



Reprise d'activité BlueXP

NetApp Solutions

NetApp
August 20, 2024

Sommaire

- Reprise d'activité BlueXP 1
 - 3-2-1 protection des données pour VMware avec le plug-in SnapCenter et sauvegarde et restauration
- BlueXP pour les VM 1
- Reprise après incident à l'aide de la DRaaS BlueXP 47

Reprise d'activité BlueXP

3-2-1 protection des données pour VMware avec le plug-in SnapCenter et sauvegarde et restauration BlueXP pour les VM

La stratégie de sauvegarde 3-2-1 est une méthode de protection des données reconnue par le secteur et offre une approche complète pour la sauvegarde des données précieuses. Cette stratégie est fiable et garantit que même en cas de sinistre inattendu, une copie des données sera toujours disponible.

Auteur : Josh Powell - Ingénierie de solutions NetApp

Présentation

La stratégie comprend trois règles fondamentales :

1. Conservez au moins trois copies de vos données. Ainsi, même en cas de perte ou de corruption d'une copie, vous avez toujours au moins deux copies restantes à remettre en marche.
2. Stockez deux copies de sauvegarde sur différents supports ou périphériques de stockage. La diversification des supports de stockage permet d'offrir une protection contre les défaillances spécifiques aux périphériques ou aux supports. Si un périphérique est endommagé ou si un type de support échoue, l'autre copie de sauvegarde n'est pas affectée.
3. Enfin, assurez-vous qu'au moins une copie de sauvegarde est hors site. Le stockage hors site sert de protection contre les incidents localisés tels que des incendies ou des inondations qui pourraient rendre les copies sur site inutilisables.

Ce document présente une solution de sauvegarde 3-2-1 avec le plug-in SnapCenter pour VMware vSphere (SCV) pour créer des sauvegardes primaires et secondaires de nos machines virtuelles sur site, et BlueXP pour la sauvegarde et la restauration des machines virtuelles afin de sauvegarder une copie de nos données dans le stockage cloud ou dans StorageGRID.





Cas d'utilisation

Cette solution répond aux cas d'utilisation suivants :

- Sauvegarde et restauration de machines virtuelles et de datastores sur site à l'aide du plug-in SnapCenter pour VMware vSphere.
- Sauvegarde et restauration de machines virtuelles et de datastores sur site, hébergés sur des clusters ONTAP, et sauvegarde sur un stockage objet à l'aide de la sauvegarde et de la restauration BlueXP pour les machines virtuelles.

Stockage des données NetApp ONTAP

ONTAP est la solution de stockage de pointe de NetApp qui offre un stockage unifié, quel que soit le protocole utilisé : SAN ou NAS. Grâce à la stratégie de sauvegarde 3-2-1, les données sur site sont protégées sur plusieurs types de supports, et NetApp propose des plateformes allant du Flash haut débit aux supports moins coûteux.

FAS	AFF C-Series	AFF A-Series	ASA A-Series
			
Hybrid flash storage	Capacity all-flash storage	Performance all-flash storage	All-flash SAN storage
Unified (file, block, object)	Unified (file, block, object)	Unified (file, block, object)	Block optimized
Lowest price storage	Balanced price storage	Premium priced storage	Aggressively priced storage
Tier 2 @ 5-10ms latency Backup / Low-cost DR	Refresh of hybrid flash, Tier 1 @ 2-4ms latency Tier 2 workloads VMware datastores	Ideal for Tier 1 business-critical workloads with <1ms latency	Ideal for Tier 1 Block Six Nines Guaranteed

Pour en savoir plus sur la plateforme matérielle NetApp, consultez la page "[Stockage des données NetApp](#)".

Plug-in SnapCenter pour VMware vSphere

Le plug-in SnapCenter pour VMware vSphere est une offre de protection des données étroitement intégrée à VMware vSphere qui facilite la gestion des sauvegardes et des restaurations des machines virtuelles. Dans le cadre de cette solution, SnapMirror offre une méthode rapide et fiable pour créer une seconde copie de sauvegarde immuable des données du serveur virtuel sur un cluster de stockage ONTAP secondaire. Une fois cette architecture en place, les opérations de restauration des machines virtuelles peuvent facilement être lancées à partir des emplacements de sauvegarde principaux ou secondaires.

SCV est déployé en tant qu'appliance virtuelle linux à l'aide d'un fichier OVA. Le plug-in utilise désormais un plug-in distant architecture. Le plug-in distant s'exécute en dehors du serveur vCenter et est hébergé sur l'appliance virtuelle SCV.

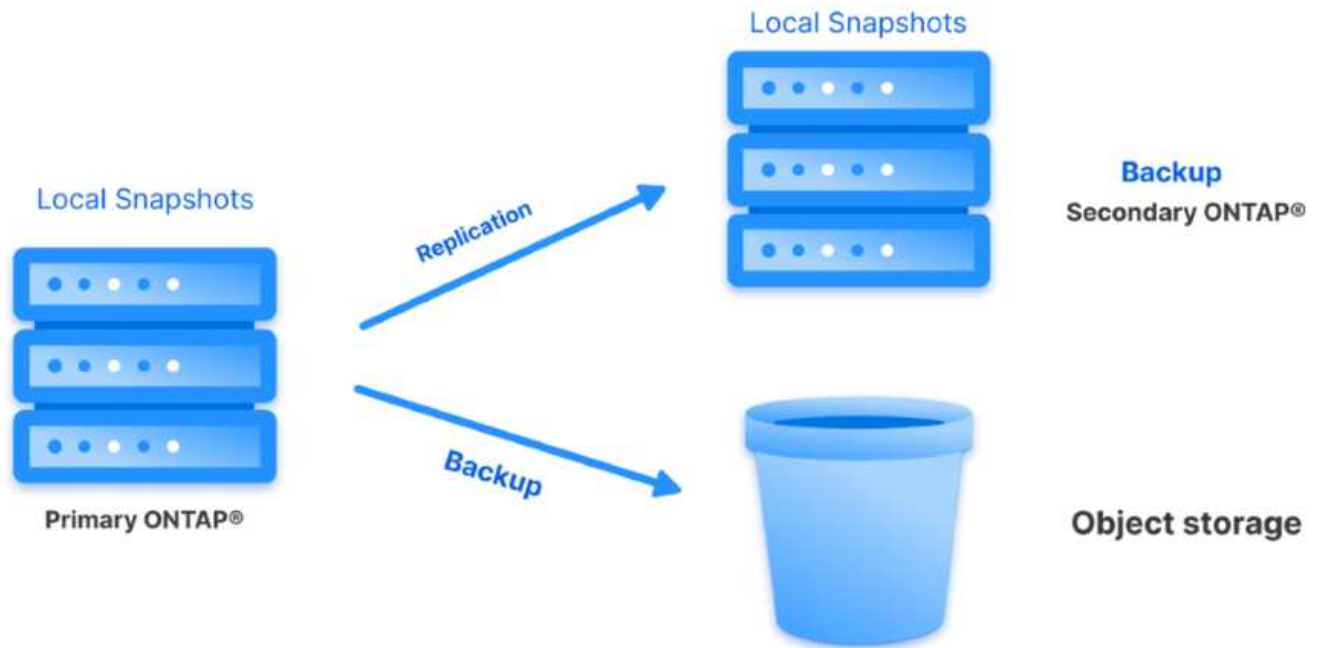
Pour plus d'informations sur le distributeur auxiliaire, se reporter à "[Documentation du plug-in SnapCenter pour VMware vSphere](#)".

Sauvegarde et restauration BlueXP pour les machines virtuelles

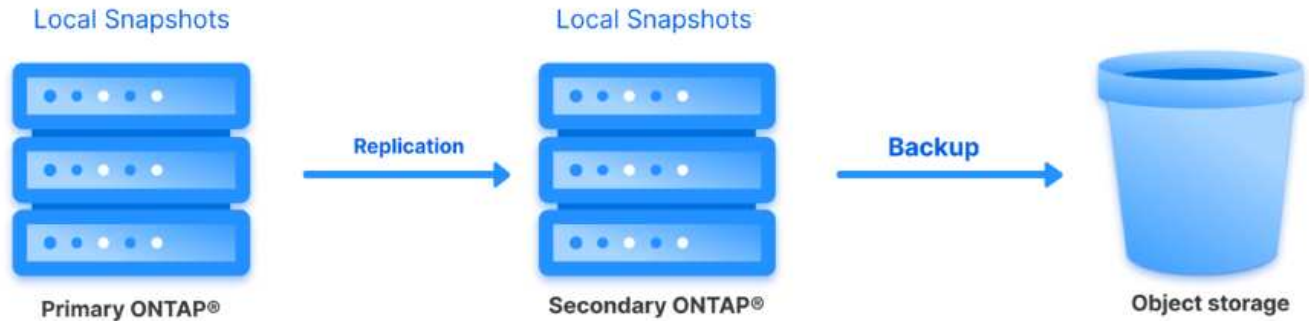
BlueXP Backup and Recovery est un outil cloud de gestion des données qui offre un plan de contrôle unique pour un large éventail d'opérations de sauvegarde et de restauration dans les environnements sur site et cloud. Une fonctionnalité de la suite de sauvegarde et de restauration NetApp BlueXP s'intègre avec le plug-in SnapCenter pour VMware vSphere (sur site) pour étendre une copie des données au stockage objet dans le cloud. Cela établit une troisième copie des données hors site, qui provient des sauvegardes de stockage primaire ou secondaire. Avec la sauvegarde et la restauration BlueXP, il est facile de définir des règles de stockage qui transfèrent des copies de vos données à partir de l'un de ces deux emplacements sur site.

En choisissant entre les sauvegardes primaires et secondaires comme source dans BlueXP Backup and Recovery, vous implémentez l'une des deux topologies suivantes :

Topologie « Fan-Out » – lorsqu'une sauvegarde est lancée par le plug-in SnapCenter pour VMware vSphere, un snapshot local est immédiatement pris. SCV lance ensuite une opération SnapMirror qui réplique l'instantané le plus récent sur le cluster ONTAP secondaire. Dans BlueXP Backup and Recovery, une règle spécifie le cluster ONTAP principal comme source d'une copie Snapshot des données à transférer vers le stockage objet dans le fournisseur cloud de votre choix.



Topologie en cascade – la création de copies de données primaires et secondaires à l'aide de SCV est identique à la topologie de sortie mentionnée ci-dessus. Cependant, cette fois-ci, une règle est créée dans BlueXP Backup and Recovery en spécifiant que la sauvegarde vers le stockage objet va provenir du cluster ONTAP secondaire.



La sauvegarde et la restauration BlueXP permettent de créer des copies de sauvegarde des copies ONTAP sur site vers AWS Glacier, Azure Blob et le stockage d'archives GCP.



AWS Glacier and Deep Glacier **Azure Blob Archive** **GCP Archive Storage**

En outre, vous pouvez utiliser NetApp StorageGRID comme cible de sauvegarde du stockage objet. Pour plus d'informations sur StorageGRID, reportez-vous au "[Page d'accueil StorageGRID](#)".

Présentation du déploiement de la solution

Cette liste répertorie les étapes générales nécessaires à la configuration de cette solution et à l'exécution des opérations de sauvegarde et de restauration à partir des sauvegardes et restaurations SCV et BlueXP :

1. Configurez la relation SnapMirror entre les clusters ONTAP à utiliser pour les copies de données primaires et secondaires.
2. Configuration du plug-in SnapCenter pour VMware vSphere
 - a. Ajouter des systèmes de stockage
 - b. Création de règles de sauvegarde
 - c. Créer des groupes de ressources
 - d. Exécutez d'abord les tâches de sauvegarde
3. Configurer la sauvegarde et la restauration BlueXP pour les machines virtuelles
 - a. Ajouter un environnement de travail
 - b. Découvrez les appliances SCV et vCenter
 - c. Création de règles de sauvegarde
 - d. Activer les sauvegardes
4. Restaurer les machines virtuelles à partir du stockage primaire et secondaire à l'aide de SCV.
5. Restaurez les machines virtuelles à partir du stockage objet à l'aide de la sauvegarde et de la restauration BlueXP.

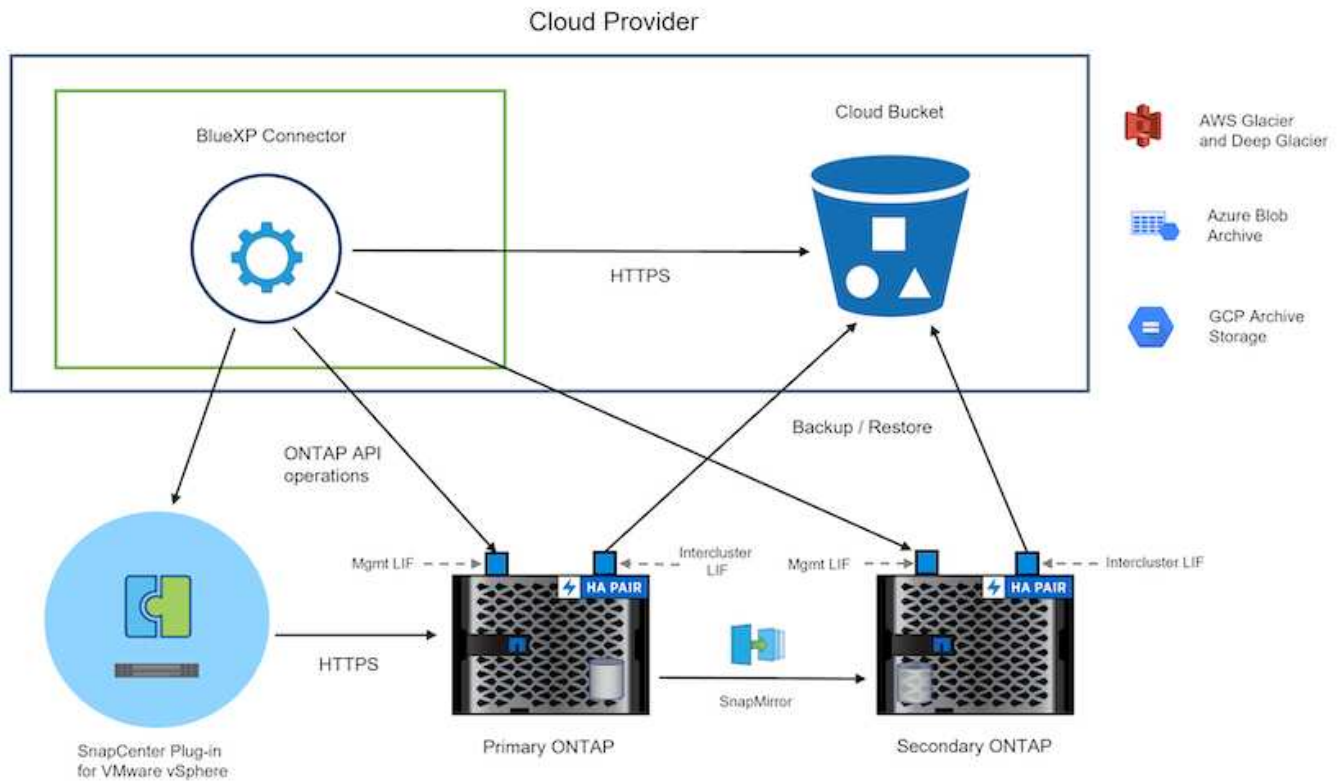
Prérequis

L'objectif de cette solution est de démontrer la protection des données des serveurs virtuels s'exécutant dans VMware vSphere et situés sur des datastores NFS hébergés par NetApp ONTAP. Cette solution suppose que les composants suivants sont configurés et prêts à l'emploi :

1. Cluster de stockage ONTAP avec datastores NFS ou VMFS connectés à VMware vSphere. Les datastores NFS et VMFS sont pris en charge. Des datastores NFS ont été utilisés pour cette solution.
2. Cluster de stockage ONTAP secondaire avec relations SnapMirror établies pour les volumes utilisés pour les datastores NFS.
3. BlueXP Connector installé pour le fournisseur cloud utilisé pour les sauvegardes de stockage objet.
4. Les machines virtuelles à sauvegarder se trouvent sur des datastores NFS résidant sur le cluster de stockage ONTAP principal.
5. Connectivité réseau entre le connecteur BlueXP et les interfaces de gestion des clusters de stockage ONTAP sur site.
6. Connectivité réseau entre le connecteur BlueXP et la machine virtuelle de l'appliance SCV sur site, et entre le connecteur BlueXP et vCenter.
7. Connectivité réseau entre les LIFs intercluster ONTAP sur site et le service de stockage objet.
8. DNS configuré pour la gestion des SVM sur les clusters de stockage ONTAP principal et secondaire. Pour plus d'informations, reportez-vous à la section "[Configurez le DNS pour la résolution du nom d'hôte](#)".

Architecture de haut niveau

Le test/validation de cette solution a été effectué dans un laboratoire qui peut correspondre ou non à l'environnement de déploiement final.



Déploiement de la solution

Dans cette solution, nous fournissons des instructions détaillées pour le déploiement et la validation d'une solution qui utilise le plug-in SnapCenter pour VMware vSphere, ainsi que la sauvegarde et la restauration BlueXP, pour effectuer la sauvegarde et la restauration de machines virtuelles Windows et Linux dans un cluster VMware vSphere situé dans un data Center sur site. Les machines virtuelles de cette configuration sont stockées dans des datastores NFS hébergés par un cluster de stockage ONTAP A300. En outre, un cluster de stockage ONTAP A300 distinct sert de destination secondaire pour les volumes répliqués à l'aide de SnapMirror. En outre, le stockage objet hébergé sur Amazon Web Services et Azure Blob ont été utilisés comme cibles pour la troisième copie des données.

Nous allons poursuivre la création de relations SnapMirror pour les copies secondaires de nos sauvegardes gérées par SCV et la configuration des tâches de sauvegarde dans les sauvegardes et les restaurations de SCV et BlueXP.

Pour plus d'informations sur le plug-in SnapCenter pour VMware vSphere, reportez-vous au "[Documentation du plug-in SnapCenter pour VMware vSphere](#)".

Pour plus d'informations sur la sauvegarde et la restauration BlueXP, reportez-vous au "[Documentation sur la sauvegarde et la restauration BlueXP](#)".

Établissement de relations SnapMirror entre clusters ONTAP

Le plug-in SnapCenter pour VMware vSphere utilise la technologie ONTAP SnapMirror pour gérer le transport des copies SnapMirror et/ou SnapVault secondaires vers un cluster ONTAP secondaire.

Les règles de sauvegarde des distributeurs sélectifs ont la possibilité d'utiliser les relations SnapMirror ou SnapVault. La principale différence est que lorsque vous utilisez l'option SnapMirror, le planning de conservation configuré pour les sauvegardes dans la règle sera le même sur les sites principal et secondaire. SnapVault est conçu pour l'archivage et si cette option permet d'établir une planification de conservation

distincte avec la relation SnapMirror pour les copies Snapshot sur le cluster de stockage ONTAP secondaire.

La configuration des relations SnapMirror peut être effectuée dans BlueXP où de nombreuses étapes sont automatisées ou via System Manager et l'interface de ligne de commande ONTAP. Toutes ces méthodes sont présentées ci-dessous.

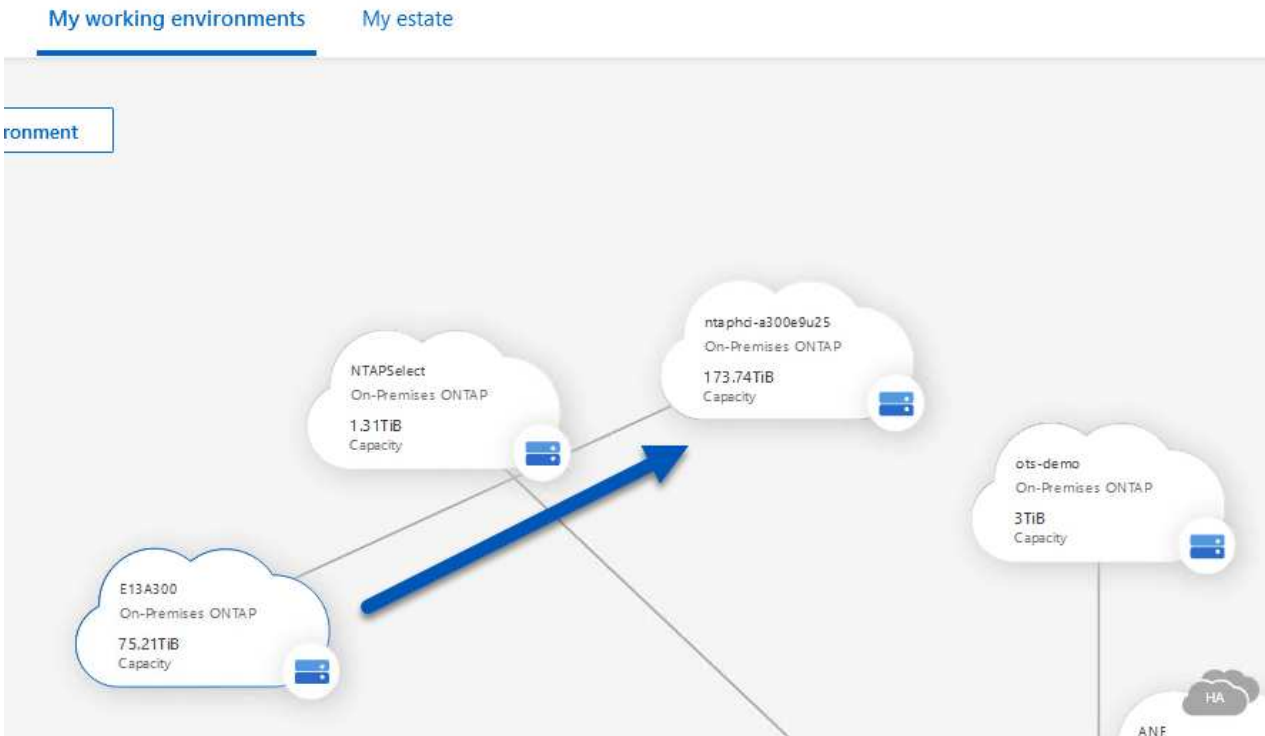
Établissez des relations SnapMirror avec BlueXP

Les étapes suivantes doivent être effectuées à partir de la console Web BlueXP :

Configuration de la réplication pour les systèmes de stockage ONTAP principaux et secondaires

Commencez par vous connecter à la console Web BlueXP et naviguer jusqu'au Canvas.

1. Glissez-déposez le système de stockage ONTAP source (principal) sur le système de stockage ONTAP de destination (secondaire).



2. Dans le menu qui s'affiche, sélectionnez **Replication**.



3. Sur la page **destination peering Setup**, sélectionnez les LIFs intercluster de destination à utiliser pour la connexion entre systèmes de stockage.

Select the destination LIFs you would like to use for cluster peering setup.
Replication requires an initial connection between the two working environments which is called a cluster peer relationship.
For more information about LIF selections, see Cloud Manager documentation.

<input type="checkbox"/> CVO_InterCluster_B ntaphci-a300-02 : a0a-3510 172.21.254.212/24 up	<input type="checkbox"/> CVO_InterCluster_A ntaphci-a300-01 : a0a-3510 172.21.254.211/24 up	<input type="checkbox"/> zoneb-n1 ntaphci-a300-01 : a0a-3484 172.21.228.21/24 up	<input type="checkbox"/> zoneb-n2 ntaphci-a300-02 : a0a-3484 172.21.228.22/24 up	<input checked="" type="checkbox"/> intercluster_node_1 ntaphci-a300-01 : a0a-181 10.61.181.193/24 up	<input checked="" type="checkbox"/> intercluster_node_2 ntaphci-a300-01 : a0a-181 10.61.181.194/24 up
--	--	---	---	---	---

4. Sur la page **destination Volume Name**, sélectionner d'abord le volume source, puis remplir le nom du volume de destination et sélectionner le SVM et l'agrégat de destination. Cliquez sur **Suivant** pour continuer.

Select the volume that you want to replicate

E13A300

288 Volumes

<p>CDM01 ONLINE</p> <p>INFO</p> <table> <tr><td>Storage VM Name</td><td>FS02</td></tr> <tr><td>Tiering Policy</td><td>None</td></tr> <tr><td>Volume Type</td><td>RW</td></tr> </table> <p>CAPACITY</p> <p>206 GB Allocated</p> <p>53.72 MB Disk Used</p>	Storage VM Name	FS02	Tiering Policy	None	Volume Type	RW	<p>Data ONLINE</p> <p>INFO</p> <table> <tr><td>Storage VM Name</td><td>FS02</td></tr> <tr><td>Tiering Policy</td><td>None</td></tr> <tr><td>Volume Type</td><td>RW</td></tr> </table> <p>CAPACITY</p> <p>512 GB Allocated</p> <p>0 GB Disk Used</p>	Storage VM Name	FS02	Tiering Policy	None	Volume Type	RW
Storage VM Name	FS02												
Tiering Policy	None												
Volume Type	RW												
Storage VM Name	FS02												
Tiering Policy	None												
Volume Type	RW												
<p>Demo ONLINE</p> <p>INFO</p> <table> <tr><td>Storage VM Name</td><td>zonea</td></tr> <tr><td>Tiering Policy</td><td>None</td></tr> <tr><td>Volume Type</td><td>RW</td></tr> </table> <p>CAPACITY</p> <p>250 GB Allocated</p> <p>1.79 GB Disk Used</p>	Storage VM Name	zonea	Tiering Policy	None	Volume Type	RW	<p>Demo02_01 ONLINE</p> <p>INFO</p> <table> <tr><td>Storage VM Name</td><td>Demo</td></tr> <tr><td>Tiering Policy</td><td>None</td></tr> <tr><td>Volume Type</td><td>RW</td></tr> </table> <p>CAPACITY</p> <p>500 GB Allocated</p> <p>34.75 MB Disk Used</p>	Storage VM Name	Demo	Tiering Policy	None	Volume Type	RW
Storage VM Name	zonea												
Tiering Policy	None												
Volume Type	RW												
Storage VM Name	Demo												
Tiering Policy	None												
Volume Type	RW												

Destination Volume Name

Destination Volume Name

Demo_copy

Destination Storage VM

EHC_NFS

Destination Aggregate

EHCaggr01

5. Choisissez le taux de transfert maximal pour la réplication.

Max Transfer Rate

You should limit the transfer rate. An unlimited rate might negatively impact the performance of other applications and it might impact your Internet performance.

- Limited to: MB/s
- Unlimited (recommended for DR only machines)

6. Choisissez la règle qui déterminera le calendrier de conservation des sauvegardes secondaires. Cette stratégie peut être créée au préalable (voir le processus manuel ci-dessous dans l'étape **Créer une stratégie de rétention d'instantanés**) ou peut être modifiée après le fait si vous le souhaitez.

Replication Setup
Replication Policy

↑ Previous Step

Default Policies
Additional Policies

CloudBackupService-1674046623282

Original Policy Name: CloudBackupService-1674046623282

Creates a SnapVault relationship which replicates Snapshot copies with the following labels to the destination volume: hourly (12), daily (15), weekly (6) (# of retained Snapshot copies in parenthesis)

CloudBackupService-1674047424679

Custom Policy - No Comment

[More info](#)

CloudBackupService-1674047718637

Custom Policy - No Comment

[More info](#)

7. Enfin, passez en revue toutes les informations et cliquez sur le bouton **Go pour lancer le processus de configuration de la réplication.**


Replication Setup
Review & Approve

↑ Previous Step


Review your selection and start the replication process

Source Volume Allocated Size:	250 GB	Destination Aggregate:	EHCAGgr01
Source Volume Used Size:	1.79 GB	Destination Storage VM:	EHC_NFS
Source Thin Provisioning:	Yes	Max Transfer Rate:	100 MB/s
Destination Volume Allocated Size:	250 GB	SnapMirror Policy:	Mirror
Destination Thin Provisioning:	No	Replication Schedule:	One-time copy

Source




E13A300




Demo

Destination



ntaphci-a300e9u25



Demo_copy

→

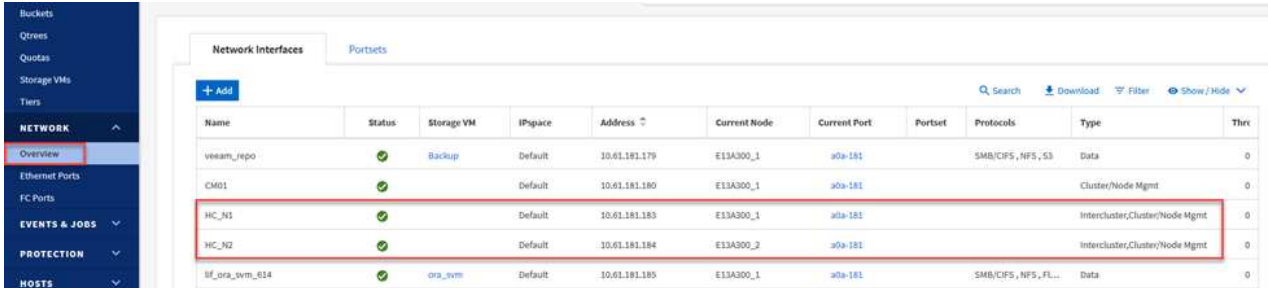
Établissez des relations SnapMirror avec System Manager et l'interface de ligne de commandes de ONTAP

Toutes les étapes requises pour établir des relations SnapMirror peuvent être effectuées à l'aide de System Manager ou de l'interface de ligne de commandes de ONTAP. La section suivante fournit des informations détaillées sur les deux méthodes :

Enregistrer les interfaces logiques intercluster source et destination

Pour les clusters ONTAP source et destination, vous pouvez récupérer les informations relatives aux LIF intercluster à partir de System Manager ou de l'interface de ligne de commandes.

1. Dans ONTAP System Manager, accédez à la page Network Overview et récupérez les adresses IP de type intercluster configurées pour communiquer avec le VPC AWS où FSX est installé.



Name	Status	Storage VM	IPspace	Address	Current Node	Current Port	Portset	Protocols	Type	Thru
veeam_repo	✓	Backup	Default	10.01.181.179	E13A300_1	a0a-181		SMB/CIFS, NFS, S3	Data	0
CM01	✓		Default	10.01.181.180	E13A300_1	a0a-181			Cluster/Node Mgmt	0
HC_N1	✓		Default	10.01.181.183	E13A300_1	a0a-181			Intercluster,Cluster/Node Mgmt	0
HC_N2	✓		Default	10.01.181.184	E13A300_2	a0a-181			Intercluster,Cluster/Node Mgmt	0
lif_ora_vvm_014	✓	ora_vvm	Default	10.01.181.185	E13A300_1	a0a-181		SMB/CIFS, NFS, FL...	Data	0

2. Pour récupérer les adresses IP intercluster à l'aide de l'interface de ligne de commandes, exécutez la commande suivante :

```
ONTAP-Dest::> network interface show -role intercluster
```

Établissement du peering de cluster entre clusters ONTAP

Pour établir le peering de cluster entre clusters ONTAP, une phrase secrète unique saisie au niveau du cluster ONTAP à l'origine doit être confirmée dans l'autre cluster.

1. Configurez le peering sur le cluster ONTAP de destination à l'aide du `cluster peer create` commande. Lorsque vous y êtes invité, saisissez une phrase secrète unique utilisée ultérieurement sur le cluster source pour finaliser le processus de création.

```
ONTAP-Dest::> cluster peer create -address-family ipv4 -peer-addr  
source_intercluster_1, source_intercluster_2  
Enter the passphrase:  
Confirm the passphrase:
```

2. Sur le cluster source, vous pouvez établir la relation de pairs de cluster à l'aide de ONTAP System Manager ou de l'interface de ligne de commandes. Dans ONTAP System Manager, accédez à `protection > Présentation` et sélectionnez `Peer Cluster`.



DASHBOARD

STORAGE

Overview

Volumes

LUNs

Consistency Groups

NVMe Namespaces

Shares

Buckets

Qtrees

Quotas

Storage VMs

Tiers

NETWORK

Overview

Ethernet Ports

FC Ports

EVENTS & JOBS

PROTECTION

Overview

Relationships

HOSTS

Overview

< Intercluster Settings

Network Interfaces

IP ADDRESS

- ✓ 10.61.181.184
- ✓ 172.21.146.217
- ✓ 10.61.181.183
- ✓ 172.21.146.216

Cluster Peers

PEERED CLUSTER NAME

- ✓ FsxId0ae40e08acc0dea67
- ✓ OTS02

Mediator ⓘ

Not configured.

Configure

Storage VM Peers

PEERED STORAGE VMS

- ✓ 3

3. Dans la boîte de dialogue Peer Cluster, saisissez les informations requises :
 - a. Entrez la phrase secrète utilisée pour établir la relation entre clusters sur le cluster ONTAP de destination.

- b. Sélectionnez **Yes** pour établir une relation chiffrée.
- c. Entrer les adresses IP du LIF intercluster du cluster ONTAP destination.
- d. Cliquez sur **initier le peering de cluster** pour finaliser le processus.

4. Vérifiez l'état de la relation entre clusters depuis le cluster ONTAP de destination à l'aide de la commande suivante :

```
ONTAP-Dest::> cluster peer show
```

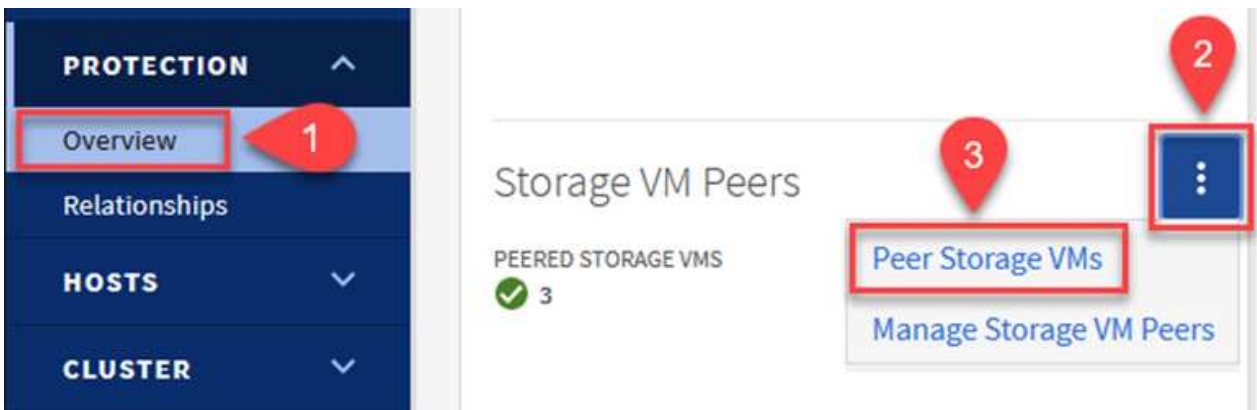
Établir une relation de peering de SVM

L'étape suivante consiste à configurer une relation de SVM entre les machines virtuelles de stockage de destination et source qui contiennent les volumes qui seront dans les relations SnapMirror.

1. Depuis le cluster ONTAP de destination, utiliser la commande suivante depuis l'interface de ligne de commandes pour créer la relation SVM peer :

```
ONTAP-Dest::> vserver peer create -vserver DestSVM -peer-vserver Backup -peer-cluster OnPremSourceSVM -applications snapmirror
```

2. Depuis le cluster ONTAP source, acceptez la relation de peering avec ONTAP System Manager ou l'interface de ligne de commandes.
3. Dans ONTAP System Manager, accédez à protection > Présentation et sélectionnez des VM de stockage homologues sous les pairs de machines virtuelles de stockage.



4. Dans la boîte de dialogue de la VM de stockage homologue, remplissez les champs requis :
 - La VM de stockage source
 - Cluster destination
 - L'VM de stockage de destination



5. Cliquez sur Peer Storage VM pour terminer le processus de peering de SVM.

Création d'une règle de conservation des snapshots

SnapCenter gère les planifications de conservation pour les sauvegardes qui existent sous forme de copies Snapshot sur le système de stockage primaire. Ceci est établi lors de la création d'une règle dans SnapCenter. SnapCenter ne gère pas de stratégies de conservation pour les sauvegardes conservées sur des systèmes de stockage secondaires. Ces règles sont gérées séparément via une règle SnapMirror créée sur le cluster FSX secondaire et associée aux volumes de destination faisant partie d'une relation SnapMirror avec le volume source.

Lors de la création d'une règle SnapCenter, vous avez la possibilité de spécifier une étiquette de règle secondaire ajoutée au label SnapMirror de chaque Snapshot généré lors de la création d'une sauvegarde SnapCenter.



Sur le stockage secondaire, ces étiquettes sont mises en correspondance avec les règles de règle associées au volume de destination pour assurer la conservation des snapshots.

L'exemple suivant montre une étiquette SnapMirror présente sur tous les snapshots générés dans le cadre d'une règle utilisée pour les sauvegardes quotidiennes de notre base de données SQL Server et des volumes des journaux.

Select secondary replication options

Update SnapMirror after creating a local Snapshot copy.

Update SnapVault after creating a local Snapshot copy.

Secondary policy label

sql-daily

Error retry count

Pour plus d'informations sur la création de stratégies SnapCenter pour une base de données SQL Server, reportez-vous au "[Documentation SnapCenter](#)".

Vous devez d'abord créer une règle SnapMirror avec des règles qui imposent le nombre de copies Snapshot à conserver.

1. Création de la règle SnapMirror sur le cluster FSX

```
ONTAP-Dest::> snapmirror policy create -vserver DestSVM -policy  
PolicyName -type mirror-vault -restart always
```

2. Ajoutez des règles à la règle avec des étiquettes SnapMirror qui correspondent aux étiquettes de règles secondaires spécifiées dans les règles de SnapCenter.

```
ONTAP-Dest::> snapmirror policy add-rule -vserver DestSVM -policy  
PolicyName -snapmirror-label SnapMirrorLabelName -keep  
#ofSnapshotsToRetain
```

Le script suivant fournit un exemple de règle qui peut être ajoutée à une règle :

```
ONTAP-Dest::> snapmirror policy add-rule -vserver sql_svm_dest  
-policy Async_SnapCenter_SQL -snapmirror-label sql-ondemand -keep 15
```



Créer des règles supplémentaires pour chaque étiquette SnapMirror et le nombre de snapshots à conserver (période de conservation).

Créer des volumes de destination

Pour créer sur ONTAP un volume de destination qui sera destinataire des copies Snapshot de nos volumes source, exécutez la commande suivante sur le cluster ONTAP de destination :

```
ONTAP-Dest::> volume create -vserver DestSVM -volume DestVolName  
-aggregate DestAggrName -size VolSize -type DP
```

Création des relations SnapMirror entre les volumes source et de destination

Pour créer une relation SnapMirror entre un volume source et un volume de destination, exécutez la commande suivante sur le cluster ONTAP de destination :

```
ONTAP-Dest::> snapmirror create -source-path  
OnPremSourceSVM:OnPremSourceVol -destination-path DestSVM:DestVol -type  
XDP -policy PolicyName
```

Initialiser les relations SnapMirror

Initialiser la relation SnapMirror Ce processus lance un nouveau snapshot généré à partir du volume source et le copie vers le volume de destination.

Pour créer un volume, exécutez la commande suivante sur le cluster ONTAP de destination :

```
ONTAP-Dest::> snapmirror initialize -destination-path DestSVM:DestVol
```

Configuration du plug-in SnapCenter pour VMware vSphere

Une fois installé, le plug-in SnapCenter pour VMware vSphere est accessible à partir de l'interface de gestion de l'appliance vCenter Server. SCV gère les sauvegardes des datastores NFS montés sur les hôtes ESXi et contenant les machines virtuelles Windows et Linux.

Vérifiez le "[Flux de travail de protection des données](#)" Section de la documentation SCV pour plus

d'informations sur les étapes de configuration des sauvegardes.

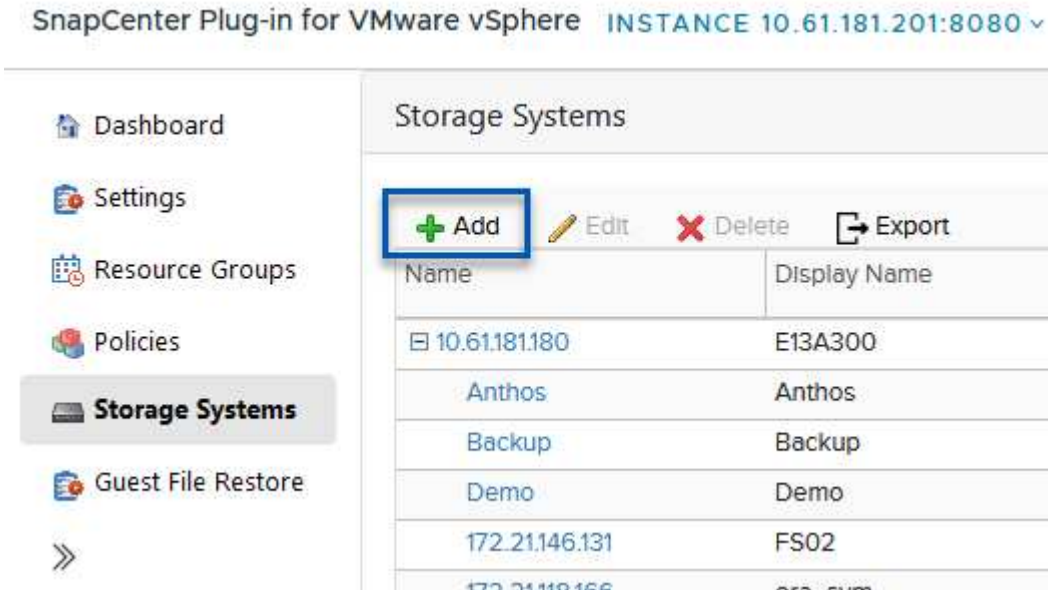
Pour configurer les sauvegardes de vos machines virtuelles et de vos datastores, les étapes suivantes doivent être effectuées à partir de l'interface du plug-in.

Découvrez les systèmes de stockage ONTAP

Découvrez les clusters de stockage ONTAP à utiliser pour les sauvegardes primaires et secondaires.

1. Dans le plug-in SnapCenter pour VMware vSphere, accédez à **systèmes de stockage** dans le menu de gauche et cliquez sur le bouton **Ajouter**.

SnapCenter Plug-in for VMware vSphere **INSTANCE 10.61.181.201:8080** ▾



The screenshot shows the SnapCenter interface for the SnapCenter Plug-in for VMware vSphere. The instance is identified as 10.61.181.201:8080. On the left, a navigation menu includes Dashboard, Settings, Resource Groups, Policies, Storage Systems (highlighted), and Guest File Restore. The main area displays the Storage Systems page with a table of existing storage systems. A blue box highlights the '+ Add' button in the top right corner of the table area.

Storage Systems	
+ Add Edit Delete Export	
Name	Display Name
10.61.181.180	E13A300
Anthos	Anthos
Backup	Backup
Demo	Demo
172.21.146.131	FS02
172.21.146.131	FS02

2. Renseignez les informations d'identification et le type de plate-forme du système de stockage ONTAP principal et cliquez sur **Ajouter**.

Add Storage System

Storage System	<input type="text" value="10.61.185.145"/>
Platform	<input type="text" value="All Flash FAS"/>
Authentication Method	<input checked="" type="radio"/> Credentials <input type="radio"/> Certificate
Username	<input type="text" value="admin"/>
Password	<input type="password" value="••••••••"/>
Protocol	<input type="text" value="HTTPS"/>
Port	<input type="text" value="443"/>
Timeout	<input type="text" value="60"/> <input type="text" value="Seconds"/>
<input type="checkbox"/> Preferred IP	<input type="text" value="Preferred IP"/>

Event Management System(EMS) & AutoSupport Setting

- Log Snapcenter server events to syslog
- Send AutoSupport Notification for failed operation to storage system

3. Répétez cette procédure pour le système de stockage ONTAP secondaire.

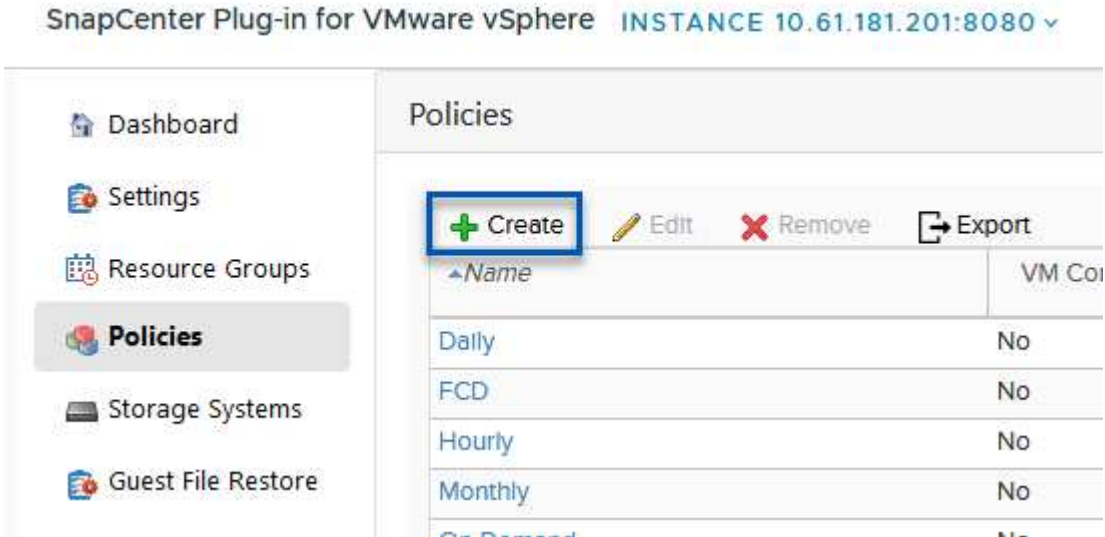
Créer des politiques de sauvegarde SCV

Les règles spécifient la période de rétention, la fréquence et les options de réplication pour les sauvegardes gérées par SCV.

Vérifiez le "[Créer des règles de sauvegarde pour les VM et les datastores](#)" pour plus d'informations, reportez-vous à la section de la documentation.

Pour créer des stratégies de sauvegarde, procédez comme suit :

1. Dans le plug-in SnapCenter pour VMware vSphere, accédez à **Politiques** dans le menu de gauche et cliquez sur le bouton **Create**.



2. Spécifiez un nom pour la règle, la période de conservation, les options de fréquence et de réplication, ainsi que le libellé de l'instantané.

New Backup Policy

Name

Description

Retention ⓘ

Frequency

Replication

- Update SnapMirror after backup ⓘ
- Update SnapVault after backup ⓘ

Snapshot label

Advanced ▾

- VM consistency ⓘ
- Include datastores with independent disks

Scripts ⓘ



Lors de la création d'une règle dans le plug-in SnapCenter, vous voyez les options pour SnapMirror et SnapVault. Si vous choisissez SnapMirror, la planification de conservation spécifiée dans la règle sera la même pour les snapshots principal et secondaire. Si vous choisissez SnapVault, la planification de conservation du snapshot secondaire sera basée sur une planification distincte implémentée avec la relation SnapMirror. Cette option est utile lorsque vous souhaitez prolonger les périodes de conservation pour les sauvegardes secondaires.



Les étiquettes de snapshots sont utiles dans la mesure où elles peuvent être utilisées pour mettre en place des stratégies avec une période de conservation spécifique pour les copies SnapVault répliquées sur le cluster ONTAP secondaire. Lorsque SCV est utilisé avec BlueXP Backup and Restore, le champ d'étiquette de Snapshot doit être vide ou match le libellé spécifié dans la règle de sauvegarde BlueXP.

3. Répétez la procédure pour chaque police requise. Par exemple, des règles distinctes pour les sauvegardes quotidiennes, hebdomadaires et mensuelles.

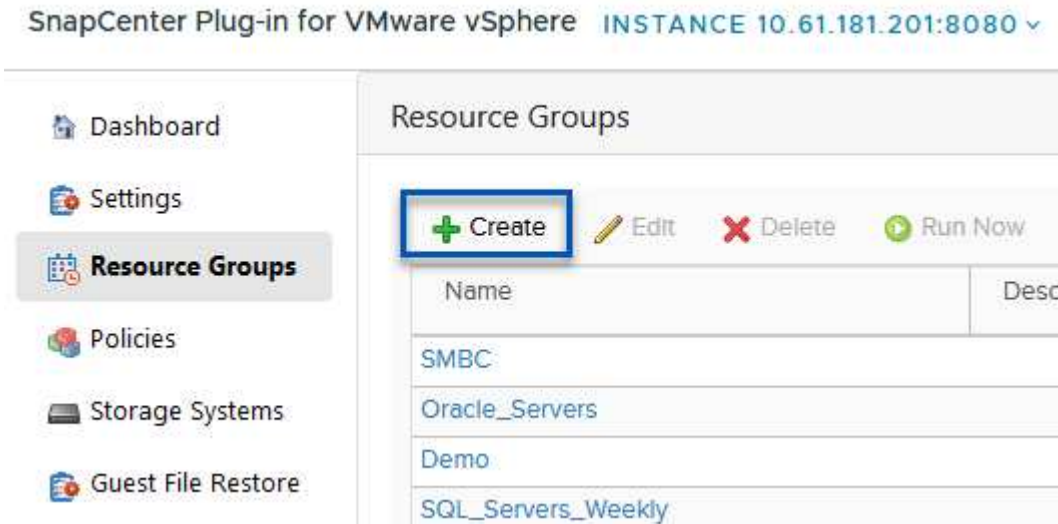
Créer des groupes de ressources

Les groupes de ressources contiennent les datastores et les machines virtuelles à inclure dans une tâche de sauvegarde, ainsi que la stratégie et le planning de sauvegarde associés.

Vérifiez le "[Créer des groupes de ressources](#)" pour plus d'informations, reportez-vous à la section de la documentation.

Pour créer des groupes de ressources, procédez comme suit.

1. Dans le plug-in SnapCenter pour VMware vSphere, accédez à **Resource Groups** dans le menu de gauche et cliquez sur le bouton **Create**.



2. Dans l'assistant Créer un groupe de ressources, entrez un nom et une description pour le groupe, ainsi que les informations requises pour recevoir les notifications. Cliquez sur **Suivant**
3. Sur la page suivante, sélectionnez les datastores et les machines virtuelles à inclure dans la tâche de sauvegarde, puis cliquez sur **Suivant**.

Create Resource Group

1. General info & notification

2. Resource

3. Spanning disks

4. Policies

5. Schedules

6. Summary

Scope:

Datacenter:

Entity name:

Available entities

- Demo
- DemoDS
- destination
- esxi7-hc-01 Local
- esxi7-hc-02 Local
- esxi7-hc-03 Local
- esxi7-hc-04 Local

Selected entities

- NFS_SCV
- NFS_WKLD



Vous avez la possibilité de sélectionner des VM spécifiques ou des datastores entiers. Quelle que soit l'option choisie, la totalité du volume (et du datastore) est sauvegardée, car la sauvegarde résulte de la création d'un snapshot du volume sous-jacent. Dans la plupart des cas, il est plus facile de choisir l'intégralité du datastore. Toutefois, si vous souhaitez limiter la liste des machines virtuelles disponibles lors de la restauration, vous ne pouvez choisir qu'un sous-ensemble de machines virtuelles à sauvegarder.

4. Choisissez des options de répartition des datastores pour les machines virtuelles avec VMDK qui résident sur plusieurs datastores, puis cliquez sur **Next**.

Create Resource Group

1. General info & notification

2. Resource

3. Spanning disks

4. Policies

5. Schedules

6. Summary

Always exclude all spanning datastores

This means that only the datastores directly added to the resource group and the primary datastore of VMs directly added to the resource group will be backed up

Always include all spanning datastores

All datastores spanned by all included VMs are included in this backup

Manually select the spanning datastores to be included

You will need to modify the list every time new VMs are added

There are no spanned entities in the selected virtual entities list.



La sauvegarde et la restauration BlueXP ne prennent pas actuellement en charge la sauvegarde des machines virtuelles avec des VMDK qui s'étendent sur plusieurs datastores.

5. Sur la page suivante, sélectionnez les stratégies qui seront associées au groupe de ressources et cliquez sur **Suivant**.

Create Resource Group

- ✓ 1. General info & notification
- ✓ 2. Resource
- ✓ 3. Spanning disks
- 4. Policies**
- 5. Schedules
- 6. Summary

+ Create

<input type="checkbox"/>	Name	VM Consistent	Include independent di...	Schedule
<input checked="" type="checkbox"/>	Daily	No	No	Daily
<input type="checkbox"/>	FCD	No	Yes	On Demand Only
<input type="checkbox"/>	Monthly	No	No	Monthly
<input type="checkbox"/>	On Demand	No	No	On Demand Only
<input type="checkbox"/>	Weekly	No	No	Weekly



Lors de la sauvegarde des snapshots gérés par SCV dans le stockage objet à l'aide de la sauvegarde et de la restauration BlueXP, chaque groupe de ressources ne peut être associé qu'à une seule règle.

6. Sélectionnez une planification qui déterminera à quelle heure les sauvegardes seront exécutées. Cliquez sur **Suivant**.

Create Resource Group

- ✓ 1. General info & notification
- ✓ 2. Resource
- ✓ 3. Spanning disks
- ✓ 4. Policies
- ✓ 5. Schedules**
- ✓ 6. Summary

Daily



Type

Daily

Every

1 Day(s)

Starting

06/23/2023

At

07 00 PM

7. Enfin, passez en revue la page de résumé, puis sur **Terminer** pour terminer la création du groupe de ressources.

Exécutez une tâche de sauvegarde

Dans cette dernière étape, exécutez une tâche de sauvegarde et surveillez sa progression. Au moins une tâche de sauvegarde doit être effectuée avec succès dans SCV pour que les ressources puissent être découvertes à partir de la sauvegarde et de la restauration BlueXP.

1. Dans le plug-in SnapCenter pour VMware vSphere, accédez à **Resource Groups** dans le menu de gauche.
2. Pour lancer une tâche de sauvegarde, sélectionnez le groupe de ressources souhaité et cliquez sur le bouton **Exécuter maintenant**.

SnapCenter Plug-in for VMware vSphere **INSTANCE 10.61.181.201:8080** ▾



The screenshot shows the SnapCenter interface for VMware vSphere. On the left is a navigation menu with options: Dashboard, Settings, Resource Groups (highlighted), Policies, Storage Systems, and Guest File Restore. The main area is titled 'Resource Groups' and contains a table with columns 'Name' and 'Description'. Above the table are buttons for '+ Create', 'Edit', 'Delete', 'Run Now' (highlighted with a blue box), and 'Suspend'. The table lists several resource groups: Win01, SMBC, Oracle_Servers, Demo, SQL_Servers_Daily (highlighted in blue), and SQL_Servers_Weekly.

Name	Description
Win01	
SMBC	
Oracle_Servers	
Demo	
SQL_Servers_Daily	
SQL_Servers_Weekly	

3. Pour surveiller la tâche de sauvegarde, accédez à **Dashboard** dans le menu de gauche. Sous **activités récentes**, cliquez sur le numéro d'ID du travail pour surveiller la progression du travail.

Job Details : 2614

- ✓ Validate Retention Settings
- ✓ Quiescing Applications
- ✓ Retrieving Metadata
- ✓ Creating Snapshot copy
- ✓ Unquiescing Applications
- ✓ Registering Backup
- ✓ Backup Retention
- ✓ Clean Backup Cache
- ✓ Send EMS Messages
- ▶ (Job 2616)SnapVault Update

▶ Running, Start Time: 07/31/2023 07:24:40 PM.

[CLOSE](#) [DOWNLOAD JOB LOGS](#)

Configurez les sauvegardes vers le stockage objet dans la sauvegarde et la restauration BlueXP

Pour que BlueXP puisse gérer efficacement l'infrastructure de données, il faut au préalable installer un connecteur. Le connecteur exécute les actions impliquées dans la découverte des ressources et la gestion des opérations de données.

Pour plus d'informations sur le connecteur BlueXP, reportez-vous à la section "[En savoir plus sur les connecteurs](#)" Dans la documentation BlueXP.

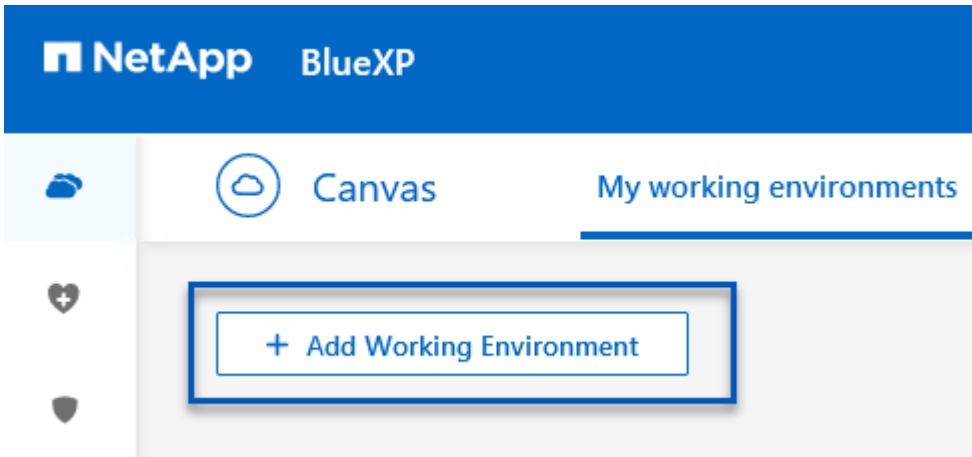
Une fois le connecteur installé pour le fournisseur de cloud utilisé, une représentation graphique du stockage objet est visible dans la zone de dessin.

Pour configurer la sauvegarde et la restauration BlueXP pour les données de sauvegarde gérées par SCV sur site, effectuez les opérations suivantes :

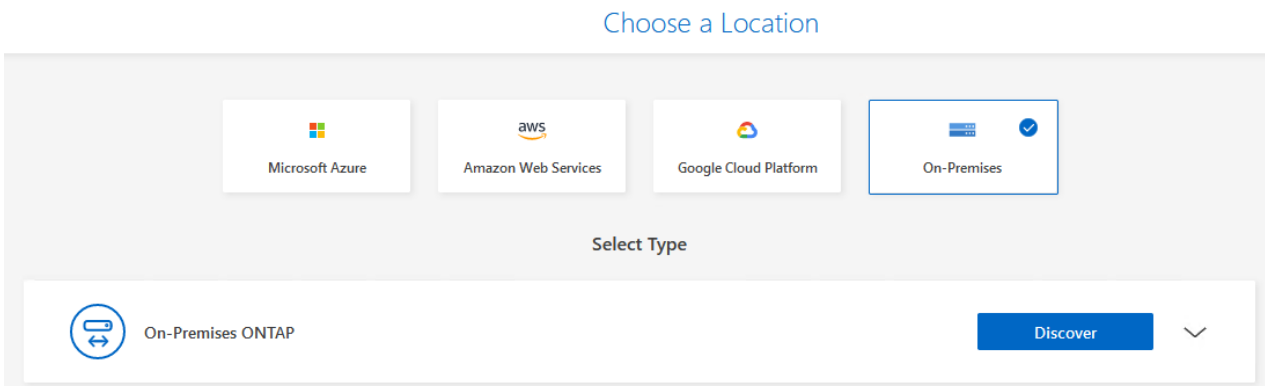
Ajoutez des environnements de travail au canevas

La première étape consiste à ajouter les systèmes de stockage ONTAP sur site à BlueXP

1. Dans la zone de travail, sélectionnez **Ajouter un environnement de travail** pour commencer.



2. Sélectionnez **sur place** dans les emplacements de votre choix, puis cliquez sur le bouton **découvrir**.



3. Renseignez les informations d'identification du système de stockage ONTAP et cliquez sur le bouton **découvrir** pour ajouter l'environnement de travail.

ONTAP Cluster IP

10.61.181.180

User Name

admin

Password

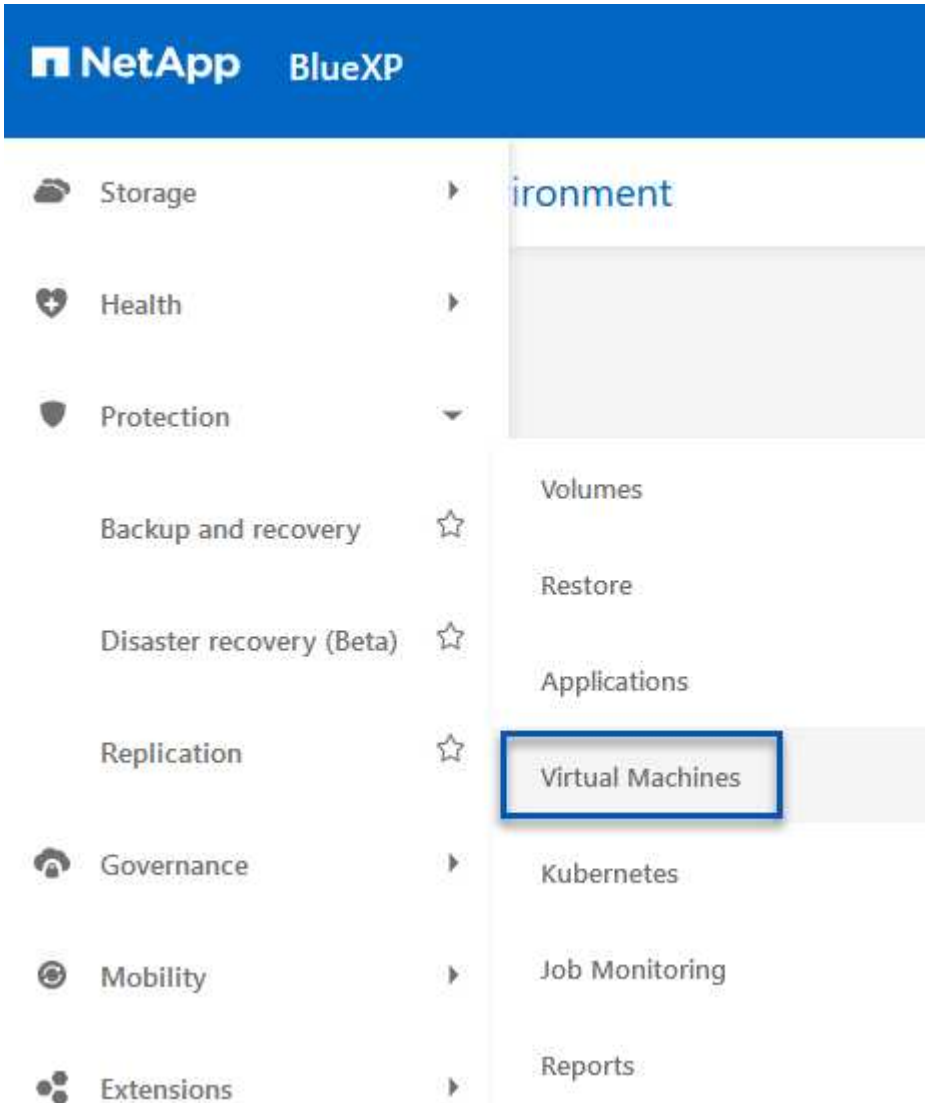
••••••••



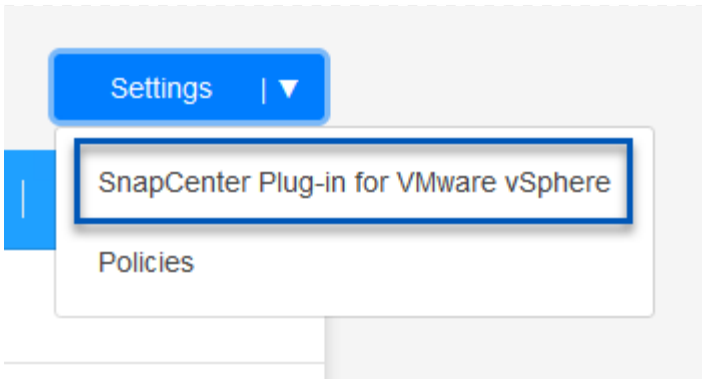
Découvrez l'appliance SCV sur site et vCenter

Pour découvrir les ressources des datastores sur site et des machines virtuelles, ajoutez des informations pour le courtier de données SCV et des informations d'identification pour l'appliance de gestion vCenter.

1. Dans le menu de gauche de BlueXP, sélectionnez **protection > sauvegarde et restauration > machines virtuelles**



2. Dans l'écran principal des machines virtuelles, accédez au menu déroulant **Paramètres** et sélectionnez **Plug-in SnapCenter pour VMware vSphere**.



3. Cliquez sur le bouton **Enregistrer**, puis entrez l'adresse IP et le numéro de port de l'apppliance de plug-in SnapCenter, ainsi que le nom d'utilisateur et le mot de passe de l'apppliance de gestion vCenter. Cliquez sur le bouton **Register** pour commencer le processus de découverte.

Register SnapCenter Plug-in for VMware vSphere

SnapCenter Plug-in for VMware vSphere


Username

Port


Password

4. La progression des travaux peut être contrôlée à partir de l'onglet surveillance des travaux.


Job Name: Discover Virtual Resources from SnapCenter Plug-in for VMWare vSphere
Job Id: 559167ba-8876-45db-9131-b918a165d0a1




Other
Job Type



Jul 31 2023, 9:18:22 pm
Start Time



Jul 31 2023, 9:18:26 pm
End Time



Success
Job Status

Sub-Jobs(2) Collapse All ^

Job Name	Job ID	Start Time	End Time	Duration
Discover Virtual Resources from SnapCenter Plu...	559167ba-8876-45db-...	Jul 31 2023, 9:18:22 pm	Jul 31 2023, 9:18:26 pm	4 Seconds
Discovering Virtual Resources	99446761-f997-4c80-8...	Jul 31 2023, 9:18:22 pm	Jul 31 2023, 9:18:24 pm	2 Seconds
Registering Datastores	b7ab4195-1ee5-40ff-9a...	Jul 31 2023, 9:18:24 pm	Jul 31 2023, 9:18:26 pm	2 Seconds

5. Une fois la découverte terminée, vous pourrez afficher les datastores et les machines virtuelles sur tous les dispositifs SCV découverts.

4 Working Environments

6 Datastores

14 Virtual Machines

Datastore Protection

4 Protected

2 Unprotected

6 Datastores

Filter By +

VM View

Settings

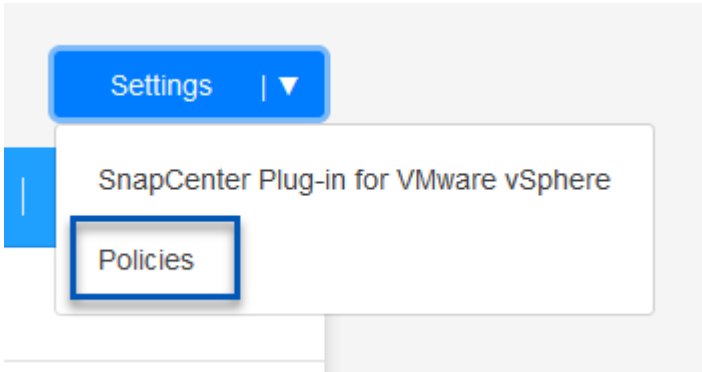
Datastore	Datastore Type	vCenter	Policy Name	Protection Status
NFS_SCV	NFS	vcsa7-hc.sddc.netapp.com		Unprotected
OTS_DS01	NFS	172.21.254.160	1 Year Daily LTR	Protected
SCV_WKLD	NFS	vcsa7-hc.sddc.netapp.com	1 Year Daily LTR	Protected
NFS_SQL	NFS	vcsa7-hc.sddc.netapp.com	1 Year Daily LTR	Protected
NFS_SQL2	NFS	vcsa7-hc.sddc.netapp.com	1 Year Daily LTR	Protected
SCV_DEMO	NFS	vcsa7-hc.sddc.netapp.com		Unprotected

Créez des règles de sauvegarde BlueXP

Dans le cadre de la sauvegarde et de la restauration BlueXP pour les machines virtuelles, créez des règles pour spécifier la période de conservation, la source de sauvegarde et la règle d'archivage.

Pour plus d'informations sur la création de règles, reportez-vous à la section "[Créer une stratégie pour sauvegarder les datastores](#)".

1. Sur la page principale de BlueXP Backup and Recovery for Virtual machines, accédez au menu déroulant **Settings** et sélectionnez **Policies**.



2. Cliquez sur **Create Policy** pour accéder à la fenêtre **Create Policy for Hybrid Backup**.
 - a. Ajoutez un nom à la règle
 - b. Sélectionnez la période de conservation souhaitée
 - c. Indiquez si les sauvegardes seront effectuées à partir du système de stockage ONTAP sur site principal ou secondaire
 - d. Vous pouvez également spécifier après quelle période les sauvegardes seront hiérarchisées vers le stockage d'archivage pour réaliser des économies supplémentaires.

Create Policy for Hybrid Backup

Policy Details

Policy Name
12 week - daily backups

Retention ⓘ

Daily ^

Backups to retain: 84 SnapMirror Label: Daily

Weekly Setup Retention Weekly ∨

Monthly Setup Retention Monthly ∨

Backup Source

Primary

Secondary

Archival Policy ⓘ

Backups reside in standard storage for frequently accessed data. Optionally, you can tier backups to archival storage for further cost optimization.

Tier Backups to Archival

Archival After (Days)



Le libellé SnapMirror saisi ici permet également d'identifier les sauvegardes à appliquer à la règle. Le nom de l'étiquette doit correspondre au nom de l'étiquette dans la politique de distributeur sélectif sur site correspondante.

3. Cliquez sur **Créer** pour terminer la création de la police.

Sauvegarde des datastores vers Amazon Web Services

L'étape finale consiste à activer la protection des données pour les datastores et les machines virtuelles individuels. Les étapes suivantes expliquent comment activer les sauvegardes dans AWS.

Pour plus d'informations, reportez-vous à la section "[Sauvegarde des datastores dans Amazon Web Services](#)".

1. Sur la page principale sauvegarde et restauration BlueXP pour les machines virtuelles, accédez à la liste déroulante des paramètres du datastore à sauvegarder et sélectionnez **Activer la sauvegarde**.

The screenshot shows the 'Datastores' section of the VMware backup and restore interface. It features a table with columns for Datastore, Datastore Type, vCenter, Policy Name, and Protection Status. The first datastore, NFS_SCV, is currently 'Unprotected'. A context menu is open for this row, showing options for 'View Details' and 'Activate Backup', with 'Activate Backup' highlighted by a red box.

Datastore	Datastore Type	vCenter	Policy Name	Protection Status
NFS_SCV	NFS	vcsa7-hc.sddc.netapp.com		Unprotected
OTS_DS01	NFS	172.21.254.160	1 Year Daily LTR	Protected
SCV_WKLD	NFS	vcsa7-hc.sddc.netapp.com	1 Year Daily LTR	Protected

2. Attribuez la stratégie à utiliser pour l'opération de protection des données et cliquez sur **Suivant**.

The screenshot shows the 'Assign Policy' step of the configuration wizard. It includes a progress bar with five steps: 1. Assign Policy (selected), 2. Add Working Environments, 3. Select Provider, 4. Configure Provider, and 5. Review. Below the progress bar is a table titled '21 Policies' with columns for Policy Name, SnapMirror Label, Retention Count, Backup Source, and Archival Policy. The second policy, '5 Year Daily LTR', is selected with a blue checkmark.

Policy Name	SnapMirror Label	Retention Count	Backup Source	Archival Policy
<input type="radio"/> 5 Year Daily LTR	daily	daily : 1830	Primary	Not Active
<input checked="" type="radio"/> 5 Year Daily LTR	daily	daily : 1830	Primary	Not Active
<input type="radio"/> 7 Year Weekly LTR	weekly	weekly : 370	Primary	Not Active

3. Sur la page **Ajouter des environnements de travail**, le datastore et l'environnement de travail avec une coche doivent apparaître si l'environnement de travail a été découvert précédemment. Si l'environnement de travail n'a pas été découvert précédemment, vous pouvez l'ajouter ici. Cliquez sur **Suivant** pour continuer.

- 1 Assign Policy 2 Add Working Environments 3 Select Provider 4 Configure Provider 5 Review

Add Working Environments

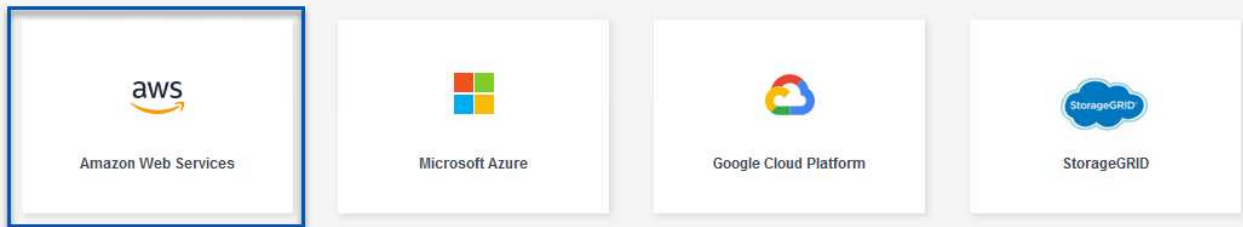
Provide ONTAP cluster (working environment) details that you want Cloud Manager to discover. Working environment details will appear for all volumes that reside on the same cluster. You will need to enter multiple working environments when volumes reside on different clusters.

SVM	Volume	Working Environment	
EHC_NFS	NFS_SCV	 OnPremWorkingEnvironment-6MzE27u1	Edit

4. Sur la page **Select Provider**, cliquez sur AWS, puis sur le bouton **Next** pour continuer.

- 1 Assign Policy 2 Add Working Environments 3 Select Provider 4 Configure Provider 5 Review

Select Provider



5. Remplissez les informations d'identification spécifiques au fournisseur pour AWS, notamment la clé d'accès AWS et la clé secrète, la région et le Tier d'archivage à utiliser. Vous pouvez également sélectionner l'espace IP ONTAP du système de stockage ONTAP sur site. Cliquez sur **Suivant**.

Configure Provider

Cloud Manager needs the following details to connect with the cloud provider.

Provider Information

AWS Account

AWS Access Key

Required

AWS Secret Key

Required

Location and Connectivity

Region

IP space for Environment

OnPremWorkingEnvironment-6MzE27u1

Archival Tier

- Enfin, passez en revue les détails de la tâche de sauvegarde et cliquez sur le bouton **Activer la sauvegarde** pour lancer la protection des données du datastore.

Review

Policy	5 Year Daily LTR
SVM	EHC_NFS
Volumes	NFS_SCV
Working Environment	OnPremWorkingEnvironment-6MzE27u1
Backup Source	Primary
Cloud Service Provider	AWS
AWS Account	[REDACTED]
AWS Access Key	[REDACTED]
Region	US East (N. Virginia)
IP space	Default
Tier Backups to Archival	No

Previous

Activate Backup



À ce stade, le transfert de données peut ne pas commencer immédiatement. La sauvegarde et la restauration BlueXP analysent afin de détecter tout snapshot exceptionnel toutes les heures, puis les transfère vers le stockage objet.

Restauration de machines virtuelles en cas de perte de données

Assurer la sauvegarde de vos données n'est qu'un aspect de la protection complète des données. Il est tout aussi important de pouvoir restaurer rapidement vos données en tout lieu en cas de perte de données ou d'attaque par ransomware. Cette fonctionnalité est essentielle pour assurer la transparence des opérations et atteindre les objectifs de point de récupération.

NetApp propose une stratégie 3-2-1 extrêmement flexible qui offre un contrôle personnalisé des calendriers de conservation dans les emplacements de stockage principal, secondaire et objet. Cette stratégie offre la flexibilité nécessaire pour adapter les approches de protection des données aux besoins spécifiques.

Cette section présente le processus de restauration des données du plug-in SnapCenter pour VMware vSphere ainsi que la sauvegarde et la restauration BlueXP pour les machines virtuelles.

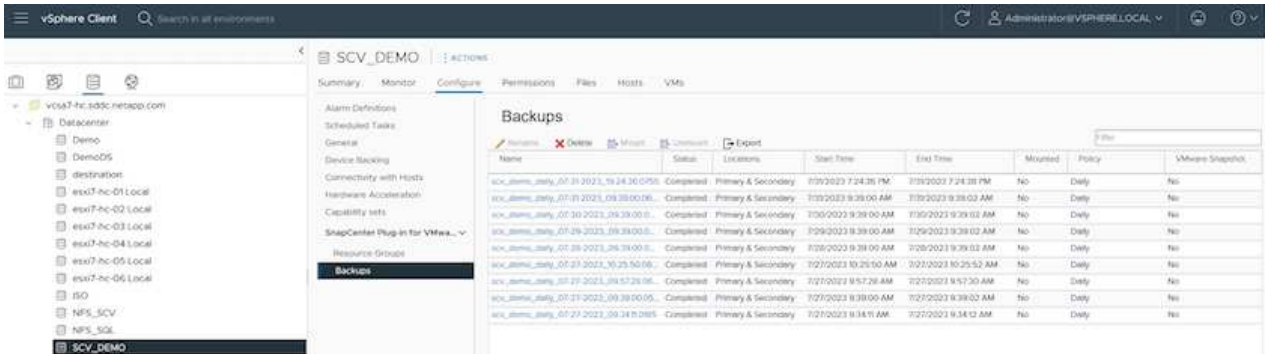
Restauration de machines virtuelles à partir du plug-in SnapCenter pour VMware vSphere

Pour cette solution, les machines virtuelles ont été restaurées dans leur emplacement d'origine et dans d'autres emplacements. Tous les aspects des capacités de restauration des données de SCV ne seront pas abordés dans cette solution. Pour plus d'informations sur tout ce que le distributeur auxiliaire doit offrir, voir ["Restauration de machines virtuelles à partir des sauvegardes"](#) dans la documentation du produit.

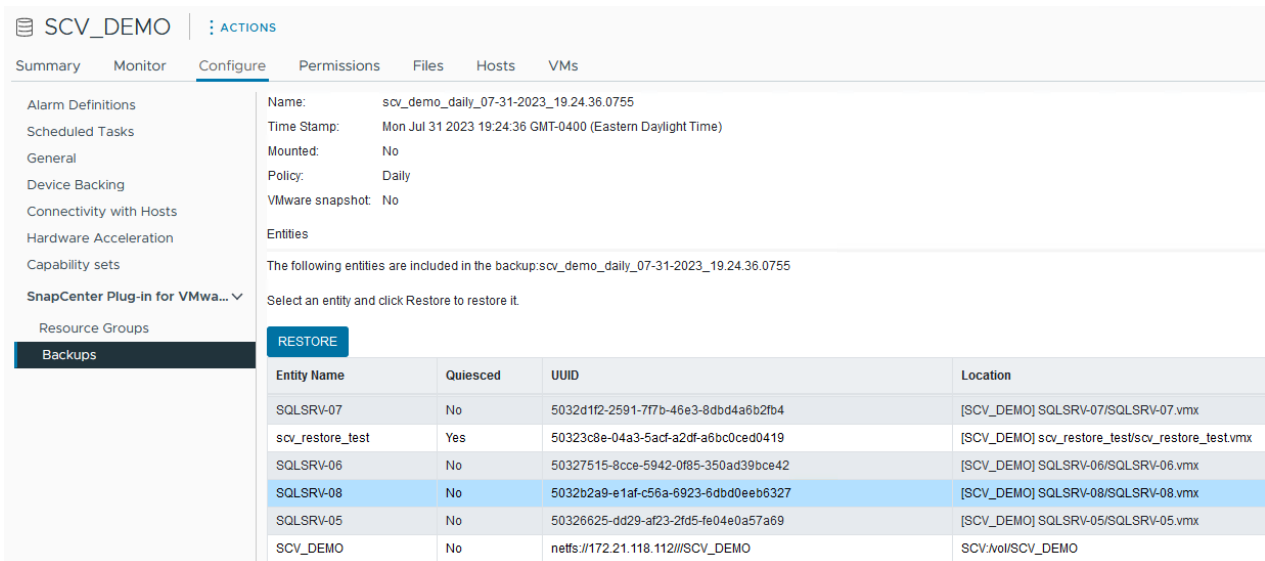
Restaurer les machines virtuelles à partir du distributeur sélectif

Procédez comme suit pour restaurer une machine virtuelle à partir du stockage principal ou secondaire.

1. Dans le client vCenter, accédez à **Inventory > Storage** et cliquez sur le datastore contenant les machines virtuelles que vous souhaitez restaurer.
2. Dans l'onglet **configurer**, cliquez sur **sauvegardes** pour accéder à la liste des sauvegardes disponibles.



3. Cliquez sur une sauvegarde pour accéder à la liste des machines virtuelles, puis sélectionnez une machine virtuelle à restaurer. Cliquez sur **Restaurer**.



4. Dans l'assistant de restauration, sélectionnez pour restaurer la machine virtuelle entière ou un VMDK spécifique. Sélectionnez cette option pour installer dans l'emplacement d'origine ou dans un autre emplacement, indiquez le nom de la machine virtuelle après la restauration et le datastore de destination. Cliquez sur **Suivant**.

Restore ✕

✓ 1. Select scope

2. Select location

3. Summary

Restore scope Entire virtual machine ▾

Restart VM

Restore Location

Original Location
(This will restore the entire VM to the original Hypervisor with the original settings. Existing VM will be unregistered and replaced with this VM.)

Alternate Location
(This will create a new VM on selected vCenter and Hypervisor with the customized settings.)

Destination vCenter Server 10.61.181.210 ▾

Destination ESXi host esxi7-hc-04.sddc.netapp.com ▾

Network Management 181 ▾

VM name after restore SQL_SRV_08_restored

Select Datastore: NFS_SCV ▾

BACK
NEXT
FINISH
CANCEL

5. Choisissez de sauvegarder vos données depuis l'emplacement de stockage principal ou secondaire.

Restore ✕

✓ 1. Select scope

2. Select location

3. Summary

Destination datastore	Locations
SCV_DEMO	(Primary) SCV:SCV_DEMO ▾
	<div style="border: 1px solid #ccc; padding: 2px;"> (Primary) SCV:SCV_DEMO (Secondary) EHC_NFS:SCV_DEMO_dest </div>

6. Enfin, consultez un résumé de la procédure de sauvegarde et cliquez sur Terminer pour lancer le processus de restauration.

Restauration des machines virtuelles à partir de la sauvegarde et de la restauration BlueXP pour les machines virtuelles

La sauvegarde et la restauration BlueXP pour les machines virtuelles permettent de restaurer les machines virtuelles à leur emplacement d'origine. Les fonctions de restauration sont accessibles via la console Web BlueXP.

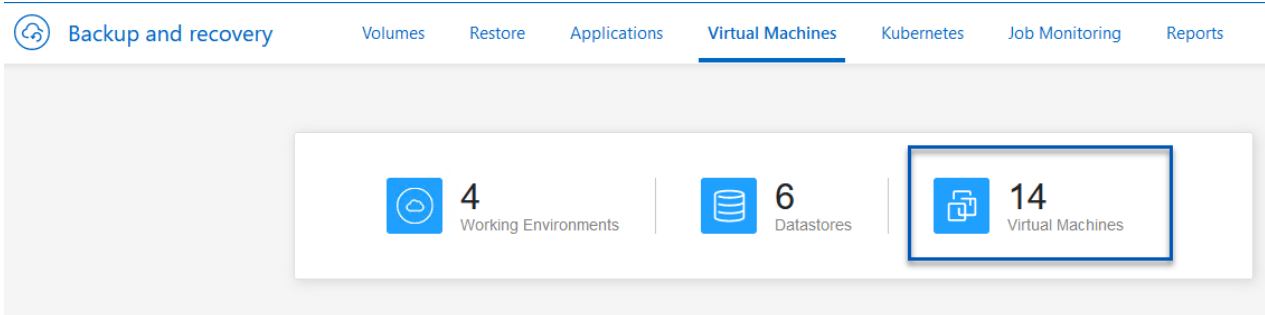
Pour plus d'informations, reportez-vous à la section "[Restaurez des données de machines virtuelles à partir du](#)

cloud".

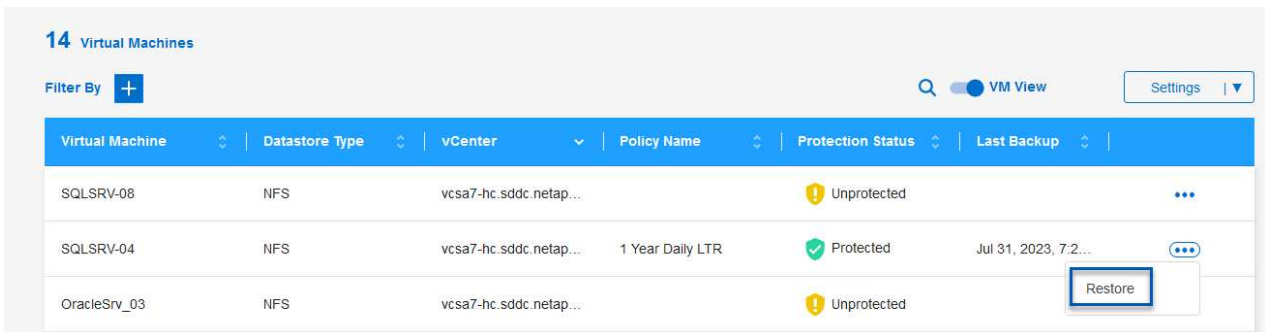
Restaurez les machines virtuelles à partir de la sauvegarde et de la restauration BlueXP

Pour restaurer une machine virtuelle à partir de la sauvegarde et de la restauration BlueXP, procédez comme suit.

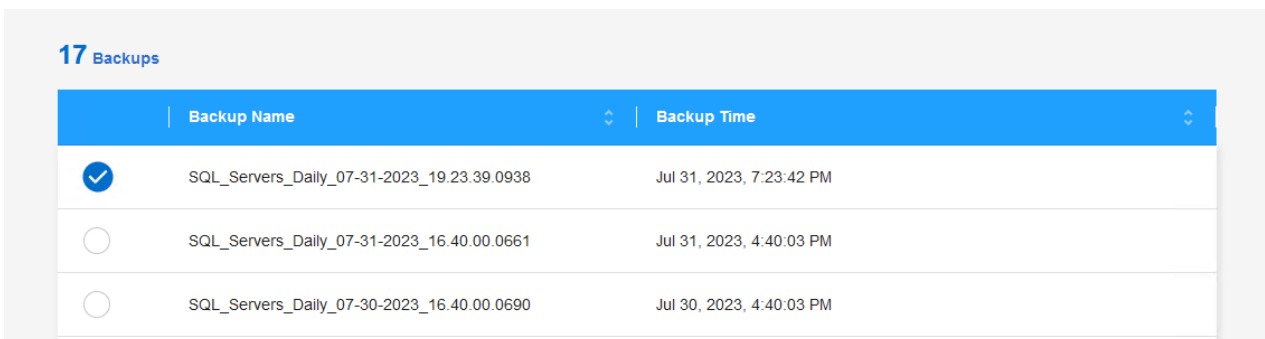
1. Accédez à **protection > sauvegarde et restauration > machines virtuelles** et cliquez sur machines virtuelles pour afficher la liste des machines virtuelles à restaurer.



2. Accédez au menu déroulant des paramètres de la machine virtuelle à restaurer et sélectionnez



3. Sélectionnez la sauvegarde à partir de laquelle effectuer la restauration et cliquez sur **Suivant**.



4. Consultez un résumé de la procédure de sauvegarde et cliquez sur **Restore** pour lancer le processus de restauration.
5. Surveillez la progression du travail de restauration à partir de l'onglet **Job Monitoring**.

Job Name: Restore 17 files from Cloud
Job Id: ec567065-dcf4-4174-b7ef-b27e6620fdbf

Restore Files (Job Type) | NFS_SQL (Restore Content) | 17 Files (Content Files) | NFS_SQL (Restore to) | In Progress (Job Status)

Restore Content

aws	ots-demo Working Environment Name	NAS_VOLS SVM Name	NFS_SQL Volume Name	SQL_Servers_Daily_07-31-2023_... Backup Name	Jul 31 2023, 7:24:03 pm Backup Time
-----	--------------------------------------	----------------------	------------------------	---	--

Restore from

aws	AWS Provider	us-east-1 Region	982589175402 Account ID	netapp-backup-d56250b0-24ad... Bucket/Container Name
-----	-----------------	---------------------	----------------------------	---

Conclusion

La stratégie de sauvegarde 3-2-1, implémentée avec le plug-in SnapCenter pour VMware vSphere et la sauvegarde et restauration BlueXP pour les machines virtuelles, offre une solution de protection des données robuste, fiable et économique. Cette stratégie assure non seulement la redondance et l'accessibilité des données, mais également la flexibilité de restauration des données en tout lieu et à partir des systèmes de stockage ONTAP sur site et du stockage objet basé dans le cloud.

Le cas d'utilisation présenté dans cette documentation est axé sur les technologies de protection des données à l'efficacité prouvée, qui mettent en avant l'intégration entre NetApp, VMware et les principaux fournisseurs de cloud. Le plug-in SnapCenter pour VMware vSphere permet une intégration transparente à VMware vSphere, ce qui permet une gestion efficace et centralisée des opérations de protection des données. Cette intégration rationalise les processus de sauvegarde et de restauration des machines virtuelles, facilitant ainsi la planification, la surveillance et les opérations de restauration flexibles au sein de l'écosystème VMware. La sauvegarde et la restauration BlueXP pour les machines virtuelles fournissent une (1) solution en 3-2-1, grâce à des sauvegardes sécurisées et à air Gap des données des machines virtuelles vers un stockage objet basé sur le cloud. L'interface intuitive et le flux de travail logique offrent une plate-forme sécurisée pour l'archivage à long terme des données critiques.

Informations supplémentaires

Pour en savoir plus sur les technologies présentées dans cette solution, consultez les informations complémentaires suivantes.

- ["Documentation du plug-in SnapCenter pour VMware vSphere"](#)
- ["Documentation BlueXP"](#)

Reprise après incident à l'aide de la DRaaS BlueXP

Présentation

La reprise sur incident est la priorité de tous les administrateurs VMware. Étant donné que VMware encapsule des serveurs entiers dans une série de fichiers qui composent la machine virtuelle, les administrateurs tirent parti de techniques basées sur le stockage bloc, telles que les clones, les snapshots et les répliques, pour protéger ces VM. Les baies ONTAP proposent une réplication intégrée pour le transfert des données de volume, et donc des serveurs virtuels résidant sur les LUN de datastore désignées, d'un site à un autre. La DRaaS de BlueXP s'intègre à vSphere et automatise l'ensemble du workflow pour un basculement et un retour arrière transparents en cas d'incident. En associant la réplication du stockage à une automatisation intelligente, les administrateurs disposent désormais d'un moyen simple de configurer, d'automatiser et de tester les plans de reprise après incident, mais aussi de les exécuter facilement en cas d'incident.

Le basculement de reprise après incident dans un environnement VMware vSphere prend le plus de temps en exécutant les étapes nécessaires pour inventorier, enregistrer, reconfigurer et mettre sous tension les machines virtuelles sur le site de reprise après incident. La solution idéale présente à la fois un RPO faible (mesuré en minutes) et un RTO faible (mesuré en minutes, voire en heures). Il est souvent négligé dans une solution de reprise sur incident car elle permet de tester efficacement la solution de reprise sur incident à intervalles réguliers.

Facteurs à prendre en compte pour concevoir une solution de reprise d'activité :

- L'objectif de délai de restauration (RTO). L'objectif de délai de restauration est la rapidité avec laquelle une entreprise peut se remettre d'un incident, ou plus particulièrement le temps nécessaire à l'exécution du processus de restauration pour assurer la disponibilité des services de l'entreprise.
- L'objectif de point de récupération (RPO). L'objectif de point de récupération est l'âge à partir duquel les données restaurées ont été mises à disposition, par rapport à l'heure à laquelle l'incident s'est produit.
- Évolutivité et adaptabilité. Ce facteur permet d'accroître les ressources de stockage progressivement en fonction de la demande.

Pour plus d'informations techniques sur les solutions disponibles, consultez :

- ["Reprise après incident à l'aide de la DRaaS BlueXP pour les datastores NFS"](#)
- ["Reprise après incident à l'aide de la DRaaS BlueXP pour les datastores VMFS"](#)

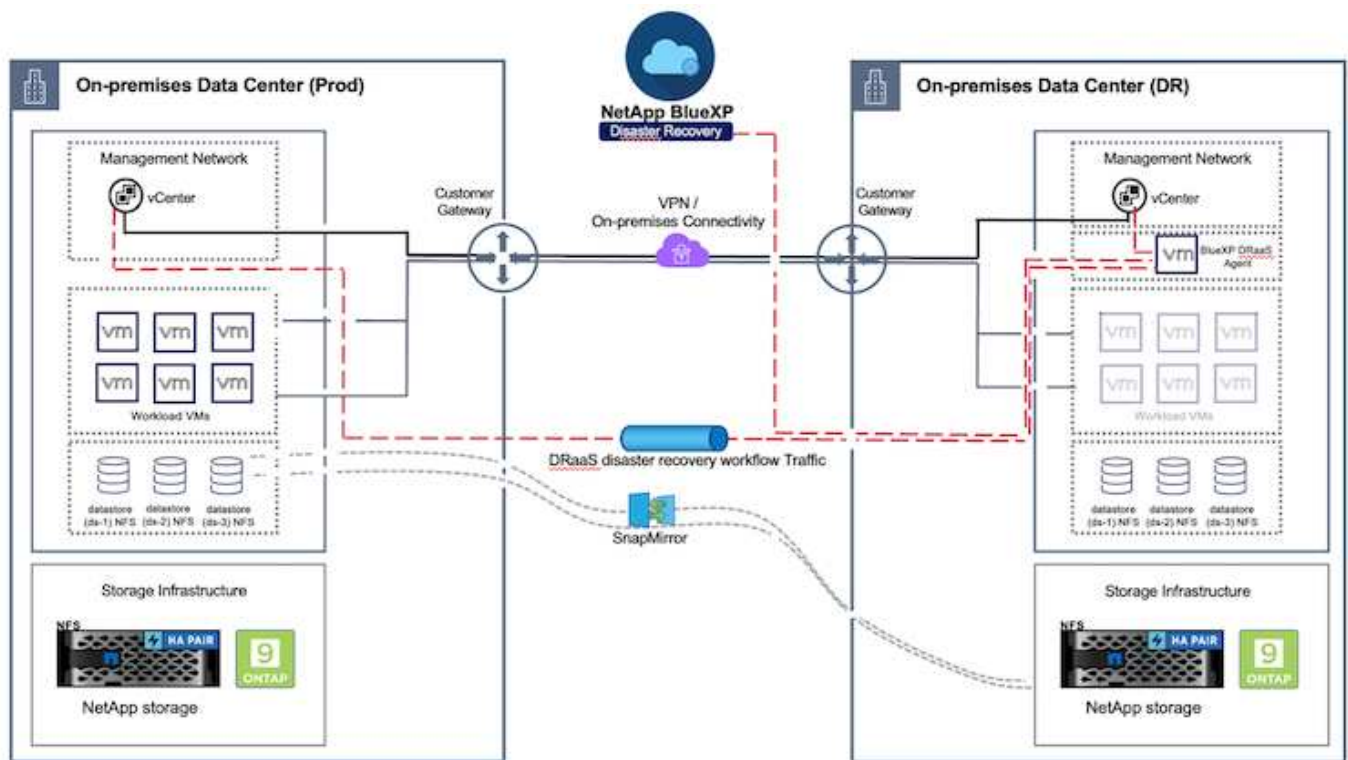
Reprise après incident à l'aide de la DRaaS BlueXP pour les datastores NFS

La mise en œuvre d'une reprise d'activité via une réplication au niveau des blocs du site de production vers le site de reprise d'activité est une méthode résiliente et économique pour protéger les workloads contre les pannes de site et la corruption des données, telles que les attaques par ransomware. Grâce à la réplication NetApp SnapMirror, les workloads VMware exécutés sur des systèmes ONTAP sur site avec un datastore NFS peuvent être répliqués sur un autre système de stockage ONTAP situé dans un data center de restauration désigné, dans lequel VMware est également déployé.

Cette section du document décrit la configuration de la DRaaS BlueXP pour la configuration de la reprise après incident pour les machines virtuelles VMware sur site sur un autre site désigné. Dans le cadre de cette configuration, le compte BlueXP, BlueXP Connector, les baies ONTAP ajoutées dans l'espace de travail BlueXP, qui est nécessaire pour permettre la communication de VMware vCenter vers le stockage ONTAP. En outre, ce document explique en détail comment configurer la réplication entre les sites et comment configurer et tester un plan de reprise d'activité. La dernière section contient les instructions permettant d'effectuer un basculement de site complet et de revenir en arrière lorsque le site principal est récupéré et acheté en ligne.

Grâce au service de reprise après incident BlueXP intégré à la console NetApp BlueXP, les entreprises peuvent facilement découvrir leurs vCenters VMware sur site et leur stockage ONTAP. Les organisations peuvent ensuite créer des regroupements de ressources, créer un plan de reprise sur incident, l'associer à des groupes de ressources et tester ou exécuter le basculement et la restauration. SnapMirror assure la réplication des blocs au niveau du stockage afin de maintenir les deux sites à jour en cas de modifications incrémentielles. L'objectif de point de récupération (RPO) peut donc atteindre 5 minutes. De plus, il est possible de simuler des procédures de reprise après incident sans affecter la production ni encourir des coûts de stockage supplémentaires.

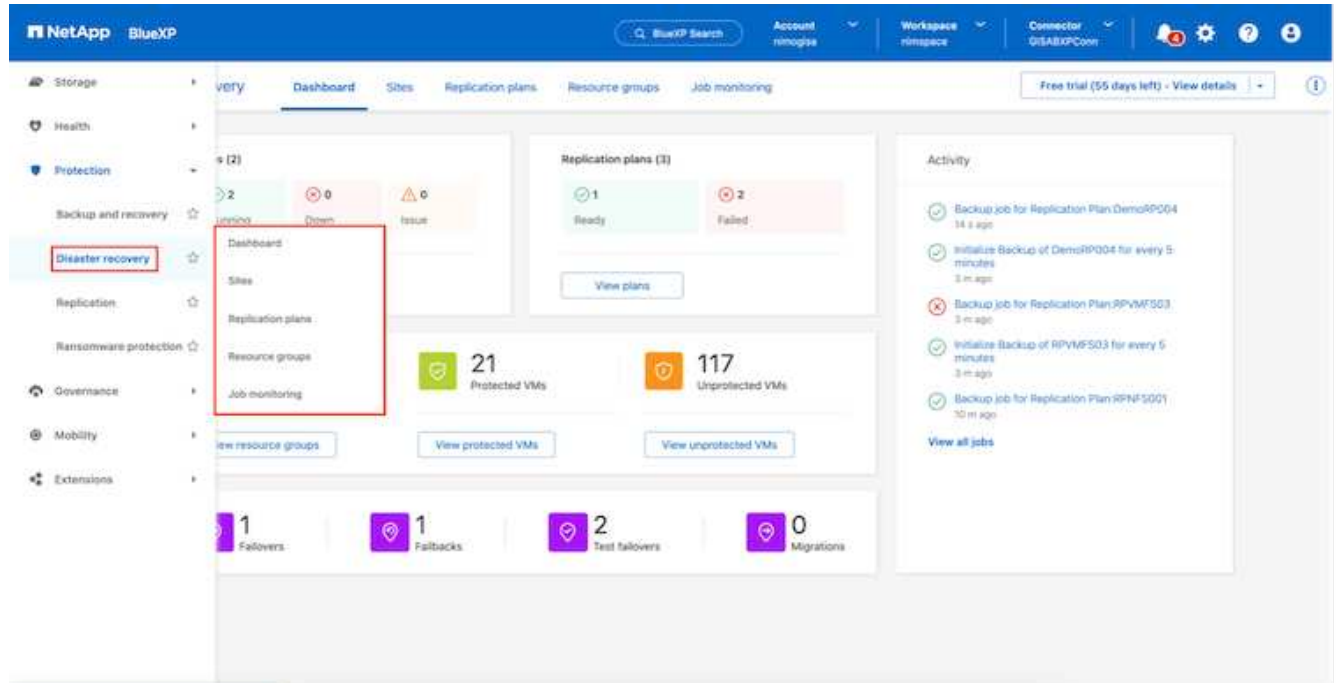
La reprise d'activité BlueXP exploite la technologie FlexClone de ONTAP pour créer une copie compacte du datastore NFS à partir du dernier snapshot répliqué sur le site de reprise d'activité. Une fois le test de reprise après incident terminé, les clients peuvent facilement supprimer l'environnement de test sans affecter les ressources de production répliquées. En cas de basculement réel, le service de reprise d'activité BlueXP orchestre toutes les étapes nécessaires pour intégrer automatiquement les machines virtuelles protégées sur le site de reprise d'activité désigné en quelques clics. Le service inverse également la relation SnapMirror sur le site principal et réplique les modifications du stockage secondaire vers le stockage primaire pour une opération de restauration, si nécessaire. Toutes ces fonctionnalités sont moins coûteuses que les autres solutions alternatives les plus connues.



Pour commencer

Pour commencer à utiliser la reprise après incident BlueXP, utilisez la console BlueXP, puis accédez au service.

1. Connectez-vous à BlueXP.
2. Dans le menu de navigation de gauche de BlueXP , sélectionnez protection > reprise après incident.
3. Le tableau de bord de reprise après incident de BlueXP s'affiche.



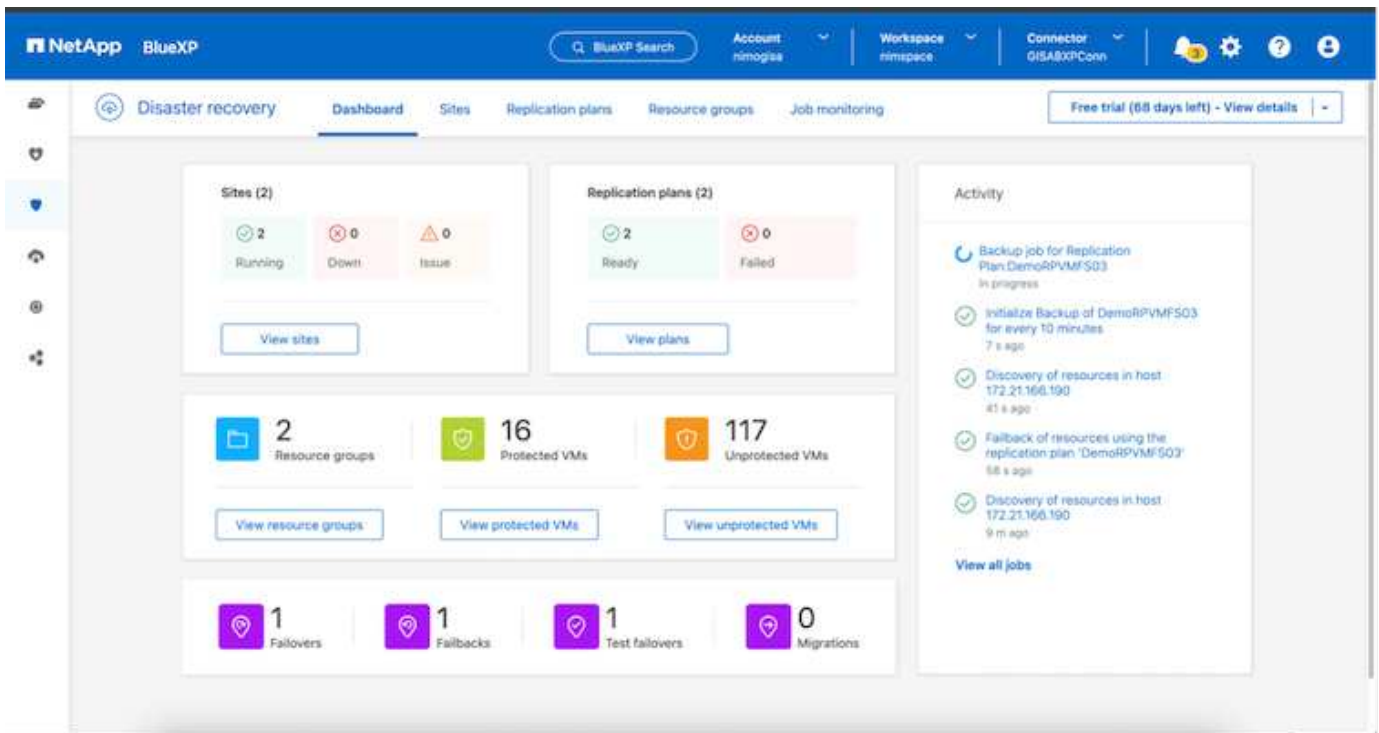
Avant de configurer le plan de reprise sur incident, assurez-vous que les conditions préalables suivantes sont remplies :

- Le connecteur BlueXP est configuré dans NetApp BlueXP .
- L'instance BlueXP Connector est connectée aux systèmes vCenter et de stockage source et de destination.
- Cluster NetApp Data ONTAP pour fournir des datastores NFS de stockage.
- Les systèmes de stockage NetApp sur site hébergeant des datastores NFS pour VMware sont ajoutés à BlueXP .
- La résolution DNS doit être en place lors de l'utilisation de noms DNS. Sinon, utilisez les adresses IP pour vCenter.
- La réplication SnapMirror est configurée pour les volumes de datastore NFS désignés.
- Assurez-vous que l'environnement dispose de versions prises en charge des serveurs vCenter Server et ESXi.

Une fois la connectivité établie entre les sites source et de destination, effectuez les étapes de configuration qui doivent prendre quelques clics et environ 3 à 5 minutes.



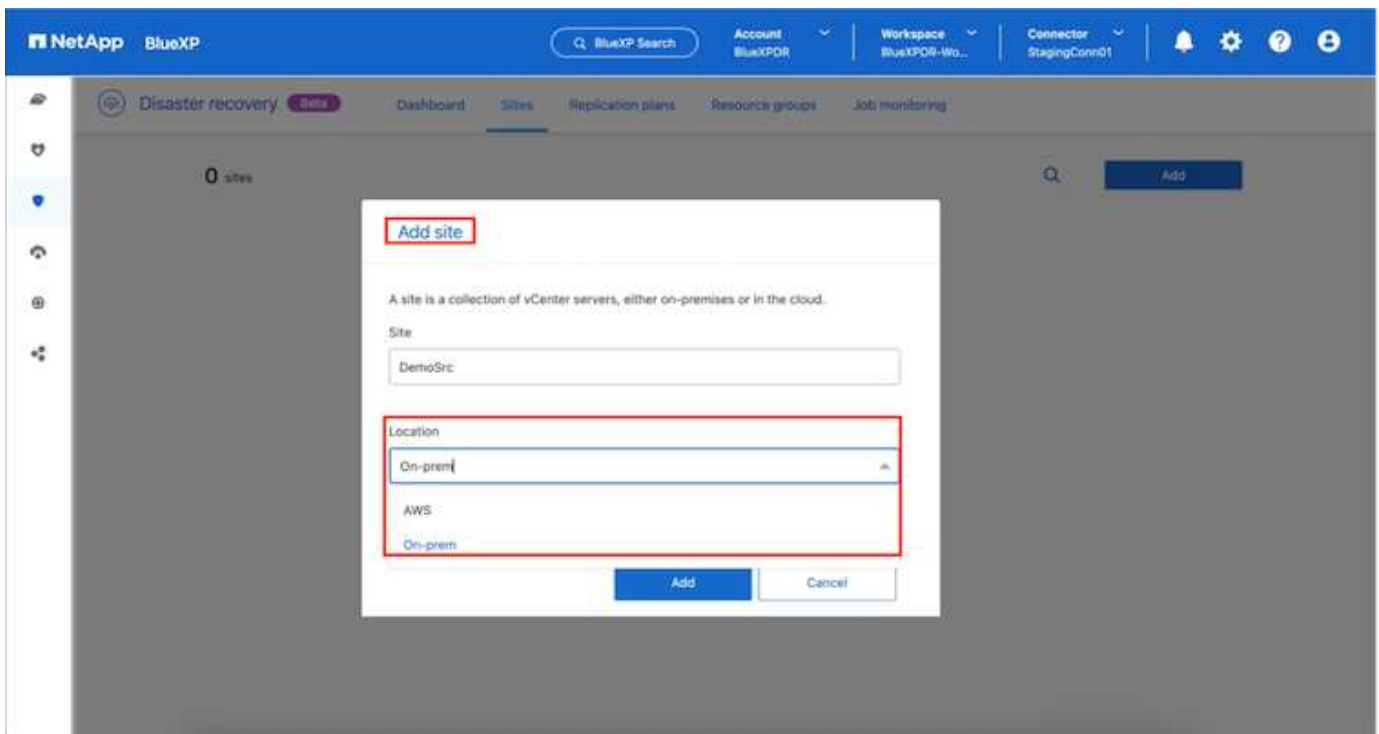
NetApp recommande de déployer le connecteur BlueXP sur le site de destination ou sur un troisième site, afin que le connecteur BlueXP puisse communiquer via le réseau avec les ressources source et de destination.



Configuration de la reprise sur incident BlueXP

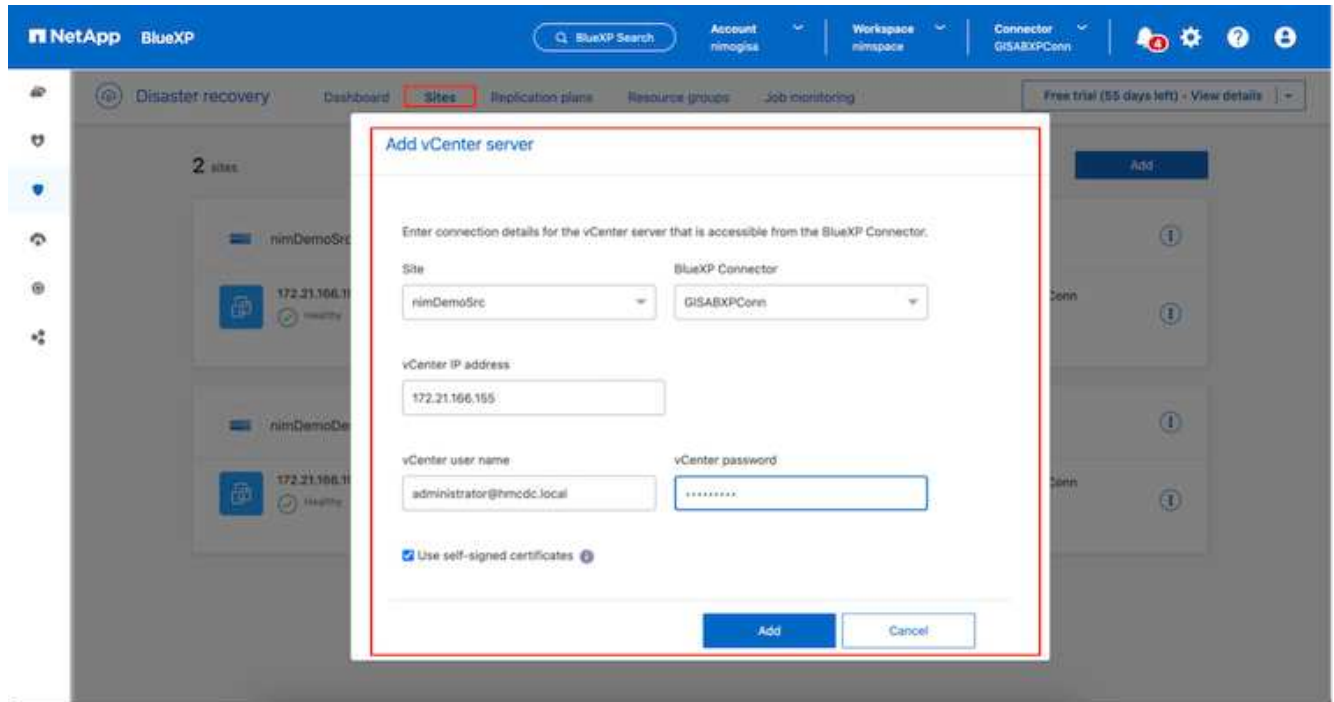
Pour préparer la reprise d'activité, la première étape consiste à découvrir et à ajouter les ressources vCenter et de stockage sur site à la reprise d'activité BlueXP .

Ouvrez la console BlueXP et sélectionnez **protection > récupération après sinistre** dans le menu de navigation de gauche. Sélectionnez **découvrir les serveurs vCenter** ou utilisez le menu supérieur, sélectionnez **sites > Ajouter > Ajouter vCenter**.

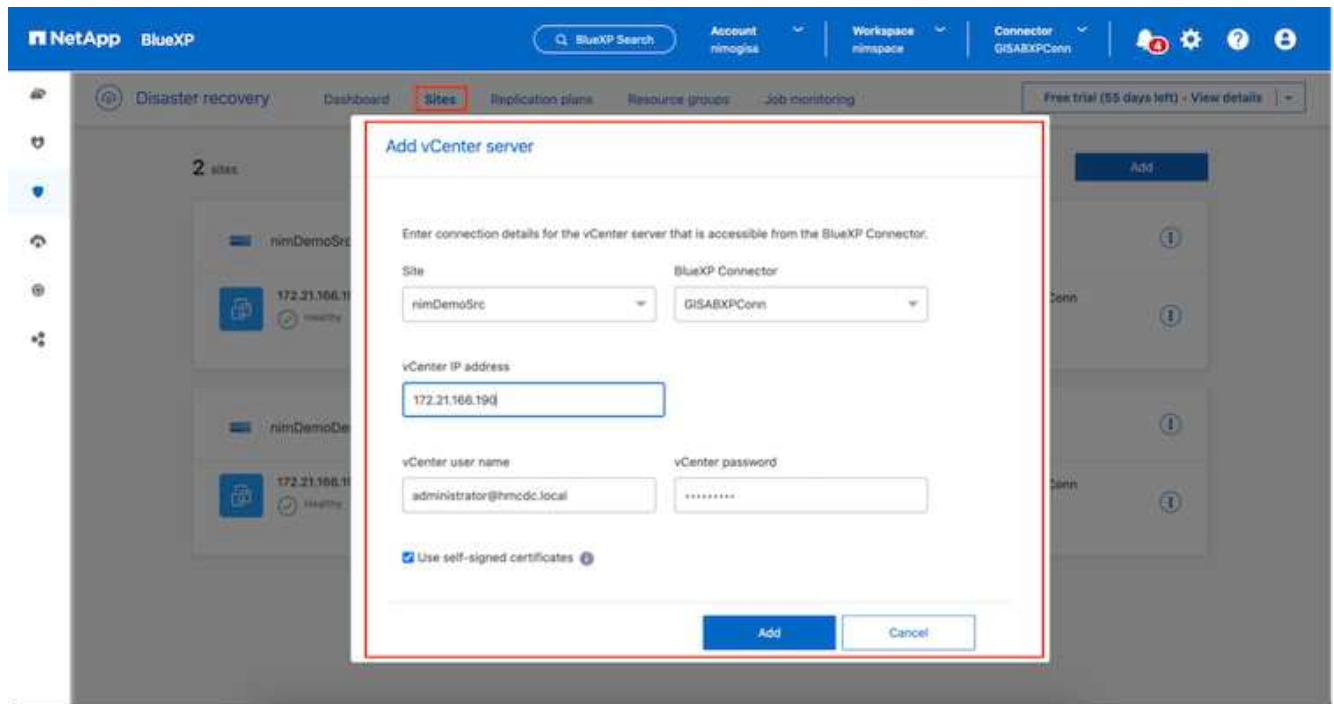


Ajoutez les plates-formes suivantes :

- **Source.** VCenter sur site



- **Destination.** VMC SDDC vCenter



Une fois les vCenters ajoutés, la découverte automatisée est déclenchée.

Configuration de la réplication de stockage entre la baie de site source et la baie de site de destination

SnapMirror assure la réplication des données dans un environnement NetApp. Basée sur la technologie NetApp Snapshot®, la réplication SnapMirror est extrêmement efficace car elle réplique uniquement les blocs qui ont été modifiés ou ajoutés depuis la mise à jour précédente. SnapMirror est facilement configuré à l'aide

de NetApp OnCommand® System Manager ou de l'interface de ligne de commande ONTAP. La DRaaS de BlueXP crée également la relation SnapMirror, à condition que le cluster et le peering de SVM soient configurés au préalable.

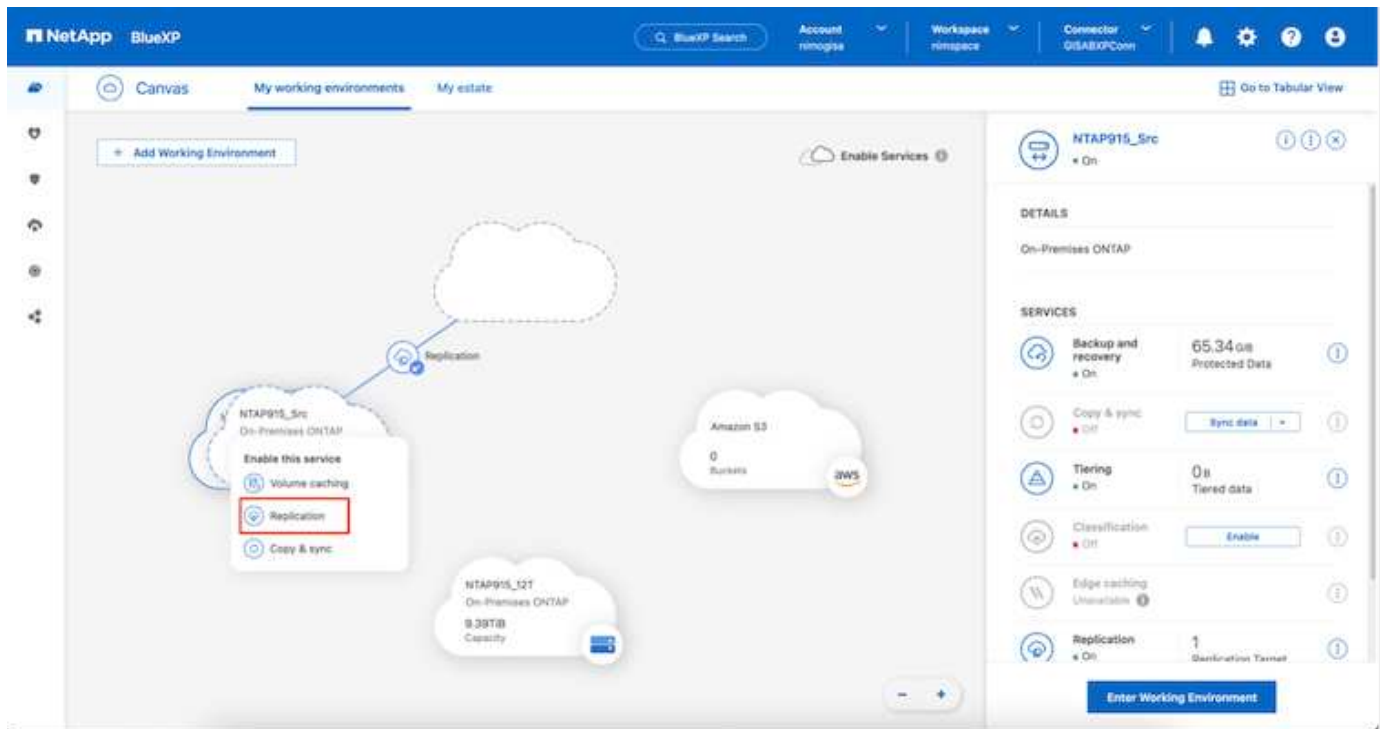
Si le stockage primaire n'est pas totalement perdu, SnapMirror fournit un moyen efficace de resynchroniser les sites primaire et de reprise d'activité. SnapMirror peut resynchroniser les deux sites, en transférant uniquement les données nouvelles ou modifiées vers le site primaire à partir du site de reprise d'activité, simplement en inversant les relations SnapMirror. Cela signifie que les plans de réplication dans BlueXP DRaaS peuvent être resynchronisés dans les deux sens après un basculement, sans recopier la totalité du volume. Si une relation est resynchronisée dans le sens inverse, seules les données écrites depuis la dernière synchronisation réussie de la copie Snapshot sont renvoyées vers la destination.



Si la relation SnapMirror est déjà configurée pour le volume via l'interface de ligne de commande ou le Gestionnaire système, BlueXP DRaaS reprend la relation et poursuit les opérations du reste du workflow.

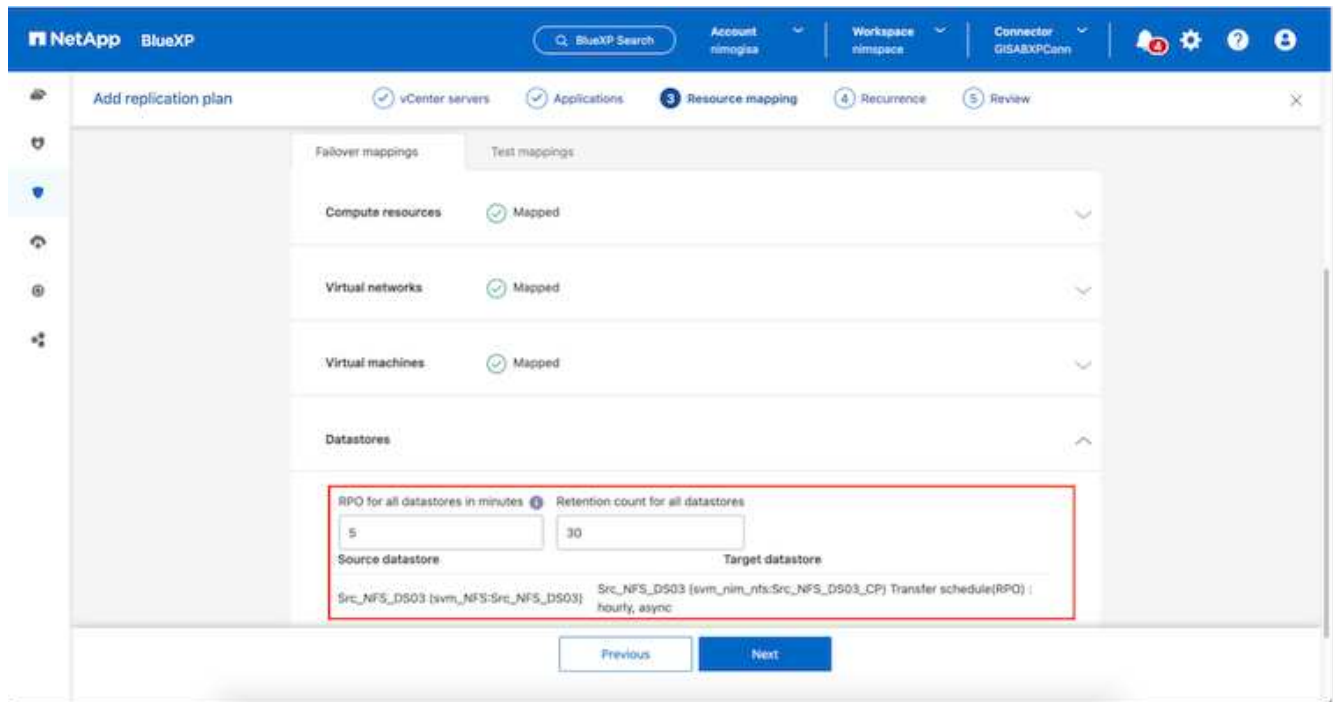
Configuration de la reprise d'activité VMware

Le processus de création de réplication SnapMirror reste le même pour une application donnée. Le processus peut être manuel ou automatisé. Le moyen le plus simple est d'utiliser BlueXP pour configurer la réplication SnapMirror à l'aide d'un simple glisser-déposer du système ONTAP source de l'environnement vers la destination afin de déclencher l'assistant qui guide le reste du processus.



La DRaaS de BlueXP peut également automatiser la même chose, à condition que les deux critères suivants soient remplis :

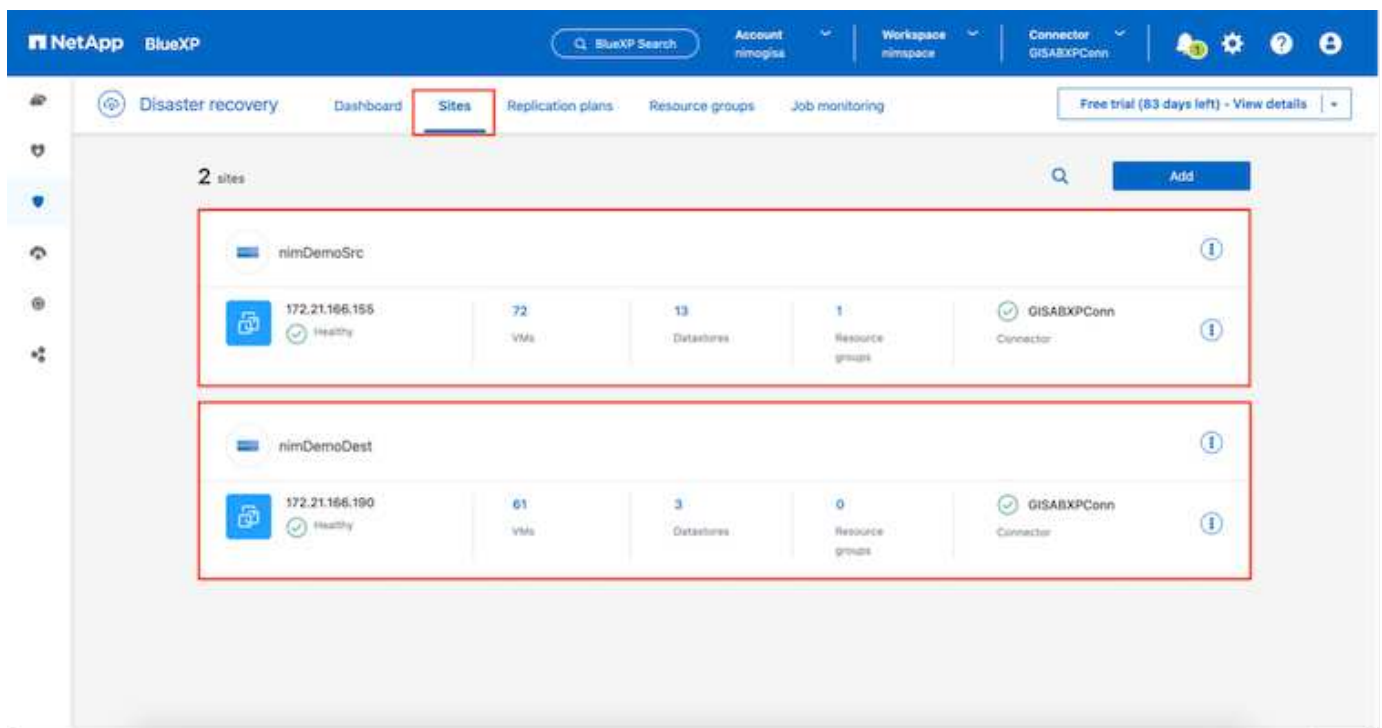
- Les clusters source et cible ont une relation homologue.
- Les SVM source et destination ont une relation entre pairs.



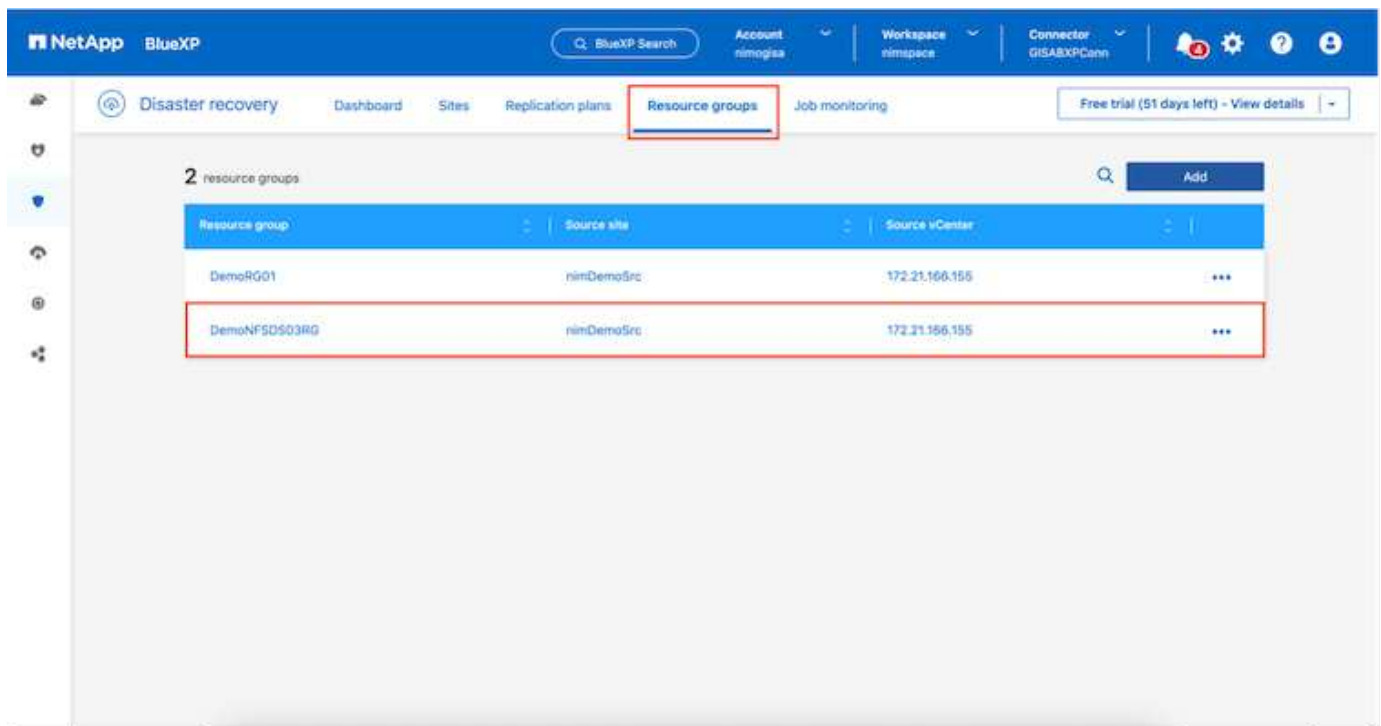
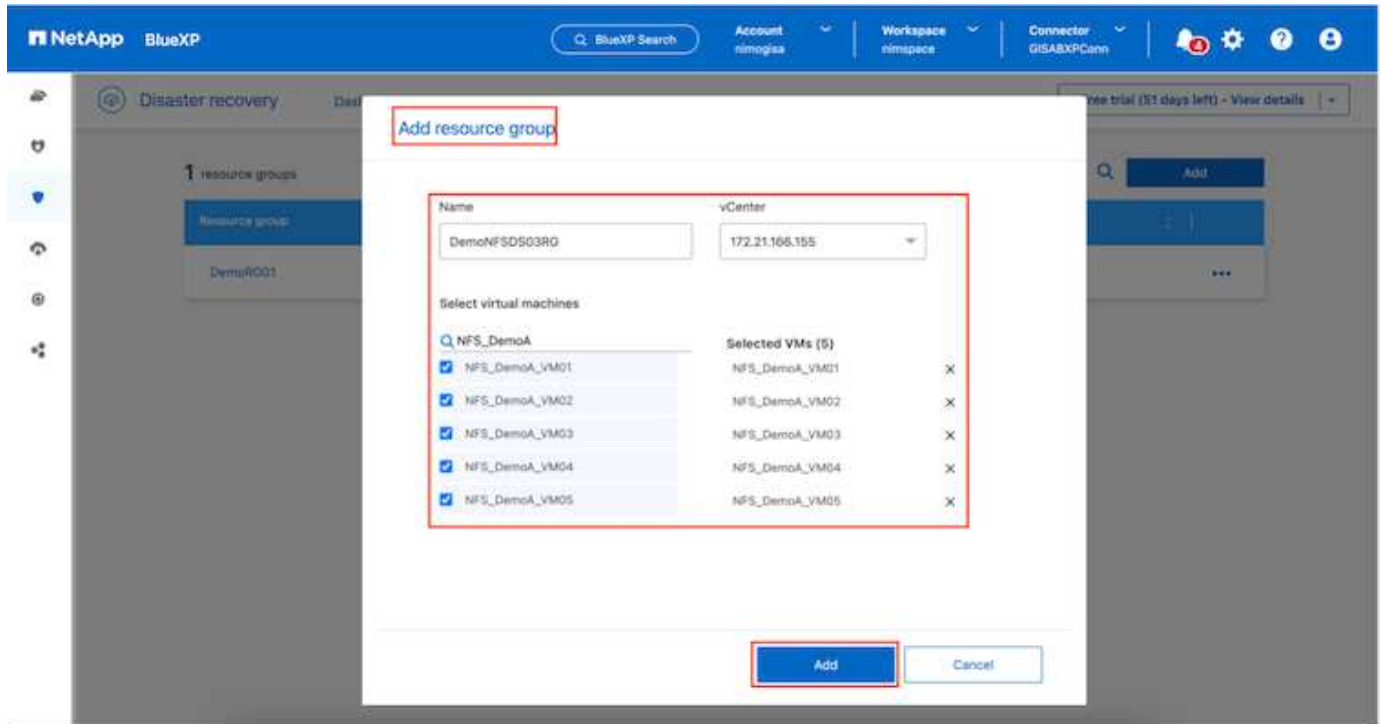
Si la relation SnapMirror est déjà configurée pour le volume via l'interface de ligne de commande, BlueXP DRaaS reprend la relation et poursuit les opérations du reste du workflow.

Quels avantages la reprise d'activité BlueXP peut-elle apporter pour vous ?

Une fois les sites source et de destination ajoutés, la reprise d'activité BlueXP effectue une détection approfondie automatique et affiche les VM ainsi que les métadonnées associées. Par ailleurs, la reprise d'activité BlueXP détecte automatiquement les réseaux et les groupes de ports utilisés par les machines virtuelles et les remplit.

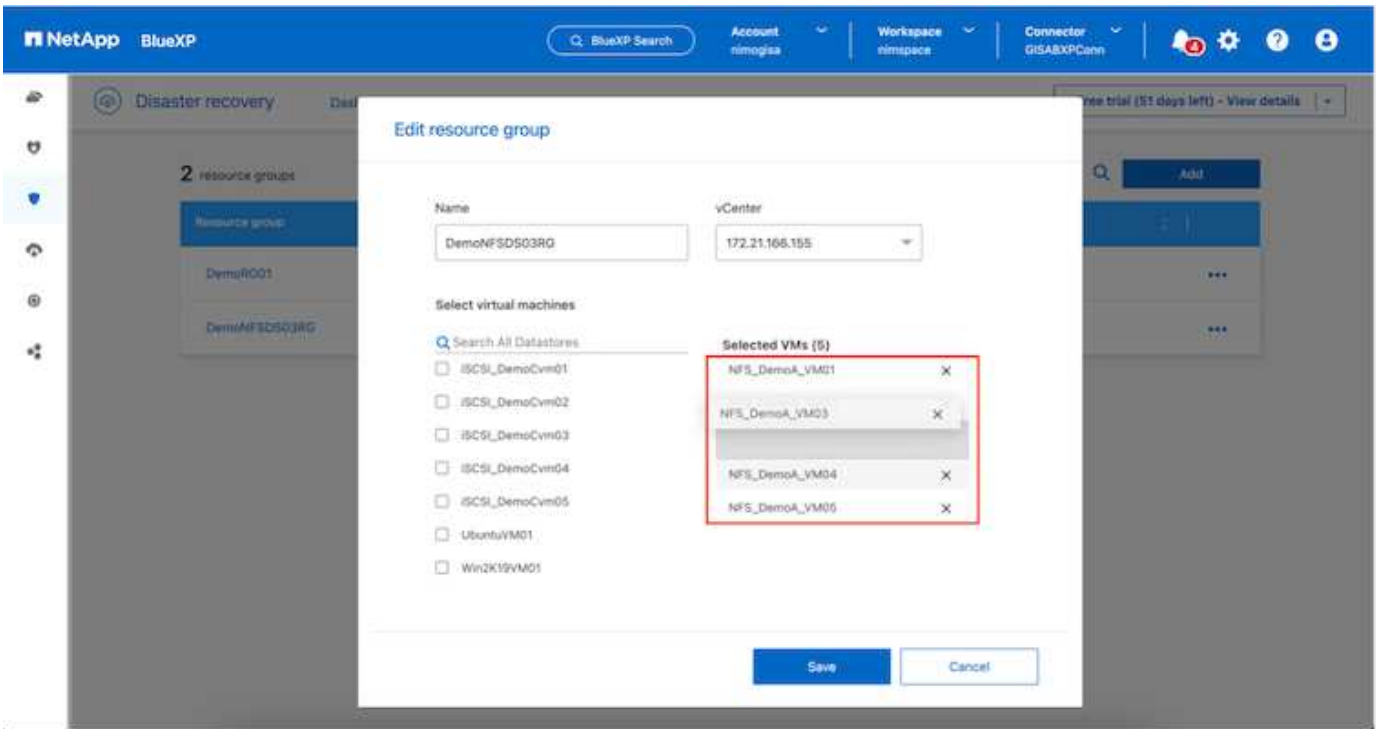


Une fois les sites ajoutés, les VM peuvent être regroupées en groupes de ressources. Les groupes de ressources de reprise sur incident BlueXP vous permettent de regrouper un ensemble de machines virtuelles dépendantes en groupes logiques contenant leurs ordres de démarrage et leurs délais de démarrage pouvant être exécutés lors de la restauration. Pour commencer à créer des groupes de ressources, accédez à **groupes de ressources** et cliquez sur **Créer un nouveau groupe de ressources**.

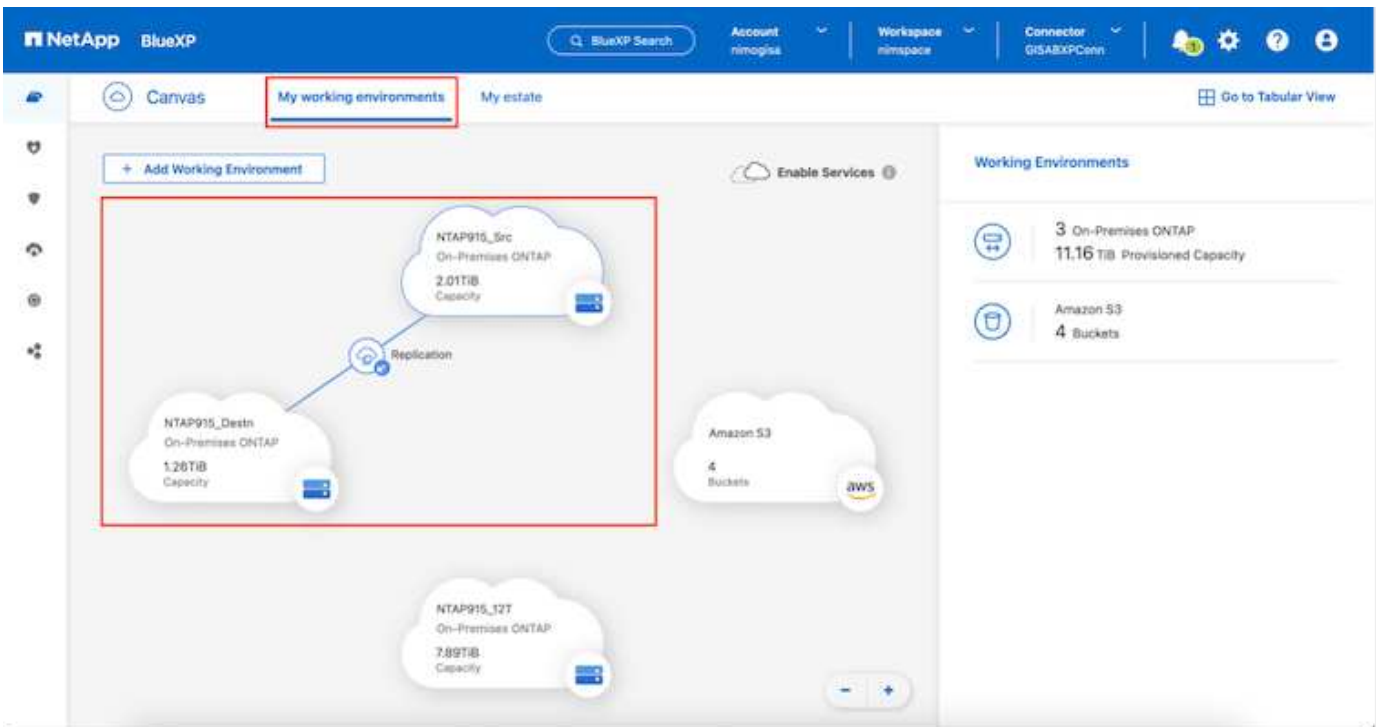


Le groupe de ressources peut également être créé lors de la création d'un plan de réplication.

L'ordre de démarrage des machines virtuelles peut être défini ou modifié lors de la création de groupes de ressources à l'aide d'un simple mécanisme de glisser-déposer.



Une fois les groupes de ressources créés, l'étape suivante consiste à créer le modèle d'exécution ou un plan de restauration des machines virtuelles et des applications en cas d'incident. Comme indiqué dans les conditions préalables, la réplication SnapMirror peut être configurée au préalable ou DRaaS peut la configurer à l'aide du RPO et du nombre de rétention spécifiés lors de la création du plan de réplication.



NetApp BlueXP

Account nimogisa Workspace nimspace Connector GISABXPConn

Replication

Volume Relationships (8)

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer
	NTAP915_Src	NTAP915_Destn				20.3 MB
✓	Demo_TPS_DS01 NTAP915_Src	Demo_TPS_DS01_Copy NTAP915_Destn	13 seconds	idle	snapmirrored	Aug 5, 2024, 6:15 388.63 MiB
✓	Src_250_Vol01 NTAP915_Src	Src_250_Vol01_Copy NTAP915_Destn	4 seconds	idle	snapmirrored	Aug 16, 2024, 12: 79.23 MiB
✓	Src_NFS_DS03 NTAP915_Src	Src_NFS_DS03_CP NTAP915_Destn	12 seconds	idle	snapmirrored	Aug 16, 2024, 12: 24.64 MiB
✓	Src_NFS_DS04 NTAP915_Src	Src_NFS_DS04_CP NTAP915_Destn	3 seconds	idle	snapmirrored	Aug 16, 2024, 12: 47.38 MiB
✓	Src_JSCSI_DS04 NTAP915_Src	Src_JSCSI_DS04_copy NTAP915_Destn	4 seconds	idle	snapmirrored	Aug 16, 2024, 12: 108.87 MiB
✓	nimpra NTAP915_Src	nimpra_dest NTAP915_Destn	2 seconds	idle	snapmirrored	Aug 16, 2024, 12: 3.48 KiB

Configurez le plan de réplication en sélectionnant les plates-formes vCenter source et cible dans la liste déroulante, puis sélectionnez les groupes de ressources à inclure dans le plan, ainsi que le regroupement de la manière dont les applications doivent être restaurées et mises sous tension et le mappage des clusters et des réseaux. Pour définir le plan de reprise, accédez à l'onglet **Plan de réplication** et cliquez sur **Ajouter un plan**.

Sélectionnez d'abord le vCenter source, puis le vCenter de destination.

NetApp BlueXP

Account nimogisa Workspace nimspace Connector GISABXPConn

Add replication plan

1 vCenter servers 2 Applications 3 Resource mapping 4 Recurrence 5 Review

Replication plan name
DemoNFSDS03RP

Select a source vCenter where your data exists, to replicate to the selected target vCenter.

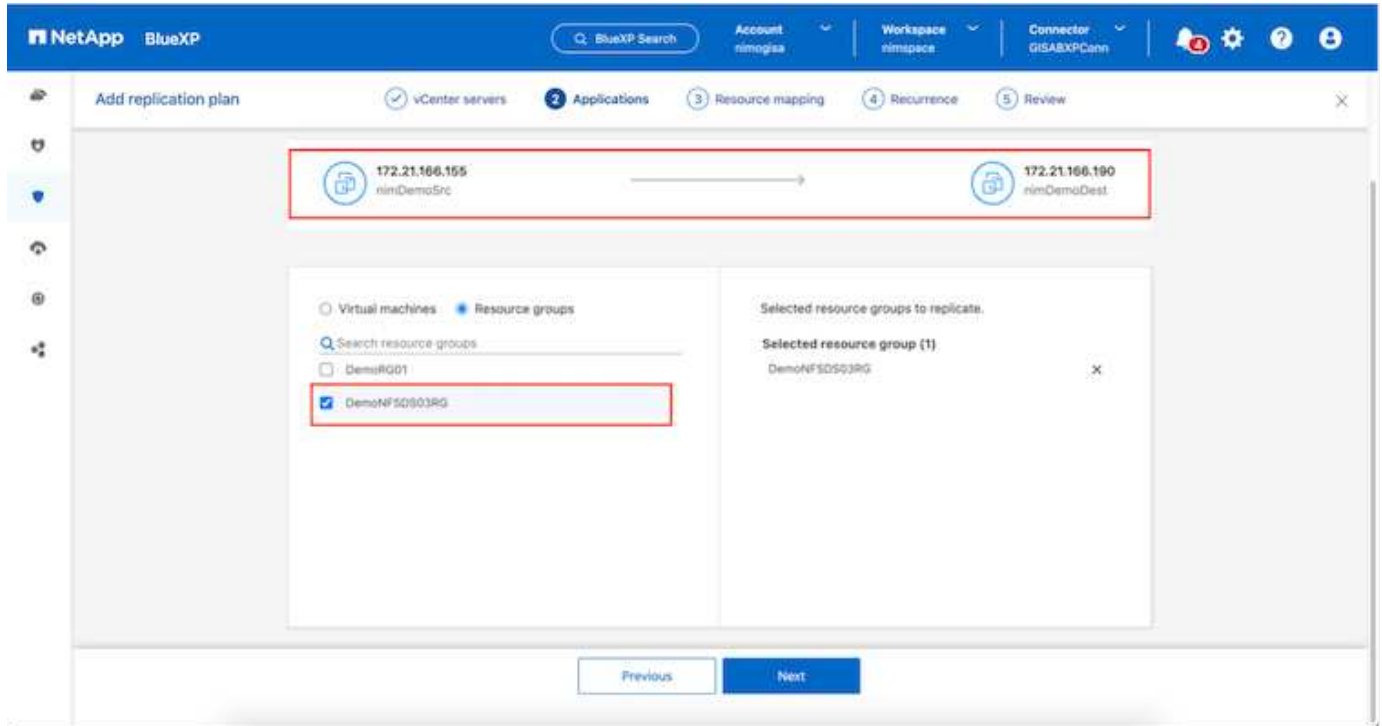
Source vCenter: 172.21.166.155

Target vCenter: 172.21.166.190

Cancel Next

L'étape suivante consiste à sélectionner des groupes de ressources existants. Si aucun groupe de ressources n'est créé, l'assistant vous aide à regrouper les machines virtuelles requises (en créant essentiellement des

groupes de ressources fonctionnelles) en fonction des objectifs de restauration. Cela permet également de définir la séquence de fonctionnement de la restauration des machines virtuelles d'applications.

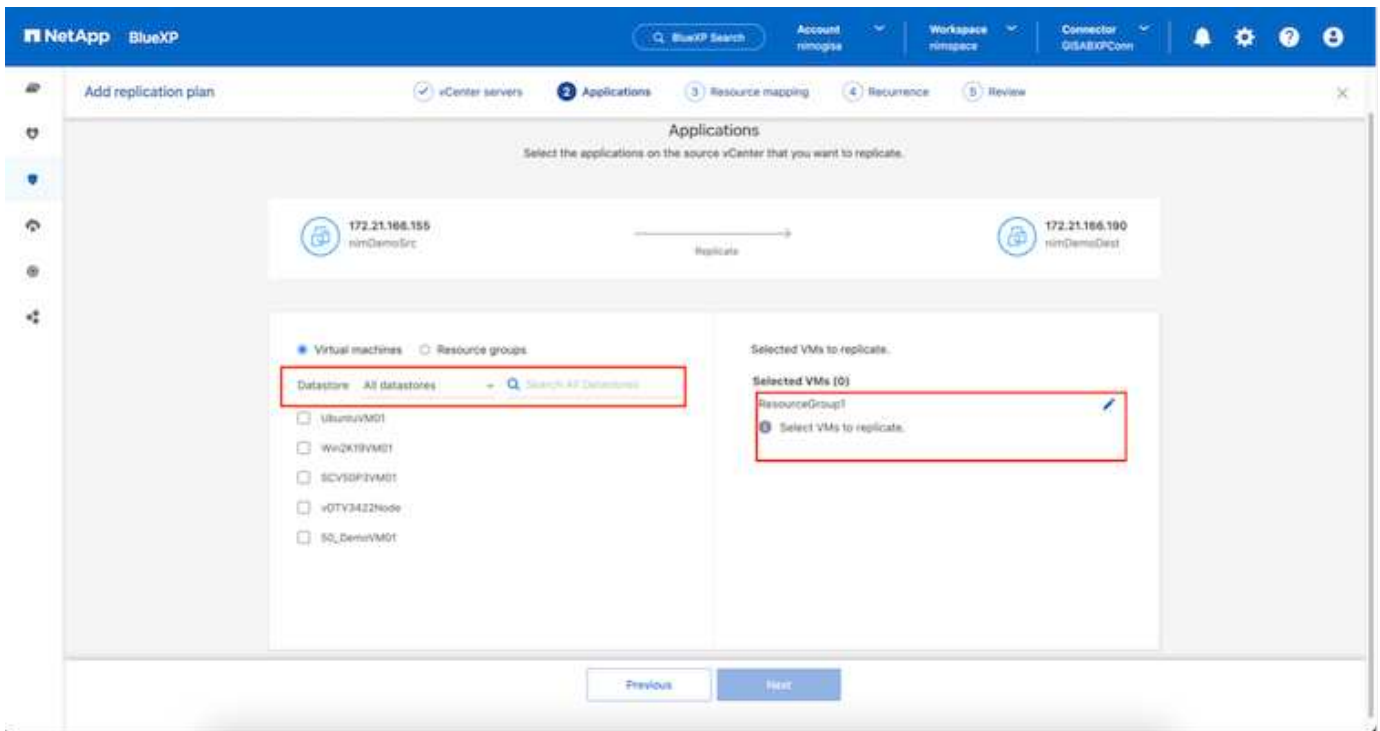


Le groupe de ressources permet de définir l'ordre de démarrage à l'aide de la fonctionnalité glisser-déposer. Il peut être utilisé pour modifier facilement l'ordre de mise sous tension des VM pendant le processus de restauration.

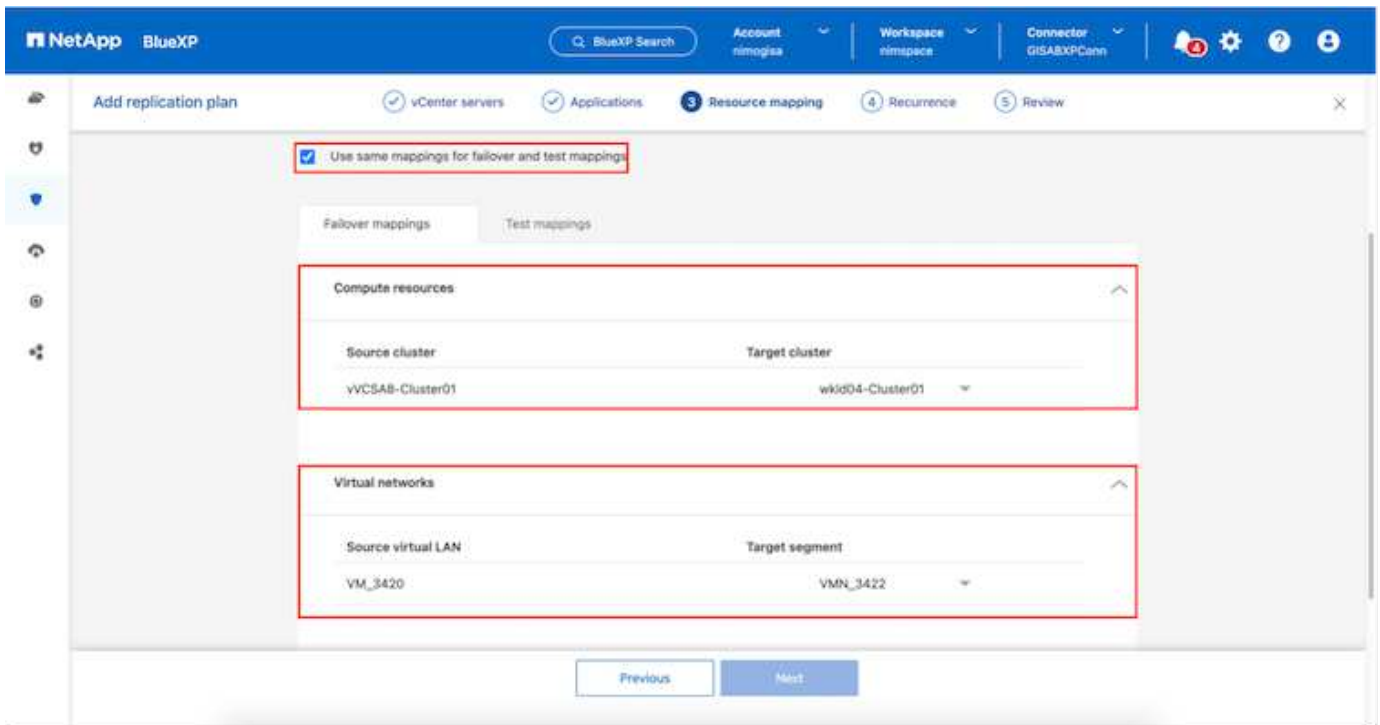


Chaque machine virtuelle au sein d'un groupe de ressources est démarrée dans l'ordre indiqué. Deux groupes de ressources sont démarrés en parallèle.

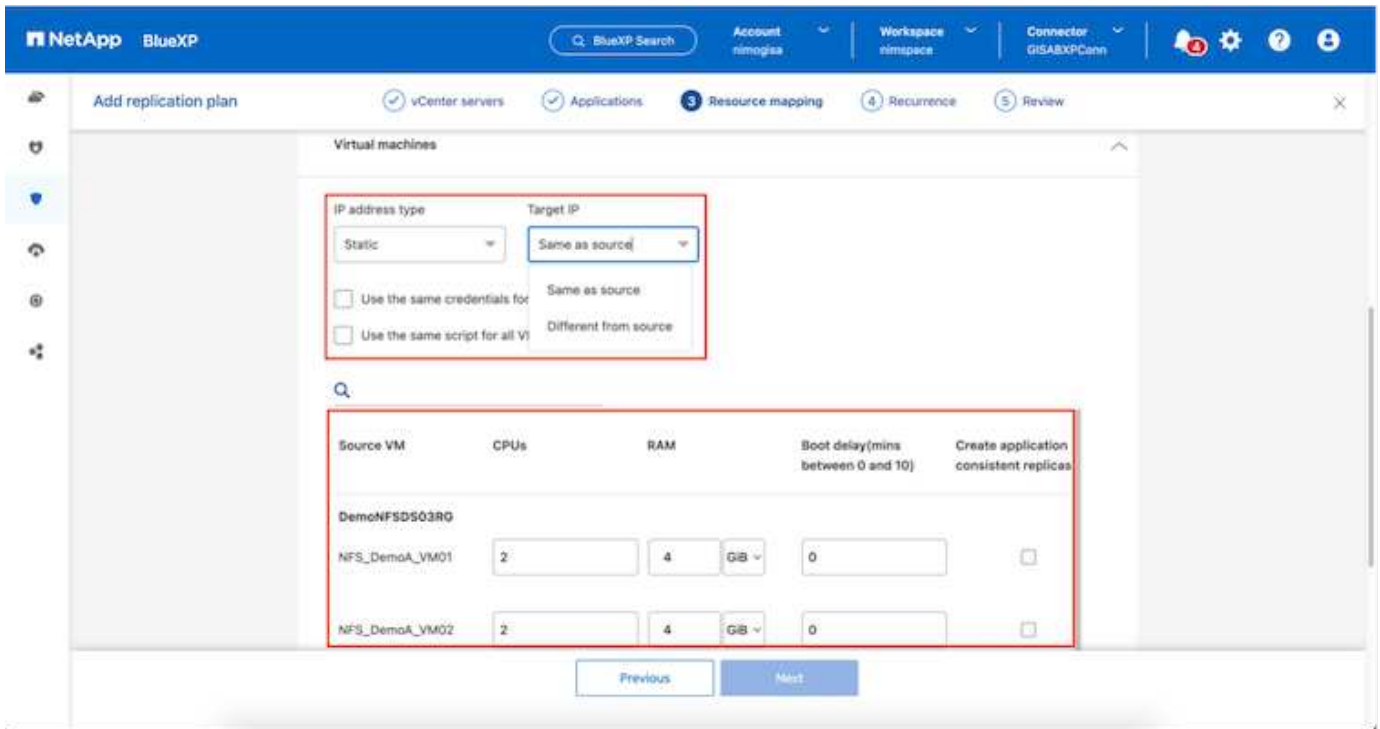
La capture d'écran ci-dessous présente l'option de filtrage des machines virtuelles ou des datastores spécifiques en fonction des besoins organisationnels si les groupes de ressources ne sont pas créés au préalable.



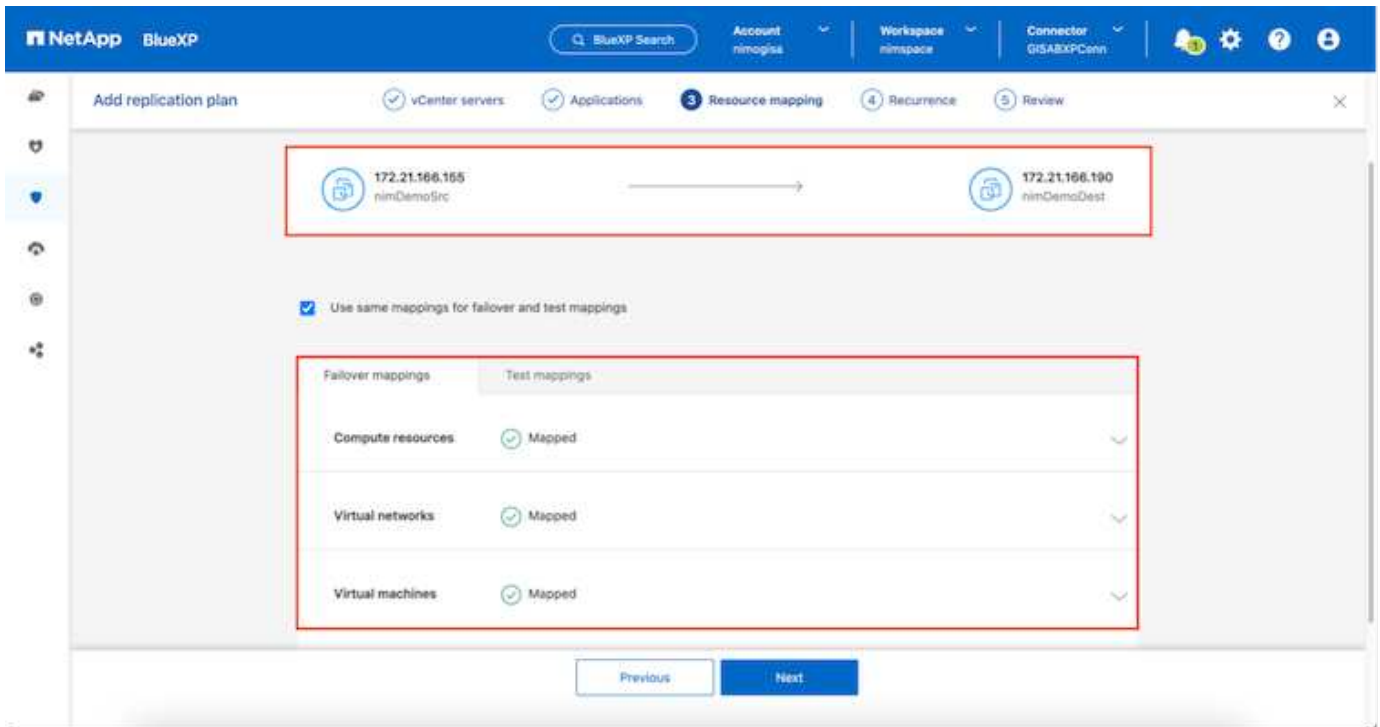
Une fois les groupes de ressources sélectionnés, créez les mappages de basculement. Dans cette étape, spécifiez la façon dont les ressources de l'environnement source sont mises en correspondance avec la destination. Cela inclut les ressources de calcul, les réseaux virtuels. Personnalisation IP, pré et post-scripts, délais de démarrage, cohérence des applications, etc. Pour plus d'informations, reportez-vous "[Créer un plan de réplication](#)" à la .



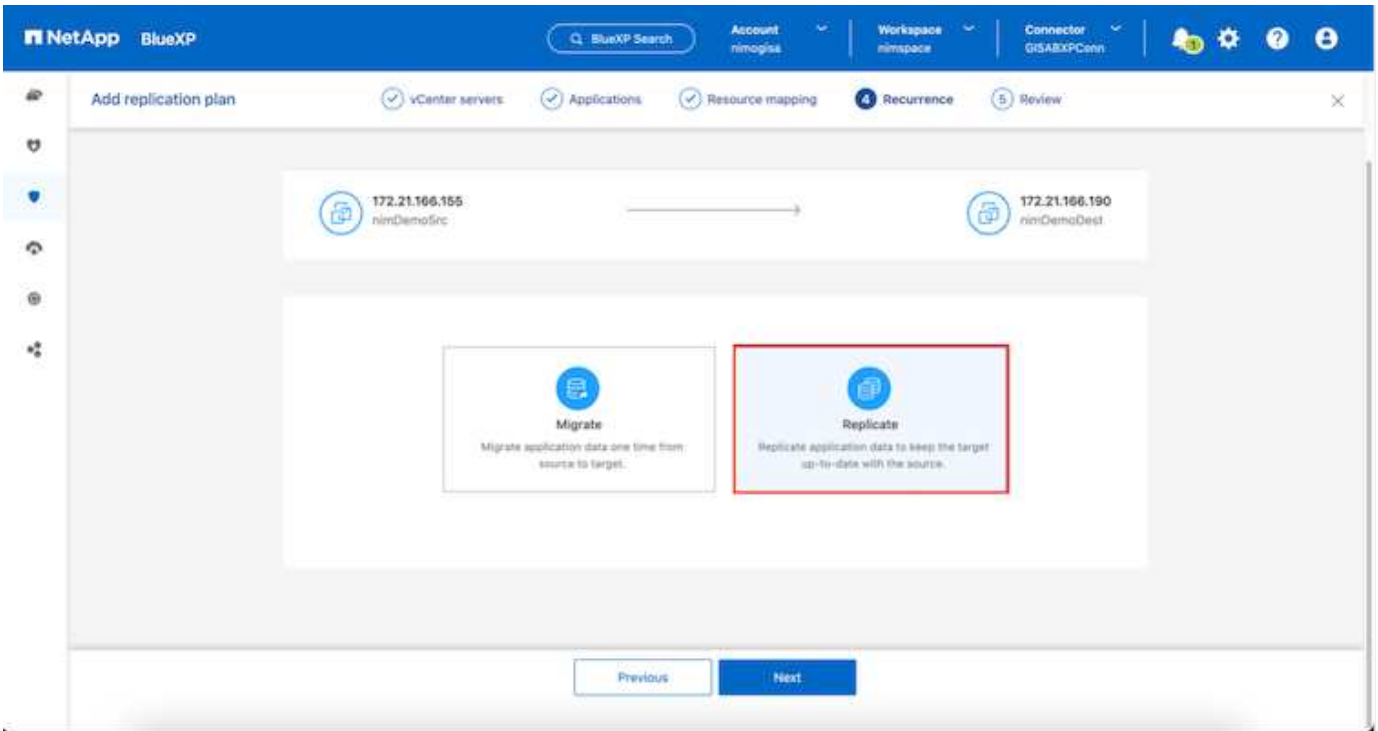
Par défaut, les mêmes paramètres de mappage sont utilisés pour les opérations de test et de basculement. Pour définir des mappages différents pour l'environnement de test, sélectionnez l'option Tester le mappage après avoir décochée la case comme indiqué ci-dessous :



Une fois le mappage des ressources terminé, cliquez sur Suivant.



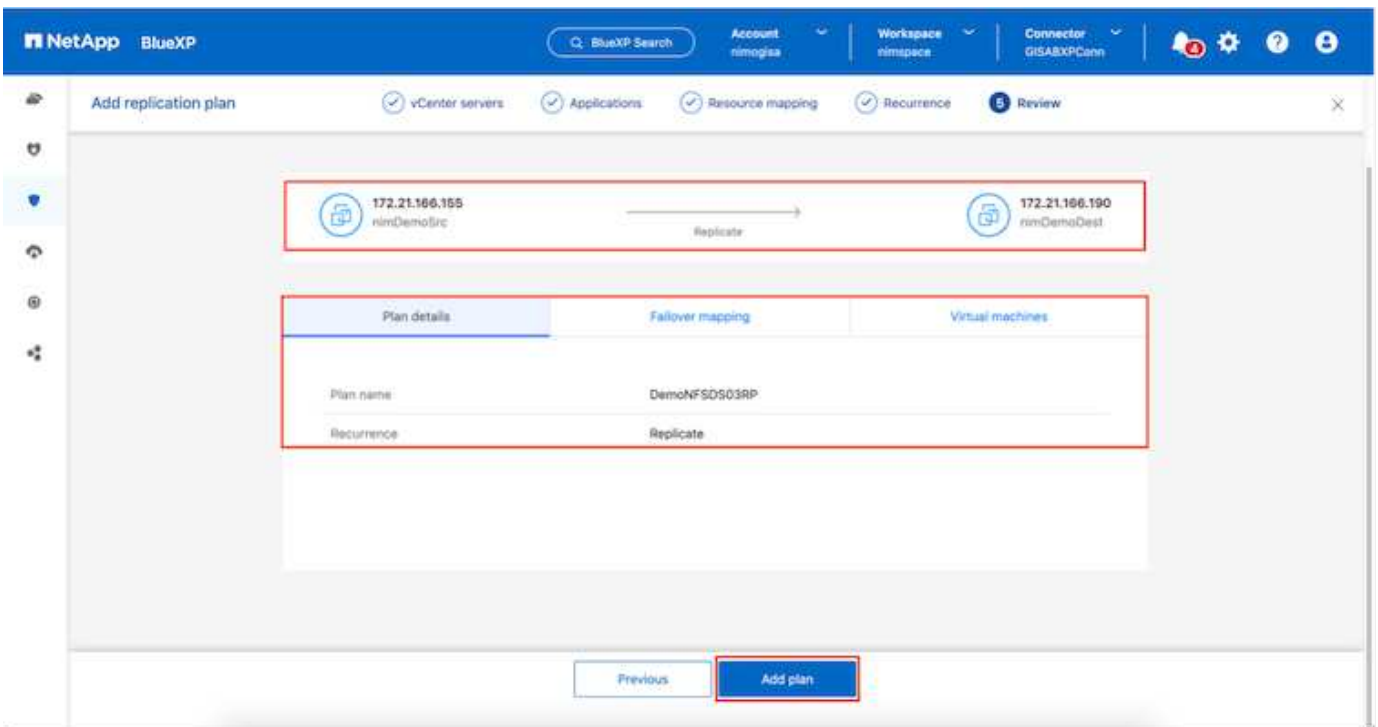
Sélectionnez le type de récurrence. En d'autres termes, sélectionnez Migrate (migration unique avec basculement) ou l'option de réplication continue récurrente. Dans cette procédure, l'option de réplication est sélectionnée.

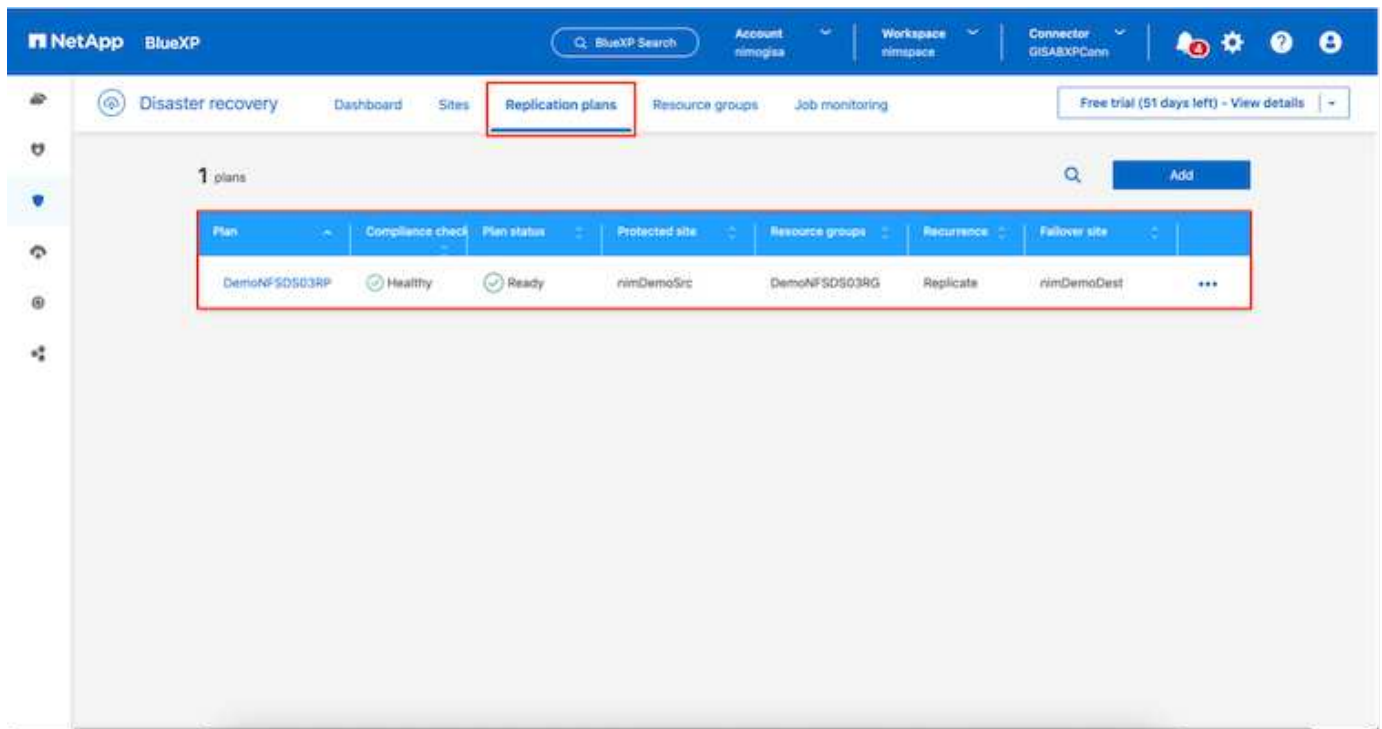


Une fois terminé, vérifiez les mappages créés, puis cliquez sur **Ajouter un plan**.



Un plan de réplication peut inclure les machines virtuelles de différents volumes et SVM. Selon le placement des machines virtuelles (que ce soit sur le même volume ou sur un volume distinct au sein du même SVM, des volumes distincts sur différents SVM), la reprise d'activité BlueXP crée une copie Snapshot de groupe de cohérence.



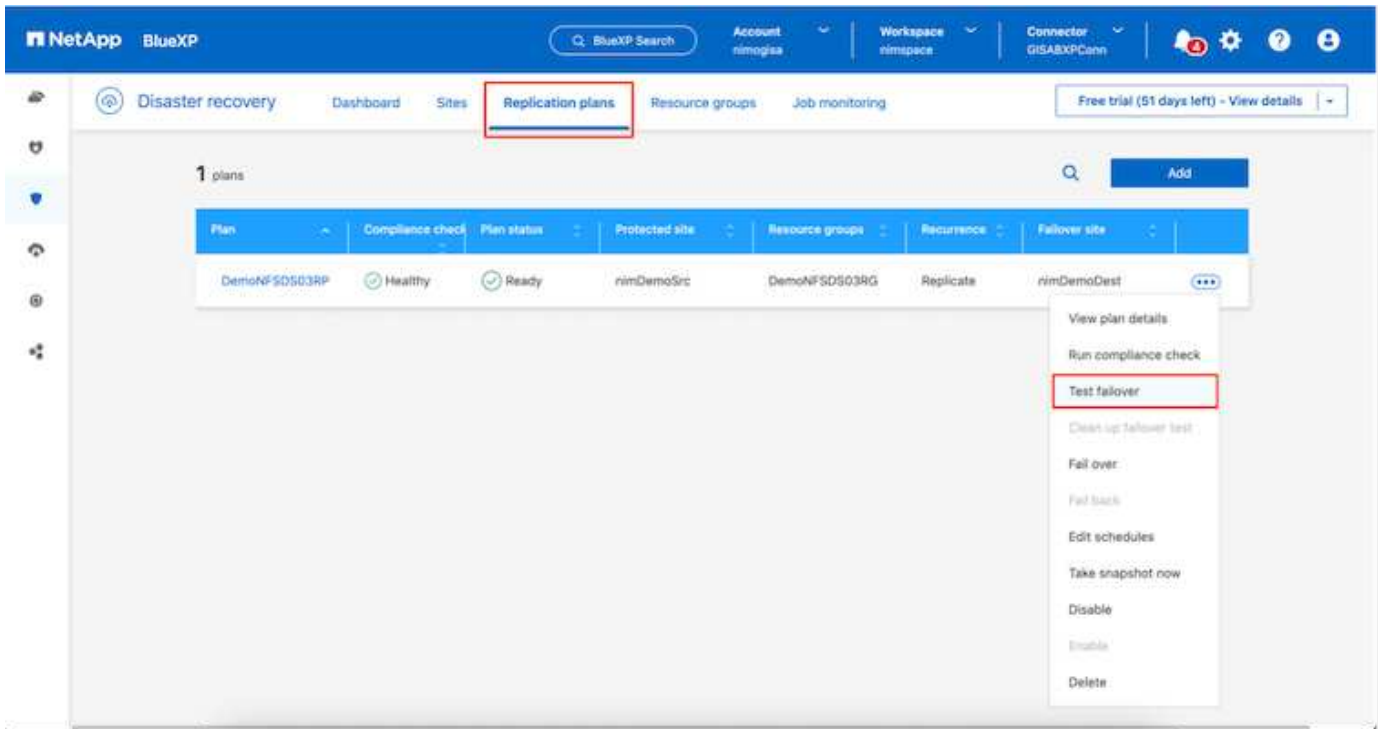


La DRaaS de BlueXP comprend les workflows suivants :

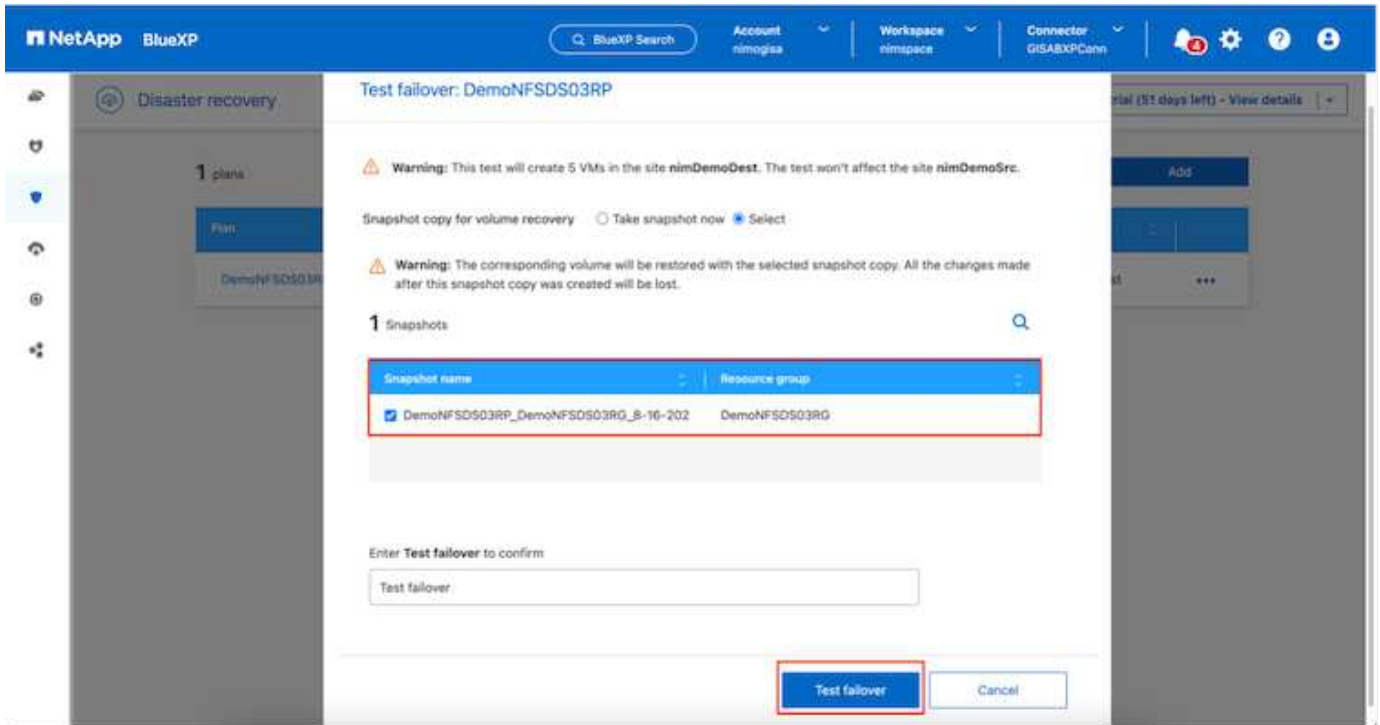
- Test du basculement (y compris simulations automatisées périodiques)
- Test de basculement de nettoyage
- Basculement
- Du rétablissement

Tester le basculement

Le basculement de test dans BlueXP DRaaS est une procédure opérationnelle qui permet aux administrateurs VMware de valider intégralement leurs plans de reprise d'activité sans perturber leurs environnements de production.



La DRaaS de BlueXP permet de sélectionner l'instantané en tant que fonctionnalité facultative lors de l'opération de test de basculement. Cette fonctionnalité permet à l'administrateur VMware de vérifier que toutes les modifications récemment apportées à l'environnement sont répliquées sur le site de destination et sont donc présentes pendant le test. Ces modifications incluent des correctifs pour le système d'exploitation invité de la machine virtuelle

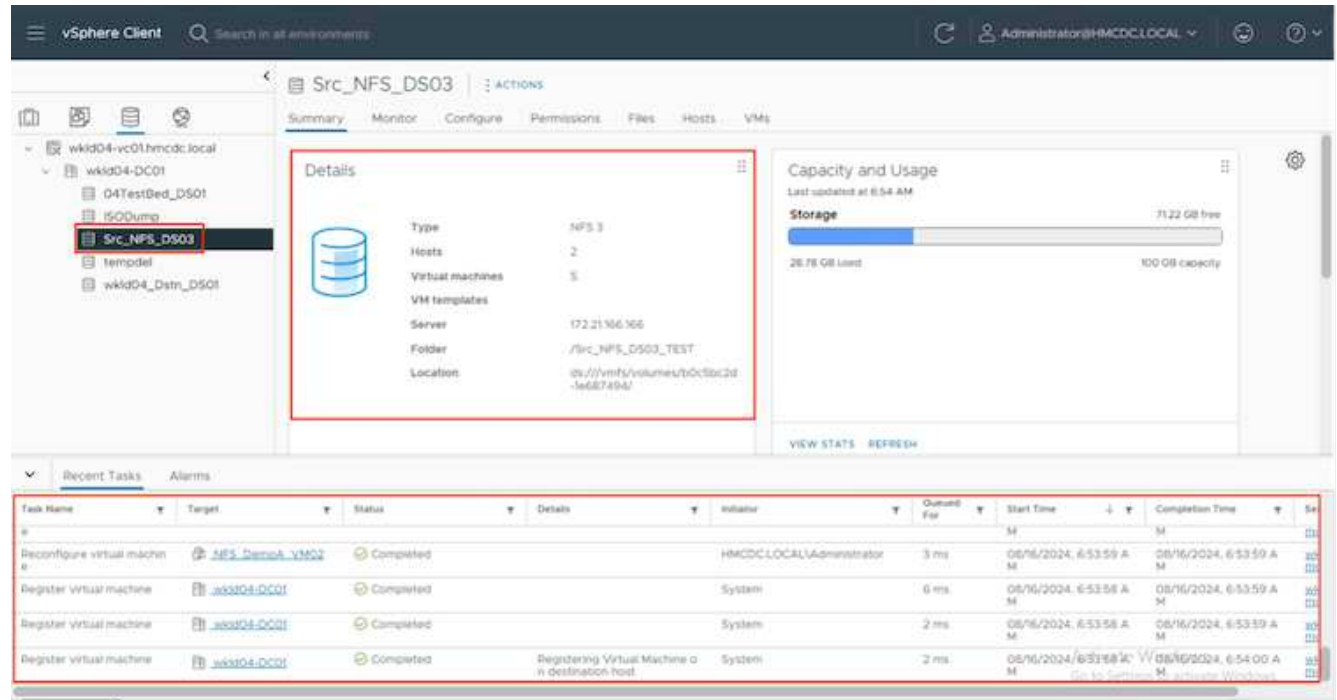


Lorsque l'administrateur VMware exécute une opération de basculement test, BlueXP DRaaS automatise les tâches suivantes :

- Déclenchement de relations SnapMirror pour mettre à jour le stockage sur le site de destination avec toute

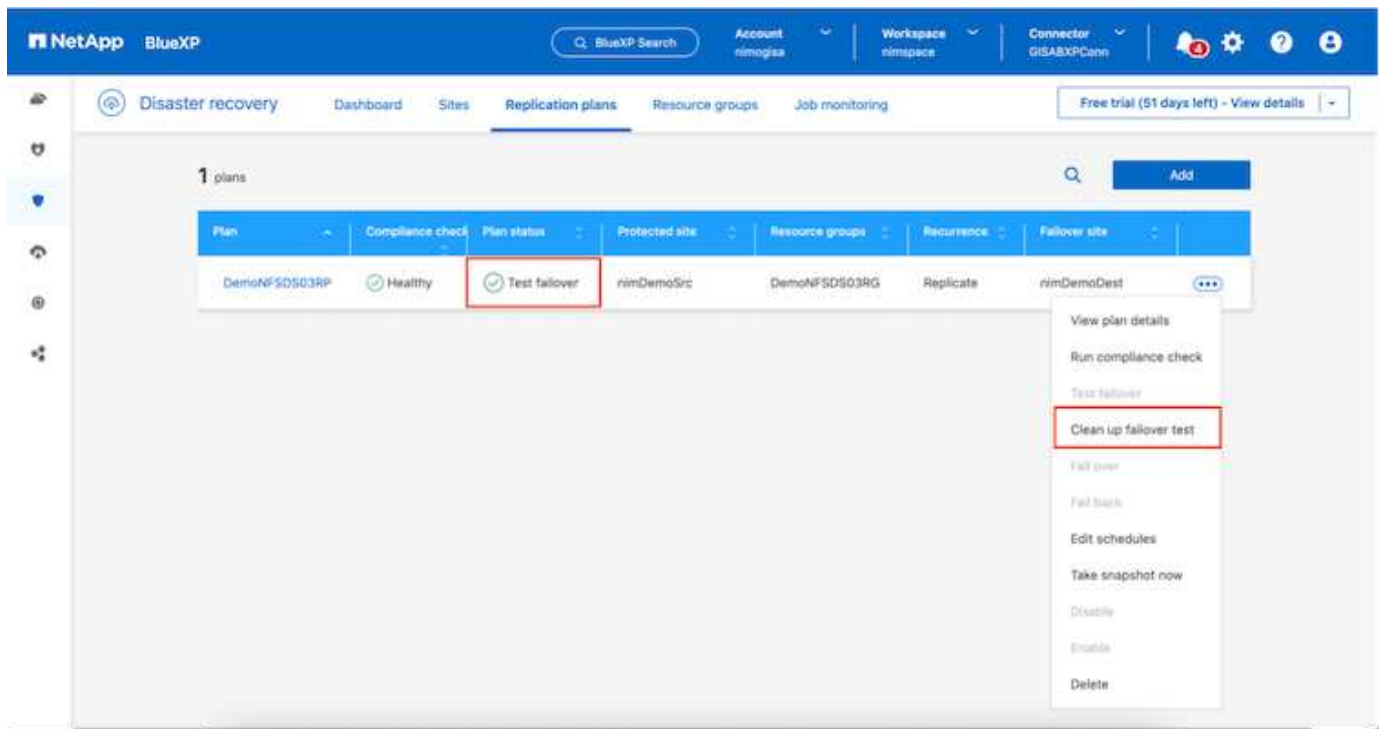
modification récente effectuée sur le site de production.

- Création des volumes NetApp FlexClone des volumes FlexVol sur la baie de stockage de reprise après incident.
- Connexion des datastores NFS des volumes FlexClone aux hôtes ESXi sur le site de reprise après incident.
- Connexion des adaptateurs réseau de la machine virtuelle au réseau de test spécifié lors du mappage.
- Reconfiguration des paramètres réseau du système d'exploitation invité de la machine virtuelle, comme défini pour le réseau sur le site de reprise après incident.
- Exécution des commandes personnalisées qui ont été stockées dans le plan de réplication.
- Mise sous tension des machines virtuelles dans l'ordre défini dans le plan de réplication.



Opération de test de basculement de nettoyage

L'opération de test de basculement de nettoyage a lieu une fois le test du plan de réplication terminé et l'administrateur VMware répond à l'invite de nettoyage.



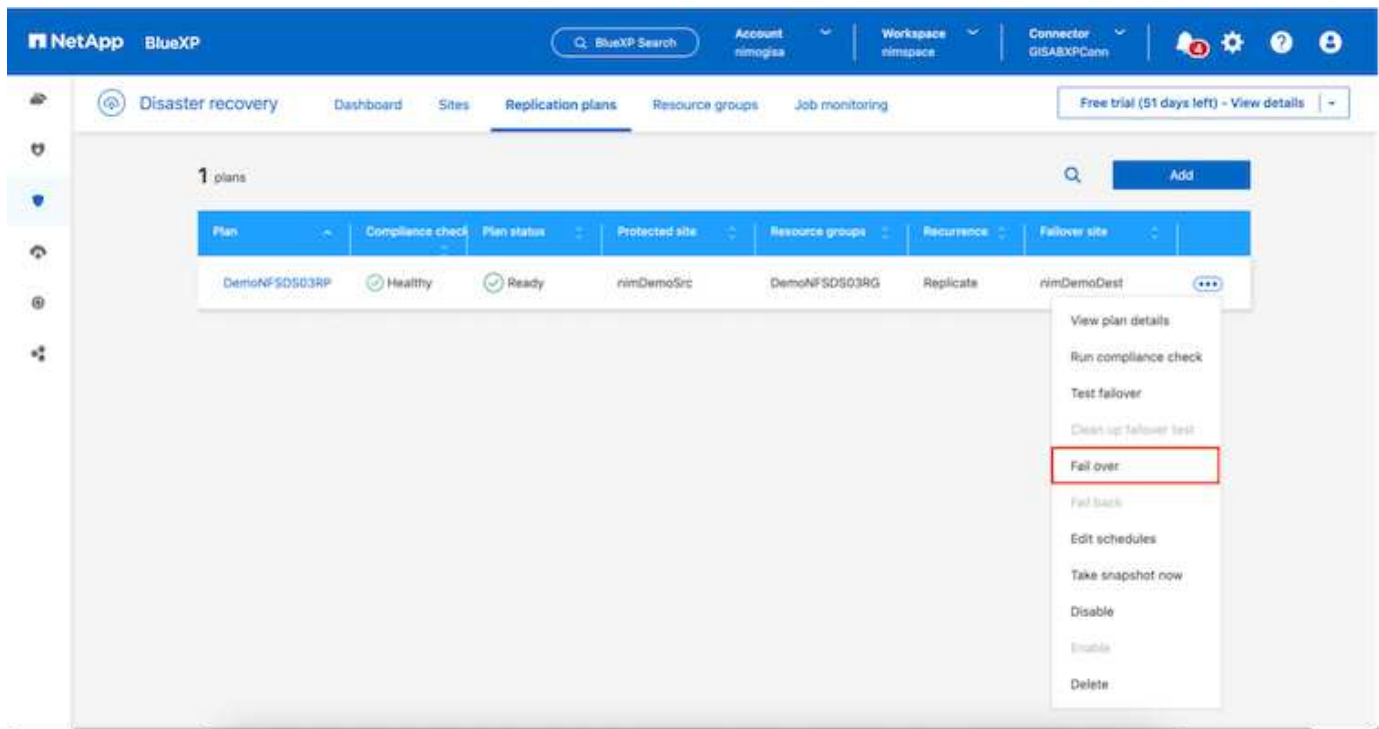
Cette action réinitialise les machines virtuelles (VM) et l'état du plan de réplication à l'état prêt.

Lorsque l'administrateur VMware effectue une opération de restauration, BlueXP DRaaS effectue le processus suivant :

1. Il met hors tension chaque VM restaurée dans la copie FlexClone qui a été utilisée à des fins de test.
2. Elle supprime le volume FlexClone utilisé pour présenter les VM restaurées pendant le test.

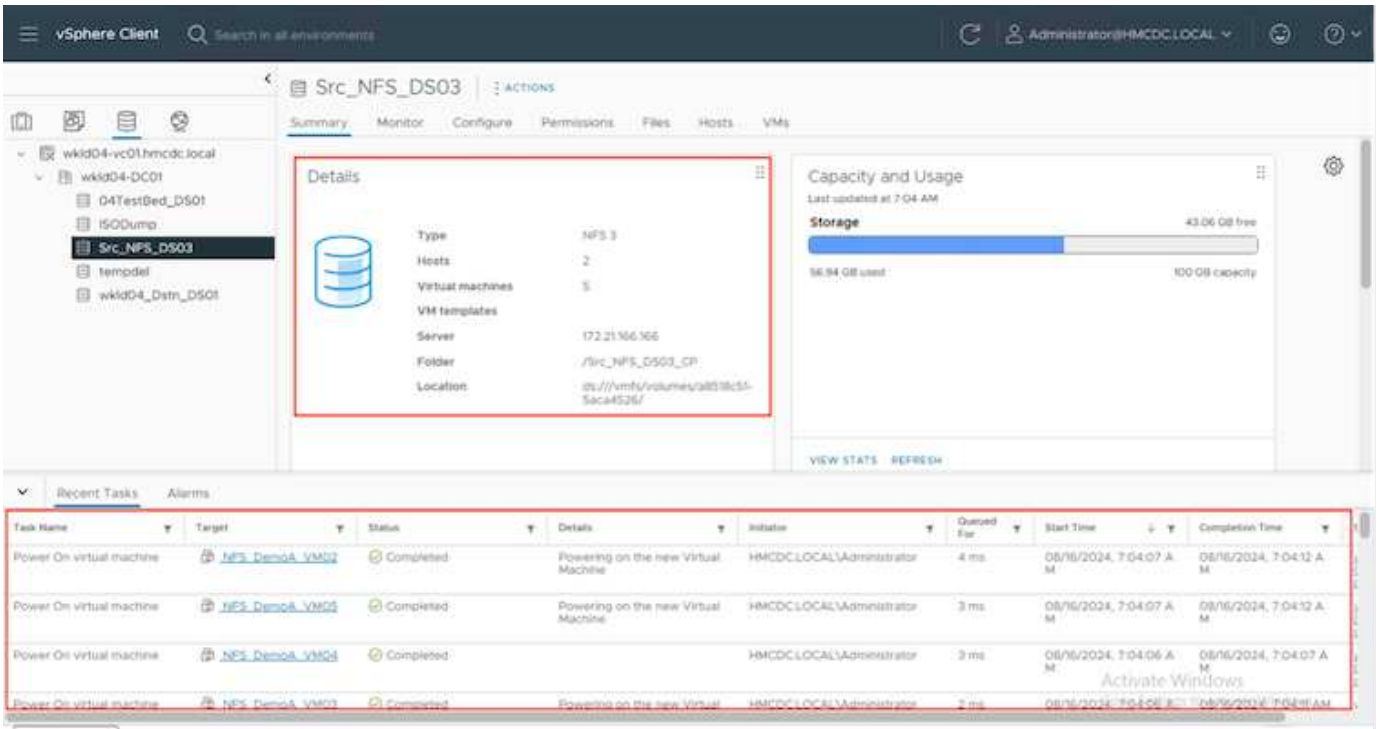
Migration planifiée et basculement

La DRaaS de BlueXP propose deux méthodes pour effectuer un vrai basculement : la migration planifiée et le basculement. La première méthode, la migration planifiée, intègre l'arrêt des ordinateurs virtuels et la synchronisation de la réplication du stockage dans le processus de restauration ou de déplacement efficace des ordinateurs virtuels vers le site de destination. La migration planifiée nécessite l'accès au site source. La seconde méthode, le basculement, est un basculement planifié/non planifié dans lequel les serveurs virtuels sont restaurés sur le site de destination à partir du dernier intervalle de réplication du stockage qui a pu se terminer. En fonction du RPO défini dans la solution, une perte de données peut être due à une certaine quantité dans le scénario de reprise d'activité.



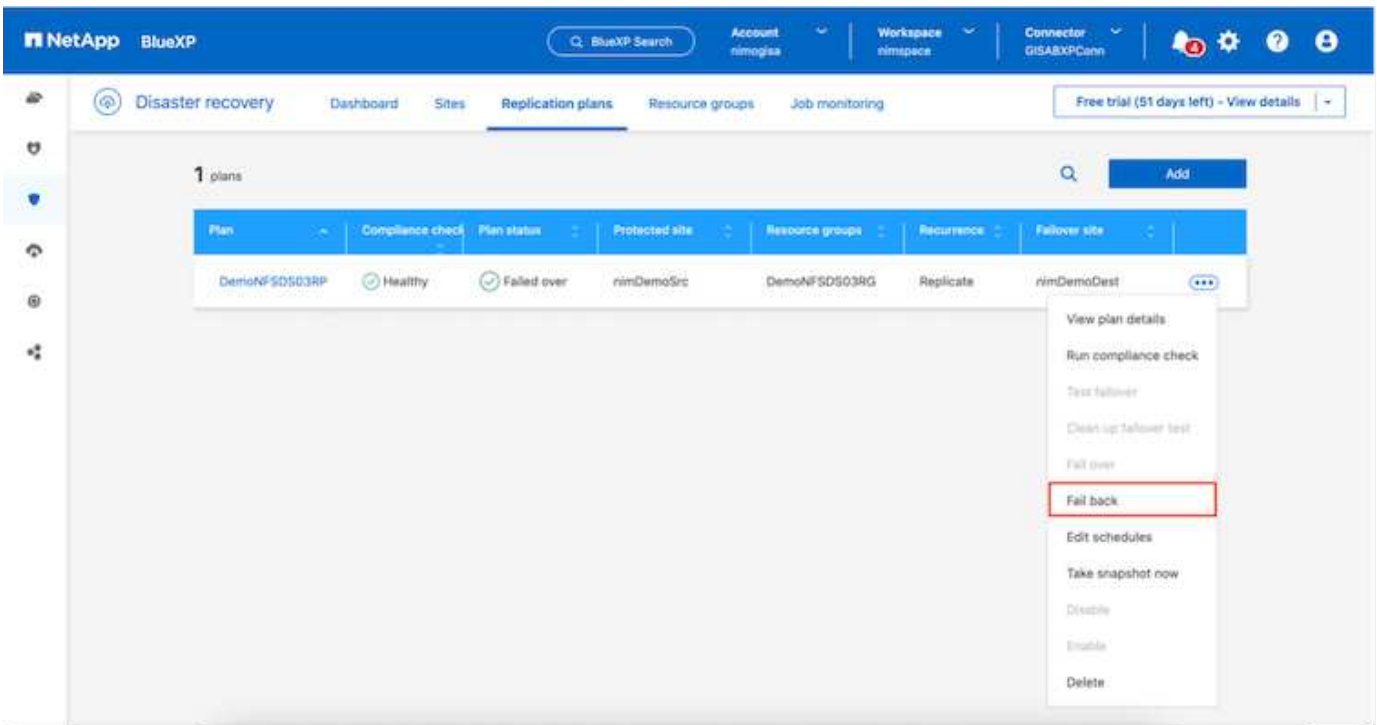
Lorsque l'administrateur VMware effectue une opération de basculement, BlueXP DRaaS automatise les tâches suivantes :

- Rompez et basculez les relations NetApp SnapMirror.
- Connecter les datastores NFS répliqués aux hôtes ESXi sur le site de reprise après incident.
- Connectez les adaptateurs réseau de la machine virtuelle au réseau du site de destination approprié.
- Reconfigurez les paramètres réseau du système d'exploitation invité de la machine virtuelle, tels que définis pour le réseau sur le site de destination.
- Exécutez toutes les commandes personnalisées (le cas échéant) qui ont été stockées dans le plan de réplication.
- Mettez les machines virtuelles sous tension dans l'ordre défini dans le plan de réplication.



Du rétablissement

Un retour arrière est une procédure facultative qui restaure la configuration d'origine des sites source et de destination après une restauration.



Les administrateurs VMware peuvent configurer et exécuter une procédure de restauration lorsqu'ils sont prêts à restaurer des services vers le site source d'origine.

REMARQUE : BlueXP DRaaS réplique (resyncs) les modifications apportées à la machine virtuelle source d'origine avant d'inverser le sens de la réplication. Ce processus commence à partir d'une relation qui a

terminé le basculement vers une cible et implique les étapes suivantes :

- Mettez hors tension et désenregistrez les machines virtuelles et les volumes sur le site de destination sont démontés.
- Interrompre la relation SnapMirror sur la source d'origine est rompue pour la faire en lecture/écriture.
- Resynchronisez la relation SnapMirror pour annuler la réplication.
- Montez le volume sur la source, mettez-le sous tension et enregistrez les machines virtuelles sources.

Pour plus d'informations sur l'accès et la configuration de BlueXP DRaaS, consultez le "[Découvrez la reprise d'activité BlueXP pour VMware](#)".

Surveillance et tableau de bord

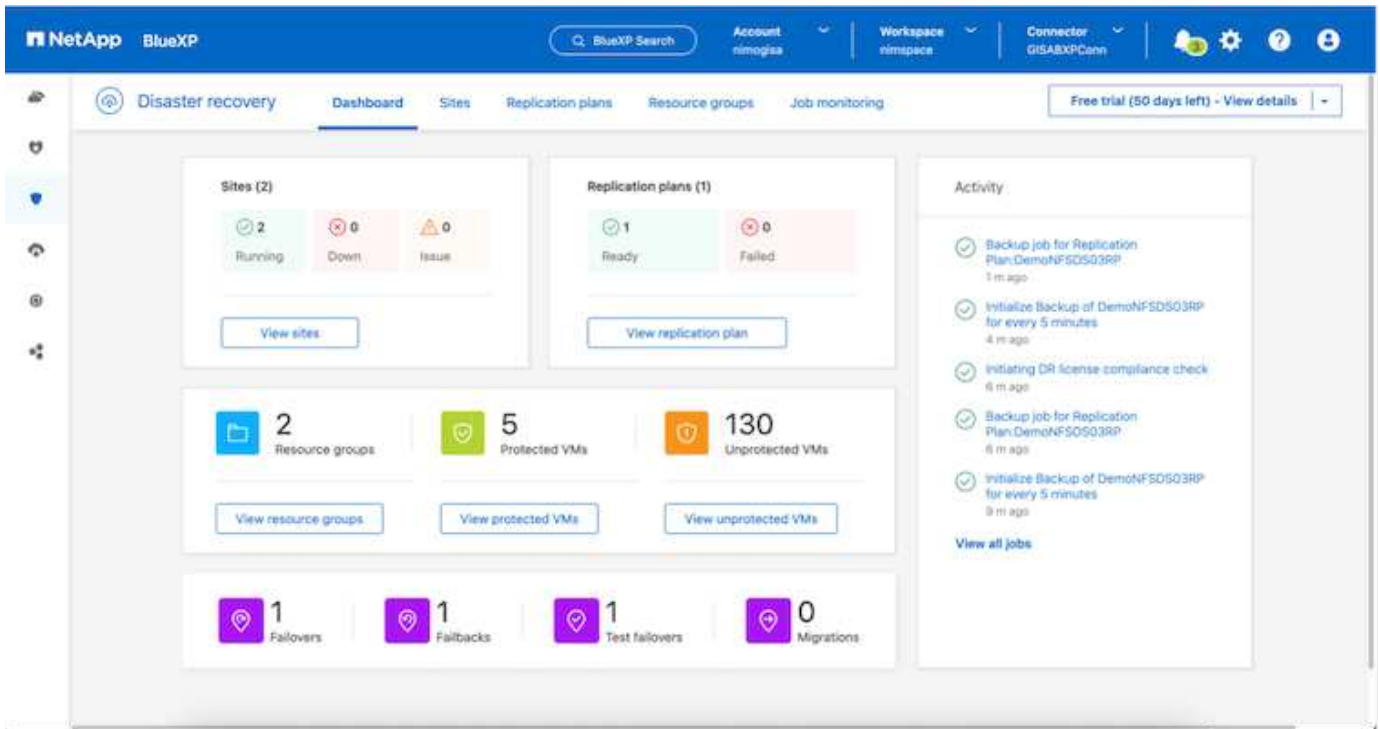
À partir de BlueXP ou de l'interface de ligne de commandes de ONTAP, vous pouvez contrôler l'état de la réplication pour les volumes de datastore appropriés. Vous pouvez également suivre l'état d'un basculement ou d'un basculement de test via la surveillance des tâches.

ID	Status	Workload	Name	Start time	End time	
d923e507-b2c2-401	In pro...	Backup	Backup job for Replication Plan:DemoNF...	08/16/2024, 04:5...	-	Cancel job?
3549cc9c-aa4e-45e	Succe...	Backup	Initialize Backup of DemoNFSDS03RP for...	08/16/2024, 04:5...	08/16/2024, 04:5...	
5cb01bcc-9ea6-4af1	Succe...	Backup	Backup job for Replication Plan:DemoNF...	08/16/2024, 04:4...	08/16/2024, 04:5...	
a21225d9-b7be-4c2f	Succe...	Backup	Initialize Backup of DemoNFSDS03RP for...	08/16/2024, 04:4...	08/16/2024, 04:4...	
2f8b44d4-4be2-46e	Succe...	Compliance	Compliance check for Replication Plan: D...	08/16/2024, 04:4...	08/16/2024, 04:4...	
398bc6a3-afa8-48d	Succe...	Compliance	Initialize Compliance of DemoNFSDS03R...	08/16/2024, 04:4...	08/16/2024, 04:4...	
97f1bed8-6f77-459f	Succe...	Backup	Backup job for Replication Plan:DemoNF...	08/16/2024, 04:4...	08/16/2024, 04:4...	
bffc018e-ca3a-409d	Succe...	Backup	Initialize Backup of DemoNFSDS03RP for...	08/16/2024, 04:4...	08/16/2024, 04:4...	
cde759a8-ebef-498e	Succe...	Backup	Backup job for Replication Plan:DemoNF...	08/16/2024, 04:3...	08/16/2024, 04:4...	
a414daba-8630-4c5	Succe...	Backup	Initialize Backup of DemoNFSDS03RP for...	08/16/2024, 04:3...	08/16/2024, 04:3...	



Si un travail est en cours ou en file d'attente et que vous souhaitez l'arrêter, il existe une option pour l'annuler.

Évaluez en toute confiance l'état des sites de reprise d'activité et des plans de réplication avec le tableau de bord de reprise d'activité BlueXP . Les administrateurs peuvent ainsi identifier rapidement les sites et les plans sains, déconnectés ou dégradés.



Il s'agit d'une solution puissante permettant de gérer un plan de reprise d'activité personnalisé. Le basculement peut s'effectuer en cas de basculement planifié ou de basculement d'un simple clic en cas d'incident et si la décision d'activer le site de reprise est prise.

Pour en savoir plus sur ce processus, n'hésitez pas à suivre la vidéo de présentation détaillée ou à utiliser le ["simulateur de solution"](#).

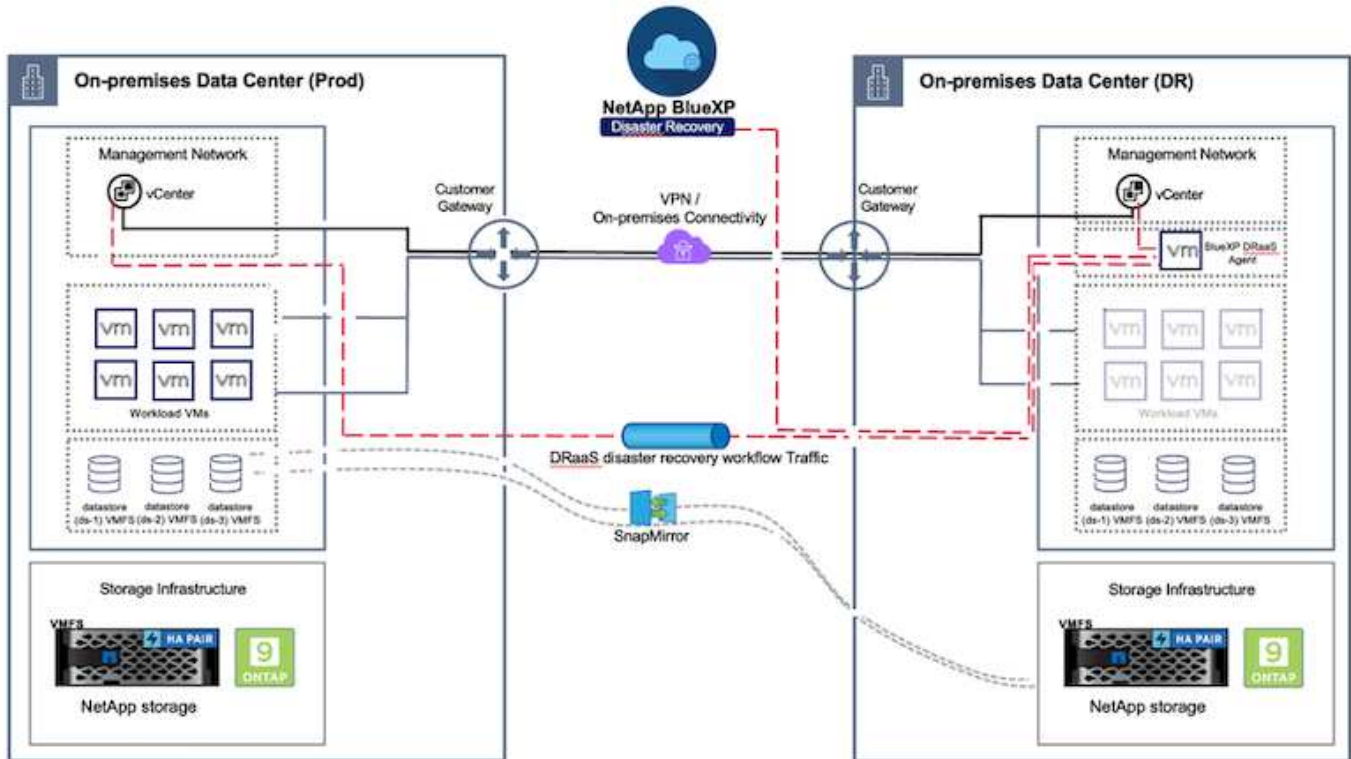
Reprise après incident à l'aide de la DRaaS BlueXP pour les datastores VMFS

La reprise d'activité, grâce à la réplication au niveau des blocs entre le site de production et le site de reprise d'activité, est un moyen résilient et économique de protéger les workloads contre les pannes sur site et les corruptions de données, telles que les attaques par ransomware. Avec la réplication NetApp SnapMirror, les workloads VMware qui exécutent des systèmes ONTAP sur site utilisant un datastore VMFS peuvent être répliqués sur un autre système de stockage ONTAP dans un data Center de restauration désigné où réside VMware

Cette section du document décrit la configuration de la DRaaS BlueXP pour la configuration de la reprise après incident pour les machines virtuelles VMware sur site sur un autre site désigné. Dans le cadre de cette configuration, le compte BlueXP, BlueXP Connector, les baies ONTAP ajoutées dans l'espace de travail BlueXP, qui est nécessaire pour permettre la communication de VMware vCenter vers le stockage ONTAP. En outre, ce document explique en détail comment configurer la réplication entre les sites et comment configurer et tester un plan de reprise d'activité. La dernière section contient les instructions permettant d'effectuer un basculement de site complet et de revenir en arrière lorsque le site principal est récupéré et acheté en ligne.

Grâce au service de reprise après incident BlueXP intégré à la console NetApp BlueXP, les clients peuvent découvrir leurs vCenters VMware sur site avec le stockage ONTAP, créer des regroupements de ressources, créer un plan de reprise après incident, l'associer à des groupes de ressources et tester ou exécuter le basculement et la restauration. SnapMirror assure la réplication des blocs au niveau du stockage afin de maintenir les deux sites à jour avec des modifications incrémentielles. Le RPO peut atteindre 5 minutes. Il est également possible de simuler des procédures de reprise après incident comme une analyse régulière, sans

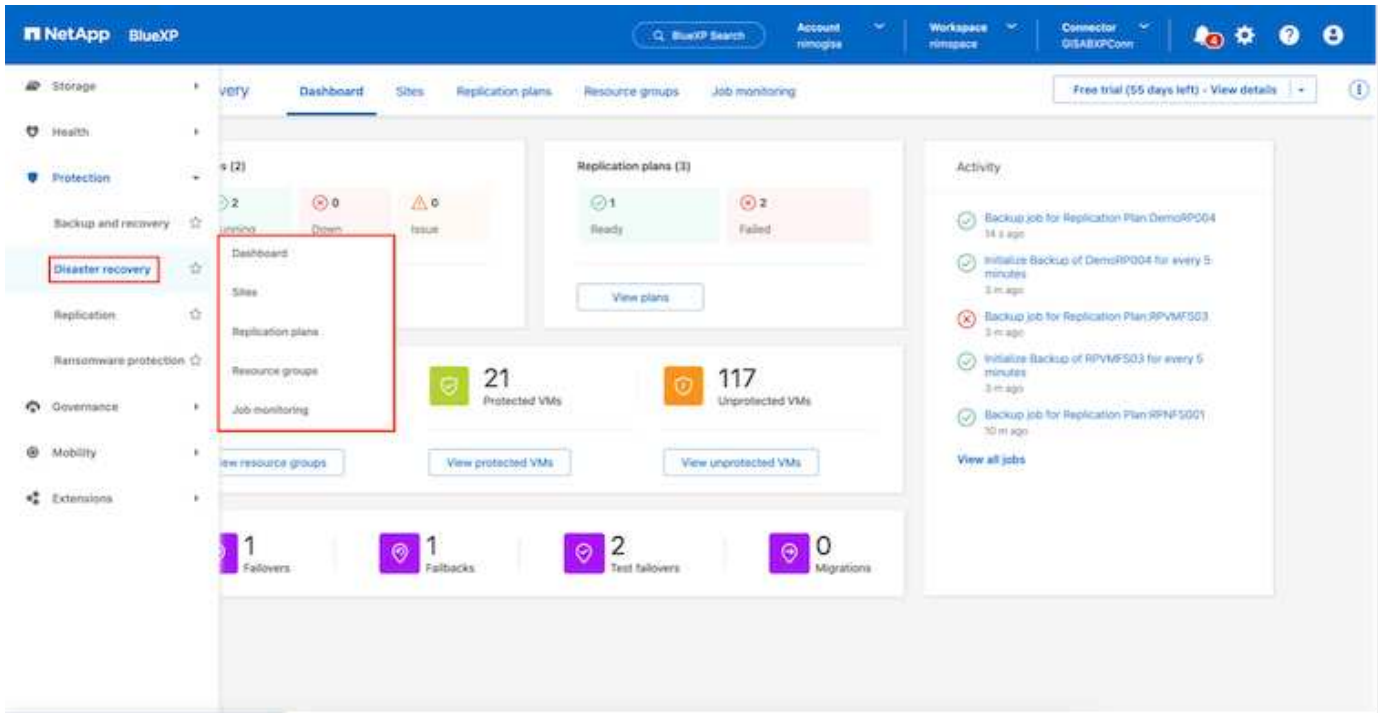
impact sur la production et les datastores répliqués, ni coûts de stockage supplémentaires. La reprise d'activité BlueXP tire parti de la technologie FlexClone de ONTAP pour créer une copie compacte du datastore VMFS à partir du dernier Snapshot répliqué sur le site de reprise après incident. Une fois le test de reprise après incident terminé, il vous suffit de supprimer l'environnement de test, une fois encore, sans impact sur les ressources de production réellement répliquées. Lorsqu'un basculement réel est nécessaire (planifié ou non), en quelques clics, le service de reprise d'activité BlueXP orchestre toutes les étapes nécessaires pour intégrer automatiquement les machines virtuelles protégées sur le site de reprise d'activité désigné. Le service inverse également la relation SnapMirror sur le site principal et réplique les modifications du stockage secondaire au stockage primaire dans le cadre d'une opération de restauration, le cas échéant. Tous ces objectifs peuvent être atteints avec un coût moindre par rapport à d'autres solutions bien connues.



Pour commencer

Pour commencer à utiliser la reprise après incident BlueXP, utilisez la console BlueXP, puis accédez au service.

1. Connectez-vous à BlueXP.
2. Dans le menu de navigation de gauche de BlueXP, sélectionnez protection > reprise après incident.
3. Le tableau de bord de reprise après incident de BlueXP s'affiche.



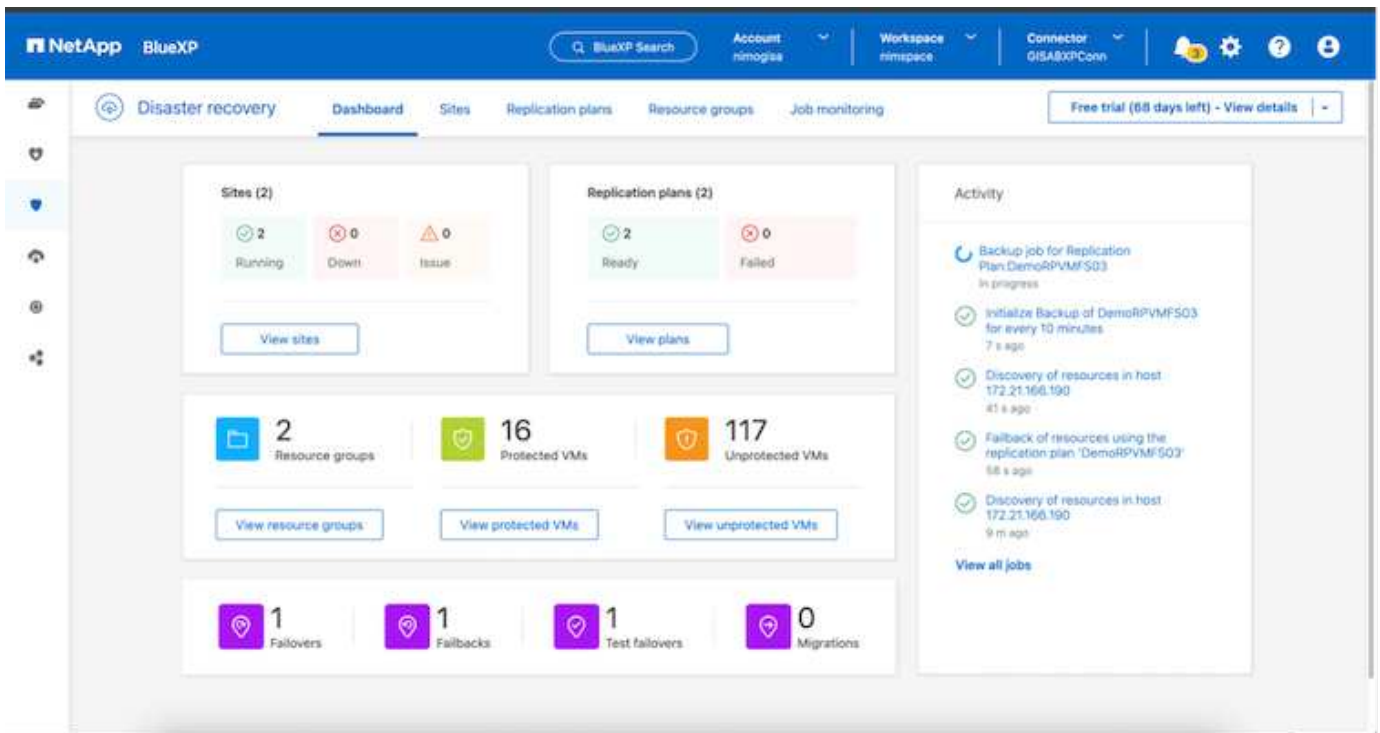
Avant de configurer le plan de reprise sur incident, assurez-vous que les conditions préalables suivantes sont remplies :

- Le connecteur BlueXP est configuré dans NetApp BlueXP . Le connecteur doit être déployé dans le VPC AWS.
- L'instance BlueXP Connector est connectée aux systèmes vCenter et de stockage source et de destination.
- Les systèmes de stockage NetApp sur site hébergeant des datastores VMFS pour VMware sont ajoutés à BlueXP .
- La résolution DNS doit être en place lors de l'utilisation de noms DNS. Sinon, utilisez les adresses IP pour vCenter.
- La réplication SnapMirror est configurée pour les volumes de datastores VMFS désignés.

Une fois la connectivité établie entre les sites source et de destination, procédez aux étapes de configuration qui doivent prendre entre 3 et 5 minutes.



NetApp recommande de déployer BlueXP Connector sur le site de reprise après incident ou dans un troisième site, afin que BlueXP Connector puisse communiquer via le réseau avec les ressources source et de destination en cas de pannes réelles ou de catastrophes naturelles.



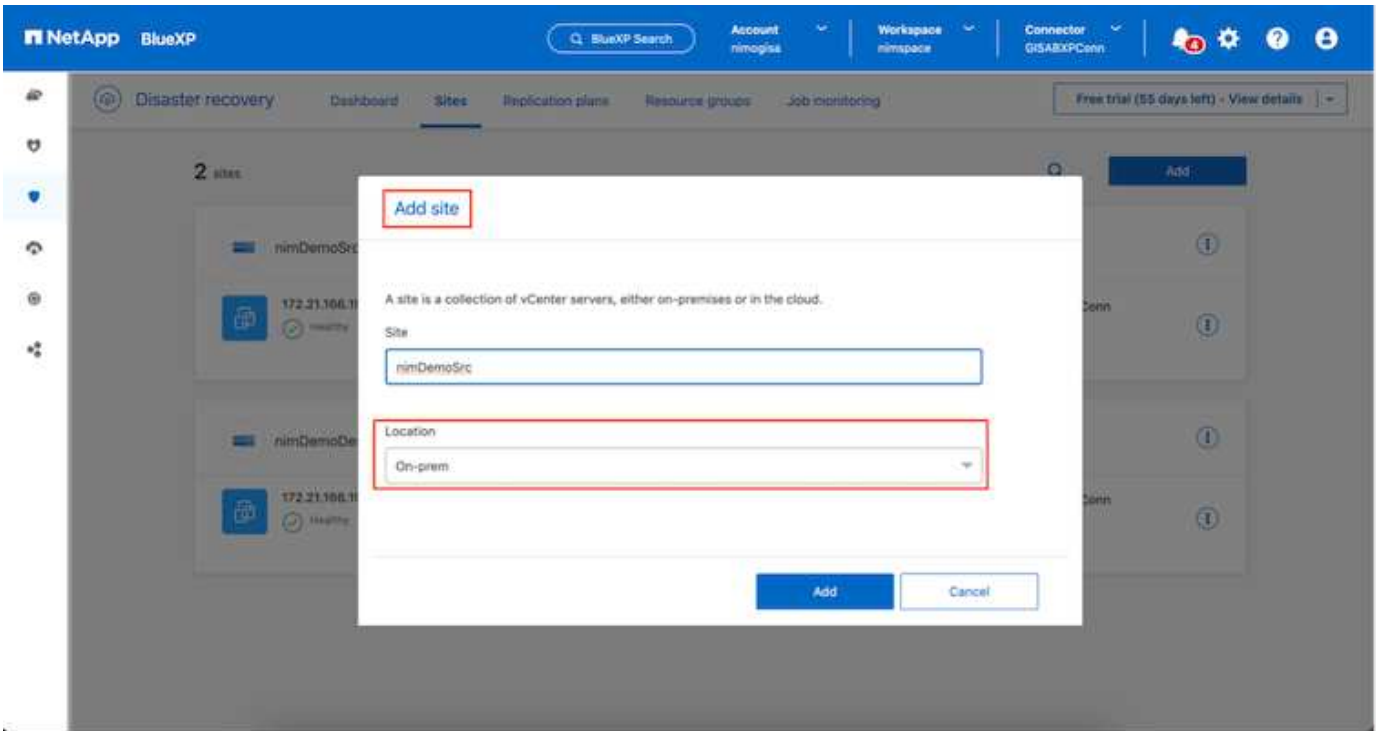
La prise en charge des datastores VMFS sur site et sur site est disponible en préversion technologique lors de la rédaction de ce document. Cette fonctionnalité est prise en charge avec les datastores VMFS basés sur le protocole FC et iSCSI.

Configuration de la reprise sur incident BlueXP

Pour préparer la reprise d'activité, la première étape consiste à découvrir et à ajouter les ressources vCenter et de stockage sur site à la reprise d'activité BlueXP .

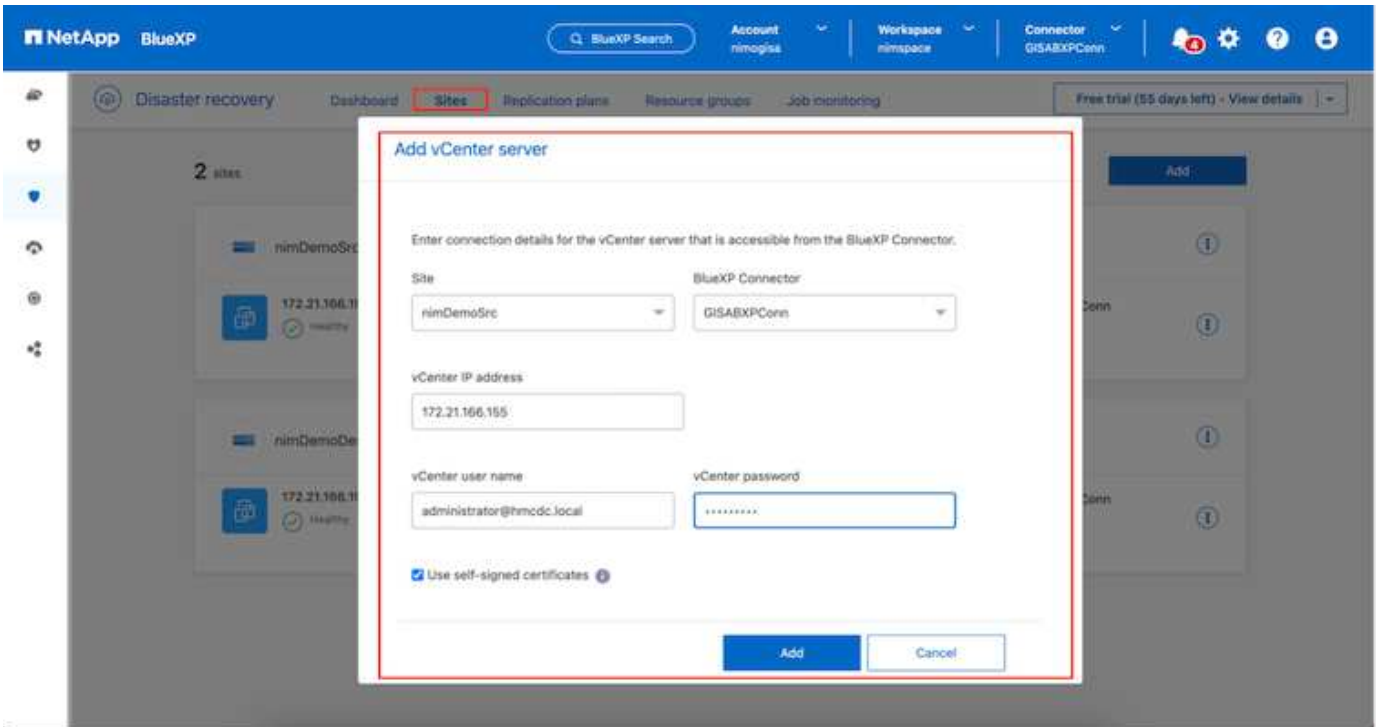


Assurez-vous que les systèmes de stockage ONTAP sont ajoutés à l'environnement de travail dans le canevas. Ouvrez la console BlueXP et sélectionnez **protection > récupération après sinistre** dans le menu de navigation de gauche. Sélectionnez **découvrir les serveurs vCenter** ou utilisez le menu supérieur, sélectionnez **sites > Ajouter > Ajouter vCenter**.

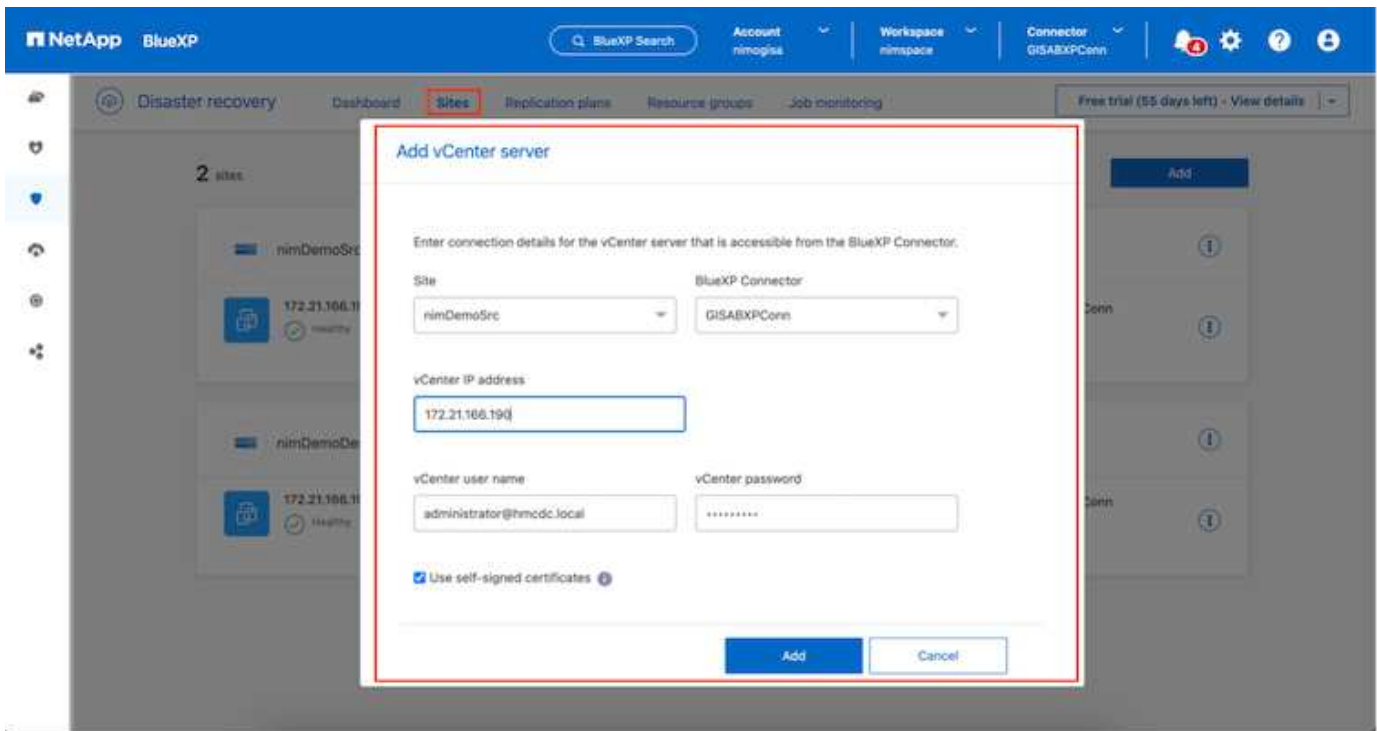


Ajoutez les plates-formes suivantes :

- **Source.** VCenter sur site



- **Destination.** VMC SDDC vCenter



Une fois les vCenters ajoutés, la découverte automatisée est déclenchée.

Configuration de la réplication de stockage entre le site source et le site de destination

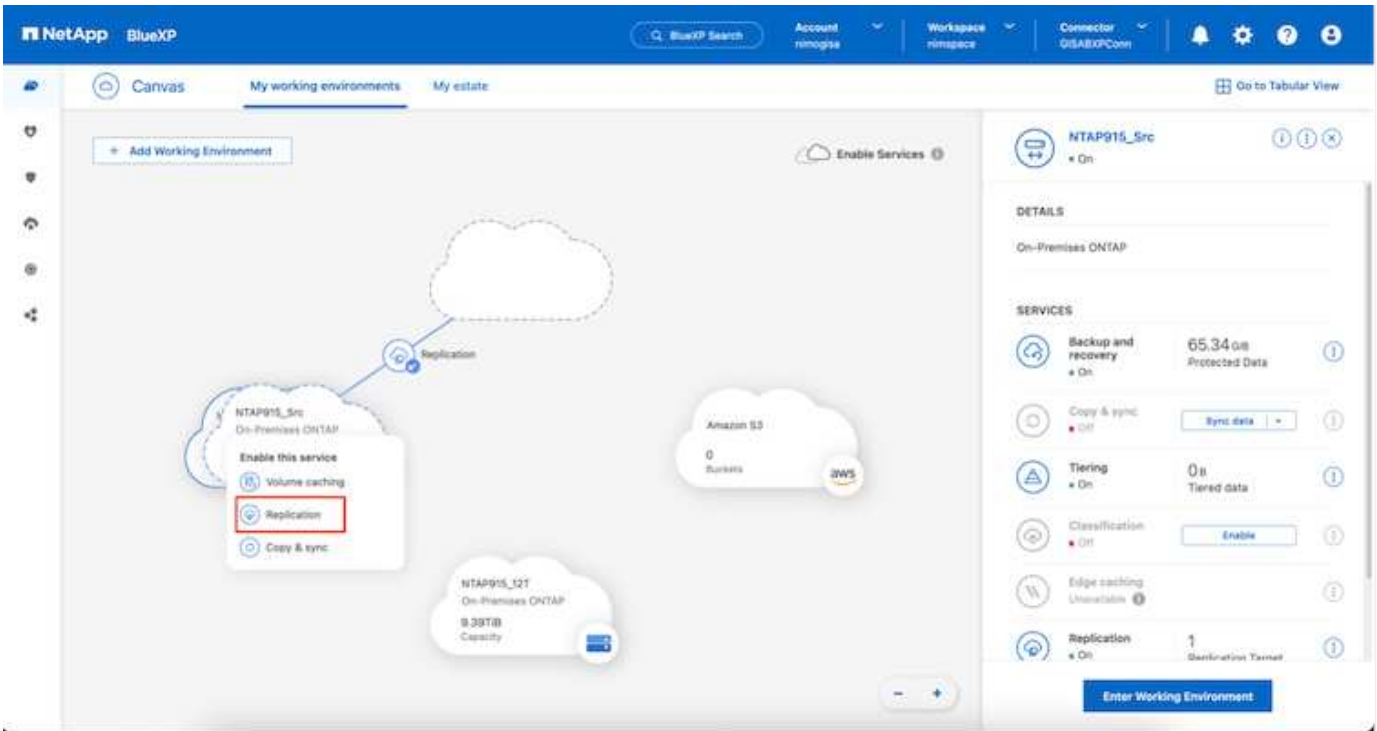
SnapMirror utilise les snapshots ONTAP pour gérer le transfert de données d'un emplacement à un autre. Initialement, une copie complète basée sur un snapshot du volume source est copiée vers la destination pour effectuer une synchronisation de base. À mesure que des modifications des données se produisent à la source, un nouvel instantané est créé et comparé au snapshot de référence. Les blocs modifiés sont ensuite répliqués vers la destination, le nouveau snapshot devenant la référence actuelle, ou le snapshot commun le plus récent. Cela permet de répéter le processus et d'envoyer des mises à jour incrémentielles vers la destination.

Lorsqu'une relation SnapMirror a été établie, le volume de destination est en lecture seule en ligne et reste donc accessible. SnapMirror fonctionne avec des blocs de stockage physiques, plutôt qu'au niveau d'un fichier ou d'un autre niveau logique. Cela signifie que le volume de destination est une réplique identique de la source, y compris les snapshots, les paramètres des volumes, etc. Si des fonctionnalités d'efficacité de l'espace ONTAP, telles que la compression des données et la déduplication des données, sont utilisées par le volume source, le volume répliqué conservera ces optimisations.

Une rupture de la relation SnapMirror rend le volume de destination inscriptible. En général, il serait utilisé pour effectuer un basculement lorsque SnapMirror est utilisé pour synchroniser les données vers un environnement de reprise d'activité. SnapMirror est suffisamment sophistiqué pour permettre de resynchroniser efficacement les données modifiées sur le site de basculement vers le système principal, si elles sont par la suite reconnectées, puis de rétablir la relation SnapMirror d'origine.

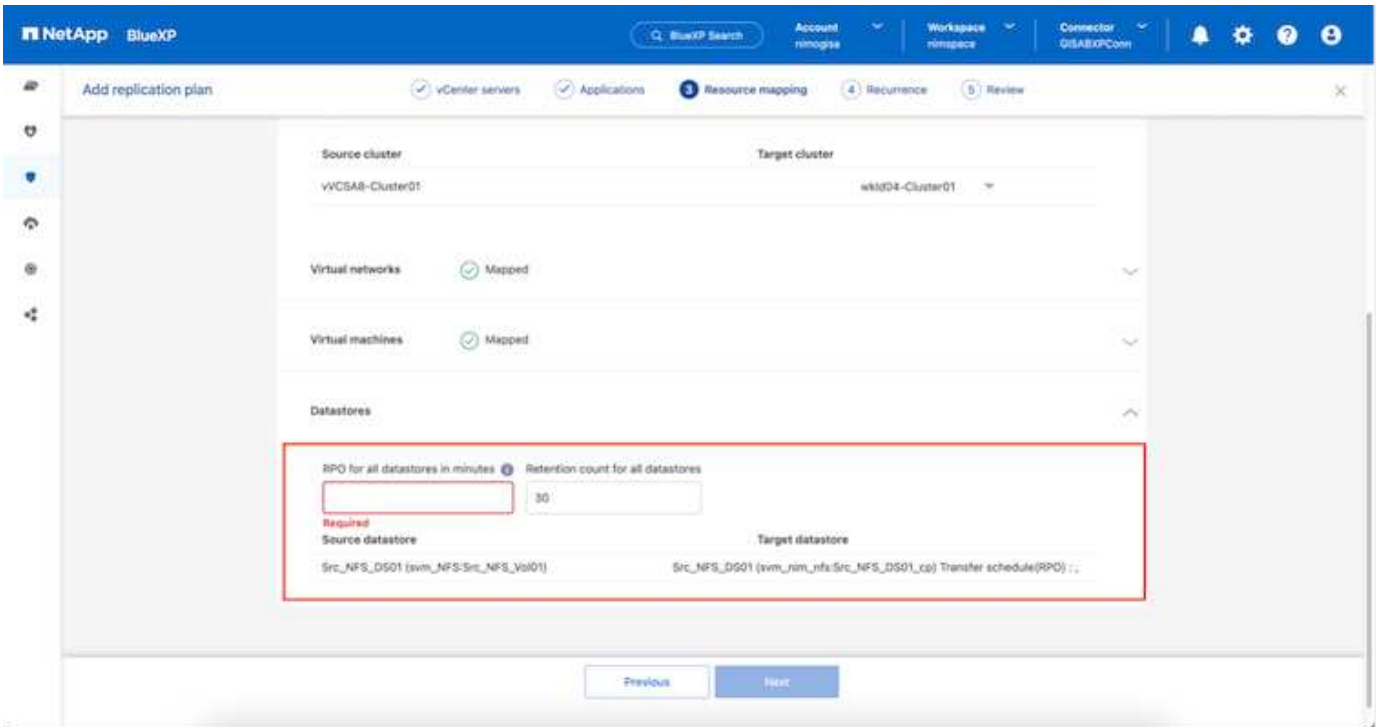
Configuration de la reprise d'activité VMware

Le processus de création de réplication SnapMirror reste le même pour une application donnée. Le processus peut être manuel ou automatisé. Le moyen le plus simple est d'utiliser BlueXP pour configurer la réplication SnapMirror à l'aide d'un simple glisser-déposer du système ONTAP source de l'environnement vers la destination afin de déclencher l'assistant qui guide le reste du processus.



La DRaaS de BlueXP peut également automatiser la même chose, à condition que les deux critères suivants soient remplis :

- Les clusters source et cible ont une relation homologue.
- Les SVM source et destination ont une relation entre pairs.



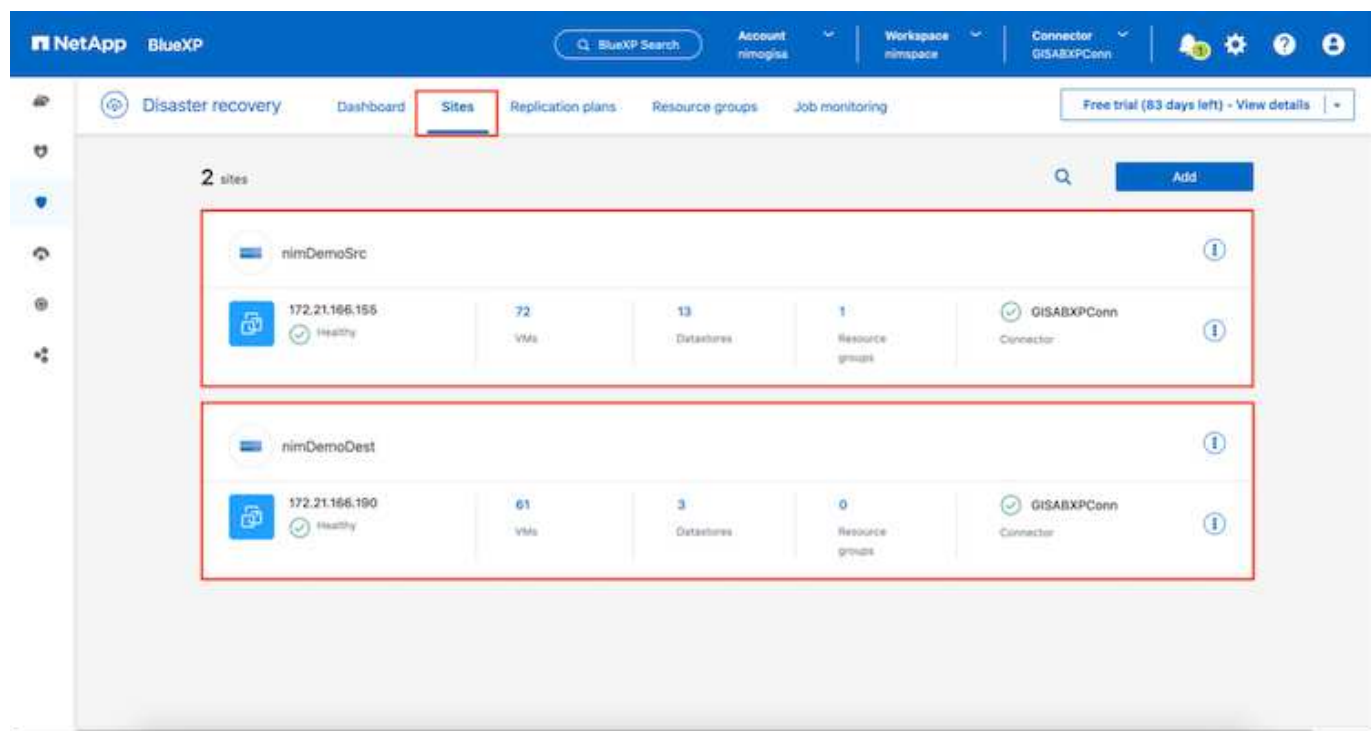
Si la relation SnapMirror est déjà configurée pour le volume via l'interface de ligne de commande, BlueXP DRaaS reprend la relation et poursuit les opérations du reste du workflow.



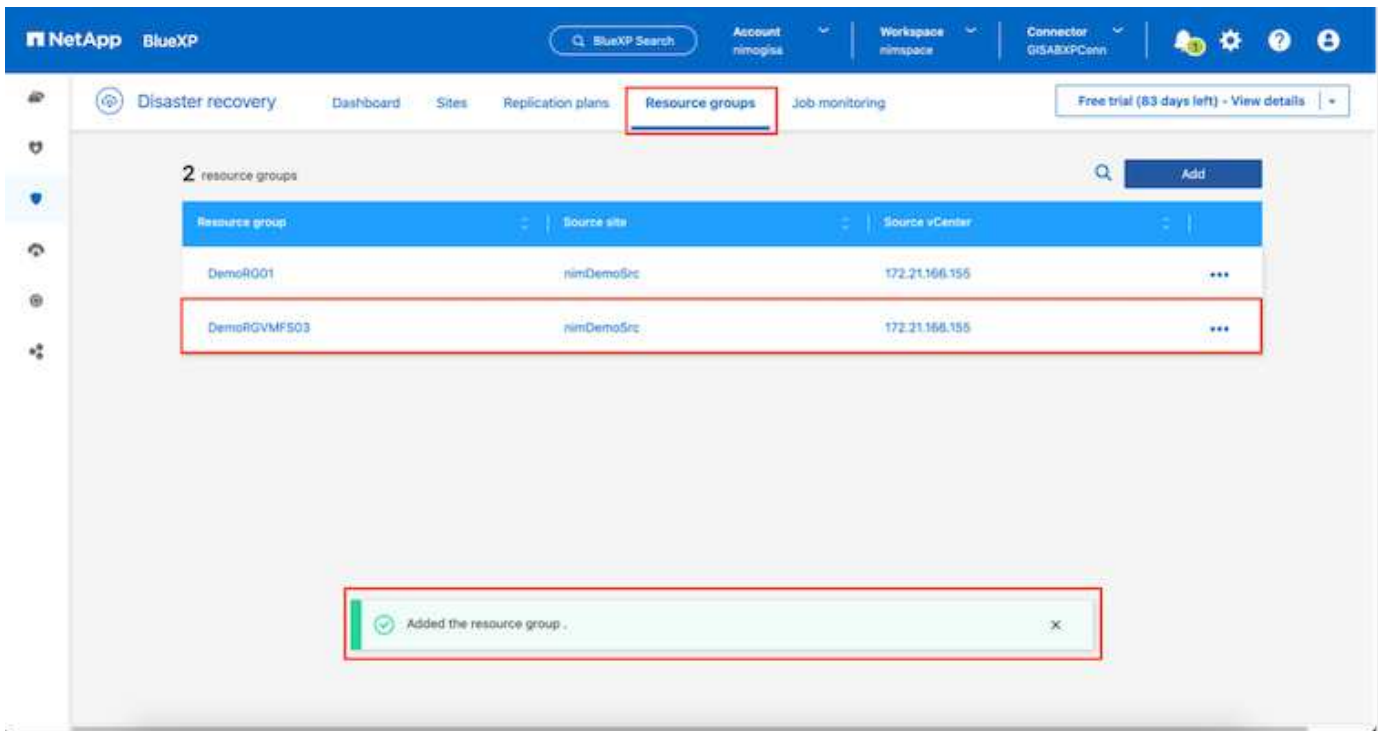
Outre les approches ci-dessus, la réplication SnapMirror peut également être créée via l'interface de ligne de commande ONTAP ou System Manager. Quelle que soit l'approche utilisée pour synchroniser les données à l'aide de SnapMirror, BlueXP la DRaaS orchestre le workflow pour des opérations de reprise d'activité transparentes et efficaces.

Quels avantages la reprise d'activité BlueXP peut-elle apporter pour vous ?

Une fois les sites source et de destination ajoutés, la reprise d'activité BlueXP effectue une détection approfondie automatique et affiche les VM ainsi que les métadonnées associées. Par ailleurs, la reprise d'activité BlueXP détecte automatiquement les réseaux et les groupes de ports utilisés par les machines virtuelles et les remplit.

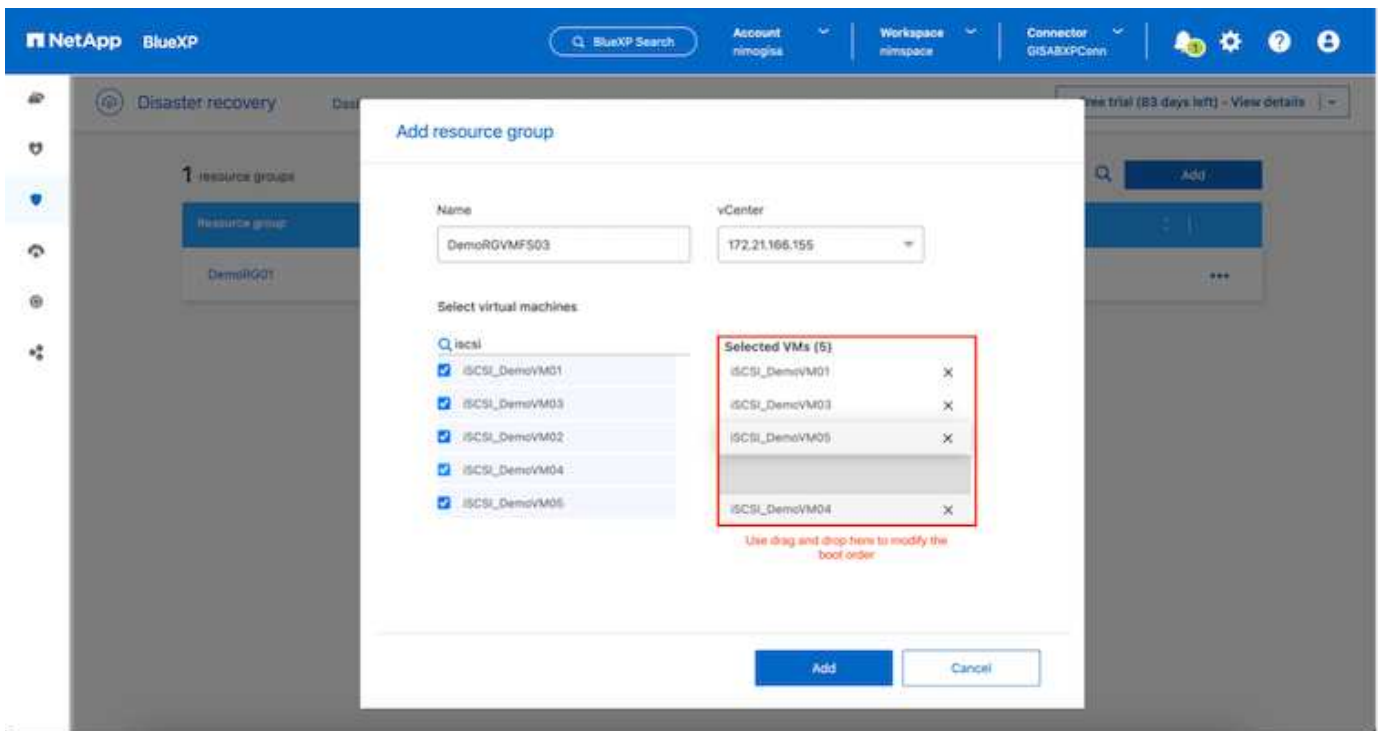


Une fois les sites ajoutés, les VM peuvent être regroupées en groupes de ressources. Les groupes de ressources de reprise sur incident BlueXP vous permettent de regrouper un ensemble de machines virtuelles dépendantes en groupes logiques contenant leurs ordres de démarrage et leurs délais de démarrage pouvant être exécutés lors de la restauration. Pour commencer à créer des groupes de ressources, accédez à **groupes de ressources** et cliquez sur **Créer un nouveau groupe de ressources**.

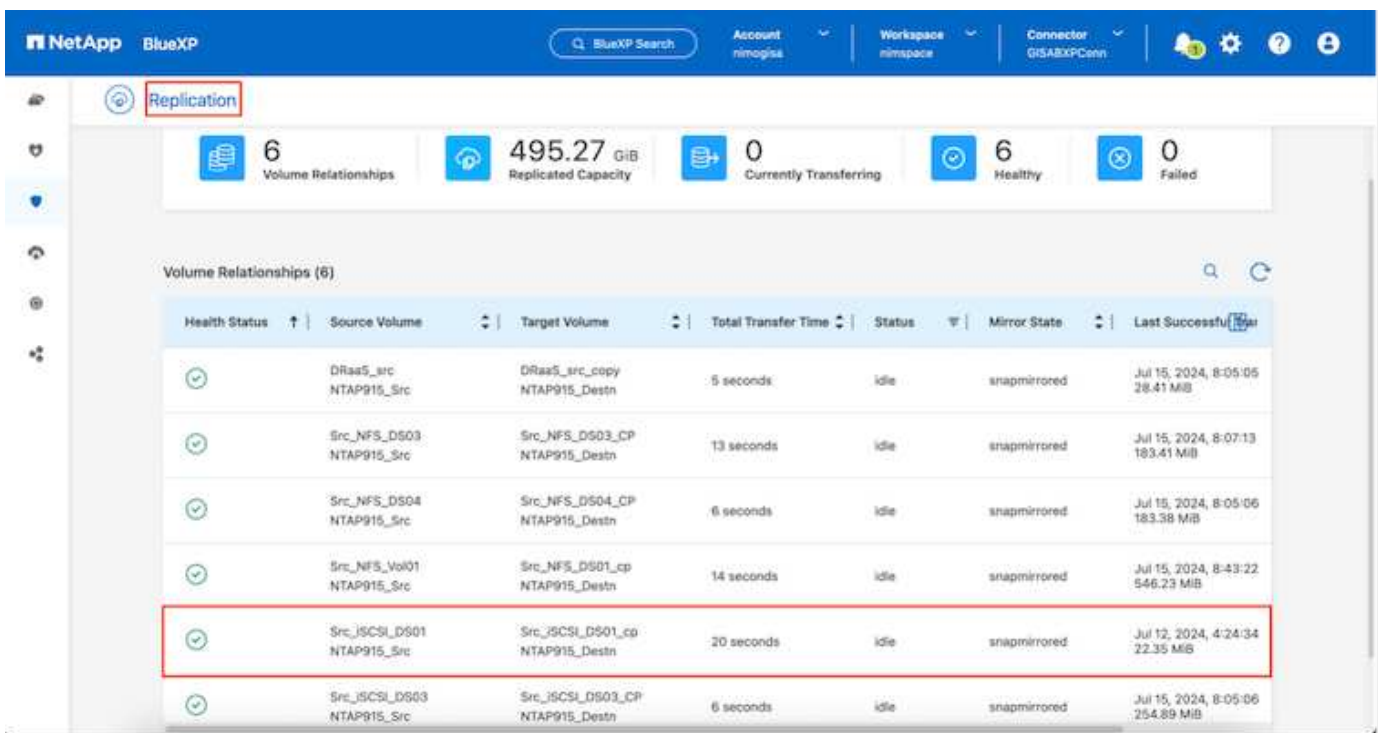
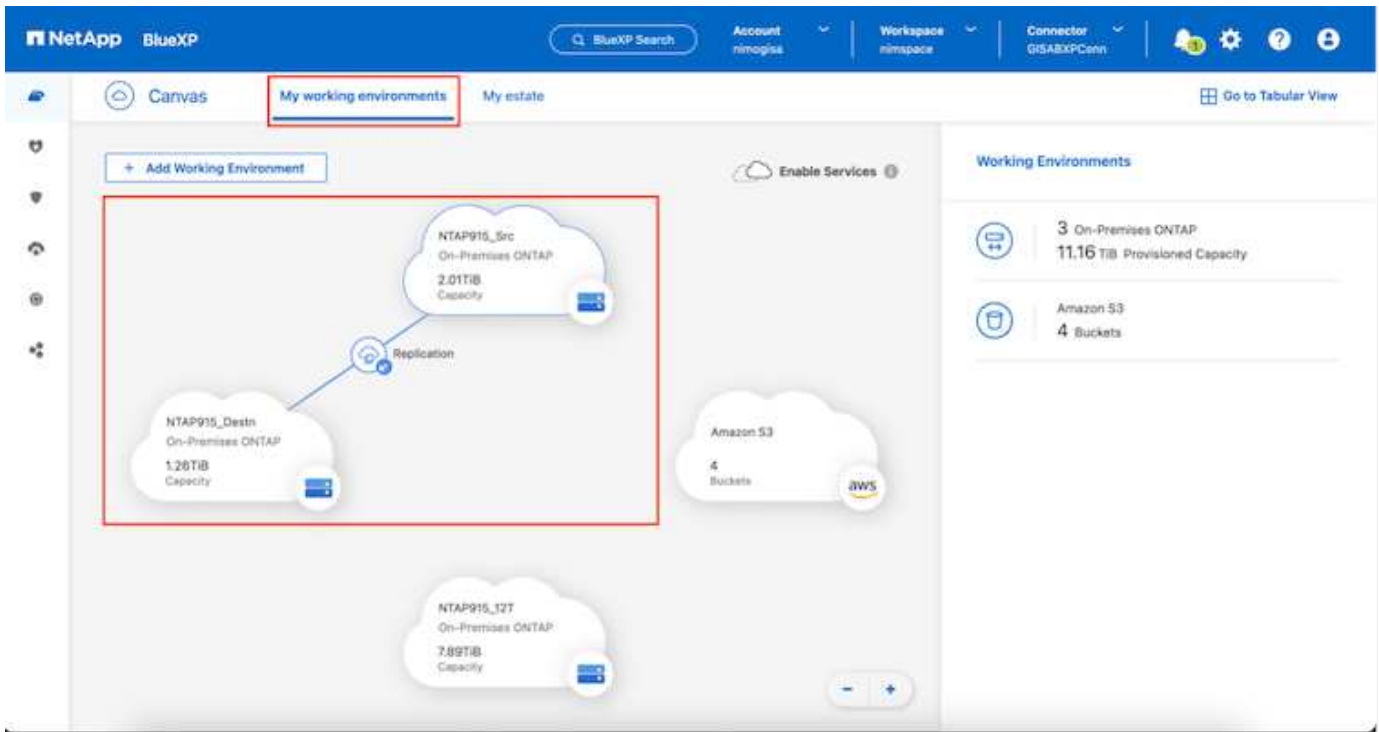


Le groupe de ressources peut également être créé lors de la création d'un plan de réplication.

L'ordre de démarrage des machines virtuelles peut être défini ou modifié lors de la création de groupes de ressources à l'aide d'un simple mécanisme de glisser-déposer.

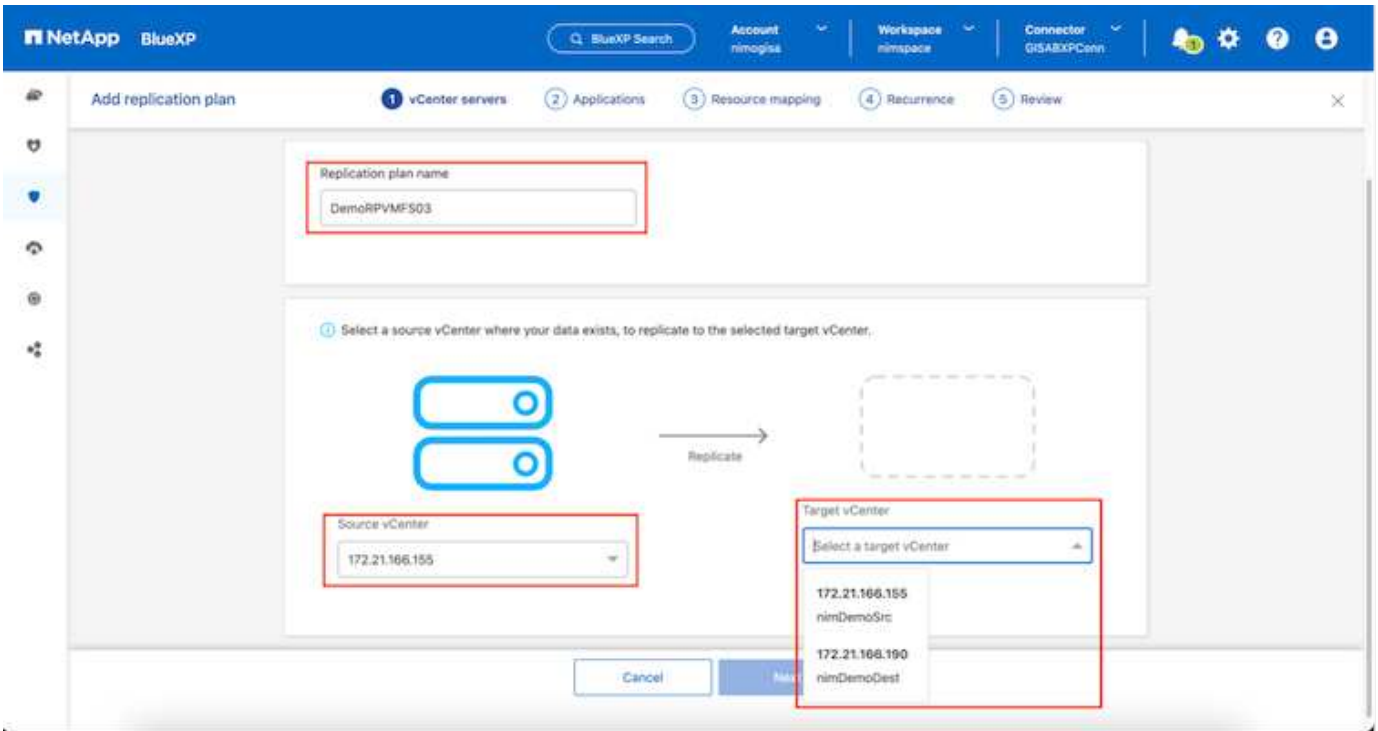


Une fois les groupes de ressources créés, l'étape suivante consiste à créer le modèle d'exécution ou un plan de restauration des machines virtuelles et des applications en cas d'incident. Comme indiqué dans les conditions préalables, la réplication SnapMirror peut être configurée au préalable ou DRaaS peut la configurer à l'aide du RPO et du nombre de rétention spécifiés lors de la création du plan de réplication.

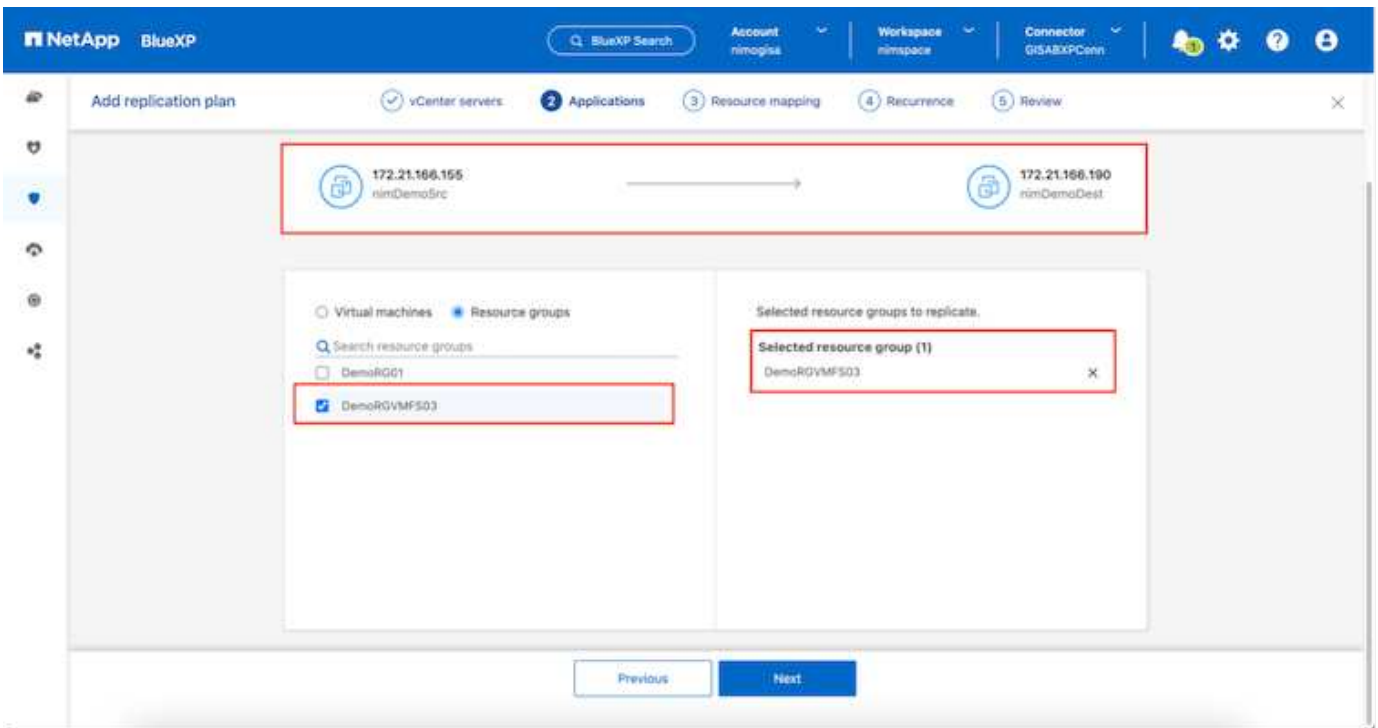


Configurez le plan de réplication en sélectionnant les plates-formes vCenter source et cible dans la liste déroulante, puis sélectionnez les groupes de ressources à inclure dans le plan, ainsi que le regroupement de la manière dont les applications doivent être restaurées et mises sous tension et le mappage des clusters et des réseaux. Pour définir le plan de reprise, accédez à l'onglet **Plan de réplication** et cliquez sur **Ajouter un plan**.

Sélectionnez d'abord le vCenter source, puis le vCenter de destination.



L'étape suivante consiste à sélectionner des groupes de ressources existants. Si aucun groupe de ressources n'est créé, l'assistant vous aide à regrouper les machines virtuelles requises (en créant essentiellement des groupes de ressources fonctionnelles) en fonction des objectifs de restauration. Cela permet également de définir la séquence de fonctionnement de la restauration des machines virtuelles d'applications.

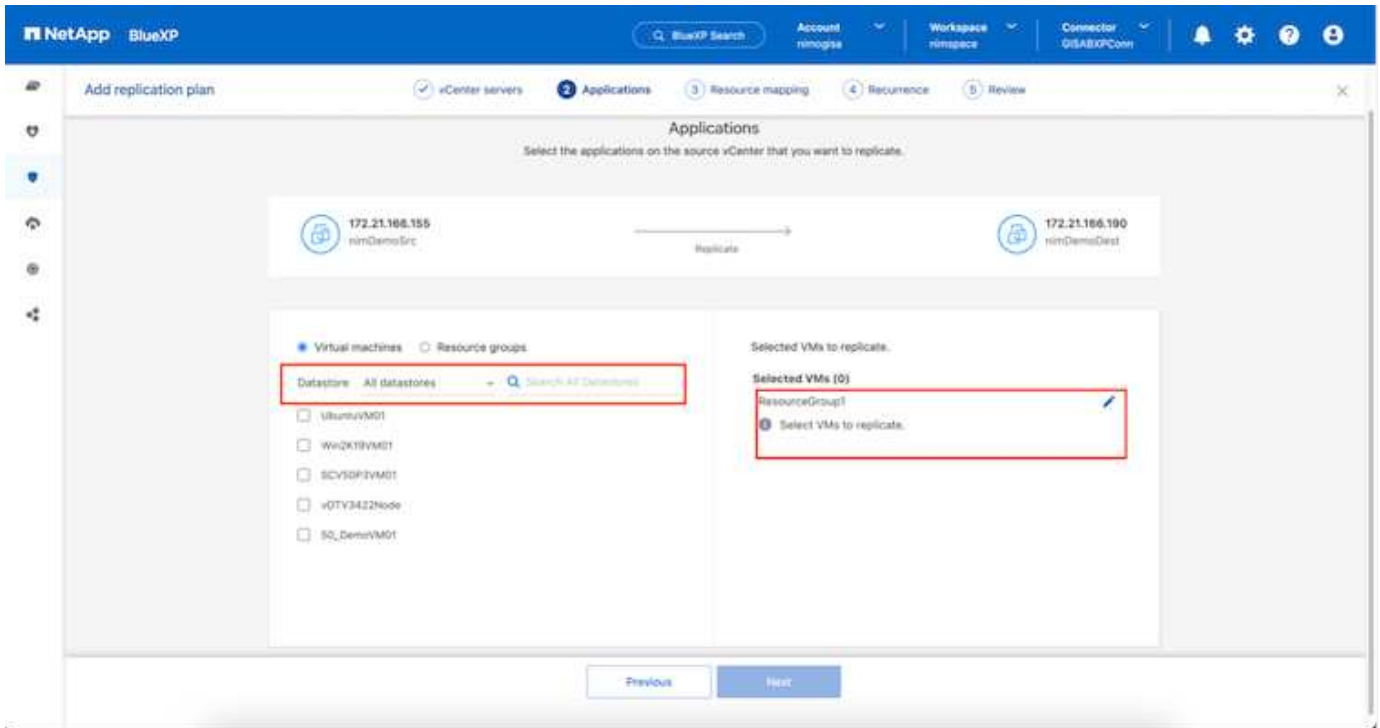


Le groupe de ressources permet de définir l'ordre de démarrage à l'aide de la fonctionnalité glisser-déposer. Il peut être utilisé pour modifier facilement l'ordre de mise sous tension des VM pendant le processus de restauration.

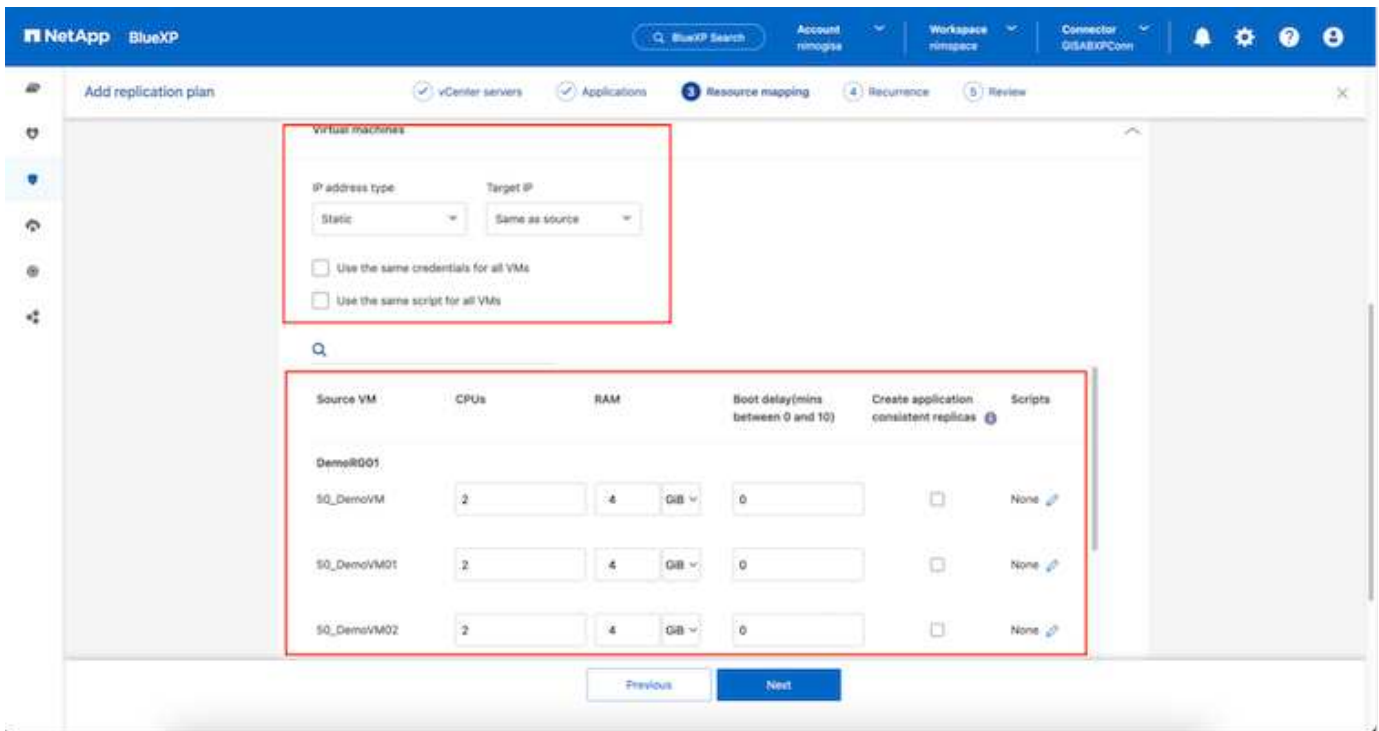


Chaque machine virtuelle au sein d'un groupe de ressources est démarrée dans l'ordre indiqué. Deux groupes de ressources sont démarrés en parallèle.

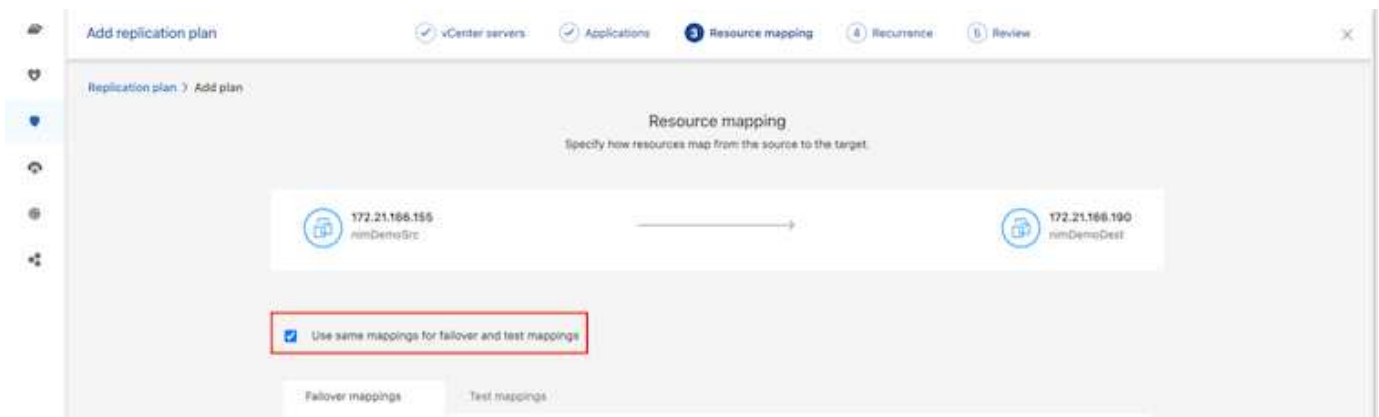
La capture d'écran ci-dessous présente l'option de filtrage des machines virtuelles ou des datastores spécifiques en fonction des besoins organisationnels si les groupes de ressources ne sont pas créés au préalable.



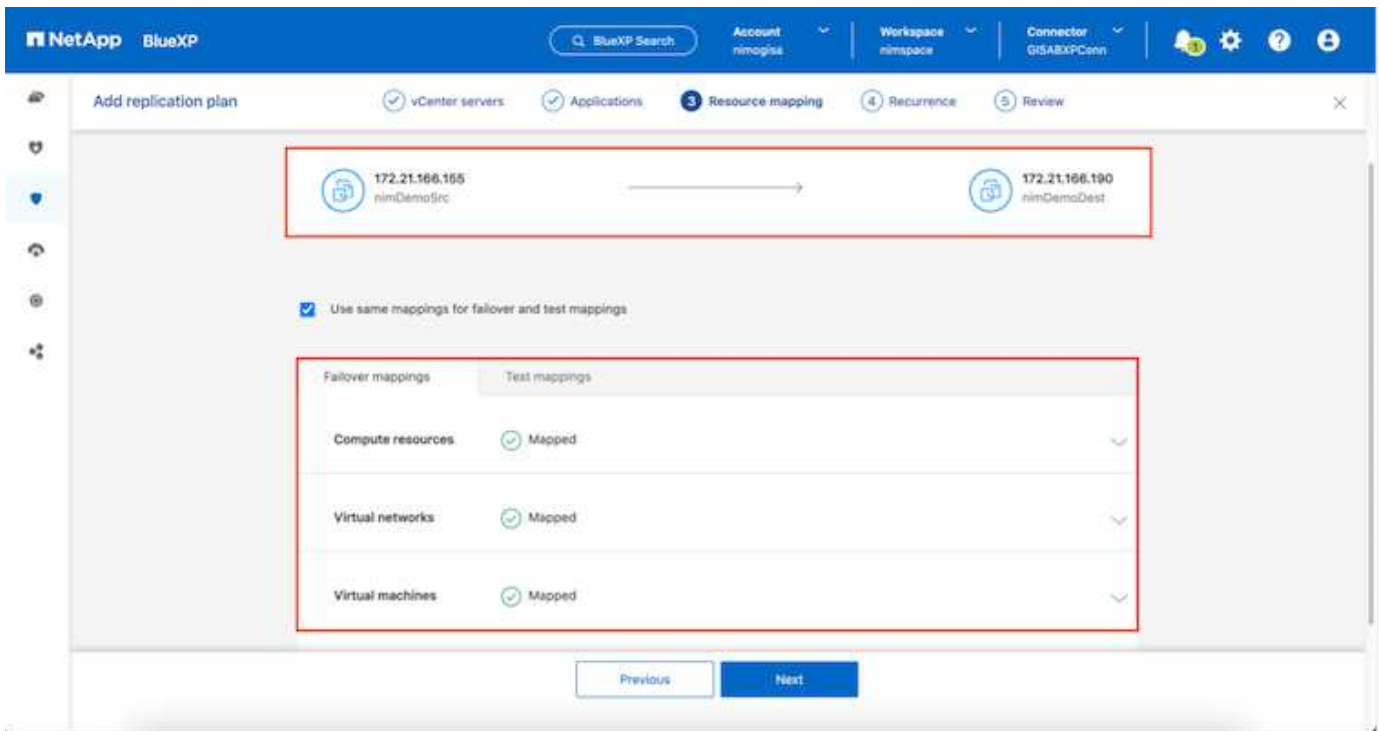
Une fois les groupes de ressources sélectionnés, créez les mappages de basculement. Dans cette étape, spécifiez la façon dont les ressources de l'environnement source sont mises en correspondance avec la destination. Cela inclut les ressources de calcul, les réseaux virtuels. Personnalisation IP, pré et post-scripts, délais de démarrage, cohérence des applications, etc. Pour plus d'informations, reportez-vous "[Créer un plan de réplication](#)" à la .



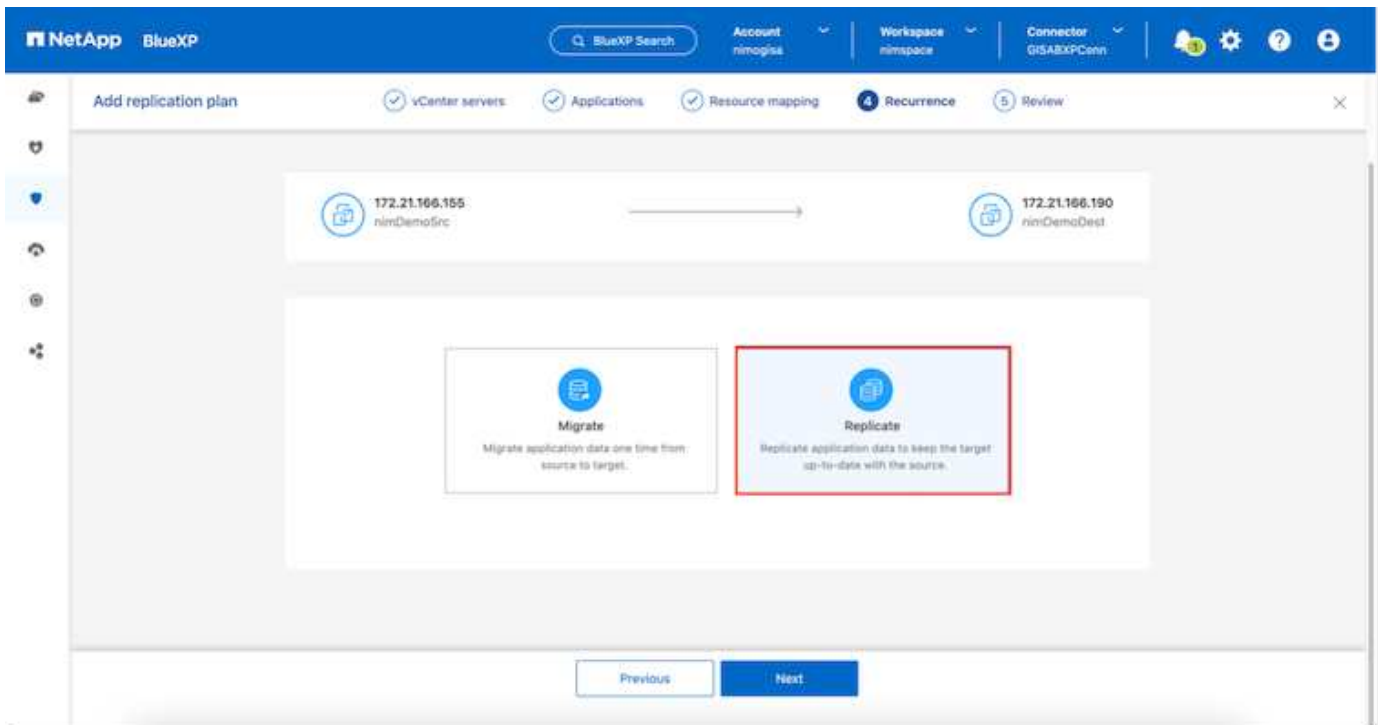
Par défaut, les mêmes paramètres de mappage sont utilisés pour les opérations de test et de basculement. Pour appliquer des mappages différents à l'environnement de test, sélectionnez l'option Tester le mappage après avoir décochée la case comme indiqué ci-dessous :



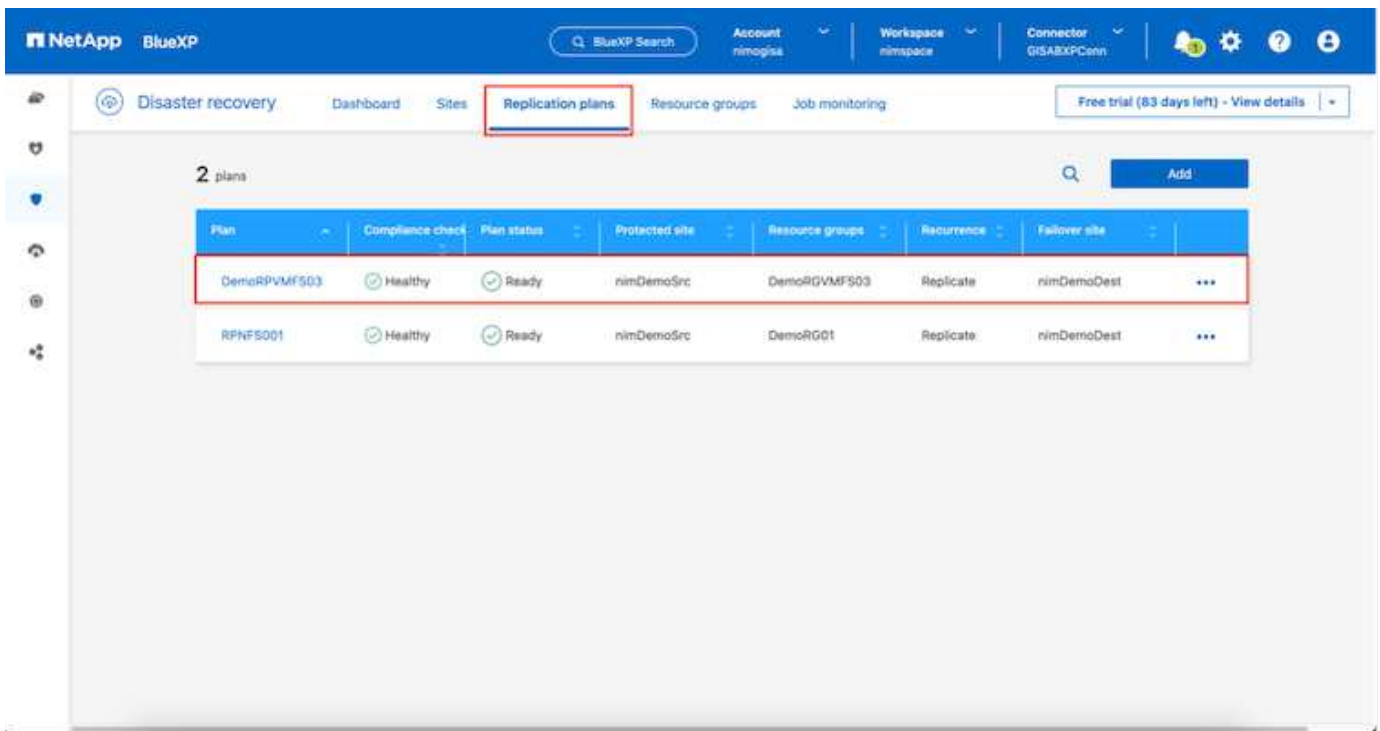
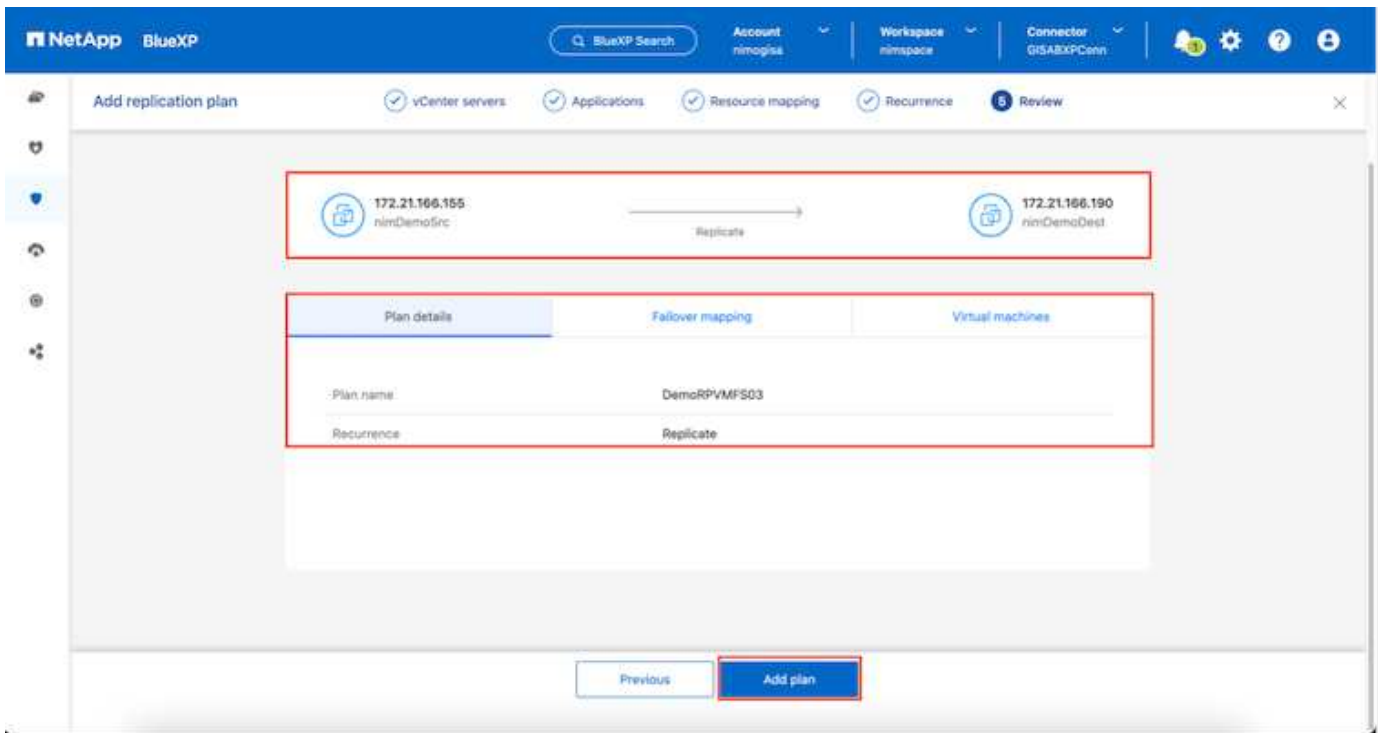
Une fois le mappage des ressources terminé, cliquez sur Suivant.



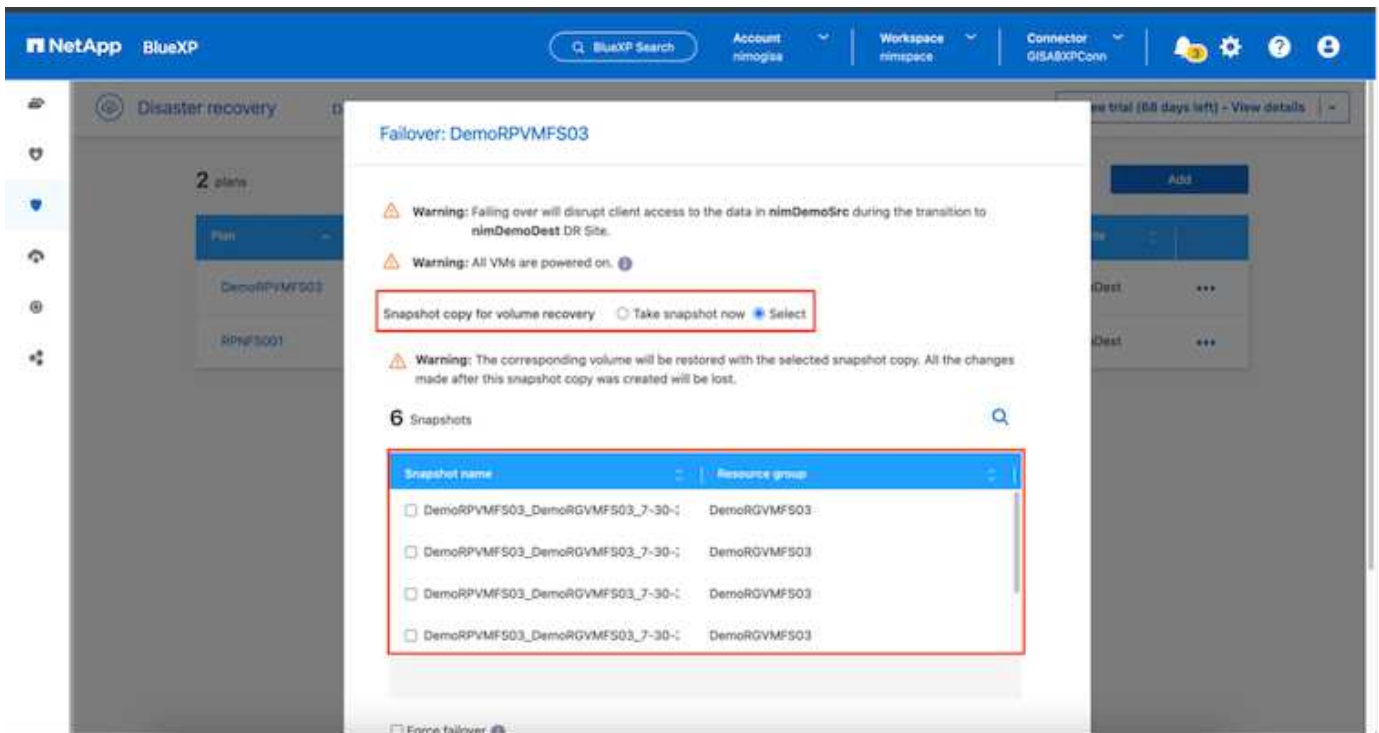
Sélectionnez le type de récurrence. En d'autres termes, sélectionnez Migrate (migration unique avec basculement) ou l'option de réplication continue récurrente. Dans cette procédure, l'option de réplication est sélectionnée.



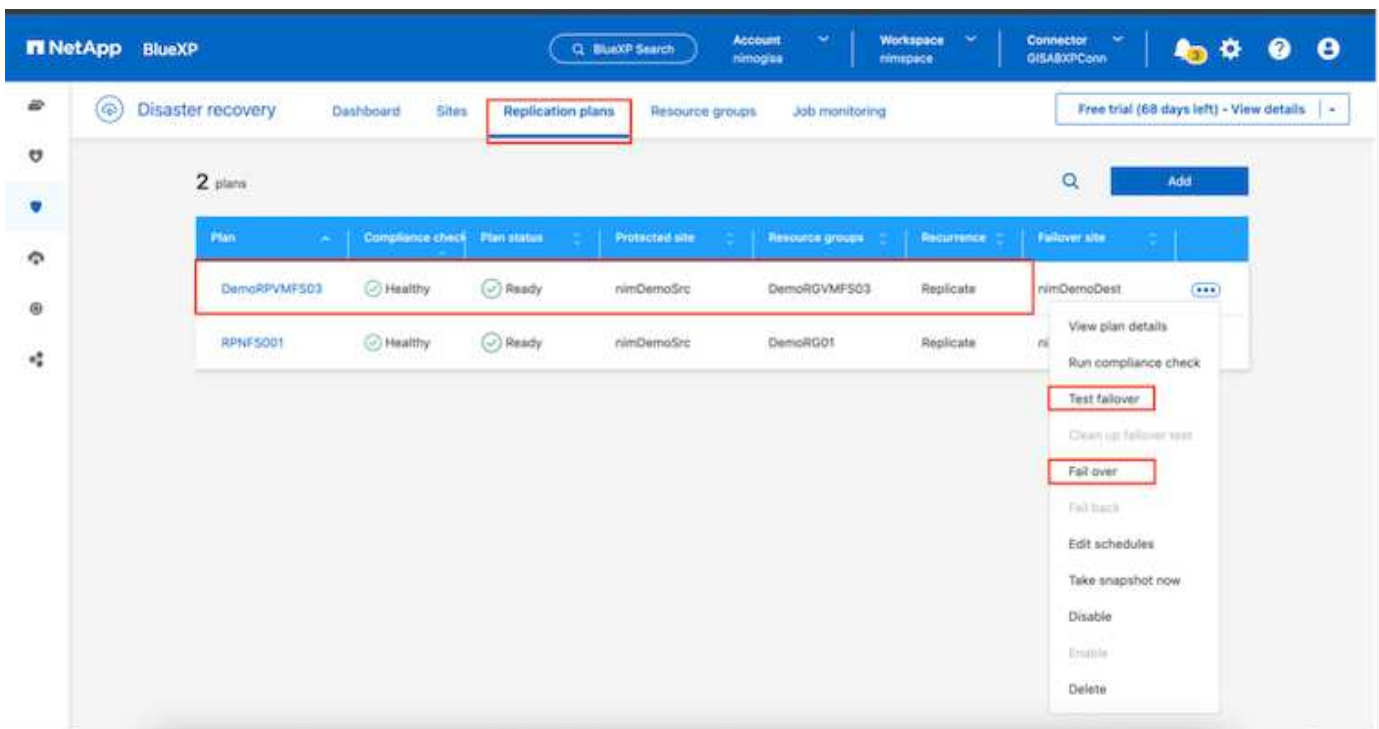
Une fois l'opération terminée, vérifiez les mappages créés, puis cliquez sur Ajouter un plan.



Une fois le plan de réplication créé, le basculement peut être effectué en fonction des besoins en sélectionnant l'option de basculement, l'option test-basculement ou l'option de migration. La reprise après incident BlueXP garantit l'exécution du processus de réplication conformément au plan toutes les 30 minutes. Au cours des options de basculement et de test/basculement, vous pouvez utiliser la dernière copie Snapshot SnapMirror ou sélectionner une copie Snapshot spécifique à partir d'une copie Snapshot instantanée (conformément à la règle de conservation de SnapMirror). L'option instantanée peut s'avérer très utile en cas de corruption comme une attaque par ransomware, où les répliques les plus récentes sont déjà compromises ou chiffrées. La reprise d'activité BlueXP affiche tous les points de restauration disponibles.



Pour déclencher le basculement ou tester le basculement avec la configuration spécifiée dans le plan de réplication, cliquez sur **basculement** ou **Test du basculement**.



Que se passe-t-il lors d'une opération de basculement ou de test ?

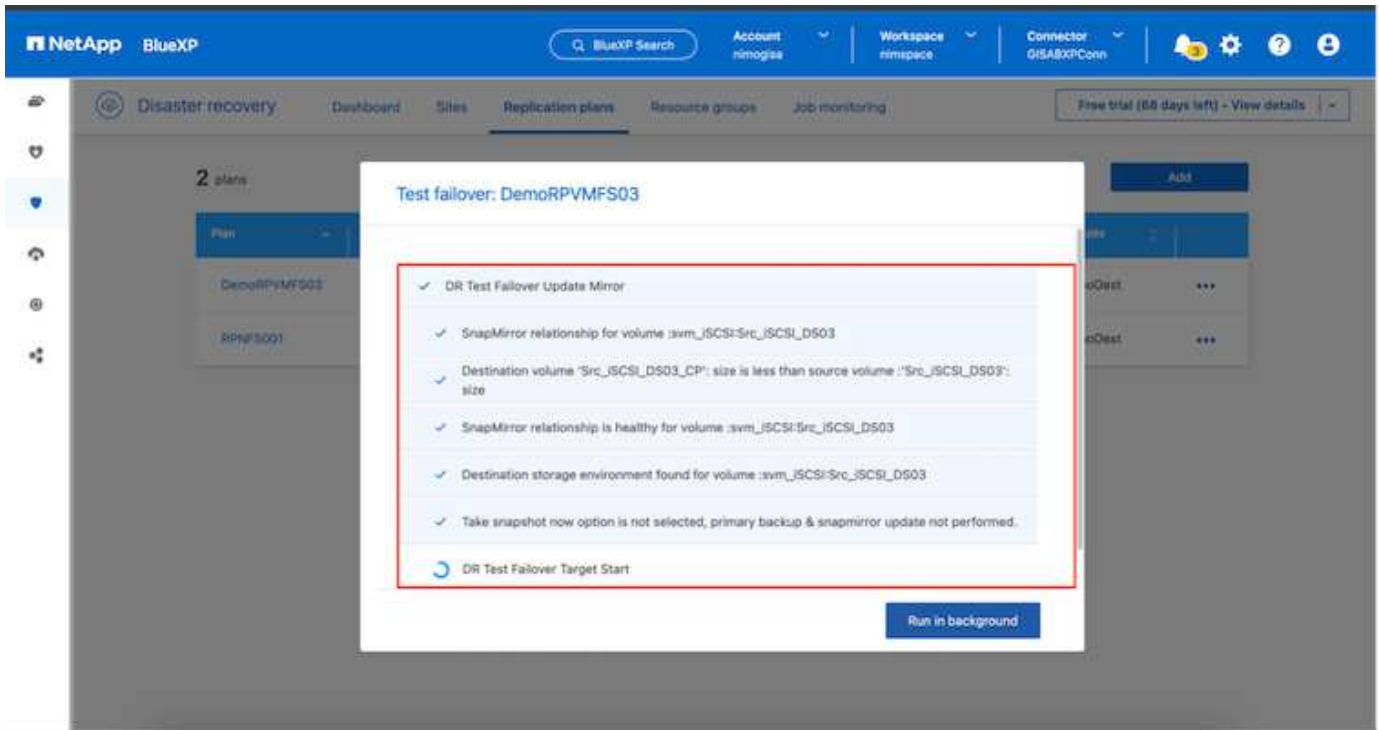
Lors d'une opération de basculement de test, BlueXP Disaster Recovery crée un volume FlexClone sur le système de stockage ONTAP de destination en utilisant la dernière copie Snapshot ou un snapshot sélectionné du volume de destination.



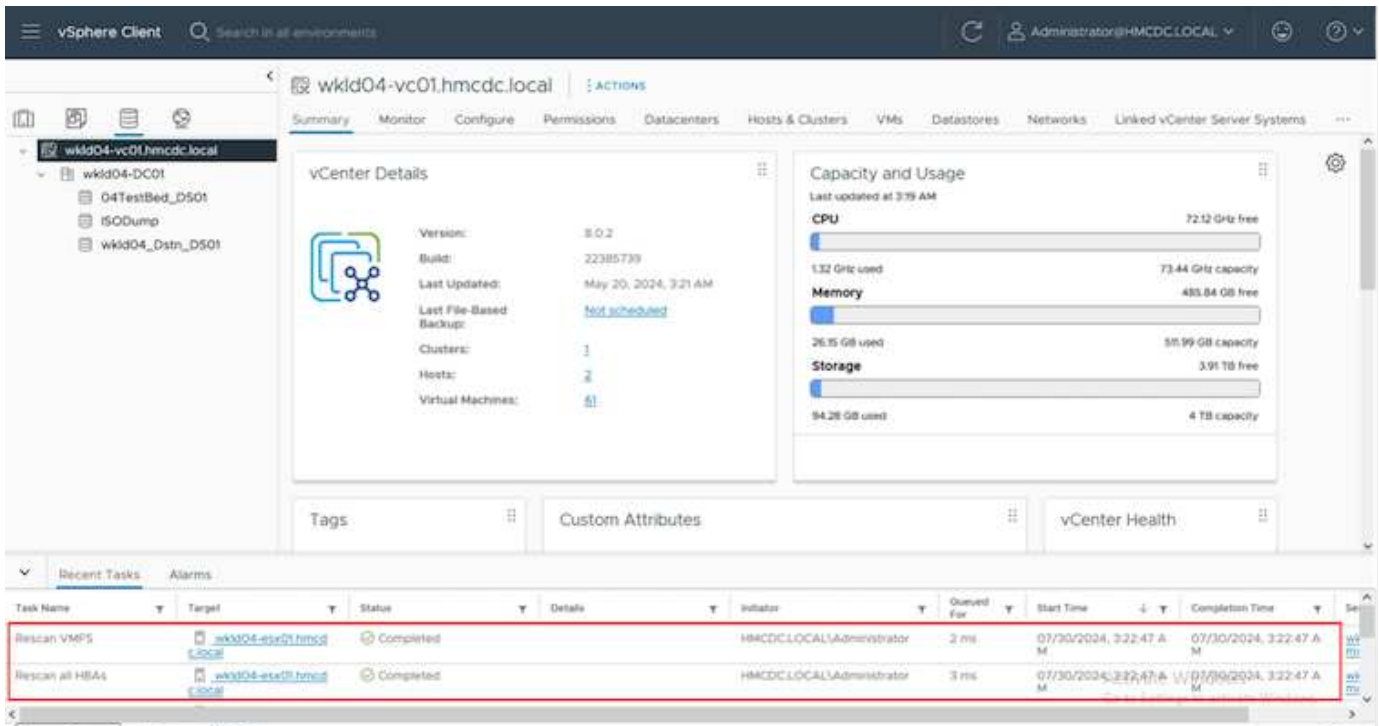
Une opération de basculement test crée un volume cloné sur le système de stockage ONTAP de destination.

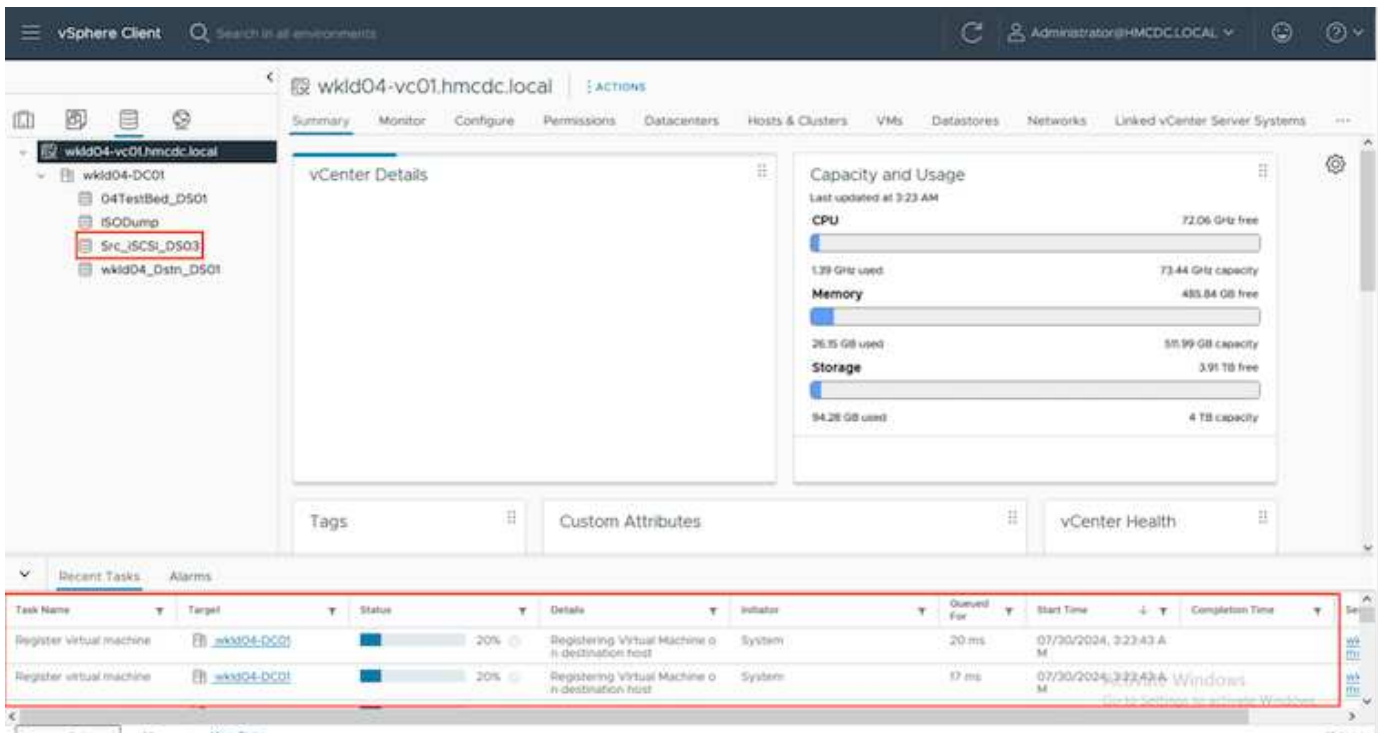


L'exécution d'une opération de restauration test n'affecte pas la réplication SnapMirror.



Pendant ce processus, la reprise d'activité BlueXP ne mappe pas le volume cible d'origine. À la place, il crée un nouveau volume FlexClone à partir de l'instantané sélectionné et un datastore temporaire sur lequel le volume FlexClone est soutenu est mappé vers les hôtes ESXi.

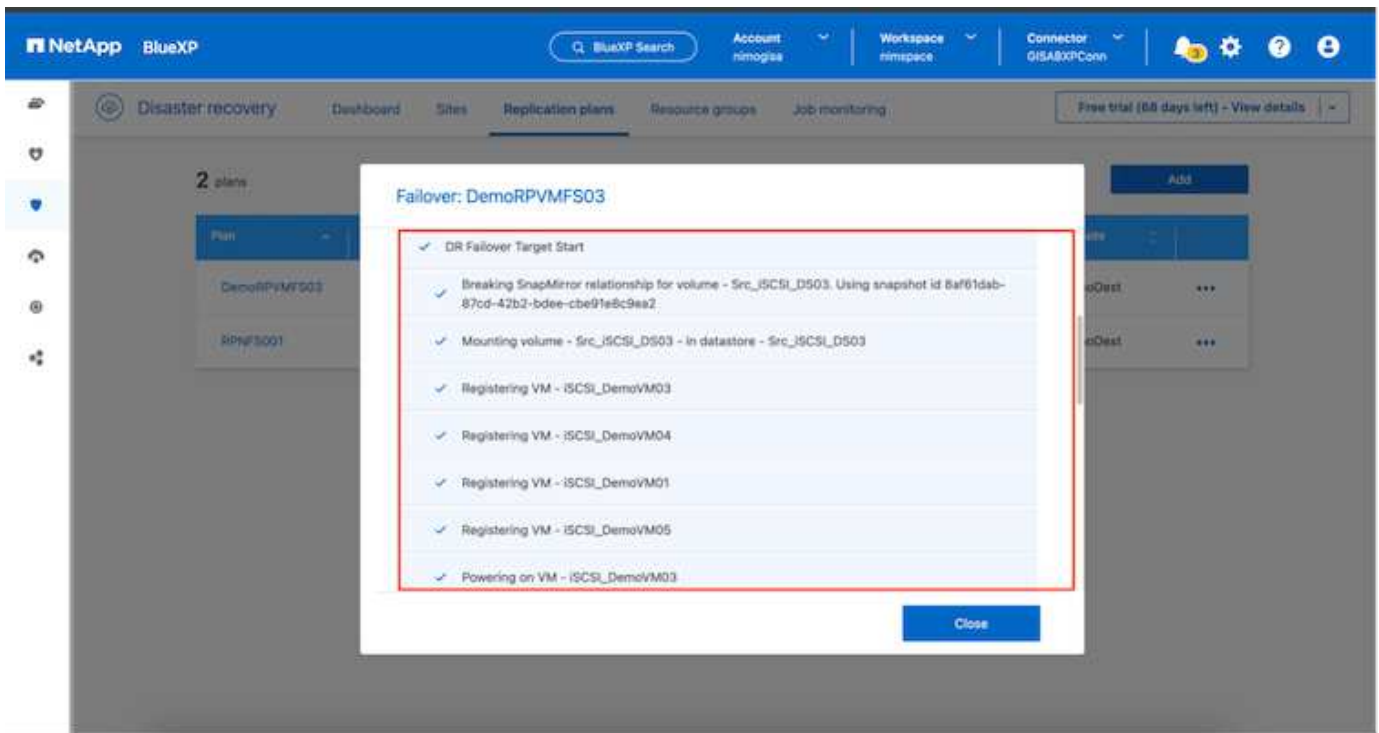




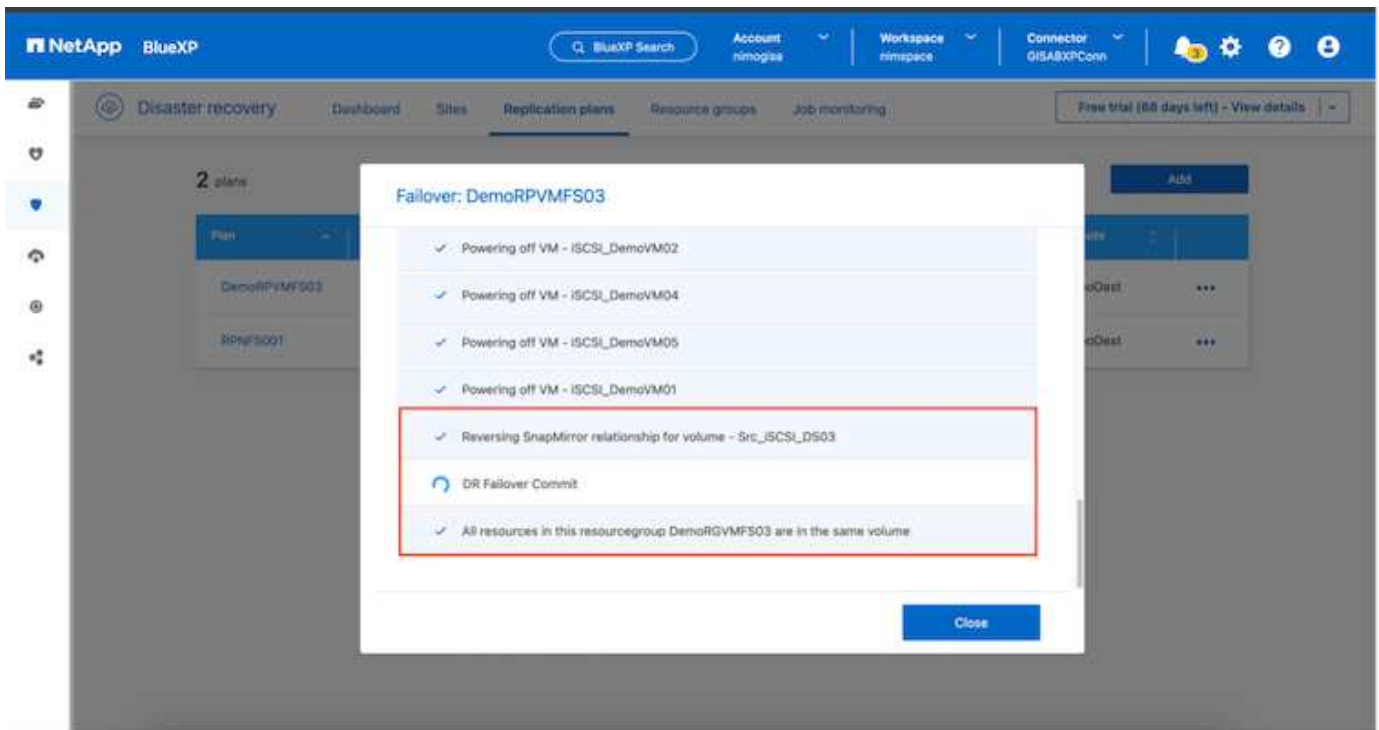
Une fois l'opération de basculement de test terminée, l'opération de nettoyage peut être déclenchée à l'aide de « **Test de basculement de nettoyage** ». Au cours de cette opération, la reprise sur incident BlueXP détruit le volume FlexClone utilisé dans l'opération.

En cas d'incident réel, la reprise sur incident BlueXP effectue les opérations suivantes :

1. Rompt la relation SnapMirror entre les sites.
2. Monte le volume du datastore VMFS après la resignature pour une utilisation immédiate.
3. Enregistrer les VM
4. Mettez les machines virtuelles sous tension

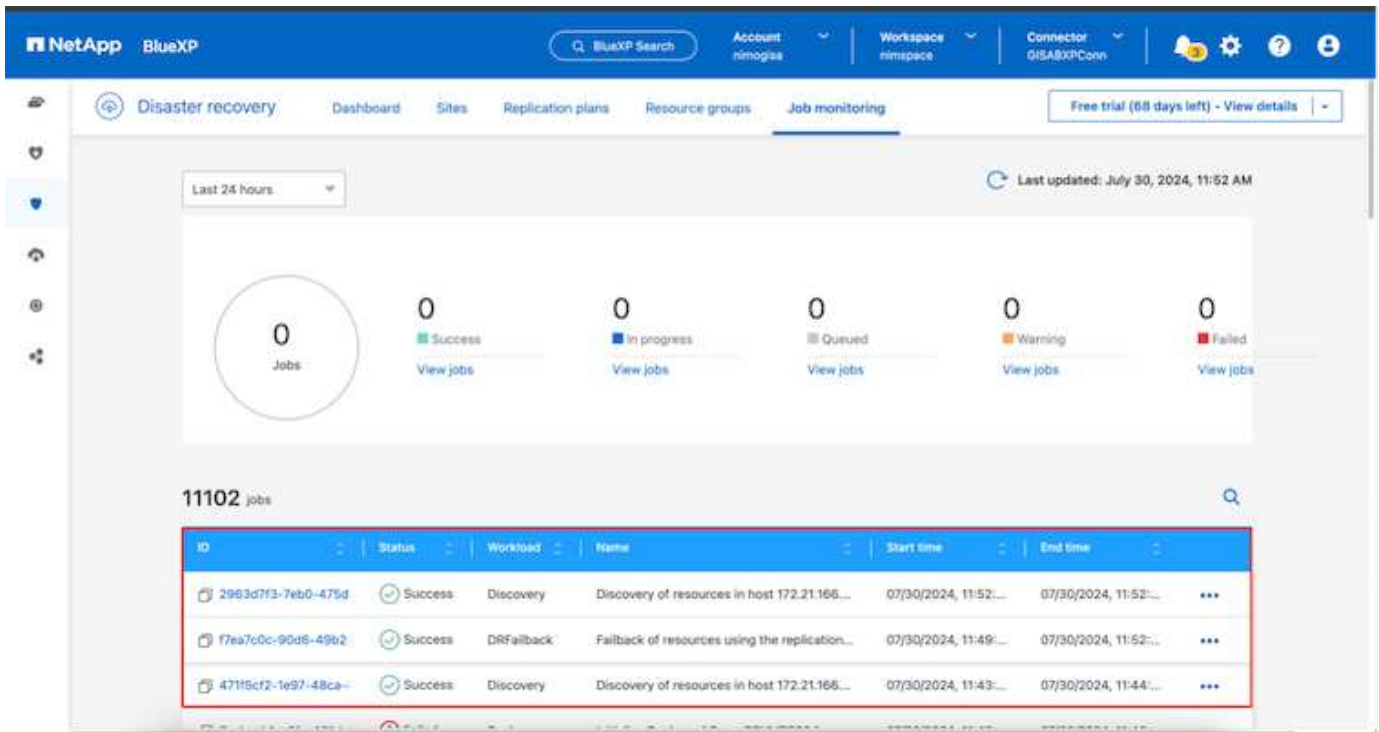


Une fois le site primaire opérationnel, la reprise d'activité BlueXP permet d'inverser la resynchronisation pour SnapMirror et d'activer le retour arrière, qui peut à nouveau être effectuée en un seul clic.



Si l'option de migration est choisie, elle est considérée comme un événement de basculement planifié. Dans ce cas, une étape supplémentaire est déclenchée, qui consiste à arrêter les machines virtuelles sur le site source. Le reste de ces étapes reste identique à l'événement de basculement.

À partir de BlueXP ou de l'interface de ligne de commandes de ONTAP, vous pouvez contrôler l'état de la réplication pour les volumes de datastore appropriés. Vous pouvez également suivre l'état d'un basculement ou d'un basculement de test via la surveillance des tâches.



Il s'agit d'une solution puissante permettant de gérer un plan de reprise d'activité personnalisé. Le basculement peut s'effectuer en cas de basculement planifié ou de basculement d'un simple clic en cas d'incident et si la décision d'activer le site de reprise est prise.

Pour en savoir plus sur ce processus, n'hésitez pas à suivre la vidéo de présentation détaillée ou à utiliser le "simulateur de solution".

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.