Cloud hybride FlexPod avec Cloud Volumes ONTAP pour Epic

FlexPod

NetApp
January 21, 2025

Sommaire

Cloud hybride FlexPod avec Cloud Volumes ONTAP pour Epic . . . 1
Tr-4960 : cloud hybride FlexPod avec Cloud Volumes ONTAP pour Epic . . . 1
Composants de la solution . . . 3
Installation et configuration . . . 8
Configuration SAN . . . 13
Validation des solutions . . . 26
Conclusion . . . 36
Où trouver des informations complémentaires . . . 37

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.

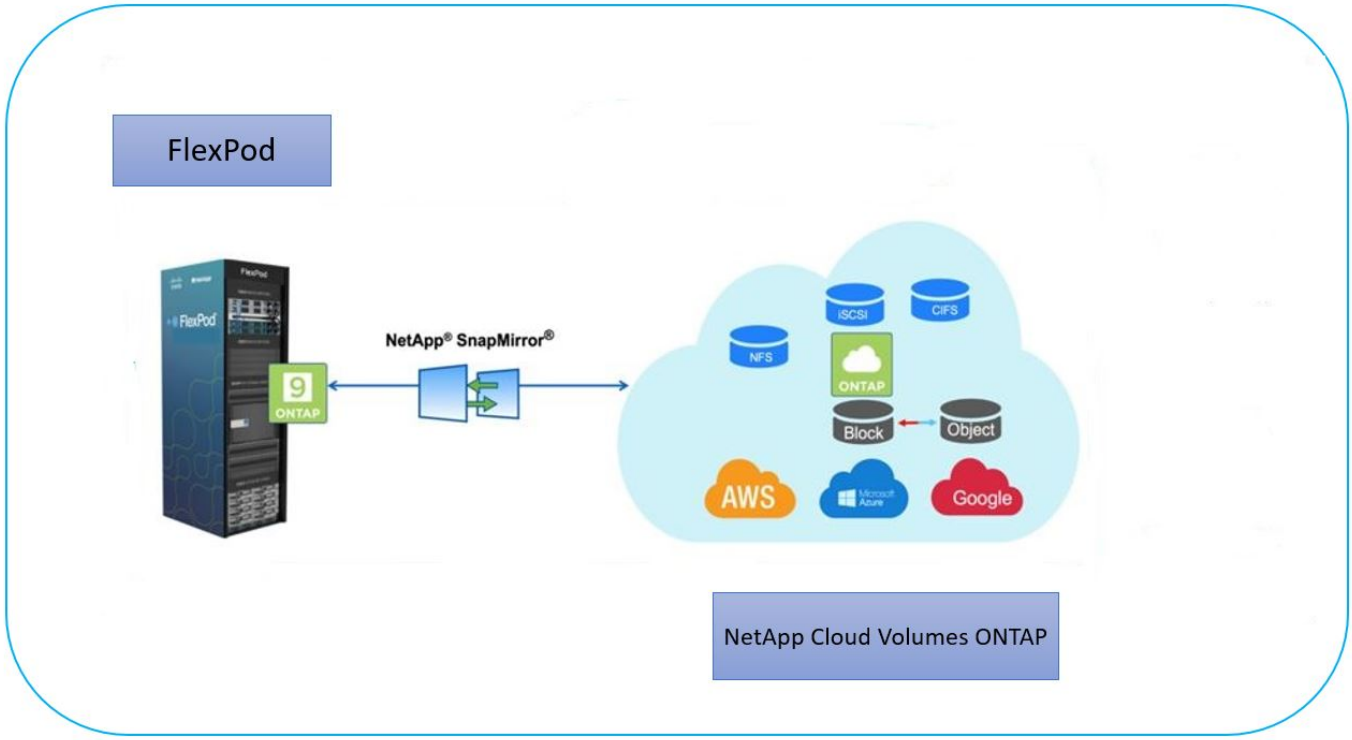
Face à la taille croissante des données de santé et aux informations exploitables qu'elles peuvent fournir, les services de données de santé et la protection des données sont deux aspects à la fois essentiels et complexes. Premièrement, les données de santé doivent être à la fois disponibles et protégées 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 :

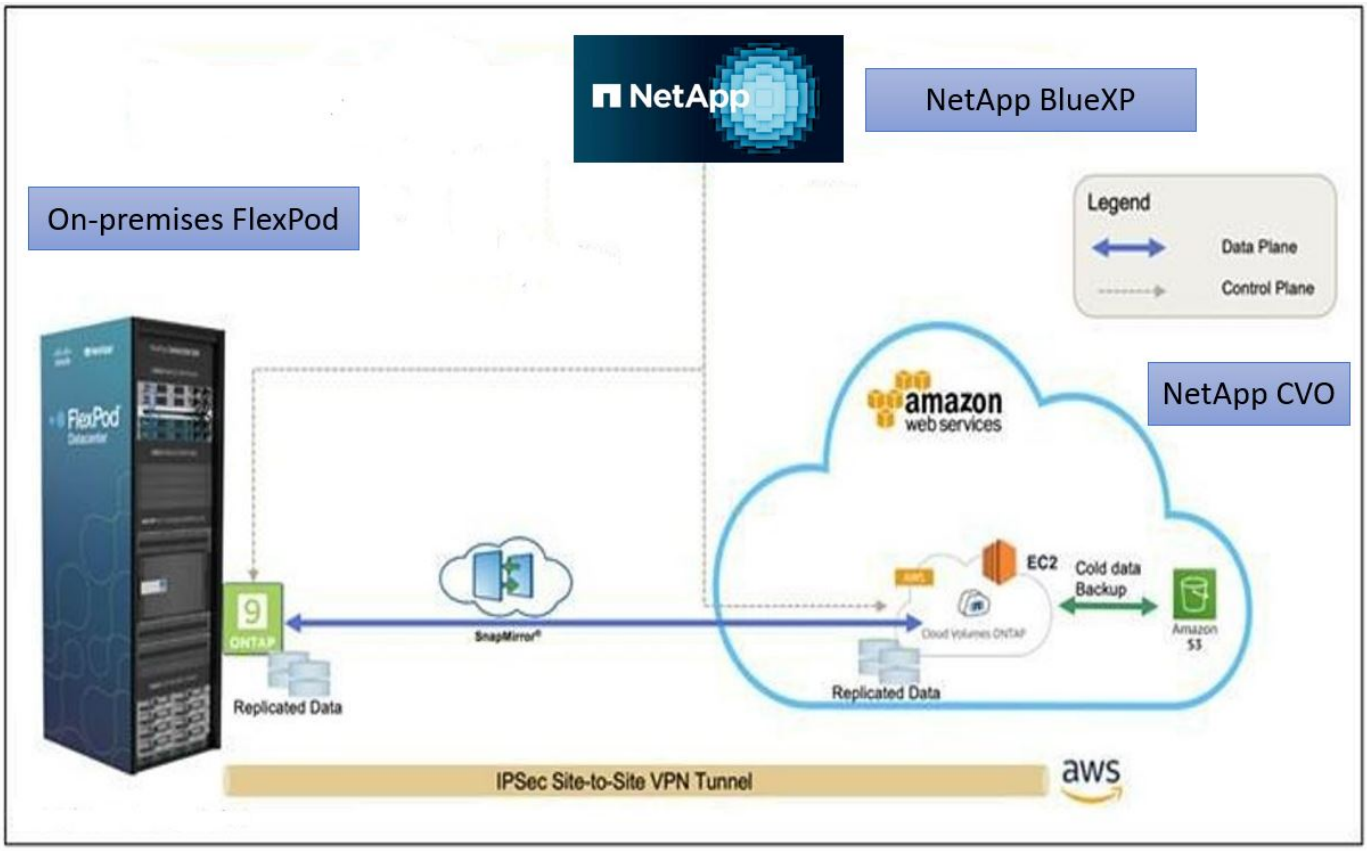
- **Protection personnalisée.** Cloud Volumes ONTAP assure la réplication des données au niveau des blocs de ONTAP vers le cloud afin de maintenir la destination à jour grâce à des mises à jour incrémentielles. Les utilisateurs peuvent spécifier une planification de synchronisation pour déterminer quand 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.

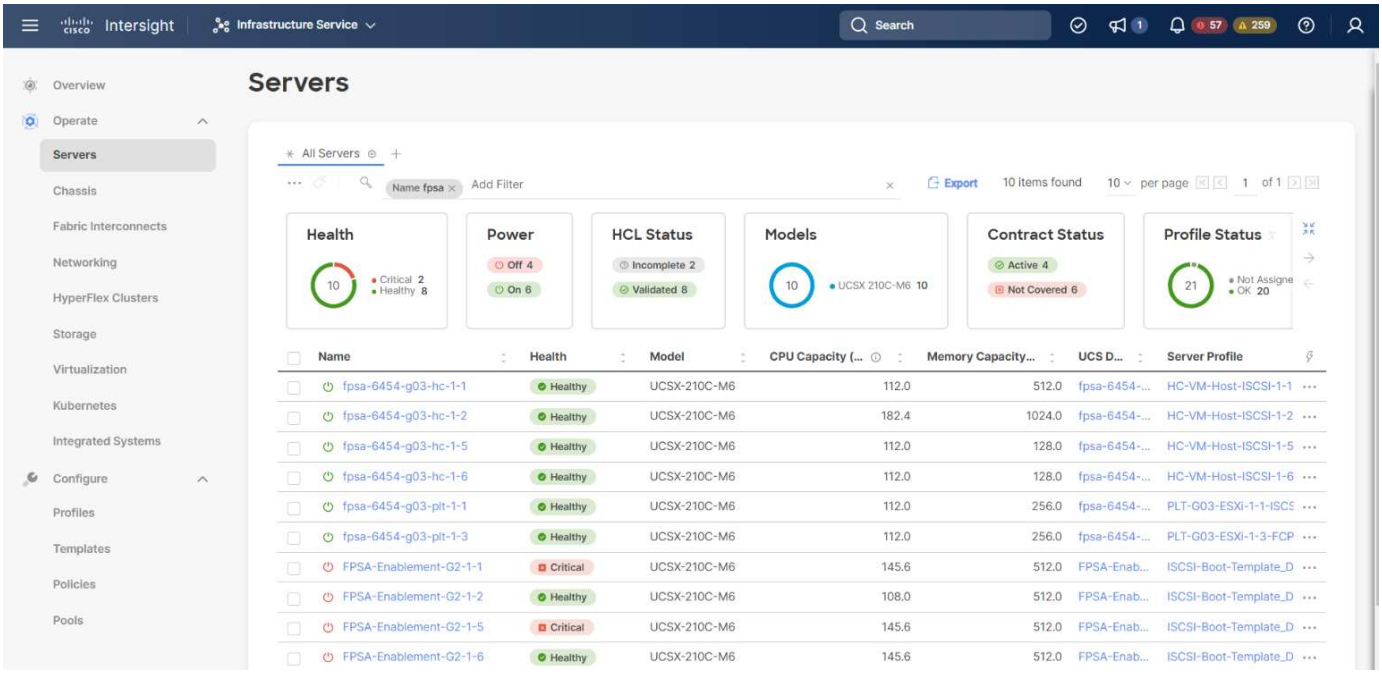
Pour plus d'informations, voir "Active IQ Unified Manager".

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.

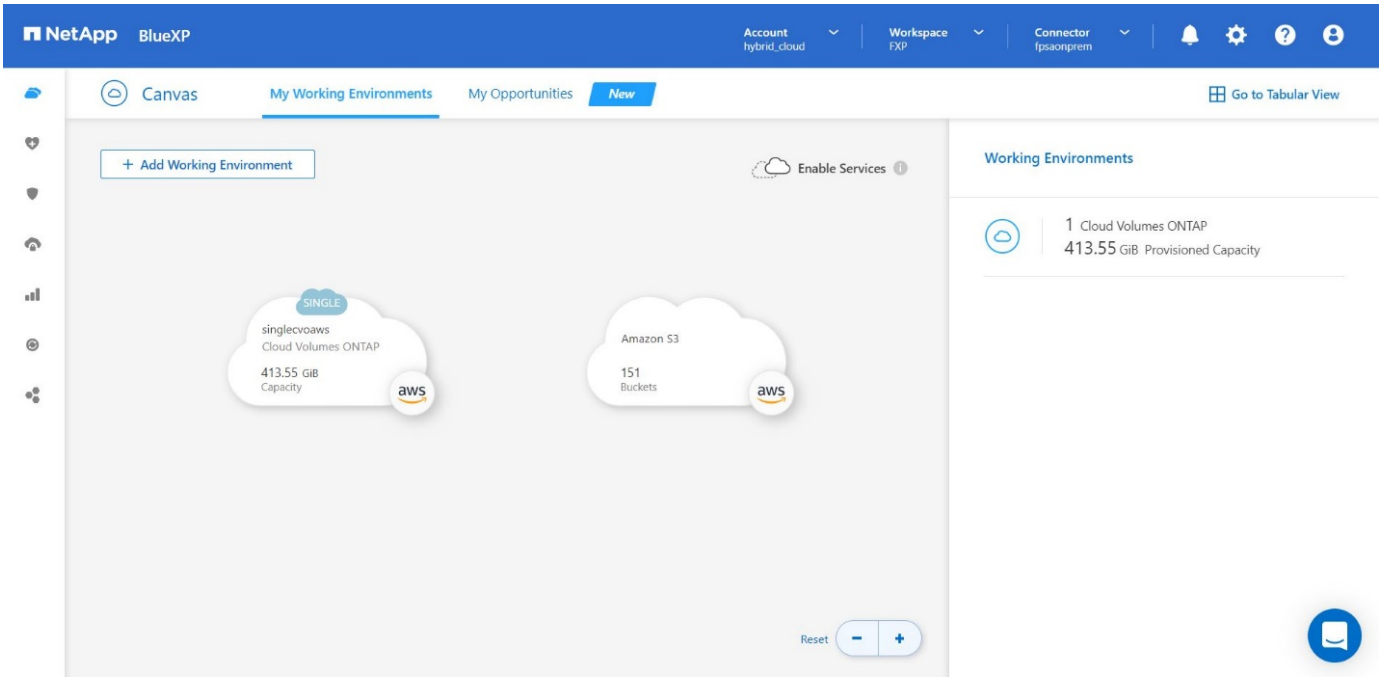
   Avant d'ajouter un environnement de travail Cloud volumes ONTAP, vous devez déployer Connector. BlueXP vous invite si vous essayez de créer votre premier environnement de travail Cloud Volumes ONTAP sans connecteur. Pour déployer Connector dans AWS à partir de BlueXP, consultez cette page "lien".

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`.

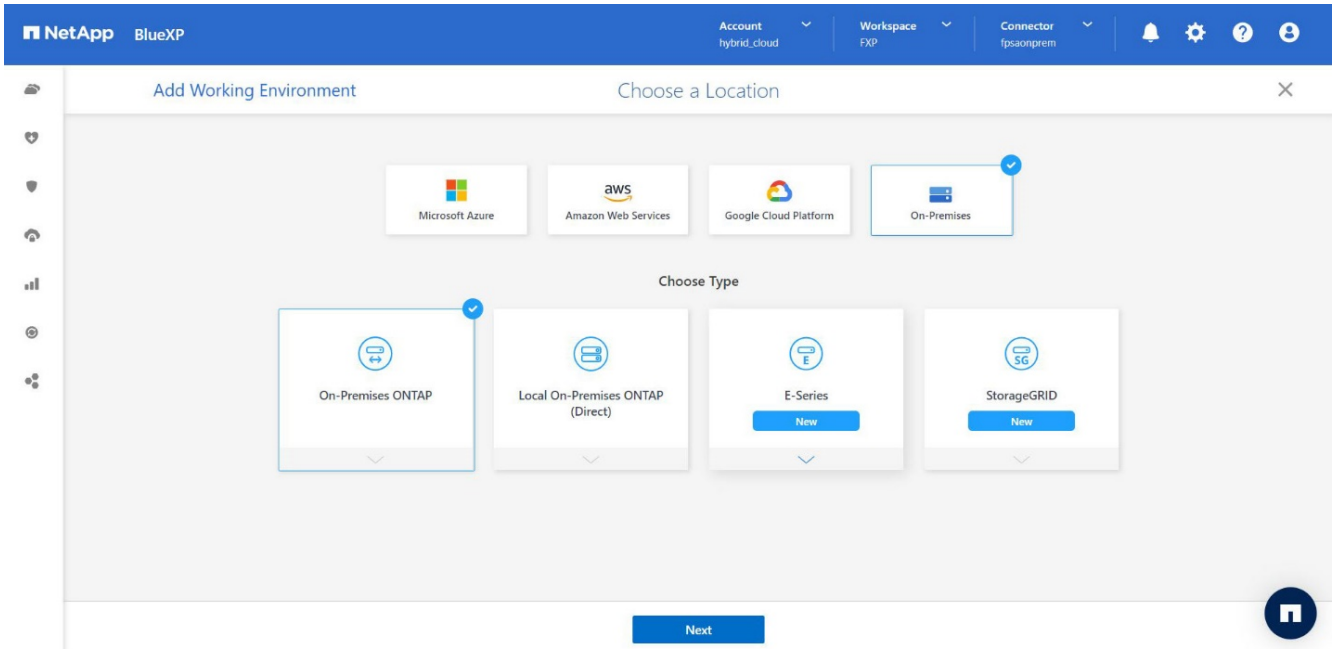
6. Mappez la LUN sur le groupe initiateur.

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

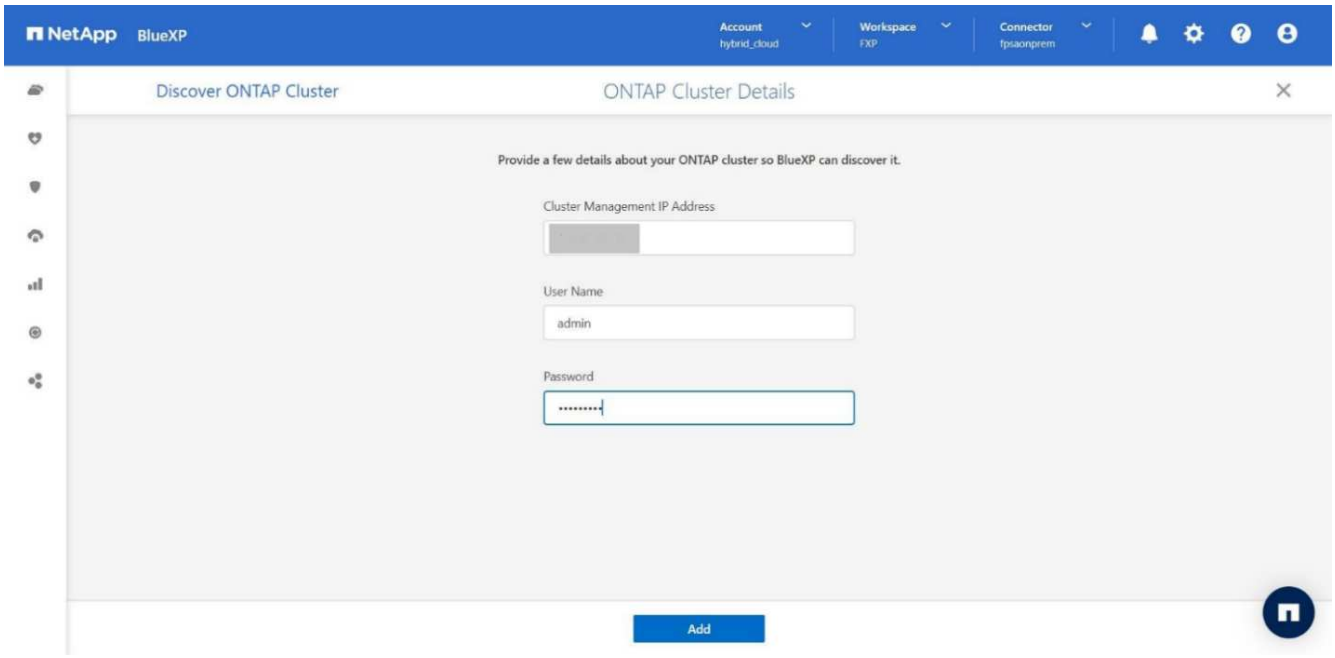
Ajoutez le stockage FlexPod sur site à BlueXP

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**.

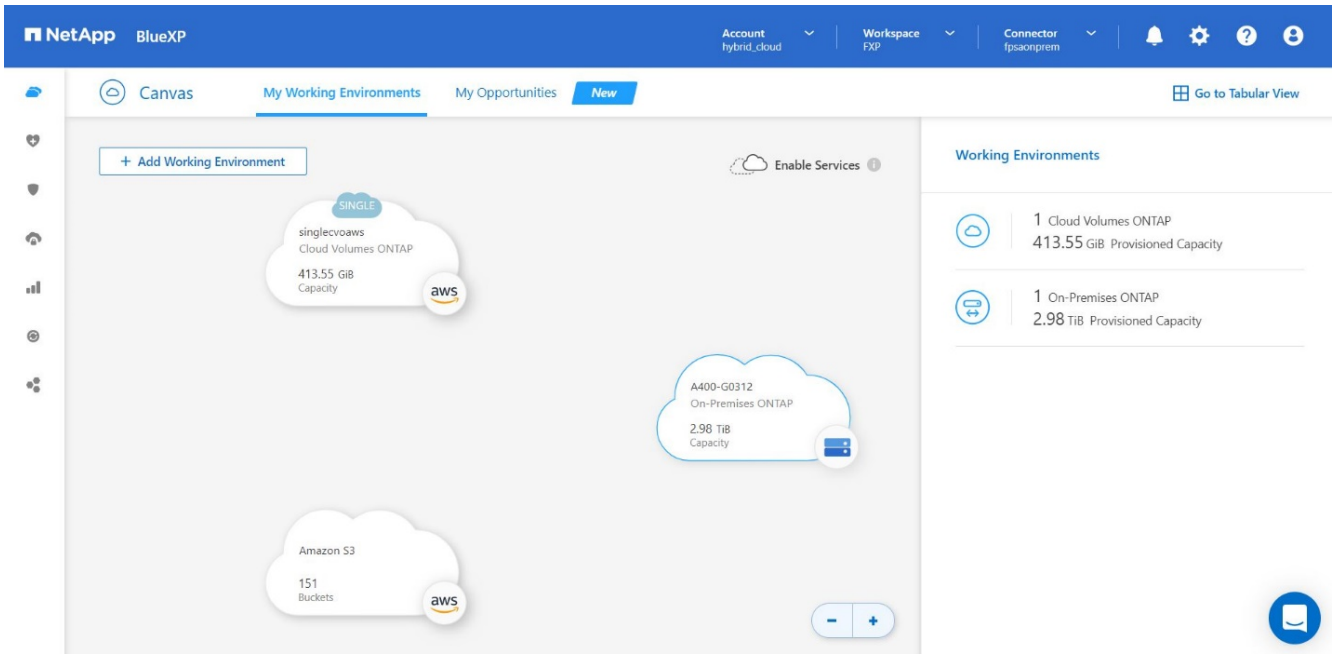


4. Sur la page ONTAP Cluster Details (Détails du cluster ONTAP), entrez l'adresse IP de gestion du cluster et le mot de passe du compte d'utilisateur admin. Cliquez ensuite sur **Ajouter**.



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
```

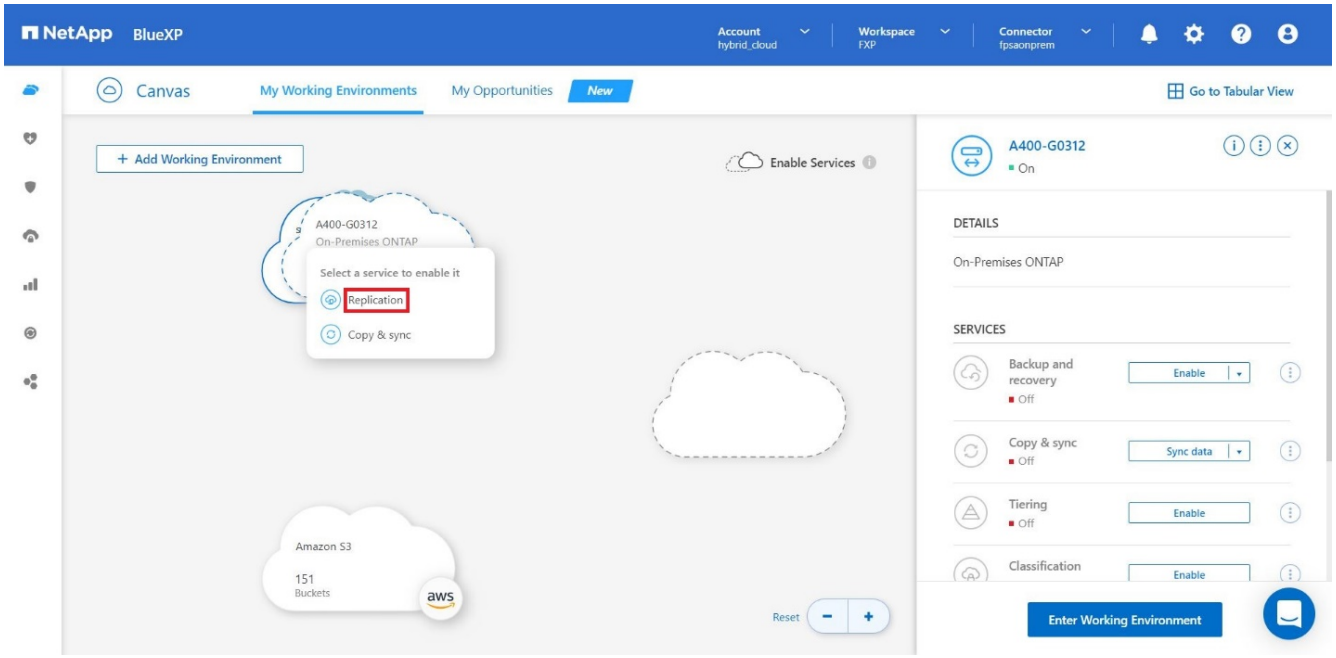
En cours d'exécution, le `Dgen.pl` script utilise 85 % du système de fichiers pour la génération de données par défaut.

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.

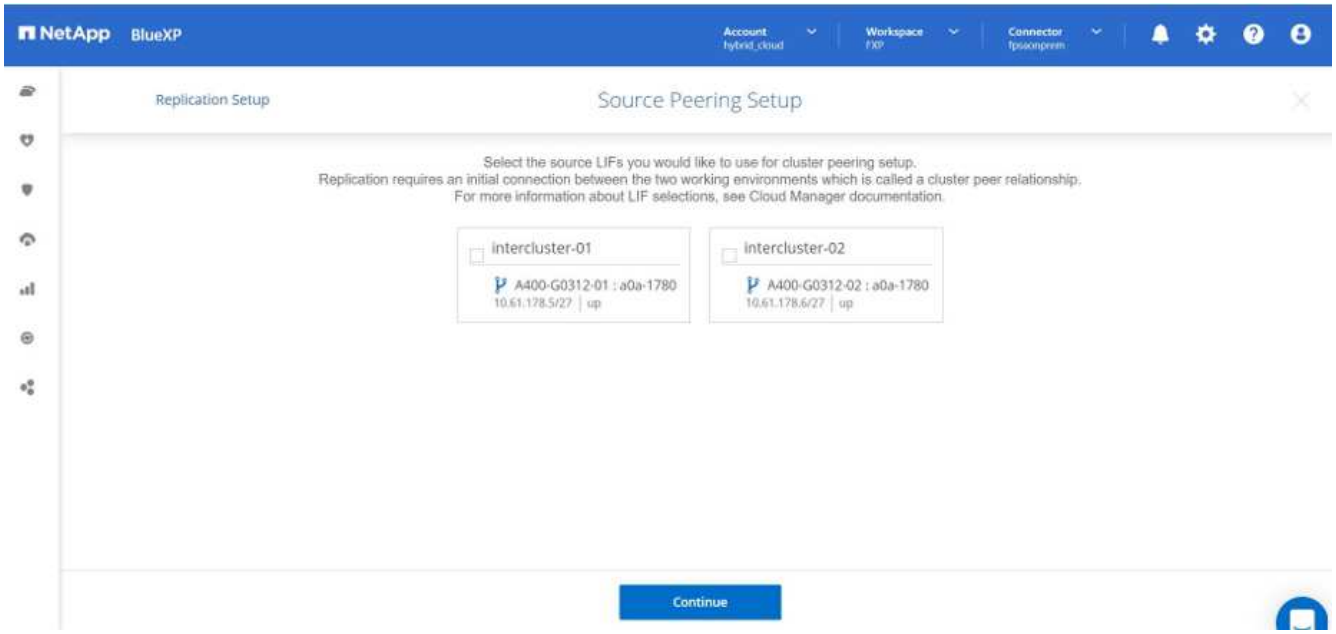
Effectuez les étapes suivantes pour configurer la réplication SnapMirror entre votre système ONTAP sur site et CVO.

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**.

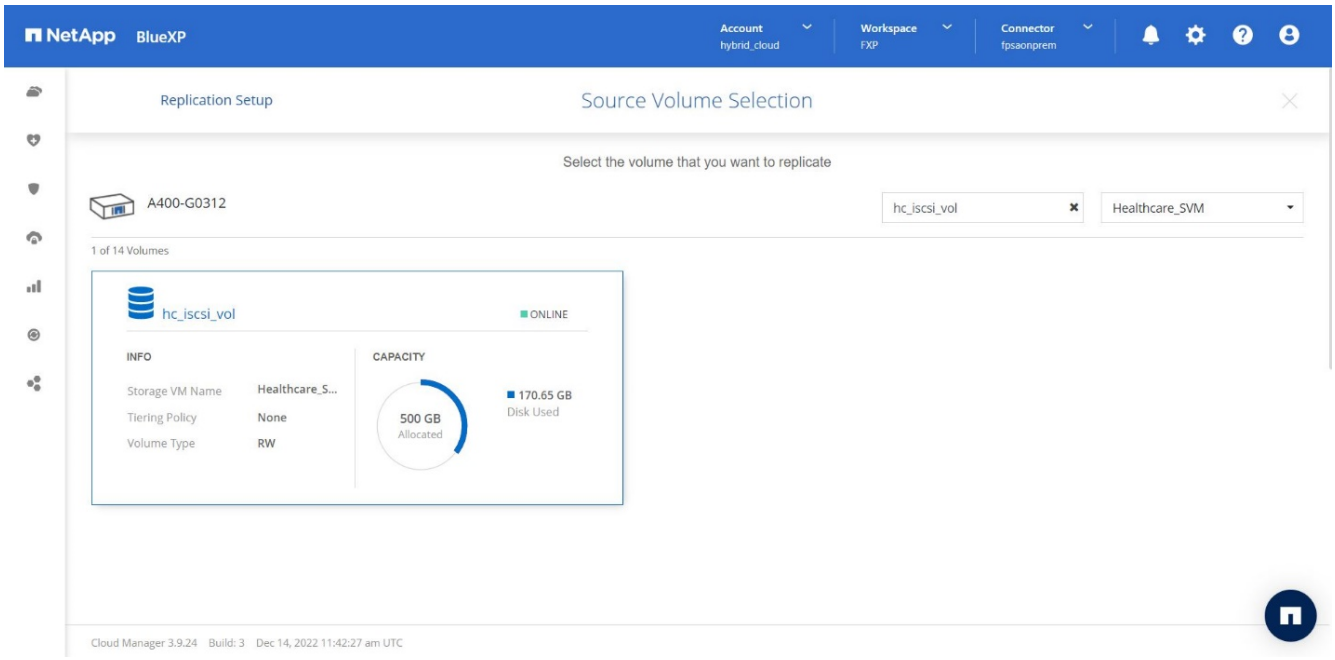


Les autres étapes expliquent comment créer une relation synchrone entre Cloud Volumes ONTAP et les clusters ONTAP sur site.

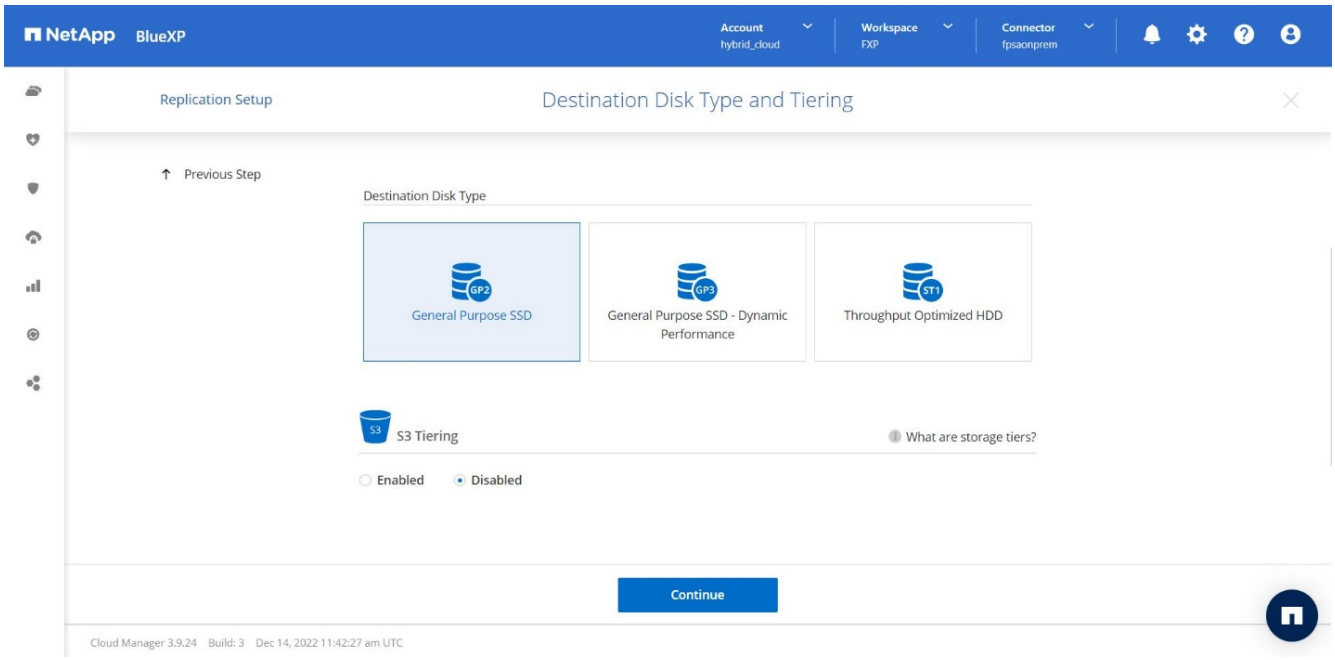
3. **Configuration du peering source et destination.** si cette page s'affiche, sélectionnez toutes les LIFs intercluster pour la relation entre pairs de cluster.



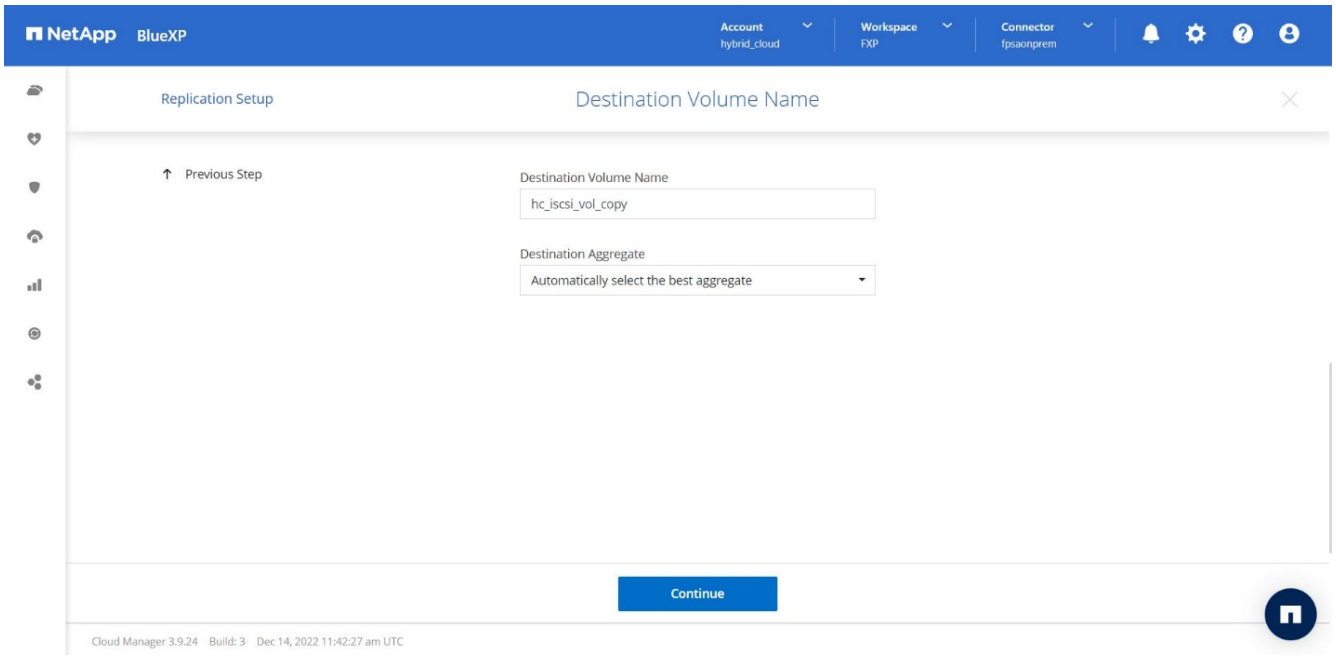
4. **Sélection du volume source.** sélectionnez le volume que vous souhaitez répliquer.



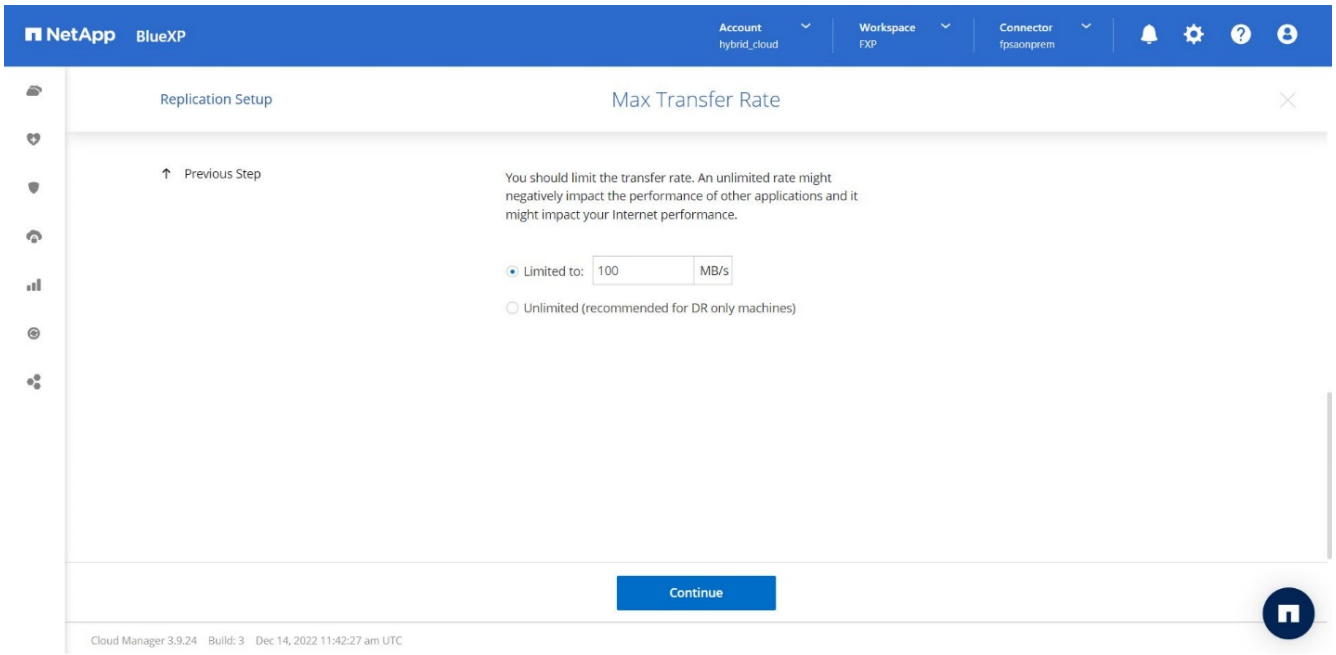
5. **Type de disque de destination et hiérarchisation.** si la cible est un système Cloud Volumes ONTAP, sélectionnez le type de disque de destination et choisissez si vous souhaitez activer la hiérarchisation des données.



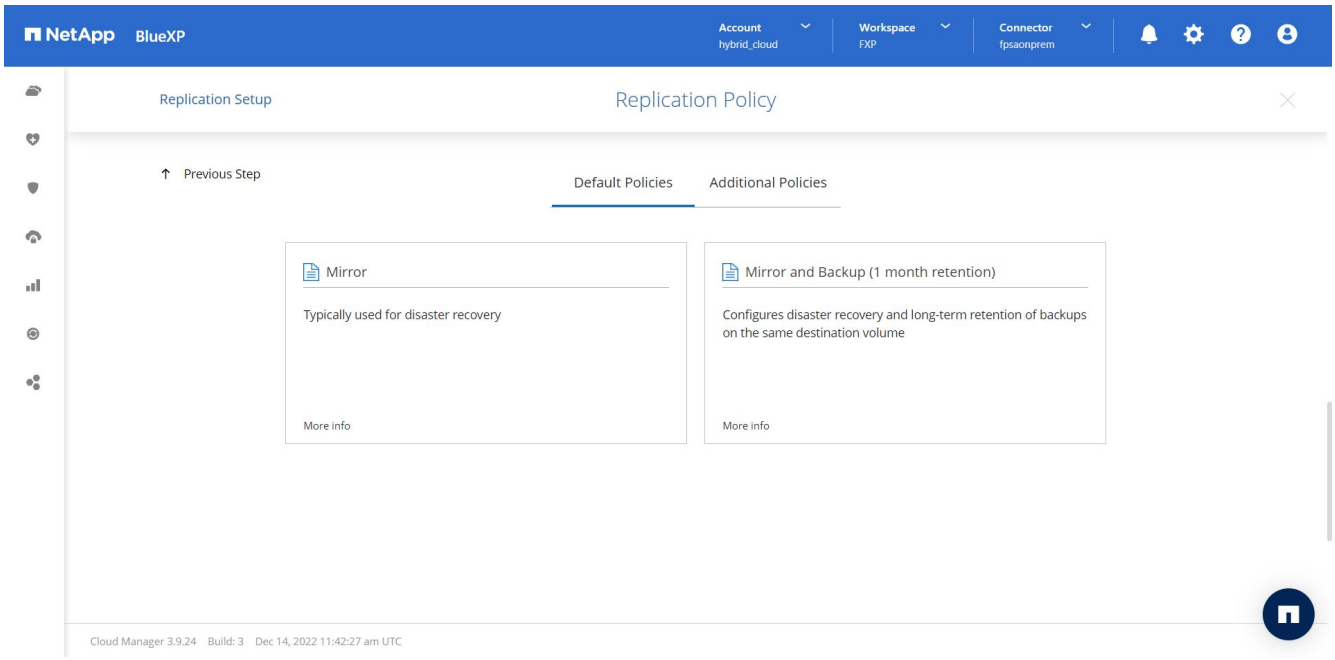
6. **Nom du volume de destination :** Indiquez le nom du volume de destination et choisissez l'agrégat de destination. Si la destination est un cluster ONTAP, vous devez également spécifier la VM de stockage de destination.



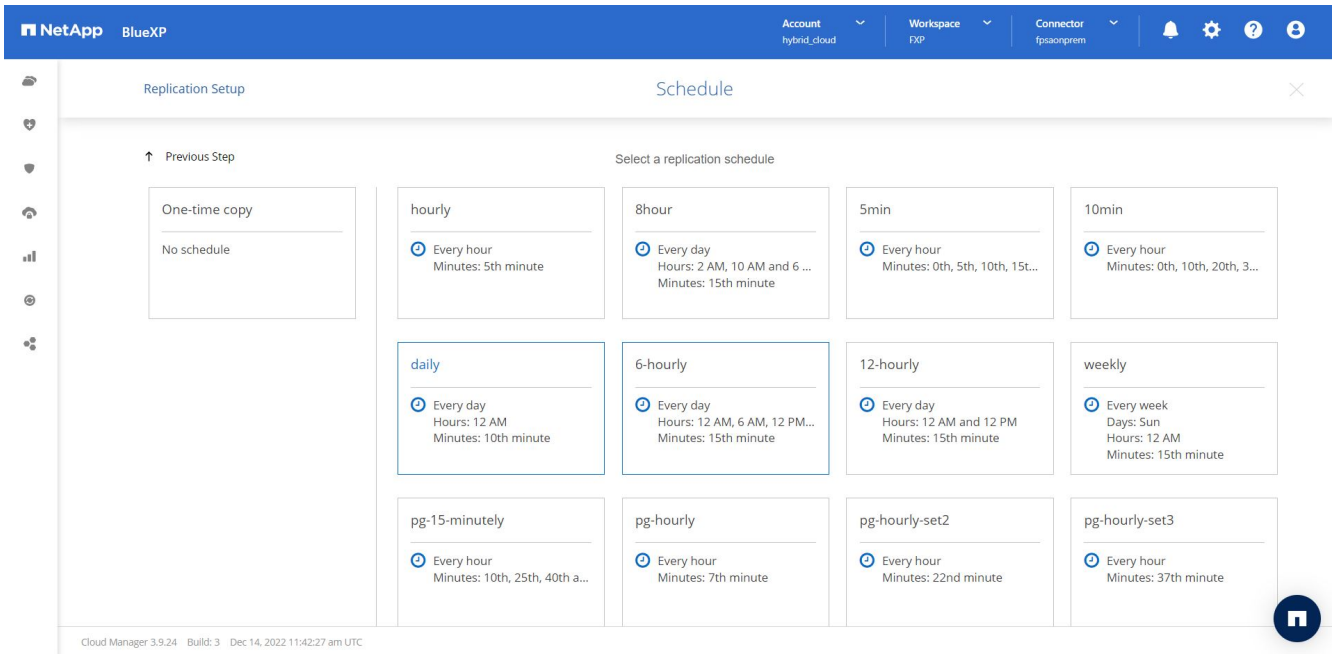
7. **Taux de transfert max.** Indiquez le taux maximal (en mégaoctets par seconde) auquel les données peuvent être transférées.



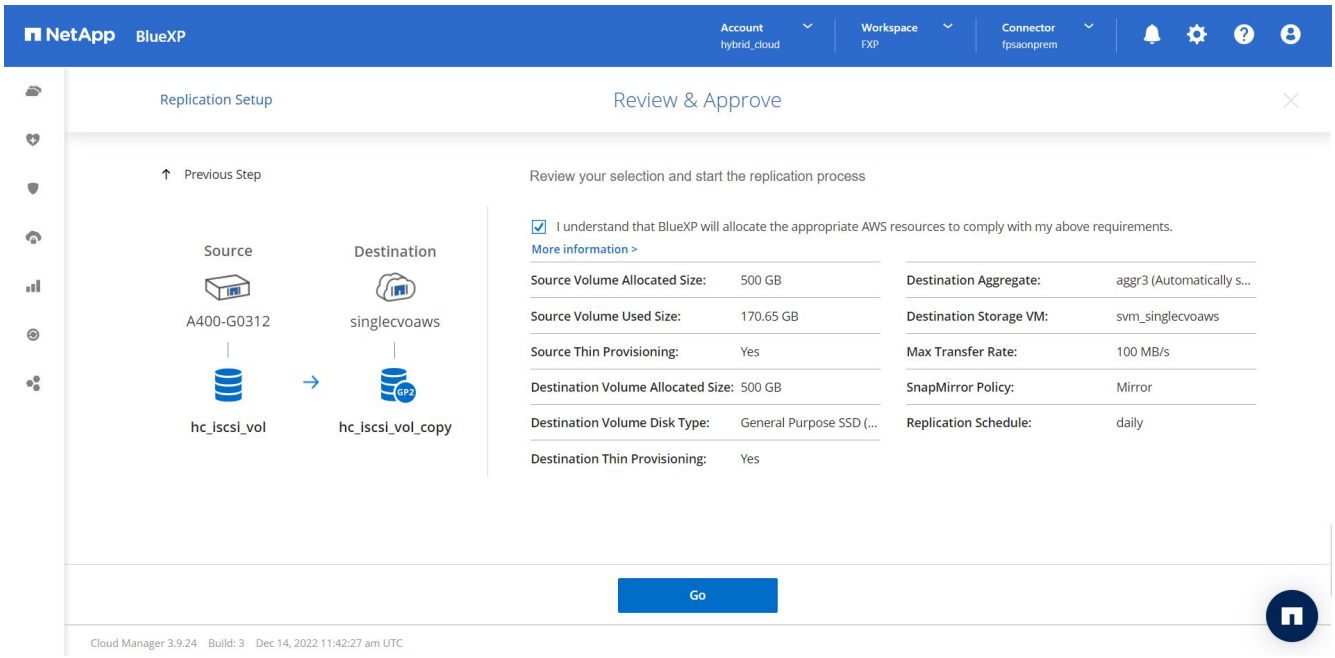
8. **Règle de réplication.** Choisissez une stratégie par défaut ou cliquez sur **règles supplémentaires**, puis sélectionnez l'une des stratégies avancées. Pour obtenir de l'aide, "en savoir plus sur les règles de réplication".



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.

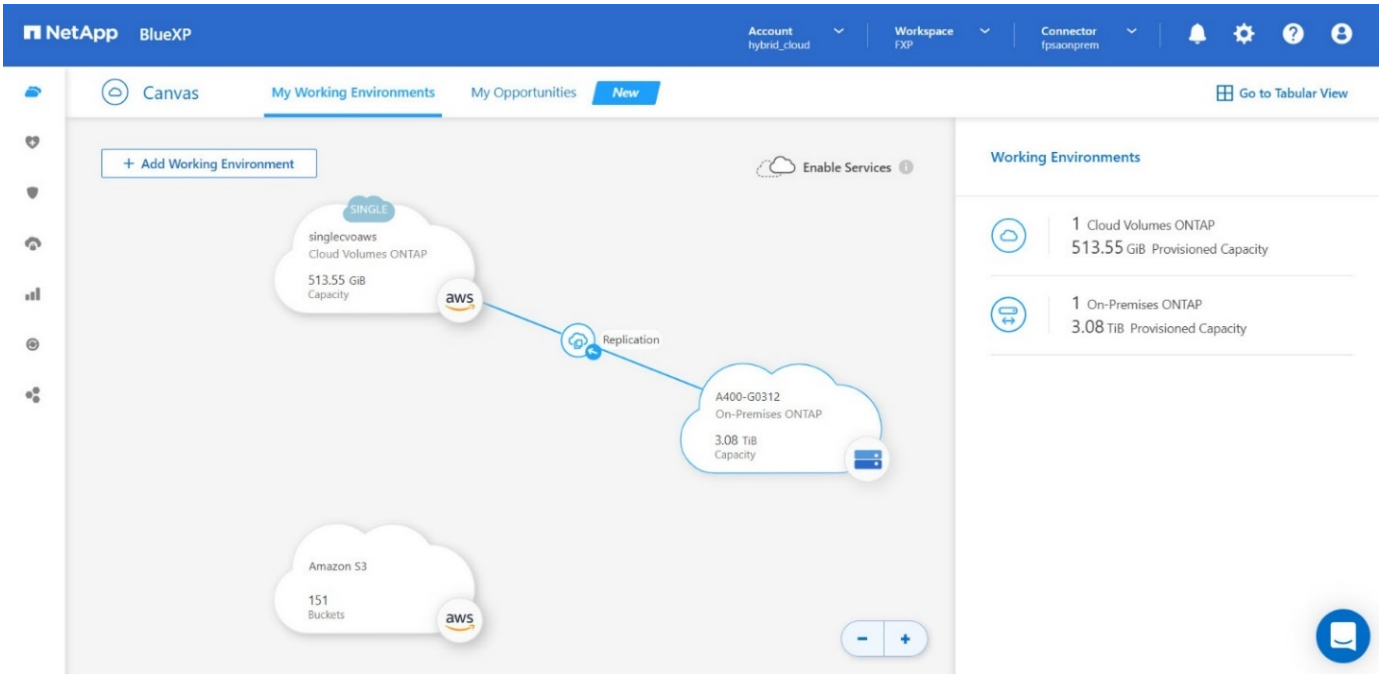


10. **Revoir.** revoir vos sélections et cliquer sur **aller**.

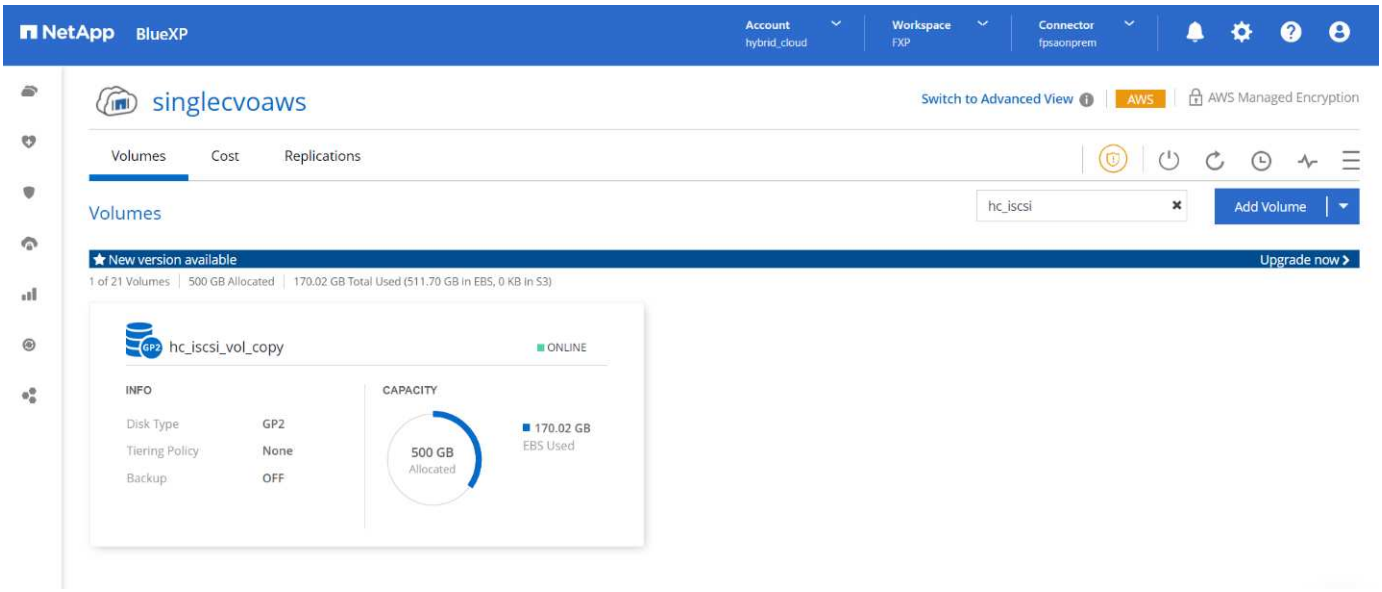


Pour plus d'informations sur ces étapes de configuration, reportez-vous à la section "ici".

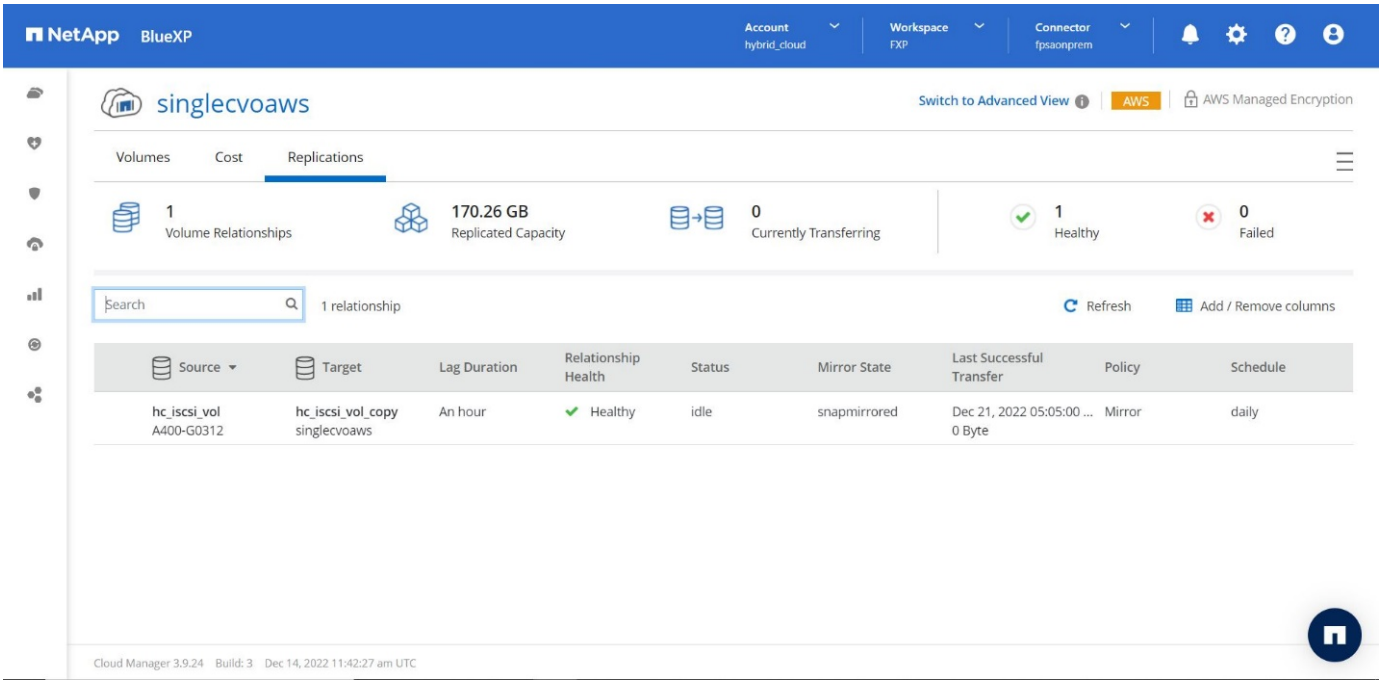
BlueXP démarre le processus de réplication des données. Maintenant, vous pouvez voir le service **Replication** qui a été établi entre votre système ONTAP sur site et Cloud Volumes ONTAP.



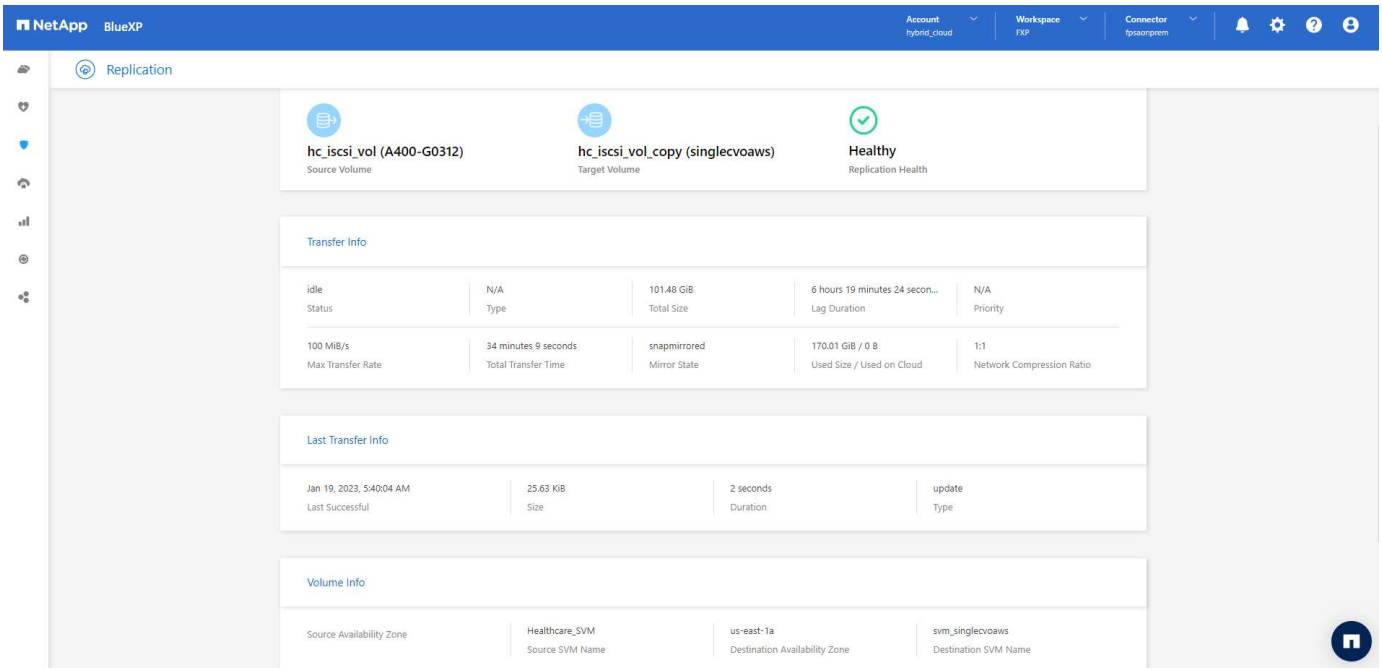
Dans le cluster Cloud Volumes ONTAP, vous pouvez afficher le volume qui vient d'être créé.



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.

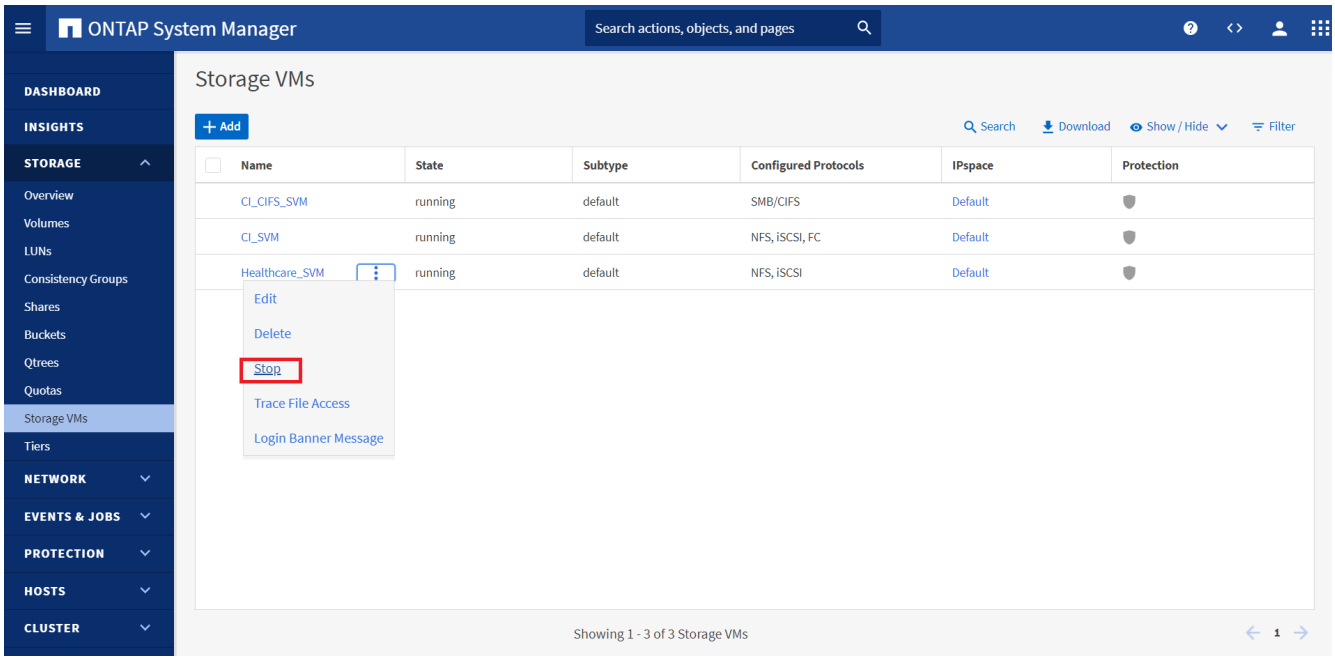
Reprise après incident

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.

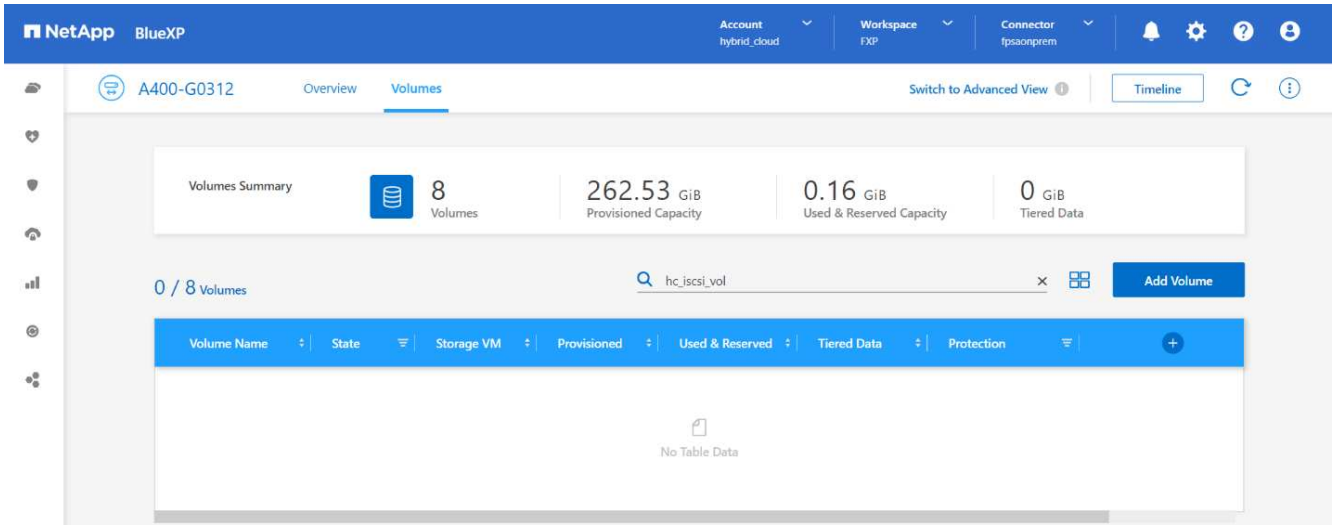
Pour effectuer la validation d'un scénario DR réussi, procédez comme suit :

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



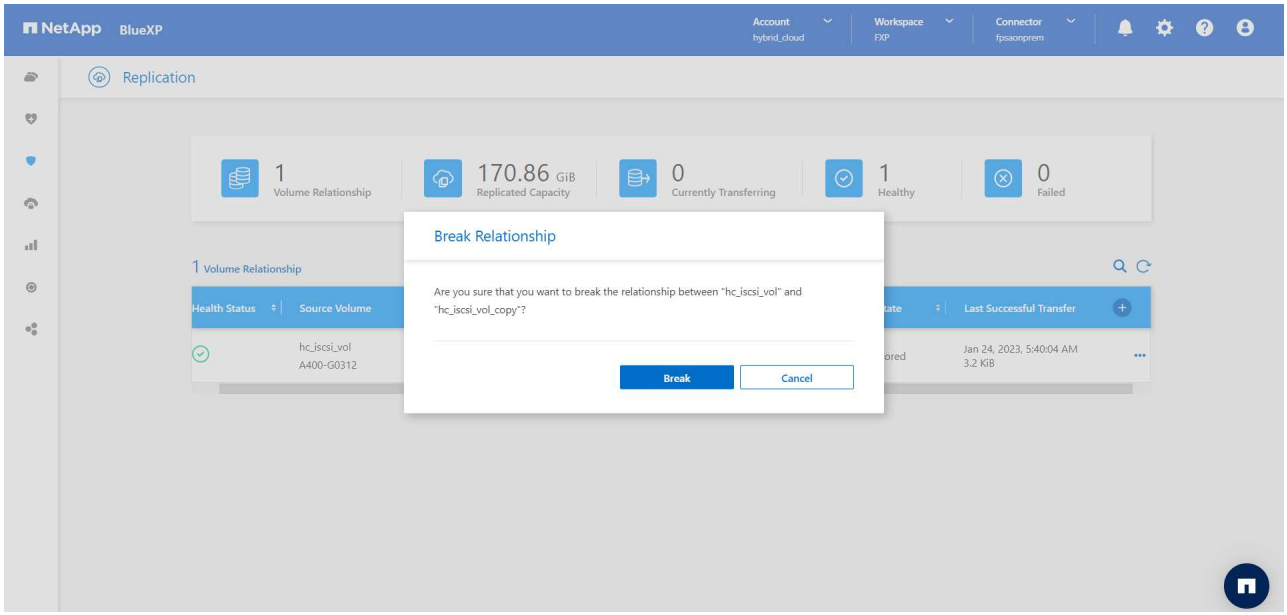
Assurez-vous que la réplication SnapMirror est déjà configurée entre l'ONTAP sur site dans l'instance FlexPod et Cloud Volumes ONTAP dans AWS, afin de pouvoir créer fréquemment des copies Snapshot d'application.

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
```

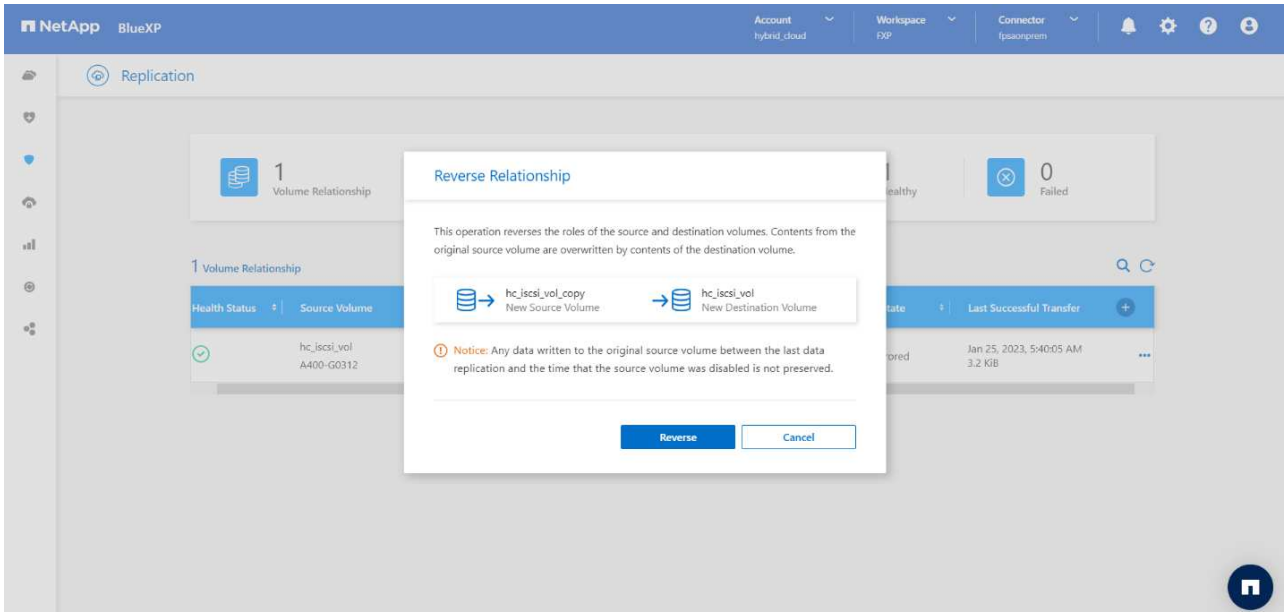
e. Enfin, montez le système de fichiers et affichez les informations sur le système de fichiers.

```
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
```

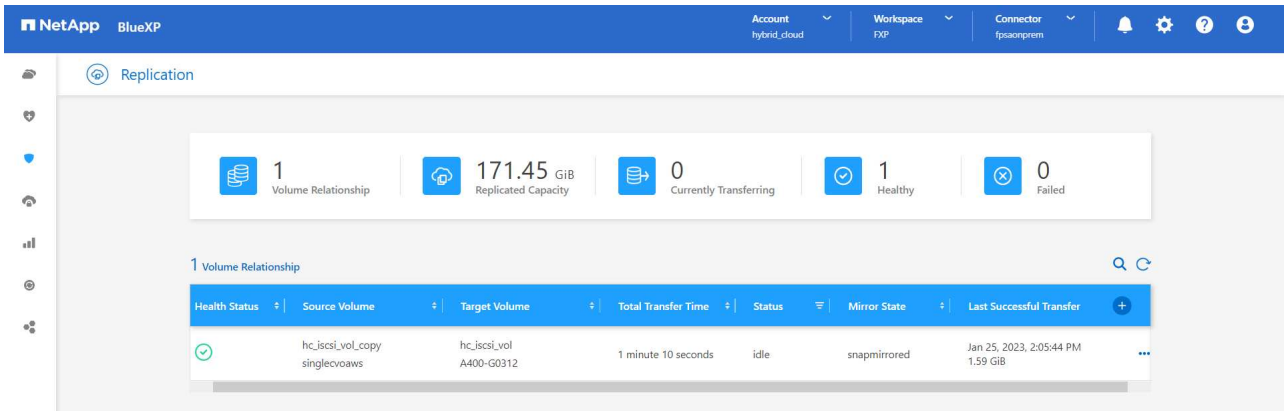
Ce résultat indique que les utilisateurs peuvent accéder aux données répliquées sur le réseau jusqu'à ce que le site de production soit récupéré après sinistre.

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.

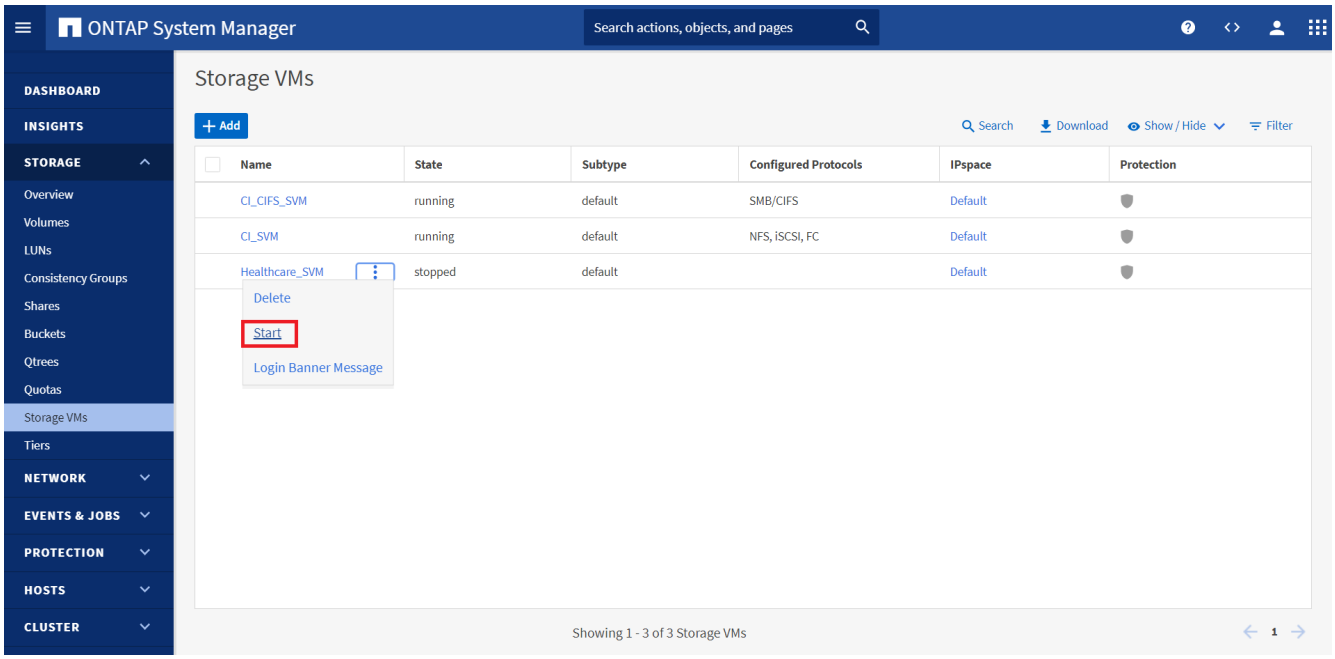
Vérification des données sur le site de production

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.

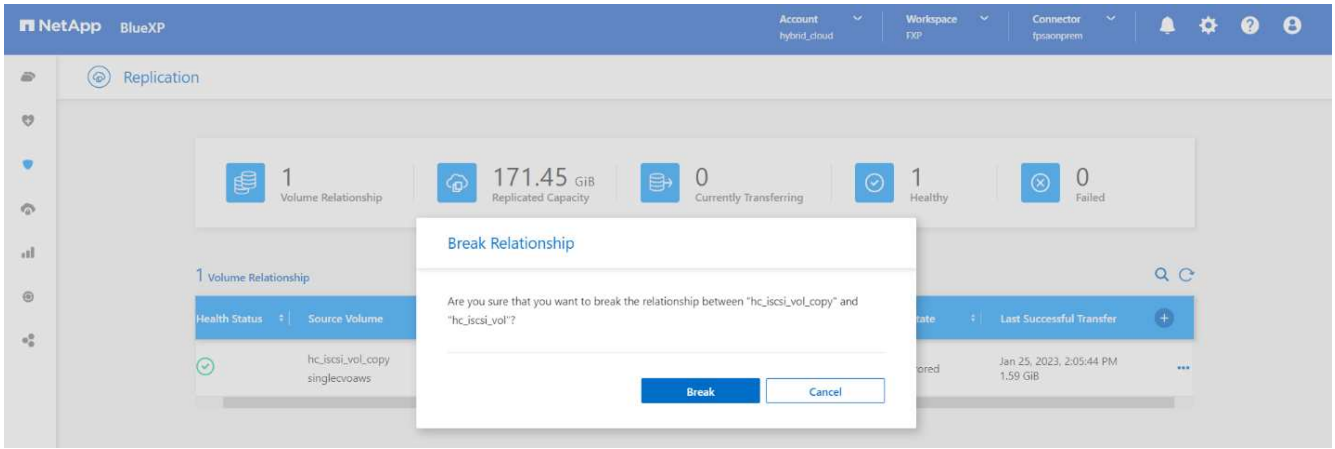
Dans cette section, nous abordons l'accès au site source et la restauration de la relation SnapMirror entre ONTAP sur site et Cloud Volumes ONTAP, puis nous avons enfin effectué un contrôle d'intégrité des données à l'extrémité source

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`).



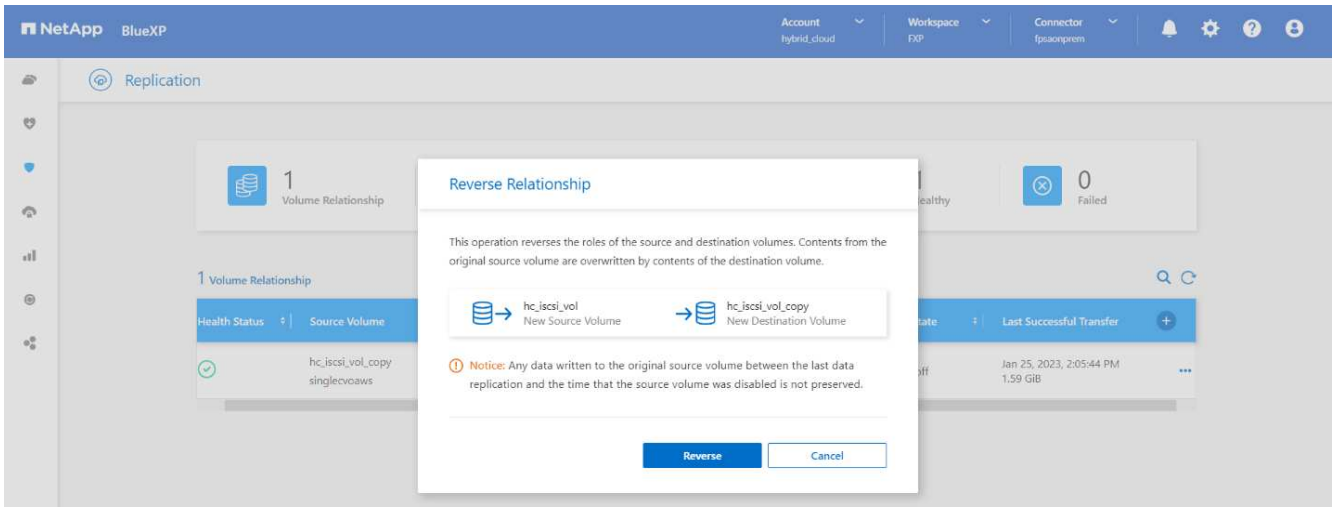
2. Rompre la relation de réplication SnapMirror entre Cloud Volumes ONTAP et ONTAP sur site et promouvoir le volume sur site (`hc_iscsi_vol`) de retour à la production.



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.

```
[root@hc-cloud-secure-1 ~]# mount -t xfs /dev/datavg/datalv /file1
[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  kamini
dir02  dir06  dir10  dir14  dir18  dir22  dir26  dir30  dir34  dir38  dir42  dir46  dir50  dir54  dir58  dir62  dir66  dir70  dir74  dir78  latest_file
dir03  dir07  dir11  dir15  dir19  dir23  dir27  dir31  dir35  dir39  dir43  dir47  dir51  dir55  dir59  dir63  dir67  dir71  dir75  dir79  newfile
dir04  dir08  dir12  dir16  dir20  dir24  dir28  dir32  dir36  dir40  dir44  dir48  dir52  dir56  dir60  dir64  dir68  dir72  dir76  dir80
```

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