TR-4955 : Reprise après sinistre avec Azure NetApp Files (ANF) et Azure VMware Solution (AVS)

NetApp public and hybrid cloud solutions

NetApp
August 18, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/netapp-solutions-cloud/vmware/vmw-azure-avs-dro.html on August 18, 2025. Always check docs.netapp.com for the latest.

Sommaire

TR-4955 : Reprise après sinistre avec Azure NetApp Files (ANF) et Azure VMware Solution (AVS) . . . 1
Aperçu . . . 1
Prérequis et recommandations générales . . . 1
Commencer . . . 2
Déployer la solution Azure VMware . . . 2
Provisionner et configurer Azure NetApp Files . . . 2
Installation de DRO . . . 3
Configuration DRO . . . 4
Groupements de ressources . . . 8
Plans de réplication . . . 9
Récupération après un ransomware . . . 15
Conclusion . . . 15
Où trouver des informations supplémentaires . . . 15

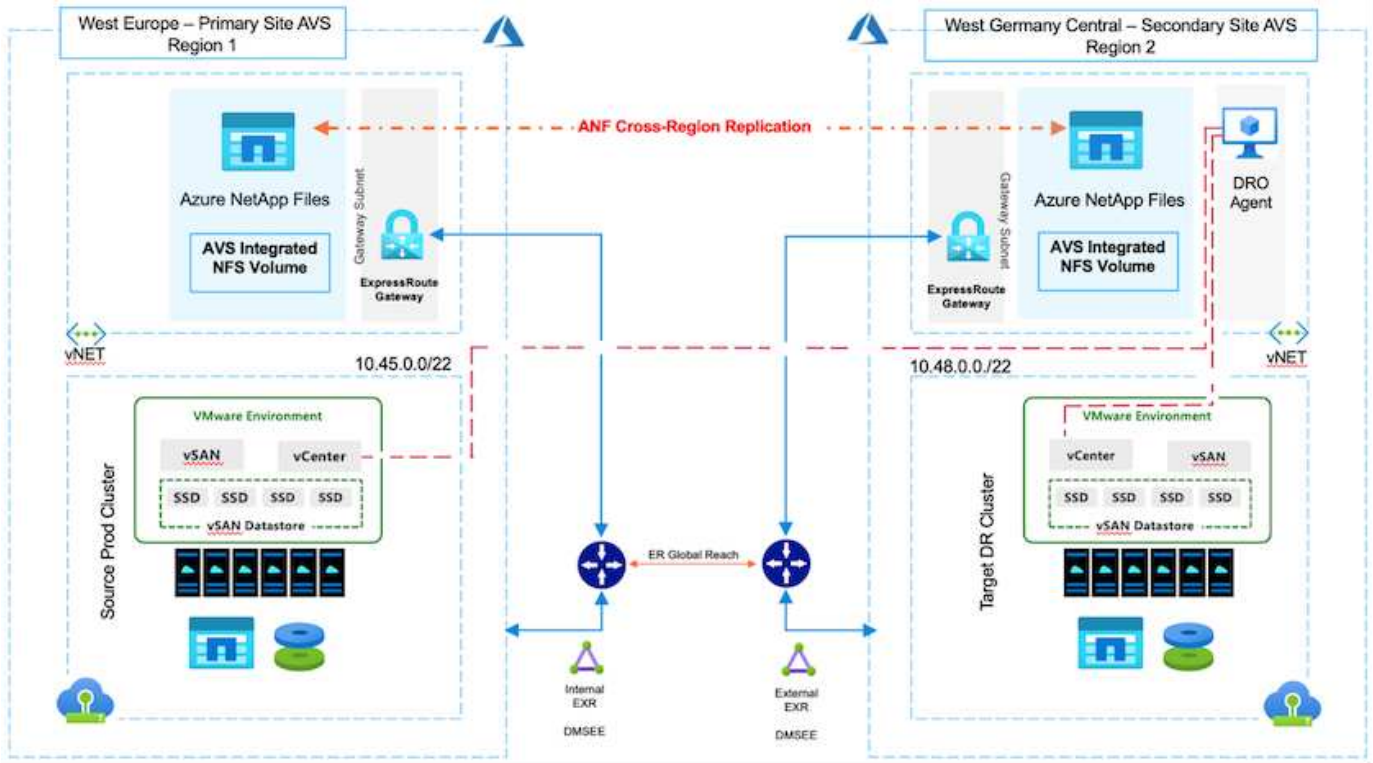
TR-4955 : Reprise après sinistre avec Azure NetApp Files (ANF) et Azure VMware Solution (AVS)

La reprise après sinistre utilisant la réplication au niveau des blocs entre les régions du cloud est un moyen résilient et rentable de protéger les charges de travail contre les pannes de site et les événements de corruption de données (par exemple, les ransomwares).

Aperçu

Avec la réplication de volume interrégionale Azure NetApp Files (ANF), les charges de travail VMware exécutées sur un site SDDC Azure VMware Solution (AVS) utilisant des volumes Azure NetApp Files comme banque de données NFS sur le site AVS principal peuvent être répliquées vers un site AVS secondaire désigné dans la région de récupération cible.

Disaster Recovery Orchestrator (DRO) (une solution scriptée avec une interface utilisateur) peut être utilisé pour récupérer de manière transparente les charges de travail répliquées d'un SDDC AVS vers un autre. DRO automatise la récupération en interrompant le peering de réplication, puis en montant le volume de destination en tant que banque de données, via l'enregistrement de la machine virtuelle sur AVS, vers des mappages réseau directement sur NSX-T (inclus avec tous les clouds privés AVS).



Prérequis et recommandations générales

- Vérifiez que vous avez activé la réplication interrégionale en créant un peering de réplication. Voir "Créer une réplication de volume pour Azure NetApp Files" .

- Vous devez configurer ExpressRoute Global Reach entre les clouds privés Azure VMware Solution source et cible.
- Vous devez disposer d'un principal de service pouvant accéder aux ressources.
- La topologie suivante est prise en charge : site AVS principal vers site AVS secondaire.
- Configurer le "réplication" planifier chaque volume de manière appropriée en fonction des besoins de l'entreprise et du taux de modification des données.

> Les topologies en cascade et en éventail ne sont pas prises en charge.

Commencer

Déployer la solution Azure VMware

Le "Solution Azure VMware" (AVS) est un service cloud hybride qui fournit des SDDC VMware entièrement fonctionnels au sein d'un cloud public Microsoft Azure. AVS est une solution propriétaire entièrement gérée et prise en charge par Microsoft et vérifiée par VMware qui utilise l'infrastructure Azure. Par conséquent, les clients bénéficient de VMware ESXi pour la virtualisation du calcul, de vSAN pour le stockage hyperconvergé et de NSX pour la mise en réseau et la sécurité, tout en profitant de la présence mondiale de Microsoft Azure, des installations de centre de données de pointe et de la proximité du riche écosystème de services et de solutions Azure natifs. Une combinaison d'Azure VMware Solution SDDC et Azure NetApp Files offre les meilleures performances avec une latence réseau minimale.

Pour configurer un cloud privé AVS sur Azure, suivez les étapes décrites dans cet article."lien" pour la documentation NetApp et dans ce "lien" pour la documentation Microsoft. Un environnement de veilleuse configuré avec une configuration minimale peut être utilisé à des fins de reprise après sinistre. Cette configuration contient uniquement les composants principaux pour prendre en charge les applications critiques et peut évoluer et générer davantage d'hôtes pour prendre en charge la majeure partie de la charge en cas de basculement.

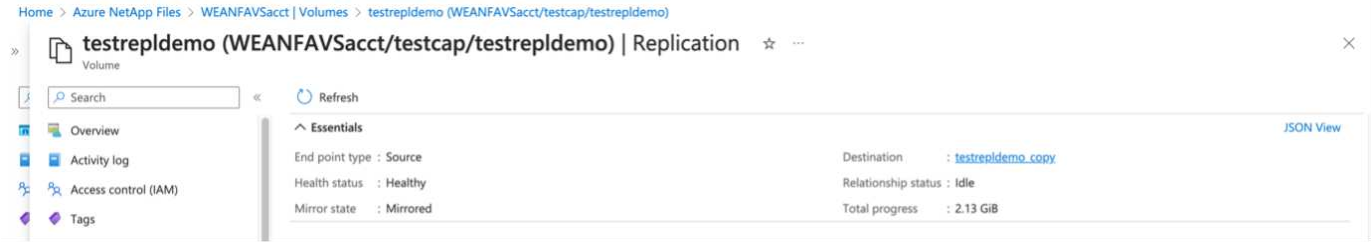
> Dans la version initiale, DRO prend en charge un cluster AVS SDDC existant. La création de SDDC à la demande sera disponible dans une prochaine version.

Provisionner et configurer Azure NetApp Files

"Azure NetApp Files"est un service de stockage de fichiers à hautes performances, de niveau entreprise et mesuré. Suivez les étapes de cette "lien" pour provisionner et configurer Azure NetApp Files en tant que banque de données NFS afin d'optimiser les déploiements de cloud privé AVS.

Créer une réplication de volume pour les volumes de banque de données alimentés par Azure NetApp Files

La première étape consiste à configurer la réplication interrégionale pour les volumes de banque de données souhaités du site principal AVS vers le site secondaire AVS avec les fréquences et les rétentions appropriées.



Suivez les étapes de cette "lien" pour configurer la réplication inter-régionale en créant un peering de réplication. Le niveau de service du pool de capacité de destination peut correspondre à celui du pool de capacité source. Cependant, pour ce cas d'utilisation spécifique, vous pouvez sélectionner le niveau de service standard, puis "modifier le niveau de service" en cas de catastrophe réelle ou de simulations DR.

> Une relation de réplication inter-régionale est une condition préalable et doit être créée au préalable.

Installation de DRO

Pour commencer avec DRO, utilisez le système d'exploitation Ubuntu sur la machine virtuelle Azure désignée et assurez-vous de remplir les conditions préalables. Ensuite, installez le package.

Prérequis :

- Principal de service pouvant accéder aux ressources.
- Assurez-vous qu'une connectivité appropriée existe avec les instances SDDC source et de destination et Azure NetApp Files .
- La résolution DNS doit être en place si vous utilisez des noms DNS. Sinon, utilisez les adresses IP pour vCenter.

Configuration requise pour le système d'exploitation :

- Ubuntu Focal 20.04 (LTS)Les packages suivants doivent être installés sur la machine virtuelle de l'agent désigné :
- Docker
- Docker-compose
- JqChange `docker.sock` à cette nouvelle permission : `sudo chmod 666 /var/run/docker.sock` .

> Le `deploy.sh` le script exécute tous les prérequis requis.

Les étapes sont les suivantes :

1. Téléchargez le package d'installation sur la machine virtuelle désignée :

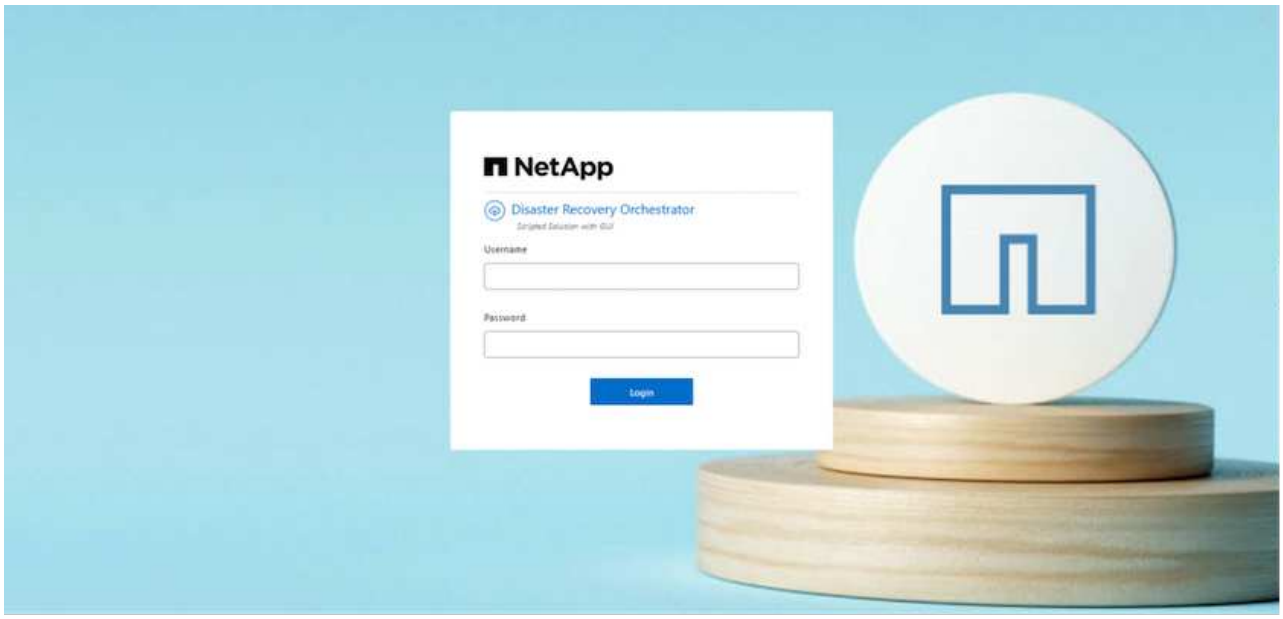
```
git clone https://github.com/NetApp/DRO-Azure.git
```

> L'agent doit être installé dans la région du site AVS secondaire ou dans la région du site AVS principal dans une zone de disponibilité distincte de celle du SDDC.

2. Décompressez le package, exécutez le script de déploiement et entrez l'adresse IP de l'hôte (par exemple, `10.10.10.10`).

```
tar xvf draas_package.tar
Navigate to the directory and run the deploy script as below:
sudo sh deploy.sh
```

3. Accédez à l'interface utilisateur à l'aide des informations d'identification suivantes :
   - Nom d'utilisateur: `admin`
   - Mot de passe: `admin`



Configuration DRO

Une fois Azure NetApp Files et AVS correctement configurés, vous pouvez commencer à configurer DRO pour automatiser la récupération des charges de travail du site AVS principal vers le site AVS secondaire. NetApp recommande de déployer l'agent DRO sur le site AVS secondaire et de configurer la connexion de passerelle ExpressRoute afin que l'agent DRO puisse communiquer via le réseau avec les composants AVS et Azure NetApp Files appropriés.

La première étape consiste à ajouter des informations d'identification. DRO nécessite une autorisation pour découvrir Azure NetApp Files et la solution Azure VMware. Vous pouvez accorder les autorisations requises à un compte Azure en créant et en configurant une application Azure Active Directory (AD) et en obtenant les informations d'identification Azure dont DRO a besoin. Vous devez lier le principal du service à votre abonnement Azure et lui attribuer un rôle personnalisé disposant des autorisations requises. Lorsque vous ajoutez des environnements source et de destination, vous êtes invité à sélectionner les informations d'identification associées au principal du service. Vous devez ajouter ces informations d'identification à DRO avant de pouvoir cliquer sur Ajouter un nouveau site.

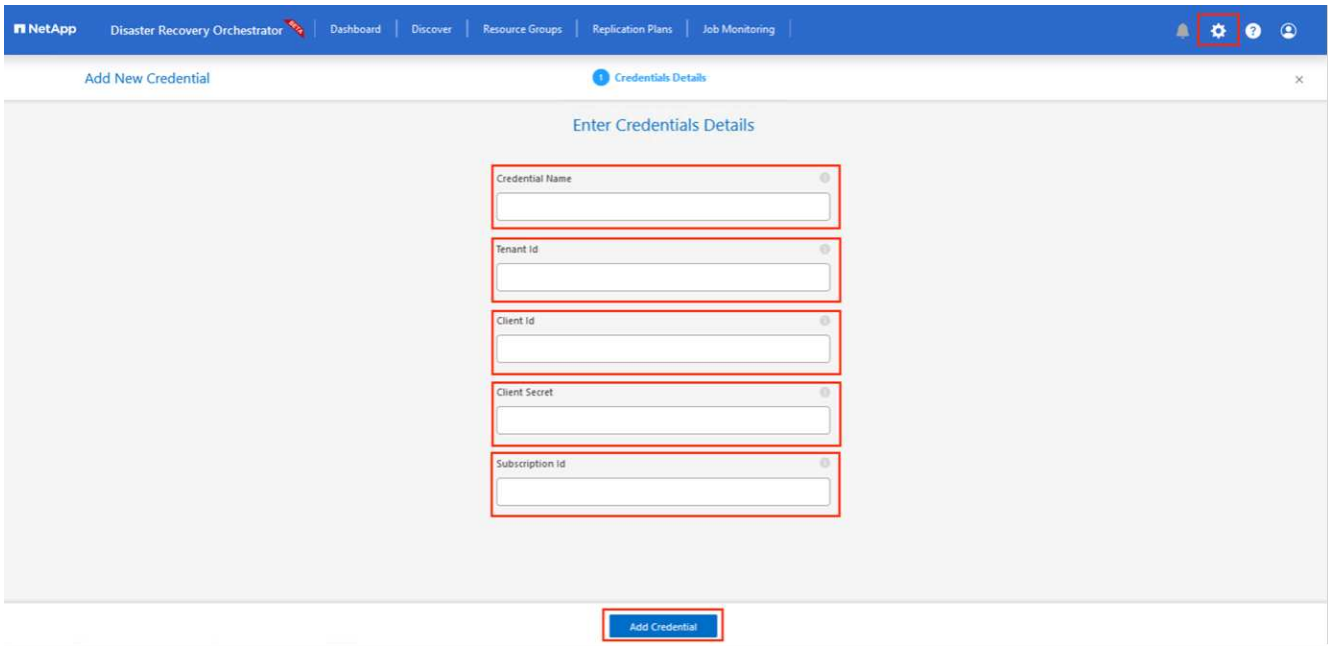
Pour effectuer cette opération, procédez comme suit :

1. Ouvrez DRO dans un navigateur pris en charge et utilisez le nom d'utilisateur et le mot de passe par

défaut/`admin`/`admin`). Le mot de passe peut être réinitialisé après la première connexion à l'aide de l'option Modifier le mot de passe.

2. Dans le coin supérieur droit de la console DRO, cliquez sur l'icône **Paramètres** et sélectionnez **Informations d'identification**.
3. Cliquez sur Ajouter de nouvelles informations d'identification et suivez les étapes de l'assistant.
4. Pour définir les informations d'identification, entrez les informations sur le principal du service Azure Active Directory qui accorde les autorisations requises :
   - Nom d'identification
   - ID du locataire
   - ID client
   - Secret client
   - ID d'abonnement

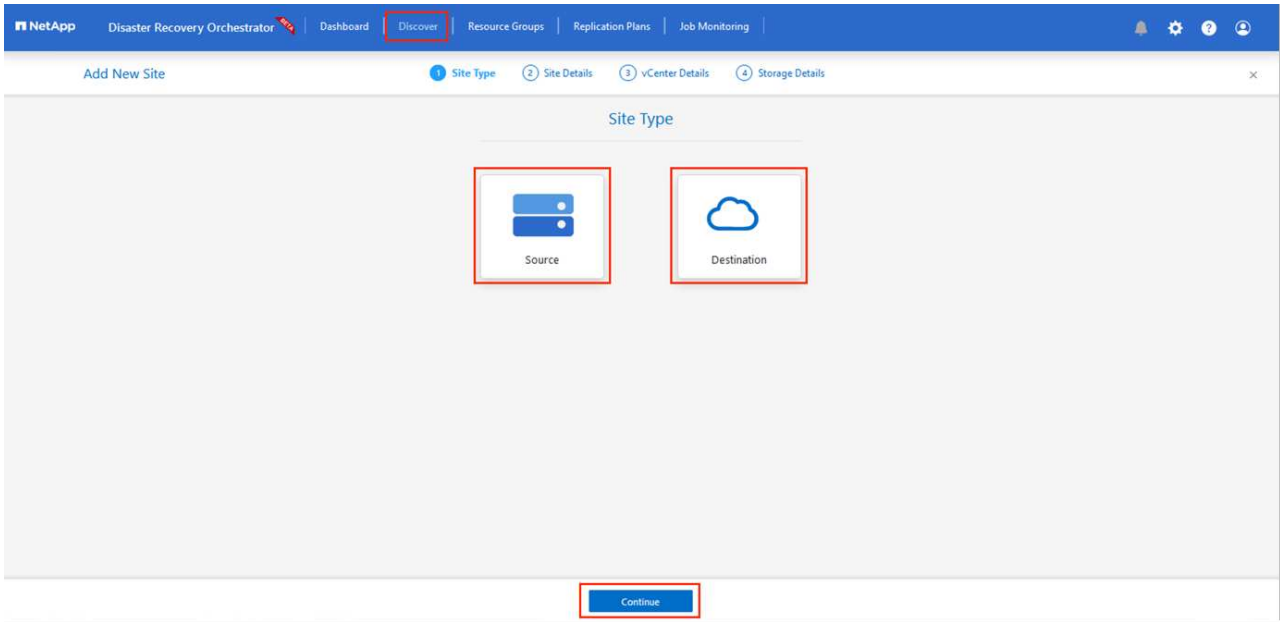
     Vous auriez dû capturer ces informations lorsque vous avez créé l'application AD.
5. Confirmez les détails des nouvelles informations d'identification et cliquez sur Ajouter des informations d'identification.



Après avoir ajouté les informations d'identification, il est temps de découvrir et d'ajouter les sites AVS principal et secondaire (vCenter et le compte de stockage des fichiers Azure NetApp) à DRO. Pour ajouter le site source et le site de destination, procédez comme suit :

6. Accédez à l'onglet **Découvrir**.
7. Cliquez sur **Ajouter un nouveau site**.
8. Ajoutez le site AVS principal suivant (désigné comme **Source** dans la console).
   - SDDC vCenter
   - Compte de stockage Azure NetApp Files
9. Ajoutez le site AVS secondaire suivant (désigné comme **Destination** dans la console).

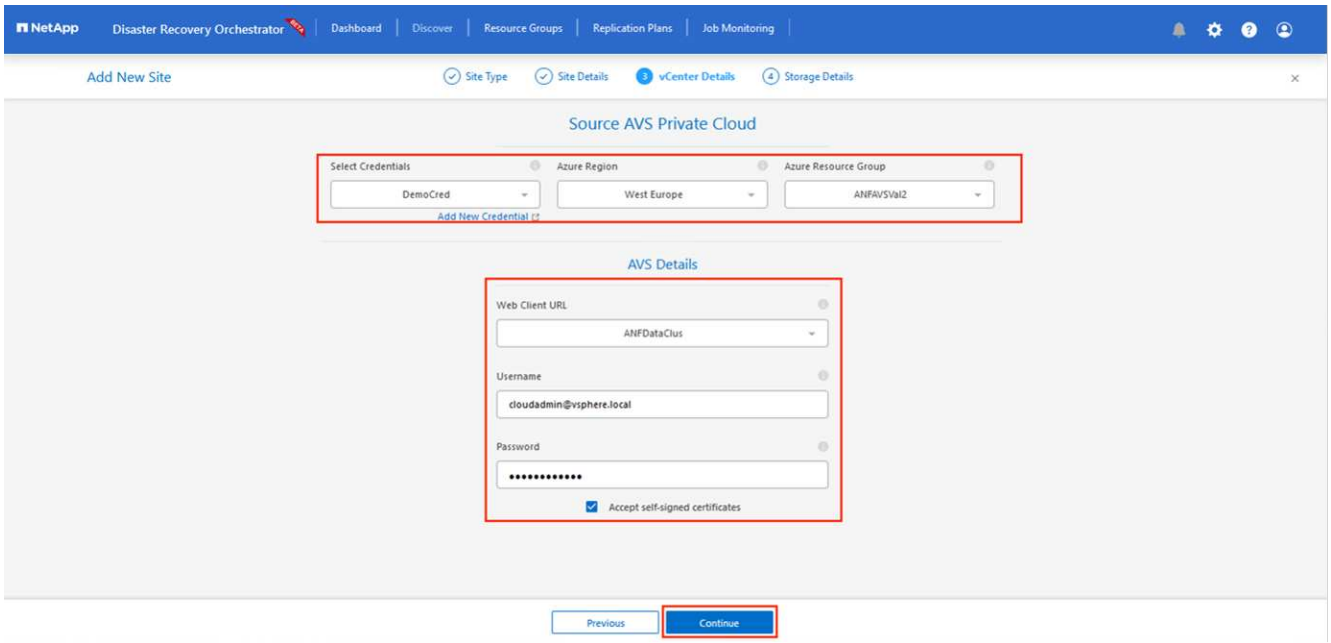
- SDDC vCenter
- Compte de stockage Azure NetApp Files



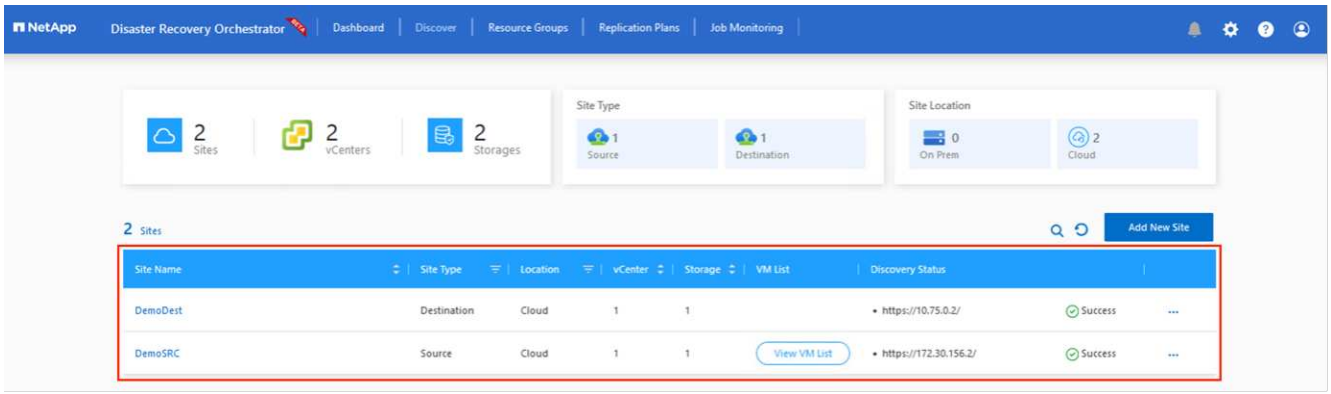
10. Ajoutez les détails du site en cliquant sur **Source**, en saisissant un nom de site convivial et en sélectionnant le connecteur. Cliquez ensuite sur **Continuer**.

> À des fins de démonstration, l'ajout d'un site source est abordé dans ce document.

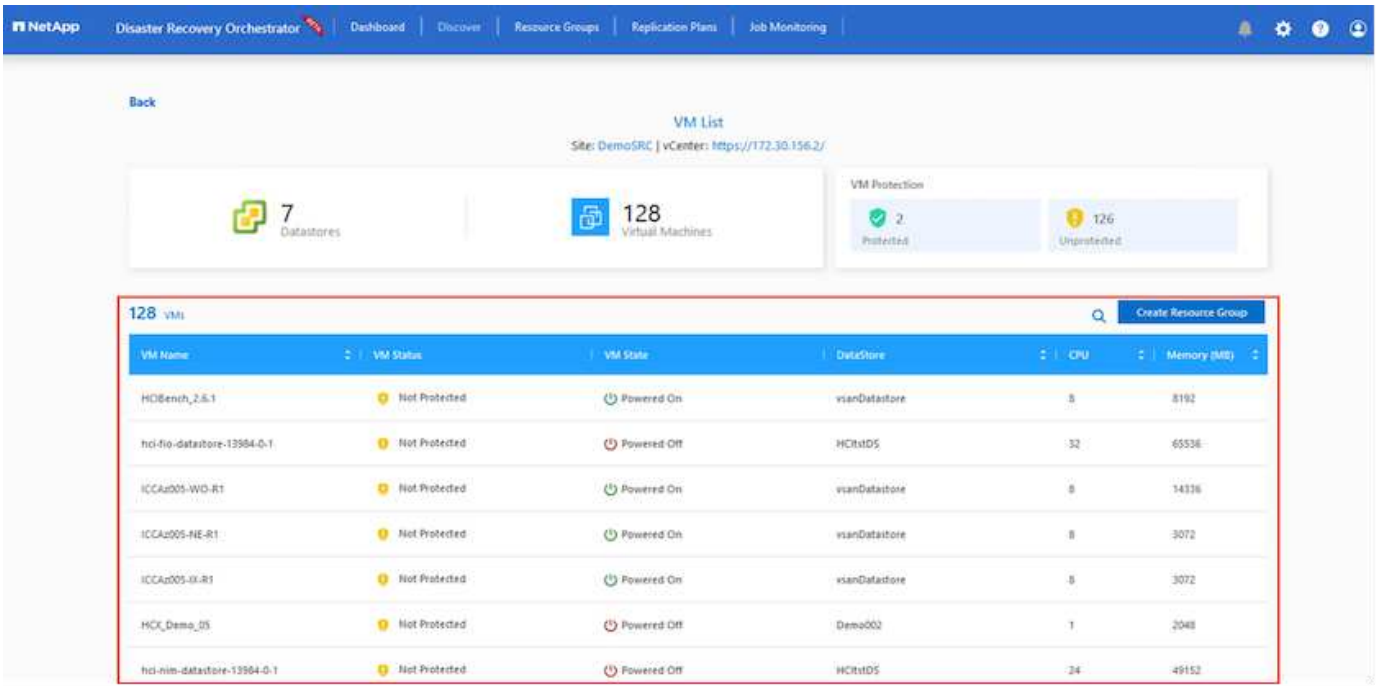
11. Mettre à jour les détails de vCenter. Pour ce faire, sélectionnez les informations d'identification, la région Azure et le groupe de ressources dans la liste déroulante du SDDC AVS principal.
12. DRO répertorie tous les SDDC disponibles dans la région. Sélectionnez l'URL du cloud privé désigné dans la liste déroulante.
13. Entrez le `cloudadmin@vsphere.local` informations d'identification de l'utilisateur. Vous pouvez y accéder depuis le portail Azure. Suivez les étapes mentionnées dans ce "lien" . Une fois terminé, cliquez sur **Continuer**.



14. Sélectionnez les détails du stockage source (ANF) en sélectionnant le groupe de ressources Azure et le compte NetApp .
15. Cliquez sur **Créer un site**.



Une fois ajouté, DRO effectue une découverte automatique et affiche les machines virtuelles qui ont des répliques interrégionales correspondantes du site source au site de destination. DRO détecte automatiquement les réseaux et les segments utilisés par les machines virtuelles et les remplit.



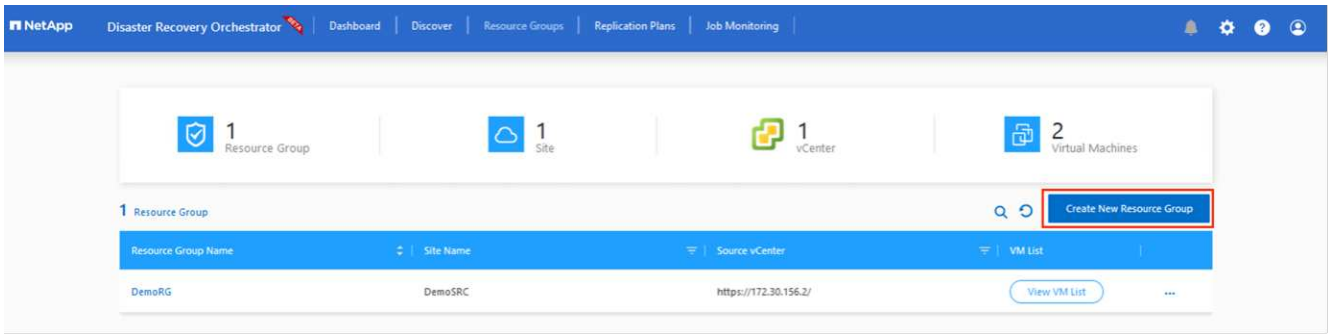
L'étape suivante consiste à regrouper les machines virtuelles requises dans leurs groupes fonctionnels en tant que groupes de ressources.

Groupements de ressources

Une fois les plates-formes ajoutées, regroupez les machines virtuelles que vous souhaitez récupérer dans des groupes de ressources. Les groupes de ressources DRO vous permettent de regrouper un ensemble de machines virtuelles dépendantes en groupes logiques contenant leurs ordres de démarrage, leurs délais de démarrage et leurs validations d'application facultatives qui peuvent être exécutées lors de la récupération.

Pour commencer à créer des groupes de ressources, cliquez sur l'élément de menu **Créer un nouveau groupe de ressources**.

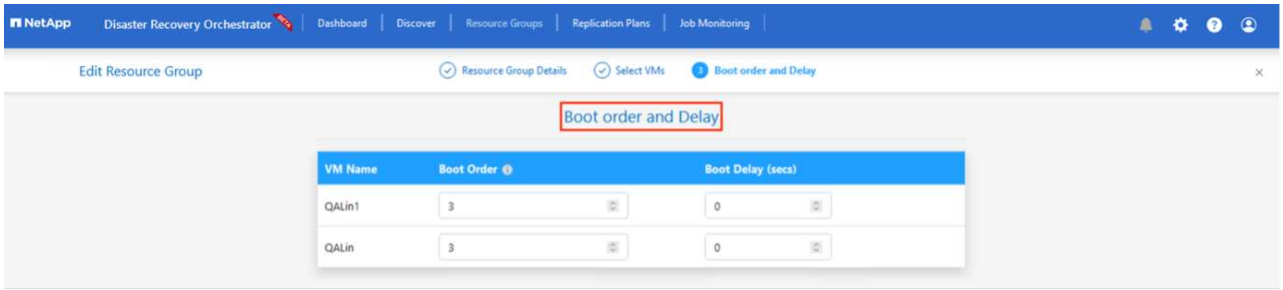
1. Accédez aux **Groupes de ressources** et cliquez sur **Créer un nouveau groupe de ressources**.



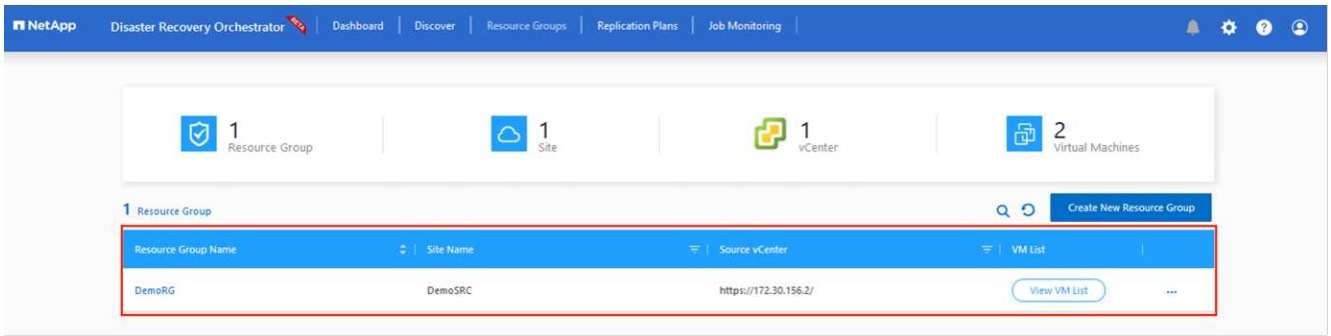
2. Sous Nouveau groupe de ressources, sélectionnez le site source dans la liste déroulante et cliquez sur **Créer**.
3. Fournissez les détails du groupe de ressources et cliquez sur **Continuer**.
4. Sélectionnez les machines virtuelles appropriées à l'aide de l'option de recherche.
5. Sélectionnez l'**Ordre de démarrage** et le **Délai de démarrage** (en secondes) pour toutes les machines virtuelles sélectionnées. Définissez l'ordre de la séquence de mise sous tension en sélectionnant chaque

machine virtuelle et en définissant sa priorité. La valeur par défaut pour toutes les machines virtuelles est 3. Les options sont les suivantes :

- La première machine virtuelle à s'allumer
- Défaut
- La dernière machine virtuelle à s'allumer



6. Cliquez sur **Créer un groupe de ressources**.

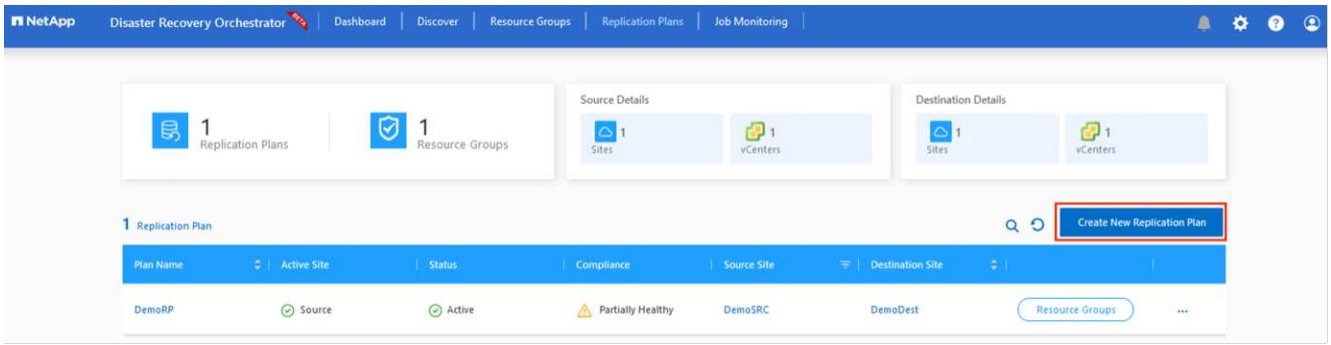


Plans de réplication

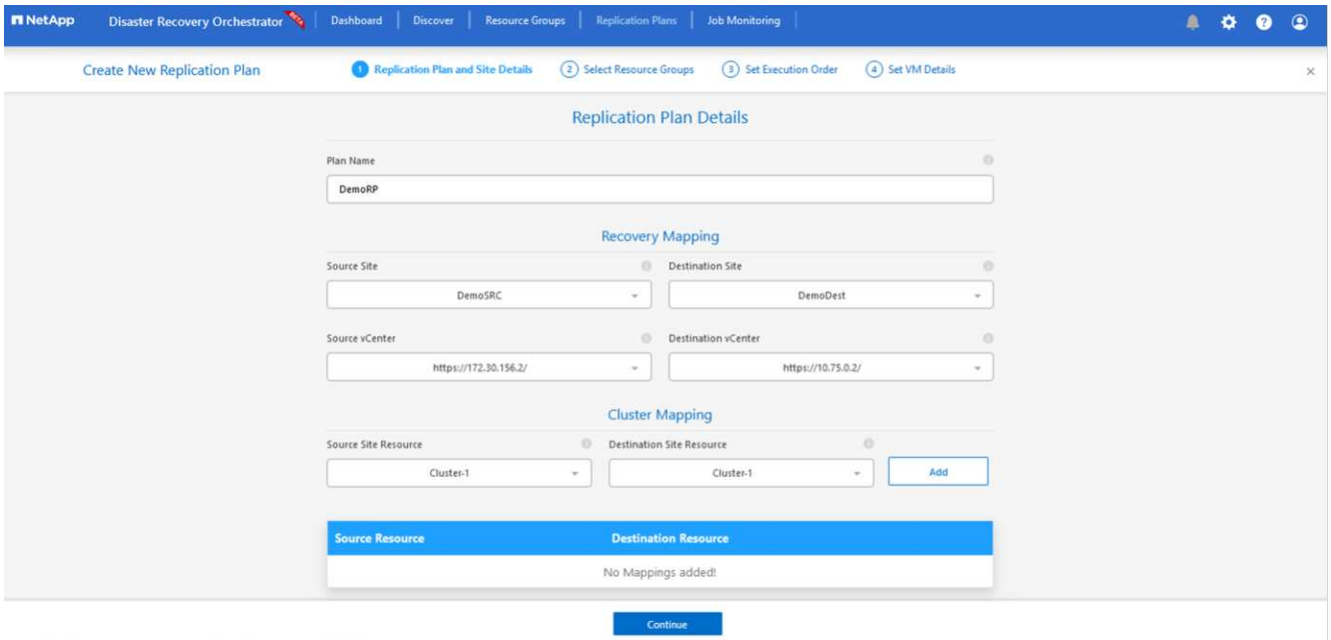
Vous devez disposer d'un plan pour récupérer les applications en cas de sinistre. Sélectionnez les plates-formes vCenter source et de destination dans la liste déroulante, choisissez les groupes de ressources à inclure dans ce plan et incluez également le regroupement de la manière dont les applications doivent être restaurées et mises sous tension (par exemple, contrôleurs de domaine, niveau 1, niveau 2, etc.). Les plans sont souvent également appelés schémas directeurs. Pour définir le plan de récupération, accédez à l'onglet Plan de réplication et cliquez sur **Nouveau plan de réplication**.

Pour commencer à créer un plan de réplication, procédez comme suit :

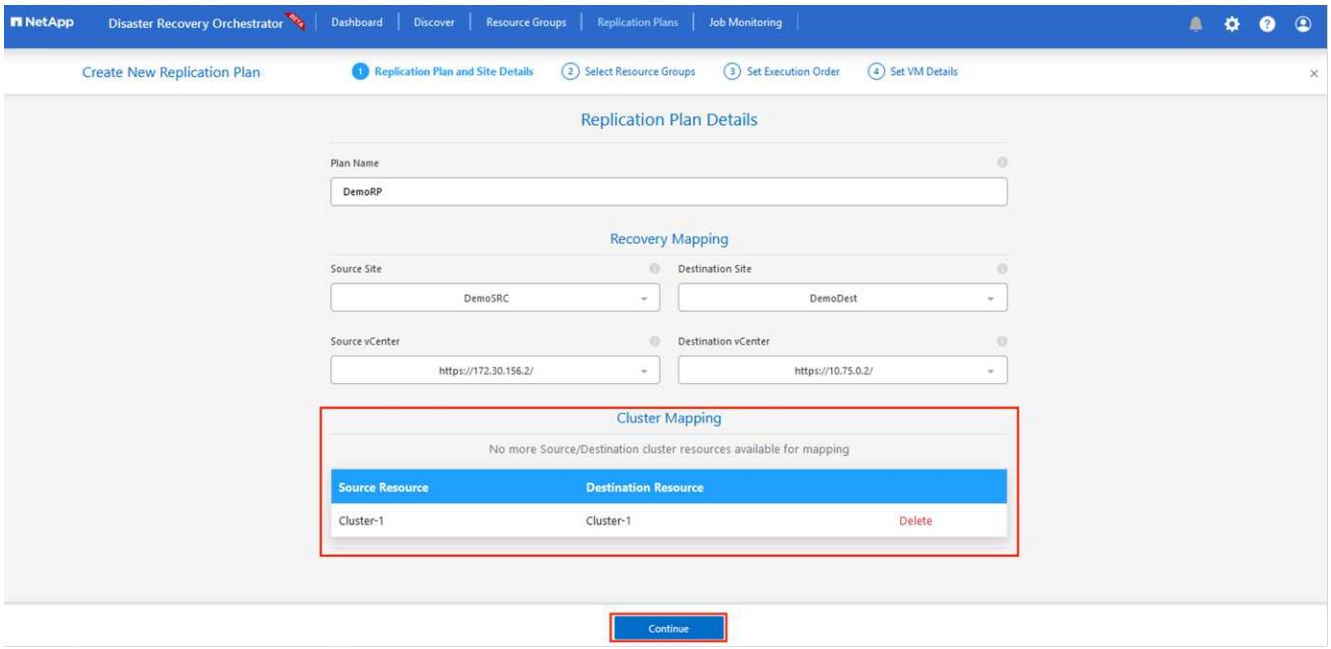
1. Accédez à **Plans de réplication** et cliquez sur **Créer un nouveau plan de réplication**.



2. Dans le **Nouveau plan de réplication**, indiquez un nom pour le plan et ajoutez des mappages de récupération en sélectionnant le site source, le vCenter associé, le site de destination et le vCenter associé.

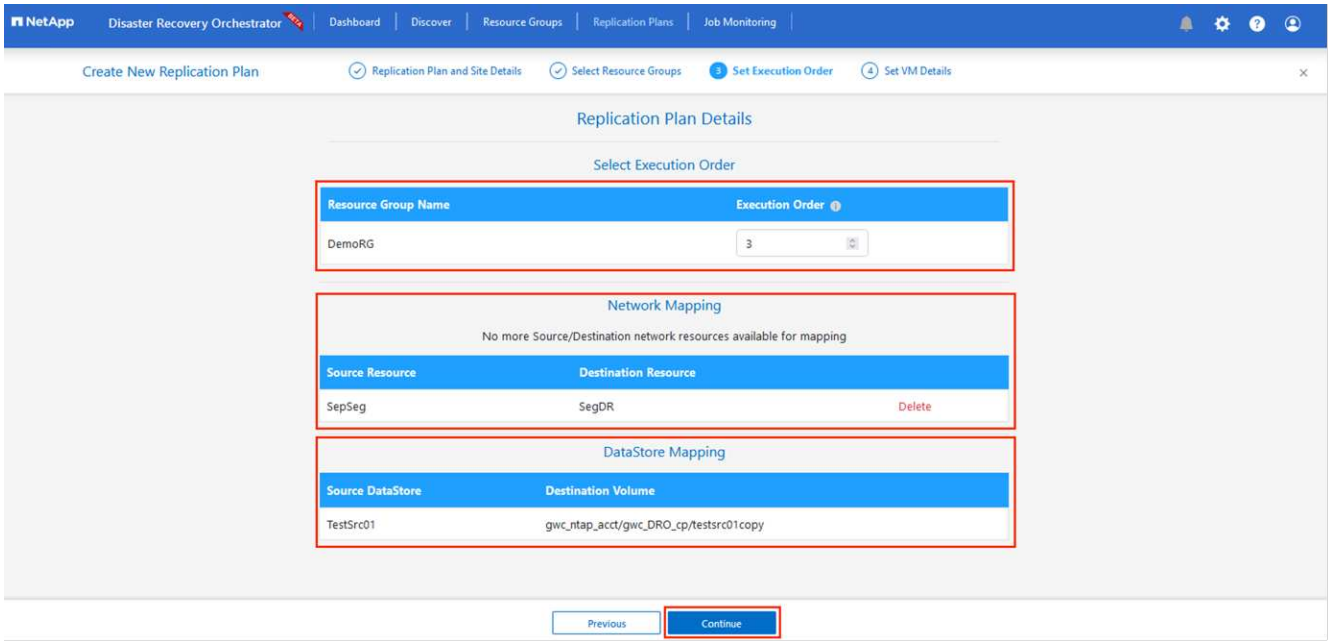


3. Une fois le mappage de récupération terminé, sélectionnez le **Mappage de cluster**.

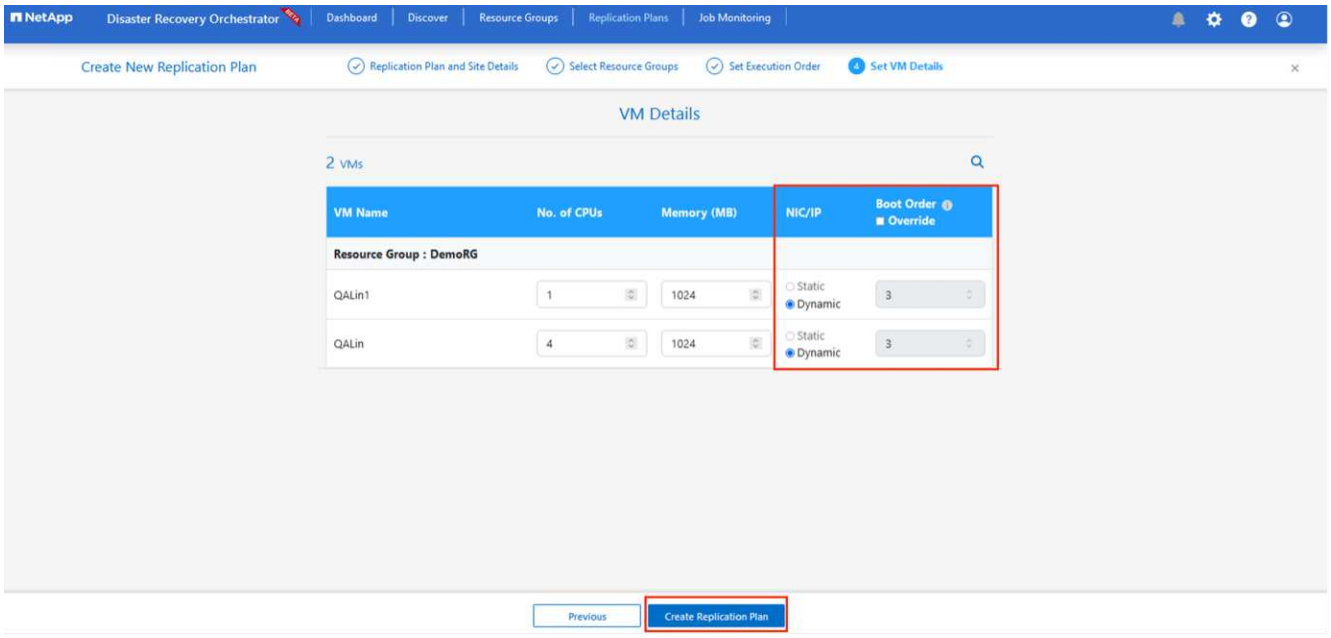


4. Sélectionnez **Détails du groupe de ressources** et cliquez sur **Continuer**.
5. Définissez l'ordre d'exécution du groupe de ressources. Cette option vous permet de sélectionner la séquence d'opérations lorsque plusieurs groupes de ressources existent.
6. Une fois terminé, définissez le mappage réseau sur le segment approprié. Les segments doivent déjà être provisionnés sur le cluster AVS secondaire et, pour mapper les machines virtuelles à ceux-ci, sélectionnez le segment approprié.
7. Les mappages de magasins de données sont automatiquement sélectionnés en fonction de la sélection des machines virtuelles.

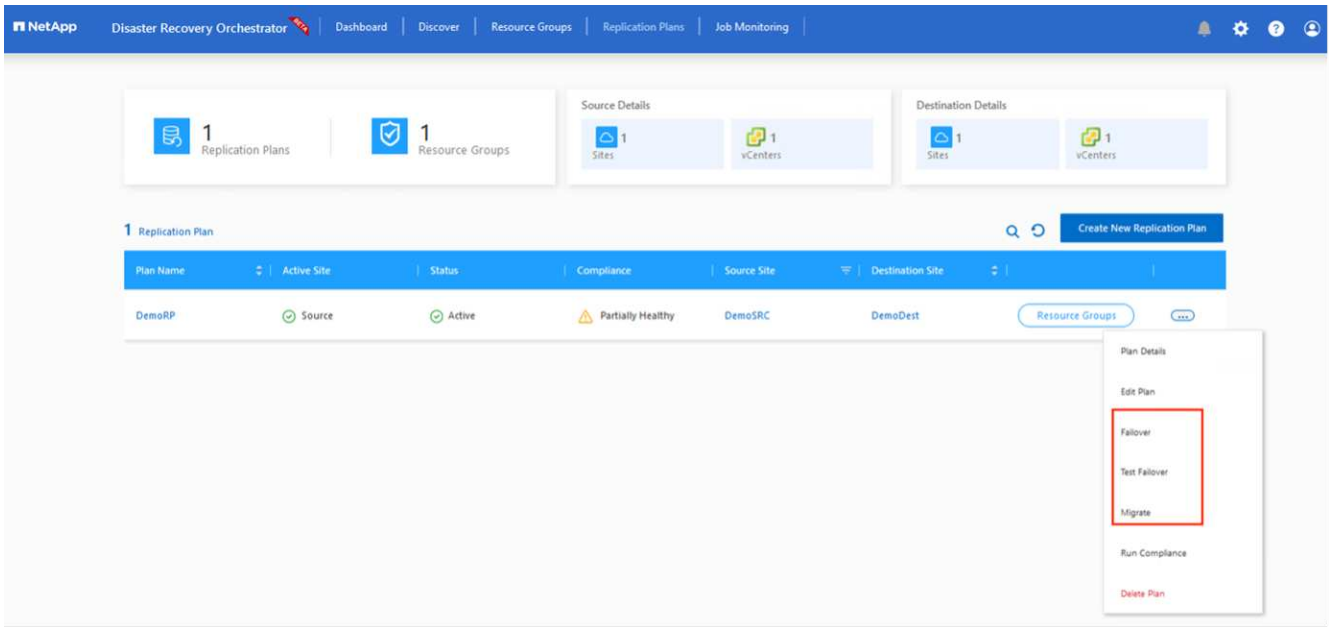
La réplication interrégionale (CRR) se fait au niveau du volume. Par conséquent, toutes les machines virtuelles résidant sur le volume respectif sont répliquées vers la destination CRR. Assurez-vous de sélectionner toutes les machines virtuelles qui font partie du magasin de données, car seules les machines virtuelles qui font partie du plan de réplication sont traitées.



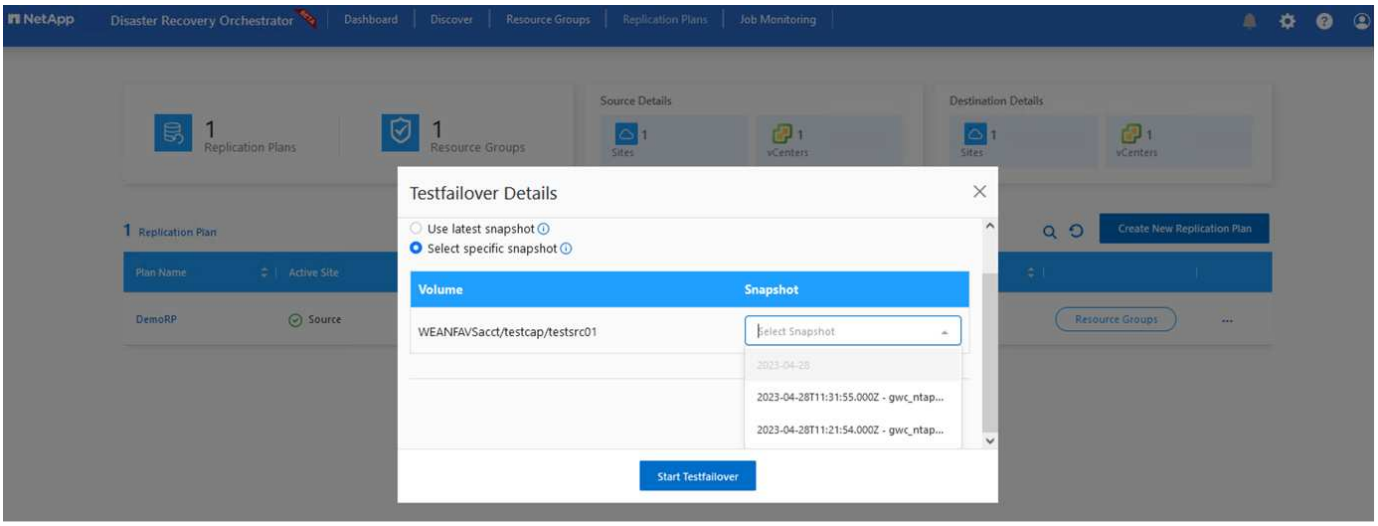
8. Sous les détails de la machine virtuelle, vous pouvez éventuellement redimensionner les paramètres CPU et RAM des machines virtuelles. Cela peut être très utile lorsque vous récupérez de grands environnements vers des clusters cibles plus petits ou lorsque vous effectuez des tests DR sans avoir à provisionner une infrastructure VMware physique individuelle. Modifiez également l'ordre de démarrage et le délai de démarrage (en secondes) pour toutes les machines virtuelles sélectionnées dans les groupes de ressources. Il existe une option supplémentaire pour modifier l'ordre de démarrage si des modifications sont nécessaires par rapport à ce que vous avez sélectionné lors de la sélection de l'ordre de démarrage du groupe de ressources. Par défaut, l'ordre de démarrage sélectionné lors de la sélection du groupe de ressources est utilisé, mais toutes les modifications peuvent être effectuées à ce stade.



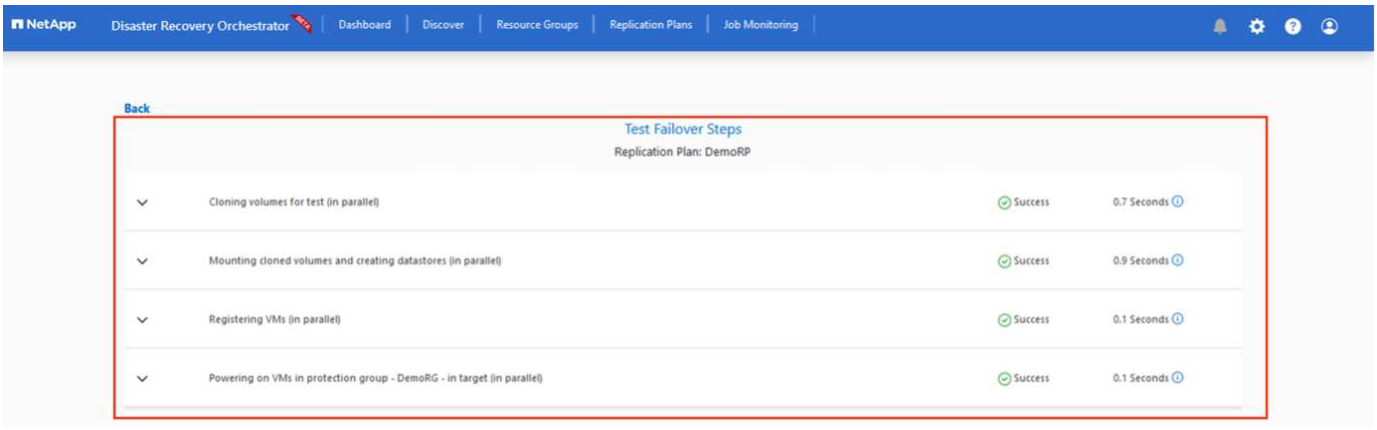
9. Cliquez sur **Créer un plan de réplication**. Une fois le plan de réplication créé, vous pouvez exercer les options de basculement, de test de basculement ou de migration en fonction de vos besoins.



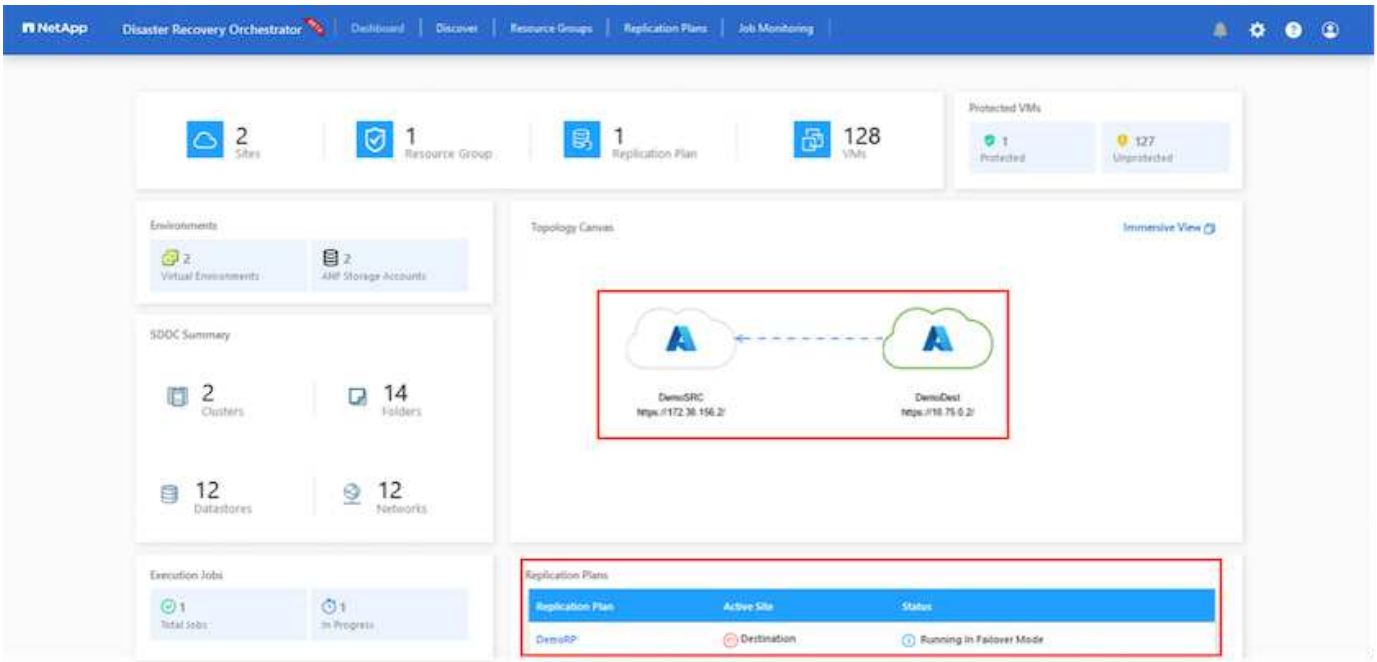
Lors des options de basculement et de test de basculement, l'instantané le plus récent est utilisé ou un instantané spécifique peut être sélectionné à partir d'un instantané ponctuel. L'option ponctuelle peut être très bénéfique si vous êtes confronté à un événement de corruption comme un ransomware, où les répliques les plus récentes sont déjà compromises ou cryptées. DRO affiche tous les points de temps disponibles.



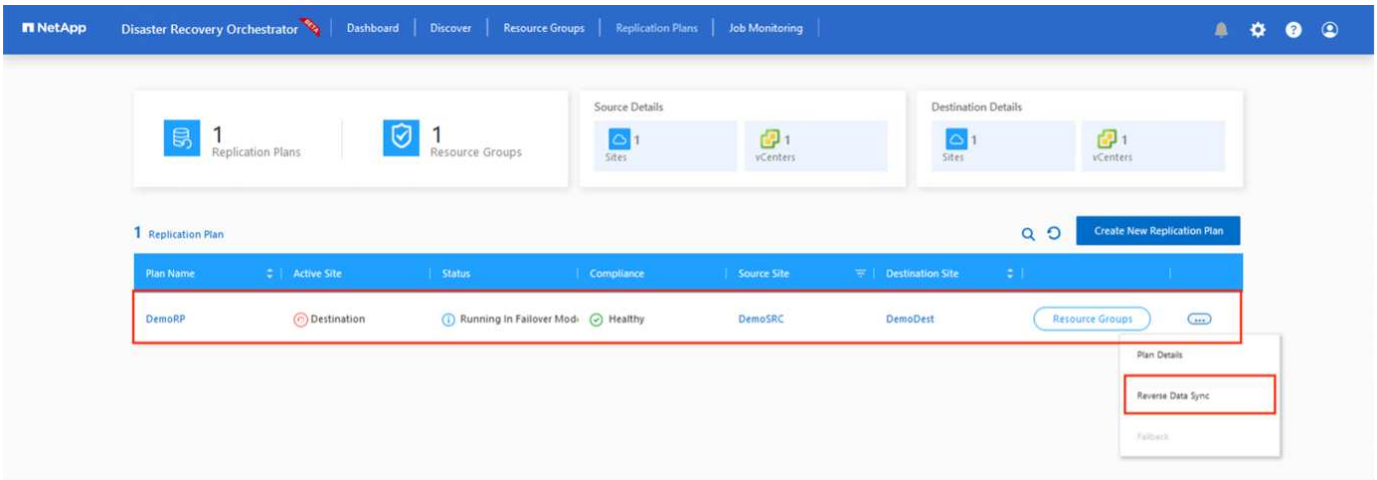
Pour déclencher un basculement ou un test de basculement avec la configuration spécifiée dans le plan de réplication, vous pouvez cliquer sur **Basculement** ou **Tester le basculement**. Vous pouvez surveiller le plan de réplication dans le menu des tâches.



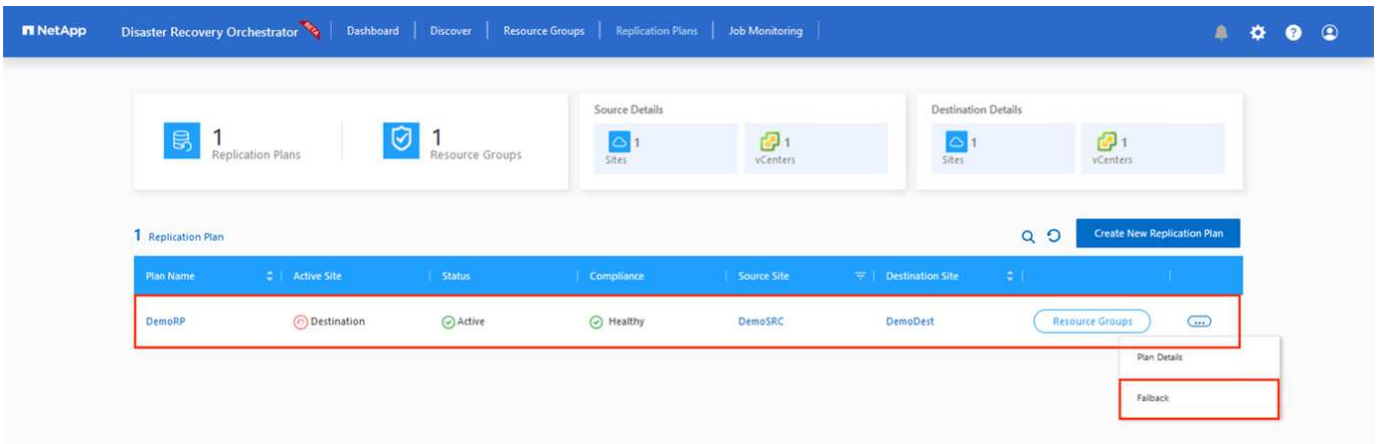
Une fois le basculement déclenché, les éléments récupérés peuvent être vus dans le site secondaire AVS SDDC vCenter (machines virtuelles, réseaux et banques de données). Par défaut, les machines virtuelles sont récupérées dans le dossier Workload.

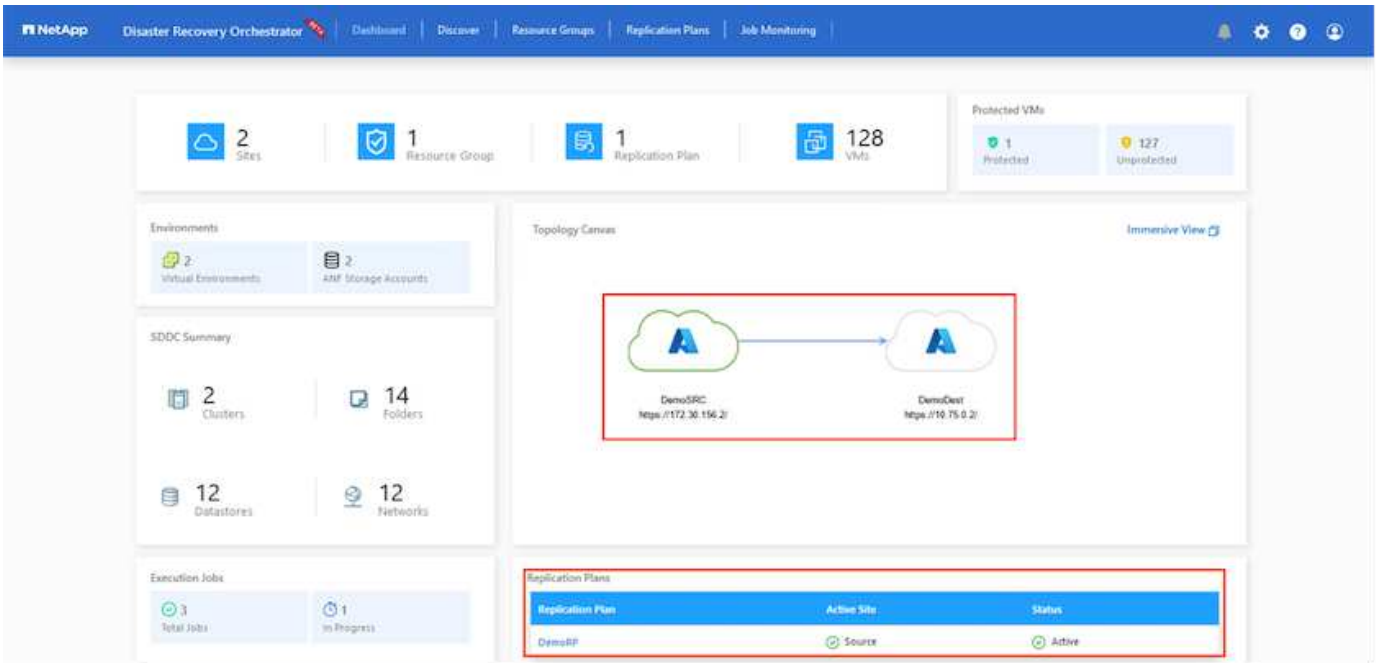


La restauration peut être déclenchée au niveau du plan de réplication. En cas de basculement de test, l'option de suppression peut être utilisée pour annuler les modifications et supprimer le volume nouvellement créé. Les retours en arrière liés au basculement sont un processus en deux étapes. Sélectionnez le plan de réplication et sélectionnez **Synchronisation des données inversées**.



Une fois cette étape terminée, déclenchez la restauration automatique pour revenir au site AVS principal.





À partir du portail Azure, nous pouvons voir que l'intégrité de la réplication a été interrompue pour les volumes appropriés qui ont été mappés au site secondaire AVS SDDC en tant que volumes de lecture/écriture. Lors du basculement de test, DRO ne mappe pas le volume de destination ou de réplication. Au lieu de cela, il crée un

nouveau volume de l'instantané de réplication interrégional requis et expose le volume en tant que banque de données, ce qui consomme une capacité physique supplémentaire du pool de capacité et garantit que le volume source n'est pas modifié. En particulier, les tâches de réplication peuvent se poursuivre pendant les tests DR ou les flux de travail de triage. De plus, ce processus garantit que la récupération peut être nettoyée sans risque de destruction de la réplique en cas d'erreurs ou de récupération de données corrompues.

Récupération après un ransomware

Se remettre d'un ransomware peut être une tâche ardue. Plus précisément, il peut être difficile pour les organisations informatiques d'identifier précisément le point de retour sûr et, une fois celui-ci déterminé, de garantir que les charges de travail récupérées sont protégées contre les attaques récurrentes (par exemple, contre des logiciels malveillants dormants ou via des applications vulnérables).

DRO répond à ces préoccupations en permettant aux organisations de récupérer à partir de n'importe quel moment disponible. Les charges de travail sont ensuite récupérées sur des réseaux fonctionnels et pourtant isolés, de sorte que les applications peuvent fonctionner et communiquer entre elles mais ne sont exposées à aucun trafic nord-sud. Ce processus offre aux équipes de sécurité un endroit sûr pour effectuer des analyses médico-légales et identifier tout logiciel malveillant caché ou dormant.

Conclusion

La solution de reprise après sinistre Azure NetApp Files et Azure VMware vous offre les avantages suivants :

- Tirez parti d'une réplication interrégionale Azure NetApp Files efficace et résiliente.
- Récupérez à n'importe quel moment disponible avec la conservation des instantanés.
- Automatisez entièrement toutes les étapes requises pour récupérer des centaines à des milliers de machines virtuelles à partir des étapes de stockage, de calcul, de réseau et de validation des applications.
- La récupération de la charge de travail exploite le processus « Créer de nouveaux volumes à partir des instantanés les plus récents », qui ne manipule pas le volume répliqué.
- Évitez tout risque de corruption de données sur les volumes ou les snapshots.
- Évitez les interruptions de réplication pendant les flux de travail de test DR.
- Exploitez les données DR et les ressources de calcul cloud pour les flux de travail au-delà de la DR, tels que le développement/test, les tests de sécurité, les tests de correctifs et de mise à niveau et les tests de correction.
- L'optimisation du processeur et de la RAM peut contribuer à réduire les coûts du cloud en permettant la récupération vers des clusters de calcul plus petits.

Où trouver des informations supplémentaires

Pour en savoir plus sur les informations décrites dans ce document, consultez les documents et/ou sites Web suivants :

- Créer une réplication de volume pour Azure NetApp Files

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-create-peering"

- Réplication interrégionale des volumes Azure NetApp Files

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-introduction#service-level-objectives"

- "Solution Azure VMware"

  "https://learn.microsoft.com/en-us/azure/azure-vmware/introduction"

- Déployer et configurer l'environnement de virtualisation sur Azure

  "Configurer AVS sur Azure"

- Déployer et configurer la solution Azure VMware

  https://learn.microsoft.com/en-us/azure/azure-vmware/deploy-azure-vmware-solution?tabs=azure-portal

Informations sur le copyright

Copyright © 2025 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 DÉLICTUELLE (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.