



# Utiliser NetApp Disaster Recovery

## NetApp Disaster Recovery

NetApp

January 12, 2026

This PDF was generated from <https://docs.netapp.com/fr-fr/data-services-disaster-recovery/use/use-overview.html> on January 12, 2026. Always check docs.netapp.com for the latest.

# Sommaire

Utiliser NetApp Disaster Recovery .....	1
Présentation de NetApp Disaster Recovery .....	1
Consultez l'état de vos plans de NetApp Disaster Recovery sur le tableau de bord .....	1
Ajouter des vCenters à un site dans NetApp Disaster Recovery .....	2
Ajouter un mappage de sous-réseau pour un site vCenter .....	6
Modifier le site du serveur vCenter et personnaliser le calendrier de découverte .....	8
Actualiser la découverte manuellement .....	10
Créer un groupe de ressources pour organiser les machines virtuelles ensemble dans NetApp Disaster Recovery .....	11
Créer un plan de réplication dans NetApp Disaster Recovery .....	15
Créer le plan .....	16
Modifier les plannings pour tester la conformité et garantir le fonctionnement des tests de basculement .....	30
Répliquer des applications vers un autre site avec NetApp Disaster Recovery .....	32
Migrer des applications vers un autre site avec NetApp Disaster Recovery .....	32
Basculez les applications vers un site distant avec NetApp Disaster Recovery .....	33
Tester le processus de basculement .....	33
Nettoyer l'environnement de test après un test de basculement .....	34
Basculer le site source vers un site de reprise après sinistre .....	34
Restaurez les applications à la source d'origine avec NetApp Disaster Recovery .....	36
À propos du failback .....	37
Avant de commencer .....	37
Étapes .....	37
Gérez les sites, les groupes de ressources, les plans de réplication, les banques de données et les informations sur les machines virtuelles avec NetApp Disaster Recovery .....	37
Gérer les sites vCenter .....	38
Gérer les groupes de ressources .....	38
Gérer les plans de réplication .....	39
Afficher les informations sur les magasins de données .....	41
Afficher les informations sur les machines virtuelles .....	42
Surveiller les tâches de NetApp Disaster Recovery .....	42
Voir les offres d'emploi .....	42
Annuler un travail .....	42
Créer des rapports de NetApp Disaster Recovery .....	43

# Utiliser NetApp Disaster Recovery

## Présentation de NetApp Disaster Recovery

Grâce à NetApp Disaster Recovery, vous pouvez atteindre les objectifs suivants :

- ["Consultez l'état de vos plans de reprise après sinistre"](#) .
- ["Ajouter des sites vCenter"](#) .
- ["Créer des groupes de ressources pour organiser les machines virtuelles ensemble"](#)
- ["Créer un plan de reprise après sinistre"](#) .
- ["Répliquer les applications VMware"](#) sur votre site principal vers un site distant de reprise après sinistre dans le cloud à l'aide de la réplication SnapMirror .
- ["Migrer les applications VMware"](#) sur votre site principal vers un autre site.
- ["Tester le fail over"](#) sans perturber les machines virtuelles d'origine.
- En cas de catastrophe, ["basculer votre site principal"](#) vers VMware Cloud sur AWS avec FSx pour NetApp ONTAP.
- Une fois la catastrophe résolue, ["retour en arrière"](#) du site de reprise après sinistre au site principal.
- ["Surveiller les opérations de reprise après sinistre"](#) sur la page Suivi des tâches.

## Consultez l'état de vos plans de NetApp Disaster Recovery sur le tableau de bord

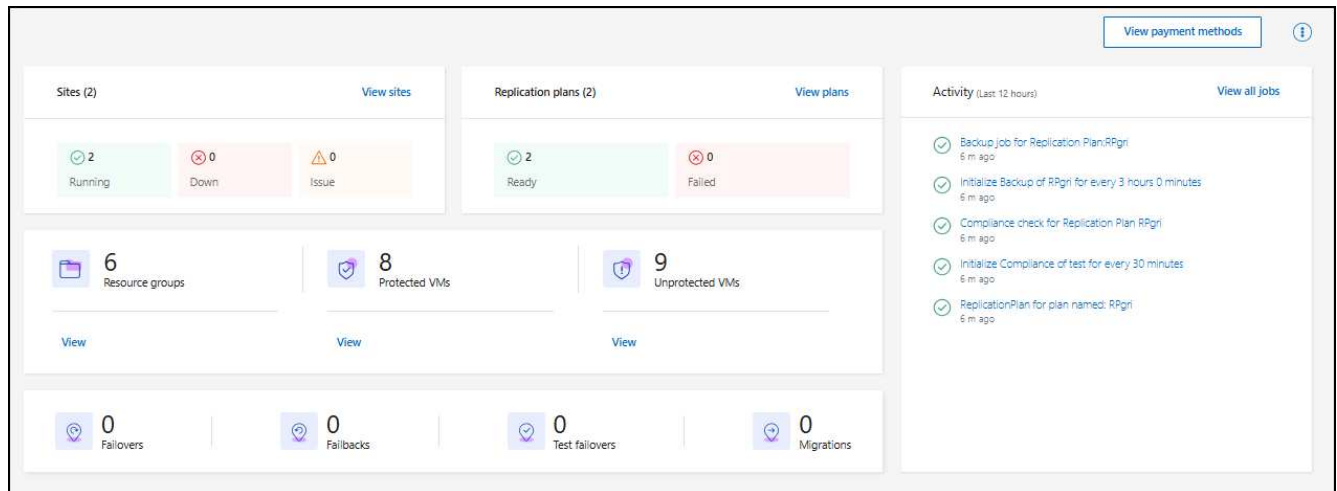
À l'aide du tableau de bord de NetApp Disaster Recovery , vous pouvez déterminer l'état de vos sites de reprise après sinistre et vos plans de réplication. Vous pouvez rapidement déterminer quels sites et quels plans sont sains, déconnectés ou dégradés.

**Rôle de NetApp Console requis** Administrateur d'organisation, Administrateur de dossier ou de projet, Administrateur de reprise après sinistre, Administrateur d'application de reprise après sinistre ou Rôle d'observateur de reprise après sinistre.

["En savoir plus sur les rôles et les autorisations des utilisateurs dans NetApp Disaster Recovery"](#). ["En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services"](#).

### Étapes

1. Connectez-vous à la ["NetApp Console"](#) .
2. Dans la navigation de gauche de la NetApp Console , sélectionnez **Protection > Reprise après sinistre**.
3. Dans le menu NetApp Disaster Recovery , sélectionnez **Tableau de bord**.



4. Consultez les informations suivantes sur le tableau de bord :

- **Sites** : Consultez l'état de santé de vos sites. Un site peut avoir l'un des statuts suivants :
  - **En cours d'exécution** : le vCenter est connecté, sain et en cours d'exécution.
  - **En panne** : Le vCenter n'est pas accessible ou rencontre des problèmes de connectivité.
  - **Problème** : Le vCenter n'est pas accessible ou rencontre des problèmes de connectivité.

Pour voir les détails du site, sélectionnez **Afficher tout** pour un statut ou **Afficher les sites** pour les voir tous.

- **Plans de réplication** : affichez l'état de vos plans. Un plan peut avoir l'un des statuts suivants :
  - **Prêt**
  - **Échoué**

Pour consulter les détails du plan de réplication, sélectionnez **Afficher tout** pour un statut ou **Afficher les plans de réplication** pour les voir tous.

- **Groupes de ressources** : Affichez l'état de vos groupes de ressources. Un groupe de ressources peut avoir l'un des statuts suivants :
- **VM protégées** : Les machines virtuelles font partie d'un groupe de ressources.
- **VM non protégées** : Les machines virtuelles ne font pas partie d'un groupe de ressources.

Pour consulter les détails, sélectionnez le lien **Afficher** sous chaque élément.

- Le nombre de basculements, de basculements de test et de migrations. Par exemple, si vous avez créé deux plans et migré vers les destinations, le nombre de migrations apparaît comme « 2 ».

5. Passez en revue toutes les opérations dans le volet Activité. Pour afficher toutes les opérations sur le moniteur de tâches, sélectionnez **Afficher toutes les tâches**.

## Ajouter des vCenters à un site dans NetApp Disaster Recovery

Avant de pouvoir créer un plan de reprise après sinistre, vous devez ajouter un serveur vCenter principal à un site et un site de reprise après sinistre vCenter cible dans la NetApp Console.



Assurez-vous que les vCenters source et de destination utilisent le même agent de NetApp Console .

Une fois les vCenter ajoutés, NetApp Disaster Recovery effectue une découverte approfondie des environnements vCenter, notamment les clusters vCenter, les hôtes ESXi, les banques de données, l’empreinte de stockage, les détails des machines virtuelles, les répliques SnapMirror et les réseaux de machines virtuelles.

**Rôle de NetApp Console requis** Administrateur d’organisation, administrateur de dossier ou de projet ou administrateur de reprise après sinistre.

["En savoir plus sur les rôles et les autorisations des utilisateurs dans NetApp Disaster Recovery"](#). ["En savoir plus sur les rôles d’accès à la NetApp Console pour tous les services"](#).

### À propos de cette tâche

Si vous avez ajouté des vCenters dans les versions précédentes et que vous souhaitez personnaliser la planification de la découverte, vous devez modifier le site du serveur vCenter et définir la planification.



NetApp Disaster Recovery effectue la découverte une fois toutes les 24 heures. Après avoir configuré un site, vous pouvez ultérieurement modifier le vCenter pour personnaliser le calendrier de découverte qui répond à vos besoins. Par exemple, si vous disposez d’un grand nombre de machines virtuelles, vous pouvez définir la planification de découverte pour qu’elle s’exécute toutes les 23 heures et 59 minutes. Si vous disposez d’un petit nombre de machines virtuelles, vous pouvez définir la planification de découverte pour qu’elle s’exécute toutes les 12 heures. L’intervalle minimum est de 30 minutes et le maximum est de 24 heures.

Vous devez d’abord effectuer quelques découvertes manuelles pour obtenir les informations les plus récentes sur votre environnement. Après cela, vous pouvez définir le calendrier pour qu’il s’exécute automatiquement.

Si vous disposez de vCenters de versions antérieures et que vous souhaitez modifier le moment d’exécution de la découverte, modifiez le site du serveur vCenter et définissez la planification.

Les machines virtuelles nouvellement ajoutées ou supprimées sont reconnues lors de la prochaine découverte planifiée ou lors d’une découverte manuelle immédiate.

Les machines virtuelles ne peuvent être protégées que si le plan de réplication est dans l’un des états suivants :

- Prêt
- Failback validé
- Test de basculement validé

**Clusters vCenter dans un site** Chaque site contient un ou plusieurs vCenter. Ces vCenters utilisent un ou plusieurs clusters de stockage ONTAP pour héberger des banques de données NFS ou VMFS.

Un cluster vCenter ne peut résider que sur un seul site. Vous avez besoin des informations suivantes pour ajouter un cluster vCenter à un site :

- L’adresse IP de gestion vCenter ou FQDN
- Informations d’identification pour un compte vCenter avec les privilèges requis pour effectuer des opérations. Voir ["privilèges vCenter requis"](#) pour plus d’informations.

- Pour les sites VMware hébergés dans le cloud, les clés d'accès au cloud requises
- Un certificat de sécurité pour accéder à votre vCenter.



Le service prend en charge les certificats de sécurité auto-signés ou les certificats provenant d'une autorité de certification centrale (CA).

## Étapes

1. Connectez-vous à la "[NetApp Console](#)".
2. Dans la navigation de gauche de la NetApp Console, sélectionnez **Protection > Reprise après sinistre**.

Si vous utilisez NetApp Disaster Recovery pour la première fois, vous devez ajouter les informations vCenter. Si vous avez déjà ajouté des informations vCenter, vous verrez le tableau de bord.



Différents champs apparaissent en fonction du type de site que vous ajoutez.

3. Si certains sites vCenter existent déjà et que vous souhaitez en ajouter d'autres, dans le menu, sélectionnez **Sites** puis sélectionnez **Ajouter**.
4. Dans la page Sites, sélectionnez le site, puis sélectionnez **Ajouter vCenter**.
5. **Source** : sélectionnez **Découvrir les serveurs vCenter** pour saisir des informations sur le site vCenter source.



Pour ajouter d'autres sites vCenter, sélectionnez **Sites** puis **Ajouter**.

### Add vCenter server

Enter connection details for the vCenter server that is accessible from the Console Agent.

Site	Console Agent
<input type="text" value="sit .gri2"/>	<input type="text" value="DRaaSTest"/>
vCenter IP address	Port
<input type="text"/>	<input type="text" value="443"/>
vCenter user name	vCenter password
<input type="text" value="admin"/>	<input type="password" value="....."/>

☒ Use self-signed certificates ⓘ

ⓘ By default, vCenter discovery will run automatically once every 24 hours. This can be edited later. Discovery can also be triggered manually at any time.

- Sélectionnez un site, puis l'agent NetApp Console , et fournissez les informations d'identification vCenter.
- **Pour les sites sur site uniquement** : Pour accepter les certificats auto-signés pour le vCenter source, cochez la case.



Les certificats auto-signés ne sont pas aussi sécurisés que les autres certificats. Si votre vCenter n'est **PAS** configuré avec des certificats d'autorité de certification (CA), vous devez cocher cette case ; sinon, la connexion au vCenter ne fonctionnera pas.

6. Sélectionnez **Ajouter**.

Ensuite, ajoutez un vCenter cible.

7. Ajoutez à nouveau un site pour le vCenter cible.

8. Sélectionnez à nouveau **Ajouter vCenter** et ajoutez les informations du vCenter cible.

9. **Cible**:

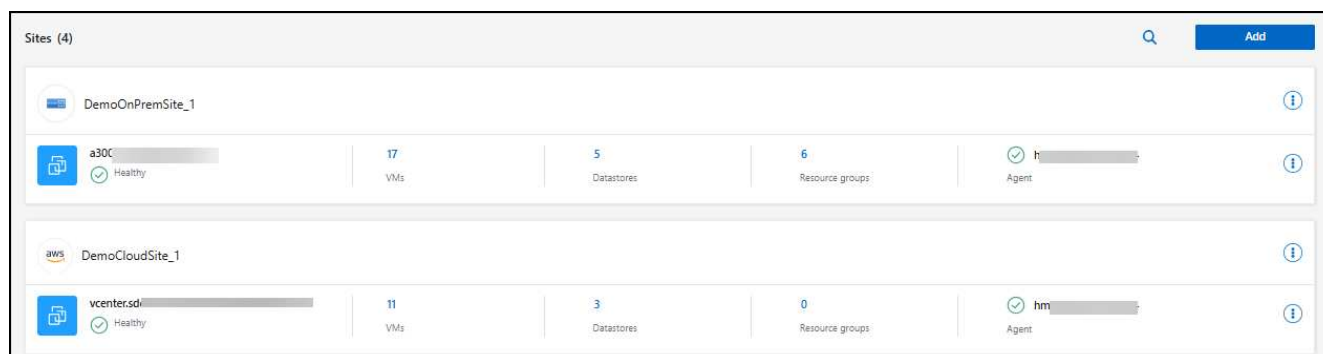
a. Choisissez le site cible et l'emplacement. Si la cible est le cloud, sélectionnez **AWS**.

- (S'applique uniquement aux sites cloud) **Jeton API** : saisissez le jeton API pour autoriser l'accès au service pour votre organisation. Créez le jeton API en fournissant des rôles d'organisation et de service spécifiques.

- (S'applique uniquement aux sites cloud) **ID d'organisation long** : saisissez l'ID unique de l'organisation. Vous pouvez identifier cet ID en cliquant sur le nom d'utilisateur dans la section Compte de la NetApp Console.

b. Sélectionnez **Ajouter**.

Les vCenters source et cible apparaissent dans la liste des sites.



10. Pour voir la progression de l'opération, dans le menu, sélectionnez **Suivi des tâches**.

## Ajouter un mappage de sous-réseau pour un site vCenter

Vous pouvez gérer les adresses IP lors des opérations de basculement à l'aide du mappage de sous-réseaux, qui vous permet d'ajouter des sous-réseaux pour chaque vCenter. Lorsque vous faites cela, vous définissez le CIDR IPv4, la passerelle par défaut et le DNS pour chaque réseau virtuel.

En cas de basculement, NetApp Disaster Recovery utilise le CIDR du réseau mappé pour attribuer à chaque vNIC une nouvelle adresse IP.

Par exemple:

- RéseauA = 10.1.1.0/24
- RéseauB = 192.168.1.0/24

VM1 dispose d'une vNIC (10.1.1.50) connectée à NetworkA. NetworkA est mappé à NetworkB dans les paramètres du plan de réplication.

Lors du basculement, NetApp Disaster Recovery remplace la partie réseau de l'adresse IP d'origine (10.1.1) et conserve l'adresse hôte (.50) de l'adresse IP d'origine (10.1.1.50). Pour VM1, NetApp Disaster Recovery examine les paramètres CIDR pour NetworkB et utilise la partie réseau NetworkB 192.168.1 tout en conservant la partie hôte (.50) pour créer la nouvelle adresse IP pour VM1. La nouvelle IP devient 192.168.1.50.


En résumé, l'adresse de l'hôte reste la même, tandis que l'adresse réseau est remplacée par celle configurée dans le mappage de sous-réseau du site. Cela vous permet de gérer plus facilement la réaffectation des adresses IP lors du basculement, en particulier si vous avez des centaines de réseaux et des milliers de machines virtuelles à gérer.

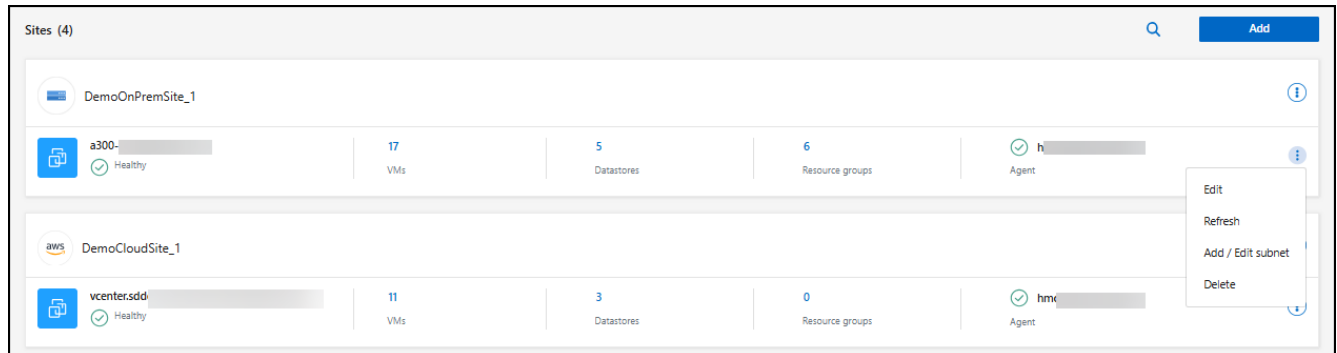
L'utilisation du mappage de sous-réseau est un processus facultatif en deux étapes :

- Tout d'abord, ajoutez le mappage de sous-réseau pour chaque site vCenter.
- Deuxièmement, dans le plan de réplication, indiquez que vous souhaitez utiliser le mappage de sous-réseau dans l'onglet Machines virtuelles et le champ IP cible.

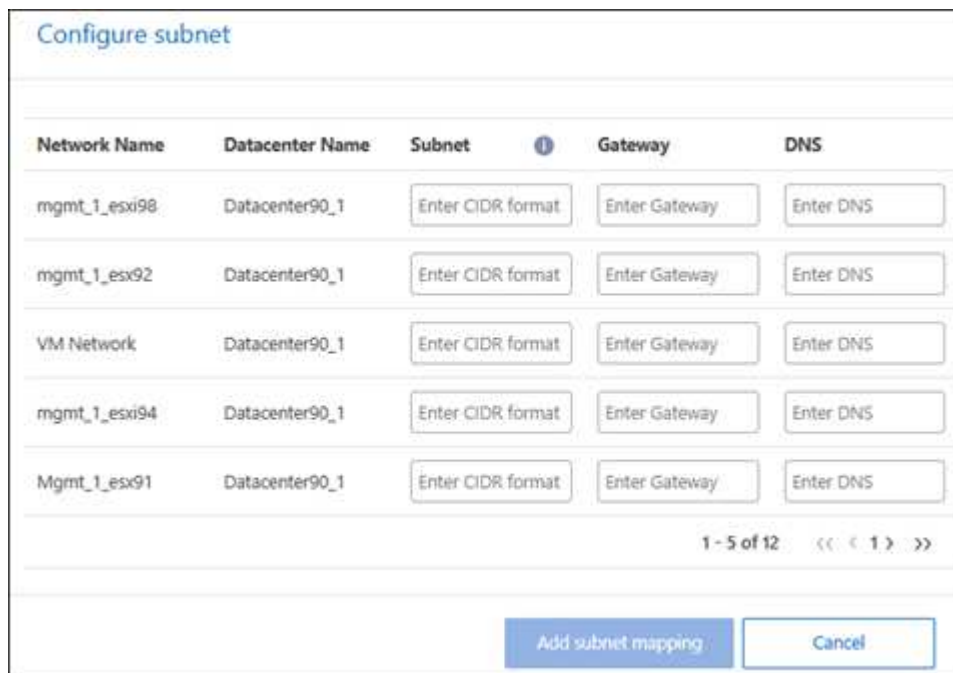


## Étapes

1. Dans le menu NetApp Disaster Recovery , sélectionnez **Sites**.
2. Des actions  icône sur la droite, sélectionnez **Ajouter un sous-réseau**.



La page Configurer le sous-réseau s'affiche :



Network Name	Datacenter Name	Subnet	Gateway	DNS
mgmt_1_esxi98	Datacenter90_1	Enter CIDR format	Enter Gateway	Enter DNS
mgmt_1_esx92	Datacenter90_1	Enter CIDR format	Enter Gateway	Enter DNS
VM Network	Datacenter90_1	Enter CIDR format	Enter Gateway	Enter DNS
mgmt_1_esxi94	Datacenter90_1	Enter CIDR format	Enter Gateway	Enter DNS
Mgmt_1_esx91	Datacenter90_1	Enter CIDR format	Enter Gateway	Enter DNS

1 - 5 of 12 << < 1 > >>

Add subnet mapping Cancel

3. Dans la page Configurer le sous-réseau, saisissez les informations suivantes :
  - a. Sous-réseau : saisissez le CIDR IPv4 pour le sous-réseau jusqu'à /32.



La notation CIDR est une méthode de spécification des adresses IP et de leurs masques de réseau. Le /24 désigne le masque de réseau. Le numéro se compose d'une adresse IP avec le numéro après le « / » indiquant combien de bits de l'adresse IP désignent le réseau. Par exemple, 192.168.0.50/24, l'adresse IP est 192.168.0.50 et le nombre total de bits dans l'adresse réseau est 24. 192.168.0.50 255.255.255.0 devient 192.168.0.0/24.

- b. Passerelle : saisissez la passerelle par défaut pour le sous-réseau.
- c. DNS : saisissez le DNS du sous-réseau.

4. Sélectionnez **Ajouter un mappage de sous-réseau**.

### Sélectionner le mappage de sous-réseau pour un plan de réplication

Lorsque vous créez un plan de réplication, vous pouvez sélectionner le mappage de sous-réseau pour le plan de réplication.

L'utilisation du mappage de sous-réseau est un processus facultatif en deux étapes :

- Tout d'abord, ajoutez le mappage de sous-réseau pour chaque site vCenter.
- Deuxièmement, dans le plan de réplication, indiquez que vous souhaitez utiliser le mappage de sous-réseau.

### Étapes

1. Dans le menu NetApp Disaster Recovery , sélectionnez **Plans de réplication**.
2. Sélectionnez **Ajouter** pour ajouter un plan de réplication.
3. Remplissez les champs de la manière habituelle en ajoutant les serveurs vCenter, en sélectionnant les groupes de ressources ou les applications et en complétant les mappages.
4. Dans la page Plan de réplication > Mappage des ressources, sélectionnez la section **Machines virtuelles**.

Virtual machines

IP address type: Static

Target IP: Use subnet mapping

*When a subnet exhausts its IP addresses, you cannot add more VMs to it. New VMs must connect to a different subnet with available IP addresses, which can be an existing alternative subnet or a newly created one.*

☐ Use the same credentials for all VMs

☐ Use Windows LAPS

☐ Use the same script for all VMs

Target VM prefix: Optional

Target VM suffix: Optional

Preview: Sample VM name

5. Dans le champ **IP cible**, sélectionnez **Utiliser le mappage de sous-réseau** dans la liste déroulante.



S'il existe deux machines virtuelles (par exemple, l'une est Linux et l'autre est Windows), les informations d'identification ne sont nécessaires que pour Windows.

6. Continuez avec la création du plan de réplication.

### Modifier le site du serveur vCenter et personnaliser le calendrier de découverte


Vous pouvez modifier le site du serveur vCenter pour personnaliser la planification de la découverte. Par exemple, si vous disposez d'un grand nombre de machines virtuelles, vous pouvez définir la planification de

découverte pour qu'elle s'exécute toutes les 23 heures et 59 minutes. Si vous disposez d'un petit nombre de machines virtuelles, vous pouvez définir la planification de découverte pour qu'elle s'exécute toutes les 12 heures.

Si vous disposez de vCenters de versions antérieures et que vous souhaitez modifier le moment d'exécution de la découverte, modifiez le site du serveur vCenter et définissez la planification.

Si vous ne souhaitez pas planifier la découverte, vous pouvez désactiver l'option de découverte planifiée et actualiser la découverte manuellement à tout moment.

### Étapes

1. Dans le menu NetApp Disaster Recovery , sélectionnez **Sites**.
2. Sélectionnez le site que vous souhaitez modifier.
3. Sélectionnez les actions  icône sur la droite et sélectionnez **Modifier**.
4. Dans la page Modifier le serveur vCenter, modifiez les champs selon vos besoins.
5. Pour personnaliser le calendrier de découverte, cochez la case **Activer la découverte planifiée** et sélectionnez l'intervalle de date et d'heure souhaité.

## Edit vCenter server

Enter connection details for the vCenter server that is accessible from the BlueXP Connector.

Site

Source

BlueXP Connector

SecLab\_Connector\_4

vCenter IP address

172.26.212.218

port

443

vCenter user name

vCenter password

☒ Use self-signed certificates ⓘ
   
☒ Enable scheduled discovery
   

Start discovery from

2025-04-02

 ⓘ

12

 : 

00

AM

 ⓘ

Run discovery once every

23

 Hour(s)

59

 Minute(s)

Save

Cancel

6. Sélectionnez **Enregistrer**.


## Actualiser la découverte manuellement

Vous pouvez actualiser la découverte manuellement à tout moment. Ceci est utile si vous avez ajouté ou supprimé des machines virtuelles et que vous souhaitez mettre à jour les informations dans NetApp Disaster Recovery.

### Étapes

1. Dans le menu NetApp Disaster Recovery , sélectionnez **Sites**.
2. Sélectionnez le site que vous souhaitez actualiser.

3.

Sélectionnez les actions  icône sur la droite et sélectionnez **Actualiser**.

## Créer un groupe de ressources pour organiser les machines virtuelles ensemble dans NetApp Disaster Recovery

Après avoir ajouté des sites vCenter, vous pouvez créer des groupes de ressources pour protéger les machines virtuelles par machine virtuelle ou par banque de données en tant qu'unité unique. Les groupes de ressources vous permettent d'organiser un ensemble de machines virtuelles dépendantes en groupes logiques qui répondent à vos besoins. Par exemple, vous pouvez regrouper les machines virtuelles associées à une application ou regrouper les applications ayant des niveaux similaires. À titre d'exemple, les groupes peuvent contenir des ordres de démarrage différés qui peuvent être exécutés lors de la récupération.

**Rôle de NetApp Console requis** Rôle d'administrateur d'organisation, d'administrateur de dossier ou de projet, d'administrateur de reprise après sinistre ou d'administrateur d'application de reprise après sinistre.

["En savoir plus sur les rôles et les autorisations des utilisateurs dans NetApp Disaster Recovery"](#). ["En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services"](#).

### À propos de cette tâche

Vous pouvez regrouper les machines virtuelles elles-mêmes ou les machines virtuelles dans des magasins de données.

Vous pouvez créer des groupes de ressources à l'aide des méthodes suivantes :

- À partir de l'option Groupes de ressources
- Pendant que vous créez un plan de reprise après sinistre ou de réplication. Si vous disposez d'un grand nombre de machines virtuelles hébergées par un cluster vCenter source, il peut être plus simple de créer les groupes de ressources pendant que vous créez le plan de réplication. Pour obtenir des instructions sur la création de groupes de ressources lors de la création d'un plan de réplication, consultez ["Créer un plan de réplication"](#).



Chaque groupe de ressources peut inclure une ou plusieurs machines virtuelles ou banques de données. Les machines virtuelles s'allumeront en fonction de la séquence dans laquelle vous les incluez dans le plan de réplication. Vous pouvez modifier l'ordre en faisant glisser les machines virtuelles ou les banques de données vers le haut ou vers le bas de la liste des groupes de ressources.

### À propos des groupes de ressources

Les groupes de ressources vous permettent de combiner des machines virtuelles ou des banques de données en une seule unité.

Par exemple, une application de point de vente peut utiliser plusieurs machines virtuelles pour les bases de données, la logique métier et les vitrines. Vous pouvez gérer toutes ces machines virtuelles avec un seul groupe de ressources. Configurez des groupes de ressources pour appliquer les règles du plan de réplication pour l'ordre de démarrage des machines virtuelles, la connexion réseau et la récupération de toutes les

machines virtuelles nécessaires à l'application.

### Comment ça marche ?

NetApp Disaster Recovery protège les machines virtuelles en répliquant les volumes ONTAP sous-jacents et les LUN hébergeant les machines virtuelles dans le groupe de ressources. Pour ce faire, le système interroge vCenter pour connaître le nom de chaque magasin de données hébergeant des machines virtuelles dans un groupe de ressources. NetApp Disaster Recovery identifie ensuite le volume ONTAP source ou le LUN hébergeant ce magasin de données. Toute la protection est effectuée au niveau du volume ONTAP à l'aide de la réplication SnapMirror .

Si les machines virtuelles du groupe de ressources sont hébergées sur différents magasins de données, NetApp Disaster Recovery utilise l'une des méthodes suivantes pour créer un instantané cohérent avec les données des volumes ONTAP ou des LUN.

Emplacement relatif des volumes FlexVol	Processus de réplication d'instantanés
Plusieurs magasins de données - Volumes FlexVol dans le <b>même SVM</b>	<ul style="list-style-type: none"><li>• Groupe de cohérence ONTAP créé</li><li>• Instantanés du groupe de cohérence pris</li><li>• Réplication SnapMirror à l'échelle du volume effectuée</li></ul>
Plusieurs magasins de données - Volumes FlexVol dans <b>plusieurs SVM</b>	<ul style="list-style-type: none"><li>• API ONTAP : <code>cg_start</code> . Met en veille tous les volumes afin que des instantanés puissent être pris et lance des instantanés à l'échelle du volume de tous les volumes du groupe de ressources.</li><li>• API ONTAP : <code>cg_end</code> . Reprend les E/S sur tous les volumes et active la réplication SnapMirror au niveau du volume après la prise des snapshots.</li></ul>

Lorsque vous créez des groupes de ressources, tenez compte des points suivants :

- Avant d'ajouter des banques de données à des groupes de ressources, démarrez d'abord une découverte manuelle ou une découverte planifiée des machines virtuelles. Cela garantit que les machines virtuelles sont découvertes et répertoriées dans le groupe de ressources. Si vous ne démarrez pas une découverte manuelle, les machines virtuelles risquent de ne pas être répertoriées dans le groupe de ressources.
- Assurez-vous qu'il existe au moins une machine virtuelle dans le magasin de données. S'il n'y a aucune machine virtuelle dans le magasin de données, Disaster Recovery ne découvre pas le magasin de données.
- Un seul magasin de données ne doit pas héberger de machines virtuelles protégées par plusieurs plans de réplication.
- N'hébergez pas de machines virtuelles protégées et non protégées sur le même magasin de données. Si des machines virtuelles protégées et non protégées sont hébergées sur le même magasin de données, les problèmes suivants peuvent survenir :
  - Étant donné que NetApp Disaster Recovery utilise SnapMirror et que le système réplique l'intégralité des volumes ONTAP , la capacité utilisée de ce volume est utilisée pour les considérations de licence. Dans ce cas, l'espace de volume consommé par les machines virtuelles protégées et non protégées serait inclus dans ce calcul.
  - Si le groupe de ressources et ses banques de données associées doivent être basculés vers le site de reprise après sinistre, toutes les machines virtuelles non protégées (machines virtuelles ne faisant pas partie du groupe de ressources, mais hébergées sur le volume ONTAP ) n'existeront plus sur le site

source à partir du processus de basculement, ce qui entraînera l'échec des machines virtuelles non protégées sur le site source. De plus, NetApp Disaster Recovery ne démarrera pas ces machines virtuelles non protégées sur le site vCenter de basculement.

- Pour qu'une machine virtuelle soit protégée, elle doit être incluse dans un groupe de ressources.

**MEILLEURE PRATIQUE** : Organisez vos machines virtuelles avant de déployer NetApp Disaster Recovery afin de minimiser la « prolifération des banques de données ». Placez les machines virtuelles qui ont besoin d'être protégées sur un sous-ensemble de banques de données et placez les machines virtuelles qui ne seront pas protégées sur un autre sous-ensemble de banques de données. Assurez-vous que les machines virtuelles d'un magasin de données donné ne sont pas protégées par des plans de réplication différents.

## Étapes

1. Connectez-vous à la "[NetApp Console](#)".
2. Dans la navigation de gauche de la NetApp Console, sélectionnez **Protection > Reprise après sinistre**.
3. Dans le menu NetApp Disaster Recovery, sélectionnez **Groupe de ressources**.
4. Sélectionnez **Ajouter**.
5. Saisissez un nom pour le groupe de ressources.
6. Sélectionnez le cluster vCenter source où se trouvent les machines virtuelles.
7. Sélectionnez **Machines virtuelles** ou **Magasins de données** selon la manière dont vous souhaitez effectuer la recherche.
8. Sélectionnez l'onglet **Ajouter des groupes de ressources**. Le système répertorie tous les magasins de données ou machines virtuelles du cluster vCenter sélectionné. Si vous avez sélectionné **Datastores**, le système répertorie tous les magasins de données du cluster vCenter sélectionné. Si vous avez sélectionné **Machines virtuelles**, le système répertorie toutes les machines virtuelles du cluster vCenter sélectionné.
9. Sur le côté gauche de la page Ajouter des groupes de ressources, sélectionnez les machines virtuelles que vous souhaitez protéger.

## Add resource group

Name  vCenter

☒ Virtual machines ☐ Datastores

Select virtual machines

Search all datastores

- ☒ VMFS\_Centos\_vm1\_ds4
- ☒ VMFS\_Centos\_vm1\_ds5
- ☒ VMFS\_RHEL\_vm2\_ds1
- ☐ VMFS\_RHEL\_vm2\_ds2
- ☐ VMFS\_RHEL\_vm2\_ds3
- ☐ VMFS\_RHEL\_vm2\_ds4
- ☐ VMFS\_RHEL\_vm2\_ds5

**Selected VMs (3)**

VMFS_Centos_vm1_ds4	×
VMFS_Centos_vm1_ds5	×
VMFS_RHEL_vm2_ds1	×

## Add resource group

Name  vCenter

☐ Virtual machines ☒ Datastores

Select datastores

Search datastores

- ☐ DS4\_auto\_vmfs\_6d7
- ☐ DS2\_auto\_vmfs\_6d7
- ☐ DS1\_surya\_nfs\_scale
- ☒ DS4\_auto\_nfs\_450
- ☒ DS3\_auto\_nfs\_450
- ☐ DS1\_auto\_nfs\_450
- ☐ DS2\_auto\_nfs\_450

**Selected datastores (2)**

DS4_auto_nfs_450	×
DS3_auto_nfs_450	×



10. Vous pouvez également modifier l'ordre des machines virtuelles sur la droite en faisant glisser chaque machine virtuelle vers le haut ou vers le bas de la liste. Les machines virtuelles s'allumeront en fonction de la séquence dans laquelle vous les incluez.
11. Sélectionnez **Ajouter**.

## Créer un plan de réplication dans NetApp Disaster Recovery

Une fois les sites vCenter ajoutés, vous êtes prêt à créer un plan de reprise après sinistre ou un plan de réplication. Les plans de réplication gèrent la protection des données de l'infrastructure VMware. Sélectionnez les vCenters source et de destination, choisissez les groupes de ressources et déterminez la manière dont les applications doivent être restaurées et mises sous tension. Par exemple, vous pouvez regrouper des machines virtuelles (VM) associées à une application ou regrouper des applications ayant des niveaux similaires. De tels plans sont parfois appelés *plans*.

**Rôle de NetApp Console requis** Administrateur d'organisation, Administrateur de dossier ou de projet, Administrateur de reprise après sinistre, Administrateur de basculement de reprise après sinistre ou Administrateur d'application de reprise après sinistre.

["En savoir plus sur les rôles et les autorisations des utilisateurs dans NetApp Disaster Recovery"](#). ["En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services"](#).

### À propos de cette tâche

Vous pouvez créer un plan de réplication et également modifier les calendriers de conformité et de test. Exécutez des tests de basculement de machines virtuelles sans affecter les charges de travail de production.

Vous pouvez protéger plusieurs machines virtuelles sur plusieurs banques de données. NetApp Disaster Recovery crée des groupes de cohérence ONTAP pour tous les volumes ONTAP hébergeant des banques de données de machines virtuelles protégées.

Les machines virtuelles ne peuvent être protégées que si le plan de réplication est dans l'un des états suivants :

- Prêt
- Failback validé
- Test de basculement validé


### Instantanés du plan de réplication

La récupération après sinistre conserve le même nombre de snapshots sur les clusters source et de destination. Par défaut, le service exécute un processus de réconciliation de snapshots toutes les 24 heures pour garantir que le nombre de snapshots sur les clusters source et de destination est le même.

Les situations suivantes peuvent entraîner une différence dans le nombre de snapshots entre les clusters source et de destination :

- Certaines situations peuvent amener les opérations ONTAP en dehors de la reprise après sinistre à ajouter ou supprimer des snapshots du volume :

- S'il manque des instantanés sur le site source, les instantanés correspondants sur le site de destination peuvent être supprimés, en fonction de la stratégie SnapMirror par défaut pour la relation.
- S'il manque des instantanés sur le site de destination, le service peut supprimer les instantanés correspondants sur le site source lors du prochain processus de rapprochement d'instantanés planifié, en fonction de la stratégie SnapMirror par défaut pour la relation.
- Une réduction du nombre de rétentions d'instantanés du plan de réplication peut amener le service à supprimer les instantanés les plus anciens sur les sites source et de destination pour respecter le nombre de rétention nouvellement réduit.

Dans ces cas, Disaster Recovery supprime les anciens snapshots des clusters source et de destination lors de la prochaine vérification de cohérence. Ou, l'administrateur peut effectuer un nettoyage instantané immédiat en sélectionnant **Actions\***  **icône sur le plan de réplication et en sélectionnant \*Nettoyer les snapshots.**

Le service effectue des contrôles de symétrie des instantanés toutes les 24 heures.

### Avant de commencer

- Avant de créer une relation SnapMirror, configurez le cluster et le peering SVM en dehors de Disaster Recovery.
- Avec Google Cloud, vous ne pouvez ajouter qu'un seul volume ou datastore à un plan de réplication.



Organisez vos machines virtuelles avant de déployer NetApp Disaster Recovery afin de minimiser la prolifération des datastores. Placez les machines virtuelles qui ont besoin d'être protégées sur un sous-ensemble de banques de données et placez les machines virtuelles qui ne seront pas protégées sur un autre sous-ensemble de banques de données. Utilisez une protection basée sur le magasin de données pour garantir que les machines virtuelles d'un magasin de données donné sont protégées.

## Créer le plan

Un assistant vous guide à travers ces étapes :

- Sélectionnez les serveurs vCenter.
- Sélectionnez les machines virtuelles ou les banques de données que vous souhaitez répliquer et attribuez des groupes de ressources.
- Cartographiez la manière dont les ressources de l'environnement source sont mappées vers la destination.
- Définissez la fréquence d'exécution du plan, exécutez un script hébergé par l'invité, définissez l'ordre de démarrage et sélectionnez l'objectif du point de récupération.
- Revoyez le plan.

Lorsque vous créez le plan, vous devez suivre ces directives :

- Utilisez les mêmes informations d'identification pour toutes les machines virtuelles du plan.
- Utilisez le même script pour toutes les machines virtuelles du plan.
- Utilisez le même sous-réseau, le même DNS et la même passerelle pour toutes les machines virtuelles du plan.

## Sélectionner les serveurs vCenter

Tout d'abord, vous sélectionnez le vCenter source, puis sélectionnez le vCenter de destination.

### Étapes

1. Connectez-vous à la ["NetApp Console"](#) .
2. Dans la navigation de gauche de la NetApp Console , sélectionnez **Protection > Reprise après sinistre**.
3. Dans le menu NetApp Disaster Recovery , sélectionnez **Plans de réplication** et sélectionnez **Ajouter**. Ou, si vous commencez tout juste à utiliser le service, depuis le tableau de bord, sélectionnez **Ajouter un plan de réplication**.

**Add replication plan**

1 vCenter servers 2 Applications 3 Resource mapping 4 Review

Replication plan > Add plan

**vCenter servers**  
Provide the plan name and select the source and target vCenter servers.

Replication plan name  
RPgr4

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

Source vCenter  
a30

Target vCenter  
vcenter.sdd

Replicate

Cancel Next

4. Créez un nom pour le plan de réplication.
5. Sélectionnez les vCenters source et cible dans les listes vCenter source et cible.
6. Sélectionnez **Suivant**.

## Sélectionnez les applications à répliquer et attribuez des groupes de ressources

L'étape suivante consiste à regrouper les machines virtuelles ou les banques de données requises dans des groupes de ressources fonctionnels. Les groupes de ressources vous permettent de protéger un ensemble de machines virtuelles ou de banques de données avec un instantané commun.

Lorsque vous sélectionnez des applications dans le plan de réplication, vous pouvez voir le système d'exploitation de chaque machine virtuelle ou banque de données dans le plan. Cela est utile pour décider comment regrouper les machines virtuelles ou les banques de données dans un groupe de ressources.



Chaque groupe de ressources peut inclure une ou plusieurs machines virtuelles ou banques de données.

Lorsque vous créez des groupes de ressources, tenez compte des points suivants :

- Avant d'ajouter des banques de données à des groupes de ressources, démarrez d'abord une découverte manuelle ou une découverte planifiée des machines virtuelles. Cela garantit que les machines virtuelles sont découvertes et répertoriées dans le groupe de ressources. Si vous ne déclenchez pas de découverte manuelle, les machines virtuelles risquent de ne pas être répertoriées dans le groupe de ressources.
- Assurez-vous qu'il existe au moins une machine virtuelle dans le magasin de données. S'il n'y a pas de machines virtuelles dans le magasin de données, le magasin de données ne sera pas découvert.
- Un seul magasin de données ne doit pas héberger de machines virtuelles protégées par plusieurs plans de réplication.
- N'hébergez pas de machines virtuelles protégées et non protégées sur le même magasin de données. Si des machines virtuelles protégées et non protégées sont hébergées sur le même magasin de données, les problèmes suivants peuvent survenir :
  - Étant donné que NetApp Disaster Recovery utilise SnapMirror et que le système réplique l'intégralité des volumes ONTAP, la capacité utilisée de ce volume est utilisée pour les considérations de licence. Dans ce cas, l'espace de volume consommé par les machines virtuelles protégées et non protégées serait inclus dans ce calcul.
  - Si le groupe de ressources et ses banques de données associées doivent être basculés vers le site de reprise après sinistre, toutes les machines virtuelles non protégées (machines virtuelles ne faisant pas partie du groupe de ressources, mais hébergées sur le volume ONTAP) n'existeront plus sur le site source à partir du processus de basculement, ce qui entraînera l'échec des machines virtuelles non protégées sur le site source. De plus, NetApp Disaster Recovery ne démarrera pas ces machines virtuelles non protégées sur le site vCenter de basculement.
- Pour qu'une machine virtuelle soit protégée, elle doit être incluse dans un groupe de ressources.



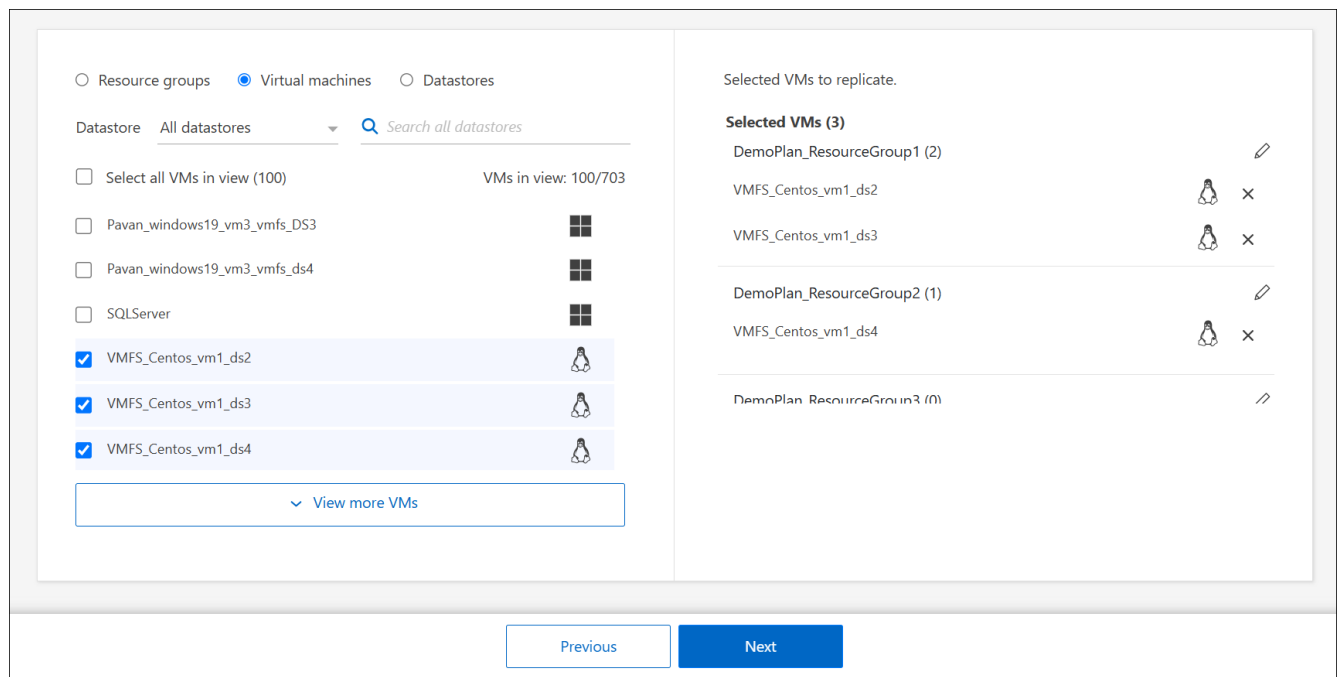
Créez un ensemble de mappages dédié et distinct pour vos tests de basculement afin d'empêcher que les machines virtuelles soient connectées aux réseaux de production en utilisant les mêmes adresses IP.

## Étapes

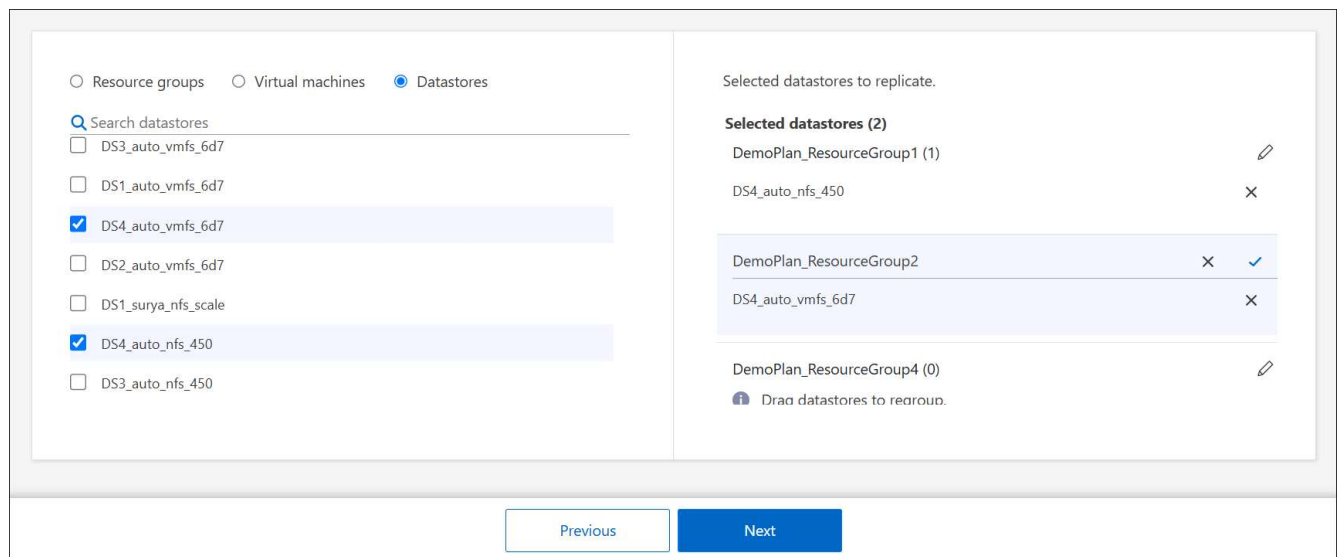
1. Sélectionnez **Machines virtuelles** ou **Magasins de données**.
2. Recherchez éventuellement une machine virtuelle ou un magasin de données spécifique par nom.
3. Sur le côté gauche de la page Applications, sélectionnez les machines virtuelles ou les banques de données que vous souhaitez protéger et affecter au groupe sélectionné.

Le vCenter source doit résider sur le vCenter local. Le vCenter cible peut être un deuxième vCenter sur site, situé sur le même site ou sur un site distant, ou un centre de données défini par logiciel (SDDC) basé sur le cloud, tel que VMware Cloud on AWS. Les deux vCenters devraient déjà avoir été ajoutés à votre environnement de travail de reprise après sinistre.


La ressource sélectionnée est automatiquement ajoutée au groupe 1 et un nouveau groupe 2 est démarré. Chaque fois que vous ajoutez une ressource au dernier groupe, un autre groupe est ajouté.



Ou, pour les magasins de données :



4. Vous pouvez également effectuer l'une des opérations suivantes :

- Pour modifier le nom du groupe, cliquez sur le groupe \*Modifier\*  icône.
- Pour supprimer une ressource d'un groupe, sélectionnez **X** à côté de la ressource.
- Pour déplacer une ressource vers un autre groupe, faites-la glisser et déposez-la dans le nouveau groupe.



Pour déplacer une banque de données vers un autre groupe de ressources, désélectionnez la banque de données indésirable et soumettez le plan de réplication. Ensuite, créez ou modifiez l'autre plan de réplication et resélectionnez le magasin de données.

5. Sélectionnez **Suivant**.

## Mapper les ressources sources vers la cible

À l'étape Mappage des ressources, spécifiez comment les ressources de l'environnement source doivent être mappées à la cible. Lorsque vous créez un plan de réplication, vous pouvez définir un délai et un ordre de démarrage pour chaque machine virtuelle du plan. Cela vous permet de définir une séquence de démarrage des machines virtuelles.

Si vous prévoyez d'effectuer des tests de basculement dans le cadre de votre plan de reprise après sinistre, vous devez fournir un ensemble de mappages de basculement de test pour garantir que les machines virtuelles démarrées pendant le test de basculement n'interfèrent pas avec les machines virtuelles de production. Vous pouvez y parvenir soit en fournissant des machines virtuelles de test avec des adresses IP différentes, soit en mappant les cartes réseau virtuelles des machines virtuelles de test à un réseau différent, isolé de la production mais doté de la même configuration IP (appelé *bulle* ou *réseau de test*).

### Avant de commencer

Si vous souhaitez créer une relation SnapMirror dans ce service, le cluster et son peering SVM doivent déjà avoir été configurés en dehors de NetApp Disaster Recovery.

### Étapes

1. Sur la page de mappage des ressources, cochez la case pour utiliser les mêmes mappages pour les opérations de basculement et de test.

**Add replication plan** ✓ vCenter servers ✓ Applications **3 Resource mapping** 4 Review

Replication plan > Add plan

### Resource mapping

Specify how resources map from the source to the target.

DemoOnPremSite\_1 vcenter 58-58 DemoCloudSite\_1

☒ Use same mappings for failover and test mappings

Failover mappings	Test mappings
Compute resources	Mapping required
Virtual networks	Mapping required
Virtual machines	Mapped
Datastores	Mapping required

[Previous](#) [Next](#)

2. Dans l'onglet Mappages de basculement, sélectionnez la flèche vers le bas à droite de chaque ressource et mappez les ressources dans chaque section :

- Ressources de calcul
- Réseaux virtuels
- Machines virtuelles
- Magasins de données

## Ressources cartographiques > Section Ressources de calcul

La section Ressources de calcul définit où les machines virtuelles seront restaurées après un basculement. Mappez le centre de données et le cluster vCenter source vers un centre de données et un cluster cibles.

En option, les machines virtuelles peuvent être redémarrées sur un hôte vCenter ESXi spécifique. Si VMWare DRS est activé, vous pouvez déplacer automatiquement la machine virtuelle vers un autre hôte si nécessaire pour respecter la politique DR configurée.

En option, vous pouvez placer toutes les machines virtuelles de ce plan de réplication dans un dossier unique avec vCenter. Cela fournit un moyen simple d'organiser rapidement les machines virtuelles basculées dans vCenter.

Sélectionnez la flèche vers le bas à côté de **Ressources de calcul**.

- **Centres de données source et cible**
- **Groupe cible**
- **Hôte cible** (facultatif) : après avoir sélectionné le cluster, vous pouvez définir ces informations.



Si un vCenter dispose d'un planificateur de ressources distribuées (DRS) configuré pour gérer plusieurs hôtes dans un cluster, vous n'avez pas besoin de sélectionner un hôte. Si vous sélectionnez un hôte, NetApp Disaster Recovery placera toutes les machines virtuelles sur l'hôte sélectionné. \* **Dossier de machine virtuelle cible** (facultatif) : créez un nouveau dossier racine pour stocker les machines virtuelles sélectionnées.

## Ressources cartographiques > Section Réseaux virtuels

Les machines virtuelles utilisent des cartes réseau virtuelles connectées à des réseaux virtuels. Dans le processus de basculement, le service connecte ces cartes réseau virtuelles aux réseaux virtuels définis dans l'environnement VMware de destination. Pour chaque réseau virtuel source utilisé par les machines virtuelles du groupe de ressources, le service nécessite une attribution de réseau virtuel de destination.



Vous pouvez affecter plusieurs réseaux virtuels sources au même réseau virtuel cible. Cela pourrait cependant créer des conflits de configuration du réseau IP. Vous pouvez mapper plusieurs réseaux sources à un seul réseau cible pour garantir que tous les réseaux sources ont la même configuration.

Dans l'onglet Mappages de basculement, sélectionnez la flèche vers le bas à côté de **Réseaux virtuels**. Sélectionnez le LAN virtuel source et le LAN virtuel cible.

Sélectionnez le mappage réseau vers le LAN virtuel approprié. Les réseaux locaux virtuels doivent déjà être provisionnés, sélectionnez donc le réseau local virtuel approprié pour mapper la machine virtuelle.

## Ressources cartographiques > section machines virtuelles

Vous pouvez configurer chaque machine virtuelle du groupe de ressources protégé par le plan de réplication en fonction de l'environnement virtuel vCenter de destination en définissant l'une des options suivantes :

- Le nombre de CPU virtuels
- La quantité de DRAM virtuelle
- La configuration de l'adresse IP
- La possibilité d'exécuter des scripts shell du système d'exploitation invité dans le cadre du processus de basculement
- La possibilité de modifier les noms des machines virtuelles ayant échoué en utilisant un préfixe et un suffixe uniques
- La possibilité de définir l'ordre de redémarrage lors du basculement de la machine virtuelle

Dans l'onglet Mappages de basculement, sélectionnez la flèche vers le bas à côté de **Machines virtuelles**.

La valeur par défaut pour les machines virtuelles est mappée. Le mappage par défaut utilise les mêmes paramètres que ceux utilisés par les machines virtuelles dans l'environnement de production (même adresse IP, même masque de sous-réseau et même passerelle).

Si vous apportez des modifications aux paramètres par défaut, vous devez modifier le champ IP cible sur « Différent de la source ».



Si vous modifiez les paramètres sur « Différent de la source », vous devez fournir les informations d'identification du système d'exploitation invité de la machine virtuelle.

Cette section peut afficher des champs différents en fonction de votre sélection.

Vous pouvez augmenter ou diminuer le nombre de processeurs virtuels attribués à chaque machine virtuelle basculée. Cependant, chaque machine virtuelle nécessite au moins un processeur virtuel. Vous pouvez modifier le nombre de processeurs virtuels et de DRAM virtuelle attribués à chaque machine virtuelle. La raison la plus courante pour laquelle vous souhaitez peut-être modifier les paramètres par défaut du processeur virtuel et de la DRAM virtuelle est si les nœuds du cluster vCenter cible ne disposent pas d'autant de ressources disponibles que le cluster vCenter source.

**Paramètres réseau** Disaster Recovery prend en charge un vaste ensemble d'options de configuration pour les réseaux de machines virtuelles. Leur modification peut être nécessaire si le site cible dispose de réseaux virtuels qui utilisent des paramètres TCP/IP différents de ceux des réseaux virtuels de production sur le site source.

Au niveau le plus basique (et par défaut), les paramètres utilisent simplement les mêmes paramètres réseau TCP/IP pour chaque machine virtuelle sur le site de destination que ceux utilisés sur le site source. Cela nécessite que vous configuriez les mêmes paramètres TCP/IP sur les réseaux virtuels source et de destination.

Le service prend en charge les paramètres réseau de configuration IP statique ou Dynamic Host Configuration Protocol (DHCP) pour les machines virtuelles. DHCP fournit une méthode basée sur des normes permettant de configurer dynamiquement les paramètres TCP/IP d'un port réseau hôte. DHCP doit fournir, au minimum, une adresse TCP/IP et peut également fournir une adresse de passerelle par défaut (pour le routage vers une connexion Internet externe), un masque de sous-réseau et une adresse de serveur DNS. DHCP est couramment utilisé pour les périphériques informatiques des utilisateurs finaux tels que les ordinateurs de bureau, les ordinateurs portables et les connexions de téléphones portables des employés, mais il peut



également être utilisé pour tout périphérique informatique réseau tel que les serveurs.

- Option **Utiliser les mêmes paramètres de masque de sous-réseau, DNS et de passerelle** : Étant donné que ces paramètres sont généralement les mêmes pour toutes les machines virtuelles connectées aux mêmes réseaux virtuels, il peut être plus simple de les configurer une seule fois et de laisser Disaster Recovery utiliser les paramètres pour toutes les machines virtuelles du groupe de ressources protégé par le plan de réplication. Si certaines machines virtuelles utilisent des paramètres différents, vous devez décocher cette case et fournir ces paramètres pour chaque machine virtuelle.
- **Type d'adresse IP** : reconfigurez la configuration des machines virtuelles pour qu'elle corresponde aux exigences du réseau virtuel cible. NetApp Disaster Recovery propose deux options : DHCP ou IP statique. Pour les adresses IP statiques, configurez le masque de sous-réseau, la passerelle et les serveurs DNS. Saisissez également les informations d'identification des machines virtuelles.
  - **DHCP** : sélectionnez ce paramètre si vous souhaitez que vos machines virtuelles obtiennent des informations de configuration réseau à partir d'un serveur DHCP. Si vous choisissez cette option, vous fournissez uniquement les informations d'identification de la machine virtuelle.
  - **IP statique** : sélectionnez ce paramètre si vous souhaitez spécifier manuellement les informations de configuration IP. Vous pouvez sélectionner l'une des options suivantes : identique à la source, différent de la source ou mappage de sous-réseau. Si vous choisissez la même chose que la source, vous n'avez pas besoin de saisir d'informations d'identification. D'autre part, si vous choisissez d'utiliser des informations différentes de la source, vous pouvez fournir les informations d'identification, l'adresse IP de la machine virtuelle, le masque de sous-réseau, le DNS et les informations de passerelle. Les informations d'identification du système d'exploitation invité de la machine virtuelle doivent être fournies soit au niveau global, soit au niveau de chaque machine virtuelle.

Cela peut être très utile lors de la récupération de grands environnements vers des clusters cibles plus petits ou pour effectuer des tests de reprise après sinistre sans avoir à provisionner une infrastructure VMware physique individuelle.

---

Virtual machines

---

IP address type	Target IP		
<div>Static ▼</div>	<div>Same as source ▼</div>		
<div><input type="checkbox"/> Use the same credentials for all VMs</div>			
<div><input type="checkbox"/> Use the same script for all VMs</div>			
<div><input type="checkbox"/> Downgrade VM hardware version and register ⓘ</div>			
<div><input checked="" type="checkbox"/> Retain original folder hierarchy ⓘ</div>			
Target VM prefix	Optional	Target VM suffix	Optional
<div></div>		<div></div>	
			Preview: Sample VM name

---

- **Scripts** : Vous pouvez inclure des scripts personnalisés hébergés par le système d'exploitation invité au format .sh, .bat ou .ps1 en tant que post-processus. Grâce aux scripts personnalisés, la reprise après sinistre peut exécuter votre script après un basculement, un retour en arrière et une migration de

processus. Par exemple, vous pouvez utiliser un script personnalisé pour reprendre toutes les transactions de la base de données une fois le basculement terminé. Ce service peut exécuter des scripts au sein de machines virtuelles fonctionnant sous Microsoft Windows ou toute variante Linux prise en charge avec des paramètres de ligne de commande. Vous pouvez attribuer un script à des machines virtuelles individuelles ou à toutes les machines virtuelles du plan de réplication.

Pour activer l'exécution de script avec le système d'exploitation invité de la machine virtuelle, les conditions suivantes doivent être remplies :

- VMware Tools doit être installé sur la machine virtuelle.
- Des informations d'identification utilisateur appropriées doivent être fournies avec des privilèges de système d'exploitation invité adéquats pour exécuter le script.
- Vous pouvez éventuellement inclure une valeur de délai d'expiration en secondes pour le script.

**VM exécutant Microsoft Windows** : peuvent exécuter des scripts Windows batch (.bat) ou PowerShell (ps1). Les scripts Windows peuvent utiliser des arguments de ligne de commande. Formatez chaque argument dans le `arg_name$value` format, où `arg_name` est le nom de l'argument et `$value` est la valeur de l'argument et un point-virgule sépare chaque `argument$value` paire.

**VM exécutant Linux** : peuvent exécuter n'importe quel script shell (.sh) pris en charge par la version de Linux utilisée par la VM. Les scripts Linux peuvent utiliser des arguments de ligne de commande. Fournissez des arguments dans une liste de valeurs séparées par des points-virgules. Les arguments nommés ne sont pas pris en charge. Ajoutez chaque argument à la `Arg[x]` liste d'arguments et référencez chaque valeur à l'aide d'un pointeur dans le `Arg[x]` tableau, par exemple, `value1;value2;value3`.

- **Rétrograder la version matérielle de la VM et l'enregistrer** : Sélectionnez cette option si la version de l'hôte ESX de destination est antérieure à celle de la source afin qu'elles correspondent lors de l'enregistrement.
- **Conserver la hiérarchie des dossiers d'origine** : Par défaut, la reprise après sinistre conserve la hiérarchie de l'inventaire des machines virtuelles (structure des dossiers) en cas de basculement. Si le répertoire cible de récupération ne possède pas l'arborescence de dossiers d'origine, la fonction de récupération après sinistre la crée.

Décochez cette case pour ignorer l'arborescence des dossiers d'origine.

- **Préfixe et suffixe de la machine virtuelle cible** : sous les détails des machines virtuelles, vous pouvez éventuellement ajouter un préfixe et un suffixe à chaque nom de machine virtuelle basculée. Cela peut être utile pour différencier les machines virtuelles basculées des machines virtuelles de production exécutées sur le même cluster vCenter. Par exemple, vous pouvez ajouter un préfixe « DR- » et un suffixe « -failover » au nom de la machine virtuelle. Certaines personnes ajoutent un deuxième vCenter de production pour héberger temporairement des machines virtuelles sur un site différent en cas de sinistre. L'ajout d'un préfixe ou d'un suffixe peut vous aider à identifier rapidement les machines virtuelles ayant échoué. Vous pouvez également utiliser le préfixe ou le suffixe dans les scripts personnalisés.

Vous pouvez utiliser la méthode alternative de définition du dossier de la machine virtuelle cible dans la section Ressources de calcul.

- **Source VM CPU et RAM** : Sous les détails des machines virtuelles, vous pouvez éventuellement redimensionner les paramètres VM CPU et RAM.



Vous pouvez configurer la DRAM en gigaoctets (Gio) ou en mégaoctets (Mio). Bien que chaque machine virtuelle nécessite au moins un Mio de RAM, la quantité réelle doit garantir que le système d'exploitation invité de la machine virtuelle et toutes les applications en cours d'exécution peuvent fonctionner efficacement.

Source VM	Operating system	CPUs	RAM (GB)	Boot order	Boot delay (mins)	Create application-consistent replicas	Scripts	Credentials
<b>Resource group 1</b>								
SQL_PRD_1	Linux	4	16	1	0	<input checked="" type="checkbox"/>	None	Required
<b>Resource group 2</b>								
SQL_PRD_2	Linux	4	32	2	0	<input checked="" type="checkbox"/>	file.py, +2	Required
SQL_PRD_3	Linux	8	64	3	0	<input checked="" type="checkbox"/>	sql_dr_prod.py	Provided
SQL_PRD_4	Linux	8	64	4	0	<input checked="" type="checkbox"/>	sql_dr_prod.py	Provided
SQL_PRD_5	Linux	8	64	5	0	<input checked="" type="checkbox"/>	sql_dr_prod.py	Provided
SQL_PRD_6	Linux	8	64	6	0	<input checked="" type="checkbox"/>	sql_dr_prod.py	Provided
<b>Datastores</b> <input checked="" type="checkbox"/> Mapped								

- **Ordre de démarrage** : vous pouvez modifier l'ordre de démarrage après un basculement pour toutes les machines virtuelles sélectionnées dans les groupes de ressources. Par défaut, toutes les machines virtuelles démarrent ensemble en parallèle ; toutefois, vous pouvez apporter des modifications à ce stade. Cela est utile pour garantir que toutes vos machines virtuelles de priorité 1 sont en cours d'exécution avant le démarrage des machines virtuelles de priorité suivantes.

La reprise après sinistre démarre en parallèle toutes les machines virtuelles ayant le même numéro d'ordre de démarrage.

- Démarrage séquentiel : attribuez à chaque machine virtuelle un numéro unique pour démarrer dans l'ordre attribué, par exemple, 1, 2, 3, 4, 5.
- Démarrage simultané : attribuez le même numéro à toutes les machines virtuelles pour les démarrer en même temps, par exemple, 1,1,1,1,2,2,3,4,4.
- **Délai de démarrage** : ajustez le délai en minutes de l'action de démarrage, indiquant la durée pendant laquelle la machine virtuelle attendra avant de démarrer le processus de mise sous tension. Entrez une valeur comprise entre 0 et 10 minutes.



Pour réinitialiser l'ordre de démarrage aux valeurs par défaut, sélectionnez **Réinitialiser les paramètres de la machine virtuelle aux valeurs par défaut**, puis choisissez les paramètres que vous souhaitez rétablir aux valeurs par défaut.

- **Créer des répliques cohérentes avec l'application** : indiquez s'il faut créer des copies instantanées cohérentes avec l'application. Le service mettra l'application en veille, puis prendra un instantané pour obtenir un état cohérent de l'application. Cette fonctionnalité est prise en charge avec Oracle exécuté sur

Windows et Linux et SQL Server exécuté sur Windows. Voir plus de détails ensuite.

- **Utiliser Windows LAPS** : si vous utilisez la solution de mot de passe administrateur local Windows (Windows LAPS), cochez cette case. Cette option n'est disponible que si vous avez sélectionné l'option **IP statique**. Lorsque vous cochez cette case, vous n'avez pas besoin de fournir un mot de passe pour chacune de vos machines virtuelles. Au lieu de cela, vous fournissez les détails du contrôleur de domaine.

Si vous n'utilisez pas Windows LAPS, la machine virtuelle est une machine virtuelle Windows et l'option d'informations d'identification sur la ligne de la machine virtuelle est activée. Vous pouvez fournir les informations d'identification de la machine virtuelle.

Disaster recovery  
Add replication plan

✓ vCenter servers ✓ Applications 3 Resource mapping 4 Recurrence 5 Review

DHCP

☐ Use the same credentials for all VMs  
☐ Use the same scripts for all VMs

Source VM Operating system CPUs RAM (GB) Boot order Boot delay (mins) Create application-consistent replicas Scripts Credentials

Resource group 1

SQL_PRD_1	Linux	4	16	1	0	<input checked="" type="checkbox"/>	None	Required
-----------	-------	---	----	---	---	-------------------------------------	------	----------

Resource group 2

SQL_PRD_2	Linux	4	32	2	0	<input checked="" type="checkbox"/>	file.py, +2	Required
SQL_PRD_3	Linux	8	64	3	0	<input checked="" type="checkbox"/>	sql_dr_prod.py	Provided
SQL_PRD_4	Linux	8	64	4	0	<input checked="" type="checkbox"/>	sql_dr_prod.py	Provided
SQL_PRD_5	Linux	8	64	5	0	<input checked="" type="checkbox"/>	sql_dr_prod.py	Provided
SQL_PRD_6	Linux	8	64	6	0	<input checked="" type="checkbox"/>	sql_dr_prod.py	Provided

Datastores ☒ Mapped

Previous Next

### Créer des répliques cohérentes avec les applications

De nombreuses machines virtuelles hébergent des serveurs de bases de données tels qu'Oracle ou Microsoft SQL Server. Ces serveurs de base de données nécessitent des instantanés cohérents avec les applications pour garantir que la base de données est dans un état cohérent lorsque l'instantané est pris.

Les instantanés cohérents avec les applications garantissent que la base de données est dans un état cohérent lorsque l'instantané est pris. Ceci est important car cela garantit que la base de données peut être restaurée à un état cohérent après une opération de basculement ou de restauration.

Les données gérées par le serveur de base de données peuvent être hébergées sur le même magasin de données que la machine virtuelle hébergeant le serveur de base de données, ou elles peuvent être hébergées sur un magasin de données différent. Le tableau suivant présente les configurations prises en charge pour les snapshots cohérents avec les applications dans la reprise après sinistre :

Emplacement des données	Soutenu	Remarques
Dans le même datastore vCenter que la machine virtuelle	Oui	Étant donné que le serveur de base de données et la base de données résident tous deux sur le même magasin de données, le serveur et les données seront synchronisés lors du basculement.
Dans une banque de données vCenter différente de la machine virtuelle	Non	<p>La récupération après sinistre ne peut pas identifier quand les données d'un serveur de base de données se trouvent sur une autre banque de données vCenter. Le service ne peut pas répliquer les données, mais peut répliquer la machine virtuelle du serveur de base de données.</p> <p>Bien que les données de la base de données ne puissent pas être répliquées, le service garantit que le serveur de base de données exécute toutes les étapes nécessaires pour garantir que la base de données est mise au repos au moment de la sauvegarde de la machine virtuelle.</p>
Au sein d'une source de données externe	Non	<p>Si les données résident sur un LUN monté sur invité ou sur un partage NFS, Disaster Recovery ne peut pas répliquer les données, mais peut répliquer la machine virtuelle du serveur de base de données.</p> <p>Bien que les données de la base de données ne puissent pas être répliquées, le service garantit que le serveur de base de données exécute toutes les étapes nécessaires pour garantir que la base de données est mise au repos au moment de la sauvegarde de la machine virtuelle.</p>

Lors d'une sauvegarde planifiée, Disaster Recovery met en veille le serveur de base de données, puis prend un instantané de la machine virtuelle hébergeant le serveur de base de données. Cela garantit que la base de données est dans un état cohérent lorsque l'instantané est pris.

- Pour les machines virtuelles Windows, le service utilise le service Microsoft Volume Shadow Copy Service (VSS) pour se coordonner avec l'un ou l'autre serveur de base de données.
- Pour les machines virtuelles Linux, le service utilise un ensemble de scripts pour placer le serveur Oracle en mode de sauvegarde.

Pour activer les répliques cohérentes avec les applications des machines virtuelles et de leurs banques de données d'hébergement, cochez la case en regard de **Créer des répliques cohérentes avec les applications** pour chaque machine virtuelle et fournissez les informations d'identification de connexion invité avec les privilèges appropriés.

## Ressources cartographiques > Section Magasins de données

Les banques de données VMware sont hébergées sur des volumes ONTAP FlexVol ou des LUN ONTAP iSCSI ou FC à l'aide de VMware VMFS. Utilisez la section Banques de données pour définir le cluster ONTAP

cible, la machine virtuelle de stockage (SVM) et le volume ou LUN pour répliquer les données sur disque vers la destination.

Sélectionnez la flèche vers le bas à côté de **Datastores**. En fonction de la sélection des machines virtuelles, les mappages de banques de données sont automatiquement sélectionnés.

Cette section peut être activée ou désactivée en fonction de votre sélection.

The screenshot shows the 'Datastores' configuration interface. It includes a checkbox for 'Use platform managed backups and retention schedules', a date and time picker for 'Start running retention from', a frequency picker for 'Run retention once every', a text input for 'Retention count for all datastores', and dropdown menus for 'Source datastore', 'Target datastore', 'Preferred NFS LIF', and 'Export policy'.

- **Utiliser les sauvegardes gérées par la plateforme et les planifications de conservation** : si vous utilisez une solution de gestion des snapshots externe, cochez cette case. NetApp Disaster Recovery prend en charge l'utilisation de solutions de gestion de snapshots externes telles que le planificateur de politiques ONTAP SnapMirror natif ou des intégrations tierces. Si chaque banque de données (volume) du plan de réplication dispose déjà d'une relation SnapMirror gérée ailleurs, vous pouvez utiliser ces snapshots comme points de récupération dans NetApp Disaster Recovery.

Lorsque cette option est sélectionnée, NetApp Disaster Recovery ne configure pas de planification de sauvegarde. Cependant, vous devez toujours configurer un calendrier de conservation, car des instantanés peuvent toujours être pris pour des opérations de test, de basculement et de restauration automatique.

Une fois cette configuration effectuée, le service ne prend aucun instantané planifié régulièrement, mais s'appuie plutôt sur l'entité externe pour prendre et mettre à jour ces instantanés.

- **Heure de début** : saisissez la date et l'heure auxquelles vous souhaitez que les sauvegardes et la conservation commencent à s'exécuter.
- **Intervalle d'exécution** : saisissez l'intervalle de temps en heures et minutes. Par exemple, si vous entrez 1 heure, le service prendra un instantané toutes les heures.
- **Nombre de rétention** : saisissez le nombre d'instantanés que vous souhaitez conserver.



Le nombre d'instantanés conservés ainsi que le taux de modification des données entre chaque instantané déterminent la quantité d'espace de stockage consommée sur la source et la destination. Plus vous conservez d'instantanés, plus l'espace de stockage consommé est important.

- **Magasins de données source et cible** : si plusieurs relations SnapMirror (en éventail) existent, vous pouvez sélectionner la destination à utiliser. Si un volume possède déjà une relation SnapMirror établie, les

banques de données source et cible correspondantes s'affichent. Si un volume ne possède pas de relation SnapMirror, vous pouvez en créer une maintenant en sélectionnant un cluster cible, en sélectionnant une SVM cible et en fournissant un nom de volume. Le service créera le volume et la relation SnapMirror.



Si vous souhaitez créer une relation SnapMirror dans ce service, le cluster et son peering SVM doivent déjà avoir été configurés en dehors de NetApp Disaster Recovery.

- Si les machines virtuelles proviennent du même volume et du même SVM, le service effectue un instantané ONTAP standard et met à jour les destinations secondaires.
  - Si les machines virtuelles proviennent de volumes différents et du même SVM, le service crée un instantané du groupe de cohérence en incluant tous les volumes et met à jour les destinations secondaires.
  - Si les machines virtuelles proviennent de volumes différents et de SVM différents, le service effectue une phase de démarrage du groupe de cohérence et un instantané de la phase de validation en incluant tous les volumes dans le même cluster ou dans un cluster différent et met à jour les destinations secondaires.
  - Pendant le basculement, vous pouvez sélectionner n'importe quel instantané. Si vous sélectionnez le dernier instantané, le service crée une sauvegarde à la demande, met à jour la destination et utilise cet instantané pour le basculement.
- **LIF NFS préféré et Politique d'exportation** : en règle générale, laissez le service sélectionner le LIF NFS préféré et la politique d'exportation. Si vous souhaitez utiliser une politique NFS LIF ou d'exportation spécifique, sélectionnez la flèche vers le bas à côté de chaque champ et sélectionnez l'option appropriée.

Vous pouvez éventuellement utiliser des interfaces de données spécifiques (LIF) pour un volume après un événement de basculement. Ceci est utile pour équilibrer le trafic de données si le SVM cible possède plusieurs LIF.

Pour un contrôle supplémentaire sur la sécurité d'accès aux données NAS, le service peut attribuer des politiques d'exportation NAS spécifiques à différents volumes de banque de données. Les politiques d'exportation définissent les règles de contrôle d'accès pour les clients NFS qui accèdent aux volumes de la banque de données. Si vous ne spécifiez pas de politique d'exportation, le service utilise la politique d'exportation par défaut pour le SVM.



Il est recommandé de créer une politique d'exportation dédiée qui limite l'accès au volume aux seuls hôtes vCenter ESXi source et de destination qui hébergeront les machines virtuelles protégées. Cela garantit que les entités externes ne peuvent pas accéder à l'exportation NFS.

## Ajouter des mappages de basculement de test

### Étapes

1. Pour définir des mappages différents pour l'environnement de test, décochez la case et sélectionnez l'onglet **Mappages de test**.
2. Parcourez chaque onglet comme précédemment, mais cette fois pour l'environnement de test.

Dans l'onglet Mappages de test, les mappages de machines virtuelles et de magasins de données sont désactivés.



Vous pourrez ensuite tester l'ensemble du plan. Vous configurez actuellement les mappages pour l'environnement de test.

## Revoir le plan de réplication

Enfin, prenez quelques instants pour examiner le plan de réplication.



Vous pouvez ultérieurement désactiver ou supprimer le plan de réplication.

### Étapes

1. Consultez les informations dans chaque onglet : Détails du plan, Mappage de basculement et Machines virtuelles.
2. Sélectionnez **Ajouter un plan**.

Le plan est ajouté à la liste des plans.

## Modifier les plannings pour tester la conformité et garantir le fonctionnement des tests de basculement

Vous souhaitez peut-être configurer des calendriers pour tester les tests de conformité et de basculement afin de garantir qu'ils fonctionneront correctement si vous en avez besoin.

- **Impact sur le temps de conformité** : Lorsqu'un plan de réplication est créé, le service crée un calendrier de conformité par défaut. Le temps de conformité par défaut est de 30 minutes. Pour modifier cette heure, vous pouvez utiliser la fonction Modifier la planification dans le plan de réplication.
- **Test d'impact du basculement** : Vous pouvez tester un processus de basculement à la demande ou selon une planification. Cela vous permet de tester le basculement des machines virtuelles vers une destination spécifiée dans un plan de réplication.


Un basculement de test crée un volume FlexClone , monte la banque de données et déplace la charge de travail sur cette banque de données. Une opération de basculement de test n'a *pas* d'impact sur les charges de travail de production, la relation SnapMirror utilisée sur le site de test et les charges de travail protégées qui doivent continuer à fonctionner normalement.

En fonction du calendrier, le test de basculement s'exécute et garantit que les charges de travail se déplacent vers la destination spécifiée par le plan de réplication.

### Étapes

1. Dans le menu NetApp Disaster Recovery , sélectionnez **Plans de réplication**.

Replication plans (3)							Q	Create report	Add
Name	Compliance status	Plan status	Protected site	Resource groups	Failover site				
RP_DRAAS	Healthy	Ready	DemoOnPremSite_1	RG2, RG1, RG4	DemoCloudSite_1	...			
RPgri	Healthy	Ready	DemoOnPremSite_1	rggri1	DemoCloudSite_1	...			
rpgr3	Healthy	Ready	site-onprem-gri2	rpgr3_ResourceGroup1	DemoOnPremSite_1	...			

2. Sélectionnez les **Actions\***  et sélectionnez **\*Modifier les horaires**.
3. Saisissez la fréquence en minutes à laquelle vous souhaitez que NetApp Disaster Recovery vérifie la conformité des tests.
4. Pour vérifier que vos tests de basculement sont sains, cochez **Exécuter les basculements selon un**



## calendrier mensuel.

- Sélectionnez le jour du mois et l'heure à laquelle vous souhaitez que ces tests soient exécutés.
- Saisissez la date au format aaaa-mm-jj à laquelle vous souhaitez que le test commence.

Edit schedules: RP\_DRAAS

Compliance checks and test failovers run on a recurring basis. Enter how often these actions should occur.

**Compliance check**

Frequency (min) ⓘ

30

**Test failover**

☒ Run test failovers on a schedule ⓘ

☒ Use on-demand snapshot for scheduled test failover

Repeat

Daily ▼

Hour : Minute AM/PM Start date ⓘ

12 : 00 AM 2025-05-13

☒ Automatically cleanup 10 minutes after test failover ⓘ

Save Cancel

5. **Utiliser un instantané à la demande pour le basculement de test planifié** : pour prendre un nouvel instantané avant de lancer le basculement de test automatisé, cochez cette case.
6. Pour nettoyer l'environnement de test une fois le test de basculement terminé, cochez **Nettoyer automatiquement après le basculement du test** et entrez le nombre de minutes que vous souhaitez attendre avant le début du nettoyage.



Ce processus annule l'enregistrement des machines virtuelles temporaires de l'emplacement de test, supprime le volume FlexClone qui a été créé et démonte les banques de données temporaires.

7. Sélectionnez **Enregistrer**.

# Répliquer des applications vers un autre site avec NetApp Disaster Recovery

À l'aide de NetApp Disaster Recovery, vous pouvez répliquer les applications VMware de votre site source vers un site distant de reprise après sinistre dans le cloud à l'aide de la réplication SnapMirror .



Une fois que vous avez créé le plan de reprise après sinistre, identifié la récurrence dans l'assistant et lancé une réplication vers un site de reprise après sinistre, toutes les 30 minutes, NetApp Disaster Recovery vérifie que la réplication se déroule réellement conformément au plan. Vous pouvez suivre la progression dans la page Job Monitor.

**Rôle de NetApp Console requis** Rôle d'administrateur d'organisation, d'administrateur de dossier ou de projet, d'administrateur de reprise après sinistre ou d'administrateur de basculement de reprise après sinistre.

["En savoir plus sur les rôles et les autorisations des utilisateurs dans NetApp Disaster Recovery"](#). ["En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services"](#).

## Avant de commencer

Avant de lancer la réplication, vous devez avoir créé un plan de réplication et choisi de répliquer les applications. Ensuite, l'option **Répliquer** apparaît dans le menu Actions.

## Étapes

1. Connectez-vous à la ["NetApp Console"](#) .
2. Dans la navigation de gauche de la NetApp Console , sélectionnez **Protection > Reprise après sinistre**.
3. Dans le menu, sélectionnez **Plans de réplication**.
4. Sélectionnez le plan de réplication.
5. Sur la droite, sélectionnez l'option **Actions\*** **...** et sélectionnez **\*Répliquer**.

# Migrer des applications vers un autre site avec NetApp Disaster Recovery

À l'aide de NetApp Disaster Recovery, vous pouvez migrer les applications VMware de votre site source vers un autre site.




Une fois le plan de réplication créé, la récurrence identifiée dans l'assistant et la migration lancée, NetApp Disaster Recovery vérifie toutes les 30 minutes que la migration se déroule réellement conformément au plan. Vous pouvez suivre la progression dans la page Job Monitor.

## Avant de commencer

Avant de lancer la migration, vous devez avoir créé un plan de réplication et choisi de migrer les applications. Ensuite, l'option **Migrer** apparaît dans le menu Actions.

## Étapes

1. Connectez-vous à la ["NetApp Console"](#) .
2. Dans la navigation de gauche de la NetApp Console , sélectionnez **Protection > Reprise après sinistre**.

3. Dans le menu, sélectionnez **Plans de réplication**.
4. Sélectionnez le plan de réplication.
5. Sur la droite, sélectionnez l'option **Actions\***  et sélectionnez **\*Migrer**.

## Basculez les applications vers un site distant avec NetApp Disaster Recovery

En cas de sinistre, basculez votre site VMware principal sur site vers un autre site VMware sur site ou VMware Cloud sur AWS. Vous pouvez tester le processus de basculement pour garantir sa réussite lorsque vous en avez besoin.

**Rôle de NetApp Console requis** Rôle d'administrateur d'organisation, d'administrateur de dossier ou de projet, d'administrateur de reprise après sinistre ou d'administrateur de basculement de reprise après sinistre.

["En savoir plus sur les rôles et les autorisations des utilisateurs dans NetApp Disaster Recovery"](#). ["En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services"](#).

### À propos de cette tâche

Lors d'un basculement, la reprise après sinistre utilise par défaut la copie instantanée SnapMirror la plus récente, bien que vous puissiez sélectionner une instantanée spécifique à partir d'une instantanée à un instant donné (conformément à la politique de rétention de SnapMirror). Utilisez l'option de point dans le temps si les répliques les plus récentes sont compromises, par exemple lors d'une attaque de ransomware.

Ce processus diffère selon que le site de production est sain ou non et que vous effectuez un basculement vers le site de reprise après sinistre pour des raisons autres qu'une défaillance critique de l'infrastructure :

- Panne critique du site de production où le cluster vCenter ou ONTAP source n'est pas accessible : NetApp Disaster Recovery vous permet de sélectionner n'importe quel snapshot disponible à partir duquel effectuer la restauration.
- L'environnement de production est sain : vous pouvez soit « Prendre un instantané maintenant » ou sélectionner un instantané précédemment créé.

Cette procédure rompt la relation de réplication, place les machines virtuelles sources vCenter hors ligne, enregistre les volumes en tant que banques de données dans le vCenter de récupération après sinistre, redémarre les machines virtuelles protégées à l'aide des règles de basculement du plan et active la lecture/écriture sur le site cible.

### Tester le processus de basculement

Avant de démarrer le basculement, vous pouvez tester le processus. Le test ne met pas les machines virtuelles hors ligne.

Lors d'un test de basculement, la reprise après sinistre crée temporairement des machines virtuelles. Disaster Recovery mappe un datastore temporaire soutenant le volume FlexClone sur les hôtes ESXi.

Ce processus ne consomme pas de capacité physique supplémentaire sur le stockage ONTAP sur site ou sur le stockage FSx pour NetApp ONTAP dans AWS. Le volume source d'origine n'est pas modifié et les tâches de réplication peuvent se poursuivre même pendant une reprise après sinistre.


Une fois le test terminé, vous devez réinitialiser les machines virtuelles avec l'option **Nettoyer le test**. Bien que cela soit recommandé, ce n'est pas obligatoire.

Une opération de basculement de test n'a *pas* d'impact sur les charges de travail de production, la relation SnapMirror utilisée sur le site de test et les charges de travail protégées qui doivent continuer à fonctionner normalement.

Pour un test de basculement, Disaster Recovery effectue les opérations suivantes :

- Effectuez des vérifications préalables sur le cluster de destination et la relation SnapMirror .
- Créez un nouveau volume FlexClone à partir du snapshot sélectionné pour chaque volume ONTAP protégé sur le cluster ONTAP du site cible.
- Si des banques de données sont VMFS, créez et mappez un iGroup à chaque LUN.
- Enregistrez les machines virtuelles cibles dans vCenter en tant que nouvelles banques de données.
- Mettez sous tension les machines virtuelles cibles en fonction de l'ordre de démarrage capturé dans la page Groupes de ressources.
- Désactivez toutes les applications de base de données prises en charge dans les machines virtuelles indiquées comme « cohérentes avec les applications ».
- Si les clusters vCenter et ONTAP sources sont toujours actifs, créez une relation SnapMirror en sens inverse pour répliquer toutes les modifications lors de l'état de basculement vers le site source d'origine.


### Étapes

1. Connectez-vous à la "[NetApp Console](#)" .
2. Dans la navigation de gauche de la NetApp Console , sélectionnez **Protection > Reprise après sinistre**.
3. Dans le menu NetApp Disaster Recovery , sélectionnez **Plans de réplication**.
4. Sélectionnez le plan de réplication.
5. Sur la droite, sélectionnez l'option **Actions\***  et sélectionnez **\*Tester le basculement**.
6. Dans la page Test de basculement, saisissez « Test de basculement » et sélectionnez **Test de basculement**.
7. Une fois le test terminé, nettoyez l'environnement de test.

## Nettoyer l'environnement de test après un test de basculement

Une fois le test de basculement terminé, vous devez nettoyer l'environnement de test. Ce processus supprime les machines virtuelles temporaires de l'emplacement de test, les FlexClones et les magasins de données temporaires.

### Étapes

1. Dans le menu NetApp Disaster Recovery , sélectionnez **Plans de réplication**.
2. Sélectionnez le plan de réplication.
3. À droite, sélectionnez l'option **Actions**  puis **Nettoyer le test de basculement**.
4. Sur la page de test de basculement, saisissez « Nettoyage du basculement », puis sélectionnez **Test de nettoyage du basculement**.

## Basculer le site source vers un site de reprise après sinistre

En cas de sinistre, basculez à la demande votre site VMware principal sur site vers un autre site VMware sur site ou VMware Cloud sur AWS avec FSx pour NetApp ONTAP.

Le processus de basculement implique les opérations suivantes :

- Disaster Recovery effectue des vérifications préalables sur le cluster de destination et la relation SnapMirror .
- Si vous avez sélectionné le dernier instantané, la mise à jour de SnapMirror est effectuée pour répliquer les dernières modifications.
- Les machines virtuelles sources sont hors tension.
- La relation SnapMirror est rompue et le volume cible est en lecture/écriture.
- En fonction de la sélection de l'instantané, le système de fichiers actif est restauré sur l'instantané spécifié (le plus récent ou sélectionné).
- Les banques de données sont créées et montées sur le cluster ou l'hôte VMware ou VMC en fonction des informations capturées dans le plan de réplication. Si des banques de données sont VMFS, créez et mappez un iGroup à chaque LUN.
- Les machines virtuelles cibles sont enregistrées dans vCenter en tant que nouvelles banques de données.
- Les machines virtuelles cibles sont mises sous tension en fonction de l'ordre de démarrage capturé dans la page Groupes de ressources.
- Si le vCenter source est toujours actif, mettez hors tension toutes les machines virtuelles côté source qui sont en cours de basculement.
- Désactivez toutes les applications de base de données prises en charge dans les machines virtuelles indiquées comme « cohérentes avec les applications ».
- Si les clusters vCenter et ONTAP sources sont toujours actifs, créez une relation SnapMirror en sens inverse pour répliquer toutes les modifications lors de l'état de basculement vers le site source d'origine. La relation SnapMirror est inversée de la machine virtuelle cible à la machine virtuelle source.




Pour les plans de réplication basés sur un datastore, si vous avez ajouté et découvert des machines virtuelles mais n'avez pas fourni de détails de mappage, ces machines virtuelles sont incluses dans le basculement. Le basculement échouera et une notification sera affichée dans les tâches. Vous devez fournir les détails de mappage pour que le basculement réussisse.



Une fois le basculement démarré, vous pouvez voir les machines virtuelles récupérées dans le vCenter du site de reprise après sinistre (machines virtuelles, réseaux et banques de données). Par défaut, les machines virtuelles sont récupérées dans le dossier Charge de travail.

## Étapes

1. Dans le menu NetApp Disaster Recovery , sélectionnez **Plans de réplication**.
2. Sélectionnez le plan de réplication.
3. Sur la droite, sélectionnez l'option **Actions\***  et sélectionnez **\*Fail over**.

Failover: RP\_DRAAS

**Warning:** Failing over will disrupt client access to the data in **DemoOnPremSite\_1** during the transition to **DemoCloudSite\_1** DR Site.

Snapshot copy for volume recovery ☒ Take snapshot now ☐ Select

**i** A new snapshot copy of the current source will be created and replicated to the current destination before failing over.

☐ Force failover **i**

☒ Skip protection **i**

Enter **Failover** to confirm

Failover

Failover Cancel

4. Sur la page de basculement, créez un nouvel instantané maintenant ou choisissez un instantané existant que la banque de données utilisera comme base de récupération. La valeur par défaut est la plus récente.

Un instantané de la source actuelle sera pris et répliqué vers la destination actuelle avant que le basculement ne se produise.

5. Vous pouvez également sélectionner **Forcer le basculement** si vous souhaitez que le basculement se produise même si une erreur est détectée qui empêcherait normalement le basculement de se produire.
6. Vous pouvez également sélectionner **Ignorer la protection** si vous souhaitez que le service ne crée pas automatiquement une relation de protection SnapMirror inversée après un basculement de plan de réplication. Cela est utile si vous souhaitez effectuer des opérations supplémentaires sur le site restauré avant de le remettre en ligne dans NetApp Disaster Recovery.



Vous pouvez établir une protection inverse en sélectionnant **Protéger les ressources** dans le menu Actions du plan de réplication. Cela tente de créer une relation de réplication inverse pour chaque volume du plan. Vous pouvez exécuter cette tâche à plusieurs reprises jusqu'à ce que la protection soit restaurée. Une fois la protection restaurée, vous pouvez lancer une restauration automatique de la manière habituelle.

7. Tapez « failover » dans la case.
8. Sélectionnez **Fail over**.
9. Pour vérifier la progression, dans le menu, sélectionnez **Suivi des tâches**.

## Restaurez les applications à la source d'origine avec NetApp Disaster Recovery

Une fois une catastrophe résolue, revenez du site de reprise après sinistre au site source pour revenir aux opérations normales. Vous pouvez sélectionner l'instantané à partir

duquel effectuer la récupération.

**Rôle de NetApp Console requis** Rôle d'administrateur d'organisation, d'administrateur de dossier ou de projet, d'administrateur de reprise après sinistre ou d'administrateur de basculement de reprise après sinistre.

["En savoir plus sur les rôles et les autorisations des utilisateurs dans NetApp Disaster Recovery"](#). ["En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services"](#).

## À propos du failback


En cas de retour en arrière, NetApp Disaster Recovery réplique (resynchronise) toutes les modifications vers la machine virtuelle source d'origine avant d'inverser le sens de la réplication. Ce processus débute à partir d'une relation qui a basculé vers une cible et comprend les étapes suivantes :

- Effectuer un contrôle de conformité sur le site récupéré.
- Actualisez les informations vCenter pour chaque cluster vCenter identifié comme situé sur le site récupéré.
- Sur le site cible, mettez hors tension et désenregistrez les machines virtuelles, puis démontez les volumes.
- Rompre la relation SnapMirror sur la source d'origine pour la rendre en lecture/écriture.
- Resynchronisez la relation SnapMirror pour inverser la réplication.
- Mettez sous tension et enregistrez les machines virtuelles sources, puis montez les volumes sur la source.

## Avant de commencer

Si vous utilisez une protection basée sur un datastore, les machines virtuelles ajoutées au datastore peuvent être ajoutées à ce dernier lors du processus de basculement. Si cela s'est produit, assurez-vous de fournir les informations de mappage supplémentaires pour ces machines virtuelles avant de lancer le basculement. Pour modifier le mappage des ressources, consultez ["Gérer les plans de réplication"](#).

## Étapes

1. Dans la navigation de gauche de la NetApp Console , sélectionnez **Protection > Reprise après sinistre**.
2. Dans le menu NetApp Disaster Recovery , sélectionnez **Plans de réplication**.
3. Sélectionnez le plan de réplication.
4. Sur la droite, sélectionnez l'option **Actions\***  et sélectionnez **\*Retour en arrière**.
5. Saisissez le nom du plan de réplication pour démarrer le basculement.
6. Choisissez l'instantané du magasin de données à partir duquel effectuer la récupération. La valeur par défaut est la plus récente.
7. Pour suivre l'avancement de la tâche, sélectionnez **Suivi des tâches** dans le menu Reprise après sinistre.

## Gérez les sites, les groupes de ressources, les plans de réplication, les banques de données et les informations sur les machines virtuelles avec NetApp Disaster Recovery

NetApp Disaster Recovery offre des aperçus et des perspectives plus détaillées sur toutes vos ressources :

- Sites
- Groupes de ressources
- Plans de réplication
- Magasins de données
- Machines virtuelles

Les tâches nécessitent différents rôles de NetApp Console . Pour plus de détails, consultez la section **Rôle de NetApp Console requis** dans chaque tâche.


["En savoir plus sur les rôles et les autorisations des utilisateurs dans NetApp Disaster Recovery"](#). ["En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services"](#).

## Gérer les sites vCenter

Vous pouvez modifier le nom du site vCenter et le type de site (sur site ou AWS).

**Rôle de NetApp Console requis** Rôle d'administrateur d'organisation, d'administrateur de dossier ou de projet ou d'administrateur de reprise après sinistre.

### Étapes

1. Dans le menu, sélectionnez **Sites**.
2. Sélectionnez l'option **Actions\***  à droite du nom du vCenter et sélectionnez **\*Modifier**.
3. Modifiez le nom et l'emplacement du site vCenter.

## Gérer les groupes de ressources

Vous pouvez créer des groupes de ressources par machines virtuelles ou par banques de données. Ils peuvent être ajoutés lors de la création du plan de réplication ou ultérieurement.

**Rôle de NetApp Console requis** Rôle d'administrateur d'organisation, d'administrateur de dossier ou de projet, d'administrateur de reprise après sinistre ou d'administrateur d'application de reprise après sinistre.

Vous pouvez créer un groupe de ressources par magasins de données des manières suivantes :

- Lorsque vous ajoutez un groupe de ressources à l'aide de magasins de données, vous pouvez voir une liste de magasins de données. Vous pouvez sélectionner un ou plusieurs magasins de données pour créer un groupe de ressources.
- Lorsque vous créez un plan de réplication et créez un groupe de ressources dans le plan, vous pouvez voir les machines virtuelles dans les banques de données.

Vous pouvez effectuer les tâches suivantes avec les groupes de ressources :

- Modifier le nom du groupe de ressources.
- Ajoutez des machines virtuelles au groupe de ressources.
- Supprimez les machines virtuelles du groupe de ressources.
- Supprimer les groupes de ressources.

Pour plus de détails sur la création d'un groupe de ressources, reportez-vous à ["Créer un groupe de](#)



## Étapes

1. Dans le menu, sélectionnez **Groupes de ressources**.
2. Pour ajouter un groupe de ressources, sélectionnez **Ajouter un groupe**.
3. Vous pouvez modifier ou supprimer le groupe de ressources en sélectionnant l'option **Actions**. ... .

## Gérer les plans de réplication

Vous pouvez désactiver, activer et supprimer les plans de réplication. Vous pouvez modifier les horaires.

**Rôle de NetApp Console requis** Administrateur d'organisation, Administrateur de dossier ou de projet, Administrateur de reprise après sinistre, Administrateur de basculement de reprise après sinistre ou Administrateur d'application de reprise après sinistre.

- Si vous souhaitez suspendre temporairement un plan de réplication, vous pouvez le désactiver et le réactiver ultérieurement.
- Si vous n'avez plus besoin du plan, vous pouvez le supprimer.

## Étapes

1. Dans le menu, sélectionnez **Plans de réplication**.

Replication plans (3)							Q	Create report	Add
Name	Compliance status	Plan status	Protected site	Resource groups	Failover site				
RP_DRAAS	Healthy	Ready	DemoOnPremSite_1	RG2, RG1, RG4	DemoCloudSite_1	...			
RPgri	Healthy	Ready	DemoOnPremSite_1	rggri1	DemoCloudSite_1	...			
rpgr3	Healthy	Ready	site-onprem-gri2	rpgr3_ResourceGroup1	DemoOnPremSite_1	...			

2. Pour afficher les détails du plan, sélectionnez l'option **Actions**\* ... et sélectionnez **\*Afficher les détails du plan**.
3. Effectuez l'une des opérations suivantes :
  - Pour modifier les détails du plan (modifier la récurrence), sélectionnez l'onglet **Détails du plan** et sélectionnez l'icône **Modifier** à droite.
  - Pour modifier les mappages de ressources, sélectionnez l'onglet **Mappage de basculement** et sélectionnez l'icône **Modifier**.
  - Pour ajouter ou modifier les machines virtuelles, sélectionnez l'onglet **Machines virtuelles** et sélectionnez l'option **Ajouter des machines virtuelles** ou l'icône **Modifier**.
4. Revenez à la liste des plans en sélectionnant « Plans de réplication » dans le fil d'Ariane à gauche.
5. Pour effectuer des actions avec le plan, dans la liste des plans de réplication, sélectionnez l'option **Actions**\* ... à droite du plan et sélectionnez l'une des options, telles que **\*Modifier les planifications**, **Tester le basculement**, **Basculer**, **Retour en arrière**, **Migrer**, **Prendre un instantané maintenant**, **Nettoyer les anciens instantanés**, **Désactiver**, **Activer** ou **Supprimer**.
6. Pour définir ou modifier un calendrier de basculement de test ou définir la vérification de la fréquence de conformité, sélectionnez l'option **Actions**\* ... à droite du plan et sélectionnez **\*Modifier les horaires**.
  - a. Dans la page Modifier les planifications, entrez la fréquence en minutes à laquelle vous souhaitez que

la vérification de conformité de basculement se produise.

- b. Cochez **Exécuter les tests de basculement selon un calendrier**.
- c. Dans l'option Répéter, sélectionnez le programme quotidien, hebdomadaire ou mensuel.
- d. Sélectionnez **Enregistrer**.

## Rapprocher les instantanés à la demande

La reprise après sinistre supprime automatiquement les instantanés de la source toutes les 24 heures. Si vous constatez que les instantanés ne sont pas synchronisés entre la source et la destination, vous devez résoudre cette incohérence afin de garantir la cohérence entre les sites.

**Rôle de NetApp Console requis** Administrateur d'organisation, Administrateur de dossier ou de projet, Administrateur de reprise après sinistre, Administrateur de basculement de reprise après sinistre ou Administrateur d'application de reprise après sinistre.

## Étapes

1. Dans le menu, sélectionnez **Plans de réplication**.

Replication plans (3)							Q	Create report	Add
Name	Compliance status	Plan status	Protected site	Resource groups	Failover site				
RP_DRAAS	Healthy	Ready	DemoOnPremSite_1	RG2, RG1, RG4	DemoCloudSite_1	...			
RPgr1	Healthy	Ready	DemoOnPremSite_1	rggr1	DemoCloudSite_1	...			
rpgr3	Healthy	Ready	site-onprem-gr12	rpgr3_ResourceGroup1	DemoOnPremSite_1	...			

2. Dans la liste des plans de réplication, sélectionnez l'option **Actions**. ... puis **Réconcilier les instantanés**.
3. Consultez les informations de rapprochement.
4. Sélectionnez **Réconcilier**.

## Supprimer un plan de réplication

Si vous supprimez un plan de réplication, vous pouvez également supprimer les snapshots principaux et secondaires créés par le plan.

**Rôle de NetApp Console requis** Administrateur d'organisation, Administrateur de dossier ou de projet, Administrateur de reprise après sinistre, Administrateur de basculement de reprise après sinistre ou Administrateur d'application de reprise après sinistre.

## Étapes

1. Dans le menu, sélectionnez **Plans de réplication**.
2. Sélectionnez l'option **Actions\*** ... à droite du plan et sélectionnez **\*Supprimer**.
3. Choisissez si vous souhaitez supprimer les instantanés principaux, les instantanés secondaires ou uniquement les métadonnées créées par le plan.
4. Saisissez « supprimer » pour confirmer la suppression.
5. Sélectionnez **Supprimer**.

## Modifier le nombre de rétentions pour les planifications de basculement

Modifier le nombre de données conservées vous permet d'augmenter ou de diminuer le nombre de bases de données enregistrées.

**Rôle de NetApp Console requis** Administrateur d'organisation, Administrateur de dossier ou de projet, Administrateur de reprise après sinistre, Administrateur de basculement de reprise après sinistre ou Administrateur d'application de reprise après sinistre.

### Étapes

1. Dans le menu, sélectionnez **Plans de réplication**.
2. Sélectionnez le plan de réplication, puis l'onglet **Mappage de basculement**. Sélectionnez l'icône en forme de crayon **Modifier**.
3. Sélectionnez la flèche vers le bas dans la ligne **Datstores** pour la développer.

The screenshot shows the 'Datstores' configuration page in the NetApp console. The page is divided into two main sections: 'Source datastore' on the left and 'Target datastore' on the right. The 'Source datastore' section includes a 'Retention count for all datstores' field set to 30, and a list of source datstores: 'BizAppDatastore (Temp\_3510\_N1:DR\_Prod\_Source)', 'DS\_SFO (Temp\_3510\_N1:DR\_SFO)', 'DS\_Testing\_Staging (Temp\_3510\_N1:DR\_Vol\_Staging)', and 'BizAppDatastore (Temp\_3510\_N1:DR\_Prod\_Source)'. The 'Target datastore' section includes a 'Target datastore' dropdown set to 'test-DR\_Prod\_dest', and a table of target datstores with columns for 'Preferred NFS LIF', 'Export policy', 'System', 'SVM', and 'Destination volume name'. The 'Preferred NFS LIF' and 'Export policy' are set to 'Select preferred NFS LIF' and 'Select export policy' respectively. The 'System' is set to 'Select a System' and the 'SVM' is set to 'Select an SVM'. The 'Destination volume name' is set to 'DR\_SFO\_dest'. At the bottom, there are 'Cancel' and 'Save' buttons.

4. Modifiez la valeur du **Nombre de rétentions pour tous les magasins de données**.
5. Une fois le plan de réplication sélectionné, sélectionnez le menu Actions, puis sélectionnez **Nettoyer les anciens snapshots** pour supprimer les anciens snapshots sur la cible afin qu'ils correspondent au nouveau nombre de rétention.

## Afficher les informations sur les magasins de données

Vous pouvez afficher des informations sur le nombre de magasins de données existants sur la source et sur la cible.

**Rôle de NetApp Console requis** Administrateur d'organisation, Administrateur de dossier ou de projet, Administrateur de reprise après sinistre, Administrateur de basculement de reprise après sinistre, Administrateur d'application de reprise après sinistre ou Rôle d'observateur de reprise après sinistre.

### Étapes

1. Dans le menu, sélectionnez **Tableau de bord**.

2. Sélectionnez le vCenter dans la ligne du site.
3. Sélectionnez **Datastores**.
4. Afficher les informations des magasins de données.

## Afficher les informations sur les machines virtuelles

Vous pouvez afficher des informations sur le nombre de machines virtuelles existantes sur la source et sur la cible, ainsi que sur le processeur, la mémoire et la capacité disponible.

**Rôle de NetApp Console requis** Administrateur d'organisation, Administrateur de dossier ou de projet, Administrateur de reprise après sinistre, Administrateur de basculement de reprise après sinistre, Administrateur d'application de reprise après sinistre ou Rôle d'observateur de reprise après sinistre.

### Étapes

1. Dans le menu, sélectionnez **Tableau de bord**.
2. Sélectionnez le vCenter dans la ligne du site.
3. Sélectionnez **Machines virtuelles**.
4. Afficher les informations des machines virtuelles.

## Surveiller les tâches de NetApp Disaster Recovery

Vous pouvez surveiller toutes les tâches de NetApp Disaster Recovery et déterminer leur progression.

### Voir les offres d'emploi

**Rôle de NetApp Console requis** Administrateur d'organisation, Administrateur de dossier ou de projet, Administrateur de reprise après sinistre, Administrateur d'application de reprise après sinistre ou Rôle d'observateur de reprise après sinistre.

["En savoir plus sur les rôles et les autorisations des utilisateurs dans NetApp Disaster Recovery"](#). ["En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services"](#).

### Étapes

1. Connectez-vous à la ["NetApp Console"](#).
2. Dans la navigation de gauche de la NetApp Console, sélectionnez **Protection > Reprise après sinistre**.
3. Dans le menu, sélectionnez **Surveillance des tâches**.
4. Explorez tous les travaux liés aux opérations et examinez leurs horodatages et leur statut.
5. Pour afficher les détails d'une tâche particulière, sélectionnez cette ligne.
6. Pour actualiser les informations, sélectionnez **Actualiser**.

### Annuler un travail

Si une tâche est en cours ou dans un état en file d'attente et que vous ne souhaitez pas qu'elle continue, vous pouvez l'annuler. Vous souhaitez peut-être annuler une tâche si elle est bloquée dans le même état et que vous souhaitez libérer l'opération suivante dans la file d'attente. Vous souhaitez peut-être annuler une tâche avant qu'elle n'expire.

**Rôle de NetApp Console requis** Administrateur d'organisation, Administrateur de dossier ou de projet, Administrateur de reprise après sinistre, Administrateur de basculement de reprise après sinistre ou Administrateur d'application de reprise après sinistre.

["En savoir plus sur les rôles et les autorisations des utilisateurs dans NetApp Disaster Recovery"](#). ["En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services"](#).

### Étapes

1. Dans la barre de navigation de gauche de la NetApp Console , sélectionnez **Protection > Reprise après sinistre**.
2. Dans le menu, sélectionnez **Surveillance des tâches**.
3. Dans la page du moniteur de tâches, notez l'ID de la tâche que vous souhaitez annuler.

Le travail doit être dans un état « En cours » ou « En file d'attente ».

4. Dans la colonne Actions, sélectionnez **Annuler le travail**.

## Créer des rapports de NetApp Disaster Recovery

L'examen des rapports de NetApp Disaster Recovery peut vous aider à analyser votre préparation à la reprise après sinistre. Les rapports prédéfinis incluent un résumé des basculements de test, des détails du plan de réplication et des détails des tâches sur tous les sites d'un compte au cours des sept derniers jours.

Vous pouvez télécharger des rapports au format PDF, HTML ou JSON.

Le lien de téléchargement est valable six heures.

### Étapes

1. Connectez-vous à la ["NetApp Console"](#) .
2. Dans la navigation de gauche de la NetApp Console , sélectionnez **Protection > Reprise après sinistre**.
3. Dans la barre de navigation de gauche de la NetApp Console , sélectionnez **Plans de réplication**.
4. Sélectionnez **Créer un rapport**.
5. Sélectionnez le type de format de fichier et la période au cours des 7 derniers jours.
6. Sélectionnez **Créer**.



L'affichage du rapport peut prendre quelques minutes.

7. Pour télécharger un rapport, sélectionnez **Télécharger le rapport** et sélectionnez-le dans le dossier Téléchargement de l'administrateur.

## Informations sur le copyright

Copyright © 2026 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.