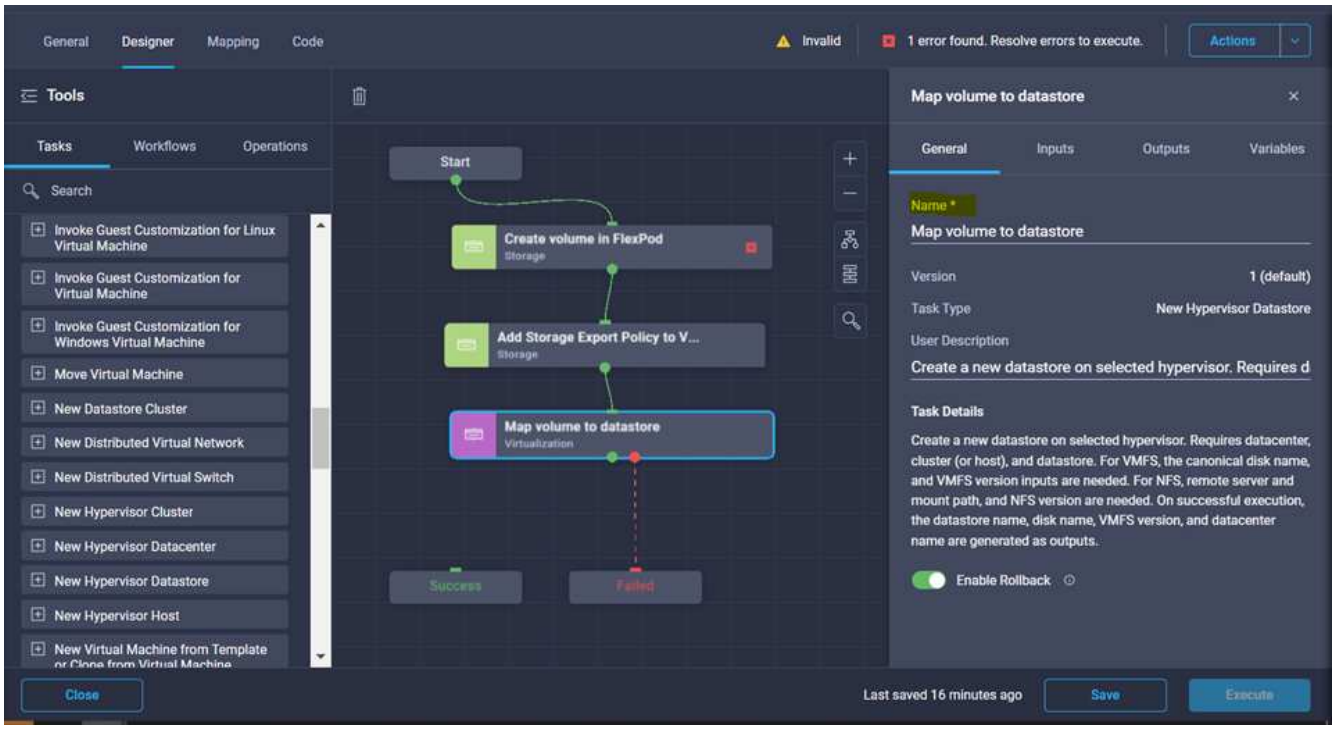
L'ajout d'une export-policy au volume est maintenant terminé. Ensuite, vous créez un nouveau datastore mappant le volume créé.

Procédure 4 : mappe de volumes FlexPod sur le datastore

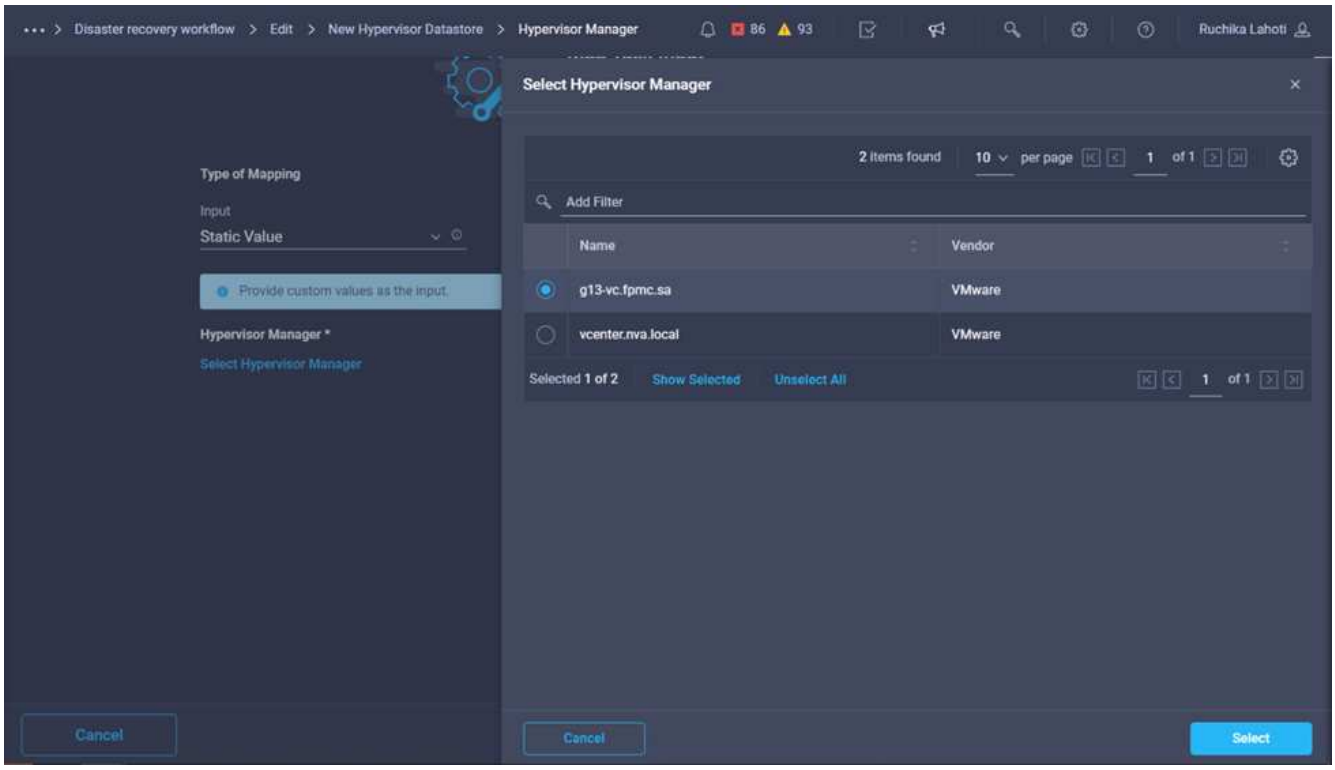
1. Accédez à l'onglet **Designer** et cliquez sur **tâches** dans la section **Outils**.
2. Faites glisser et déposez la tâche **virtualisation > Nouveau datastore d'hyperviseur** de la section **Outils** de la zone **Design**.
3. Utilisez Connector pour établir une connexion entre les tâches **Ajouter stratégie d'exportation de stockage** et **Nouveau datastore d'hyperviseur**. Cliquez sur **Enregistrer**.



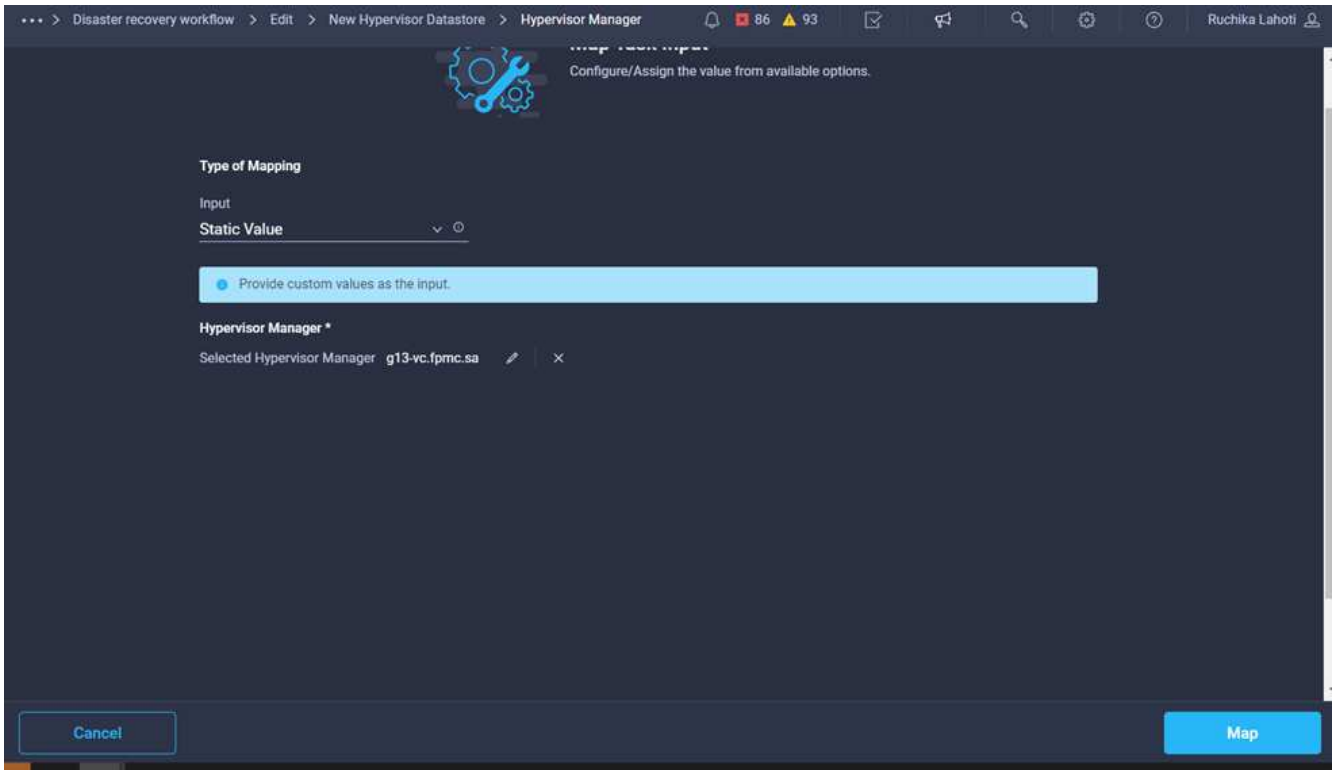
4. Cliquez sur **Nouveau datastore d'hyperviseur**. Dans la zone **Propriétés de tâche**, cliquez sur l'onglet **général**. Vous pouvez également modifier le nom et la description de cette tâche. Dans cet exemple, le nom de la tâche est **mapper le volume sur le datastore**.



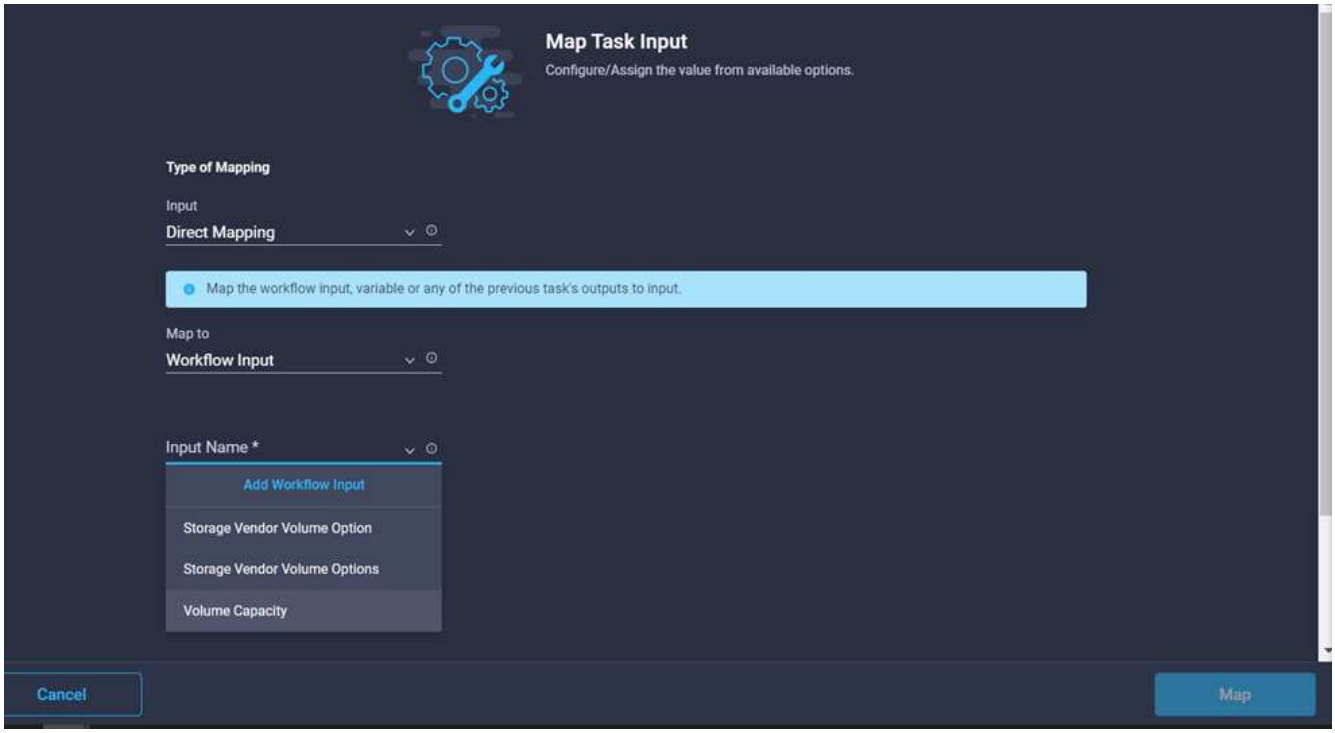
5. Dans la zone **Propriétés de tâche**, cliquez sur **entrées**.
6. Cliquez sur **Map** dans le champ **Hypervisor Manager**.
7. Choisissez **valeur statique** et cliquez sur **Select Hypervisor Manager**. Cliquez sur la cible VMware vCenter.



8. Cliquez sur **carte**.



9. Cliquez sur **carte** dans le champ **Data Center**. Il s'agit du data Center associé au nouveau datastore.
10. Choisissez **mappage direct** et cliquez sur **entrée de flux de travail**.
11. Cliquez sur **Nom d'entrée**, puis sur **Créer entrée de flux de travail**.

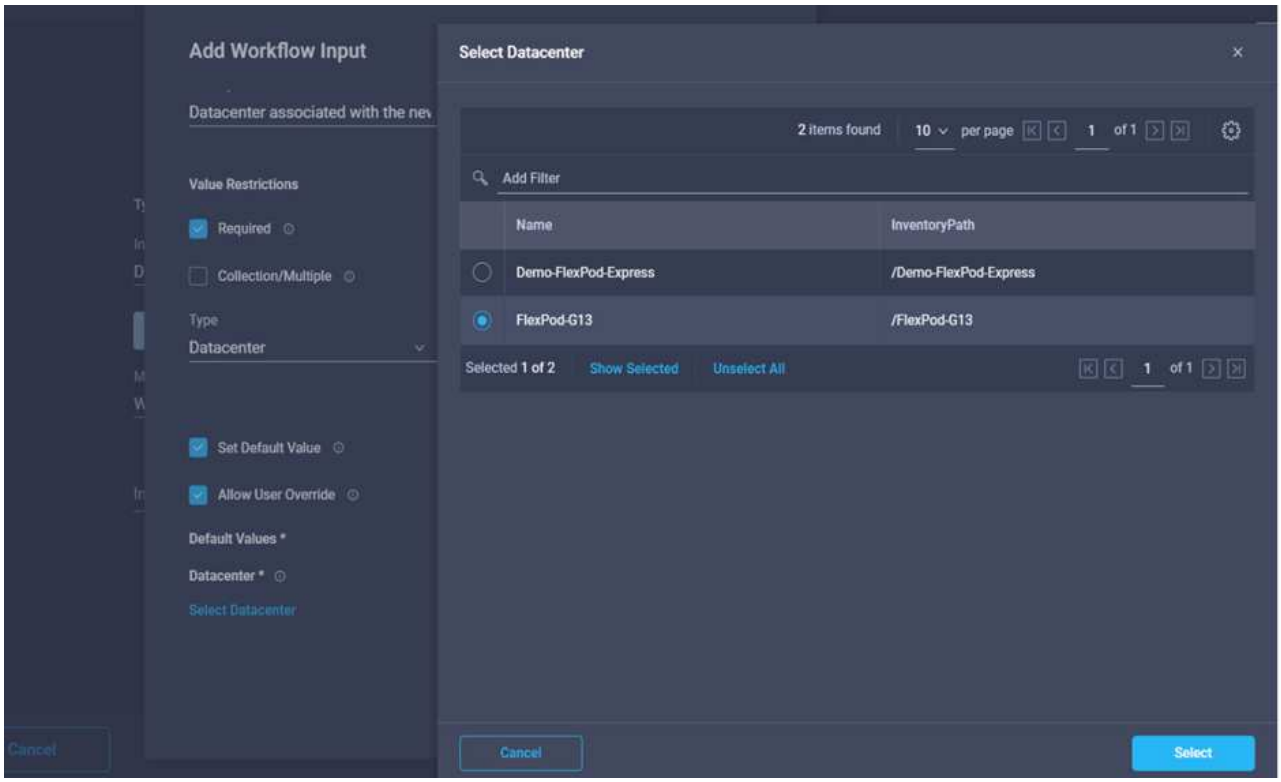


12. Dans l'assistant Ajouter une entrée, procédez comme suit :
    a. Indiquez un nom d'affichage et un nom de référence (facultatif).
    b. Sélectionnez **Datacenter** comme type.

c. Cliquez sur **définir la valeur par défaut et remplacer**.

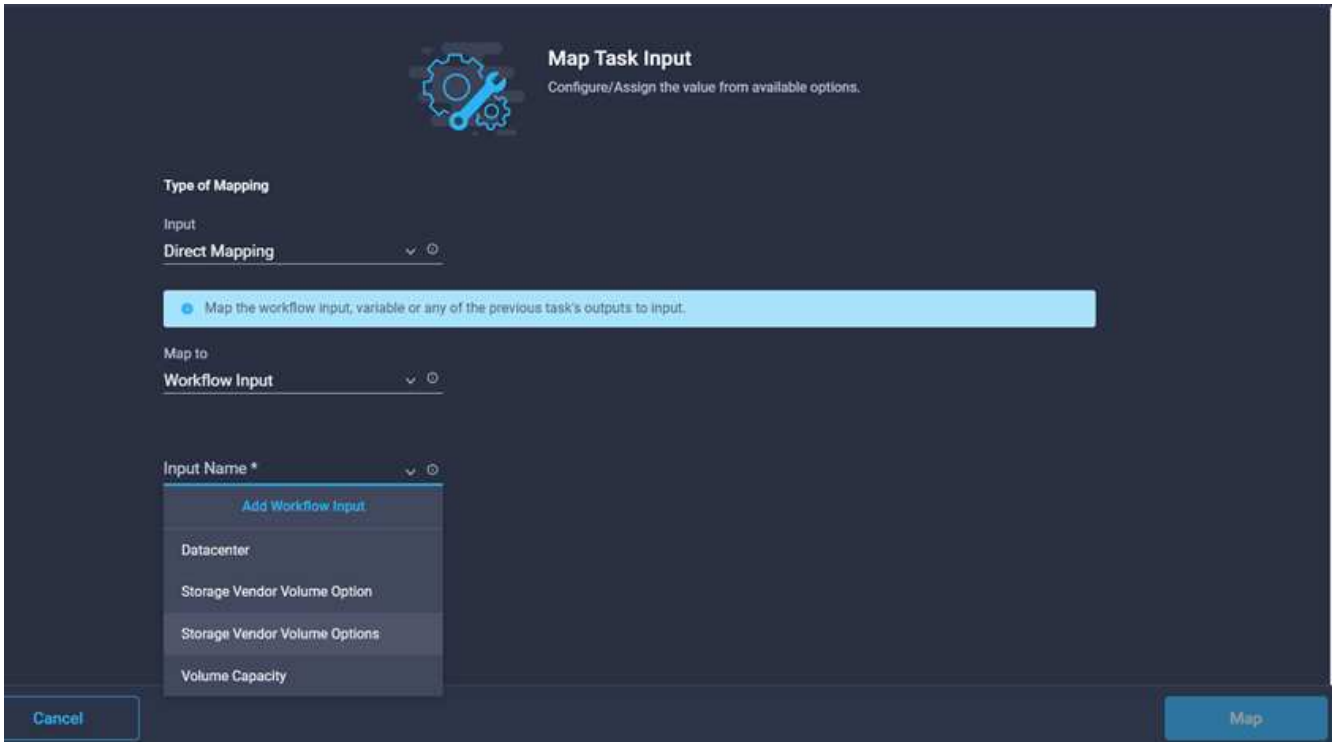
d. Cliquez sur **Select Datacenter**.

e. Cliquez sur le centre de données associé au nouveau datastore, puis sur **Select**.

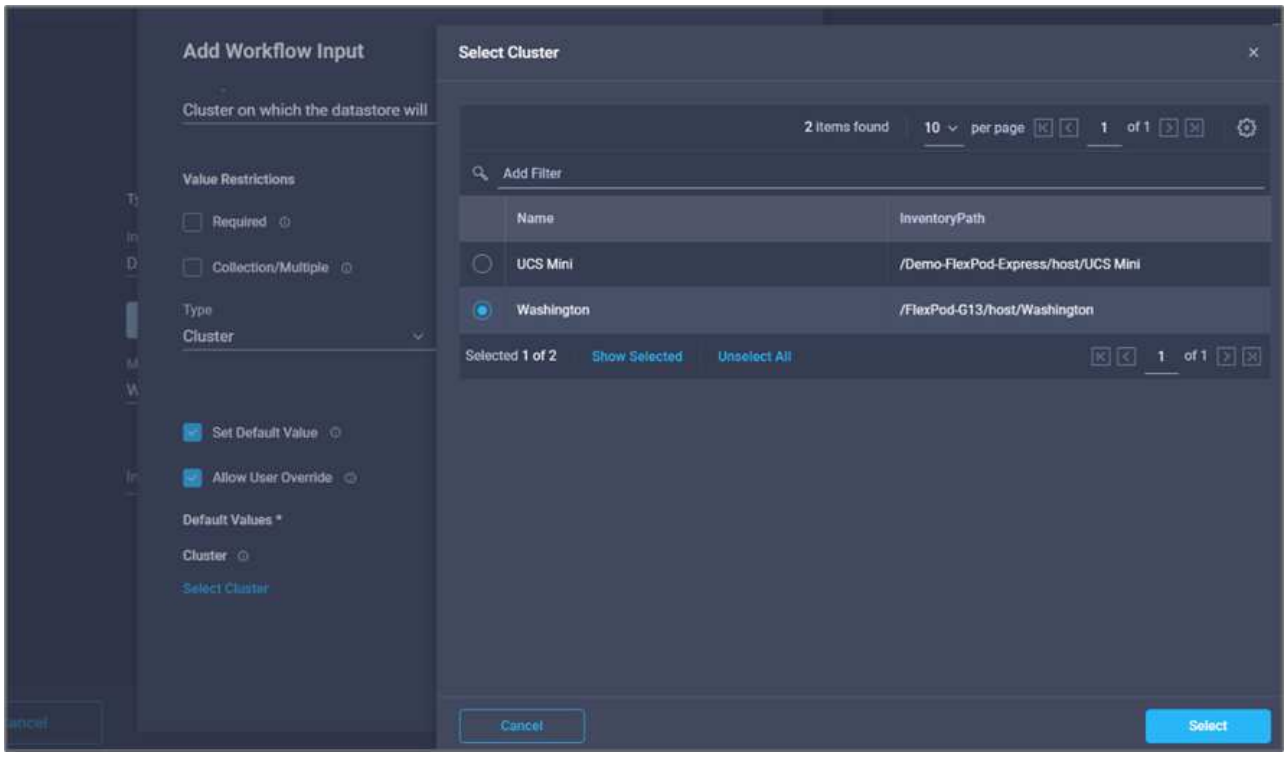


- Cliquez sur **Ajouter**.

13. Cliquez sur **carte**.
14. Cliquez sur **carte** dans le champ **Cluster**.
15. Choisissez **mappage direct** et cliquez sur **entrée de flux de travail**.

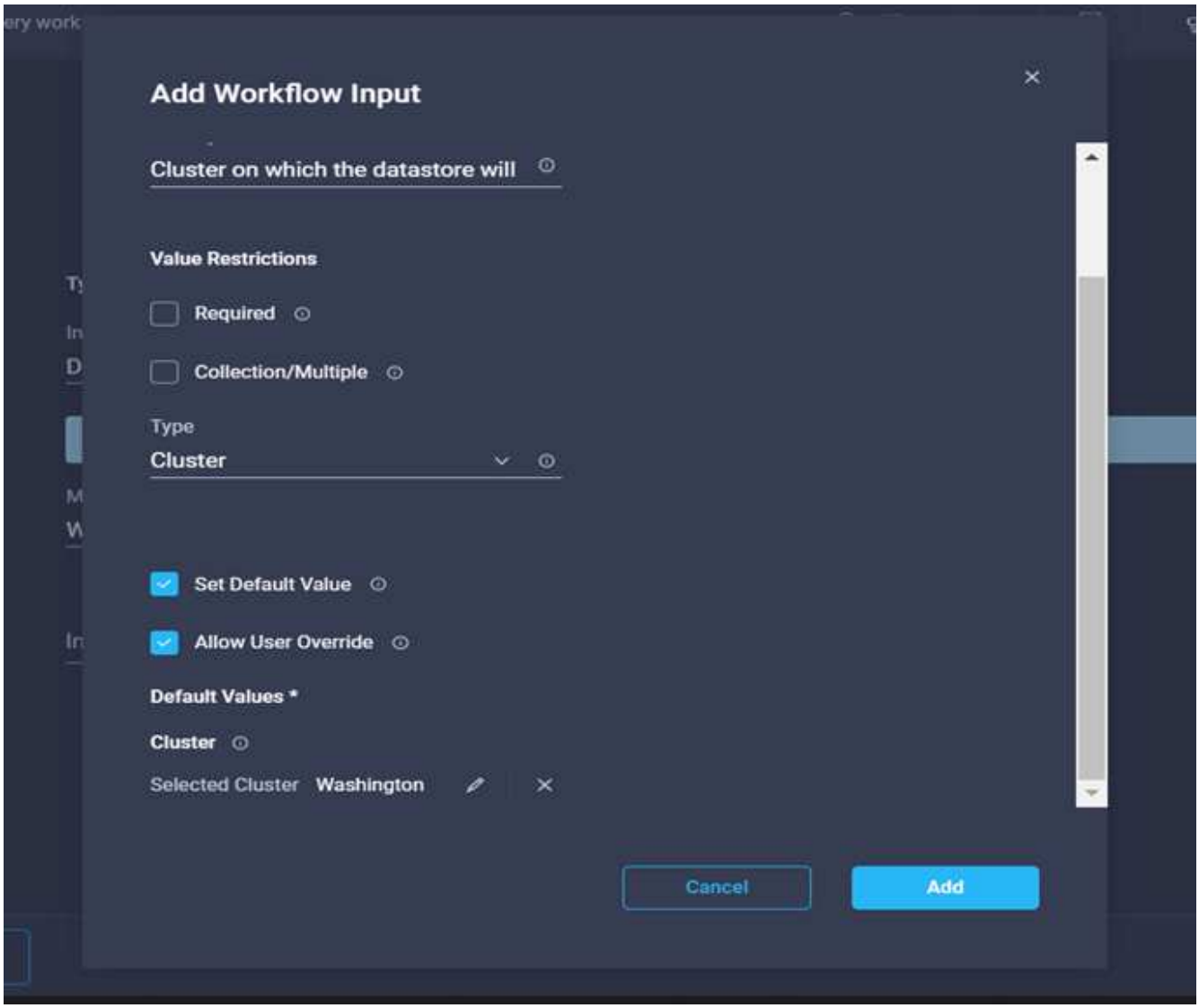


16. Dans l’assistant Ajouter une entrée, procédez comme suit :
    a. Indiquez un nom d’affichage et un nom de référence (facultatif).
    b. Cliquez sur **requis**.
    c. Sélectionnez Cluster comme type.
    d. Cliquez sur **définir la valeur par défaut et remplacer**.
    e. Cliquez sur **Sélectionner un cluster**.
    f. Cliquez sur le cluster associé au nouveau datastore.
    g. Cliquez sur **Sélectionner**.

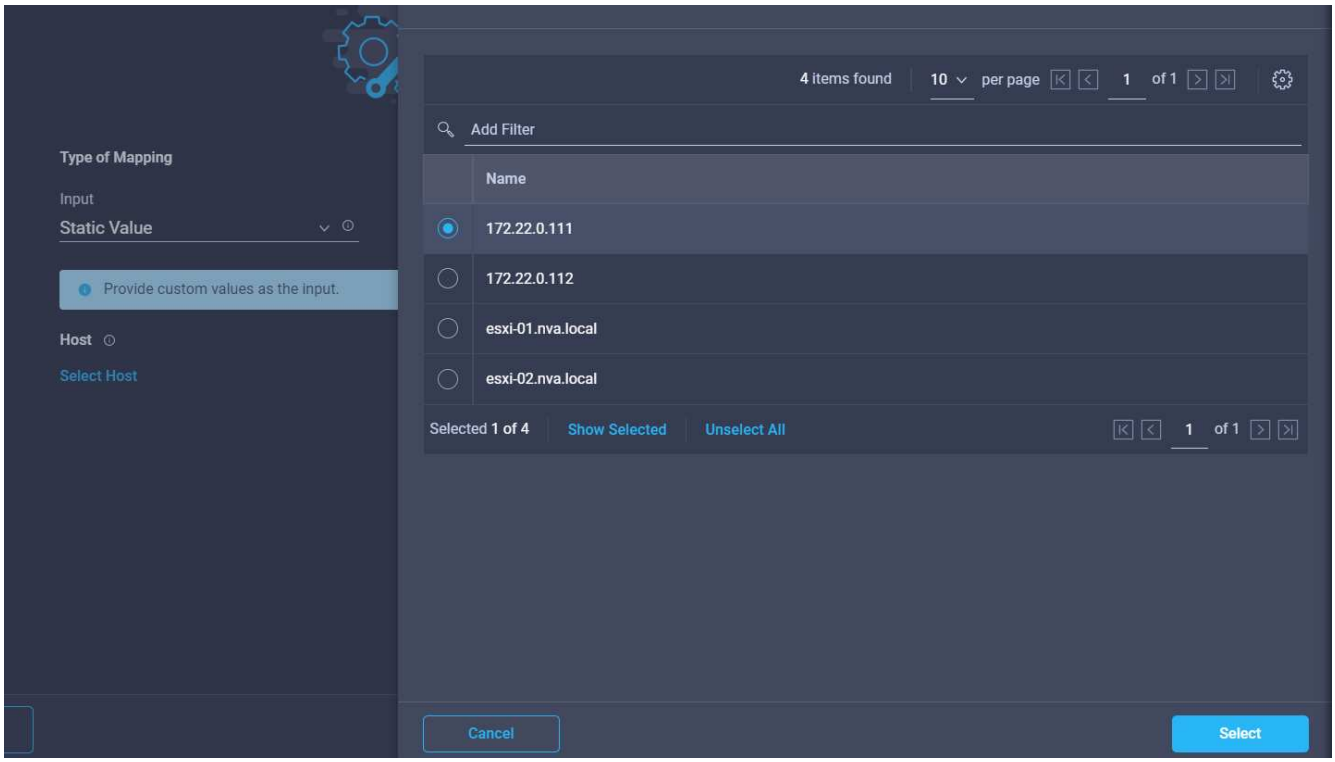


h. Cliquez sur **Ajouter**.

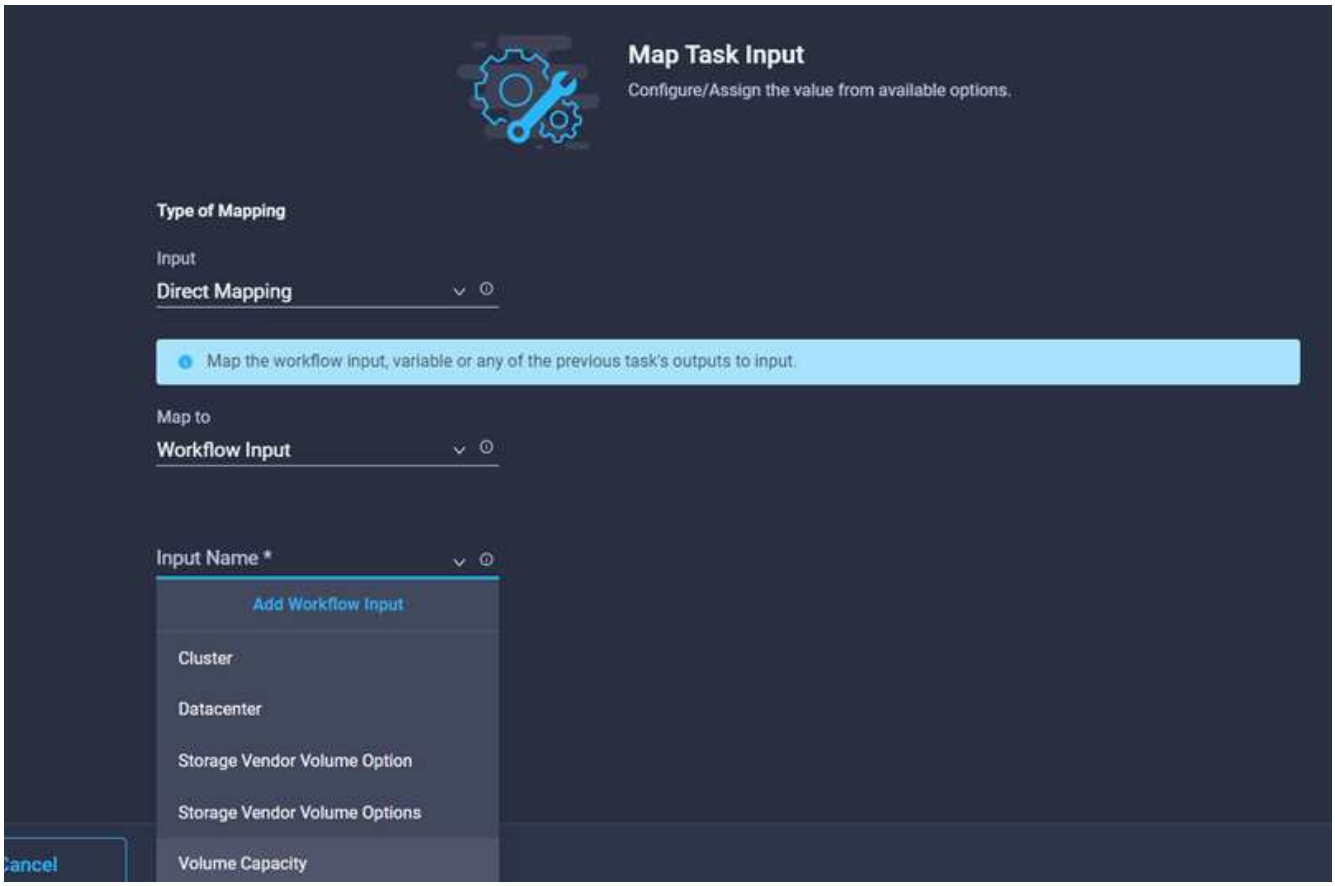
17. Cliquez sur **carte**.
18. Cliquez sur **Map** dans le champ **Host**.



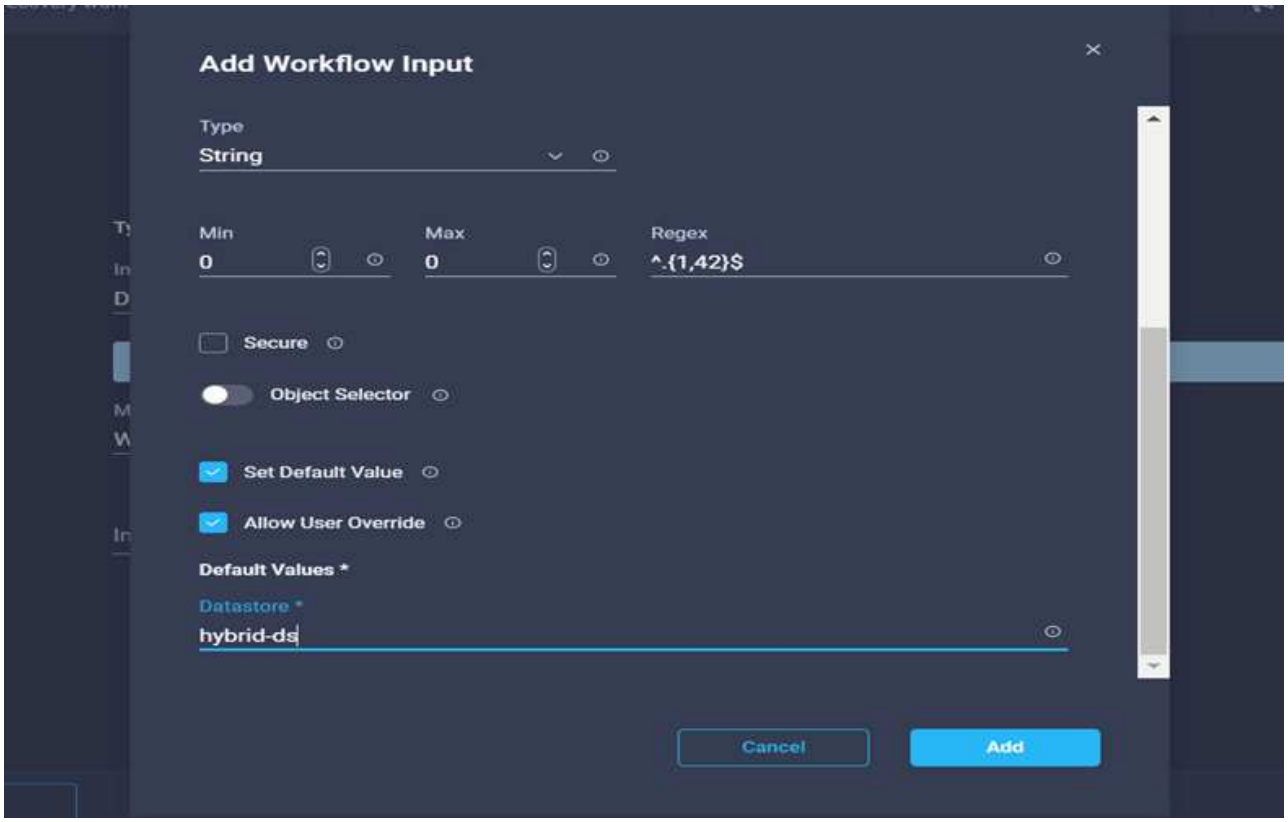
19. Choisissez **valeur statique** et cliquez sur l'hôte sur lequel le datastore sera hébergé. Si un cluster est spécifié, l'hôte est ignoré.



20. Cliquez sur **Sélectionner et carte**.
21. Cliquez sur **Map** dans le champ **datastore**.
22. Choisissez **mappage direct** et cliquez sur **entrée de flux de travail**.
23. Cliquez sur **Nom d'entrée** et **Créer une entrée de flux de travail**.

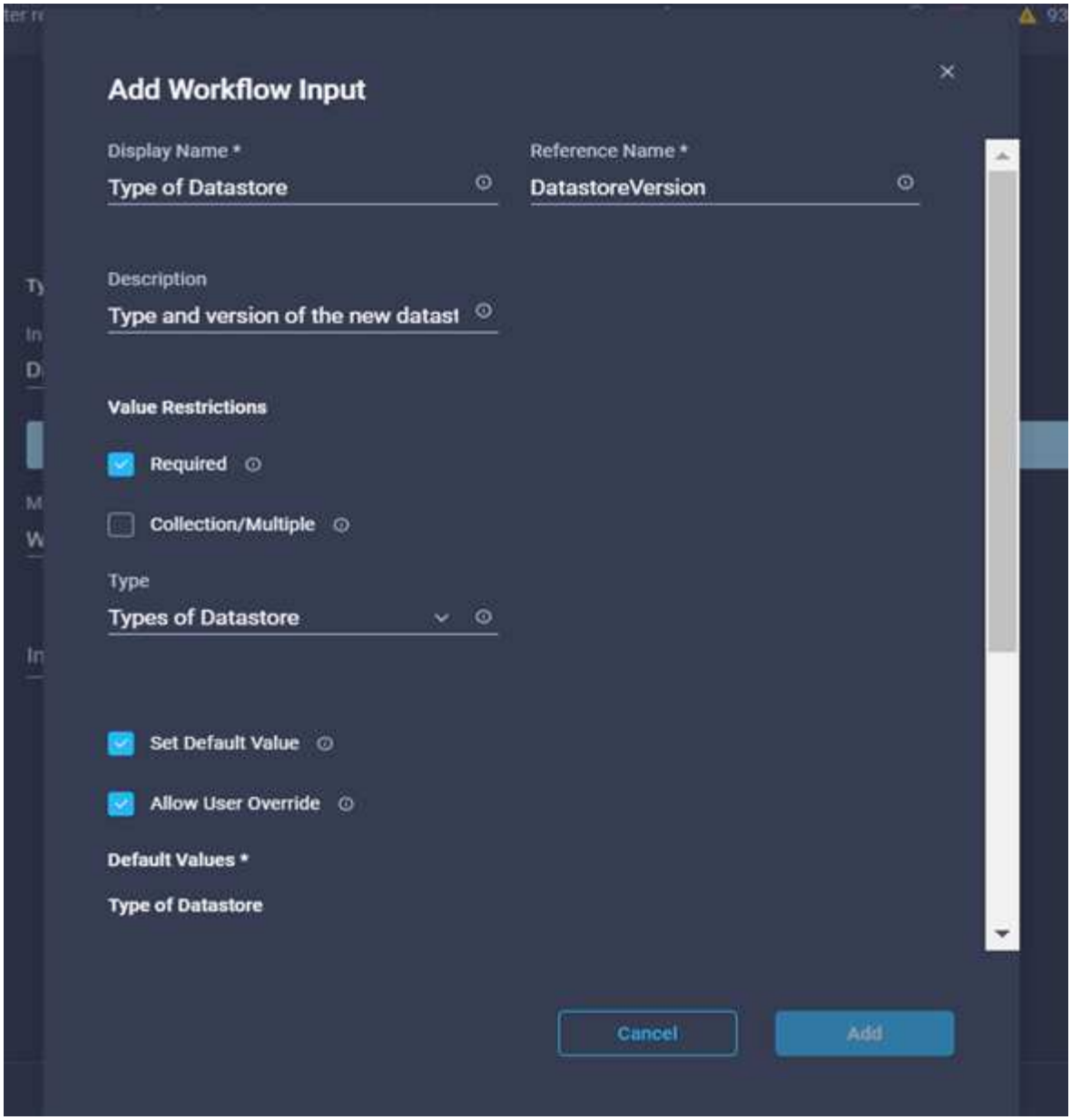


24. Dans l’assistant Ajouter une entrée :
    a. Indiquez un nom d’affichage et un nom de référence (facultatif).
    b. Cliquez sur **requis**.
    c. Cliquez sur **définir la valeur par défaut et remplacer**.
    d. Indiquez une valeur par défaut pour le datastore et cliquez sur **Ajouter**.



25. Cliquez sur **carte**.
26. Cliquez sur **carte** dans le champ de saisie **Type de datastore**.
27. Choisissez **mappage direct** et cliquez sur **entrée de flux de travail**.
28. Cliquez sur **Nom d’entrée** et **Créer une entrée de flux de travail**.

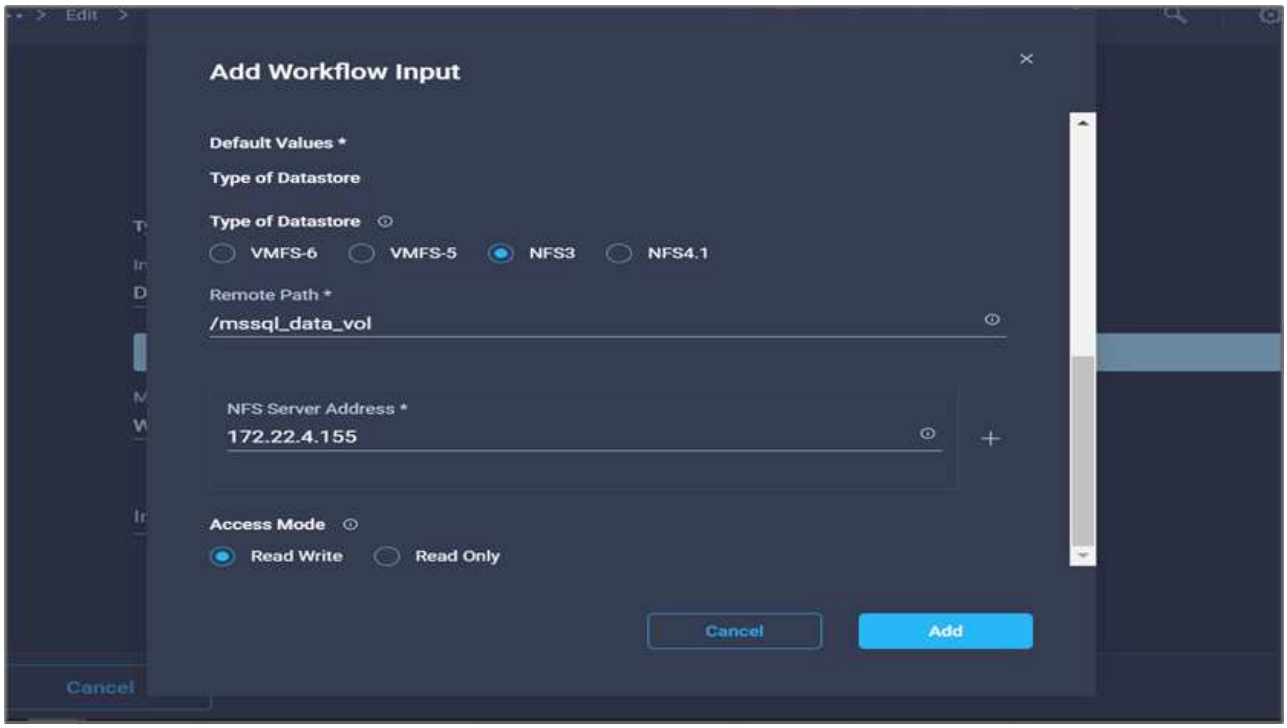
29. Dans l'assistant Ajouter une entrée, procédez comme suit :
    a. Indiquez un nom d'affichage et un nom de référence (facultatif) et cliquez sur **requis**.
    b. Assurez-vous de sélectionner le type **types de datastore** et cliquez sur **définir la valeur par défaut et remplacer**.



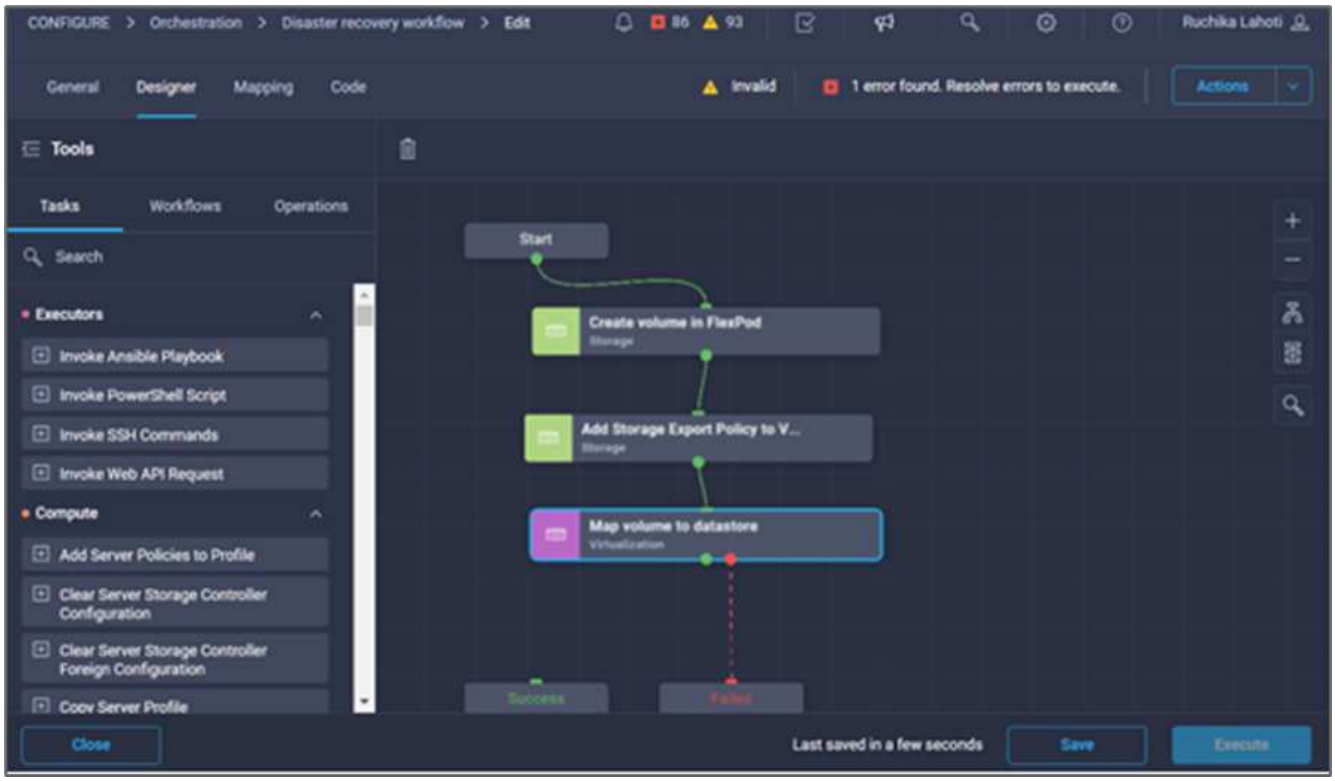
c. Indiquez le chemin distant. Il s'agit du chemin d'accès distant du point de montage NFS.

d. Indiquez les noms d'hôte ou les adresses IP du serveur NFS distant dans l'adresse du serveur NFS.

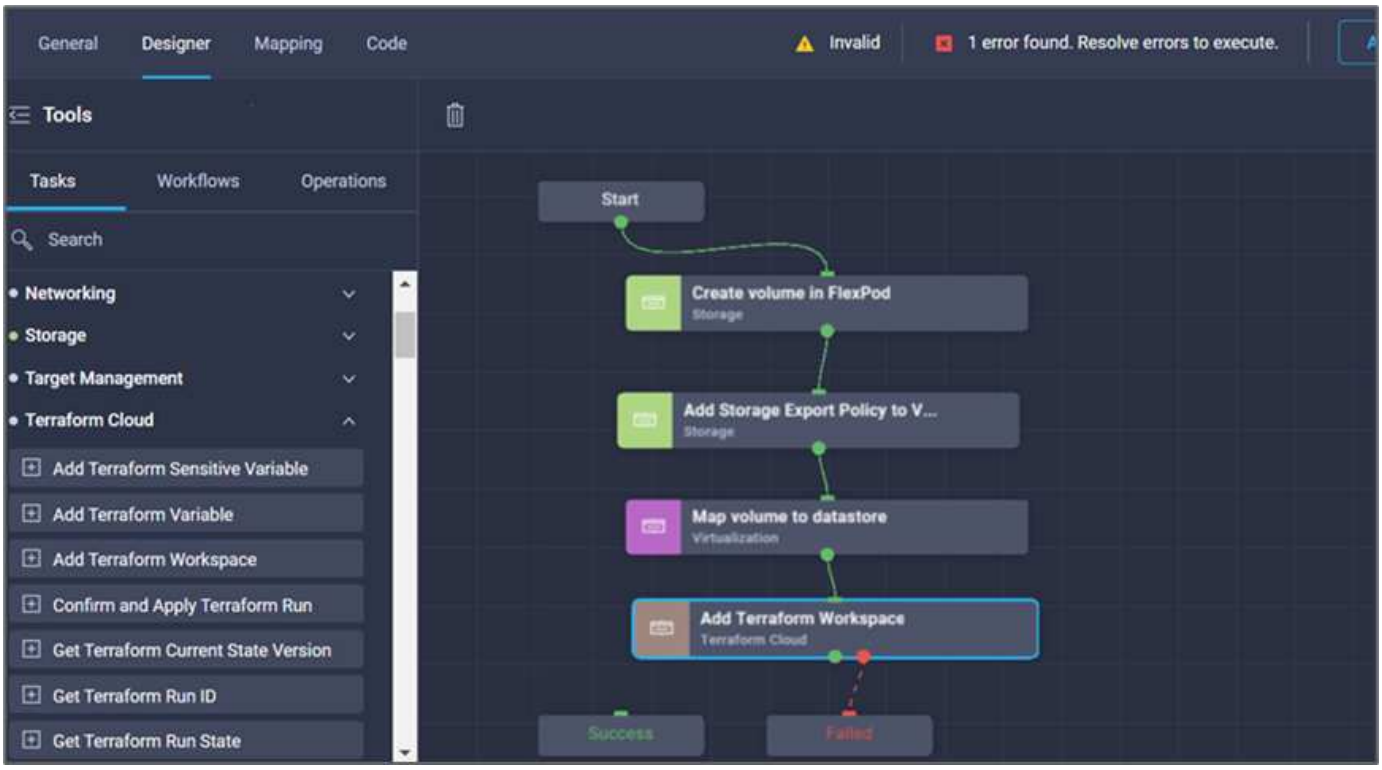
e. Cliquez sur le **mode d'accès**. Le mode d'accès est destiné au serveur NFS. Cliquez sur lecture seule si les volumes sont exportés en lecture seule. Cliquez sur **Ajouter**.



30. Cliquez sur **carte**.
31. Cliquez sur **Enregistrer**.

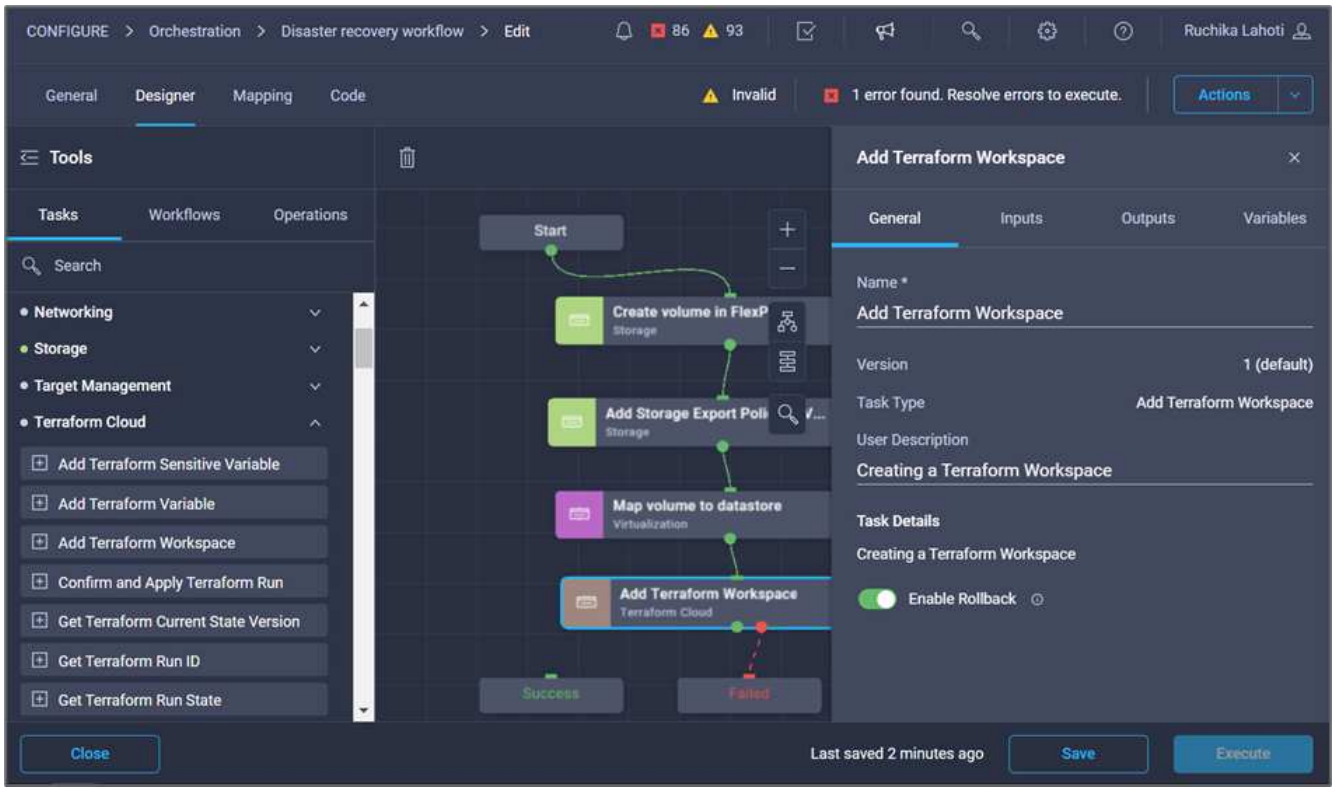


La tâche de création du datastore est terminée. Toutes les tâches effectuées dans le data Center FlexPod sur site sont effectuées.

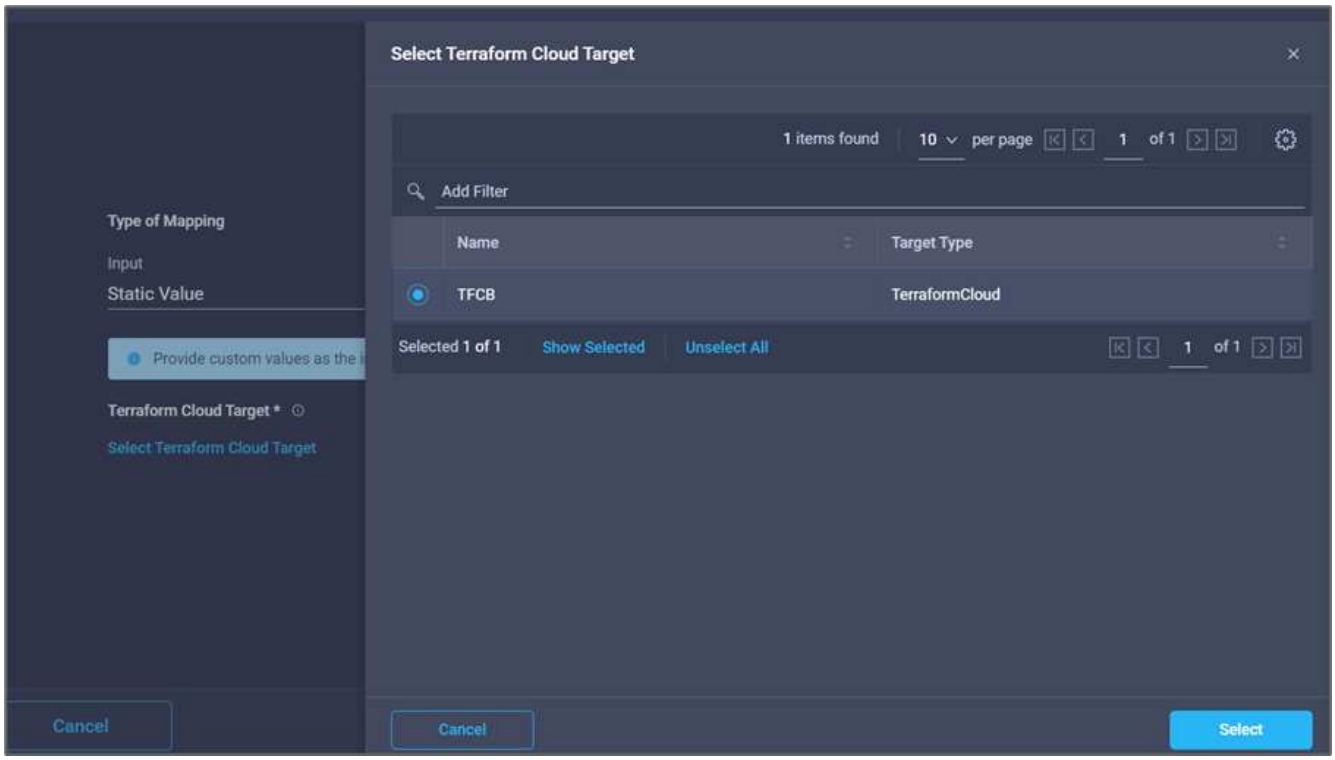


Procédure 5 : Ajout d'un nouvel espace de travail Terraform

1. Accédez à l'onglet **Designer** et cliquez sur **tâches** dans la section **Outils**.
2. Faites glisser et déposez la tâche **Terraform Cloud > Ajouter un espace de travail Terraform** dans la section Outils de la zone conception.
3. Utilisez Connector pour connecter les tâches **Map volume au datastore** et **Add Terraform Workspace** et cliquez sur **Save**.
4. Cliquez sur **Ajouter un espace de travail Terraform**. Dans la zone Propriétés de la tâche, cliquez sur l'onglet **général**. Vous pouvez également modifier le nom et la description de cette tâche.

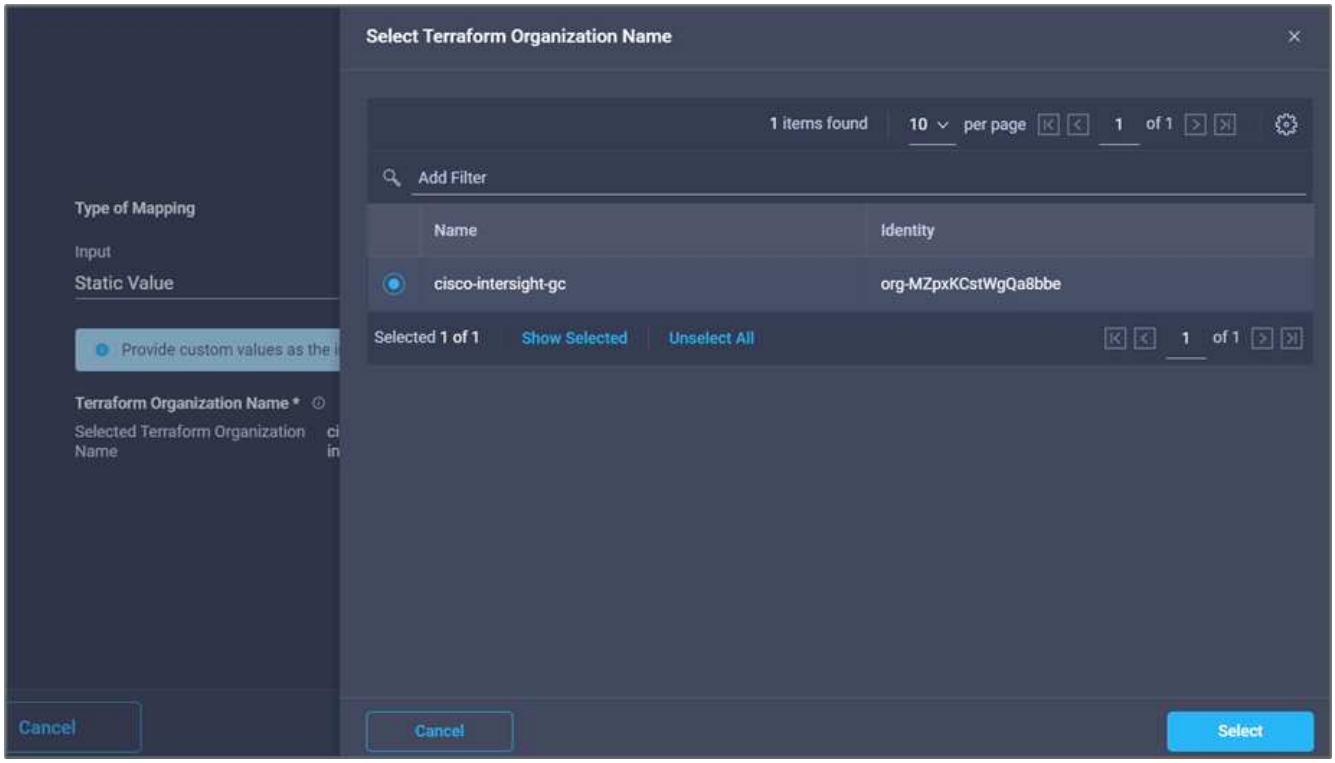


5. Dans la zone Propriétés de la tâche, cliquez sur **entrées**.
6. Cliquez sur **carte** dans le champ de saisie **Terraform Cloud Target**.
7. Choisissez **valeur statique** et cliquez sur **Sélectionner la cible de nuage Terraform**. Sélectionnez le compte Terraform Cloud for Business ajouté comme expliqué dans "Configurez Cisco Intersight Service pour HashiCorp Terraform". ».

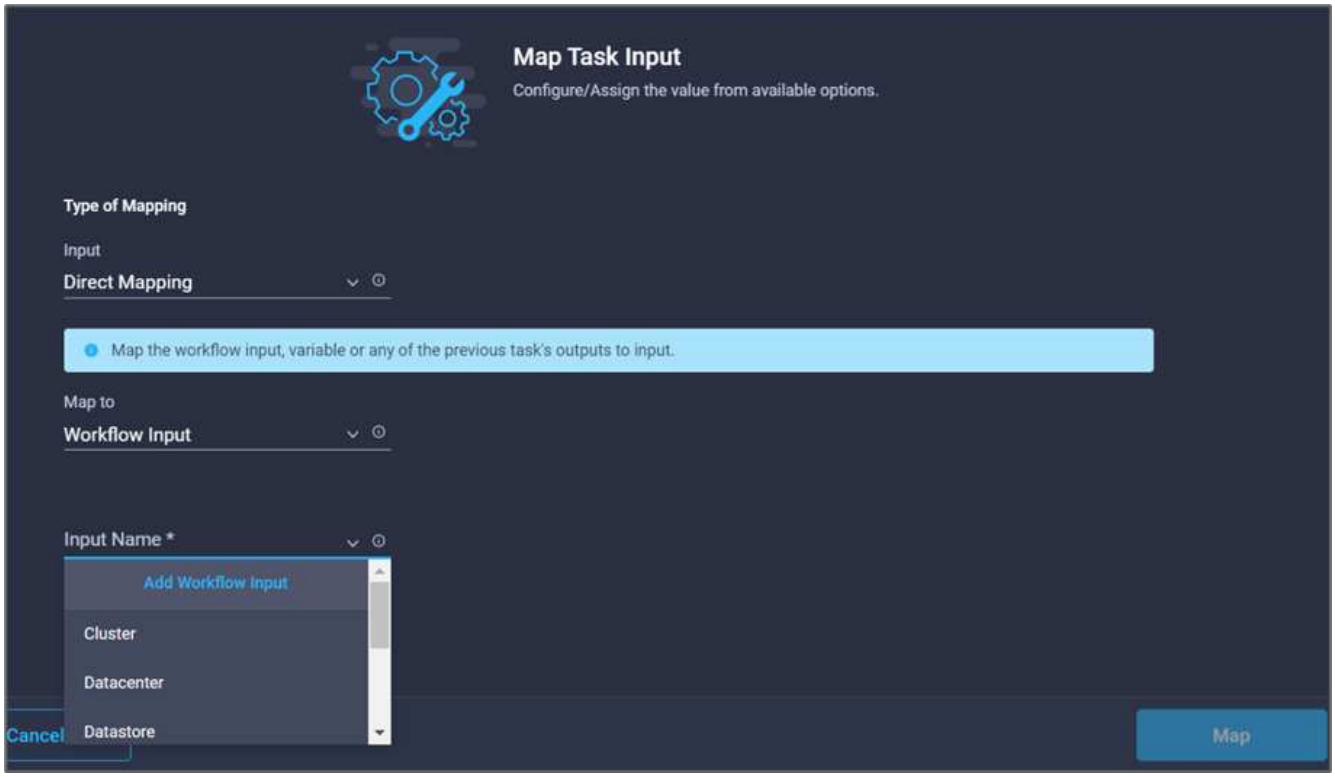


8. Cliquez sur **carte**.

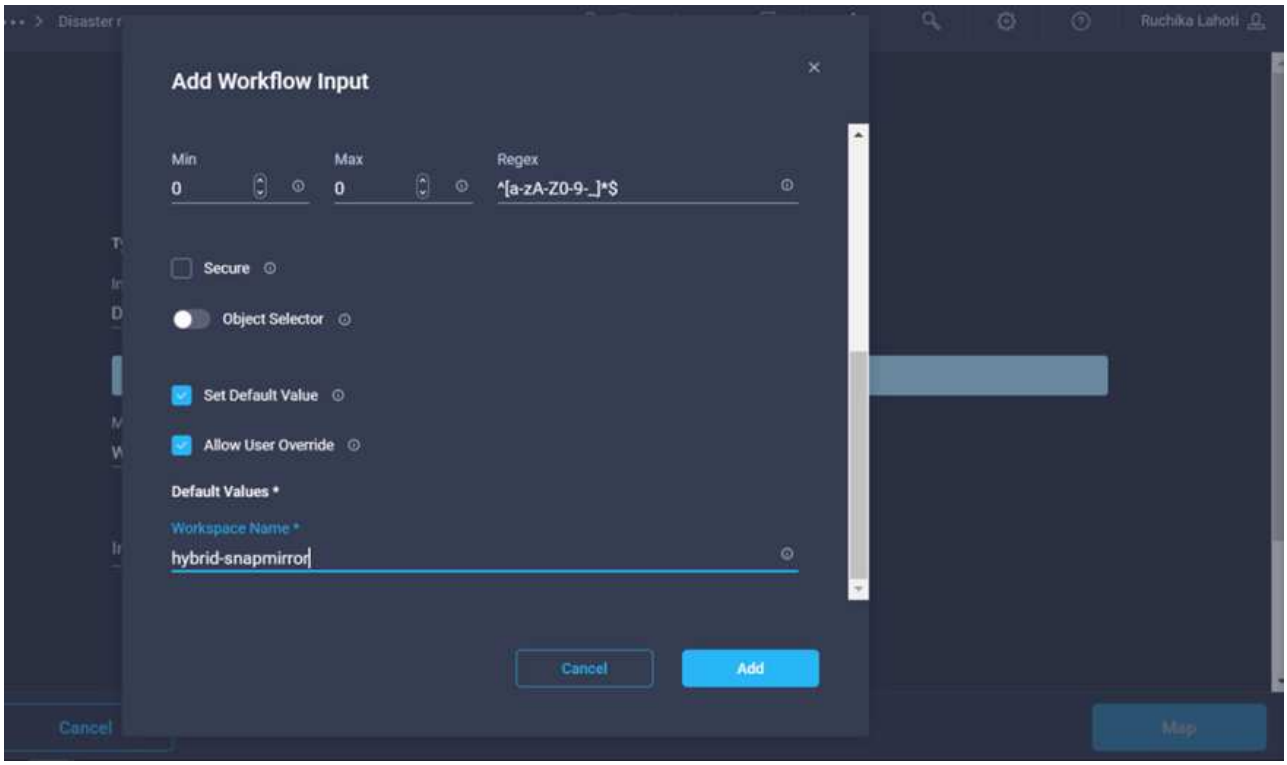
9. Cliquez sur **carte** dans le champ de saisie **Nom de l'organisation Terraform**.
10. Choisissez **valeur statique**, puis cliquez sur **Sélectionner l'organisation Terraform**. Sélectionnez le nom de l'organisation Terraform dont vous faites partie dans votre compte Terraform Cloud for Business.



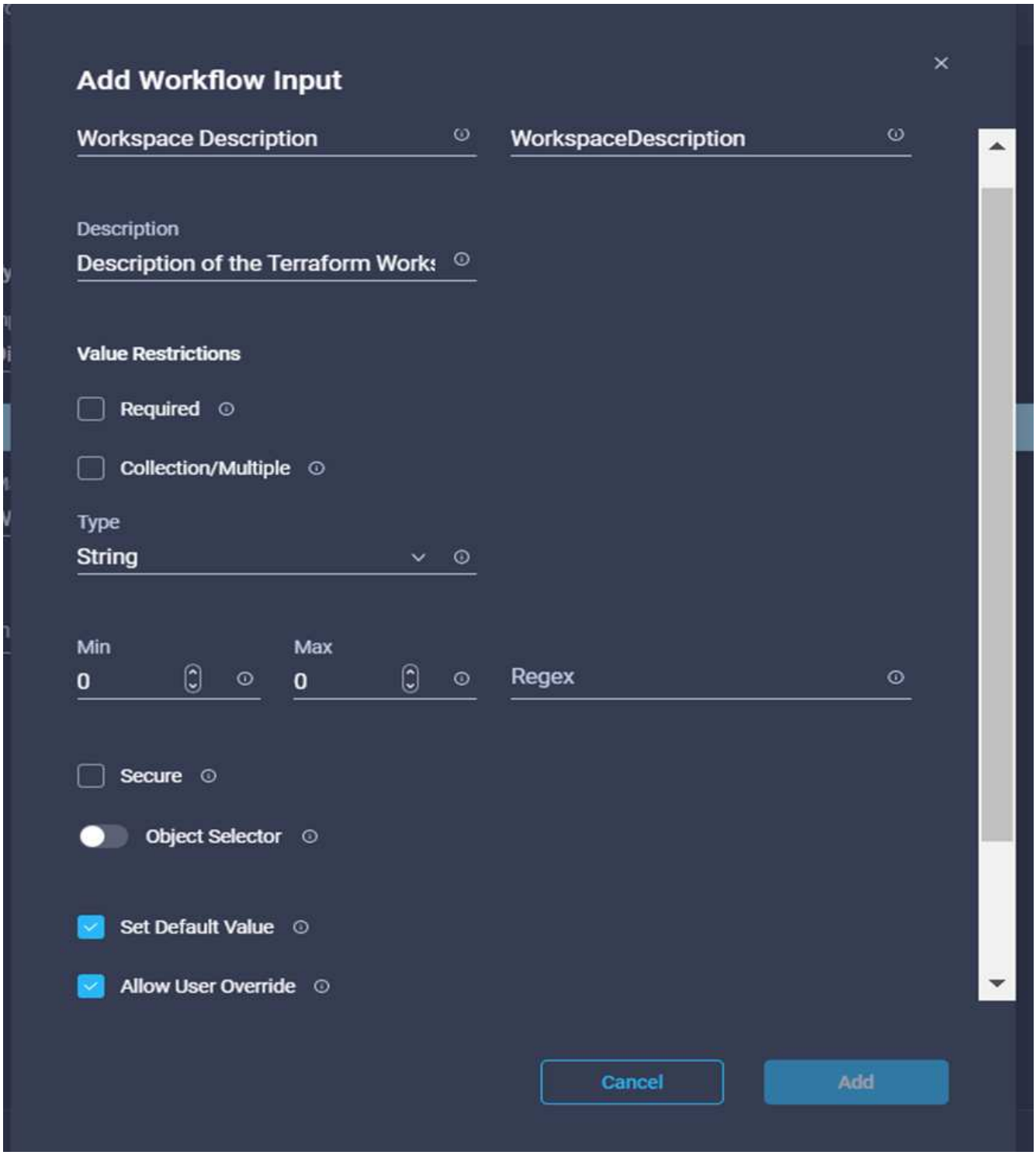
11. Cliquez sur **carte**.
12. Cliquez sur **carte** dans le champ **Nom de l'espace de travail Terraform**. Il s'agit du nouvel espace de travail dans le compte Terraform Cloud for Business.
13. Choisissez **mappage direct** et cliquez sur **entrée de flux de travail**.
14. Cliquez sur **Nom d'entrée** et **Créer une entrée de flux de travail**.



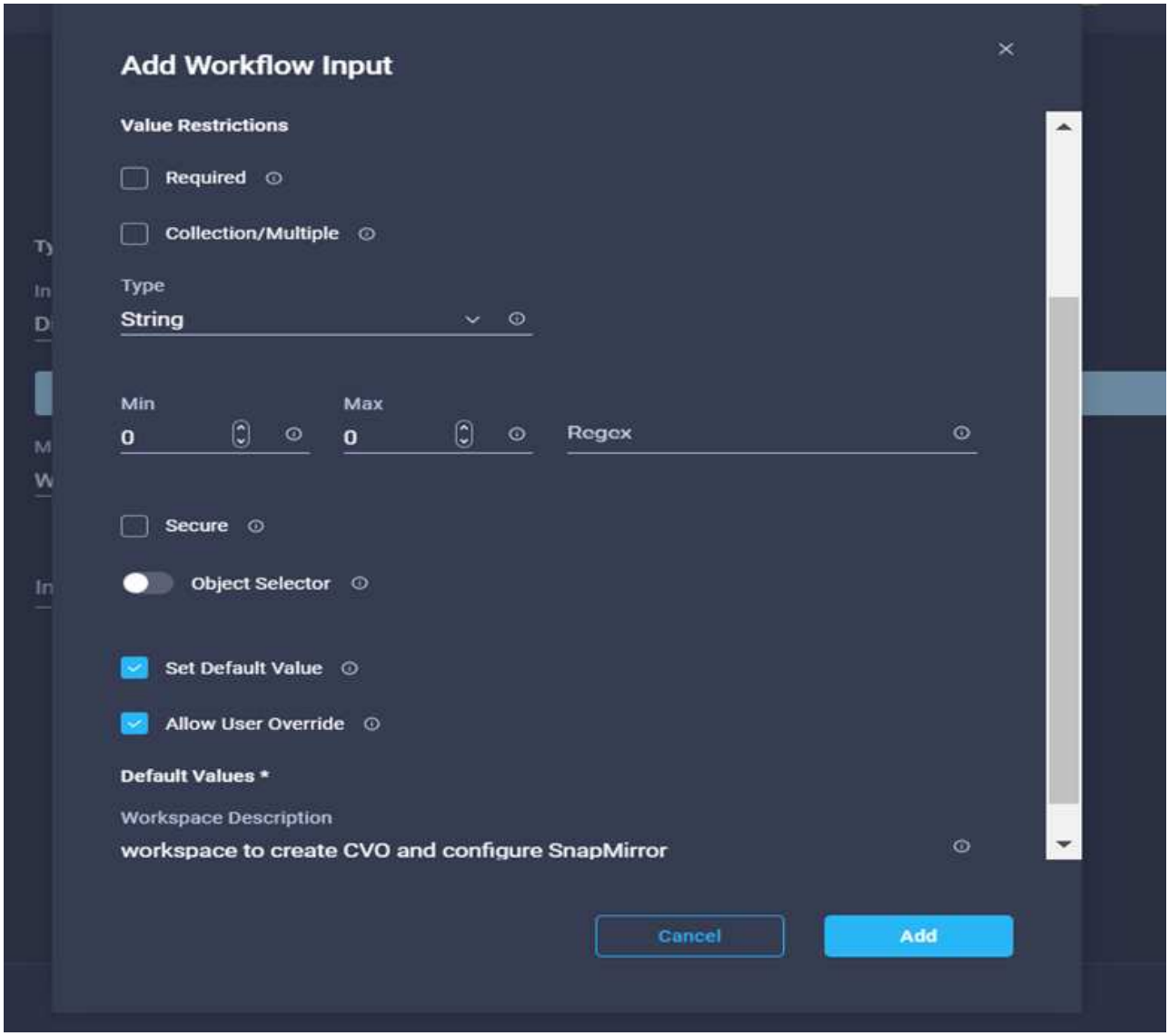
15. Dans l'assistant Ajouter une entrée, procédez comme suit :
    a. Indiquez un nom d'affichage et un nom de référence (facultatif).
    b. Cliquez sur **requis**.
    c. Assurez-vous de sélectionner **String** pour **Type**.
    d. Cliquez sur **définir la valeur par défaut et remplacer**.
    e. Indiquez un nom par défaut pour l'espace de travail.
    f. Cliquez sur **Ajouter**.



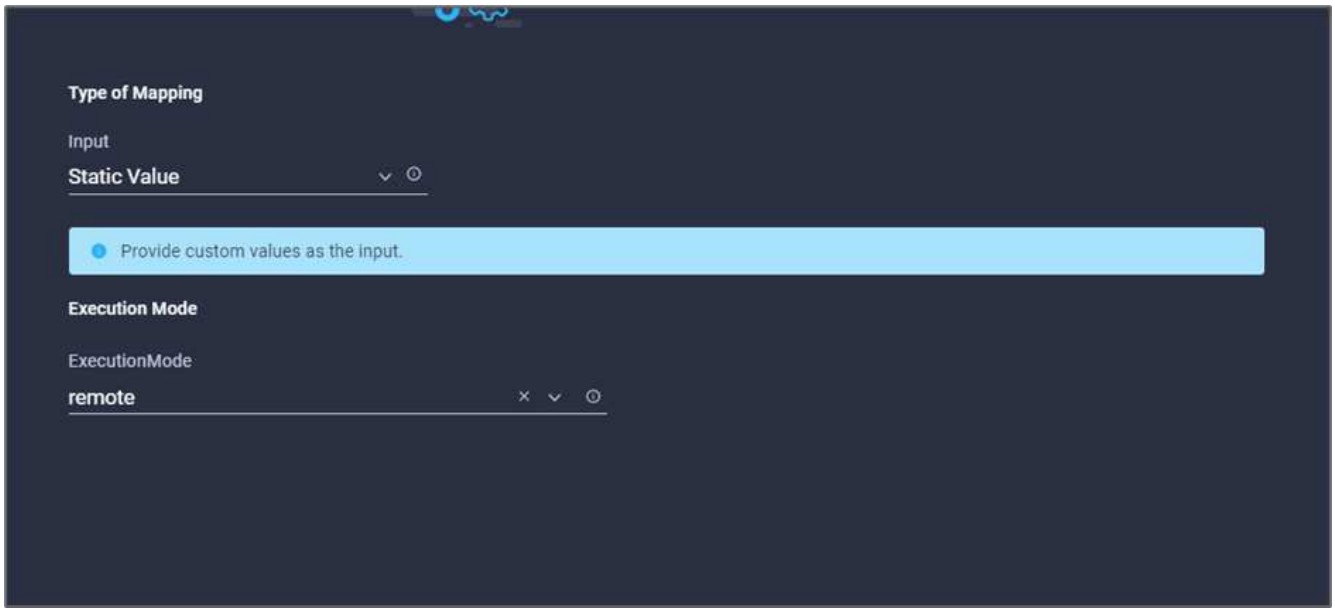
16. Cliquez sur **carte**.
17. Cliquez sur **carte** dans le champ **Description de l'espace de travail**.
18. Choisissez **mappage direct** et cliquez sur **entrée de flux de travail**.
19. Cliquez sur **Nom d'entrée** et **Créer une entrée de flux de travail**.



20. Dans l’assistant Ajouter une entrée, procédez comme suit :
    a. Indiquez un nom d’affichage et un nom de référence (facultatif).
    b. Assurez-vous de sélectionner **String** pour **Type**.
    c. Cliquez sur **définir la valeur par défaut et remplacer**.
    d. Fournissez une description de l’espace de travail et cliquez sur **Ajouter**.



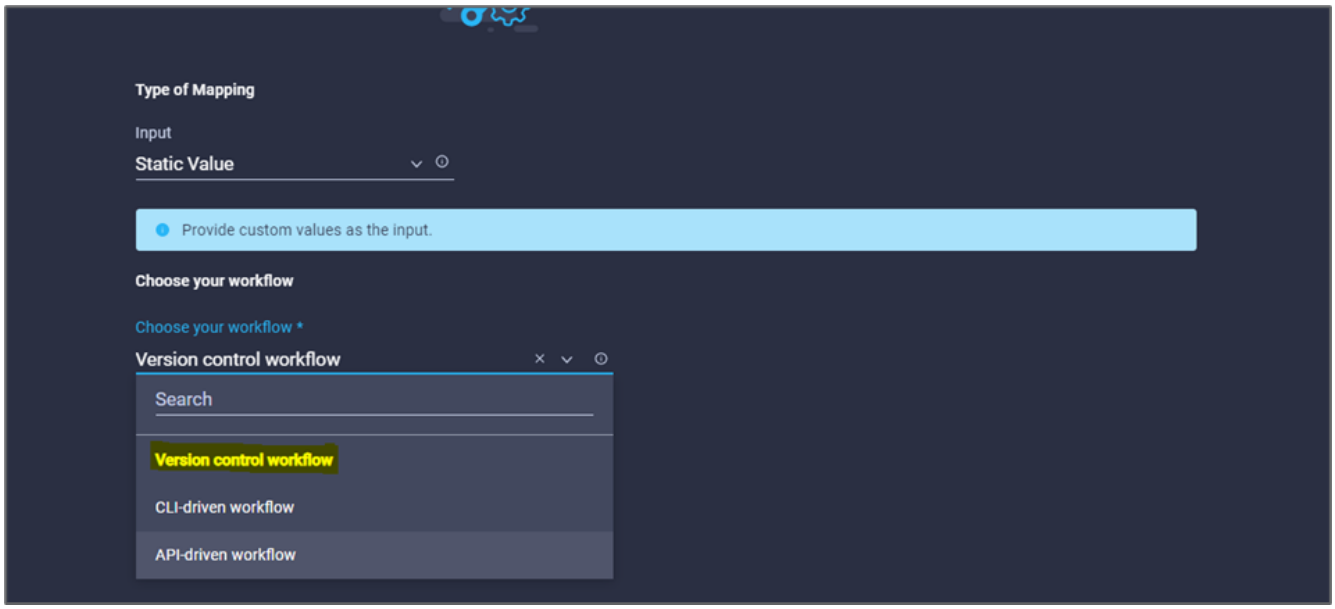
21. Cliquez sur **carte**.
22. Cliquez sur **Map** dans le champ **Execution mode**.
23. Choisissez **valeur statique**, cliquez sur **mode d'exécution**, puis sur **remote**.



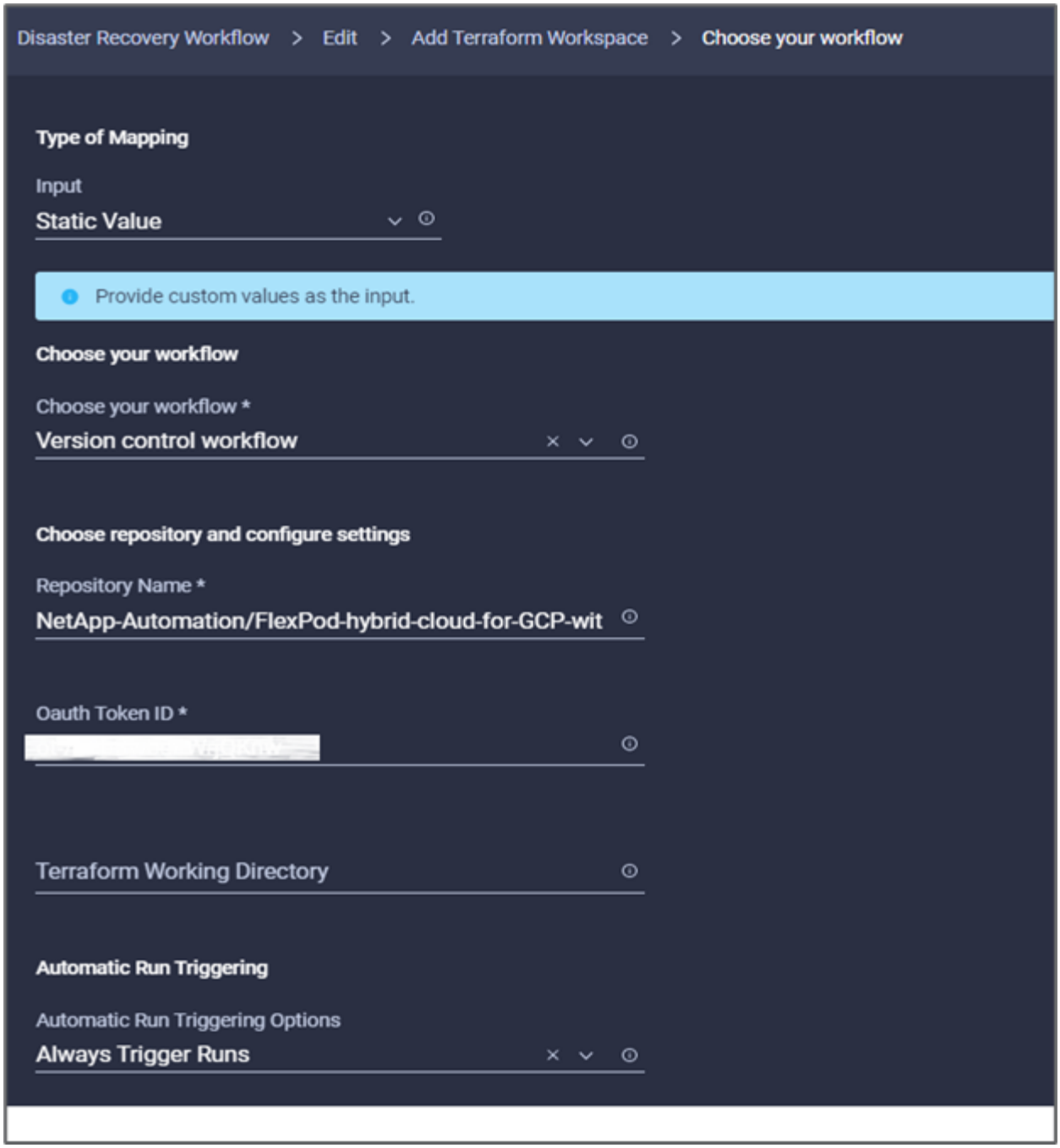
24. Cliquez sur **carte**.
25. Cliquez sur **carte** dans le champ **appliquer méthode**.
26. Choisissez **valeur statique** et cliquez sur **appliquer méthode**. Cliquez sur **application manuelle**.

27. Cliquez sur **carte**.
28. Cliquez sur **Map** dans le champ **User interface**.
29. Choisissez **valeur statique** et cliquez sur **interface utilisateur**. Cliquez sur **interface utilisateur de la console**.

30. Cliquez sur **carte**.
31. Cliquez sur **Map** dans le champ de saisie et sélectionnez votre flux de travail.
32. Sélectionnez **valeur statique**, puis cliquez sur **Choisissez votre flux de travail**. Cliquez sur **version Control Workflow**.



33. Fournissez les informations suivantes sur le référentiel GitHub :
    a. Dans **Nom du référentiel**, entrez le nom du référentiel détaillé dans la section "« Configurer les conditions préalables à l'environnement »".
    b. Indiquez l'ID de token OAuth comme détaillé dans la section "« Configurer les conditions préalables à l'environnement »".
    c. Sélectionnez l'option **déclenchement automatique**.



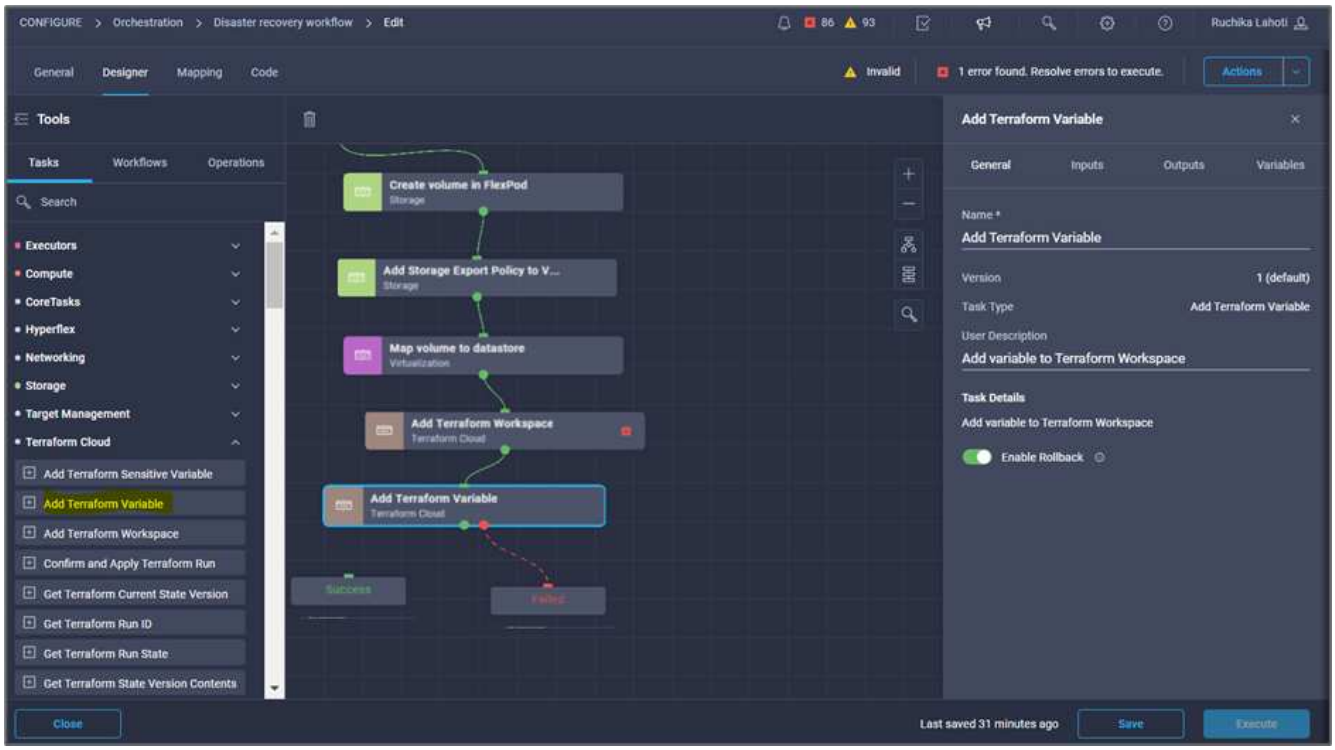
34. Cliquez sur **carte**.
35. Cliquez sur **Enregistrer**.

Cela termine la création d'un espace de travail dans un compte Terraform Cloud for Business.

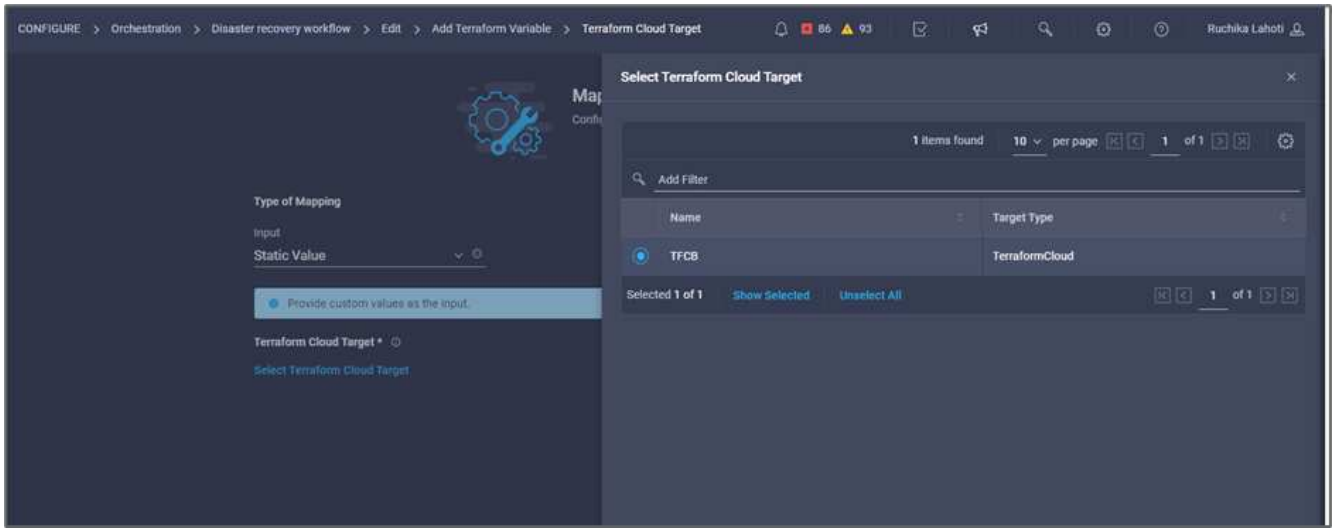
Procédure 6 : ajoutez des variables non sensibles à l'espace de travail

1. Accédez à l'onglet **Designer** et cliquez sur la section **workflows à partir d'Outils**.
2. Faites glisser et déposez le flux de travail **Terraform > Ajouter des variables Terraform** à partir de la section **Tools** de la zone **Design**.
3. Utilisez Connector pour connecter les tâches **Add Terraform Workspace** et **Add Terraform variables**. Cliquez sur **Enregistrer**.

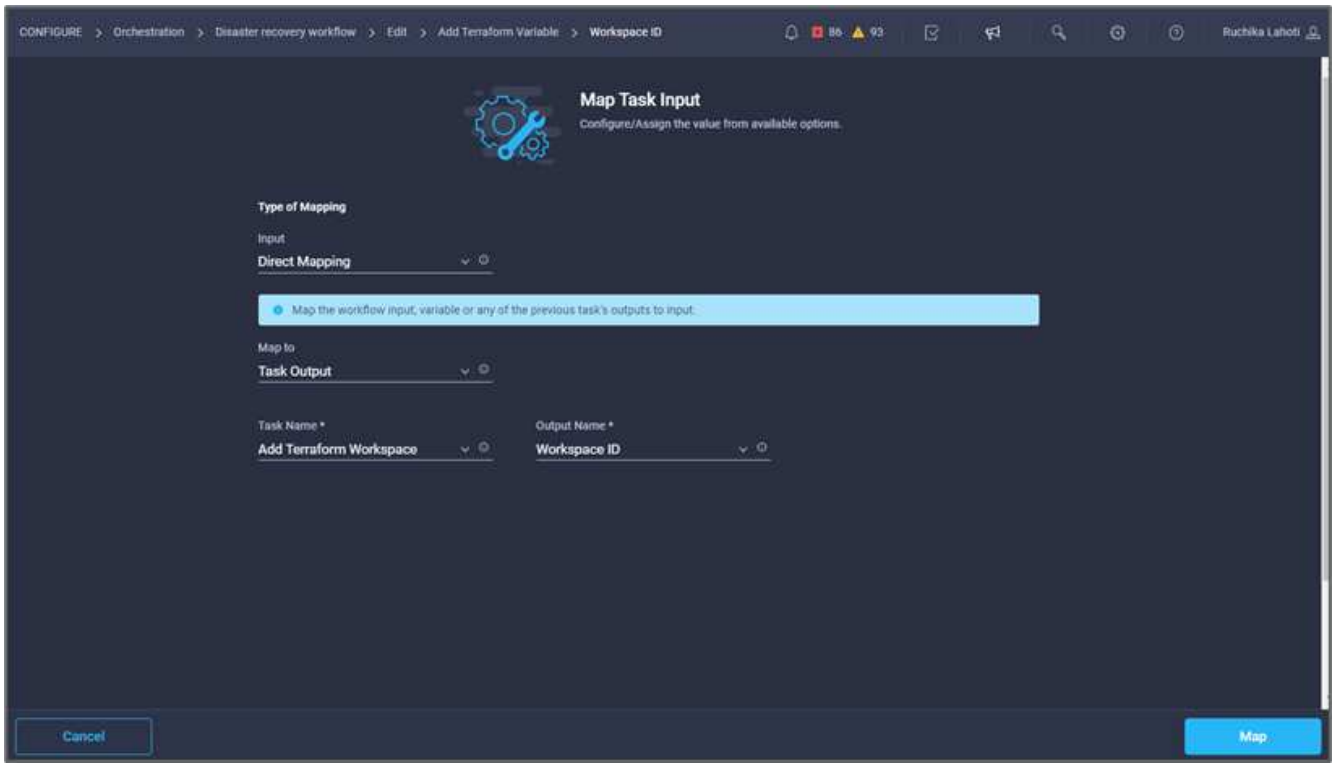
4. Cliquez sur **Ajouter variables Terraform**. Dans la zone **Propriétés du flux de travail**, cliquez sur l'onglet **général**. Vous pouvez également modifier le nom et la description de cette tâche.



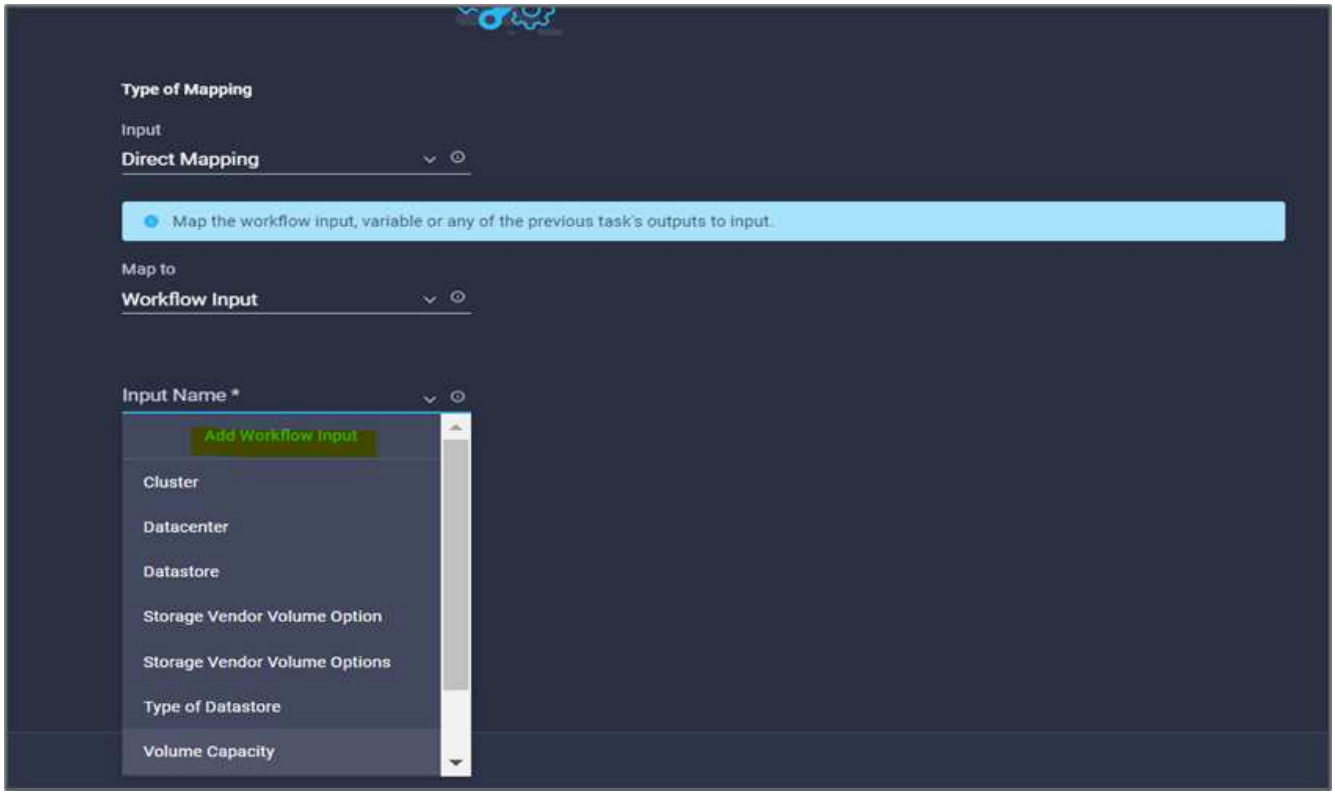
5. Dans la zone **Propriétés du workflow**, cliquez sur **entrées**.
6. Cliquez sur **carte** dans le champ **Terraform Cloud Target**.
7. Choisissez **valeur statique** et cliquez sur **Sélectionner la cible de nuage Terraform**. Sélectionnez le compte Terraform Cloud for Business ajouté comme expliqué dans "Configurez Cisco Intersight Service pour HashiCorp Terraform". ».



8. Cliquez sur **carte**.
9. Cliquez sur **carte** dans le champ *Nom de l'organisation Terraform *.
10. Choisissez **valeur statique** et cliquez sur **Sélectionner l'organisation Terraform**. Sélectionnez le nom de l'organisation Terraform dont vous faites partie dans votre compte Terraform Cloud for Business.

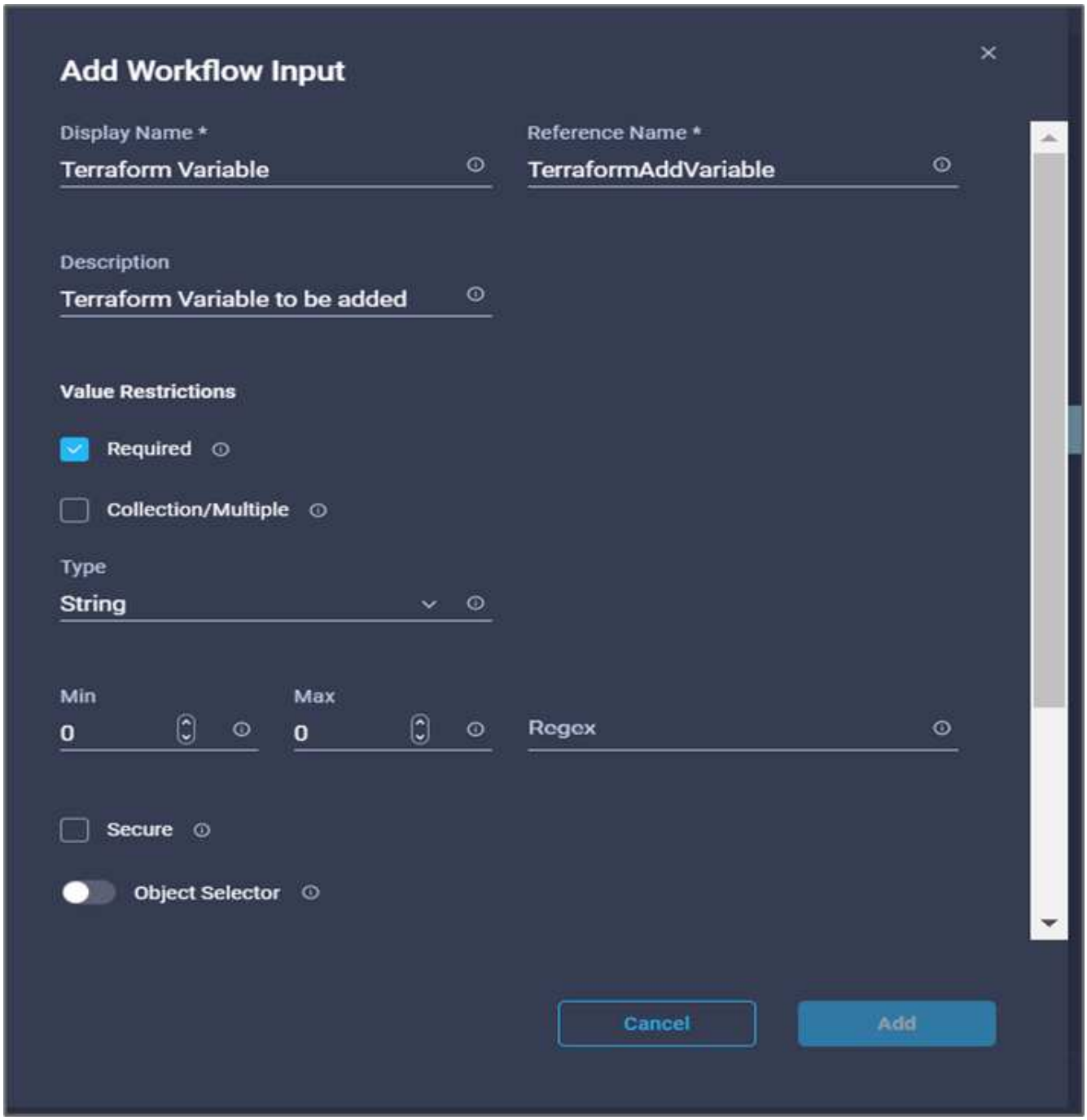


11. Cliquez sur **carte**.
12. Cliquez sur **carte** dans le champ **Nom de l'espace de travail Terraform**.
13. Choisissez **mappage direct** et cliquez sur **sortie tâche**.
14. Cliquez sur **Nom de la tâche** et cliquez sur **Ajouter un espace de travail Terraform**.



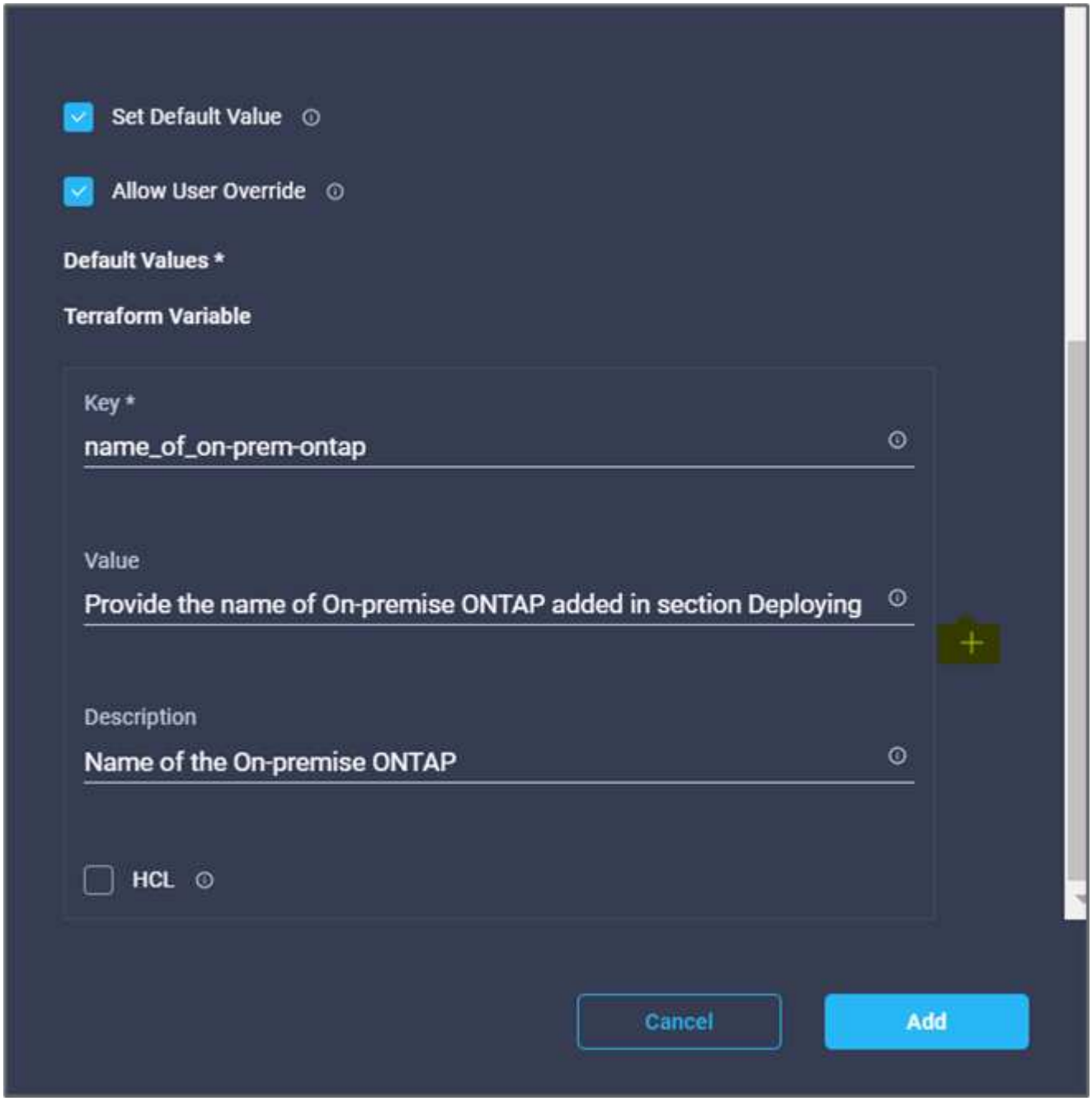
15. Cliquez sur **Nom de sortie** et cliquez sur **Nom d'espace de travail**.

16. Cliquez sur **carte**.
17. Cliquez sur **Map** dans le champ **Add variables Options**.
18. Choisissez **mappage direct** et cliquez sur **entrée de flux de travail**.
19. Cliquez sur **Nom d'entrée** et **Créer une entrée de flux de travail**.



20. Dans l'assistant Ajouter une entrée, procédez comme suit :
    a. Indiquez un nom d'affichage et un nom de référence (facultatif).
    b. Assurez-vous de sélectionner **String** pour **Type**.
    c. Cliquez sur **définir la valeur par défaut et remplacer**.
    d. Cliquez sur **Type de variable**, puis sur **variables non sensibles**.

21. Dans la section **Ajouter des variables Terraform**, fournissez les informations suivantes :
    - **Clé.** `name_of_on-prem-ontap`
    - **Valeur.** indiquer le nom de ONTAP sur site.
    - **Description.** Nom du ONTAP sur place.
22. Cliquez sur **+** pour ajouter d'autres variables.

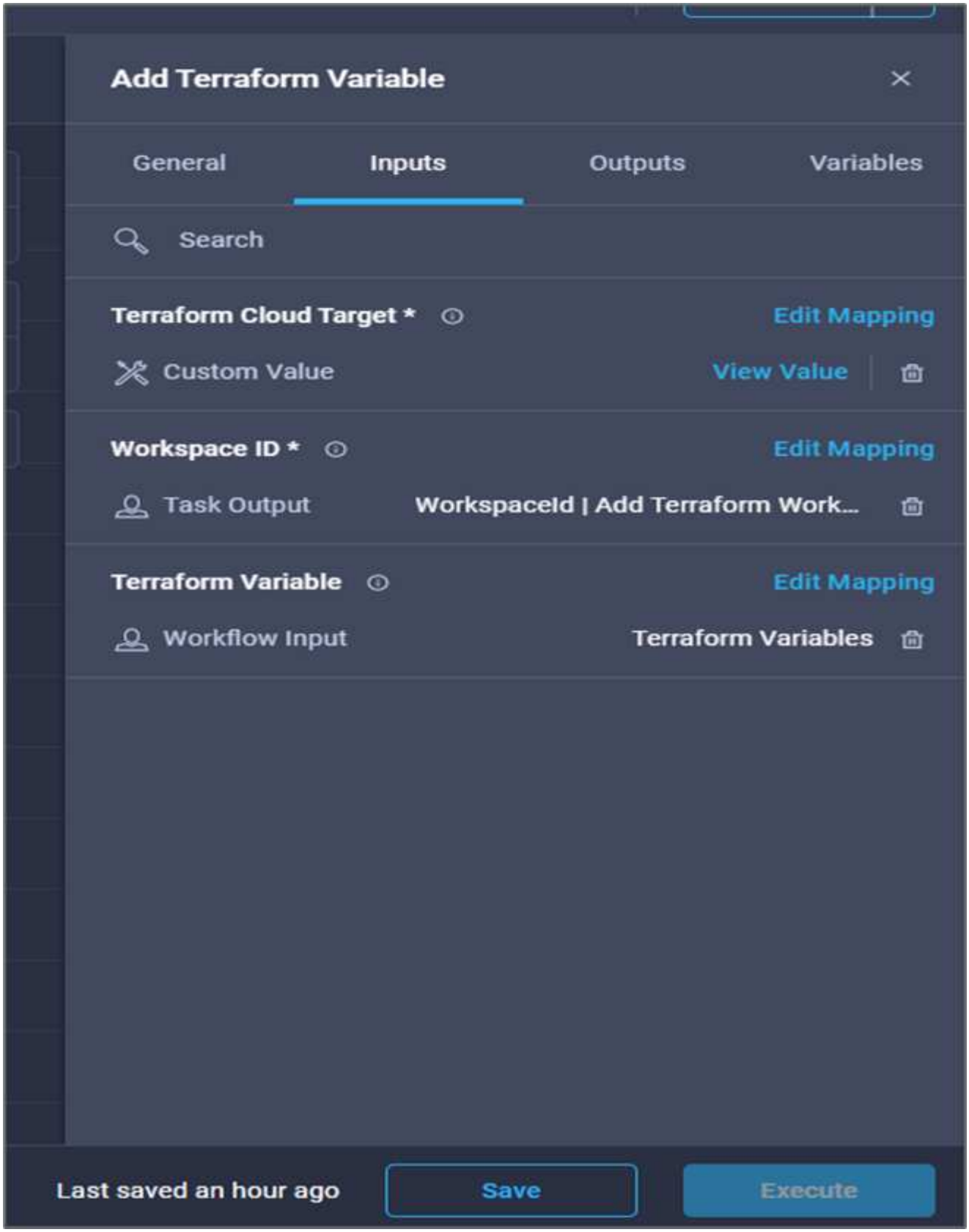


23. Ajoutez toutes les variables Terraform comme indiqué dans le tableau suivant. Vous pouvez également fournir une valeur par défaut.

Nom de la variable Terraform	Description
nom_of_on-ontap sur site	Nom du ONTAP sur site (FlexPod)

Nom de la variable Terraform	Description
ip_cluster_ontap_sur site	L'adresse IP de l'interface de gestion du cluster de stockage
nom_utilisateur_ontap_sur site	Nom d'utilisateur admin pour le cluster de stockage
Zone	Région GCP dans laquelle l'environnement de travail sera créé
id_sous-réseau	ID de sous-réseau GCP dans lequel l'environnement de travail sera créé
id_vpc	ID VPC dans lequel l'environnement de travail sera créé
capacity_package_name	Type de licence à utiliser
volume_source	Nom du volume source
nom_vm_stockage_source	Nom du SVM source
volume_destination	Nom du volume sur Cloud Volumes ONTAP
schedule_of_replication	La valeur par défaut est 1 heure
nom_du_volume_to_create_on_cvo	Nom du volume cloud
id_espace_de_travail	Espace de travail_ID où l'environnement de travail sera créé
ID_projet	ID_projet où l'environnement de travail sera créé
nom_du_cluster_cvo	Nom de l'environnement de travail Cloud Volumes ONTAP
compte_service_gcp	gcp_service_compte de l'environnement de travail Cloud Volumes ONTAP

24. Cliquez sur **carte**, puis sur **Enregistrer**.



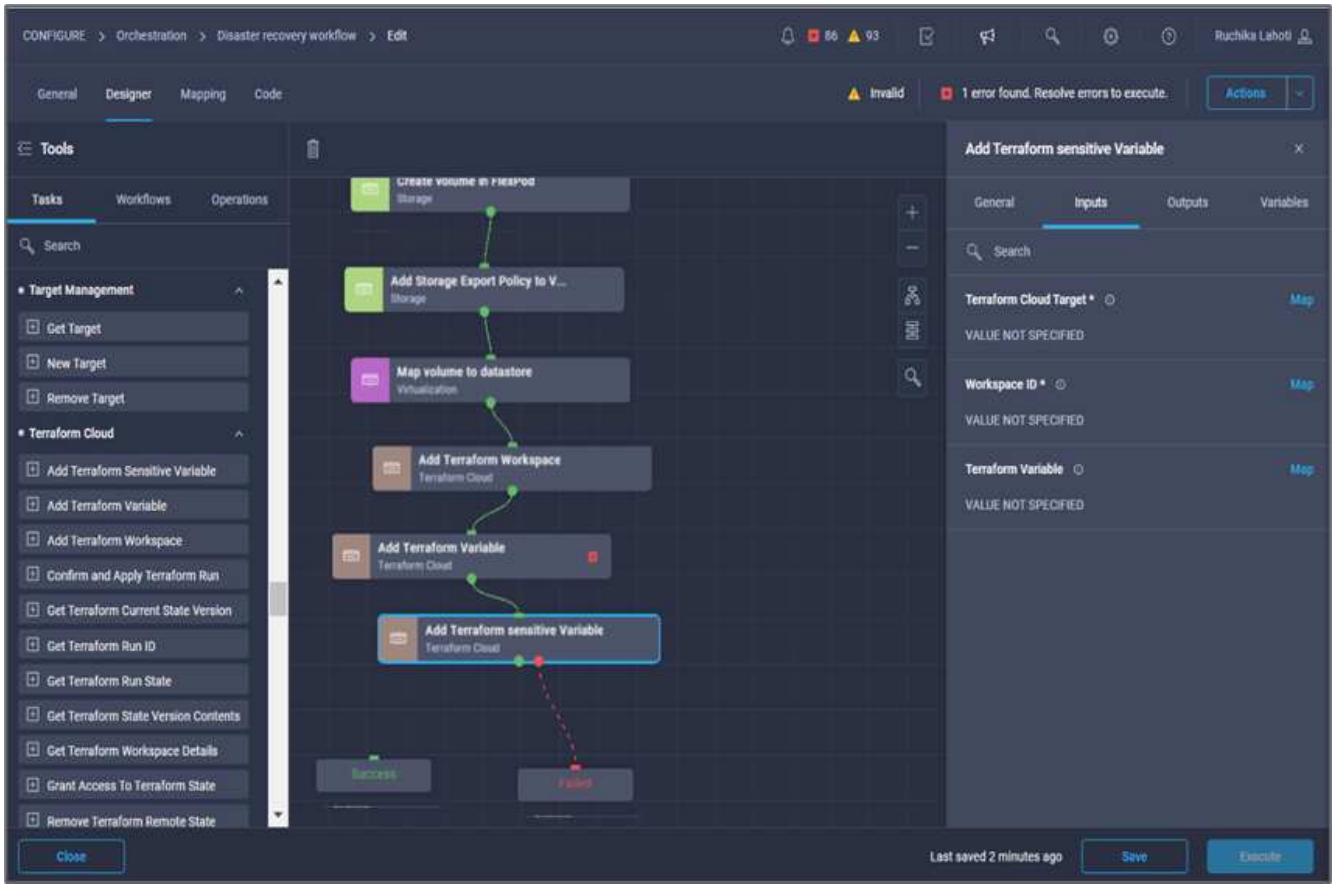
La tâche d’ajout des variables Terraform requises à l’espace de travail est alors terminée. Ajoutez ensuite les variables Terraform sensibles requises à l’espace de travail. Vous pouvez également les combiner en une seule tâche.

Procédure 7 : ajoutez des variables sensibles à un espace de travail

1. Accédez à l'onglet **Designer** et cliquez sur **workflows** dans la section **Outils**.
2. Faites glisser et déposez le flux de travail **Terraform > Ajouter des variables Terraform** à partir de la section **Tools** de la zone **Design**.
3. Utilisez Connector pour connecter les deux tâches **Ajouter un espace de travail Terraform**. Cliquez sur **Enregistrer**.

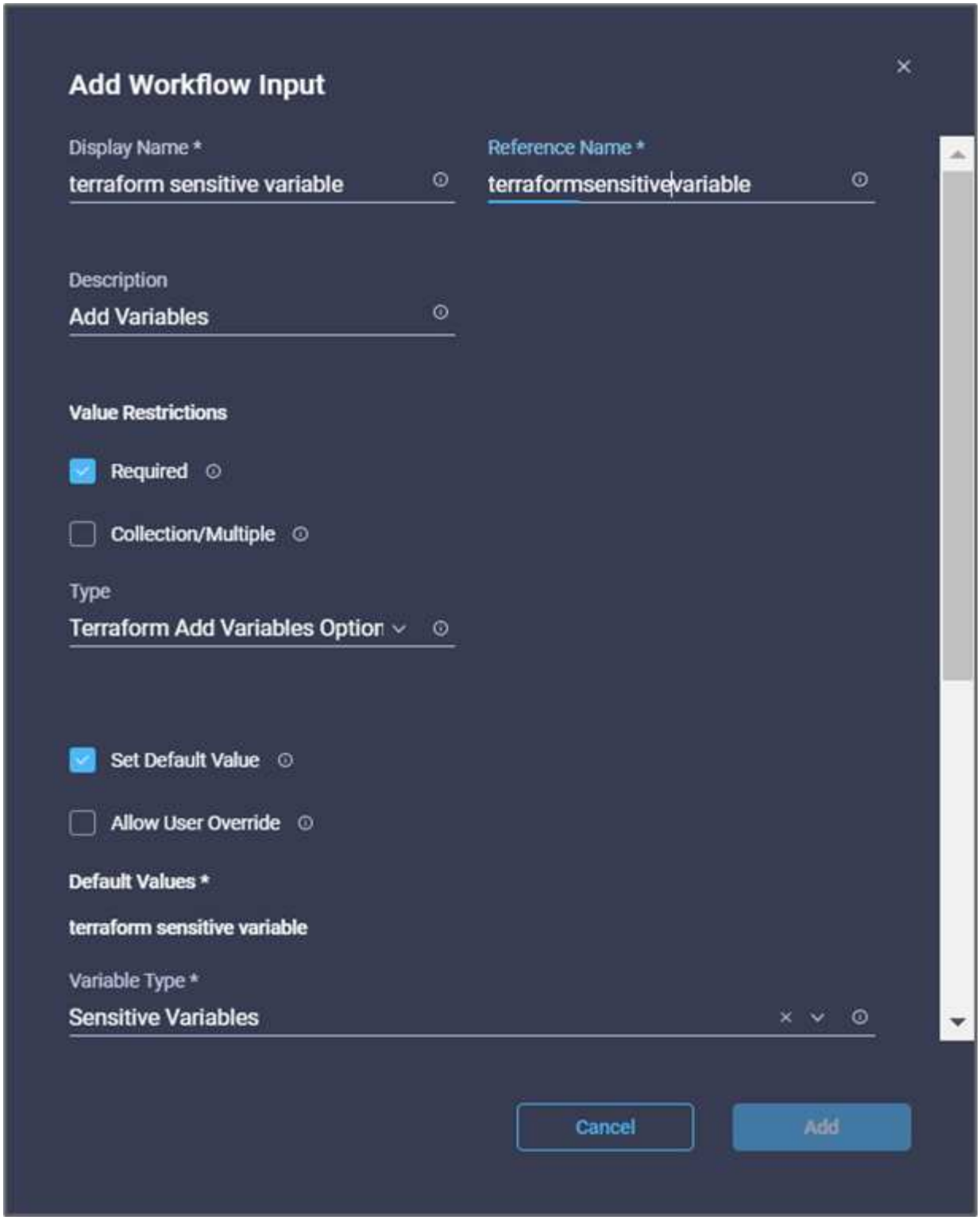
> Un avertissement s'affiche pour indiquer que les deux tâches ont le même nom. Ignorer l'erreur pour l'instant car vous modifiez le nom de la tâche à l'étape suivante.

4. Cliquez sur **Ajouter variables Terraform**. Dans la zone **Propriétés du flux de travail**, cliquez sur l'onglet **général**. Modifiez le nom en **Ajouter des variables sensibles Terraform**.



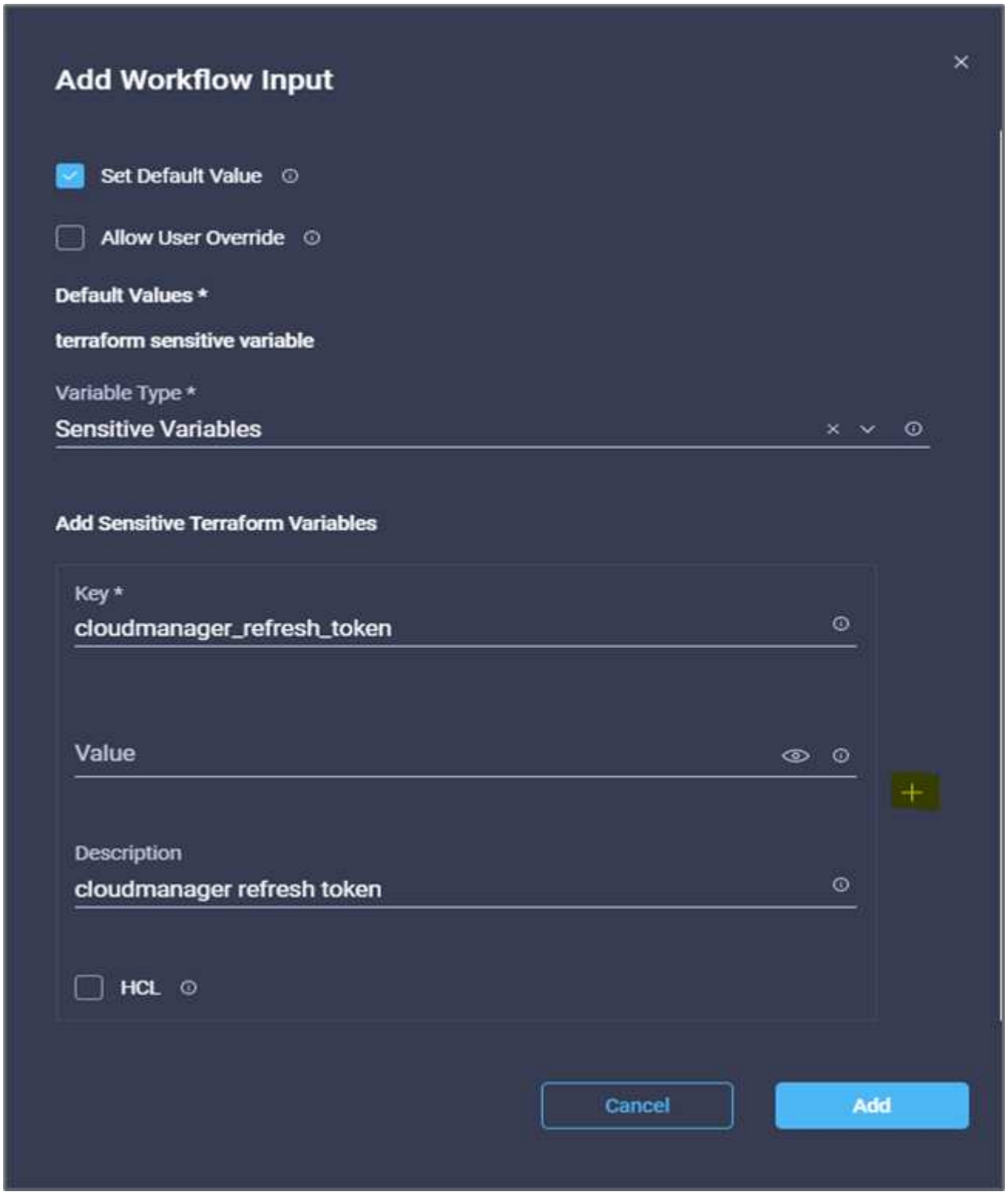
5. Dans la zone **Propriétés du workflow**, cliquez sur **entrées**.
6. Cliquez sur **carte** dans le champ **Terraform Cloud Target**.
7. Choisissez **valeur statique** et cliquez sur **Sélectionner la cible de nuage Terraform**. Sélectionnez le compte Terraform Cloud for Business ajouté dans la section "Configurez Cisco Intersight Service pour HashiCorp Terraform". »
8. Cliquez sur **carte**.
9. Cliquez sur **carte** dans le champ **Nom de l'organisation Terraform**.
10. Choisissez **valeur statique** et cliquez sur **Sélectionner l'organisation Terraform**. Sélectionnez le nom de l'organisation Terraform dont vous faites partie dans votre compte Terraform Cloud for Business.
11. Cliquez sur **carte**.

12. Cliquez sur **carte** dans le champ **Nom de l’espace de travail Terraform**.
13. Choisissez **mappage direct** et cliquez sur **sortie tâche**.
14. Cliquez sur **Nom de la tâche**, puis sur **Ajouter un espace de travail Terraform**.
15. Cliquez sur **Nom de sortie** et cliquez sur sortie **Nom d’espace de travail**.
16. Cliquez sur **carte**.
17. Cliquez sur **Map** dans le champ **Add variables Options**.
18. Choisissez **mappage direct**, puis cliquez sur **entrée de flux de travail**.
19. Cliquez sur **Nom d’entrée** et **Créer une entrée de flux de travail**.
20. Dans l’assistant Ajouter une entrée, procédez comme suit :
    a. Indiquez un nom d’affichage et un nom de référence (facultatif).
    b. Assurez-vous de sélectionner **Terraform Ajouter des variables Options** pour le type.
    c. Cliquez sur **définir la valeur par défaut**.
    d. Cliquez sur **Type de variable**, puis sur **variables sensibles**.
    e. Cliquez sur **Ajouter**.



21. Dans la section **Ajouter des variables Terraform**, fournissez les informations suivantes :
    - **Clé.** `cloudmanager_refresh_token`.
    - **Valeur.** saisissez le jeton d'actualisation pour les opérations de l'API NetApp Cloud Manager.
    - **Description.** Actualiser jeton.

Pour en savoir plus sur l'obtention d'un jeton de mise à jour pour les opérations de l'API NetApp Cloud Manager, consultez la section "« Configurer les conditions préalables à l'environnement »."



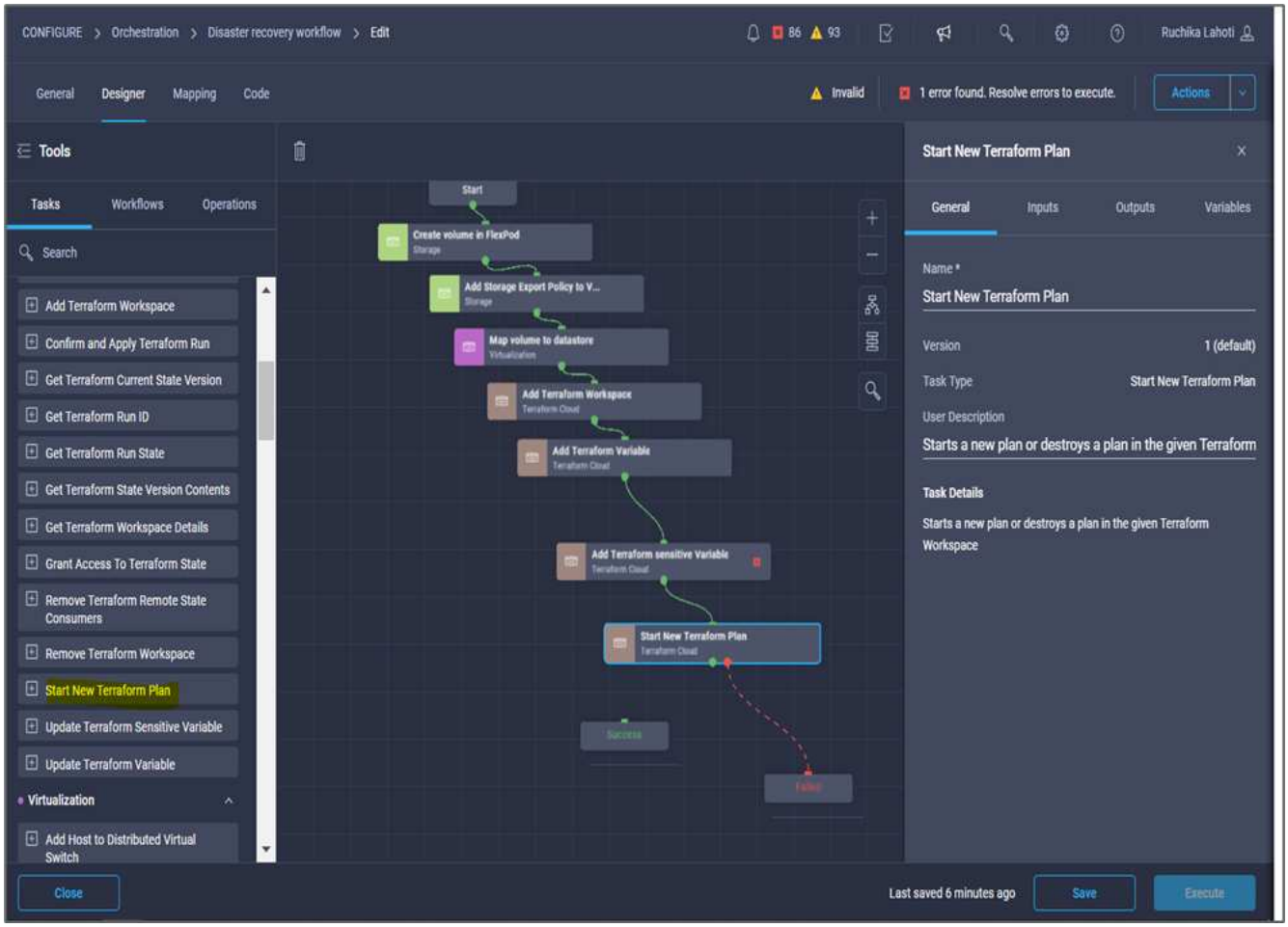
22. Ajoutez toutes les variables sensibles à la Terraform comme indiqué dans le tableau ci-dessous. Vous pouvez également fournir une valeur par défaut.

Nom de variable sensible Terraform	Description
cloudmanager_refresh_token	Actualiser le jeton. Vous pouvez l'obtenir auprès de :
id_connecteur	L'ID client du connecteur Cloud Manager. Obtenez-le à partir de
cvo_admin_password	Mot de passe d'administration pour Cloud Volumes ONTAP
mot_de_passe_utilisateur_ontap_sur site	Mot de passe d'administration pour le cluster de stockage

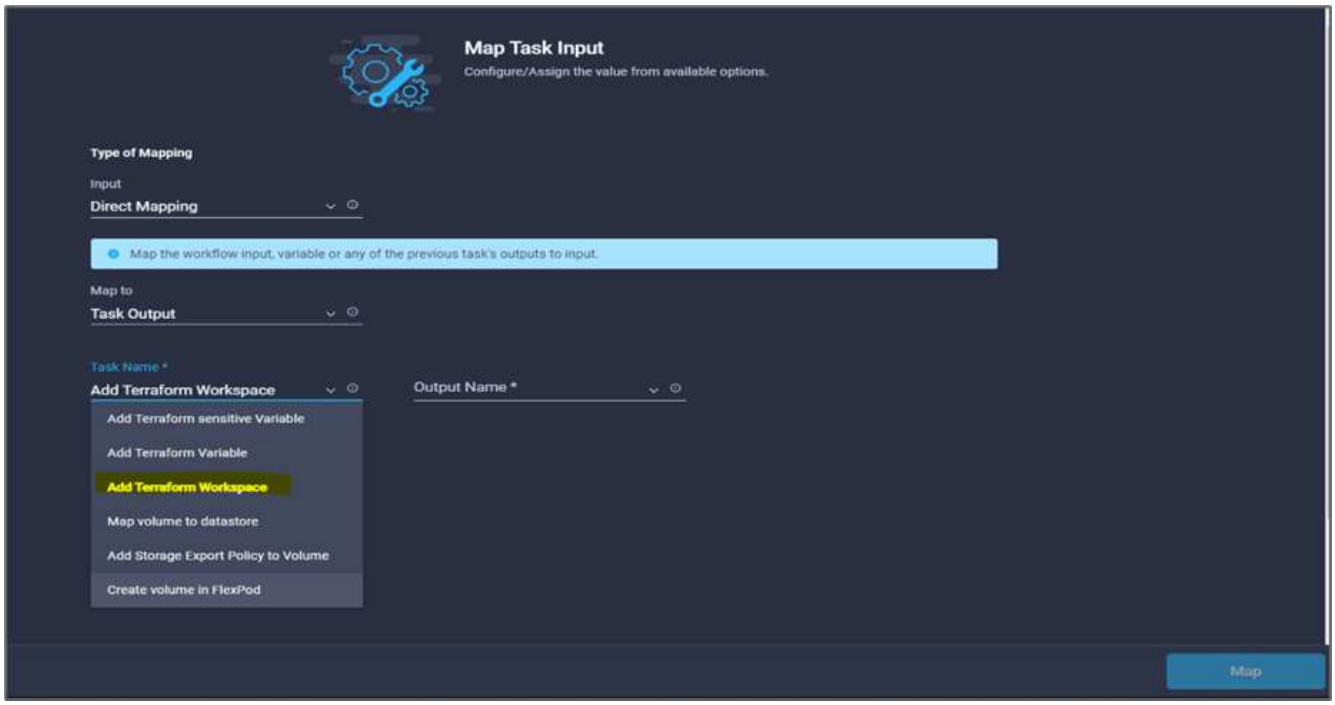
23. Cliquez sur **Map**.cette opération permet d'ajouter les variables sensibles Terraform requises à l'espace de travail. Ensuite, démarrez un nouveau plan Terraform dans l'espace de travail configuré.

Procédure 8 : démarrez un nouveau plan Terraform

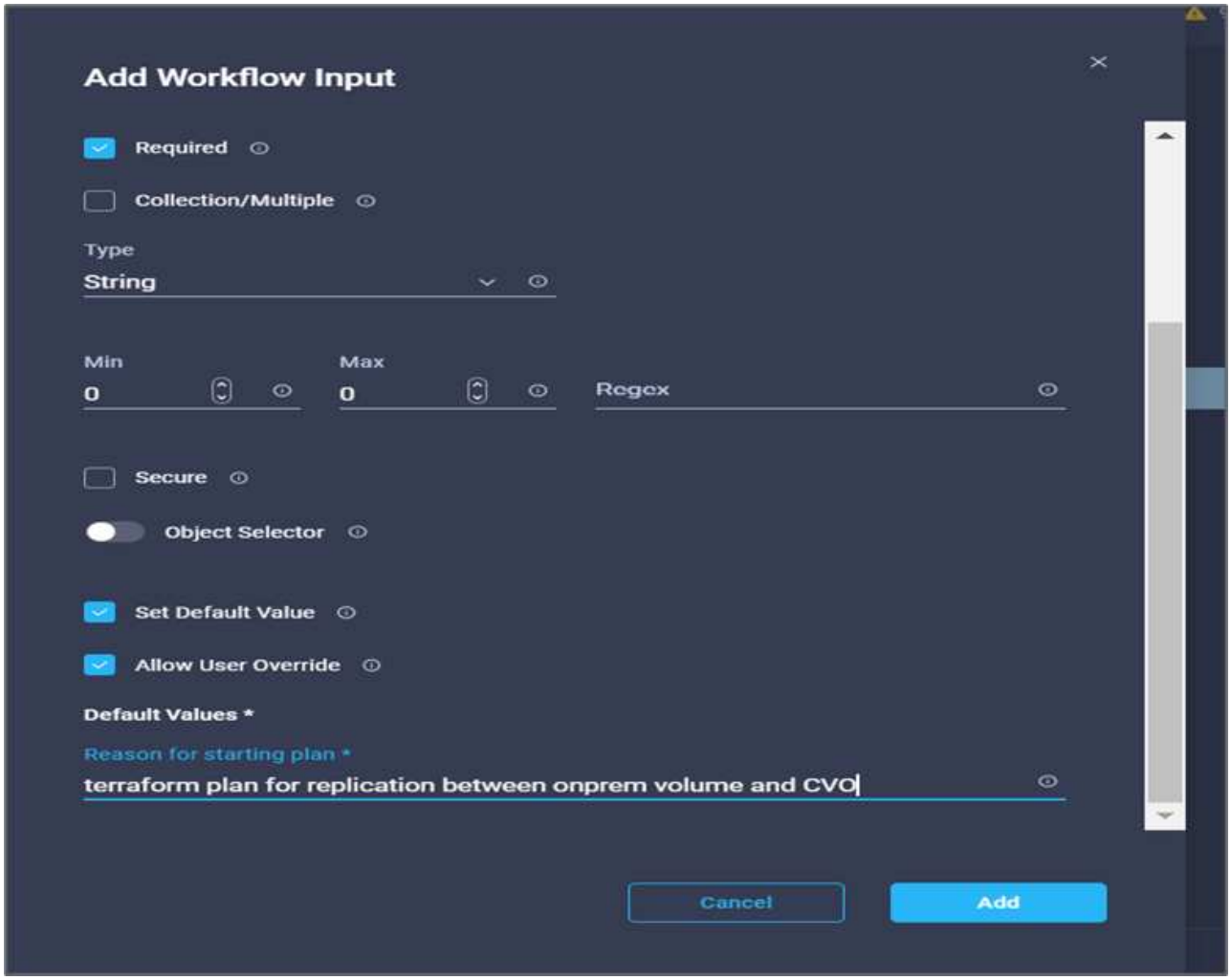
1. Accédez à l'onglet **Designer** et cliquez sur **tâches** dans la section **Outils**.
2. Faites glisser et déposez la tâche **Terraform Cloud > Start New Terraform Plan** de la section **Tools** de la zone **Design**.
3. Utilisez Connector pour vous connecter entre les tâches **Ajouter des variables sensibles Terraform** et **Démarrer de nouvelles tâches Terraform Plan**. Cliquez sur **Enregistrer**.
4. Cliquez sur **Démarrer Nouveau plan Terraform**. Dans la zone **Propriétés de tâche**, cliquez sur l'onglet **général**. Vous pouvez également modifier le nom et la description de cette tâche.



5. Dans la zone **Propriétés de tâche**, cliquez sur **entrées**.
6. Cliquez sur **carte** dans le champ **Terraform Cloud Target**.
7. Choisissez **valeur statique** et cliquez sur **Sélectionner la cible de nuage Terraform**. Sélectionnez le compte Terraform Cloud for Business ajouté dans la section « Configuration de Cisco Intersight Service for HashiCorp Terraform ».
8. Cliquez sur **carte**.
9. Cliquez sur **Map** dans le champ **Workspace ID**.
10. Choisissez **mappage direct** et cliquez sur **sortie tâche**.
11. Cliquez sur **Nom de la tâche**, puis sur **Ajouter un espace de travail Terraform**.



12. Cliquez sur **Nom de sortie**, **ID d'espace de travail**, puis sur **carte**.
13. Cliquez sur **carte** dans le champ **motif de démarrage du plan**.
14. Choisissez **mappage direct**, puis cliquez sur **entrée de flux de travail**.
15. Cliquez sur **Nom d'entrée**, puis sur **Créer entrée de flux de travail**.
16. Dans l'assistant Ajouter une entrée, procédez comme suit :
    a. Indiquez un nom d'affichage et un nom de référence (facultatif).
    b. Assurez-vous de sélectionner **String** pour **Type**.
    c. Cliquez sur **définir la valeur par défaut et remplacer**.
    d. Entrez une valeur par défaut pour **Reason for Starting plan** et cliquez sur **Add**.



17. Cliquez sur **carte**.
18. Cliquez sur **Map** dans le champ **Plan Operation**.
19. Choisissez **valeur statique** et cliquez sur **opération de plan**. Cliquez sur **New plan**.

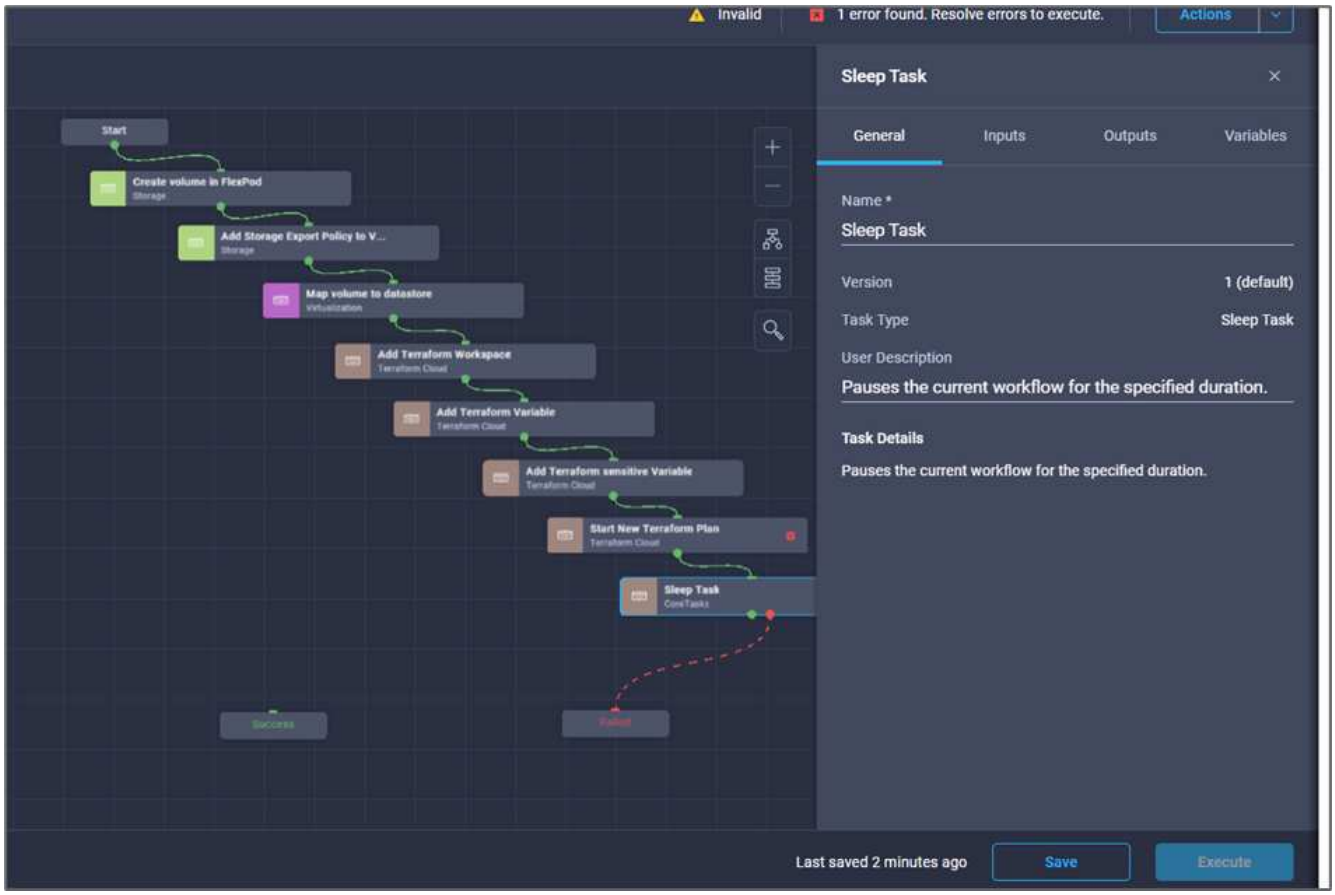
20. Cliquez sur **carte**.
21. Cliquez sur **Enregistrer**.

Cela complète la tâche d'ajout d'un plan Terraform dans le compte Terraform Cloud for Business. Ensuite, créez une tâche de veille pendant quelques secondes.

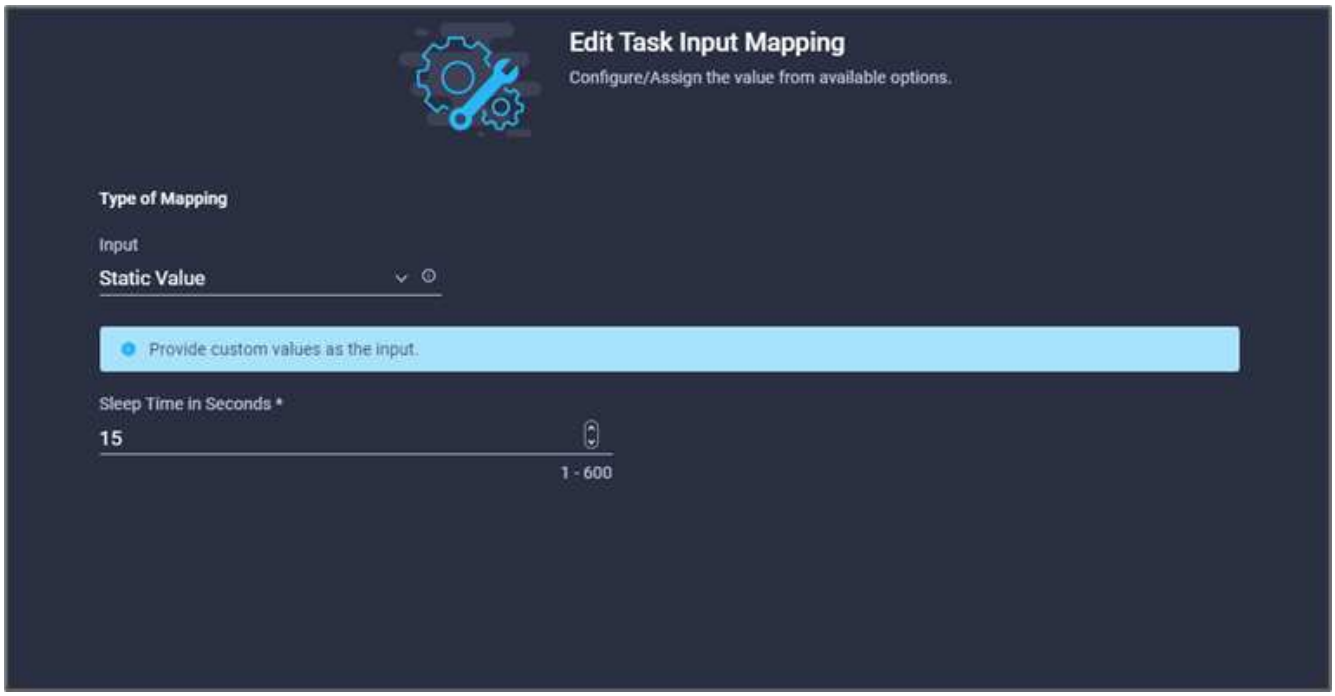
Procédure 9 : tâche de veille pour la synchronisation

Terraform Apply nécessite un runId, qui est généré dans le cadre de la tâche Plan Terraform. L'attente de quelques secondes entre le Plan Terraform et les actions d'application Terraform évite les problèmes de synchronisation.

1. Accédez à l'onglet **Designer** et cliquez sur **tâches** dans la section **Outils**.
2. Faites glisser et déposez la tâche **Core Tasks > Sleep Task** dans la section **Tools** de la zone **Design**.
3. Utilisez Connector pour connecter les tâches **Démarrer Nouveau plan Terraform** et **tâche veille**. Cliquez sur **Enregistrer**.



4. Cliquez sur **tâche veille**. Dans la zone **Propriétés de tâche**, cliquez sur l'onglet **général**. Vous pouvez également modifier le nom et la description de cette tâche. Dans cet exemple, le nom de la tâche est **Synchroniser**.
5. Dans la zone **Propriétés de tâche**, cliquez sur **entrées**.
6. Cliquez sur **carte** dans le champ **temps de veille en secondes**.
7. Choisissez **valeur statique** et saisissez **15** dans pour le **temps de veille en secondes**.

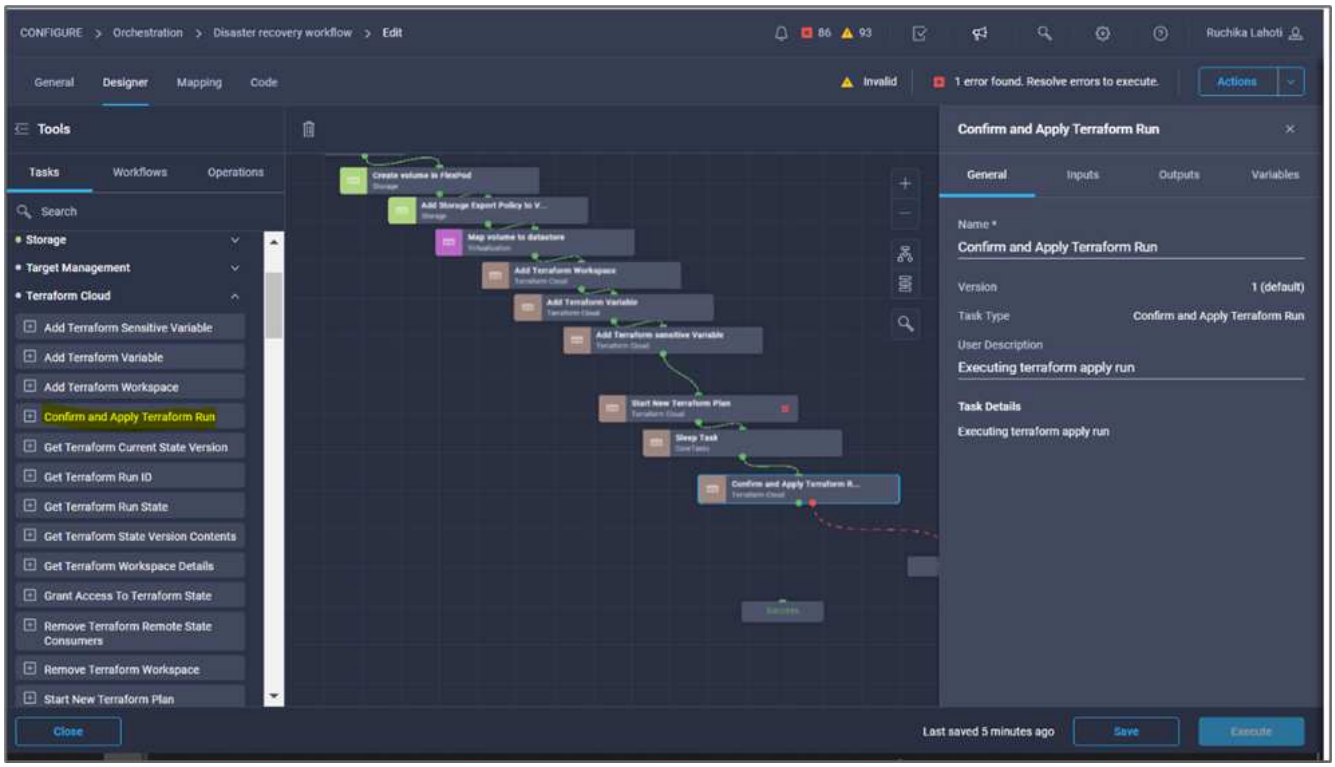


8. Cliquez sur **carte**.
9. Cliquez sur **Enregistrer**.

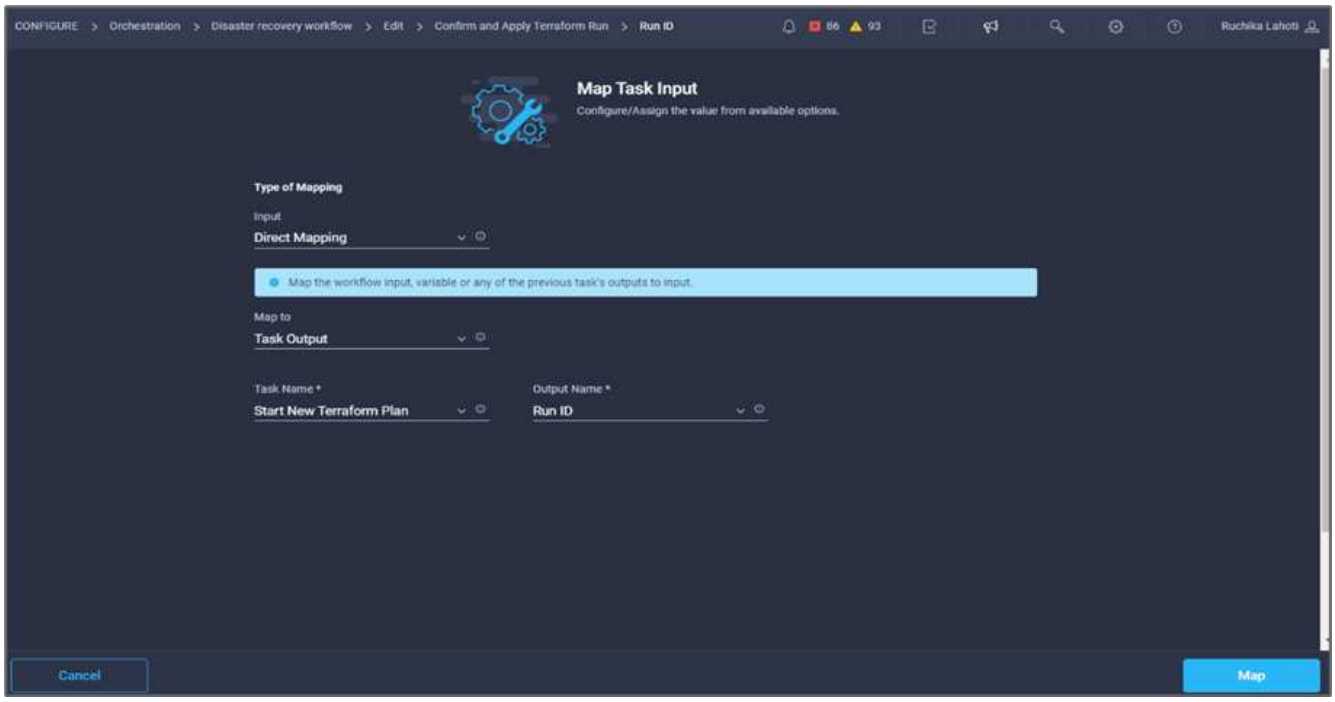
La tâche de veille est terminée. Ensuite, créez la dernière tâche de ce flux de travail, en confirmant et en appliquant l'exécution Terraform.

Procédure 10 : confirmer et appliquer Terraform Run

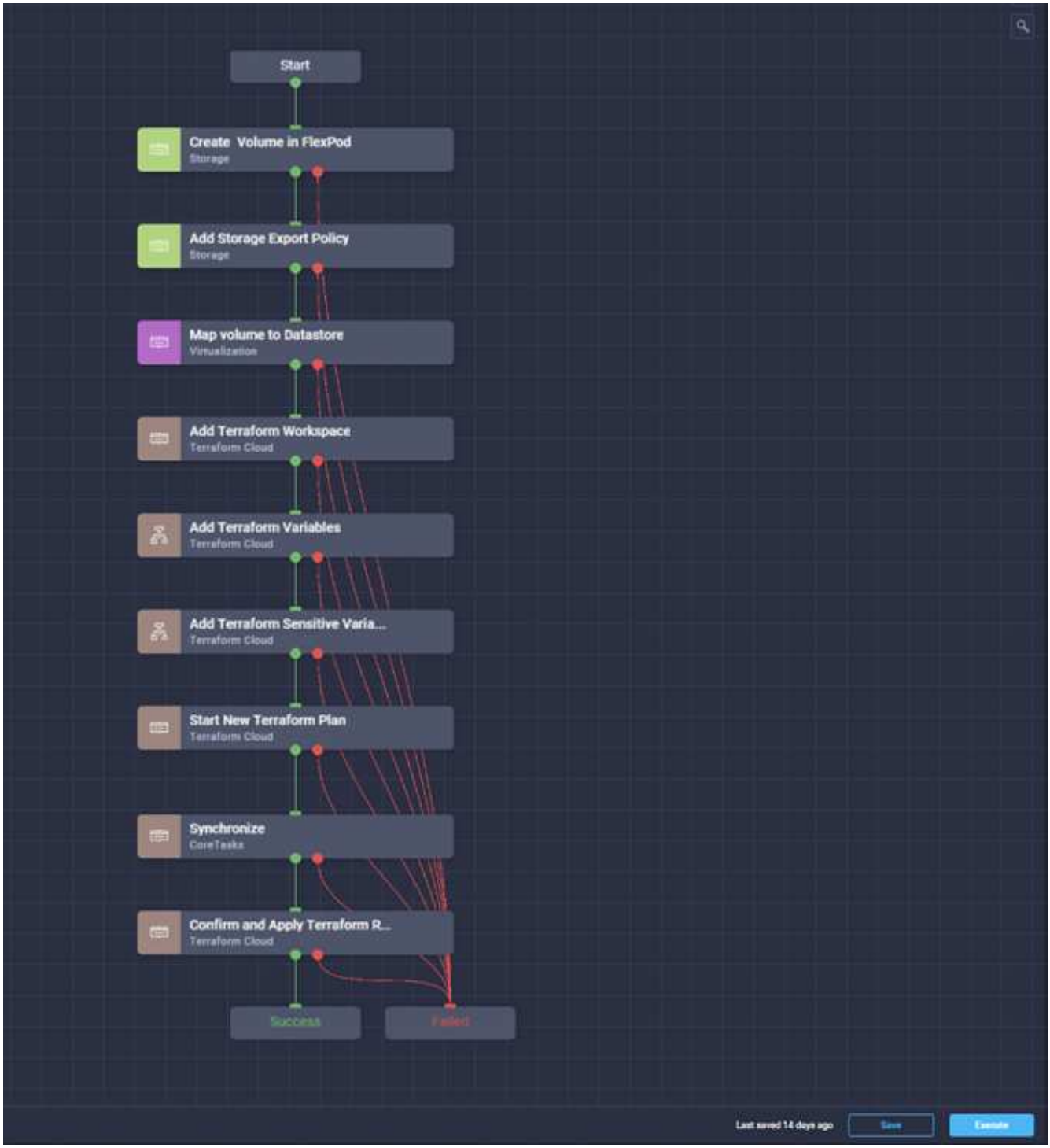
1. Accédez à l'onglet **Designer** et cliquez sur **tâches** dans la section **Outils**.
2. Faites glisser et déposez la tâche **Terraform Cloud > confirmer et appliquer Terraform Run** à partir de la section **Tools** de la zone **Design**.
3. Utilisez Connector pour connecter les tâches **Synchroniser** et **confirmer et appliquer Terraform Run**. Cliquez sur **Enregistrer**.
4. Cliquez sur **confirmer** et **appliquer Terraform Run**. Dans la zone **Propriétés de tâche**, cliquez sur l'onglet **général**. Vous pouvez également modifier le nom et la description de cette tâche.



5. Dans la zone **Propriétés de tâche**, cliquez sur **entrées**.
6. Cliquez sur **carte** dans le champ **Terraform Cloud Target**.
7. Choisissez **valeur statique** et cliquez sur **Sélectionner la cible de nuage Terraform**. Sélectionnez le compte Terraform Cloud for Business ajouté dans "Configurez Cisco Intersight Service pour HashiCorp Terraform". »
8. Cliquez sur **carte**.
9. Cliquez sur **Map** dans le champ **Run ID**.
10. Choisissez **mappage direct** et cliquez sur **sortie tâche**.
11. Cliquez sur **Nom de la tâche** et cliquez sur **Démarrer Nouveau plan Terraform**.
12. Cliquez sur **Nom de sortie**, puis sur **ID d'exécution**.



13. Cliquez sur **carte**.
14. Cliquez sur **Enregistrer**.
15. Cliquez sur **alignement automatique du flux de travail** pour que toutes les tâches soient alignées. Cliquez sur **Enregistrer**.



La tâche confirmer et appliquer Terraform Run est terminée. Utilisez Connector pour vous connecter entre la tâche **confirmer et appliquer Terraform Run** et les tâches **Success** et **failed**.

Procédure 11 : importation d'un flux de travail conçu par Cisco

Cisco Intersight Cloud Orchestrator vous permet d'exporter des workflows d'un compte Cisco Intersight vers votre système, puis de les importer dans un autre compte. Un fichier JSON a été créé en exportant le flux de travail créé qui peut être importé vers votre compte.

Un fichier JSON pour le composant de flux de travail est disponible dans "Référentiel GitHub".

"Next : exécution Terraform à partir du contrôleur."

Exécution Terraform à partir du contrôleur

"Précédent : flux de travail de reprise après incident."

Nous pouvons exécuter le plan Terraform à l'aide d'un contrôleur. Vous pouvez ignorer cette section si vous avez déjà exécuté votre plan Terraform à l'aide d'un flux de travail ICO.

Prérequis

La configuration de la solution commence par une station de travail de gestion qui a accès à Internet et avec une installation de Terraform.

Vous trouverez un guide d'installation de Terraform "ici".

Cloner GitHub

La première étape du processus consiste à cloner le GitHub repo vers un nouveau dossier vide sur la station de travail de gestion. Pour cloner le référentiel GitHub, procédez comme suit :

1. À partir du poste de travail de gestion, créez un nouveau dossier pour le projet. Créez un nouveau dossier dans ce dossier nommé `/root/snapmirror-cvo` Et clonez le référentiel GitHub.
2. Ouvrez une interface de ligne de commande ou de console sur le poste de travail de gestion et modifiez les répertoires dans le nouveau dossier que vous venez de créer.
3. Clonez la collection GitHub à l'aide de la commande suivante :

```
Git clone https://github.com/NetApp-Automation/FlexPod-hybrid-cloud-for-GCP-with-Intersight-and-CVO
```

1. Remplacez les répertoires par le nouveau dossier nommé `snapmirror-cvo`.

Exécution Terraform

- **Init.** initialiser l'environnement Terraform (local). Généralement exécuté une seule fois par session.
- **Plan.** Comparez l'état du terraform avec l'état d'entrée dans le nuage et construisez et affichez un plan d'exécution. Cela ne modifie pas le déploiement (lecture seule).
- **Appliquer.** appliquer le plan à partir de la phase du plan. Cela peut potentiellement changer le déploiement (lecture et écriture).
- **Détruire.** toutes les ressources qui sont régies par cet environnement terraform spécifique.

Pour plus de détails, voir "ici".

"Ensuite, validation de la solution."

Validation des solutions

"Précédent : exécution Terraform à partir du contrôleur."

Dans cette section, nous revisitons la solution avec un exemple de workflow de réplication des données et prenons quelques mesures pour vérifier l'intégrité de la réplication des données depuis l'instance NetApp ONTAP exécutée dans FlexPod vers NetApp Cloud Volumes ONTAP s'exécutant sur Google Cloud.

Nous avons utilisé Cisco Intersight workflow orchestrator dans cette solution et nous continuerons à l'utiliser pour notre cas d'utilisation.

De fait, le nombre limité de flux de travail Cisco Intersight utilisés dans cette solution ne représente pas l'ensemble complet des flux de travail utilisés par Cisco Intersight. Vous pouvez créer des flux de travail personnalisés en fonction de vos exigences spécifiques et les avoir déclenchés à partir de Cisco Intersight.

Pour valider un scénario de reprise sur incident réussi, commencez par déplacer les données d'un volume dans ONTAP qui fait partie de FlexPod vers Cloud Volumes ONTAP à l'aide de SnapMirror. Vous pouvez alors tenter d'accéder aux données à partir de l'instance de calcul cloud Google, suivie d'un contrôle de l'intégrité des données.

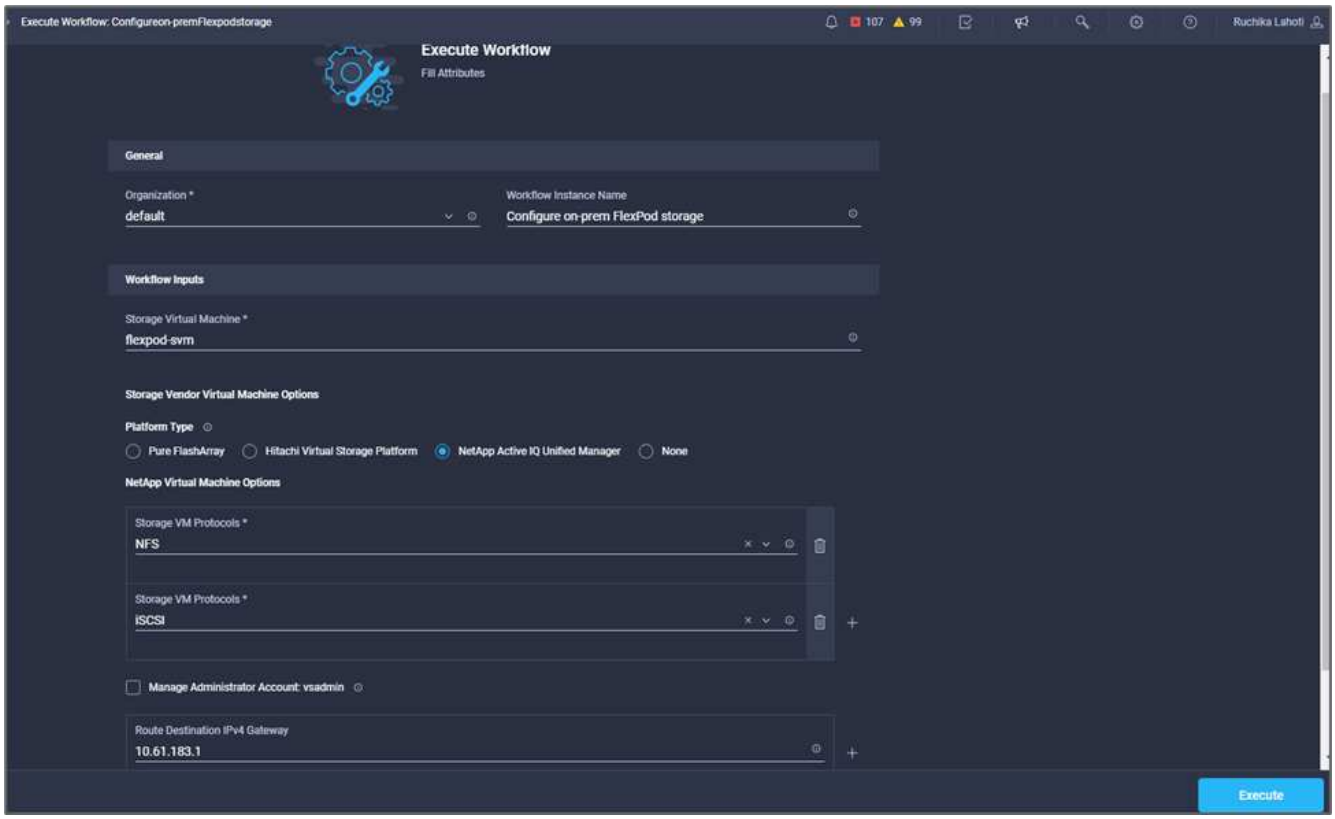
Les étapes générales suivantes permettent de vérifier les critères de réussite de cette solution :

1. Générer un checksum SHA256 sur l'exemple de dataset présent dans un volume ONTAP dans FlexPod.
2. Configurez une relation SnapMirror volume entre ONTAP dans FlexPod et Cloud Volumes ONTAP.
3. Répliquer l'exemple de jeu de données de FlexPod vers Cloud Volumes ONTAP.
4. Interrompre la relation SnapMirror et promouvoir le volume en Cloud Volumes ONTAP vers la production.
5. Mappez le volume Cloud Volumes ONTAP avec le dataset sur une instance de calcul dans Google Cloud.
6. Générer un checksum SHA256 sur l'exemple de dataset dans Cloud Volumes ONTAP.
7. Comparez la somme de contrôle de la source et de la destination, probablement les sommes de contrôle des deux côtés correspondent.

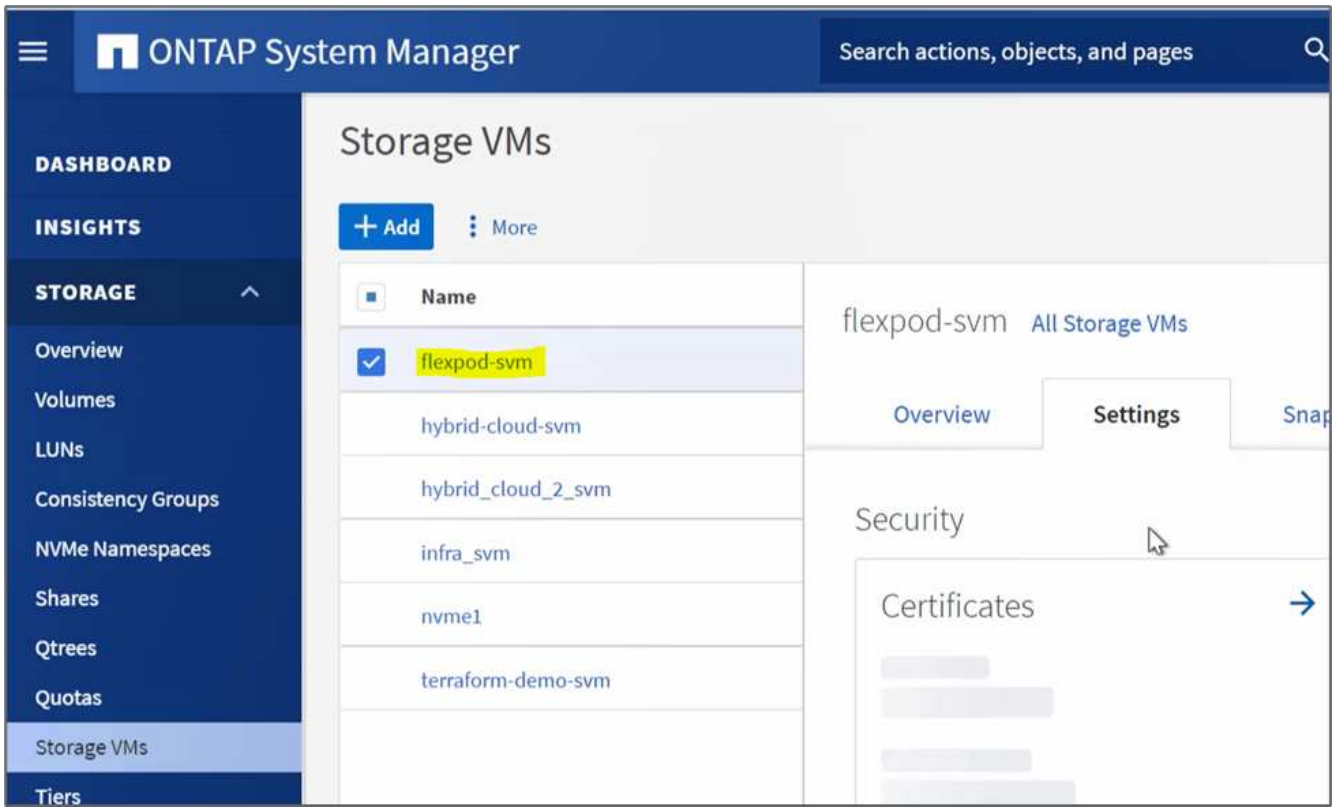
Pour exécuter le workflow sur site, procédez comme suit :

1. Créez un workflow dans InterSight pour les systèmes FlexPod sur site.

2. Fournissez les entrées requises et exécutez le flux de travail.

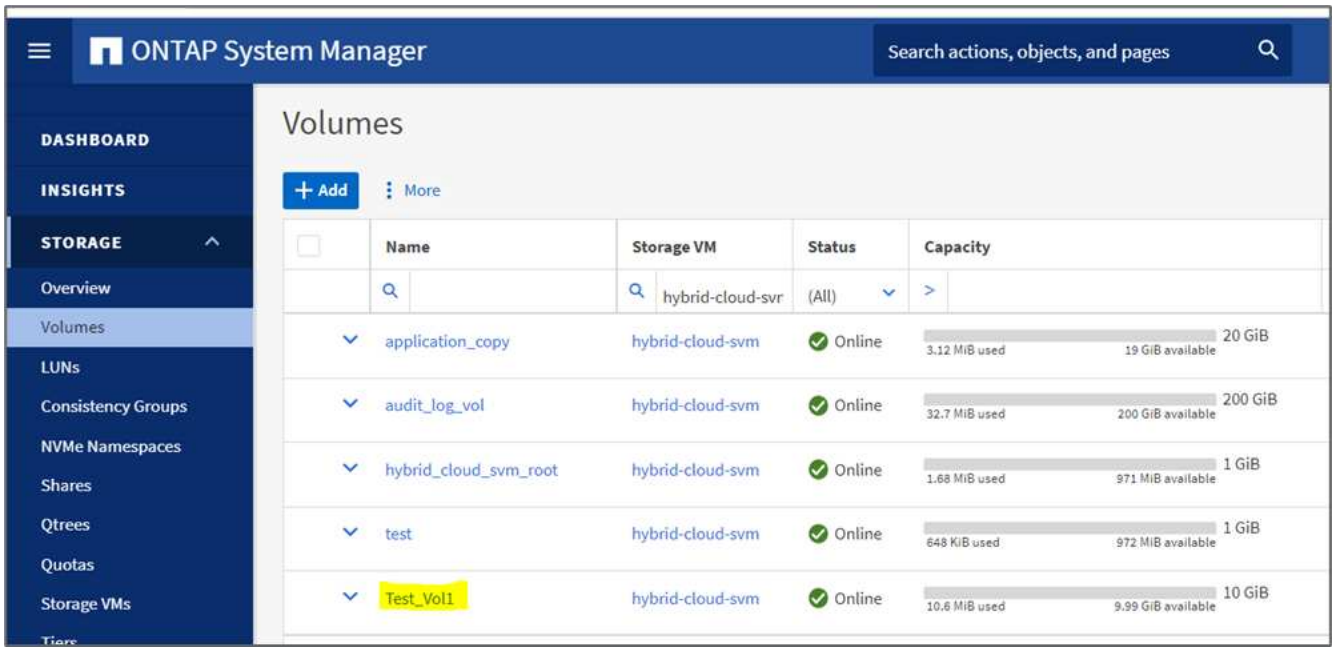


3. Vérifier le nouveau SVM créé dans System Manager



4. Créez et exécutez un autre workflow de reprise d'activité pour créer un volume dans FlexPod sur site et établir une relation SnapMirror entre ce volume dans FlexPod et Cloud Volumes ONTAP.

5. Vérifiez le nouveau volume créé dans ONTAP System Manager.

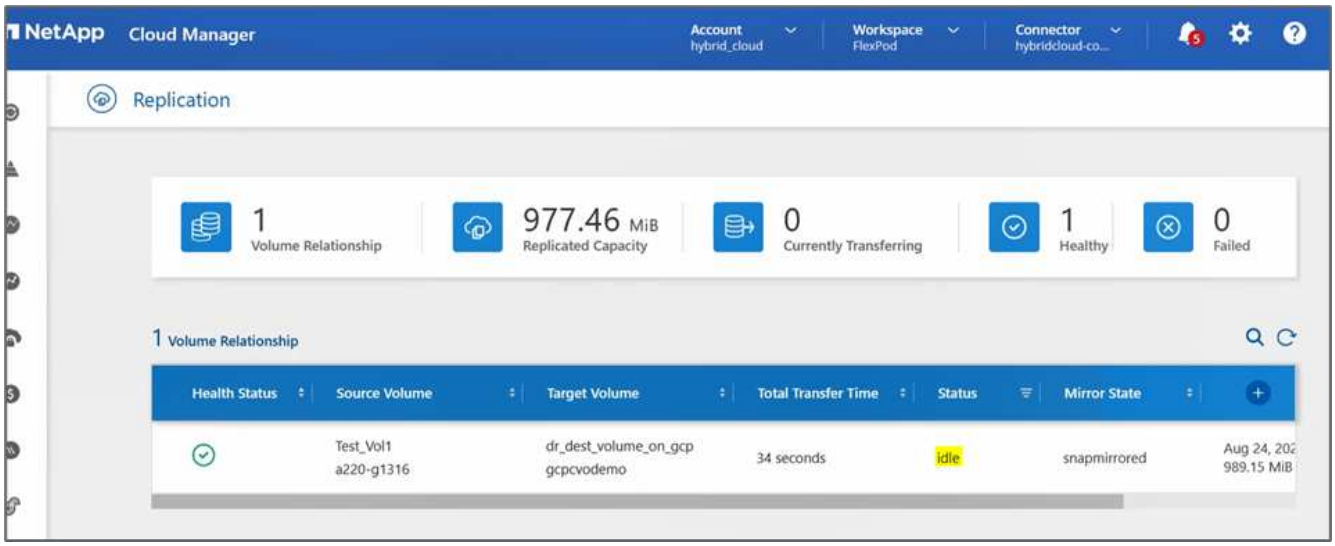


6. Montez le même volume NFS sur une machine virtuelle sur site, puis copiez l'exemple de dataset et exécutez le checksum.

```
root@hybridcloudbackup:/snapmirror_demo# mount -t nfs 172.22.4.157:/Test_Vol1 /snapmirror_demo
root@hybridcloudbackup:/snapmirror_demo# df -kh
Filesystem                  Size  Used Avail Use% Mounted on
udev                        1.9G     0  1.9G   0% /dev
tmpfs                       394M  1.1M  393M   1% /run
/dev/sda2                    16G   11G  4.2G  72% /
tmpfs                       2.0G     0  2.0G   0% /dev/shm
tmpfs                       5.0M     0  5.0M   0% /run/lock
tmpfs                       2.0G     0  2.0G   0% /sys/fs/cgroup
/dev/loop1                   55M   55M     0 100% /snap/core18/1705
/dev/loop2                   69M   69M     0 100% /snap/lxd/14804
/dev/loop0                   28M   28M     0 100% /snap/snapd/7264
172.22.4.157:/Test_Vol1      10G  512K   10G   1% /snapmirror_demo
root@hybridcloudbackup:/snapmirror_demo#
```

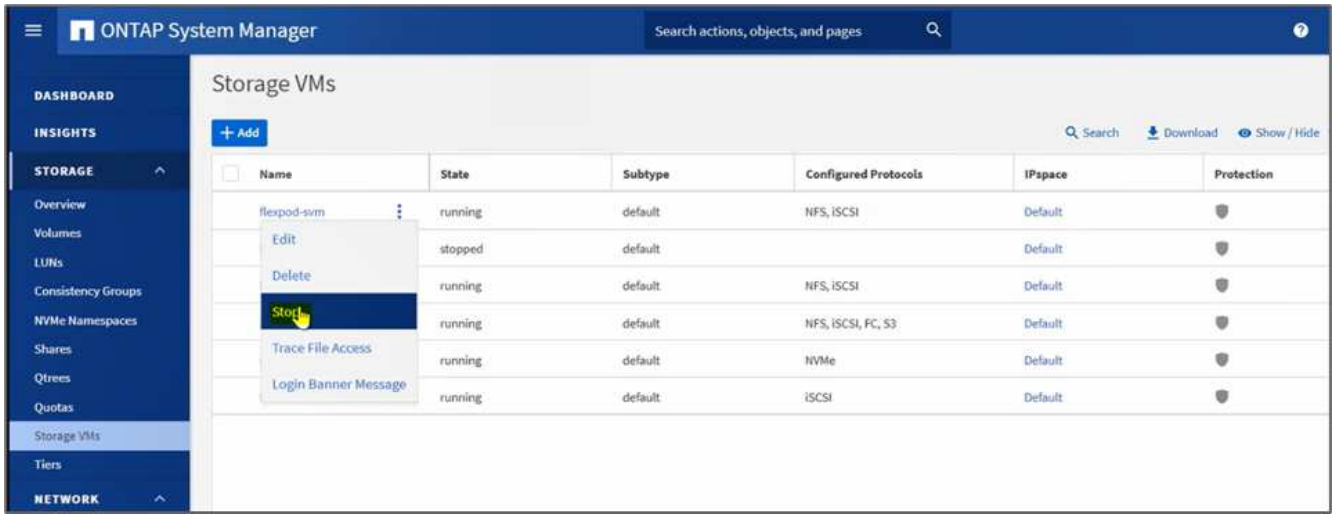
```
root@hybridcloudbackup:/snapmirror_demo#
root@hybridcloudbackup:/snapmirror_demo# sha256sum test.zip
888a23c8495ad33fdf11a931ffc344c3643f15d5cefedbbf1326016e31ec5a59  test.zip
root@hybridcloudbackup:/snapmirror_demo#
root@hybridcloudbackup:/snapmirror_demo#
```

7. Vérifiez l'état de la réplication dans Cloud Manager. Le transfert de données peut prendre quelques minutes en fonction de la taille des données. Une fois cette opération terminée, vous pouvez voir l'état de SnapMirror comme **Idle**.

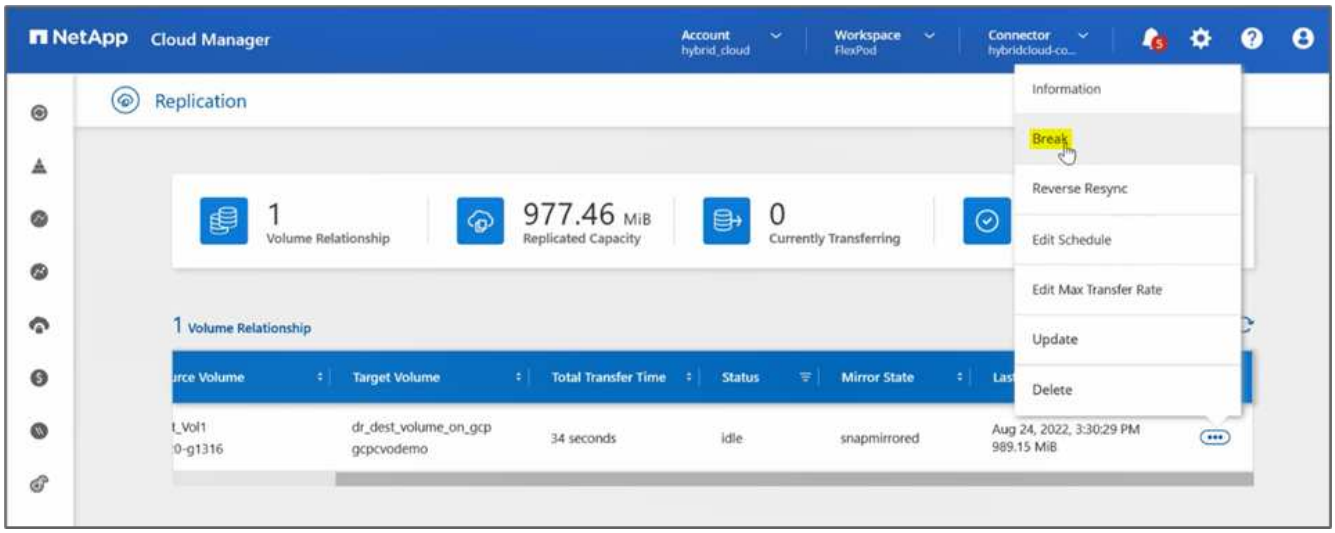


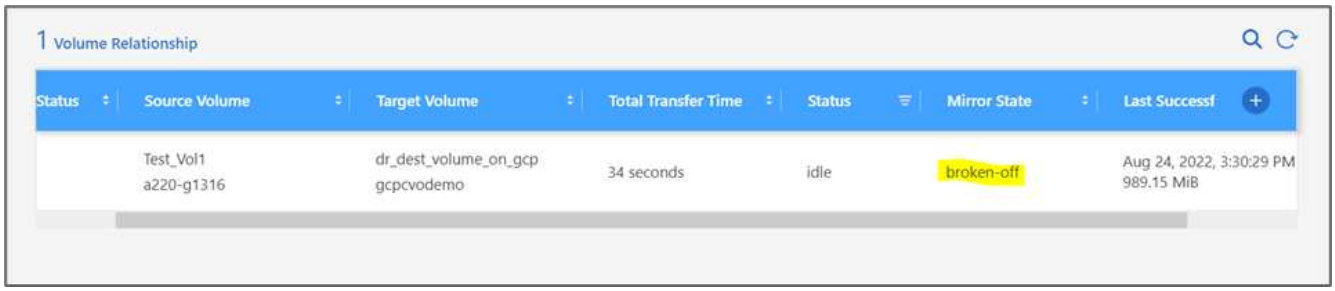
8. Lorsque le transfert de données est terminé, simuler un incident côté source en arrêtant le SVM qui héberge le `Test_vol1` volumétrie.

   Après l'arrêt du SVM, le `Test_vol1` Le volume n'est pas visible dans Cloud Manager.

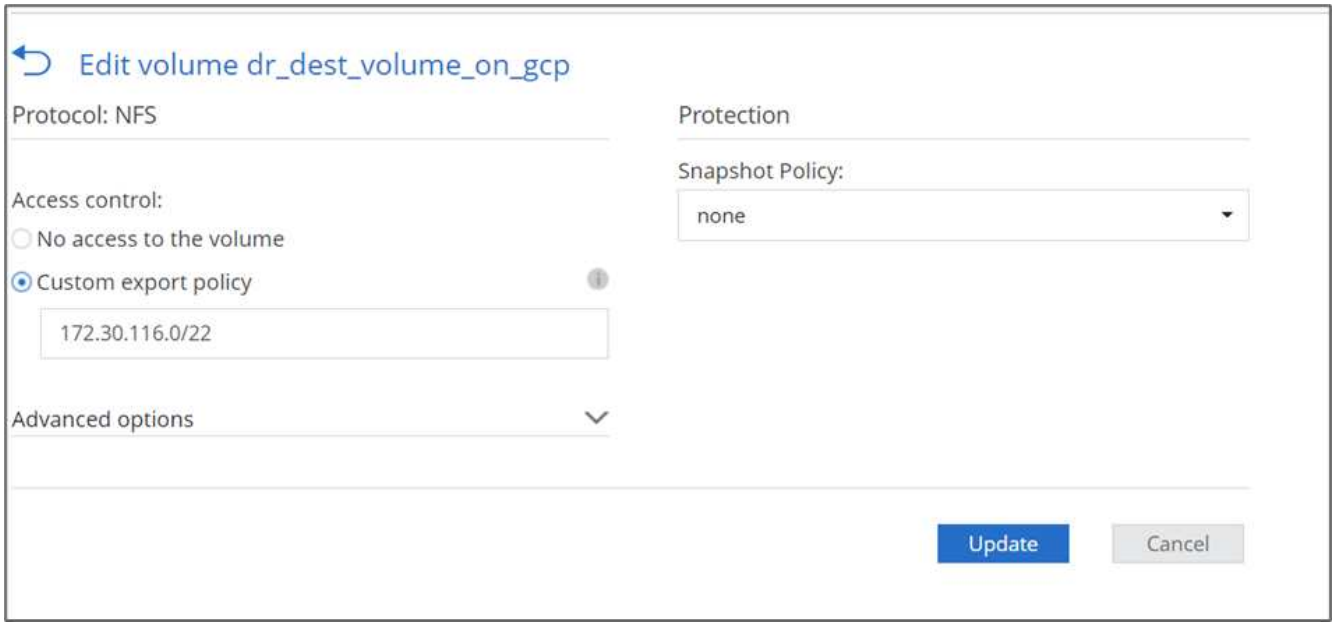


9. Interrompre la relation de réplication et promouvoir le volume de destination Cloud Volumes ONTAP en production.

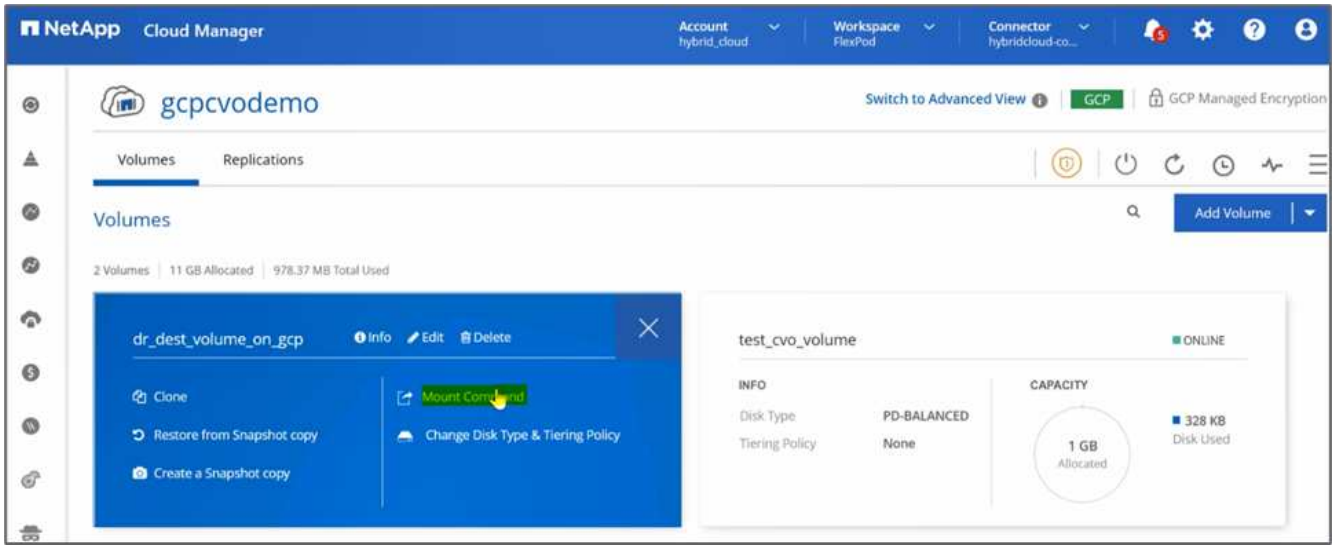




10. Modifiez le volume et activez l’accès client en l’associant à une export policy.



11. Procurez-vous la commande de montage prête à l’emploi pour le volume.



12. Monter le volume sur une instance de calcul, vérifier la présence des données dans le volume de destination et générer le checksum SHA256 du `sample_dataset_2GB` fichier.

```
drwxr-xr-x 21 root   root             4096 Aug 24 10:20 ../
-rwxr-xr-x  1 nobody 4294967294 1015306240 Aug 24 09:59 test.zip*
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$ sha256sum test.zip
888a23c8495ad33fdf11a931ffc344c3643f15d5cefedbbf1326016e31ec5a59  test.zip
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$
```

13. Comparer les valeurs de somme de contrôle à la fois à la source (FlexPod) et à la destination (Cloud Volumes ONTAP).
14. Les checksums correspondent à la source et à la destination.

Vous pouvez confirmer que la réplication des données de la source vers la destination a été correctement effectuée et que l'intégrité des données a été maintenue. Ces données peuvent désormais être consommées en toute sécurité par les applications afin de servir les clients pendant que le site source passe par la restauration.

"Suivant: Conclusion."

Conclusion

"Précédent : validation de la solution."

Dans cette solution, le service de données cloud NetApp, Cloud Volumes ONTAP et l'infrastructure de data Center FlexPod ont été utilisés pour créer une solution de reprise après incident avec un cloud public optimisé par Cisco Intersight Cloud Orchestrator. La solution FlexPod a constamment évolué pour permettre aux clients de moderniser leurs applications et leurs processus de distribution. Avec cette solution, vous pouvez créer un plan de reprise après incident BCDR avec le cloud public, point de passage à un plan de reprise après incident transitoire ou à plein temps, tout en réduisant le coût de la solution de reprise après incident.

La réplication des données entre FlexPod sur site et NetApp Cloud Volumes ONTAP a été gérée par la technologie SnapMirror éprouvée, mais vous pouvez également sélectionner d'autres outils NetApp de transfert et de synchronisation comme Cloud Sync pour vos besoins en termes de mobilité des données. Sécurité des données à la volée assurée par des technologies de chiffrement intégrées basées sur TLS/AES.

Que vous ayez un plan de reprise sur incident temporaire pour une application ou un plan de reprise sur incident à temps plein pour une entreprise, le portefeuille de produits utilisés dans cette solution peut répondre aux deux besoins à grande échelle. Optimisé par Cisco Intersight Workflow Orchestrator, il en va de même pour l'automatisation avec des flux de travail prédéfinis qui éliminent non seulement les processus de reconstruction, mais accélèrent également la mise en œuvre d'un plan de CDR.

Cette solution permet de gérer FlexPod sur site et la réplication des données dans un cloud hybride de manière très simple et pratique, grâce à l'automatisation et à l'orchestration fournies par Cisco Intersight Cloud Orchestrator.

Où trouver des informations complémentaires

Pour en savoir plus sur les informations données dans ce livre blanc, consultez ces documents et/ou sites web :

GitHub

- Toutes les configurations Terraform utilisées

  "https://github.com/NetApp-Automation/FlexPod-hybrid-cloud-for-GCP-with-Intersight-and-CVO"

- Fichiers JSON pour l'importation des flux de production

  "https://github.com/ucs-compute-solutions/FlexPod_DR_Workflows"

Cisco Intersight

- Centre d'aide Cisco Intersight

  "https://intersight.com/help/saas/home"

- Documentation Cisco Intersight Cloud Orchestrator :

  "https://intersight.com/help/saas/features/orchestration/configure#intersight_cloud_orchestrator"

- Cisco Intersight Service pour la documentation Terraform de HashiCorp

  "https://intersight.com/help/saas/features/terraform_cloud/admin"

- Fiche technique Cisco Intersight

  "https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/intersight-ds.html"

- Fiche technique Cisco Intersight Cloud Orchestrator

  "https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/nb-06-intersight-cloud-orch-aag-cte-en.html"

- Fiche technique Cisco Intersight Service for HashiCorp Terraform

  "https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/nb-06-intersight-terraf-ser-aag-cte-en.html"

FlexPod

- Page d'accueil de FlexPod

  "https://www.flexpod.com"

- Guides de conception et de déploiement validés par Cisco pour FlexPod

  "FlexPod Datacenter avec Cisco UCS 4.2(1) en mode géré UCS, VMware vSphere 7.0 U2 et NetApp ONTAP 9.9 : Guide de conception"

- FlexPod Datacenter avec Cisco UCS X-Series

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_esxi7u2_design.html"

Interopérabilité

- Matrice d'interopérabilité NetApp

  "http://support.netapp.com/matrix/"

- Outil d'interopérabilité matérielle et logicielle Cisco UCS

  "http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"

- Guide de compatibilité VMware

  "http://www.vmware.com/resources/compatibility/search.php"

Documents de référence de NetApp Cloud Volumes ONTAP

- NetApp Cloud Manager

  "https://docs.netapp.com/us-en/occm/concept_overview.html"

- Cloud Volumes ONTAP

  https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/task-getting-started-gcp.html

- Calculateur de coût total de possession Cloud Volumes ONTAP

  https://cloud.netapp.com/google-cloud-calculator

- Cloud Volumes ONTAP Sizer

  "https://cloud.netapp.com/cvo-sizer"

- Outil d'évaluation du cloud

  https://cloud.netapp.com/assessments

- Le cloud hybride NetApp

  https://cloud.netapp.com/hybrid-cloud

- Documentation de l'API Cloud Manager

  "https://docs.netapp.com/us-en/occm/reference_infrastructure_as_code.html"

Résolution des problèmes

"https://kb.netapp.com/Advice_and_Troubleshooting/Cloud_Services/Cloud_Volumes_ONTAP_(CVO)"

Terraform

- Terraform Cloud

  "https://www.terraform.io/cloud"

- Documentation Terraform

  "https://www.terraform.io/docs/"

- Registre NetApp Cloud Manager

  "https://registry.terraform.io/providers/NetApp/netapp-cloudmanager/lates"

GCP

- ONTAP haute disponibilité pour GCP

  "https://cloud.netapp.com/blog/gcp-cvo-blg-what-makes-cloud-volumes-ontap-high-availability-for-gcp-tick"

- Avantages de GCP

  https://netapp.hosted.panopto.com/Panopto/Pages/Viewer.aspx?id=f3d0368b-7165-4d43-a76e-ae01011853d6

Cloud hybride FlexPod avec NetApp Astra et Cisco Intersight pour Red Hat OpenShift

Tr-4936 : cloud hybride FlexPod avec NetApp Astra et Cisco Intersight pour Red Hat OpenShift

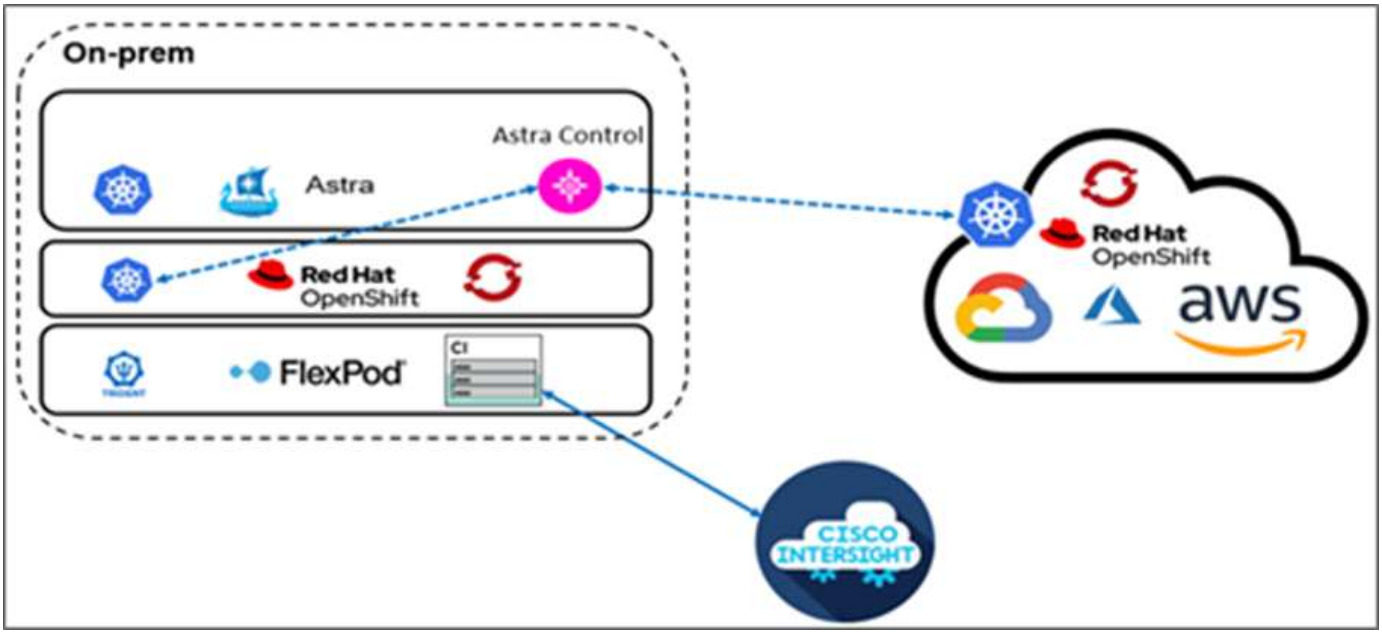
Abhinav Singh

Introduction

Les conteneurs et Kubernetes s'imposent comme la solution idéale pour développer, déployer, exécuter, gérer et faire évoluer les applications conteneurisées, et les entreprises déploient de plus en plus d'applications stratégiques. Les applications stratégiques dépendent fortement de l'état des applications. Une application avec état possède des informations associées à l'état, aux données et à la configuration, et dépend des transactions de données précédentes pour exécuter sa logique applicative. Les applications stratégiques s'exécutant sur Kubernetes continuent de satisfaire aux exigences de disponibilité et de continuité de l'activité telles que les applications classiques. Une panne de service peut avoir des conséquences graves sur la perte de chiffre d'affaires, la productivité et la réputation de l'entreprise. Il est donc essentiel de protéger, restaurer et déplacer les workloads Kubernetes rapidement et facilement dans et entre les clusters, les data centers sur site et les environnements de cloud hybride. Les entreprises ont vu les avantages de basculer leur activité vers un modèle de cloud hybride et de moderniser leurs applications dans un format cloud natif.

Dans ce rapport technique, nous Unis d'un centre de contrôle NetApp Astra avec Red Hat OpenShift Container Platform sur une solution d'infrastructure convergée FlexPod. Il s'étend à Amazon Web Services (AWS) pour former un data Center de cloud hybride. Sur la base de la connaissance "FlexPod et Red Hat OpenShift", Ce document présente NetApp Astra Control Center, qui commence par l'installation, la configuration, les workflows de protection des applications et la migration des applications entre le site et le cloud. Il présente également les avantages des fonctionnalités de gestion des données intégrant la cohérence applicative (notamment la sauvegarde et la restauration, la continuité de l'activité) avec NetApp Astra Control Center pour les applications conteneurisées qui s'exécutent sur Red Hat OpenShift.

La figure suivante illustre la présentation de la solution.



Public

Le public visé est composé de directeurs de la technologie (CTO), de développeurs d'applications, d'architectes de solutions cloud, d'ingénieurs de fiabilité des sites, d'ingénieurs DevOps, d'opérations IT et d'équipes de services professionnels axés sur la conception, l'hébergement et la gestion des applications conteneurisées.

NetApp Astra Control – principales utilisations

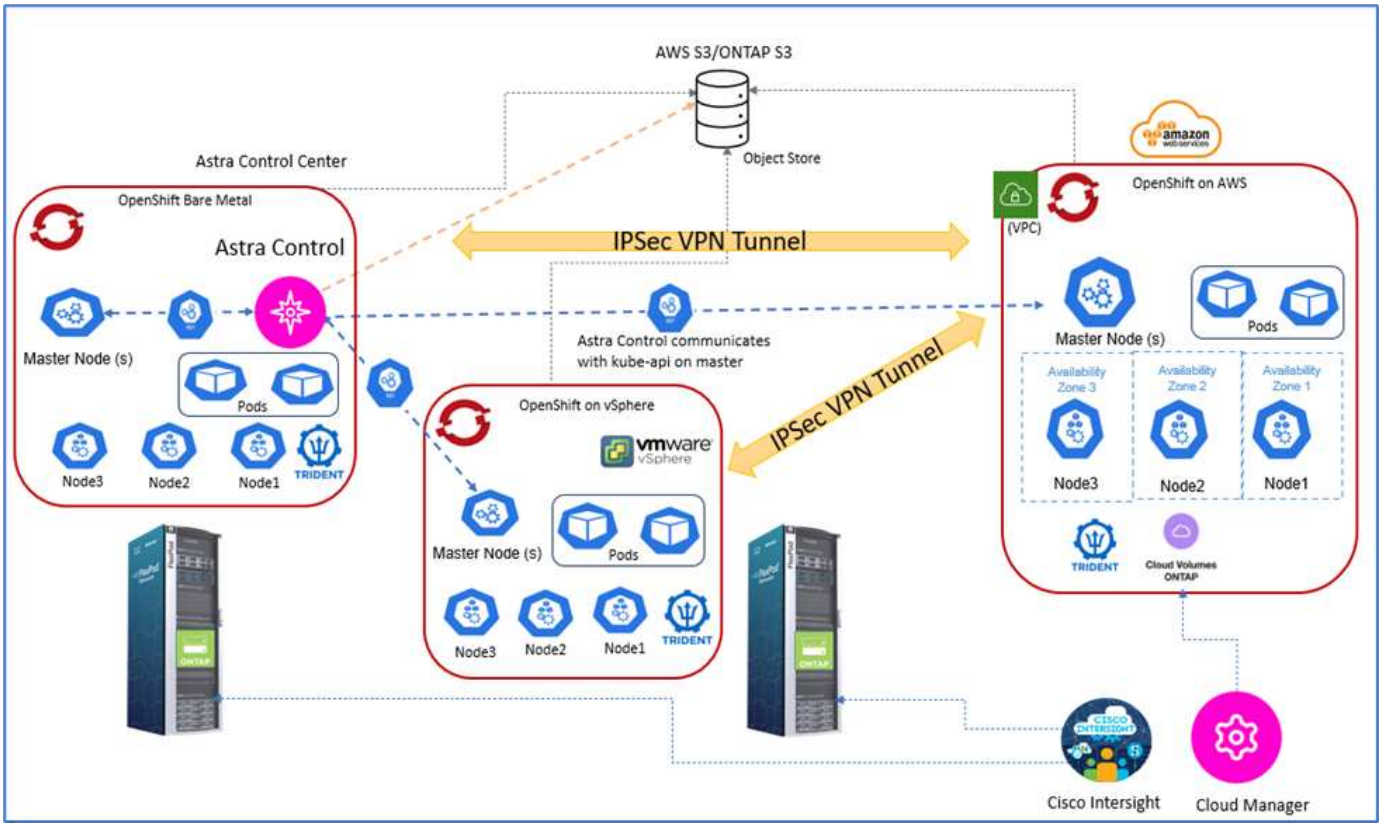
NetApp Astra Control vise à simplifier la protection des applications pour les clients qui gèrent des microservices cloud natifs :

- **Représentation d'application instantanée avec snapshots.** avec Astra Control, vous pouvez effectuer des snapshots de bout en bout de vos applications conteneurisées qui incluent les détails de configuration de l'application exécutée sur Kubernetes et le stockage persistant associé. En cas d'incident, les applications peuvent être restaurées à un état de fonctionnement connu en cliquant sur le bouton.
- **Sauvegarde complète de l'application de copie.** avec Astra Control, vous pouvez effectuer une sauvegarde complète de l'application selon un calendrier prédéfini qui peut être utilisé pour restaurer l'application vers le même cluster K8s ou vers un autre cluster à la demande de façon automatisée.
- **Portabilité des applications et migration avec des clones.** avec Astra Control, vous pouvez cloner une application entière avec ses données d'un cluster Kubernetes vers un autre cluster ou au sein d'un même cluster K8s. Cette fonction contribue également à déplacer ou migrer une application sur les clusters K8s, quel que soit l'emplacement des clusters (il suffit de supprimer l'instance d'application source après le clonage).
- **Personnaliser la cohérence des applications.** avec Astra Control, vous pouvez prendre le contrôle de la définition des États de mise en attente des applications en utilisant les crochets d'exécution. Lorsque vous placez les crochets d'exécution « pré » et « post » dans les flux de travail de snapshot et de sauvegarde, vos applications seront suspendues de votre manière avant qu'un snapshot ou une sauvegarde ne soit créé.
- **Automatisez la reprise après incident au niveau applicatif.** avec Astra Control, vous pouvez configurer un plan de reprise après incident pour la continuité de l'activité pour vos applications conteneurisées. NetApp SnapMirror est utilisé en back-end et la mise en œuvre complète du workflow de reprise après incident est automatisée.

Topologie de la solution

Cette section décrit la topologie logique de la solution.

L'illustration suivante représente la topologie de la solution, constituée de l'environnement FlexPod sur site exécutant des clusters OpenShift Container Platform et d'un cluster OpenShift Container Platform autogéré sur AWS avec NetApp Cloud Volumes ONTAP, Cisco Intersight et la plateforme NetApp Cloud Manager SaaS.



Le premier cluster OpenShift Container Platform est une installation sans système d'exploitation sur FlexPod. Le second cluster OpenShift Container Platform est déployé sur VMware vSphere exécuté sur FlexPod, et le troisième cluster OpenShift Container Platform est déployé en tant que "cluster privé" Dans un cloud privé virtuel (VPC) existant sur AWS en tant qu'infrastructure autonome.

Avec cette solution, FlexPod est connecté à AWS par le biais d'un VPN site à site. Cependant, les clients peuvent également utiliser les implémentations de connexion directe pour s'étendre à un cloud hybride. Cisco Intersight permet de gérer les composants de l'infrastructure FlexPod.

Dans cette solution, Astra Control Center gère l'application conteneurisée hébergée sur le cluster OpenShift Container Platform qui s'exécute sur FlexPod et sur AWS. Astra Control Center est installé sur l'instance OpenShift bare-Metal qui s'exécute sur FlexPod. Astra Control communique avec l'api kube sur le nœud maître et surveille en permanence le cluster Kubernetes pour y apporter des modifications. Toutes les nouvelles applications ajoutées au cluster K8s sont automatiquement découvertes et mises à disposition pour la gestion.

La représentation des applications conteneurisées peut être capturée sous forme de copies Snapshot à l'aide d'Astra Control Center. Les snapshots d'applications peuvent être déclenchés par une stratégie de protection planifiée ou à la demande. Pour les applications prises en charge par Astra, le snapshot est cohérent en cas de panne. Un snapshot d'application constitue un snapshot des données d'application dans les volumes persistants, ainsi que des métadonnées d'application des différentes ressources Kubernetes associées à cette application.

Il est possible de créer une copie de sauvegarde complète d'une application à l'aide d'Astra Control avec un programme de sauvegarde prédéfini ou à la demande. Un stockage objet est utilisé pour stocker la sauvegarde des données d'application. NetApp ONTAP S3, NetApp StorageGRID et toutes les implémentations S3 génériques peuvent être utilisées comme un magasin d'objets.

"Ensuite, les composants de la solution."

Composants de la solution

"Précédent : présentation de la solution."

FlexPod

FlexPod est un ensemble défini de matériels et de logiciels qui constitue une base intégrée pour les solutions virtualisées et non virtualisées. FlexPod inclut le stockage NetApp ONTAP, les réseaux Cisco Nexus, les réseaux de stockage Cisco MDS, Cisco Unified Computing System (Cisco UCS). La conception est suffisamment flexible pour que le réseau, le calcul et le stockage puissent s'intégrer dans un seul rack de data Center ou être déployés selon la conception du centre de données du client. La densité des ports permet aux composants réseau de prendre en charge plusieurs configurations.

Contrôle Astra

Astra Control propose des services de protection des données cohérents avec les applications cloud, hébergés dans des clouds publics et sur site. Astra Control assure la protection des données, la reprise d'activité et la migration de vos applications conteneurisées exécutées sur Kubernetes.

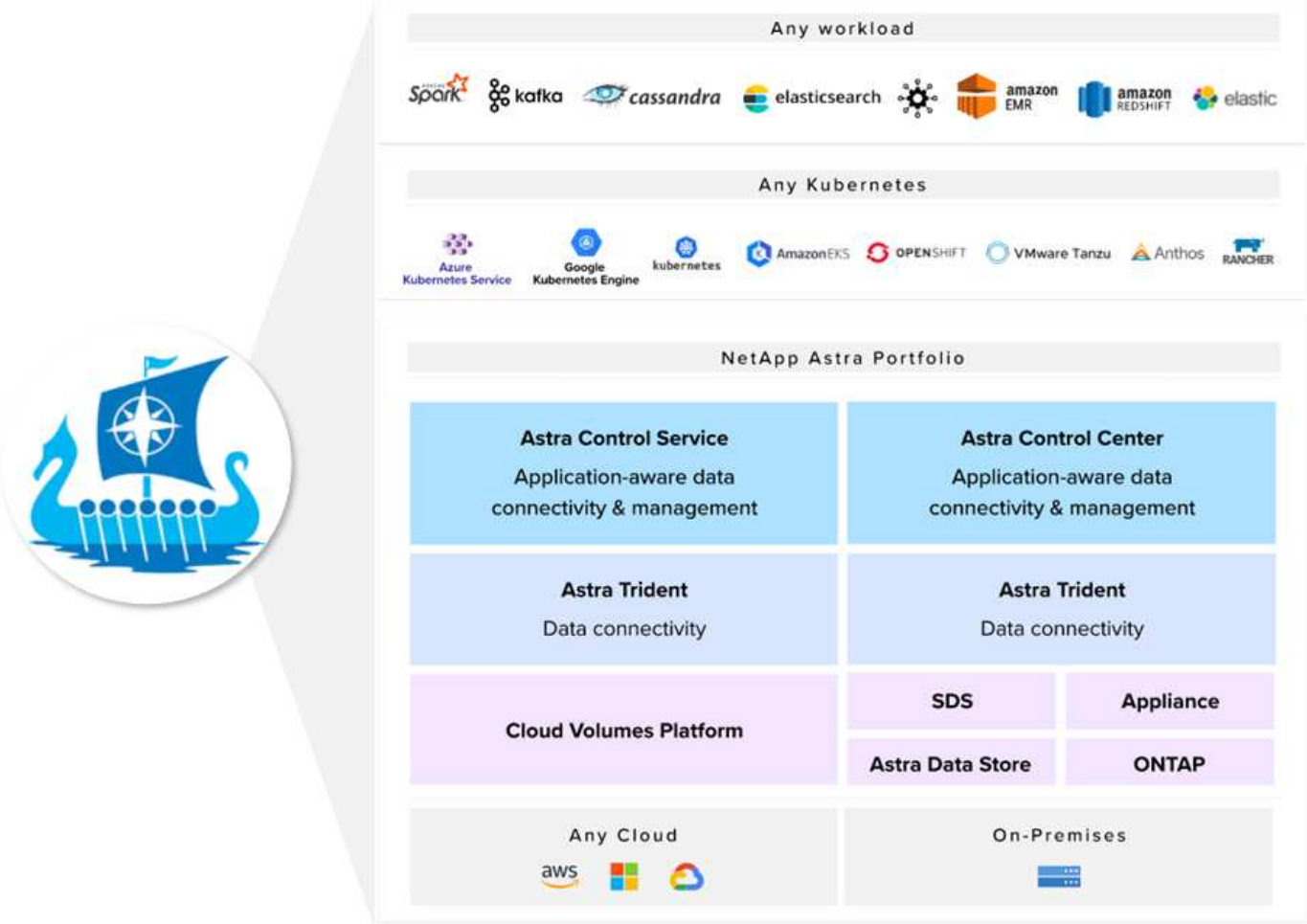
Caractéristiques

Astra Control offre des fonctionnalités stratégiques pour la gestion du cycle de vie des données d'application Kubernetes :

- Gérez automatiquement le stockage persistant
- Création de copies Snapshot et de sauvegardes cohérentes avec les applications à la demande
- Opérations de sauvegarde et de snapshots automatisées basées sur des règles
- Migrez des applications et des données associées d'un cluster Kubernetes vers un autre dans une configuration de cloud hybride
- Clonez une application sur le même cluster K8s ou sur un autre cluster K8s
- Visualisation de l'état de la protection des applications
- Fournit une interface utilisateur graphique et une liste exhaustive d'API REST permettant de mettre en œuvre tous les flux de travail de protection à partir des outils internes existants.

Astra Control offre une visualisation centralisée pour vos applications conteneurisées qui fournit un aperçu des ressources associées créées dans le cluster Kubernetes. Vous pouvez afficher tous vos clusters, toutes vos applications, dans tous les clouds ou dans tous les data centers à partir d'un portail unique. Vous pouvez utiliser les API de contrôle Astra dans tous les environnements (sur site ou dans des clouds publics) pour implémenter vos workflows de gestion des données.

L'image suivante montre les fonctions de contrôle Astra.



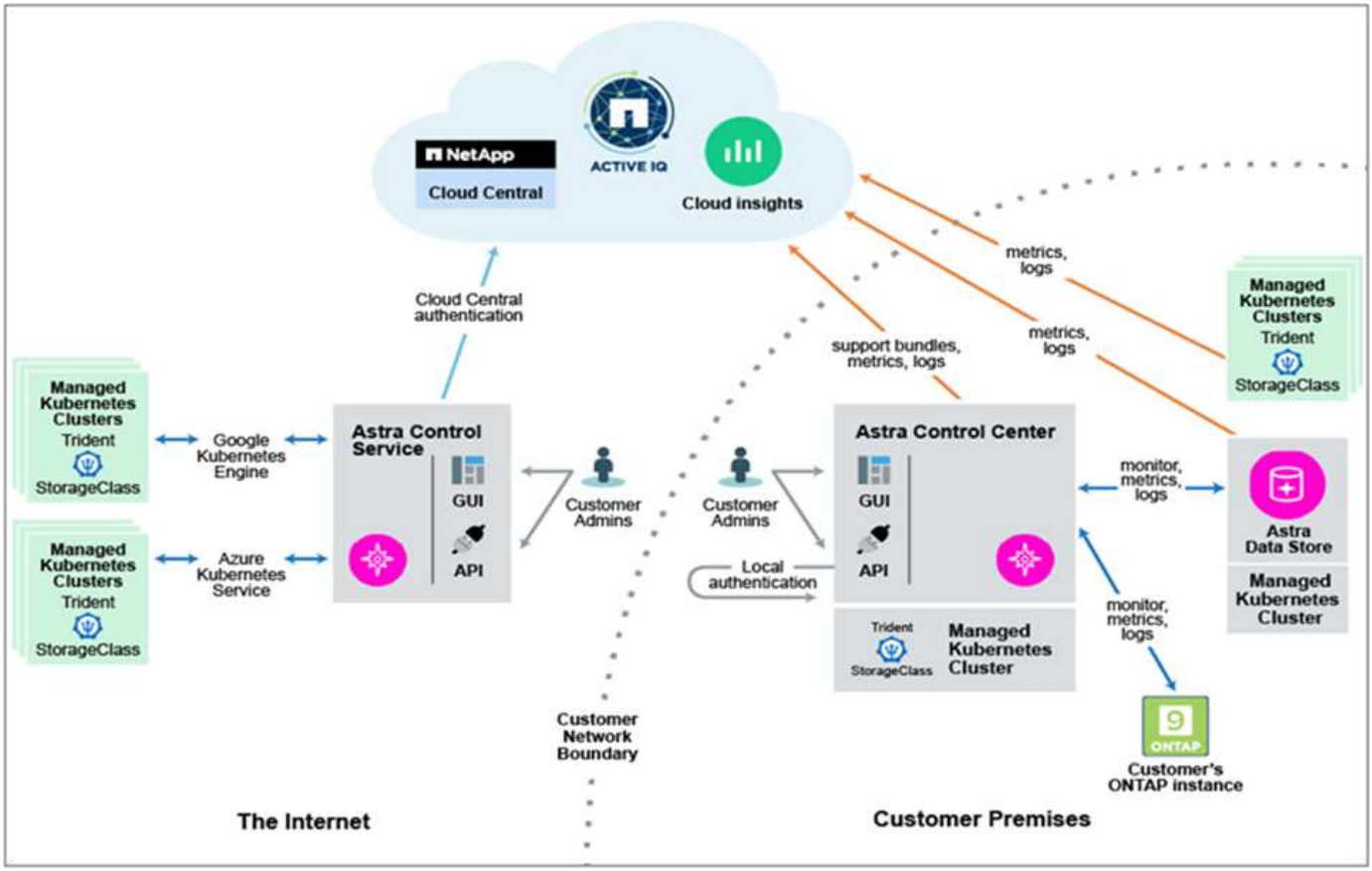
Modèles de consommation Astra Control

Astra Control est disponible en deux modèles de consommation :

- **Astra Control Service.** Un service entièrement géré hébergé par NetApp qui permet la gestion des données intégrant la cohérence applicative des clusters Kubernetes dans Google Kubernetes Engine (GKE), Azure Kubernetes Service (AKS).
- **Astra Control Center.** logiciel autogéré qui assure la gestion des données intégrant la cohérence applicative de clusters Kubernetes exécutés dans votre environnement sur site et de cloud hybride.

Dans ce rapport technique, Astra Control Center est utilisé pour la gestion des applications cloud natives qui s'exécutent sur Kubernetes.

L'image suivante montre l'architecture Astra Control.



Astra Trident

Astra Trident est un orchestrateur de stockage open source entièrement pris en charge pour les conteneurs et les distributions Kubernetes. Il a été conçu dès le départ pour vous aider à répondre aux exigences de persistance de vos applications conteneurisées à l'aide d'interfaces standard, telles que le "Interface de stockage de conteneurs (CSI)". Avec Astra Trident, les microservices et les applications conteneurisées peuvent bénéficier des services de stockage haute performance fournis par le portefeuille NetApp de systèmes de stockage.

Astra Trident est déployé sur des clusters Kubernetes en tant que pods et fournit des services d'orchestration du stockage dynamique pour vos workloads Kubernetes. Il permet à vos applications conteneurisées de consommer le stockage persistant rapidement et facilement depuis le vaste portefeuille de NetApp, qui inclut NetApp ONTAP (NetApp AFF, NetApp FAS, NetApp ONTAP Select, cloud, Et Amazon FSX pour NetApp ONTAP), NetApp Element (NetApp SolidFire), ainsi que le service Azure NetApp Files, Cloud Volume Service sur Google Cloud et Cloud volumes Service sur AWS. Dans un environnement FlexPod, Astra Trident permet de provisionner et de gérer de manière dynamique les volumes persistants pour les conteneurs qui sont sauvegardés par des volumes NetApp FlexVol et des LUN hébergés sur une plateforme de stockage ONTAP, comme les systèmes NetApp AFF, FAS et Cloud Volumes ONTAP. Trident joue également un rôle clé dans la mise en œuvre de systèmes de protection des applications proposés par Astra Control. Pour en savoir plus sur Astra Trident, rendez-vous sur le "Documentation Astra Trident."

Système back-end

Pour utiliser Astra Trident, vous avez besoin d'un système back-end de stockage pris en charge. Un système back-end Trident définit la relation entre Trident et un système de stockage. Il explique à Trident comment communiquer avec ce système de stockage et comment Trident doit provisionner les volumes à partir de celui-ci. Trident va automatiquement proposer des pools de stockage back-end correspondant aux exigences définies par une classe de stockage.

- Système back-end ONTAP AFF et FAS. En tant que plateforme matérielle et logicielle de stockage, ONTAP fournit des services de stockage de base, la prise en charge de plusieurs protocoles d'accès au stockage et des fonctionnalités de gestion du stockage, comme les copies Snapshot et la mise en miroir NetApp.
- Système back-end Cloud Volumes ONTAP
- "Magasin de données Astra" système back-end

NetApp Cloud Volumes ONTAP

NetApp Cloud Volumes ONTAP est une offre de stockage Software-defined qui offre des fonctionnalités avancées de gestion des données pour les workloads de fichiers et de blocs. Avec Cloud Volumes ONTAP, vous pouvez optimiser vos coûts de stockage cloud et augmenter les performances de vos applications tout en améliorant la protection des données, la sécurité et la conformité.

Parmi les principaux avantages :

- Exploitez les fonctionnalités intégrées de déduplication et de compression des données, de provisionnement fin et de clonage pour réduire les coûts de stockage.
- Fiabilité exceptionnelle et continuité de l'activité en cas de défaillances dans votre environnement cloud.
- Cloud Volumes ONTAP exploite SnapMirror, la technologie de réplication leader de NetApp, pour répliquer les données sur site dans le cloud de façon à pouvoir disposer de copies secondaires dans différents cas d'utilisation.
- Cloud Volumes ONTAP s'intègre également avec Cloud Backup Service pour fournir des fonctionnalités de sauvegarde et de restauration pour la protection et l'archivage à long terme de vos données cloud.
- Basculez entre pools de stockage hautes performances et faibles performances à la demande sans interrompre les applications.
- Cohérence des copies Snapshot avec NetApp SnapCenter
- Cloud Volumes ONTAP prend en charge le cryptage des données et protège contre les virus et les attaques par ransomware.
- L'intégration avec Cloud Data SENSE vous aide à comprendre le contexte des données et à identifier les données sensibles.

Cloud Central

Cloud Central est une plateforme centralisée qui permet d'accéder aux services de données cloud NetApp et de les gérer. Ces services vous permettent d'exécuter des applications stratégiques dans le cloud, de créer des sites automatisés de reprise d'activité, de sauvegarder les données et de migrer et contrôler efficacement les données entre plusieurs clouds. Pour plus d'informations, voir "Cloud Central."

Le gestionnaire Cloud

Cloud Manager est une plateforme de gestion SaaS de grande qualité qui permet aux experts INFORMATIQUES et aux architectes clouds de gérer de manière centralisée leur infrastructure multicloud hybride à l'aide des solutions clouds NetApp. Cette solution offre un système centralisé pour afficher et gérer vos environnements de stockage sur site et cloud, prenant en charge des environnements de cloud hybride de plusieurs fournisseurs et comptes. Pour plus d'informations, voir "Le gestionnaire Cloud".

Connecteur

Connector est une instance qui permet à Cloud Manager de gérer les ressources et les processus dans un

environnement de cloud public. Un connecteur est nécessaire pour utiliser de nombreuses fonctionnalités offertes par Cloud Manager. Un connecteur peut être déployé dans le cloud ou sur site.

Le connecteur est pris en charge aux emplacements suivants :

- AWS
- Microsoft Azure
- Google Cloud
- Sur site

Pour en savoir plus sur le connecteur, voir "ce lien."

NetApp Cloud Insights

Avec l'outil NetApp de surveillance de l'infrastructure cloud, Cloud Insights vous permet de surveiller la performance et l'utilisation de vos clusters Kubernetes gérés par Astra Control Center. Cloud Insights met en corrélation l'utilisation du stockage avec les charges de travail. Lorsque vous activez la connexion Cloud Insights dans le centre de contrôle Astra, les informations de télémétrie s'affichent dans les pages de l'interface utilisateur du centre de contrôle Astra.

NetApp Active IQ Unified Manager

Avec NetApp Active IQ Unified Manager, vous pouvez contrôler vos clusters de stockage ONTAP à partir d'une interface intuitive unique, reconçue pour exploiter les connaissances de la communauté et l'analytique d'IA. Elle fournit des informations opérationnelles, de performance et proactives sur l'environnement de stockage et les machines virtuelles qui s'exécutent sur celui-ci. Lorsqu'un problème survient sur l'infrastructure de stockage, Unified Manager vous informe des détails du problème pour vous aider à identifier la cause première. Le tableau de bord des machines virtuelles vous offre une vue détaillée des statistiques de performances de la machine virtuelle. Vous pouvez ainsi examiner l'ensemble du chemin d'E/S depuis l'hôte VMware vSphere, via le réseau et enfin vers le stockage. Certains événements fournissent également des mesures correctives qui peuvent être prises pour corriger le problème. Vous pouvez configurer des alertes personnalisées en cas d'événements afin que, lorsque des problèmes se produisent, vous soyez averti par e-mail et par des traps SNMP. Active IQ Unified Manager vous permet de planifier les besoins en stockage de vos utilisateurs en anticipant les besoins en stockage et en vous permettant d'anticiper les problèmes, ce qui évite de prendre des décisions réactives à court terme et même d'engendrer des problèmes supplémentaires à long terme.

Cisco Intersight

Cisco Intersight est une plateforme SaaS qui assure une automatisation, une observabilité et une optimisation intelligentes pour les applications et l'infrastructure classiques et cloud. La plateforme contribue aux changements avec les équipes IT et propose un modèle d'exploitation conçu pour le cloud hybride.

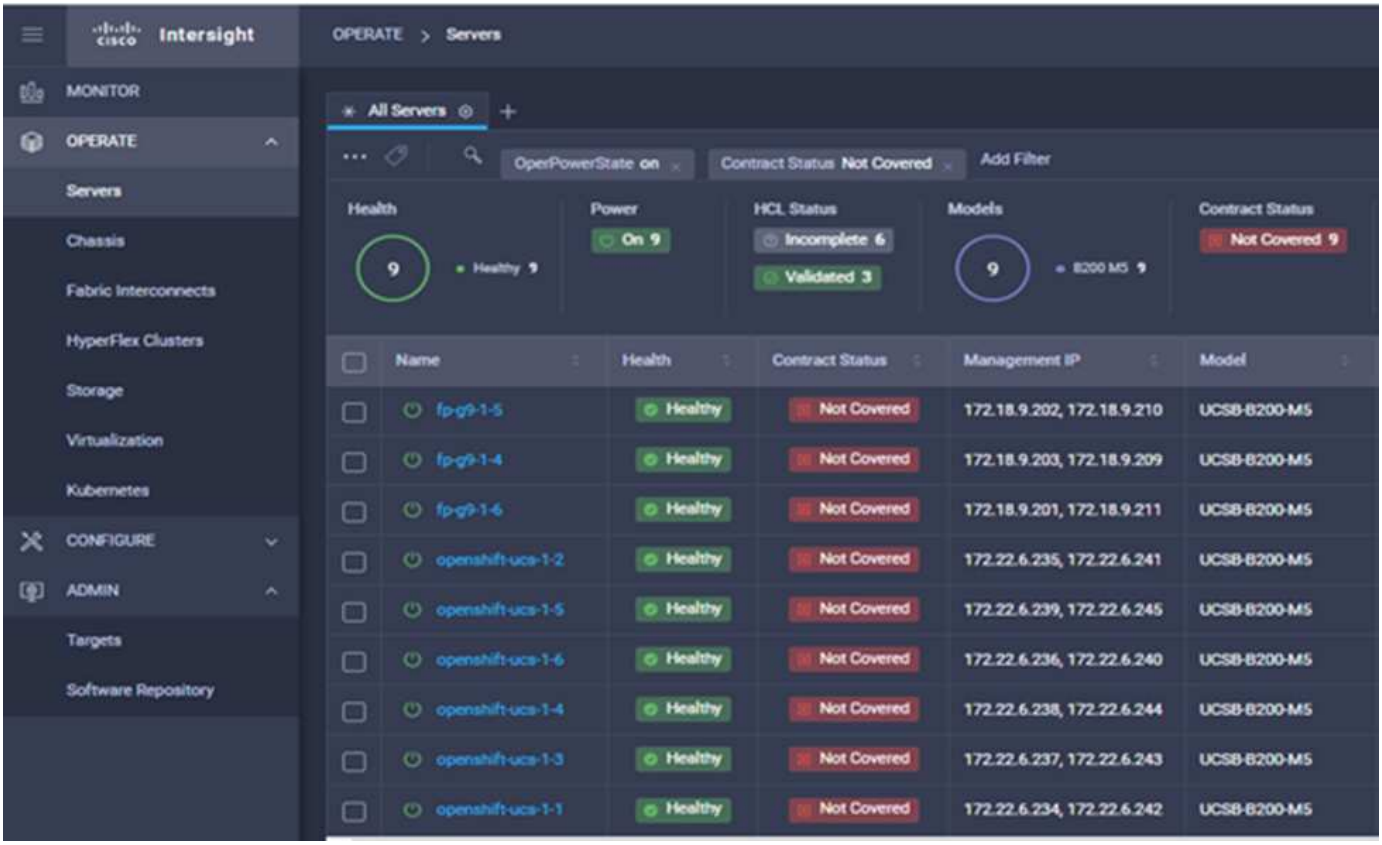
Cisco Intersight offre les avantages suivants :

- **Livraison plus rapide.** livraison en tant que service depuis le cloud ou dans le centre de données du client avec des mises à jour fréquentes et une innovation continue, grâce à un modèle de développement logiciel agile. De cette façon, le client peut se concentrer sur l'accélération de la livraison pour le secteur d'activité.
- **Opérations simplifiées.** simplifier les opérations en utilisant un seul outil SaaS sécurisé avec inventaire, authentification et API communs pour travailler sur l'ensemble de la pile et tous les emplacements, éliminant ainsi les silos entre les équipes. De la gestion des serveurs physiques et des hyperviseurs sur site aux machines virtuelles, K8s, sans serveur, automatisation, l'optimisation et le contrôle des coûts à la fois sur site et dans les clouds publics.

- **Optimisation continue.** optimisation continue de votre environnement en utilisant l'intelligence fournie par Cisco Intersight sur chaque couche, ainsi que Cisco TAC. Cette intelligence est convertie en actions recommandées et automatisable, ce qui vous permet de vous adapter en temps réel à chaque changement : du déplacement des charges de travail et du contrôle de l'état des serveurs physiques, au dimensionnement automatique des clusters, aux recommandations de réduction des coûts des clouds publics avec lesquels vous travaillez.

Il existe deux modes d'opérations de gestion possibles avec Cisco Intersight : Umm (UCSM Managed mode) et IMM (Intersight Managed mode). Vous pouvez sélectionner l'UMM natif ou IMM pour les systèmes Cisco UCS reliés au fabric lors de la configuration initiale des interconnexions de fabric. Dans cette solution, l'UMM natif est utilisé.

L'image suivante montre le tableau de bord Cisco Intersight.



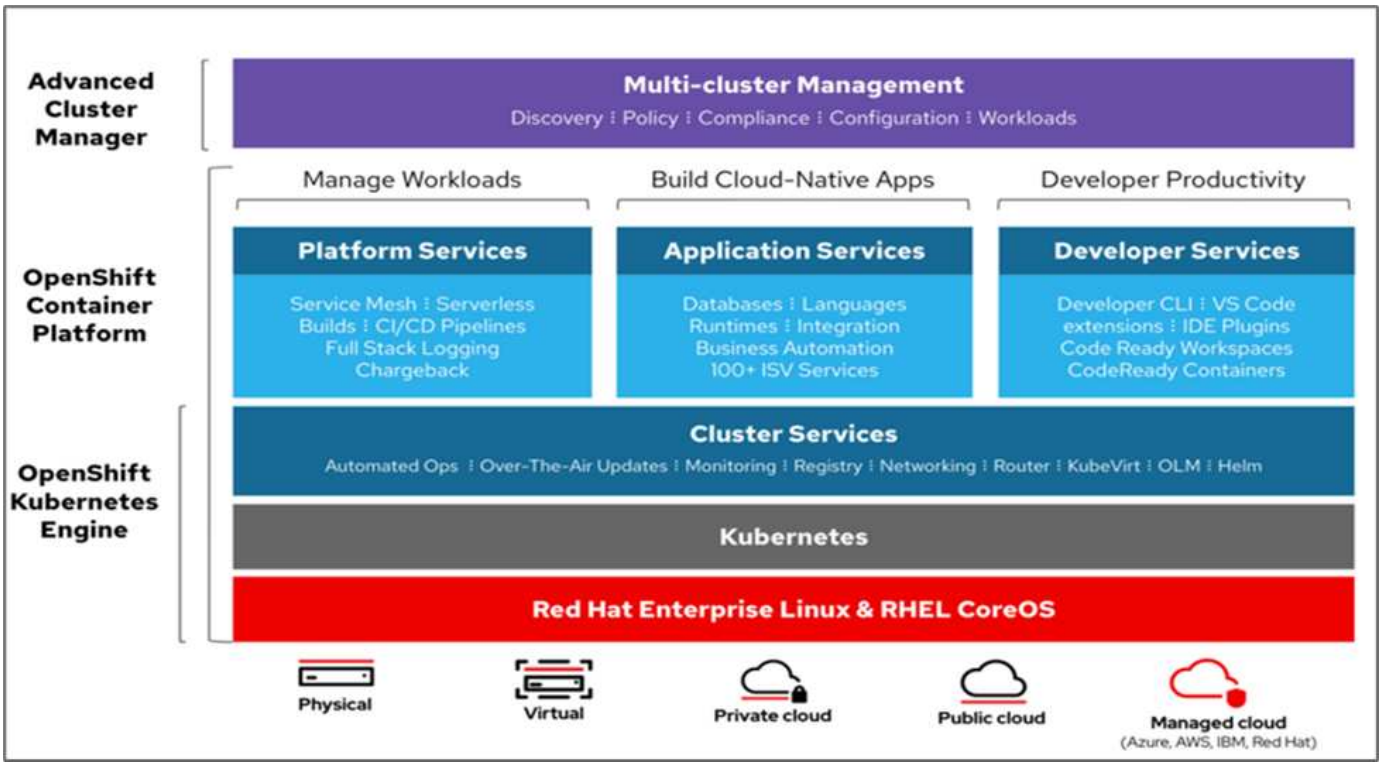
Plateforme de conteneurs Red Hat OpenShift

Red Hat OpenShift Container Platform est une plateforme applicative de conteneurs qui rassemble CRI-O et Kubernetes et qui fournit une API et une interface Web pour gérer ces services. CRI-O est une implémentation de l'interface d'exécution du conteneur Kubernetes (CRI) pour permettre l'utilisation des runtimes compatibles avec l'initiative OCI (Open Container Initiative). Il s'agit d'une alternative légère à l'utilisation de Docker en tant que composant d'exécution pour Kubernetes.

OpenShift Container Platform permet aux clients de créer et de gérer des conteneurs. Les conteneurs sont des processus autonomes qui s'exécutent dans leur propre environnement, indépendamment du système d'exploitation et de l'infrastructure sous-jacente. OpenShift Container Platform aide à développer, déployer et gérer les applications basées sur des conteneurs. Il offre une plateforme en libre-service pour créer, modifier et déployer des applications à la demande, ce qui accélère le développement et la commercialisation des cycles de vie. OpenShift Container Platform est dotée d'une architecture basée sur des microservices de petites unités découplées. Elle s'exécute sur un cluster Kubernetes, et les données relatives aux objets stockés dans

ETCD, un magasin de clés à valeur ajoutée en cluster fiable.

L'image suivante présente la plateforme de conteneurs Red Hat OpenShift.



Infrastructure Kubernetes

Dans OpenShift Container Platform, Kubernetes gère les applications conteneurisées sur un ensemble d'hôtes d'exécution CRI-O, et fournit des mécanismes pour le déploiement, la maintenance et l'évolutivité des applications. Les packages de service CRI-O, instancient et exécutent des applications conteneurisées.

Un cluster Kubernetes comprend un ou plusieurs maîtres et un ensemble de nœuds workers. Cette solution intègre les fonctionnalités de haute disponibilité (HA) au niveau du matériel et de la pile logicielle. Un cluster Kubernetes est conçu pour s'exécuter en mode HA avec trois nœuds maîtres et au moins deux nœuds workers afin de vous aider à assurer que le cluster ne présente aucun point de défaillance unique.

Système d'exploitation Red Hat Core

OpenShift Container Platform exploite Red Hat Enterprise Linux CoreOS (RHCOS), un système d'exploitation orienté conteneurs qui combine les meilleures fonctionnalités des systèmes d'exploitation hôtes atomiques CoreOS et Red Hat. RHCOS est spécialement conçu pour exécuter des applications conteneurisées à partir d'OpenShift Container Platform et fonctionne avec de nouveaux outils pour permettre une installation rapide, une gestion basée sur l'opérateur et des mises à niveau simplifiées.

RHCOS inclut les fonctions suivantes :

- Ignition, qu'OpenShift Container Platform utilise comme première configuration de système de démarrage pour l'initialisation et la configuration des machines.
- CRI-O, implémentation d'un exécution de conteneurs natif Kubernetes qui s'intègre étroitement au système d'exploitation pour offrir une expérience Kubernetes efficace et optimisée. CRI-O permet de faire fonctionner, d'arrêter et de redémarrer les conteneurs. Elle remplace entièrement le moteur de conteneurs Docker, qui a été utilisé dans OpenShift Container Platform 3.

- Kubelet, l'agent de nœud principal pour Kubernetes, est responsable du lancement et de la surveillance des conteneurs.

VMware vSphere 7.0

VMware vSphere est une plateforme de virtualisation qui permet de gérer de manière holistique de vastes ensembles d'infrastructures (ressources notamment les processeurs, le stockage et le réseau), sous la forme d'un environnement d'exploitation transparent, polyvalent et dynamique. Contrairement aux systèmes d'exploitation traditionnels qui gèrent une machine individuelle, VMware vSphere agrège l'infrastructure d'un data Center dans son ensemble pour créer une seule puissance avec des ressources qui peuvent être allouées rapidement et dynamiquement à n'importe quelle application, selon les besoins.

Pour plus d'informations, voir "VMware vSphere".

VMware vSphere vCenter

VMware vCenter Server assure une gestion unifiée de tous les hôtes et machines virtuelles depuis une console unique et rassemble le contrôle des performances des clusters, des hôtes et des machines virtuelles. VMware vCenter Server offre aux administrateurs des informations détaillées sur l'état et la configuration des clusters de calcul, des hôtes, des VM, du stockage, du système d'exploitation invité, et autres composants essentiels d'une infrastructure virtuelle. VMware vCenter gère la richesse des fonctionnalités disponibles dans un environnement VMware vSphere.

Révisions matérielles et logicielles

Cette solution peut être étendue à tout environnement FlexPod qui exécute des versions logicielles, micrologicielles et matérielles prises en charge, telles que définies dans le "Matrice d'interopérabilité NetApp" et "Liste de compatibilité matérielle Cisco UCS." Le cluster OpenShift est installé sur FlexPod sans système d'exploitation, ainsi que sur VMware vSphere.

Une seule instance d'Astra Control Center est nécessaire pour gérer plusieurs clusters OpenShift (k8), tandis que Trident CSI est installé sur chaque cluster OpenShift. Astra Control Center peut être installé sur l'un de ces clusters OpenShift. Dans cette solution, Astra Control Center est installé sur le cluster OpenShift bare-Metal.

Le tableau suivant répertorie les révisions matérielles et logicielles FlexPod pour OpenShift.

Composant	Solution NetApp	Version
Calcul	Cisco UCS Fabric Interconnect 6454	4.1(3c)
	Serveurs Cisco UCS B200 M5	4.1(3c)
Le réseau	Cisco Nexus 9336C-FX2 NX-OS	9.3(8)
Stockage	NetApp AFF A700	9.11.1
	NetApp Astra Control Center	22.04.0
	Plug-in NetApp Astra Trident CSI	22.04.0
	NetApp Active IQ Unified Manager	9.11
Logiciel	Pilote Ethernet nenic VMware ESXi	1.0.35.0
	VSphere ESXi	7.0(U2)

Composant	Solution NetApp	Version
	Appliance VMware vCenter	7.0 U2b
	Appliance virtuelle Cisco InterSight Assist	1.0.9-342
	Plateforme de conteneurs OpenShift	4.9
	Nœud principal OpenShift Container Platform	RHCOS 4.9
	Nœud de travail OpenShift Container Platform	RHCOS 4.9

Le tableau suivant répertorie les versions logicielles d'OpenShift sur AWS.

Composant	Solution NetApp	Version
Calcul	Type d'instance maître : m5.XLarge	s/o
	Type d'instance de travailleur : m5.large	s/o
Le réseau	Passerelle de transit du cloud privé virtuel	s/o
Stockage	NetApp Cloud Volumes ONTAP	9.11.1
	Plug-in NetApp Astra Trident CSI	22.04.0
Logiciel	Plateforme de conteneurs OpenShift	4.9
	Nœud principal OpenShift Container Platform	RHCOS 4.9
	Nœud de travail OpenShift Container Platform	RHCOS 4.9

"Suivant : installation de FlexPod pour OpenShift Container Platform 4 sans système d'exploitation."

Installation et configuration

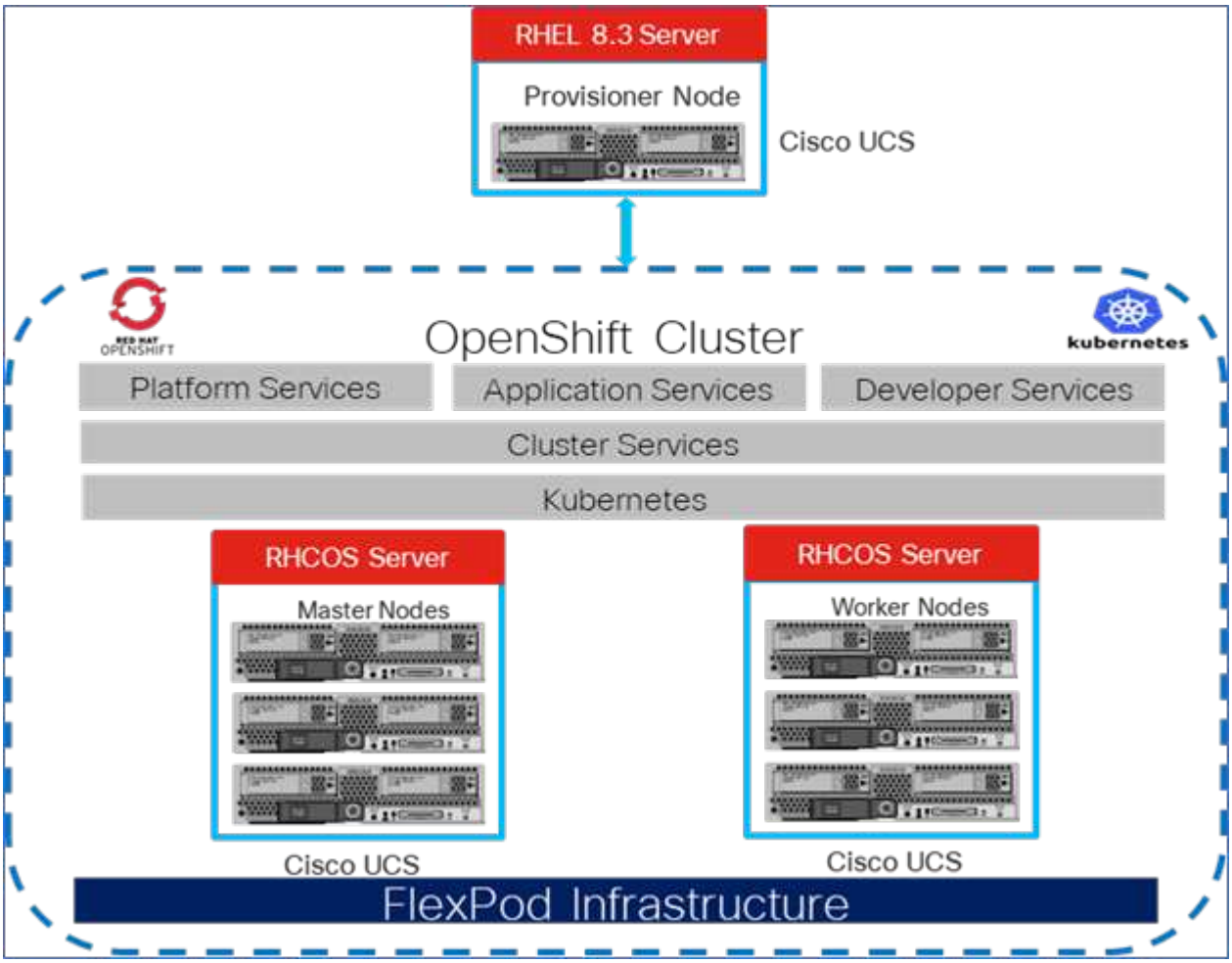
Installation de FlexPod pour OpenShift Container Platform 4 sans système d'exploitation

"Précédent : composants de la solution."

Pour comprendre la conception sans système d'exploitation FlexPod pour OpenShift Container Platform 4, les détails du déploiement et l'installation et la configuration de NetApp Astra Trident, consultez "Guide de déploiement et de conception validée par Cisco pour FlexPod avec OpenShift Cisco (CVD)". Ce CVD couvre le déploiement d'FlexPod et de OpenShift Container Platform avec Ansible. Le CVD fournit également des informations détaillées sur la préparation des nœuds de travail, de l'installation d'Astra Trident, du système de stockage back-end et des configurations de classes de stockage, qui sont les quelques prérequis au déploiement et à la configuration d'Astra

Control Center.

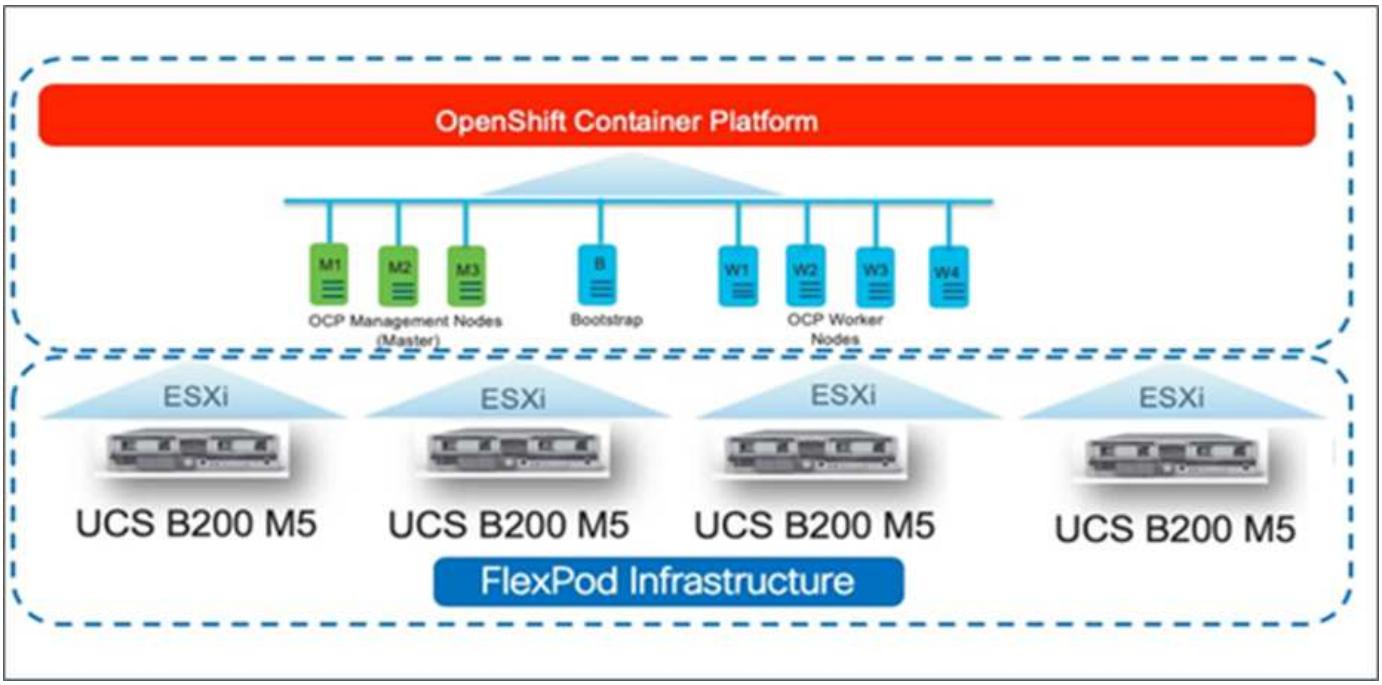
La figure suivante illustre la plateforme de conteneurs OpenShift 4 sans système d'exploitation sur FlexPod.



FlexPod pour OpenShift Container Platform 4 sur installation VMware

Pour en savoir plus sur le déploiement de Red Hat OpenShift Container Platform 4 sur un système FlexPod exécutant VMware vSphere, consultez la page "FlexPod Datacenter pour OpenShift Container Platform 4".

La figure suivante illustre FlexPod pour OpenShift Container Platform 4 sur vSphere.

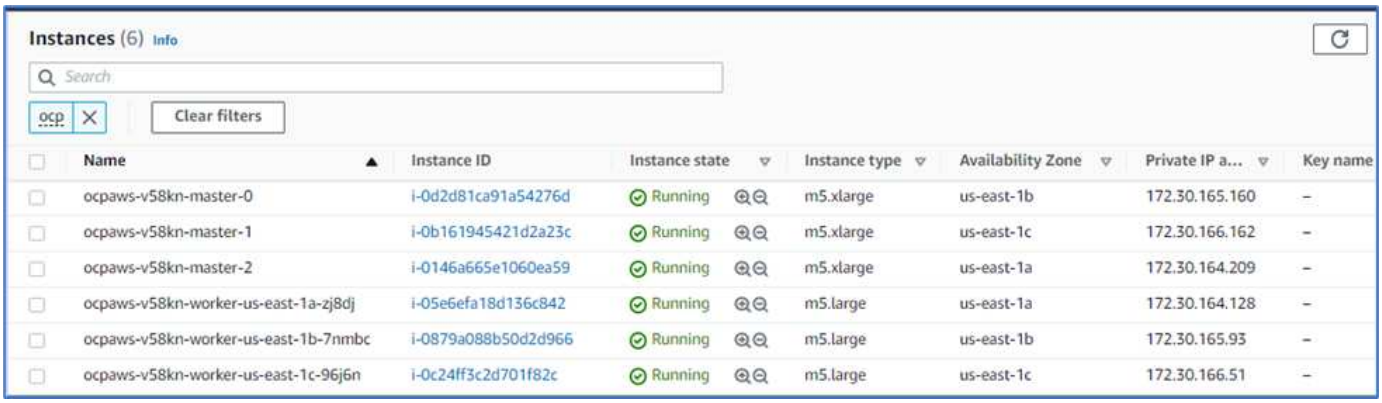


"Suivant : Red Hat OpenShift sur AWS."

Red Hat OpenShift sur AWS

"Précédent : installation de FlexPod pour OpenShift Container Platform 4 sans système d'exploitation."

Un cluster OpenShift Container Platform 4 autogéré est déployé sur AWS en tant que site de reprise après incident. Les nœuds maîtres et workers s'étendent sur trois zones de disponibilité pour une haute disponibilité.



Instances (6) Info

Search

ocp | Clear filters

Name	Instance ID	Instance state	Instance type	Availability Zone	Private IP a...	Key name
ocpaws-v58kn-master-0	i-0d2d81ca91a54276d	Running	m5.xlarge	us-east-1b	172.30.165.160	–
ocpaws-v58kn-master-1	i-0b161945421d2a23c	Running	m5.xlarge	us-east-1c	172.30.166.162	–
ocpaws-v58kn-master-2	i-0146a665e1060ea59	Running	m5.xlarge	us-east-1a	172.30.164.209	–
ocpaws-v58kn-worker-us-east-1a-zj8dj	i-05e6efa18d136c842	Running	m5.large	us-east-1a	172.30.164.128	–
ocpaws-v58kn-worker-us-east-1b-7nmbc	i-0879a088b50d2d966	Running	m5.large	us-east-1b	172.30.165.93	–
ocpaws-v58kn-worker-us-east-1c-96j6n	i-0c24ff3c2d701f82c	Running	m5.large	us-east-1c	172.30.166.51	–

```
[ec2-user@ip-172-30-164-92 ~]$ oc get nodes
NAME                              STATUS   ROLES    AGE   VERSION
ip-172-30-164-128.ec2.internal    Ready    worker   29m   v1.22.8+f34b40c
ip-172-30-164-209.ec2.internal    Ready    master   36m   v1.22.8+f34b40c
ip-172-30-165-160.ec2.internal    Ready    master   33m   v1.22.8+f34b40c
ip-172-30-165-93.ec2.internal     Ready    worker   30m   v1.22.8+f34b40c
ip-172-30-166-162.ec2.internal    Ready    master   36m   v1.22.8+f34b40c
ip-172-30-166-51.ec2.internal     Ready    worker   28m   v1.22.8+f34b40c
```

OpenShift est déployé en tant que A. "cluster privé" Dans un VPC existant sur AWS. Un cluster OpenShift Container Platform privé n'expose pas les terminaux externes. Il est accessible uniquement à partir d'un réseau interne et n'est pas visible sur Internet. NetApp Cloud Volumes ONTAP est déployé à un seul nœud à l'aide de NetApp Cloud Manager qui fournit un système back-end de stockage à Astra Trident.

Pour plus d'informations sur l'installation d'OpenShift sur AWS, consultez "Documentation OpenShift".

"Suivant : NetApp Cloud Volumes ONTAP."

NetApp Cloud Volumes ONTAP

"Précédent : Red Hat OpenShift sur AWS."

L'instance NetApp Cloud Volumes ONTAP est déployée sur AWS et sert de stockage back-end à Astra Trident. Avant d'ajouter un environnement de travail Cloud Volumes ONTAP, un connecteur doit être déployé. Cloud Manager vous invite à créer votre premier environnement de travail Cloud Volumes ONTAP sans connecteur. Pour déployer un connecteur dans AWS, voir "Créer un connecteur".

Pour déployer Cloud Volumes ONTAP sur AWS, consultez la section "Démarrage rapide pour AWS".

Une fois Cloud Volumes ONTAP déployé, vous pouvez installer Astra Trident et configurer le système de stockage back-end et la classe Snapshot sur le cluster OpenShift Container Platform.

"Suivant : installation d'Astra Control Center sur OpenShift Container Platform."

Installation d'Astra Control Center sur OpenShift Container Platform

"Précédent : NetApp Cloud Volumes ONTAP."

Vous pouvez installer Astra Control Center sur un cluster OpenShift qui s'exécute sur FlexPod ou sur AWS avec un système de stockage back-end Cloud Volumes ONTAP. Dans cette solution, Astra Control Center est déployé sur le cluster OpenShift bare-Metal.

Le centre de contrôle Astra peut être installé selon la procédure standard décrite "ici" Ou depuis Red Hat OpenShift OperatorHub. L'opérateur de contrôle Astra est un opérateur certifié Red Hat. Dans cette solution, Astra Control Center est installé à l'aide de Red Hat OperatorHub.

De l'environnement

- Astra Control Center prend en charge plusieurs distributions Kubernetes. Pour Red Hat OpenShift, les

versions prises en charge incluent Red Hat OpenShift Container Platform 4.8 ou 4.9.

- Astra Control Center requiert les ressources suivantes en plus des exigences de l'environnement et de l'utilisateur final en matière de ressources applicatives :

Composants	Conditions requises
Capacité du système back-end	Au moins 500 Go disponibles
Nœuds worker	Au moins 3 nœuds workers et doté de 4 cœurs de processeurs et de 12 Go de RAM chacun
Adresse de nom de domaine complet (FQDN)	Une adresse FQDN pour Astra Control Center
Astra Trident	Astra Trident 21.04 ou plus récent installé et configuré
Contrôleur d'entrée ou équilibreur de charge	Configurez le contrôleur d'entrée pour exposer Astra Control Center avec un URL ou un équilibreur de charge afin de fournir une adresse IP qui sera définie pour le FQDN

- Vous devez disposer d'un registre d'images privées existant dans lequel vous pouvez pousser les images de création d'Astra Control Center. Vous devez fournir l'URL du registre d'images où vous téléchargez les images.

> Certaines images sont extraites lors de l'exécution de certains flux de travail et des conteneurs sont créés et détruits si nécessaire.

- Avec Astra Control Center, il est nécessaire de créer une classe de stockage et de la définir comme classe de stockage par défaut. Le centre de contrôle Astra prend en charge les pilotes ONTAP suivants fournis par Astra Trident :
  - ontap-nas
  - ontap-nas-flexgroup
  - ontap-san
  - ontap-san-économie

> Nous supposons qu'Astra Trident est installé et configuré avec un système back-end ONTAP, et qu'une classe de stockage par défaut est également définie.

- En ce qui concerne le clonage d'applications dans les environnements OpenShift, Astra Control Center doit permettre à OpenShift de monter des volumes et de modifier la propriété des fichiers. Pour modifier la export policy ONTAP pour permettre ces opérations, lancer les commandes suivantes :

```
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -superuser sys
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -anon 65534
```

> Pour ajouter un deuxième environnement opérationnel OpenShift comme ressource de calcul gérée, assurez-vous que la fonctionnalité de snapshot de volume Astra Trident est activée. Pour activer et tester des copies Snapshot de volume avec Astra Trident, consultez le responsable "Instructions d'Astra Trident".

- A "Classe VolumeSnapClass" Doit être configuré sur tous les clusters Kubernetes à partir de l'emplacement de gestion des applications. Ceci peut également inclure le cluster K8s sur lequel Astra Control Center est installé. Astra Control Center peut gérer les applications du cluster K8s sur lequel il est exécuté.

De gestion des applications

- **Licence.** pour gérer des applications à l'aide d'Astra Control Center, vous avez besoin d'une licence Astra Control Center.
- **Espaces de noms.** Un espace de noms est la plus grande entité qui peut être gérée en tant qu'application par Astra Control Center. Vous pouvez choisir de filtrer les composants en fonction des étiquettes d'application et des étiquettes personnalisées dans un espace de noms existant et de gérer un sous-ensemble de ressources en tant qu'application.
- **StorageClass.** si vous installez une application avec une classe de stockage définie explicitement et que vous devez cloner l'application, le cluster cible pour l'opération de clonage doit avoir la classe de stockage spécifiée à l'origine. Le clonage d'une application avec une classe de stockage explicitement définie vers un cluster ne présentant pas la même classe de stockage échoue.
- **Ressources Kubernetes.** les applications qui utilisent des ressources Kubernetes non capturées par Astra Control peuvent ne pas disposer de fonctionnalités complètes de gestion des données d'application. Astra Control peut capturer les ressources Kubernetes suivantes :

Ressources Kubernetes		
ClusterRole	ClusterRoleBinding	ConfigMap
CustomResourceDefinition	Ressource CustomResource	Cronjob
Ensemble de démonstrations	HorizontalPodAutoscaler	Entrée
Déploiement.Config	MutatingWebhook	Demande de volume persistant
Pod	PodPetitionBudget	PodTemplate
Stratégie réseau	Et de réplication	Rôle
RoleBinding	Itinéraire	Secret
ValidétingWebhook		

Installez Astra Control Center à l'aide d'OpenShift OperatorHub

La procédure suivante permet d'installer Astra Control Center à l'aide de Red Hat OperatorHub. Dans cette solution, Astra Control Center est installé sur un cluster OpenShift bare-Metal exécuté sur FlexPod.

1. Téléchargez le pack Astra Control Center (`astra-control-center-[version].tar.gz`) du "Site de support NetApp".
2. Téléchargez le fichier .zip pour les certificats et clés Astra Control Center à partir du "Site de support NetApp".
3. Vérifiez la signature du lot.

```
openssl dgst -sha256 -verify astra-control-center[version].pub
-signature <astra-control-center[version].sig astra-control-
center[version].tar.gz
```

4. Extraire les images Astra.

```
tar -vxzf astra-control-center-[version].tar.gz
```

5. Passez au répertoire Astra.

```
cd astra-control-center-[version]
```

6. Ajoutez les images à votre registre local.

```
For Docker:
docker login [your_registry_path]OR
For Podman:
podman login [your_registry_path]
```

7. Utilisez le script approprié pour charger les images, les marquer et les pousser dans votre registre local.

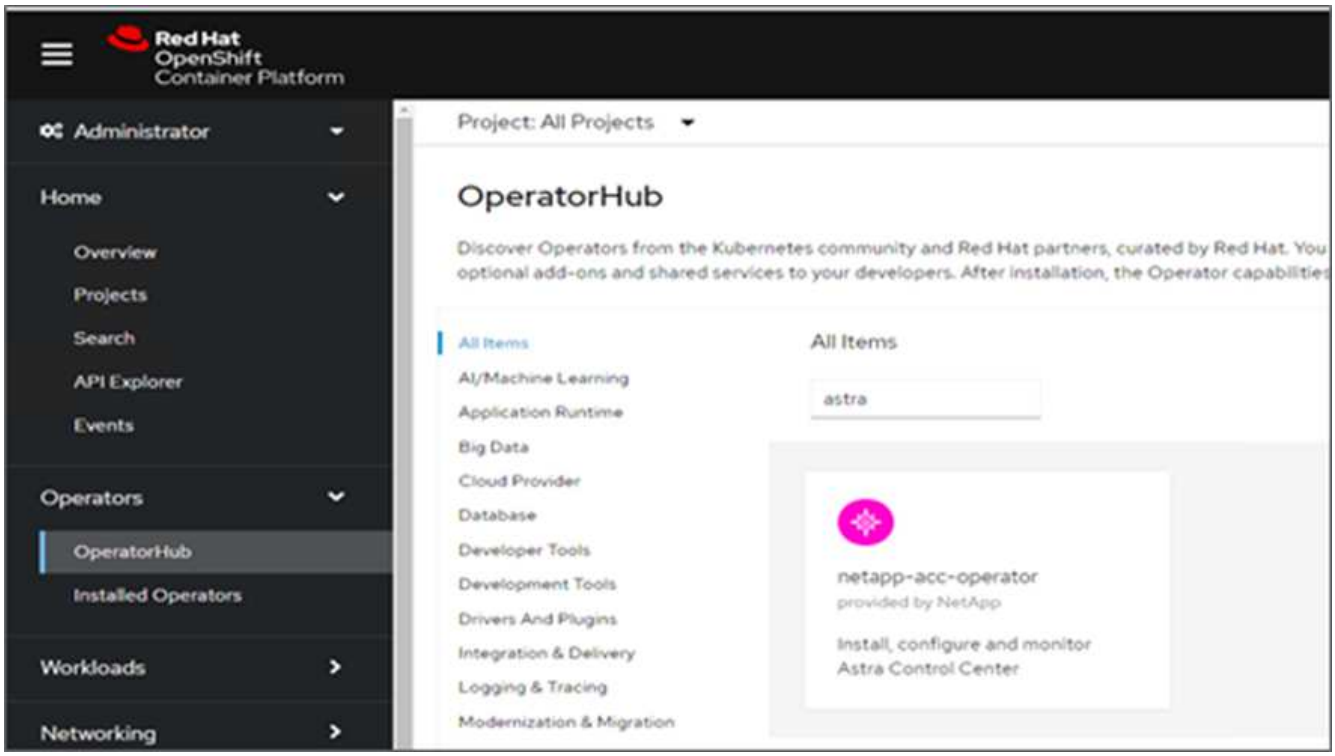
   Pour Docker :

```
export REGISTRY=[Docker_registry_path]
for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded image trimming
the 'Loaded images: '
  astraImage=$(docker load --input ${astraImageFile} | sed 's/Loaded
image: //')
  astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
  # Tag with local image repo.
  docker tag ${astraImage} ${REGISTRY}/${astraImage}
  # Push to the local repo.
  docker push ${REGISTRY}/${astraImage}
done
```

   Pour Podman :

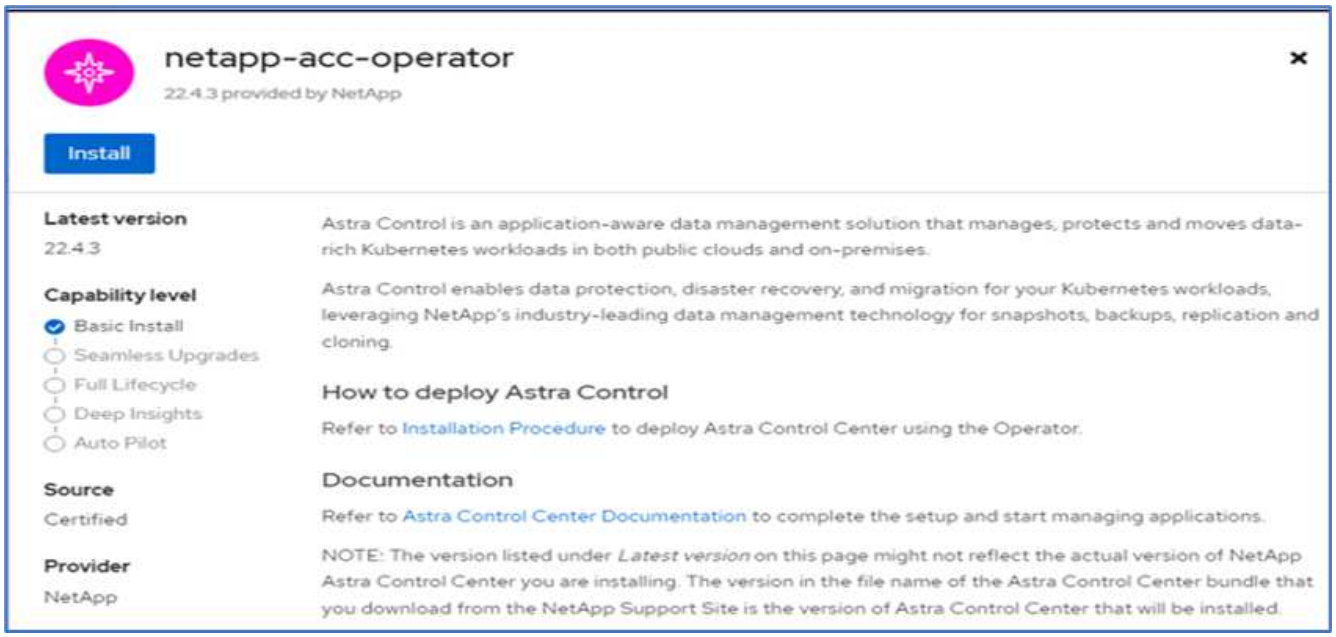
```
export REGISTRY=[Registry_path]
for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded image trimming
the 'Loaded images: '
  astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //')
  astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
  # Tag with local image repo.
  podman tag ${astraImage} ${REGISTRY}/${astraImage}
  # Push to the local repo.
  podman push ${REGISTRY}/${astraImage}
done
```

8. Connectez-vous à la console web du cluster OpenShift sans système d'exploitation. Dans le menu latéral, sélectionnez opérateurs > OperatorHub. Entrez `astra` pour afficher la liste `netapp-acc-operator`.

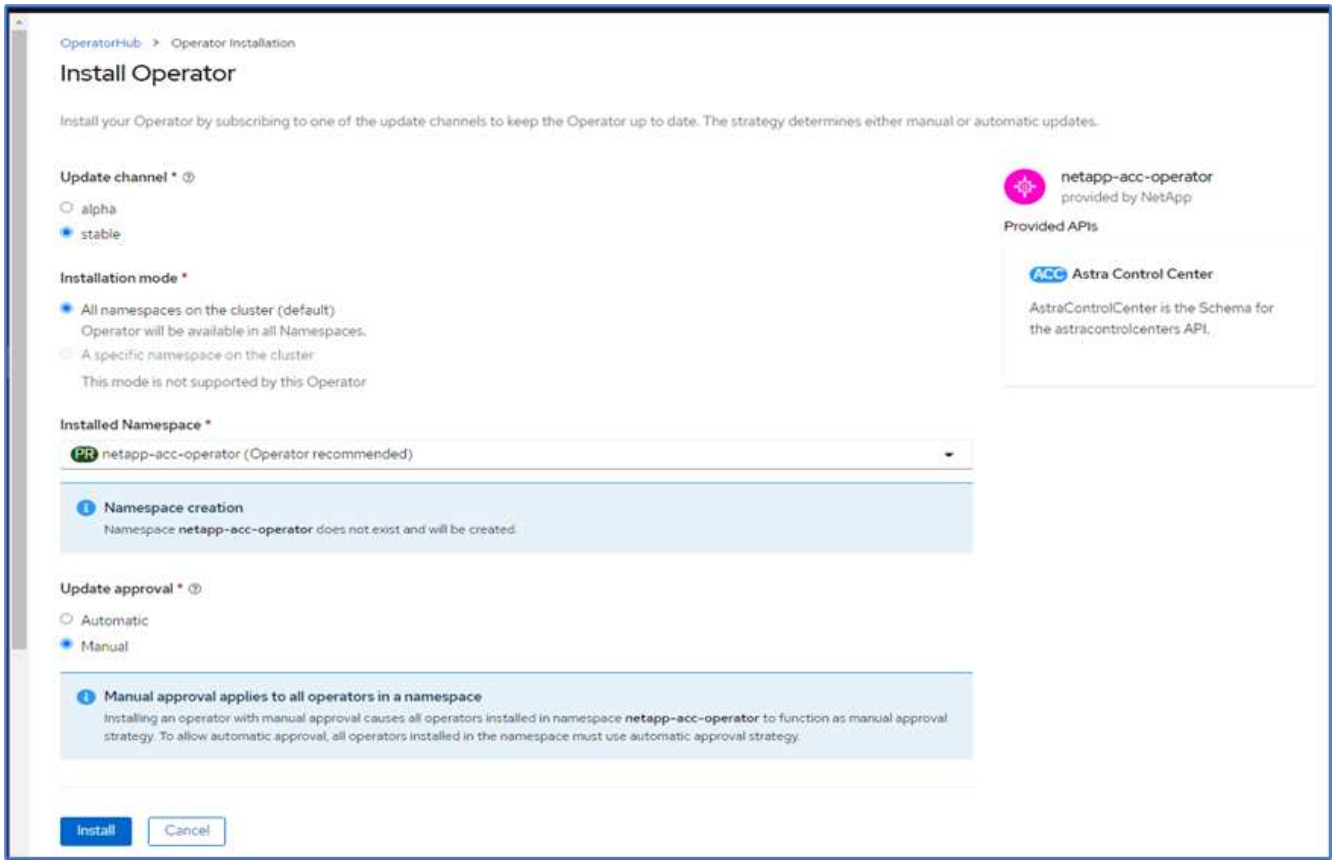


> `netapp-acc-operator` Est un opérateur Red Hat OpenShift certifié. Il est répertorié dans le catalogue OperatorHub.

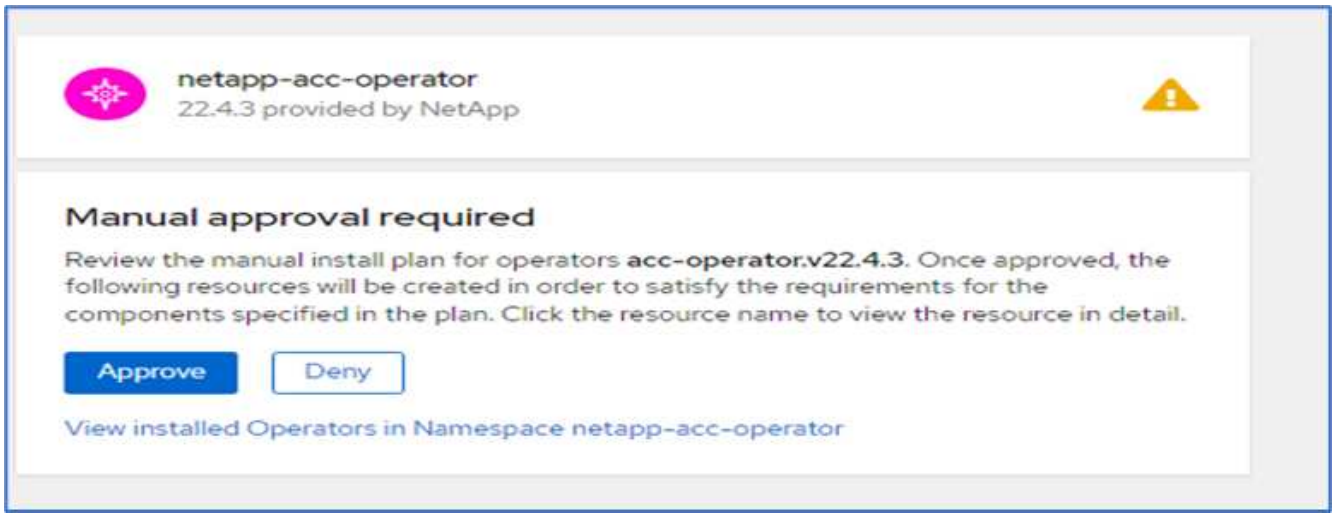
9. Sélectionnez `netapp-acc-operator` Cliquez ensuite sur installation.



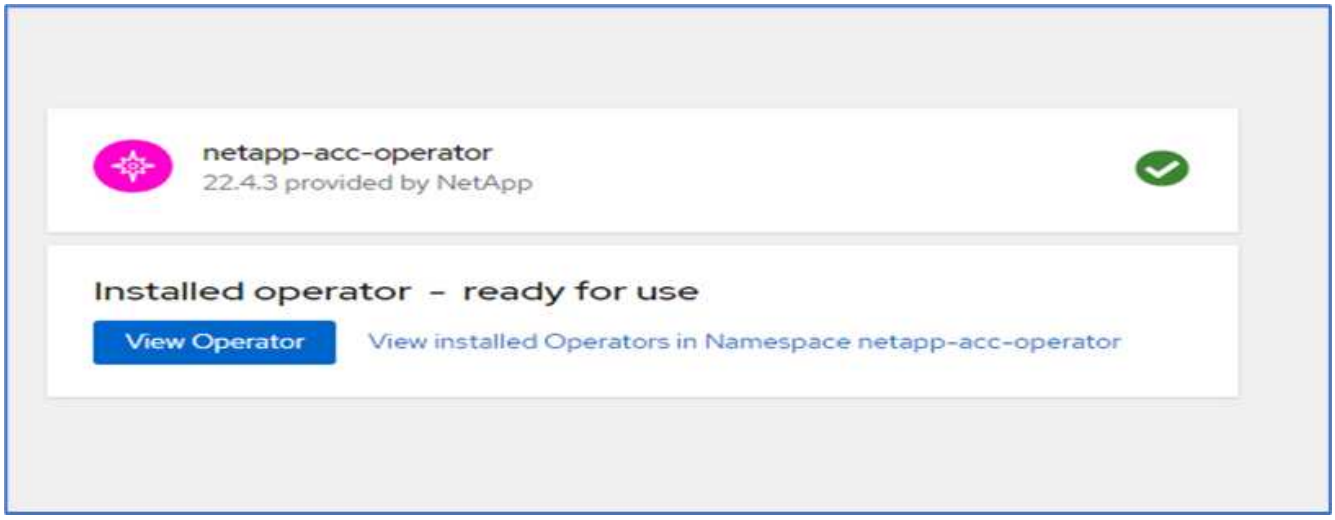
10. Sélectionnez les options appropriées et cliquez sur installer.



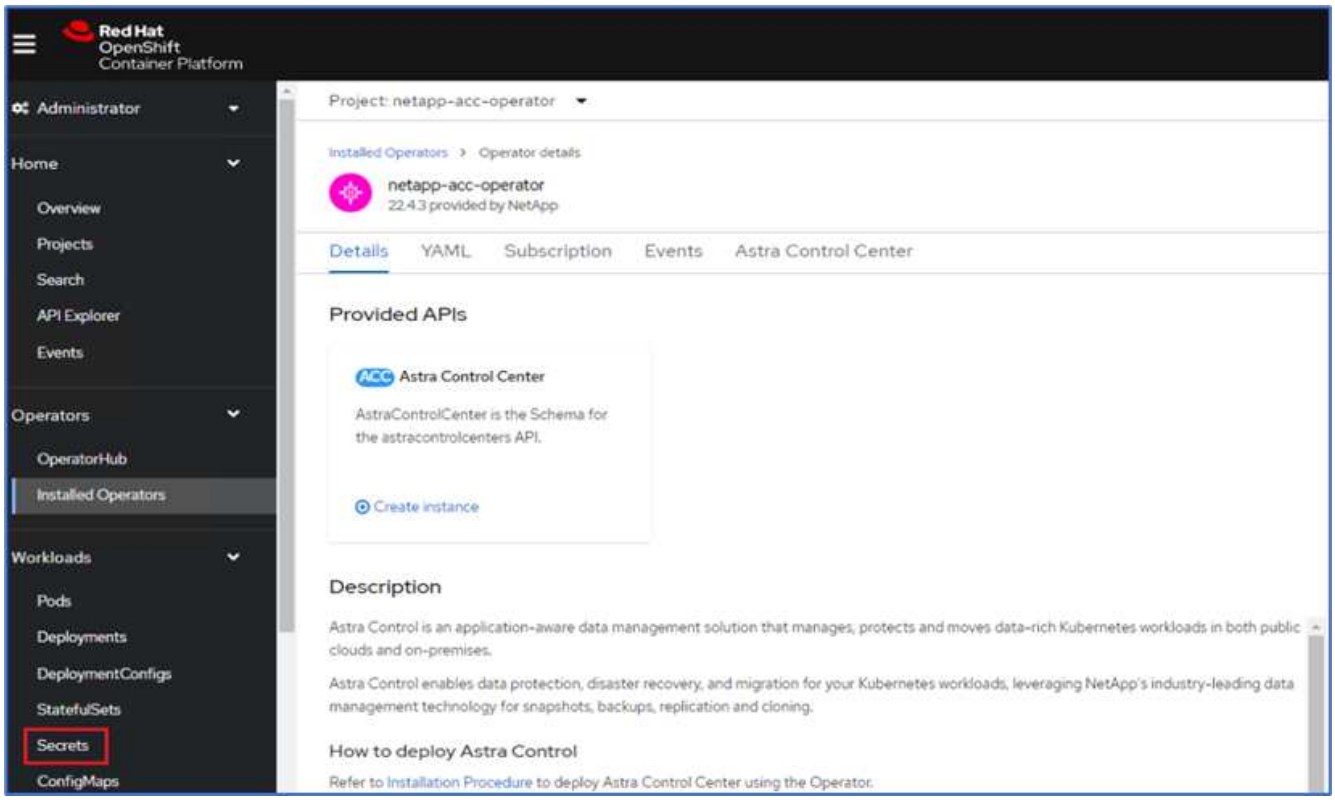
11. Approuver l'installation et attendre que l'opérateur soit installé.



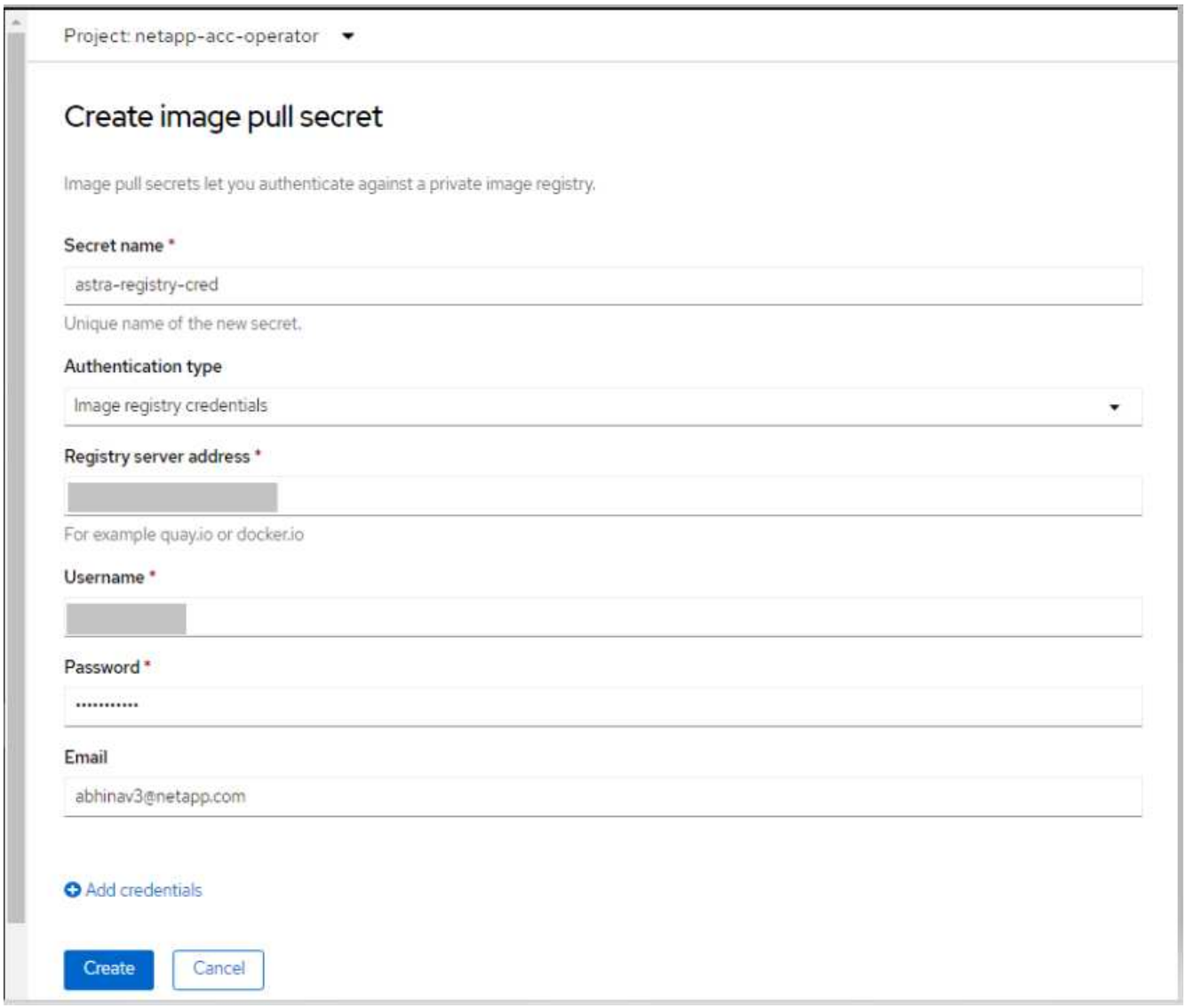
12. À ce stade, l'opérateur est installé avec succès et prêt à l'emploi. Cliquez sur Afficher l'opérateur pour démarrer l'installation du centre de contrôle Astra.



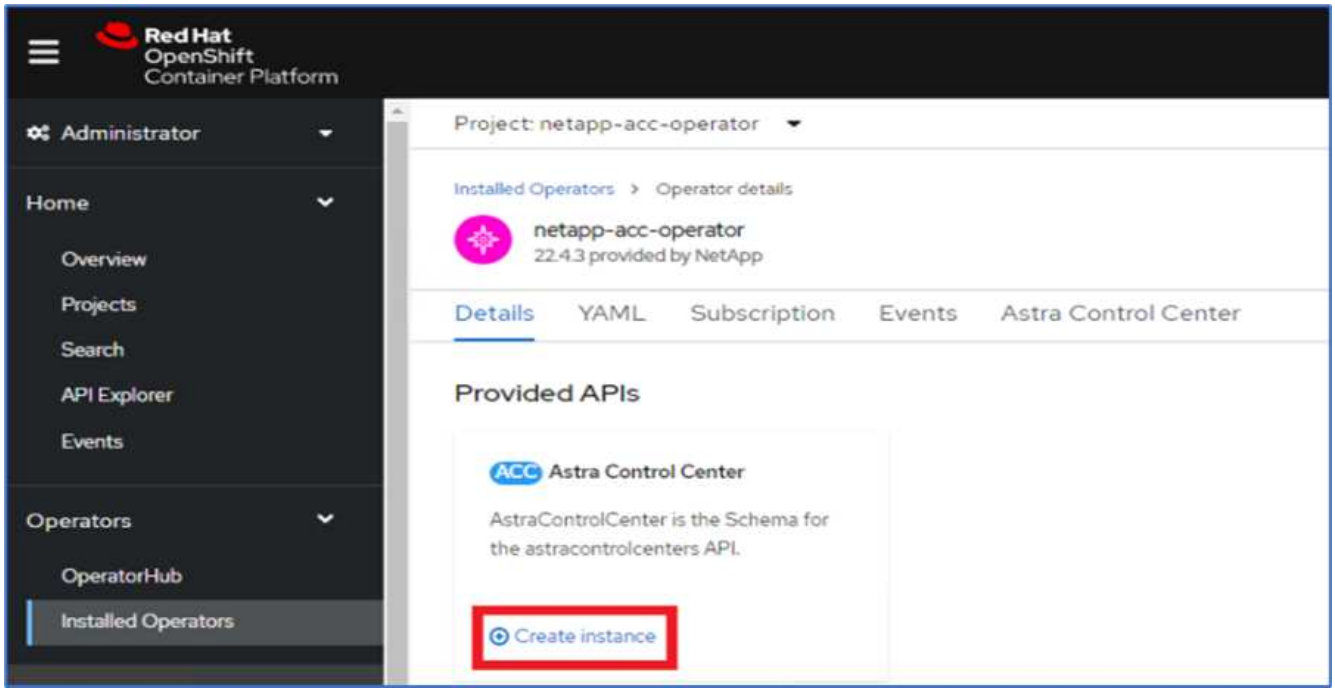
13. Avant d'installer Astra Control Center, créez le secret pour télécharger des images Astra à partir du registre Docker que vous avez poussé plus tôt.



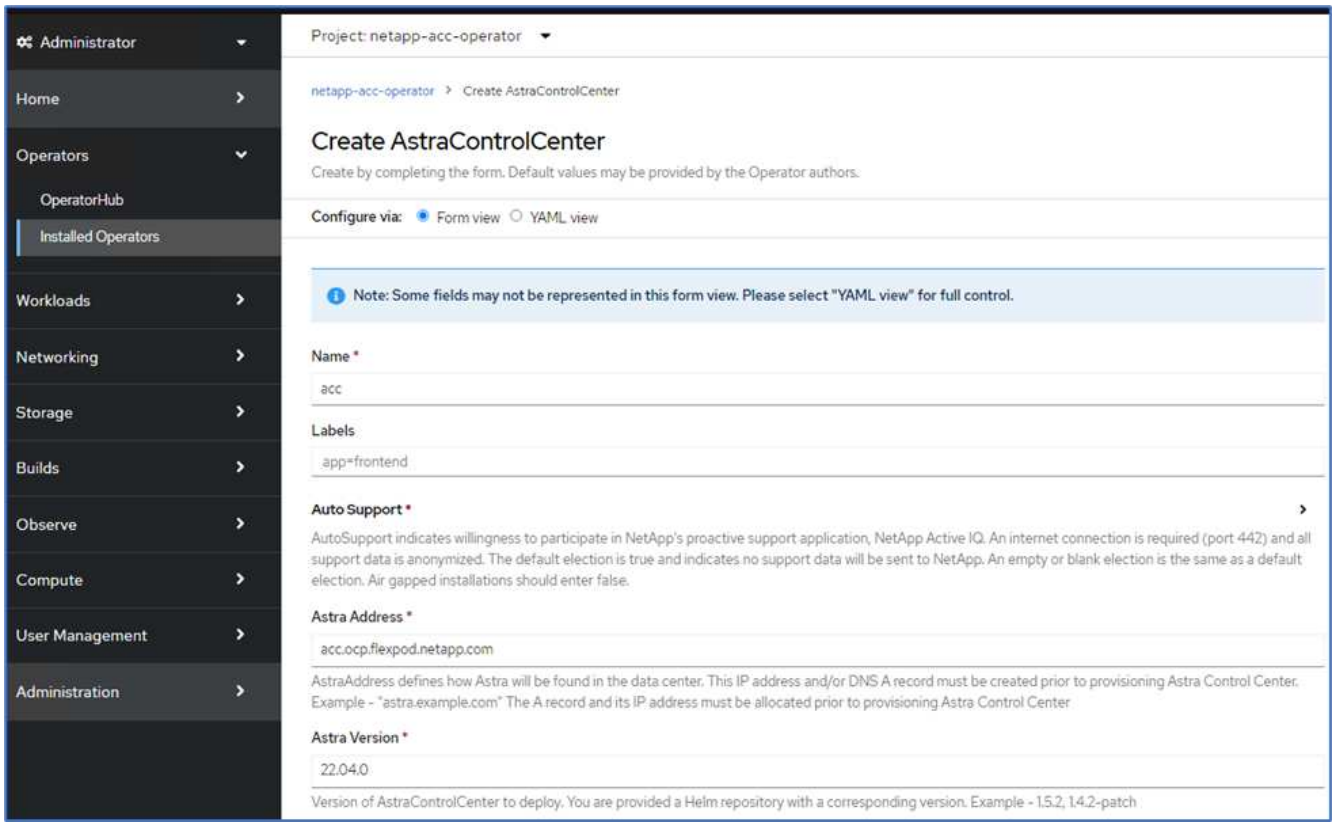
14. Pour extraire les images du centre de contrôle Astra de votre repo privé Docker, créez un secret dans le `netapp-acc-operator` espace de noms. Ce nom secret est fourni dans le manifeste YAML du Centre de contrôle Astra dans une étape ultérieure.



15. Dans le menu latéral, sélectionnez opérateurs > opérateurs installés et cliquez sur Créer une instance dans la section API fournie.



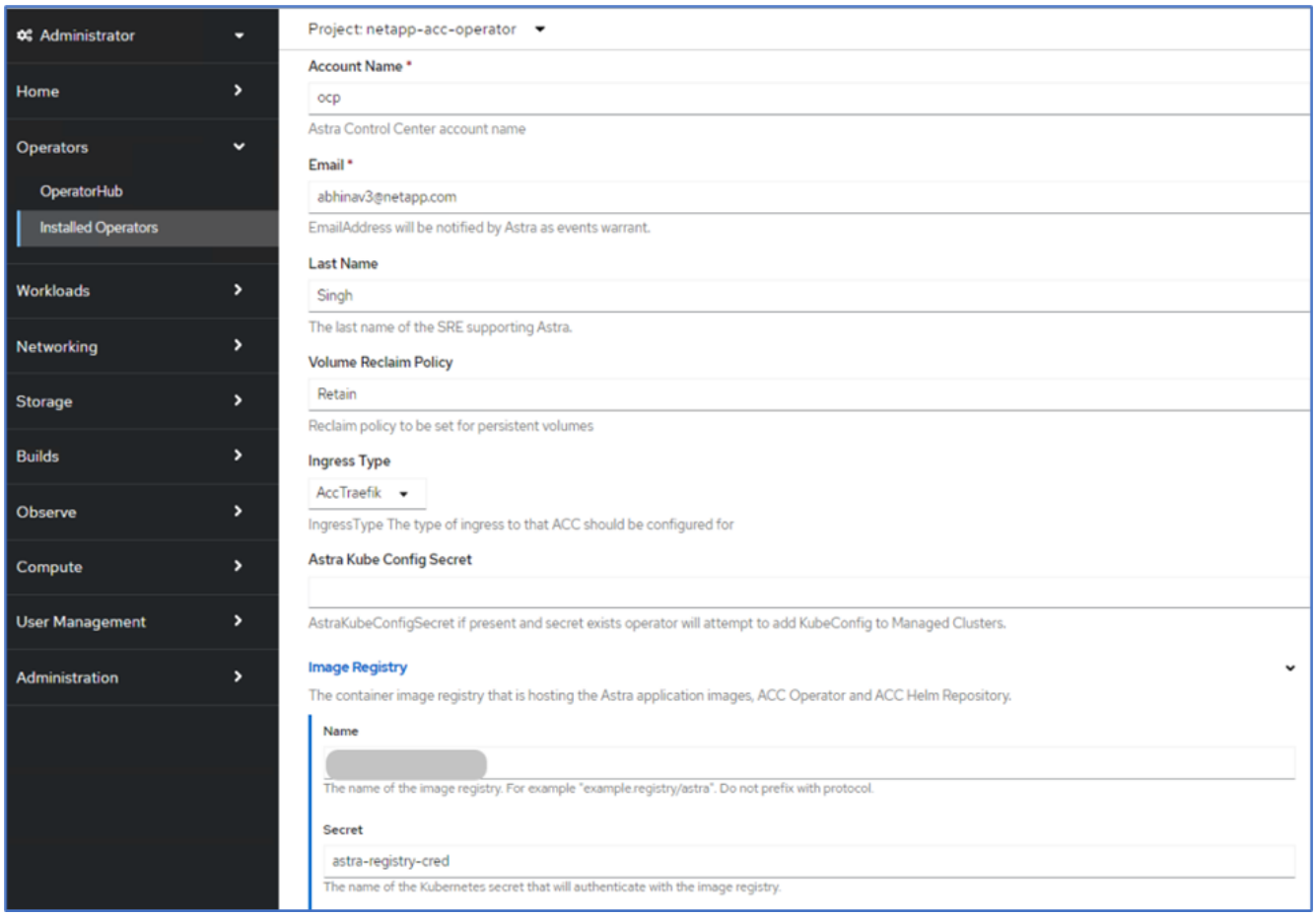
16. Remplissez le formulaire Create AstrakControlCenter. Indiquez le nom, l'adresse Astra et la version Astra.



> Sous adresse Astra, indiquez l'adresse FQDN pour Astra Control Center. Cette adresse permet d'accéder à la console Web Astra Control Center. Le FQDN doit également se résoudre à un réseau IP accessible et doit être configuré dans le DNS.

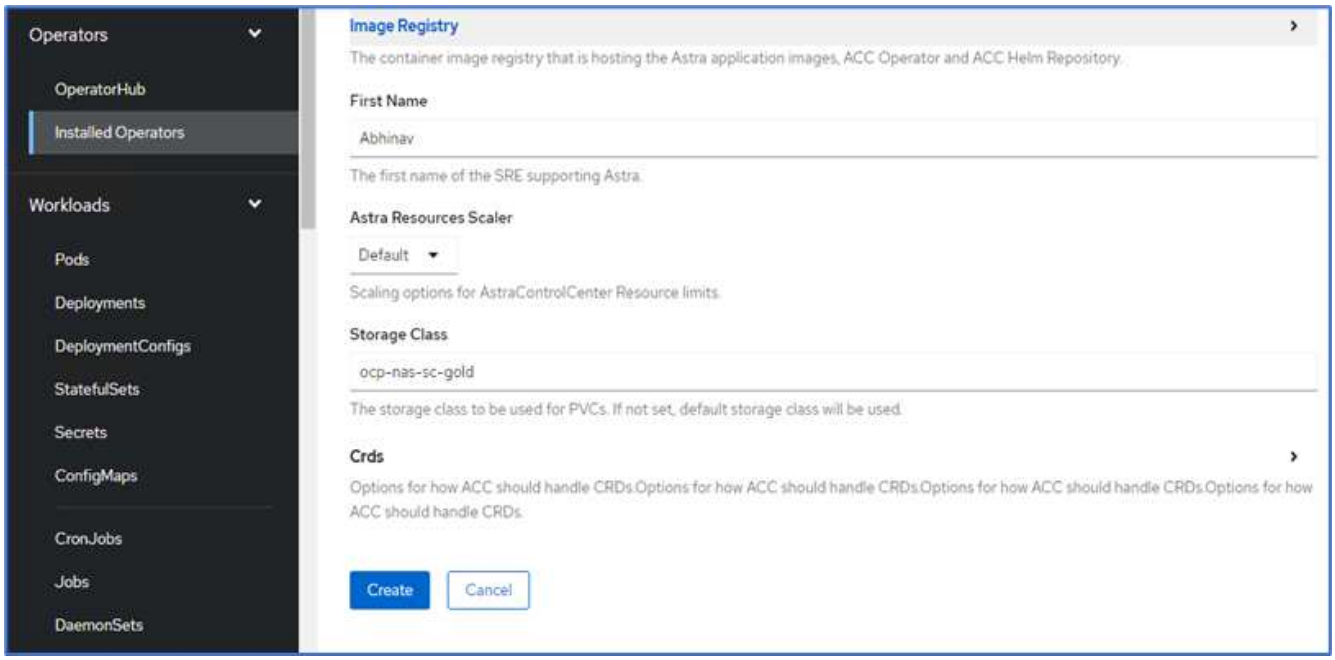
17. Entrez un nom de compte, une adresse e-mail, un nom d'administrateur et conservez la stratégie de récupération du volume par défaut. Si vous utilisez un équilibreur de charge, définissez le Type d'entrée

sur `AccTraefik`. Sinon, sélectionnez générique pour `Ingress.Controller`. Sous Registre d'images, entrez le chemin et le secret du registre d'images du conteneur.

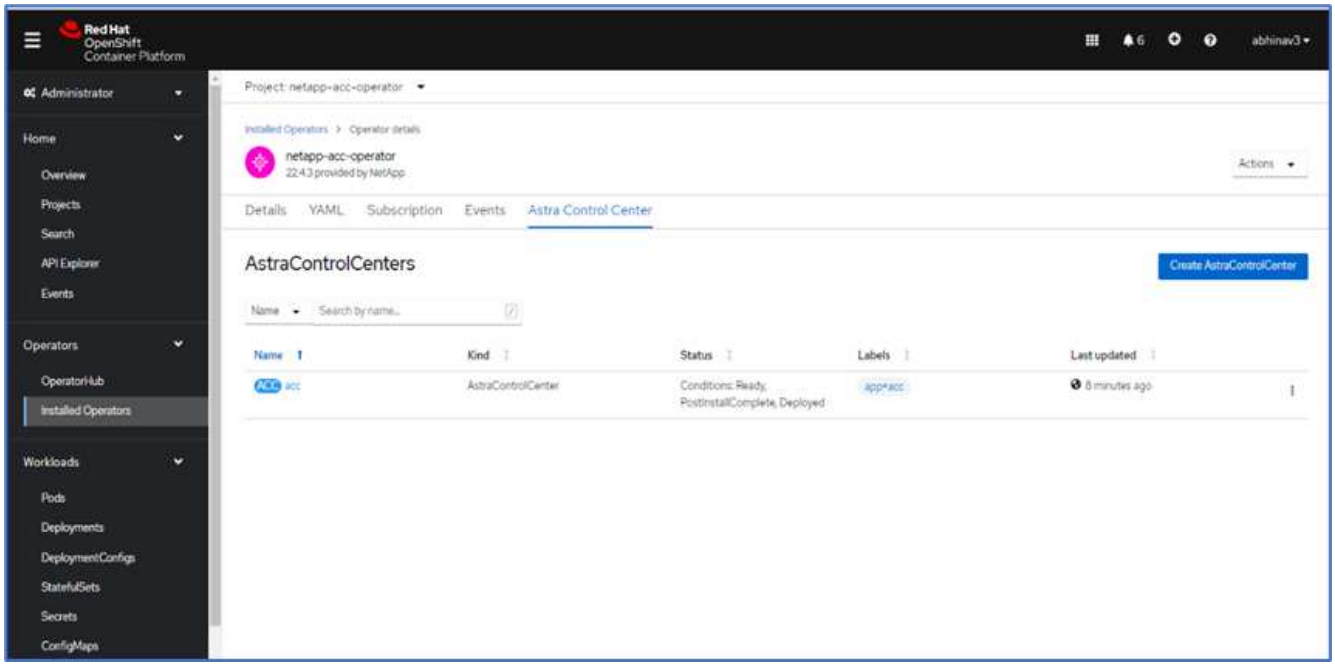


> Dans cette solution, l'équilibreur de charge Metallb est utilisé. Par conséquent, le type d'entrée est AccTraefik. Cela expose la passerelle Ttrafik Astra Control Center en tant que service Kubernetes de type LoadBalancer.

18. Entrez le prénom de l'administrateur, configurez la mise à l'échelle des ressources et fournissez la classe de stockage. Cliquez sur Créer .



L'état de l'instance Astra Control Center doit passer de déploiement à prêt.



19. Vérifiez que tous les composants du système ont été correctement installés et que tous les modules fonctionnent.

```
root@abhinav-ansible# oc get pods -n netapp-acc-operator
NAME                                                READY   STATUS
RESTARTS   AGE
acc-helm-repo-77745b49b5-7zg2v                      1/1     Running   0
10m
acc-operator-controller-manager-5c656c44c6-tqnmn    2/2     Running   0
13m
```

```
activity-589c6d59f4-x2sfs                          1/1     Running   0
6m4s
api-token-authentication-4q5lj                     1/1     Running   0
5m26s
api-token-authentication-pzptd                     1/1     Running   0
5m27s
api-token-authentication-tbtg6                     1/1     Running   0
5m27s
asup-669df8d49-qps54                               1/1     Running   0
5m26s
authentication-5867c5f56f-dnpp2                    1/1     Running   0
3m54s
bucketservice-85495bc475-5zcc5                     1/1     Running   0
5m55s
cert-manager-67f486bbc6-txhh6                      1/1     Running   0
9m5s
cert-manager-cainjector-75959db744-4l5p5           1/1     Running   0
9m6s
cert-manager-webhook-765556b869-g6wdf              1/1     Running   0
9m6s
cloud-extension-5d595f85f-txrfl                    1/1     Running   0
5m27s
cloud-insights-service-674649567b-5s4wd            1/1     Running   0
5m49s
composite-compute-6b58d48c69-46vhc                 1/1     Running   0
6m11s
composite-volume-6d447fd959-chnrt                  1/1     Running   0
5m27s
credentials-66668f8ddd-8qc5b                       1/1     Running   0
7m20s
entitlement-fd6fc5c58-wxnmh                        1/1     Running   0
6m20s
features-756bbb7c7c-rgcrm                          1/1     Running   0
5m26s
fluent-bit-ds-278pg                                1/1     Running   0
3m35s
fluent-bit-ds-5pqc6                                1/1     Running   0
3m35s
fluent-bit-ds-8l7cq                                1/1     Running   0
3m35s
fluent-bit-ds-9qbft                                1/1     Running   0
3m35s
fluent-bit-ds-nj475                                1/1     Running   0
3m35s
fluent-bit-ds-x9pd8                                1/1     Running   0
3m35s
```

```
graphql-server-698d6f4bf-kftwc                    1/1     Running   0
3m20s
identity-5d4f4c87c9-wjz6c                         1/1     Running   0
6m27s
influxdb2-0                                       1/1     Running   0
9m33s
krakend-657d44bf54-8cb56                          1/1     Running   0
3m21s
license-594bbdc-rghdg                             1/1     Running   0
6m28s
login-ui-6c65fbbbd4-jg8wz                         1/1     Running   0
3m17s
loki-0                                            1/1     Running   0
9m30s
metrics-facade-75575f69d7-hnlk6                   1/1     Running   0
6m10s
monitoring-operator-65dff79cfb-z78vk              2/2     Running   0
3m47s
nats-0                                            1/1     Running   0
10m
nats-1                                            1/1     Running   0
9m43s
nats-2                                            1/1     Running   0
9m23s
nautilus-7bb469f857-4hlc6                         1/1     Running   0
6m3s
nautilus-7bb469f857-vz94m                         1/1     Running   0
4m42s
openapi-8586db4bcd-gwwvf                          1/1     Running   0
5m41s
packages-6bdb949cfb-nrq8l                         1/1     Running   0
6m35s
polaris-consul-consul-server-0                    1/1     Running   0
9m22s
polaris-consul-consul-server-1                    1/1     Running   0
9m22s
polaris-consul-consul-server-2                    1/1     Running   0
9m22s
polaris-mongodb-0                                 2/2     Running   0
9m22s
polaris-mongodb-1                                 2/2     Running   0
8m58s
polaris-mongodb-2                                 2/2     Running   0
8m34s
polaris-ui-5df7687dbd-trcnf                       1/1     Running   0
3m18s
```

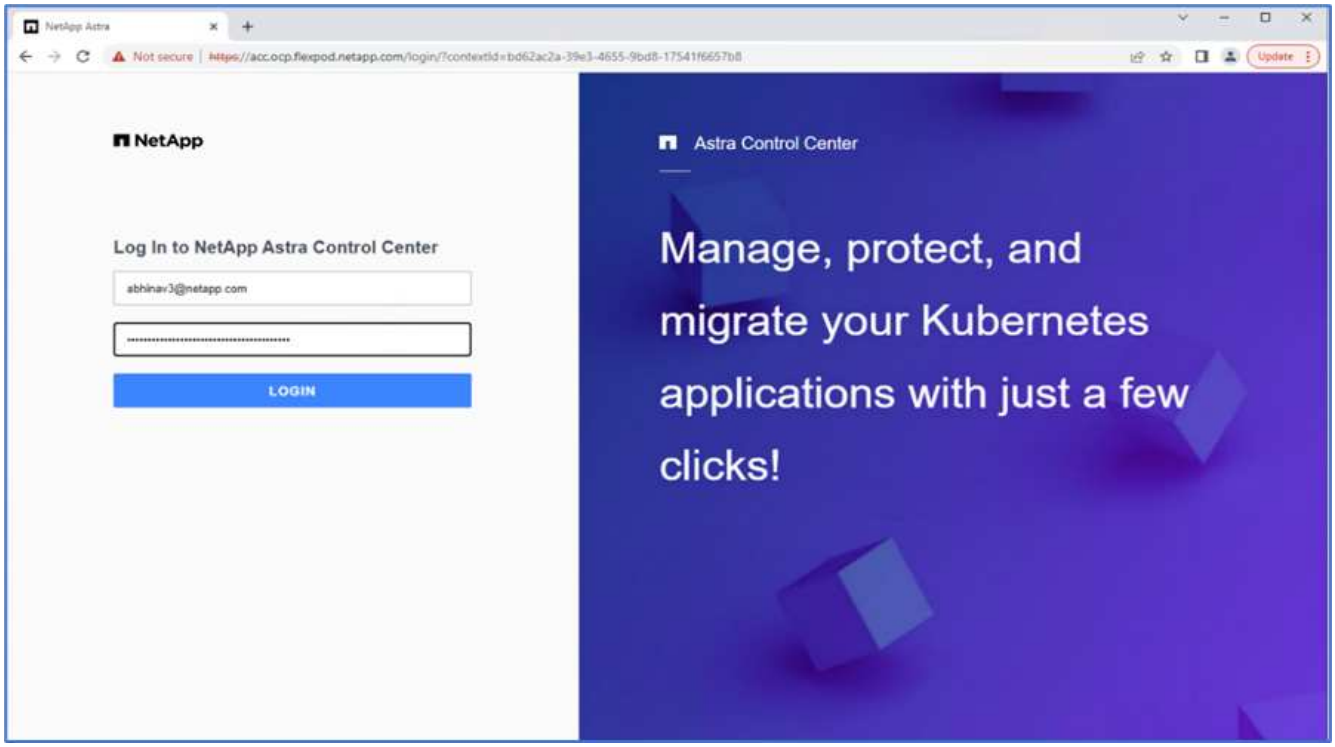
```
polaris-vault-0                                     1/1     Running   0
9m18s
polaris-vault-1                                     1/1     Running   0
9m18s
polaris-vault-2                                     1/1     Running   0
9m18s
public-metrics-7b96476f64-j88bw                     1/1     Running   0
5m48s
storage-backend-metrics-5fd6d7cd9c-vcb4j            1/1     Running   0
5m59s
storage-provider-bb85ff965-m7qrq                    1/1     Running   0
5m25s
telegraf-ds-4zqgz                                   1/1     Running   0
3m36s
telegraf-ds-cp9x4                                   1/1     Running   0
3m36s
telegraf-ds-h4n59                                   1/1     Running   0
3m36s
telegraf-ds-jnp2q                                   1/1     Running   0
3m36s
telegraf-ds-pdz5j                                   1/1     Running   0
3m36s
telegraf-ds-znqtp                                   1/1     Running   0
3m36s
telegraf-rs-rt64j                                   1/1     Running   0
3m36s
telemetry-service-7dd9c74bfc-sfkzt                  1/1     Running   0
6m19s
tenancy-d878b7fb6-wf8x9                             1/1     Running   0
6m37s
traefik-6548496576-5v2g6                            1/1     Running   0
98s
traefik-6548496576-g82pq                            1/1     Running   0
3m8s
traefik-6548496576-psn49                            1/1     Running   0
38s
traefik-6548496576-qrkfd                            1/1     Running   0
2m53s
traefik-6548496576-srs6r                            1/1     Running   0
98s
trident-svc-679856c67-78kbt                         1/1     Running   0
5m27s
vault-controller-747d664964-xmn6c                   1/1     Running   0
7m37s
```

Chaque pod doit avoir l'état en cours d'exécution. Le déploiement des modules du système peut prendre plusieurs minutes.

20. Lorsque tous les pods s'exécutent, exécutez la commande suivante pour récupérer le mot de passe à une seule fois. Dans la version YAML de la sortie, vérifiez le `status.deploymentState` pour la valeur déployée, puis copiez le `status.uuid` valeur. Le mot de passe est `ACC-` Suivi de la valeur UUID. (ACC-[UUID]).

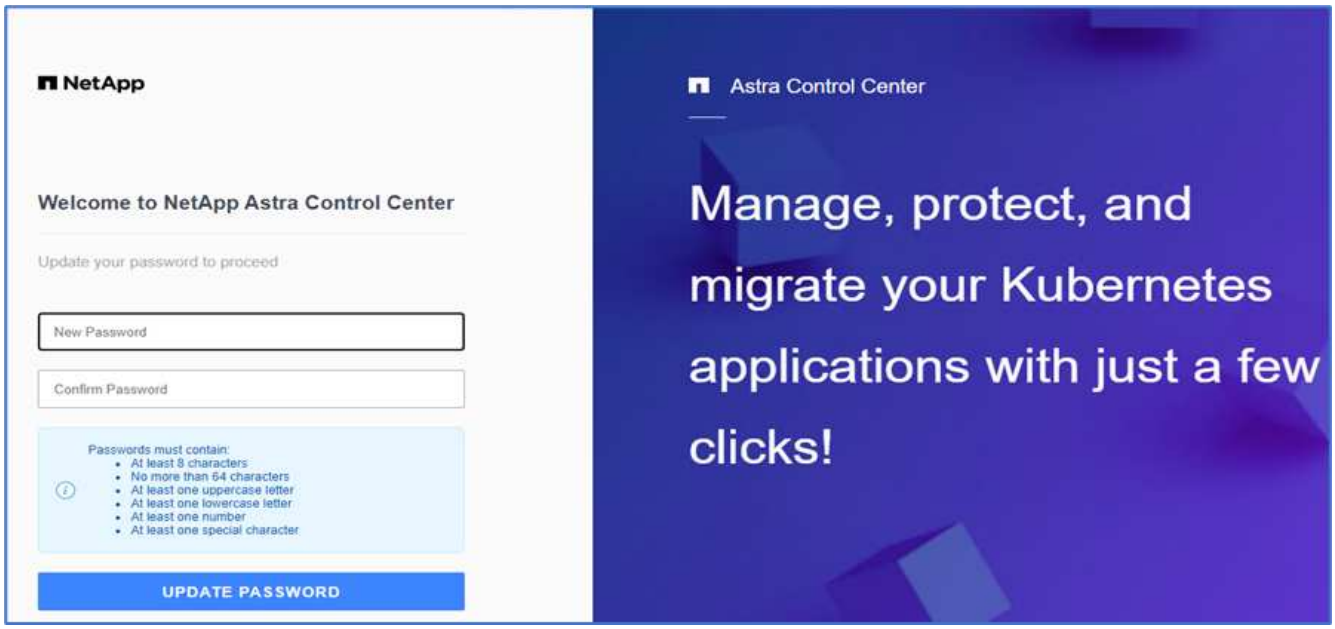
```
root@abhinav-ansible# oc get acc -o yaml -n netapp-acc-operator
```

21. Dans un navigateur, accédez à l'URL en utilisant le FQDN que vous avez fourni.
22. Connectez-vous à l'aide du nom d'utilisateur par défaut, à savoir l'adresse électronique fournie lors de l'installation et le mot de passe à usage unique ACC-[UUID].



Si vous saisissez trois fois un mot de passe incorrect, le compte administrateur est verrouillé pendant 15 minutes.

23. Modifiez le mot de passe et continuez.

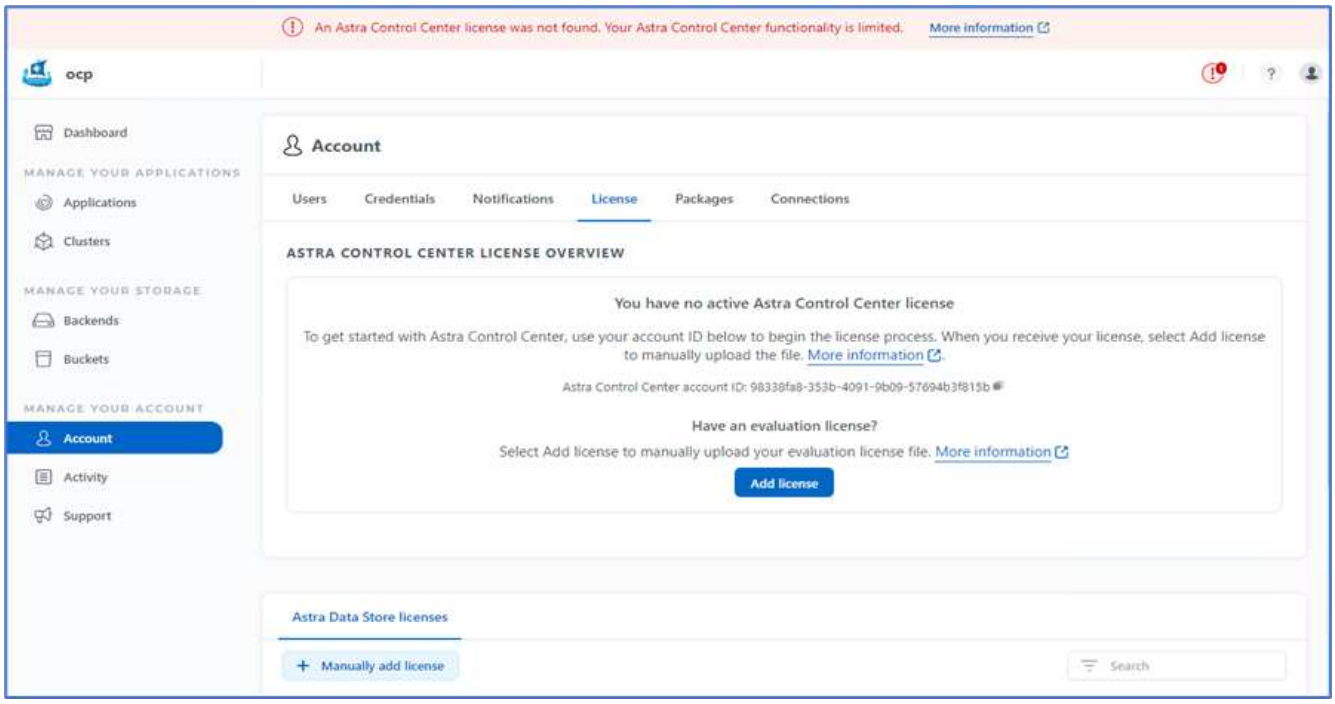


Pour en savoir plus sur l'installation du centre de contrôle Astra, consultez le "Présentation de l'installation du centre de contrôle Astra" page.

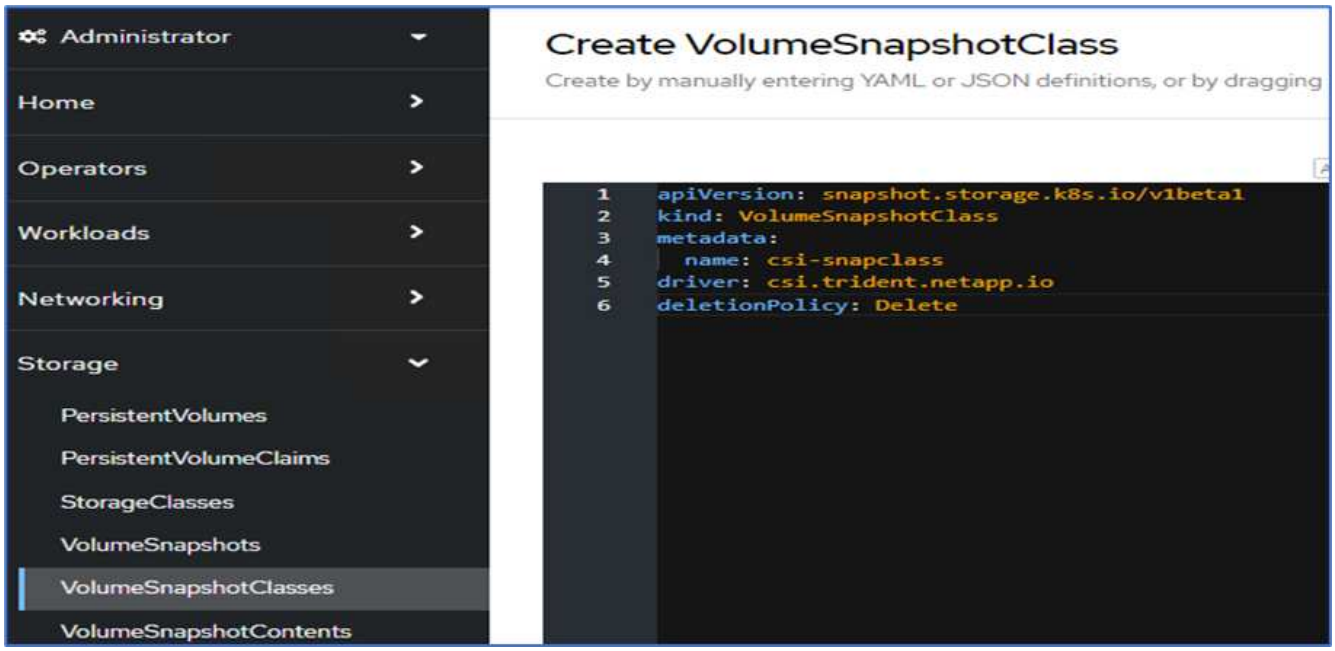
Configurer le centre de contrôle Astra

Une fois Astra Control Center installé, connectez-vous à l'interface utilisateur, téléchargez la licence, ajoutez des clusters, gérez le stockage et ajoutez des compartiments.

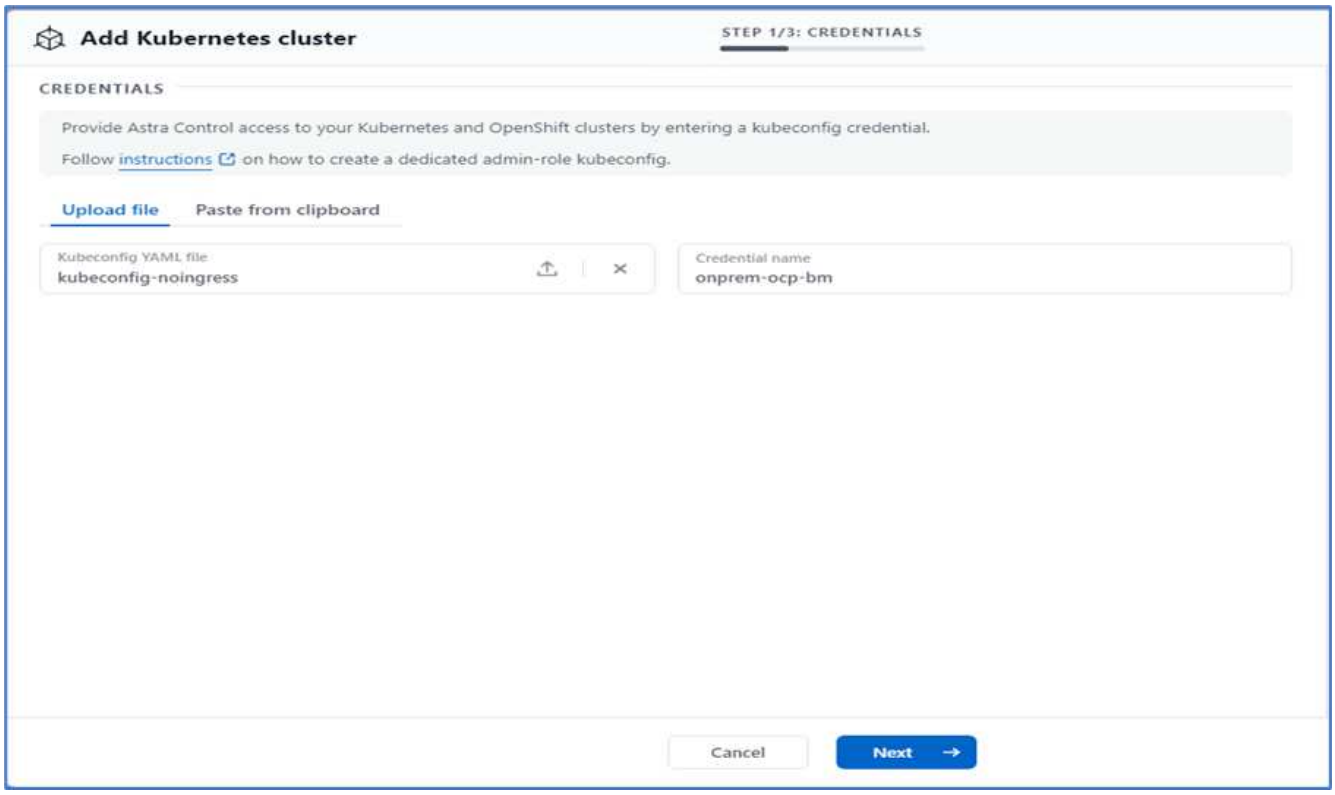
1. Sur la page d'accueil sous compte, accédez à l'onglet Licence et sélectionnez Ajouter une licence pour télécharger la licence Astra.



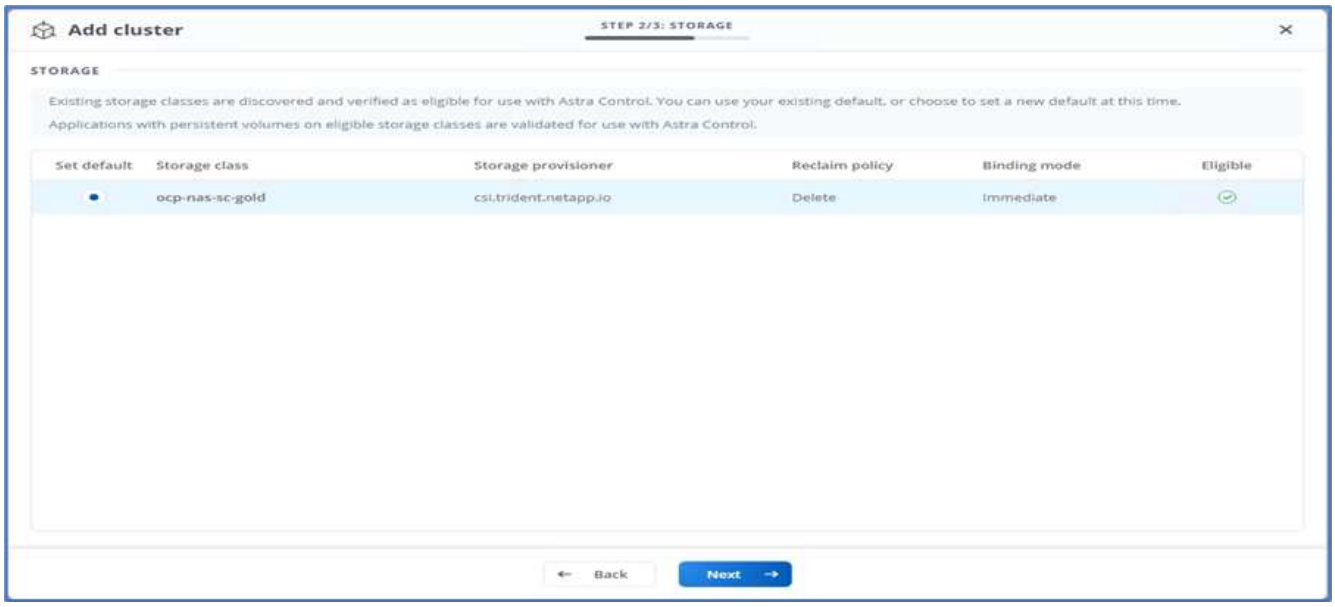
2. Avant d'ajouter le cluster OpenShift, créez une classe de snapshot de volume Astra Trident à partir de la console web OpenShift. La classe de snapshot de volume est configurée avec le `csi.trident.netapp.io` conducteur.



3. Pour ajouter le cluster Kubernetes, accédez à clusters sur la page d'accueil et cliquez sur Ajouter un cluster Kubernetes. Téléchargez ensuite le `kubeconfig` fichier du cluster et indiquez un nom d'identifiant. Cliquez sur Suivant.



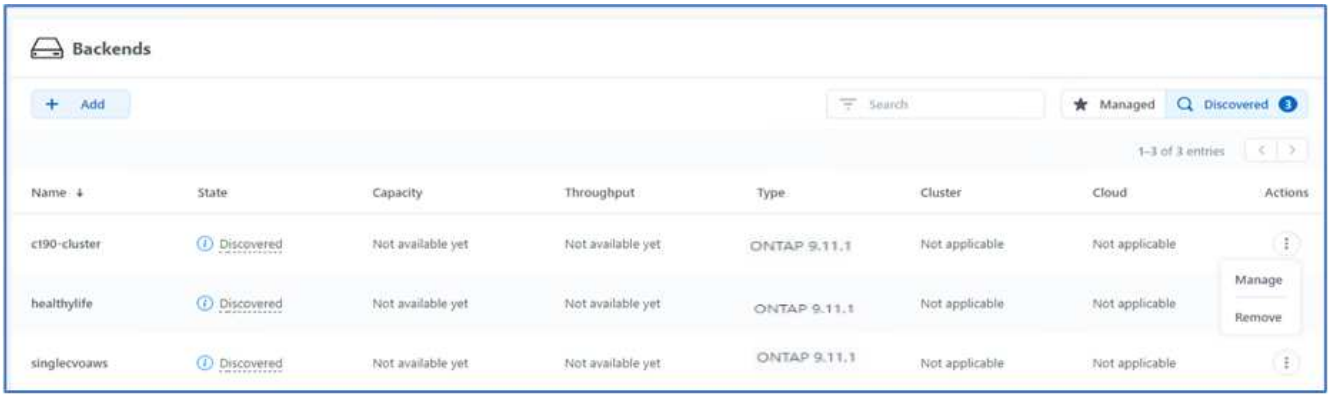
4. Les classes de stockage existantes sont automatiquement découvertes. Sélectionnez la classe de stockage par défaut, cliquez sur Suivant, puis sur Ajouter un cluster.



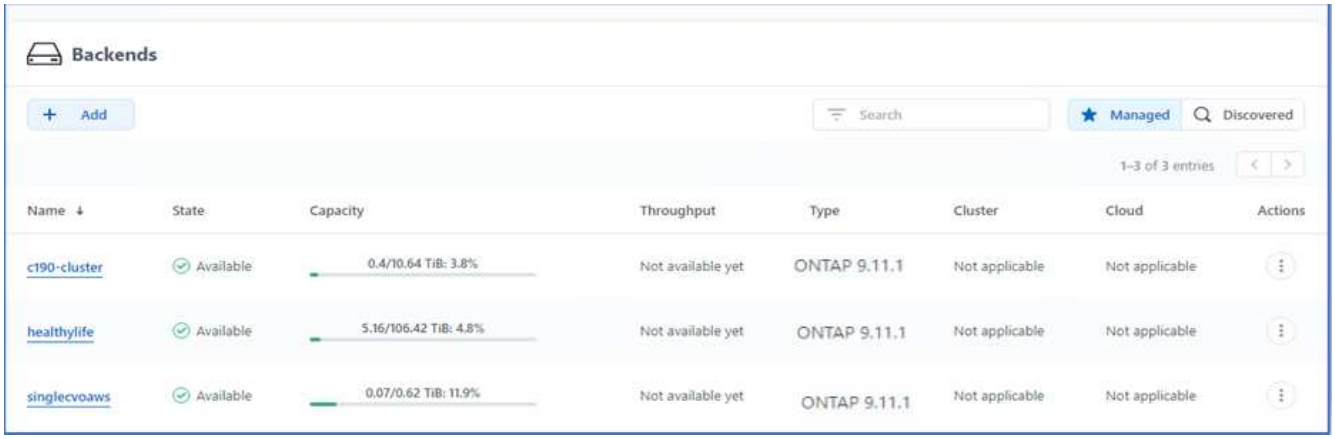
5. Le cluster est ajouté en quelques minutes. Pour ajouter d'autres clusters OpenShift Container Platform, répétez les étapes 1 à 4.

> Pour ajouter un environnement opérationnel OpenShift supplémentaire en tant que ressource de calcul gérée, assurez-vous qu'Astra Trident "Objets VolumeSnapshotClass" sont définis.

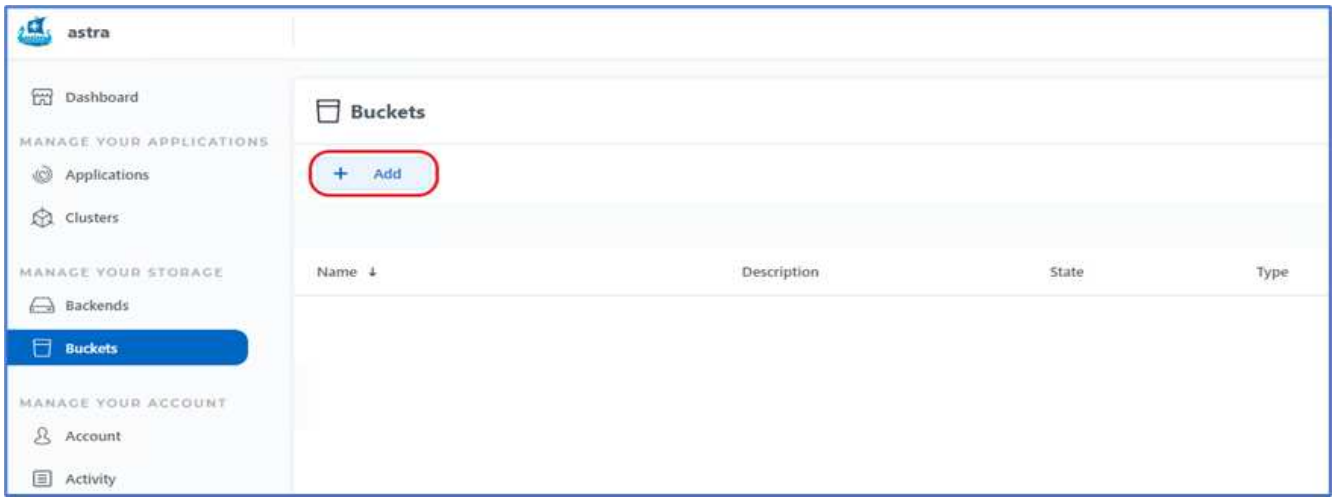
6. Pour gérer le stockage, accédez à Backends, cliquez sur les trois points sous actions par rapport au back-end que vous souhaitez gérer. Cliquez sur gérer.



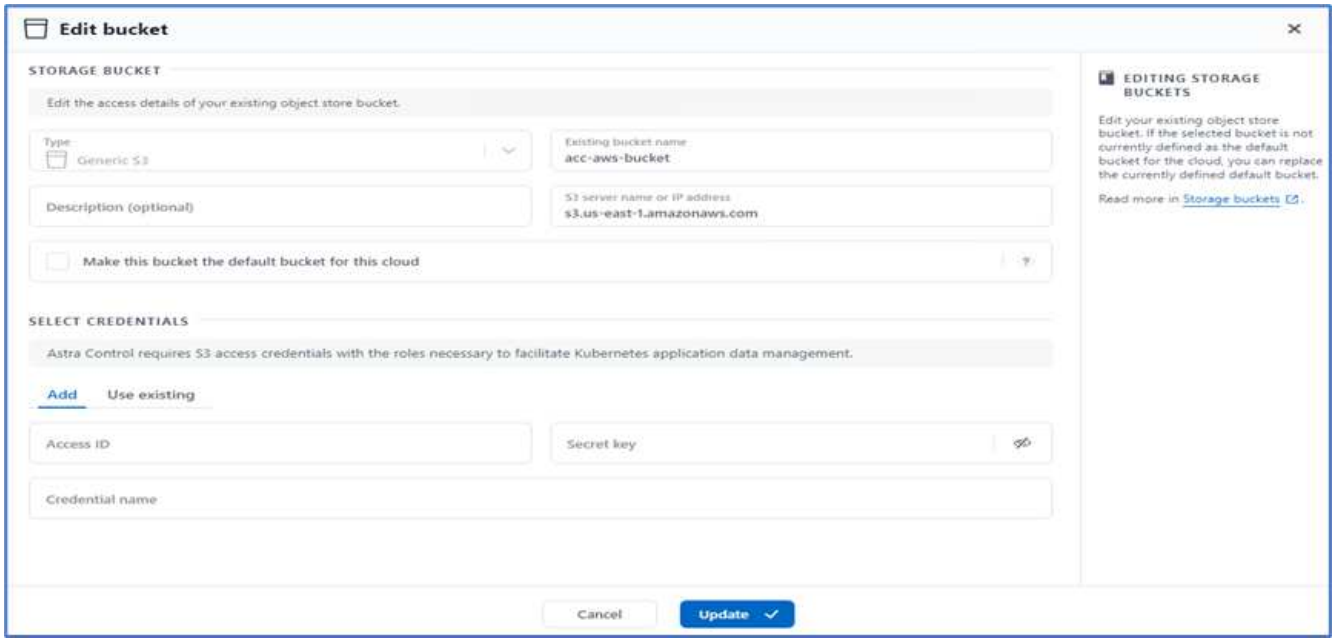
7. Indiquez les identifiants ONTAP et cliquez sur Next (Suivant). Vérifiez les informations et cliquez sur géré. Le système back-end doit être semblable à l'exemple suivant.



8. Pour ajouter un godet à la commande Astra, sélectionnez godets et cliquez sur Ajouter.

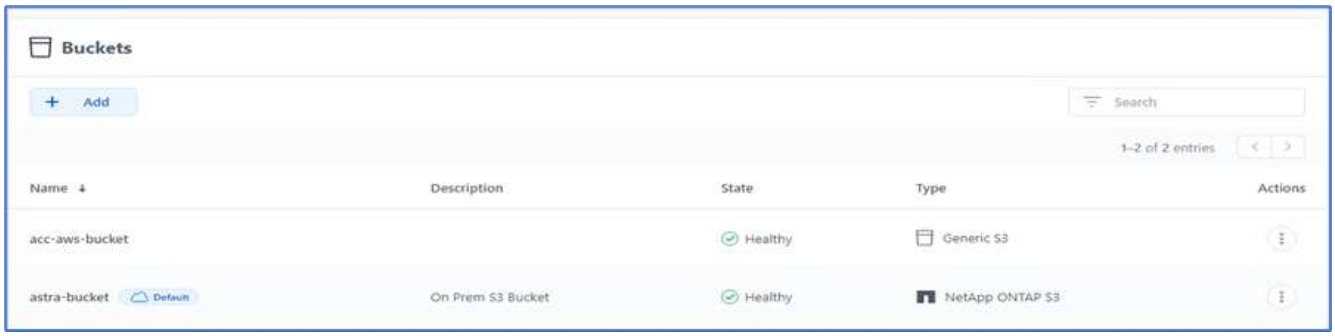


9. Sélectionnez le type de compartiment et indiquez le nom du compartiment, le nom du serveur S3 ou l'adresse IP et les identifiants S3. Cliquez sur mettre à jour.



Dans cette solution, des compartiments AWS S3 et ONTAP S3 sont tous deux utilisés. Vous pouvez également utiliser StorageGRID.

L'état du godet doit être sain.



Dans le cadre de l'enregistrement de clusters Kubernetes avec Astra Control Center pour la gestion des données intégrant la cohérence applicative, Astra Control crée automatiquement des liaisons de rôles et un espace de noms de contrôle NetApp qui contrôle la collecte de metrics et de journaux à partir des pods d'applications et des nœuds workers. Définir l'une des classes de stockage ONTAP par défaut prises en charge.

Après vous "Ajoutez un cluster à la gestion Astra Control", Vous pouvez installer des applications sur le cluster (en dehors d'Astra Control), puis aller à la page applications d'Astra Control pour gérer les applications et leurs ressources. Pour en savoir plus sur la gestion des applications avec Astra, consultez le "Besoins en termes de gestion des applications".

"Ensuite : présentation de la validation de la solution."

Validation des solutions

Présentation

"Précédent : installation d'Astra Control Center sur OpenShift Container Platform."

Dans cette section, nous revisiterons la solution en incluant quelques cas d'utilisation :

- Restauration d'une application avec état d'une sauvegarde à distance vers un autre cluster OpenShift exécuté dans le cloud.
- Restauration d'une application avec état dans le même espace de noms du cluster OpenShift
- Mobilité des applications par clonage d'un système FlexPod (OpenShift Container Platform bare Metal) vers un autre système FlexPod (OpenShift Container Platform sur VMware).

En particulier, seules quelques utilisations ont été validées dans cette solution. Cette validation ne correspond en aucune façon à l'ensemble des fonctionnalités d'Astra Control Center.

"Ensuite : restauration des applications avec sauvegardes distantes."

Restauration d'applications avec sauvegardes distantes

"Précédent : présentation de la validation de la solution."

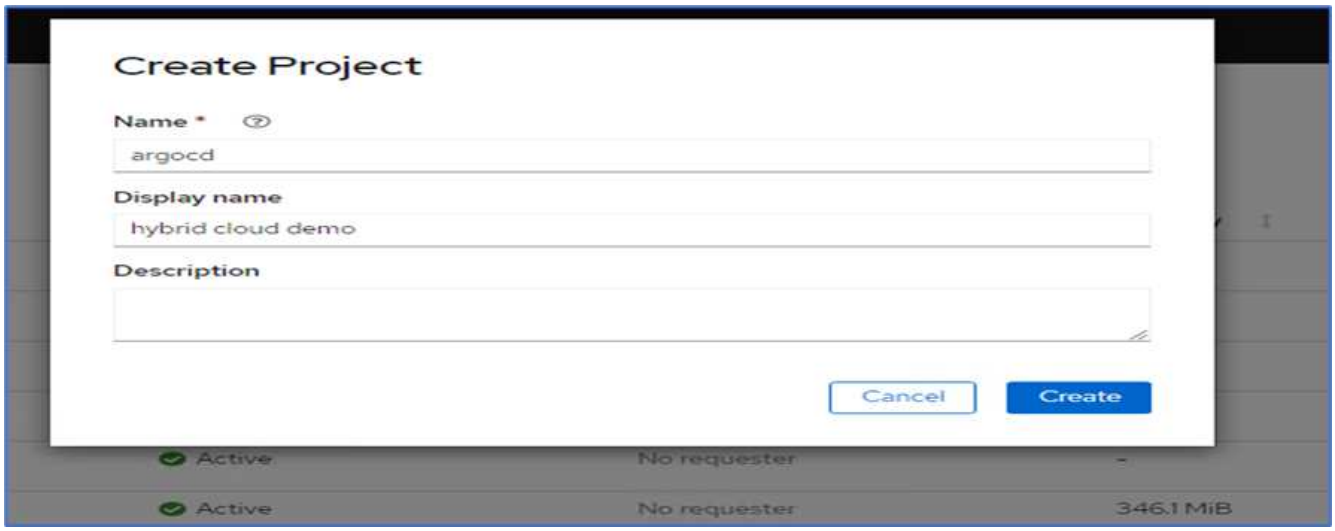
Avec Astra, vous pouvez effectuer une sauvegarde complète et cohérente avec les

applications qui permet de restaurer les données de votre application vers un autre cluster Kubernetes qui s'exécute dans un data Center sur site ou dans un cloud public.

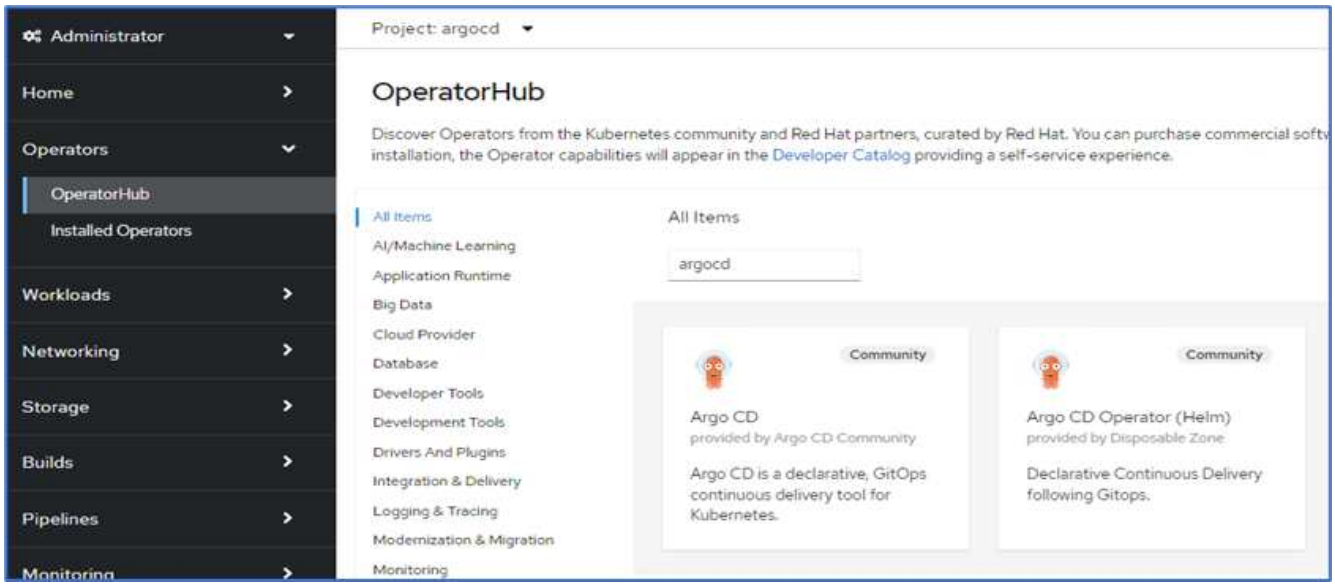
Pour valider la restauration d'application, simulez une défaillance sur site d'une application exécutée sur le système FlexPod et restaurez l'application sur un cluster K8s dans le cloud à l'aide d'une sauvegarde à distance.

L'exemple d'application est une application de liste de prix qui utilise MySQL pour la base de données. Pour automatiser le déploiement, nous avons utilisé le "CD Argo" outil. Argo CD est un outil de livraison continue déclaratif, GitOps.

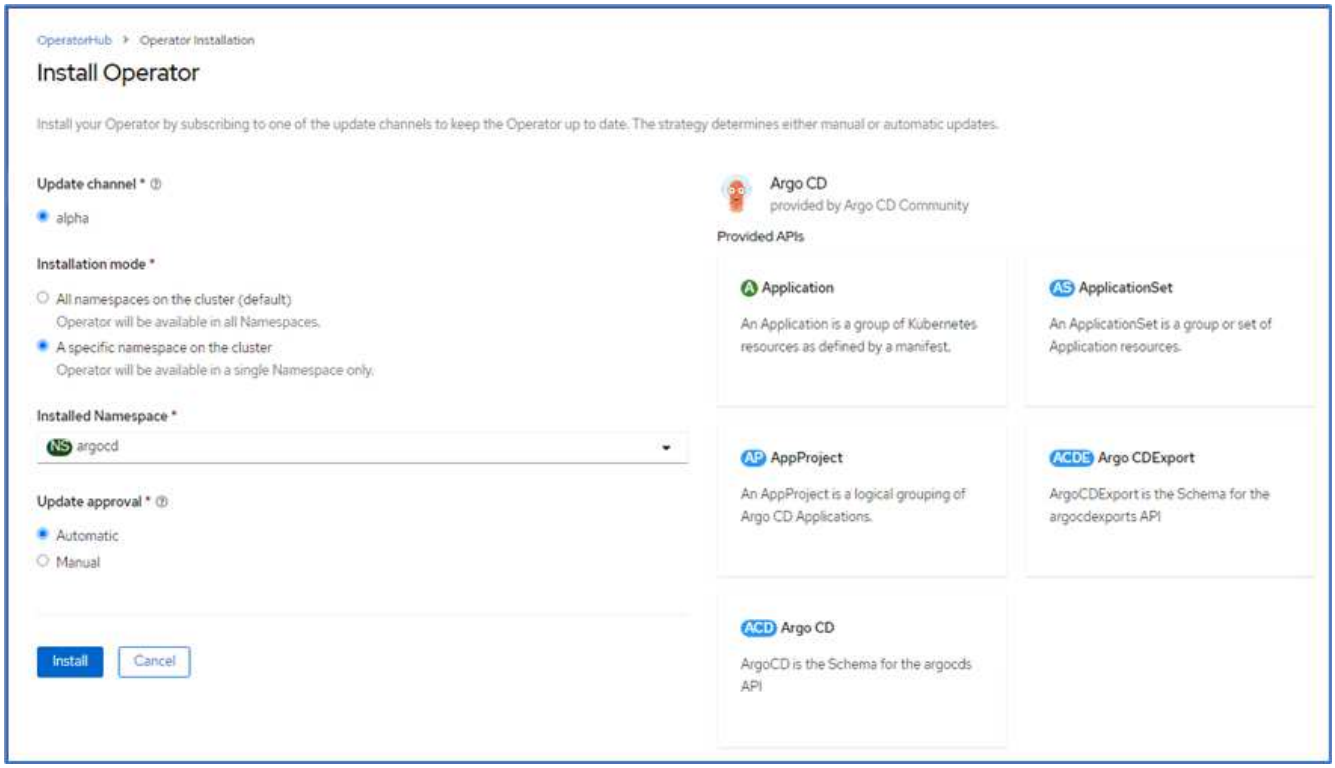
1. Connectez-vous au cluster OpenShift sur site et créez un nouveau projet sous son nom `argocd`.



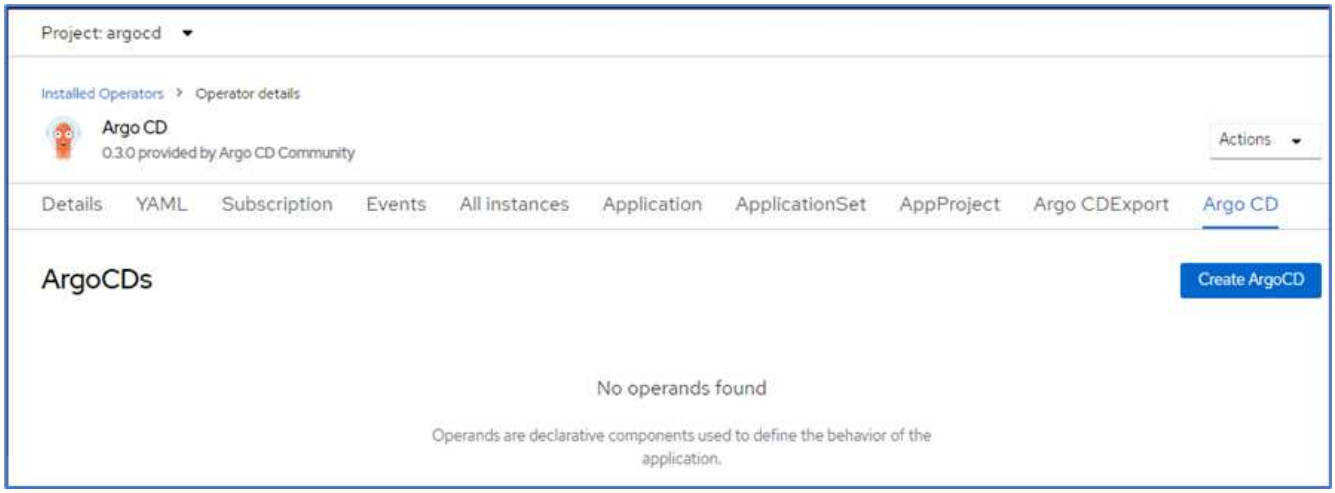
2. Dans OperatorHub, recherchez `argocd` Et sélectionnez opérateur du CD Argo.



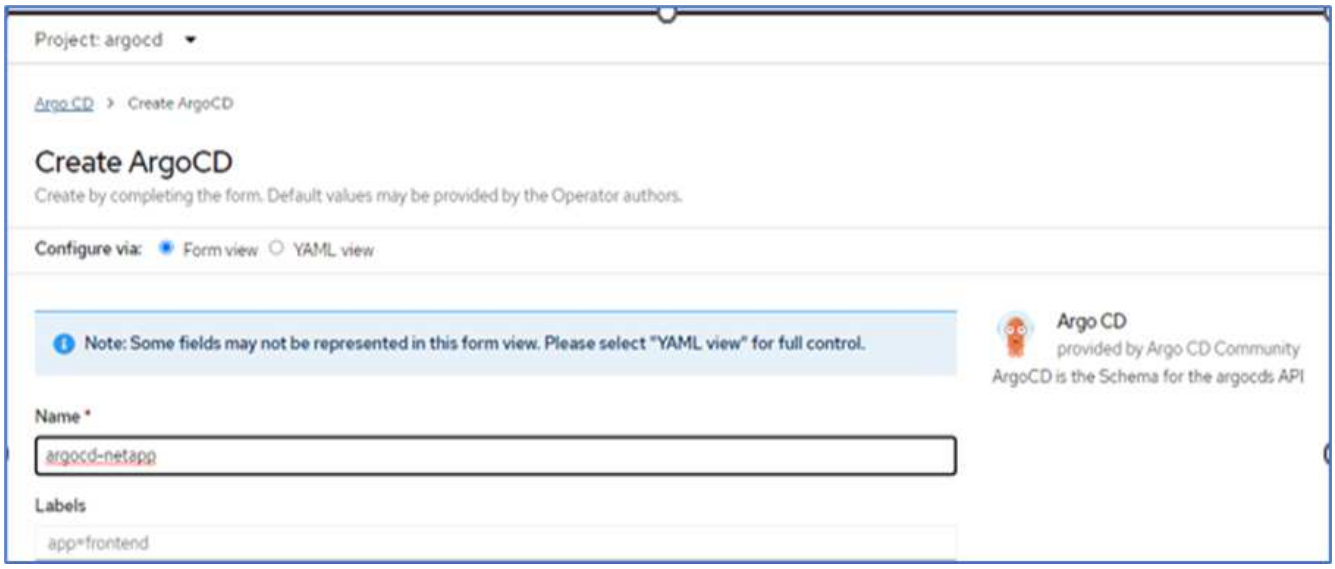
3. Installer l'opérateur dans le `argocd` espace de noms.



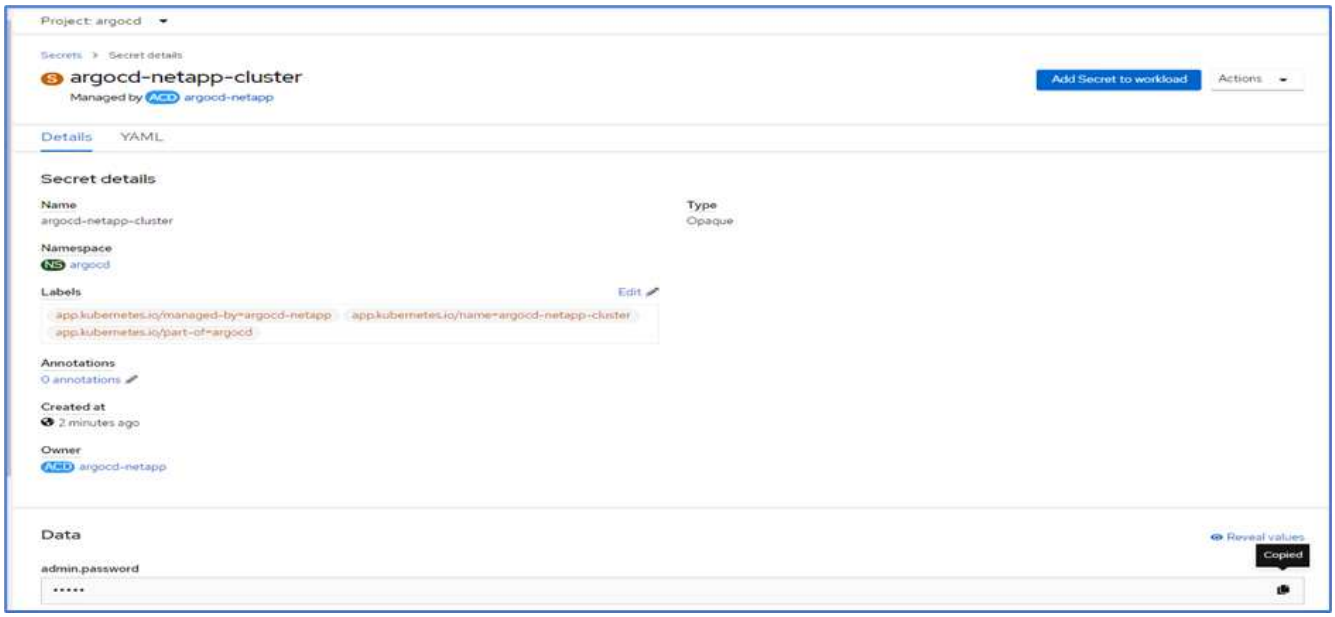
4. Accédez à l'opérateur et cliquez sur Créer un ArgoCD.



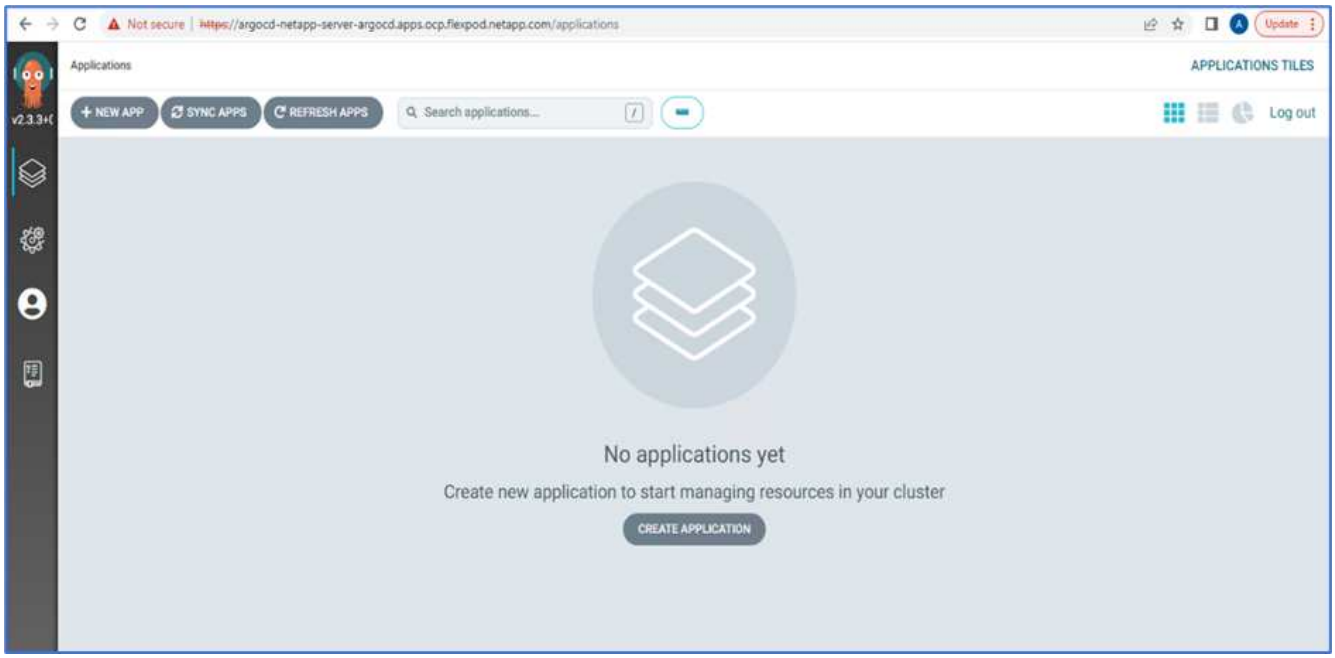
5. Pour déployer l'instance de CD Argo dans le `argocd` Donnez un nom au projet, puis cliquez sur Créer.



6. Pour vous connecter au CD Argo, l'utilisateur par défaut est admin et le mot de passe se trouve dans un fichier secret portant le nom `argocd-netapp-cluster`.



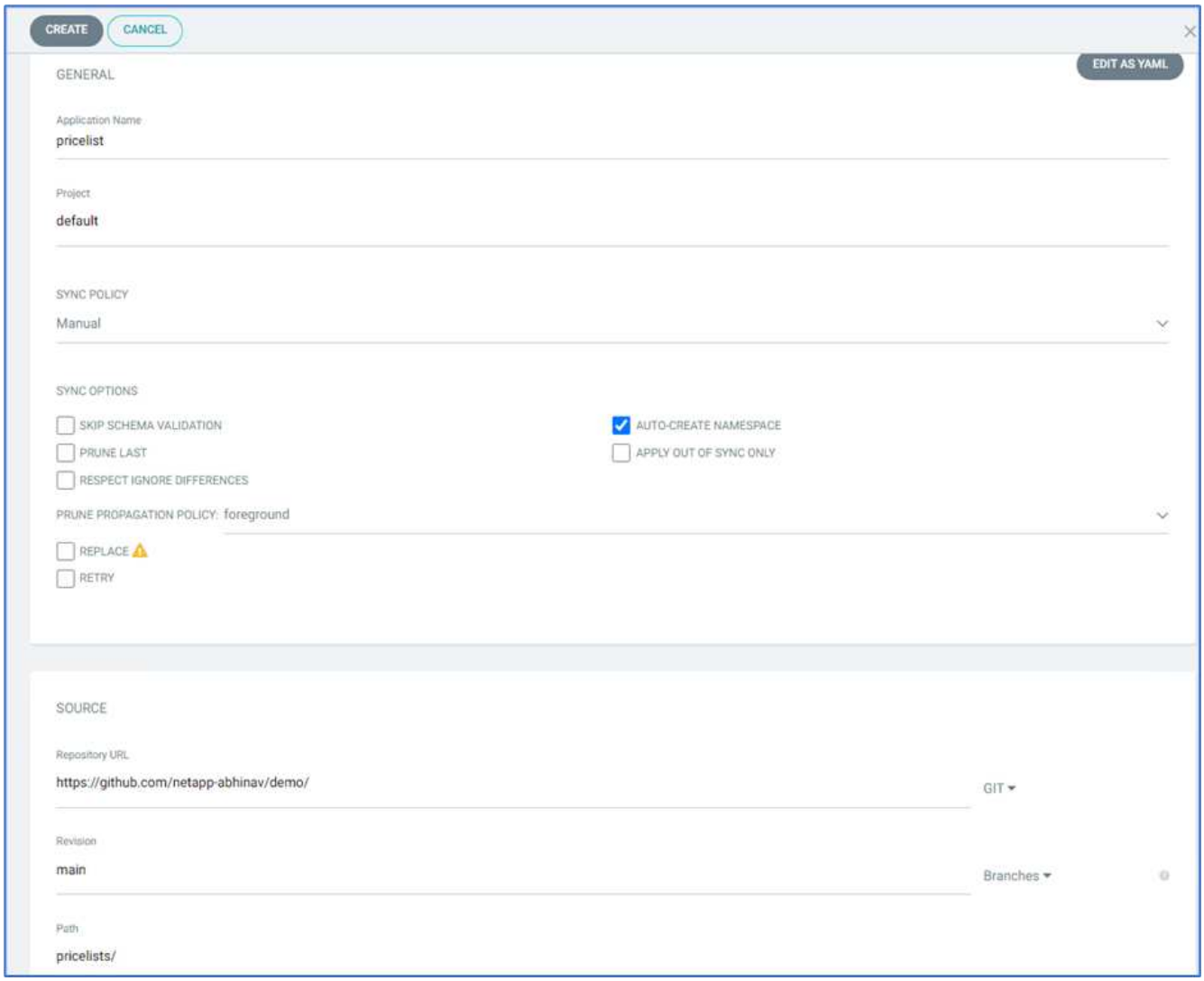
7. Dans le menu latéral, sélectionnez routes > emplacement et cliquez sur l'URL de l' `argocd` itinéraires. Entrez le nom d'utilisateur et le mot de passe.



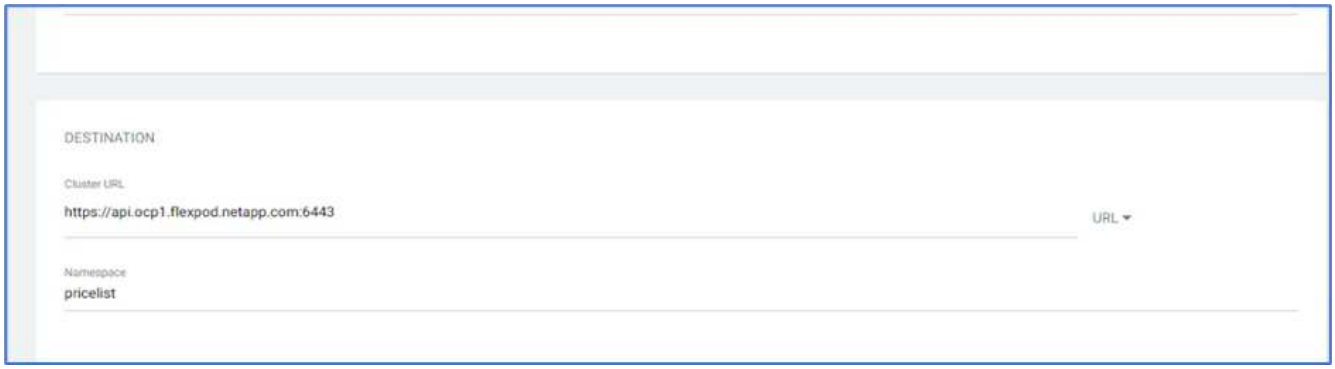
8. Ajoutez le cluster OpenShift sur site au CD Argo via l'interface de ligne de commande.

```
####Login to Argo CD####
abhinav3@abhinav-ansible$ argocd-linux-amd64 login argocd-netapp-server-
argocd.apps.ocp.flexpod.netapp.com --insecure
Username: admin
Password:
'admin:login' logged in successfully
Context'argocd-netapp-server-argocd.apps.ocp.flexpod.netapp.com' updated
####List the On-Premises OpenShift cluster####
abhinav3@abhinav-ansible$ argocd-linux-amd64 cluster add
ERRO[0000] Choose a context name from:
CURRENT  NAME
CLUSTER              SERVER
*        default/api-ocp-flexpod-netapp-com:6443/abhinav3
api-ocp-flexpod-netapp-com:6443
https://api.ocp.flexpod.netapp.com:6443
         default/api-ocp1-flexpod-netapp-com:6443/abhinav3
api-ocp1-flexpod-netapp-com:6443
https://api.ocp1.flexpod.netapp.com:6443
####Add On-Premises OpenShift cluster###
abhinav3@abhinav-ansible$ argocd-linux-amd64 cluster add default/api-
ocp1-flexpod-netapp-com:6443/abhinav3
WARNING: This will create a service account `argocd-manager` on the
cluster referenced by context `default/api-ocp1-flexpod-netapp-
com:6443/abhinav3` with full cluster level admin privileges. Do you want
to continue [y/N]? y
INFO[0002] ServiceAccount "argocd-manager" already exists in namespace
"kube-system"
INFO[0002] ClusterRole "argocd-manager-role" updated
INFO[0002] ClusterRoleBinding "argocd-manager-role-binding" updated
Cluster 'https://api.ocp1.flexpod.netapp.com:6443' added
```

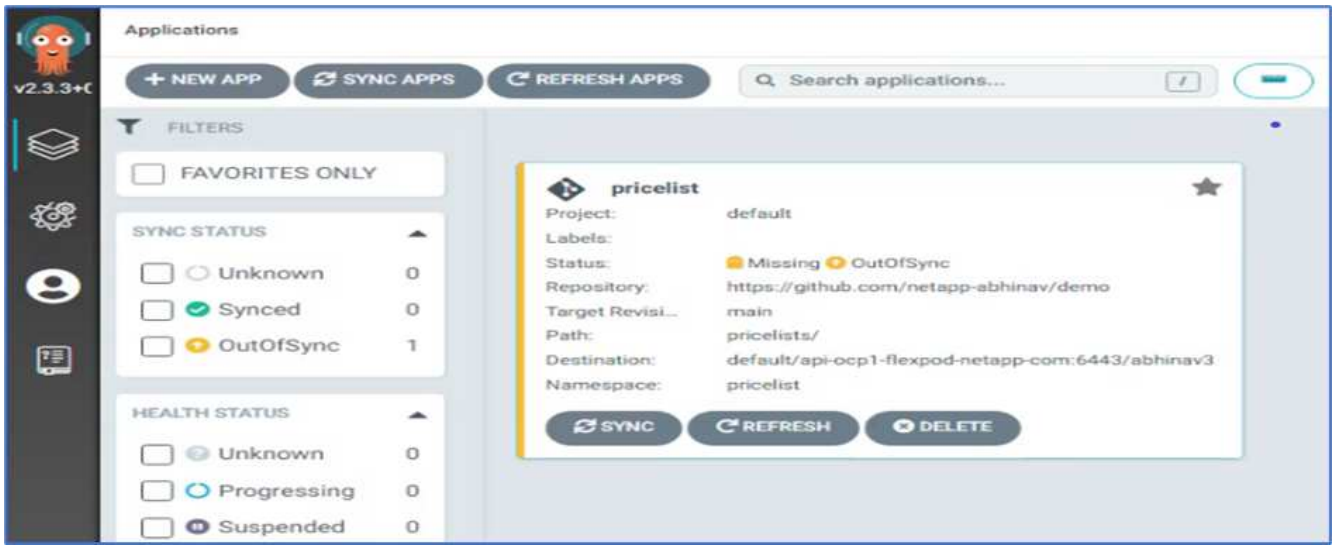
9. Dans l’interface utilisateur ArgoCD, cliquez sur NOUVELLE APPLICATION et entrez les détails du nom de l’application et du référentiel de code.



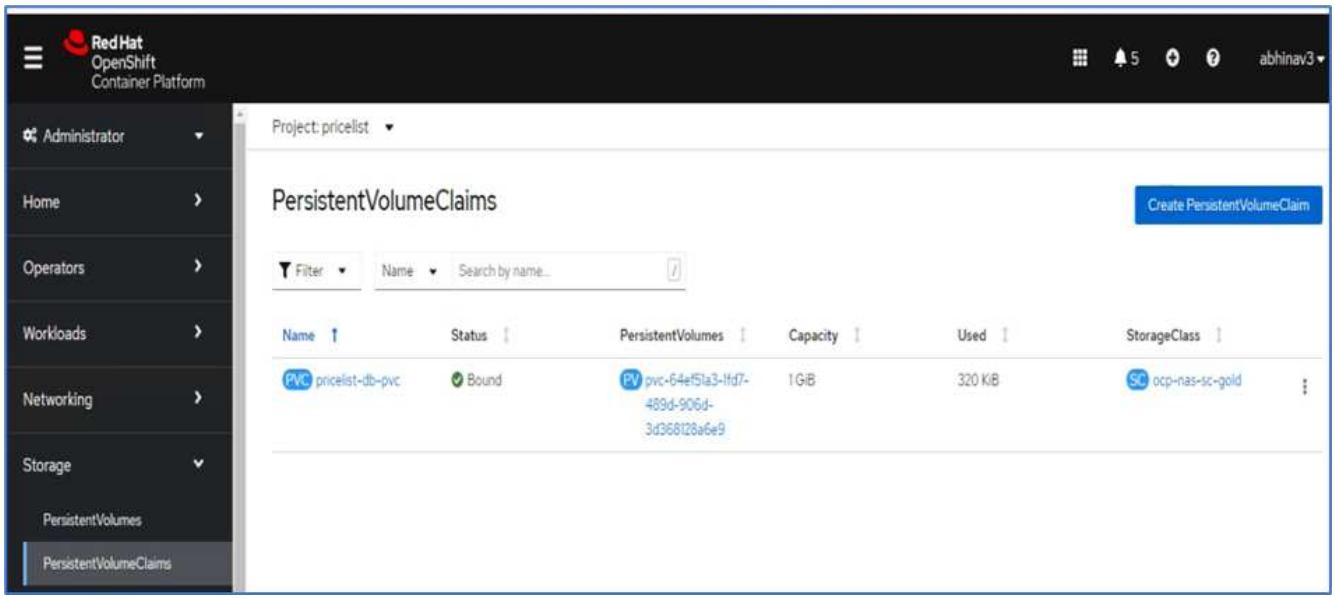
10. Entrez le cluster OpenShift où l’application sera déployée avec le namespace.



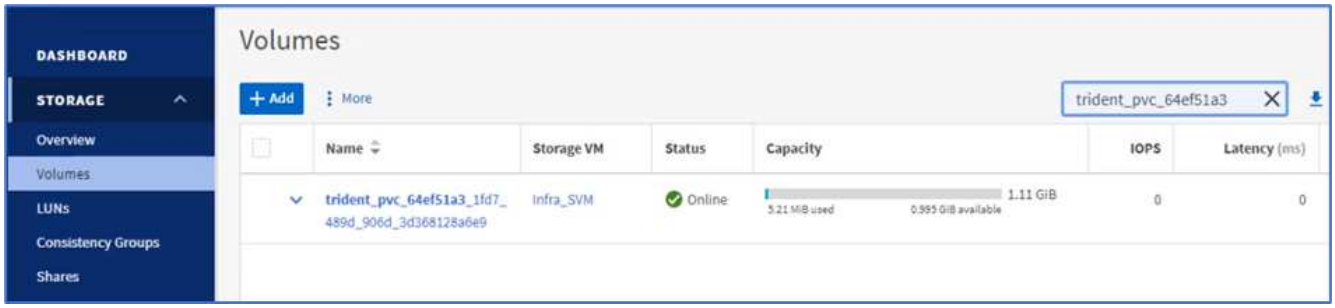
11. Pour déployer l’application sur le cluster OpenShift sur site, cliquez sur SYNC.



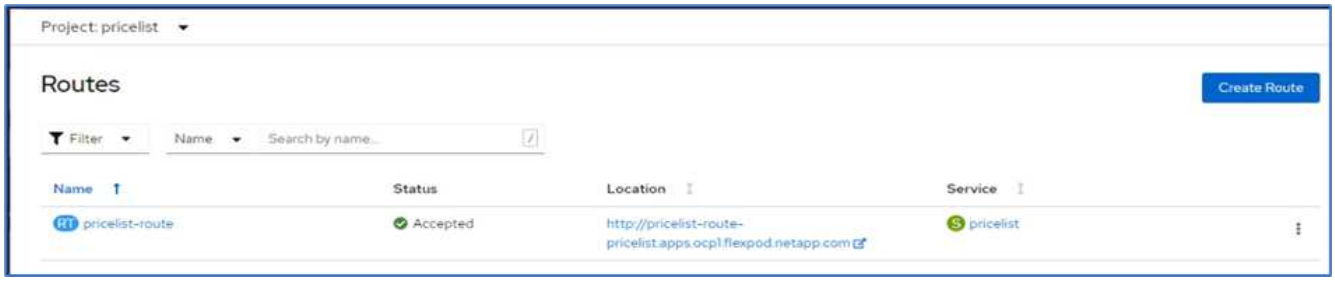
12. Dans la console OpenShift Container Platform, accédez à la liste des tarifs du projet et, sous Storage, vérifiez le nom et la taille de la demande de volume persistant.



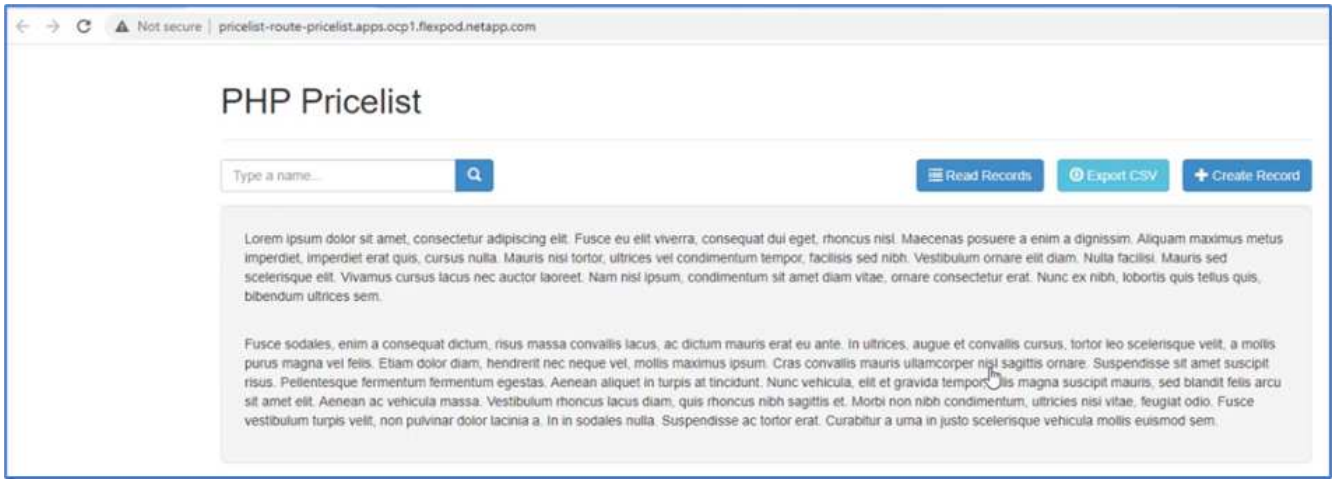
13. Connectez-vous à System Manager et vérifiez le volume persistant.



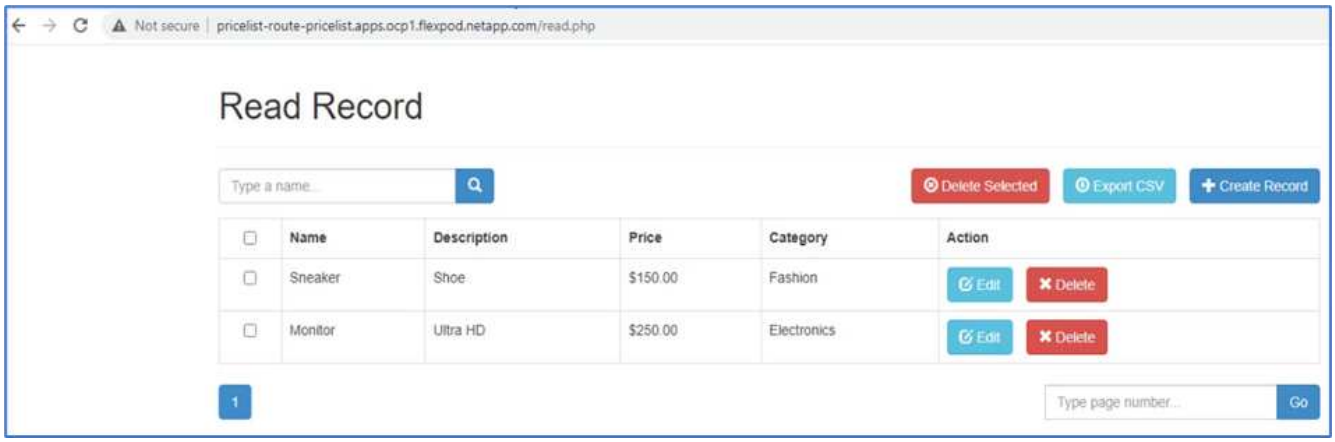
14. Une fois les pods en cours d'exécution, sélectionnez réseau > routes dans le menu latéral, puis cliquez sur l'URL sous emplacement.



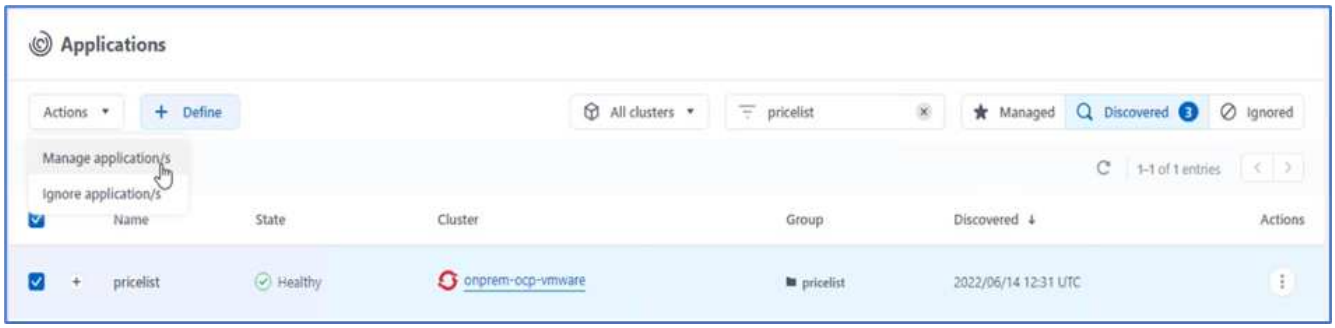
15. La page d'accueil de l'application Tarifs s'affiche.



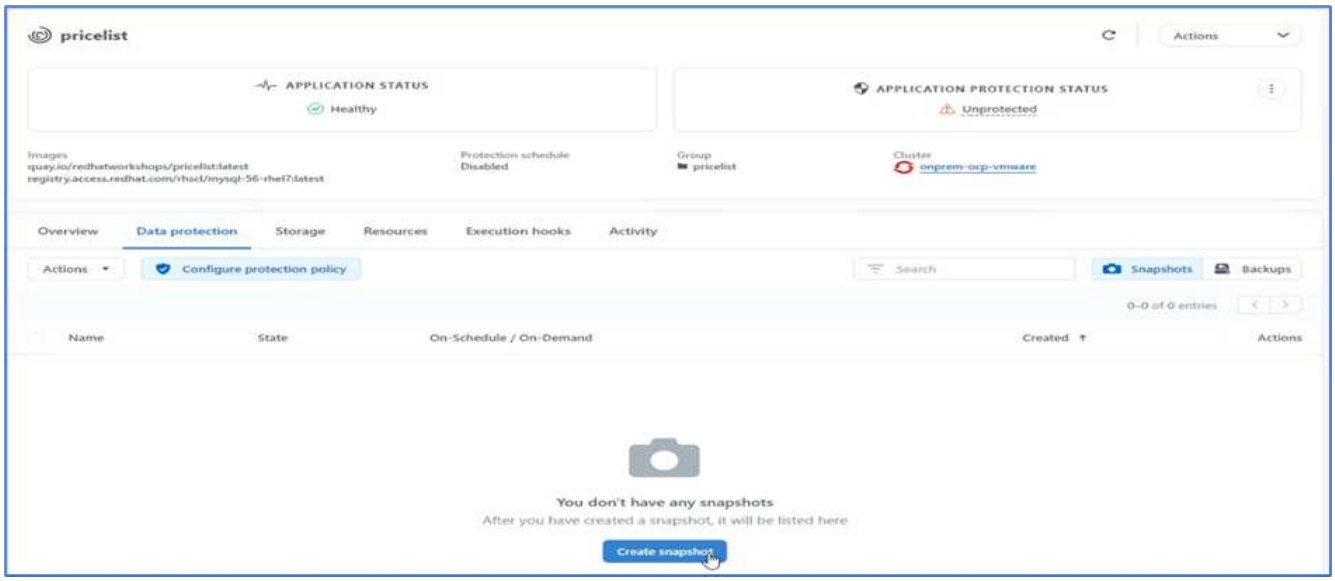
16. Créez quelques enregistrements sur la page Web.



17. L'application est découverte dans Astra Control Center. Pour gérer l'application, accédez à applications > découverte, sélectionnez l'application Barème des prix, puis cliquez sur gérer les applications sous actions.

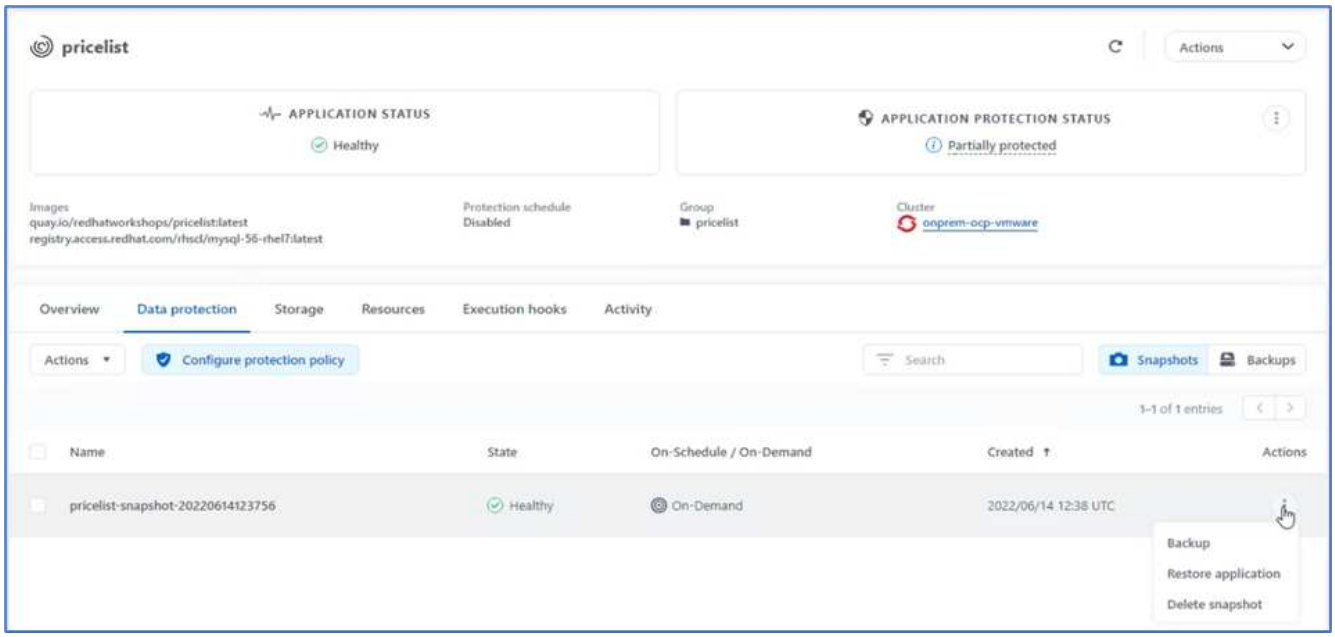


18. Cliquez sur l'application Barème des prix et sélectionnez protection des données. À ce stade, il ne doit y avoir aucun Snapshot ni aucune sauvegarde. Cliquez sur Créer un snapshot pour créer un snapshot à la demande.

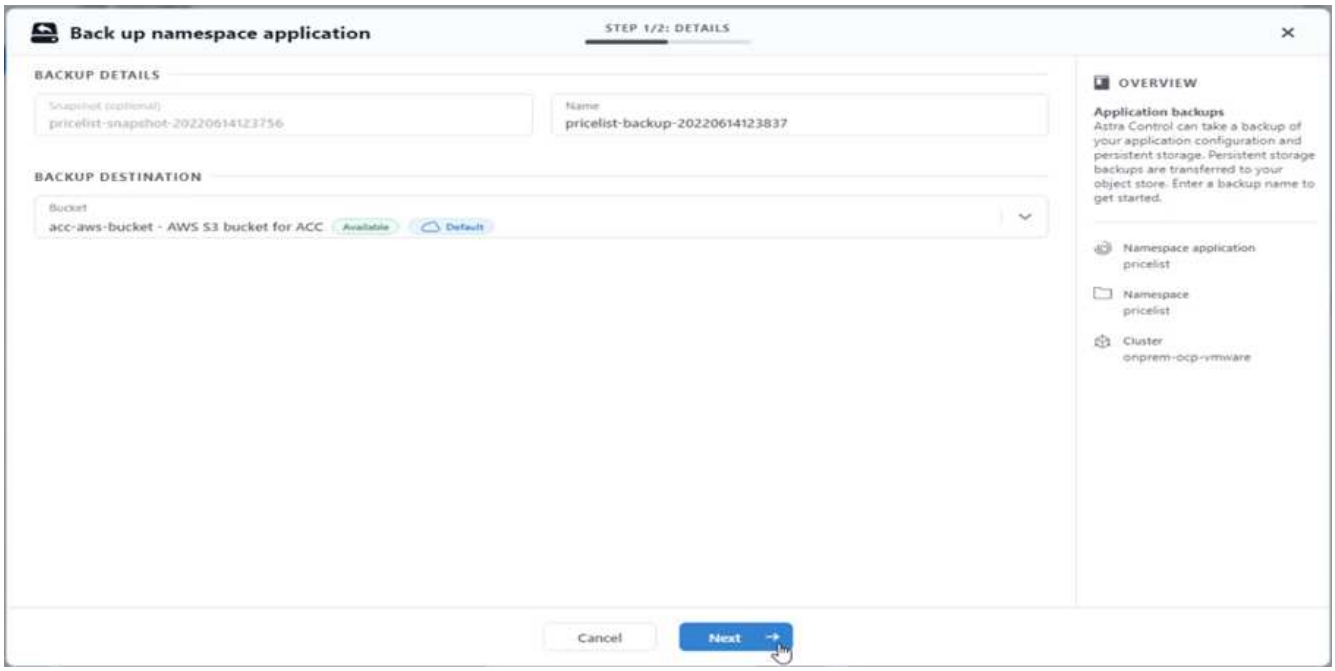


Le NetApp Astra Control Center prend en charge à la demande et les sauvegardes Snapshot et planifiées.

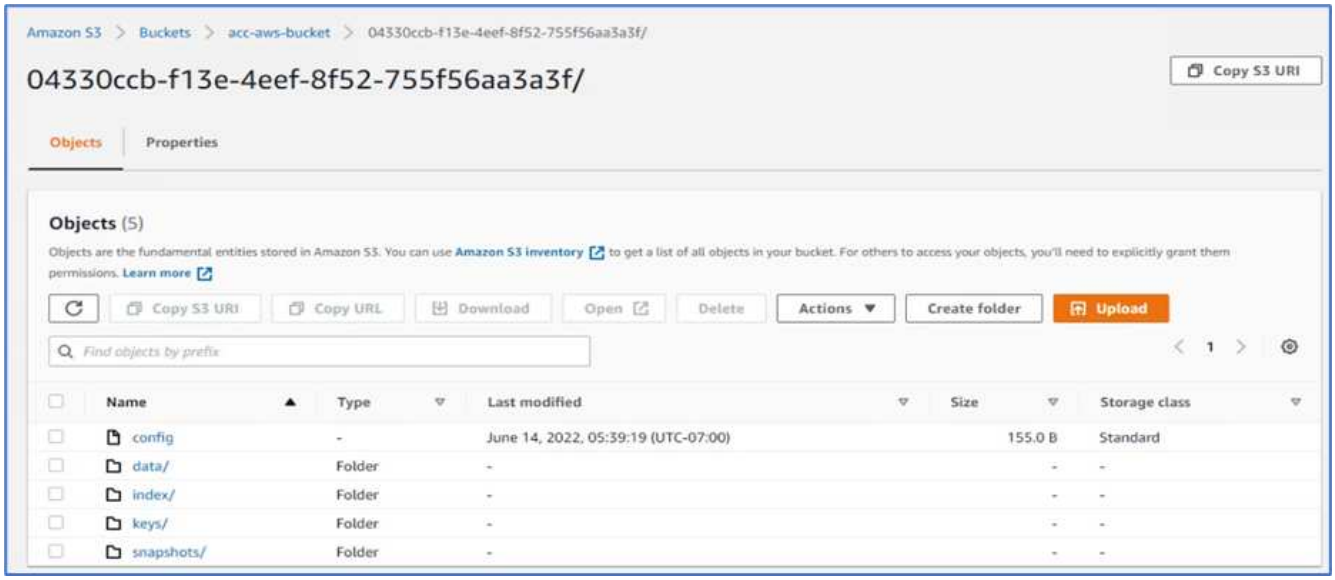
19. Une fois le snapshot créé et l'état fonctionnel, créez une sauvegarde à distance à l'aide de ce snapshot. Cette sauvegarde est stockée dans le compartiment S3.



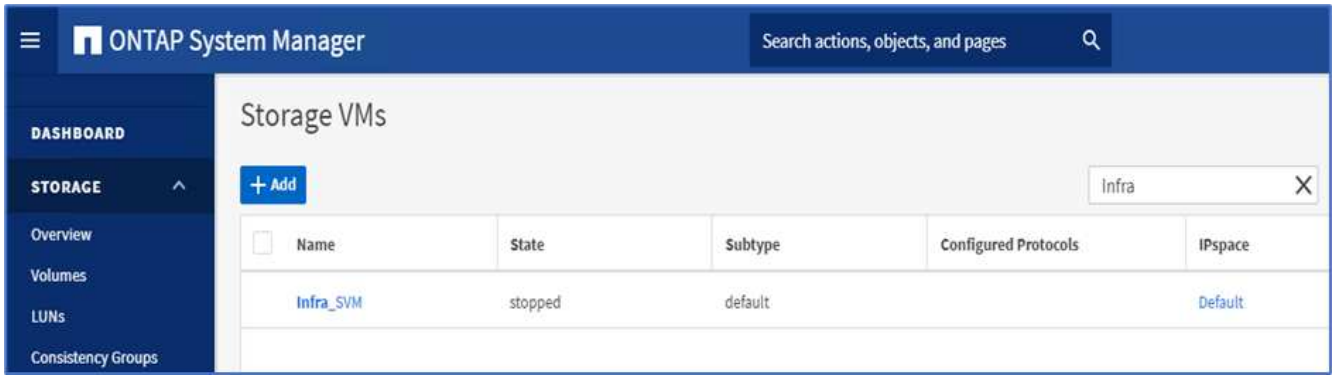
20. Sélectionnez le compartiment AWS S3 et lancez l'opération de sauvegarde.



21. L'opération de sauvegarde doit créer un dossier contenant plusieurs objets dans le compartiment AWS S3.



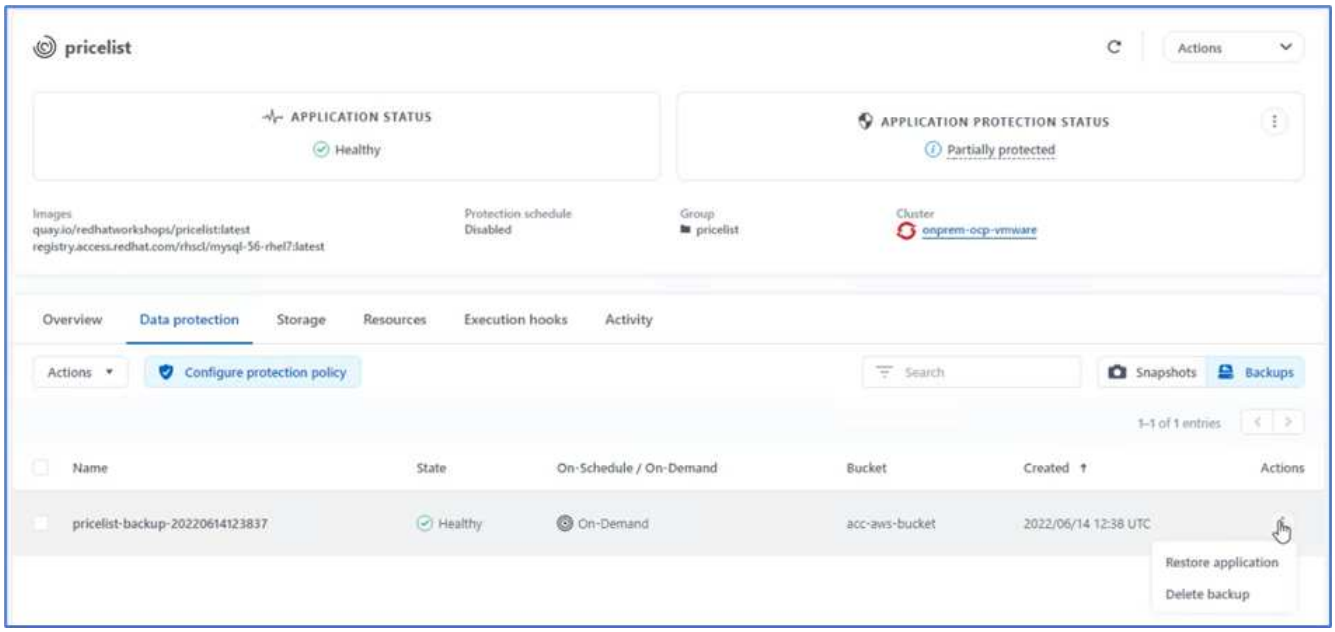
22. Une fois la sauvegarde à distance terminée, simulez un incident sur site en arrêtant la machine virtuelle de stockage (SVM) qui héberge le volume de support du volume persistant.



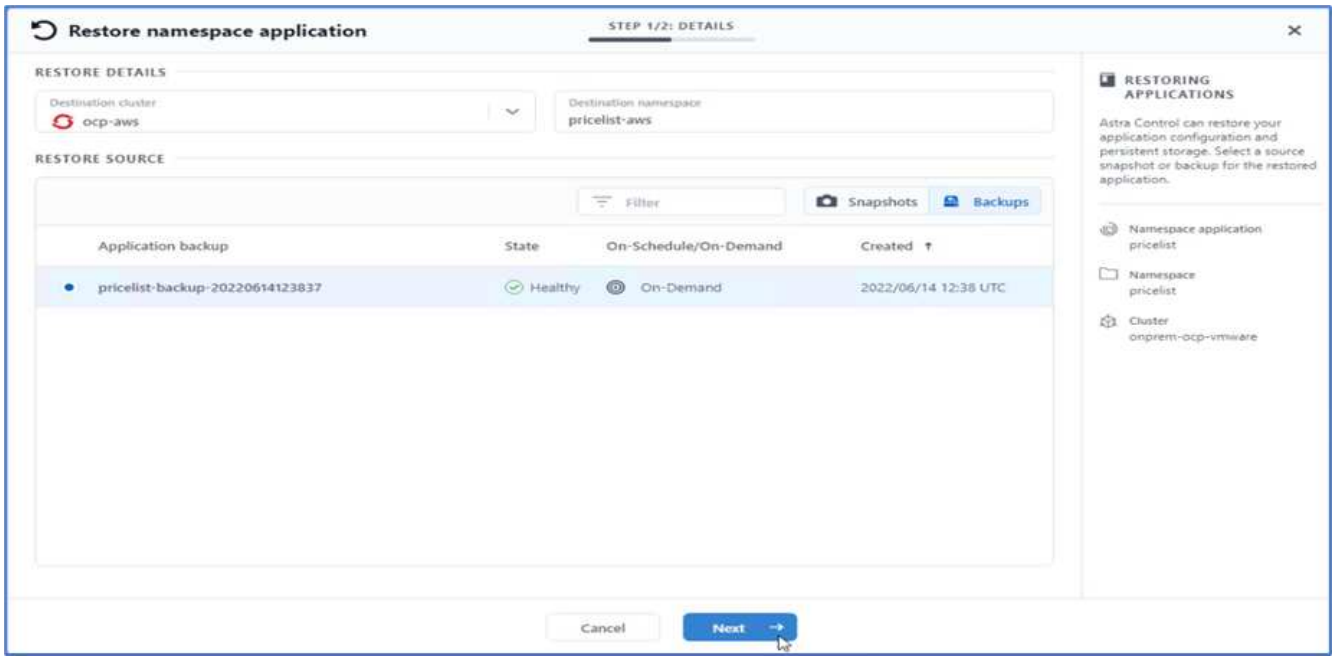
23. Actualisez la page Web pour confirmer l'interruption. La page Web n'est pas disponible.

Comme on pouvait s'y attendre, le site Web est en panne. Restaurez rapidement l'application à partir de la sauvegarde à distance en utilisant Astra vers le cluster OpenShift exécuté dans AWS.

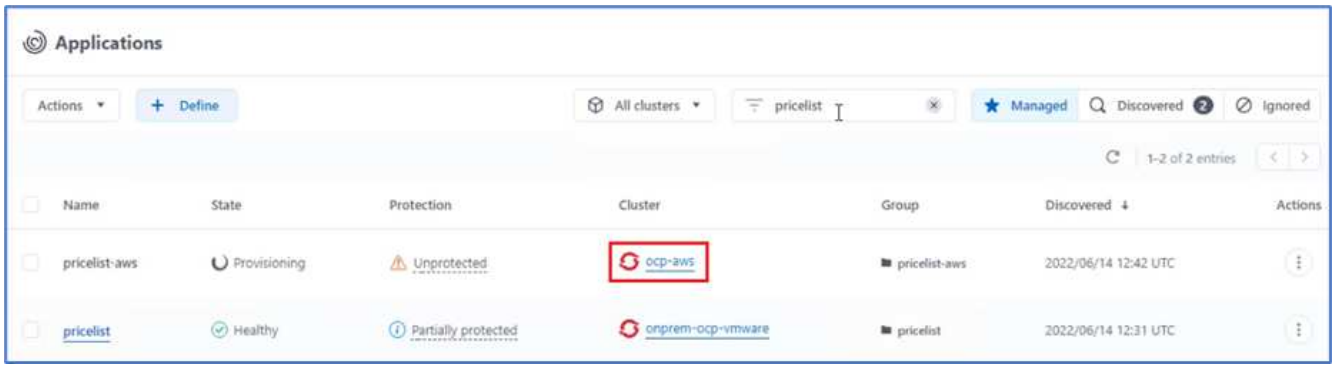
24. Dans Astra Control Center, cliquez sur l'application Pricelist et sélectionnez protection des données > sauvegardes. Sélectionnez la sauvegarde, puis cliquez sur Restaurer l'application sous action.



25. Sélectionnez `ocp-aws` comme cluster de destination et donner un nom au namespace. Cliquez sur sauvegarde à la demande, puis sur Suivant, puis sur Restaurer.

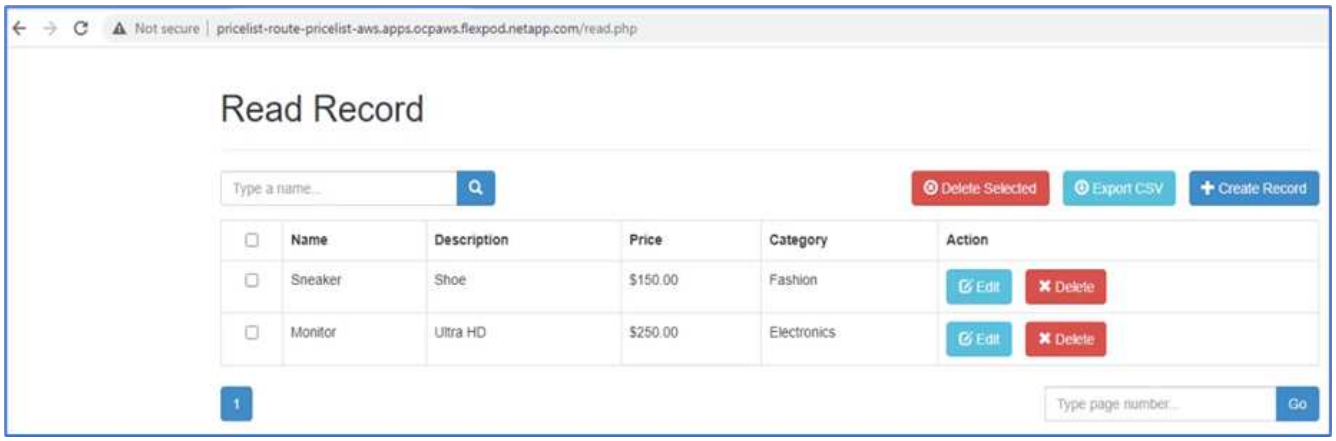


26. Une nouvelle application portant le nom `pricelist-app` Est mise à la disposition du cluster OpenShift exécuté dans AWS.



27. Vérifiez la même chose dans la console web OpenShift.

28. Après toutes les gousses sous le `pricelist-aws` Le projet est en cours d'exécution, accédez aux itinéraires et cliquez sur l'URL pour lancer la page Web.



Ce processus valide la restauration de l'application prichère et le maintien de l'intégrité des données sur le cluster OpenShift fonctionnant de façon transparente sur AWS avec l'aide d'Astra Control Center.

Protection des données avec les copies Snapshot et mobilité des applications pour DevTest

Ce cas d'utilisation se compose de deux parties, comme décrit dans les sections suivantes.

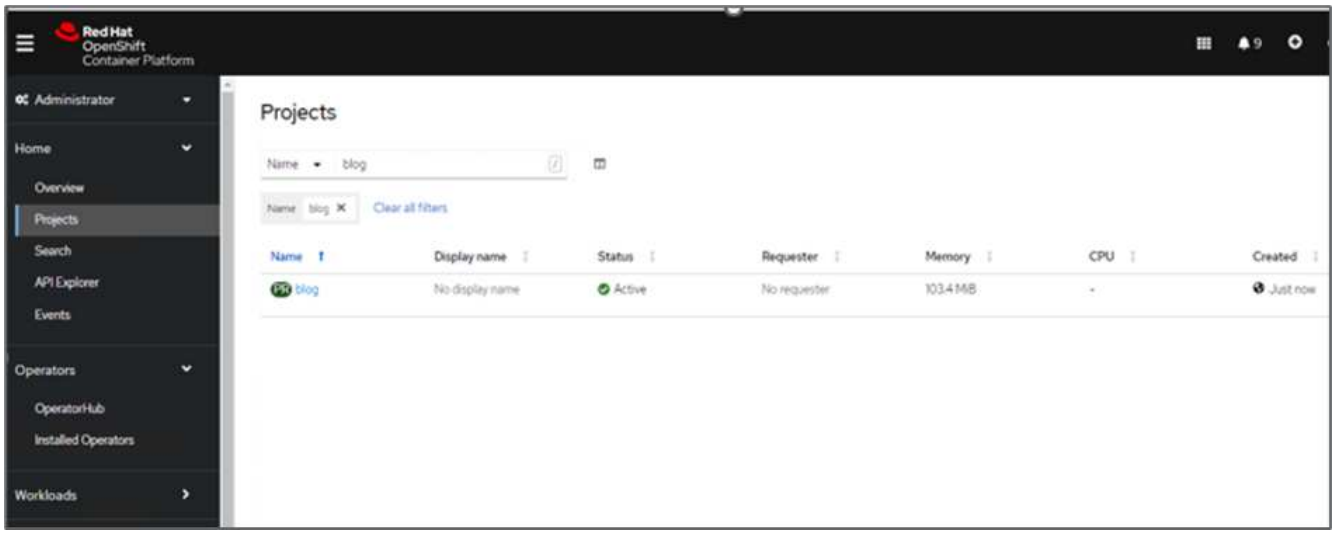
Partie 1

Avec Astra Control Center, vous pouvez créer des snapshots respectueux des applications pour une protection locale des données. Si vous supprimez ou corrompre accidentellement vos données, vous pouvez restaurer vos applications et les données associées à un état correct connu à l'aide d'un instantané précédemment enregistré.

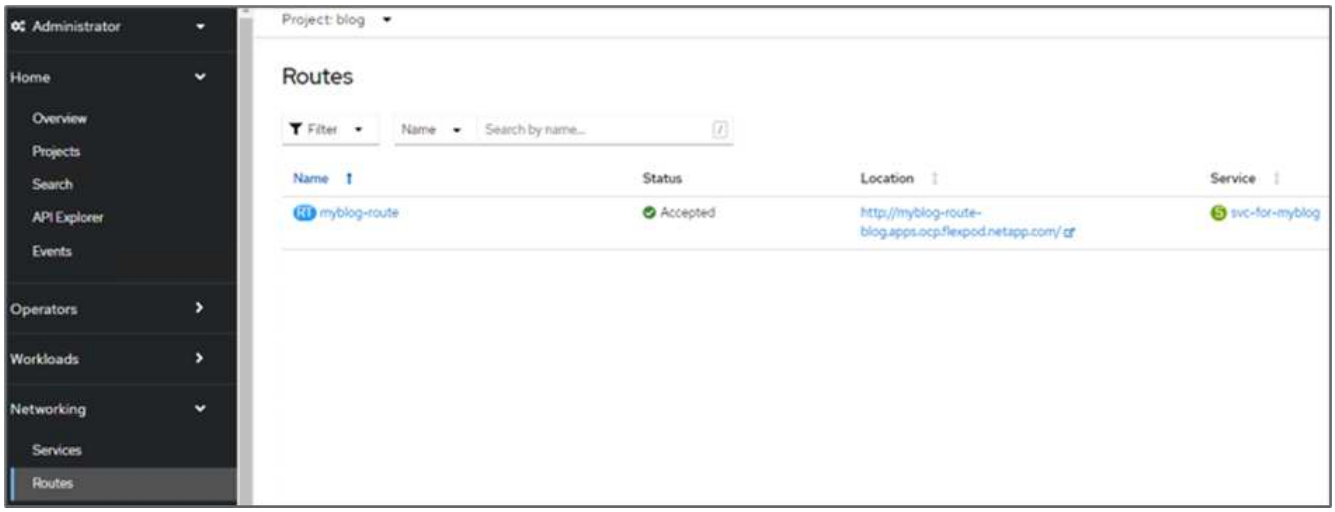
Dans ce scénario, une équipe de développement et de test (DevTest) déploie un exemple d'application avec état (site de blog) qui est une application de blog Ghost, ajoute du contenu et met à niveau l'application vers la dernière version disponible. L'application Ghost utilise SQLite pour la base de données. Avant de mettre à niveau l'application, un snapshot (à la demande) est utilisé avec Astra Control Center pour la protection des données. Les étapes détaillées sont les suivantes :

1. Déployez l'application exemple de blogging et synchronisez-la à partir d'ArgoCD.

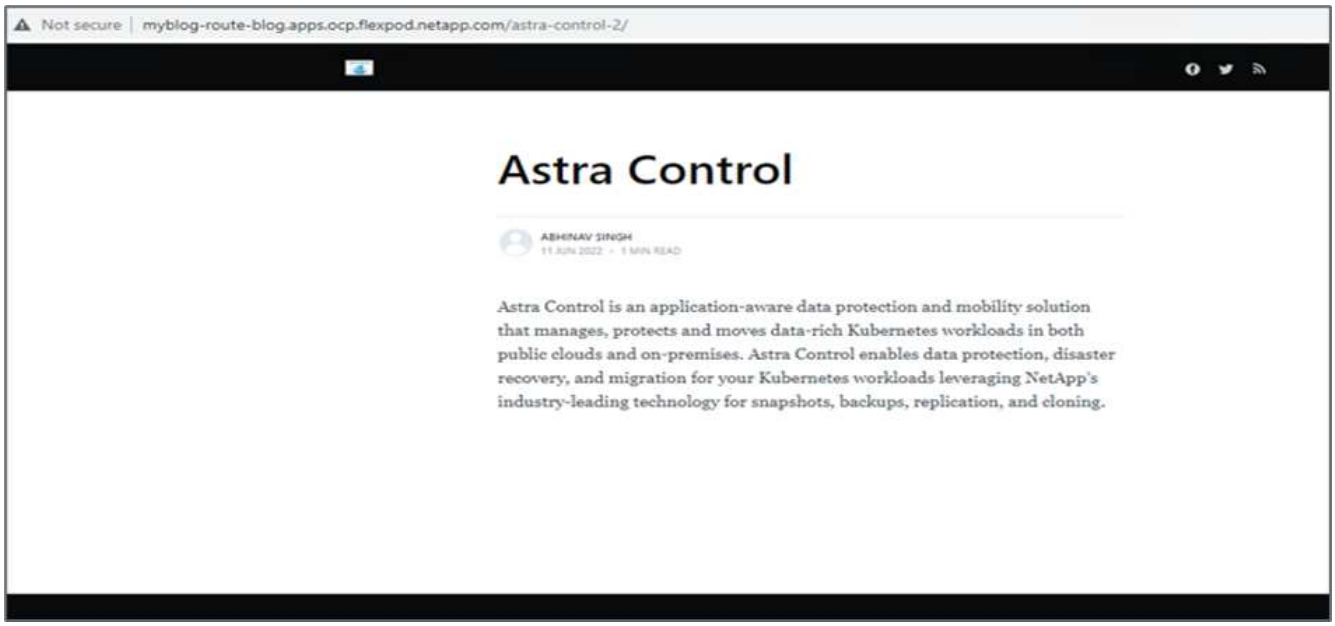
2. Connectez-vous au premier cluster OpenShift, accédez à Project et entrez Blog dans la barre de recherche.



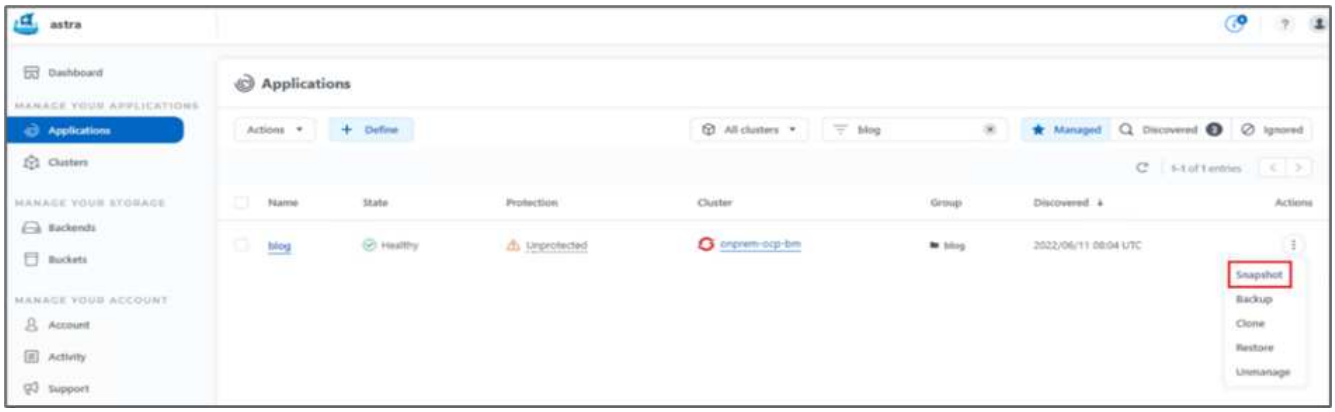
3. Dans le menu latéral, sélectionnez réseau > routes et cliquez sur l'URL.



4. La page d'accueil du blog s'affiche. Ajoutez du contenu au site du blog et publiez-le.



5. Rendez-vous à Astra Control Center. Commencez par gérer l'application à partir de l'onglet découverte, puis effectuez une copie Snapshot.

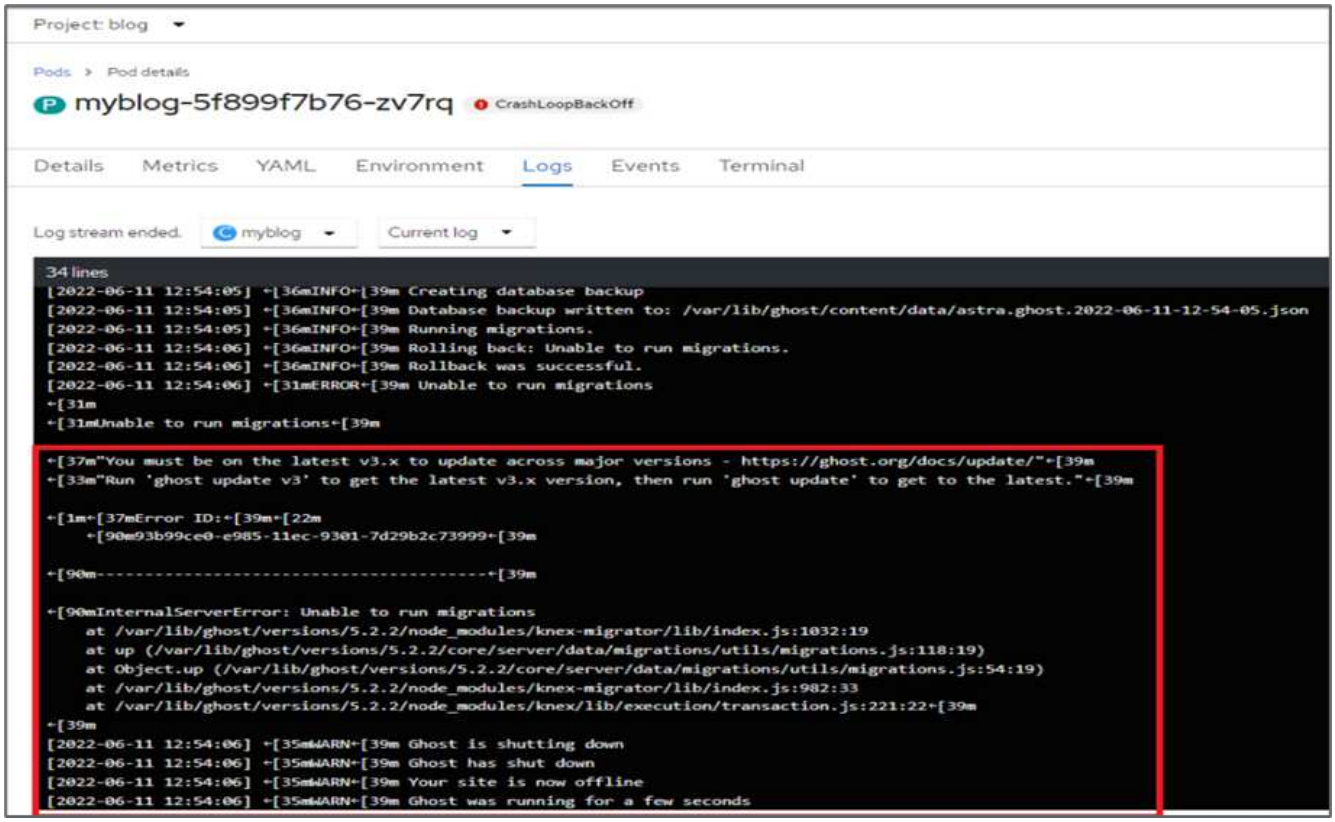


Vous pouvez également protéger vos applications en créant des snapshots, des sauvegardes ou les deux à un calendrier défini. Pour plus d'informations, voir "Protéger les applications avec les snapshots et les sauvegardes".

6. Une fois le snapshot à la demande créé, mettez l'application à niveau vers la dernière version. La version actuelle de l'image est `ghost: 3.6-alpine` et la version cible est `ghost:latest`. Pour mettre à niveau l'application, apportez directement des modifications au référentiel Git et synchronisez-les sur le CD Argo.

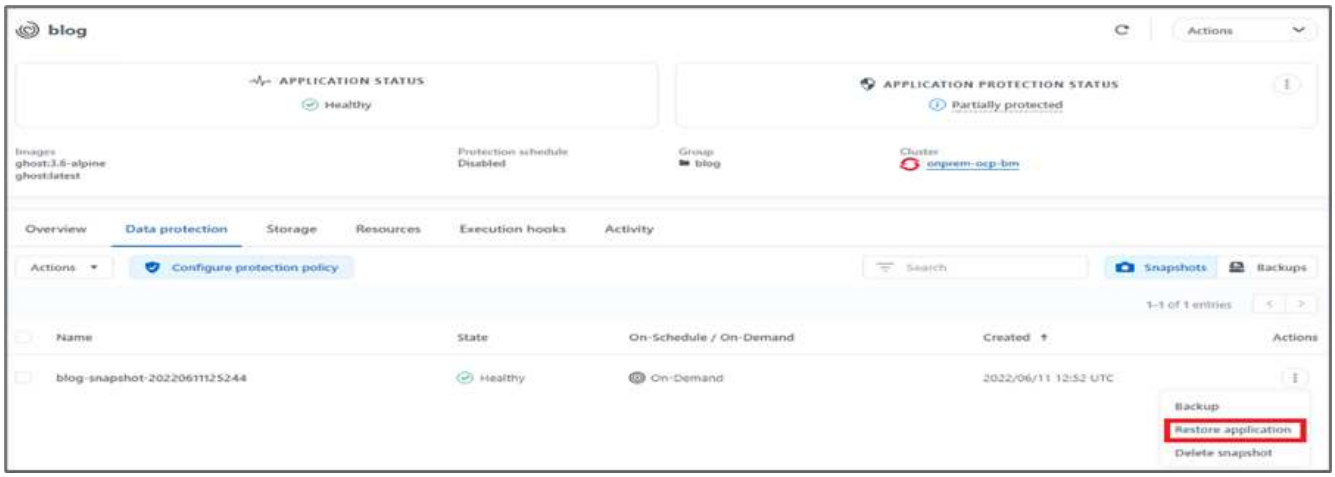
```
spec:
  containers:
  - name: myblog
    image: ghost:latest
    imagePullPolicy: Always
    ports:
    - containerPort: 2368
```

7. Vous pouvez voir que la mise à niveau directe vers la dernière version n'est pas prise en charge car le site du blog est en panne et l'application entière est corrompue.

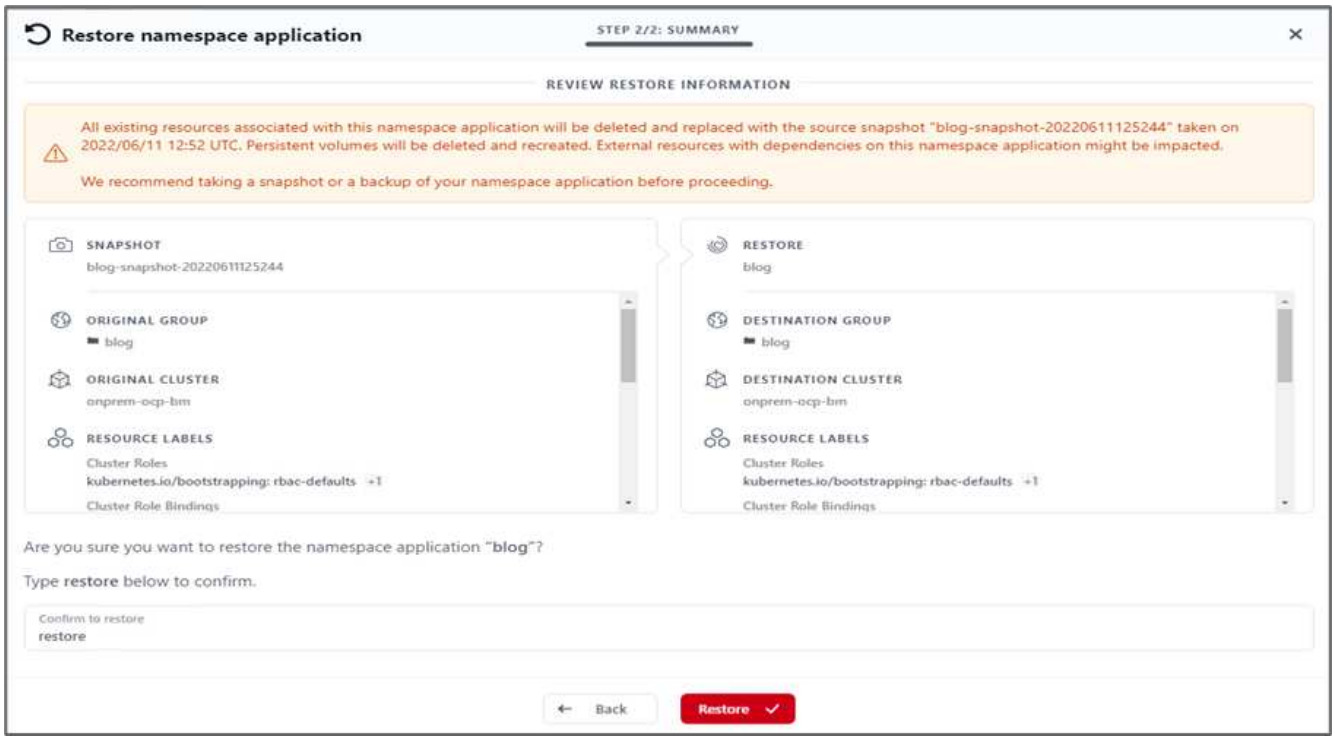


8. Pour confirmer l’indisponibilité du site du blog, actualisez l’URL.

9. Restaurez l’application à partir du snapshot.



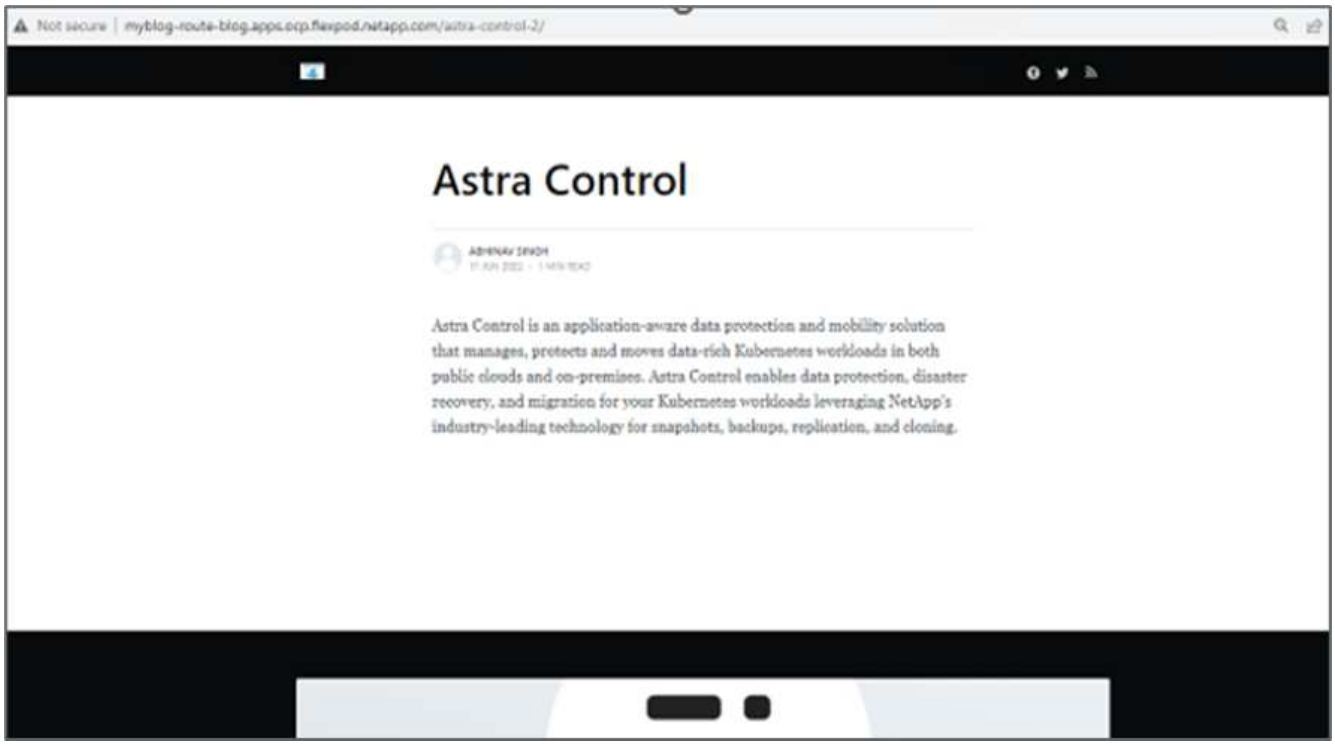
10. L'application est restaurée sur le même cluster OpenShift.



11. Le processus de restauration des applications démarre immédiatement.

12. En quelques minutes, l'application est restaurée à partir du snapshot disponible.

13. Pour voir si la page Web est disponible, actualisez l'URL.

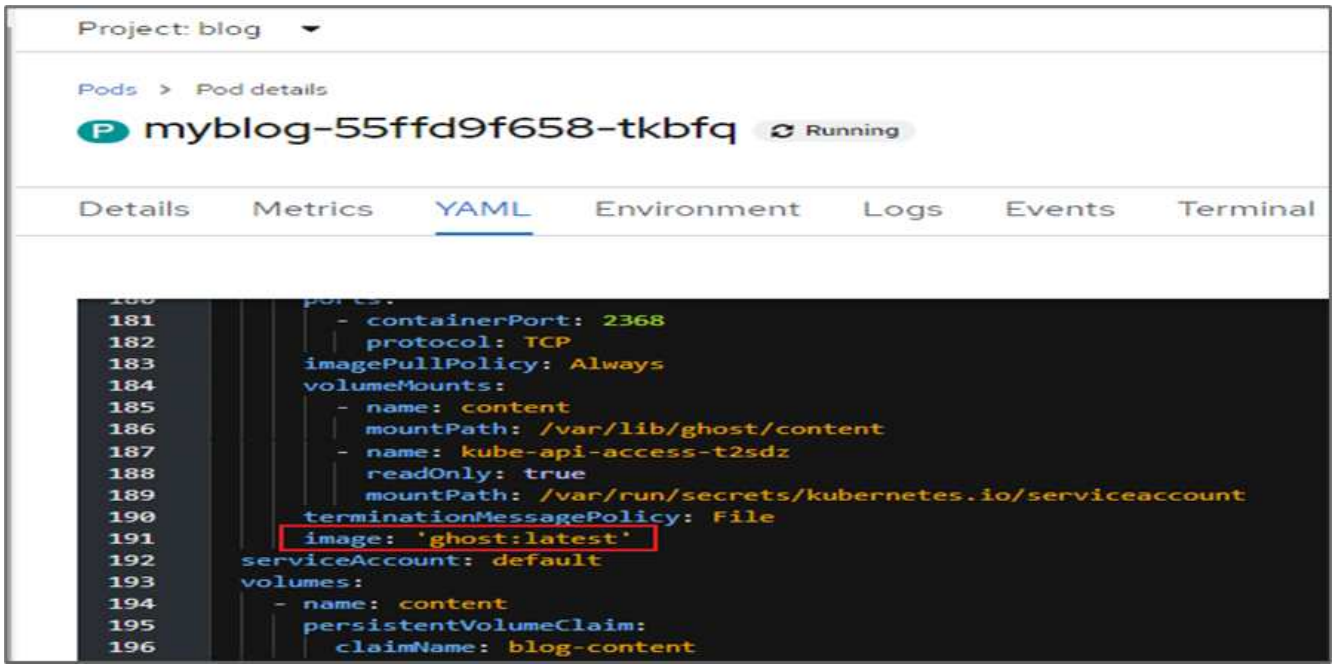


Avec l'aide d'Astra Control Center, une équipe DevTest peut réussir la récupération d'une application de blog et de ses données associées à l'aide de la capture d'écran.

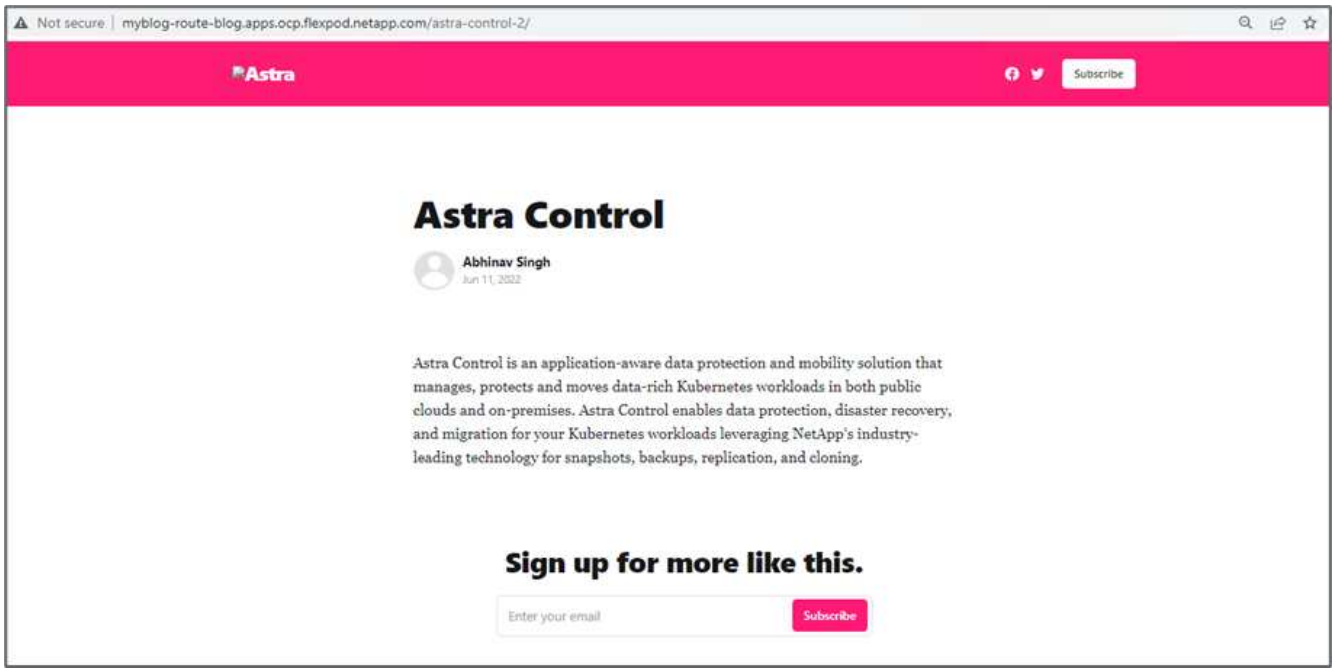
Partie 2

Avec Astra Control Center, vous pouvez déplacer l'ensemble d'une application avec ses données d'un cluster Kubernetes vers un autre, quel que soit l'emplacement des clusters (sur site ou dans le cloud).

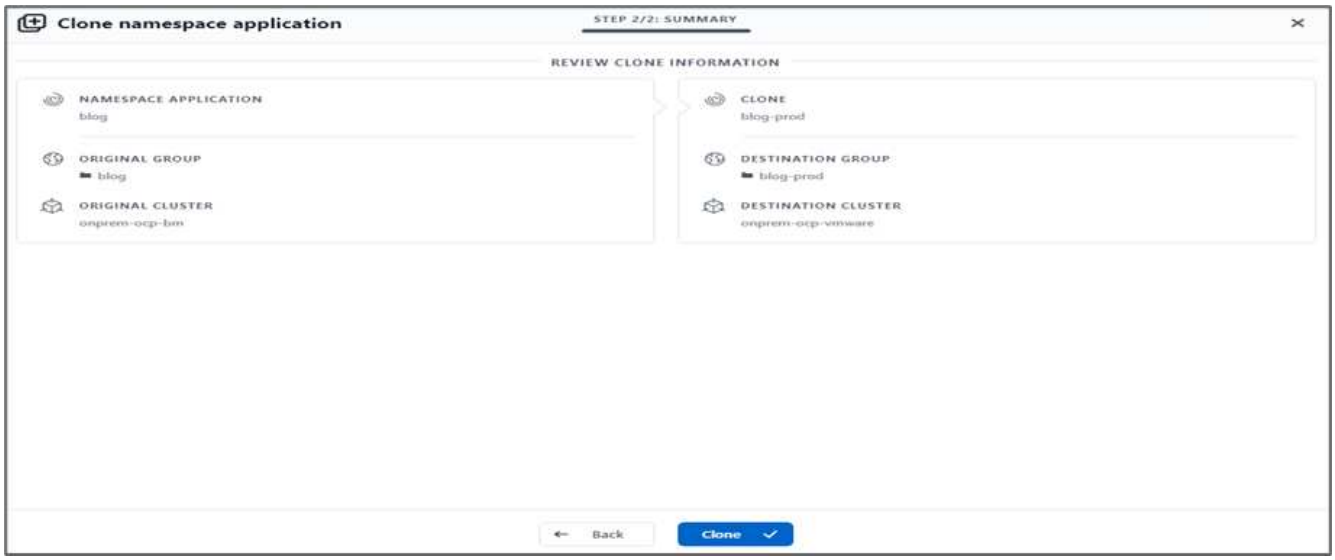
1. L'équipe DevTest met initialement à niveau l'application vers la version prise en charge (`ghost-4.6-alpine`) avant la mise à niveau vers la version finale (`ghost-latest`) pour la préparer à la production. Ils publient ensuite une mise à niveau de l'application clonée vers le cluster OpenShift de production s'exécutant sur un autre système FlexPod.
2. À ce stade, l'application est mise à niveau vers la dernière version et prête à être clonée sur le cluster de production.



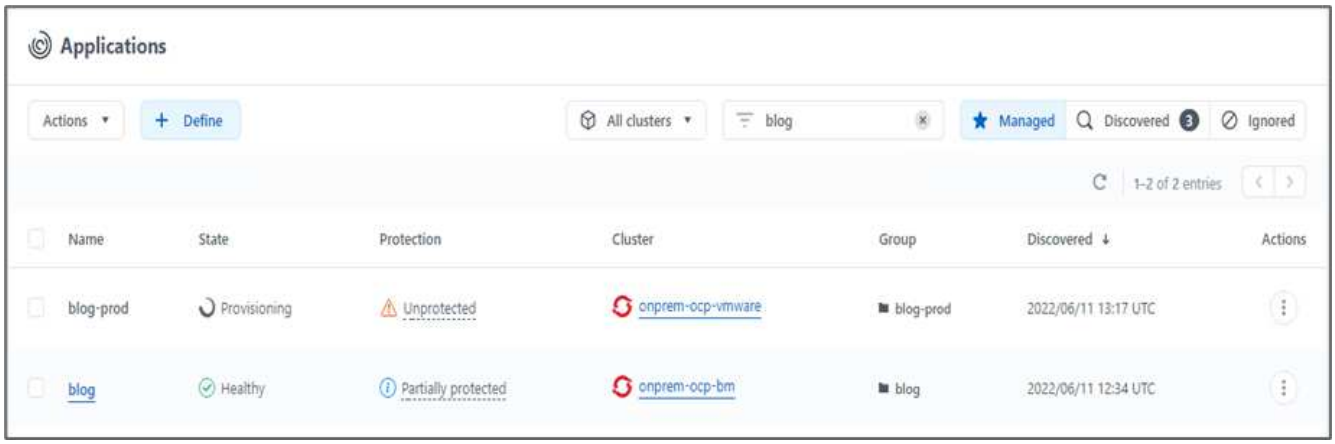
3. Pour vérifier le nouveau thème, actualisez le site du blog.



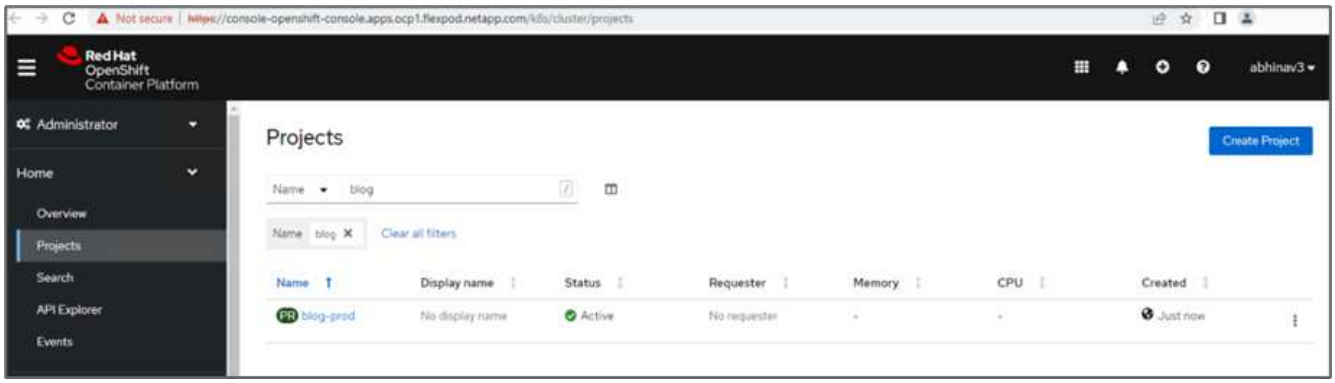
4. À partir d'Astra Control Center, clonez l'application vers l'autre cluster OpenShift de production qui s'exécute sur VMware vSphere.



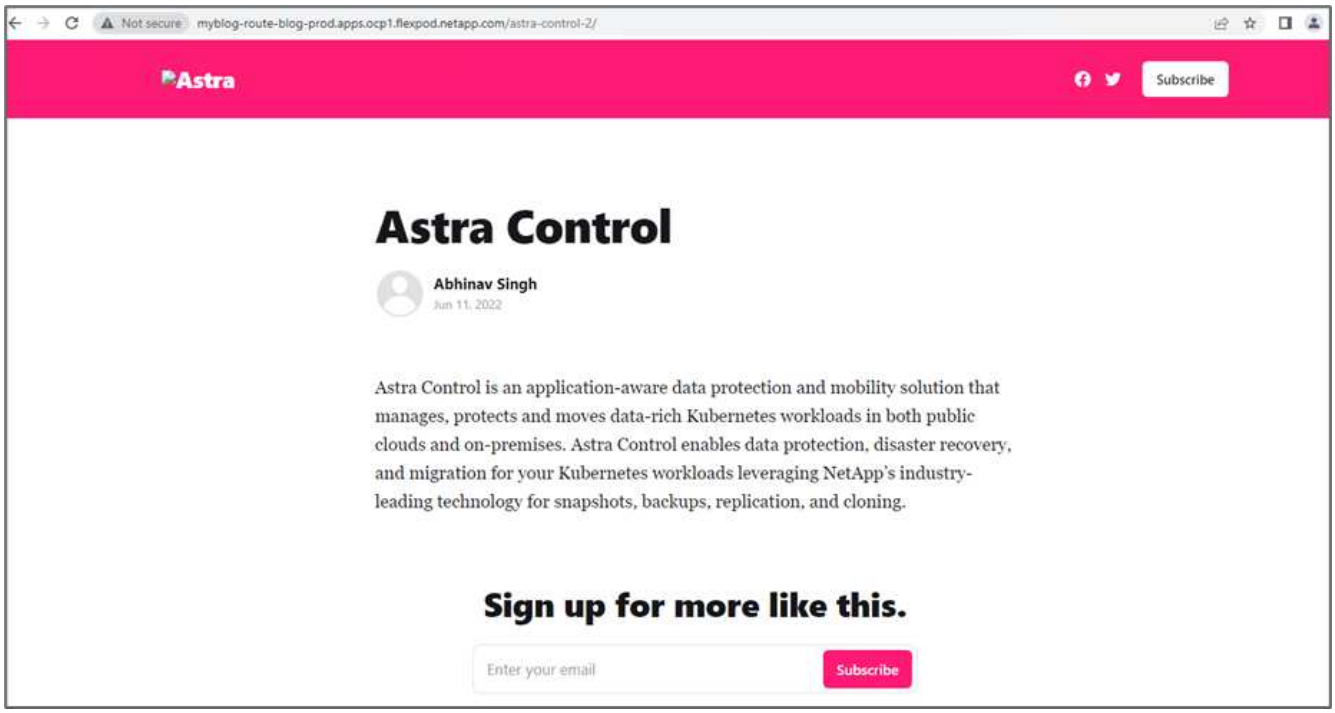
Un nouveau clone d'application est désormais provisionné dans le cluster OpenShift de production.



5. Connectez-vous au cluster OpenShift de production et recherchez le blog du projet.



6. Dans le menu latéral, sélectionnez réseau > itinéraires et cliquez sur l'URL sous emplacement. La même page d'accueil avec le contenu s'affiche.



La validation de la solution Astra Control Center est maintenant terminée. Vous pouvez désormais cloner une application et ses données d'un cluster Kubernetes à un autre, quel que soit l'emplacement du cluster Kubernetes.

"Suivant: Conclusion."

Conclusion

"Précédente : restauration d'applications avec sauvegardes distantes."

Avec cette solution, nous avons mis en œuvre un plan de protection pour les applications conteneurisées qui sont exécutées sur FlexPod et AWS à l'aide du portefeuille NetApp Astra. NetApp Astra Control Center et Astra Trident, ainsi que Cloud Volumes ONTAP, Red Hat OpenShift et l'infrastructure FlexPod, ont constitué les principaux composants de cette solution.

Nous avons démontré la protection des applications en capturant des snapshots et en exécutant des sauvegardes complètes afin de restaurer les applications sur différents clusters K8s exécutés sur les environnements cloud et sur site.

Nous avons également démontré le clonage des applications sur les clusters K8s, afin de permettre aux clients de migrer leurs applications vers les clusters K8s de leur choix.

FlexPod a constamment évolué pour permettre à ses clients de moderniser leurs applications et leurs processus de fourniture d'informations. Avec cette solution, les clients de FlexPod peuvent créer en toute confiance leur plan de reprise après incident BCDR pour leurs applications cloud natives, en utilisant le cloud public comme emplacement dans le cadre d'un plan de reprise après incident transitoire ou à temps complet, tout en conservant le coût de la solution le plus bas.

Astra Control vous permet de déplacer une application avec ses données d'un cluster Kubernetes vers un autre, quel que soit l'emplacement des clusters. Elle accélère également le déploiement, les opérations et la protection de vos applications cloud.

Dépannage

Pour obtenir des conseils de dépannage, reportez-vous à la section "documentation en ligne".

Où trouver des informations complémentaires

Pour en savoir plus sur les informations données dans ce livre blanc, consultez ces documents et/ou sites web :

- Page d'accueil de FlexPod

  "https://www.flexpod.com"

- Guides de conception et de déploiement validés par Cisco pour FlexPod

  "https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html"

- Déploiement de FlexPod avec Infrastructure as code pour VMware avec Ansible

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_m6_esxi7u2.html#AnsibleAutomationWorkflowandSolutionDeployment"

- Déploiement de FlexPod avec Infrastructure as code pour Red Hat OpenShift bare Metal avec Ansible

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_iac_redhat_openshift.html"

- Outil d'interopérabilité matérielle et logicielle Cisco UCS

  "http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"

- Fiche technique Cisco Intersight

  "https://intersight.com/help/saas/home"

- Documentation NetApp Astra

  "https://docs.netapp.com/us-en/astra-control-center/index.html"

- NetApp Astra Control Center

  "https://docs.netapp.com/us-en/astra-control-center/index.html"

- NetApp Astra Trident

  "https://docs.netapp.com/us-en/trident/index.html"

- NetApp Cloud Manager

  "https://docs.netapp.com/us-en/occm/concept_overview.html"

- NetApp Cloud Volumes ONTAP

  "https://docs.netapp.com/us-en/occm/task_getting_started_aws.html"

- Red Hat OpenShift

  "https://www.openshift.com/"

- Matrice d'interopérabilité NetApp

  "http://support.netapp.com/matrix/"

Historique des versions

Version	Date	Historique des versions du document
Version 1.0	Juillet 2022	Lancement de l'ACC 22.04.0.

NetApp Cloud Insights pour FlexPod

Tr-4868 : NetApp Cloud Insights pour FlexPod

Alan Cowles, NetApp

En partenariat avec :

Dans ce rapport technique, la solution détaillée est la configuration du service NetApp Cloud Insights pour surveiller le système de stockage NetApp AFF A800 exécutant NetApp ONTAP, qui est déployé dans le cadre d'une solution FlexPod Datacenter.

En valeur pour le client

La description détaillée de cette solution apporte une valeur ajoutée aux clients qui souhaitent bénéficier d'une solution de surveillance complète pour leurs environnements de cloud hybride, dans lesquels ONTAP est déployé comme système de stockage principal. Cela inclut les environnements FlexPod qui utilisent les systèmes de stockage NetApp AFF et FAS.

Cas d'utilisation

Cette solution s'applique aux cas d'utilisation suivants :

- Organisations qui souhaitent surveiller différentes ressources et l'utilisation de leur système de stockage ONTAP déployé dans le cadre d'une solution FlexPod.
- Les entreprises qui souhaitent résoudre les problèmes et réduire le temps de résolution des incidents survenant dans la solution FlexPod avec leurs systèmes AFF ou FAS.
- Les entreprises intéressées par des projections d'optimisation des coûts, notamment des tableaux de bord personnalisés qui fournissent des informations détaillées sur la perte de ressources et permettent de réaliser des économies dans leur environnement FlexPod, y compris ONTAP.

Public visé

La solution cible plusieurs groupes d'utilisateurs :

- Cadres informatiques et ceux chargés de l'optimisation des coûts et de la continuité de l'activité.
- Architectes de solutions intéressés par la conception et la gestion de data centers ou de clouds hybrides.
- Ingénieurs du support technique chargés du dépannage et de la résolution d'incident.

Vous pouvez configurer Cloud Insights pour fournir plusieurs types de données utiles que vous pouvez utiliser pour vous aider dans la planification, la résolution de problèmes, la maintenance et la continuité de l'activité. En surveillant la solution de data Center de FlexPod avec Cloud Insights et présentant les données agrégées sous forme de tableaux de bord personnalisés facilement digestibles ; non seulement il est possible de prévoir quand les ressources d'un déploiement doivent évoluer pour répondre à leurs besoins, mais également d'identifier des applications ou des volumes de stockage spécifiques qui causent des problèmes au sein du système. Cela permet de s'assurer que l'infrastructure surveillée est prévisible et fonctionne selon les attentes, ce qui permet à une organisation de respecter les SLA définis et de faire évoluer l'infrastructure en fonction des besoins, éliminant ainsi le gaspillage et les coûts supplémentaires.

Architecture

Dans cette section, nous analysons l'architecture d'une infrastructure convergée FlexPod Datacenter, dont un système NetApp AFF A800 surveillé par Cloud Insights.

Technologie de la solution

La solution de data Center FlexPod comprend les composants minimum suivants afin de fournir un environnement d'infrastructure convergée haute disponibilité, facilement évolutif, validé et pris en charge.

- Deux nœuds de stockage NetApp ONTAP (une paire haute disponibilité)
- Deux commutateurs réseau pour data Center Cisco Nexus
- Deux commutateurs de structure Cisco MDS (en option pour les déploiements FC)
- Deux interconnexions de fabric Cisco UCS
- Un châssis lame Cisco UCS avec deux serveurs lames Cisco UCS B-Series

Ou

- Deux serveurs Cisco UCS C-Series montés en rack

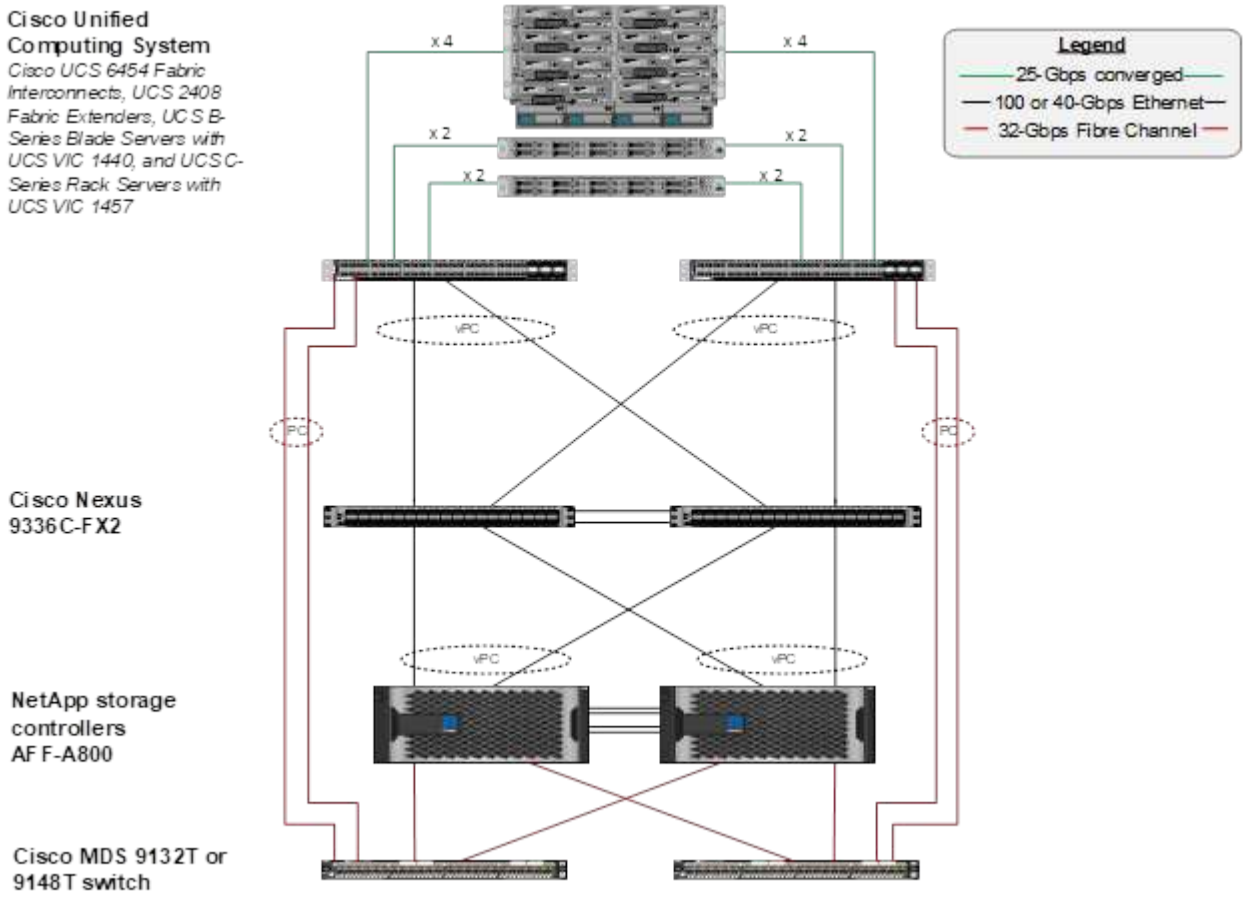
Pour que Cloud Insights puisse collecter des données, une entreprise doit déployer une unité d'acquisition en tant que machine virtuelle ou physique dans son environnement FlexPod Datacenter ou sur un emplacement où elle peut contacter les composants à partir desquels elle collecte les données. Vous pouvez installer le logiciel acquisition Unit sur un système exécutant plusieurs systèmes d'exploitation Windows ou Linux pris en charge. Le tableau suivant répertorie les composants de la solution pour ce logiciel.

Système d'exploitation	Version
Microsoft Windows	10
Serveur Microsoft Windows	2012, 2012 R2, 2016, 2019
Red Hat Enterprise Linux	7.2 – 7.6
CentOS	7.2 – 7.6

Système d'exploitation	Version
Oracle Enterprise Linux	7.5
Debian	9
Ubuntu	18.04 LTS

Diagramme architectural

La figure suivante illustre l'architecture de la solution.



Configuration matérielle requise

Le tableau suivant répertorie les composants matériels requis pour implémenter la solution. Ils peuvent varier selon la mise en œuvre de la solution et les besoins du client.

Sous-jacent	Quantité
Cisco Nexus 9336C-FX2	2
Fabric Interconnect Cisco UCS 6454	2
Châssis lame Cisco UCS 5108	1
Cisco UCS 2408 Fabric Extender	2
Lames Cisco UCS B200 M5	2

Sous-jacent	Quantité
NetApp AFF A800	2

Configuration logicielle requise

Le tableau suivant répertorie les composants logiciels requis pour implémenter la solution. Ils peuvent varier selon la mise en œuvre de la solution et les besoins du client.

Logiciel	Version
Firmware Cisco Nexus	9.3(5)
Version de Cisco UCS	4.1(2a)
Version de NetApp ONTAP	9.7
Version de NetApp Cloud Insights	Septembre 2020, Basic
Red Hat Enterprise Linux	7.6
VMware vSphere	6.7U3

Détails du cas d'utilisation

Cette solution s'applique aux cas d'utilisation suivants :

- L'analyse de l'environnement avec des données fournies au conseiller digital NetApp Active IQ pour évaluer les risques liés aux systèmes de stockage et formuler des recommandations sur l'optimisation du stockage.
- Résolution des problèmes dans le système de stockage ONTAP déployé dans une solution de data Center FlexPod en examinant les statistiques système en temps réel.
- Création de tableaux de bord personnalisés afin de surveiller facilement les points d'intérêt spécifiques pour les systèmes de stockage ONTAP déployés dans une infrastructure convergée FlexPod Datacenter.

Considérations relatives à la conception

La solution FlexPod Datacenter est une infrastructure convergée conçue par Cisco et NetApp offrant un environnement de data Center dynamique, extrêmement disponible et évolutif pour l'exécution des charges de travail d'entreprise. Les ressources de calcul et de réseau de la solution sont fournies par les produits Cisco UCS et Nexus, et les ressources de stockage sont fournies par le système de stockage ONTAP. La conception de la solution est régulièrement optimisée lorsque des modèles matériels ou logiciels et micrologiciels mis à jour sont disponibles. Ces détails, ainsi que les meilleures pratiques de conception et de déploiement de solutions, sont publiés régulièrement dans des documents CVD (Cisco Validated Design) ou NVA (NetApp Verified Architecture).

Le dernier document CVD détaillant la conception de la solution FlexPod Datacenter est disponible "ici".

Déployez Cloud Insights pour FlexPod

Pour déployer la solution, vous devez effectuer les tâches suivantes :

1. Abonnez-vous au service Cloud Insights
2. Créez une machine virtuelle VMware (VM) à configurer comme unité d'acquisition
3. Installez l'hôte Red Hat Enterprise Linux (RHEL)
4. Créez une instance d'unité d'acquisition dans le portail Cloud Insights et installez le logiciel
5. Ajoutez le système de stockage surveillé du data Center FlexPod à Cloud Insights.

Abonnez-vous au service NetApp Cloud Insights

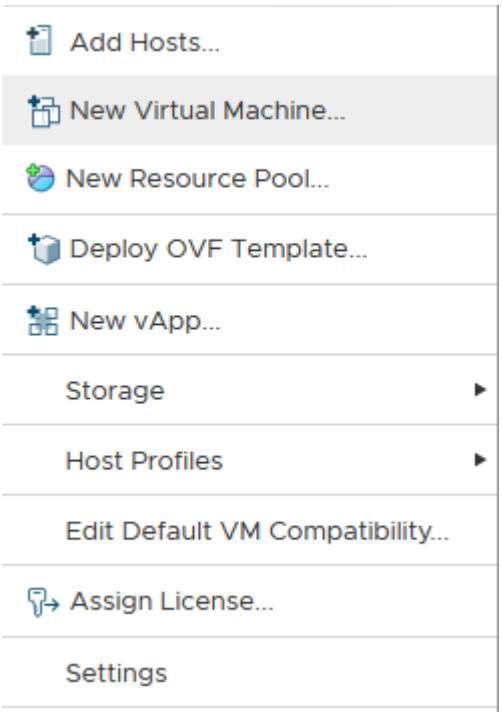
Pour vous inscrire au service NetApp Cloud Insights, procédez comme suit :

1. Accédez à "https://cloud.netapp.com/cloud-insights"
2. Cliquez sur le bouton au centre de l'écran pour lancer l'essai gratuit de 14 jours ou sur le lien en haut à droite pour vous inscrire ou vous connecter à un compte NetApp Cloud Central.

Créez une machine virtuelle VMware à configurer en tant qu'unité d'acquisition

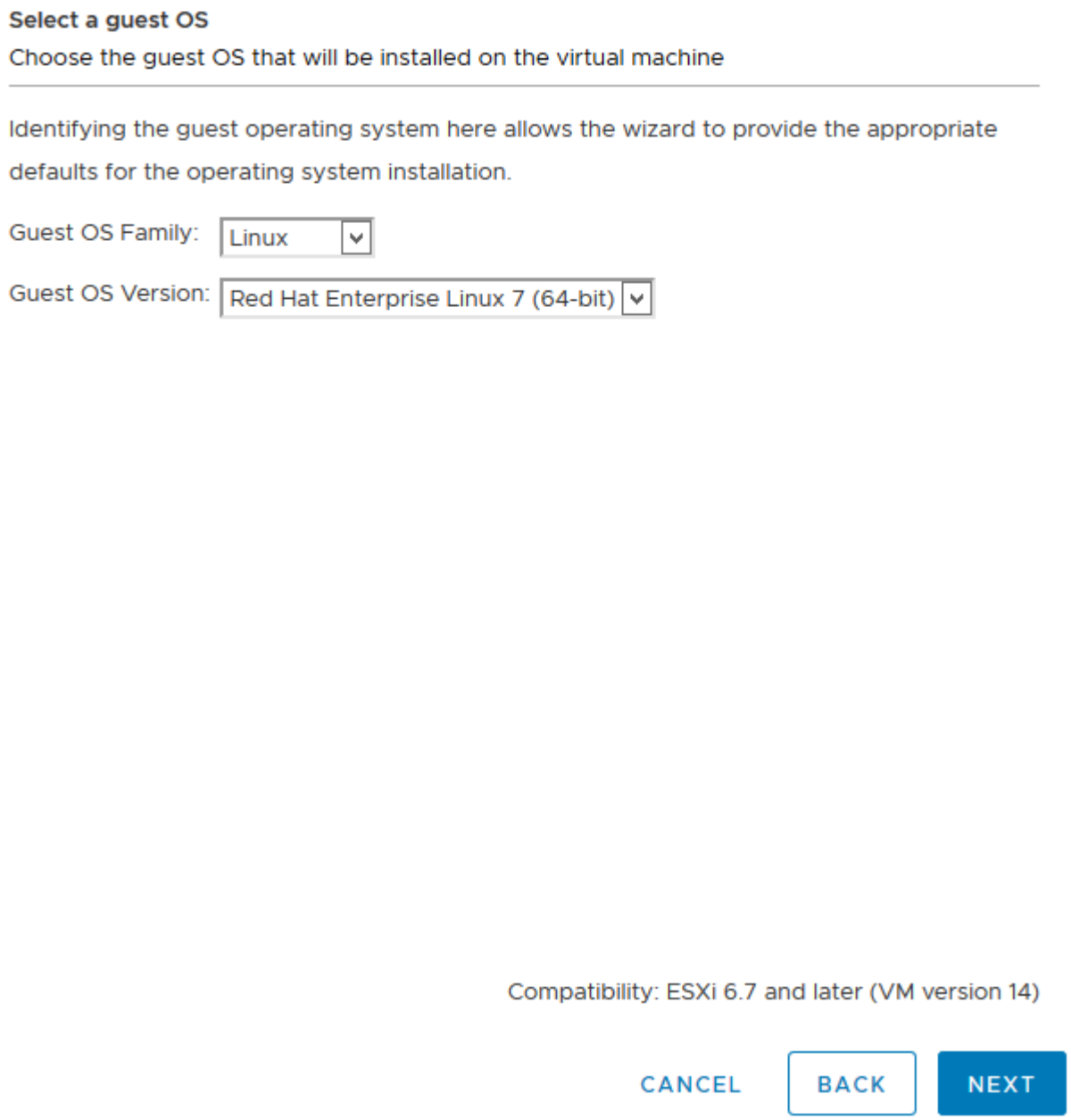
Pour créer un VM VMware à configurer comme unité d'acquisition, procédez comme suit :

1. Lancez un navigateur Web, connectez-vous à VMware vSphere et sélectionnez le cluster que vous souhaitez héberger.
2. Cliquez avec le bouton droit de la souris sur ce cluster et sélectionnez Créer Une machine virtuelle dans le menu.



3. Dans l'assistant New Virtual machine (Nouvelle machine virtuelle), cliquez sur Next (Suivant).
4. Indiquez le nom de la machine virtuelle, puis sélectionnez le data Center auquel vous souhaitez l'installer, puis cliquez sur Next (Suivant).
5. Sur la page suivante, sélectionnez le cluster, les nœuds ou le groupe de ressources auquel vous souhaitez installer la machine virtuelle, puis cliquez sur Suivant.

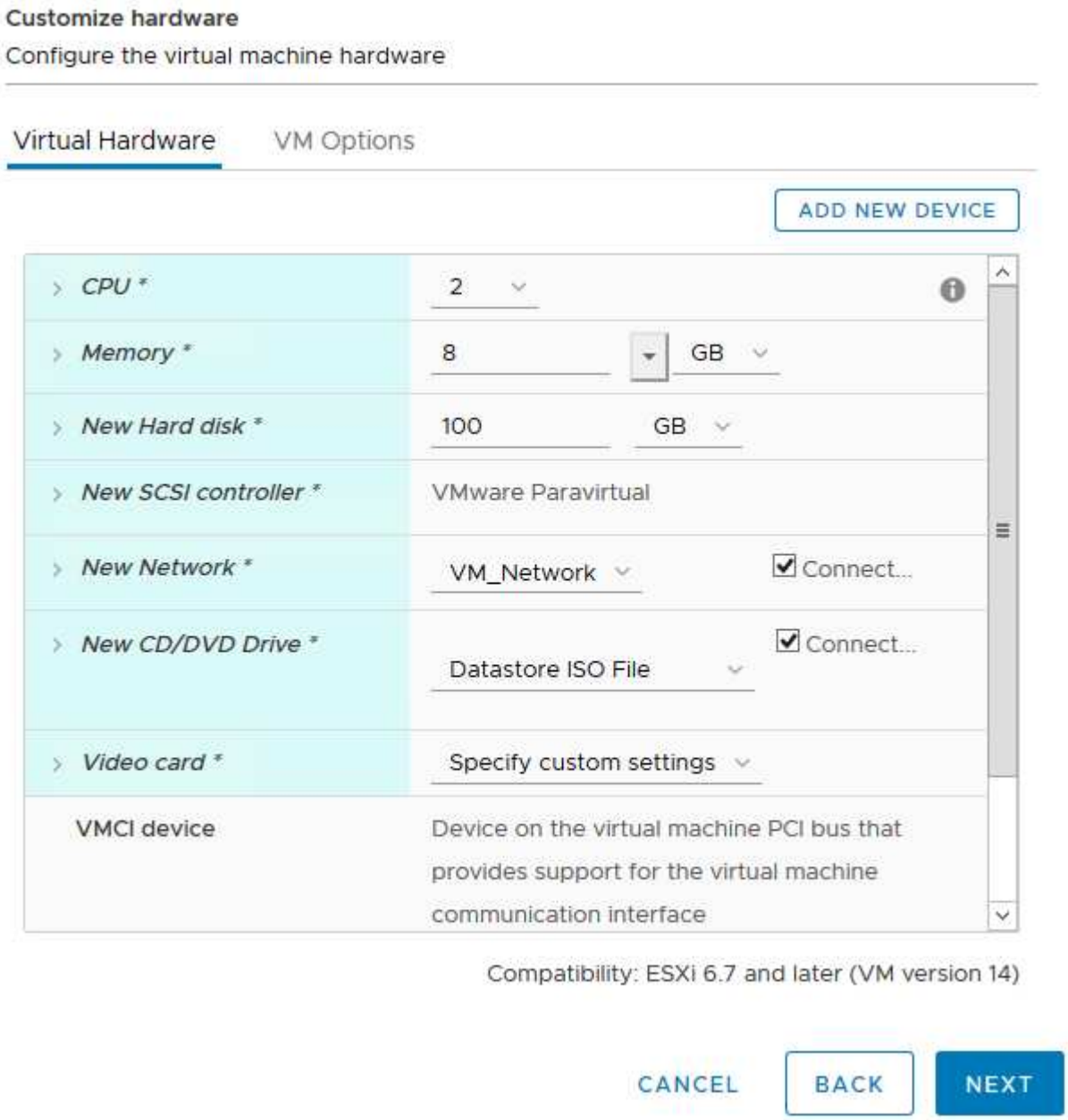
6. Sélectionnez le datastore partagé qui héberge vos machines virtuelles et cliquez sur Next (Suivant).
7. Vérifiez que le mode de compatibilité de la machine virtuelle est défini sur `ESXi 6.7 or later` Et cliquez sur Suivant.
8. Sélectionnez Guest OS Family Linux, Guest OS version : Red Hat Enterprise Linux 7 (64 bits).



9. La page suivante permet la personnalisation des ressources matérielles sur la machine virtuelle. L'unité d'acquisition Cloud Insights nécessite les ressources suivantes. Une fois les ressources sélectionnées, cliquez sur Suivant :
   a. Deux processeurs
   b. 8 Go de RAM
   c. 100 Go d'espace disque
   d. Réseau pouvant accéder aux ressources dans le centre de données FlexPod et le serveur Cloud

Insights via une connexion SSL sur le port 443.

e. Image ISO de la distribution Linux choisie (Red Hat Enterprise Linux) à partir de laquelle démarrer.

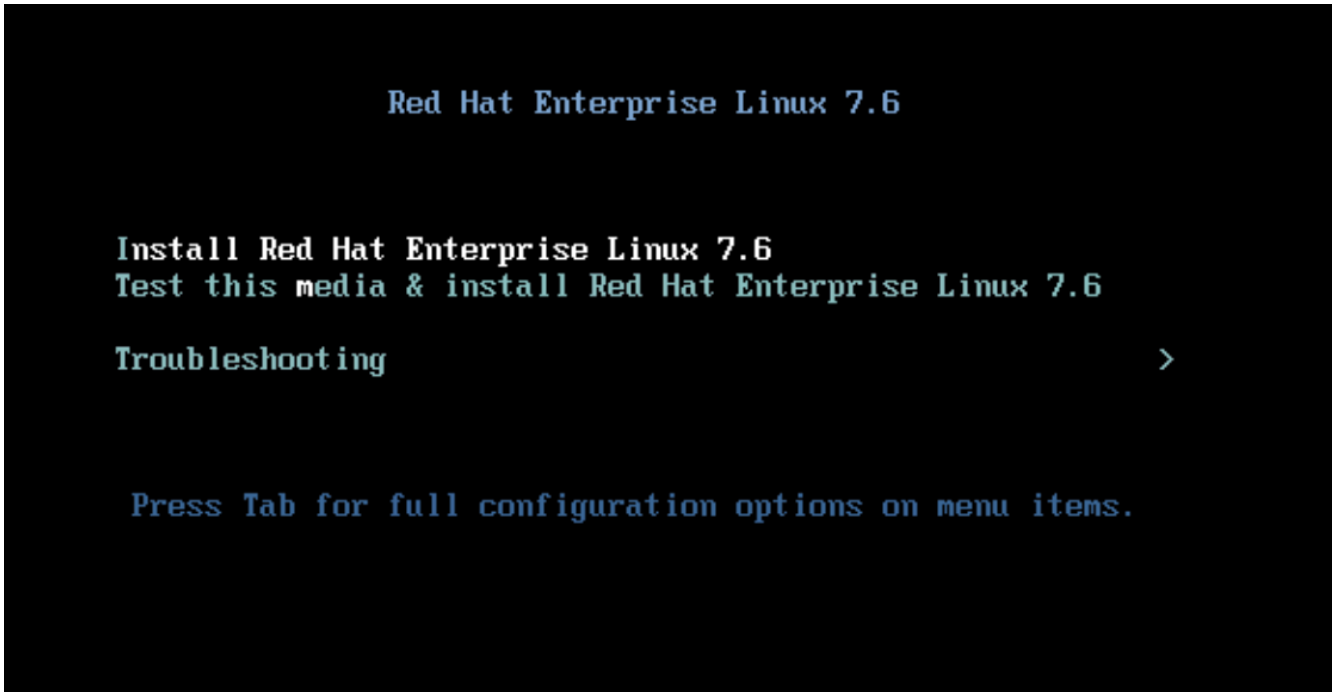


10. Pour créer la machine virtuelle, sur la page Ready to Complete (prêt à terminer), vérifiez les paramètres et cliquez sur Finish (Terminer).

Installez Red Hat Enterprise Linux

Pour installer Red Hat Enterprise Linux, procédez comme suit :

1. Mettez la machine virtuelle sous tension, cliquez sur la fenêtre pour lancer la console virtuelle, puis sélectionnez l’option d’installation de Red Hat Enterprise Linux 7.6.

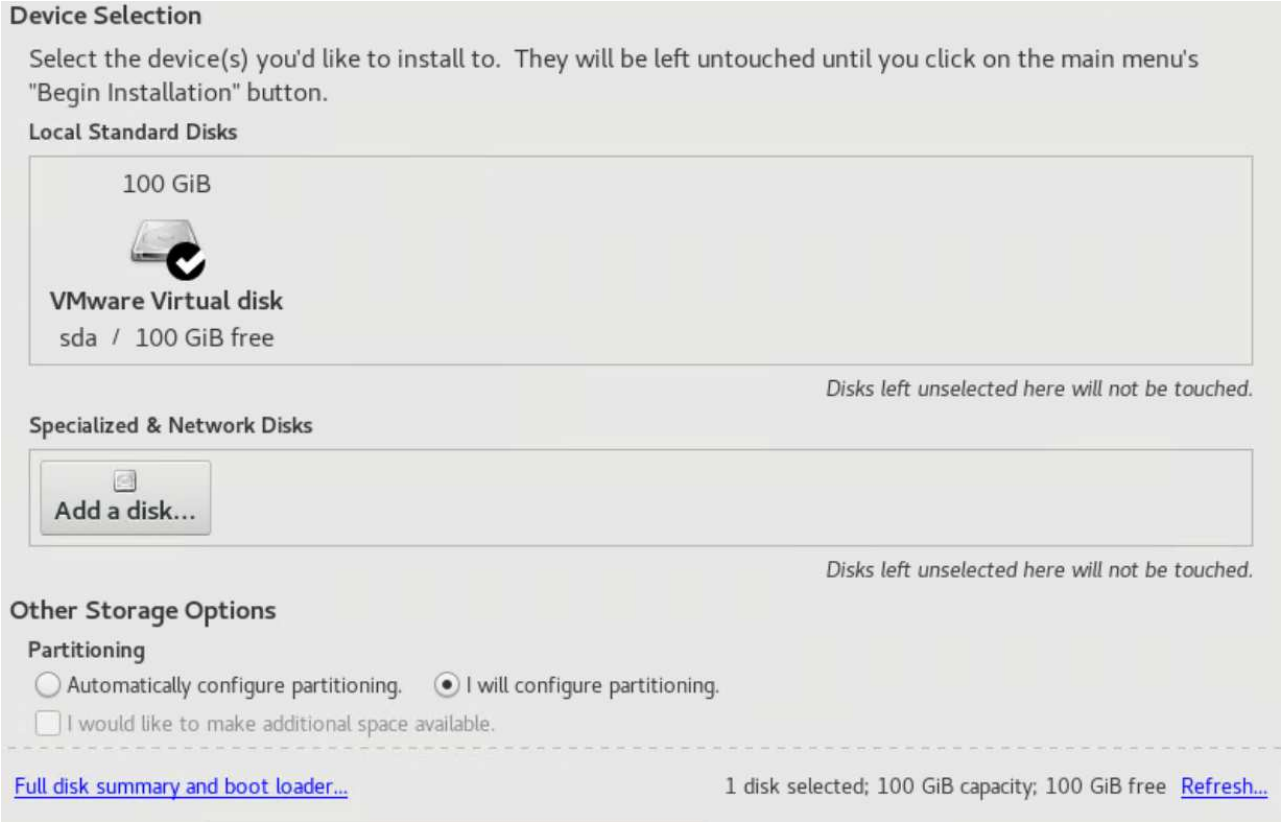


2. Sélectionnez la langue de votre choix et cliquez sur Continuer.

   La page suivante est le résumé de l'installation. Les paramètres par défaut doivent être acceptables pour la plupart de ces options.

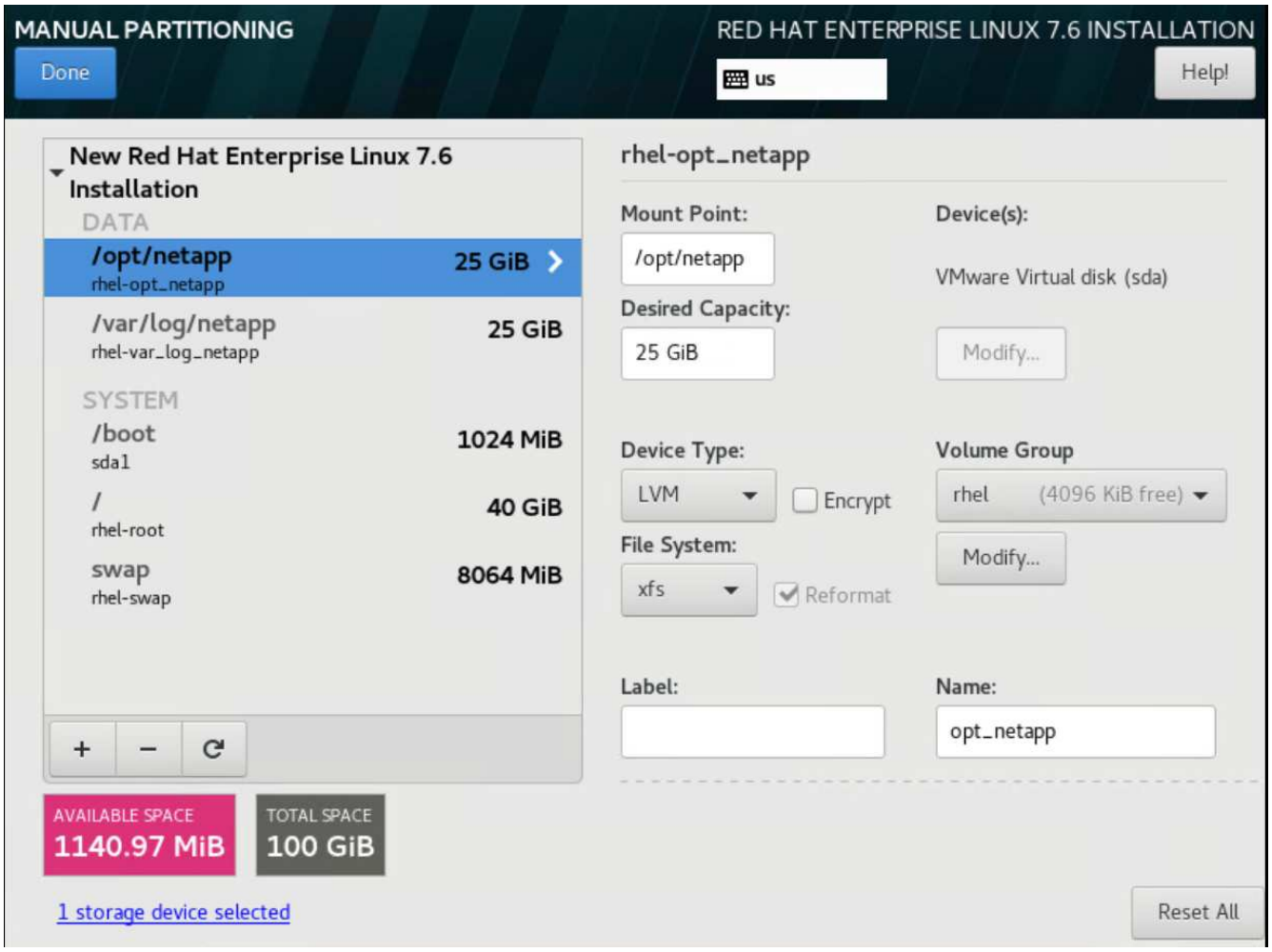
3. Vous devez personnaliser l'organisation du stockage en effectuant les options suivantes :

   a. Pour personnaliser le partitionnement du serveur, cliquez sur destination de l'installation.
   b. Vérifier que le disque virtuel VMware de 100 Gio est sélectionné avec une coche noire et sélectionner le bouton radio I will configure Partitioning.



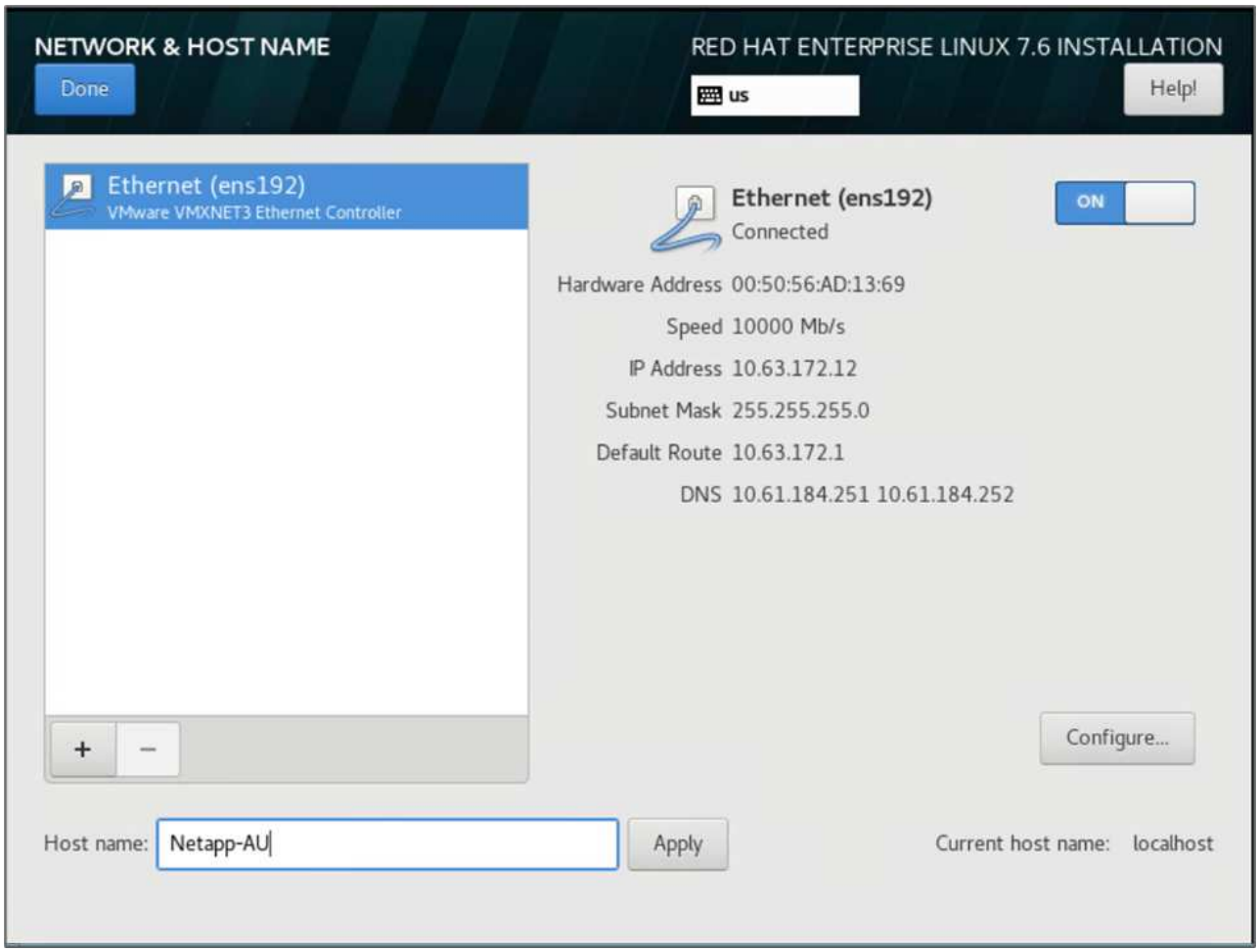
c. Cliquez sur terminé.

   Un nouveau menu s'affiche pour vous permettre de personnaliser la table de partition. Dédier 25 Go à chaque `/opt/netapp` et `/var/log/netapp`. Vous pouvez allouer automatiquement le reste du stockage au système.



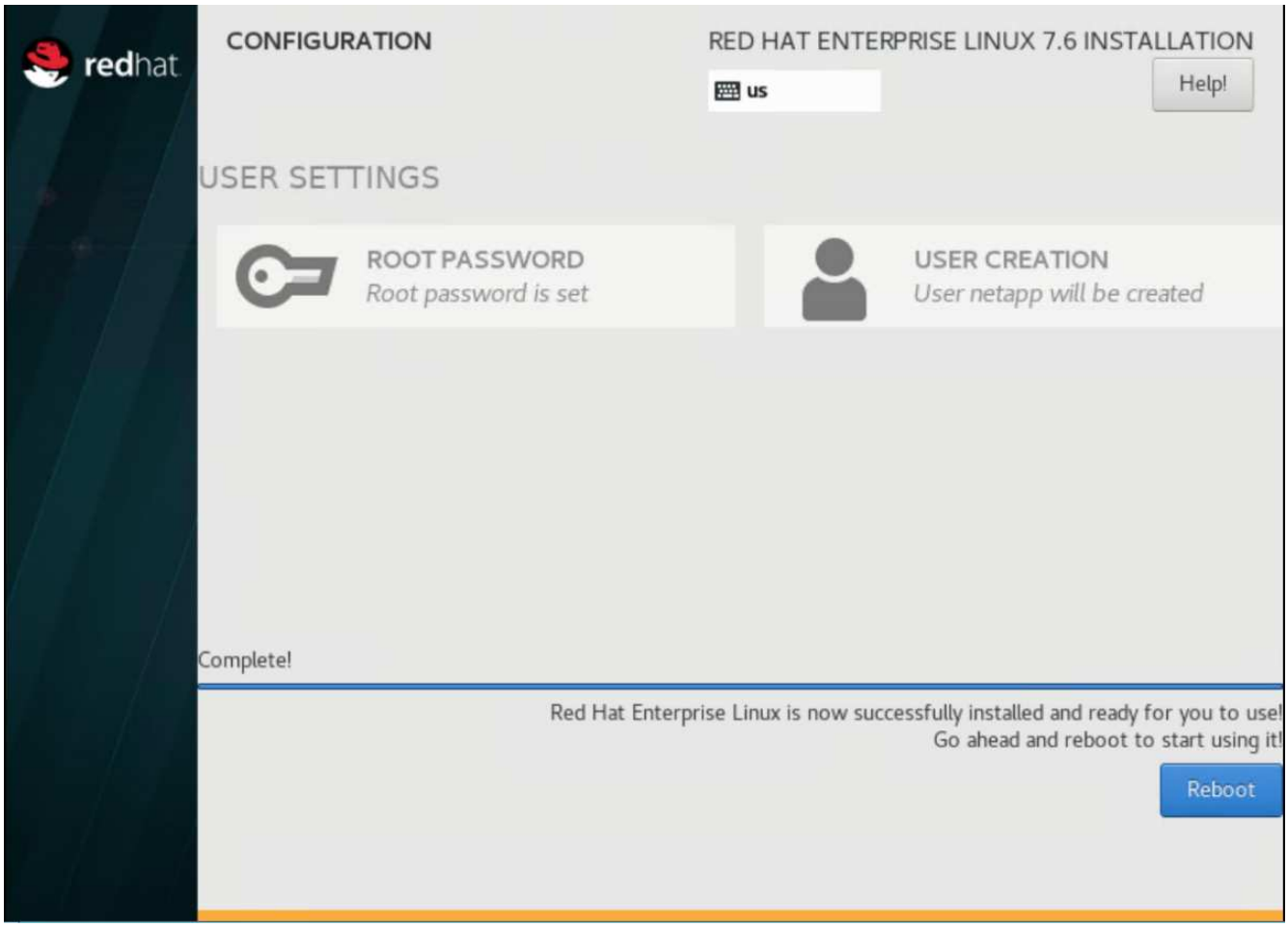
a. Pour revenir au résumé de l'installation, cliquez sur terminé.

4. Cliquez sur Nom du réseau et de l'hôte.
   a. Entrez un nom d'hôte pour le serveur.
   b. Activez la carte réseau en cliquant sur le curseur. Si le protocole DHCP (Dynamic Host Configuration Protocol) est configuré sur votre réseau, vous recevrez une adresse IP. Si ce n'est pas le cas, cliquez sur configurer et attribuez une adresse manuellement.



c. . Cliquez sur terminé pour revenir au résumé de l'installation.

5. Sur la page Récapitulatif d'installation, cliquez sur commencer l'installation.
6. Sur la page progression de l'installation, vous pouvez définir le mot de passe racine ou créer un compte utilisateur local. Une fois l'installation terminée, cliquez sur redémarrer pour redémarrer le serveur.



7. Une fois le système redémarré, connectez-vous à votre serveur et enregistrez-le à l'aide de Red Hat Subscription Manager.

```
[root@Netapp-AU ~]# subscription-manager register
Registering to: subscription.rhsm.redhat.com:443/subscription
Username: alan.cowles@netapp.com
Password:
The system has been registered with ID: a47f2e7b-81cd-4757-85c7-eb1818c2c2a1
The registered system name is: Netapp-AU
[root@Netapp-AU ~]#
```

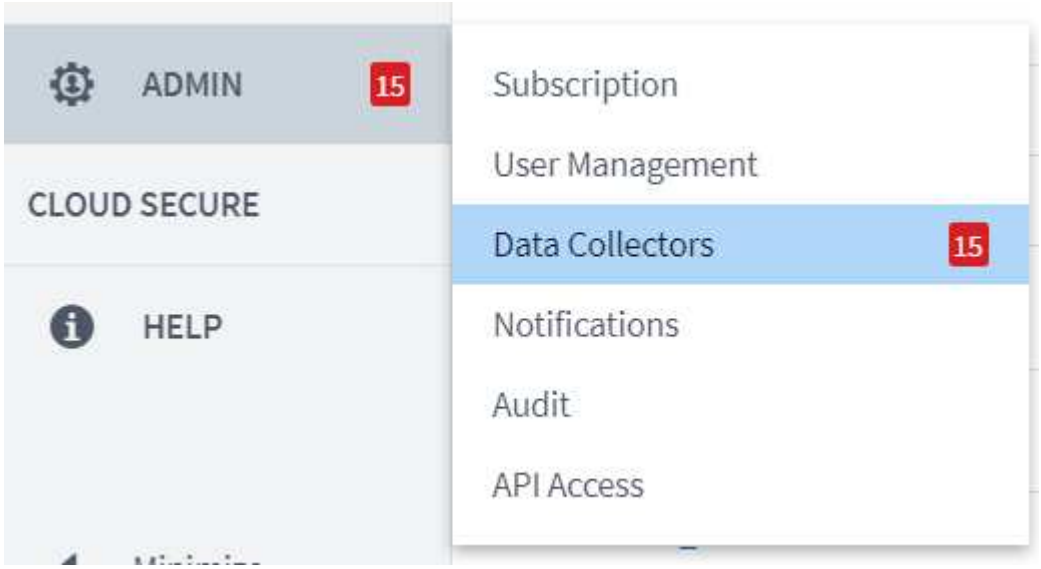
8. Joignez un abonnement disponible à Red Hat Enterprise Linux.

```
[root@Netapp-AU ~]# subscription-manager attach --pool=8a85f99b710f3b1901713b90b9e154cf
Successfully attached a subscription for: Red Hat Enterprise Linux, Standard Support (128 Sockets, NFR, Partner Only)
[root@Netapp-AU ~]#
```

Créez une instance d'unité d'acquisition dans le portail Cloud Insights et installez le logiciel

Pour créer une instance d'unité d'acquisition sur le portail Cloud Insights et installer le logiciel, procédez comme suit :

1. Sur la page d'accueil de Cloud Insights, passez le curseur de la souris sur l'entrée Admin du menu principal vers la gauche et sélectionnez Data Collectors dans le menu.



2. En haut au centre de la page collecteurs de données, cliquez sur le lien unités d'acquisition.

3. Pour créer une nouvelle unité d'acquisition, cliquez sur le bouton à droite.

4. Sélectionnez le système d'exploitation que vous souhaitez utiliser pour héberger votre unité d'acquisition et suivez les étapes pour copier le script d'installation à partir de la page Web.

   Dans cet exemple, il s'agit d'un serveur Linux, qui fournit un fragment et un jeton à coller dans la CLI de notre hôte. La page Web attend que l'unité d'acquisition se connecte.

Install Acquisition Unit

Cloud Insights collects device data via one or more Acquisition Units installed on local servers. Each Acquisition Unit can host multiple Data Collectors, which send device metrics to Cloud Insights for analysis.

What Operating System or Platform Are You Using?

Linux | Linux Versions Supported | Production Best Practices

Installation Instructions | Need Help?

1. Copy Installer Snippet

This snippet has a unique key valid for 24 hours for this Acquisition Unit only.

Reveal Installer Snippet


```
token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzM4NCJ9.eyJhdWxvZ2luVXJsIjoiaHR0cHM6Ly9hdWxvZ2luLmMwMS
5jbG91ZGluc2lnaHRzLm5ldGFwcC5jb20iLCJvbmV0aW1lVG9rZW5JZCI6IjdkYzI1ZWNjLWU5MjctNDQ4YS05NmV
hLThlNDJkYWIwOGI2MyIsInJvbGVzIjpbImFjcXVpc2l0aW9uX3NpZ25lciJdLCJzZXJ2ZXJVcmwiOiJodHRwczov
LzhkNDE5NWE2LWViYjgtNGFkMC1hNmVmLTQxMzAyMzQwYjVhZi5jMDEuY2xvdWRpbnNpZ2h0cy5uZXRhcHAuY29tI
iwiaXNzIjoib2NpIiwiZXhwIjoxNjAyMDk5MjA2LCJsb2dpbiI6ImFjcXVpc2l0aW9uLjAzOTI0MDIyLTg2YzQtND
JmMC1hZDJmLWFhYWE1ZDEzMzhhMiIsImlhdCI6MTYwMjAxMjc0NiwidXVpZCI6IjAzOTI0MDIyLTg2YzQtNDJmMC1
```


2. Paste the snippet into a bash shell to run the installer.

3. Please ensure you have copied and pasted the snippet into the bash shell.

5. Collez le fragment dans la CLI de la machine Red Hat Enterprise Linux qui a été provisionnée, puis cliquez sur entrée.


```
[root@Netapp-AU ~]# token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzM4NCJ9.eyJhdWxvZ2luVXJsIjoiaHR0cHM6Ly9hdWxvZ2luLmMwMS5jbG91ZGluc
2lnaHRzLm5ldGFwcC5jb20iLCJvbmV0aW1lVG9rZW5JZCI6IjQ5ZTY0MGM5LTY5MTItNDQ4Yi04YmI4LTIwNGY2OTQ2YzY1YSIsInJvbGVzIjpbImFjcXVpc
2l0aW9uX3NpZ25lciJdLCJzZXJ2ZXJVcmwiOiJodHRwczovLzhkNDE5NWE2LWViYjgtNGFkMC1hNmVmLTQxMzAyMzQwYjVhZi5jMDEuY2xvdWRpbnNpZ2h0c
y5uZXRhcHAuY29tIiwiaXNzIjoib2NpIiwiZXhwIjoxNjAyMTgyNzg2LCJsb2dpbiI6ImFjcXVpc2l0aW9uLjc4MTliZGI3LTk5OWQtNGNiYS05YmU1LTMwZ
TcxZjk0ODRiZCIsImlhdCI6MTYwMjA5NjMyNiwidXVpZCI6Ijc4MTliZGI3LTk5OWQtNGNiYS05YmU1LTMwZTcxZjk0ODRiZCIsInRlbmFudCI6IjhkNDE5N
WE2LWViYjgtNGFkMC1hNmVmLTQxMzAyMzQwYjVhZiIsInRlbmFudFN1YmRvbWFpbiI6InBzMTMyNSJ9.RvWLR3wH1_k6fIOCiO_h-Wok2STfFPDj7VksmXqw
-GZ-JqSIe8SZE4Sv3DuWrWM6 domainUrl=https://8d4195a6-ebb8-4ad0-a6ef-41302340b5af.c01.cloudinsights.netapp.com/rest/v1/au
version=1.253.0 bootstrap=cloudinsights-au-install-bootstrap.sh && curl $proxy_auth_scheme -H "Authorization: Bearer $to
ken" -o $bootstrap $domainUrl/installerBootstrap && sudo chmod 755 $bootstrap && sudo /bin/bash -c "TOKEN=$token HTTPS_P
ROXY=$https_proxy PROXY_AUTH_SCHEME=$proxy_auth_scheme AU_VERSION=$version INSTALLER_NAME=cloudinsights-linux-au-install
er-$version INSTALLER_URL=$domainUrl/installers/linux/$version ./$bootstrap"
```

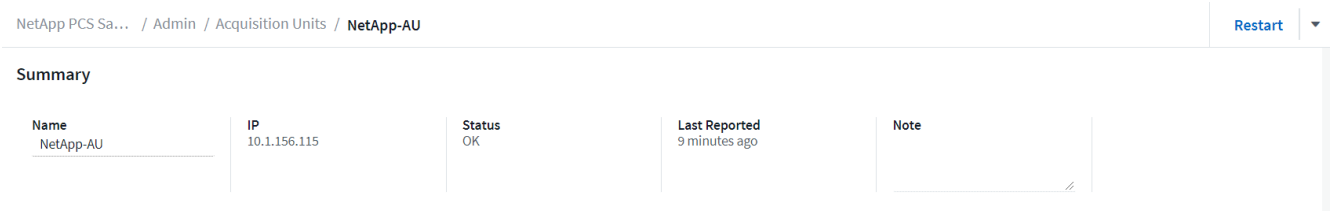

Le programme d'installation télécharge un package compressé et commence l'installation. Une fois l'installation terminée, vous recevez un message indiquant que l'unité d'acquisition a été enregistrée auprès de NetApp Cloud Insights.

```
Welcome to CloudInsights (R) ..
Acquisition Unit

NetApp (R)
Installation: /opt/netapp/cloudinsights
Logs:         /opt/netapp/cloudinsights/logs -> /var/log/netapp/cloudinsights

To control the CloudInsights service:
  sudo cloudinsights-service.sh --help
To uninstall:
  sudo cloudinsights-uninstall.sh --help

1/8 Acquisition Unit Starting
2/8 Connecting to Cloud Insights
3/8 Sending Certificate-Signing Request..
4/8 Logging in to Cloud Insights
5/8 Updating Security Settings..
6/8 Downloading Data Collection Modules
7/8 Registering to Cloud Insights
8/8 Acquisition Unit Ready

Acquisition Unit has been installed successfully.
[root@Netapp-AU ~]#
```

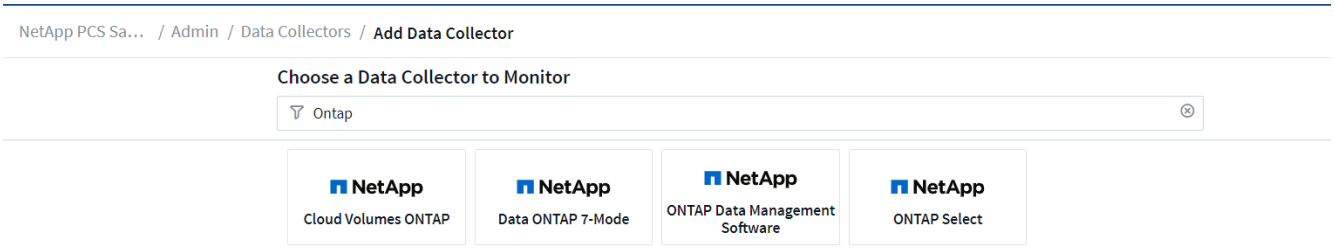
Ajoutez le système de stockage surveillé du data Center FlexPod à Cloud Insights

Pour ajouter le système de stockage ONTAP à partir d'un déploiement FlexPod, procédez comme suit :

1. Revenez à la page unités d'acquisition sur le portail Cloud Insights et recherchez l'unité nouvellement enregistrée. Pour afficher un résumé de l'unité, cliquez sur l'unité.

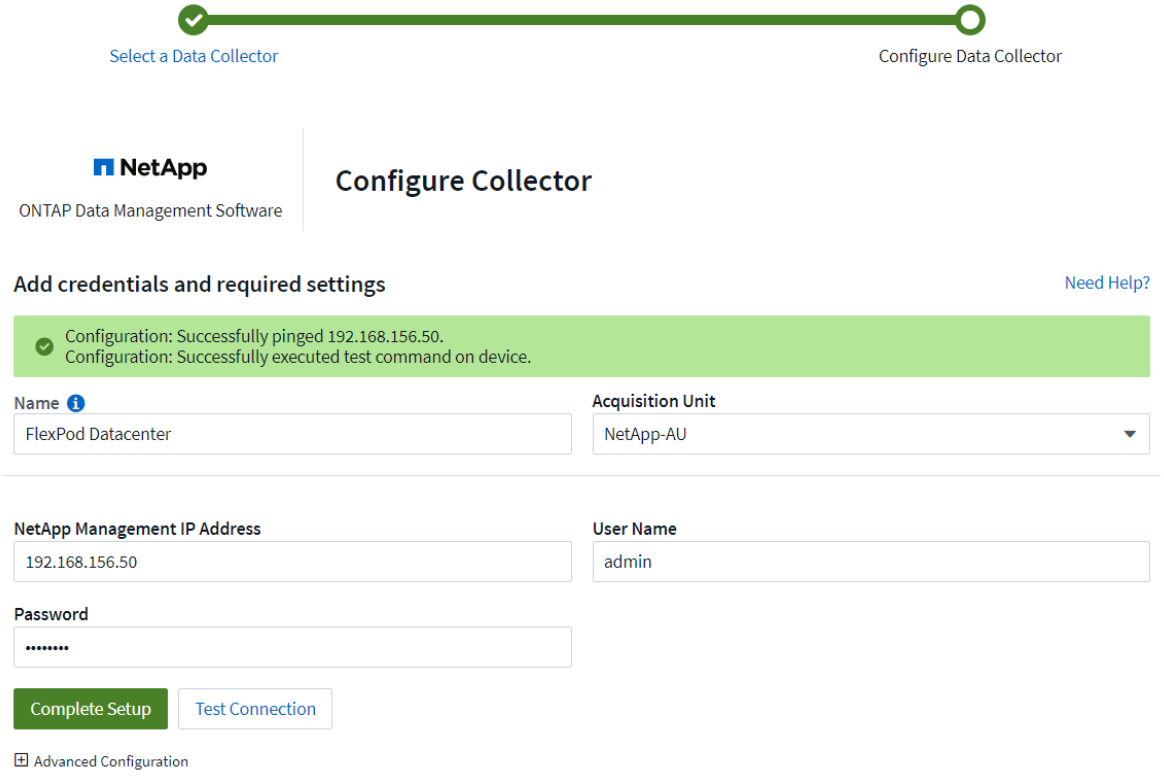


2. Pour démarrer un assistant pour ajouter le système de stockage, sur la page Résumé, cliquez sur le bouton de création d'un collecteur de données. La première page affiche tous les systèmes à partir desquels les données peuvent être collectées. Utilisez la barre de recherche pour rechercher ONTAP.



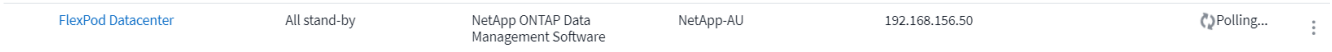
3. Sélectionnez logiciel de gestion des données ONTAP.

   Une page s'affiche pour vous permettre de nommer votre déploiement et de sélectionner l'unité d'acquisition que vous souhaitez utiliser. Vous pouvez fournir les informations d'identification et les informations de connectivité du système ONTAP et tester la connexion pour confirmer.



4. Cliquez sur Terminer la configuration.

   Le portail revient sur la page Data Collectors et le collecteur de données commence son premier sondage pour collecter les données du système de stockage ONTAP dans le FlexPod Datacenter.



Cas d'utilisation

Grâce à l'installation et à la configuration de Cloud Insights, nous FlexPod examinons

certaines des tâches que vous pouvez effectuer sur le tableau de bord afin d'évaluer et de contrôler votre environnement. Dans cette section, nous nous concentrons sur cinq cas d'utilisation principaux de Cloud Insights :

- Intégration avec Active IQ
- Exploration des tableaux de bord en temps réel
- Création de tableaux de bord personnalisés
- Dépannage avancé
- Optimisation du stockage

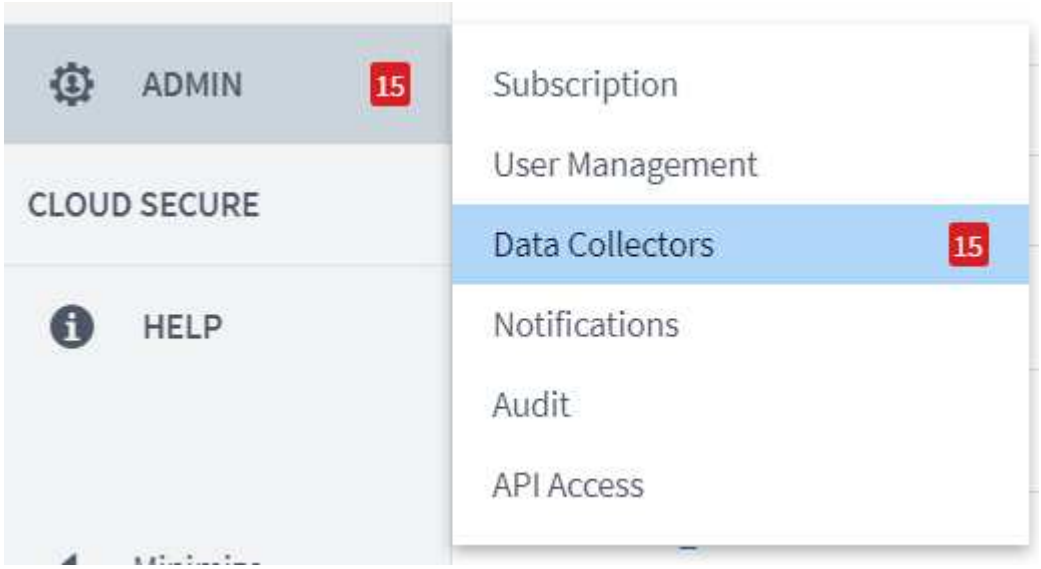
Intégration avec Active IQ

Cloud Insights est totalement intégré à la plateforme de surveillance du stockage Active IQ. Un système ONTAP, déployé dans le cadre d'une solution de data Center FlexPod, est automatiquement configuré pour renvoyer les informations à NetApp via la fonction AutoSupport, qui est intégrée à chaque système. Ces rapports sont générés de manière programmée ou dynamique lorsqu'une panne est détectée dans le système. Les données communiquées via AutoSupport sont agrégées et affichées dans des tableaux de bord facilement accessibles sous le menu Active IQ de Cloud Insights.

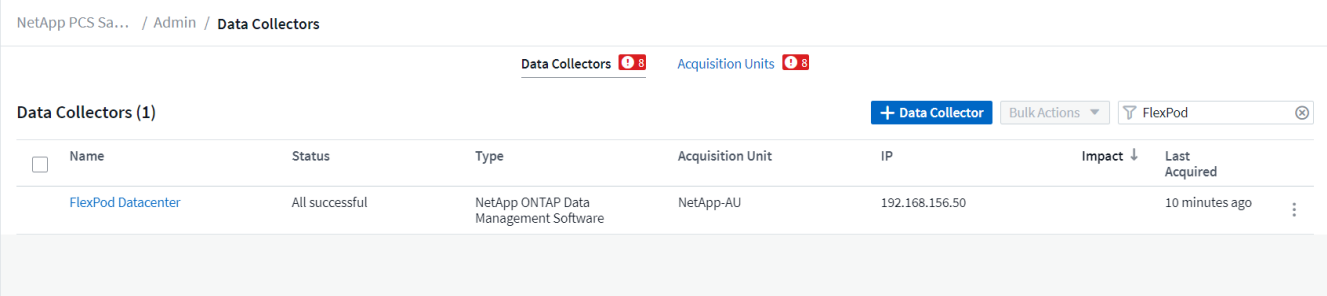
Accédez aux informations Active IQ via le tableau de bord Cloud Insights

Pour accéder aux informations de Active IQ via le tableau de bord Cloud Insights, effectuez les opérations suivantes :

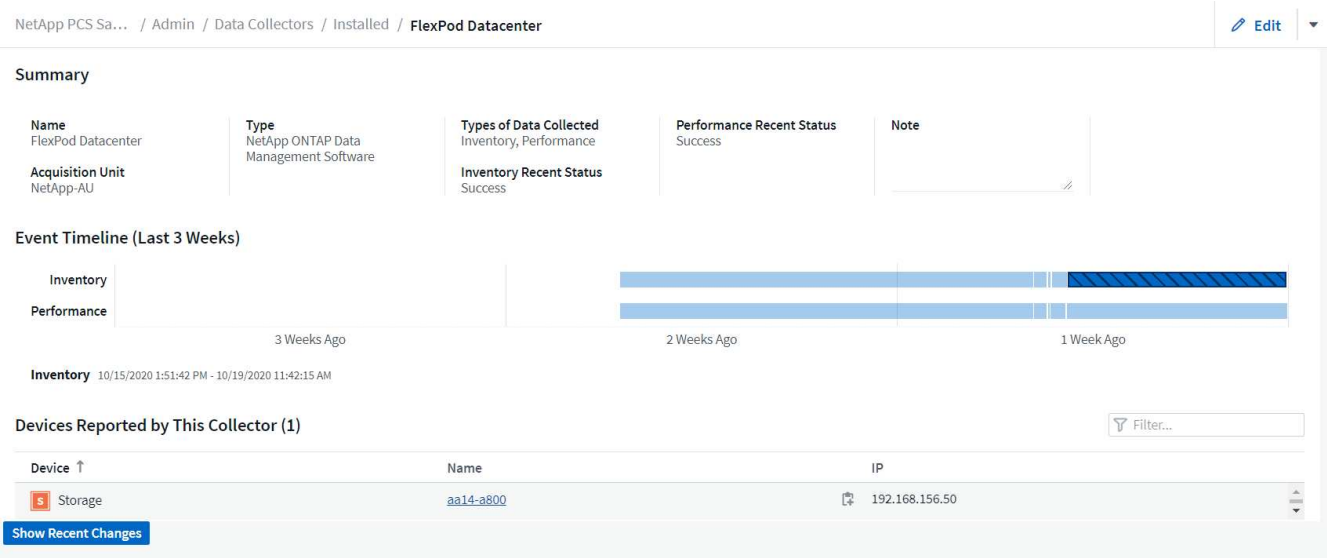
1. Cliquez sur l'option Data Collector dans le menu Admin à gauche.



2. Filtre pour le Data Collector spécifique à votre environnement. Dans cet exemple, nous filtrons par le terme FlexPod.

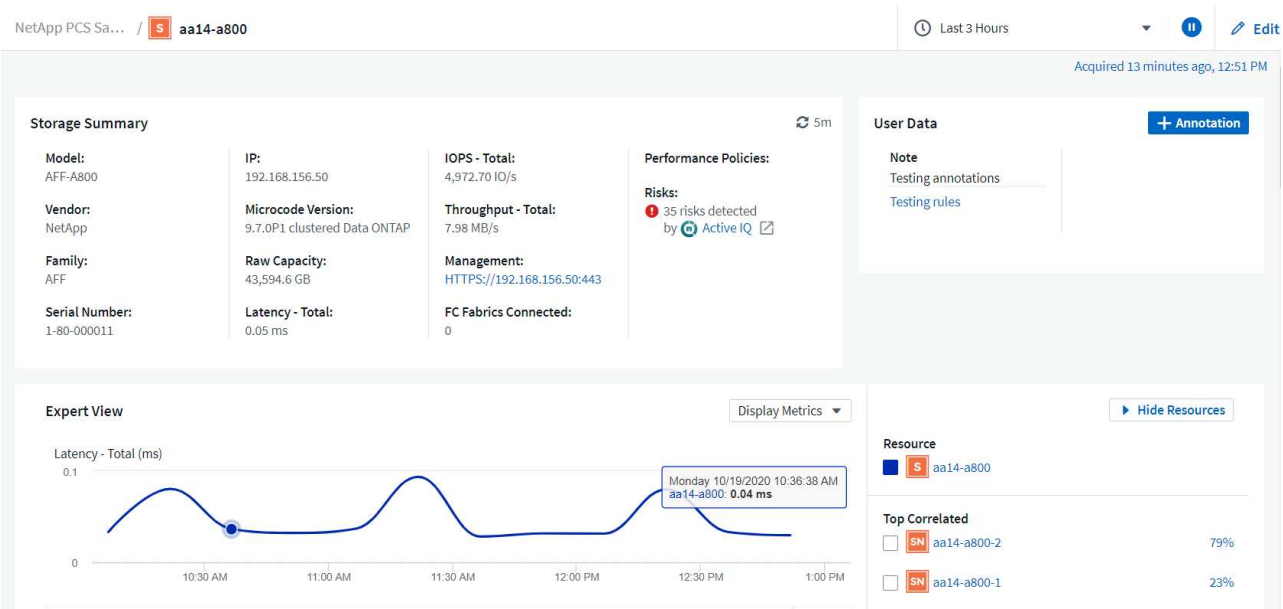


3. Cliquez sur le Data Collector pour obtenir un résumé de l'environnement et des périphériques surveillés par ce collecteur.

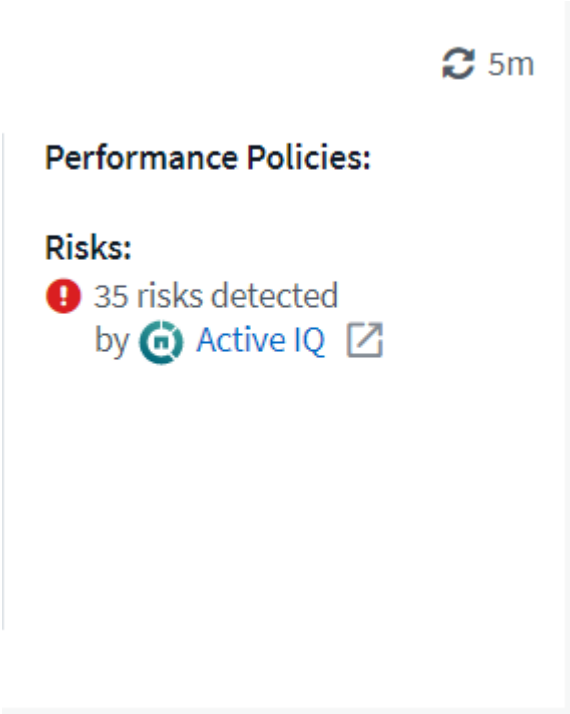


Sous la liste des périphériques en bas, cliquez sur le nom du système de stockage ONTAP surveillé. Un tableau de bord des informations collectées à propos du système s'affiche, avec les informations suivantes :

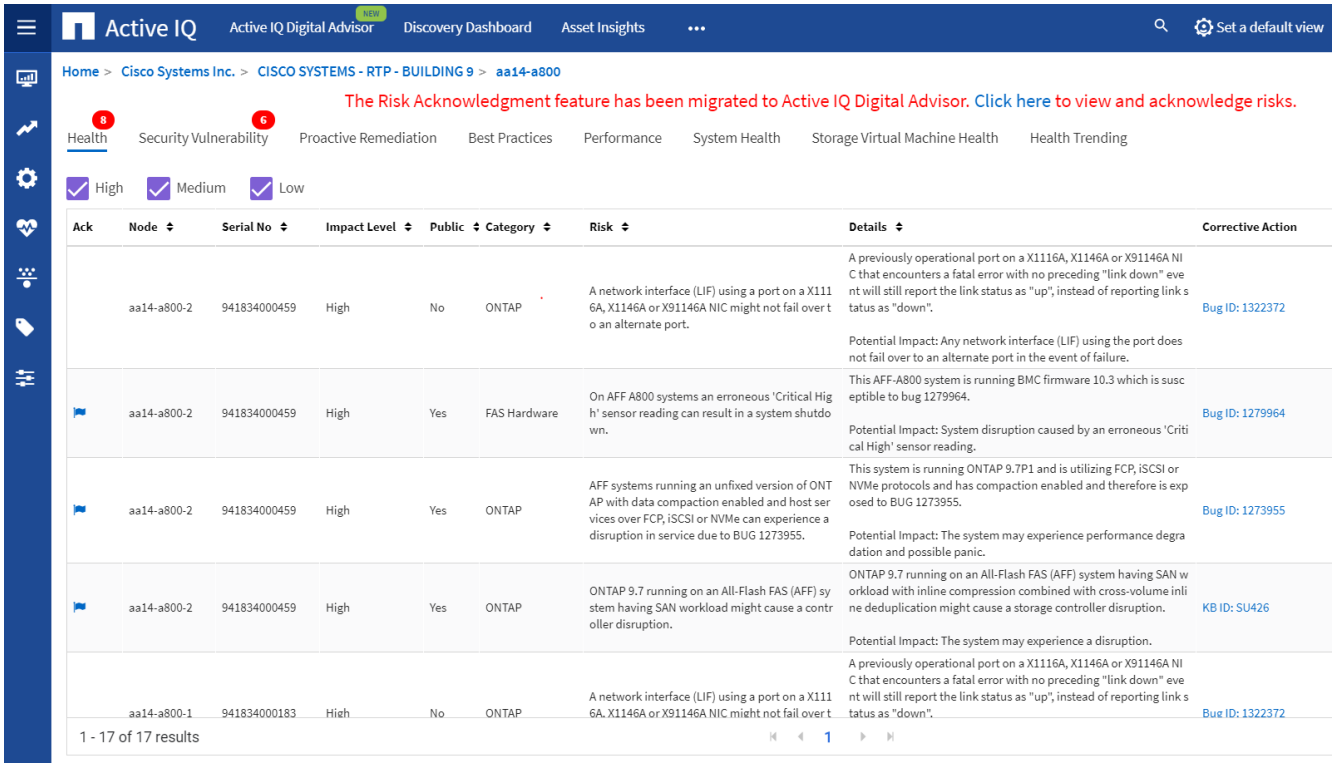
- Modèle
- Famille
- Version ONTAP
- Capacité brute
- IOPS moyennes
- Latence moyenne
- Débit moyen



De plus, sur cette page, sous la section politiques de performances, vous trouverez un lien vers NetApp Active IQ.



4. Pour ouvrir un nouvel onglet de navigateur et accéder à la page de réduction des risques, qui affiche les nœuds concernés et les risques critiques, et les actions à entreprendre pour corriger les problèmes identifiés, cliquez sur le lien Active IQ.

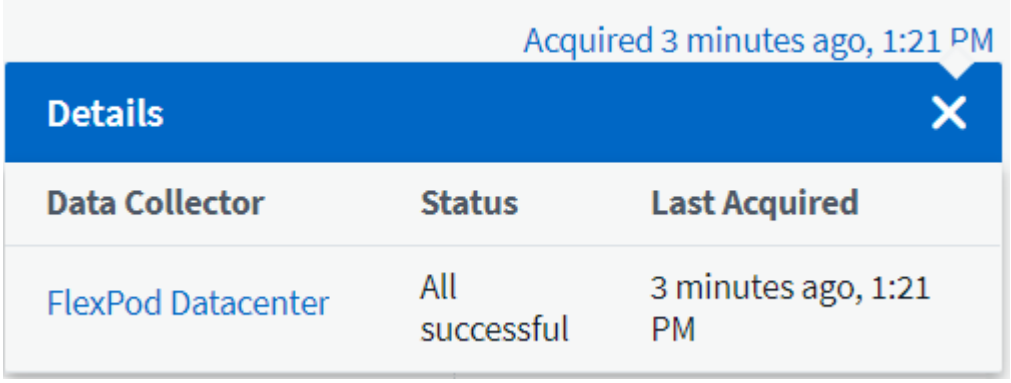


Explorez les tableaux de bord en temps réel

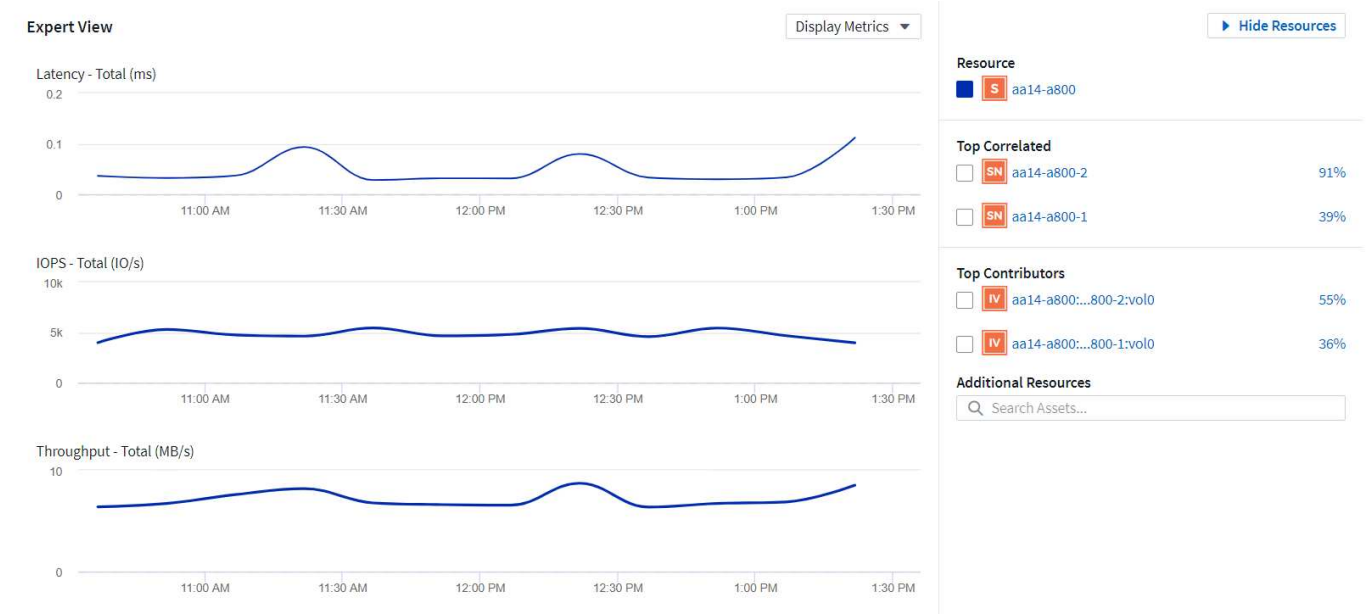
Cloud Insights peut afficher les tableaux de bord en temps réel des informations interrogées à partir du système de stockage ONTAP déployé dans une solution de data Center FlexPod. L'unité d'acquisition Cloud Insights collecte les données à intervalles réguliers et renseigne le tableau de bord du système de stockage par défaut avec les informations collectées.

Accédez aux graphiques en temps réel à partir du tableau de bord Cloud Insights

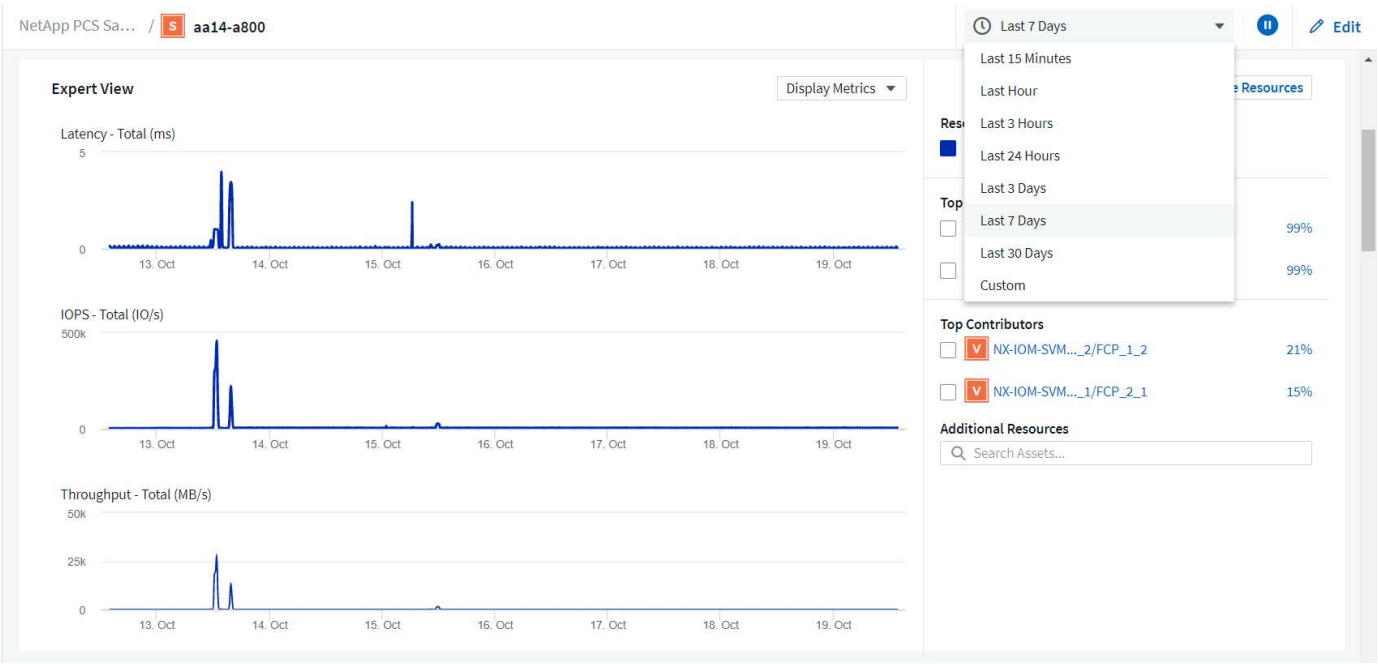
À partir du tableau de bord du système de stockage, vous pouvez voir la dernière mise à jour des informations par le Data Collector. La figure ci-dessous en est un exemple.



Par défaut, le tableau de bord du système de stockage affiche plusieurs graphiques interactifs qui présentent les metrics système de stockage interrogés ou à partir de chaque nœud, notamment la latence, les IOPS et le débit. La figure ci-dessous présente des exemples de ces graphiques par défaut.



Par défaut, les graphiques affichent des informations des trois dernières heures, mais vous pouvez les définir sur un certain nombre de valeurs différentes ou sur une valeur personnalisée dans la liste déroulante située en haut à droite du tableau de bord du système de stockage. Ceci est illustré dans la figure ci-dessous.



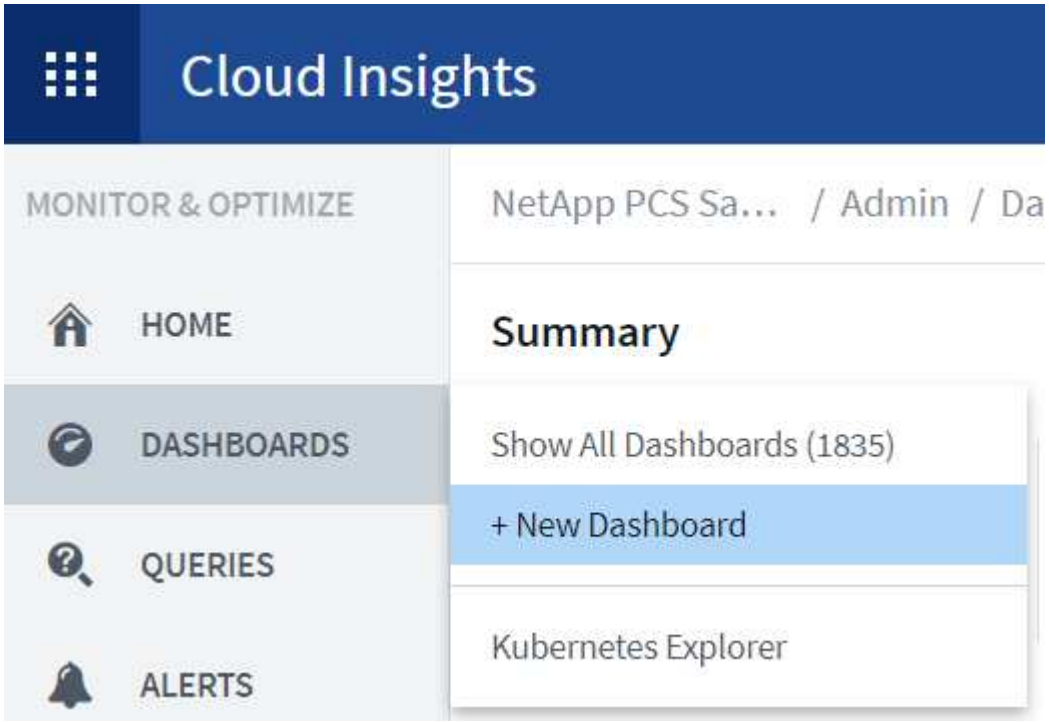
Création de tableaux de bord personnalisés

Outre l'utilisation des tableaux de bord par défaut qui affichent des informations à l'échelle du système, vous pouvez utiliser Cloud Insights pour créer des tableaux de bord entièrement personnalisés qui vous permettent de donner la priorité à l'utilisation des ressources pour des volumes de stockage spécifiques dans la solution FlexPod Datacenter, les applications déployées dans l'infrastructure convergée qui dépendent de ces volumes peuvent donc s'exécuter efficacement. Ainsi, vous pouvez améliorer la visualisation des applications spécifiques et des ressources utilisées dans l'environnement du centre de données.

Création d'un tableau de bord personnalisé pour évaluer les ressources de stockage

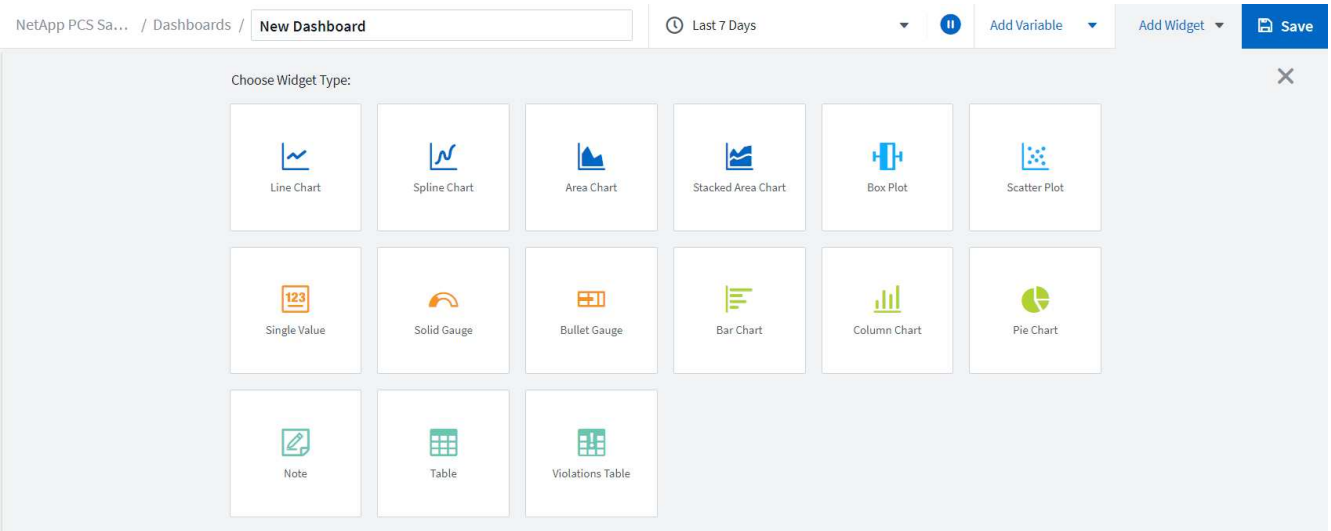
Pour créer un tableau de bord personnalisé afin d'évaluer les ressources de stockage, effectuez les opérations suivantes :

1. Pour créer un tableau de bord personnalisé, placez le pointeur de la souris sur tableaux de bord dans le menu principal de Cloud Insights, puis cliquez sur + Nouveau tableau de bord dans la liste déroulante.



   La fenêtre Nouveau tableau de bord s'ouvre.

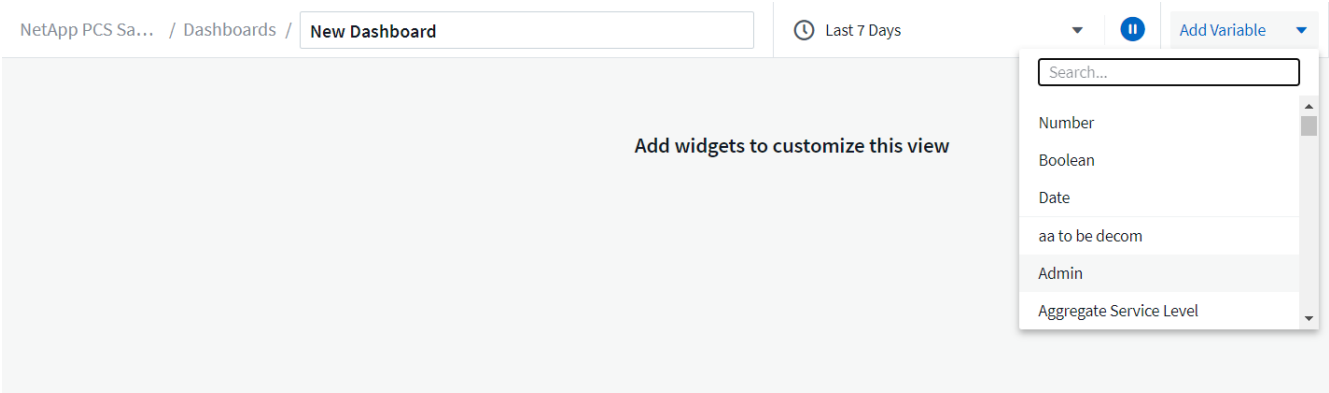
2. Nommez le tableau de bord et sélectionnez le type de widget utilisé pour afficher les données. Vous pouvez choisir parmi un certain nombre de types de graphique, même des notes ou des types de table pour présenter les données collectées.



3. Choisissez des variables personnalisées dans le menu Ajouter une variable.

   Cela permet de concentrer les données présentées pour afficher des facteurs plus spécifiques ou plus

spécialisés.



4. Pour créer un tableau de bord personnalisé, sélectionnez le type de widget que vous souhaitez utiliser, par exemple, un graphique à secteurs pour afficher l'utilisation du stockage par volume :

   a. Sélectionnez le widget Pie Chart dans la liste déroulante Ajouter un widget.

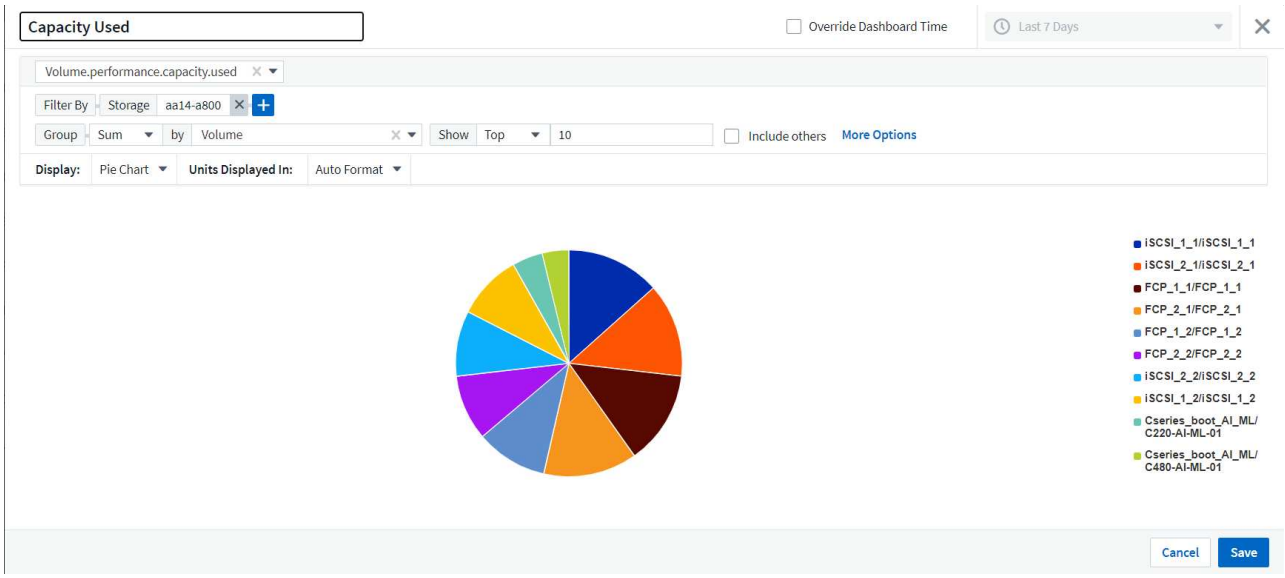
   b. Nommez le widget avec un identificateur descriptif, tel que `Capacity Used`.

   c. Sélectionnez l'objet à afficher. Par exemple, vous pouvez effectuer une recherche à l'aide de la touche terme volume et sélectionner `volume.performance.capacity.used`.

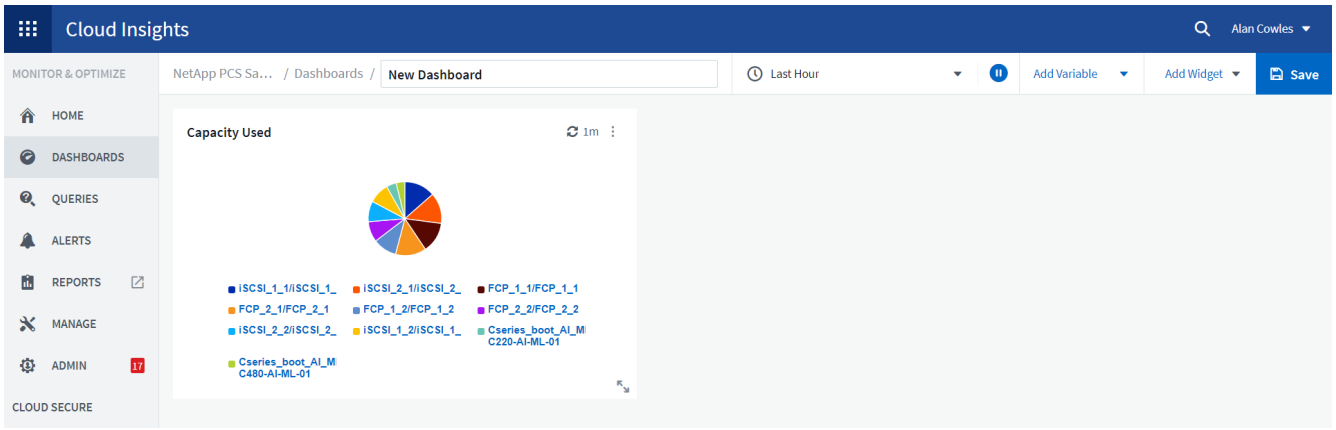
   d. Pour les filtrer par système de stockage, utilisez le filtre et tapez le nom du système de stockage de la solution FlexPod Datacenter.

   e. Personnalisez les informations à afficher. Par défaut, cette sélection affiche les volumes de données ONTAP et liste les 10 premiers.

   f. Pour enregistrer le tableau de bord personnalisé, cliquez sur Enregistrer.



   Après avoir enregistré le widget personnalisé, le navigateur retourne à la page Nouveau tableau de bord, où il affiche le widget nouvellement créé et permet de réaliser une action interactive, telle que la modification de la période d'interrogation des données.



Dépannage avancé

Cloud Insights permet d'appliquer des méthodes avancées de dépannage à n'importe quel environnement de stockage d'une infrastructure convergée FlexPod Datacenter. À l'aide des composants de chacune des fonctionnalités mentionnées ci-dessus : intégration d'Active IQ, tableaux de bord par défaut avec statistiques en temps réel et tableaux de bord personnalisés, les problèmes susceptibles d'apparaître sont détectés rapidement et résolus. Grâce à la liste des risques dans Active IQ, un client peut trouver des erreurs de configuration signalées qui pourraient entraîner un problème ou la détection de bogues qui ont été signalés et corrigés des versions de code, ce qui peut les résoudre. Les tableaux de bord en temps réel sur la page d'accueil de Cloud Insights permettent d'identifier des modèles de performances système qui pourraient être un indicateur précoce d'un problème en hausse et aider à le résoudre rapidement. Enfin, la possibilité de créer des tableaux de bord personnalisés permet aux clients de se concentrer sur les ressources les plus importantes de leur infrastructure et de les surveiller directement pour assurer la continuité de leurs objectifs.

Optimisation du stockage

Outre la résolution de problèmes, Cloud Insights peut utiliser les données collectées pour optimiser le système de stockage ONTAP déployé dans une solution d'infrastructure convergée FlexPod Datacenter. Si un volume présente une latence élevée, peut-être parce que plusieurs ordinateurs virtuels exigeant des performances élevées partagent le même datastore, ces informations sont affichées dans le tableau de bord de Cloud Insights. Avec ces informations, l'administrateur de stockage peut choisir de migrer un ou plusieurs VM vers d'autres volumes, de migrer des volumes de stockage entre les niveaux d'agrégats ou entre les nœuds du système de stockage ONTAP, pour obtenir un environnement optimisé pour les performances. Les informations fournies par l'intégration de Active IQ à Cloud Insights permettent de mettre en évidence les problèmes de configuration qui entraînent des performances supérieures aux prévisions et de proposer les actions correctives recommandées qui, si elles sont mises en œuvre, peuvent résoudre les problèmes et garantir un système de stockage parfaitement réglé.

Vidéos et démonstrations

Vous pouvez voir une démonstration vidéo de l'utilisation de NetApp Cloud Insights pour évaluer les ressources d'un environnement sur site "ici".

Vous pouvez voir une démonstration vidéo de l'utilisation de NetApp Cloud Insights pour surveiller l'infrastructure et définir des seuils d'alerte pour l'infrastructure "ici".

Vous pouvez voir une démonstration vidéo de l'utilisation de NetApp Cloud Insights pour évaluer les applications individuelles dans l'environnement "ici".

Informations supplémentaires

Pour en savoir plus sur les informations données dans ce document, consultez les sites web suivants :

- Documentation des produits Cisco

  "https://www.cisco.com/c/en/us/support/index.html"

- Data Center FlexPod

  "https://www.flexpod.com"

- NetApp Cloud Insights

  "https://cloud.netapp.com/cloud-insights"

- Documentation produit NetApp

  "https://docs.netapp.com"

FlexPod avec FabricPool : Tiering des données inactives vers Amazon AWS S3

Tr-4801 : FlexPod avec FabricPool - Tiering des données inactives vers Amazon AWS S3

Scott Kovacs, NetApp

Les prix du stockage Flash continuent de baisser, ce qui est désormais disponible pour les charges de travail et les applications qui n'étaient pas considérées comme des candidats auparavant pour le stockage Flash. Toutefois, l'utilisation la plus efficace de l'investissement de stockage est encore cruciale pour les responsables INFORMATIQUES. Le service IT reste contraintes de fournir des services plus performants avec peu ou pas d'augmentation budgétaire. En réponse à ces besoins, NetApp FabricPool vous permet d'exploiter les économies du cloud en transférant les données peu utilisées hors de votre stockage Flash sur site, cher, vers un Tier de stockage plus économique dans le cloud public. Le transfert des données peu utilisées vers le cloud libère un espace de stockage Flash précieux sur les systèmes AFF ou FAS, ce qui permet d'obtenir davantage de capacité pour les workloads stratégiques vers le Tier Flash haute performance.

Dans ce rapport technique, nous passons en revue la fonctionnalité de Tiering des données FabricPool de NetApp ONTAP dans le cadre d'une architecture d'infrastructure convergée FlexPod de NetApp et Cisco. Vous devez maîtriser l'architecture d'infrastructure convergée FlexPod Datacenter et le logiciel de stockage ONTAP pour exploiter pleinement les concepts abordés dans ce rapport technique. Connaissant bien FlexPod et ONTAP, nous présentons le FabricPool, son fonctionnement et la façon dont il peut être utilisé pour une utilisation plus efficace du stockage Flash sur site. Une grande partie du contenu de ce rapport est abordée de manière plus détaillée dans le "Tr-4598 meilleures pratiques de FabricPool" Et documentation des produits ONTAP. Le contenu a été condensé pour une infrastructure FlexPod et ne couvre pas tous les cas d'utilisation

de FabricPool. Toutes les fonctionnalités et concepts abordés sont disponibles dans ONTAP 9.6.

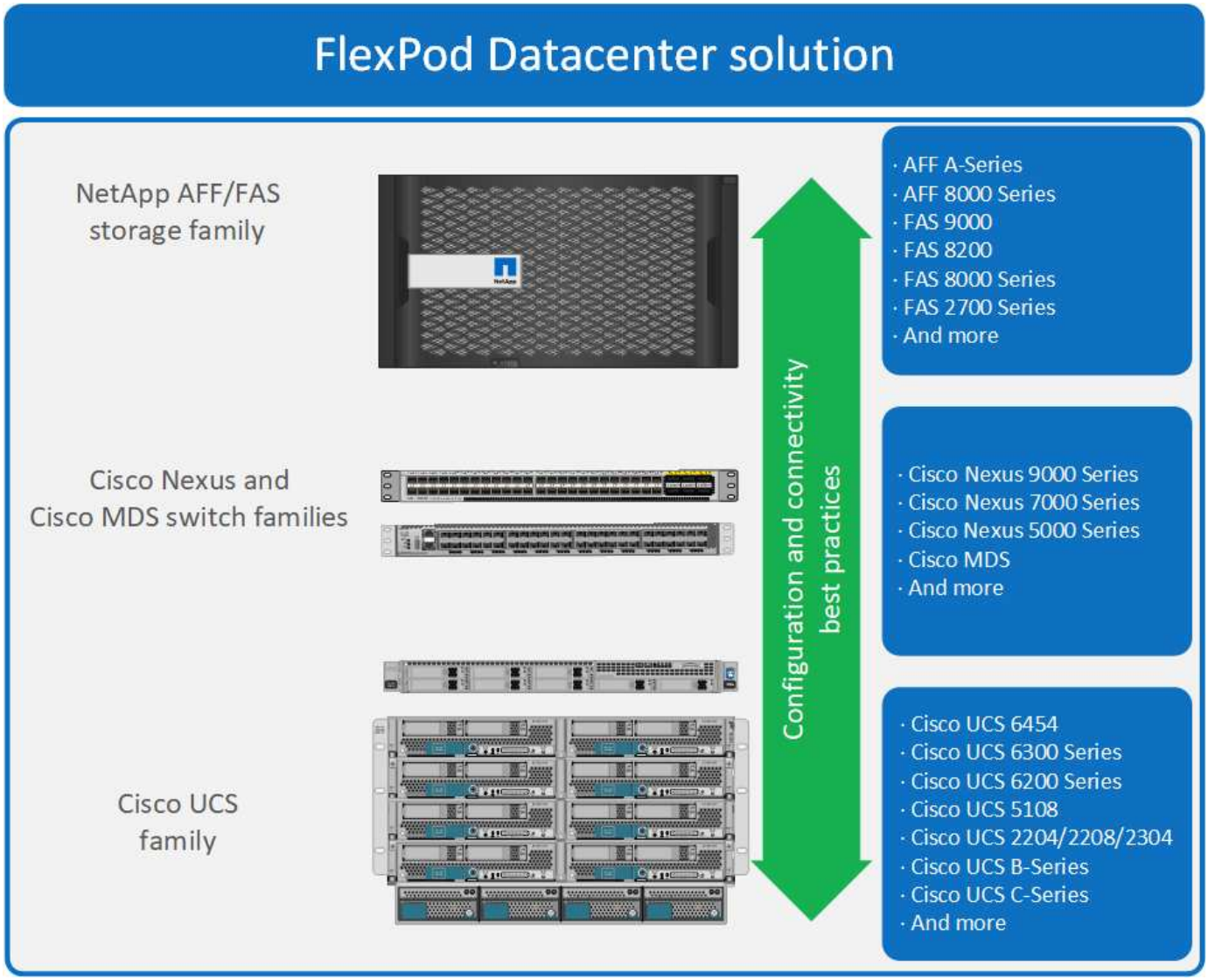
Pour plus d'informations sur FlexPod, consultez le "Tr-4036 spécifications techniques du data Center FlexPod".

Présentation et architecture de FlexPod

Présentation de FlexPod

FlexPod est un ensemble défini de matériels et de logiciels qui constitue une base intégrée pour les solutions virtualisées et non virtualisées. FlexPod inclut le stockage NetApp AFF, les réseaux Cisco Nexus, les réseaux de stockage Cisco MDS, Cisco Unified Computing System (Cisco UCS) et le logiciel VMware vSphere dans une seule offre. La conception est suffisamment flexible pour que les réseaux, l'informatique et le stockage s'adaptent à un seul rack de data Center ou puissent être déployés selon la conception du data Center du client. La densité des ports permet aux composants réseau de prendre en charge plusieurs configurations.

L'un des avantages de l'architecture FlexPod est la possibilité de personnaliser l'environnement en fonction des exigences du client. Une unité FlexPod peut facilement évoluer en fonction des besoins et de la demande. Une unité peut évoluer verticalement (ajout de ressources à une unité FlexPod) et horizontalement (ajout d'unités FlexPod). L'architecture de référence FlexPod met en avant la résilience, les avantages financiers et la facilité de déploiement d'une solution de stockage Fibre Channel et IP. Un système de stockage capable de prendre en charge plusieurs protocoles sur une interface unique offre aux clients le choix et protège leur investissement, car il s'agit d'une architecture à une seule étape. La figure suivante montre de nombreux composants matériels de FlexPod.

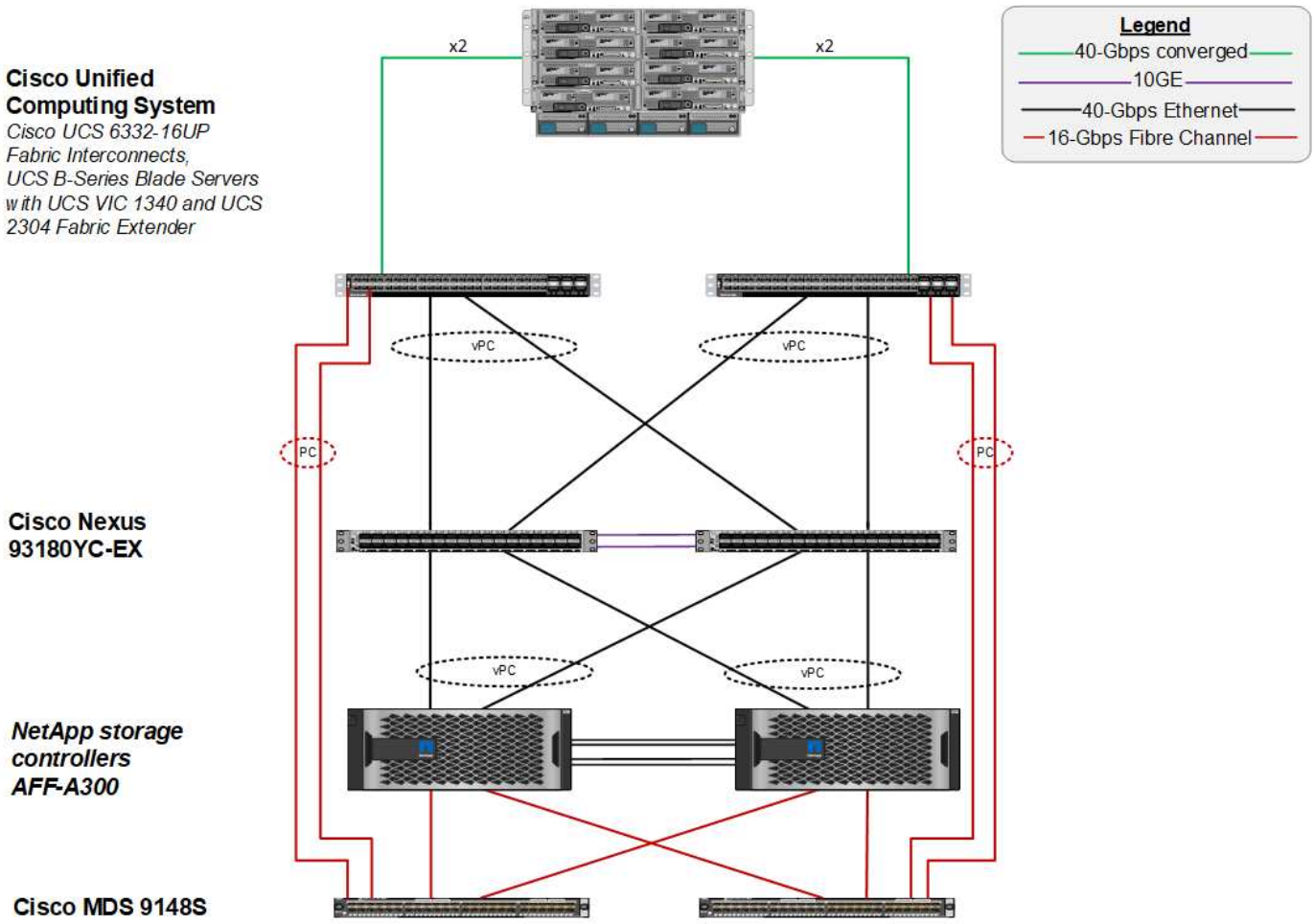


Architecture FlexPod

La figure suivante montre les composants d'une solution VMware vSphere et FlexPod, ainsi que les connexions réseau nécessaires aux interconnexions de fabric Cisco UCS 6454. Cette conception comprend les composants suivants :

- Des connexions Ethernet 40 Gb canalisées entre le châssis lame Cisco UCS 5108 et les interconnexions de fabric Cisco UCS
- Connexions Ethernet de 40 Go entre l'interconnexion de fabric Cisco UCS et le commutateur Cisco Nexus 9000
- Connexions Ethernet de 40 Go entre Cisco Nesxus 9000 et la baie de stockage NetApp AFF A300

Ces options d'infrastructure sont étendues avec l'introduction de commutateurs Cisco MDS entre le Fabric Interconnect Cisco UCS et le système NetApp AFF A300. Cette configuration fournit des hôtes FC démarrés avec un accès FC 16 Gb au niveau des blocs au stockage partagé. L'architecture de référence renforce la stratégie à un seul réseau. En effet, lors de l'ajout de stockage à l'architecture, aucune désactivation n'est requise entre les hôtes et le Fabric Interconnect Cisco UCS.



FabricPool

Présentation de FabricPool

FabricPool est une solution de stockage hybride dans ONTAP qui utilise un agrégat 100 % Flash (SSD) comme Tier de performance et un magasin d'objets dans un service de cloud public en tant que Tier cloud. Cette configuration permet le déplacement des données basé sur des règles, en fonction de l'accès fréquent ou non aux données. FabricPool est pris en charge dans ONTAP pour les agrégats AFF et 100 % SSD sur les plateformes FAS. Le traitement des données est effectué au niveau des blocs, dans la mesure où les blocs de données sont fréquemment utilisés dans le Tier de performance 100 % Flash et où les blocs fortement sollicités sont balisés comme inactives.

FabricPool permet de réduire les coûts de stockage sans nuire aux performances, à l'efficacité, à la sécurité ou à la protection. FabricPool est transparent pour les applications d'entreprise et capitalise sur l'efficacité du cloud en réduisant le TCO du stockage sans devoir repenser l'architecture de l'infrastructure applicative.

FlexPod bénéficie des fonctionnalités de hiérarchisation du stockage de FabricPool pour une utilisation plus efficace du stockage Flash ONTAP. Les machines virtuelles inactives, les modèles de machine virtuelle peu utilisés et les sauvegardes des machines virtuelles depuis NetApp SnapCenter pour vSphere peuvent consommer un espace précieux dans le volume du datastore. Le déplacement des données inactives vers le Tier cloud libère de l'espace et des ressources pour les applications stratégiques haute performance hébergées sur l'infrastructure FlexPod.

> Les protocoles Fibre Channel et iSCSI prennent généralement plus de temps avant que le délai d'attente ne soit dépassé (60 à 120 secondes), mais ils ne tentatives pas d'établir de connexion de la même manière que les protocoles NAS. Si un protocole SAN est à court de temps, l'application doit être redémarrée. Même une courte interruption peut avoir des conséquences désastreuses pour les applications de production grâce aux protocoles SAN, car il n'existe pas de moyen de garantir la connectivité aux clouds publics. Pour éviter ce problème, NetApp recommande d'utiliser des clouds privés pour le Tiering des données accessibles par les protocoles SAN.

Dans ONTAP 9.6, FabricPool s'intègre avec tous les principaux fournisseurs de cloud public : Alibaba Cloud Object Storage Service, Amazon AWS S3, Google Cloud Storage, IBM Cloud Object Storage et Microsoft Azure Blob Storage. Ce rapport est axé sur le stockage Amazon AWS S3 en tant que Tier objet cloud de votre choix.

L'agrégat composite

Une instance FabricPool est créée en associant un agrégat Flash ONTAP à un magasin d'objets cloud, par exemple un compartiment AWS S3, afin de créer un agrégat composite. Lorsque les volumes sont créés dans l'agrégat composite, ils peuvent bénéficier des fonctionnalités de Tiering de FabricPool. Lorsque les données sont écrites sur le volume, ONTAP attribue une température à chacun des blocs de données. Lors de la première écriture du bloc, une température de stockage est affectée. Lorsque le temps passe, si les données ne sont pas utilisées, elles sont soumises à un processus de refroidissement jusqu'à ce qu'elles soient finalement attribuées à l'état froid. Ces blocs de données peu utilisés sont ensuite hiérarchisés à partir de l'agrégat SSD de performance et vers le magasin d'objets cloud.

Période entre le moment où un bloc est désigné comme étant froid et le moment où il est transféré vers le stockage objet cloud par la règle de Tiering des volumes dans ONTAP. Une granularité supérieure est obtenue en modifiant les paramètres de ONTAP qui contrôlent le nombre de jours nécessaires à la mise à froid d'un bloc. Ils peuvent également être utilisés pour le Tiering des données : snapshots de volume traditionnels, sauvegardes de machine virtuelle SnapCenter pour vSphere et autres sauvegardes NetApp Snapshot, blocs peu utilisés dans un datastore vSphere, modèles de machine virtuelle et données de machine virtuelle rarement utilisées.

Reporting des données inactives

Le reporting pour les données inactives est disponible dans ONTAP pour vous aider à évaluer la quantité de données inactives pouvant être hiérarchisées à partir d'un agrégat. L'IDR est activé par défaut dans ONTAP 9.6 et utilise une stratégie de refroidissement de 31 jours par défaut pour déterminer quelles données du volume sont inactives.

> La quantité de données inactives dans le Tier dépend des règles de Tiering définies sur le volume. Cette quantité peut être différente de la quantité de données inactives détectée par l'IDR au moyen de la période de refroidissement par défaut de 31 jours.

La création d'objets et le déplacement des données

FabricPool fonctionne au niveau bloc NetApp WAFL, les blocs de refroidissement, les concaténer en objets de stockage et les migrer vers un Tier cloud. Chaque objet FabricPool est de 4 Mo et comprend 1,024 blocs de 4 Ko. La taille d'objet est fixée à 4 Mo en fonction des recommandations de performances des principaux fournisseurs cloud, et ne peut pas être modifiée. Si les blocs inactifs sont lus et mis à chaud, seuls les blocs requis de l'objet 4 Mo sont récupérés et transférés vers le Tier de performance Ni l'objet dans son intégralité, ni le fichier ne sont migrés à nouveau. Seuls les blocs nécessaires sont migrés.

> Si ONTAP détecte une opportunité pour les lectures séquentielles, il demande des blocs à partir du Tier cloud avant leur lecture pour améliorer les performances.

Par défaut, les données ne sont déplacées vers le Tier cloud que lorsque l'agrégat de performances est supérieur à 50 % utilisé. Ce seuil peut être défini sur un pourcentage inférieur pour permettre le transfert d'une quantité réduite de stockage des données dans le Tier Flash de performance vers le cloud. Cette possibilité peut être utile si la stratégie de Tiering consiste à transférer les données inactives uniquement lorsque l'agrégat approche de la capacité.

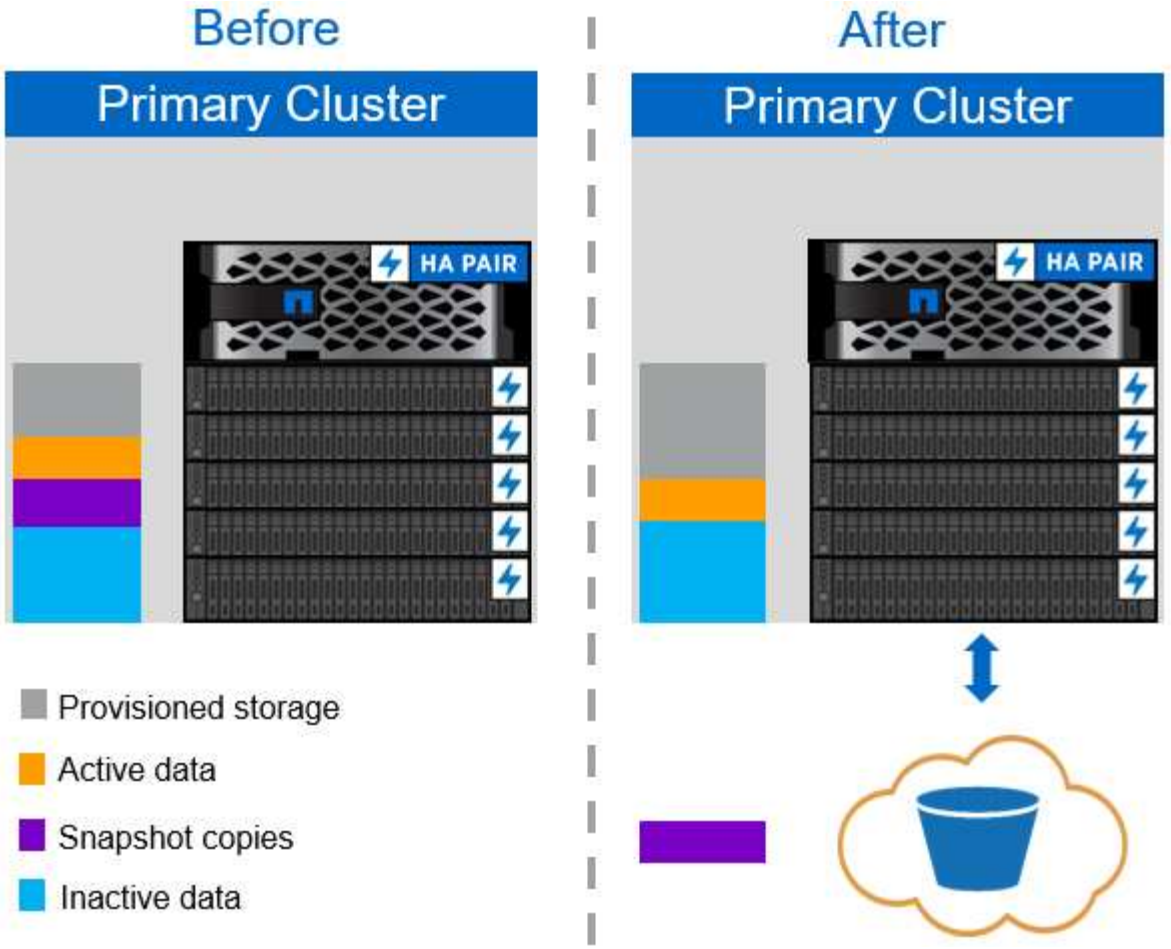
Si l'utilisation du Tier de performance dépasse les 70 % de capacité, les données inactives sont lues directement depuis le Tier cloud sans être écrites à nouveau sur le Tier de performance. En empêchant la rétro-écriture des données inactives sur les agrégats largement utilisés, FabricPool préserve l'agrégat pour les données actives.

Récupération de l'espace de Tier de performance

Comme mentionné précédemment, l'utilisation principale de FabricPool est de faciliter l'utilisation la plus efficace du stockage Flash sur site haute performance. Les données inactives sous forme de snapshots de volume et de sauvegardes de machines virtuelles au sein de l'infrastructure virtuelle FlexPod peuvent occuper une quantité significative de stockage Flash coûteux. Pour libérer les fonctionnalités de stockage au niveau de la performance, deux règles de Tiering sont disponibles : Snapshot uniquement ou Auto.

Règle de Tiering uniquement Snapshot

La règle de Tiering uniquement Snapshot, illustrée dans la figure suivante, déplace les données Snapshot des volumes inactives et les sauvegardes SnapCenter pour vSphere des machines virtuelles qui occupent de l'espace, mais qui ne partagent pas les blocs avec le système de fichiers actif dans un magasin d'objets cloud. La règle de Tiering uniquement pour Snapshot déplace les blocs de données inactives vers le Tier cloud. Pour restaurer les données, les blocs à froid dans le cloud sont fortement sollicités et sont déplacés vers le Tier de performance Flash sur site.

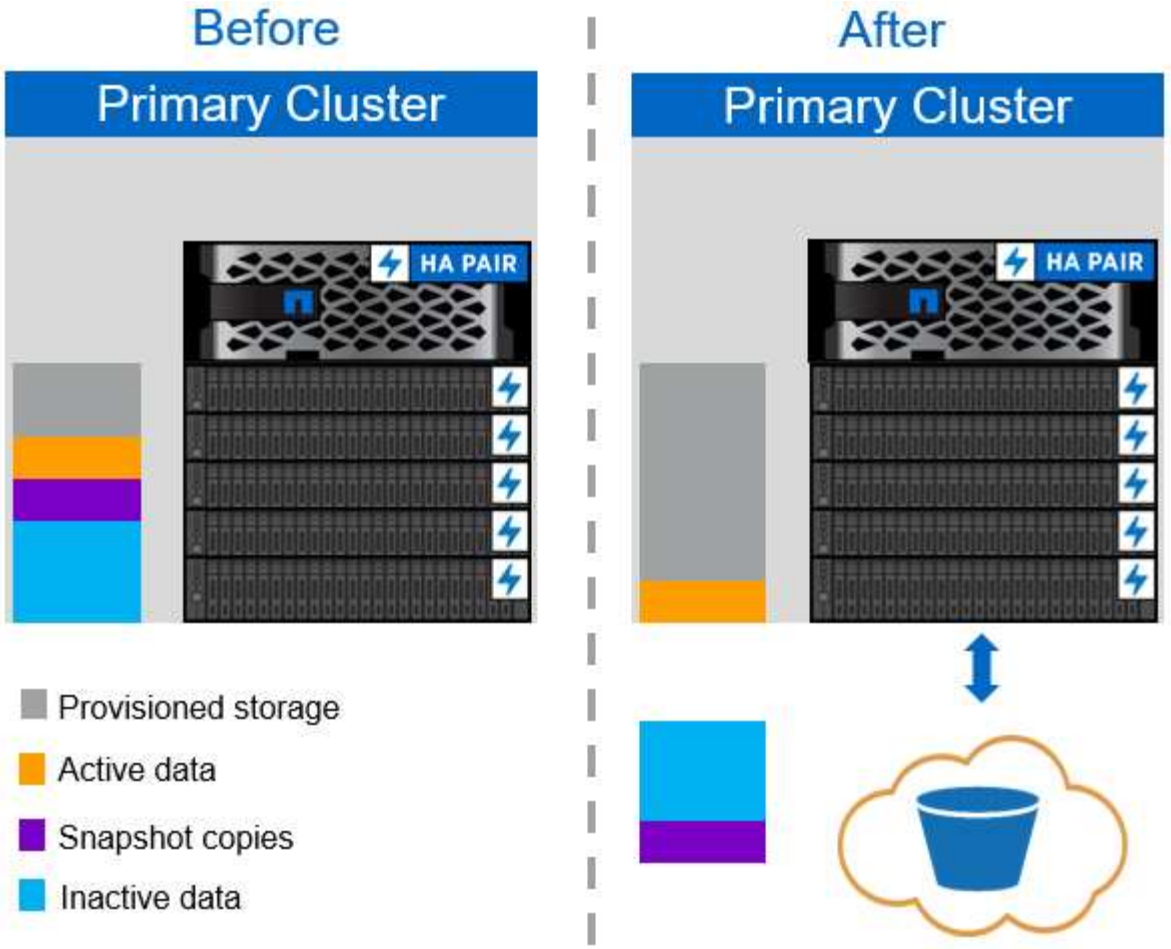


Règle de hiérarchisation automatique

La règle de hiérarchisation automatique du stockage FabricPool, illustrée dans la figure suivante, déplace non seulement les blocs de données des snapshots inactifs vers le cloud, mais déplace également les blocs de données inactives du système de fichiers actif. Cela peut inclure les modèles de VM et toutes les données de VM inutilisées dans le volume du datastore. Les blocs froids déplacés sont contrôlés par le `tiering-minimum-cooling-days` réglage du volume. Si les blocs inactifs du Tier cloud sont lus de manière aléatoire par une application, les blocs fortement sollicités sont alors retransférés vers le Tier de performance. Toutefois, si les blocs inactifs sont lus par un processus séquentiel tel qu'un antivirus, les blocs restent inactifs et restent conservés dans le magasin d'objets cloud. Ils ne sont pas déplacés vers le Tier de performance.

Lors de l'utilisation de la règle de Tiering automatique, les blocs fréquemment utilisés sont retirés du Tier cloud au débit de la connectivité cloud. Cela peut affecter les performances des machines virtuelles si l'application est sensible à la latence, qui doit être prise en compte avant d'utiliser la règle de hiérarchisation automatique sur le datastore. NetApp recommande de placer les LIFs intercluster sur des ports présentant une vitesse de 10GbE pour des performances adéquates.

> Le profileur de magasin d'objets doit être utilisé pour tester la latence et le débit vers le magasin d'objets avant de le rattacher à un agrégat FabricPool.



Toutes les règles de Tiering

À la différence des règles Auto et Snapshot uniquement, toutes les règles de Tiering déplacent immédiatement des volumes entiers de données vers le Tier cloud. Cette règle convient mieux aux volumes secondaires de protection des données ou d'archivage pour lesquels les données doivent être conservées à des fins historiques ou réglementaires, mais peu utilisées. La règle All n'est pas recommandée pour les volumes du datastore VMware car les données écrites sur le datastore sont immédiatement déplacées vers le niveau cloud. Les opérations de lecture suivantes sont effectuées depuis le cloud et peuvent éventuellement introduire des problèmes de performances pour les machines virtuelles et les applications qui résident dans le volume du datastore.

Sécurité

La sécurité est une préoccupation majeure pour le cloud et pour FabricPool. Toutes les fonctions de sécurité natives d'ONTAP sont prises en charge dans le Tier de performance, et le déplacement des données est sécurisé lors de leur transfert vers le Tier cloud. FabricPool utilise le "AES-256-GCM" algorithme de chiffrement sur le tier de performance et maintien de ce chiffrement de bout en bout dans le tier cloud. Les blocs de données qui sont déplacés vers le magasin d'objets cloud sont sécurisés par la sécurité de la couche de transport (TLS) v1.2 afin de préserver la confidentialité et l'intégrité des données entre les tiers de stockage.

> La communication avec le magasin d'objets cloud sur une connexion non chiffrée est prise en charge, mais non recommandée par NetApp.

Chiffrement des données

Le cryptage des données est indispensable à la protection de la propriété intellectuelle, des informations commerciales et des informations personnellement identifiables des clients. FabricPool prend entièrement en charge NVE (NetApp Volume Encryption) et NetApp Storage Encryption (NSE) pour conserver les stratégies de protection des données existantes. Toutes les données chiffrées stockées sur le Tier de performance restent chiffrées lors de leur déplacement vers le Tier cloud. Les clés de chiffrement côté client sont la propriété de ONTAP, et les clés de chiffrement de magasin d'objets côté serveur sont la propriété de leur magasin d'objets cloud respectif. Les données qui ne sont pas chiffrées avec NVE sont chiffrées à l'aide de l'algorithme AES-256-GCM. Aucun autre chiffrement AES-256 n'est pris en charge.

> L'utilisation de NSE ou NVE est facultative et n'est pas requise pour l'utilisation de FabricPool.

Conditions requises pour le FabricPool

FabricPool nécessite ONTAP 9.2 ou une version ultérieure et des agrégats SSD sur l'une des plateformes répertoriées dans cette section. D'autres exigences d'FabricPool dépendent du niveau de cloud associé. Si vous disposez de plateformes AFF d'entrée de gamme dont la capacité est fixe et relativement faible, comme le système NetApp AFF C190, FabricPool peut bénéficier d'une grande efficacité pour déplacer les données inactives vers le Tier cloud.

Plateformes

FabricPool est pris en charge sur les plateformes suivantes :

- NetApp AFF
  - A800
  - A700S, A700
  - A320, A300
  - A220, A200
  - C190
  - AFF8080, AFF8060 ET AFF8040
- NetApp FAS
  - FAS9000
  - FAS8200
  - FAS8080, FAS8060 ET FAS8040
  - FAS2750, FAS2720
  - FAS2650 ET FAS2620

> Seuls les agrégats SSD des plateformes FAS peuvent utiliser FabricPool.

- Tiers cloud
  - Alibaba Cloud Object Storage Service (Standard, Infrequent Access)
  - Amazon S3 (Standard, Standard-IA, une zone-IA, Tiering intelligent)

- Amazon commercial Cloud Services (C2S)
- Google Cloud Storage (multirégional, régional, Nearline, Coldline)
- Stockage objet cloud IBM (Standard, Vault, Cold Vault, Flex)
- Microsoft Azure Blob Storage (chaud et froid)

LIF intercluster

Les paires haute disponibilité du cluster qui utilisent FabricPool nécessitent deux interfaces logiques intercluster pour communiquer avec le niveau du cloud. NetApp recommande de créer un LIF intercluster sur des paires haute disponibilité supplémentaires pour relier de manière transparente des niveaux cloud aux agrégats sur ces nœuds.

Le LIF utilisé par ONTAP pour se connecter avec le magasin d'objets AWS S3 doit se trouver sur un port 10 Gbit/s.

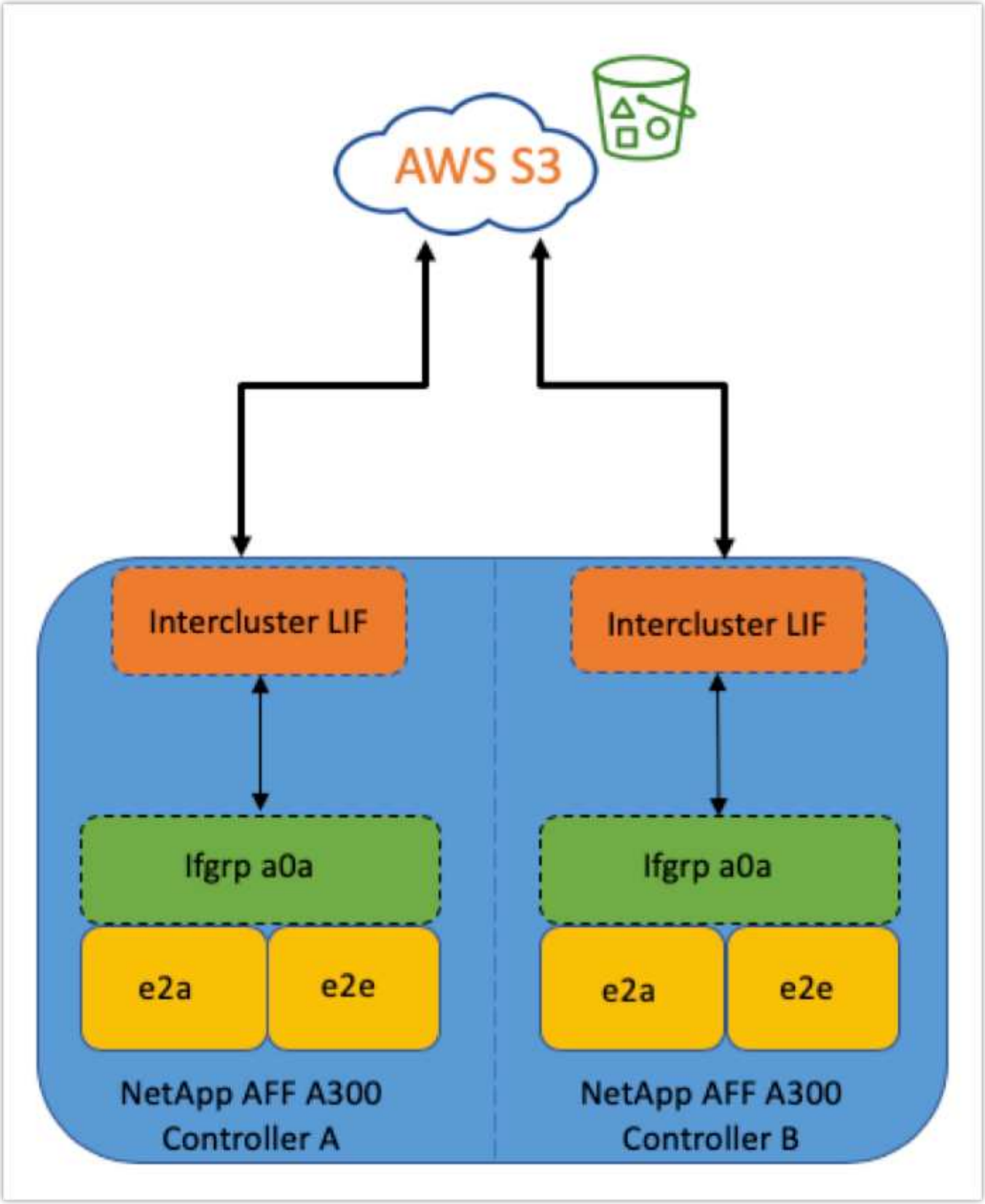
Si plusieurs LIF Intercleuser sont utilisées sur un nœud avec un routage différent, NetApp recommande de les placer dans différents IPspaces. Lors de la configuration, FabricPool peut choisir parmi plusieurs IPspaces, mais il est impossible de sélectionner des LIF intercluster spécifiques au sein d'un IPspace.

> La désactivation ou la suppression d'une LIF intercluster interrompt la communication au niveau du cloud.

Connectivité

La latence de lecture d'FabricPool dépend de la connectivité au niveau cloud. Les LIF intercluster utilisant des ports 10 Gbits/s, illustrées dans la figure suivante, offrent des performances adéquates. NetApp recommande de valider les latences et le débit d'un environnement réseau spécifique afin de déterminer son impact sur les performances d'FabricPool.

> Lorsque vous utilisez FabricPool dans des environnements à faibles performances, les exigences minimales de performance des applications client doivent rester respectées et les objectifs de délai de restauration doivent être ajustés en conséquence.



Profileur de magasin d'objets

Le profileur de magasin d'objets, comme illustré ci-dessous, est disponible via l'interface de ligne de commandes de ONTAP. Il teste la latence et les performances de débit des magasins d'objets avant qu'ils ne soient connectés à un agrégat FabricPool.

Le Tier de cloud doit être ajouté à ONTAP avant de pouvoir être utilisé avec le profileur de magasin d'objets.

Démarrez le profileur de magasin d'objets à partir du mode privilèges avancés dans ONTAP à l'aide de la commande suivante :

```
storage aggregate object-store profiler start -object-store-name <name>
-node <name>
```

Pour afficher les résultats, lancer la commande suivante :

```
storage aggregate object-store profiler show
```

Les tiers cloud n'offrent pas des performances similaires à celles du Tier de performance (généralement Go par seconde). Même si les agrégats FabricPool peuvent facilement fournir des performances similaires aux disques SATA, ils tolèrent une latence pouvant atteindre 10 secondes et un faible débit pour les solutions de Tiering qui ne nécessitent pas de performances SATA.

```
bb09-a300-2::*> storage aggregate object-store profiler show
Object store config name: aws_infra_fp_bk_1
Node name: bb09-a300-2-1
Status: Active. Issuing GETs
Start time: 10/3/2019 12:37:24

Op      Size       Total     Failed            Latency(ms)          Throughput
                                        min       max       avg
-------------------------------------------------------------------------------
PUT     4MB        1084      0         336       5951      2817      69.55MB
GET     4KB        158636    0         27        1132      41        32.22MB
GET     8KB        0         0         0         0         0         0B
GET     32KB       0         0         0         0         0         0B
GET     256KB      0         0         0         0         0         0B
5 entries were displayed.
```

Volumes

Le provisionnement fin du stockage est une pratique standard pour l'administrateur d'infrastructures virtuelles FlexPod. NetApp Virtual Storage Console (VSC) provisionne des volumes de stockage pour les datastores VMware sans les garanties d'espace (provisionnement fin) et avec des paramètres d'efficacité du stockage optimisés conformément aux meilleures pratiques NetApp. Si VSC est utilisé pour créer des datastores VMware, aucune action supplémentaire n'est requise, car aucune garantie d'espace ne doit être attribuée au volume du datastore.

FabricPool ne peut pas associer un Tier cloud à un agrégat contenant des volumes grâce à une garantie d'espace autre que aucune (par exemple, Volume).

```
volume modify -space-guarantee none
```

Réglage du `space-guarantee none` paramètre fournit le provisionnement fin pour le volume. La quantité d'espace consommée par les volumes avec ce type de garantie augmente à mesure que des données sont ajoutées au lieu d'être déterminées par la taille du volume initial. Cette approche est essentielle pour FabricPool, car les volumes doivent prendre en charge les données de Tier cloud actives et renvoyé vers le Tier de performance.

Licences

Une licence basée sur la capacité est nécessaire pour connecter des fournisseurs de stockage objet tiers (tels qu'Amazon S3) à des tiers cloud pour les systèmes AFF et FAS Flash hybrides. FabricPool

Les licences FabricPool sont disponibles en mode perpétuel ou par période (1 an ou 3 ans).

Le Tiering dans le cloud s'arrête lorsque la quantité de données (capacité utilisée) stockée sur le Tier cloud atteint la capacité sous licence. Les données supplémentaires, y compris les copies SnapMirror vers les volumes utilisant la règle de hiérarchisation, ne peuvent pas être hiérarchisées tant que la capacité de licence n'est pas augmentée. Même si le Tiering s'arrête, les données restent accessibles à partir du Tier cloud. Les données inactives supplémentaires restent sur les disques SSD jusqu'à ce que la capacité sous licence augmente.

Une licence FabricPool gratuite de 10 To basée sur une durée de validité est incluse lors de l'achat d'un nouveau cluster ONTAP 9.5 ou version ultérieure, même si des coûts de support supplémentaires peuvent s'appliquer. Les licences FabricPool (y compris la capacité supplémentaire pour les licences existantes) peuvent être achetées par incréments de 1 To.

Une licence FabricPool ne peut être supprimée que d'un cluster ne contenant aucun agrégat FabricPool.

> Les licences FabricPool portent sur l'ensemble du cluster. Vous devez avoir l'UUID disponible lors de l'achat d'une licence (`cluster identify show`). Pour plus d'informations sur la licence, reportez-vous au "Base de connaissances NetApp".

Configuration

Révisions logicielles

Le tableau suivant illustre les versions matérielles et logicielles validées.

Calque	Périphérique	Image	Commentaires
Stockage	NetApp AFF A300	ONTAP 9.6P2	
Calcul	Serveurs lames Cisco UCS B200 M5 avec Cisco UCS VIC 1340	Version 4.0(4b)	
Le réseau	Interconnexion de fabric Cisco Nexus 6332-16UP	Version 4.0(4b)	
	Commutateur Cisco Nexus 93180YC-EX en mode autonome NX-OS	Version 7.0(3)I7(6)	
Réseau de stockage	Cisco MDS 9148S	Version 8.3(2)	

Calque	Périphérique	Image	Commentaires
Hyperviseur		VMware vSphere ESXi 6.7U2	ESXi 6.7.0,13006603
		Serveur VMware vCenter	Version 6.7.0.30000 de vCenter Server 13639309
Ou du fournisseur cloud		Amazon AWS S3	Compartiment S3 standard avec options par défaut

Les critères de base pour FabricPool sont présentés dans le "Conditions requises pour le FabricPool". Une fois que toutes les conditions de base sont réunies, procédez comme suit pour configurer FabricPool :

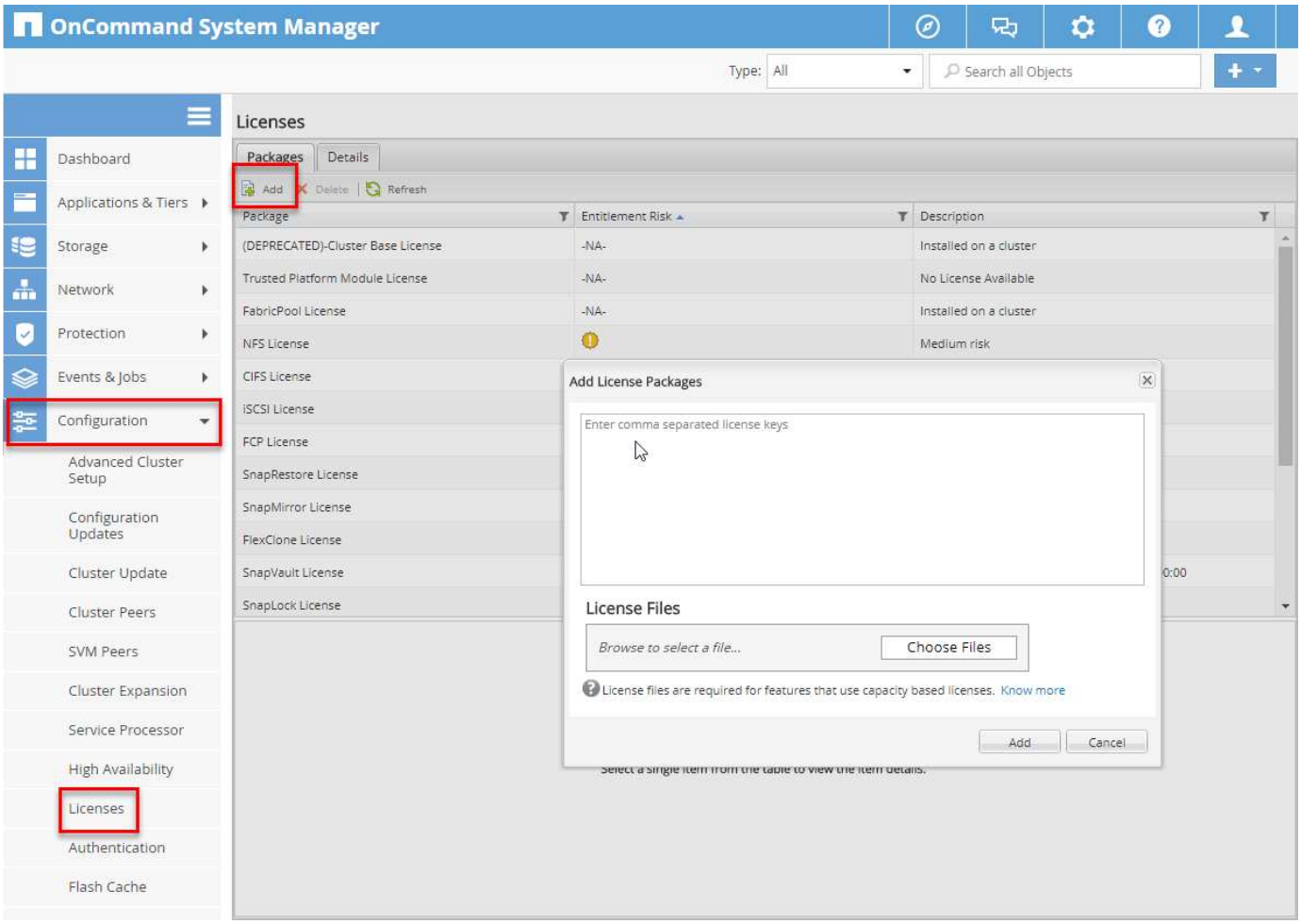
1. Installez une licence FabricPool.
2. Créez un compartiment de magasin d'objets AWS S3.
3. Ajoutez un Tier cloud à ONTAP.
4. Relier le Tier cloud à un agrégat.
5. Définissez la règle de Tiering du volume.

"Ensuite, installez la licence FabricPool."

Installez la licence FabricPool

Une fois que vous avez acquis un fichier de licence NetApp, vous pouvez l'installer avec OnCommand System Manager. Pour installer le fichier de licence, procédez comme suit :

1. Cliquez sur configurations.
2. Cliquez sur Cluster.
3. Cliquez sur licences.
4. Cliquez sur Ajouter.
5. Cliquez sur choisir les fichiers à parcourir et sélectionnez un fichier.
6. Cliquez sur Ajouter.



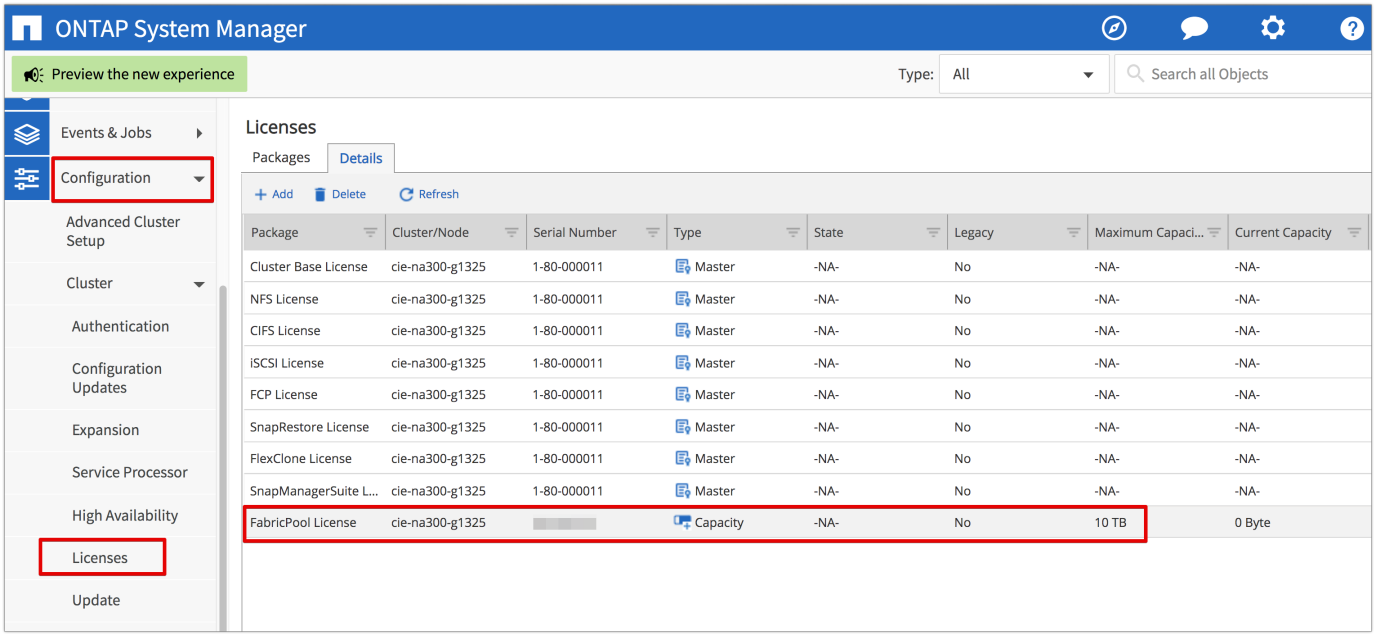
Capacité de la licence

Vous pouvez afficher la capacité de la licence à l'aide de l'interface de ligne de commandes ONTAP ou de OnCommand System Manager. Pour vérifier la capacité sous licence, exécutez la commande suivante dans l'interface de ligne de commandes de ONTAP :

```
system license show-status
```

Dans OnCommand System Manager, effectuez la procédure suivante :

1. Cliquez sur configurations.
2. Cliquez sur licences.
3. Cliquez sur l'onglet Détails.



La capacité maximale et la capacité actuelle sont indiquées sur la ligne de licence FabricPool.

"Ensuite, créez un compartiment AWS S3."

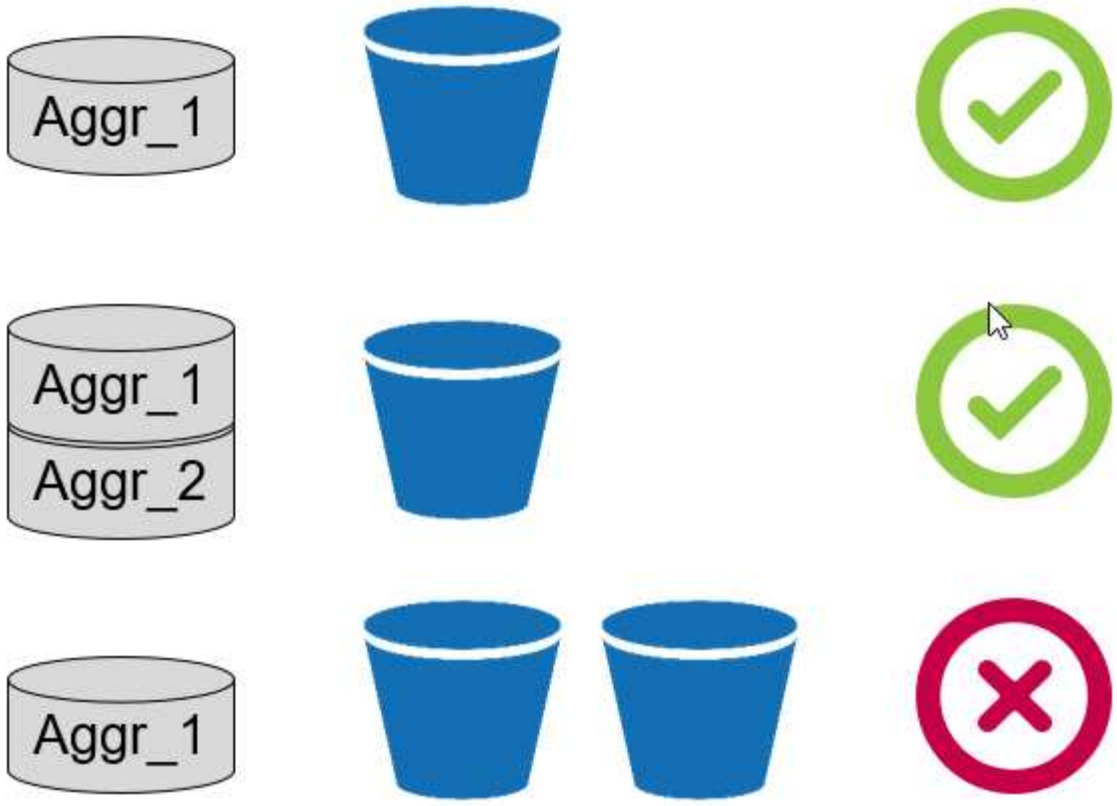
Création d'un compartiment AWS S3

Les compartiments sont des conteneurs de stockage objet qui hébergent les données. Vous devez fournir le nom et l'emplacement du compartiment dans lequel les données sont stockées avant de pouvoir être ajoutées à un agrégat en tant que Tier cloud.

> Les compartiments ne peuvent pas être créés à l'aide de OnCommand System Manager, OnCommand Unified Manager ou ONTAP.

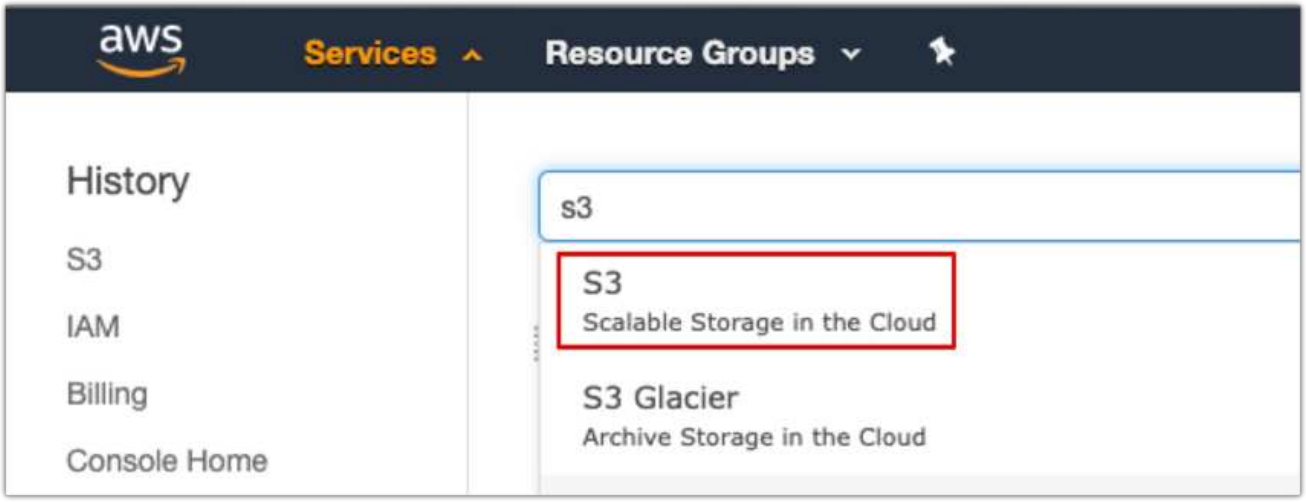
FabricPool prend en charge la connexion d'un compartiment par agrégat, comme illustré dans la figure suivante. Un seul compartiment peut être associé à un seul agrégat et un seul compartiment peut être relié à plusieurs agrégats. Toutefois, un seul agrégat ne peut pas être associé à plusieurs compartiments. Bien qu'un compartiment unique puisse être connecté à plusieurs agrégats du cluster, NetApp ne recommande pas de connecter un compartiment unique à des agrégats dans plusieurs clusters.

Lors de la planification d'une architecture de stockage, réfléchissez à l'impact possible de la relation entre compartiment et agrégat sur les performances. De nombreux fournisseurs de magasin d'objets définissent un nombre maximal d'IOPS pris en charge au niveau du compartiment ou du conteneur. Les environnements qui requièrent des performances maximales doivent utiliser plusieurs compartiments pour réduire l'éventualité où les limites des IOPS du stockage objet pouvaient affecter les performances de plusieurs agrégats FabricPool. Il est préférable de connecter un compartiment ou un conteneur unique à tous les agrégats FabricPool d'un cluster pour des environnements qui privilégient les performances de Tier cloud.

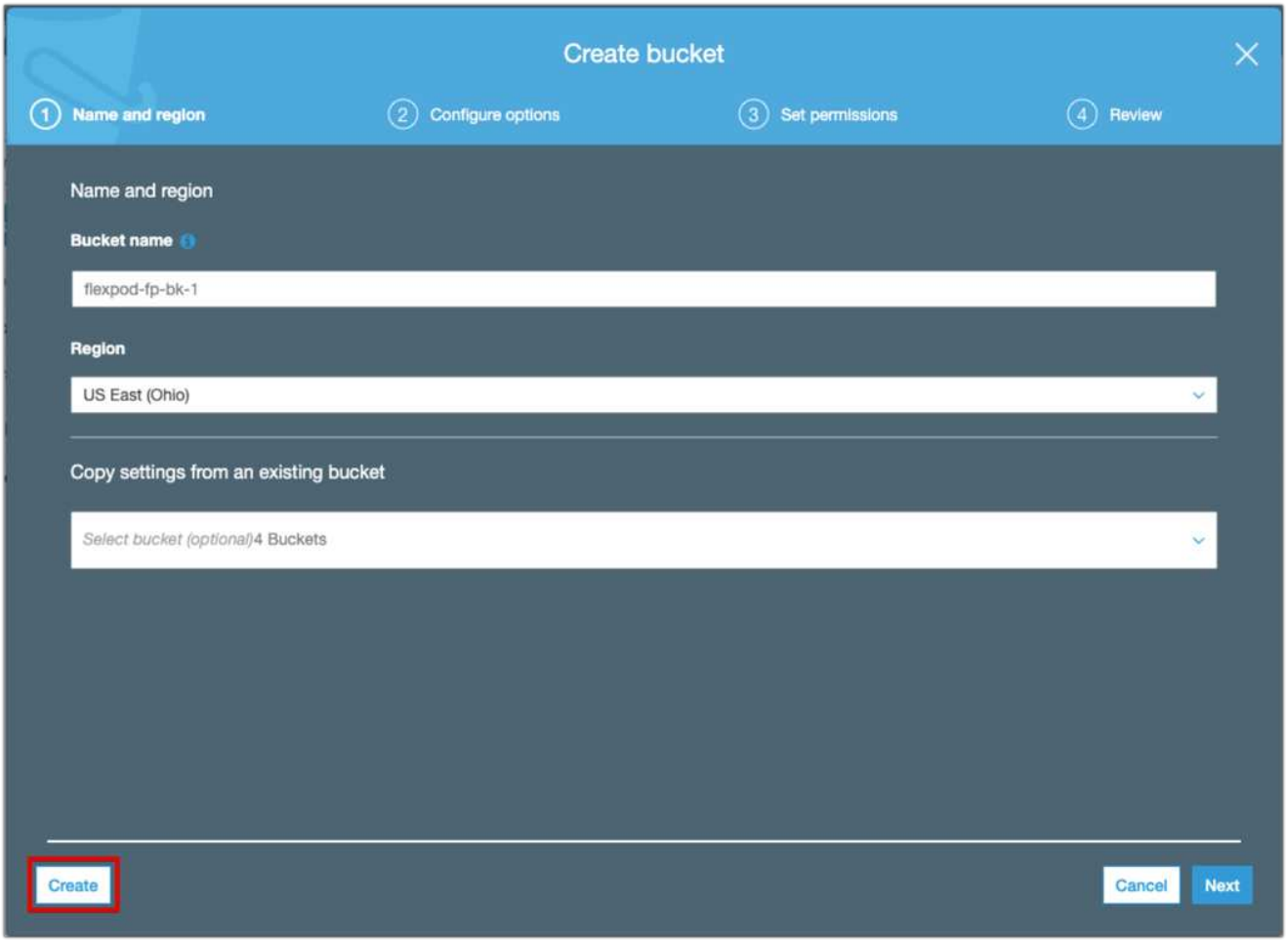


Créer un compartiment S3

1. Dans la console de gestion AWS depuis la page d'accueil, entrez S3 dans la barre de recherche.
2. Sélectionnez stockage évolutif S3 dans le cloud.



3. Sur la page d'accueil S3, sélectionnez Créer un compartiment.
4. Entrez un nom compatible DNS et choisissez la région pour créer le compartiment.



5. Cliquez sur Créer pour créer le compartiment de stockage d'objets.

"Ensuite, ajoutez un Tier cloud à ONTAP"

Ajoutez un Tier cloud à ONTAP

Avant de pouvoir joindre un magasin d'objets à un agrégat, il doit être ajouté à et identifié par ONTAP. Cette tâche peut être effectuée avec OnCommand System Manager ou l'interface de ligne de commandes de ONTAP.

FabricPool prend en charge Amazon S3, IBM Object Cloud Storage et les magasins d'objets Microsoft Azure Blob Storage en tant que tiers cloud.

Vous avez besoin des informations suivantes :

- Nom de serveur (FQDN) ; par exemple, `s3.amazonaws.com`
- ID de clé d'accès
- Clé secrète
- Nom du conteneur (nom de compartiment)

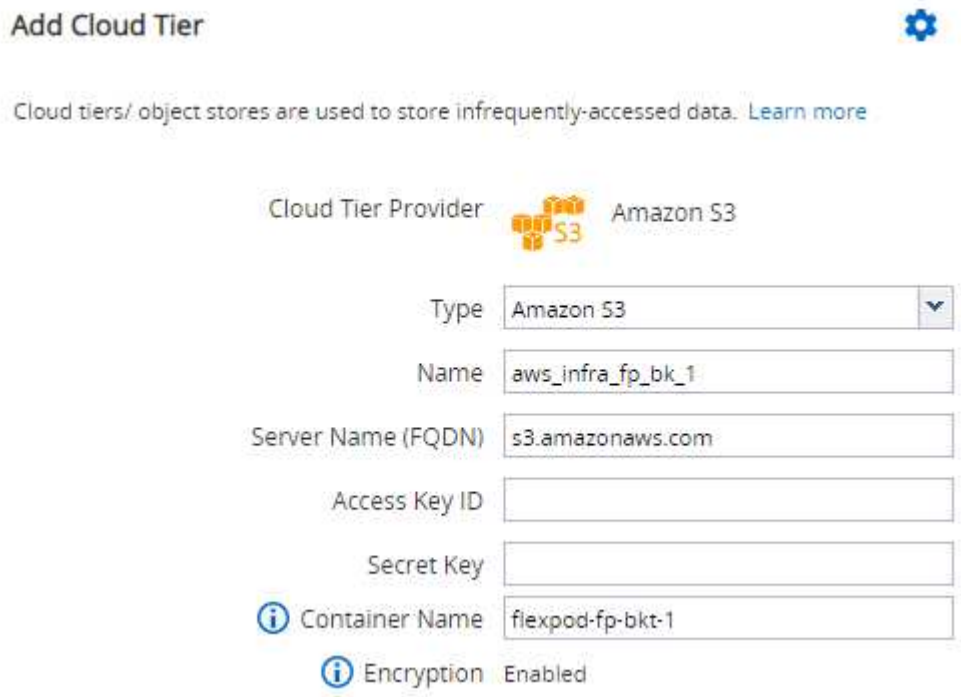
OnCommand System Manager

Pour ajouter un Tier cloud avec OnCommand System Manager, procédez comme suit :

1. Lancez OnCommand System Manager.
2. Cliquez sur stockage.
3. Cliquez sur Aggregates & disques.
4. Cliquez sur Cloud tiers.
5. Sélectionnez un fournisseur de magasin d'objets.
6. Renseignez les champs de texte requis pour le fournisseur de magasin d'objets.

   Dans le champ Nom du conteneur, entrez le nom de compartiment ou du conteneur du magasin d'objets.

7. Cliquez sur Save and Attach Aggregates.



INTERFACE DE LIGNE DE COMMANDES DE ONTAP

Pour ajouter un Tier cloud à l'aide de l'interface de ligne de commandes ONTAP, entrez les commandes suivantes :

```
object-store config create
-object-store-name <name>
-provider-type <AWS>
-port <443/8082> (AWS)
-server <name>
-container-name <bucket-name>
-access-key <string>
-secret-password <string>
-ssl-enabled true
-ipspace default
```

"Ensuite, associez un Tier cloud à un agrégat ONTAP."

Association d'un Tier cloud à un agrégat ONTAP

Lorsqu'un magasin d'objets est ajouté à et identifié par ONTAP, il doit être associé à un agrégat pour créer une FabricPool. Pour ce faire, utilisez OnCommand System Manager ou l'interface de ligne de commandes de ONTAP.

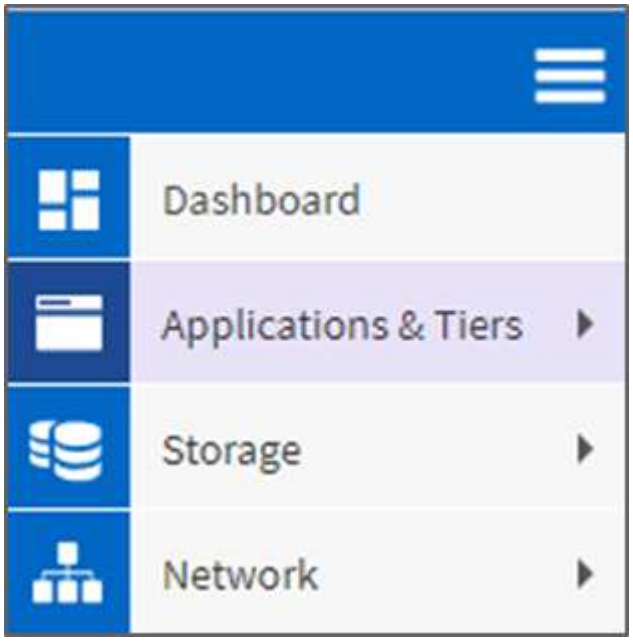
Plusieurs types de magasin d'objets peuvent être connectés à un cluster, mais un seul type de magasin d'objets peut être associé à chaque agrégat. Par exemple, un agrégat peut utiliser Google Cloud et un autre agrégat peut utiliser Amazon S3, mais un autre ne peut pas être associé aux deux.

> L'association d'un Tier cloud à un agrégat est une opération permanente. Un niveau de cloud ne peut pas être dérattaché à un agrégat auquel il est rattaché.

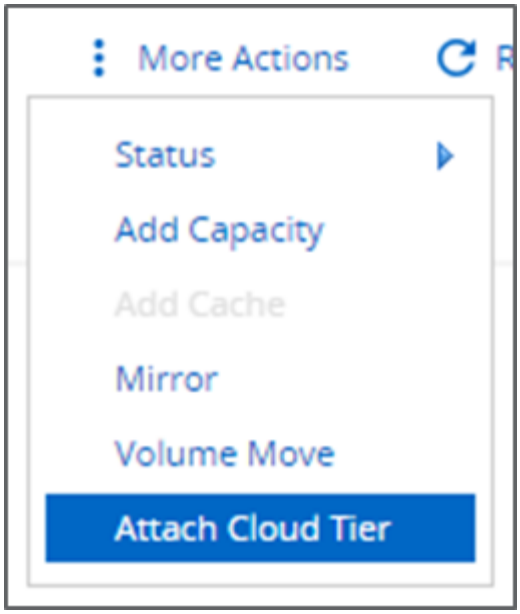
OnCommand System Manager

Pour rattacher un Tier cloud à un agrégat via OnCommand System Manager, effectuez les opérations suivantes :

1. Lancez OnCommand System Manager.
2. Cliquez sur applications et niveaux.



3. Cliquez sur niveaux de stockage.
4. Cliquer sur un agrégat.
5. Cliquez sur actions et sélectionnez attacher Cloud Tier.



6. Sélectionnez un Tier cloud.
7. Afficher et mettre à jour les règles de Tiering des volumes sur l'agrégat (facultatif). Par défaut, la règle de Tiering du volume est définie comme Snapshot uniquement.
8. Cliquez sur Enregistrer.

INTERFACE DE LIGNE DE COMMANDES DE ONTAP

Pour attacher un Tier cloud à un agrégat via l'interface de ligne de commandes ONTAP, exécutez les commandes suivantes :

```
storage aggregate object-store attach
-aggregate <name>
-object-store-name <name>
```

Exemple :

```
storage aggregate object-store attach -aggregate aggr1 -object-store-name
- aws_infra_fp_bk_1
```

"Ensuite : définissez la règle de Tiering du volume."

Définition de la règle de Tiering des volumes

Par défaut, les volumes utilisent la règle de Tiering aucun volume. Une fois la création de volume effectuée, la règle de Tiering des volumes peut être modifiée à l'aide de OnCommand System Manager ou de l'interface de ligne de commande de ONTAP.

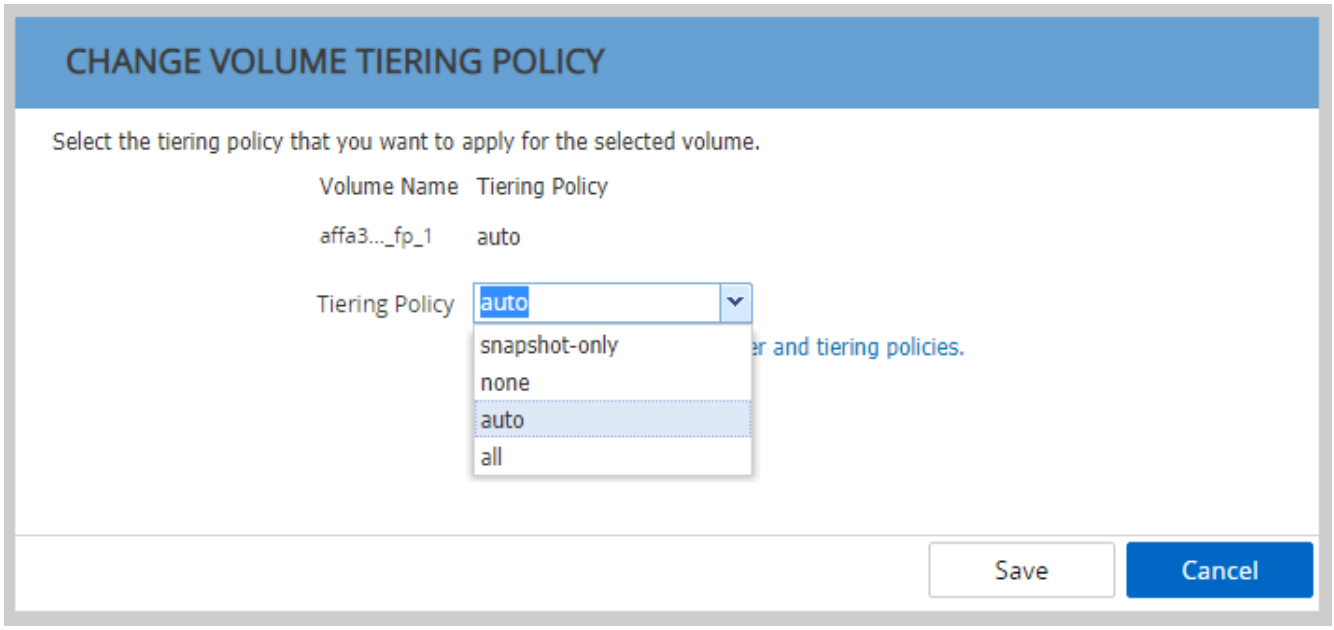
Lorsqu'il est utilisé avec FlexPod, FabricPool propose trois règles de Tiering des volumes : automatique, Snapshot uniquement et aucune.

- **Auto**
  - Tous les blocs inactifs du volume sont déplacés vers le cloud. Si l'agrégat est utilisé à plus de 50 %, il faut environ 31 jours pour que les blocs inactifs soient à froid. La période de refroidissement automatique est réglable entre 2 jours et 63 jours en utilisant le `tiering-minimum-cooling-days` réglage.
  - Lorsque les blocs inactifs d'un volume dont la règle de Tiering est définie sur Auto sont lus de manière aléatoire, ils sont écrits et mis à chaud sur le Tier de performance.
  - Lorsque les blocs inactifs dans un volume dont la règle de Tiering est définie sur Auto sont lus de manière séquentielle, ils restent inactifs et restent sur le Tier cloud. Ils ne sont pas écrits sur le Tier de performance.
- **Instantané uniquement**
  - Les blocs de snapshots inactifs dans le volume qui ne sont pas partagés avec le système de fichiers actif sont déplacés vers le Tier cloud. Si l'agrégat est utilisé à plus de 50 %, il faut environ 2 jours pour que les blocs de snapshot inactifs soient inactifs. La période de refroidissement uniquement à snapshot est réglable de 2 à 63 jours en utilisant le `tiering-minimum-cooling-days` réglage.
  - Lorsque les blocs inactifs dans un volume dont la règle de Tiering est définie sur Snapshot uniquement sont lus, ils sont écrits et mis à chaud sur le Tier de performance.
- **Aucun (par défaut)**
  - Les volumes définis sur aucune n'utilisent la règle de Tiering ne transfèrent pas les données inactives vers le Tier cloud.
  - La définition de la règle de Tiering sur aucun empêche la hiérarchisation.
  - Les données de volume précédemment transférées vers le Tier cloud restent dans le Tier cloud jusqu'à ce qu'elles soient fortement sollicitées et sont automatiquement retransférées vers le Tier de performance.

OnCommand System Manager

Pour modifier la règle de hiérarchisation d'un volume à l'aide de OnCommand System Manager, procédez comme suit :

1. Lancez OnCommand System Manager.
2. Sélectionnez un volume.
3. Cliquez sur autres actions et sélectionnez Modifier la règle de hiérarchisation.
4. Sélectionnez la règle de Tiering à appliquer au volume.
5. Cliquez sur Enregistrer.



INTERFACE DE LIGNE DE COMMANDES DE ONTAP

Pour modifier la règle de hiérarchisation d'un volume à l'aide de l'interface de ligne de commandes ONTAP, exécutez la commande suivante :

```
volume modify -vserver <svm_name> -volume <volume_name>
-tiering-policy <auto|snapshot-only|all|none>
```

"Ensuite, définissez le Tiering des volumes sur les jours de refroidissement minimum."

Définissez le Tiering des volumes sur les jours de refroidissement minimum

Le `tiering-minimum-cooling-days` Le paramètre détermine le nombre de jours devant être écoulés avant que les données inactives d'un volume à l'aide des règles Auto ou Snapshot uniquement sont considérées comme inactives et éligibles pour le Tiering.

Auto

La valeur par défaut `tiering-minimum-cooling-days` La définition de la règle de hiérarchisation automatique est définie sur 31 jours.

Étant donné que les lectures maintiennent une température élevée des blocs, l'augmentation de cette valeur peut réduire la quantité de données éligibles à un Tier et augmenter la quantité de données conservées sur le Tier de performances.

Si vous souhaitez réduire cette valeur par défaut de 31 jours, notez que les données ne doivent plus être actives avant d'être marquées comme étant inactives. Par exemple, si une charge de travail sur plusieurs jours doit effectuer un nombre important d'écritures au jour 7, celle du volume `tiering-minimum-cooling-days` le réglage ne doit pas être inférieur à 8 jours.

> Le stockage objet n'est pas transactionnel de base comme le stockage de fichiers ou de blocs. Les modifications apportées aux fichiers stockés sous forme d'objets dans des volumes dont les jours de refroidissement sont trop serrés peuvent entraîner la création de nouveaux objets, la fragmentation des objets existants et l'ajout d'inefficacités du stockage.

Snapshot uniquement

La valeur par défaut `tiering-minimum-cooling-days` La définition de la règle de Tiering uniquement Snapshot est de 2 jours. Un délai minimum de 2 jours permet des processus en arrière-plan pour un stockage optimal et empêche les processus quotidiens de protection des données d'avoir à lire les données depuis le Tier cloud.

INTERFACE DE LIGNE DE COMMANDES DE ONTAP

Pour modifier un volume `tiering-minimum-cooling-days` Pour le paramètre via l'interface de ligne de commandes de ONTAP, exécutez la commande suivante :

```
volume modify -vserver <svm_name> -volume <volume_name> -tiering-minimum
-cooling-days <2-63>
```

Le niveau de privilège avancé est requis.

> La modification de la règle de Tiering entre Auto et Snapshot uniquement (ou vice-versa) entraîne une réinitialisation de la période d'inactivité des blocs sur le Tier de performance. Par exemple, un volume utilisant la règle de Tiering automatique des volumes avec des données inactives pendant 20 jours dispose que l'inactivité des données de Tier de performance est réinitialisée à 0 jours si la règle de Tiering est définie sur Snapshot uniquement.

Performances

Dimensionnez le Tier de performance

Lorsque vous envisagez de dimensionner, gardez à l'esprit que le Tier de performance doit être capable des tâches suivantes :

- Prise en charge des données fortement sollicitées
- La prise en charge des données inactives jusqu'à l'analyse du Tiering déplace les données vers le Tier cloud
- Prendre en charge les données de Tier cloud actives et écrites à nouveau sur le Tier de performance
- Prise en charge des métadonnées WAFL associées au niveau de cloud associé

Pour la plupart des environnements, un rapport performances/capacité de 1 à 10 sur les agrégats FabricPool est extrêmement prudent, tout en permettant des économies de stockage importantes. Par exemple, si l'objectif est de transférer des 200 To vers le Tier cloud, l'agrégat de Tier de performance doit atteindre 20 To au minimum.

> Les écritures depuis le Tier cloud vers le Tier de performance sont désactivées si la capacité du Tier de performance est supérieure à 70 %. Dans ce cas, les blocs sont lus directement depuis le Tier cloud.

Dimensionnez le Tier cloud

Lors de l'évaluation du dimensionnement, le magasin d'objets agissant comme Tier cloud doit être capable de réaliser les tâches suivantes :

- Prise en charge des lectures de données inactives existantes
- Prise en charge des écritures de nouvelles données inactives
- Prise en charge de la suppression et de la défragmentation des objets

Le coût de possession

Le "Calculateur économique FabricPool" Disponible auprès du cabinet d'analyse indépendant Evaluator Group, cabinet d'analyse IT indépendant, afin de réaliser des économies sur site et dans le cloud pour le stockage des données inactives. Ce calculateur fournit une interface simple qui détermine le coût de stockage des données peu utilisées sur un Tier de performance plutôt que de les transférer vers un Tier cloud pour le reste du cycle de vie des données. Sur la base d'un calcul effectué sur 5 ans, les quatre facteurs clés (la capacité source, la croissance des données, la capacité Snapshot et le pourcentage de données inactives) sont utilisés pour déterminer les coûts de stockage sur la période.

Conclusion

La transition vers le cloud varie d'une entreprise à l'autre, et même d'une unité commerciale à l'autre. Si certains choisissent une adoption rapide, d'autres sont plus conservatrices. FabricPool s'intègre à la stratégie cloud des entreprises, quelle que soit leur taille, et quelle que soit la vitesse d'adoption du cloud. Une démonstration encore plus poussée de l'efficacité et de l'évolutivité d'une infrastructure FlexPod.

Où trouver des informations complémentaires

Pour en savoir plus sur les informations données dans ce livre blanc, consultez ces documents et/ou sites web :

- Meilleures pratiques pour FabricPool

  "www.netapp.com/us/media/tr-4598.pdf"

- Documentation produit NetApp

  "https://docs.netapp.com"

- Tr-4036 : spécifications techniques de data Center FlexPod

  "https://www.netapp.com/us/media/tr-4036.pdf"

FlexPod Datacenter avec IBM Cloud Private

Sreenivasa Edula, Cisco Thanachit Wichianchai, IBM Jacky Ben-Bassat, IBM Global Alliance, NetApp

IBM Cloud Private (ICP) est une plateforme sur site qui permet de développer et de gérer des applications conteneurisées pour les utilisations cloud natives et de modernisation des applications. Il s'agit d'un environnement intégré basé sur Kubernetes pour l'orchestration de conteneurs. Il comprend un référentiel d'images privées pour les conteneurs Docker, une console de gestion, un framework de surveillance, de nombreuses applications open source et conteneurisées IBM, et bien plus encore. L'association de cette plateforme et de FlexPod simplifie le déploiement et la gestion de votre infrastructure grâce à l'infrastructure convergée de Cisco et NetApp. Vous bénéficiez également d'une efficacité du stockage, d'une meilleure protection des données, d'une réduction des risques et de la flexibilité nécessaires pour faire évoluer cette pile d'infrastructure haute disponibilité afin de répondre aux nouveaux besoins de l'entreprise et à d'autres évolutions au fil du temps.

"FlexPod Datacenter avec IBM Cloud Private"

FlexPod Datacenter pour le cloud hybride avec Cisco CloudCenter et NetApp Private Storage : conception

Haseeb Niazi, Cisco David Arnette, NetApp

Les conceptions validées par Cisco (CVD) proposent des systèmes et des solutions conçus, testés et documentés pour faciliter et améliorer les déploiements client. Ces conceptions intègrent une large gamme de technologies et de produits dans une gamme de solutions qui ont été développées pour répondre aux besoins commerciaux des clients et pour les guider de la conception au déploiement.

"FlexPod Datacenter pour le cloud hybride avec Cisco CloudCenter et NetApp Private Storage : conception"

FlexPod Datacenter pour le multicloud avec Cisco CloudCenter et NetApp Data Fabric

Haseeb Niazi, Cisco David Arnette, NetApp

Ce document contient des instructions détaillées de configuration et d'implémentation pour la configuration de FlexPod Datacenter pour le cloud hybride. Les éléments de conception suivants distinguent cette version de FlexPod des modèles précédents :

- Intégration de Cisco CloudCenter avec FlexPod Datacenter avec l'ACI comme Cloud privé
- Intégration de Cisco CloudCenter avec les clouds publics Amazon Web Services (AWS) et Microsoft Azure Resource Manager (MS Azure RM)
- Assurer une connectivité sécurisée entre le data Center FlexPod et les clouds publics pour sécuriser le trafic entre les machines virtuelles

- Connectivité sécurisée entre le data Center FlexPod et NetApp Private Storage (NPS) pour le trafic de réplication des données
- Possibilité de déployer des instances applicatives dans des clouds publics ou privés et d'obtenir les données applicatives à jour disponibles pour ces instances via l'orchestration pilotée par Cisco CloudCenter
- Configuration, validation et mise en avant des aspects opérationnels d'un environnement de développement et de test dans ce nouveau mode de cloud hybride.

"FlexPod Datacenter pour le multicloud avec Cisco CloudCenter et NetApp Data Fabric"