Référence

NetApp Disaster Recovery

NetApp
March 09, 2026

This PDF was generated from https://docs.netapp.com/fr-fr/data-services-disaster-recovery/reference/vcenter-privileges.html on March 09, 2026. Always check docs.netapp.com for the latest.

Sommaire

Référence . . . 1
- Privilèges requis vCenter pour NetApp Disaster Recovery . . . 1
- Changer d'agent de console lors de l'utilisation de NetApp Disaster Recovery . . . 4
  - Avant de commencer . . . 4
  - Étapes . . . 4
  - Plus d'informations . . . 5
- Utiliser NetApp Disaster Recovery avec Amazon EVS . . . 5
  - Présentation de NetApp Disaster Recovery à l'aide d'Amazon Elastic VMware Service et Amazon FSx for NetApp ONTAP . . . 5
  - Présentation de la solution NetApp Disaster Recovery à l'aide d'Amazon EVS et d'Amazon FS pour NetApp ONTAP . . . 6
  - Installer l'agent NetApp Console pour NetApp Disaster Recovery . . . 8
  - Configurer NetApp Disaster Recovery pour Amazon EVS . . . 8
  - Créer des plans de réplication pour Amazon EVS . . . 21
  - Exécuter des opérations de plan de réplication avec NetApp Disaster Recovery . . . 34

Référence

Privilèges requis vCenter pour NetApp Disaster Recovery

Pour que NetApp Disaster Recovery puisse fournir ses services, le compte vCenter doit disposer d'un ensemble minimal de privilèges vCenter. Ces privilèges incluent l'enregistrement et la désinscription des banques de données, le démarrage et l'arrêt des machines virtuelles (VM), ainsi que leur reconfiguration.

Le tableau suivant répertorie tous les privilèges requis pour que la reprise après sinistre puisse interagir avec un cluster vCenter.

Type	Nom du privilège (vSphere client)	Nom du privilège (API)	Description
Magasin de données	Datastore.Config	Configurer le datastore	Permet de configurer un datastore.
	Datastore.Delete	Supprimer le datastore	Autorise la suppression d'un datastore.
	Datastore.Rename	Renommer le datastore	Permet de renommer un datastore.
Dossier	Folder.Create	Créer un dossier	Autorise la création d'un nouveau dossier.
	Folder.Delete	Supprimer le dossier	Permet de supprimer un dossier. Nécessite un privilège sur l'objet et son parent.
	Folder.Rename	Renommer le dossier	Autorise la modification du nom d'un dossier.
Réseau	Network.Assign	Attribuer un réseau	Autorise l'attribution d'un réseau à une machine virtuelle.
	Network.Config	Configurer	Permet de configurer un réseau.

Type	Nom du privilège (vSphere client)	Nom du privilège (API)	Description
Configuration de la machine virtuelle	VirtualMachine.Config.AdvancedConfig	Configuration avancée	Permet d'ajouter ou de modifier des paramètres avancés dans le fichier de configuration de la VM.
	VirtualMachine.Config.Settings	Modifier les paramètres	Permet de modifier les paramètres généraux de la machine virtuelle.
	VirtualMachine.Config.CPUCount	Modifier le nombre de CPU	Permet de modifier le nombre de processeurs virtuels.
	VirtualMachine.Config.Memory	Changer la mémoire	Permet de modifier la quantité de mémoire allouée à la VM.
	VirtualMachine.Config.Resource	Modifier la ressource	Permet de modifier la configuration des ressources des nœuds de VM dans un pool de ressources.
	VirtualMachine.Config.Rename	Renommer	Permet de renommer une VM ou de modifier ses notes.
	VirtualMachine.Config.EditDevice	Modifier les paramètres de l'appareil	Permet de modifier les propriétés d'un appareil existant.
	VirtualMachine.Config.ReloadFromPath	Recharger depuis le chemin	Permet de modifier le chemin de configuration d'une machine virtuelle tout en préservant son identité.
	VirtualMachine.Config.ResetGuestInfo	Réinitialiser les informations invité	Permet de modifier les informations du système d'exploitation invité pour une VM.
Machine virtuelle invitée	VirtualMachine.GuestOperations.ModifyAliases	Modification de l'alias de l'opération invité	Autorise la modification de l'alias pour la machine virtuelle.
	VirtualMachine.GuestOperations.QueryAliases	Requête d'alias d'opération invité	Autorise l'interrogation de l'alias d'une VM.
	VirtualMachine.GuestOperations.Modify	Modifications des opérations invité	Permet les opérations de modification, y compris le transfert d'un fichier vers la VM.
	VirtualMachine.GuestOperations.Execute	Exécution du programme d'opérations invité	Permet d'exécuter une application à l'intérieur de la VM.
	VirtualMachine.GuestOperations.Query	Requêtes d'opérations des invités	Permet d'interroger le système d'exploitation invité. Les opérations incluent la liste des fichiers.

Type	Nom du privilège (vSphere client)	Nom du privilège (API)	Description
Interaction avec une machine virtuelle	VirtualMachine.Interact.AnswerQuestion	Répondre à la question	Permet de résoudre les problèmes lors des transitions d'état de la VM ou des erreurs d'exécution.
	VirtualMachine.Interact.PowerOff	Mise hors tension	Permet d'éteindre une machine virtuelle allumée.
	VirtualMachine.Interact.PowerOn	Mise sous tension	Permet de mettre sous tension ou de reprendre une VM.
	VirtualMachine.Interact.ToolsInstall	Installation de VMware Tools	Permet de monter/démonter le programme d'installation de VMware Tools.
	VirtualMachine.Inventory.CreateFromExisting	Créer à partir de l'existant	Permet de cloner ou de déployer une VM à partir d'un template.
	VirtualMachine.Inventory.Create	Créer nouveau	Permet de créer une VM et d'allouer des ressources.
	VirtualMachine.Inventory.Register	S'inscrire	Permet d'ajouter une machine virtuelle existante à un inventaire.
	VirtualMachine.Inventory.Delete	Retirer	Permet de supprimer une machine virtuelle et ses fichiers. Nécessite des privilèges sur l'objet et son parent.
	VirtualMachine.Inventory.Unregister	Annuler l'enregistrement	Permet de désenregistrer une machine virtuelle. Cette autorisation requiert des privilèges sur l'objet et son parent.
Provisionnement de machines virtuelles	VirtualMachine.Provisioning.Clone	Cloner la machine virtuelle	Permet de cloner une machine virtuelle et d'allouer des ressources.
	VirtualMachine.Provisioning.Customize	Personnaliser l'invité	Permet de personnaliser le système d'exploitation invité de la VM.
	VirtualMachine.Provisioning.ModifyCustSpecs	Modifier la spécification de personnalisation	Permet de créer, de modifier ou de supprimer des spécifications de personnalisation.
	VirtualMachine.Provisioning.ReadCustSpecs	Lire les spécifications de personnalisation	Permet de lire une spécification de personnalisation pour une VM.
Configuration du service de machine virtuelle	VirtualMachine.Namespace.Query	Configurations du service de requête	Autorise la récupération d'une liste de services de VM.
	VirtualMachine.Namespace.ReadContent	Lire la configuration du service	Autorise la récupération de la configuration de service VM existante.

Type	Nom du privilège (vSphere client)	Nom du privilège (API)	Description
Instantané de machine virtuelle	VirtualMachine.State.CreateSnapshot	Créer un instantané	Permet de créer un instantané à partir de l'état actuel de la machine virtuelle.
	VirtualMachine.State.RemoveSnapshot	Supprimer l'instantané	Autorise la suppression d'un instantané.
	VirtualMachine.State.RenameSnapshot	Renommer le snapshot	Permet de renommer un instantané ou de mettre à jour sa description.
	VirtualMachine.State.RevertToSnapshot	Rétablir l'instantané	Permet de rétablir la machine virtuelle à l'état d'un instantané donné.

Changer d'agent de console lors de l'utilisation de NetApp Disaster Recovery

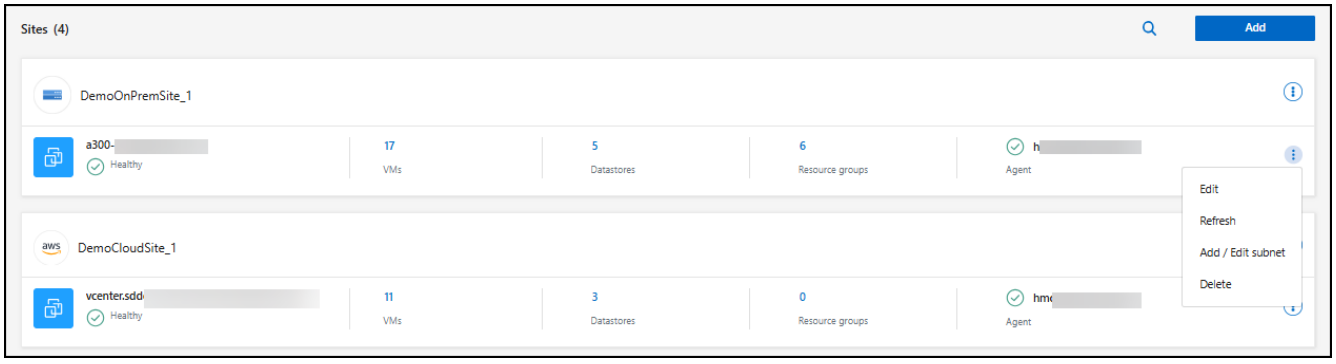
La NetApp Console prend en charge l'utilisation de plusieurs agents de console dans un seul environnement de travail. L'utilisation de plusieurs agents Console peut s'avérer utile pour maintenir l'accès aux ressources pendant la maintenance d'un autre agent Console ou en cas de défaillance d'un agent Console. Chaque agent Console possédant un identifiant unique, un changement incorrect d'agent Console peut compromettre la disponibilité des ressources dans un environnement de travail.

Avant de commencer

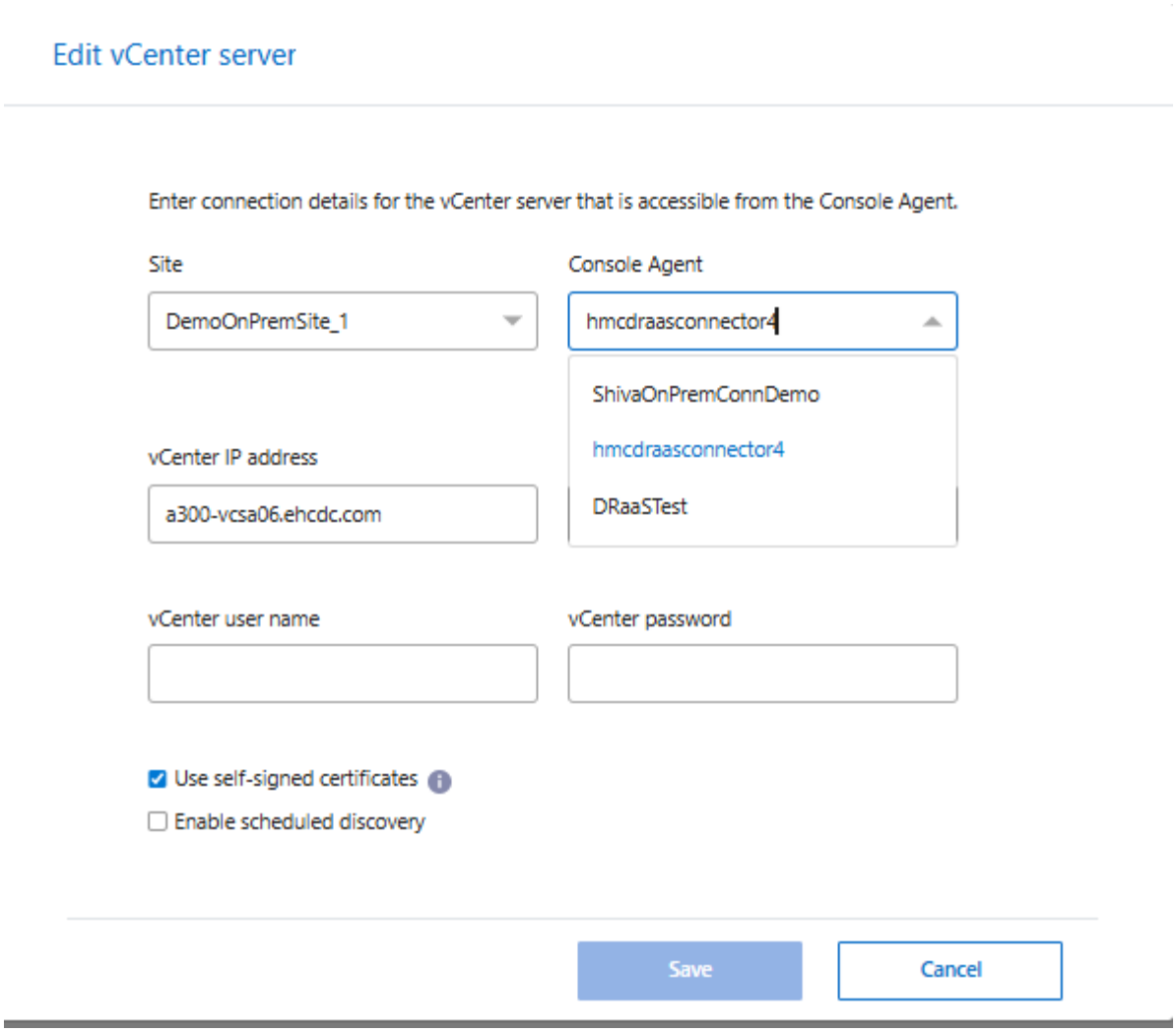
- Vous devez avoirAu moins deux agents Console ont été ajoutés à votre environnement de travail. .
- Les deux agents de console doivent contenir les mêmes clusters ONTAP .

Étapes

1. Dans la section Reprise après sinistre, sélectionnez **Sites**.
2. Vous devez modifier l'agent de la console pour les vCenters source et de destination. Identifiez les vCenters que vous souhaitez modifier. Sélectionnez le menu d'actions du vCenter, puis **Modifier**.



3. Sélectionnez l'agent Console que vous souhaitez utiliser dans le menu déroulant et saisissez à nouveau votre nom d'utilisateur et votre mot de passe vCenter. Sélectionnez **Enregistrer**.



4. Répétez les étapes 2 et 3 pour chaque vCenter supplémentaire que vous souhaitez modifier.
5. Dans le vCenter que vous avez modifié, actualisez-le pour détecter le nouvel agent de console. Répétez cette étape pour chaque vCenter que vous avez modifié.
6. Dans la section Reprise après sinistre, accédez à **Plans de réplication**.
7. Identifiez les plans de réplication que vous souhaitez utiliser pour reprendre les flux de travail. Sélectionnez le menu d'actions … puis **Actualiser les ressources**. Vous pouvez suivre l'état des tâches dans la section **Suivi des tâches**.

Plus d'informations

- "En savoir plus sur les agents de console"

Utiliser NetApp Disaster Recovery avec Amazon EVS

Présentation de NetApp Disaster Recovery à l'aide d'Amazon Elastic VMware Service et Amazon FSx for NetApp ONTAP

De plus en plus, les clients dépendent davantage des infrastructures virtualisées pour les charges de travail de calcul de production telles que celles basées sur VMware vSphere. Ces machines virtuelles (VM) étant devenues plus critiques pour leurs entreprises, les

clients doivent protéger ces VM des mêmes types de catastrophes que leurs ressources informatiques physiques. Les solutions de reprise après sinistre (DR) actuellement proposées sont complexes, coûteuses et gourmandes en ressources. NetApp, le plus grand fournisseur de stockage utilisé pour les infrastructures virtualisées, a tout intérêt à garantir que les machines virtuelles de ses clients sont protégées de la même manière que nous protégeons les données hébergées sur le stockage ONTAP de tout type. Pour atteindre cet objectif, NetApp a créé le service NetApp Disaster Recovery .

L'un des principaux défis de toute solution DR est la gestion du coût supplémentaire lié à l'achat, à la configuration et à la maintenance de ressources de calcul, de réseau et de stockage supplémentaires, simplement pour fournir une infrastructure de réplication et de récupération DR. Une option populaire pour protéger les ressources virtuelles critiques sur site consiste à utiliser des ressources virtuelles hébergées dans le cloud comme infrastructure de réplication et de récupération DR. Amazon est un exemple d'une telle solution qui peut fournir des ressources rentables compatibles avec les infrastructures de machines virtuelles hébergées par NetApp ONTAP .

Amazon a présenté son service Amazon Elastic VMware (Amazon EVS) qui active VMware Cloud Foundation au sein de votre cloud privé virtuel (VPC). Amazon EVS offre la résilience et les performances d'AWS ainsi que les logiciels et outils VMware familiers permettant aux vCenters Amazon EVS d'être intégrés en tant qu'extension de votre infrastructure virtualisée sur site.

Bien qu'Amazon EVS soit fourni avec des ressources de stockage incluses, l'utilisation du stockage natif peut réduire son efficacité pour les organisations ayant des charges de travail gourmandes en stockage. Dans ces cas, l'association d'Amazon EVS avec Amazon FSx for NetApp ONTAP (Amazon FSxN) peut fournir une solution de stockage plus flexible. De plus, lorsque vous utilisez des solutions de stockage NetApp ONTAP sur site pour héberger votre infrastructure VMware, l'utilisation d'Amazon EVS avec FSx for ONTAP signifie que vous obtenez les meilleures fonctionnalités d'interopérabilité et de protection des données entre vos infrastructures sur site et hébergées dans le cloud.

Pour plus d'informations sur Amazon FSx for NetApp ONTAP, consultez "Premiers pas avec Amazon FSx for NetApp ONTAP" .

Présentation de la solution NetApp Disaster Recovery à l'aide d'Amazon EVS et d'Amazon FS pour NetApp ONTAP

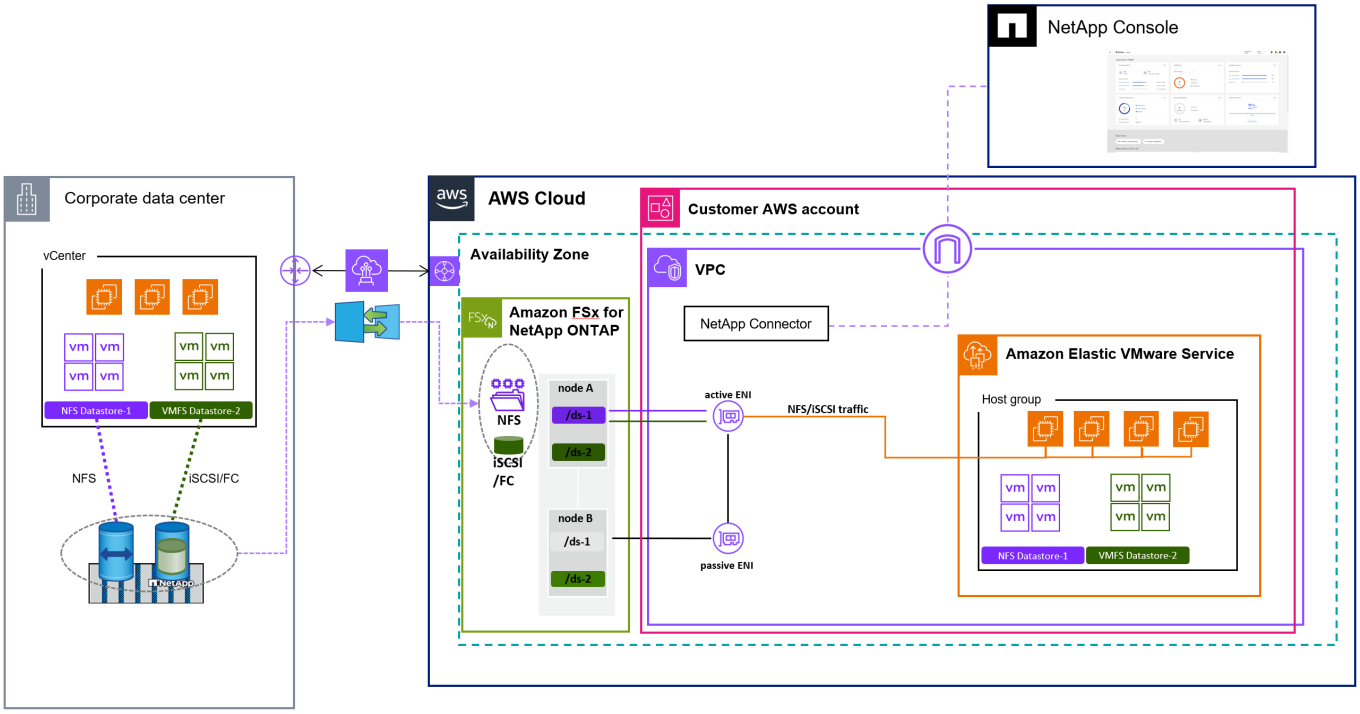
NetApp Disaster Recovery est un service à valeur ajoutée hébergé dans l'environnement logiciel en tant que service NetApp Console , qui dépend de l'architecture principale de NetApp Console . Plusieurs composants principaux composent le service DR pour la protection VMware au sein de la console.

Pour un aperçu complet de la solution NetApp Disaster Recovery , consultez"En savoir plus sur NetApp Disaster Recovery pour VMware" .

Si vous souhaitez protéger vos machines virtuelles hébergées VMware sur site sur Amazon AWS, utilisez le service pour sauvegarder sur Amazon EVS avec les magasins de données hébergés sur le stockage Amazon FSx for NetApp ONTAP .

La figure suivante montre comment le service fonctionne pour protéger vos machines virtuelles avec Amazon EVS.

Présentation de la NetApp Disaster Recovery à l'aide d'Amazon EVS et de FSx pour ONTAP



1. Amazon EVS est déployé sur votre compte dans une configuration de zone de disponibilité (AZ) unique et au sein de votre cloud privé virtuel (VPC).
2. Un système de fichiers FSx pour ONTAP est déployé dans la même zone de disponibilité que le déploiement Amazon EVS. Le système de fichiers se connecte à Amazon EVS soit directement via une interface réseau élastique (ENI), une connexion homologue VPC ou une passerelle AmazonTransit.
3. L'agent de la NetApp Console est installé sur votre VPC. L'agent NetApp Console héberge plusieurs services de gestion des données (appelés agents), notamment l'agent NetApp Disaster Recovery qui gère la reprise après sinistre de l'infrastructure VMware sur vos centres de données physiques locaux et sur vos ressources hébergées Amazon AWS.
4. L'agent NetApp Disaster Recovery communique en toute sécurité avec le service hébergé dans le cloud NetApp Console pour recevoir des tâches et distribue ces tâches aux instances de stockage vCenter et ONTAP locales et hébergées par AWS appropriées.
5. Vous créez un plan de réplication à l'aide de la console d'interface utilisateur hébergée dans le cloud NetApp Console indiquant les machines virtuelles qui doivent être protégées, la fréquence à laquelle ces machines virtuelles doivent être protégées et les procédures à exécuter pour redémarrer ces machines virtuelles en cas de basculement à partir du site local.
6. Le plan de réplication détermine quels magasins de données vCenter hébergent les machines virtuelles protégées et les volumes ONTAP qui hébergent ces magasins de données. Si les volumes n'existent pas encore sur le cluster FSx for ONTAP , NetApp Disaster Recovery les crée automatiquement.
7. Une relation SnapMirror est créée pour chaque volume ONTAP source identifié vers chaque volume ONTAP hébergé par FSx for ONTAP de destination et une planification de réplication est créée en fonction du RPO fourni par l'utilisateur dans le plan de réplication.
8. En cas de défaillance du site principal, un administrateur lance un processus de basculement manuel dans la NetApp Console et sélectionne une sauvegarde à utiliser comme point de restauration.
9. L'agent NetApp Disaster Recovery active les volumes de protection des données hébergés par FSx for ONTAP .
10. L'agent enregistre chaque volume FSx for ONTAP activé auprès d'Amazon EVS vCenter, enregistre chaque machine virtuelle protégée auprès d'Amazon EVS vCenter et démarre chacune d'elles

conformément aux règles prédéfinies contenues dans le plan de réplication.

Installer l'agent NetApp Console pour NetApp Disaster Recovery

Un agent NetApp Console vous permet de connecter vos déploiements NetApp Console à votre infrastructure afin d'orchestrer en toute sécurité des solutions sur AWS, Azure, Google Cloud ou dans des environnements sur site. L'agent Console exécute les actions que la NetApp Console doit effectuer pour gérer votre infrastructure de données. L'agent Console interroge en permanence la couche de logiciel en tant que service NetApp Disaster Recovery pour toute action qu'il doit entreprendre.

Pour NetApp Disaster Recovery, les actions effectuées orchestrent les clusters VMware vCenter et les instances de stockage ONTAP à l'aide des API natives de chaque service respectif afin d'assurer la protection des machines virtuelles de production exécutées sur un site sur site. Bien que l'agent Console puisse être installé dans n'importe lequel de vos emplacements réseau, il est recommandé d'installer l'agent Console sur le site de reprise après sinistre pour NetApp Disaster Recovery. L'installation sur le site de DR garantit qu'en cas de défaillance du site principal, l'interface utilisateur de la console NetApp maintient sa connexion à l'agent Console et peut orchestrer le processus de reprise au sein de ce site de DR.

Installation

- Pour utiliser la récupération après sinistre, installez l'agent Console en mode standard. Pour en savoir plus sur les types d'installation de l'agent Console, visitez "Découvrez les modes de déploiement de la NetApp Console".

Les étapes d'installation spécifiques de l'agent Console dépendent de votre type de déploiement. Voir "En savoir plus sur les agents de console" pour plus d'informations.

La méthode la plus simple pour installer l'agent Console avec Amazon AWS consiste à utiliser AWS Marketplace. Pour plus d'informations sur l'installation de l'agent Console à l'aide de AWS Marketplace, voir "Créez un agent Console à partir de l'AWS Marketplace".

Configurer NetApp Disaster Recovery pour Amazon EVS

Présentation de la configuration de NetApp Disaster Recovery pour Amazon EVS

Après avoir installé l'agent NetApp Console , vous devez intégrer toutes les ressources de stockage ONTAP et VMware vCenter qui participeront au processus de reprise après sinistre avec NetApp Disaster Recovery.

- "Conditions préalables pour Amazon EVS avec NetApp Disaster Recovery"
- "Ajoutez des baies de stockage ONTAP à NetApp Disaster Recovery"
- "Activer la NetApp Disaster Recovery pour Amazon EVS"
- "Ajouter des sites vCenter à NetApp Disaster Recovery"
- "Ajouter des clusters vCenter à NetApp Disaster Recovery"

Conditions préalables pour Amazon EVS avec NetApp Disaster Recovery

Assurez-vous de consulter et de respecter les exigences pour configurer Amazon EVS

avec NetApp Disaster Recovery.

Prérequis

- Examinez le "Prérequis généraux pour NetApp Disaster Recovery".
- Créez un compte utilisateur vCenter avec les privilèges VMware spécifiques requis pour NetApp Disaster Recovery pour effectuer les opérations nécessaires.

> Il est recommandé de **ne pas** utiliser le compte administrateur par défaut "administrator@vsphere.com". À la place, vous devez créer un compte utilisateur spécifique à NetApp Disaster Recovery sur tous les clusters vCenter qui participeront au processus de reprise après sinistre. Pour obtenir la liste des privilèges spécifiques requis, consultez "Privilèges vCenter nécessaires pour la NetApp Disaster Recovery".

- Assurez-vous que toutes les banques de données vCenter qui hébergeront des machines virtuelles protégées par NetApp Disaster Recovery sont situées sur des ressources de stockage NetApp ONTAP.

  La reprise après sinistre prend en charge NFS et VMFS sur iSCSI (et non FC) lors de l'utilisation d'Amazon FSx sur NetApp ONTAP. Bien que la reprise après sinistre prenne en charge FC, Amazon FSx for NetApp ONTAP ne le fait pas.

- Assurez-vous que votre Amazon EVS vCenter est connecté à un cluster de stockage Amazon FSx for NetApp ONTAP.
- Assurez-vous que les outils VMware sont installés sur toutes les machines virtuelles protégées.
- Assurez-vous que votre réseau local est connecté à votre réseau AWS VPC à l'aide d'une méthode de connexion approuvée par Amazon. Il est recommandé d'utiliser AWS Direct Connect, AWS Private Link ou un AWS Site-to-Site VPN.
- Vérifiez et assurez la conformité aux exigences de connexion et de port pour EVS avec NetApp Disaster Recovery :

Source	Destination	Port	Détails
Amazon FSxN	ONTAP sur site	TCP 11104, 11105, ICMP	SnapMirror
ONTAP sur site	Amazon FSxN	TCP 11104, 11105, ICMP	SnapMirror
Agent NetApp Console	ONTAP sur site	TCP 443, ICMP uniquement	appels API
Agent NetApp Console	Amazon FSxN	TCP 441, ICMP uniquement	appels API
Agent NetApp Console	vCenter (sur site, EVS), hôte ESXi (sur site, EVS)	443	Appels d'API, exécution de scripts

Ajoutez des baies sur site au système de NetApp Console pour Amazon EVS avec NetApp Disaster Recovery

Avant d'utiliser NetApp Disaster Recovery, vous devez ajouter des instances de stockage sur site et hébergées dans le cloud au système NetApp Console .

Vous devez effectuer les opérations suivantes :

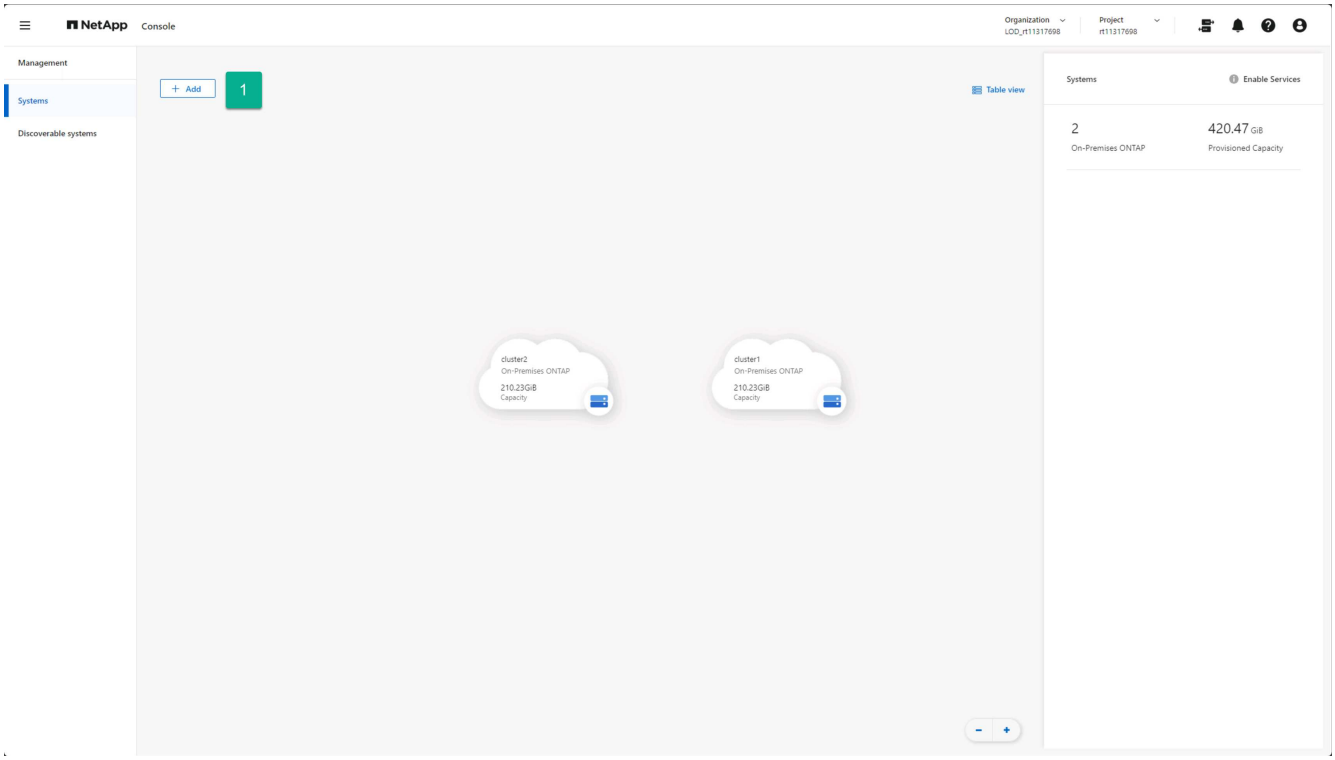
- Ajoutez des baies sur site à votre système de NetApp Console .

- Ajoutez des instances Amazon FSx for NetApp ONTAP (FSx for ONTAP) à votre système de NetApp Console .

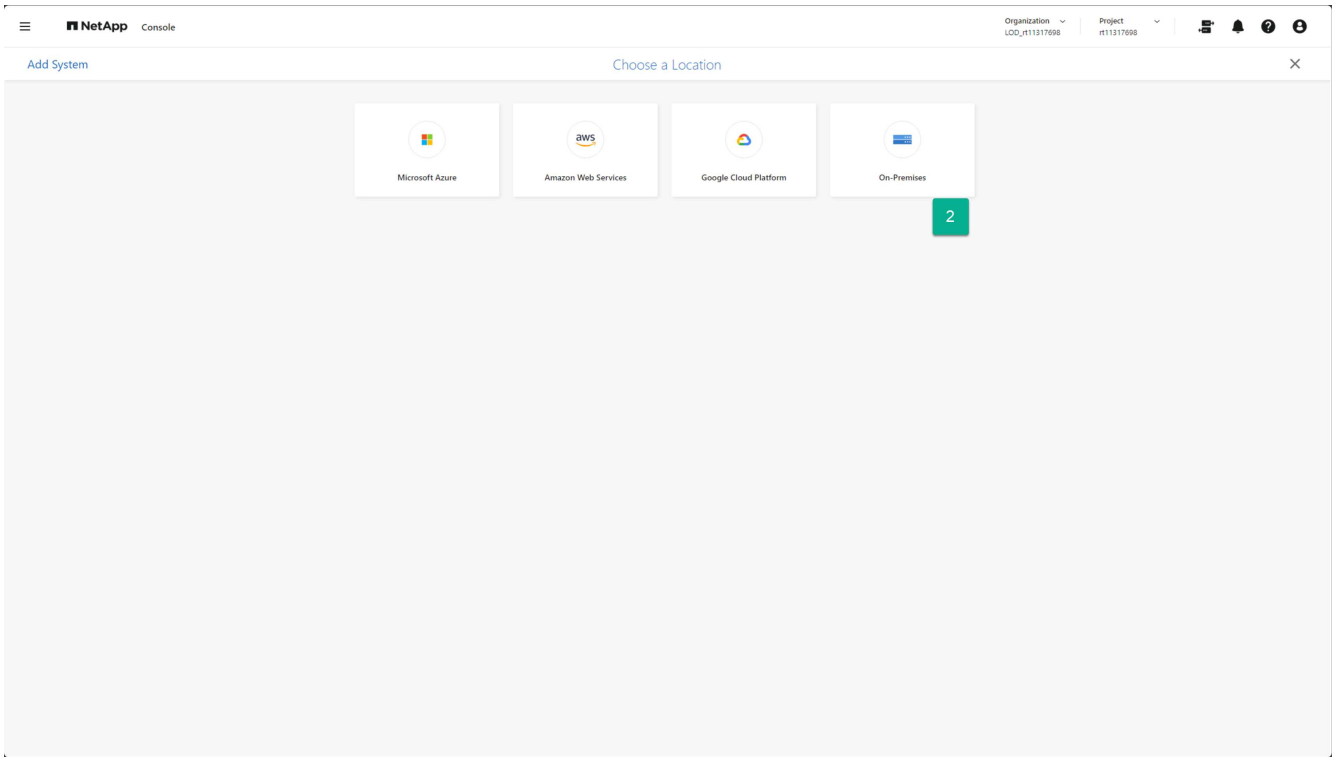
Ajouter des baies de stockage sur site au système NetApp Console

Ajoutez des ressources de stockage ONTAP sur site à votre système de NetApp Console .

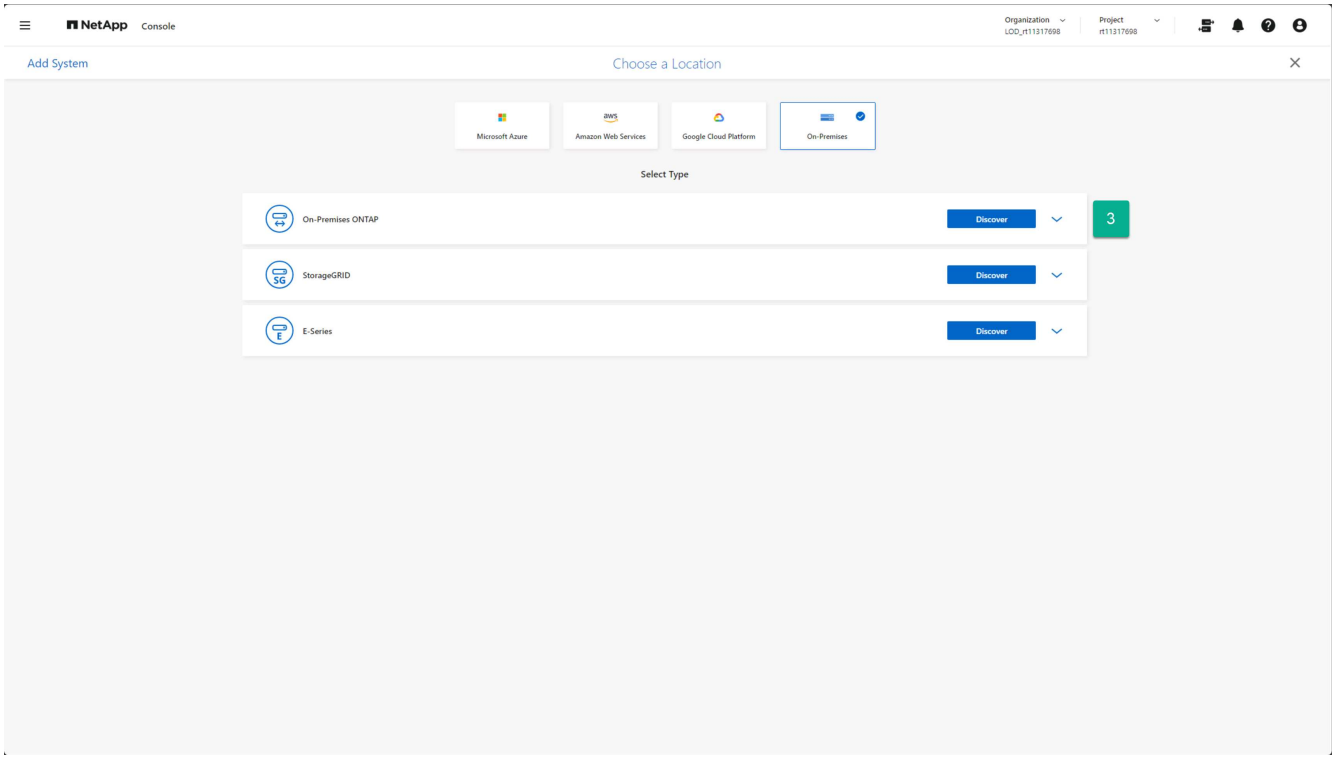
1. Depuis la page Systèmes de la NetApp Console , sélectionnez **Ajouter un système**.



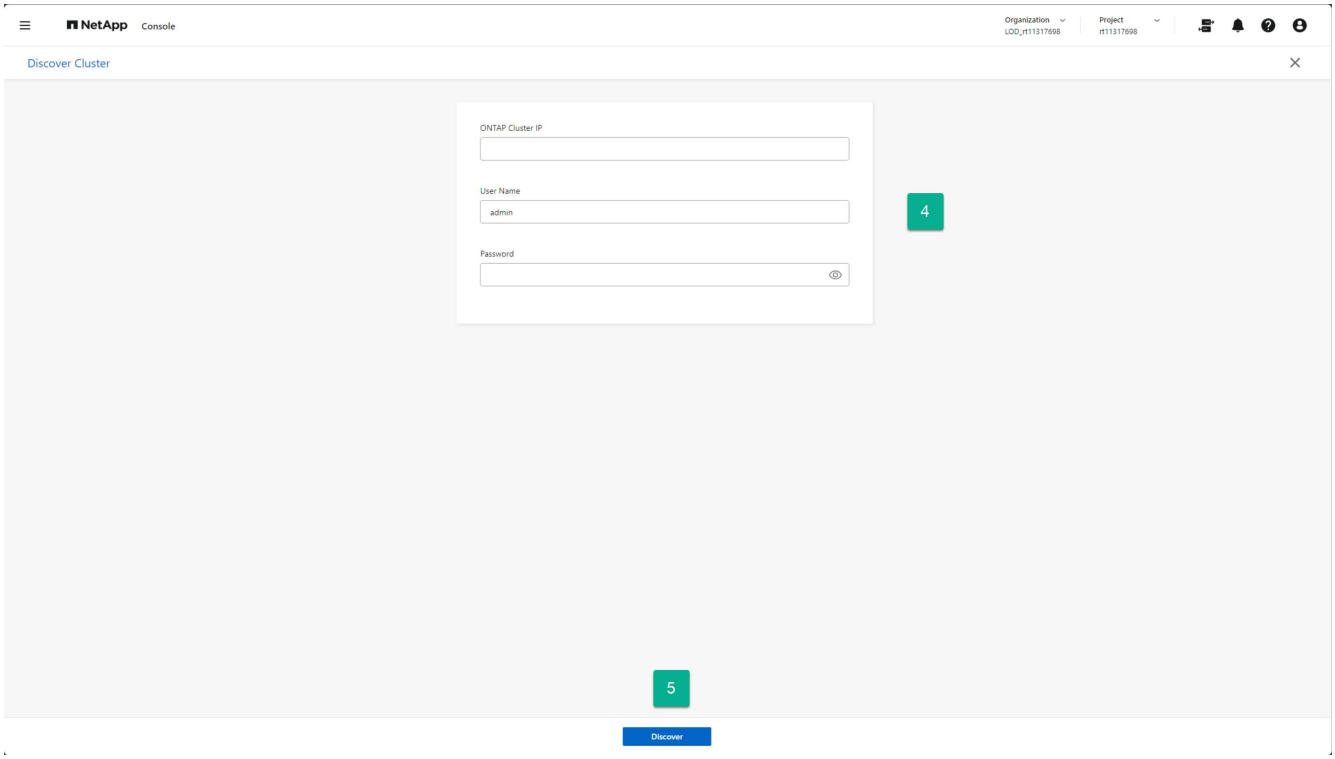
2. Depuis la page Ajouter un système, sélectionnez la carte **Sur site**.



3. Sélectionnez **Découvrir** sur la carte ONTAP sur site.



4. Sur la page Découvrir le cluster, saisissez les informations suivantes :
   a. L'adresse IP du port de gestion du cluster de matrice ONTAP
   b. Le nom d'utilisateur de l'administrateur
   c. Le mot de passe administrateur
5. Sélectionnez **Découvrir** au bas de la page.

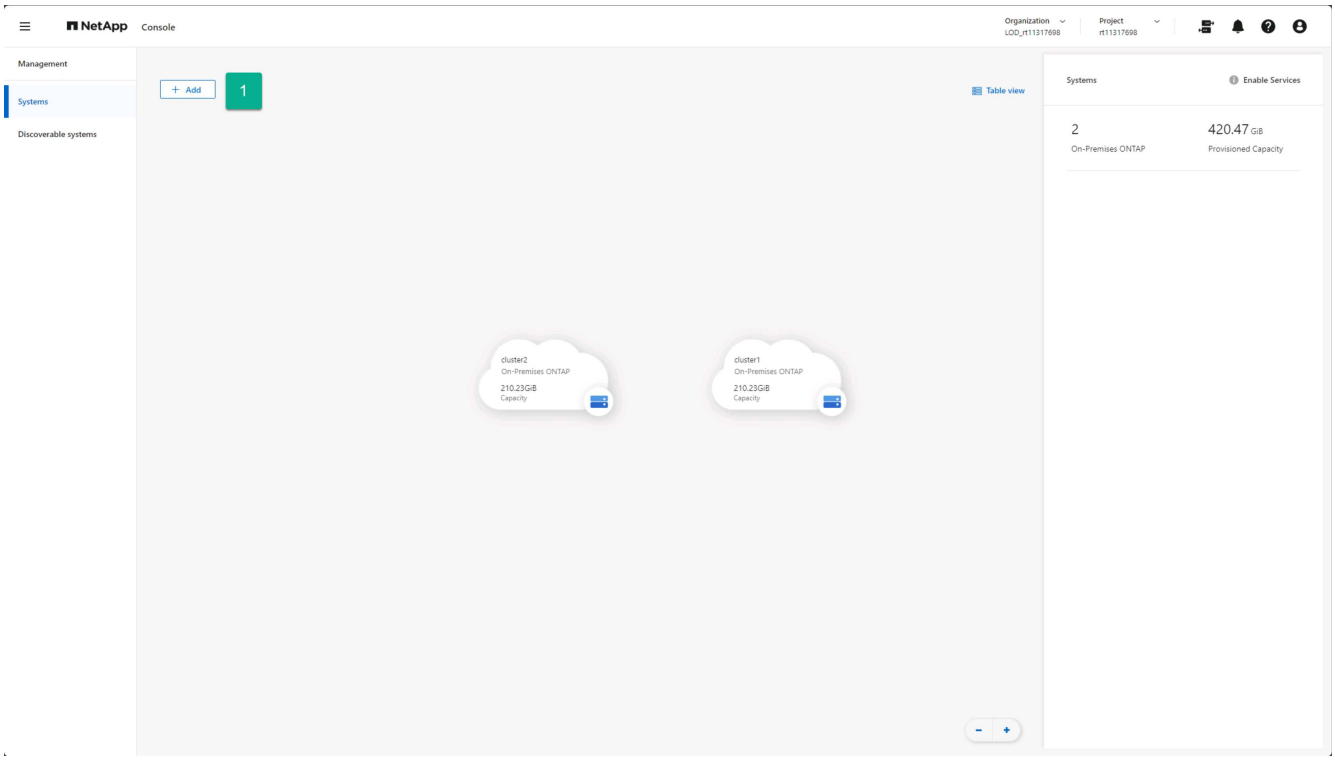


6. Répétez les étapes 1 à 5 pour chaque baie ONTAP qui hébergera les banques de données vCenter.

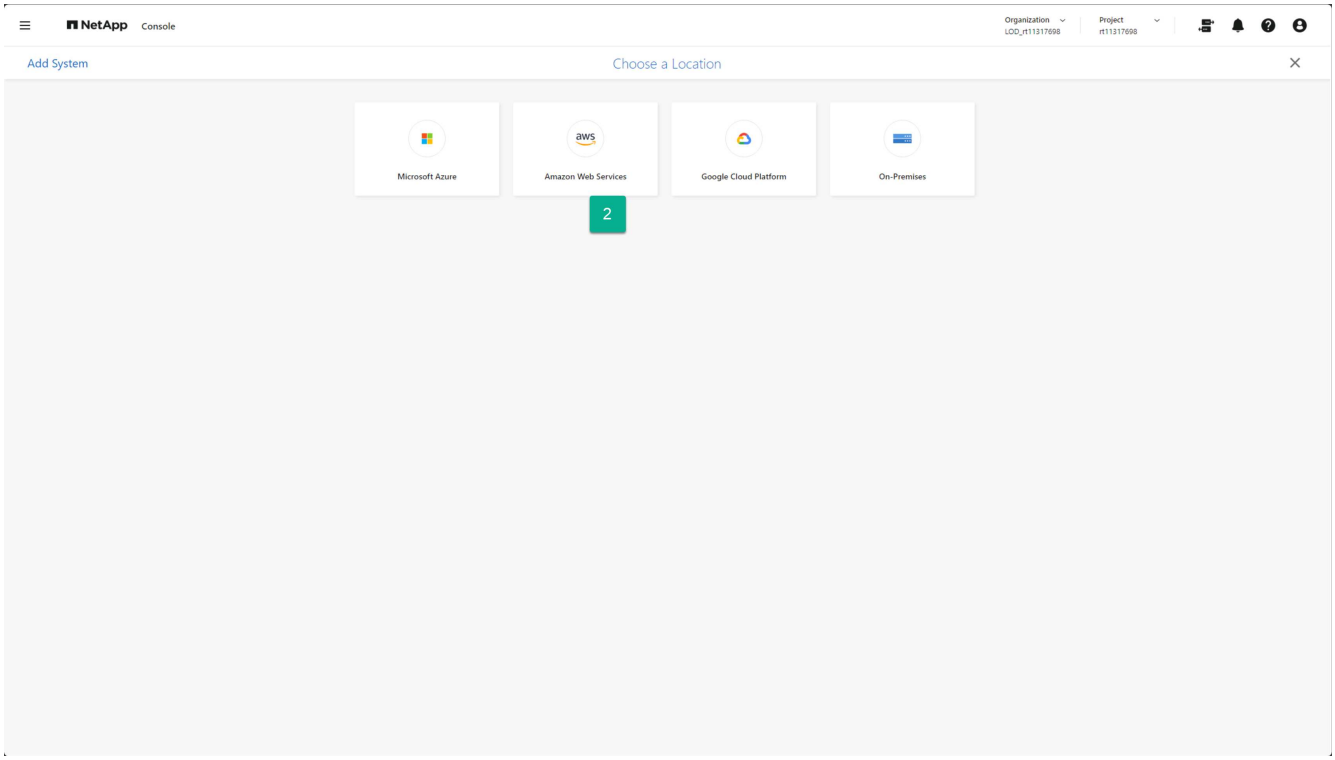
Ajoutez des instances de stockage Amazon FSx for NetApp ONTAP au système NetApp Console

Ensuite, ajoutez des ressources de stockage Amazon FSx for NetApp ONTAP à votre système de NetApp Console .

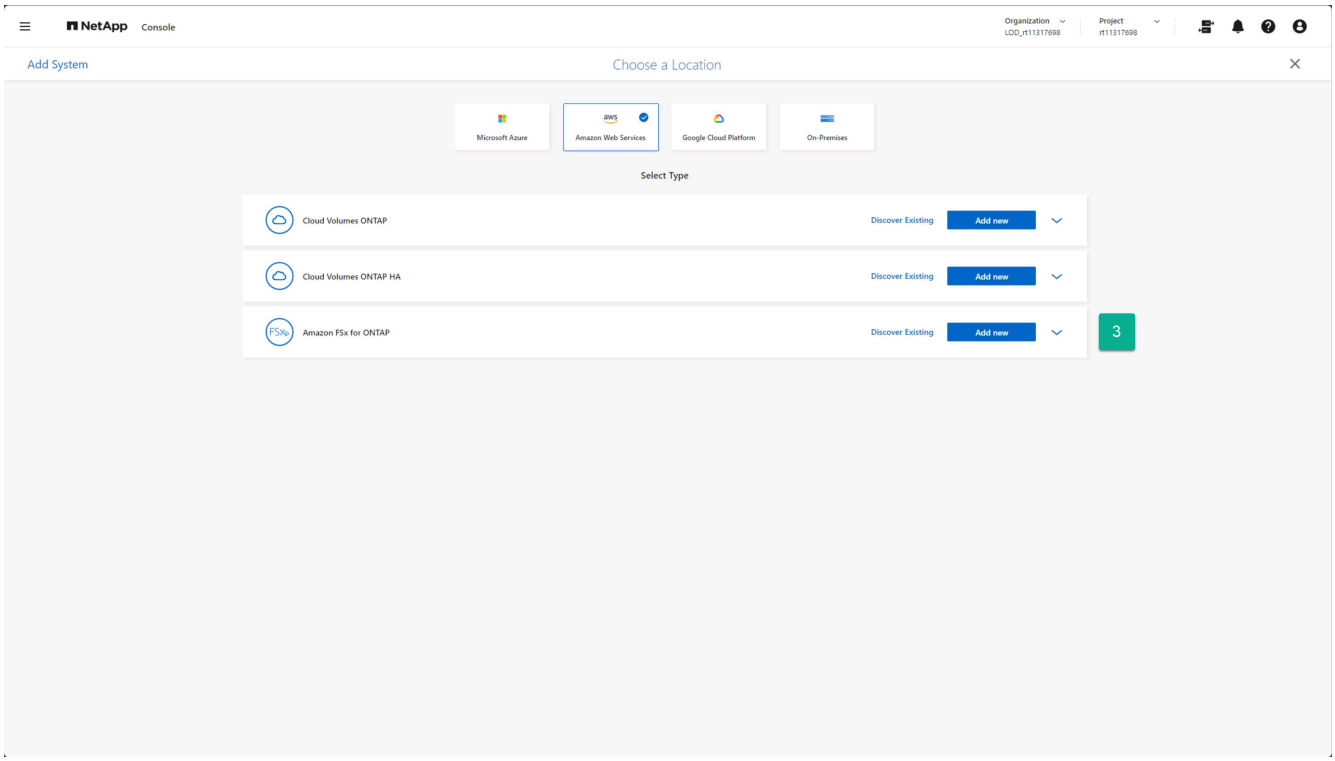
1. Depuis la page Systèmes de la NetApp Console , sélectionnez **Ajouter un système**.



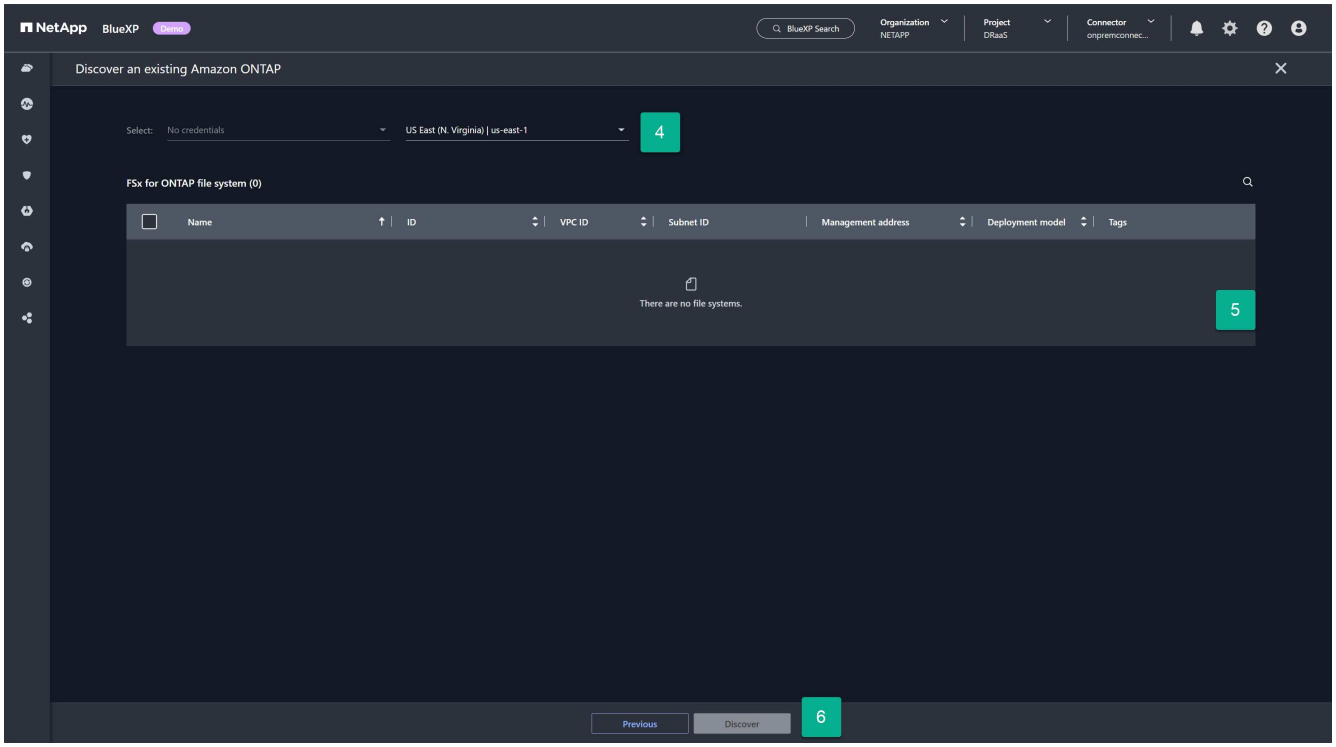
2. Depuis la page Ajouter un système, sélectionnez la carte **Amazon Web Services**.



3. Sélectionnez le lien **Découvrir l'existant** sur la carte Amazon FSx for ONTAP .



4. Sélectionnez les informations d'identification et la région AWS hébergeant l'instance FSx for ONTAP .
5. Sélectionnez un ou plusieurs systèmes de fichiers FSx for ONTAP à ajouter.
6. Sélectionnez **Découvrir** au bas de la page.



7. Répétez les étapes 1 à 6 pour chaque instance FSx for ONTAP qui hébergera les banques de données vCenter.

Ajoutez le service NetApp Disaster Recovery à votre compte NetApp Console pour Amazon EVS

NetApp Disaster Recovery est une offre de produit sous licence qui doit être achetée avant de pouvoir être utilisée. Il existe plusieurs types de licences et plusieurs façons d'acheter des licences. Une licence vous donne le droit de protéger une quantité spécifique de données pendant une durée déterminée.

Pour plus d'informations sur les licences NetApp Disaster Recovery , consultez"Configurer les licences pour NetApp Disaster Recovery" .

Types de licences

Il existe deux principaux types de licences :

- NetApp propose une"Licence d'essai de 30 jours" que vous pouvez utiliser pour évaluer NetApp Disaster Recovery à l'aide de vos ressources ONTAP et VMware. Cette licence offre 30 jours d'utilisation pour une quantité illimitée de capacité protégée.
- Achetez une licence de production si vous souhaitez une protection DR au-delà de la période d'essai de 30 jours. Cette licence peut être achetée via les places de marché de n'importe quel partenaire cloud de NetApp, mais pour ce guide, nous vous recommandons d'acheter votre licence de place de marché pour NetApp Disaster Recovery à l'aide d'Amazon AWS Marketplace. Pour en savoir plus sur l'achat d'une licence via Amazon Marketplace, consultez"Abonnez-vous via AWS Marketplace" .

Évaluez vos besoins en capacité de reprise après sinistre

Avant d'acheter votre licence, vous devez comprendre la capacité de stockage ONTAP que vous devez protéger. L'un des avantages de l'utilisation du stockage NetApp ONTAP est la grande efficacité avec laquelle NetApp stocke vos données. Toutes les données stockées dans un volume ONTAP (comme les machines

virtuelles hébergeant une banque de données VMware) sont stockées de manière très efficace. ONTAP utilise par défaut trois types d'efficacité de stockage lors de l'écriture de données sur un stockage physique : compactage, déduplication et compression. Le résultat net est une efficacité de stockage comprise entre 1,5:1 et 4:1 selon les types de données stockées. En fait, NetApp propose une "garantie d'efficacité de stockage" pour certaines charges de travail.

Cela peut vous être bénéfique car NetApp Disaster Recovery calcule la capacité à des fins de licence une fois que toutes les efficacités de stockage ONTAP ont été appliquées. Par exemple, supposons que vous ayez provisionné une banque de données NFS de 100 téraoctets (Tio) dans vCenter pour héberger 100 machines virtuelles que vous souhaitez protéger à l'aide du service. De plus, supposons que lorsque les données sont écrites sur le volume ONTAP , les techniques d'efficacité de stockage appliquées automatiquement entraînent une consommation de seulement 33 Tio par ces machines virtuelles (efficacité de stockage 3:1). NetApp Disaster Recovery doit être concédé sous licence uniquement pour 33 Tio, et non pour 100 Tio. Cela peut représenter un avantage considérable sur le coût total de possession de votre solution DR par rapport à d'autres solutions DR.

Étapes

1. Pour déterminer la quantité de données consommée sur chaque volume hébergeant une banque de données VMware à protéger, déterminez la consommation de capacité sur disque en exécutant la commande ONTAP CLI pour chaque volume : `volume show-space -volume < volume name > -vserver < SVM name >`.

   Par exemple:

```
cluster1::> volume show-space
Vserver : vm-nfs-ds1
Volume  : vol0
Feature                                  Used      Used%
------------------------------      --------     ------
User Data                             163.4MB         3%
Filesystem Metadata                     172KB         0%
Inodes                                 2.93MB         0%
Snapshot Reserve                       292.9MB         5%
Total Metadata                          185KB         0%
Total Used                             459.4MB         8%
Total Physical Used                    166.4MB         3%
```

2. Notez la valeur **Total physique utilisé** pour chaque volume. Il s'agit de la quantité de données que NetApp Disaster Recovery doit protéger et c'est la valeur que vous utiliserez pour déterminer la capacité dont vous avez besoin pour obtenir une licence.

Ajouter des sites dans NetApp Disaster Recovery pour Amazon EVS

Avant de pouvoir protéger votre infrastructure de machines virtuelles, identifiez les clusters VMware vCenter qui hébergent les machines virtuelles à protéger et où se trouvent ces vCenters. La première étape consiste à créer un site pour représenter les centres de données source et de destination. Un site est un domaine de défaillance ou un domaine de récupération.

Vous devez créer les éléments suivants :

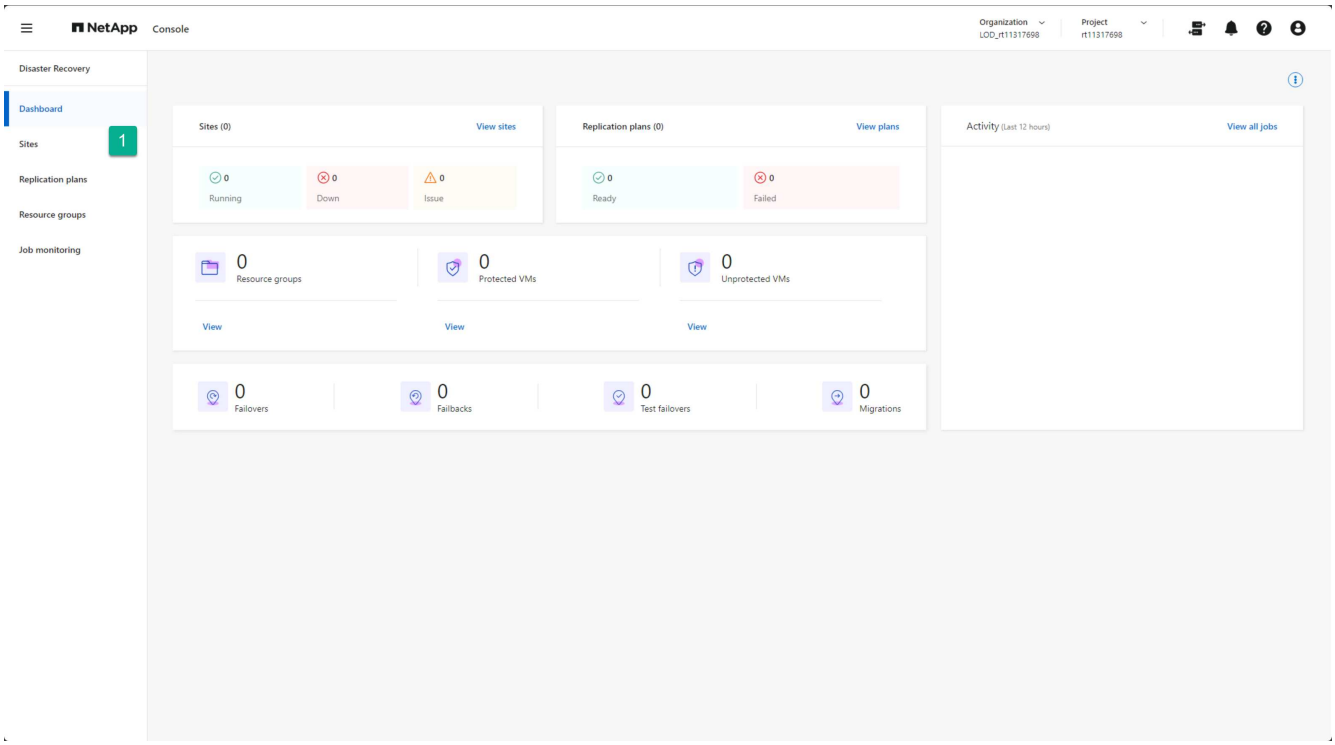
- Un site pour représenter chaque centre de données de production où résident vos clusters vCenter de production
- Un site pour votre centre de données cloud Amazon EVS/ Amazon FSx for NetApp ONTAP

Créer des sites sur site

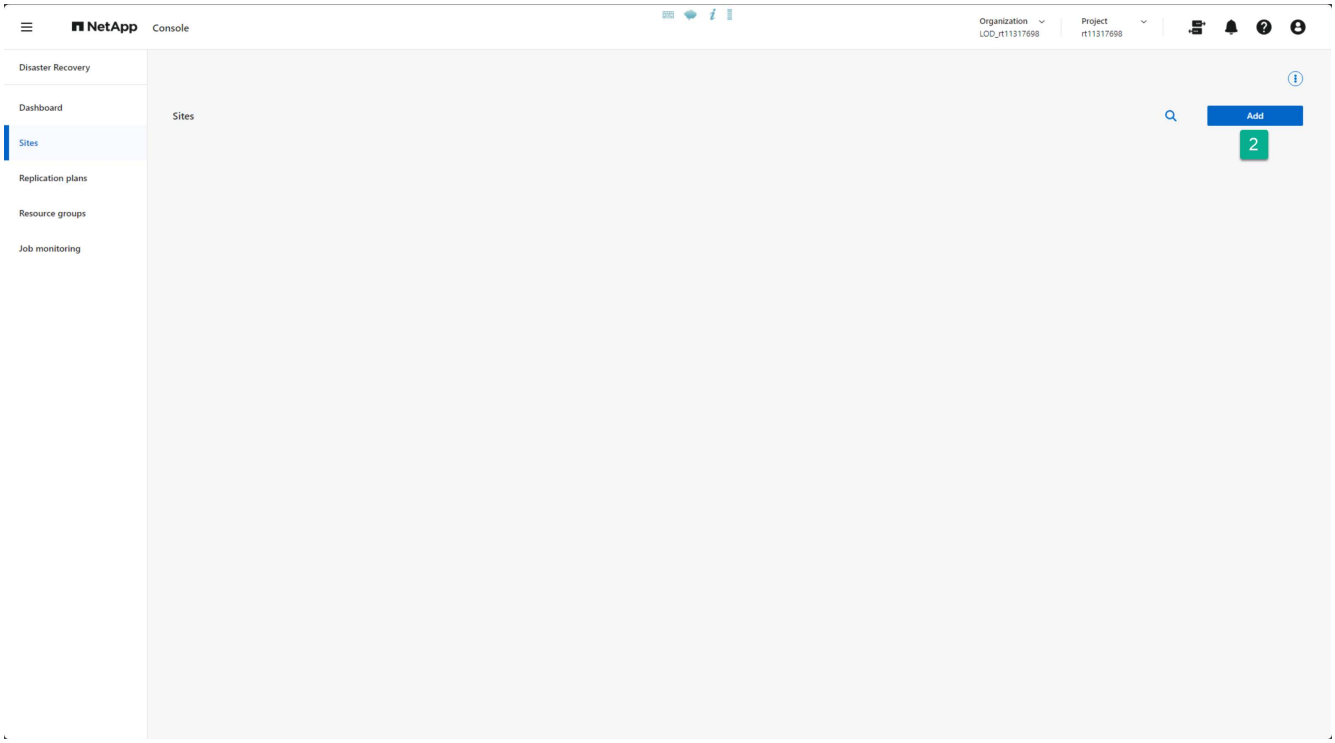
Créez un site vCenter de production.

Étapes

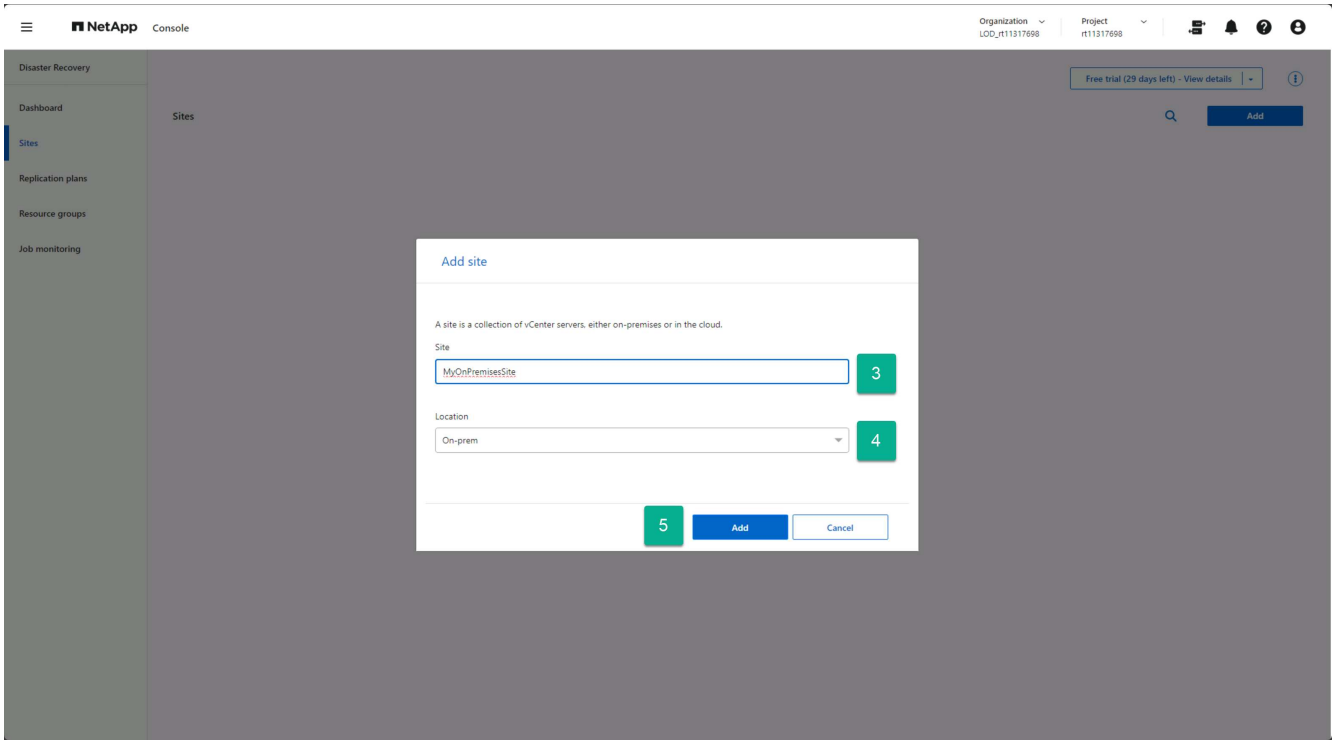
1. Dans la barre de navigation de gauche de la NetApp Console , sélectionnez **Protection** > **Reprise après sinistre**.
2. À partir de n'importe quelle page de NetApp Disaster Recovery, sélectionnez l'option **Sites**.



3. Dans l'option Sites, sélectionnez **Ajouter**.



4. Dans la boîte de dialogue Ajouter un site, indiquez un nom de site.
5. Sélectionnez « Sur site » comme emplacement.
6. Sélectionnez **Ajouter**.

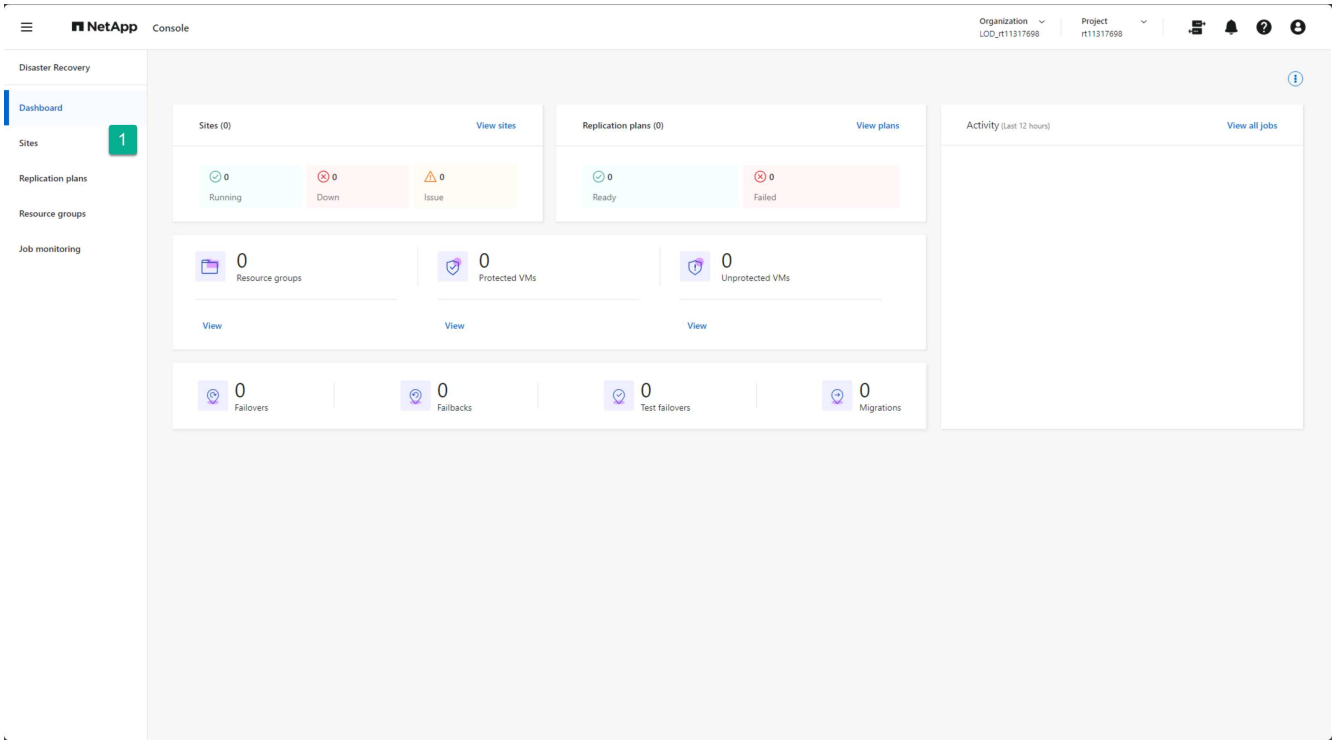


Si vous disposez d'autres sites vCenter de production, vous pouvez les ajouter en suivant les mêmes étapes.

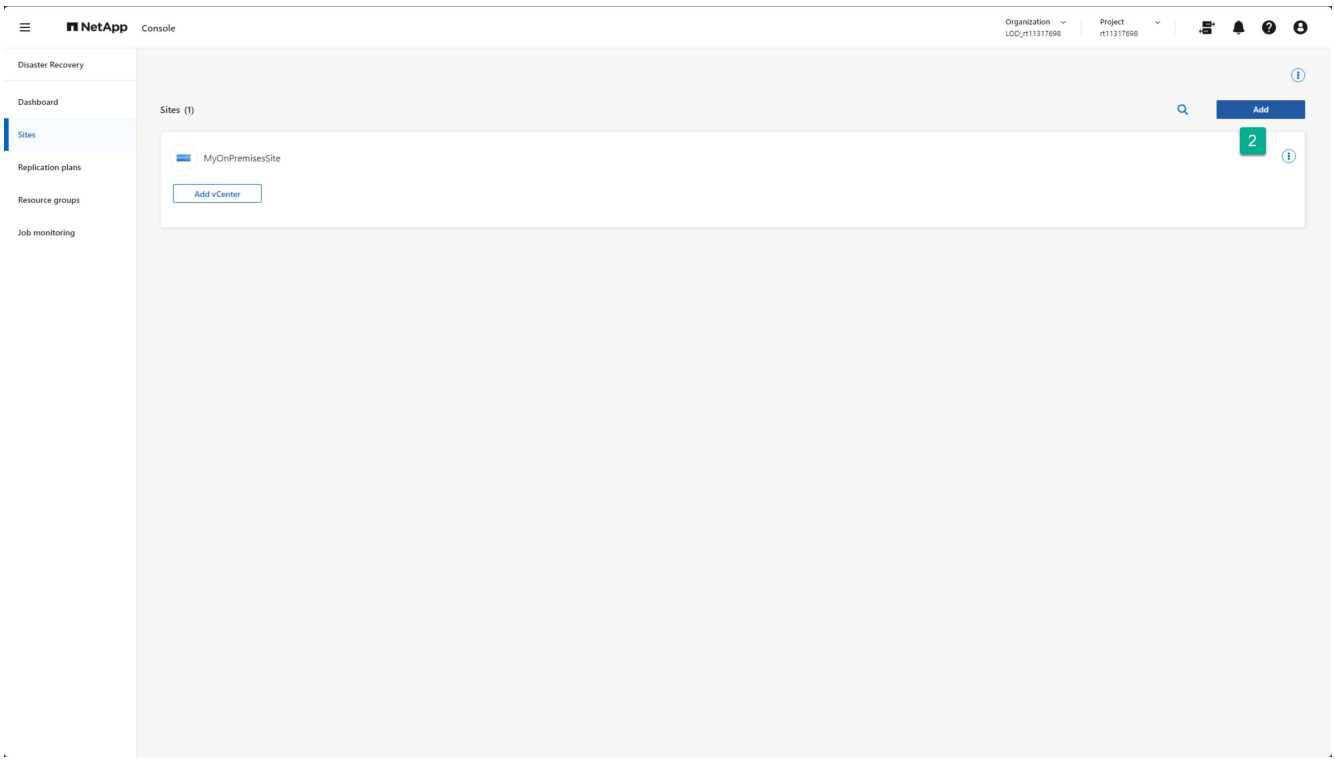
Créer des sites cloud Amazon

Créez un site DR pour Amazon EVS à l'aide Amazon FSx for NetApp ONTAP .

1. À partir de n'importe quelle page de NetApp Disaster Recovery, sélectionnez l'option **Sites**.

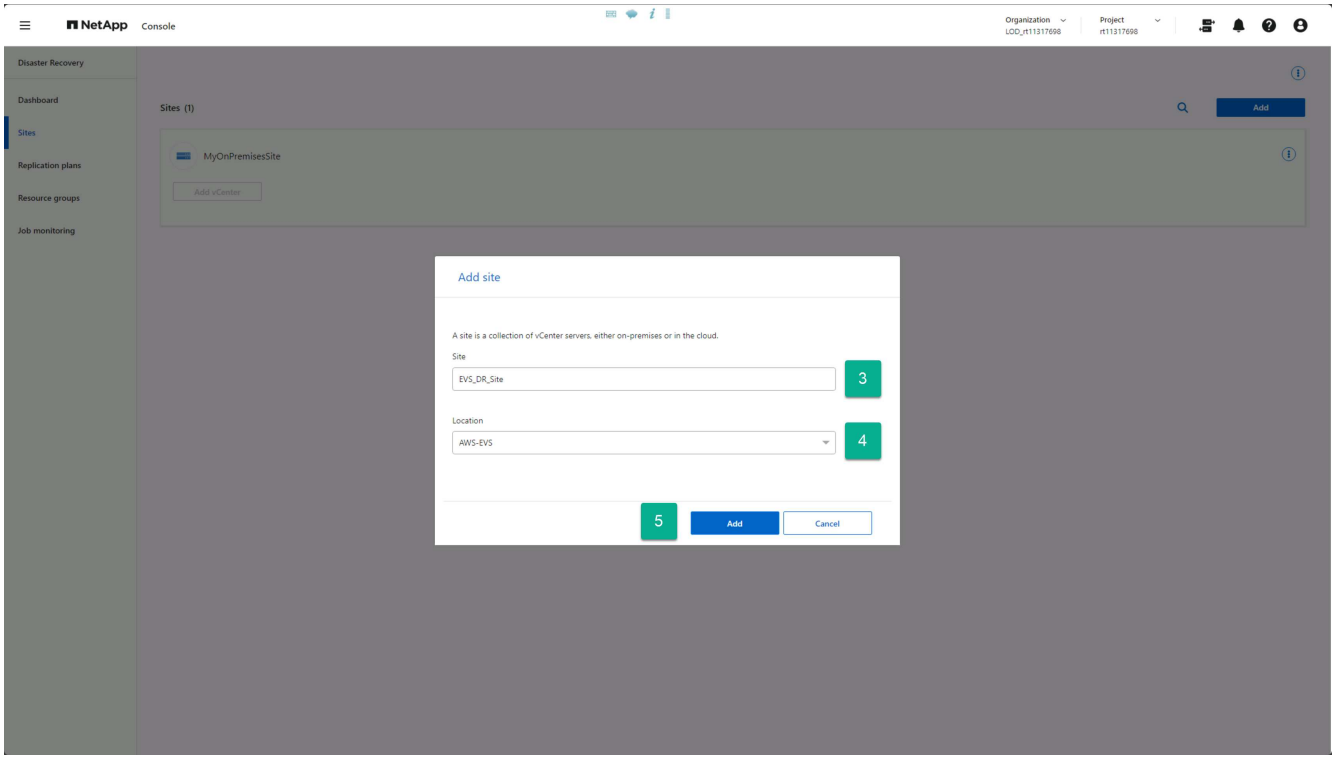


2. Dans l'option Sites, sélectionnez **Ajouter**.



3. Dans la boîte de dialogue Ajouter un site, indiquez un nom de site.

4. Sélectionnez « AWS-EVS » comme emplacement.
5. Sélectionnez **Ajouter**.



Résultat

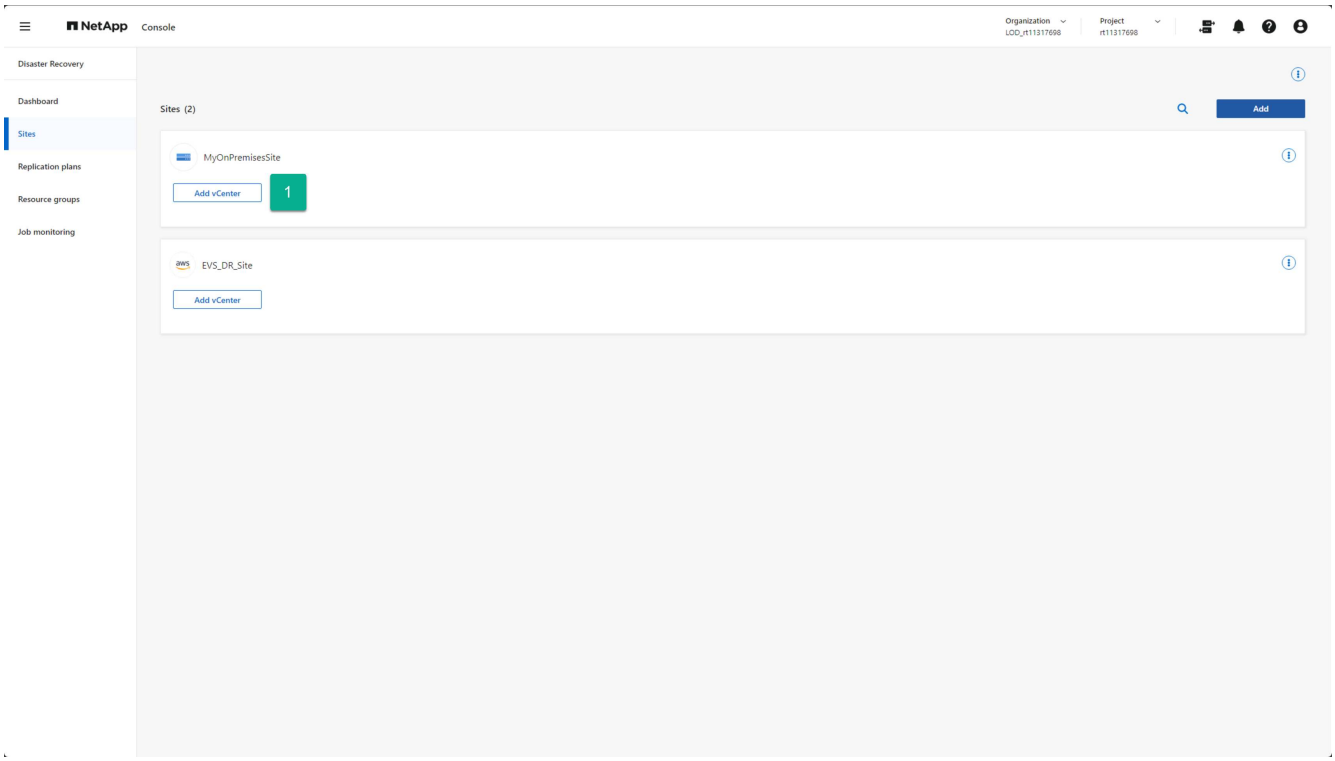
Vous avez maintenant créé un site de production (source) et un site DR (destination).

Ajoutez des clusters vCenter sur site et Amazon EVS dans NetApp Disaster Recovery

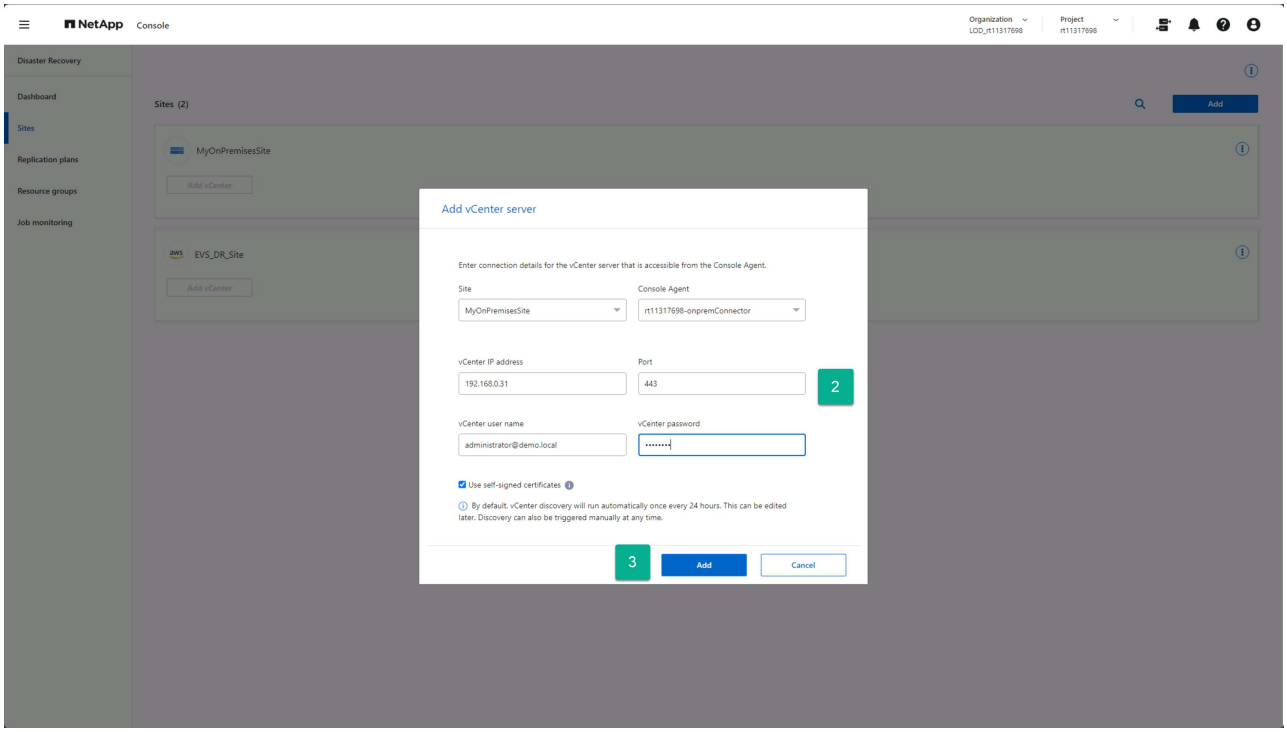
Une fois les sites créés, vous ajoutez désormais vos clusters vCenter à chaque site dans NetApp Disaster Recovery. Lors de la création de chaque site, nous avons indiqué chaque type de site. Cela indique à NetApp Disaster Recovery quel type d'accès est requis pour les vCenters hébergés dans chaque type de site. L'un des avantages d'Amazon EVS est qu'il n'y a pas de réelle différence entre un vCenter Amazon EVS et un vCenter sur site. Les deux nécessitent les mêmes informations de connexion et d'authentification.

Étapes pour ajouter un vCenter à chaque site

1. À partir de l'option **Sites**, sélectionnez **Ajouter vCenter** pour le site souhaité.



2. Dans la boîte de dialogue Ajouter un serveur vCenter, sélectionnez ou fournissez les informations suivantes :
   a. L'agent de la NetApp Console hébergé dans votre AWS VPC.
   b. L'adresse IP ou le nom de domaine complet du vCenter à ajouter.
   c. Si elle est différente, remplacez la valeur du port par le port TCP utilisé par votre gestionnaire de cluster vCenter.
   d. Le nom d'utilisateur vCenter pour le compte créé précédemment qui sera utilisé par NetApp Disaster Recovery pour gérer vCenter.
3. Si votre entreprise utilise une autorité de certification (CA) externe ou le magasin de certificats de point de terminaison vCenter pour accéder à vos vCenters, décochez la case **Utiliser des certificats auto-signés**. Sinon, laissez la case cochée.
   a. Sélectionnez **Ajouter**.



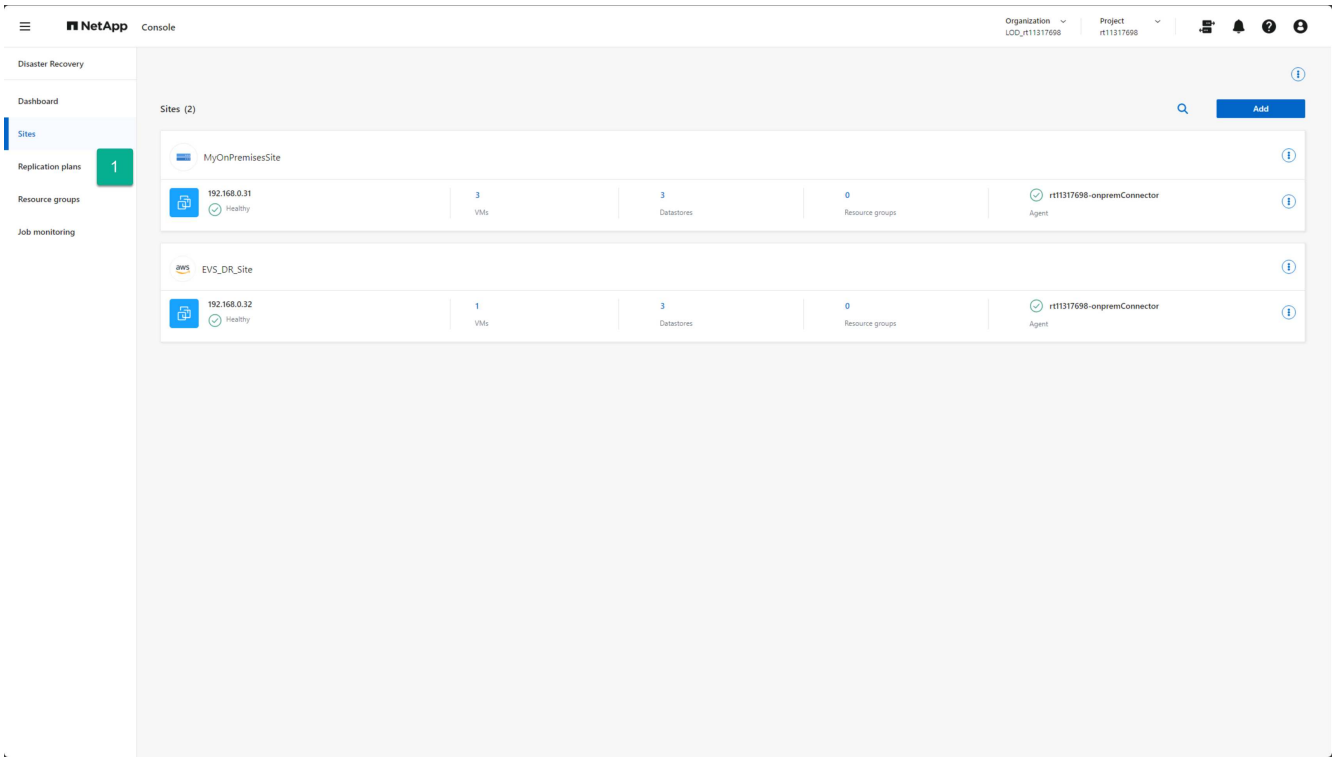
Créer des plans de réplication pour Amazon EVS

Créer des plans de réplication dans la vue d'ensemble de NetApp Disaster Recovery

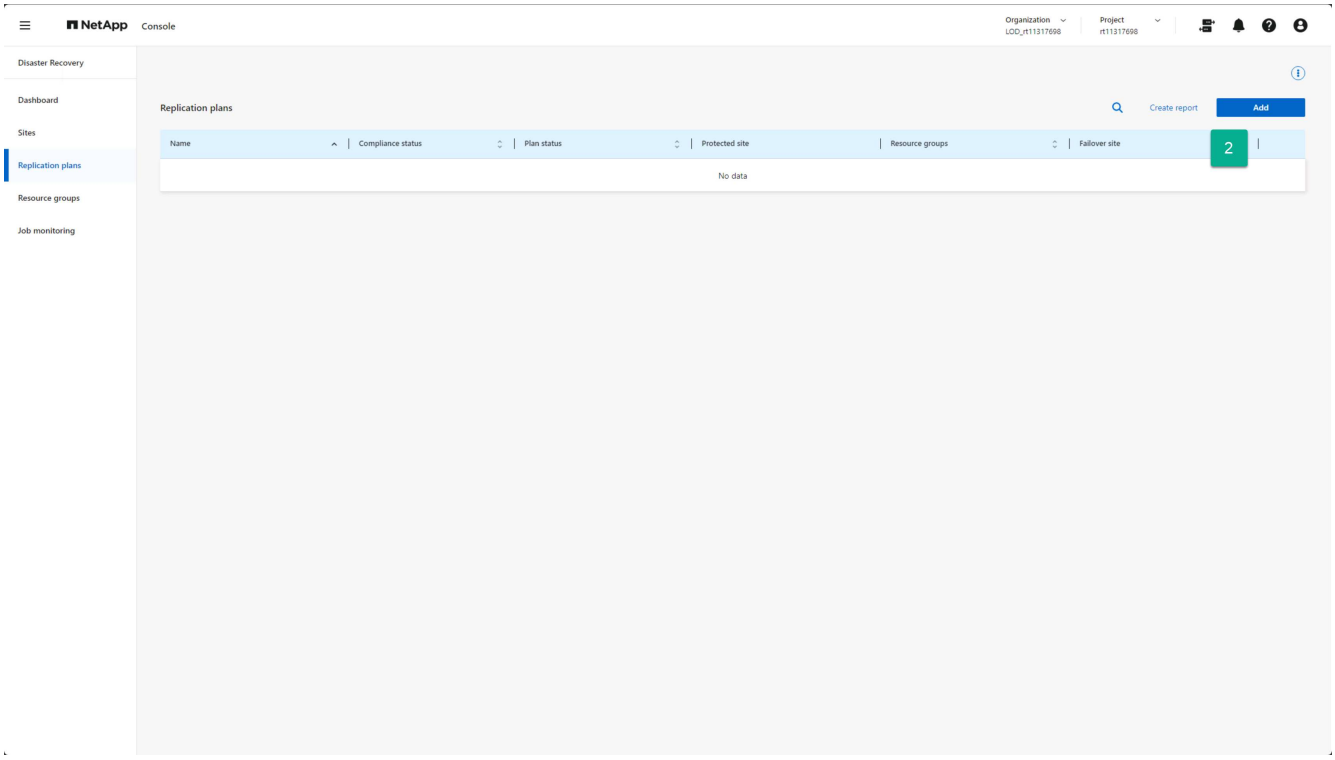
Une fois que vous avez des vCenters à protéger sur le site local et que vous disposez d'un site Amazon EVS configuré pour utiliser Amazon FSx for NetApp ONTAP que vous pouvez utiliser comme destination DR, vous pouvez créer un plan de réplication (RP) pour protéger tout ensemble de machines virtuelles hébergées sur le cluster vCenter au sein de votre site local.

Pour démarrer le processus de création du plan de réplication :

1. À partir de n'importe quel écran de NetApp Disaster Recovery , sélectionnez l'option **Plans de réplication**.



2. Depuis la page Plans de réplication, sélectionnez **Ajouter**.



Cela ouvre l'assistant Créer un plan de réplication.

Continuer avec"Assistant de création de plan de réplication Étape 1" .

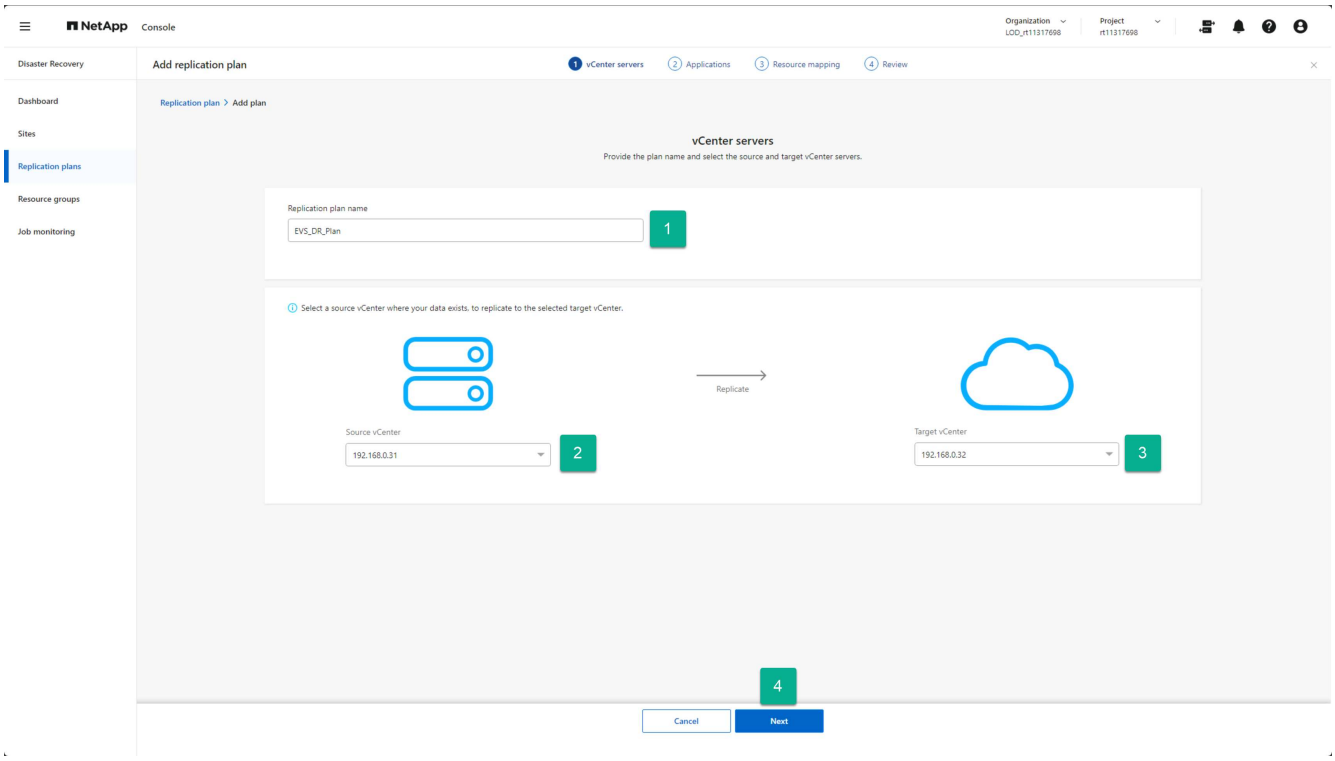
Créer un plan de réplication : Étape 1 : Sélectionner les vCenters dans NetApp Disaster Recovery

Tout d'abord, à l'aide de NetApp Disaster Recovery, indiquez un nom de plan de réplication et sélectionnez les vCenters source et de destination pour la réplication.

1. Saisissez un nom unique pour le plan de réplication.

   Seuls les caractères alphanumériques et les traits de soulignement (_) sont autorisés pour les noms de plans de réplication.

2. Sélectionnez un cluster vCenter source.
3. Sélectionnez un cluster vCenter de destination.
4. Sélectionnez **Suivant**.



Continuer avec"Assistant de création de plan de réplication Étape 2" .

Créer un plan de réplication : Étape 2 : Sélectionner les ressources de la machine virtuelle dans NetApp Disaster Recovery

Sélectionnez les machines virtuelles à protéger à l'aide de NetApp Disaster Recovery.

Il existe plusieurs façons de sélectionner les machines virtuelles à protéger :

- **Sélectionner des machines virtuelles individuelles** : Cliquer sur le bouton **Machines virtuelles** vous permet de sélectionner des machines virtuelles individuelles à protéger. Lorsque vous sélectionnez chaque machine virtuelle, le service l'ajoute à un groupe de ressources par défaut situé sur le côté droit de l'écran.
- **Sélectionnez les groupes de ressources créés précédemment** : vous pouvez créer des groupes de ressources personnalisés au préalable à l'aide de l'option Groupe de ressources du menu NetApp Disaster Recovery . Il ne s'agit pas d'une exigence, car vous pouvez utiliser les deux autres méthodes pour créer un groupe de ressources dans le cadre du processus de plan de réplication. Pour plus de détails,

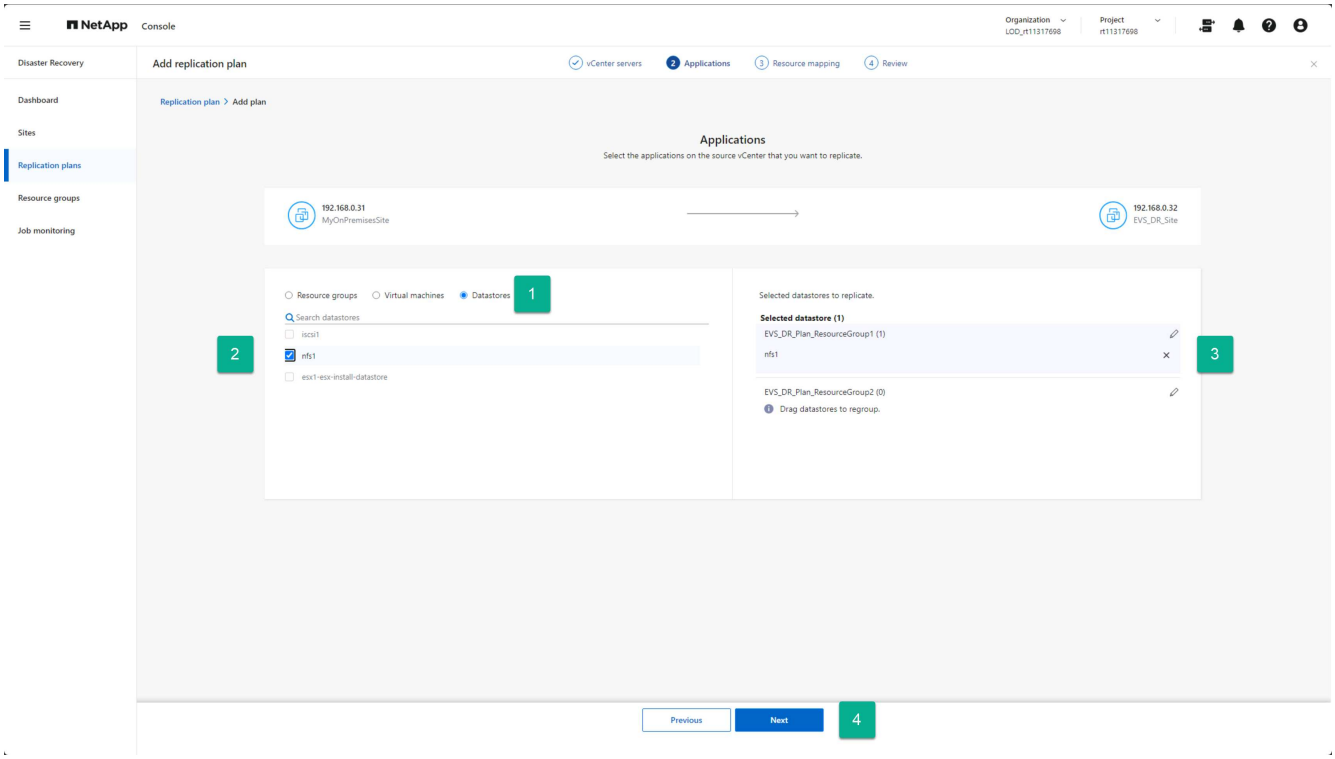
consultez la section "Créer un plan de réplication" .

- **Sélectionnez des banques de données vCenter entières** : si vous avez beaucoup de machines virtuelles à protéger avec ce plan de réplication, il peut ne pas être aussi efficace de sélectionner des machines virtuelles individuelles. Étant donné que NetApp Disaster Recovery utilise la réplication SnapMirror basée sur le volume pour protéger les machines virtuelles, toutes les machines virtuelles résidant sur une banque de données seront répliquées dans le cadre du volume. Dans la plupart des cas, vous devez demander à NetApp Disaster Recovery de protéger et de redémarrer toutes les machines virtuelles situées sur le magasin de données. Utilisez cette option pour indiquer au service d'ajouter toutes les machines virtuelles hébergées sur une banque de données sélectionnée à la liste des machines virtuelles protégées.

Pour cette instruction guidée, nous sélectionnons l'intégralité de la banque de données vCenter.

Étapes pour accéder à cette page

1. À partir de la page **Plan de réplication**, passez à la section **Applications**.
2. Consultez les informations dans la page **Applications** qui s'ouvre.



Étapes pour sélectionner le ou les magasins de données :

1. Sélectionnez **Datastores**.
2. Cochez les cases à côté de chaque banque de données que vous souhaitez protéger.
3. (Facultatif) Renommez le groupe de ressources avec un nom approprié en sélectionnant l'icône en forme de crayon à côté du nom du groupe de ressources.
4. Sélectionnez **Suivant**.

Continuer avec"Assistant de création de plan de réplication Étape 3" .

Créer un plan de réplication : Étape 3 : Mapper les ressources dans NetApp Disaster Recovery

Une fois que vous disposez d'une liste de machines virtuelles que vous souhaitez protéger à l'aide de NetApp Disaster Recovery, fournissez le mappage de basculement et les informations de configuration de machine virtuelle à utiliser lors d'un basculement.

Vous devez cartographier quatre principaux types d'informations :

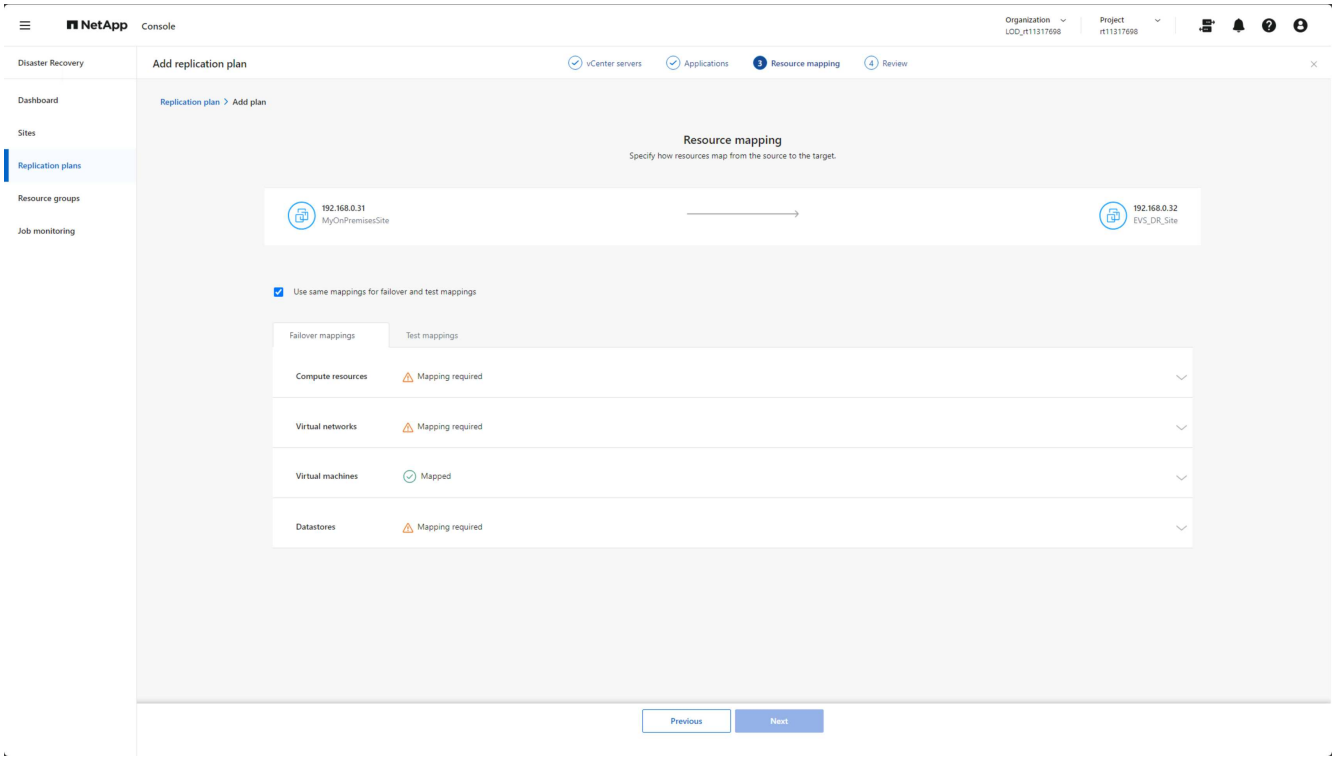
- Ressources de calcul
- Réseaux virtuels
- Reconfiguration de la machine virtuelle
- Cartographie des banques de données

Chaque machine virtuelle nécessite les trois premiers types d'informations. Le mappage de banque de données est requis pour chaque banque de données hébergeant des machines virtuelles à protéger.

- Les sections avec l'icône d'avertissement ( ) exigent que vous fournissiez des informations de cartographie.
- La section marquée avec l'icône de coche ( ) ont été mappés ou ont des mappages par défaut. Passez-les en revue pour vous assurer que la configuration actuelle répond à vos besoins.

Étapes pour accéder à cette page

1. À partir de la page **Plan de réplication**, passez à la section **Mappage des ressources**.
2. Consultez les informations sur la page **Cartographie des ressources** qui s'ouvre.



3. Pour ouvrir chaque catégorie de mappages requis, sélectionnez la flèche vers le bas (**v**) à côté de la section.

Cartographie des ressources de calcul

Étant donné qu'un site peut héberger plusieurs centres de données virtuels et plusieurs clusters vCenter, vous devez identifier le cluster vCenter sur lequel récupérer les machines virtuelles en cas de basculement.

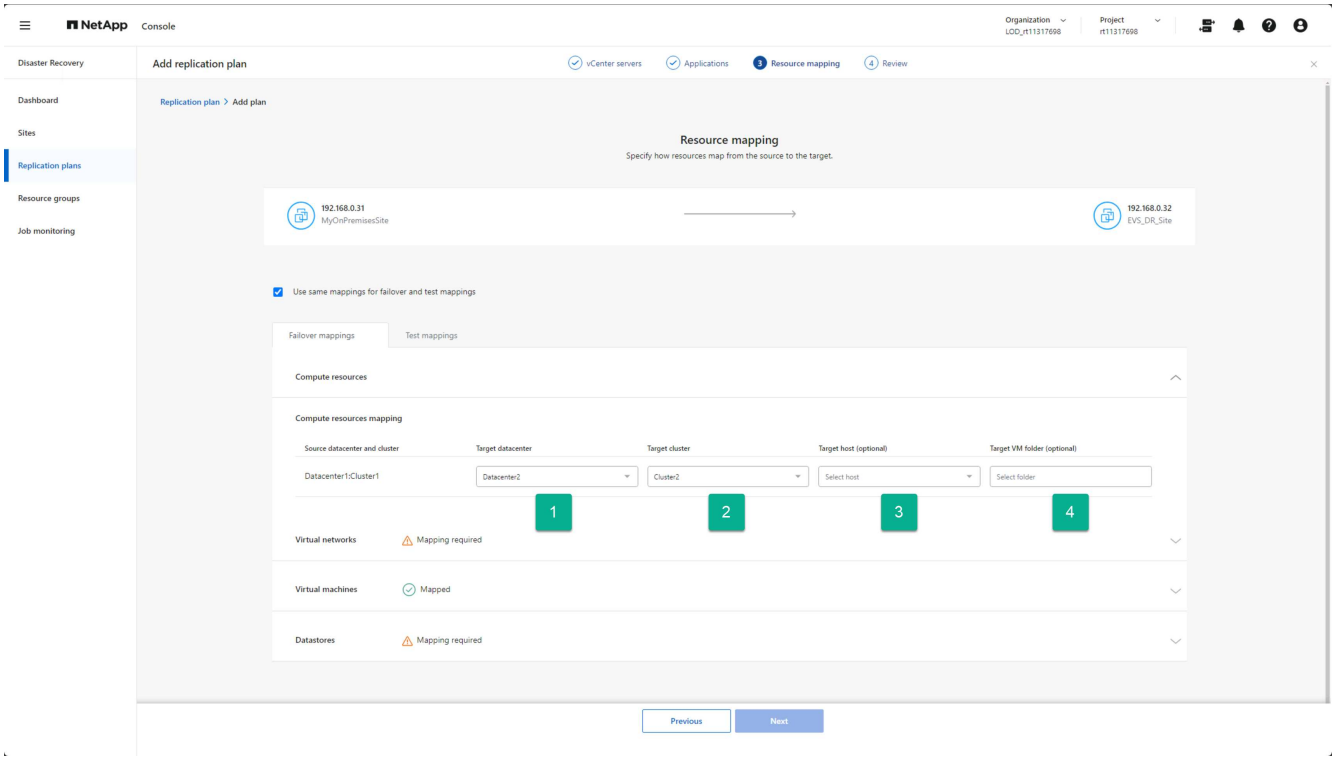
Étapes pour cartographier les ressources de calcul

1. Sélectionnez le centre de données virtuel dans la liste des centres de données situés sur le site DR.
2. Sélectionnez le cluster qui hébergera les banques de données et les machines virtuelles dans la liste des clusters au sein du centre de données virtuel sélectionné.
3. (Facultatif) Sélectionnez un hôte cible dans le cluster cible.

   Cette étape n'est pas requise car NetApp Disaster Recovery sélectionne le premier hôte ajouté au cluster dans vCenter. À ce stade, les machines virtuelles continuent de s'exécuter sur cet hôte ESXi ou VMware DRS déplace la machine virtuelle vers un autre hôte ESXi selon les besoins en fonction des règles DRS configurées.

4. (Facultatif) Indiquez le nom d'un dossier vCenter de niveau supérieur dans lequel placer les enregistrements de machines virtuelles.

   Ceci est pour vos besoins organisationnels et n'est pas obligatoire.



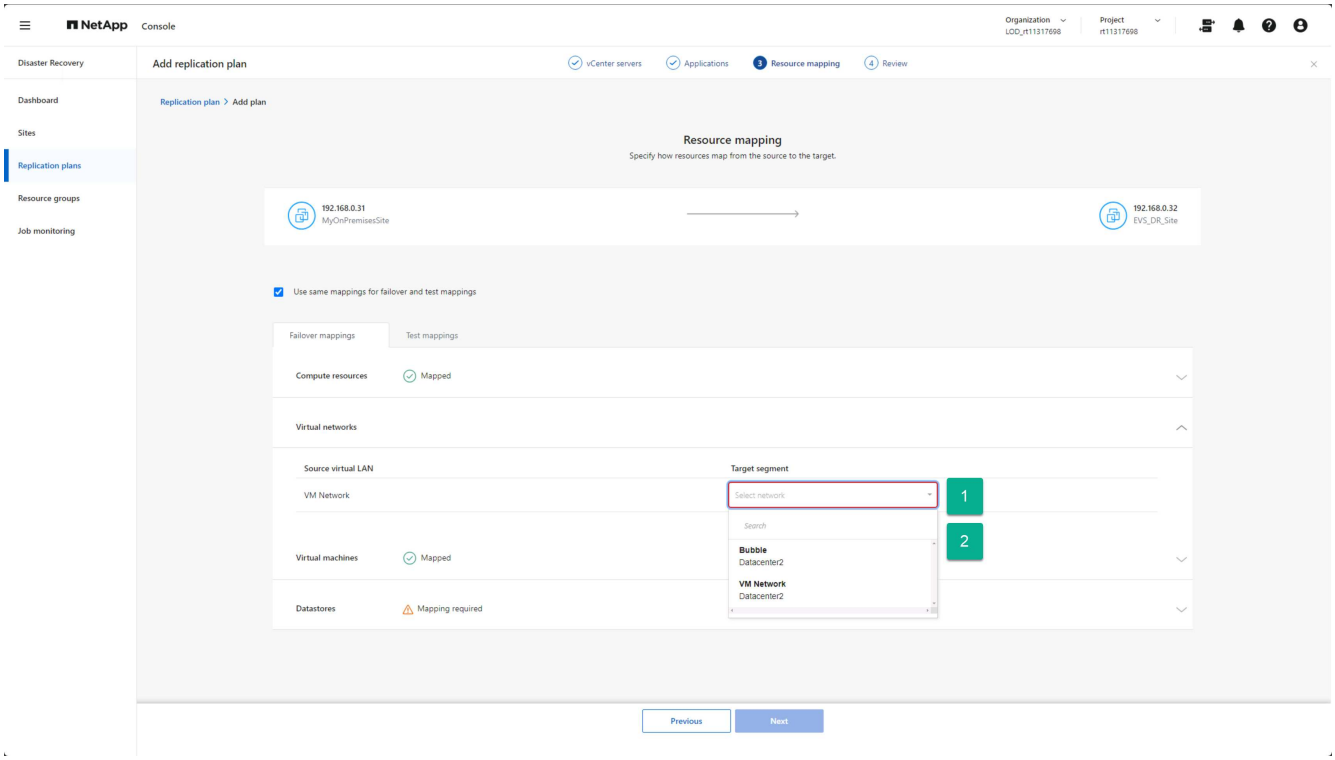
Cartographier les ressources du réseau virtuel

Chaque machine virtuelle peut avoir une ou plusieurs cartes réseau virtuelles connectées à des réseaux virtuels au sein de l'infrastructure réseau vCenter. Pour garantir que chaque machine virtuelle est correctement connectée aux réseaux souhaités lors du redémarrage sur le site DR, identifiez les réseaux virtuels du site DR auxquels connecter ces machines virtuelles. Pour ce faire, mappez chaque réseau virtuel du site local à un

réseau associé sur le site DR.

Sélectionnez le réseau virtuel de destination auquel mapper chaque réseau virtuel source

1. Sélectionnez le segment cible dans la liste déroulante.
2. Répétez l'étape précédente pour chaque réseau virtuel source répertorié.



Définir les options de reconfiguration de la machine virtuelle lors du basculement

Chaque machine virtuelle peut nécessiter des modifications pour fonctionner correctement sur le site DR vCenter. La section Machines virtuelles vous permet d'apporter les modifications nécessaires.

Par défaut, NetApp Disaster Recovery utilise les mêmes paramètres pour chaque machine virtuelle que ceux utilisés sur le site source sur site. Cela suppose que les machines virtuelles utiliseront la même adresse IP, le même processeur virtuel et la même configuration DRAM virtuelle.

Reconfiguration du réseau

Les types d'adresses IP pris en charge sont statiques et DHCP. Pour les adresses IP statiques, vous disposez des paramètres IP cible suivants :

- **Identique à la source** : Comme son nom l'indique, le service utilise la même adresse IP sur la machine virtuelle de destination que celle utilisée sur la machine virtuelle du site source. Cela nécessite que vous configuriez les réseaux virtuels qui ont été mappés à l'étape précédente pour les mêmes paramètres de sous-réseau.
- **Différent de la source** : Le service fournit un ensemble de champs d'adresse IP pour chaque machine virtuelle qui doit être configuré pour le sous-réseau approprié utilisé sur le réseau virtuel de destination, que vous avez mappé dans la section précédente. Pour chaque machine virtuelle, vous devez fournir une adresse IP, un masque de sous-réseau, un DNS et des valeurs de passerelle par défaut. Vous pouvez également utiliser les mêmes paramètres de masque de sous-réseau, DNS et passerelle pour toutes les machines virtuelles afin de simplifier le processus lorsque toutes les machines virtuelles se connectent au

même sous-réseau.

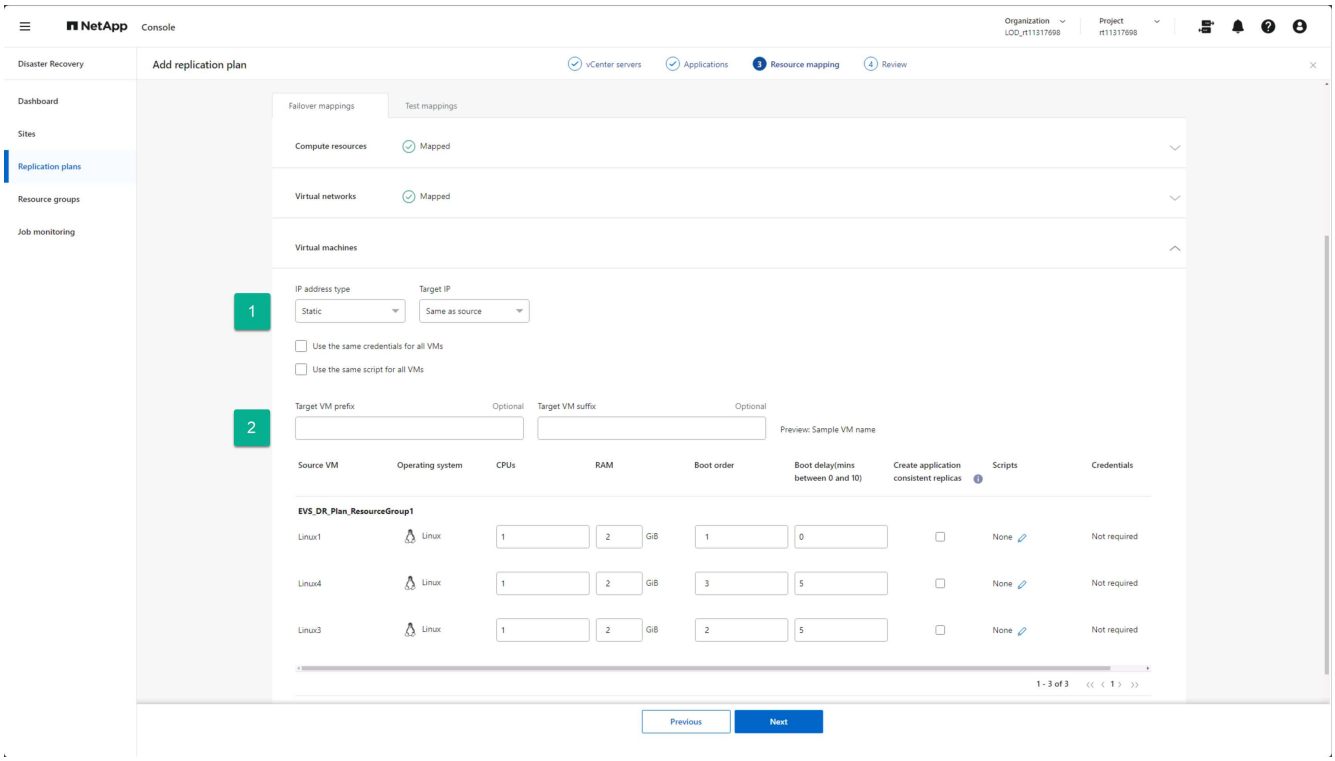
- **Mappage de sous-réseau** : cette option reconfigure l'adresse IP de chaque machine virtuelle en fonction de la configuration CIDR du réseau virtuel de destination. Pour utiliser cette fonctionnalité, assurez-vous que chaque réseau virtuel de vCenter dispose d'un paramètre CIDR défini au sein du service, tel que modifié dans les informations vCenter sur la page Sites.

Une fois les sous-réseaux configurés, le mappage de sous-réseaux utilise le même composant d'unité de l'adresse IP pour la configuration de la machine virtuelle source et de destination, mais remplace le composant de sous-réseau de l'adresse IP en fonction des informations CIDR fournies. Cette fonctionnalité nécessite également que les réseaux virtuels source et de destination aient la même classe d'adresse IP (la `/xx` composant du CIDR). Cela garantit qu'il y a suffisamment d'adresses IP disponibles sur le site de destination pour héberger toutes les machines virtuelles protégées.

Pour cette configuration EVS, nous supposons que les configurations IP source et de destination sont les mêmes et ne nécessitent aucune reconfiguration supplémentaire.

Apporter des modifications à la reconfiguration des paramètres réseau

1. Sélectionnez le type d'adressage IP à utiliser pour les machines virtuelles basculées.
2. (Facultatif) Fournissez un schéma de renommage de machine virtuelle pour les machines virtuelles redémarrées en fournissant une valeur de préfixe et de suffixe facultative.



Reconfiguration des ressources de calcul de la machine virtuelle

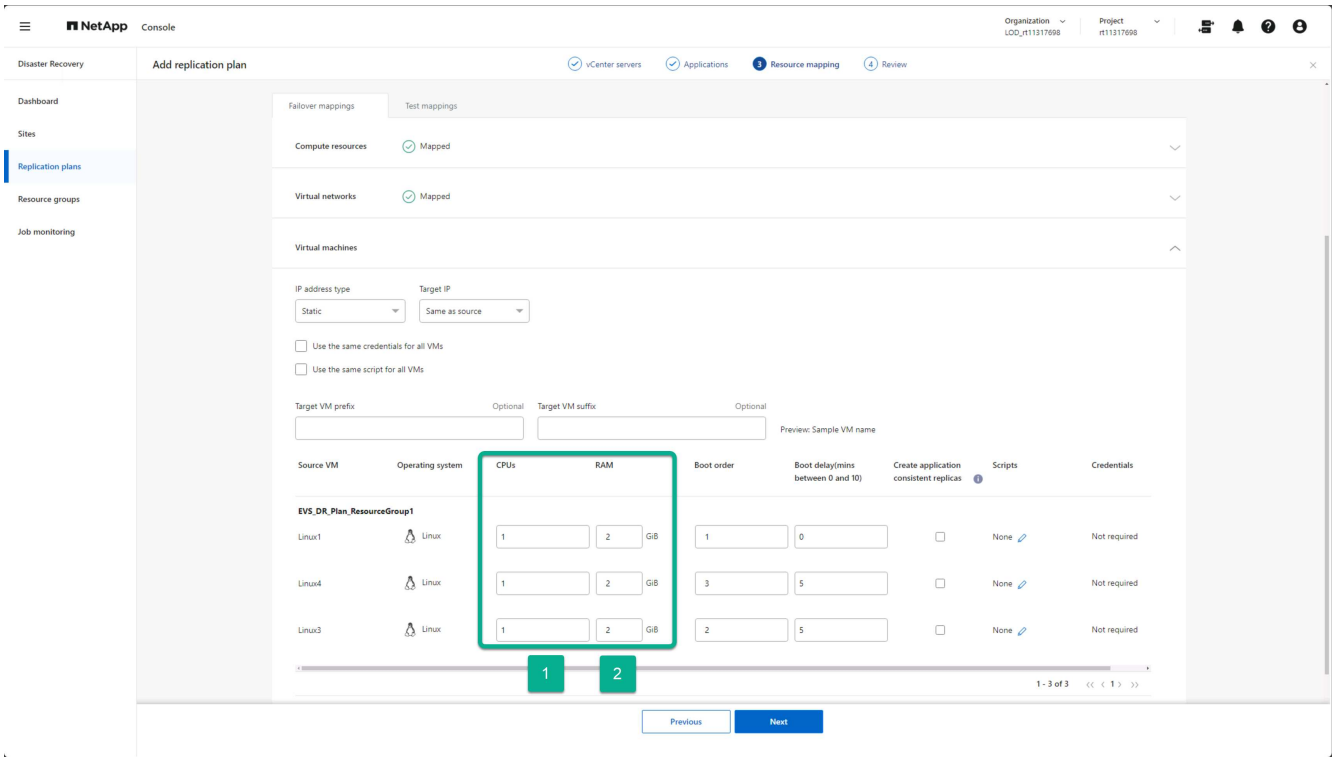
Il existe plusieurs options pour reconfigurer les ressources de calcul de la machine virtuelle. NetApp Disaster Recovery prend en charge la modification du nombre de processeurs virtuels, de la quantité de DRAM virtuelle et du nom de la machine virtuelle.

Spécifier les modifications de configuration de la machine virtuelle

1. (Facultatif) Modifiez le nombre de processeurs virtuels que chaque machine virtuelle doit utiliser. Cela peut être nécessaire si vos hôtes de cluster DR vCenter ne disposent pas d'autant de cœurs de processeur que

le cluster vCenter source.

2. (Facultatif) Modifiez la quantité de DRAM virtuelle que chaque machine virtuelle doit utiliser. Cela peut être nécessaire si vos hôtes de cluster DR vCenter ne disposent pas d'autant de DRAM physique que les hôtes de cluster vCenter source.

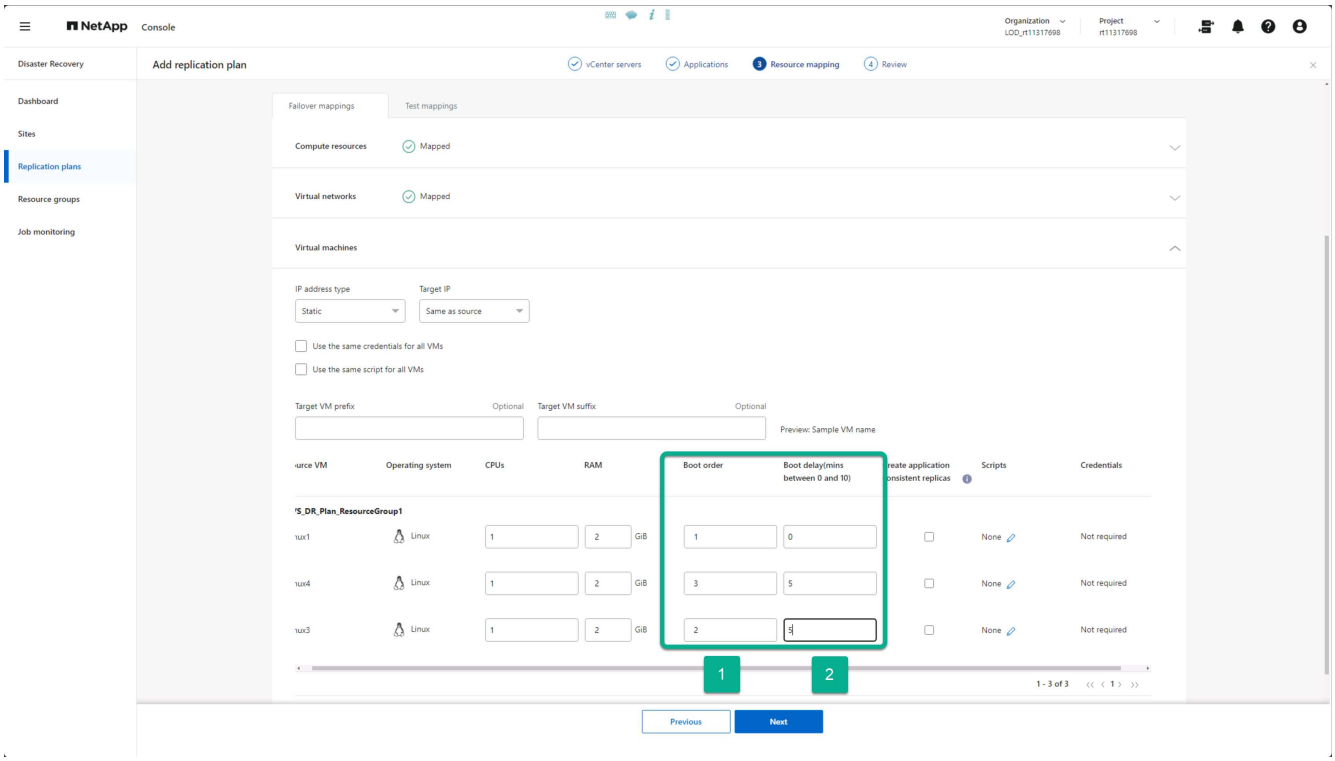


Ordre de démarrage

NetApp Disaster Recovery prend en charge un redémarrage ordonné des machines virtuelles en fonction d'un champ d'ordre de démarrage. Le champ Ordre de démarrage indique comment les machines virtuelles de chaque groupe de ressources démarrent. Les machines virtuelles avec la même valeur dans le champ Ordre de démarrage démarrent en parallèle.

Modifier les paramètres de l'ordre de démarrage

1. (Facultatif) Modifiez l'ordre dans lequel vous souhaitez que vos machines virtuelles soient redémarrées. Ce champ prend n'importe quelle valeur numérique. NetApp Disaster Recovery tente de redémarrer les machines virtuelles qui ont la même valeur numérique en parallèle.
2. (Facultatif) Fournissez un délai à utiliser entre chaque redémarrage de la machine virtuelle. Le temps est injecté après la fin du redémarrage de cette machine virtuelle et avant la ou les machines virtuelles avec le numéro d'ordre de démarrage supérieur suivant. Ce nombre est en minutes.



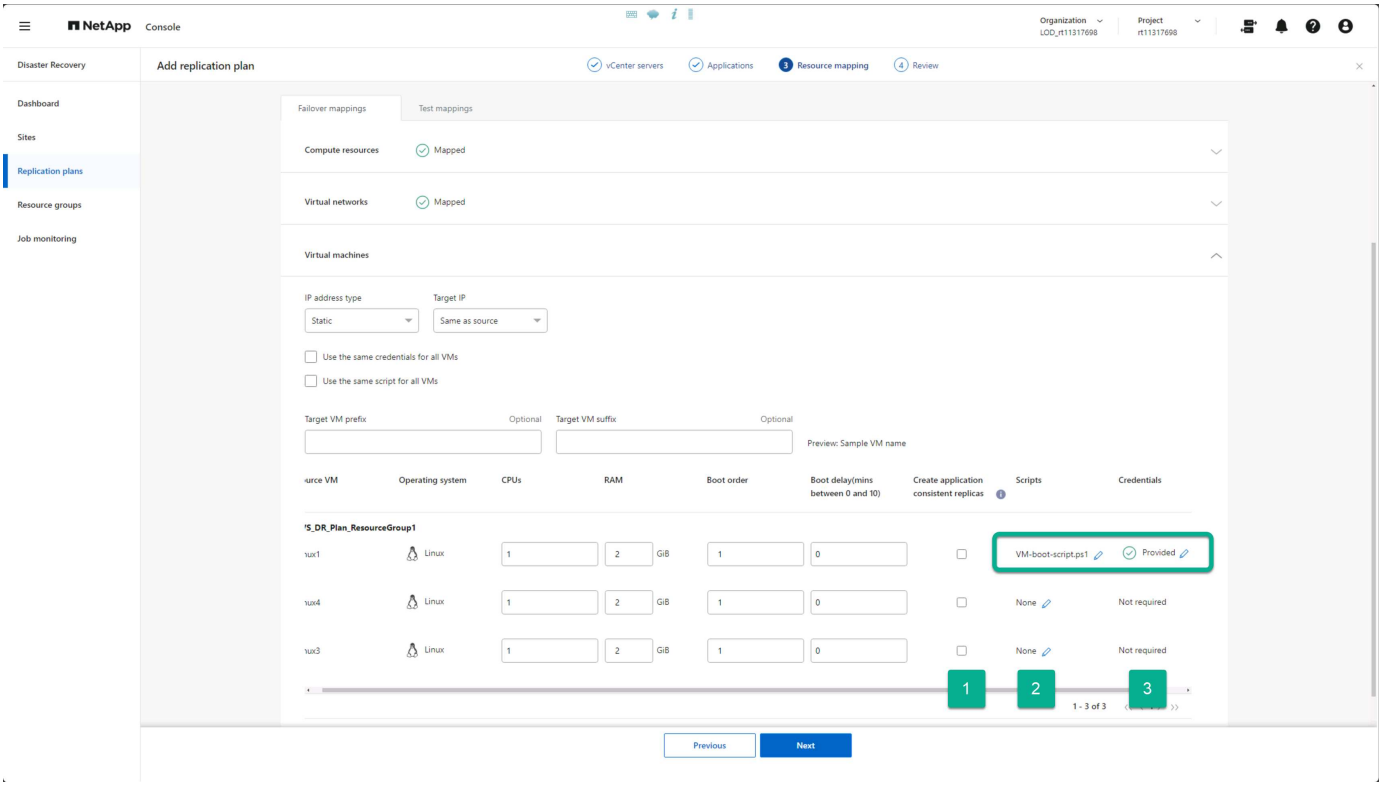
Opérations personnalisées du système d'exploitation invité

NetApp Disaster Recovery prend en charge l'exécution de certaines opérations du système d'exploitation invité pour chaque machine virtuelle :

- NetApp Disaster Recovery peut effectuer des sauvegardes cohérentes avec les applications des machines virtuelles exécutant des bases de données Oracle et des bases de données Microsoft SQL Server.
- NetApp Disaster Recovery peut exécuter des scripts personnalisés définis adaptés au système d'exploitation invité pour chaque machine virtuelle. L'exécution de tels scripts nécessite des informations d'identification utilisateur acceptables pour le système d'exploitation invité avec des privilèges suffisants pour exécuter les opérations répertoriées dans le script.

Modifier les opérations personnalisées du système d'exploitation invité de chaque machine virtuelle

1. (Facultatif) Cochez la case **Créer des répliques cohérentes avec les applications** si la machine virtuelle héberge une base de données Oracle ou SQL Server.
2. (Facultatif) Pour effectuer des actions personnalisées au sein du système d'exploitation invité dans le cadre du processus de démarrage, téléchargez un script pour toutes les machines virtuelles. Pour exécuter un seul script sur toutes les machines virtuelles, utilisez la case à cocher en surbrillance et remplissez les champs.
3. Certaines modifications de configuration nécessitent des informations d'identification utilisateur avec des autorisations adéquates pour effectuer les opérations. Fournir des informations d'identification dans les cas suivants :
    - Un script sera exécuté dans la VM par le système d'exploitation invité.
    - Un instantané cohérent avec l'application doit être effectué.



Cartographier les magasins de données

La dernière étape de la création d'un plan de réplication consiste à identifier comment ONTAP doit protéger les banques de données. Ces paramètres définissent l'objectif de point de récupération (RPO) des plans de réplication, le nombre de sauvegardes à conserver et l'emplacement où répliquer les volumes ONTAP d'hébergement de chaque banque de données vCenter.

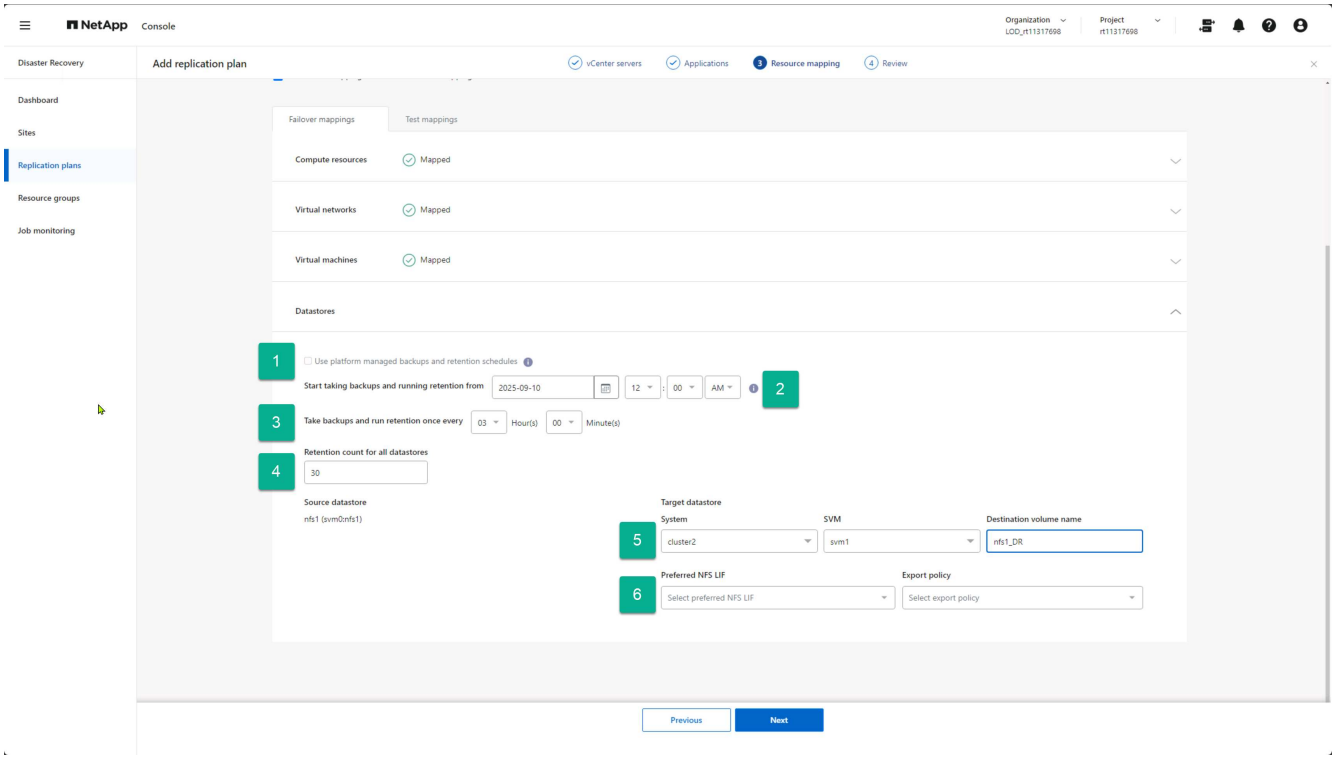
Par défaut, NetApp Disaster Recovery gère sa propre planification de réplication de snapshots. Toutefois, vous pouvez éventuellement spécifier que vous souhaitez utiliser la planification de stratégie de réplication SnapMirror existante pour la protection de la banque de données.

De plus, vous pouvez éventuellement personnaliser les LIF de données (interfaces logiques) et la politique d'exportation à utiliser. Si vous ne fournissez pas ces paramètres, NetApp Disaster Recovery utilise tous les LIF de données associés au protocole approprié (NFS, iSCSI ou FC) et utilise la stratégie d'exportation par défaut pour les volumes NFS.

Pour configurer le mappage de la banque de données (volume)

1. (Facultatif) Décidez si vous souhaitez utiliser une planification de réplication ONTAP SnapMirror existante ou laisser NetApp Disaster Recovery gérer la protection de vos machines virtuelles (par défaut).
2. Fournissez un point de départ pour le moment où le service doit commencer à effectuer des sauvegardes.
3. Spécifiez la fréquence à laquelle le service doit effectuer une sauvegarde et la répliquer vers le cluster Amazon FSx for NetApp ONTAP de destination DR.
4. Spécifiez le nombre de sauvegardes historiques à conserver. Le service conserve le même nombre de sauvegardes sur le cluster de stockage source et de destination.
5. (Facultatif) Sélectionnez une interface logique par défaut (LIF de données) pour chaque volume. Si aucun n'est sélectionné, tous les LIF de données dans la SVM de destination qui prennent en charge le protocole d'accès au volume sont configurés.
6. (Facultatif) Sélectionnez une politique d'exportation pour tous les volumes NFS. Si cette option n'est pas

sélectionnée, la politique d'exportation par défaut est utilisée



Continuer avec"Assistant de création de plan de réplication Étape 4" .

Créer un plan de réplication : Étape 4 : Vérifier les paramètres dans NetApp Disaster Recovery

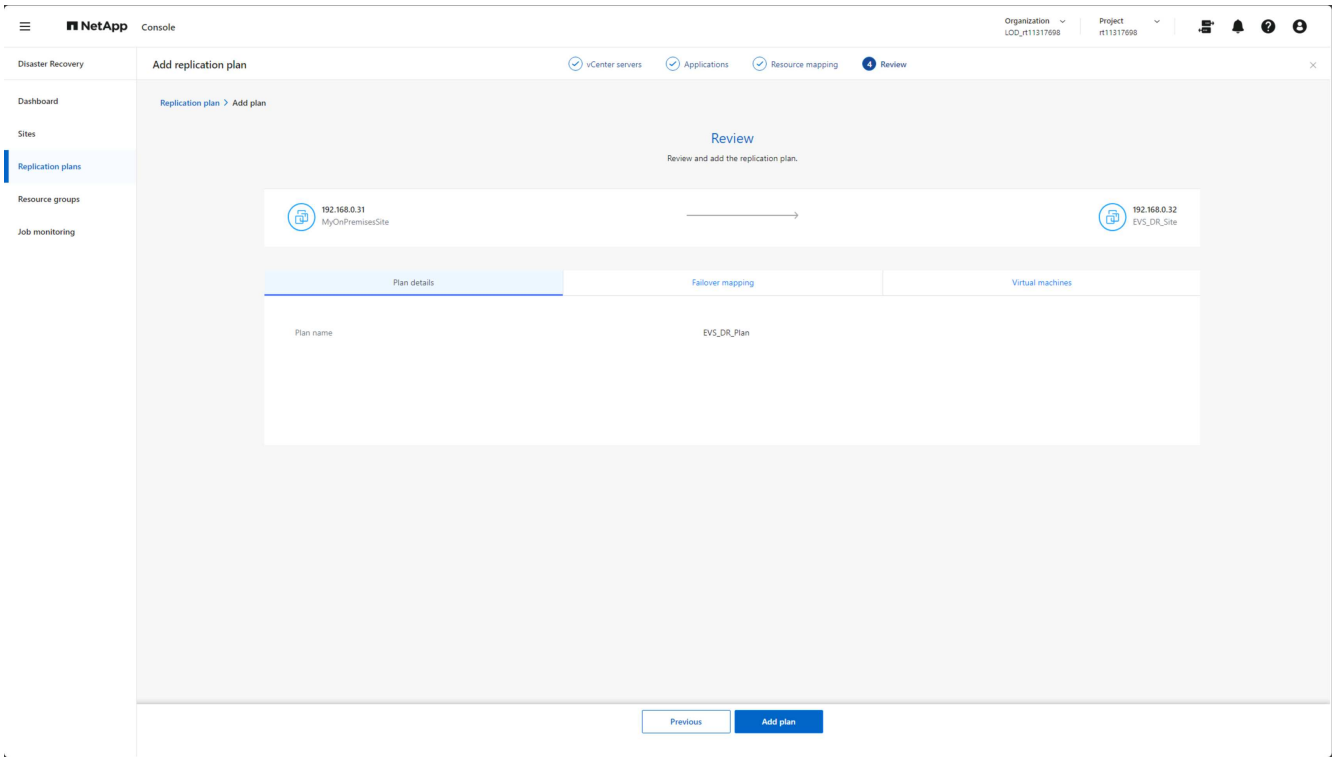
Après avoir ajouté les informations du plan de réplication dans NetApp Disaster Recovery, vérifiez que les informations que vous avez saisies sont correctes.

Étapes

1. Sélectionnez **Enregistrer** pour vérifier vos paramètres avant d'activer le plan de réplication.

   Vous pouvez sélectionner chaque onglet pour consulter les paramètres et apporter des modifications sur n'importe quel onglet en sélectionnant l'icône en forme de crayon.

   Examen des paramètres du plan de réplication



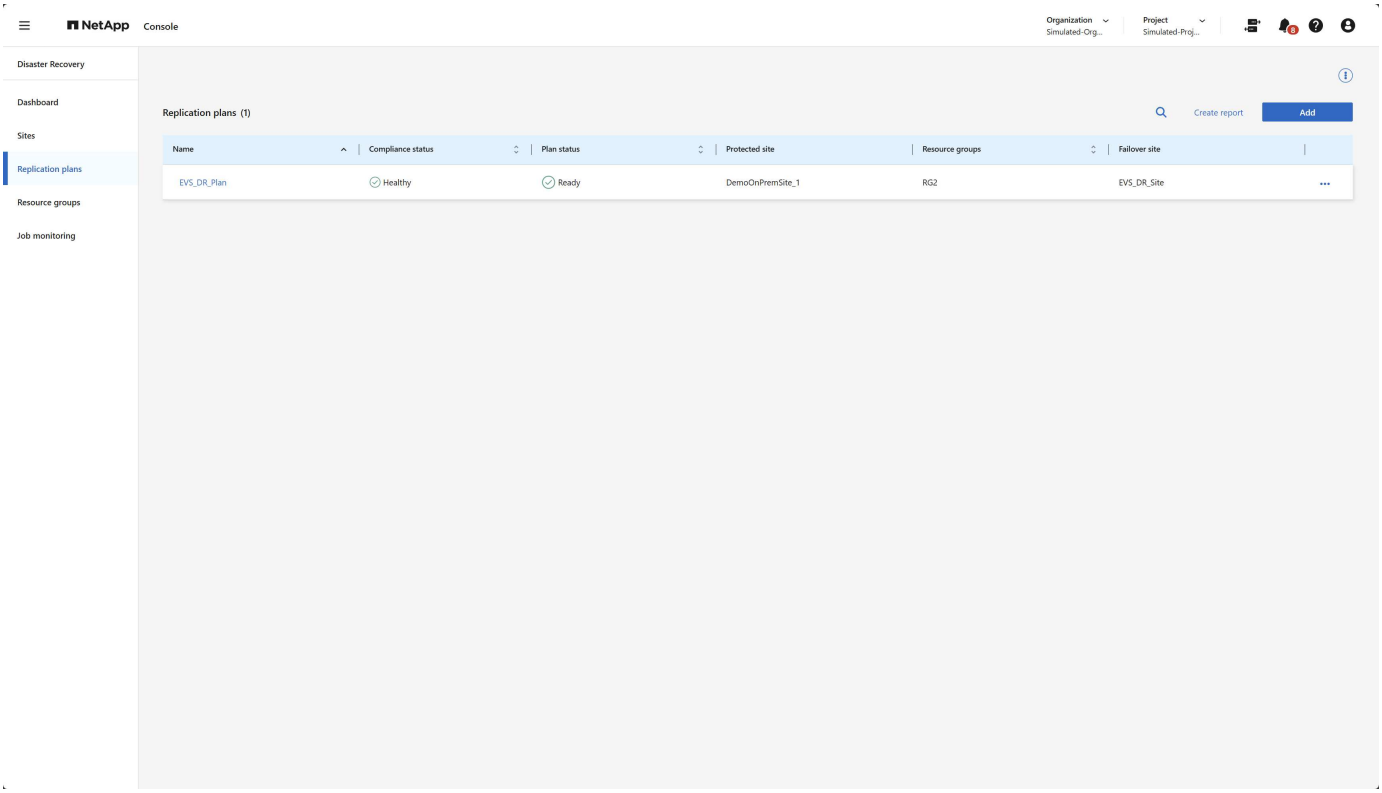
2. Lorsque vous êtes satisfait et que tous les paramètres sont corrects, sélectionnez **Ajouter un plan** en bas de l'écran.

Continuer avec"Vérifier le plan de réplication" .

Vérifiez que tout fonctionne dans NetApp Disaster Recovery

Après avoir ajouté le plan de réplication dans NetApp Disaster Recovery, vous revenez à la page Plans de réplication où vous pouvez afficher vos plans de réplication et leur état. Vous devez vérifier que le plan de réplication est dans l'état **Sain**. Si ce n'est pas le cas, vous devez vérifier l'état du plan de réplication et corriger les problèmes éventuels avant de continuer.

Figure : Page des plans de réplication



NetApp Disaster Recovery effectue une série de tests pour vérifier que tous les composants (cluster ONTAP , clusters vCenter et machines virtuelles) sont accessibles et dans l'état approprié pour que le service protège les machines virtuelles. Il s'agit d'un contrôle de conformité, qui est effectué régulièrement.

Depuis la page Plans de réplication, vous pouvez voir les informations suivantes :

- Statut du dernier contrôle de conformité
- L'état de réplication du plan de réplication
- Le nom du site protégé (source)
- La liste des groupes de ressources protégés par le plan de réplication
- Le nom du site de basculement (destination)

Exécuter des opérations de plan de réplication avec NetApp Disaster Recovery

Utilisez NetApp Disaster Recovery avec Amazon EVS et Amazon FSx for NetApp ONTAP pour effectuer les opérations suivantes : basculement, test de basculement, actualisation des ressources, migration, prise d'un instantané maintenant, désactivation/activation du plan de réplication, nettoyage des anciens instantanés, rapprochement des instantanés, suppression du plan de réplication et modification des planifications.

Basculement

L'opération principale que vous devrez peut-être effectuer est celle que vous espérez ne jamais voir se produire : basculer vers le centre de données DR (destination) en cas de panne catastrophique sur le site de production sur site.

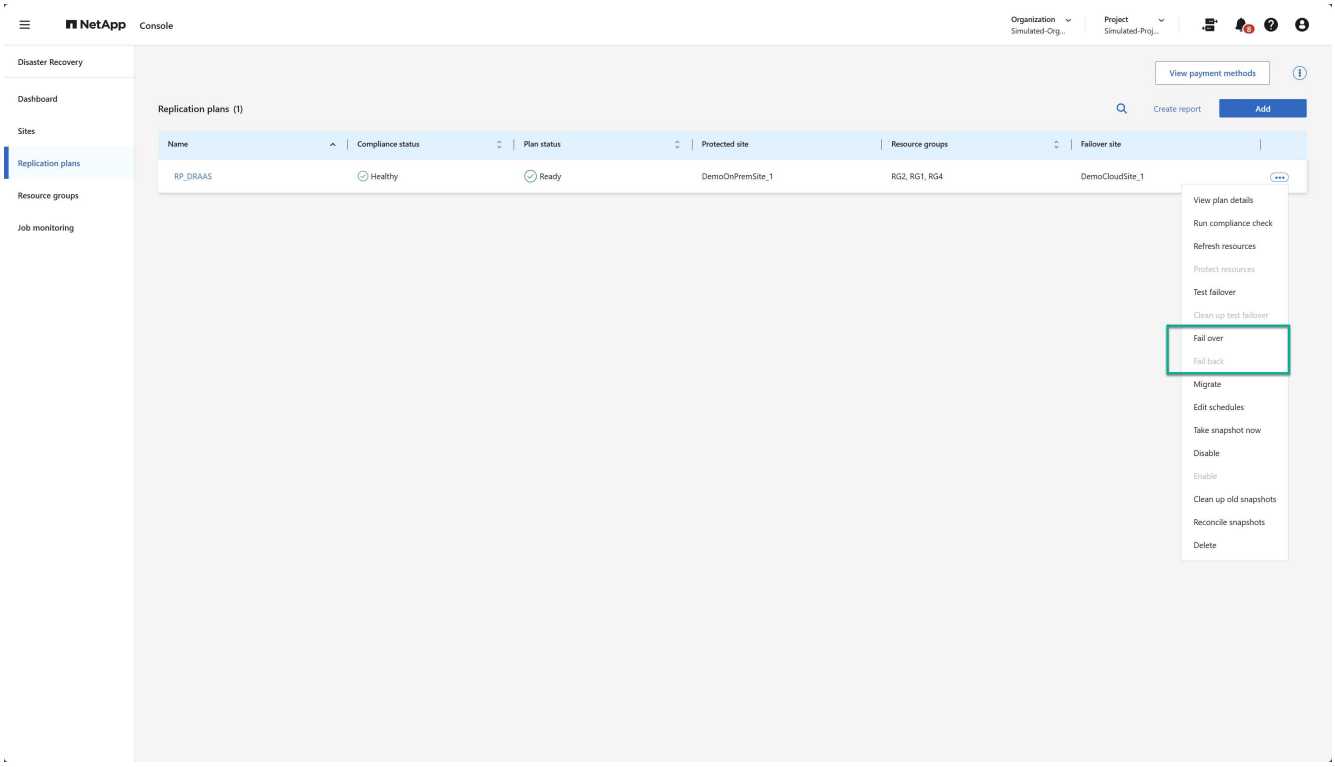
Le basculement est un processus lancé manuellement.

Étapes pour accéder à l'opération de basculement

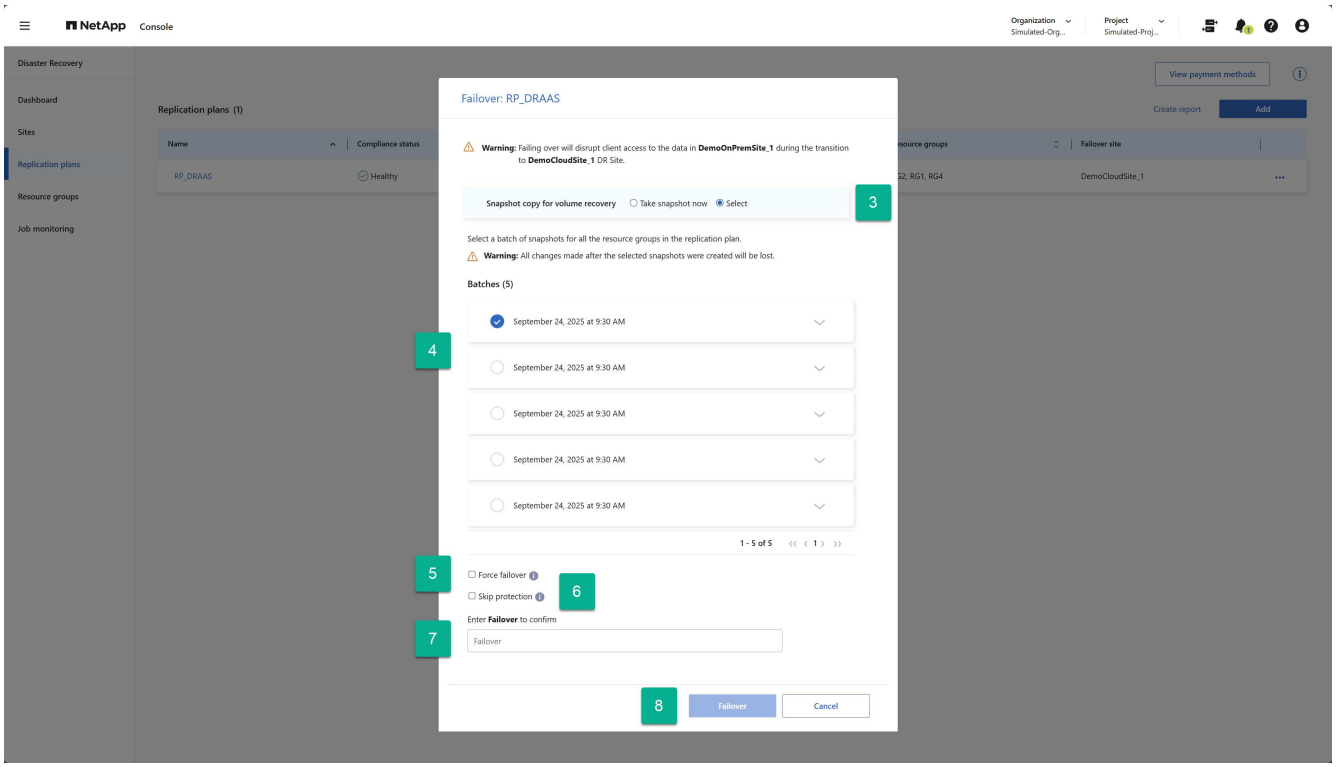
1. Dans la barre de navigation de gauche de la NetApp Console , sélectionnez **Protection** > **Reprise après sinistre**.
2. Dans le menu NetApp Disaster Recovery , sélectionnez **Plans de réplication**.

Étapes pour effectuer un basculement

1. Depuis la page Plans de réplication, sélectionnez l'option Actions du plan de réplication ••• .
2. Sélectionnez **Fail over**.



3. Si le site de production (protégé) n'est pas accessible, sélectionnez un instantané précédemment créé comme image de récupération. Pour ce faire, sélectionnez **Sélectionner**.
4. Sélectionnez la sauvegarde à utiliser pour la récupération.
5. (Facultatif) Sélectionnez si vous souhaitez que NetApp Disaster Recovery force le processus de basculement quel que soit l'état du plan de réplication. Cela ne devrait être fait qu'en dernier recours.
6. (Facultatif) Sélectionnez si vous souhaitez que NetApp Disaster Recovery crée automatiquement une relation de protection inverse une fois le site de production récupéré.
7. Tapez le mot « Failover » pour vérifier que vous souhaitez continuer.
8. Sélectionnez **Failover**.



Test de basculement

Un basculement de test est similaire à un basculement, à l'exception de deux différences.

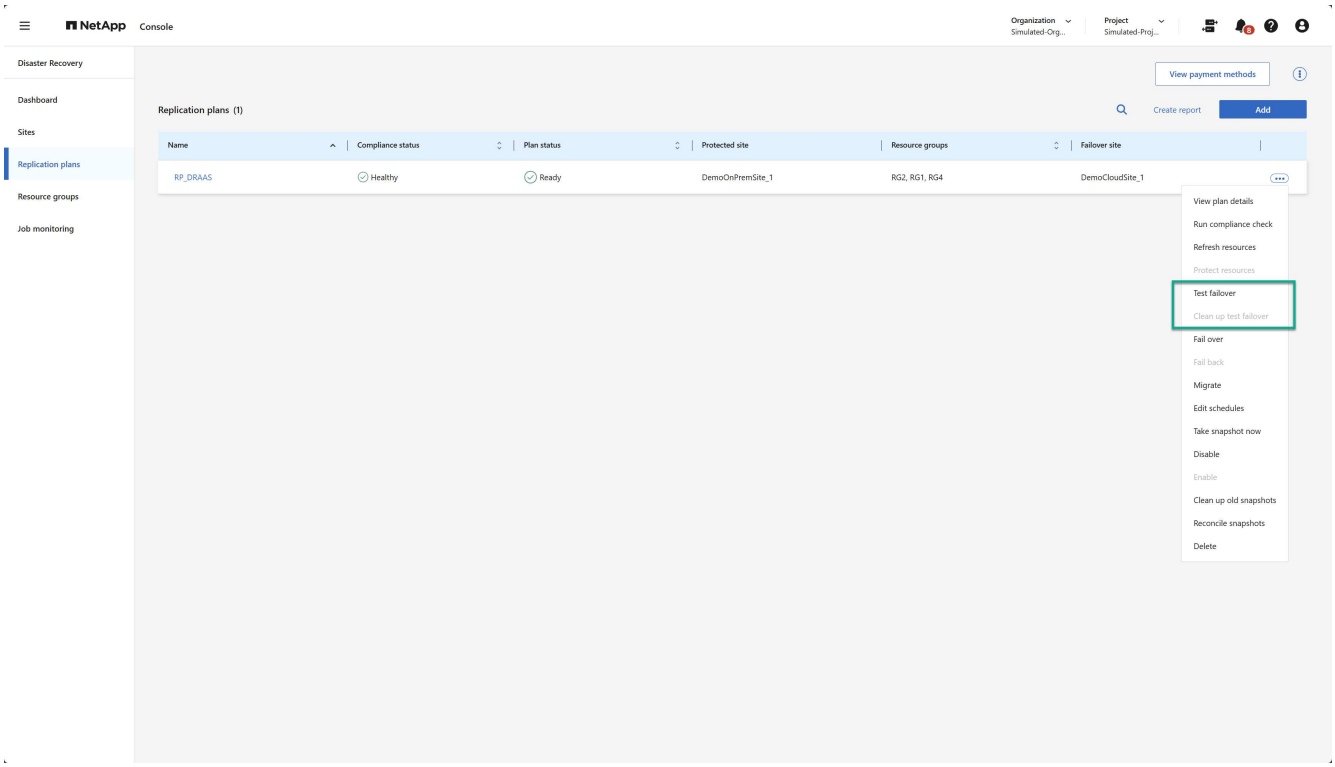
- Le site de production est toujours actif et toutes les machines virtuelles fonctionnent toujours comme prévu.
- La protection NetApp Disaster Recovery des machines virtuelles de production se poursuit.

Ceci est réalisé en utilisant des volumes ONTAP FlexClone natifs sur le site de destination. Pour en savoir plus sur le basculement des tests, consultez"Basculer des applications vers un site distant | Documentation NetApp" .

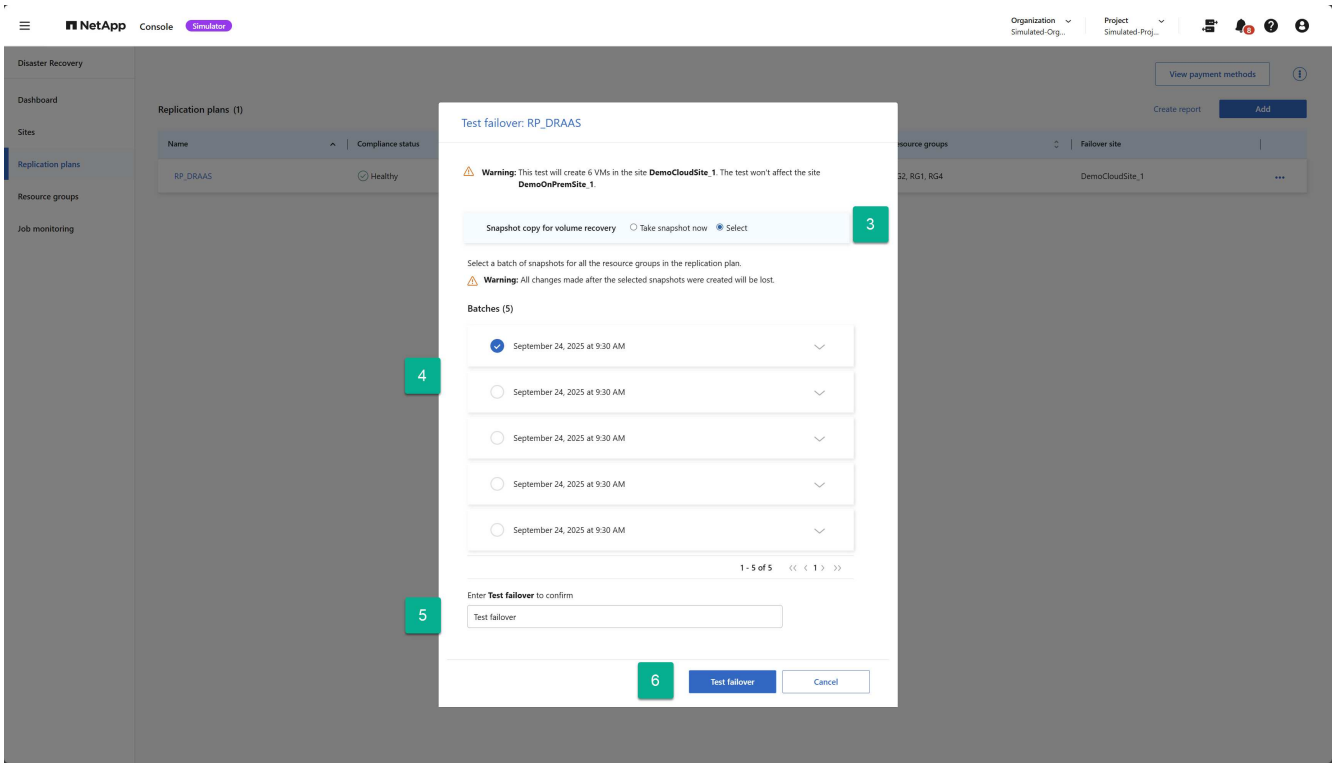
Les étapes d'exécution d'un basculement de test sont identiques à celles utilisées pour exécuter un basculement réel, sauf que vous utilisez l'opération de basculement de test dans le menu contextuel du plan de réplication.

Étapes

1. Sélectionnez l'option Actions du plan de réplication ••• .
2. Sélectionnez **Tester le basculement** dans le menu.



3. Décidez si vous souhaitez obtenir le dernier état de l'environnement de production (Prendre un instantané maintenant) ou utiliser une sauvegarde de plan de réplication précédemment créée (Sélectionner)
4. Si vous avez choisi une sauvegarde créée précédemment, sélectionnez la sauvegarde à utiliser pour la récupération.
5. Tapez le mot « Test de basculement » pour vérifier que vous souhaitez continuer.
6. Sélectionnez **Tester le basculement**.

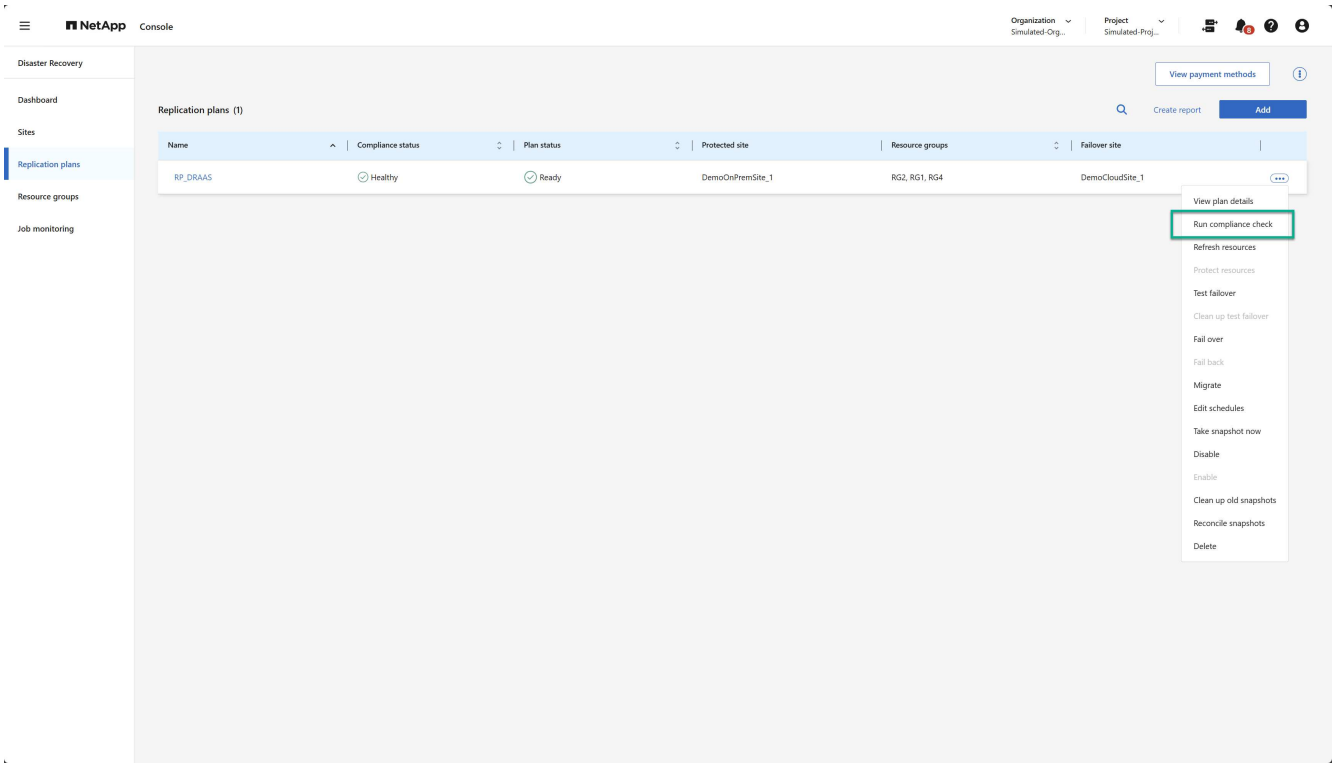


Exécuter un contrôle de conformité

Les contrôles de conformité sont exécutés toutes les trois heures, par défaut. À tout moment, vous pouvez souhaiter exécuter manuellement une vérification de conformité.

Étapes

1. Sélectionnez l'option *Actions* ••• à côté du plan de réplication.
2. Sélectionnez l'option **Exécuter la vérification de conformité** dans le menu Actions du plan de réplication :



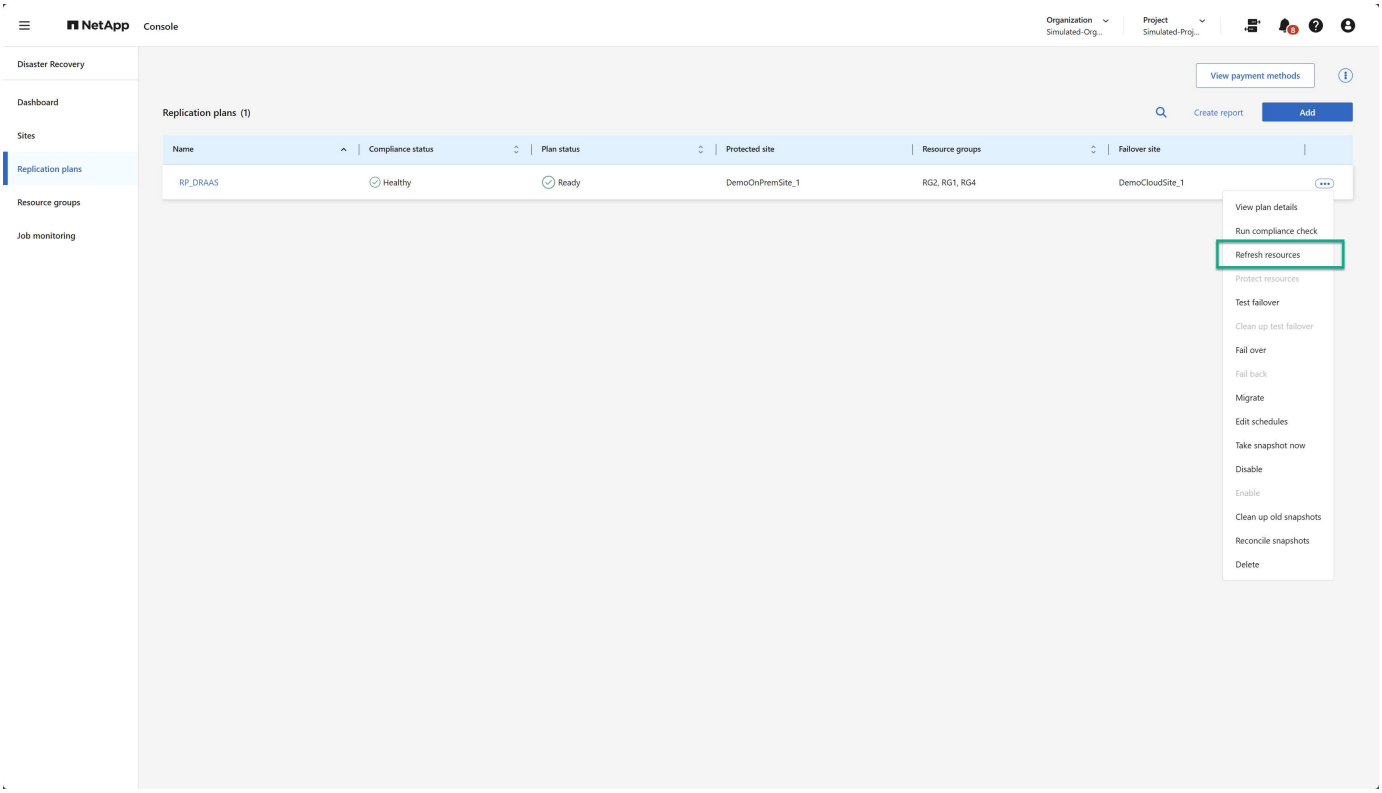
3. Pour modifier la fréquence à laquelle NetApp Disaster Recovery exécute automatiquement les contrôles de conformité, sélectionnez l'option **Modifier les planifications** dans le menu Actions du plan de réplication.

Actualiser les ressources

Chaque fois que vous apportez des modifications à votre infrastructure virtuelle (par exemple, l'ajout ou la suppression de machines virtuelles, l'ajout ou la suppression de banques de données ou le déplacement de machines virtuelles entre des banques de données), vous devez effectuer une actualisation des clusters vCenter concernés dans le service NetApp Disaster Recovery . Le service effectue cette opération automatiquement une fois toutes les 24 heures par défaut, mais une actualisation manuelle garantit que les dernières informations sur l'infrastructure virtuelle sont disponibles et prises en compte pour la protection DR.

Il existe deux cas où une actualisation est nécessaire :

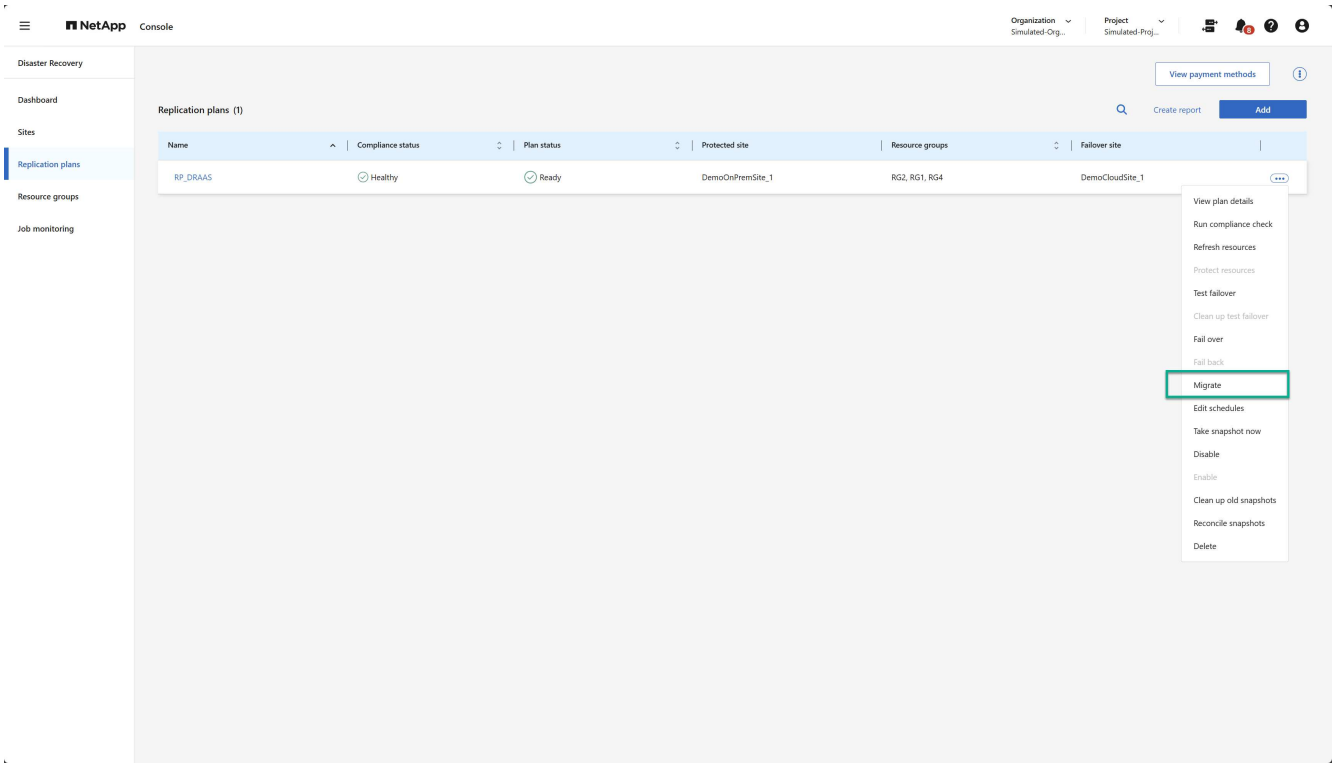
- Actualisation de vCenter : effectuez une actualisation de vCenter à chaque fois que des machines virtuelles sont ajoutées, supprimées ou déplacées hors d'un cluster vCenter :
- Actualisation du plan de réplication : effectuez une actualisation du plan de réplication chaque fois qu'une machine virtuelle est déplacée entre des banques de données dans le même cluster vCenter source.



Émigrer

Bien que NetApp Disaster Recovery soit principalement utilisé pour les cas d'utilisation de reprise après sinistre, il peut également permettre des déplacements ponctuels d'un ensemble de machines virtuelles du site source vers le site de destination. Cela pourrait être destiné à un projet de migration concertée vers le cloud ou pourrait être utilisé pour éviter des catastrophes, telles que des intempéries, des conflits politiques ou d'autres événements catastrophiques temporaires potentiels.

1. Sélectionnez l'option *Actions* ••• à côté du plan de réplication.
2. Pour déplacer les machines virtuelles d'un plan de réplication vers le cluster Amazon EVS de destination, sélectionnez **Migrer** dans le menu Actions du plan de réplication :

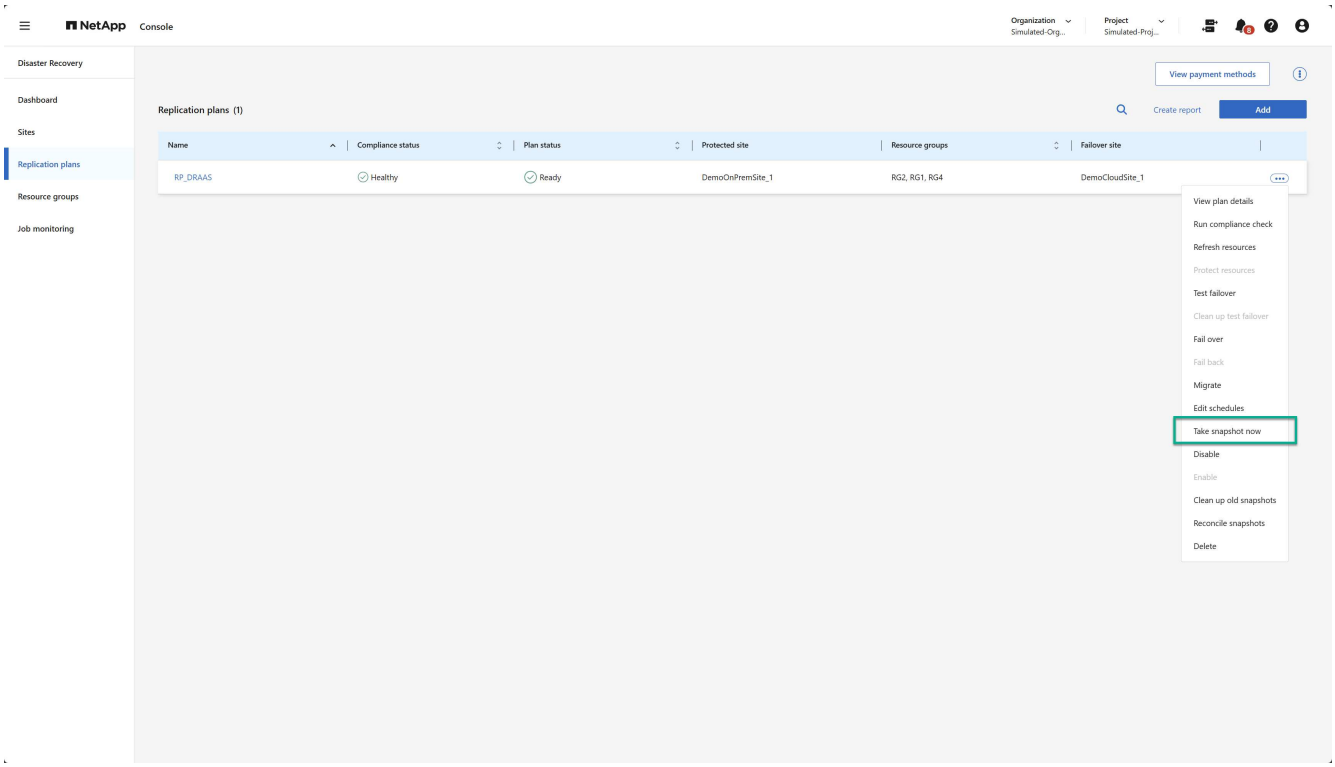


3. Saisissez les informations dans la boîte de dialogue Migrer.

Prenez un instantané maintenant

À tout moment, vous pouvez prendre un instantané immédiat du plan de réplication. Cet instantané est inclus dans les considérations de NetApp Disaster Recovery définies par le nombre de rétentions d'instantanés du plan de réplication.

1. Sélectionnez l'option *Actions* ••• à côté du plan de réplication.
2. Pour prendre un instantané immédiat des ressources du plan de réplication, sélectionnez **Prendre un instantané maintenant** dans le menu Actions du plan de réplication :

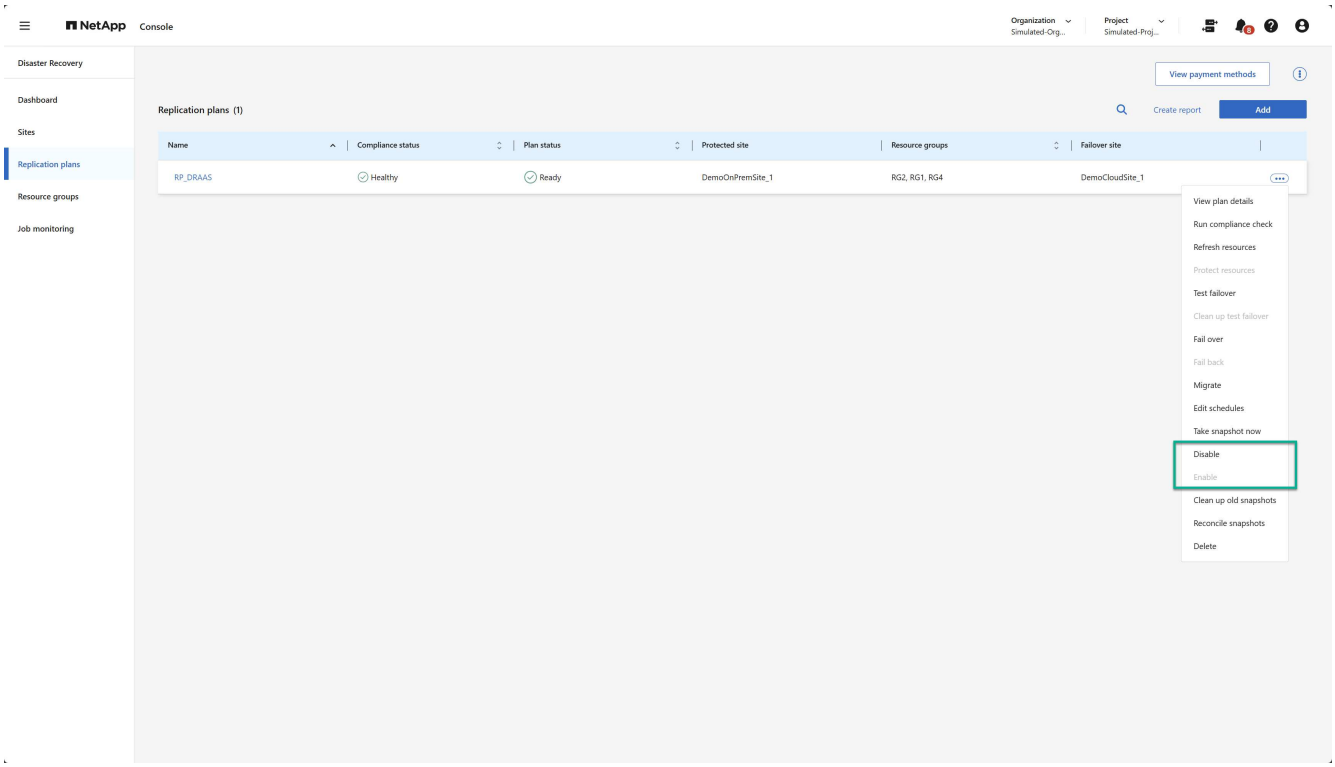


Désactiver ou activer le plan de réplication

Vous devrez peut-être arrêter temporairement le plan de réplication pour effectuer une opération ou une maintenance susceptible d'avoir un impact sur le processus de réplication. Le service fournit une méthode pour arrêter et démarrer la réplication.

1. Pour arrêter temporairement la réplication, sélectionnez **Désactiver** dans le menu Actions du plan de réplication.
2. Pour redémarrer la réplication, sélectionnez **Activer** dans le menu Actions du plan de réplication.

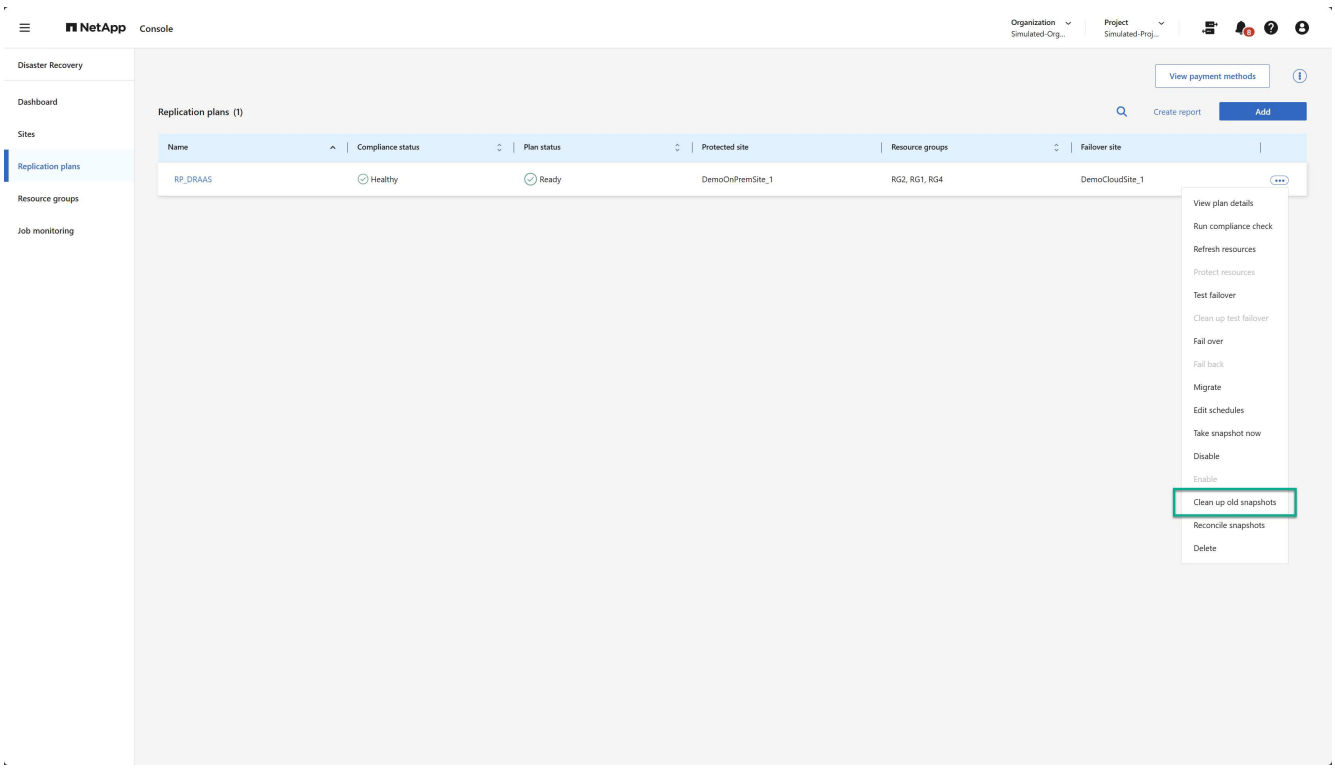
   Lorsque le plan de réplication est actif, la commande **Activer** est grisée. Lorsque le plan de réplication est désactivé, la commande **Désactiver** est grisée.



Nettoyer les anciens instantanés

Vous souhaiterez peut-être nettoyer les anciens instantanés qui ont été conservés sur les sites source et de destination. Cela peut se produire si le nombre de rétentions d'instantanés du plan de réplication est modifié.

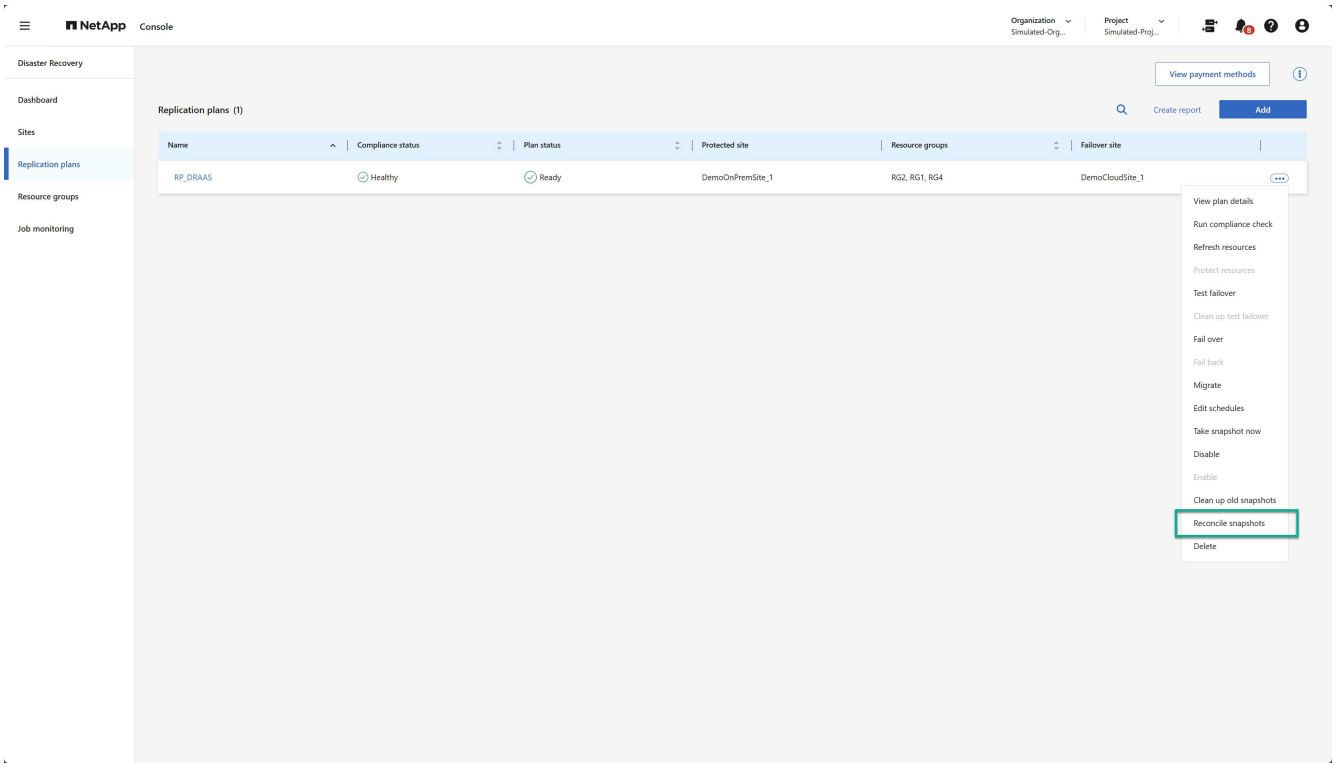
1. Sélectionnez l'option *Actions* ••• à côté du plan de réplication.
2. Pour supprimer manuellement ces anciens snapshots, sélectionnez **Nettoyer les anciens snapshots** dans le menu Actions du plan de réplication.



Réconcilier les instantanés

Étant donné que le service orchestre les snapshots de volume ONTAP , il est possible pour un administrateur de stockage ONTAP de supprimer directement les snapshots à l'aide d' ONTAP System Manager, de l'interface de ligne de commande ONTAP ou des API REST ONTAP à l'insu du service. Le service supprime automatiquement tous les snapshots sur la source qui ne se trouvent pas sur le cluster de destination toutes les 24 heures. Cependant, vous pouvez effectuer cette opération à la demande. Cette fonctionnalité vous permet de garantir que les instantanés sont cohérents sur tous les sites.

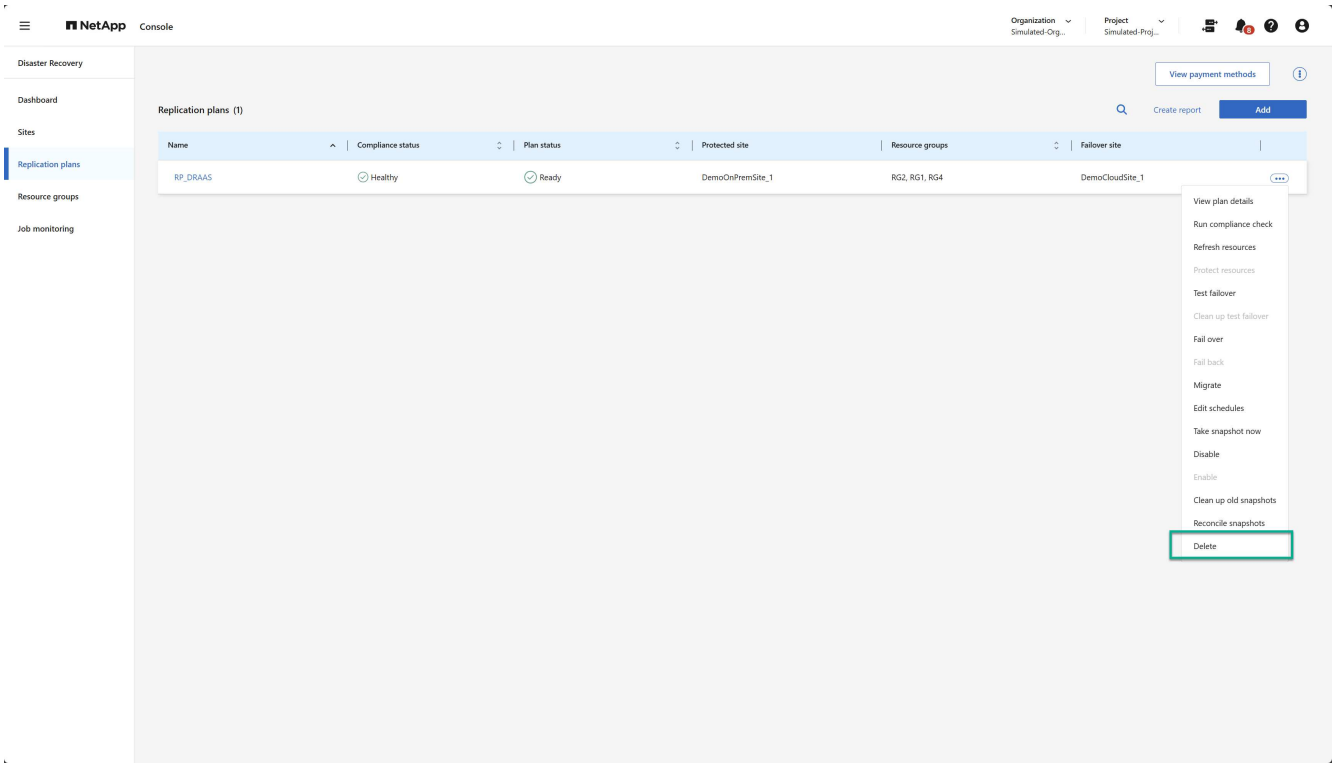
1. Sélectionnez l'option *Actions* ••• à côté du plan de réplication.
2. Pour supprimer les snapshots du cluster source qui n'existent pas sur le cluster de destination, sélectionnez **Réconcilier les snapshots** dans le menu Actions du plan de réplication.



Supprimer le plan de réplication

Si le plan de réplication n'est plus nécessaire, vous pouvez le supprimer.

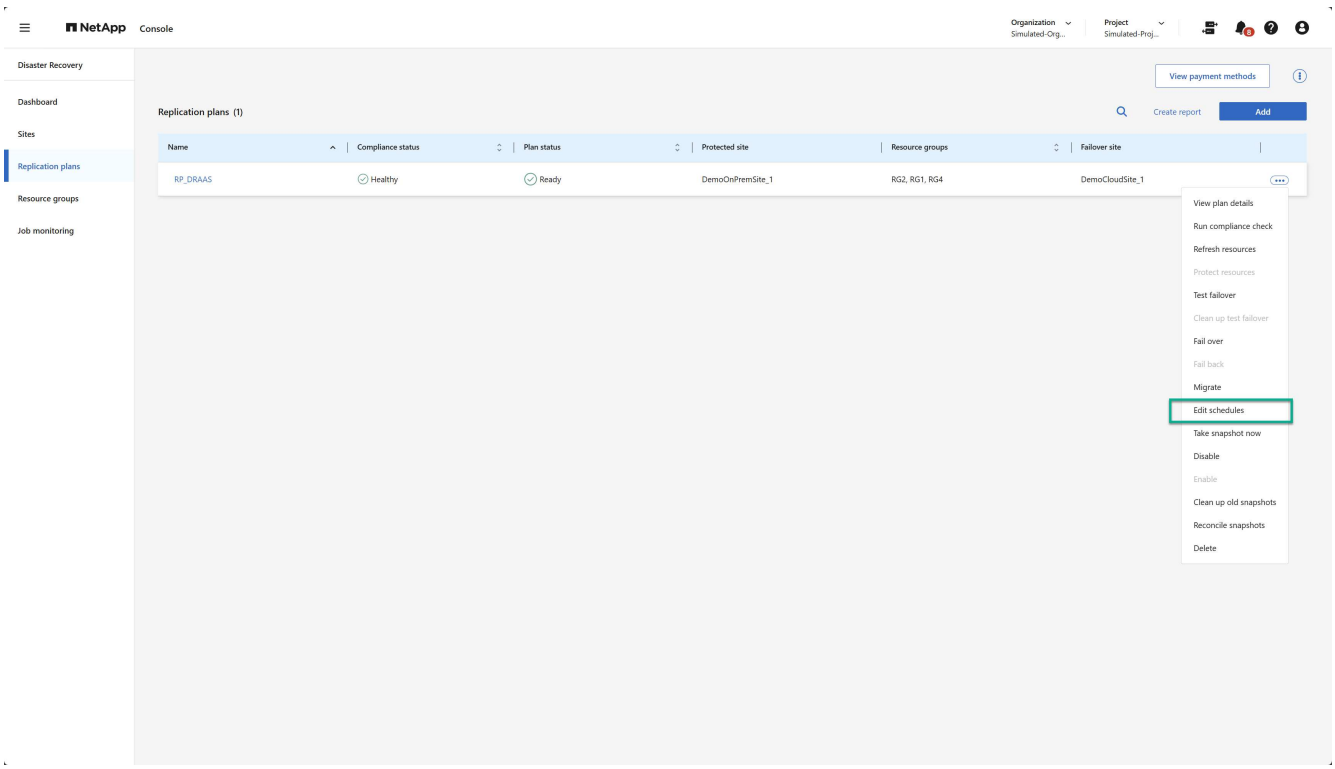
1. Sélectionnez l'option *Actions* ••• à côté du plan de réplication.
2. Pour supprimer le plan de réplication, sélectionnez **Supprimer** dans le menu contextuel du plan de réplication.



Modifier les horaires

Deux opérations sont effectuées automatiquement selon un calendrier régulier : les tests de basculement et les contrôles de conformité.

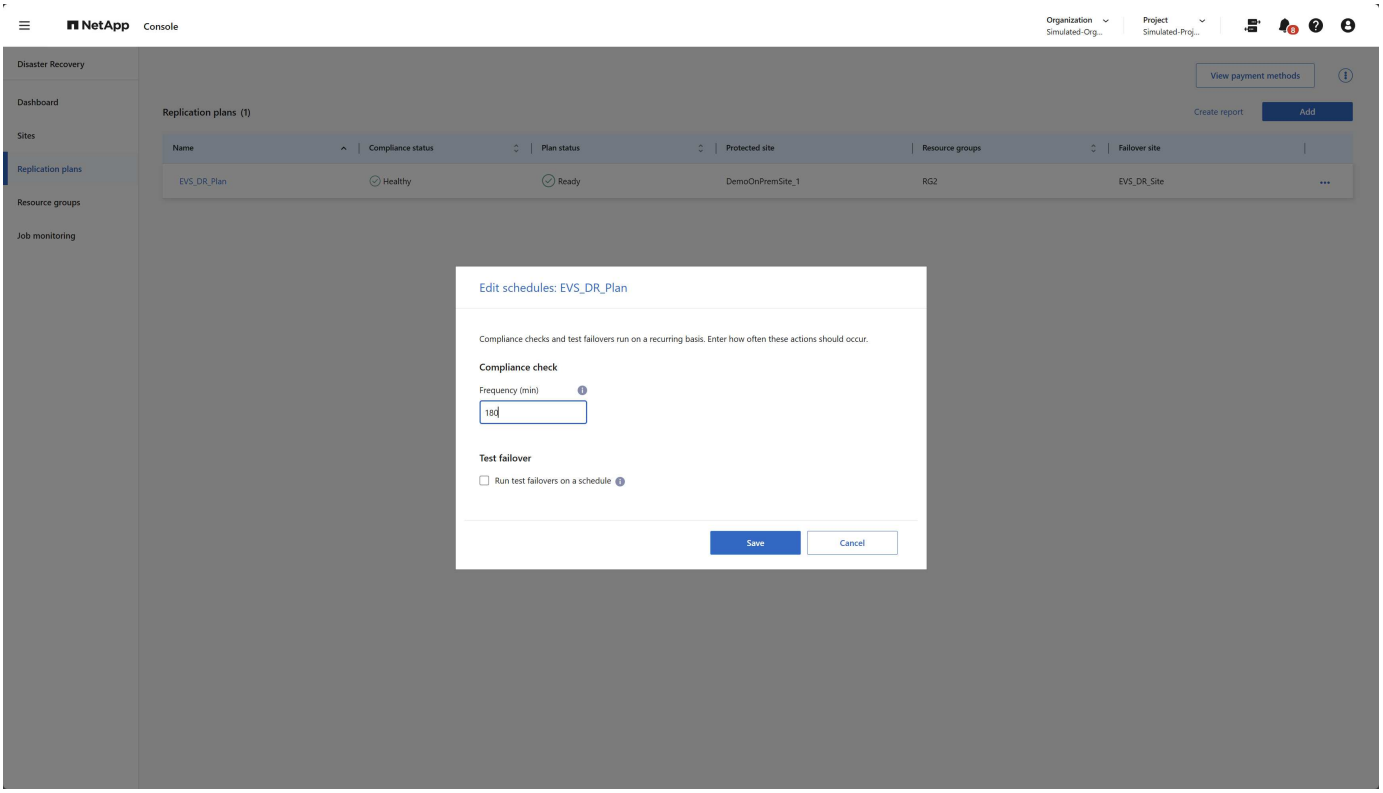
1. Sélectionnez l'option *Actions* ••• à côté du plan de réplication.
2. Pour modifier ces planifications pour l'une de ces deux opérations, sélectionnez **Modifier les planifications** pour le plan de réplication.



Modifier l'intervalle de vérification de conformité

Par défaut, les contrôles de conformité sont effectués toutes les trois heures. Vous pouvez modifier cet intervalle à n'importe quel moment entre 30 minutes et 24 heures.

Pour modifier cet intervalle, modifiez le champ Fréquence dans la boîte de dialogue Modifier les planifications :



Planifier des basculements de tests automatisés

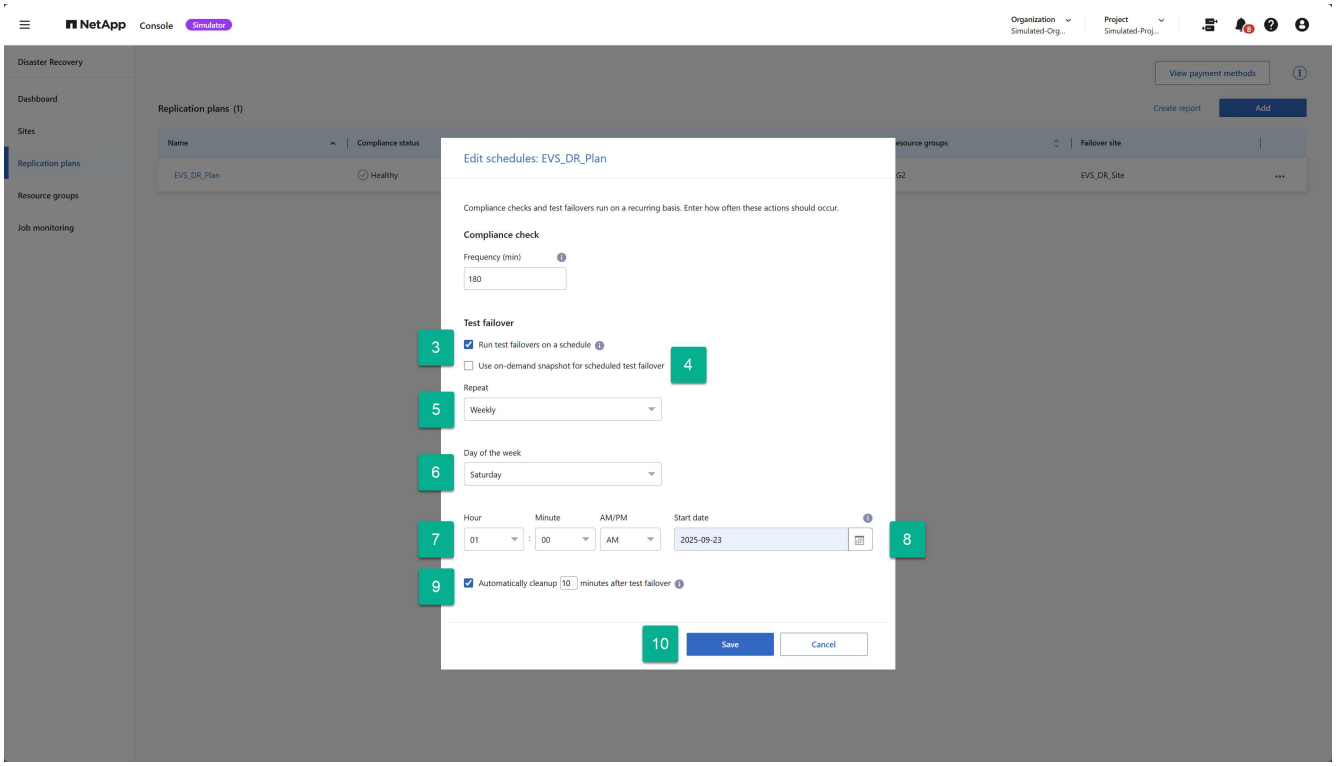
Les basculements de test sont exécutés manuellement par défaut. Vous pouvez planifier des basculements de test automatiques, ce qui permet de garantir que vos plans de réplication fonctionnent comme prévu. Pour en savoir plus sur le processus de basculement des tests, consultez"Tester le processus de basculement" .

Étapes pour planifier les basculements de test

1. Sélectionnez l'option *Actions* ••• à côté du plan de réplication.
2. Sélectionnez **Exécuter le basculement**.
3. Cochez la case **Exécuter les tests de basculement selon un calendrier**.
4. (Facultatif) Cochez la case **Utiliser un instantané à la demande pour le basculement de test planifié**.
5. Sélectionnez un type d'intervalle dans la liste déroulante Répéter.
6. Sélectionnez quand effectuer le test de basculement
   a. Hebdomadaire : sélectionnez le jour de la semaine
   b. Mensuel : sélectionnez le jour du mois
7. Choisissez l'heure de la journée pour exécuter le test de basculement
8. Choisissez la date de début.
9. Décidez si vous souhaitez que le service nettoie automatiquement l'environnement de test et combien de temps vous souhaitez que l'environnement de test s'exécute avant que le processus de nettoyage ne

démarre.

10. Sélectionnez **Enregistrer**.



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 DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

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

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

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

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

Informations sur les marques commerciales

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