Documentation sur la NetApp Disaster Recovery

NetApp Disaster Recovery

NetApp
February 04, 2026

Sommaire

Documentation sur la NetApp Disaster Recovery

Notes de version

Nouveautés de NetApp Disaster Recovery

Découvrez les nouveautés en matière de NetApp Disaster Recovery.

12 janvier 2026

Version 4.2.9

Prise en charge de plusieurs agents de console dans les environnements sur site

Si vous utilisez la reprise après sinistre sur site, vous pouvez désormais déployer un agent Console pour chaque instance vCenter, ce qui améliore la résilience.

Par exemple, si vous avez deux sites (sites A et B), le site A peut avoir l'agent de console A attaché à vCenter 1, au déploiement ONTAP 1 et au déploiement ONTAP 2. Le site B peut avoir l'agent de console B attaché aux déploiements vCenter 2 et ONTAP 3 et 4.

Pour plus d'informations sur l'agent Console dans le cadre de la reprise après sinistre, consultez "Créer l'agent de console".

Ajoutez des machines virtuelles après le basculement pour les plans de réplication utilisant la protection basée sur le datastore.

En cas de basculement, tout plan de réplication utilisant une protection basée sur la banque de données inclut les machines virtuelles ajoutées à la banque de données, à condition qu'elles aient été découvertes. Vous devez fournir les détails de mappage des machines virtuelles ajoutées avant que le basculement ne soit terminé.

Pour plus d'informations, voir "Applications de basculement".

Nouvelles notifications par e-mail

Le service de reprise après sinistre envoie désormais des notifications par e-mail pour les événements suivants :

- Limite d'utilisation de la capacité proche
- Génération du rapport terminée
- échecs professionnels
- Expiration ou infractions au permis

Améliorations de Swagger

Vous pouvez désormais accéder à la documentation Swagger directement depuis le système de reprise après sinistre. Dans la section Reprise après sinistre, sélectionnez **Paramètres** puis **Documentation API** pour accéder à Swagger, ou consultez cette URL en mode navigation privée/incognito de votre navigateur : "https://snapcenter.cloudmanager.cloud.netapp.com/api/api-doc/draas".

Interfaces utilisateur améliorées

La solution de reprise après sinistre offre désormais des avertissements et des résolutions d'erreurs améliorés. Cette version corrige une erreur qui empêchait l'affichage des tâches annulées dans l'interface utilisateur. Les tâches annulées sont désormais visibles. Un nouvel avertissement s'affiche également lorsque le même réseau de destination est associé à plusieurs réseaux sources différents.

Conserver la structure de dossiers des machines virtuelles ajoutée par défaut dans les plans de réplication

Lors de la création d'une réplication, le comportement par défaut consiste désormais à conserver la structure des dossiers de la machine virtuelle. Si le répertoire cible de récupération ne possède pas l'arborescence de dossiers d'origine, la fonction de récupération après sinistre la crée. Vous pouvez désélectionner cette option pour ignorer l'arborescence des dossiers d'origine.

Pour plus d'informations, voir "Créer un plan de réplication".

9 décembre 2025

Version 4.2.8P1

conservation de la hiérarchie des dossiers

Par défaut, la reprise après sinistre conserve la hiérarchie d'inventaire des machines virtuelles (structure des dossiers) lors d'un basculement. Si le dossier requis n'est pas présent sur la cible de récupération, la fonction de récupération après sinistre le crée.

Vous pouvez désormais modifier ce paramètre en désignant un nouveau dossier parent pour la machine virtuelle ou en décochant l'option **Conserver la hiérarchie de dossiers d'origine**.

Pour plus d'informations, voir "Créer un plan de réplication".

Mise à jour simplifiée de l'agent de console

La reprise après sinistre prend désormais en charge un processus simplifié pour l'utilisation de plusieurs agents Console dans un environnement de travail. Pour changer d'agent de console, vous devez modifier la configuration de votre vCenter, redécouvrir les informations d'identification et actualiser les plans de réplication pour utiliser le nouvel agent de console.

Pour plus d'informations, voir "Agents de la console de commutation".

1er décembre 2025

Version 4.2.8

Prise en charge de Google Cloud VMware Engine à l'aide de Google Cloud NetApp Volumes

NetApp Disaster Recovery prend désormais en charge Google Cloud VMware Engine utilisant Google Cloud NetApp Volumes pour les opérations de migration, de basculement, de restauration et de test. Cette intégration permet des flux de travail de reprise après sinistre transparents entre les environnements sur site et Google Cloud.

Assurez-vous de consulter le"prérequis" et"limites" pour Google Cloud.

10 novembre 2025

Version 4.2.7

Prise en charge du basculement en cascade

Vous pouvez désormais configurer une relation en cascade dans ONTAP et utiliser n'importe quel segment de cette relation de réplication pour la reprise après sinistre.

Rétrograder la prise en charge matérielle VMware lors de l'enregistrement

La solution de reprise après sinistre prend désormais en charge la rétrogradation du matériel VMware vers une version antérieure de vSphere lors de l'enregistrement. Cela s'avère utile lorsque l'hôte ESX source exécute une version plus récente que le site de reprise après sinistre.

Pour plus d'informations, voir "Créer un plan de réplication dans NetApp Disaster Recovery".

Arrêt en douceur

La reprise après sinistre arrête désormais les machines virtuelles en douceur au lieu de les éteindre brutalement. Si une machine virtuelle donnée met plus de dix minutes à s'éteindre, la procédure de reprise après sinistre l'éteint.

Assistance à la création de scripts avant sauvegarde

Vous pouvez désormais injecter des scripts personnalisés dans le flux de travail de basculement pour qu'ils s'exécutent avant la création d'une sauvegarde. Les scripts de pré-sauvegarde vous permettent de contrôler l'état de la machine virtuelle avant la réplication d'un instantané et de préparer une machine virtuelle à une transition. Par exemple, vous pouvez injecter un script qui démonte un montage NFS qui sera remonté à l'aide d'un script différent après le basculement.

Pour plus d'informations, voir "Créer un plan de réplication dans NetApp Disaster Recovery".

06 octobre 2025

Version 4.2.6

La BlueXP disaster recovery est désormais NetApp Disaster Recovery

La BlueXP disaster recovery a été renommée NetApp Disaster Recovery.

BlueXP est désormais NetApp Console

La NetApp Console, construite sur la base BlueXP améliorée et restructurée, fournit une gestion centralisée du stockage NetApp et des NetApp Data Services dans les environnements sur site et cloud à l'échelle de l'entreprise, offrant des informations en temps réel, des flux de travail plus rapides et une administration simplifiée, hautement sécurisée et conforme.

Pour plus de détails sur les changements, consultez le "Notes de version de la NetApp Console".

Autres mises à jour

- La prise en charge d'Amazon Elastic VMware Service (EVS) avec Amazon FSx for NetApp ONTAP était disponible en version préliminaire publique. Avec cette version, il est désormais généralement disponible.

Pour plus de détails, reportez-vous à"Présentation de NetApp Disaster Recovery à l'aide d'Amazon Elastic VMware Service et Amazon FSx for NetApp ONTAP" .

- Améliorations de la découverte du stockage, notamment des temps de découverte réduits pour les déploiements sur site
- Prise en charge de la gestion des identités et des accès (IAM), y compris le contrôle d'accès basé sur les rôles (RBAC) et les autorisations utilisateur améliorées
- Prise en charge de l'aperçu privé pour la solution Azure VMware et Cloud Volumes ONTAP. Grâce à cette prise en charge, vous pouvez désormais configurer la protection de reprise après sinistre sur site vers la solution Azure VMware à l'aide du stockage Cloud Volumes ONTAP .

4 août 2025

Version 4.2.5P2

Mises à jour de NetApp Disaster Recovery

Cette version inclut les mises à jour suivantes :

- Amélioration de la prise en charge VMFS pour gérer le même LUN présenté à partir de plusieurs machines virtuelles de stockage.
- Amélioration du nettoyage du démontage des tests pour gérer le magasin de données déjà démonté et/ou supprimé.
- Mappage de sous-réseau amélioré afin qu'il valide désormais que la passerelle saisie est contenue dans le réseau fourni.
- Correction d'un problème qui pouvait entraîner l'échec du plan de réplication si le nom de la machine virtuelle contenait « .com ».
- Suppression d'une restriction empêchant le volume de destination d'être identique au volume source lors de la création du volume dans le cadre de la création du plan de réplication.
- Ajout de la prise en charge d'un abonnement à la carte (PAYGO) aux services intelligents NetApp dans Azure Marketplace et ajout d'un lien vers Azure Marketplace dans la boîte de dialogue d'essai gratuit.

  Pour plus de détails, voir "Licences de NetApp Disaster Recovery" et "Configurer les licences pour NetApp Disaster Recovery" .

14 juillet 2025

Version 4.2.5

Rôles des utilisateurs dans NetApp Disaster Recovery

NetApp Disaster Recovery utilise désormais des rôles pour gérer l'accès de chaque utilisateur à des fonctionnalités et actions spécifiques.

Le service utilise les rôles suivants qui sont spécifiques à NetApp Disaster Recovery.

- **Administrateur de récupération après sinistre** : effectuez toutes les actions dans NetApp Disaster Recovery.
- **Administrateur de basculement de reprise après sinistre** : effectuez des actions de basculement et de migration dans NetApp Disaster Recovery.

- **Administrateur d'application de récupération après sinistre** : Créez et modifiez des plans de réplication et démarrez des tests de basculement.
- **Visionneuse de récupération après sinistre** : affichez les informations dans NetApp Disaster Recovery, mais ne pouvez effectuer aucune action.

Si vous cliquez sur le service NetApp Disaster Recovery et le configurez pour la première fois, vous devez disposer de l'autorisation **SnapCenterAdmin** ou du rôle **Organization Admin**.

Pour plus de détails, voir"Rôles et autorisations des utilisateurs dans NetApp Disaster Recovery" .

"En savoir plus sur les rôles d'accès pour tous les services".

Autres mises à jour de NetApp Disaster Recovery

- Découverte de réseau améliorée
- Améliorations de l'évolutivité :
  - Filtrage des métadonnées requises au lieu de tous les détails
  - Améliorations de la découverte pour récupérer et mettre à jour les ressources des machines virtuelles plus rapidement
  - Optimisation de la mémoire et des performances pour la récupération et la mise à jour des données
  - Améliorations de la création de clients et de la gestion des pools du SDK vCenter
- Gestion des données obsolètes lors de la prochaine découverte planifiée ou manuelle :
  - Lorsqu'une machine virtuelle est supprimée dans vCenter, NetApp Disaster Recovery la supprime désormais automatiquement du plan de réplication.
  - Lorsqu'une banque de données ou un réseau est supprimé dans vCenter, NetApp Disaster Recovery le supprime désormais du plan de réplication et du groupe de ressources.
  - Lorsqu'un cluster, un hôte ou un centre de données est supprimé dans vCenter, NetApp Disaster Recovery le supprime désormais du plan de réplication et du groupe de ressources.
- Vous pouvez désormais accéder à la documentation Swagger dans le mode navigation privée de votre navigateur. Vous pouvez y accéder depuis NetApp Disaster Recovery à partir de l'option Paramètres > Documentation API ou directement à l'URL suivante dans le mode navigation privée de votre navigateur : "Documentation de Swagger" .
- Dans certaines situations, après une opération de restauration automatique, l'iGroup a été laissé derrière une fois l'opération terminée. Cette mise à jour supprime l'iGroup s'il est obsolète.
- Si le nom de domaine complet NFS a été utilisé dans le plan de réplication, NetApp Disaster Recovery le résout désormais en une adresse IP. Cette mise à jour est utile si le nom de domaine complet n'est pas résoluble sur le site de reprise après sinistre.
- Améliorations de l'alignement de l'interface utilisateur
- Améliorations du journal pour capturer les détails de dimensionnement de vCenter après la découverte réussie

30 juin 2025

Version 4.2.4P2

Améliorations de la découverte

Cette mise à jour améliore le processus de découverte, ce qui réduit le temps nécessaire à la découverte.

23 juin 2025

Version 4.2.4P1

Améliorations du mappage des sous-réseaux

Cette mise à jour améliore la boîte de dialogue Ajouter et modifier le mappage de sous-réseau avec une nouvelle fonctionnalité de recherche. Vous pouvez désormais trouver rapidement des sous-réseaux spécifiques en saisissant des termes de recherche, ce qui facilite la gestion des mappages de sous-réseaux.

09 juin 2025

Version 4.2.4

Prise en charge de la solution de mot de passe d'administrateur local Windows (LAPS)

Windows Local Administrator Password Solution (Windows LAPS) est une fonctionnalité Windows qui gère et sauvegarde automatiquement le mot de passe d'un compte d'administrateur local sur Active Directory.

Vous pouvez désormais sélectionner les options de mappage de sous-réseau et vérifier l'option LAPS en fournissant les détails du contrôleur de domaine. En utilisant cette option, vous n'avez pas besoin de fournir un mot de passe pour chacune de vos machines virtuelles.

Pour plus de détails, reportez-vous à "Créer un plan de réplication" .

13 mai 2025

Version 4.2.3

Cartographie des sous-réseaux

Avec cette version, vous pouvez gérer les adresses IP lors du basculement d'une nouvelle manière 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.

Lors du basculement, NetApp Disaster Recovery détermine l'adresse IP appropriée de chaque vNIC en examinant le CIDR fourni pour le réseau virtuel mappé et l'utilise pour dériver la 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.

Pour plus d'informations sur l'intégration du mappage de sous-réseaux dans vos sites, veuillez consulter la documentation. "Ajouter des sites de serveur vCenter" .

Protection contre les sauts

Vous pouvez désormais ignorer la protection afin que le service ne crée pas automatiquement une relation de protection inverse 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.

Lorsque vous lancez un basculement, par défaut, le service crée automatiquement une relation de protection inverse pour chaque volume du plan de réplication, si le site source d'origine est en ligne. Cela signifie que le service crée une relation SnapMirror du site cible vers le site source. Le service inverse également automatiquement la relation SnapMirror lorsque vous lancez une restauration automatique.

Lors du lancement d'un basculement, vous pouvez désormais choisir une option **Protection contre les sauts**. Avec cela, le service n'inverse pas automatiquement la relation SnapMirror . Au lieu de cela, il laisse le volume inscriptible des deux côtés du plan de réplication.

Une fois le site source d'origine de nouveau en ligne, 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.

Pour plus de détails sur la protection contre le contournement, veuillez consulter "Basculer les applications vers un site distant" .

Mises à jour planifiées de SnapMirror dans le plan de réplication

NetApp Disaster Recovery prend désormais en charge l'utilisation de solutions de gestion de snapshots externes telles que le planificateur de politiques ONTAP SnapMirror natif ou les intégrations tierces avec ONTAP. 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.

Pour configurer, dans la section Plan de réplication > Mappage des ressources, cochez la case **Utiliser les sauvegardes gérées par la plateforme et les planifications de conservation** lors de la configuration du mappage des banques de données.

Lorsque l'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.

Pour plus de détails sur l'utilisation de solutions de snapshots externes dans le plan de réplication, reportez-vous à "Créer un plan de réplication" .

16 avril 2025

Version 4.2.2

Découverte planifiée pour les machines virtuelles

NetApp Disaster Recovery effectue la découverte une fois toutes les 24 heures. Avec cette version, vous pouvez désormais personnaliser le calendrier de découverte pour répondre à vos besoins et réduire l'impact sur les performances lorsque vous en avez besoin. 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 48 heures. 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 ne souhaitez pas planifier la découverte, vous pouvez désactiver l'option de découverte planifiée et actualiser la découverte manuellement à tout moment.

Pour plus de détails, reportez-vous à "Ajouter des sites de serveur vCenter" .

Prise en charge du magasin de données du groupe de ressources

Auparavant, vous ne pouviez créer des groupes de ressources que par machines virtuelles. Avec cette version, vous pouvez créer un groupe de ressources par magasins de données. Lorsque vous créez un plan de réplication et créez un groupe de ressources pour ce plan, toutes les machines virtuelles d'une banque de données sont répertoriées. Ceci est utile si vous disposez d'un grand nombre de machines virtuelles et que vous souhaitez les regrouper par banque de données.

Vous pouvez créer un groupe de ressources avec une banque 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.

Pour plus de détails, reportez-vous à "Créer un plan de réplication" .

Notifications d'essai gratuit ou d'expiration de licence

Cette version fournit des notifications indiquant que l'essai gratuit expirera dans 60 jours pour vous assurer d'avoir le temps d'obtenir une licence. Cette version fournit également des notifications le jour où la licence expire.

Notification des mises à jour du service

Avec cette version, une bannière apparaît en haut pour indiquer que les services sont en cours de mise à niveau et que le service est placé en mode maintenance. La bannière apparaît lorsque le service est en cours de mise à niveau et disparaît lorsque la mise à niveau est terminée. Bien que vous puissiez continuer à travailler dans l'interface utilisateur pendant que la mise à niveau est en cours, vous ne pouvez pas soumettre de nouvelles tâches. Les tâches planifiées s'exécuteront une fois la mise à jour terminée et le service reviendra en mode production.

10 mars 2025

Version 4.2.1

Prise en charge de proxy intelligent

L'agent de NetApp Console prend en charge le proxy intelligent. Le proxy intelligent est un moyen léger, sécurisé et efficace de connecter votre système sur site à NetApp Disaster Recovery. Il fournit une connexion sécurisée entre votre système et NetApp Disaster Recovery sans nécessiter de VPN ou d'accès Internet direct. Cette implémentation de proxy optimisée décharge le trafic API au sein du réseau local.

Lorsqu'un proxy est configuré, NetApp Disaster Recovery tente de communiquer directement avec VMware ou ONTAP et utilise le proxy configuré si la communication directe échoue.

L'implémentation du proxy NetApp Disaster Recovery nécessite une communication sur le port 443 entre l'agent de console et tous les serveurs vCenter et baies ONTAP utilisant un protocole HTTPS. L'agent NetApp Disaster Recovery au sein de l'agent de console communique directement avec VMware vSphere, VC ou ONTAP lors de l'exécution de toute action.

Pour plus d'informations sur le proxy intelligent pour NetApp Disaster Recovery, consultez "Configurez votre infrastructure pour la NetApp Disaster Recovery" .

Pour plus d'informations sur la configuration générale du proxy dans la NetApp Console, consultez "Configurer l'agent de console pour utiliser un serveur proxy" .

Mettre fin à l'essai gratuit à tout moment

Vous pouvez arrêter l'essai gratuit à tout moment ou attendre son expiration.

Voir "Mettre fin à l'essai gratuit" .

19 février 2025

Version 4.2

Prise en charge ASA r2 pour les machines virtuelles et les banques de données sur le stockage VMFS

Cette version de NetApp Disaster Recovery prend en charge ASA r2 pour les machines virtuelles et les banques de données sur le stockage VMFS. Sur un système ASA r2, le logiciel ONTAP prend en charge les fonctionnalités SAN essentielles tout en supprimant les fonctionnalités non prises en charge dans les environnements SAN.

Cette version prend en charge les fonctionnalités suivantes pour ASA r2 :

- Provisionnement de groupe de cohérence pour le stockage principal (groupe de cohérence plat uniquement, ce qui signifie un seul niveau sans structure hiérarchique)
- Opérations de sauvegarde (groupe de cohérence), y compris l'automatisation de SnapMirror

La prise en charge d' ASA r2 dans NetApp Disaster Recovery utilise ONTAP 9.16.1.

Bien que les banques de données puissent être montées sur un volume ONTAP ou une unité de stockage ASA r2, un groupe de ressources dans NetApp Disaster Recovery ne peut pas inclure à la fois une banque de données d' ONTAP et une autre d' ASA r2. Vous pouvez sélectionner une banque de données d' ONTAP ou une banque de données d' ASA r2 dans un groupe de ressources.

30 octobre 2024

Rapports

Vous pouvez désormais générer et télécharger des rapports pour vous aider à analyser votre paysage. Les rapports prédéfinis résument les basculements et les restaurations, affichent les détails de la réplication sur tous les sites et affichent les détails des tâches pour les sept derniers jours.

Se référer à "Créer des rapports de reprise après sinistre" .

Essai gratuit de 30 jours

Vous pouvez désormais vous inscrire pour un essai gratuit de 30 jours de NetApp Disaster Recovery. Auparavant, les essais gratuits duraient 90 jours.

Se référer à "Configurer les licences" .

Désactiver et activer les plans de réplication

Une version précédente incluait des mises à jour de la structure de planification des tests de basculement, qui étaient nécessaires pour prendre en charge les planifications quotidiennes et hebdomadaires. Cette mise à jour nécessite la désactivation et la réactivation de tous les plans de réplication existants afin de pouvoir utiliser les nouveaux calendriers de test de basculement quotidiens et hebdomadaires. Il s'agit d'une exigence unique.

Voici comment :

1. Dans le menu, sélectionnez **Plans de réplication**.
2. Sélectionnez un plan et sélectionnez l'icône Actions pour afficher le menu déroulant.
3. Sélectionnez **Désactiver**.
4. Après quelques minutes, sélectionnez **Activer**.

Mappage de dossiers

Lorsque vous créez un plan de réplication et mappez des ressources de calcul, vous pouvez désormais mapper des dossiers afin que les machines virtuelles soient récupérées dans un dossier que vous spécifiez pour le centre de données, le cluster et l'hôte.

Pour plus de détails, reportez-vous à "Créer un plan de réplication" .

Détails de la machine virtuelle disponibles pour le basculement, la restauration et le basculement de test

Lorsqu'une panne se produit et que vous démarrez un basculement, effectuez une restauration ou testez le basculement, vous pouvez désormais voir les détails des machines virtuelles et identifier celles qui n'ont pas redémarré.

Se référer à "Basculer les applications vers un site distant" .

Délai de démarrage de la machine virtuelle avec séquence de démarrage ordonnée

Lorsque vous créez un plan de réplication, vous pouvez désormais définir un délai de démarrage pour chaque machine virtuelle du plan. Cela vous permet de définir une séquence de démarrage des machines virtuelles afin de garantir que toutes vos machines virtuelles de priorité 1 s'exécutent avant le démarrage des machines virtuelles de priorité suivante.

Pour plus de détails, reportez-vous à "Créer un plan de réplication" .

Informations sur le système d'exploitation de la machine virtuelle

Lorsque vous créez un plan de réplication, vous pouvez désormais voir le système d'exploitation de chaque machine virtuelle du plan. Cela est utile pour décider comment regrouper les machines virtuelles dans un groupe de ressources.

Pour plus de détails, reportez-vous à "Créer un plan de réplication" .

Alias de nom de machine virtuelle

Lorsque vous créez un plan de réplication, vous pouvez désormais ajouter un préfixe et un suffixe aux noms de machines virtuelles sur le site de reprise après sinistre. Cela vous permet d'utiliser un nom plus descriptif pour les machines virtuelles du plan.

Pour plus de détails, reportez-vous à "Créer un plan de réplication" .

Nettoyer les anciens instantanés

Vous pouvez supprimer tous les instantanés qui ne sont plus nécessaires au-delà du nombre de rétention spécifié. Les instantanés peuvent s'accumuler au fil du temps lorsque vous réduisez votre nombre de rétention d'instantanés, et vous pouvez désormais les supprimer pour libérer de l'espace. Vous pouvez le faire à tout moment à la demande ou lorsque vous supprimez un plan de réplication.

Pour plus de détails, reportez-vous à "Gérer les sites, les groupes de ressources, les plans de réplication, les banques de données et les informations sur les machines virtuelles" .

Réconcilier les instantanés

Vous pouvez désormais réconcilier les instantanés qui ne sont pas synchronisés entre la source et la cible. Cela peut se produire si des snapshots sont supprimés sur une cible en dehors de NetApp Disaster Recovery. Le service supprime automatiquement l'instantané sur la source 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.

Pour plus de détails, reportez-vous à "Gérer les plans de réplication" .

20 septembre 2024

Prise en charge des banques de données VMware VMFS sur site vers sur site

Cette version inclut la prise en charge des machines virtuelles montées sur des banques de données de système de fichiers de machines virtuelles VMware vSphere (VMFS) pour le stockage sur site protégé par iSCSI et FC. Auparavant, le service fournissait un aperçu technologique prenant en charge les banques de données VMFS pour iSCSI et FC.

Voici quelques considérations supplémentaires concernant les protocoles iSCSI et FC :

- La prise en charge FC est destinée aux protocoles frontaux clients, pas à la réplication.
- NetApp Disaster Recovery ne prend en charge qu'un seul LUN par volume ONTAP . Le volume ne doit pas avoir plusieurs LUN.
- Pour tout plan de réplication, le volume ONTAP de destination doit utiliser les mêmes protocoles que le volume ONTAP source hébergeant les machines virtuelles protégées. Par exemple, si la source utilise un

protocole FC, la destination doit également utiliser FC.

02 août 2024

Prise en charge des banques de données VMware VMFS sur site pour FC

Cette version inclut un aperçu technologique de la prise en charge des machines virtuelles montées sur des banques de données de système de fichiers de machines virtuelles VMware vSphere (VMFS) pour le stockage sur site protégé par FC. Auparavant, le service fournissait un aperçu technologique prenant en charge les magasins de données VMFS pour iSCSI.

NetApp ne vous facture aucune capacité de charge de travail prévisualisée.

Annulation de travail

Avec cette version, vous pouvez désormais annuler une tâche dans l'interface utilisateur de Job Monitor.

Se référer à "Surveiller les emplois" .

17 juillet 2024

Calendriers de tests de basculement

Cette version inclut des mises à jour de la structure de planification des tests de basculement, qui étaient nécessaires pour prendre en charge les planifications quotidiennes et hebdomadaires. Cette mise à jour nécessite que vous désactiviez et réactiviez tous les plans de réplication existants afin de pouvoir utiliser les nouveaux calendriers de test de basculement quotidiens et hebdomadaires. Il s'agit d'une exigence unique.

Voici comment :

1. Dans le menu, sélectionnez **Plans de réplication**.
2. Sélectionnez un plan et sélectionnez l'icône Actions pour afficher le menu déroulant.
3. Sélectionnez **Désactiver**.
4. Après quelques minutes, sélectionnez **Activer**.

Mises à jour du plan de réplication

Cette version inclut des mises à jour des données du plan de réplication, ce qui résout un problème « instantané non trouvé ». Cela nécessite que vous modifiiez le nombre de rétention dans tous les plans de réplication sur 1 et que vous lanciez un snapshot à la demande. Ce processus crée une nouvelle sauvegarde et supprime toutes les anciennes sauvegardes.

Voici comment :

1. Dans le menu, sélectionnez **Plans de réplication**.
2. Sélectionnez le plan de réplication, sélectionnez l'onglet **Mappage de basculement** et sélectionnez l'icône en forme de crayon **Modifier**.
3. Sélectionnez la flèche **Datastores** pour la développer.
4. Notez la valeur du nombre de rétention dans le plan de réplication. Vous devez rétablir cette valeur d'origine une fois ces étapes terminées.

5. Réduisez le compte à 1.
6. Lancer un instantané à la demande. Pour ce faire, sur la page du plan de réplication, sélectionnez le plan, sélectionnez l'icône Actions, puis sélectionnez **Prendre un instantané maintenant**.
7. Une fois la tâche de capture instantanée terminée avec succès, augmentez le nombre dans le plan de réplication à sa valeur d'origine que vous avez notée à la première étape.
8. Répétez ces étapes pour tous les plans de réplication existants.

05 juillet 2024

Cette version de NetApp Disaster Recovery inclut les mises à jour suivantes :

Prise en charge de la série AFF A

Cette version prend en charge les plates-formes matérielles NetApp AFF série A.

Prise en charge des banques de données VMware VMFS sur site vers sur site

Cette version inclut un aperçu technologique de la prise en charge des machines virtuelles montées sur des banques de données VMware vSphere Virtual Machine File System (VMFS) protégées sur un stockage local. Avec cette version, la reprise après sinistre est prise en charge dans un aperçu technologique pour les charges de travail VMware sur site vers un environnement VMware sur site avec des banques de données VMFS.

NetApp ne vous facture aucune capacité de charge de travail prévisualisée.

Mises à jour du plan de réplication

Vous pouvez ajouter un plan de réplication plus facilement en filtrant les machines virtuelles par banque de données sur la page Applications et en sélectionnant plus de détails sur la cible sur la page Mappage des ressources. Se référer à "Créer un plan de réplication" .

Modifier les plans de réplication

Avec cette version, la page des mappages de basculement a été améliorée pour une meilleure clarté.

Se référer à "Gérer les plans" .

Modifier les machines virtuelles

Avec cette version, le processus de modification des machines virtuelles dans le plan inclut quelques améliorations mineures de l'interface utilisateur.

Se référer à "Gérer les machines virtuelles" .

Basculement des mises à jour

Avant de lancer un basculement, vous pouvez désormais déterminer l'état des machines virtuelles et si elles sont sous tension ou hors tension. Le processus de basculement vous permet désormais de prendre un instantané maintenant ou de choisir les instantanés.

Se référer à "Basculer les applications vers un site distant" .

Calendriers de tests de basculement

Vous pouvez désormais modifier les tests de basculement et définir des planifications quotidiennes, hebdomadaires et mensuelles pour le test de basculement.

Se référer à "Gérer les plans" .

Mises à jour des informations préalables

Les informations sur les conditions préalables à NetApp Disaster Recovery ont été mises à jour.

Se référer à "Conditions préalables à la NetApp Disaster Recovery" .

15 mai 2024

Cette version de NetApp Disaster Recovery inclut les mises à jour suivantes :

Réplication des charges de travail VMware d'un site vers un autre

Cette fonctionnalité est désormais disponible en tant que fonctionnalité générale. Auparavant, il s'agissait d'un aperçu technologique avec des fonctionnalités limitées.

Mises à jour des licences

Avec NetApp Disaster Recovery, vous pouvez vous inscrire à un essai gratuit de 90 jours, acheter un abonnement à la carte (PAYGO) auprès d'Amazon Marketplace ou apporter votre propre licence (BYOL), qui est un fichier de licence NetApp (NLF) que vous obtenez auprès de votre représentant commercial NetApp ou du site de support NetApp (NSS).

Pour plus de détails sur la configuration des licences pour NetApp Disaster Recovery, reportez-vous à"Configurer les licences" .

"En savoir plus sur la NetApp Disaster Recovery".

05 mars 2024

Il s'agit de la version de disponibilité générale de NetApp Disaster Recovery, qui inclut les mises à jour suivantes.

Mises à jour des licences

Avec NetApp Disaster Recovery, vous pouvez vous inscrire à un essai gratuit de 90 jours ou à Bring Your Own License (BYOL), qui est un fichier de licence NetApp (NLF) que vous obtenez auprès de votre représentant commercial NetApp . Vous pouvez utiliser le numéro de série de la licence pour activer le BYOL dans les abonnements à la NetApp Console . Les frais de NetApp Disaster Recovery sont basés sur la capacité provisionnée des magasins de données.

Pour plus d'informations sur la configuration des licences pour NetApp Disaster Recovery, veuillez consulter la documentation. "Configurer les licences" .

Pour plus d'informations sur la gestion des licences pour **tous** les services de données de la NetApp Console , veuillez consulter "Gérer les licences pour tous les services de données de la NetApp Console" .

Modifier les horaires

Avec cette version, vous pouvez désormais configurer des planifications pour tester les tests de conformité et de basculement afin de garantir qu'ils fonctionneront correctement si vous en avez besoin.

Pour plus de détails, reportez-vous à "Créer le plan de réplication" .

01 février 2024

Cette version préliminaire de NetApp Disaster Recovery inclut les mises à jour suivantes :

Amélioration du réseau

Avec cette version, vous pouvez désormais redimensionner les valeurs du processeur et de la RAM de la machine virtuelle. Vous pouvez également désormais sélectionner une adresse DHCP réseau ou une adresse IP statique pour la machine virtuelle.

- DHCP : si vous choisissez cette option, vous fournissez les informations d'identification pour la machine virtuelle.
- IP statique : vous pouvez sélectionner les mêmes informations ou des informations différentes de la machine virtuelle source. 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, le masque de sous-réseau, le DNS et les informations de passerelle.

Pour plus de détails, reportez-vous à "Créer un plan de réplication" .

Scripts personnalisés

Peut désormais être inclus en tant que processus post-basculement. Avec des scripts personnalisés, vous pouvez demander à NetApp Disaster Recovery d'exécuter votre script après un processus de basculement. Par exemple, vous pouvez utiliser un script personnalisé pour reprendre toutes les transactions de base de données une fois le basculement terminé.

Pour plus de détails, reportez-vous à "Basculer vers un site distant" .

Relation SnapMirror

Vous pouvez désormais créer une relation SnapMirror lors du développement du plan de réplication. Auparavant, vous deviez créer la relation en dehors de NetApp Disaster Recovery.

Pour plus de détails, reportez-vous à "Créer un plan de réplication" .

Groupes de cohérence

Lorsque vous créez un plan de réplication, vous pouvez inclure des machines virtuelles provenant de différents volumes et de différentes SVM. NetApp Disaster Recovery crée un snapshot de groupe de cohérence en incluant tous les volumes et met à jour tous les emplacements secondaires.

Pour plus de détails, reportez-vous à "Créer un plan de réplication" .

Option de délai de mise sous tension de la machine virtuelle

Lorsque vous créez un plan de réplication, vous pouvez ajouter des machines virtuelles à un groupe de

ressources. Avec les groupes de ressources, vous pouvez définir un délai sur chaque machine virtuelle afin qu'elles s'allument selon une séquence retardée.

Pour plus de détails, reportez-vous à "Créer un plan de réplication" .

Copies instantanées cohérentes avec les applications

Vous pouvez spécifier de créer des copies Snapshot cohérentes avec l'application. Le service mettra l'application en veille, puis prendra un instantané pour obtenir un état cohérent de l'application.

Pour plus de détails, reportez-vous à "Créer un plan de réplication" .

11 janvier 2024

Cette version préliminaire de NetApp Disaster Recovery inclut les mises à jour suivantes :

Tableau de bord plus rapidement

Avec cette version, vous pouvez accéder plus rapidement aux informations sur d'autres pages du tableau de bord.

"En savoir plus sur la NetApp Disaster Recovery".

20 octobre 2023

Cette version préliminaire de NetApp Disaster Recovery inclut les mises à jour suivantes.

Protégez les charges de travail VMware sur site basées sur NFS

Désormais, avec NetApp Disaster Recovery, vous pouvez protéger vos charges de travail VMware sur site, basées sur NFS, contre les sinistres dans un autre environnement VMware sur site, basé sur NFS, en plus du cloud public. NetApp Disaster Recovery orchestre l'achèvement des plans de reprise après sinistre.

> Avec cette offre préliminaire, NetApp se réserve le droit de modifier les détails, le contenu et le calendrier de l'offre avant la disponibilité générale.

"En savoir plus sur la NetApp Disaster Recovery".

27 septembre 2023

Cette version préliminaire de NetApp Disaster Recovery inclut les mises à jour suivantes :

Mises à jour du tableau de bord

Vous pouvez désormais sélectionner les options sur le tableau de bord, ce qui vous permet de consulter plus rapidement les informations. De plus, le tableau de bord affiche désormais l'état des basculements et des migrations.

Se référer à "Consultez l'état de vos plans de reprise après sinistre sur le tableau de bord" .

Mises à jour du plan de réplication

- **RPO** : vous pouvez désormais saisir l'objectif de point de récupération (RPO) et le nombre de rétentions dans la section Banques de données du plan de réplication. Cela indique la quantité de données qui

doivent exister et qui ne sont pas plus anciennes que l'heure définie. Si, par exemple, vous le définissez à 5 minutes, le système peut perdre jusqu'à 5 minutes de données en cas de sinistre sans impacter les besoins critiques de l'entreprise.

Se référer à "Créer un plan de réplication" .

- **Améliorations de la mise en réseau** : lorsque vous mappez la mise en réseau entre les emplacements source et cible dans la section des machines virtuelles du plan de réplication, NetApp Disaster Recovery propose désormais deux options : DHCP ou IP statique. Auparavant, seul DHCP était pris en charge. Pour les adresses IP statiques, vous configurez le sous-réseau, la passerelle et les serveurs DNS. De plus, vous pouvez désormais saisir des informations d'identification pour les machines virtuelles.

  Se référer à "Créer un plan de réplication" .

- **Modifier les planifications** : Vous pouvez désormais mettre à jour les planifications des plans de réplication.

  Se référer à "Gérer les ressources" .

- * Automatisation SnapMirror * : lorsque vous créez le plan de réplication dans cette version, vous pouvez définir la relation SnapMirror entre les volumes source et cible dans l'une des configurations suivantes :
  - 1 à 1
  - 1 à plusieurs dans une architecture en éventail
  - Plusieurs à 1 comme groupe de cohérence
  - Plusieurs à plusieurs

    Se référer à "Créer un plan de réplication" .

01 août 2023

Aperçu de la NetApp Disaster Recovery

NetApp Disaster Recovery Preview est un service de reprise après sinistre basé sur le cloud qui automatise les flux de travail de reprise après sinistre. Dans un premier temps, avec l'aperçu NetApp Disaster Recovery , vous pouvez protéger vos charges de travail VMware sur site, basées sur NFS, exécutant le stockage NetApp sur VMware Cloud (VMC) sur AWS avec Amazon FSx for ONTAP.

Avec cette offre préliminaire, NetApp se réserve le droit de modifier les détails, le contenu et le calendrier de l'offre avant la disponibilité générale.

"En savoir plus sur la NetApp Disaster Recovery".

Cette version inclut les mises à jour suivantes :

Mise à jour des groupes de ressources pour l'ordre de démarrage

Lorsque vous créez un plan de reprise après sinistre ou de réplication, vous pouvez ajouter des machines virtuelles dans des groupes de ressources fonctionnels. Les groupes de ressources vous permettent de placer un ensemble de machines virtuelles dépendantes dans des groupes logiques qui répondent à vos besoins. Par exemple, les groupes peuvent contenir un ordre de démarrage qui peut être exécuté lors de la récupération. Avec cette version, chaque groupe de ressources peut inclure une ou plusieurs machines virtuelles. Les machines virtuelles s'allumeront en fonction de la séquence dans laquelle vous les incluez dans le plan. Se

référer à "Sélectionnez les applications à répliquer et attribuez des groupes de ressources" .

Vérification de la réplication

Une fois que vous avez créé le plan de reprise après sinistre ou de réplication, 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. Se référer à "Répliquer des applications sur un autre site" .

Le plan de réplication affiche les planifications de transfert des objectifs de point de récupération (RPO)

Lorsque vous créez un plan de reprise après sinistre ou de réplication, vous sélectionnez les machines virtuelles. Dans cette version, vous pouvez désormais afficher le SnapMirror associé à chacun des volumes associés à la banque de données ou à la machine virtuelle. Vous pouvez également voir les planifications de transfert RPO associées à la planification SnapMirror . RPO vous aide à déterminer si votre planification de sauvegarde est suffisante pour assurer la récupération après une catastrophe. Se référer à "Créer un plan de réplication" .

Mise à jour du Job Monitor

La page Job Monitor inclut désormais une option Actualiser afin que vous puissiez obtenir un état à jour des opérations. Se référer à "Surveiller les tâches de reprise après sinistre" .

18 mai 2023

Il s'agit de la version initiale de NetApp Disaster Recovery.

Service de reprise après sinistre basé sur le cloud

NetApp Disaster Recovery est un service de reprise après sinistre basé sur le cloud qui automatise les flux de travail de reprise après sinistre. Dans un premier temps, avec l'aperçu NetApp Disaster Recovery , vous pouvez protéger vos charges de travail VMware sur site, basées sur NFS, exécutant le stockage NetApp sur VMware Cloud (VMC) sur AWS avec Amazon FSx for ONTAP.

"En savoir plus sur la NetApp Disaster Recovery".

Limitations de la NetApp Disaster Recovery

Les limitations connues identifient les plates-formes, les appareils ou les fonctions qui ne sont pas pris en charge par cette version du service ou qui n'interagissent pas correctement avec elle.

Attendez que la restauration soit terminée avant d'exécuter la découverte

Une fois le basculement terminé, ne lancez pas la découverte manuellement sur le vCenter source. Attendez que la restauration soit terminée, puis lancez la découverte sur le vCenter source.

La NetApp Console risque de ne pas détecter Amazon FSx for NetApp ONTAP

Parfois, la NetApp Console ne détecte pas les clusters Amazon FSx for NetApp ONTAP . Cela peut être dû au fait que les informations d'identification FSx n'étaient pas correctes.

Solution de contournement : ajoutez le cluster Amazon FSx for NetApp ONTAP dans la NetApp Console et actualisez régulièrement le cluster pour afficher les modifications.

Si vous devez supprimer le cluster ONTAP FSx de NetApp Disaster Recovery, procédez comme suit :

1. Dans l'agent de NetApp Console , utilisez les options de connectivité de votre fournisseur de cloud, connectez-vous à la machine virtuelle Linux sur laquelle l'agent de console s'exécute, redémarrez le service « occm » à l'aide de l' `docker restart occm` commande.

Se référer à "Gérer les agents de console existants" .

1. Sur la page Systèmes de NetApp Console , ajoutez à nouveau le système Amazon FSx for ONTAP et fournissez les informations d'identification FSx.

   Se référer à "Créer un système de fichiers Amazon FSx for NetApp ONTAP" .

2. Depuis NetApp Disaster Recovery, sélectionnez **Sites**, sur la ligne vCenter, sélectionnez l'option **Actions***  **, et dans le menu Actions, sélectionnez *Actualiser** pour actualiser la découverte FSx dans NetApp Disaster Recovery.

   Cela redécouvre le magasin de données, ses machines virtuelles et sa relation de destination.

Limitations des Google Cloud NetApp Volumes

- Après avoir exécuté un test de basculement, vous devez attendre au moins 52 heures avant de pouvoir supprimer le volume cloné. Vous devez supprimer le volume manuellement. Après 52 heures, vous pourrez tester à nouveau le basculement.
- Si une quelconque étape de l'opération de montage échoue, le basculement ne réussira pas et les tâches expireront. Il faut jusqu'à trois jours à Google pour examiner le problème, période pendant laquelle toutes les opérations liées au stockage de données sur vCenter sont bloquées.

Commencer

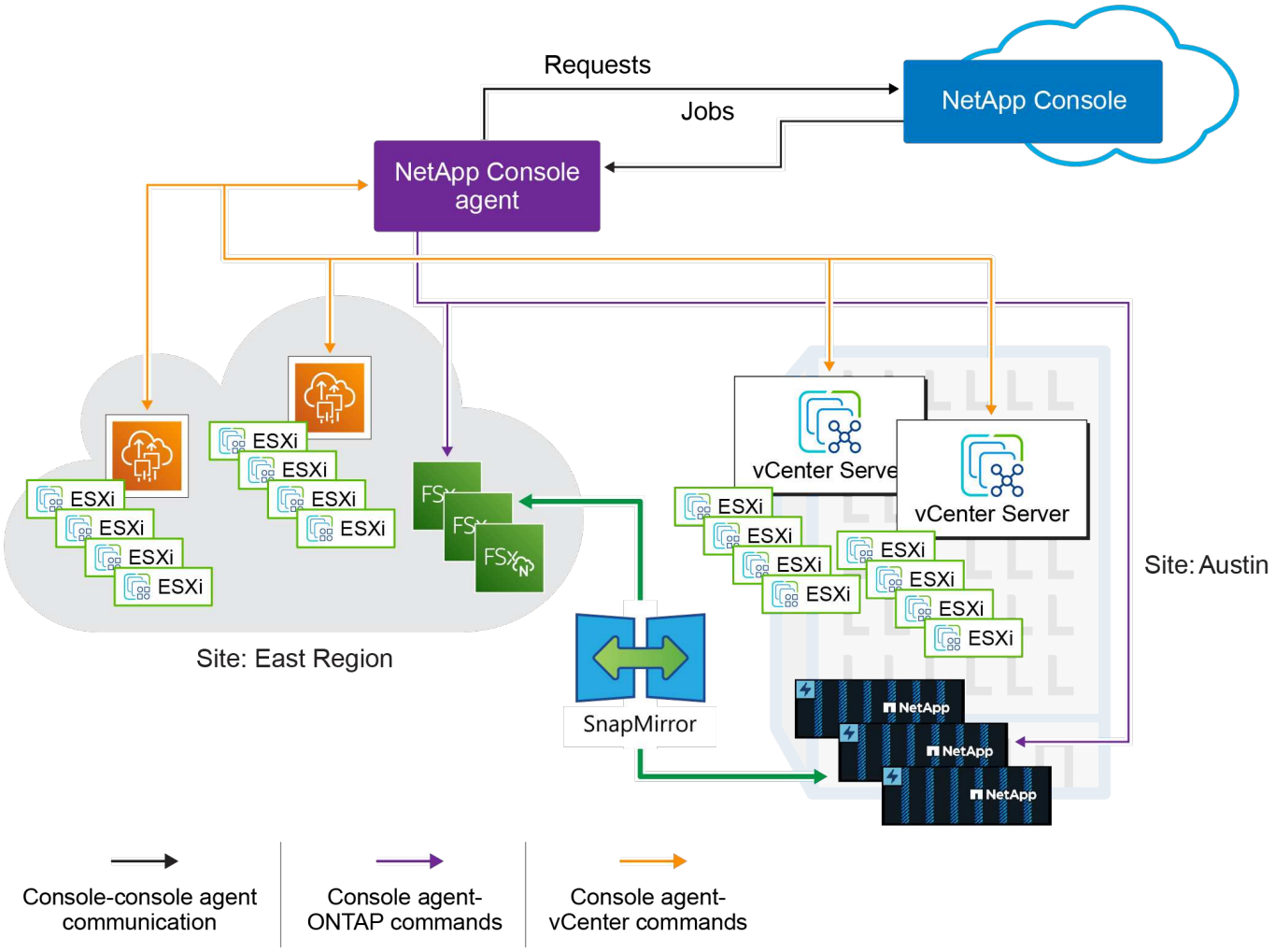
En savoir plus sur NetApp Disaster Recovery pour VMware

La reprise après sinistre dans le cloud est un moyen résilient et rentable de protéger les charges de travail contre les pannes de site et les événements de corruption de données. Avec NetApp Disaster Recovery pour VMware, vous pouvez répliquer vos charges de travail de machine virtuelle VMware ou de banque de données sur site exécutant le stockage ONTAP vers un centre de données défini par logiciel VMware dans un cloud public à l'aide du stockage cloud NetApp ou vers un autre environnement VMware sur site avec le stockage ONTAP comme site de reprise après sinistre. Vous pouvez également utiliser Disaster Recovery pour migrer les charges de travail des machines virtuelles d'un site à un autre.

NetApp Disaster Recovery est un service de reprise après sinistre basé sur le cloud qui automatise les flux de travail de reprise après sinistre. Avec NetApp Disaster Recovery, vous pouvez protéger vos charges de travail locales basées sur NFS et vos banques de données VMware vSphere Virtual Machine File System (VMFS) pour le stockage NetApp exécutant iSCSI et FC sur l'un des éléments suivants :

- Amazon Elastic VMware Service (EVS) avec Amazon FSx for NetApp ONTAP Pour plus de détails, reportez-vous à"Présentation de NetApp Disaster Recovery à l'aide d'Amazon Elastic VMware Service et Amazon FSx for NetApp ONTAP" .
- VMware Cloud (VMC) sur AWS avec Amazon FSx for NetApp ONTAP
- Solution Azure VMware (AVS) avec NetApp Cloud Volumes ONTAP (iSCSI) (version préliminaire privée)
- Google Cloud VMware Engine (GCVE) avec Google Cloud NetApp Volumes
- Un autre environnement VMware sur site basé sur NFS et/ou VMFS (iSCSI/FC) avec stockage ONTAP

NetApp Disaster Recovery utilise la technologie ONTAP SnapMirror avec l'orchestration VMware native intégrée pour protéger les machines virtuelles VMware et leurs images de système d'exploitation sur disque associées, tout en conservant tous les avantages d'efficacité de stockage d' ONTAP. La reprise après sinistre utilise ces technologies comme moyen de réplication vers le site de reprise après sinistre. Cela permet une efficacité de stockage optimale (compression et déduplication) sur les sites principaux et secondaires.



NetApp Console

NetApp Disaster Recovery est accessible via la NetApp Console.

La NetApp Console fournit une gestion centralisée des services de stockage et de données NetApp dans les environnements sur site et cloud à l'échelle de l'entreprise. La console est requise pour accéder aux services de données NetApp et les utiliser. En tant qu'interface de gestion, il vous permet de gérer de nombreuses ressources de stockage à partir d'une seule interface. Les administrateurs de console peuvent contrôler l'accès au stockage et aux services pour tous les systèmes de l'entreprise.

Vous n'avez pas besoin de licence ni d'abonnement pour commencer à utiliser NetApp Console et vous n'encourez des frais que lorsque vous devez déployer des agents de console dans votre cloud pour garantir la connectivité à vos systèmes de stockage ou à vos services de données NetApp . Cependant, certains services de données NetApp accessibles depuis la console sont sous licence ou basés sur un abonnement.

Apprenez-en davantage sur le "NetApp Console" .

Avantages de l'utilisation de NetApp Disaster Recovery pour VMware

NetApp Disaster Recovery offre les avantages suivants :

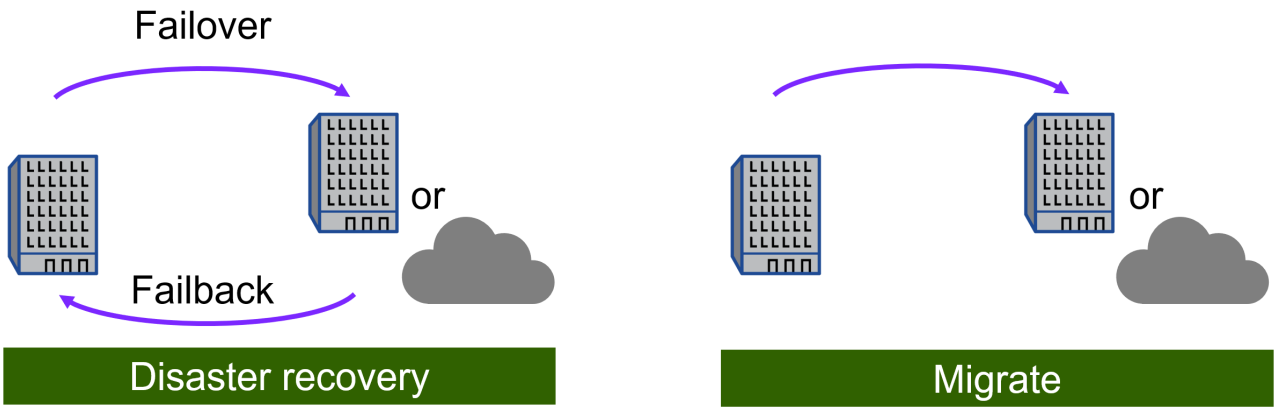
- Expérience utilisateur simplifiée pour la découverte et la récupération d'applications vCenter avec plusieurs opérations de récupération à un instant donné.

- Coût total de possession réduit avec un coût d'exploitation réduit et la possibilité de créer et d'ajuster des plans de reprise après sinistre avec des ressources minimales.
- Préparation continue à la reprise après sinistre avec des tests de basculement virtuel qui ne perturbent pas les opérations. Vous pouvez tester régulièrement vos plans de basculement DR sans impacter les charges de travail de production.
- Rentabilisation plus rapide grâce à des changements dynamiques dans votre environnement informatique et capacité à les prendre en compte dans vos plans de reprise après sinistre.
- Capacité à gérer à la fois les couches de stockage et virtuelles via l'orchestration back-end d' ONTAP et de VMware en même temps sans avoir besoin d'appliances de serveur virtuel (VSA) qui doivent être déployées et maintenues.
- Les solutions DR pour VMware peuvent nécessiter beaucoup de ressources. De nombreuses solutions DR répliquent les machines virtuelles au niveau de la couche virtuelle VMware à l'aide de VSA, ce qui peut consommer davantage de ressources de calcul et faire perdre les précieuses efficacités de stockage d' ONTAP. Étant donné que Disaster Recovery utilise la technologie ONTAP SnapMirror , il peut répliquer les données des banques de données de production vers le site DR à l'aide de notre modèle de réplication incrémentielle permanente avec toutes les efficacités natives de compression et de déduplication des données d' ONTAP.

Ce que vous pouvez faire avec NetApp Disaster Recovery pour VMware

NetApp Disaster Recovery vous permet d'utiliser pleinement plusieurs technologies NetApp pour atteindre les objectifs suivants :

- Répliquez les applications VMware sur votre site de production sur site vers un site distant de reprise après sinistre dans le cloud ou sur site à l'aide de la réplication SnapMirror .
- Migrez les charges de travail VMware de votre site d'origine vers un autre site.
- Effectuer un test de basculement. Lorsque vous faites cela, le service crée des machines virtuelles temporaires. La récupération après sinistre crée un nouveau volume FlexClone à partir du snapshot sélectionné et une banque de données temporaire, sauvegardée par le volume FlexClone , est mappée aux 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 continuer même pendant la reprise après sinistre.
- En cas de sinistre, basculez votre site principal à la demande vers le site de reprise après sinistre, qui peut être VMware Cloud sur AWS avec Amazon FSx for NetApp ONTAP ou un environnement VMware sur site avec ONTAP.
- Une fois le sinistre résolu, effectuez une restauration à la demande du site de reprise après sinistre vers le site principal.
- Regroupez les machines virtuelles ou les banques de données en groupes de ressources logiques pour une gestion efficace.



La configuration du serveur vSphere est effectuée en dehors de NetApp Disaster Recovery dans vSphere Server.

Coût

NetApp ne vous facture pas l'utilisation de la version d'essai de NetApp Disaster Recovery.

NetApp Disaster Recovery peut être utilisé avec une licence NetApp ou un plan d'abonnement annuel via Amazon Web Services.

Certaines versions incluent un aperçu technologique. NetApp ne vous facture aucune capacité de charge de travail prévisualisée. Voir"Nouveautés de NetApp Disaster Recovery" pour obtenir des informations sur les dernières avancées technologiques.

Licences

Vous pouvez utiliser les types de licences suivants :

- Inscrivez-vous pour un essai gratuit de 30 jours.
- Achetez un abonnement à la carte (PAYGO) avec Amazon Web Services (AWS) Marketplace ou Microsoft Azure Marketplace. Cette licence vous permet d'acheter une licence à capacité protégée fixe sans aucun engagement à long terme.
- Apportez votre propre licence (BYOL), qui est un fichier de licence NetApp (NLF) que vous obtenez auprès de votre représentant commercial NetApp . Vous pouvez utiliser le numéro de série de la licence pour activer le BYOL dans la NetApp Console.

Les licences pour tous les services de données NetApp sont gérées via des abonnements dans la NetApp Console. Après avoir configuré votre BYOL, vous pouvez voir une licence active pour le service dans la console.

Le service est concédé sous licence en fonction de la quantité de données hébergées sur des volumes ONTAP protégés. Le service détermine quels volumes doivent être pris en compte à des fins de licence en mappant les machines virtuelles protégées à leurs banques de données vCenter. Chaque banque de données est hébergée sur un volume ONTAP ou LUN. La capacité utilisée signalée par ONTAP pour ce volume ou LUN est utilisée pour les déterminations de licence.

Les volumes protégés peuvent héberger de nombreuses machines virtuelles. Certains peuvent ne pas faire partie d'un groupe de ressources NetApp Disaster Recovery . Quoi qu'il en soit, le stockage consommé par toutes les machines virtuelles sur ce volume ou LUN est utilisé par rapport à la capacité maximale de la licence.

> Les frais de NetApp Disaster Recovery sont basés sur la capacité utilisée des banques de données sur le site source lorsqu'il existe au moins une machine virtuelle dotée d'un plan de réplication. La capacité d'une banque de données basculée n'est pas incluse dans la capacité allouée. Pour un BYOL, si les données dépassent la capacité autorisée, les opérations dans le service sont limitées jusqu'à ce que vous obteniez une licence de capacité supplémentaire ou que vous mettiez à niveau la licence dans la NetApp Console.

Pour plus de détails sur la configuration des licences pour NetApp Disaster Recovery, reportez-vous à"Configurer les licences NetApp Disaster Recovery" .

Essai gratuit de 30 jours

Vous pouvez essayer NetApp Disaster Recovery en utilisant un essai gratuit de 30 jours.

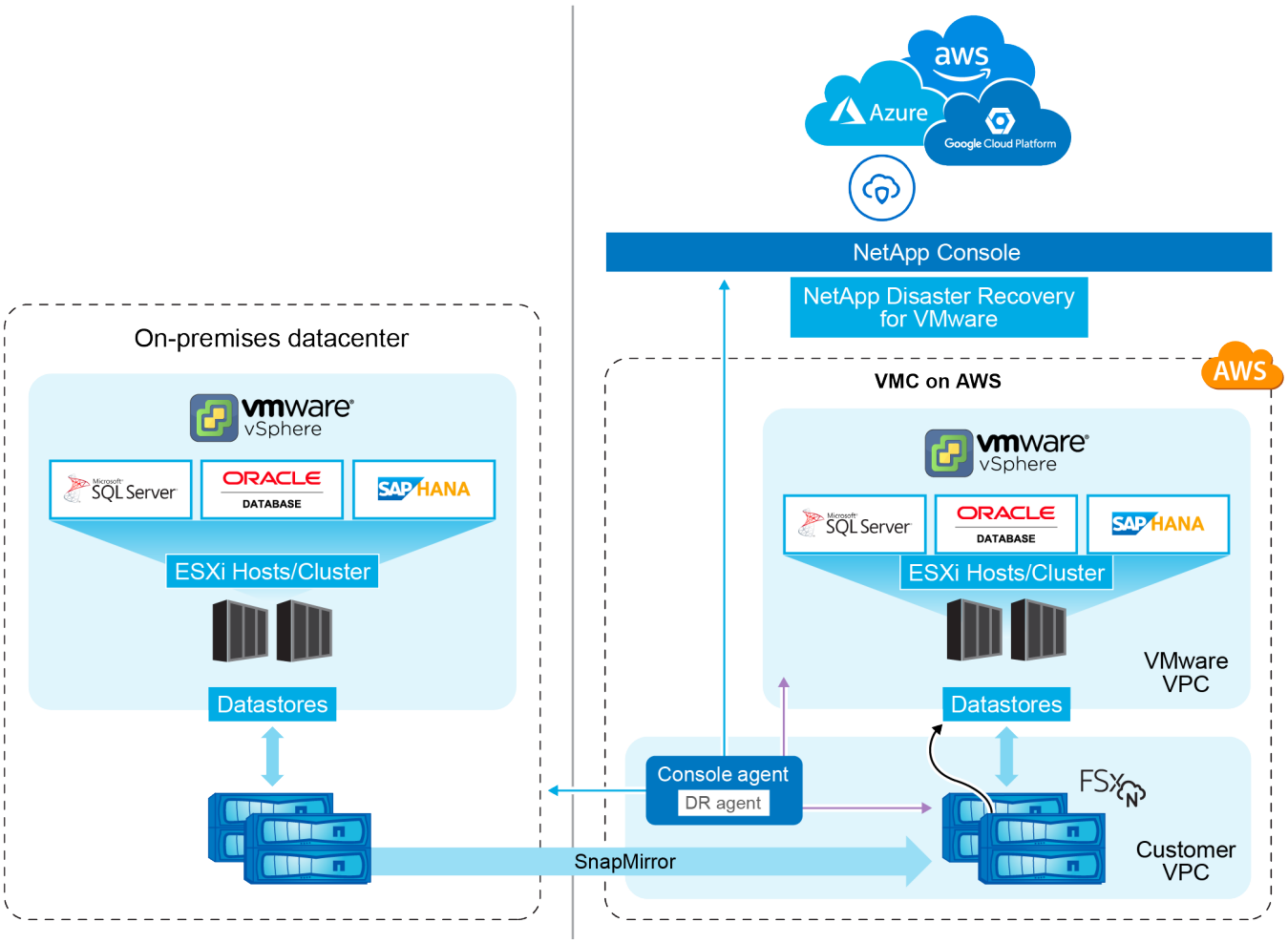
Pour continuer après l'essai de 30 jours, vous devrez obtenir un abonnement Pay-as-you-go (PAYGO) auprès de votre fournisseur de cloud ou acheter une licence BYOL auprès de NetApp.

Vous pouvez acheter une licence à tout moment et vous ne serez pas facturé avant la fin de la période d'essai de 30 jours.

Comment fonctionne la NetApp Disaster Recovery

NetApp Disaster Recovery est un service hébergé dans l'environnement logiciel en tant que service (SaaS) de la NetApp Console . La reprise après sinistre peut récupérer les charges de travail répliquées à partir d'un site local vers Amazon FSx for ONTAP ou vers un autre site local. Ce service automatise la récupération depuis SnapMirror , via l'enregistrement des machines virtuelles dans VMware Cloud sur AWS et les mappages réseau directement sur NSX-T, la plateforme de virtualisation et de sécurité réseau VMware. Cette fonctionnalité est incluse dans tous les environnements Virtual Machine Cloud.

NetApp Disaster Recovery utilise la technologie ONTAP SnapMirror , qui fournit une réplication hautement efficace et préserve l'efficacité des snapshots incrémentiels permanents ONTAP . La réplication SnapMirror garantit que les copies de snapshots cohérentes avec les applications sont toujours synchronisées et que les données sont utilisables immédiatement après un basculement.



En cas de sinistre, ce service vous aide à récupérer des machines virtuelles dans l'autre environnement VMware local ou VMC en rompant les relations SnapMirror et en rendant le site de destination actif.

- Le service vous permet également de restaurer les machines virtuelles à l'emplacement source d'origine.
- Vous pouvez tester le processus de basculement de reprise après sinistre sans perturber les machines virtuelles d'origine. Le test récupère les machines virtuelles sur un réseau isolé en créant un FlexClone du volume.
- Pour le processus de basculement ou de test de basculement, vous pouvez choisir le snapshot le plus récent (par défaut) ou sélectionné à partir duquel récupérer votre machine virtuelle.

Composants de la reprise après sinistre

La reprise après sinistre utilise les composants suivants pour assurer la reprise après sinistre des charges de travail VMware :

- * NetApp Console* : L'interface utilisateur pour la gestion de vos plans de reprise après sinistre. Vous pouvez utiliser la NetApp Console pour créer et gérer des plans de réplication, des groupes de ressources et des opérations de basculement dans vos environnements locaux et cloud.
- **Agent de console** : un composant logiciel léger qui s'exécute sur votre réseau hébergé dans le cloud ou dans votre environnement VMware sur site. Il communique avec la NetApp Console et gère la réplication des données entre votre environnement sur site et le site de reprise après sinistre. L'agent de console est installé sur une machine virtuelle dans votre environnement VMware.

- * Clusters de stockage ONTAP * : les clusters de stockage ONTAP sont les principaux systèmes de stockage qui hébergent vos charges de travail VMware. Les clusters de stockage ONTAP fournissent l'infrastructure de stockage sous-jacente pour vos plans de reprise après sinistre. La reprise après sinistre utilise les API de stockage ONTAP pour gérer les clusters de stockage ONTAP tels que les baies sur site et les solutions basées sur le cloud, telles qu'Amazon Amazon FSx for NetApp ONTAP.
- **Serveurs vCenter** : VMware vCenter est le serveur de gestion de votre environnement VMware. Il gère les hôtes ESXi et leurs banques de données associées. L'agent de console communique avec VMware vCenter pour gérer la réplication des données entre votre environnement local et le site de reprise après sinistre. Cela inclut l'enregistrement des LUN et des volumes ONTAP en tant que banques de données, la reconfiguration des machines virtuelles et le démarrage et l'arrêt des machines virtuelles.

Le flux de travail de protection de reprise après sinistre

Lorsqu'un plan de réplication est attribué à un groupe de ressources, Disaster Recovery effectue une vérification de découverte de tous les composants du groupe de ressources et du plan pour garantir que le plan peut être activé.

Si cette vérification réussit, Disaster Recovery exécute les étapes d'initialisation suivantes :

1. Pour chaque machine virtuelle du groupe de ressources cible, identifiez la banque de données VMware hébergeante.
2. Pour chaque banque de données VMware trouvée, identifiez le volume ou le LUN ONTAP FlexVol volume d'hébergement.
3. Pour chaque volume ONTAP et LUN trouvés, déterminez s'il existe une relation SnapMirror entre les volumes sources et un volume de destination sur le site de destination.
    a. S'il n'existe aucune relation SnapMirror préexistante, créez de nouveaux volumes de destination et créez une nouvelle relation SnapMirror entre chaque volume source non protégé.
    b. S'il existe une relation SnapMirror préexistante, utilisez cette relation pour effectuer toutes les opérations de réplication.

Une fois que Disaster Recovery a créé et initialisé toutes les relations, à chaque sauvegarde planifiée, le service exécute les étapes de protection des données suivantes :

1. Pour chaque machine virtuelle marquée comme « cohérente avec l'application », utilisez VMtools pour placer l'application prise en charge dans un état de sauvegarde.
2. Créez un nouvel instantané de tous les volumes ONTAP hébergeant des banques de données VMware protégées.
3. Effectuez une opération de mise à jour SnapMirror pour répliquer ces snapshots sur le cluster ONTAP de destination.
4. Déterminez si le nombre de snapshots conservés a dépassé la rétention maximale de snapshots définie dans le plan de réplication et supprimez tous les snapshots superflus des volumes source et de destination.

Cibles de protection et types de banques de données pris en charge

Types de magasins de données pris en charge NetApp Disaster Recovery prend en charge les types de magasins de données suivants :

- Banques de données NFS hébergées sur des volumes ONTAP FlexVol résidant sur des clusters ONTAP .
- Banques de données du système de fichiers de machine virtuelle VMware vSphere (VMFS) utilisant le

protocole iSCSI ou FC

Cibles de protection prises en charge

- VMware Cloud (VMC) sur AWS avec Amazon FSx for NetApp ONTAP
- Un autre environnement VMware sur site basé sur NFS avec stockage ONTAP ou un VMSF FC/iSCSI sur site
- Service VMware élastique Amazon
- Solution Azure VMware (AVS) avec NetApp Cloud Volumes ONTAP (iSCSI) (version préliminaire privée)
- Google Cloud VMware Engine (GCVE) avec Google Cloud NetApp Volumes

Termes qui pourraient vous aider avec NetApp Disaster Recovery

Il pourrait être utile de comprendre certains termes liés à la reprise après sinistre.

- **Datastore** : un conteneur de données VMware vCenter, qui utilise un système de fichiers pour contenir les fichiers VMDK. Les types de banques de données typiques sont NFS, VMFS, vSAN ou vVol. Disaster Recovery prend en charge les banques de données NFS et VMFS. Chaque banque de données VMware est hébergée sur un seul volume ONTAP ou LUN. Disaster Recovery prend en charge les banques de données NFS et VMFS hébergées sur des volumes FlexVol résidant sur des clusters ONTAP .
- **Plan de réplication** : un ensemble de règles sur la fréquence des sauvegardes et sur la manière de gérer les événements de basculement. Les plans sont attribués à un ou plusieurs groupes de ressources.
- **Objectif de point de récupération (RPO)** : La quantité maximale de perte de données acceptable en cas de sinistre. Le RPO est défini dans la fréquence de réplication des données ou dans le calendrier de réplication du plan de réplication.
- **Objectif de temps de récupération (RTO)** : La durée maximale acceptable pour récupérer après une catastrophe. Le RTO est défini dans le plan de réplication et correspond au temps nécessaire pour basculer vers le site DR et redémarrer toutes les machines virtuelles.
- **Groupe de ressources** : un conteneur logique qui vous permet de gérer plusieurs machines virtuelles comme une seule unité. Une machine virtuelle ne peut appartenir qu'à un seul groupe de ressources à la fois. Vous pouvez créer un groupe de ressources pour chaque application ou charge de travail que vous souhaitez protéger.
- **Site** : un conteneur logique généralement associé à un centre de données physique ou à un emplacement cloud hébergeant un ou plusieurs clusters vCenter et un stockage ONTAP .

Conditions préalables à la NetApp Disaster Recovery

Avant d'utiliser NetApp Disaster Recovery, assurez-vous que votre environnement répond aux exigences en matière de stockage ONTAP , de cluster VMware vCenter et de NetApp Console .

Versions du logiciel

Composant	Version minimale
Amazon FSx for NetApp ONTAP	Dernière version disponible

Composant	Version minimale
Google Cloud VMware Engine utilisant Google Cloud NetApp Volumes	Dernière version disponible
Logiciel ONTAP	ONTAP 9.10.0 ou version ultérieure
VMware Cloud pour AWS	Dernière version disponible
VMware sur site vCenter	7.0u3 ou version ultérieure

Prérequis et considérations relatifs à Google Cloud

Lors de la reprise après sinistre sur Google Cloud VMware Engine utilisant Google Cloud NetApp Volumes, assurez-vous de configurer les autorisations appropriées et de respecter les considérations mentionnées.

- Contactez l'équipe SRE de Google pour ajouter à la liste blanche :
  - API de synchronisation pour transférer les instantanés du stockage sur site vers Google Cloud NetApp Volumes.
  - le projet Google avec le moteur VMware pour la création, le montage et le démontage de banques de données.
- Vous devez"Déposez une demande pour ajouter vos volumes à la liste blanche en matière de réplication hybride." .
- Soyez conscient de"Quotas et limites de Google Cloud NetApp Volumes" .
- Vous ne pouvez ajouter qu'un seul volume ou une seule banque de données à un plan de réplication.
- Examiner"limites" .

Considérations relatives au basculement

- Le basculement n'est pris en charge qu'avec le dernier instantané. Si nécessaire, vous pouvez créer un nouvel instantané pendant le basculement (c'est-à-dire que l'option d'instantané sélectif doit être désactivée).
- Il est impossible de créer un nouvel instantané après un basculement.
- Il est impossible de conserver et de réconcilier les instantanés après un basculement.

Considérations relatives aux solutions de repli

- La restauration n'est possible qu'avec l'option de capture d'écran sélective. Il est impossible d'effectuer une restauration en prenant un nouvel instantané.
- Si vous supprimez le peering de cluster entre le stockage sur site et les clusters de stockage Google Cloud NetApp Volumes , vous devez supprimer manuellement l'entrée de peering de cluster et de machine virtuelle de stockage du cluster sur site. Pour plus d'informations, voir "Supprimer une relation d'homologue vserver".

Autorisations Google Cloud

Le principal de service dans Google Cloud doit se voir attribuer les rôles suivants ou des autorisations équivalentes :

- "Rôle d'administrateur informatique"
- "Autorisations Google Cloud pour la NetApp Console"
- "Administration des Google Cloud NetApp Volumes"
- "Administrateur de service VMware Engine"

Autorisations de la NetApp Console

L'utilisateur de la NetApp Console doit posséder les rôles suivants :

- "Administrateur Google Cloud NetApp Volumes"
- "Administrateur SnapCenter"
- "Administrateur de basculement de reprise après sinistre"

Prérequis de stockage ONTAP

Ces conditions préalables s'appliquent aux instances ONTAP ou Amazon FSX pour NetApp ONTAP .

- Les clusters source et de destination doivent avoir une relation d'homologue.
- La SVM qui héberge les volumes de reprise après sinistre doit exister sur le cluster de destination.
- La SVM source et la SVM de destination doivent avoir une relation homologue.
- En cas de déploiement avec Amazon FSx for NetApp ONTAP, la condition préalable suivante s'applique :
  - Une instance Amazon FSx for NetApp ONTAP pour héberger les magasins de données VMware DR doit exister dans votre VPC. Pour commencer, voir"la documentation Amazon FSx pour ONTAP" .

Conditions préalables pour les clusters VMware vCenter

Ces conditions préalables s'appliquent à la fois aux clusters vCenter sur site et au centre de données défini par logiciel (SDDC) VMware Cloud for AWS.

- Revoir"privilèges vCenter" requis pour la NetApp Disaster Recovery.
- Tous les clusters VMware que vous souhaitez que NetApp Disaster Recovery gère utilisent les volumes ONTAP pour héberger toutes les machines virtuelles que vous souhaitez protéger.
- Toutes les banques de données VMware à gérer par NetApp Disaster Recovery doivent utiliser l'un des protocoles suivants :
  - NFS
  - VMFS utilisant le protocole iSCSI ou FC
- VMware vSphere version 7.0 Update 3 (7.0v3) ou ultérieure
- Si vous utilisez VMware Cloud SDDC, ces conditions préalables s'appliquent.
  - Dans la console VMware Cloud, utilisez les rôles de service Administrateur et Administrateur NSX Cloud. Utilisez également le propriétaire de l'organisation pour le rôle Organisation. Se référer à "Utilisation de VMware Cloud Foundations avec la documentation AWS FSx pour NetApp ONTAP" .
  - Liez le SDDC VMware Cloud à l'instance Amazon FSx for NetApp ONTAP . Se référer à "Informations sur le déploiement de l'intégration de VMware Cloud sur AWS avec Amazon FSx for NetApp ONTAP" .

Prérequis de la NetApp Console

Démarrer avec la NetApp Console

Si vous ne l'avez pas déjà fait, "inscrivez-vous à la NetApp Console et créez une organisation" .

Collecter les informations d'identification pour ONTAP et VMware

- Les informations d'identification Amazon FSx for ONTAP et AWS doivent être ajoutées au système dans le cadre du projet NetApp Console qui gère la NetApp Disaster Recovery.
- NetApp Disaster Recovery nécessite des informations d'identification vCenter. Vous entrez les informations d'identification vCenter lorsque vous ajoutez un site dans NetApp Disaster Recovery.

  Pour obtenir la liste des privilèges vCenter nécessaires, reportez-vous à"Privilèges vCenter nécessaires pour la NetApp Disaster Recovery" . Pour obtenir des instructions sur la façon d'ajouter un site, reportez-vous à"Ajouter un site" .

Créer l'agent de la NetApp Console

L'agent de console est un composant logiciel qui permet à la console de communiquer avec votre stockage ONTAP et vos clusters VMware vCenter. Il est nécessaire au bon fonctionnement de la reprise après sinistre. L'agent réside dans votre réseau privé (un centre de données sur site ou un VPC cloud) et communique avec vos instances de stockage ONTAP et tous les composants serveur et application supplémentaires. Pour la reprise après sinistre, il s'agit d'un accès à vos clusters vCenter gérés.

Un agent de console doit être configuré dans la NetApp Console. Lorsque vous utilisez l'agent, il inclura les fonctionnalités appropriées pour le service de reprise après sinistre.

- NetApp Disaster Recovery fonctionne uniquement avec le déploiement d'agent en mode standard. Voir "Prise en main de la NetApp Console en mode standard" .
- Assurez-vous que les clusters vCenter source et de destination utilisent le même agent Console.
- Type d'agent de console requis :
  - **Reprise après sinistre sur site à site** : Installez l'agent Console local sur le site de reprise après sinistre. Grâce à cette méthode, une panne du site principal n'empêche pas le service de redémarrer vos ressources virtuelles sur le site de reprise après sinistre. Reportez-vous à "Installer et configurer l'agent de console sur site".

    La reprise après sinistre prend également en charge l'utilisation de plusieurs agents de console avec des configurations sur site. Dans ce scénario, les agents de la console dirigent les actions vers les vCenters et les clusters de baies ONTAP , et la source et la cible auraient chacune leur propre agent de console. L'utilisation de plusieurs agents Console est recommandée pour réduire la latence et améliorer le temps de récupération en cas de défaillance d'un agent Console ou d'un site.

  - **Sur site sur AWS** : installez l'agent de console pour AWS dans votre AWS VPC. Se référer à "Options d'installation de l'agent de console dans AWS" .

    Pour les connexions sur site vers sur site, utilisez l'agent de console sur site. Pour les connexions sur site vers AWS, utilisez l'agent de la console AWS, qui a accès au vCenter sur site source et au vCenter sur site de destination.

  - L'agent Console installé doit pouvoir accéder à toutes les instances de cluster VMware vCenter et aux hôtes ESXi gérés par ces clusters vCenter que la reprise après sinistre gérera.

- Toutes les baies ONTAP à gérer par NetApp Disaster Recovery doivent être ajoutées à tout système du projet NetApp Console qui sera utilisé pour gérer NetApp Disaster Recovery.

  Voir "Découvrez les clusters ONTAP sur site" .

- Pour plus d'informations sur la configuration d'un proxy intelligent pour NetApp Disaster Recovery, consultez"Configurez votre infrastructure pour la NetApp Disaster Recovery" .

Prérequis de charge de travail

Pour garantir la réussite des processus de cohérence des applications, appliquez ces conditions préalables :

- Assurez-vous que les outils VMware (ou les outils Open VM) sont en cours d'exécution sur les machines virtuelles qui seront protégées.
- Pour les machines virtuelles Windows exécutant Microsoft SQL Server, Oracle Database ou les deux, les bases de données doivent avoir leurs rédacteurs VSS activés.
- Les bases de données Oracle exécutées sur un système d'exploitation Linux doivent avoir l'authentification utilisateur du système d'exploitation activée pour le rôle SYSDBA de la base de données Oracle.

Plus d'informations

- Privilèges requis vCenter
- Conditions préalables pour Amazon EVS avec NetApp Disaster Recovery

Démarrage rapide pour la reprise NetApp Disaster Recovery

Voici un aperçu des étapes nécessaires pour démarrer avec NetApp Disaster Recovery. Les liens à l'intérieur de chaque étape vous mènent à une page qui fournit plus de détails.

Réviser les prérequis

"Assurez-vous que votre système répond à ces exigences" .

Configurer la NetApp Disaster Recovery

- "Mettre en place l'infrastructure du service" .
- "Configurer les licences" .

Quelle est la prochaine étape ?

Après avoir configuré le service, voici ce que vous pouvez faire ensuite.

- "Ajoutez vos sites vCenter à NetApp Disaster Recovery" .
- "Créez votre premier groupe de ressources" .
- "Créez votre premier plan de réplication" .
- "Répliquer des applications sur un autre site" .

- "Basculer les applications vers un site distant" .
- "Rétablir les applications vers le site source d'origine" .
- "Gérer les sites, les groupes de ressources et les plans de réplication" .
- "Surveiller les opérations de reprise après sinistre" .

Configurez votre infrastructure pour la NetApp Disaster Recovery

Pour utiliser NetApp Disaster Recovery, effectuez quelques étapes pour le configurer à la fois dans Amazon Web Services (AWS) et dans la NetApp Console.

Revoir"prérequis" pour vous assurer que votre système est prêt.

Vous pouvez utiliser NetApp Disaster Recovery dans les infrastructures suivantes :

- DR cloud hybride qui réplique un centre de données VMware plus ONTAP sur site vers une infrastructure DR AWS basée sur VMware Cloud on AWS et Amazon FSx for NetApp ONTAP.
- Cloud privé DR qui réplique un VMware plus ONTAP vCenter sur site vers un autre VMware plus ONTAP vCenter sur site.

Cloud hybride avec VMware Cloud et Amazon FSx for NetApp ONTAP

Cette méthode consiste en une infrastructure vCenter de production sur site utilisant des banques de données hébergées sur des volumes ONTAP FlexVol à l'aide d'un protocole NFS. Le site DR se compose d'une ou plusieurs instances VMware Cloud SDDC utilisant des banques de données hébergées sur des volumes FlexVol fournis par une ou plusieurs instances FSx for ONTAP à l'aide d'un protocole NFS.

Les sites de production et de reprise après sinistre sont reliés par une connexion sécurisée compatible AWS. Les types de connexion courants sont un VPN sécurisé (privé ou fourni par AWS), AWS Direct Connect ou d'autres méthodes d'interconnexion approuvées.

Pour la reprise après sinistre impliquant l'infrastructure cloud AWS, vous devez utiliser l'agent de console pour AWS. L'agent doit être installé dans le même VPC que l'instance FSx for ONTAP . Si des instances FSx for ONTAP supplémentaires ont été déployées dans d'autres VPC, le VPC hébergeant l'agent doit avoir accès aux autres VPC.

Zones de disponibilité AWS

AWS prend en charge le déploiement de solutions dans une ou plusieurs zones de disponibilité (AZ) au sein d'une région donnée. Disaster Recovery utilise deux services hébergés par AWS : VMware Cloud pour AWS et AWS FSx pour NetApp ONTAP.

- **VMware Cloud pour AWS** : prend en charge le déploiement dans un environnement SDDC à cluster extensible mono-AZ ou double-AZ. Disaster Recovery prend en charge un déploiement SDDC mono-AZ uniquement pour Amazon VMware Cloud for AWS.
- **AWS FSx pour NetApp ONTAP** : lorsqu'il est déployé dans une configuration double AZ, chaque volume appartient à un seul système FSx. Chaque volume appartient à un seul système FSx. Les données du volume sont mises en miroir sur le deuxième système FSx. Les systèmes FSx pour ONTAP peuvent être déployés dans des déploiements à une ou deux zones de disponibilité. Disaster Recovery prend en charge les déploiements FSx for FSx for ONTAP mono- et multi-AZ.

MEILLEURE PRATIQUE : Pour la configuration du site AWS DR, NetApp recommande d'utiliser des déploiements mono-AZ pour les instances VMware Cloud et AWS FSx for ONTAP . Étant donné qu'AWS est utilisé pour la reprise après sinistre, il n'y a aucun avantage à introduire plusieurs zones de disponibilité (AZ). Les multi-AZ peuvent augmenter les coûts et la complexité.

Sur site vers AWS

AWS fournit les méthodes suivantes pour connecter des centres de données privés au cloud AWS. Chaque solution a ses avantages et ses coûts.

- **AWS Direct Connect** : il s'agit d'une interconnexion cloud AWS située dans la même zone géographique que votre centre de données privé et fournie par un partenaire AWS. Cette solution fournit une connexion sécurisée et privée entre votre centre de données local et le cloud AWS sans avoir besoin d'une connexion Internet publique. Il s'agit de la méthode de connexion la plus directe et la plus efficace proposée par AWS.
- **AWS Internet Gateway** : cela fournit une connectivité publique entre les ressources cloud AWS et les ressources de calcul externes. Ce type de connexion est généralement utilisé pour fournir des offres de services à des clients externes, tels que le service HTTP/HTTPS où la sécurité n'est pas une exigence. Il n'y a aucun contrôle de qualité de service, de sécurité ou de garantie de connectivité. Pour cette raison, cette méthode de connexion n'est pas recommandée pour connecter un centre de données de production au cloud.
- **AWS Site-Site VPN** : Cette connexion de réseau privé virtuel peut être utilisée pour fournir des connexions d'accès sécurisées avec un fournisseur de services Internet public. Le VPN crypte et décrypte toutes les données circulant vers et depuis le cloud AWS. Les VPN peuvent être basés sur des logiciels ou du matériel. Pour les applications d'entreprise, le fournisseur d'accès Internet public (FAI) doit offrir des garanties de qualité de service pour garantir qu'une bande passante et une latence adéquates sont fournies pour la réplication DR.

MEILLEURE PRATIQUE : Pour la configuration du site AWS DR, NetApp recommande d'utiliser AWS Direct Connect. Cette solution offre les meilleures performances et sécurité pour les applications d'entreprise. Si ce n'est pas disponible, une connexion FAI publique haute performance ainsi qu'un VPN doivent être utilisés. Assurez-vous que le FAI propose des niveaux de service QoS commerciaux pour garantir des performances réseau adéquates.

Interconnexions VPC à VPC

AWS propose les types d'interconnexions VPC à VPC suivants. Chaque solution a ses avantages et ses coûts.

- **Peering VPC** : il s'agit d'une connexion privée entre deux VPC. C'est la méthode de connexion la plus directe et la plus efficace proposée par AWS. Le peering VPC peut être utilisé pour connecter des VPC dans la même région AWS ou dans des régions AWS différentes.
- **AWS Internet Gateway** : elle est généralement utilisée pour fournir des connexions entre les ressources AWS VPC et les ressources et points de terminaison non AWS. Tout le trafic suit un chemin en « épingle à cheveux » où le trafic VPC destiné à un autre VPC sort de l'infrastructure AWS via la passerelle Internet et revient à l'infrastructure AWS via la même passerelle ou une passerelle différente. Il ne s'agit pas d'un type de connexion VPC adapté aux solutions VMware d'entreprise.
- **AWS Transit Gateway** : il s'agit d'un type de connexion centralisé basé sur un routeur qui permet à chaque VPC de se connecter à une passerelle centrale unique, qui agit comme un hub central pour tout le trafic VPC à VPC. Cela peut également être connecté à votre solution VPN pour permettre aux ressources du centre de données sur site d'accéder aux ressources hébergées par AWS VPC. Ce type de connexion nécessite généralement un coût supplémentaire à mettre en œuvre.

MEILLEURE PRATIQUE : Pour les solutions DR impliquant VMware Cloud et un seul FSx pour ONTAP VPC, NetApp recommande d'utiliser la connexion homologue VPC. Si plusieurs VPC FSx pour ONTAP sont

déployés, nous vous recommandons d'utiliser une passerelle de transit AWS pour réduire la charge de gestion de plusieurs connexions homologues VPC.

Préparez-vous à la protection sur site vers le cloud avec AWS

Pour configurer NetApp Disaster Recovery pour la protection sur site vers le cloud à l'aide d'AWS, vous devez configurer les éléments suivants :

- Configurer AWS FSx pour NetApp ONTAP
- Configurer VMware Cloud sur AWS SDDC

Configurer AWS FSx pour NetApp ONTAP

- Créez un système de fichiers Amazon FSx for NetApp ONTAP .
  - Provisionner et configurer FSx pour ONTAP. Amazon FSx for NetApp ONTAP est un service entièrement géré qui fournit un stockage de fichiers hautement fiable, évolutif, performant et riche en fonctionnalités, basé sur le système de fichiers NetApp ONTAP .
  - Suivez les étapes dans "Rapport technique 4938 : Monter Amazon FSx ONTAP comme banque de données NFS avec VMware Cloud sur AWS" et "Démarrage rapide d' Amazon FSx for NetApp ONTAP" provisionner et configurer FSx pour ONTAP.
- Ajoutez Amazon FSx pour ONTAP au système et ajoutez les informations d'identification AWS pour FSx pour ONTAP.
- Créez ou vérifiez votre destination ONTAP SVM dans l'instance AWS FSx pour ONTAP .
- Configurez la réplication entre votre cluster ONTAP source sur site et votre instance FSx for ONTAP dans la NetApp Console.

Se référer à "comment configurer un système FSx pour ONTAP" pour les étapes détaillées.

Configurer VMware Cloud sur AWS SDDC

"VMware Cloud sur AWS"offre une expérience cloud native pour les charges de travail basées sur VMware dans l'écosystème AWS. Chaque centre de données défini par logiciel VMware (SDDC) s'exécute dans un Amazon Virtual Private Cloud (VPC) et fournit une pile VMware complète (y compris vCenter Server), une mise en réseau définie par logiciel NSX-T, un stockage défini par logiciel vSAN et un ou plusieurs hôtes ESXi qui fournissent des ressources de calcul et de stockage aux charges de travail.

Pour configurer un environnement VMware Cloud sur AWS, suivez les étapes décrites dans "Déployer et configurer l'environnement de virtualisation sur AWS" Un groupe de veilleuses peut également être utilisé à des fins de reprise après sinistre.

Cloud privé

Vous pouvez utiliser NetApp Disaster Recovery pour protéger les machines virtuelles VMware hébergées sur un ou plusieurs clusters vCenter en répliquant les banques de données de machines virtuelles vers un autre cluster vCenter, soit dans le même centre de données privé, soit vers un centre de données privé ou colocalisé distant.

Pour les situations sur site vers sur site, installez l'agent de console sur l'un des sites physiques.

La récupération après sinistre prend en charge la réplication de site à site à l'aide d'Ethernet et de TCP/IP. Assurez-vous qu'une bande passante adéquate est disponible pour prendre en charge les taux de modification des données sur les machines virtuelles du site de production afin que toutes les modifications puissent être

répliquées sur le site DR dans le délai de l'objectif de point de récupération (RPO).

Préparez-vous à une protection sur site vers sur site

Assurez-vous que les exigences suivantes sont remplies avant de configurer NetApp Disaster Recovery pour la protection sur site vers sur site :

- Stockage de l'ONTAP
  - Assurez-vous que vous disposez des informations d'identification ONTAP .
  - Créez ou vérifiez votre site de reprise après sinistre.
  - Créez ou vérifiez votre destination ONTAP SVM.
  - Assurez-vous que vos SVM ONTAP source et de destination sont appairés.
- clusters vCenter
  - Assurez-vous que les machines virtuelles que vous souhaitez protéger sont hébergées sur des banques de données NFS (à l'aide de volumes ONTAP NFS) ou des banques de données VMFS (à l'aide de LUN iSCSI NetApp).
  - Revoir"privilèges vCenter" requis pour la NetApp Disaster Recovery.
  - Créez un compte d'utilisateur de récupération après sinistre (pas le compte d'administrateur vCenter par défaut) et attribuez les privilèges vCenter au compte.

Prise en charge de proxy intelligent

L'agent de NetApp Console prend en charge le proxy intelligent. Le proxy intelligent est un moyen léger, sécurisé et efficace de connecter votre environnement local à la NetApp Console. Il fournit une connexion sécurisée entre votre système et le service Console sans nécessiter de VPN ou d'accès Internet direct. Cette implémentation de proxy optimisée décharge le trafic API au sein du réseau local.

Lorsqu'un proxy est configuré, NetApp Disaster Recovery tente de communiquer directement avec VMware ou ONTAP et utilise le proxy configuré si la communication directe échoue.

L'implémentation du proxy NetApp Disaster Recovery nécessite une communication sur le port 443 entre l'agent de console et tous les serveurs vCenter et baies ONTAP utilisant un protocole HTTPS. L'agent NetApp Disaster Recovery au sein de l'agent de console communique directement avec VMware vSphere, VC ou ONTAP lors de l'exécution de toute action.

Pour plus d'informations sur la configuration générale du proxy dans la NetApp Console, consultez "Configurer l'agent de console pour utiliser un serveur proxy" .

Accéder à la NetApp Disaster Recovery

Vous utilisez la NetApp Console pour vous connecter au service NetApp Disaster Recovery .

Pour vous connecter, vous pouvez utiliser vos informations d'identification du site de support NetApp ou vous inscrire pour une connexion au cloud NetApp à l'aide de votre e-mail et d'un mot de passe. "En savoir plus sur la connexion" .

Des tâches spécifiques nécessitent des rôles d'utilisateur spécifiques. "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".

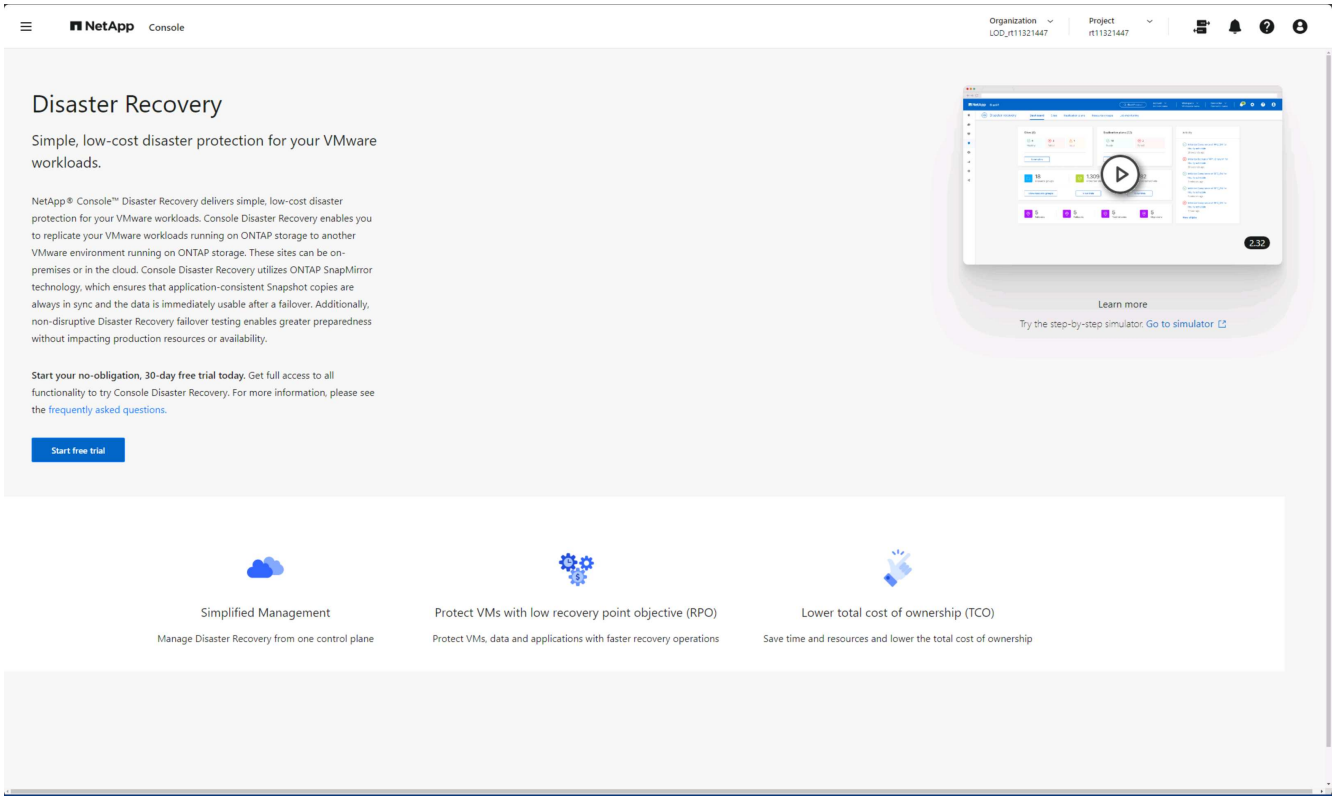
Étapes

1. Ouvrez un navigateur Web et accédez à la "NetApp Console" .

   La page de connexion à la NetApp Console s'affiche.

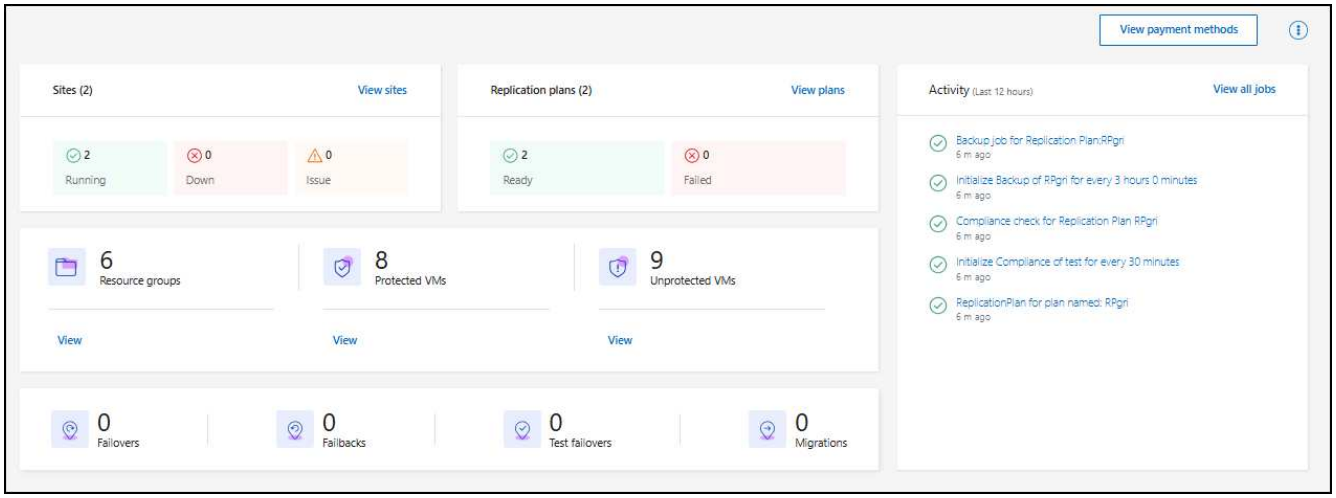
2. Connectez-vous à la NetApp Console.
3. Dans la navigation de gauche de la NetApp Console , sélectionnez **Protection** > **Reprise après sinistre**.

   Si c'est la première fois que vous vous connectez à ce service, la page de destination apparaît et vous pouvez vous inscrire pour un essai gratuit.



Sinon, le tableau de bord de NetApp Disaster Recovery s'affiche.

- Si vous n'avez pas encore ajouté d'agent de NetApp Console , vous devrez en ajouter un. Pour ajouter l'agent, reportez-vous à "En savoir plus sur les agents de console" .
- Si vous êtes un utilisateur de la NetApp Console avec un agent existant, lorsque vous sélectionnez « Récupération après sinistre », un message s'affiche concernant l'inscription.
- Si vous utilisez déjà le service, lorsque vous sélectionnez « Récupération après sinistre », le tableau de bord apparaît.



Configurer les licences pour NetApp Disaster Recovery

Avec NetApp Disaster Recovery, vous pouvez utiliser différents plans de licence, notamment un essai gratuit, un abonnement à la carte ou apporter votre propre licence.

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 pour tous les services".

Options de licence Vous pouvez utiliser les options de licence suivantes :

- Inscrivez-vous pour un essai gratuit de 30 jours.
- Achetez un abonnement à la carte (PAYGO) à Amazon Web Services (AWS) Marketplace ou à Microsoft Azure Marketplace.
- Apportez votre propre licence (BYOL), qui est un fichier de licence NetApp (NLF) que vous obtenez auprès de votre représentant commercial NetApp . Vous pouvez utiliser le numéro de série de la licence pour activer le BYOL dans la NetApp Console.

> Les frais de NetApp Disaster Recovery sont basés sur la capacité utilisée des banques de données sur le site source lorsqu'il existe au moins une machine virtuelle dotée d'un plan de réplication. La capacité d'une banque de données basculée n'est pas incluse dans la capacité allouée. Pour un BYOL, si les données dépassent la capacité autorisée, les opérations dans le service sont limitées jusqu'à ce que vous obteniez une licence de capacité supplémentaire ou que vous mettiez à niveau la licence dans la NetApp Console.

"En savoir plus sur les abonnements".

Une fois l'essai gratuit terminé ou la licence expirée, vous pouvez toujours effectuer les opérations suivantes dans le service :

- Affichez n'importe quelle ressource, telle qu'une charge de travail ou un plan de réplication.
- Supprimez toute ressource, telle qu'une charge de travail ou un plan de réplication.
- Exécutez toutes les opérations planifiées qui ont été créées pendant la période d'essai ou sous la licence.

Essayez-le en utilisant un essai gratuit de 30 jours

Vous pouvez essayer NetApp Disaster Recovery en utilisant un essai gratuit de 30 jours.

Aucune limite de capacité n'est appliquée pendant le procès.

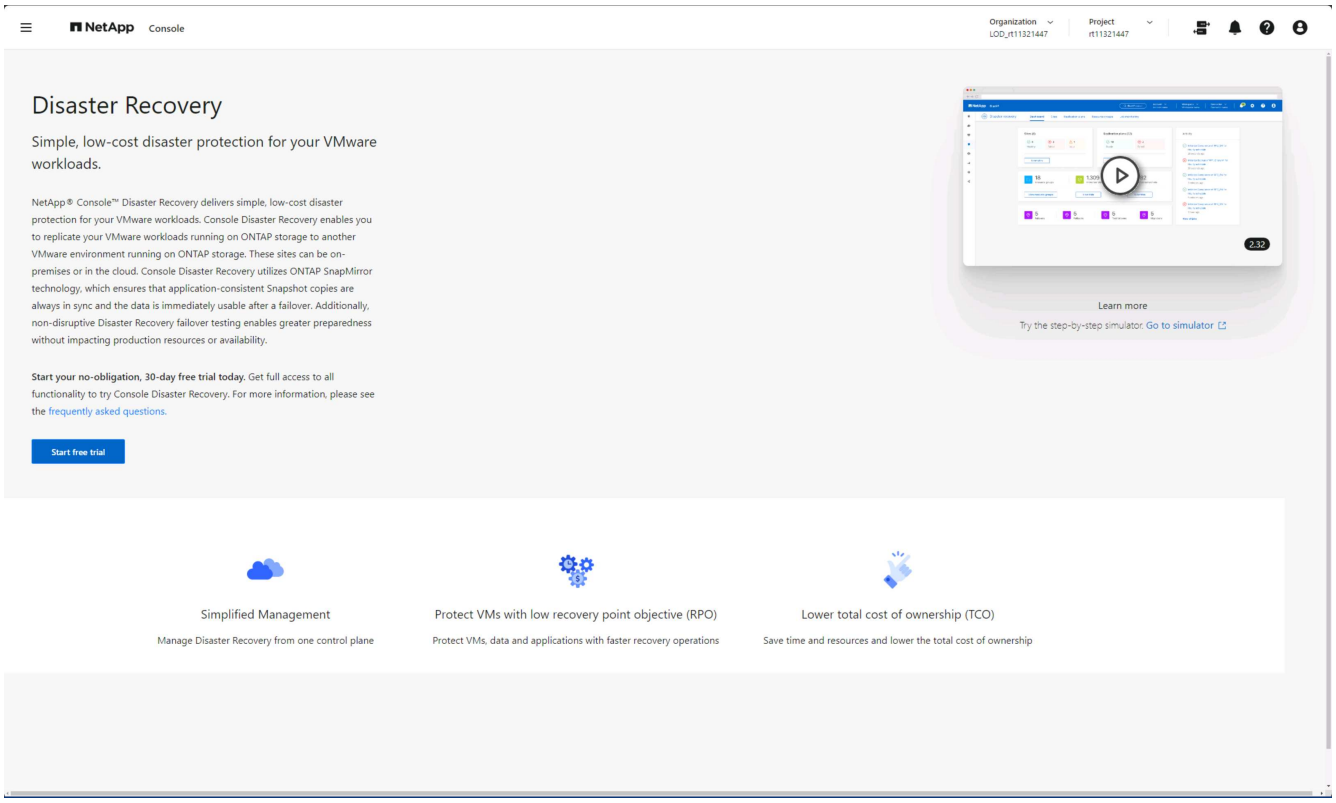
Pour continuer après l'essai, vous devrez acheter une licence BYOL ou un abonnement AWS PAYGO. Vous pouvez obtenir une licence à tout moment et vous ne serez pas facturé avant la fin de la période d'essai.

Pendant la période d'essai, vous bénéficiez de toutes les fonctionnalités.

Étapes

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

   Si c'est la première fois que vous vous connectez à ce service, la page de destination apparaît.



3. Si vous n'avez pas déjà ajouté un agent de console pour d'autres services, ajoutez-en un.

   Pour ajouter un agent Console, reportez-vous à "En savoir plus sur les agents de console" .

4. Une fois l'agent configuré, dans la page d'accueil de NetApp Disaster Recovery , le bouton permettant d'ajouter l'agent se transforme en bouton permettant de démarrer un essai gratuit. Sélectionnez **Démarrer l'essai gratuit**.
5. Commencez par ajouter des vCenters.

   Pour plus de détails, consultez la section "Ajouter des sites vCenter" .

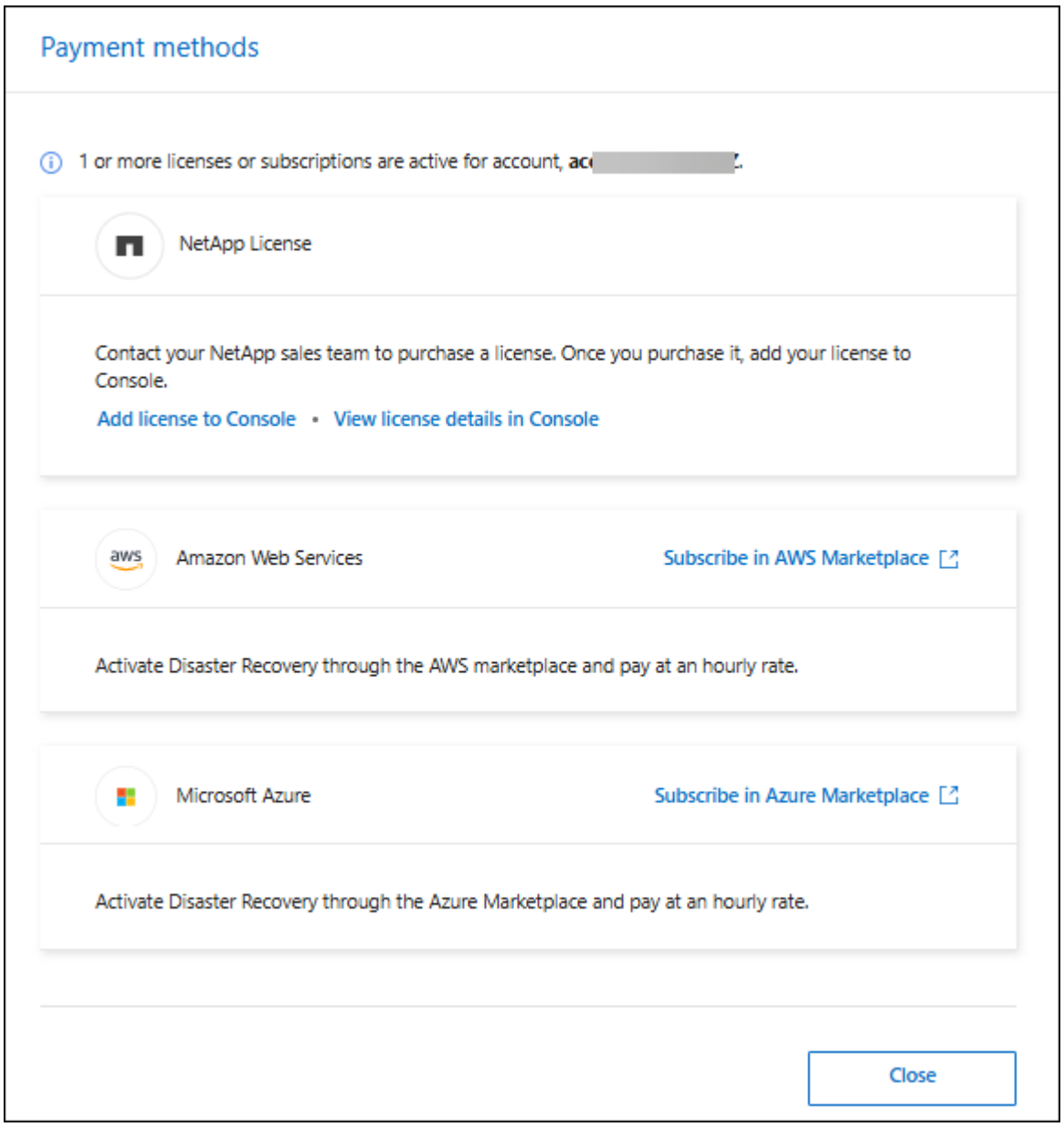
Une fois l’essai terminé, abonnez-vous via l’une des places de marché

Une fois l’essai gratuit terminé, vous pouvez acheter une licence auprès de NetApp ou vous abonner via AWS Marketplace ou Microsoft Azure Marketplace. Cette procédure fournit un aperçu de haut niveau sur la manière de s’abonner directement sur l’une des places de marché.

Étapes

1. Dans NetApp Disaster Recovery, vous voyez un message indiquant que la version d’essai gratuite expire. Dans le message, sélectionnez **S’abonner ou acheter une licence**.

   Ou, à partir du , sélectionnez **Afficher les modes de paiement**.



2. Sélectionnez **S’abonner sur AWS Marketplace** ou **S’abonner sur Azure Marketplace**.
3. Utilisez AWS Marketplace ou Microsoft Azure Marketplace pour vous abonner à * NetApp Disaster Recovery*.
4. Lorsque vous revenez à NetApp Disaster Recovery, un message indique que vous êtes abonné.

Vous pouvez afficher les détails de l'abonnement sur la page d'abonnement de la NetApp Console . "En savoir plus sur la gestion des abonnements avec la NetApp Console".

Une fois la période d'essai terminée, achetez une licence BYOL via NetApp

Une fois la période d'essai terminée, vous pouvez acheter une licence auprès de votre représentant commercial NetApp .

Si vous apportez votre propre licence (BYOL), la configuration comprend l'achat de la licence, l'obtention du fichier de licence NetApp (NLF) et l'ajout de la licence à la NetApp Console.

Ajoutez la licence à la NetApp Console* Après avoir acheté votre licence NetApp Disaster Recovery auprès d'un représentant commercial NetApp , vous pouvez gérer la licence dans la console.

"En savoir plus sur l'ajout de licences avec la NetApp Console".

Mettez à jour votre licence lorsqu'elle expire

Si votre durée de licence approche de la date d'expiration ou si votre capacité sous licence atteint la limite, vous en serez informé dans l'interface utilisateur de NetApp Disaster Recovery . Vous pouvez mettre à jour votre licence NetApp Disaster Recovery avant son expiration afin d'éviter toute interruption de votre capacité à accéder à vos données numérisées.

Ce message apparaît également dans la NetApp Console et dans "Notifications" .

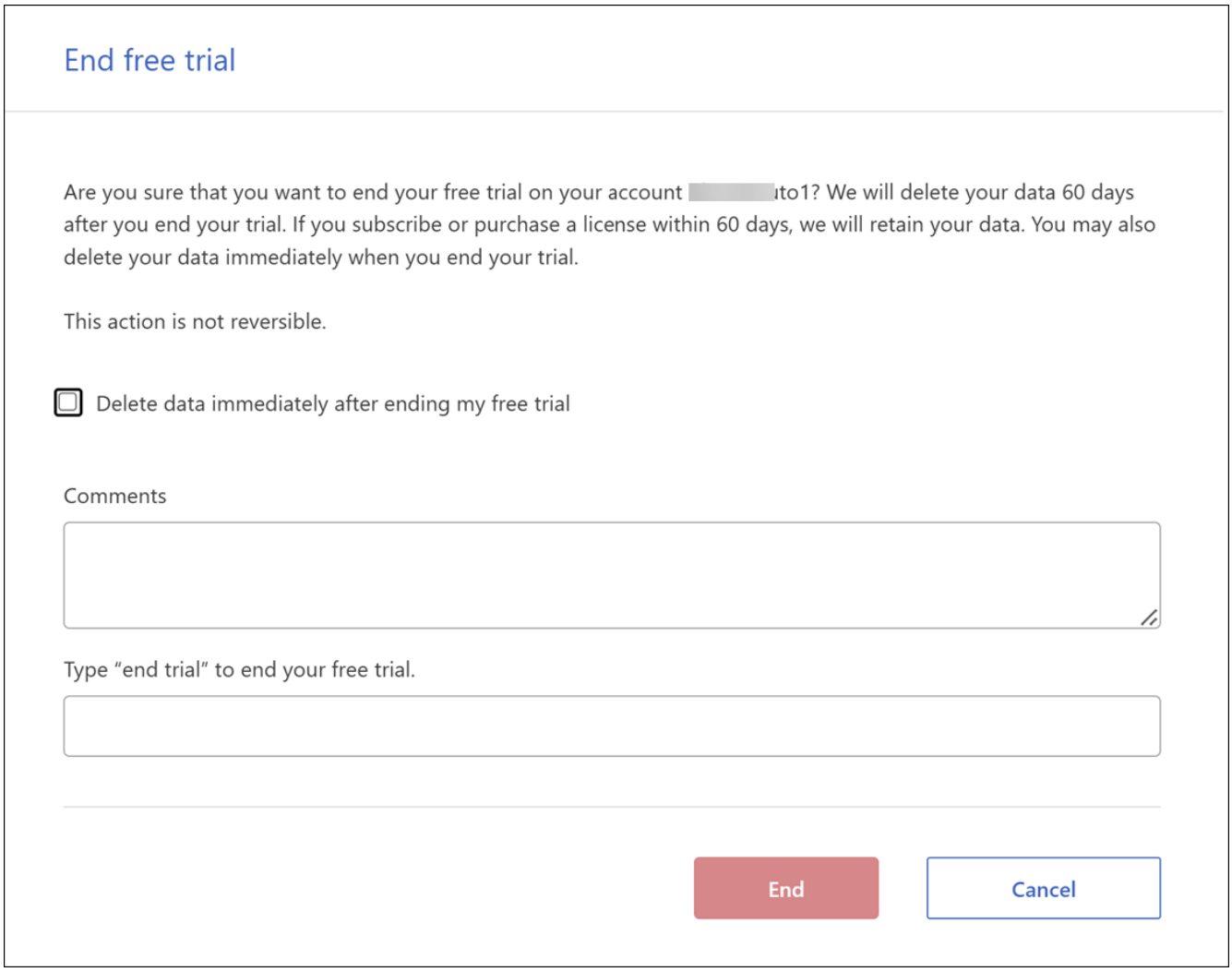
"En savoir plus sur la mise à jour des licences avec la NetApp Console".

Mettre fin à l'essai gratuit

Vous pouvez arrêter l'essai gratuit à tout moment ou attendre son expiration.

Étapes

1. Dans NetApp Disaster Recovery, sélectionnez **Essai gratuit - Afficher les détails**.
2. Dans les détails déroulants, sélectionnez **Terminer l'essai gratuit**.



3. Si vous souhaitez supprimer toutes les données, cochez **Supprimer les données immédiatement après la fin de mon essai gratuit**.

   Cela supprime toutes les planifications, plans de réplication, groupes de ressources, vCenters et sites. Les données d'audit, les journaux d'opérations et l'historique des tâches sont conservés jusqu'à la fin de la durée de vie du produit.

   > Si vous mettez fin à l'essai gratuit, n'avez pas demandé la suppression de données et n'achetez pas de licence ou d'abonnement, NetApp Disaster Recovery supprime toutes vos données 60 jours après la fin de l'essai gratuit.

4. Tapez « fin de l'essai » dans la zone de texte.
5. Sélectionnez **Fin**.

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

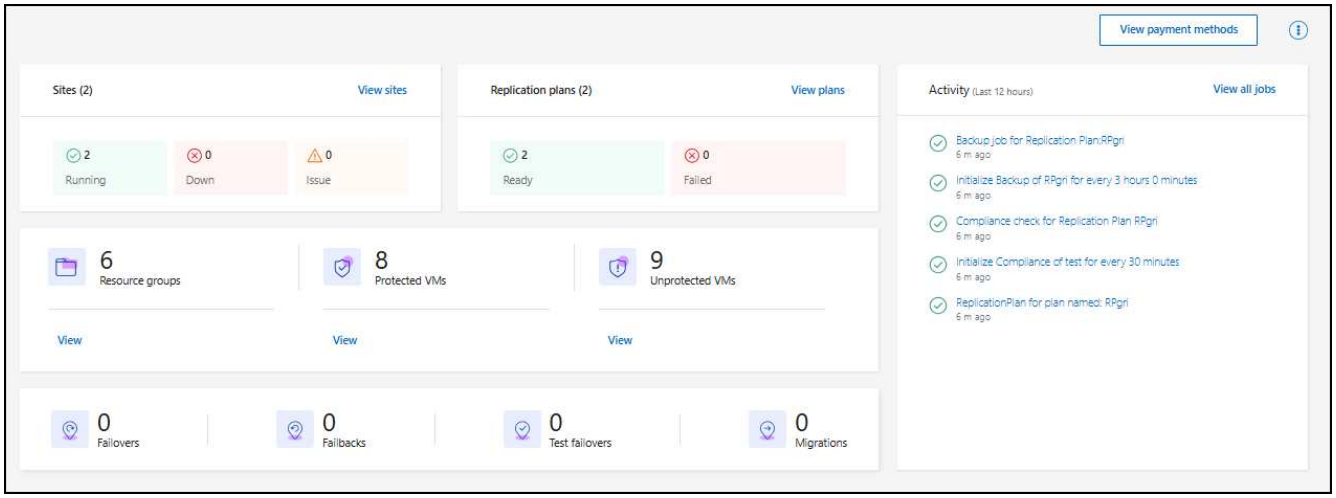
À l'aide du tableau de bord de NetApp Disaster Recovery , vous pouvez déterminer l'état de vos sites de reprise après sinistre et vos plans de réplication. Vous pouvez rapidement déterminer quels sites et quels plans sont sains, déconnectés ou dégradés.

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

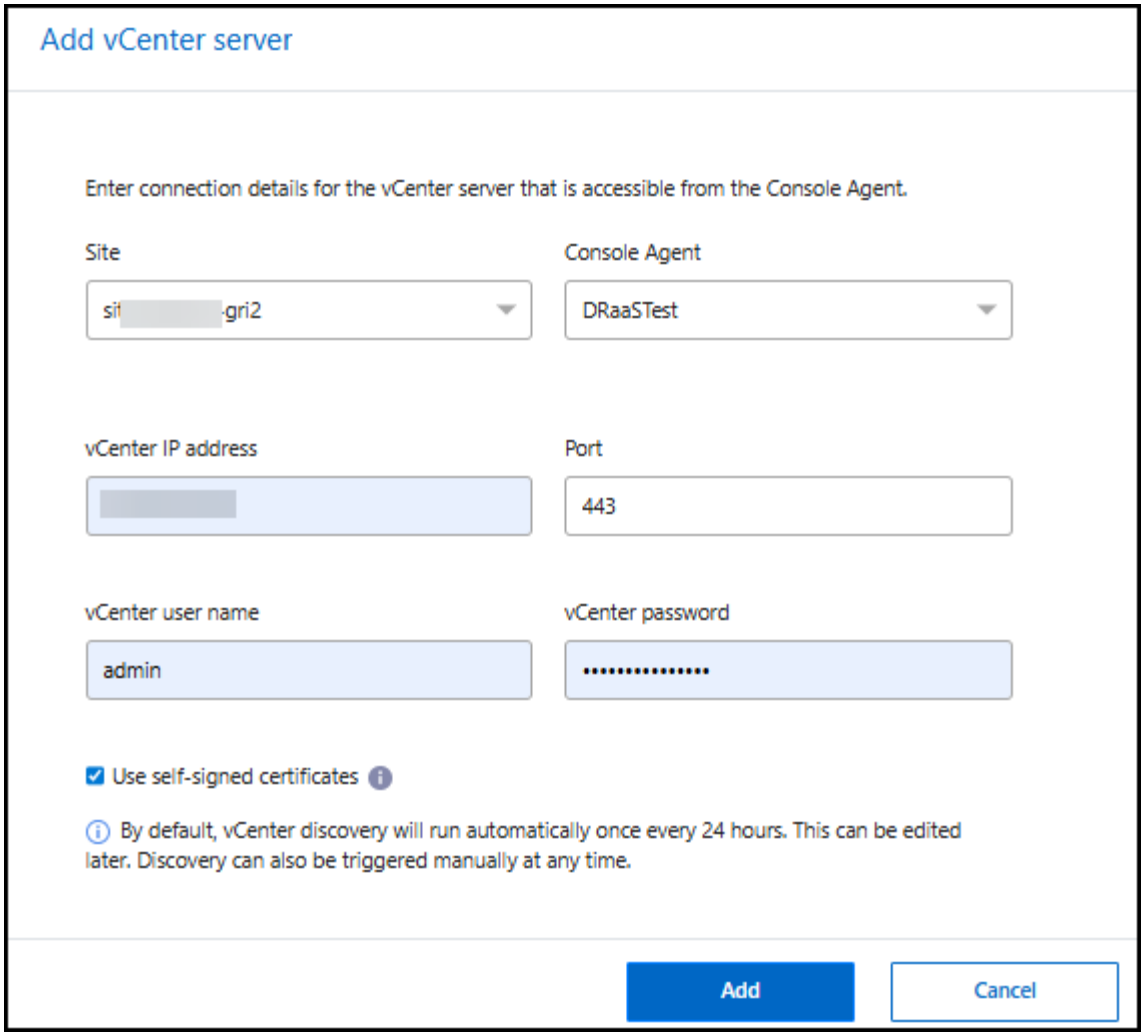
1. Connectez-vous à la "NetApp Console" .
2. Dans la navigation de gauche de la NetApp Console , sélectionnez **Protection** > **Reprise après sinistre**.

   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**.



- 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.

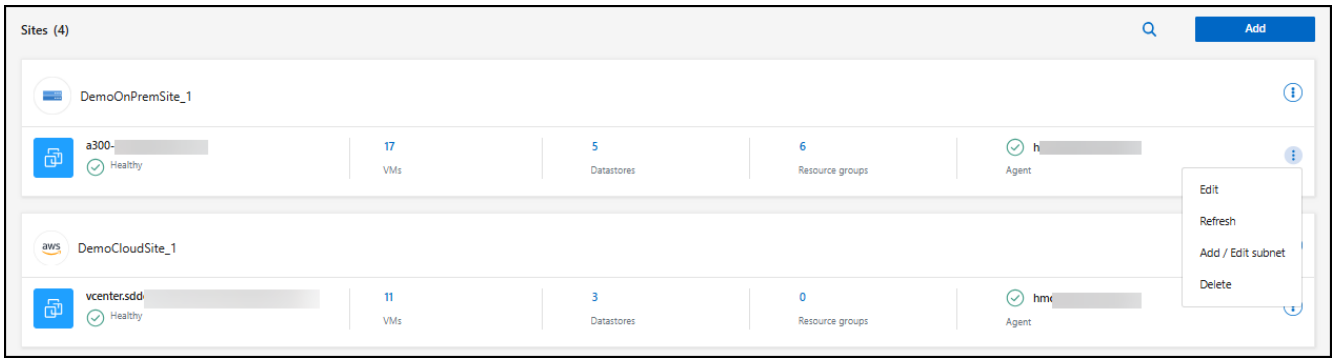
En résumé, l'adresse de l'hôte reste la même, tandis que l'adresse réseau est remplacée par celle configurée dans le mappage de sous-réseau du site. Cela vous permet de gérer plus facilement la réaffectation des adresses IP lors du basculement, en particulier si vous avez des centaines de réseaux et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

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

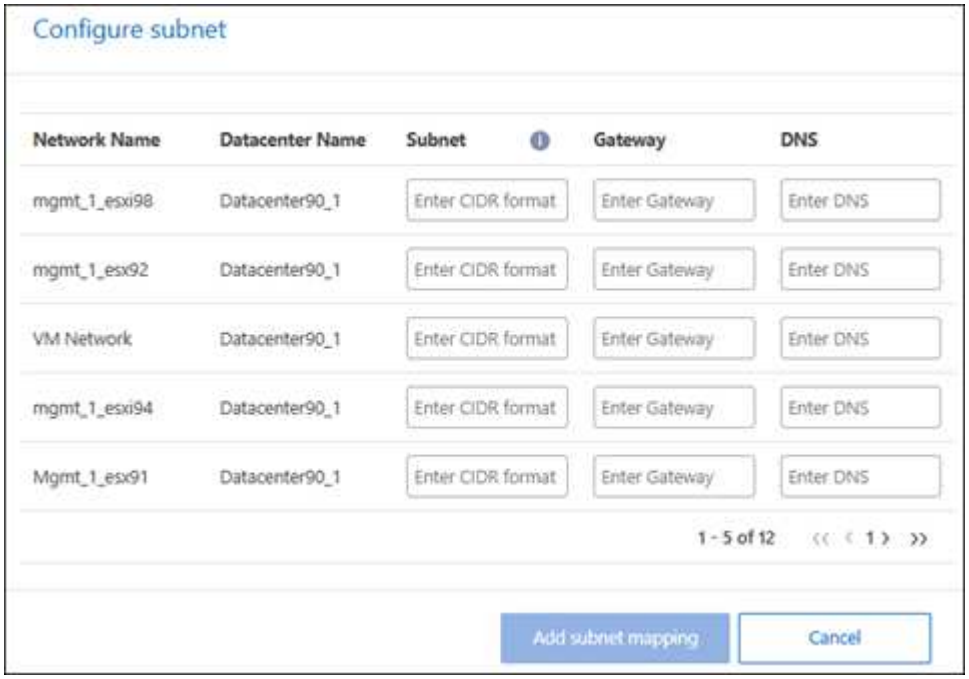
- Tout d'abord, ajoutez le mappage de sous-réseau pour chaque site vCenter.
- Deuxièmement, dans le plan de réplication, indiquez que vous souhaitez utiliser le mappage de sous-réseau dans l'onglet Machines virtuelles et le champ IP cible.

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 :



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

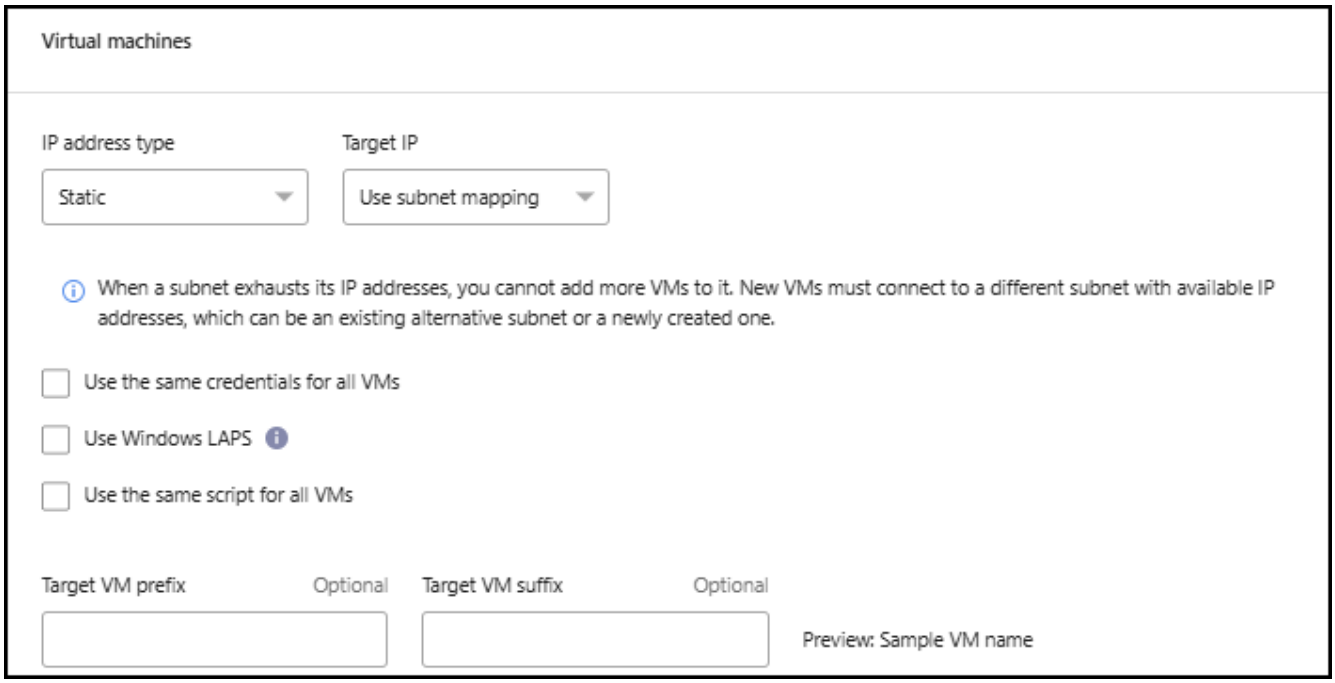
Lorsque vous créez un plan de réplication, vous pouvez sélectionner le mappage de sous-réseau pour le plan de réplication.

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**.



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

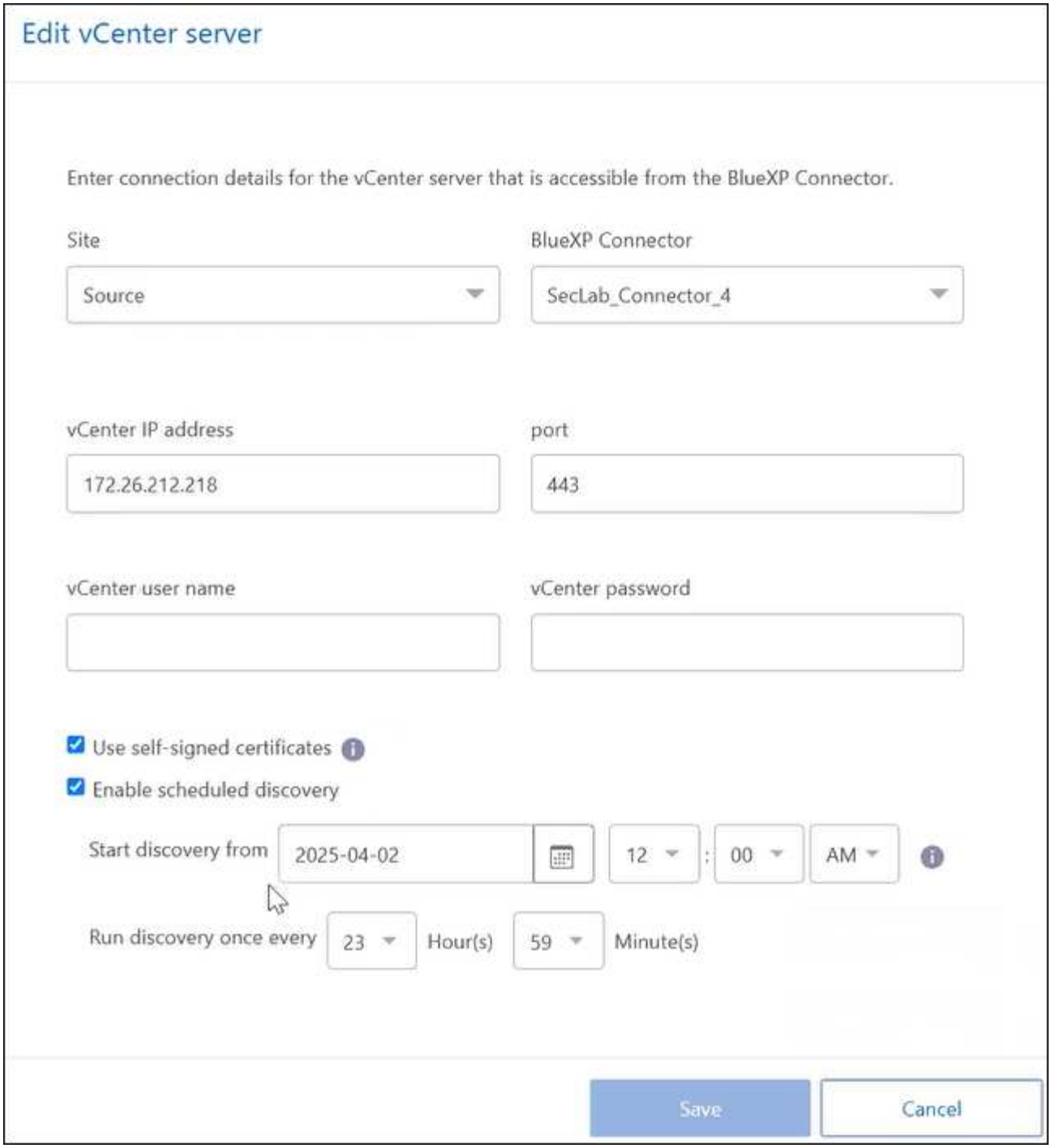
découverte pour qu'elle s'exécute toutes les 23 heures et 59 minutes. Si vous disposez d'un petit nombre de machines virtuelles, vous pouvez définir la planification de découverte pour qu'elle s'exécute toutes les 12 heures.

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.



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 **même SVM**	• Groupe de cohérence ONTAP créé • Instantanés du groupe de cohérence pris • Réplication SnapMirror à l'échelle du volume effectuée
Plusieurs magasins de données - Volumes FlexVol dans **plusieurs SVM**	• API ONTAP : `cg_start` . 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. • API ONTAP : `cg_end` . Reprend les E/S sur tous les volumes et active la réplication SnapMirror au niveau du volume après la prise des snapshots.

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

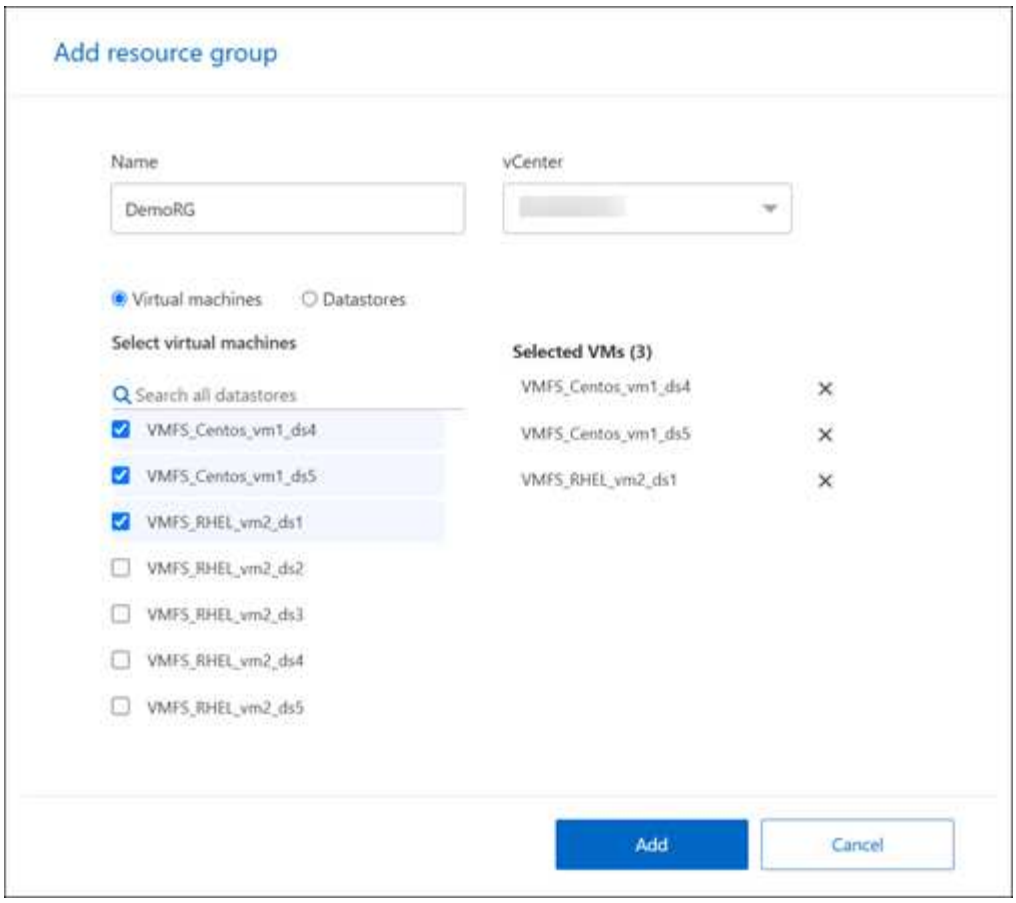
source à partir du processus de basculement, ce qui entraînera l'échec des machines virtuelles non protégées sur le site source. De plus, NetApp Disaster Recovery ne démarrera pas ces machines virtuelles non protégées sur le site vCenter de basculement.

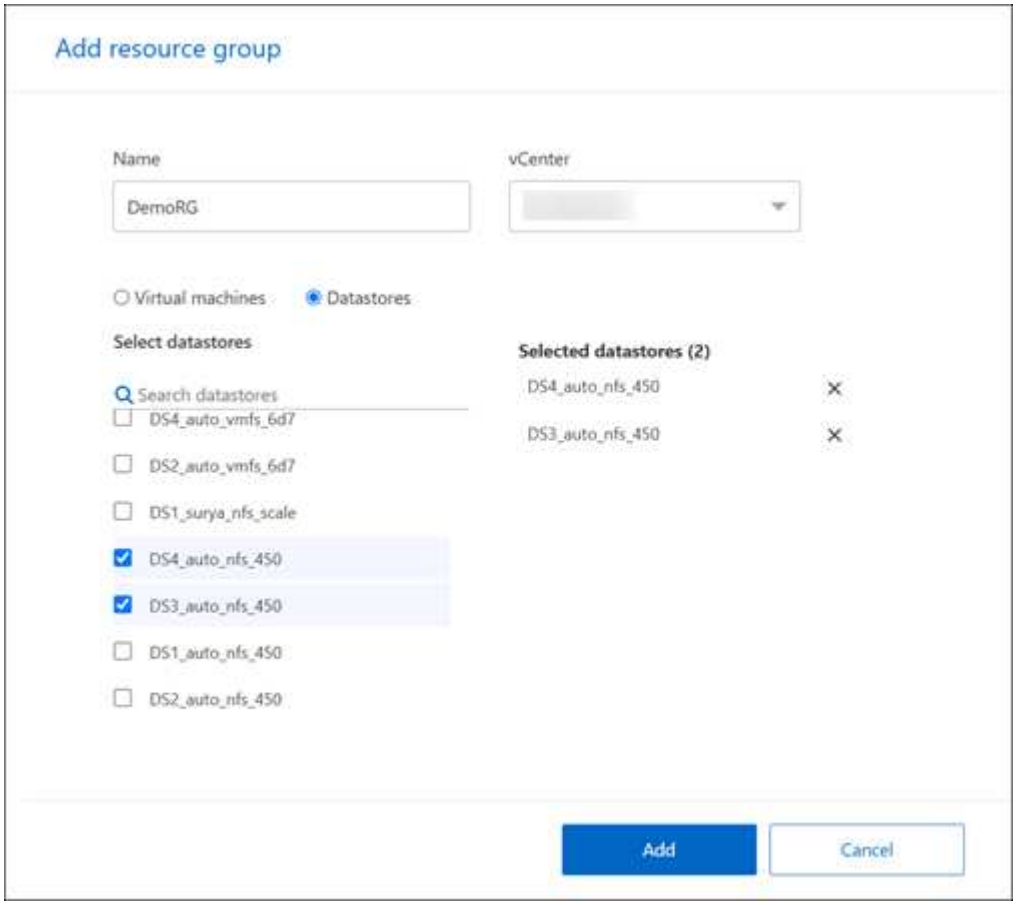
- Pour qu'une machine virtuelle soit protégée, elle doit être incluse dans un groupe de ressources.

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 **Groupes 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
DemoRG
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
Cancel


Add resource group
Name
DemoRG
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
Add
Cancel

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 :

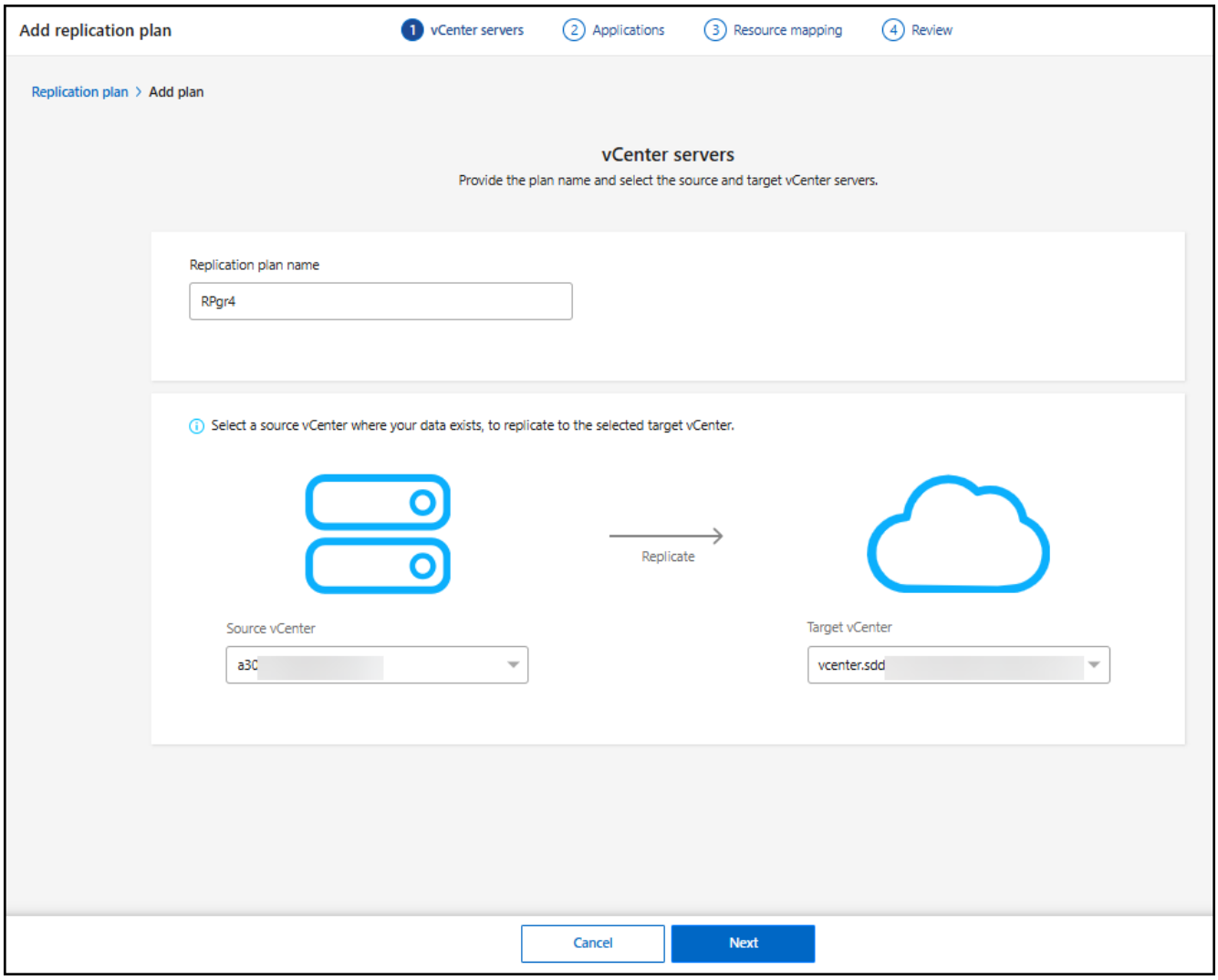
- Utilisez les mêmes informations d'identification pour toutes les machines virtuelles du plan.
- Utilisez le même script pour toutes les machines virtuelles du plan.
- Utilisez le même sous-réseau, le même DNS et la même passerelle pour toutes les machines virtuelles du plan.

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**.



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.

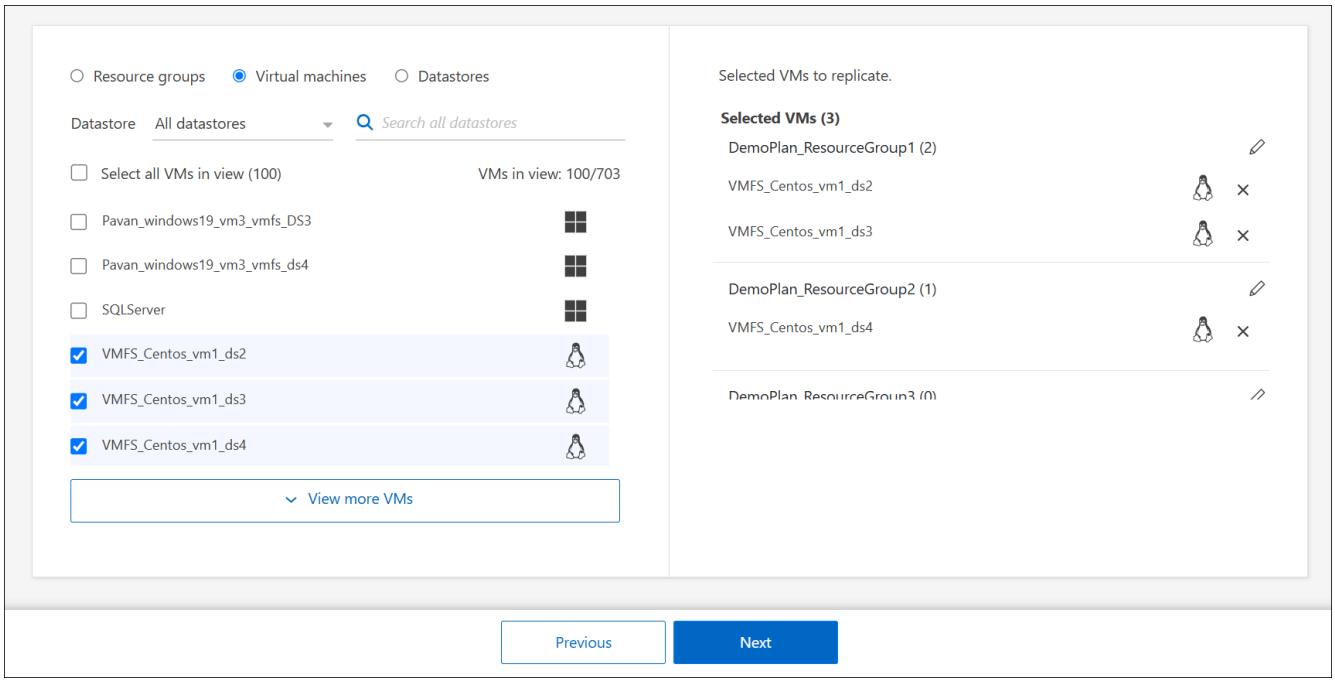
Créez un ensemble de mappages dédié et distinct pour vos tests de basculement afin d'empêcher que les machines virtuelles soient connectées aux réseaux de production en utilisant les mêmes adresses IP.

Étapes

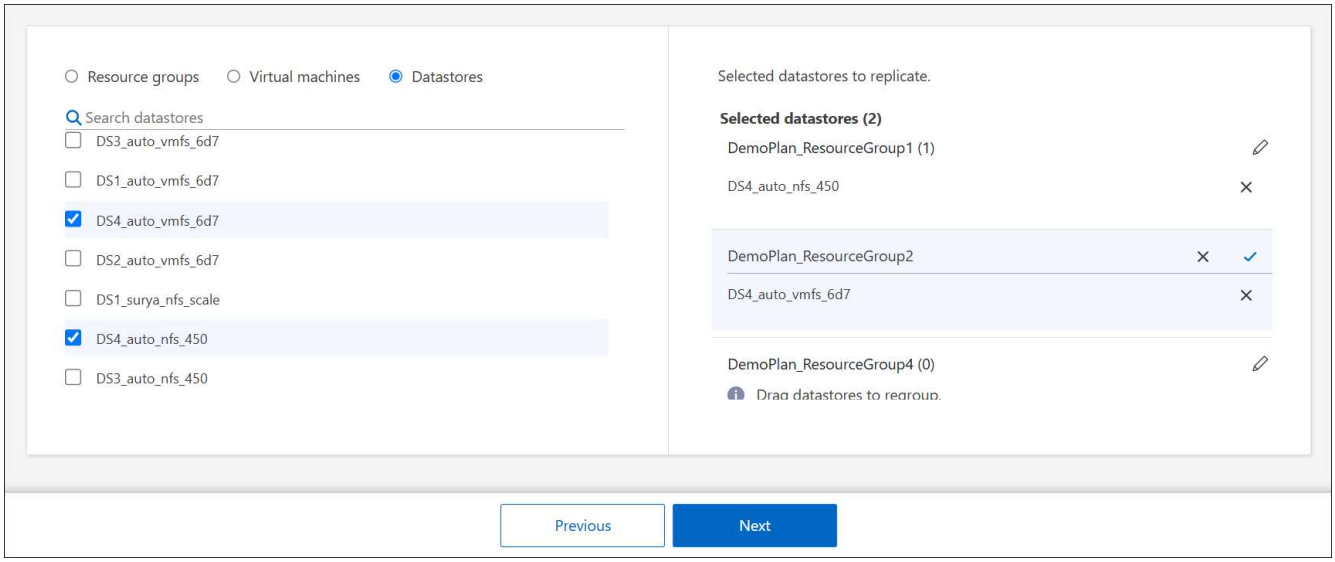
1. Sélectionnez **Machines virtuelles** ou **Magasins de données**.
2. Recherchez éventuellement une machine virtuelle ou un magasin de données spécifique par nom.
3. Sur le côté gauche de la page Applications, sélectionnez les machines virtuelles ou les banques de données que vous souhaitez protéger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

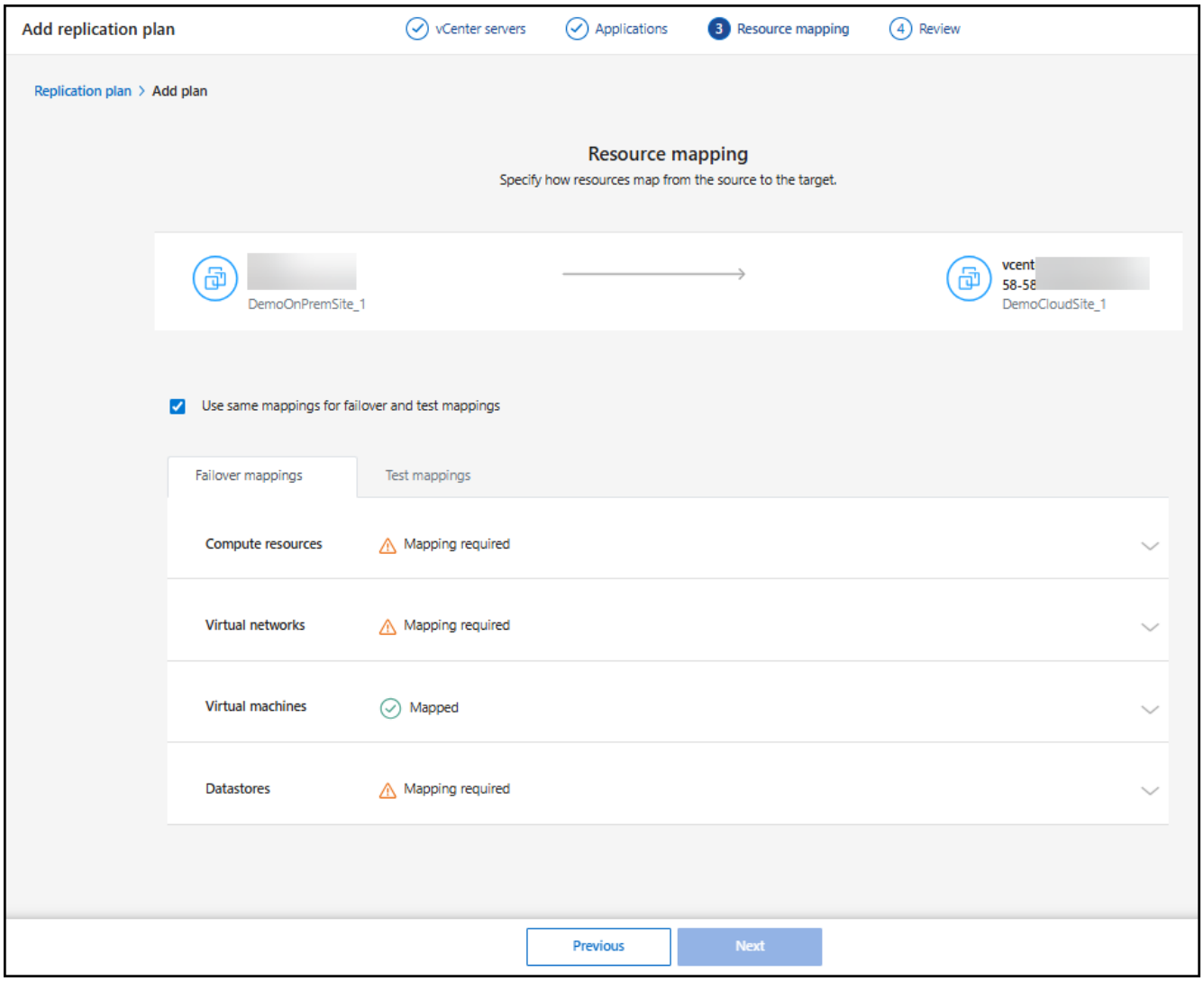
Si vous prévoyez d'effectuer des tests de basculement dans le cadre de votre plan de reprise après sinistre, vous devez fournir un ensemble de mappages de basculement de test pour garantir que les machines virtuelles démarrées pendant le test de basculement n'interfèrent pas avec les machines virtuelles 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.



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 souhaiterez 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.

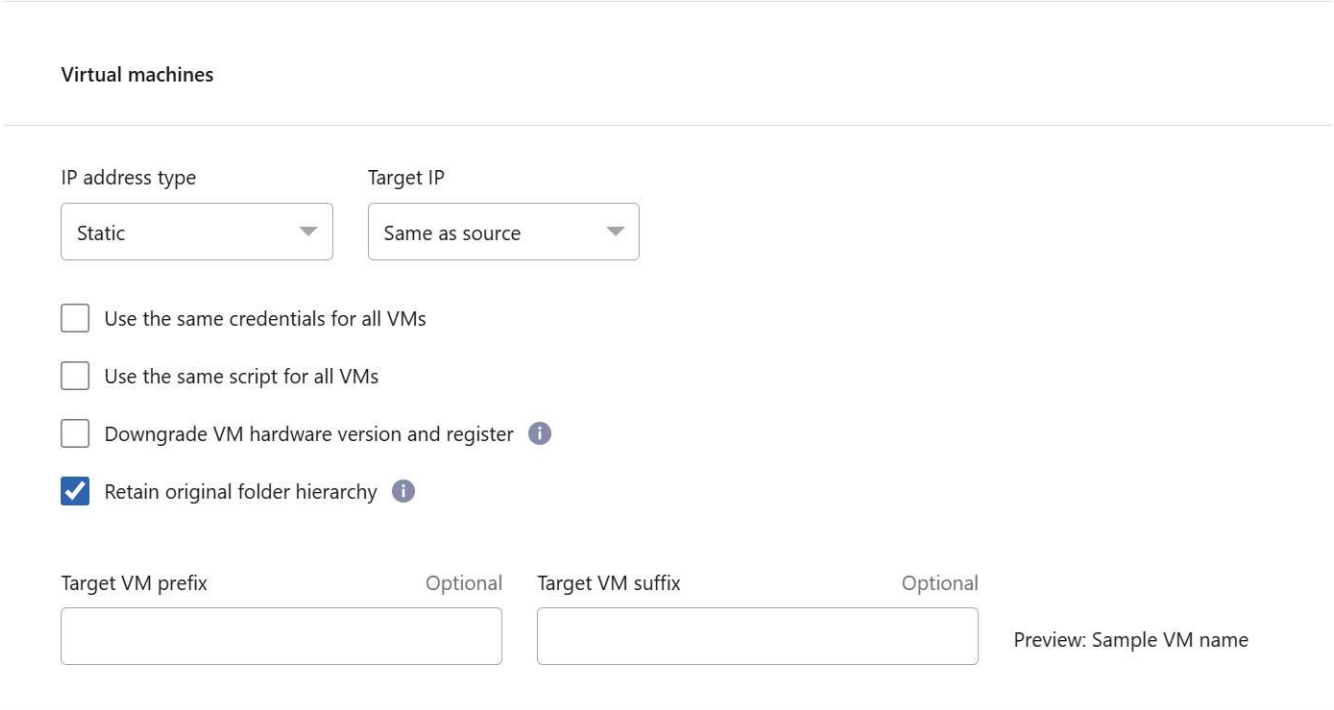
Au niveau le plus basique (et par défaut), les paramètres utilisent simplement les mêmes paramètres réseau TCP/IP pour chaque machine virtuelle sur le site de destination que ceux utilisés sur le site source. Cela nécessite que vous configuriez les mêmes paramètres TCP/IP sur les réseaux virtuels source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



- **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.

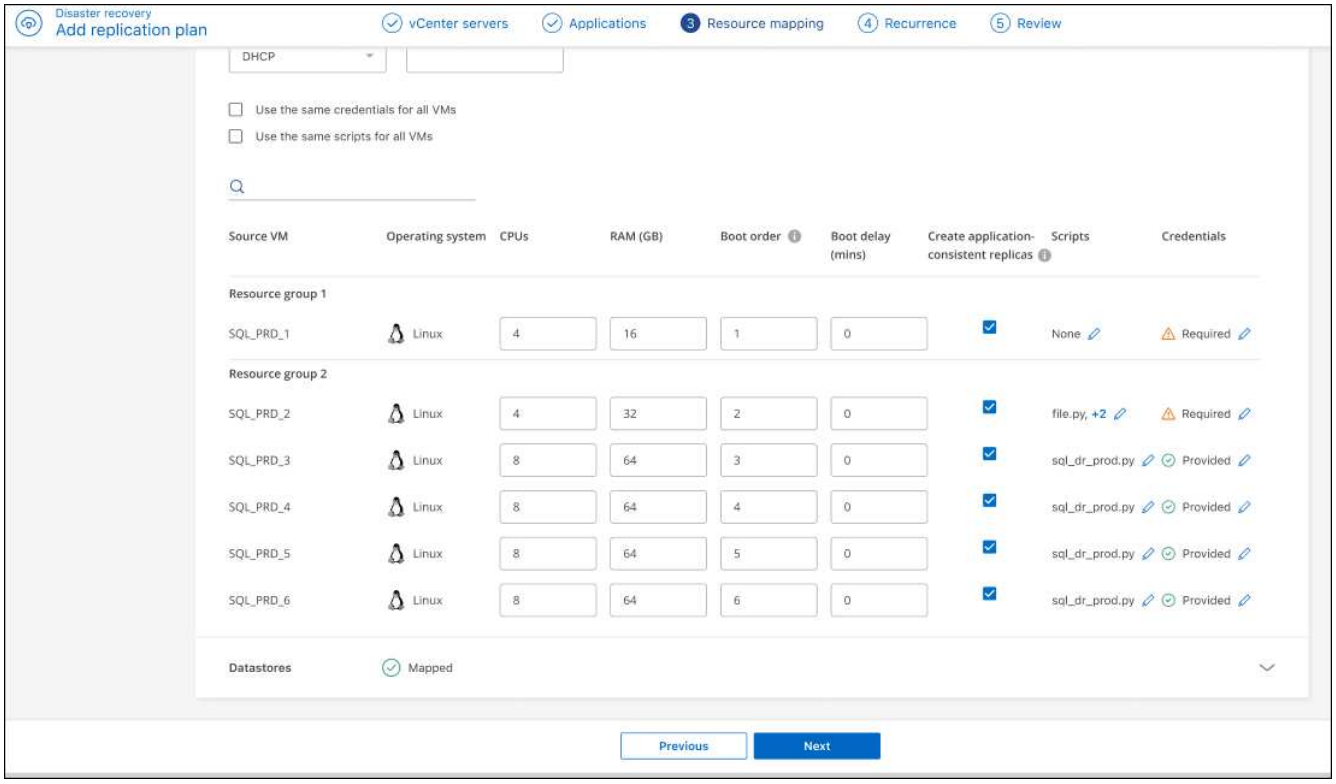
  Décochez cette case pour ignorer l'arborescence des dossiers d'origine.

- **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.



- **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.

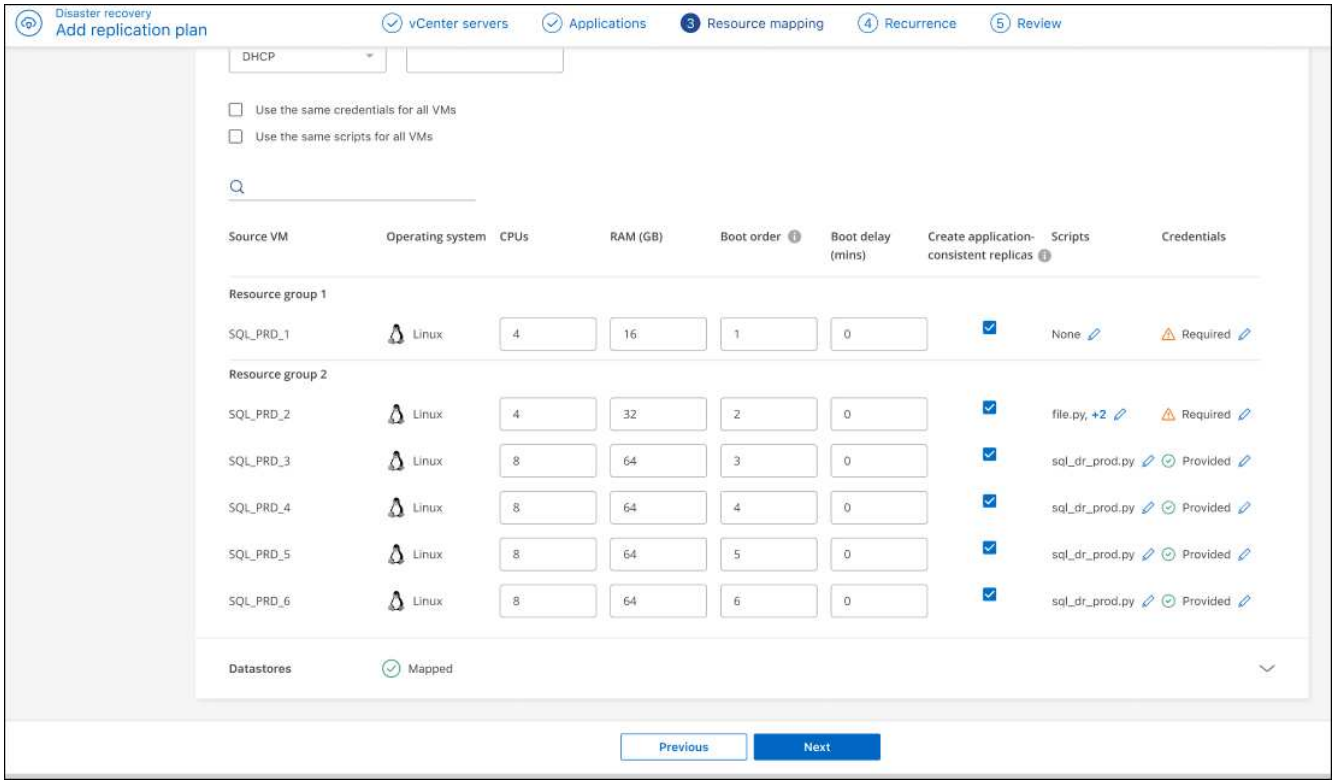
Pour réinitialiser l'ordre de démarrage aux valeurs par défaut, sélectionnez **Réinitialiser les paramètres de la machine virtuelle aux valeurs par défaut**, puis choisissez les paramètres que vous souhaitez rétablir aux valeurs par défaut.

- **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.



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	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. 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.
Au sein d'une source de données externe	Non	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. 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.

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.

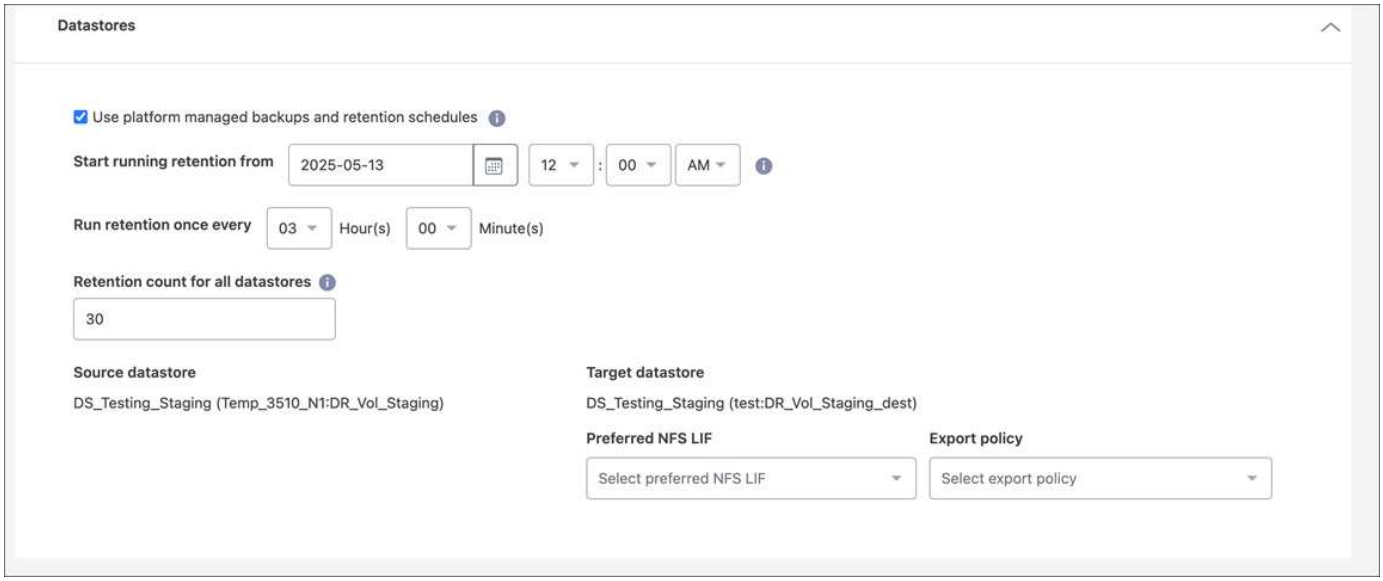
Ressources cartographiques > Section Magasins de données

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.



- **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 souhaiterez 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.

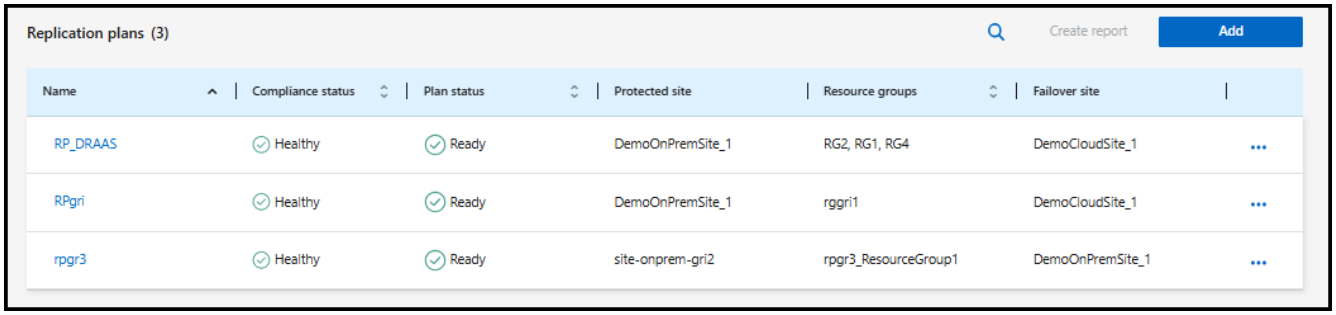
- **Impact sur le temps de conformité** : Lorsqu'un plan de réplication est créé, le service crée un calendrier de conformité par défaut. Le temps de conformité par défaut est de 30 minutes. Pour modifier cette heure, vous pouvez utiliser la fonction Modifier la planification dans le plan de réplication.
- **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**.

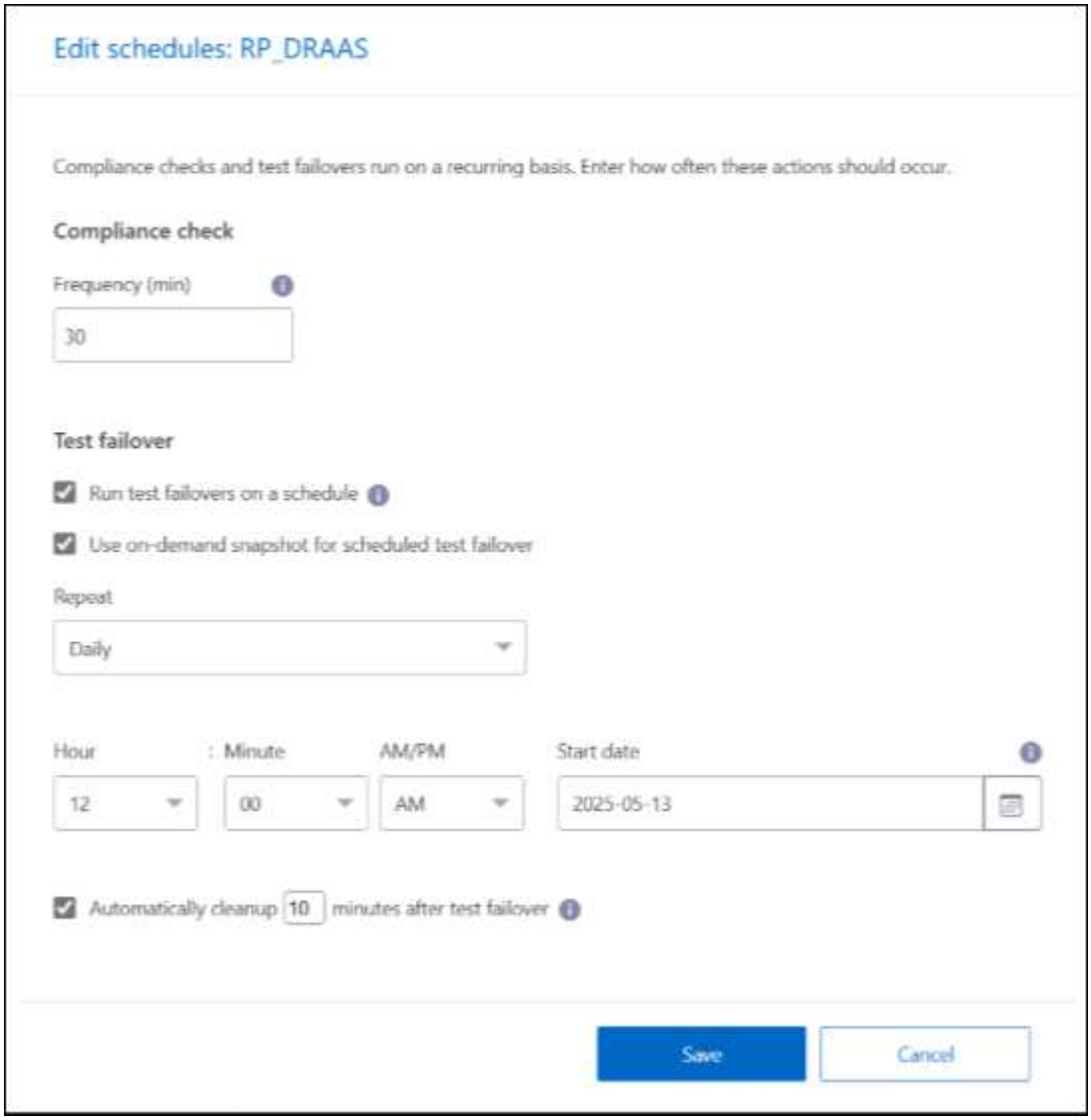


2. Sélectionnez les **Actions*** ••• **icône et sélectionnez *Modifier les horaires**.
3. Saisissez la fréquence en minutes à laquelle vous souhaitez que NetApp Disaster Recovery vérifie la conformité des tests.
4. Pour vérifier que vos tests de basculement sont sains, cochez **Exécuter les basculements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

calendrier mensuel.

a. Sélectionnez le jour du mois et l'heure à laquelle vous souhaitez que ces tests soient exécutés.

b. Saisissez la date au format aaaa-mm-jj à laquelle vous souhaitez que le test commence.



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. Risaster 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 :

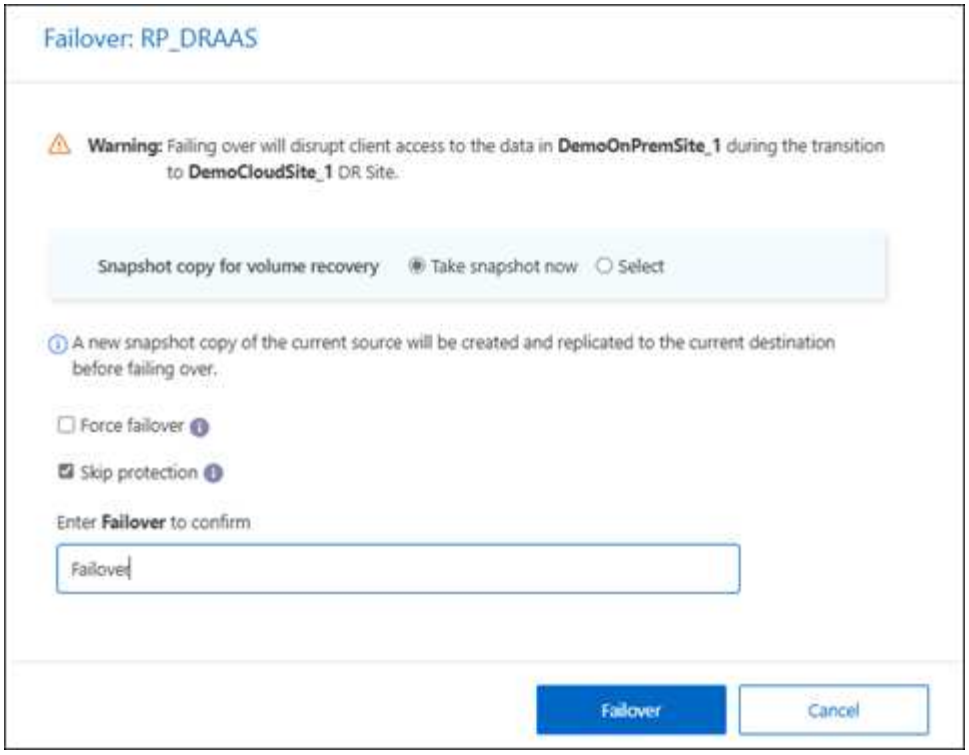
- Disaster Recovery effectue des vérifications préalables sur le cluster de destination et la relation SnapMirror .
- Si vous avez sélectionné le dernier instantané, la mise à jour de SnapMirror est effectuée pour répliquer les dernières modifications.
- Les machines virtuelles sources sont hors tension.
- 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**.



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

ressources pour organiser les machines virtuelles ensemble" .

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

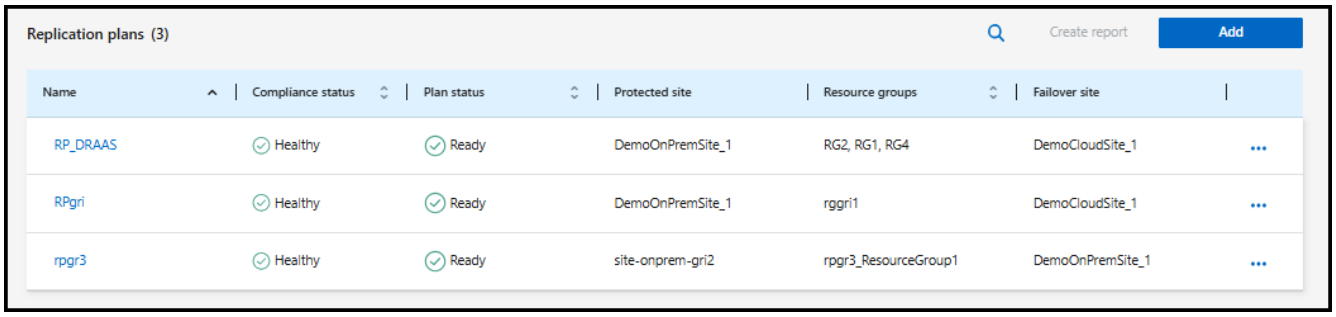
Vous pouvez désactiver, activer et supprimer les plans de réplication. Vous pouvez modifier les horaires.

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**.



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**.

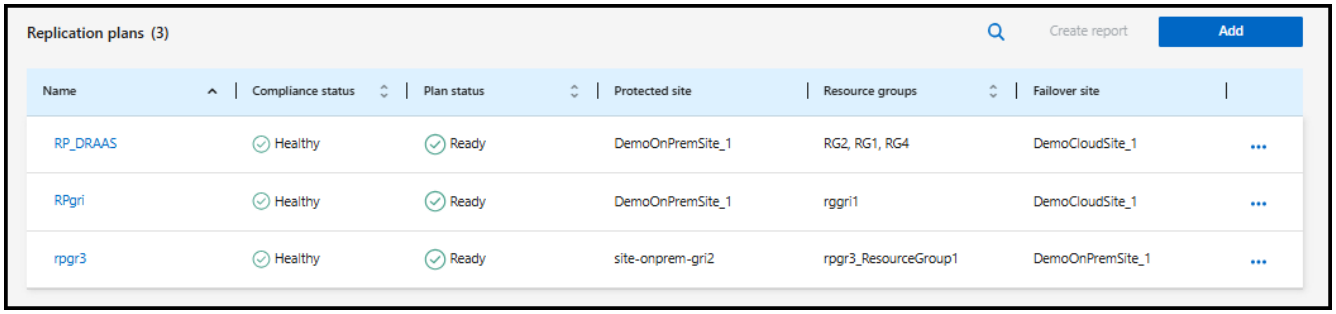
Rapprocher les instantanés à la demande

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**.



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**.

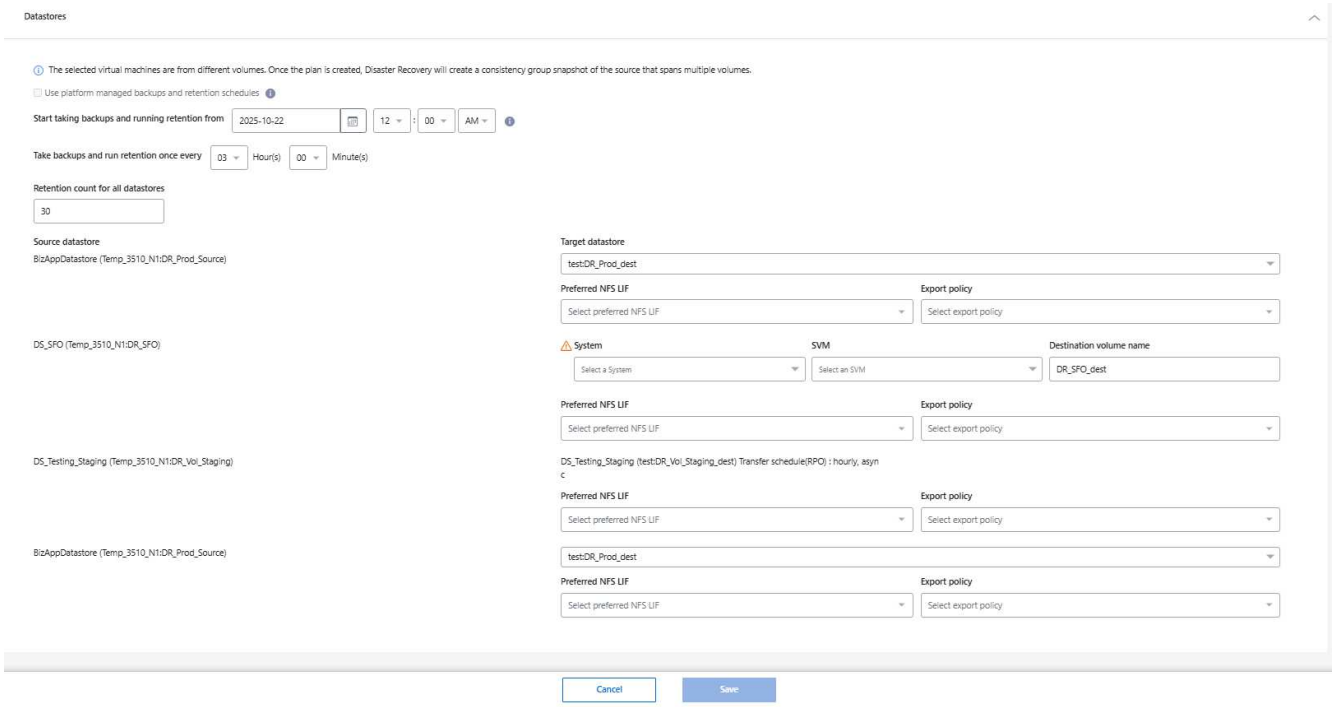
Modifier le nombre de rétentions pour les planifications de basculement

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 **Datastores** pour la développer.



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 souhaiterez 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 souhaiterez 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.

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

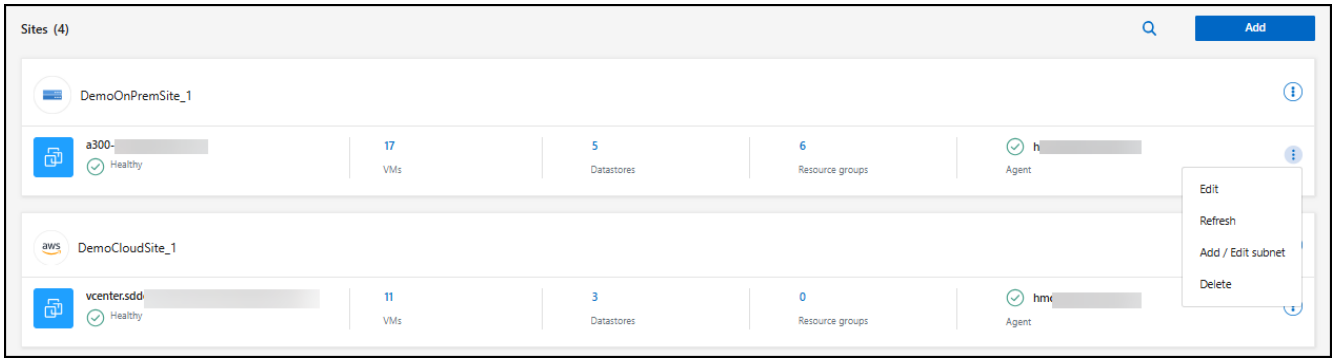
La NetApp Console prend en charge l'utilisation de plusieurs agents de console dans un seul environnement de travail. L'utilisation de plusieurs agents Console peut s'avérer utile pour maintenir l'accès aux ressources pendant la maintenance d'un autre agent Console ou en cas de défaillance d'un agent 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

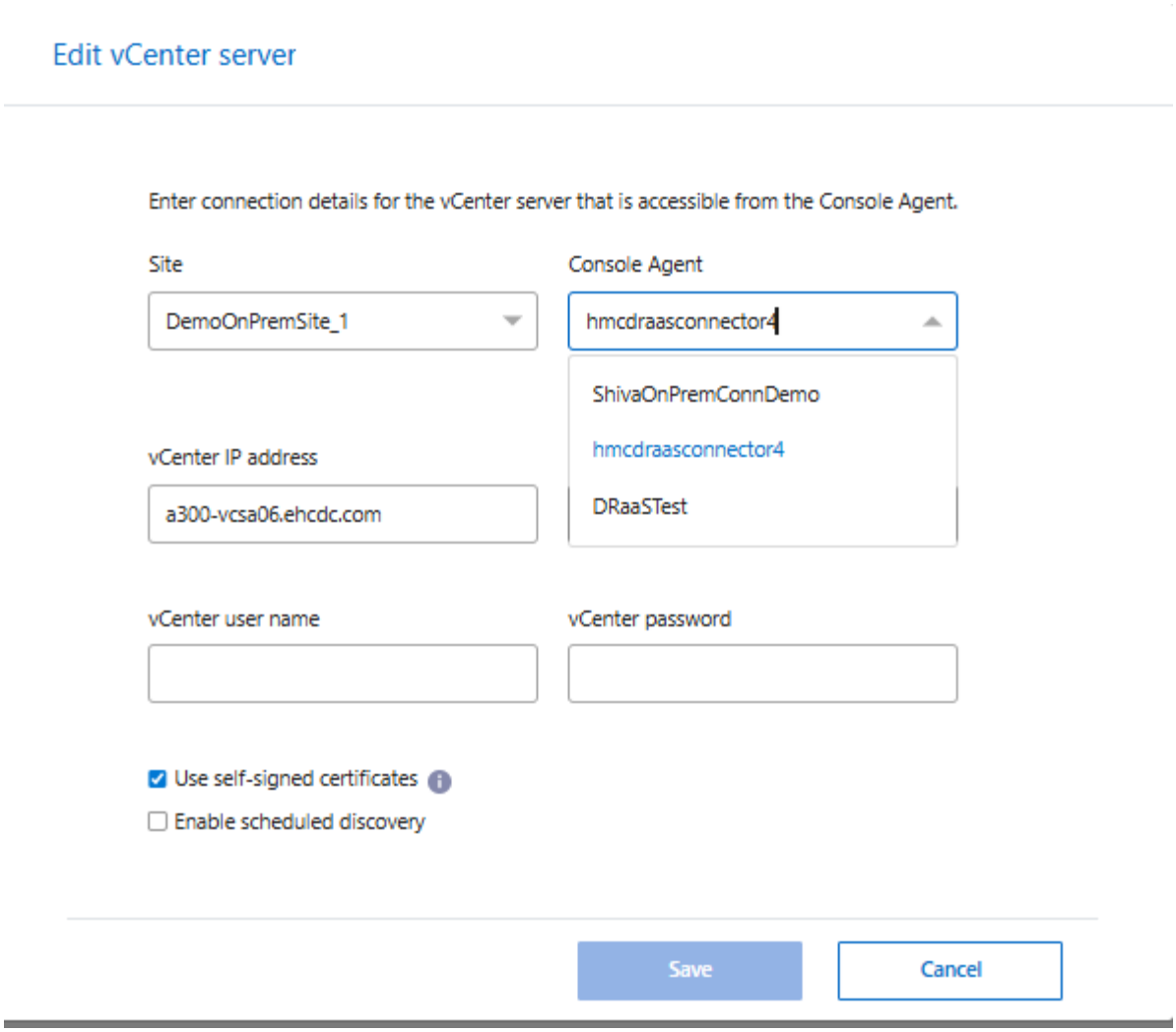
- Vous devez avoirAu moins deux agents Console ont été ajoutés à votre environnement de travail. .
- Les deux agents de console doivent contenir les mêmes clusters ONTAP .

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

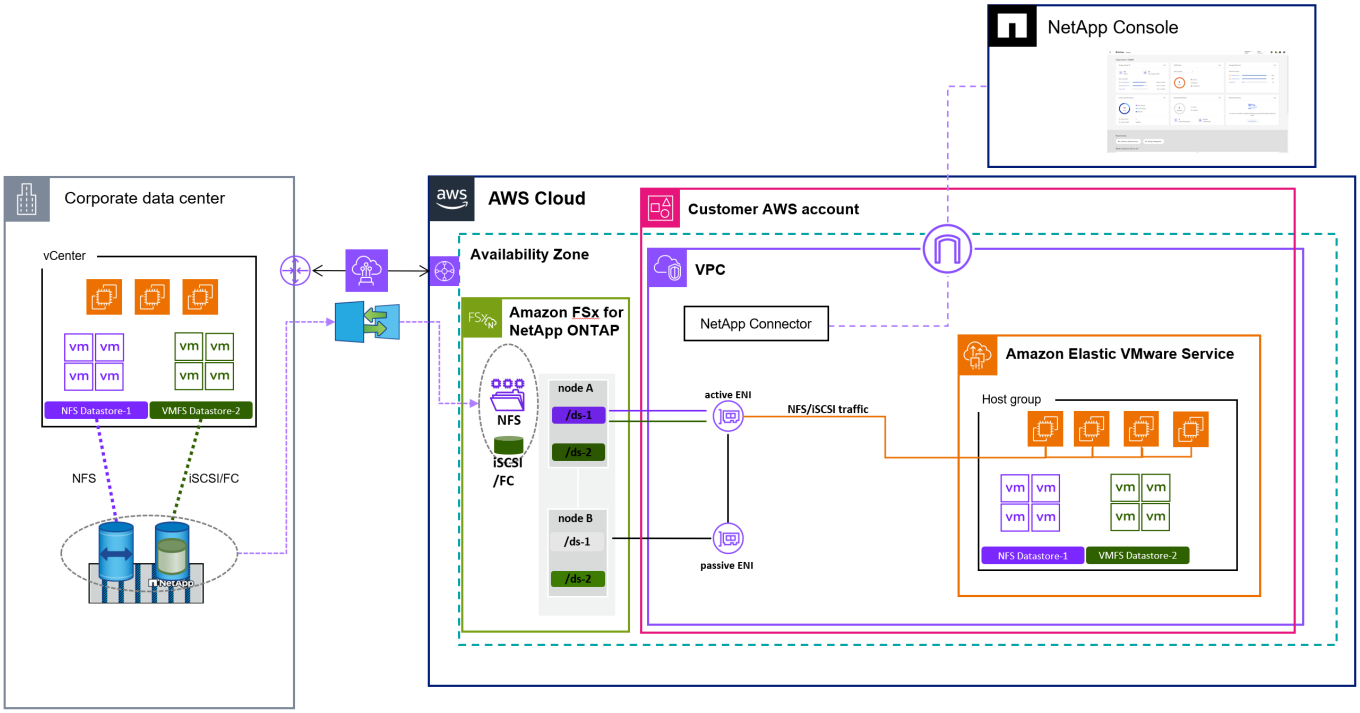
NetApp Disaster Recovery est un service à valeur ajoutée hébergé dans l'environnement logiciel en tant que service NetApp Console , qui dépend de l'architecture principale de NetApp Console . Plusieurs composants principaux composent le service DR pour la protection VMware au sein de la console.

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 :

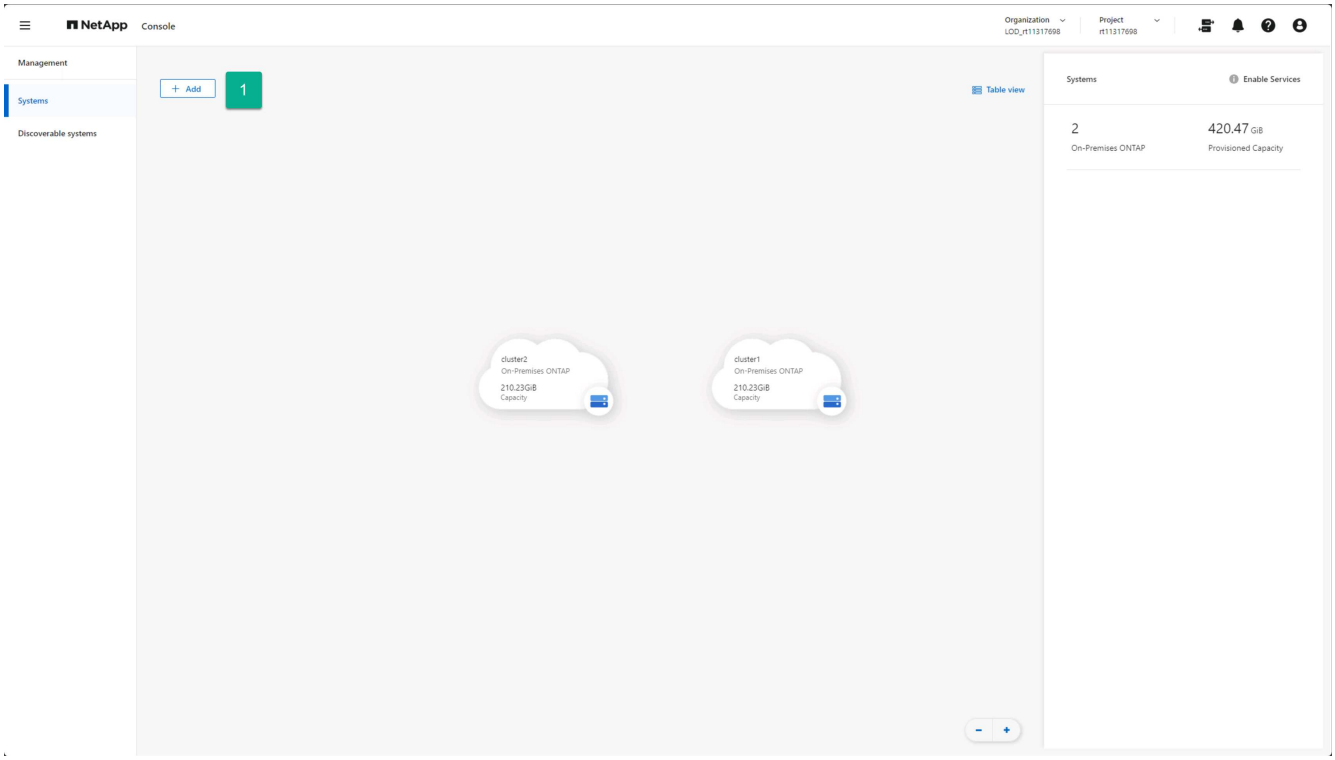
- Ajoutez des baies sur site à votre système de NetApp Console .

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

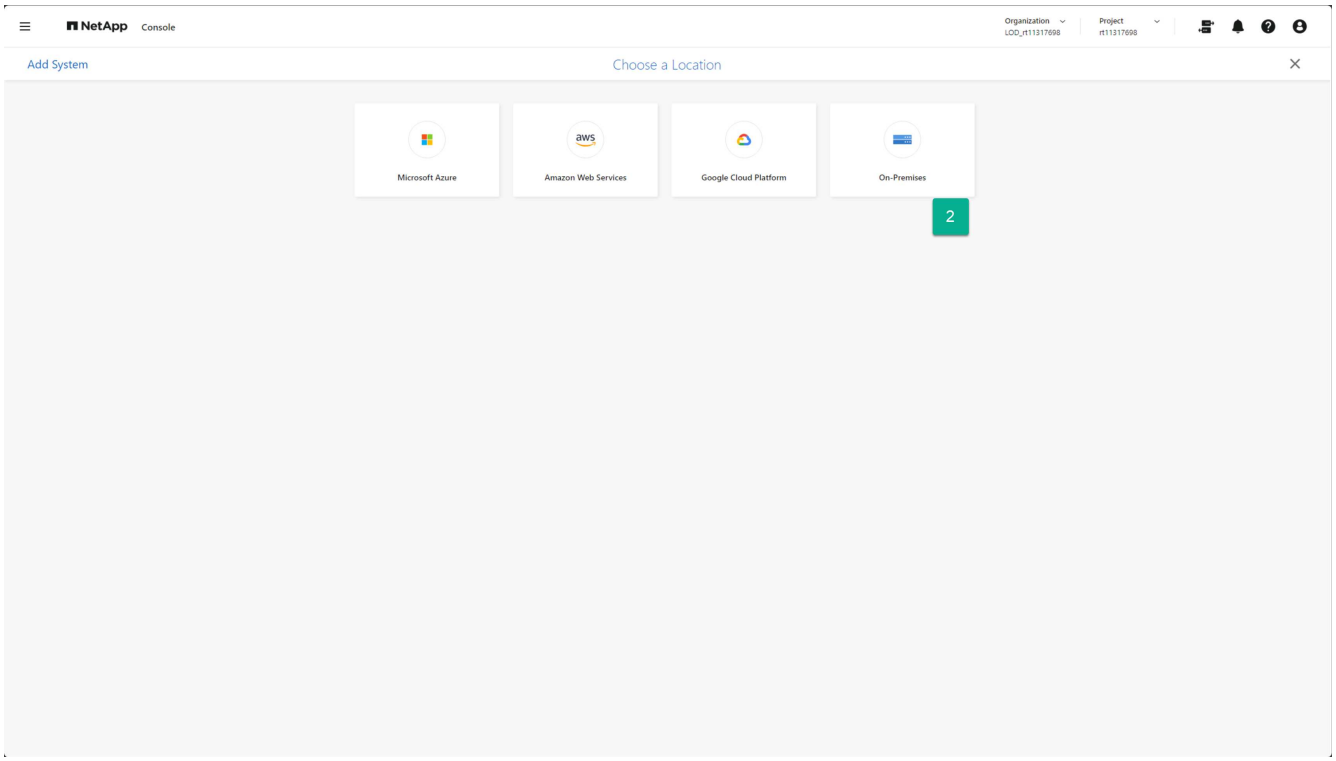
Ajouter des baies de stockage sur site au système NetApp Console

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

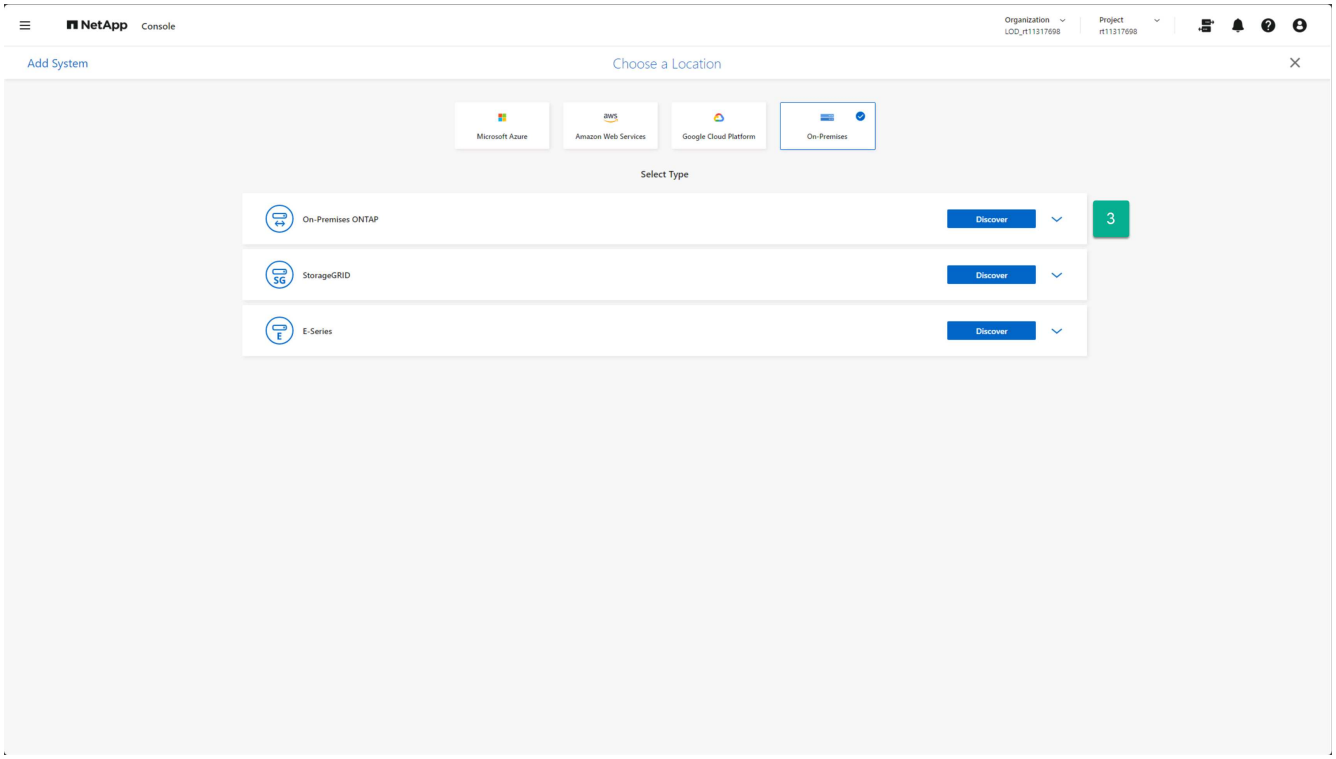
1. Depuis la page Systèmes de la NetApp Console , sélectionnez **Ajouter un système**.



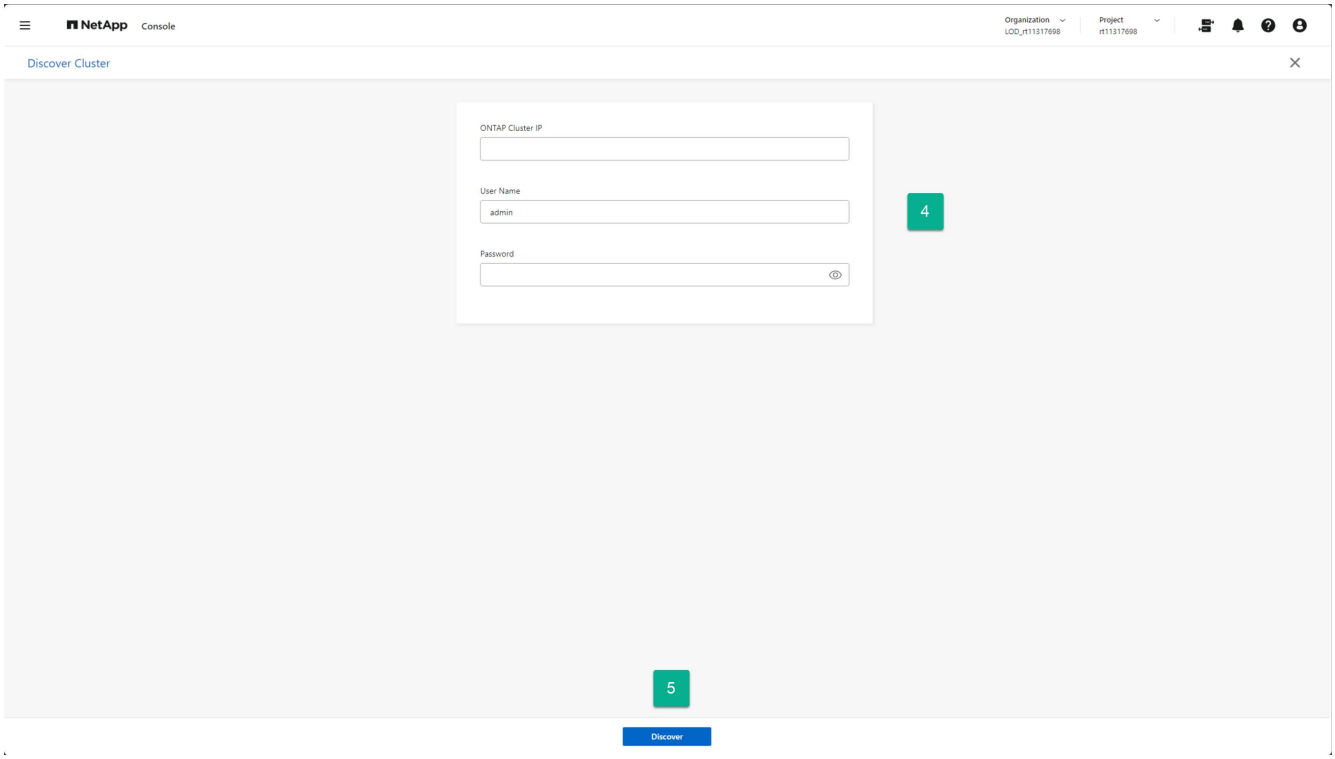
2. Depuis la page Ajouter un système, sélectionnez la carte **Sur site**.



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.

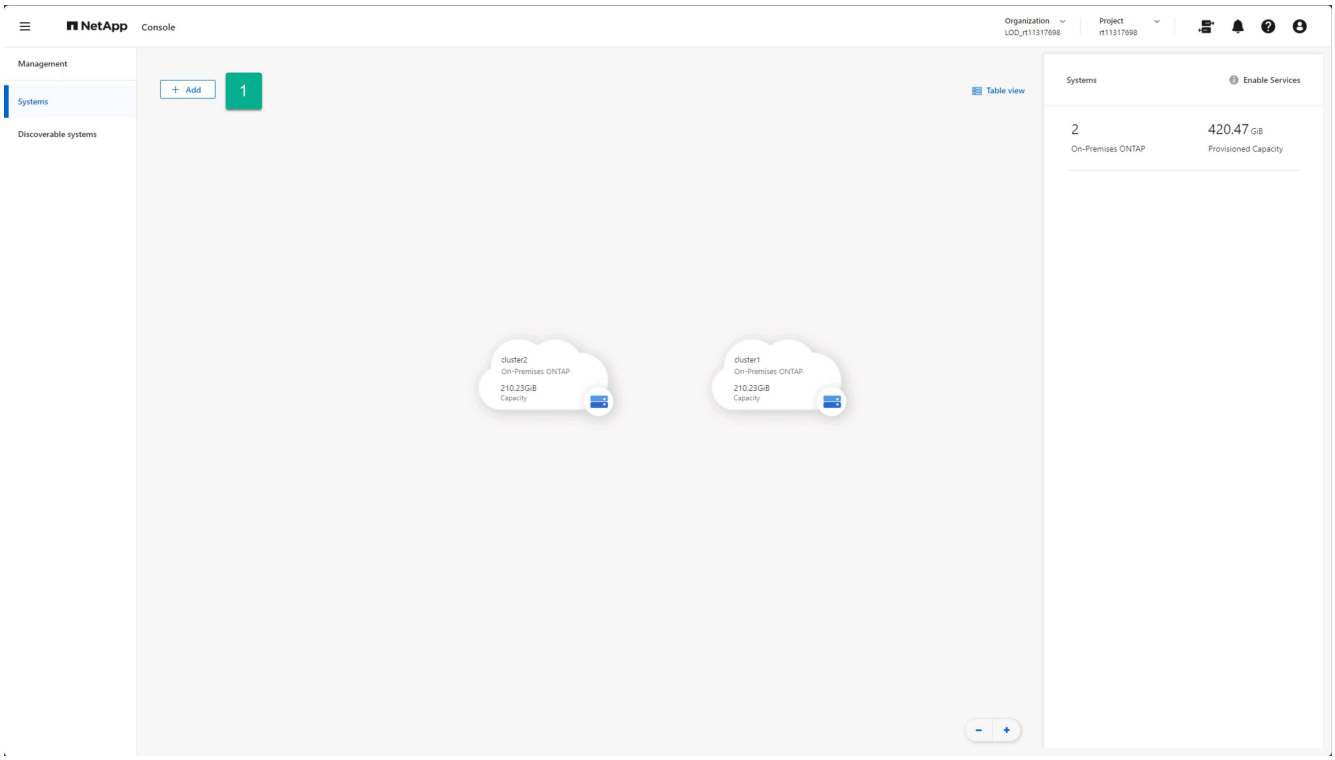


6. Répétez les étapes 1 à 5 pour chaque baie ONTAP qui hébergera les banques de données vCenter.

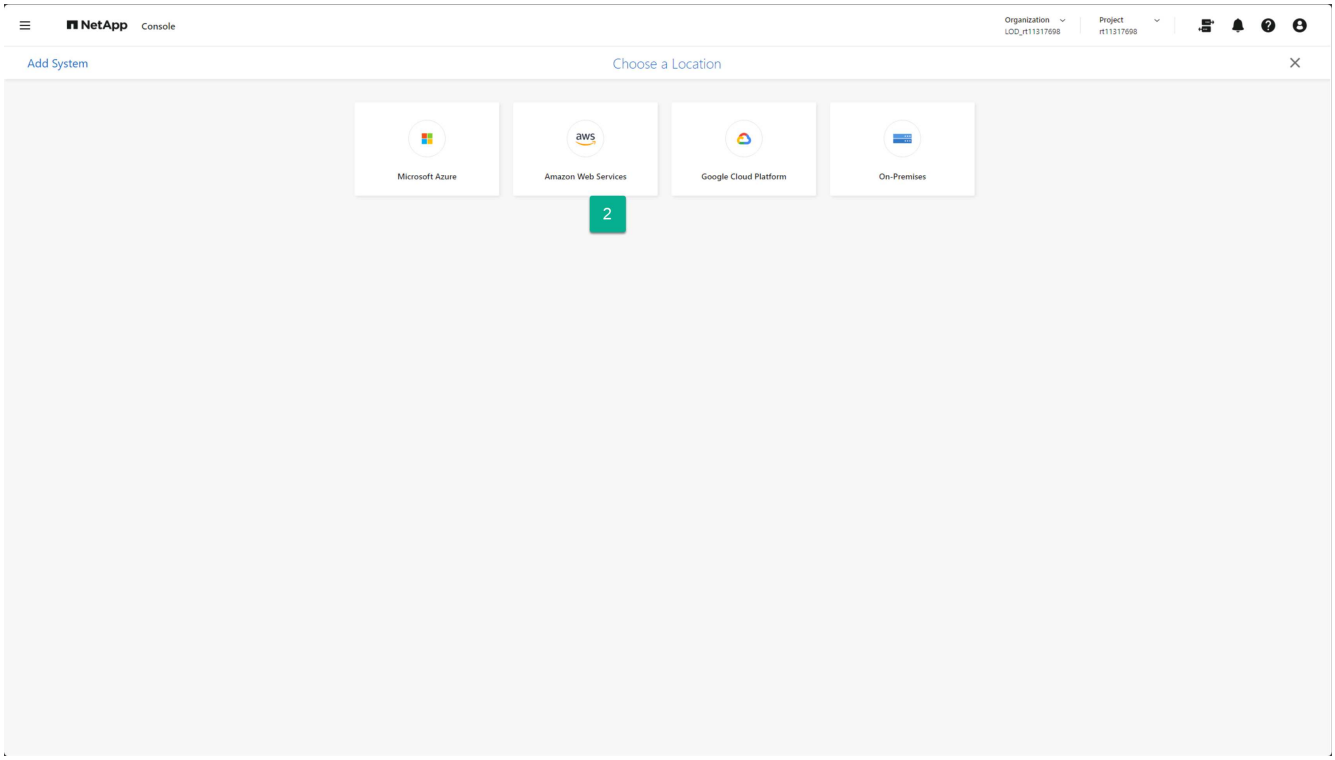
Ajoutez des instances de stockage Amazon FSx for NetApp ONTAP au système NetApp Console

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

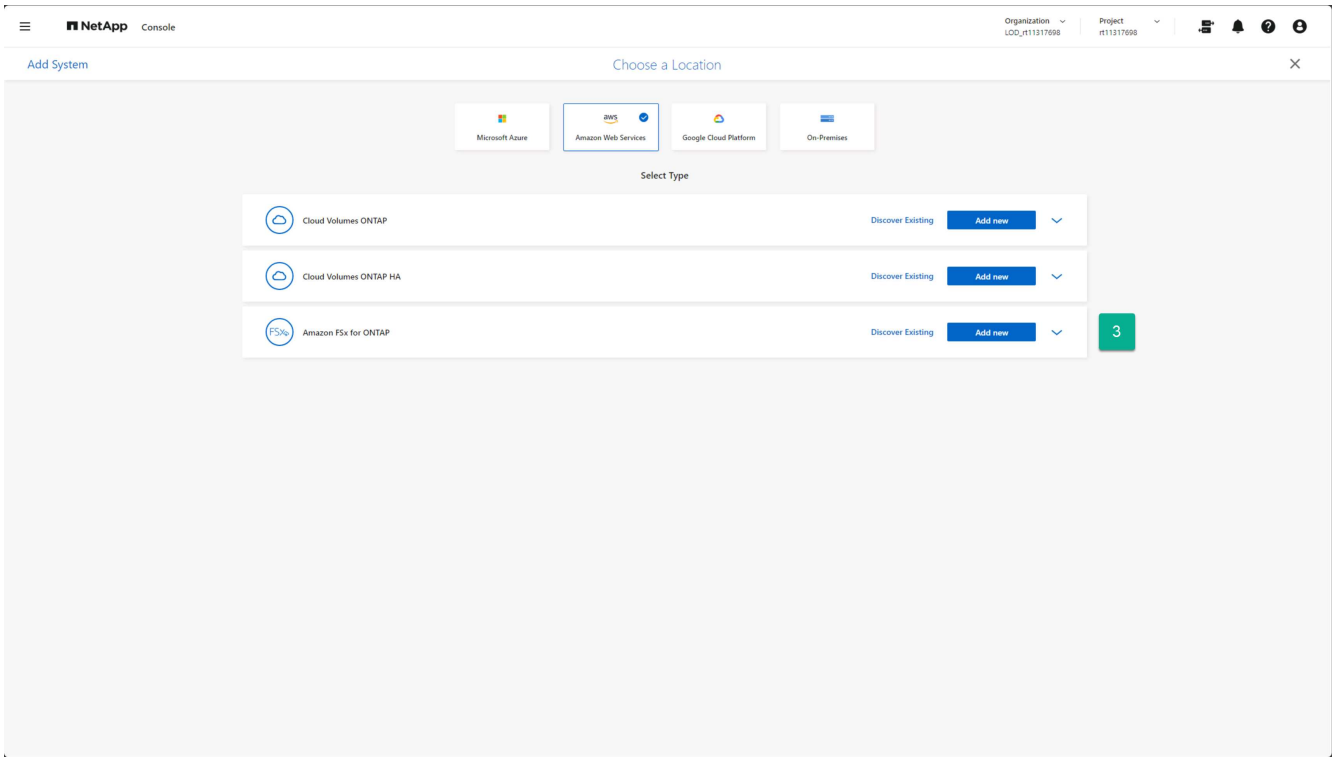
1. Depuis la page Systèmes de la NetApp Console , sélectionnez **Ajouter un système**.



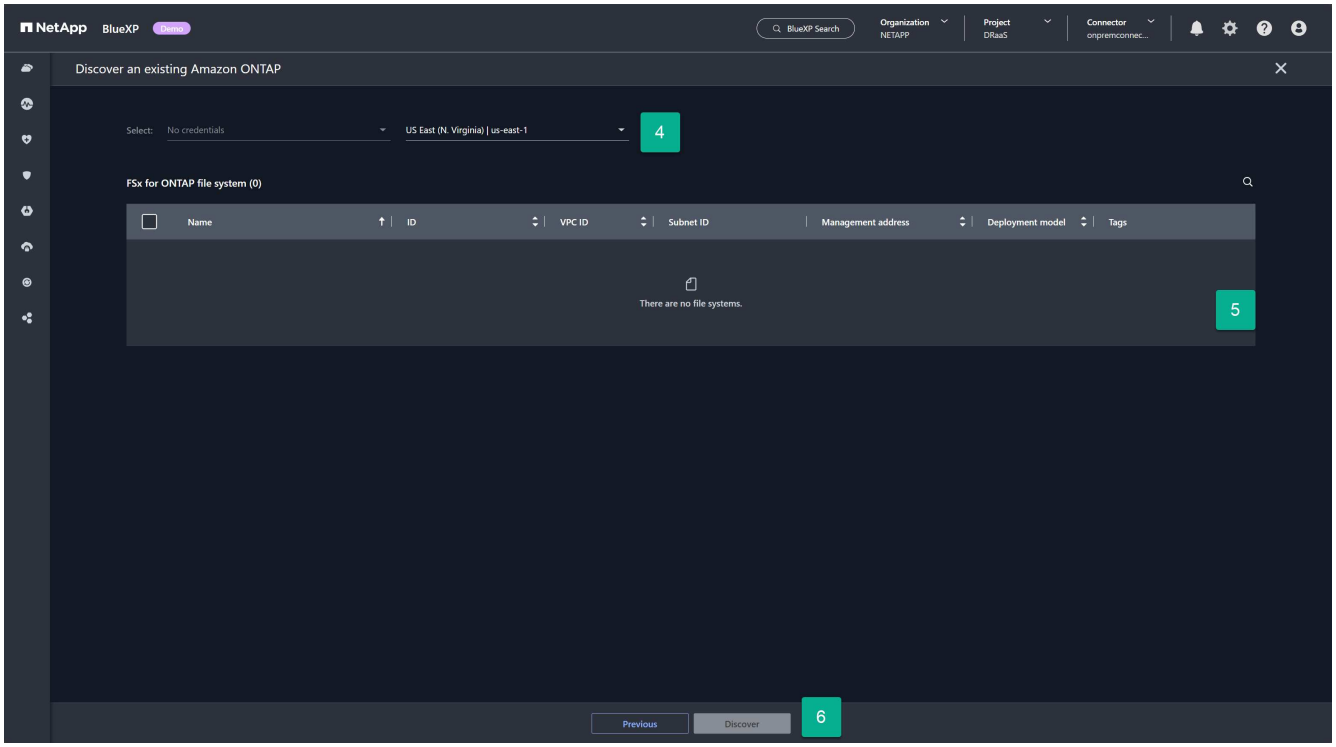
2. Depuis la page Ajouter un système, sélectionnez la carte **Amazon Web Services**.



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 :

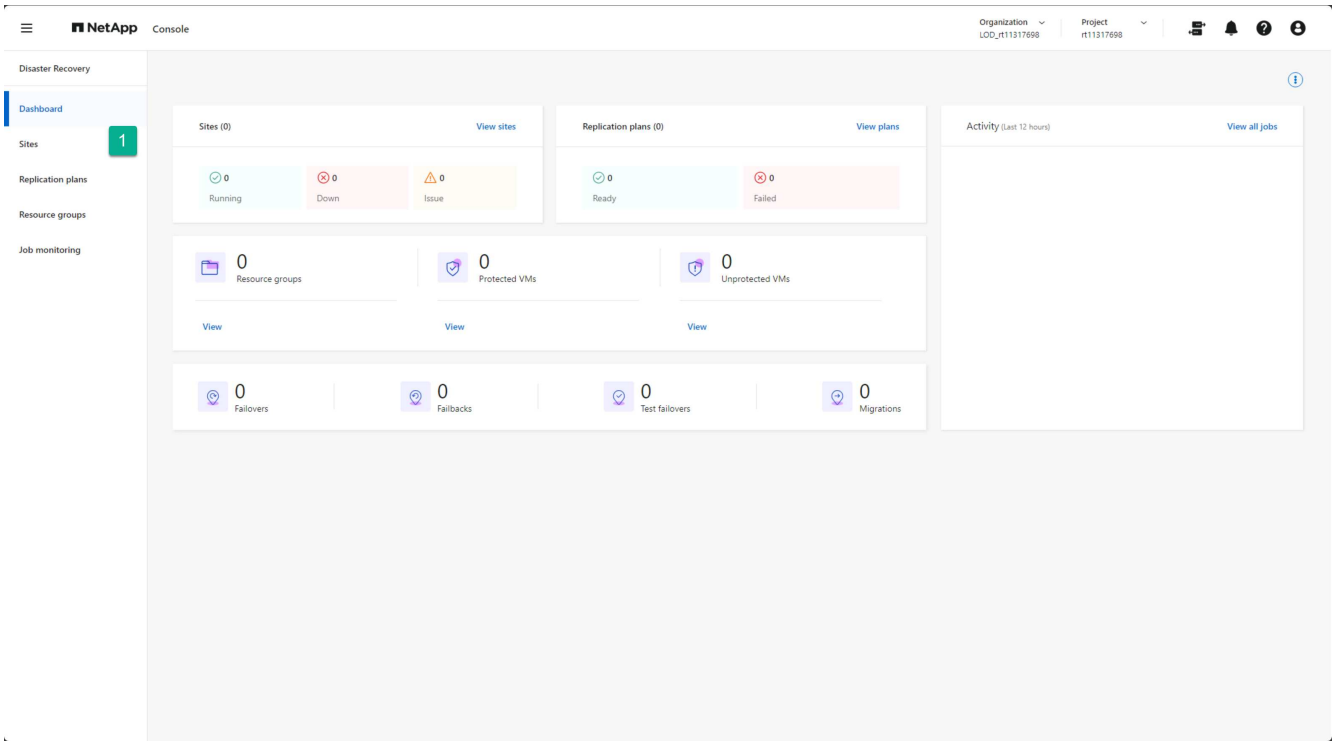
- Un site pour représenter chaque centre de données de production où résident vos clusters vCenter de production
- Un site pour votre centre de données cloud Amazon EVS/ Amazon FSx for NetApp ONTAP

Créer des sites sur site

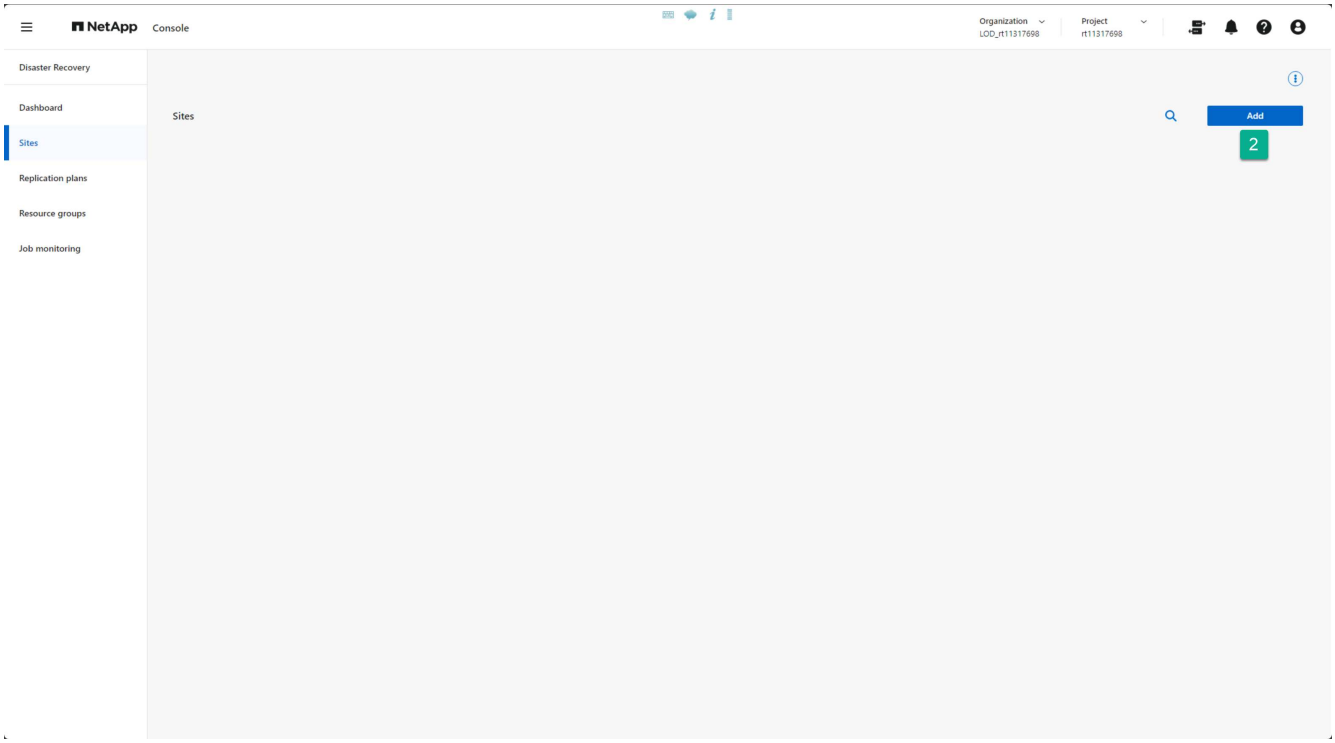
Créez un site vCenter de production.

Étapes

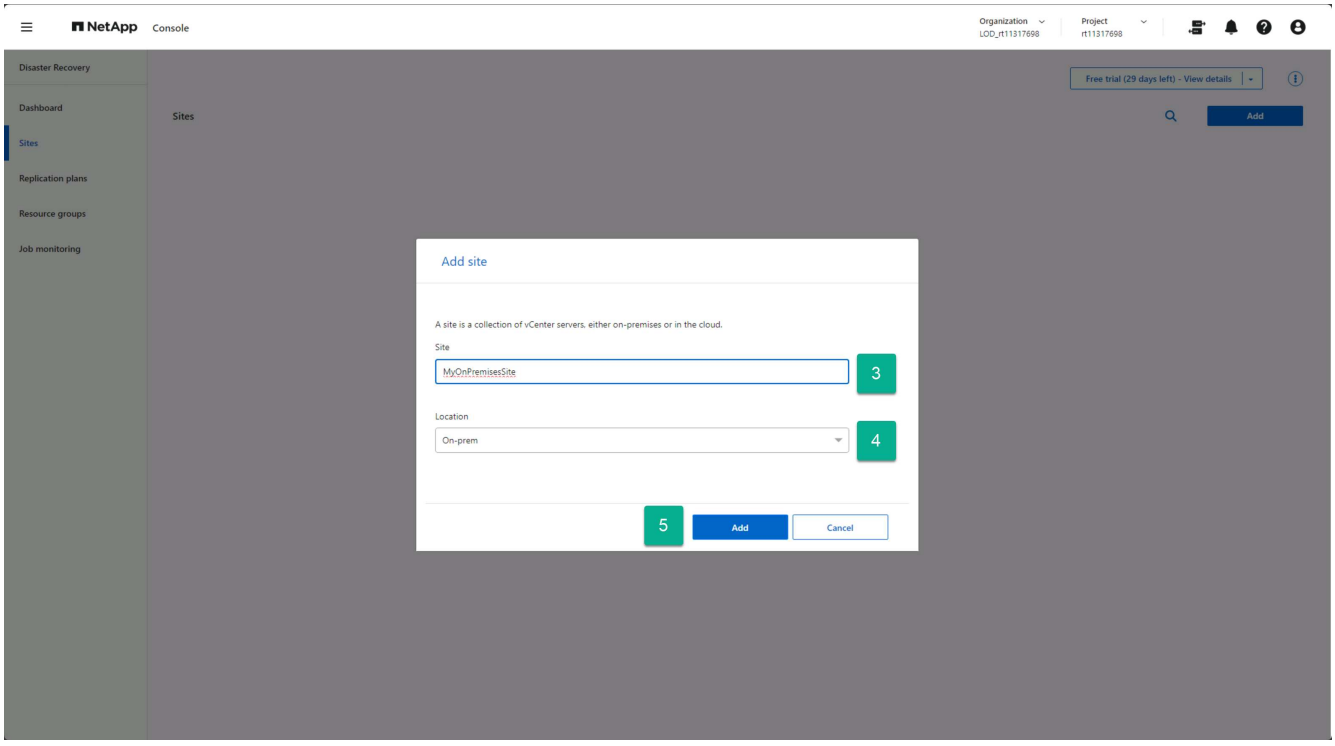
1. Dans la barre de navigation de gauche de la NetApp Console , sélectionnez **Protection** > **Reprise après sinistre**.
2. À partir de n'importe quelle page de NetApp Disaster Recovery, sélectionnez l'option **Sites**.



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**.

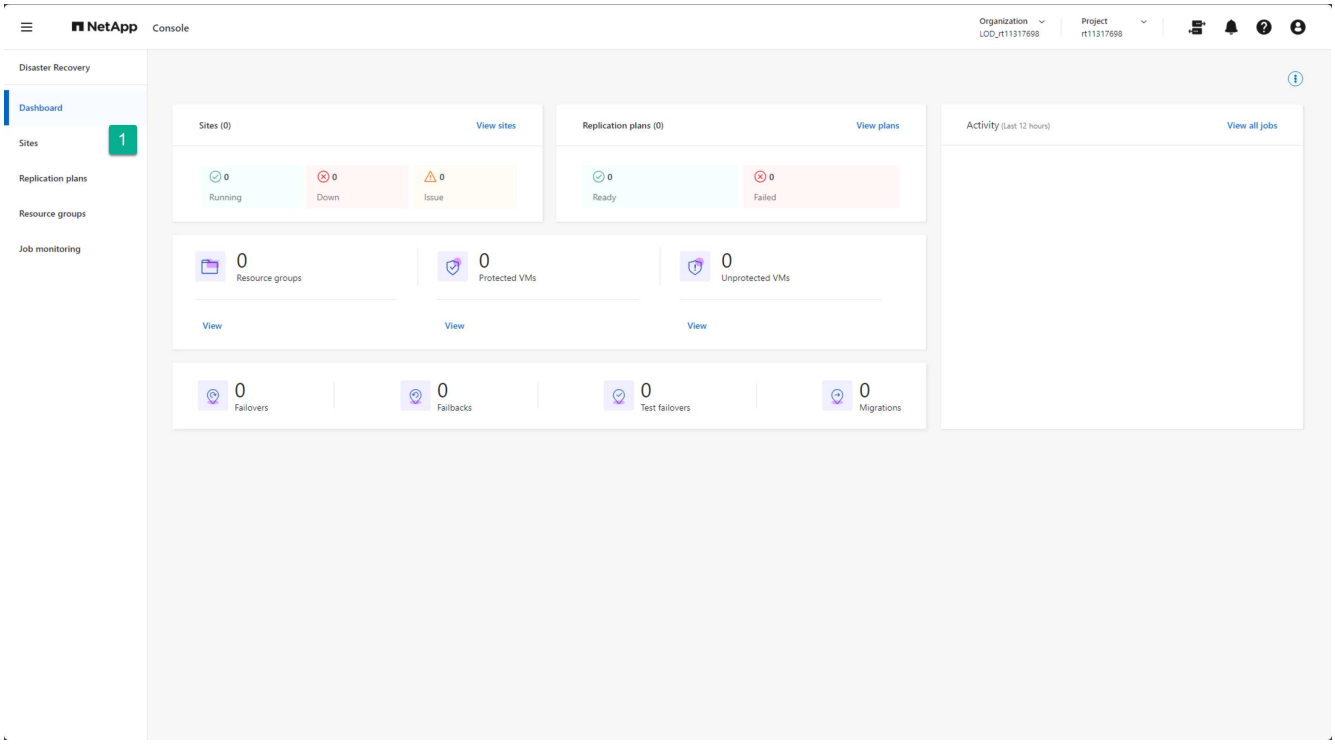


Si vous disposez d'autres sites vCenter de production, vous pouvez les ajouter en suivant les mêmes étapes.

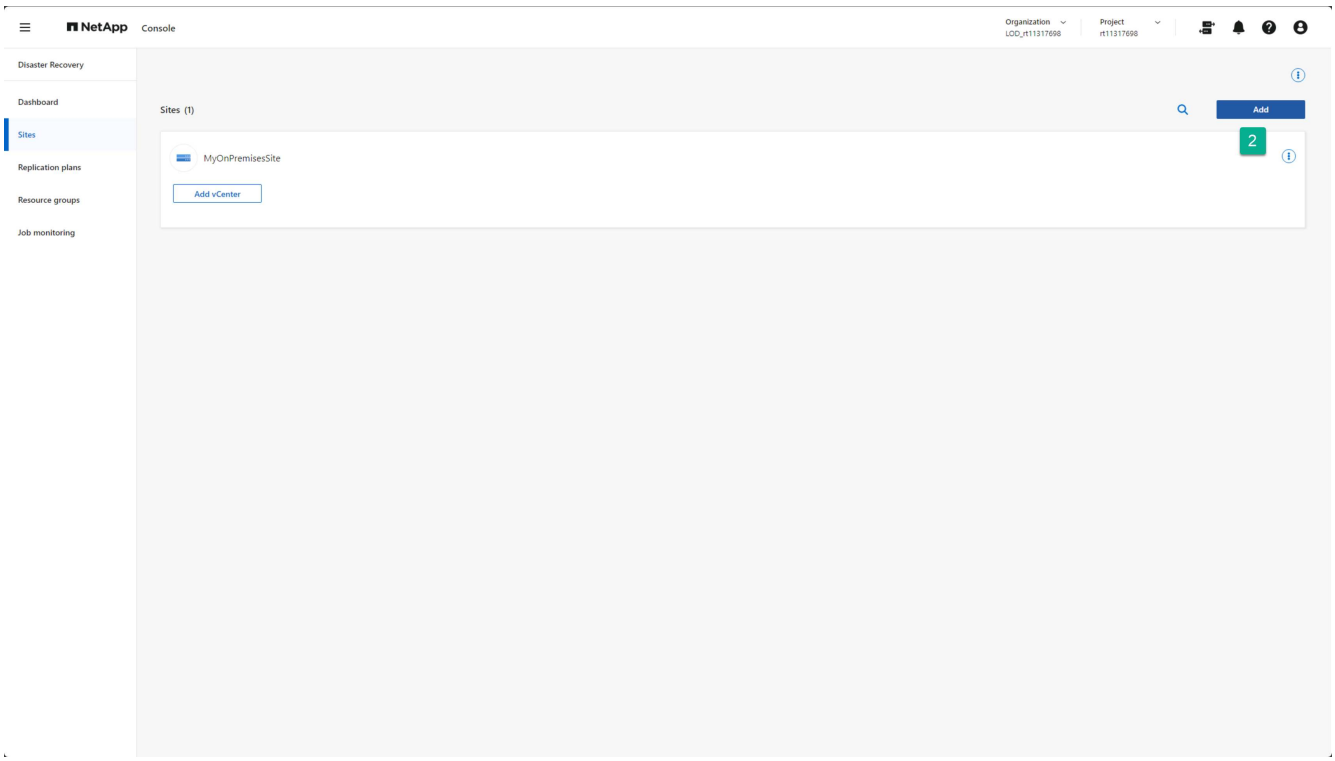
Créer des sites cloud Amazon

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**.

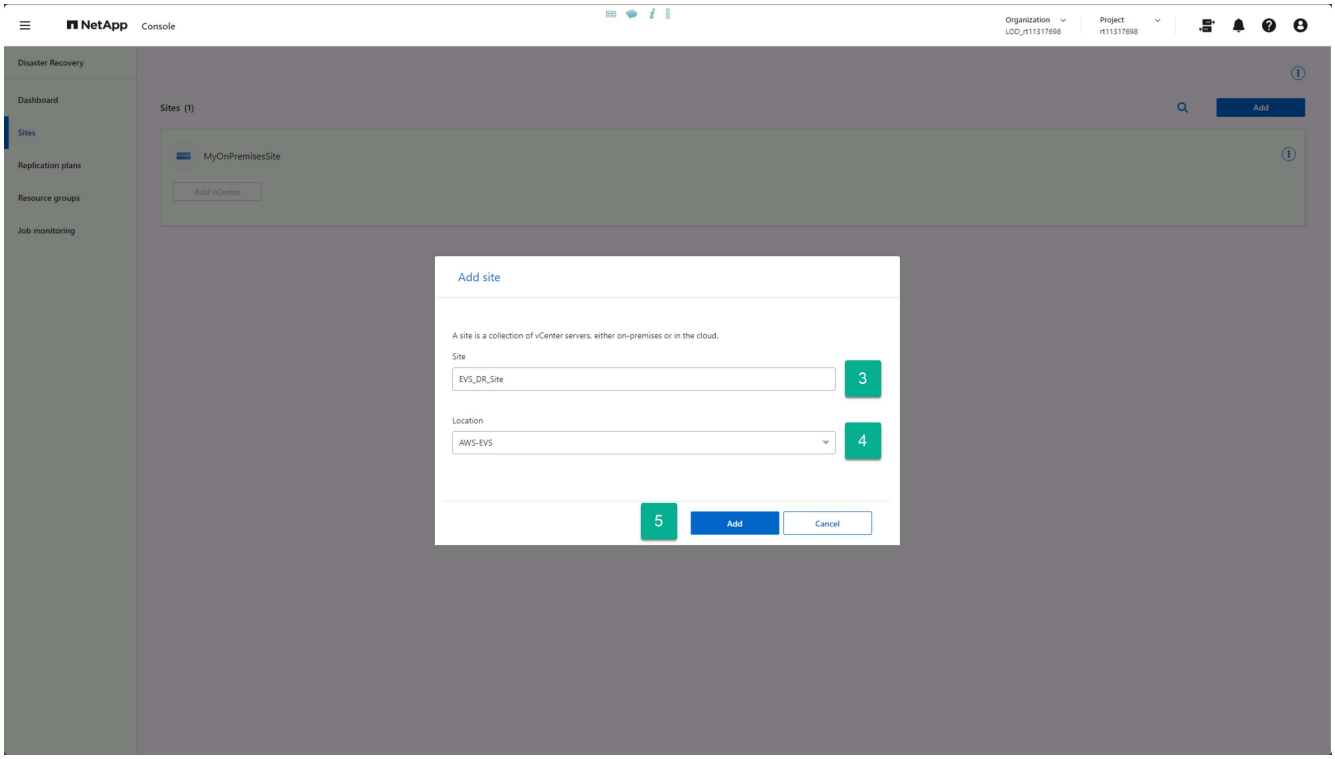


2. Dans l'option Sites, sélectionnez **Ajouter**.



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

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



Résultat

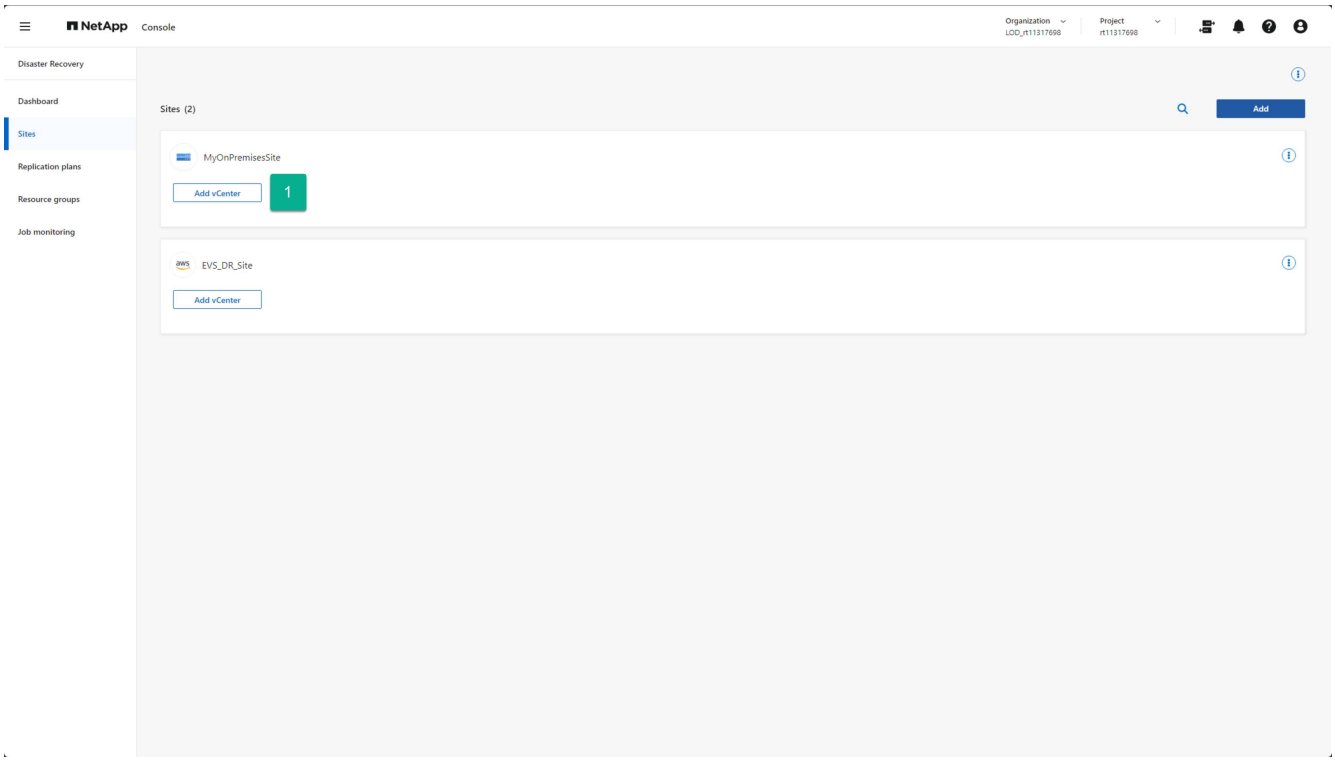
Vous avez maintenant créé un site de production (source) et un site DR (destination).

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

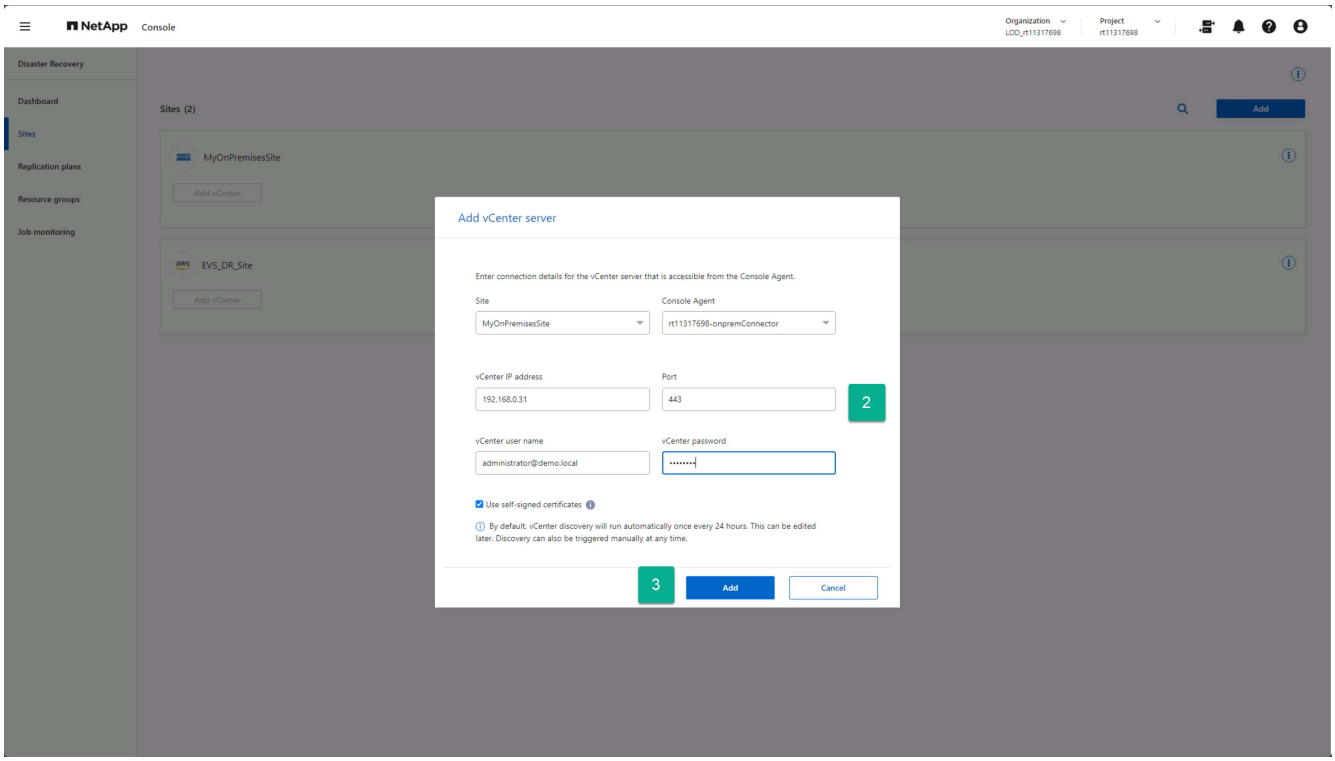
Une fois les sites créés, vous ajoutez désormais vos clusters vCenter à chaque site dans NetApp Disaster Recovery. Lors de la création de chaque site, nous avons indiqué chaque type de site. Cela indique à NetApp Disaster Recovery quel type d'accès est requis pour les vCenters hébergés dans chaque type 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.
   e. Le mot de passe vCenter pour le nom d'utilisateur fourni.
   f. 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.
3. Sélectionnez **Ajouter**.



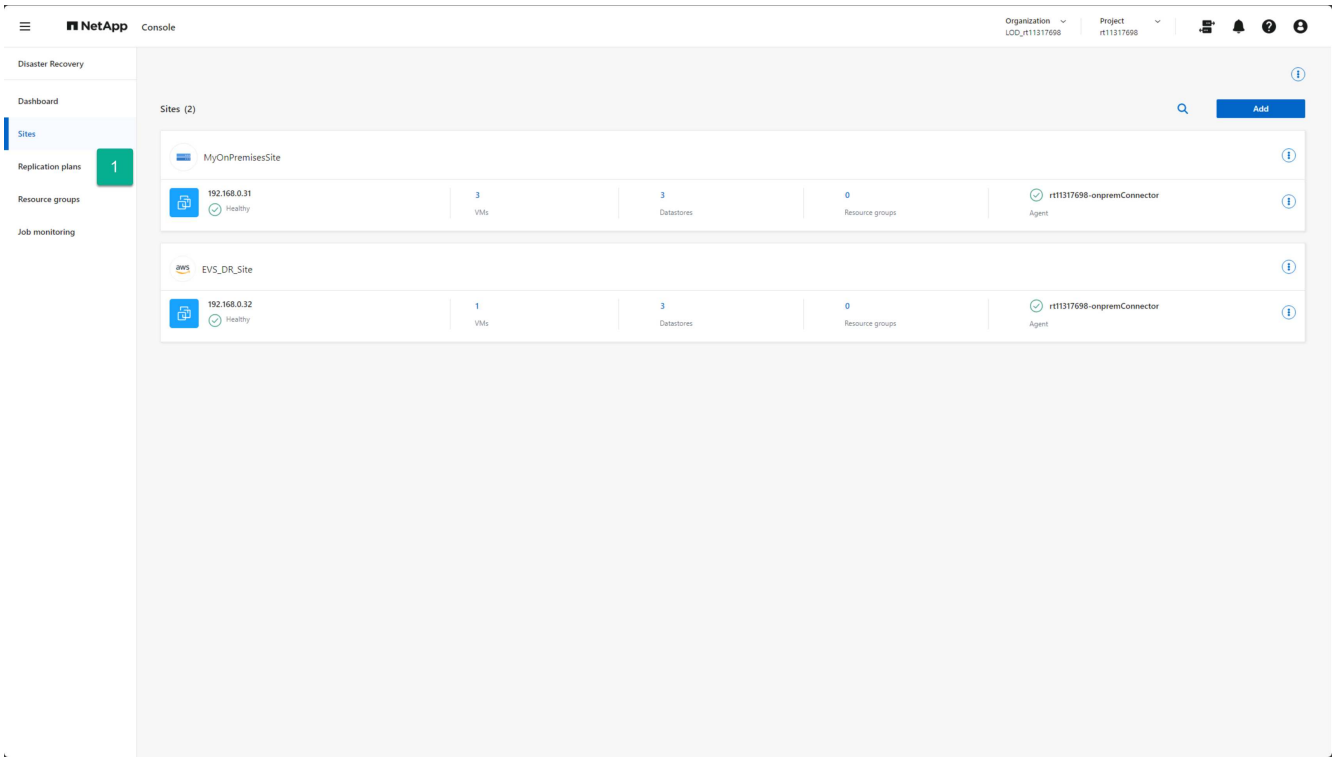
Créer des plans de réplication pour Amazon EVS

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

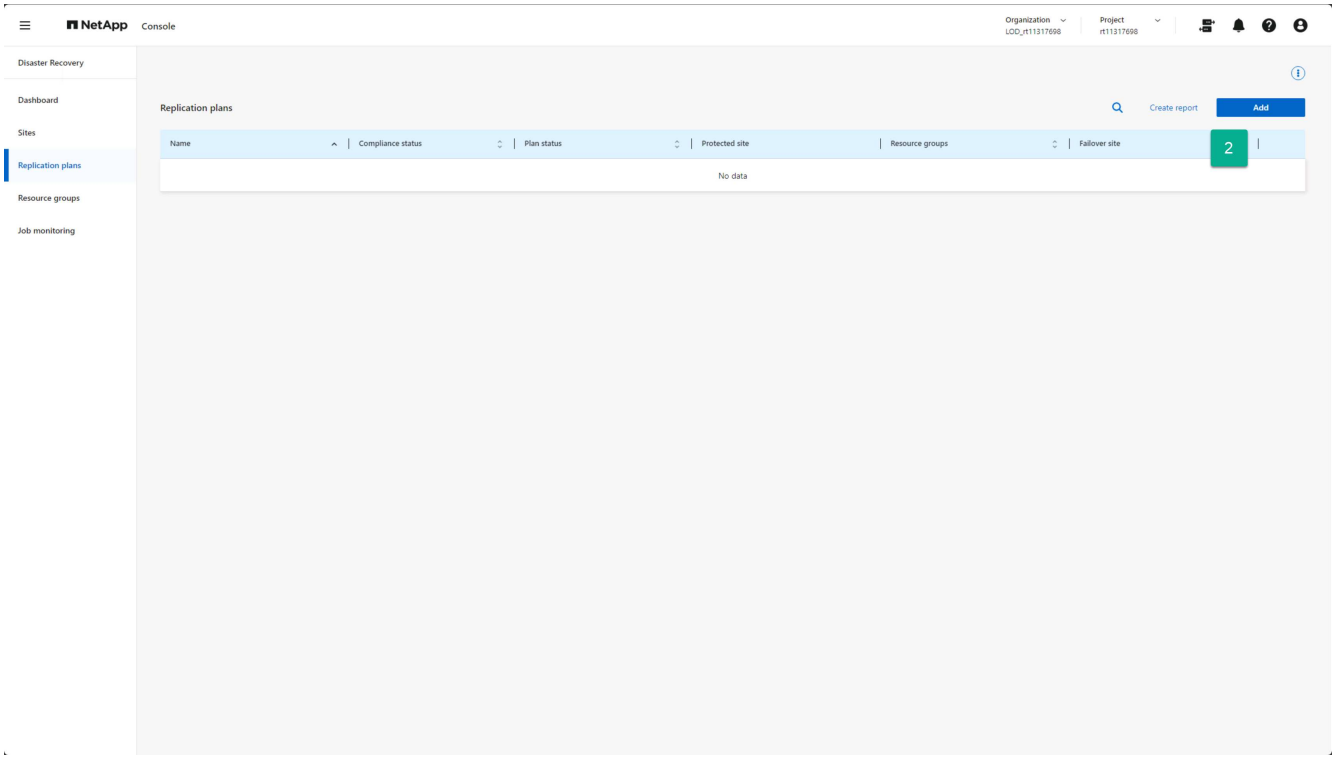
Une fois que vous avez des vCenters à protéger sur le site local et que vous disposez d'un site Amazon EVS configuré pour utiliser Amazon FSx for NetApp ONTAP que vous pouvez utiliser comme destination DR, vous pouvez créer un plan de réplication (RP) pour protéger tout ensemble de machines virtuelles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

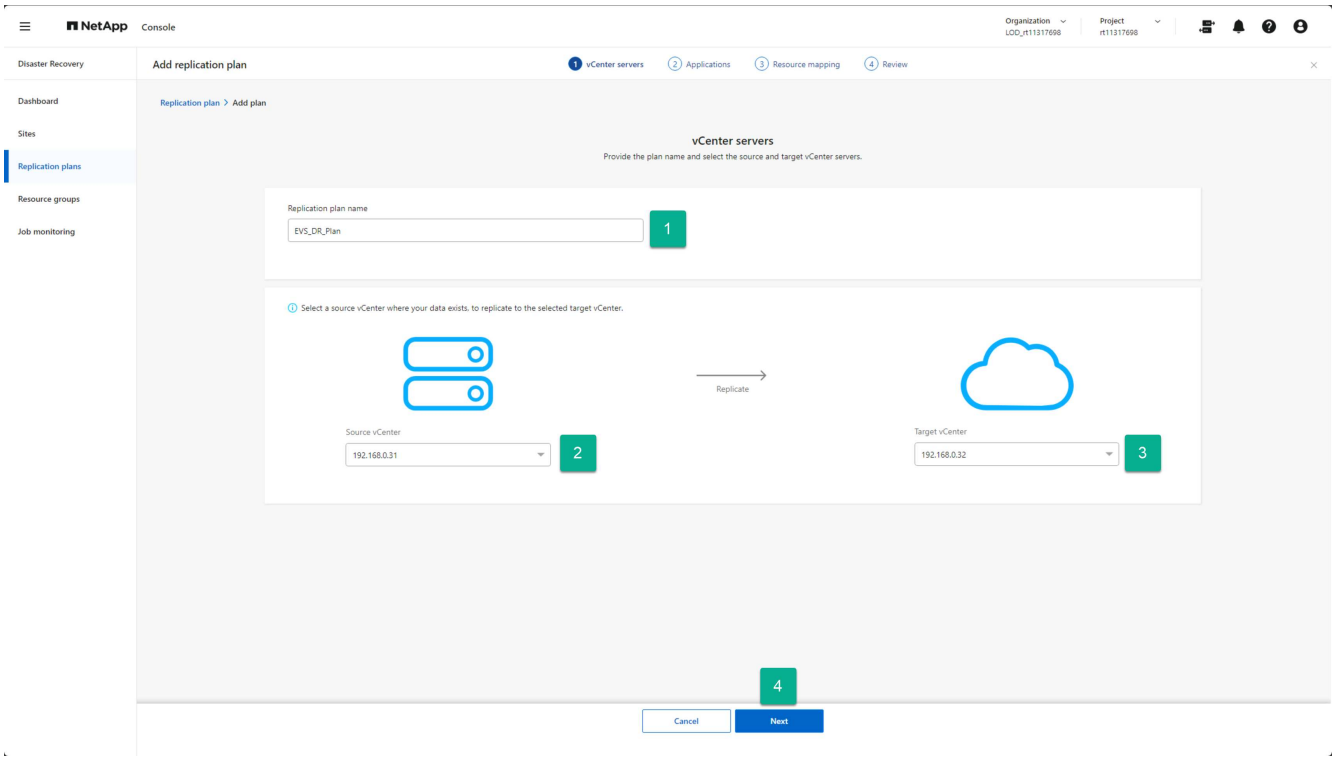
Créer un plan de réplication : Étape 1 : Sélectionner les vCenters dans NetApp Disaster Recovery

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,

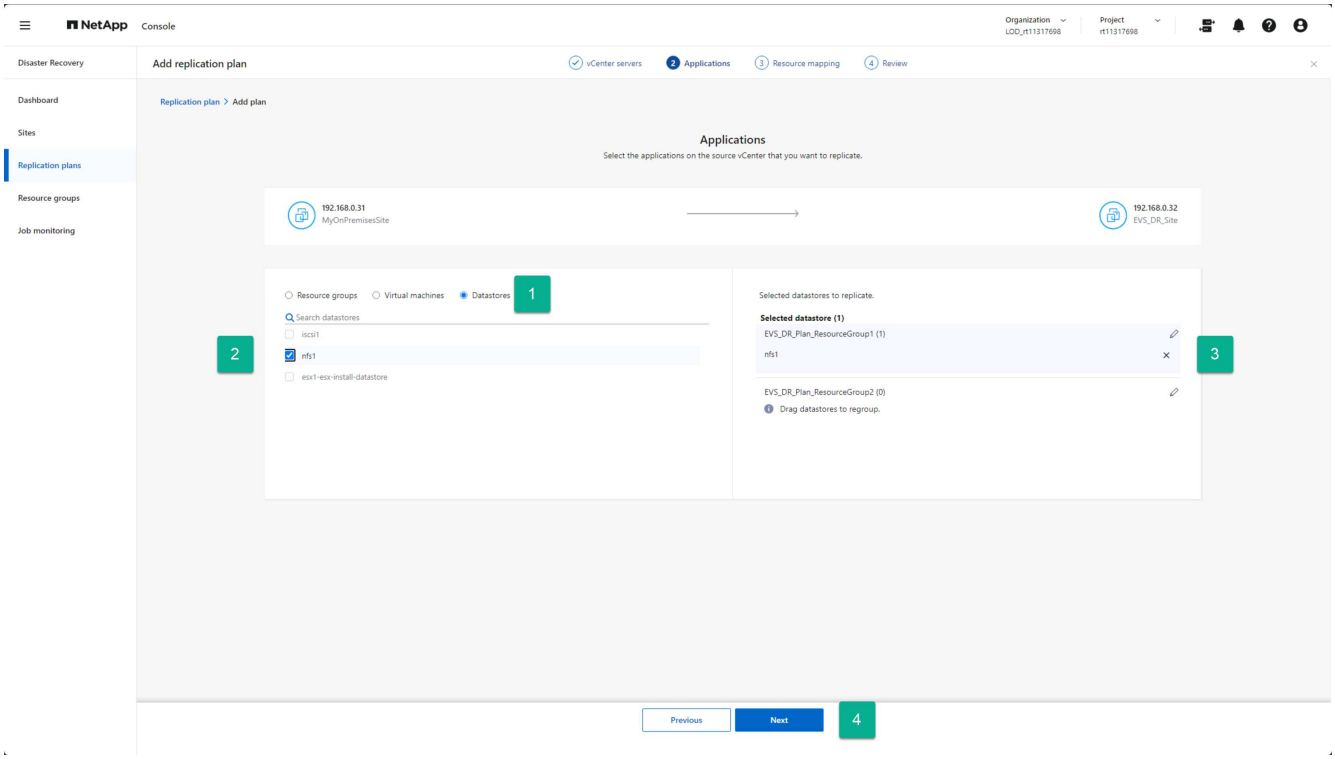
consultez la section "Créer un plan de réplication" .

- **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 :

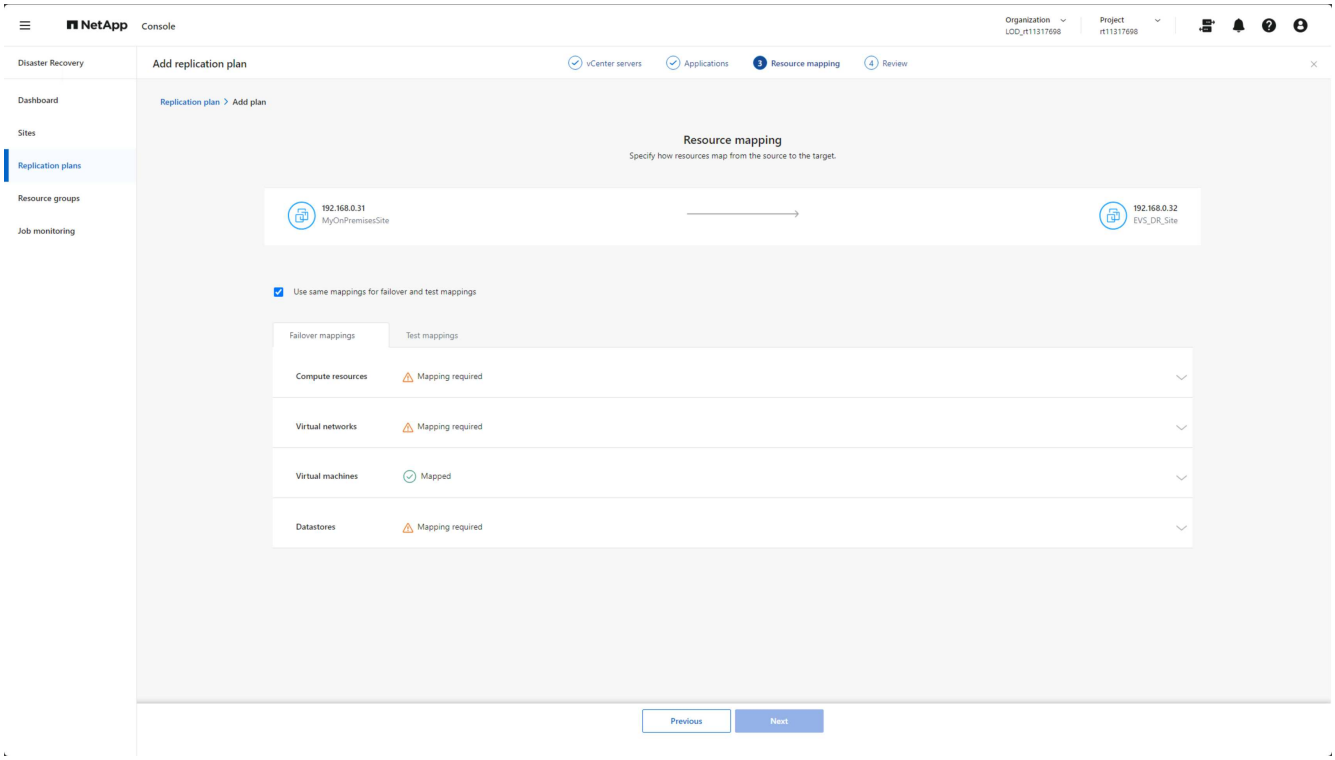
- Ressources de calcul
- Réseaux virtuels
- Reconfiguration de la machine virtuelle
- Cartographie des banques de données

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.

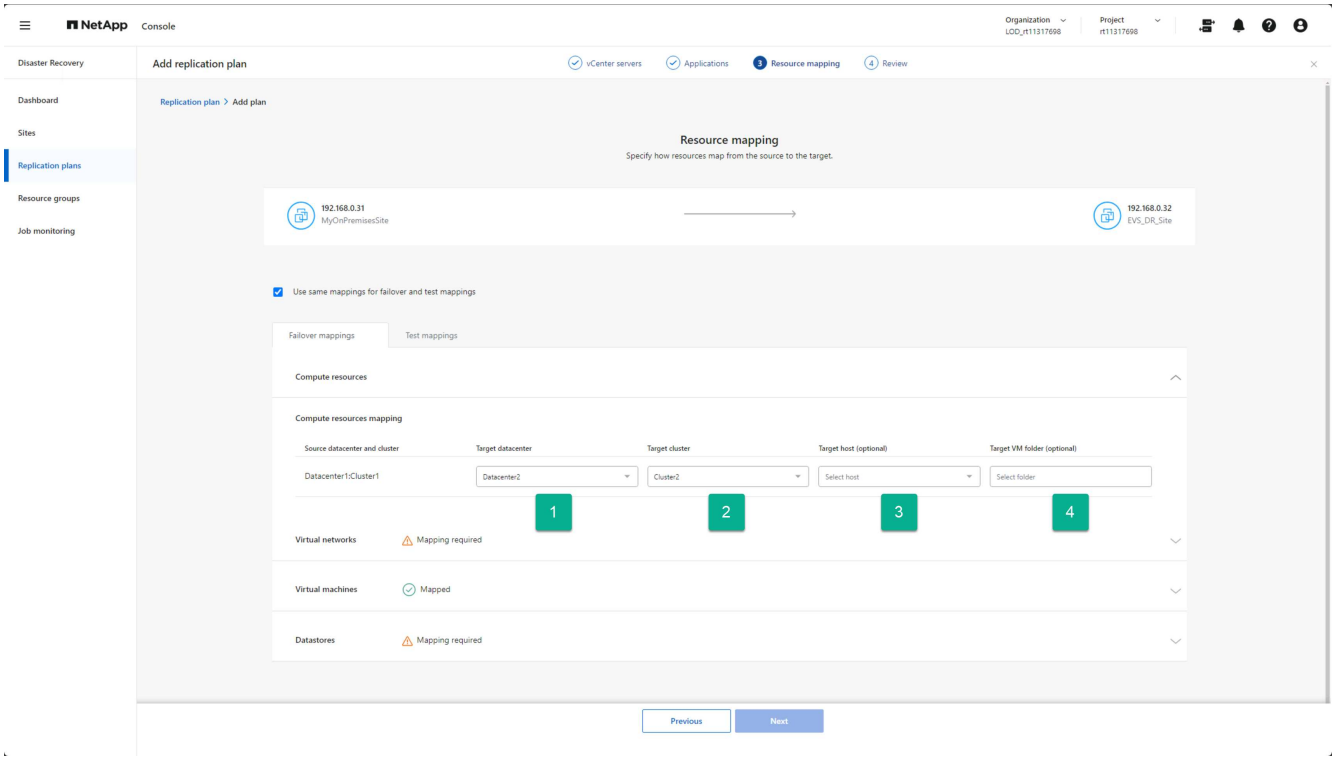
Étapes pour cartographier les ressources de calcul

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.



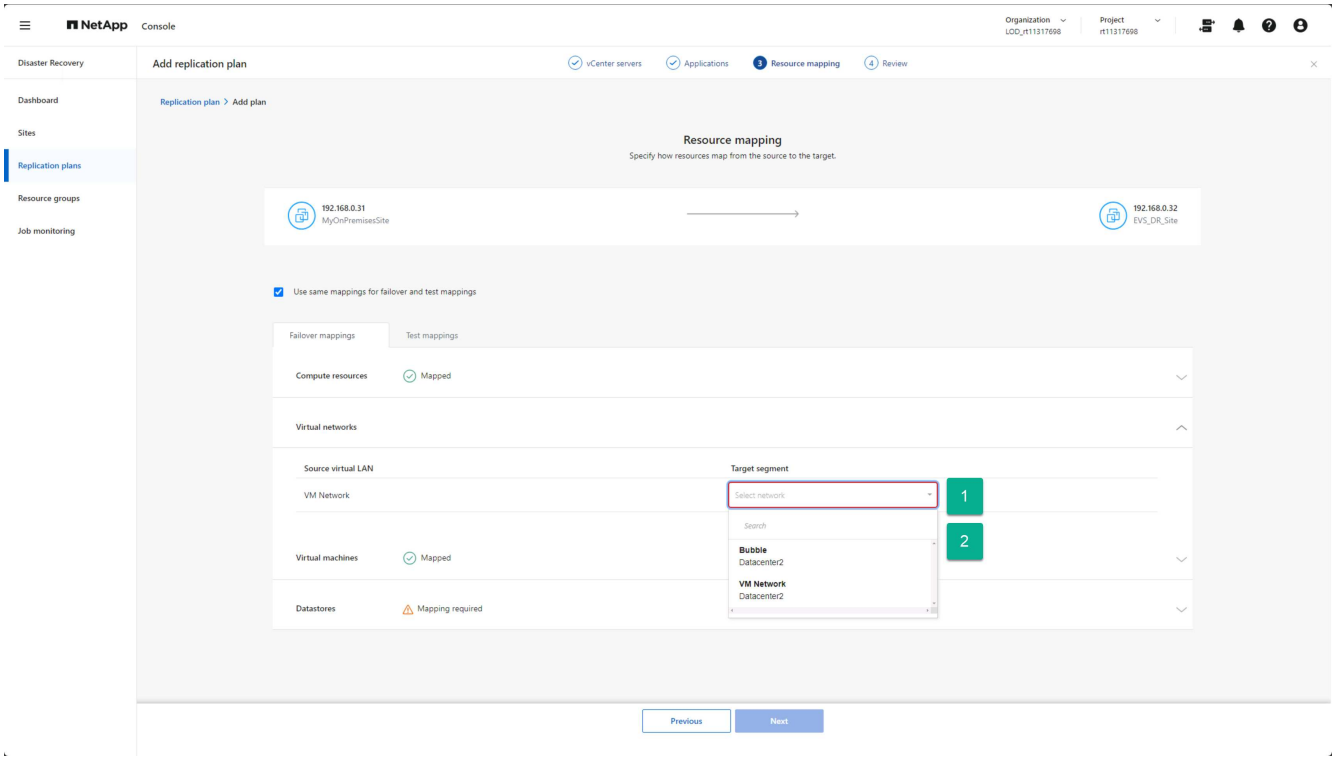
Cartographier les ressources du réseau virtuel

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.

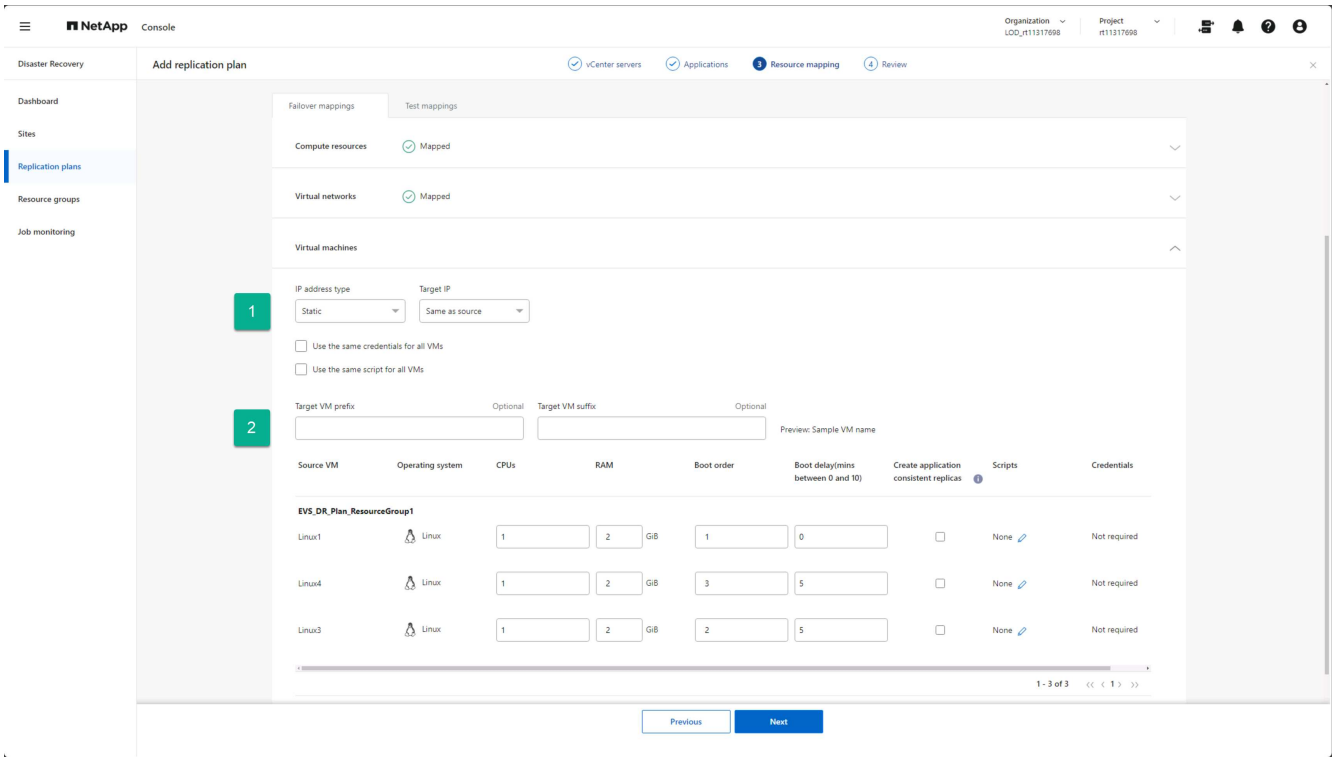
- **Mappage de sous-réseau** : cette option reconfigure l'adresse IP de chaque machine virtuelle en fonction de la configuration CIDR du réseau virtuel de destination. Pour utiliser cette fonctionnalité, assurez-vous que chaque réseau virtuel de vCenter dispose d'un paramètre CIDR défini au sein du service,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

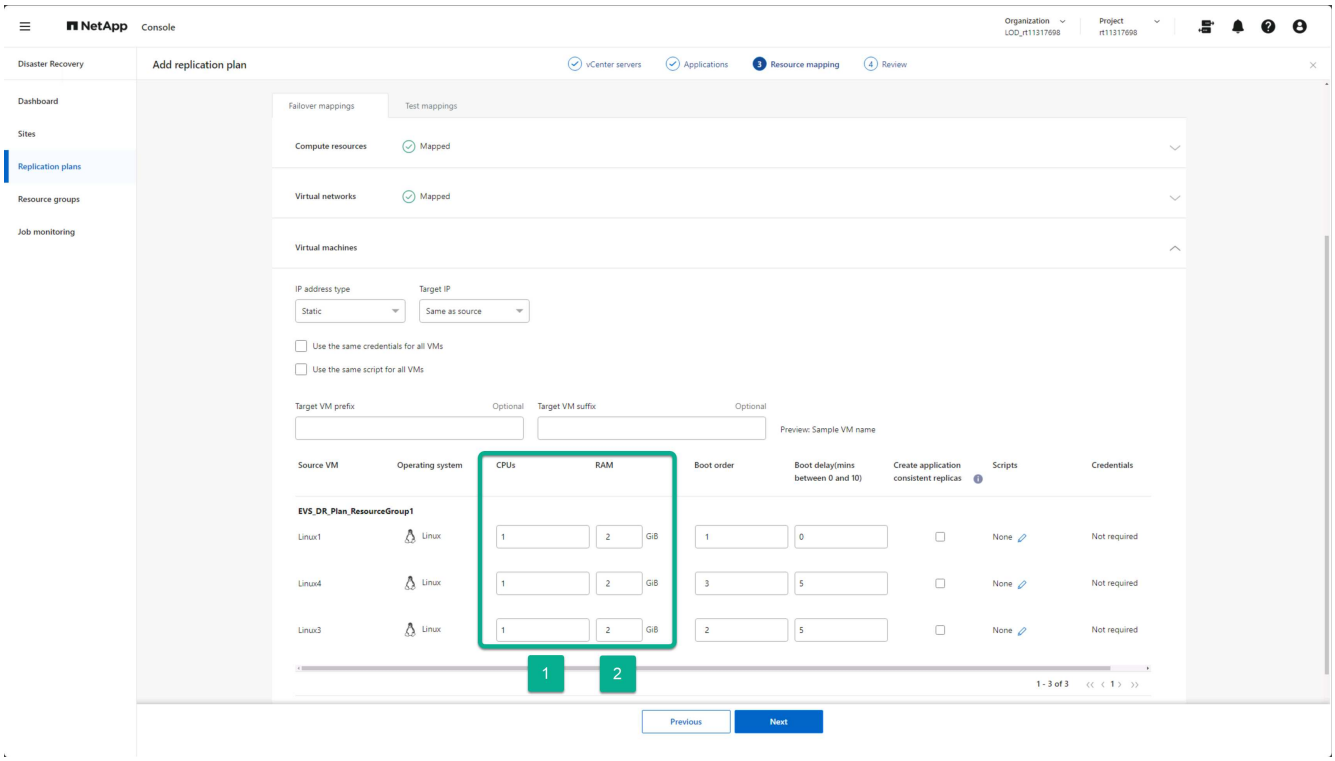
Il existe plusieurs options pour reconfigurer les ressources de calcul de la machine virtuelle. NetApp Disaster Recovery prend en charge la modification du nombre de processeurs virtuels, de la quantité de DRAM virtuelle et du nom de la machine virtuelle.

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.

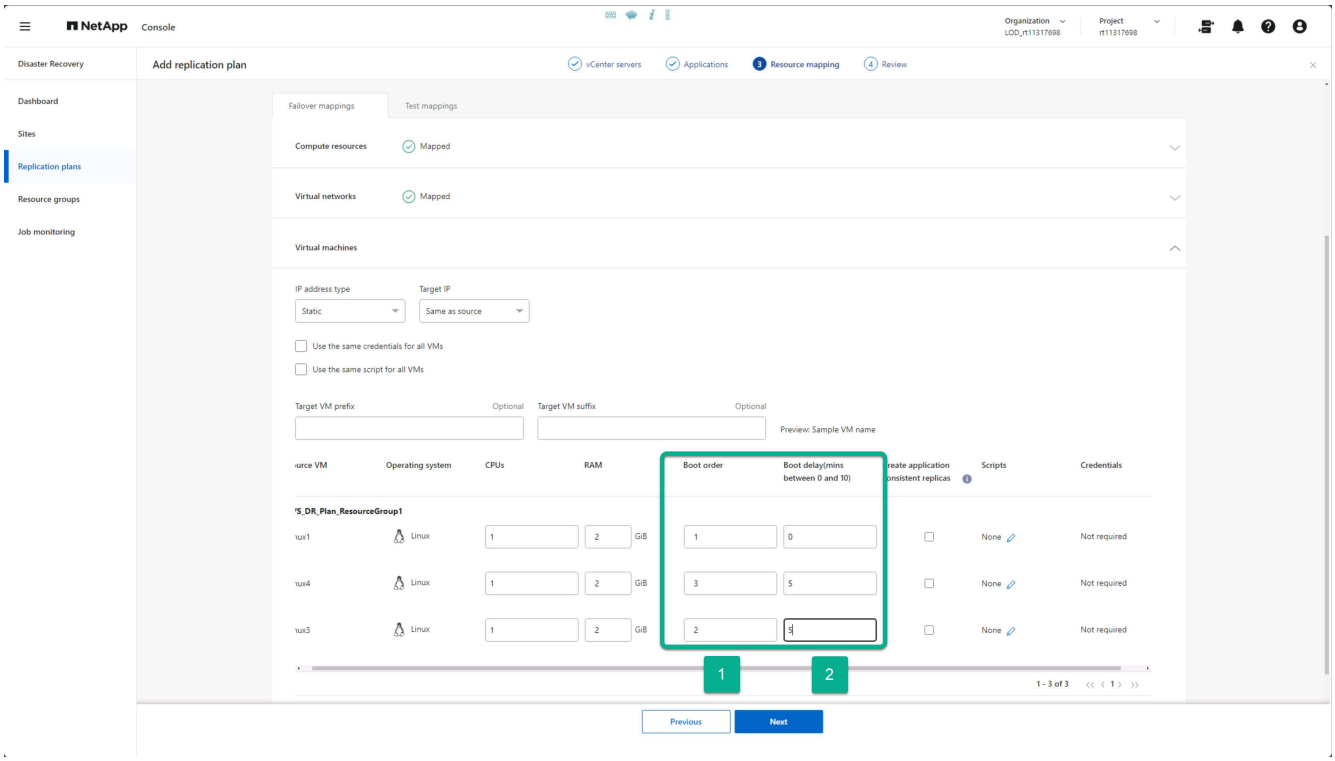


Ordre de démarrage

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.



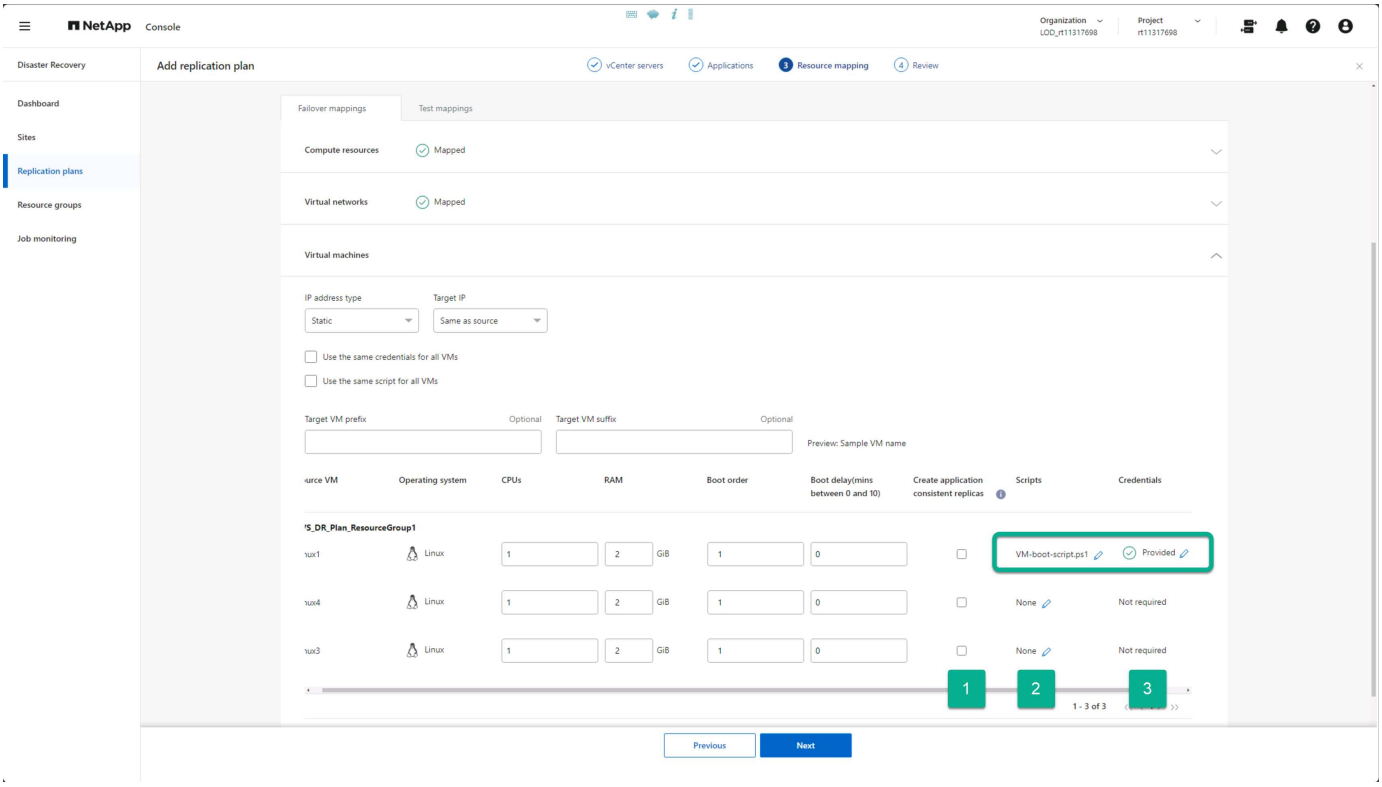
Opérations personnalisées du système d'exploitation invité

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.

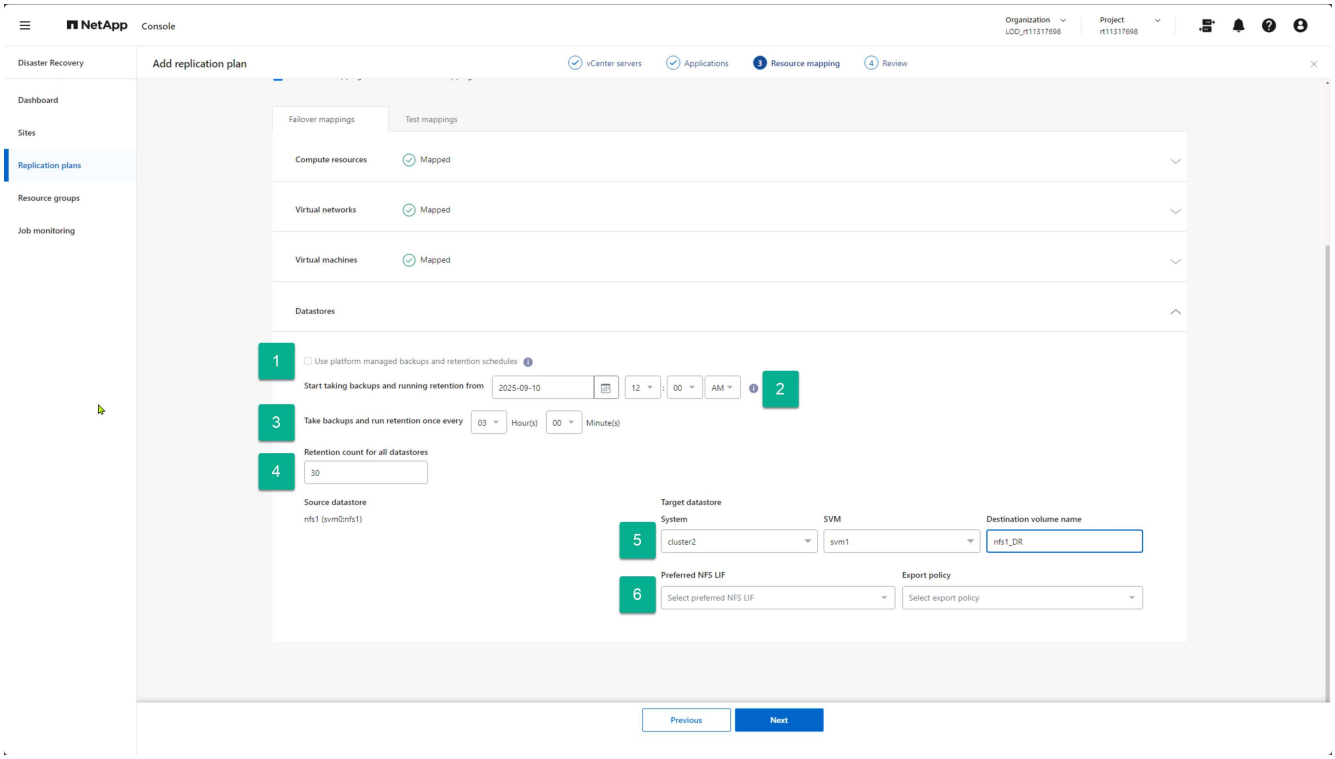
Par défaut, NetApp Disaster Recovery gère sa propre planification de réplication de snapshots. Toutefois, vous pouvez éventuellement spécifier que vous souhaitez utiliser la planification de stratégie de réplication SnapMirror existante pour la protection de la banque de données.

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

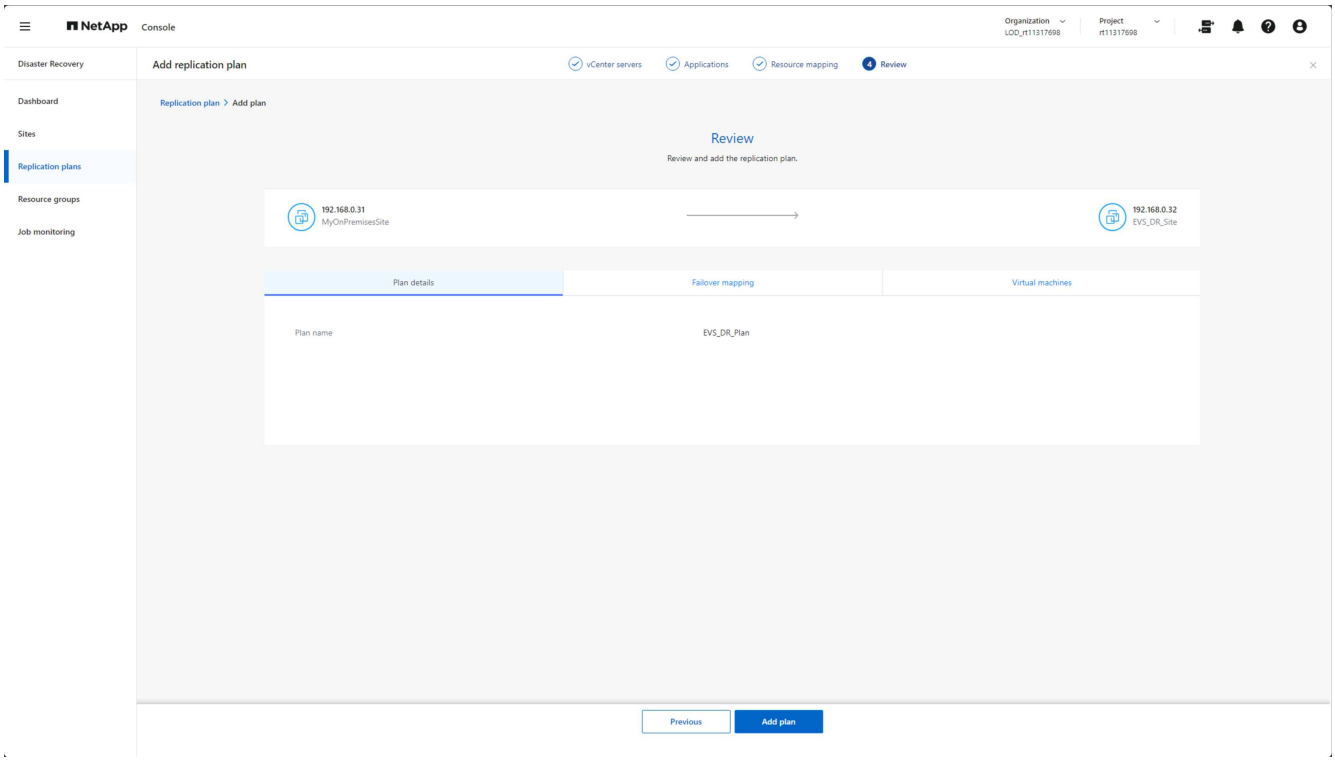
Après avoir ajouté les informations du plan de réplication dans NetApp Disaster Recovery, vérifiez que les informations que vous avez saisies sont correctes.

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



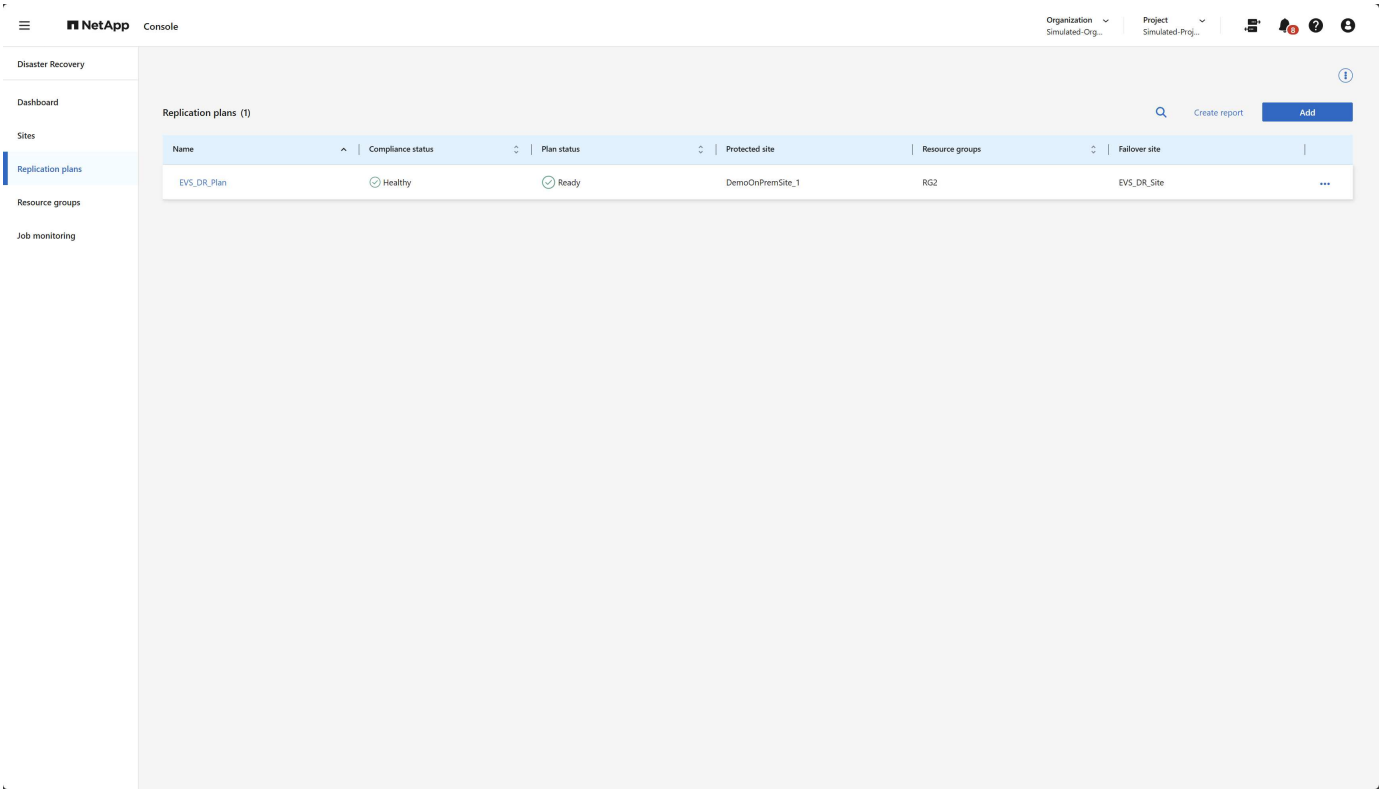
2. Lorsque vous êtes satisfait et que tous les paramètres sont corrects, sélectionnez **Ajouter un plan** en bas de l'écran.

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.

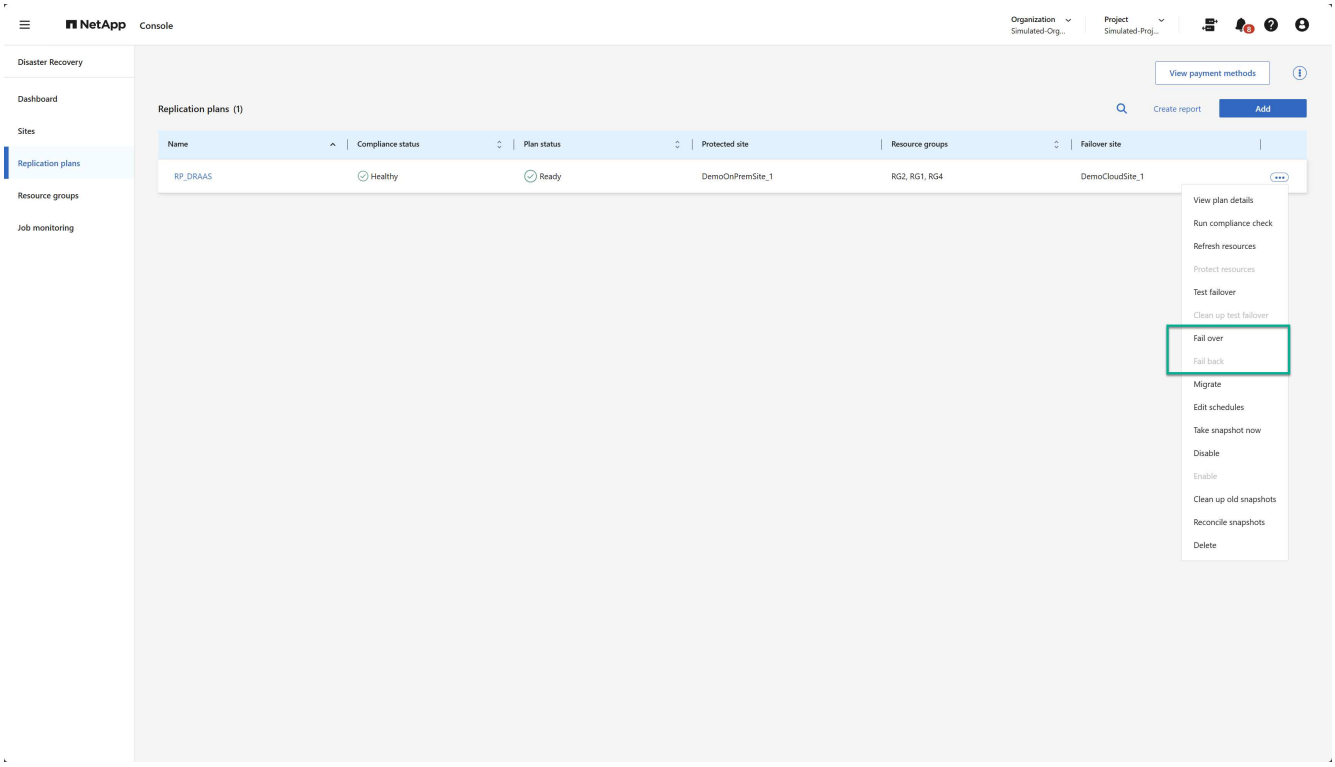
Le basculement est un processus lancé manuellement.

Étapes pour accéder à l'opération de basculement

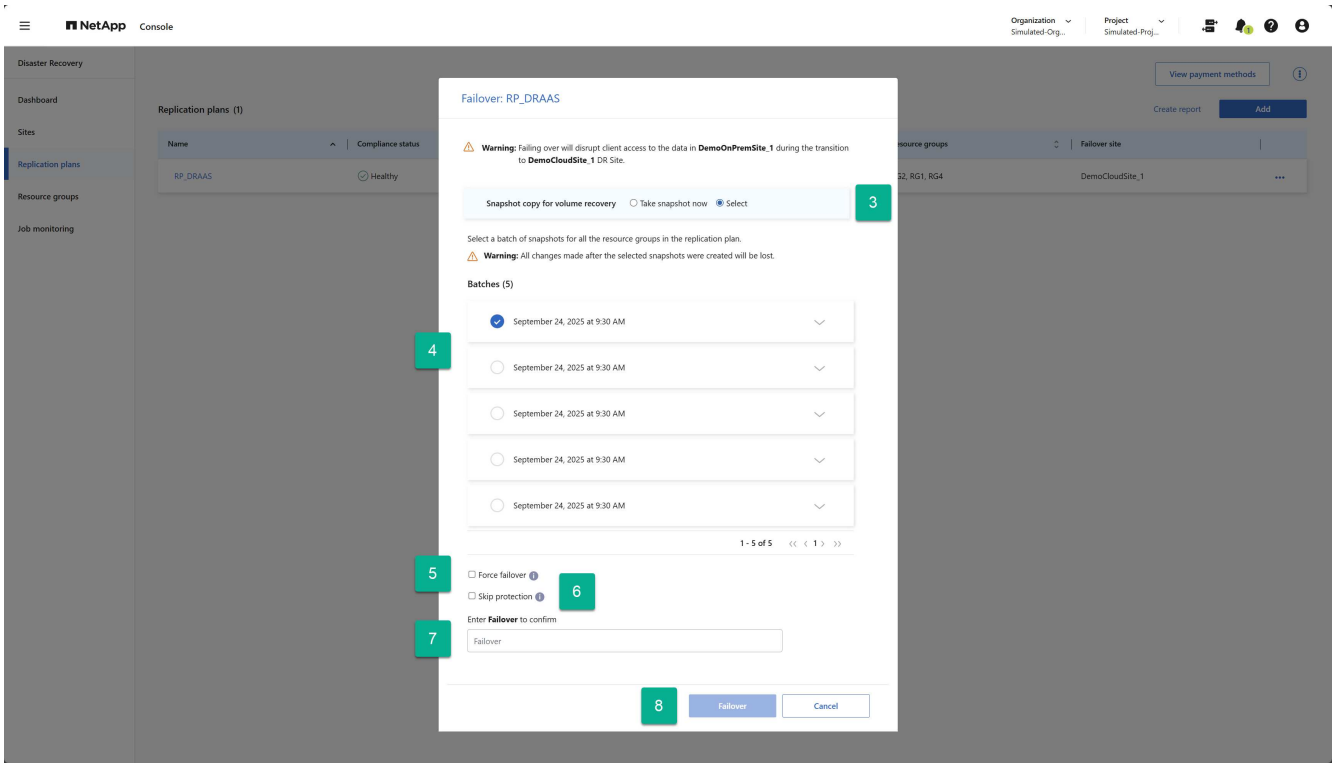
1. Dans la barre de navigation de gauche de la NetApp Console , sélectionnez **Protection** > **Reprise après sinistre**.
2. Dans le menu NetApp Disaster Recovery , sélectionnez **Plans de réplication**.

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.

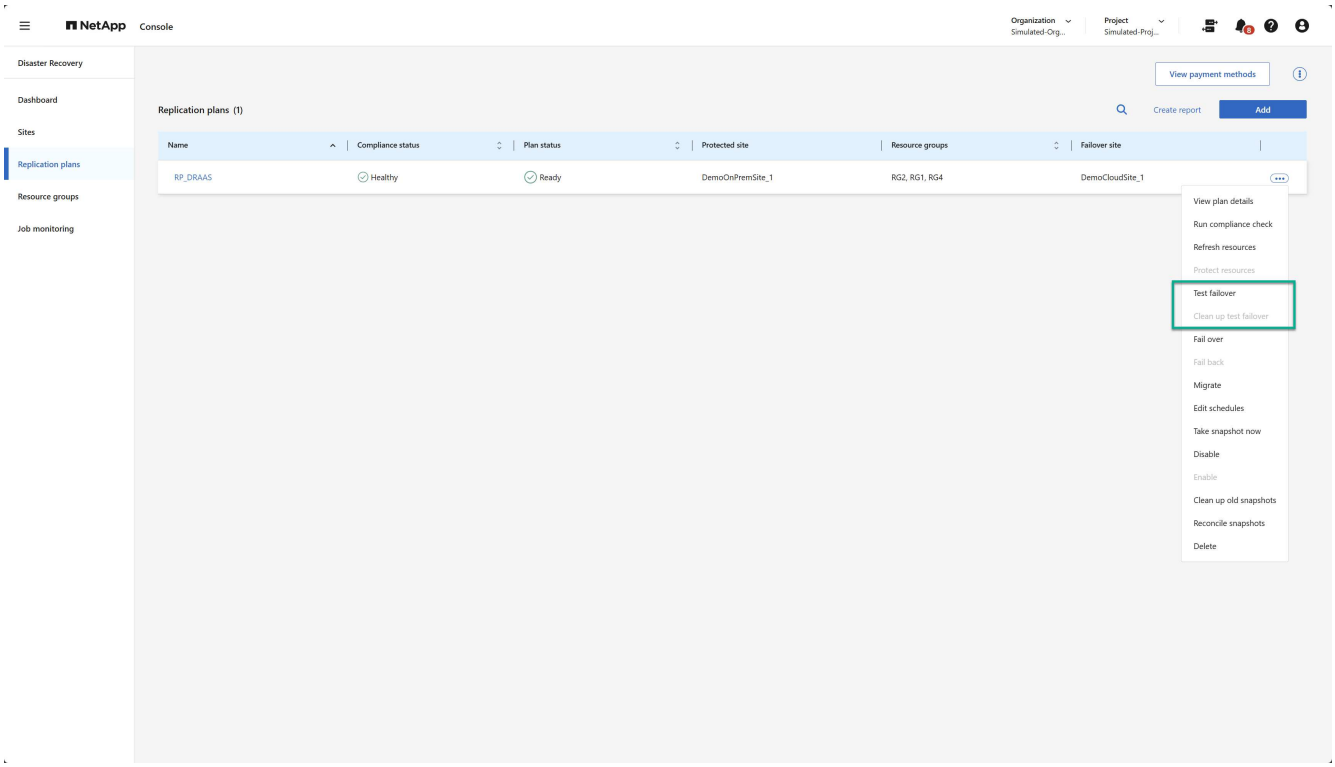
- Le site de production est toujours actif et toutes les machines virtuelles fonctionnent toujours comme prévu.
- La protection NetApp Disaster Recovery des machines virtuelles de production se poursuit.

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" .

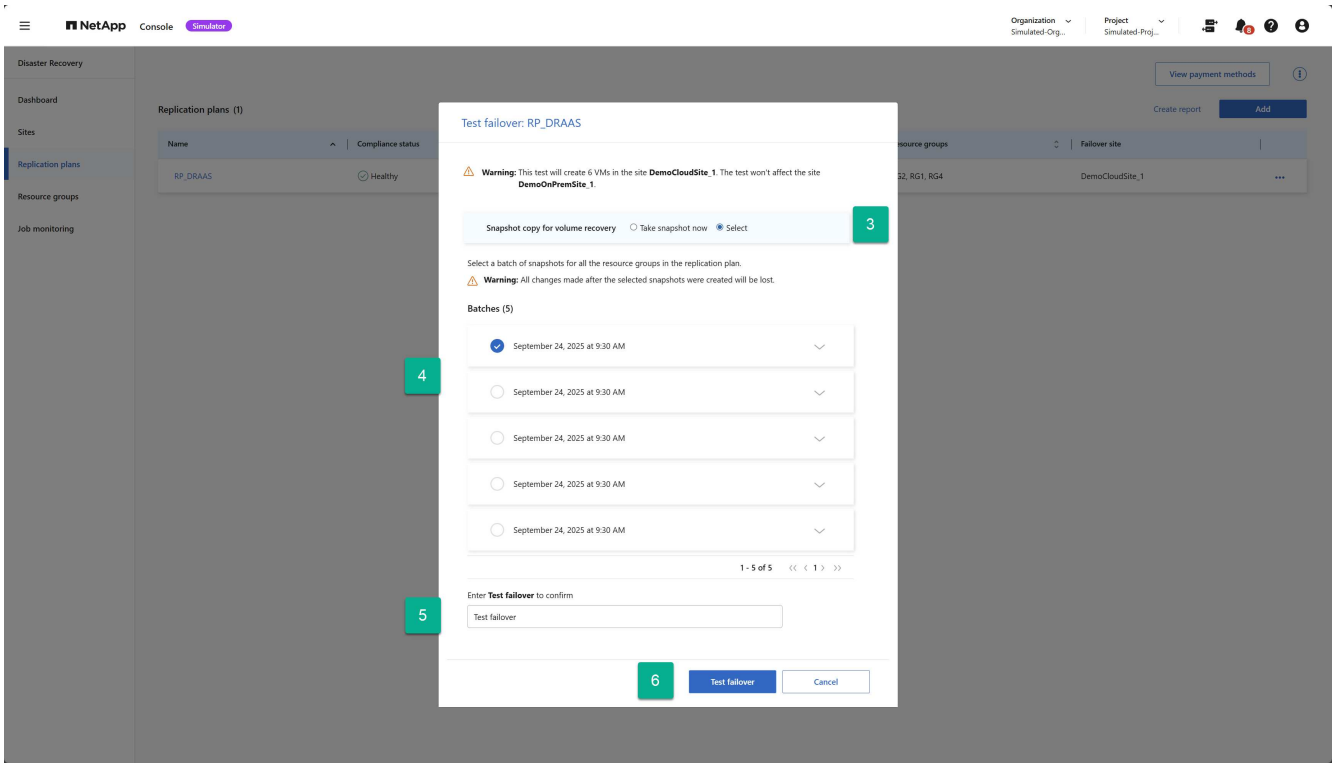
Les étapes d'exécution d'un basculement de test sont identiques à celles utilisées pour exécuter un basculement réel, sauf que vous utilisez l'opération de basculement de test dans le menu contextuel du plan de réplication.

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**.

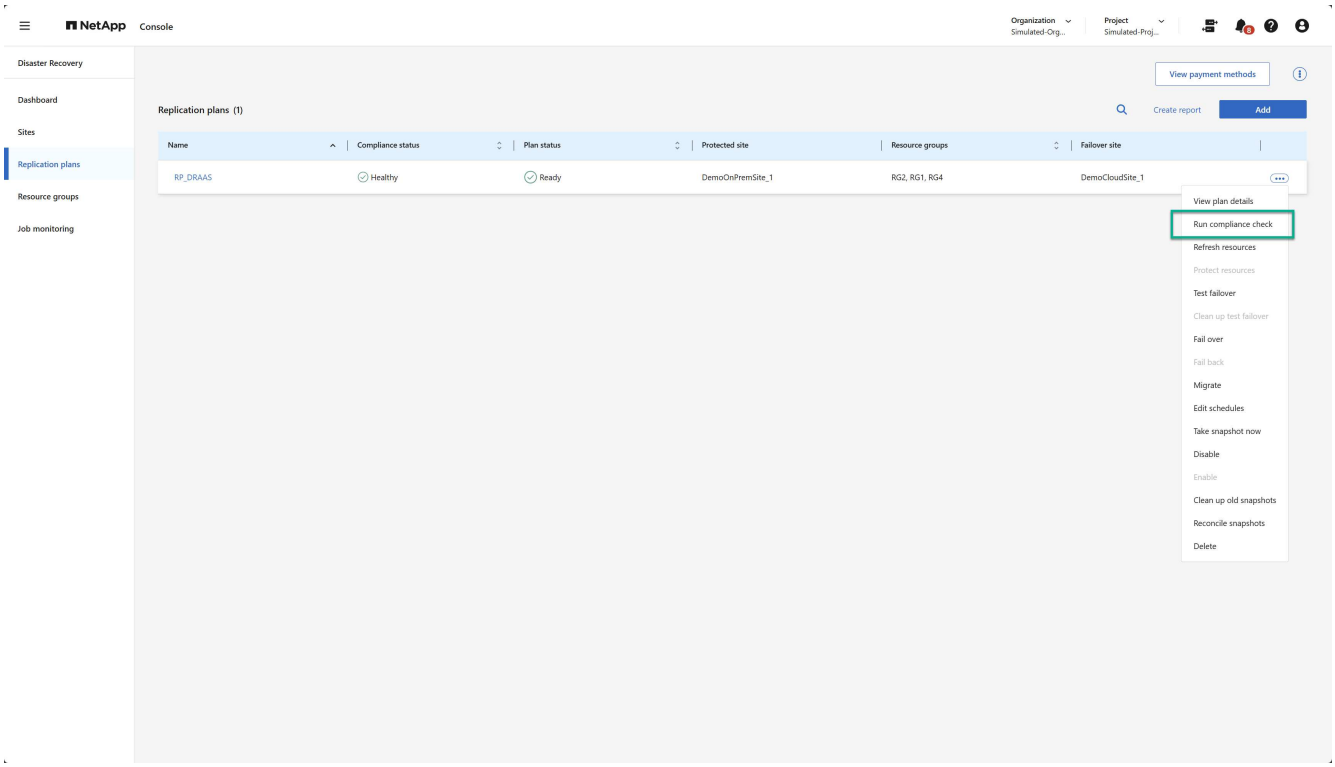


Exécuter un contrôle de conformité

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 :



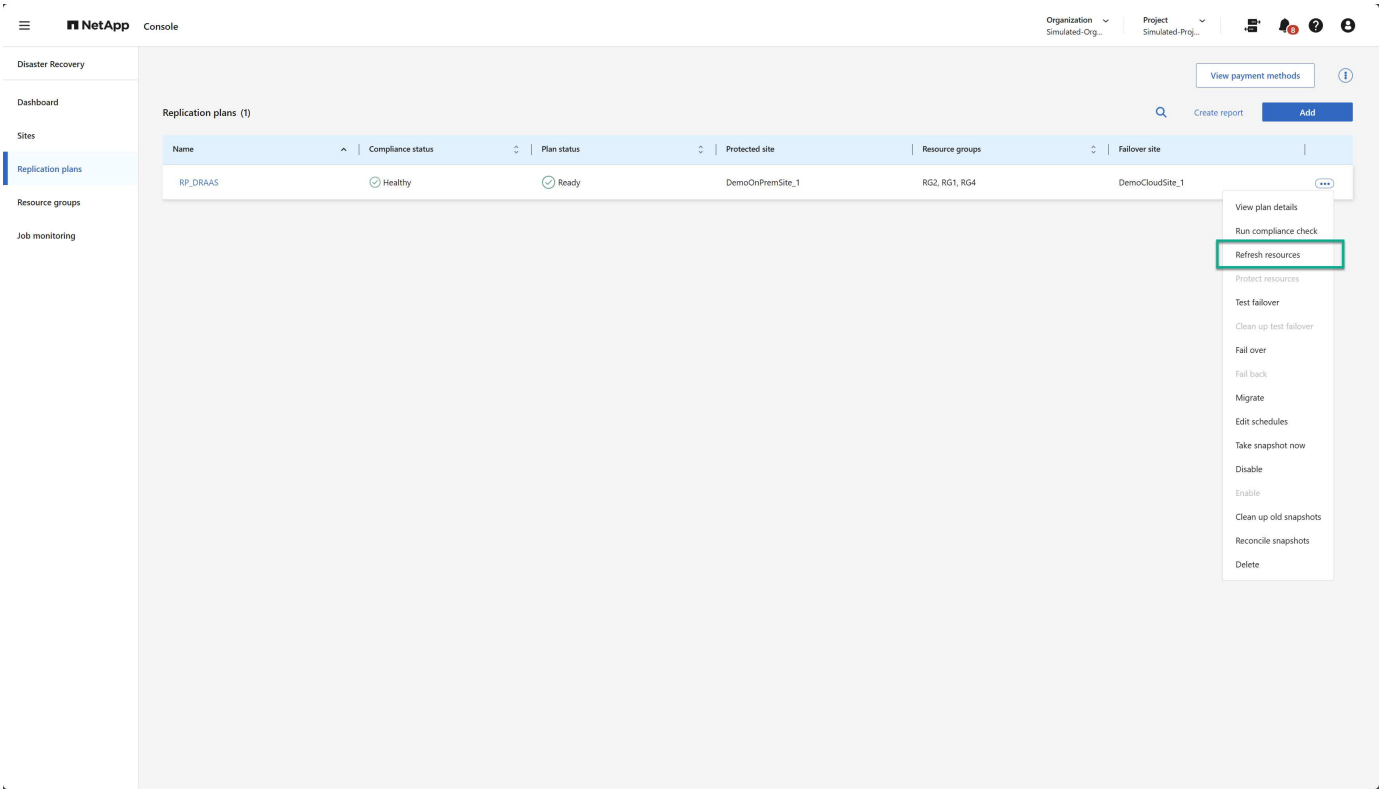
3. Pour modifier la fréquence à laquelle NetApp Disaster Recovery exécute automatiquement les contrôles de conformité, sélectionnez l'option **Modifier les planifications** dans le menu Actions du plan de réplication.

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 :

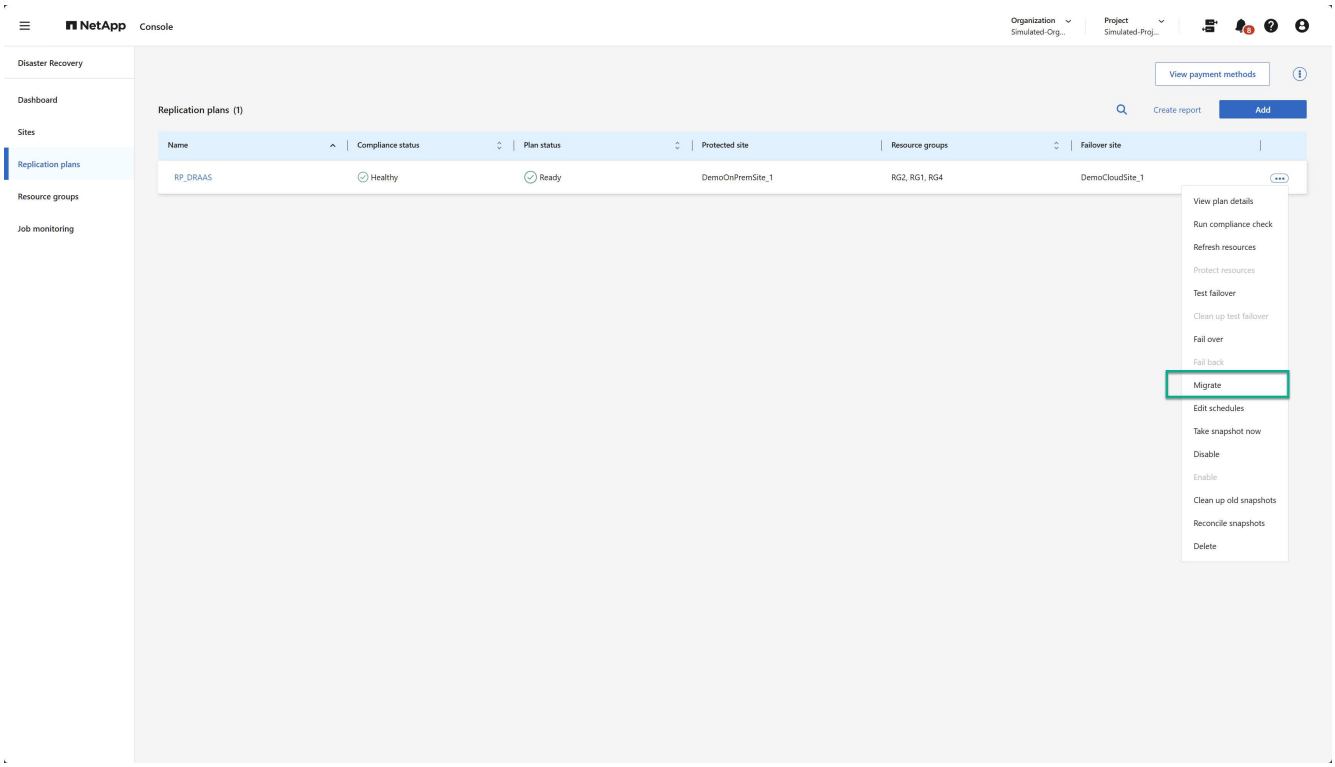
- Actualisation de vCenter : effectuez une actualisation de vCenter à chaque fois que des machines virtuelles sont ajoutées, supprimées ou déplacées hors d'un cluster vCenter :
- Actualisation du plan de réplication : effectuez une actualisation du plan de réplication chaque fois qu'une machine virtuelle 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 :

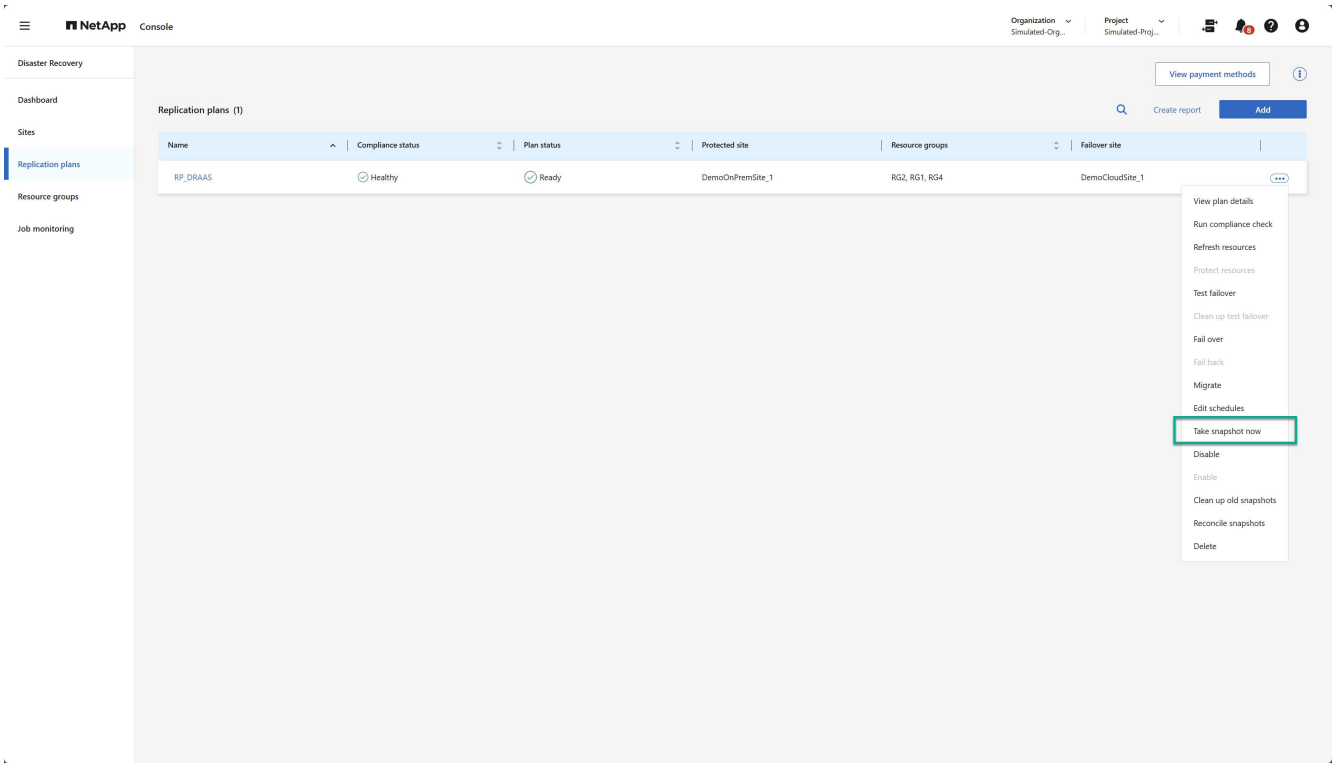


3. Saisissez les informations dans la boîte de dialogue Migrer.

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 :

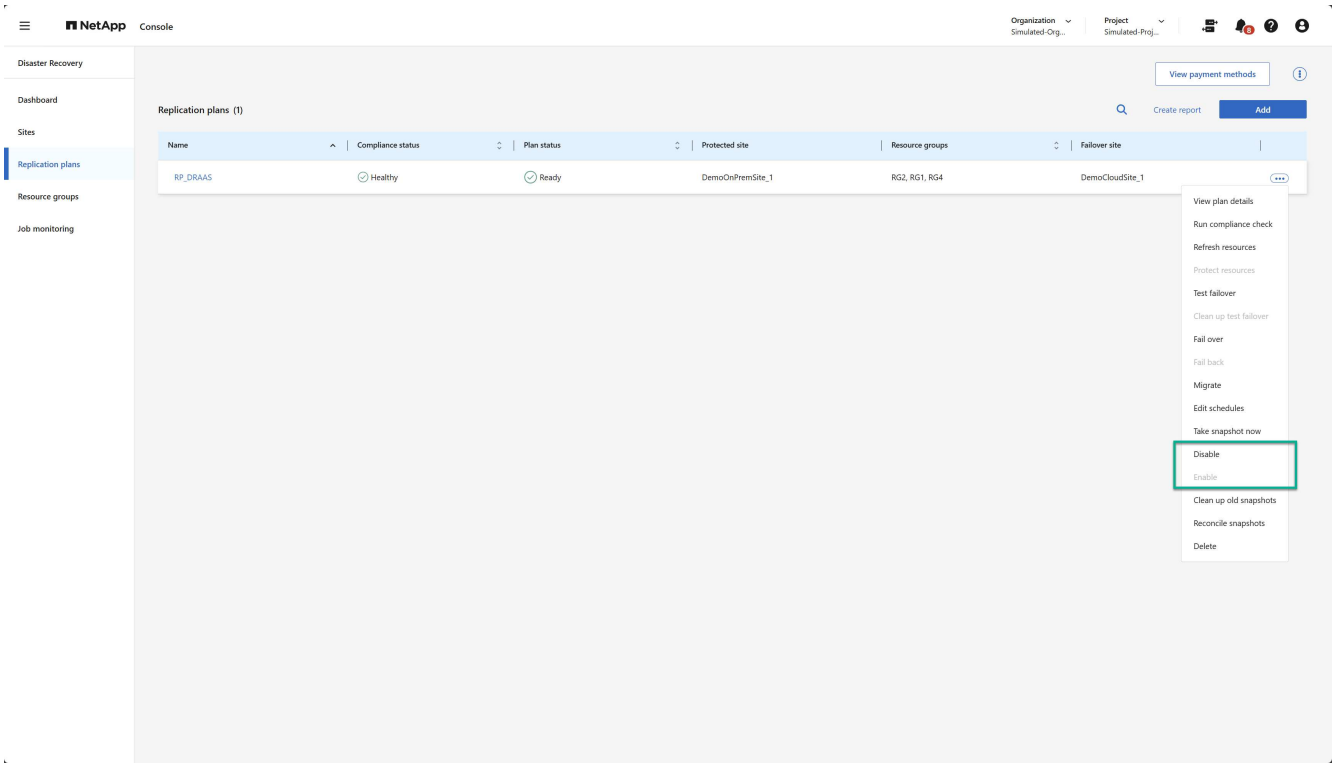


Désactiver ou activer le plan de réplication

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.

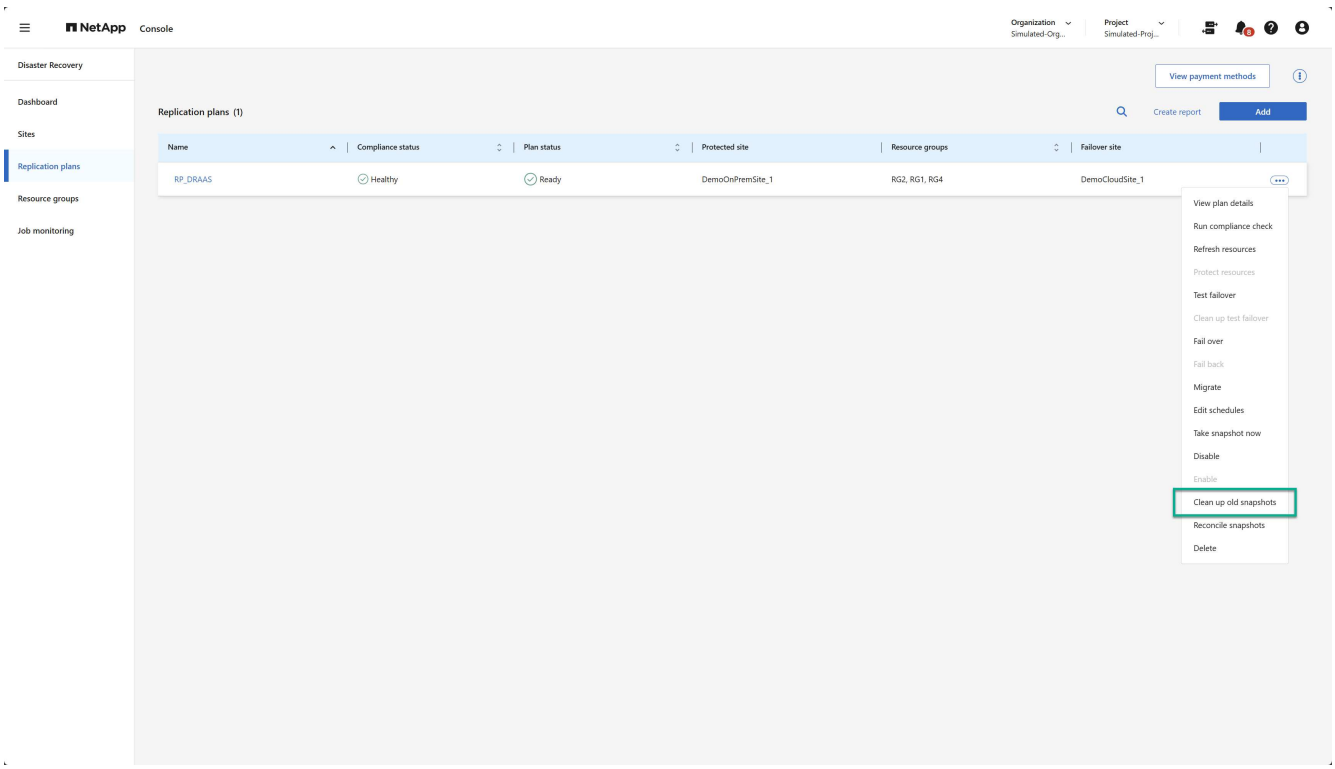
   Lorsque le plan de réplication est actif, la commande **Activer** est grisée. Lorsque le plan de réplication est désactivé, la commande **Désactiver** est grisée.



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.

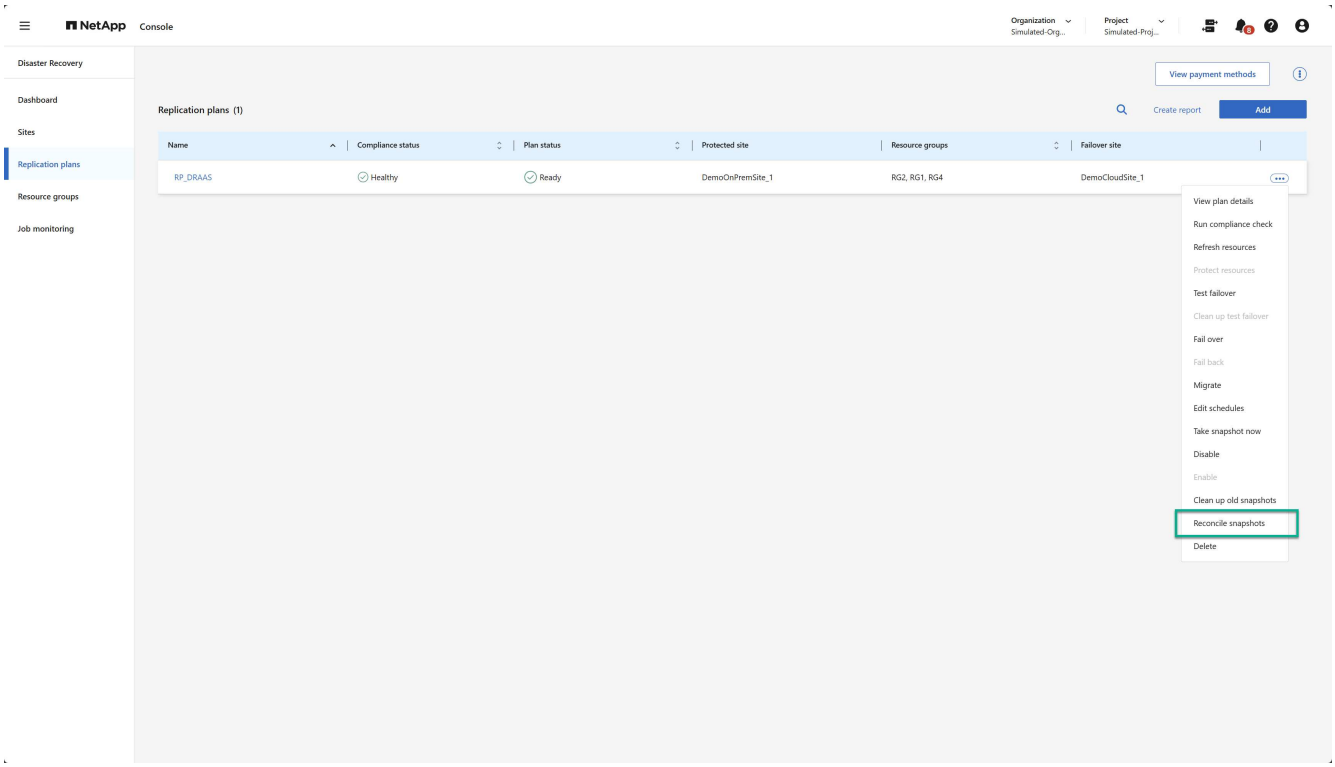
1. Sélectionnez l'option *Actions* ••• à côté du plan de réplication.
2. Pour supprimer manuellement ces anciens snapshots, sélectionnez **Nettoyer les anciens snapshots** dans le menu Actions du plan de réplication.



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.

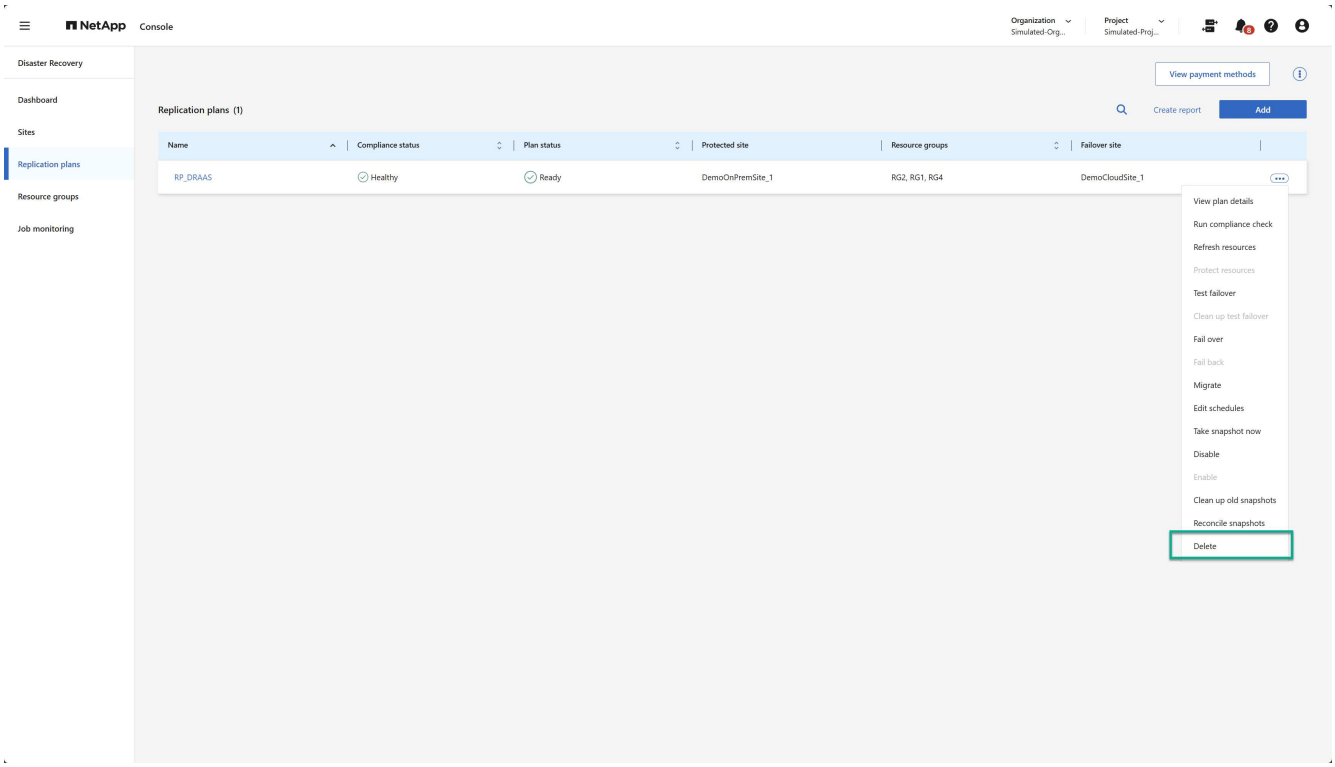
1. Sélectionnez l'option *Actions* ••• à côté du plan de réplication.
2. Pour supprimer les snapshots du cluster source qui n'existent pas sur le cluster de destination, sélectionnez **Réconcilier les snapshots** dans le menu Actions du plan de réplication.



Supprimer le plan de réplication

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

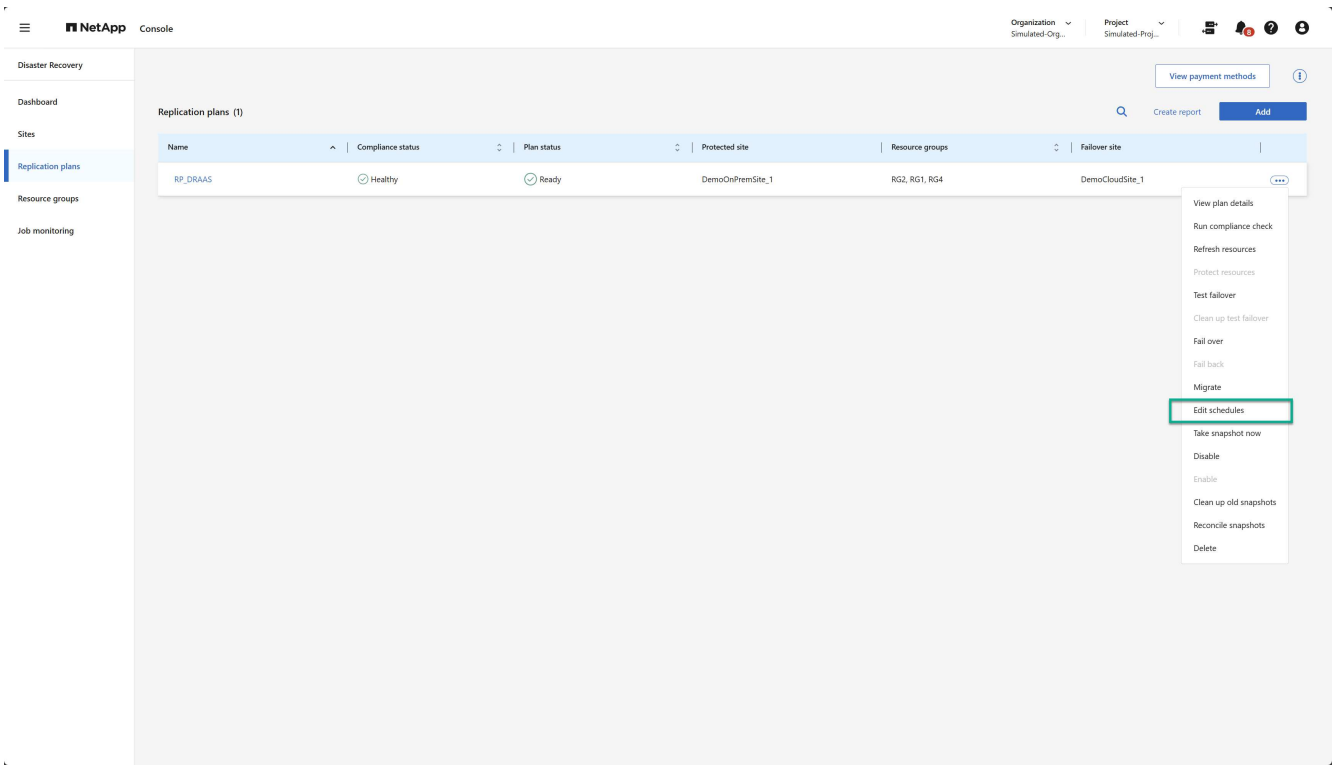
1. Sélectionnez l'option *Actions* ••• à côté du plan de réplication.
2. Pour supprimer le plan de réplication, sélectionnez **Supprimer** dans le menu contextuel du plan de réplication.



Modifier les horaires

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

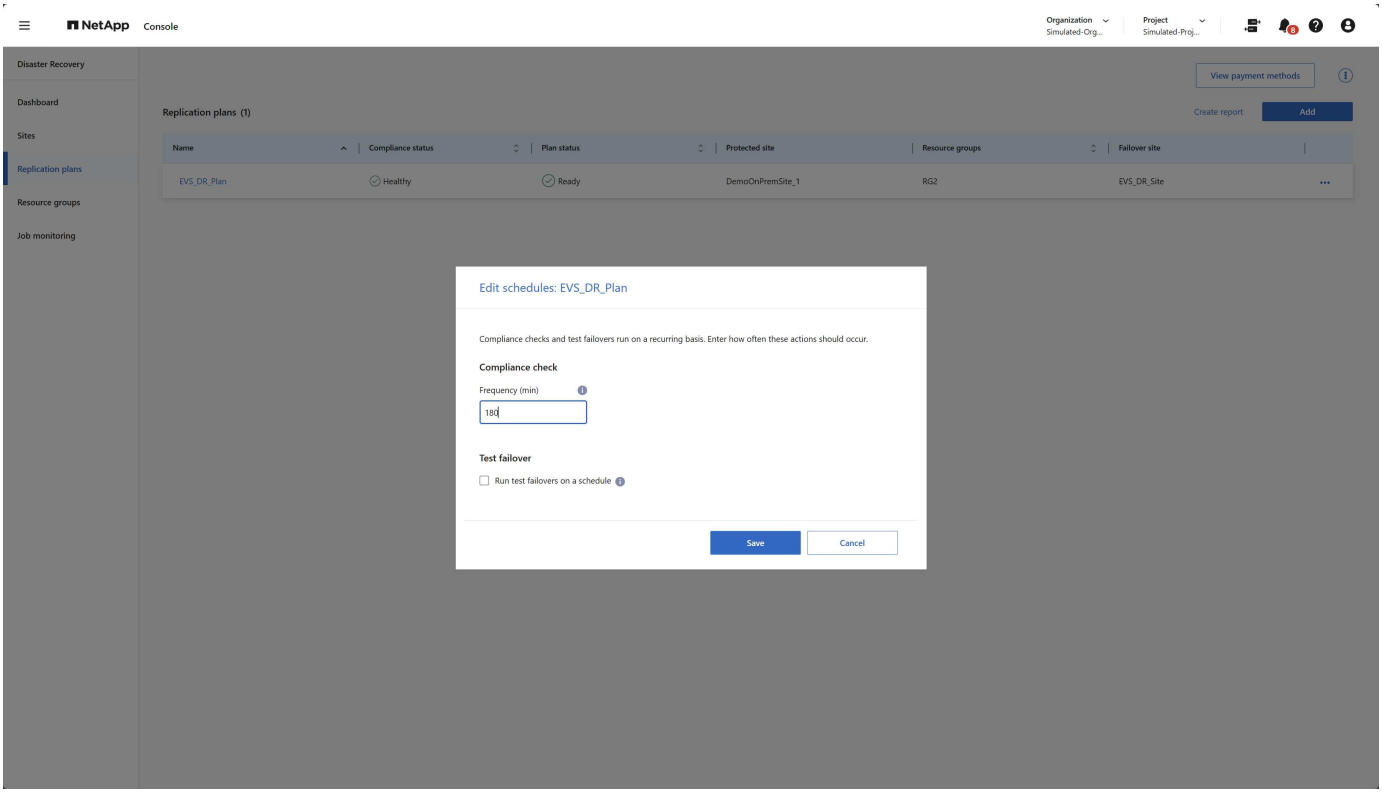
1. Sélectionnez l'option *Actions* ••• à côté du plan de réplication.
2. Pour modifier ces planifications pour l'une de ces deux opérations, sélectionnez **Modifier les planifications** pour le plan de réplication.



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

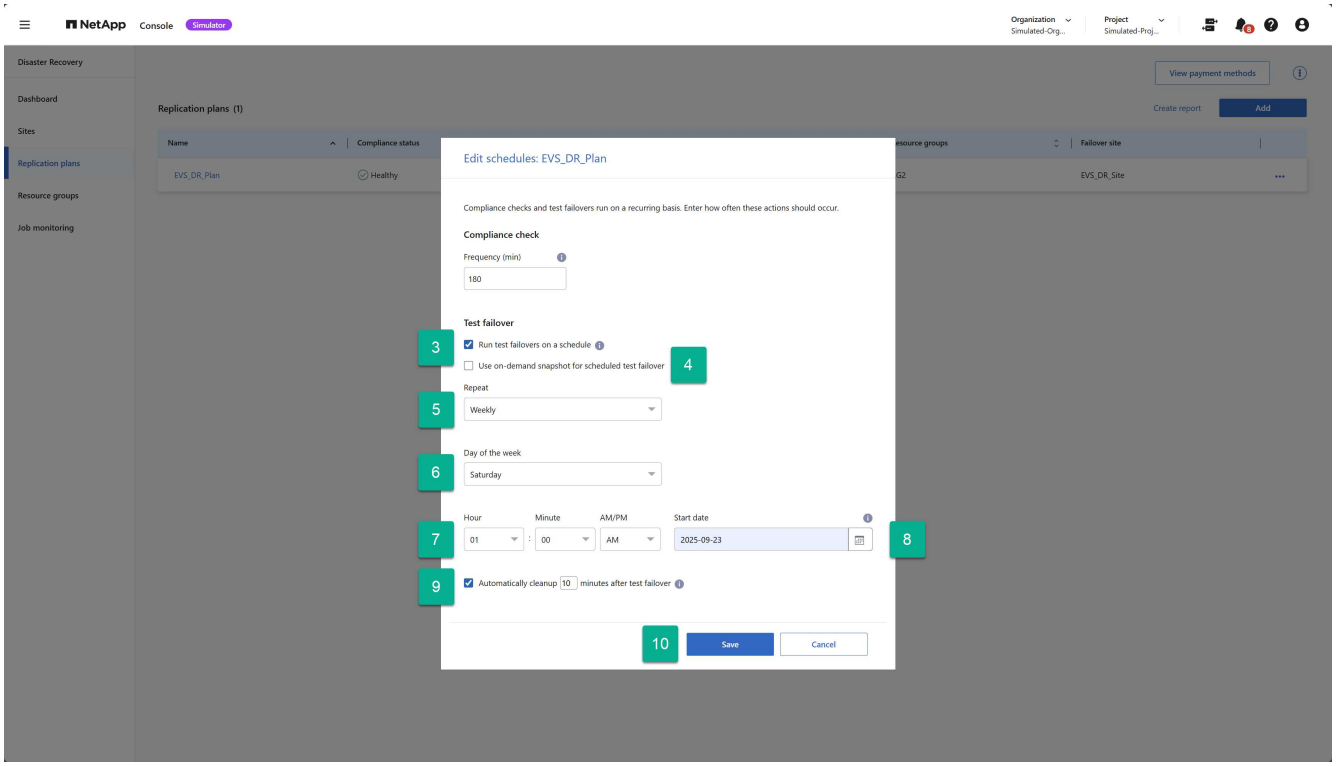
Les basculements de test sont exécutés manuellement par défaut. Vous pouvez planifier des basculements de test automatiques, ce qui permet de garantir que vos plans de réplication fonctionnent comme prévu. Pour en savoir plus sur le processus de basculement des tests, consultez"Tester le processus de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



Questions fréquemment posées sur la NetApp Disaster Recovery

Cette FAQ peut vous aider si vous cherchez simplement une réponse rapide à une question.

Quelle est l'URL de NetApp Disaster Recovery ? Pour l'URL, dans un navigateur, saisissez : "https://console.netapp.com/" pour accéder à la console NetApp .

Avez-vous besoin d'une licence pour utiliser NetApp Disaster Recovery? Une licence NetApp Disaster Recovery est requise pour un accès complet. Cependant, vous pouvez l'essayer avec l'essai gratuit.

Pour plus de détails sur la configuration des licences pour NetApp Disaster Recovery, reportez-vous à"Configurer les licences NetApp Disaster Recovery" .

Comment accéder à NetApp Disaster Recovery? NetApp Disaster Recovery ne nécessite aucune activation. L'option de récupération après sinistre apparaît automatiquement dans la navigation de gauche de la NetApp Console .

Connaissances et soutien

Inscrivez-vous pour obtenir de l'aide

L'enregistrement du support est requis pour bénéficier d'un support technique spécifique à la NetApp Console et à ses solutions de stockage et services de données. L'enregistrement du support est également requis pour activer les flux de travail clés pour les systèmes Cloud Volumes ONTAP .

L'inscription au support n'active pas la prise en charge NetApp pour un service de fichiers de fournisseur cloud. Pour obtenir une assistance technique relative à un service de fichiers de fournisseur cloud, à son infrastructure ou à toute solution utilisant le service, reportez-vous à « Obtenir de l'aide » dans la documentation de ce produit.

- "Amazon FSx pour ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Présentation de l'enregistrement de l'assistance

Il existe deux formes d'inscription pour activer le droit au support :

- Enregistrement du numéro de série de votre compte NetApp Console (votre numéro de série 960xxxxxxxxx à 20 chiffres situé sur la page Ressources de support de la console).

  Il s'agit de votre identifiant d'abonnement d'assistance unique pour tout service au sein de la console. Chaque compte de console doit être enregistré.

- Enregistrement des numéros de série Cloud Volumes ONTAP associés à un abonnement sur la place de marché de votre fournisseur de cloud (il s'agit de numéros de série 909201xxxxxxxx à 20 chiffres).

  Ces numéros de série sont communément appelés *numéros de série PAYGO* et sont générés par la NetApp Console au moment du déploiement de Cloud Volumes ONTAP .

L'enregistrement des deux types de numéros de série permet des fonctionnalités telles que l'ouverture de tickets d'assistance et la génération automatique de dossiers. L'enregistrement est terminé en ajoutant des comptes NetApp Support Site (NSS) à la console comme décrit ci-dessous.

Enregistrez la NetApp Console pour le support NetApp

Pour vous inscrire au support et activer le droit de support, un utilisateur de votre compte NetApp Console doit associer un compte de site de support NetApp à sa connexion à la console. La manière dont vous vous inscrivez au support NetApp dépend du fait que vous possédez déjà ou non un compte NetApp Support Site (NSS).

Client existant avec un compte NSS

Si vous êtes un client NetApp avec un compte NSS, il vous suffit de vous inscrire pour bénéficier de l'assistance via la console.

Étapes

1. Sélectionnez **Administration** > **Informations d'identification**.
2. Sélectionnez **Informations d'identification de l'utilisateur**.
3. Sélectionnez **Ajouter des informations d'identification NSS** et suivez l'invite d'authentification du site de support NetApp (NSS).
4. Pour confirmer que le processus d'inscription a réussi, sélectionnez l'icône Aide, puis sélectionnez **Assistance**.

   La page **Ressources** devrait indiquer que votre compte Console est enregistré pour l'assistance.

   Notez que les autres utilisateurs de la console ne verront pas ce même statut d'enregistrement de support s'ils n'ont pas associé un compte de site de support NetApp à leur connexion. Cependant, cela ne signifie pas que votre compte n'est pas enregistré pour bénéficier de l'assistance. Tant qu'un utilisateur de l'organisation a suivi ces étapes, votre compte a été enregistré.

Client existant mais pas de compte NSS

Si vous êtes un client NetApp existant avec des licences et des numéros de série existants mais *pas* de compte NSS, vous devez créer un compte NSS et l'associer à votre connexion à la console.

Étapes

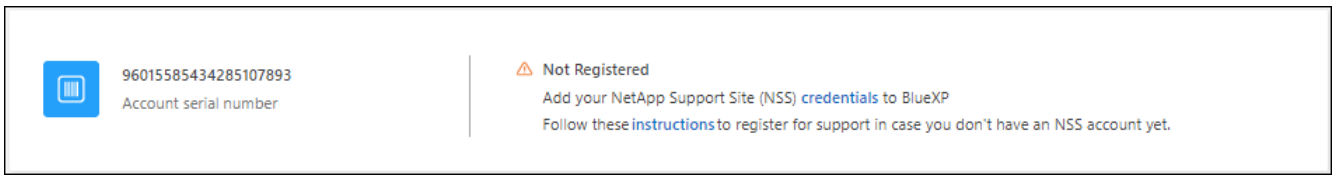
1. Créez un compte sur le site de support NetApp en remplissant le "Formulaire d'inscription des utilisateurs du site de support NetApp"
   a. Assurez-vous de sélectionner le niveau d'utilisateur approprié, qui est généralement * Client/Utilisateur final NetApp *.
   b. Assurez-vous de copier le numéro de série du compte de console (960xxxx) utilisé ci-dessus pour le champ du numéro de série. Cela accélérera le traitement du compte.
2. Associez votre nouveau compte NSS à votre connexion à la console en suivant les étapes ci-dessousClient existant avec un compte NSS .

Tout nouveau chez NetApp

Si vous êtes nouveau sur NetApp et que vous n'avez pas de compte NSS, suivez chaque étape ci-dessous.

Étapes

1. Dans le coin supérieur droit de la console, sélectionnez l'icône Aide, puis sélectionnez **Support**.
2. Recherchez le numéro de série de votre identifiant de compte sur la page d'inscription au support.



3. Accéder à "Site d'inscription au support de NetApp" et sélectionnez **Je ne suis pas un client NetApp enregistré**.
4. Remplissez les champs obligatoires (ceux avec des astérisques rouges).
5. Dans le champ **Gamme de produits**, sélectionnez **Cloud Manager**, puis sélectionnez votre fournisseur de facturation applicable.
6. Copiez le numéro de série de votre compte à l'étape 2 ci-dessus, effectuez la vérification de sécurité, puis

confirmez que vous avez lu la politique de confidentialité des données mondiales de NetApp.

Un email est immédiatement envoyé à la boîte mail prévue à cet effet pour finaliser cette transaction sécurisée. Assurez-vous de vérifier vos dossiers spam si l'e-mail de validation n'arrive pas dans quelques minutes.

7. Confirmez l'action depuis l'e-mail.

   La confirmation soumet votre demande à NetApp et vous recommande de créer un compte sur le site de support NetApp .

8. Créez un compte sur le site de support NetApp en remplissant le "Formulaire d'inscription des utilisateurs du site de support NetApp"
   a. Assurez-vous de sélectionner le niveau d'utilisateur approprié, qui est généralement * Client/Utilisateur final NetApp *.
   b. Assurez-vous de copier le numéro de série du compte (960xxxx) utilisé ci-dessus pour le champ du numéro de série. Cela accélérera le traitement.

Après avoir terminé

NetApp devrait vous contacter au cours de ce processus. Il s'agit d'un exercice d'intégration unique pour les nouveaux utilisateurs.

Une fois que vous avez votre compte de site de support NetApp , associez le compte à votre connexion à la console en suivant les étapes ci-dessousClient existant avec un compte NSS .

Associer les informations d'identification NSS pour la prise en charge de Cloud Volumes ONTAP

L'association des informations d'identification du site de support NetApp à votre compte de console est requise pour activer les workflows clés suivants pour Cloud Volumes ONTAP:

- Enregistrement des systèmes Cloud Volumes ONTAP prépayés pour le support

  Fournir votre compte NSS est nécessaire pour activer le support de votre système et pour accéder aux ressources de support technique NetApp .

- Déploiement de Cloud Volumes ONTAP lorsque vous apportez votre propre licence (BYOL)

  Il est nécessaire de fournir votre compte NSS pour que la console puisse télécharger votre clé de licence et activer l'abonnement pour la durée que vous avez achetée. Cela inclut les mises à jour automatiques pour les renouvellements de mandat.

- Mise à niveau du logiciel Cloud Volumes ONTAP vers la dernière version

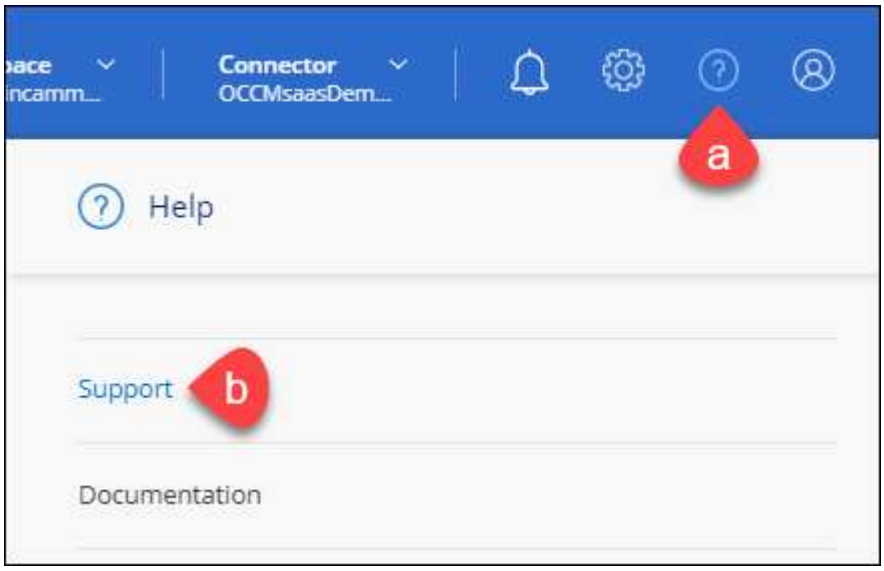
L'association des informations d'identification NSS à votre compte de NetApp Console est différente du compte NSS associé à une connexion utilisateur de console.

Ces informations d'identification NSS sont associées à votre ID de compte de console spécifique. Les utilisateurs appartenant à l'organisation Console peuvent accéder à ces informations d'identification depuis **Support > Gestion NSS**.

- Si vous disposez d'un compte client, vous pouvez ajouter un ou plusieurs comptes NSS.
- Si vous disposez d'un compte partenaire ou revendeur, vous pouvez ajouter un ou plusieurs comptes NSS, mais ils ne peuvent pas être ajoutés aux côtés des comptes de niveau client.

Étapes

1. Dans le coin supérieur droit de la console, sélectionnez l'icône Aide, puis sélectionnez **Support**.



2. Sélectionnez **Gestion NSS > Ajouter un compte NSS**.
3. Lorsque vous y êtes invité, sélectionnez **Continuer** pour être redirigé vers une page de connexion Microsoft.

   NetApp utilise Microsoft Entra ID comme fournisseur d'identité pour les services d'authentification spécifiques au support et aux licences.

4. Sur la page de connexion, indiquez votre adresse e-mail et votre mot de passe enregistrés sur le site de support NetApp pour effectuer le processus d'authentification.

   Ces actions permettent à la console d'utiliser votre compte NSS pour des tâches telles que les téléchargements de licences, la vérification des mises à niveau de logiciels et les futures inscriptions au support.

   Notez ce qui suit :

   - Le compte NSS doit être un compte de niveau client (pas un compte invité ou temporaire). Vous pouvez avoir plusieurs comptes NSS au niveau client.
   - Il ne peut y avoir qu'un seul compte NSS si ce compte est un compte de niveau partenaire. Si vous essayez d'ajouter des comptes NSS au niveau client et qu'un compte au niveau partenaire existe, vous obtiendrez le message d'erreur suivant :

     « Le type de client NSS n'est pas autorisé pour ce compte car il existe déjà des utilisateurs NSS de types différents. »

   Il en va de même si vous disposez de comptes NSS préexistants au niveau client et que vous essayez d'ajouter un compte au niveau partenaire.

   - Une fois la connexion réussie, NetApp stockera le nom d'utilisateur NSS.

     Il s'agit d'un identifiant généré par le système qui correspond à votre e-mail. Sur la page **Gestion NSS**, vous pouvez afficher votre e-mail à partir du ••• menu.

- Si vous avez besoin d'actualiser vos jetons d'identification de connexion, il existe également une option **Mettre à jour les informations d'identification** dans le ••• menu.

  L'utilisation de cette option vous invite à vous reconnecter. Notez que le jeton de ces comptes expire après 90 jours. Une notification sera publiée pour vous en informer.

Obtenir de l'aide

NetApp fournit un support pour NetApp Console et ses services cloud de diverses manières. De nombreuses options d'auto-assistance gratuites sont disponibles 24h/24 et 7j/7, telles que des articles de la base de connaissances (KB) et un forum communautaire. Votre inscription au support inclut une assistance technique à distance via un ticket web.

Obtenir de l'aide pour un service de fichiers d'un fournisseur cloud

Pour obtenir une assistance technique relative à un service de fichiers de fournisseur cloud, à son infrastructure ou à toute solution utilisant le service, reportez-vous à la documentation de ce produit.

- "Amazon FSx pour ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Pour bénéficier d'un support technique spécifique à NetApp et à ses solutions de stockage et services de données, utilisez les options de support décrites ci-dessous.

Utiliser les options d'auto-assistance

Ces options sont disponibles gratuitement, 24 heures sur 24, 7 jours sur 7 :

- Documentation

  La documentation de la NetApp Console que vous consultez actuellement.

- "Base de connaissances"

  Recherchez dans la base de connaissances NetApp pour trouver des articles utiles pour résoudre les problèmes.

- "Communautés"

  Rejoignez la communauté NetApp Console pour suivre les discussions en cours ou en créer de nouvelles.

Créer un dossier auprès du support NetApp

En plus des options d'auto-assistance ci-dessus, vous pouvez travailler avec un spécialiste du support NetApp pour résoudre tout problème après avoir activé le support.

Avant de commencer

- Pour utiliser la fonctionnalité **Créer un dossier**, vous devez d'abord associer vos informations

d'identification du site de support NetApp à votre connexion à la console. "Découvrez comment gérer les informations d'identification associées à votre connexion à la console" .

- Si vous ouvrez un dossier pour un système ONTAP doté d'un numéro de série, votre compte NSS doit être associé au numéro de série de ce système.

Étapes

1. Dans la NetApp Console, sélectionnez **Aide > Support**.
2. Sur la page **Ressources**, choisissez l'une des options disponibles sous Support technique :

   a. Sélectionnez **Appelez-nous** si vous souhaitez parler à quelqu'un au téléphone. Vous serez redirigé vers une page sur netapp.com qui répertorie les numéros de téléphone que vous pouvez appeler.

   b. Sélectionnez **Créer un dossier** pour ouvrir un ticket avec un spécialiste du support NetApp :

      - **Service** : sélectionnez le service auquel le problème est associé. Par exemple, * NetApp Console* lorsqu'il s'agit d'un problème de support technique lié aux flux de travail ou aux fonctionnalités de la console.
      - **Système** : Si applicable au stockage, sélectionnez * Cloud Volumes ONTAP* ou **On-Prem**, puis l'environnement de travail associé.

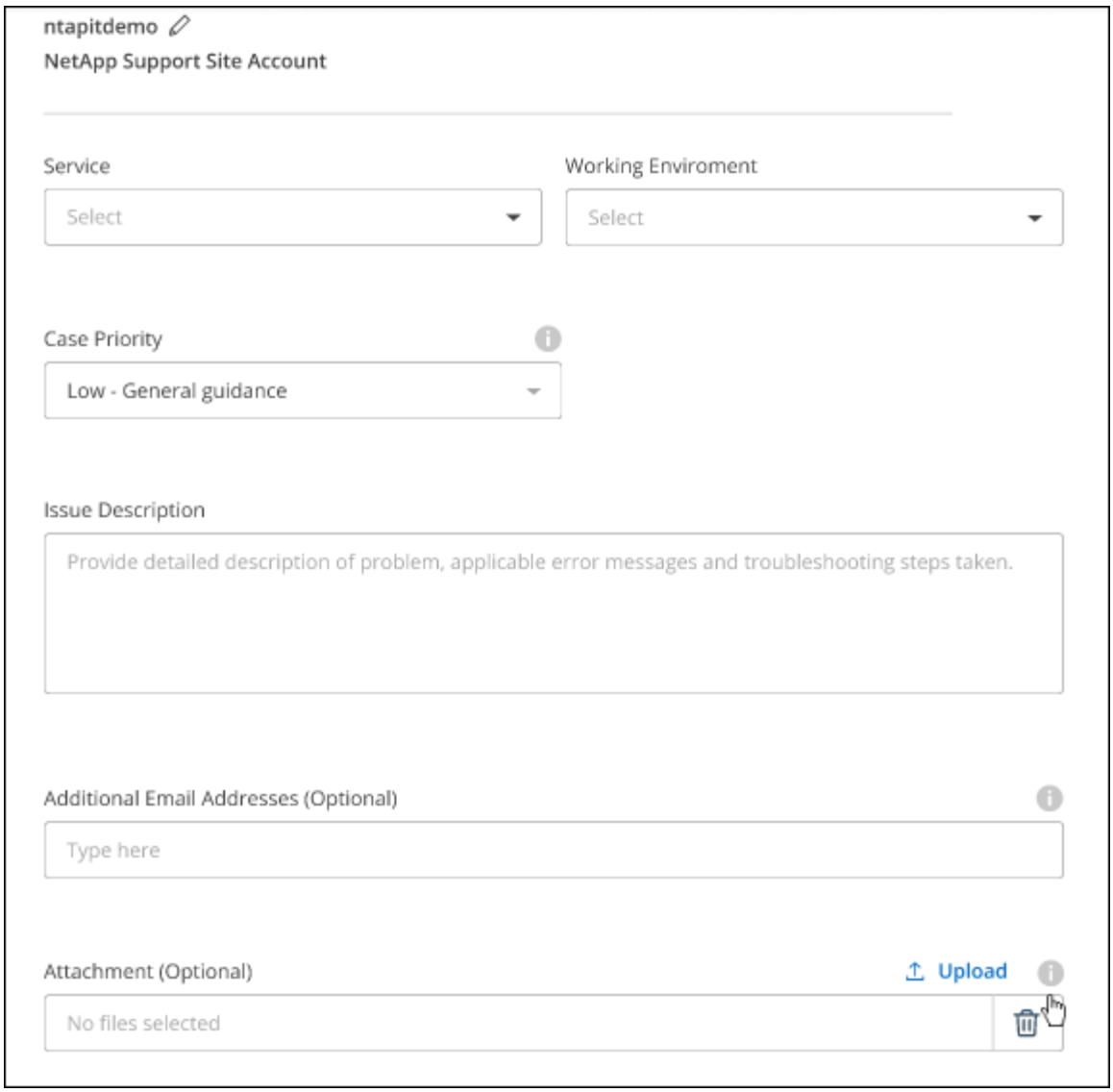
        La liste des systèmes est dans le périmètre de l'organisation de la console et de l'agent de console que vous avez sélectionné dans la bannière supérieure.

      - **Priorité du cas** : Choisissez la priorité du cas, qui peut être Faible, Moyenne, Élevée ou Critique.

        Pour en savoir plus sur ces priorités, passez votre souris sur l'icône d'information à côté du nom du champ.

      - **Description du problème** : Fournissez une description détaillée de votre problème, y compris tous les messages d'erreur applicables ou les étapes de dépannage que vous avez effectuées.
      - **Adresses e-mail supplémentaires** : saisissez des adresses e-mail supplémentaires si vous souhaitez informer quelqu'un d'autre de ce problème.
      - **Pièce jointe (facultatif)** : Téléchargez jusqu'à cinq pièces jointes, une à la fois.

        Les pièces jointes sont limitées à 25 Mo par fichier. Les extensions de fichiers suivantes sont prises en charge : txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx et csv.



Après avoir terminé

Une fenêtre contextuelle apparaîtra avec votre numéro de dossier d'assistance. Un spécialiste du support NetApp examinera votre cas et vous répondra dans les plus brefs délais.

Pour un historique de vos demandes d'assistance, vous pouvez sélectionner **Paramètres > Chronologie** et rechercher les actions nommées « créer une demande d'assistance ». Un bouton à l'extrême droite vous permet de développer l'action pour voir les détails.

Il est possible que vous rencontriez le message d'erreur suivant lorsque vous essayez de créer un dossier :

« Vous n'êtes pas autorisé à créer un dossier contre le service sélectionné »

Cette erreur peut signifier que le compte NSS et la société d'enregistrement à laquelle il est associé ne sont pas la même société d'enregistrement pour le numéro de série du compte NetApp Console (c'est-à-dire. 960xxxx) ou le numéro de série de l'environnement de travail. Vous pouvez demander de l'aide en utilisant l'une des options suivantes :

- Soumettez un cas non technique à https://mysupport.netapp.com/site/help

Gérez vos cas d’assistance

Vous pouvez afficher et gérer les cas d’assistance actifs et résolus directement depuis la console. Vous pouvez gérer les cas associés à votre compte NSS et à votre entreprise.

Notez ce qui suit :

- Le tableau de bord de gestion des cas en haut de la page offre deux vues :
  - La vue de gauche montre le nombre total de dossiers ouverts au cours des 3 derniers mois par le compte utilisateur NSS que vous avez fourni.
  - La vue de droite affiche le nombre total de dossiers ouverts au cours des 3 derniers mois au niveau de votre entreprise en fonction de votre compte utilisateur NSS.

  Les résultats du tableau reflètent les cas liés à la vue que vous avez sélectionnée.
- Vous pouvez ajouter ou supprimer des colonnes d’intérêt et filtrer le contenu des colonnes telles que Priorité et Statut. D’autres colonnes fournissent simplement des capacités de tri.

  Consultez les étapes ci-dessous pour plus de détails.
- Au niveau de chaque cas, nous offrons la possibilité de mettre à jour les notes du cas ou de fermer un cas qui n’est pas déjà au statut Fermé ou En attente de fermeture.

Étapes

1. Dans la NetApp Console, sélectionnez **Aide > Support**.
2. Sélectionnez **Gestion des cas** et si vous y êtes invité, ajoutez votre compte NSS à la console.

   La page **Gestion des cas** affiche les cas ouverts liés au compte NSS associé à votre compte utilisateur de la console. Il s’agit du même compte NSS qui apparaît en haut de la page **Gestion NSS**.
3. Modifiez éventuellement les informations qui s’affichent dans le tableau :
   - Sous **Cas de l’organisation**, sélectionnez **Afficher** pour afficher tous les cas associés à votre entreprise.
   - Modifiez la plage de dates en choisissant une plage de dates exacte ou en choisissant une période différente.
   - Filtrer le contenu des colonnes.
   - Modifiez les colonnes qui apparaissent dans le tableau en sélectionnant et ensuite choisir les colonnes que vous souhaitez afficher.
4. Gérer un dossier existant en sélectionnant et en sélectionnant l’une des options disponibles :
   - **Voir le cas** : Afficher tous les détails sur un cas spécifique.
   - **Mettre à jour les notes du cas** : fournissez des détails supplémentaires sur votre problème ou sélectionnez **Télécharger des fichiers** pour joindre jusqu’à un maximum de cinq fichiers.

     Les pièces jointes sont limitées à 25 Mo par fichier. Les extensions de fichiers suivantes sont prises en charge : txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx et csv.
   - **Fermer le dossier** : Fournissez des détails sur les raisons pour lesquelles vous fermez le dossier et sélectionnez **Fermer le dossier**.

Mentions légales

Les mentions légales donnent accès aux déclarations de droits d'auteur, aux marques déposées, aux brevets et bien plus encore.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marques de commerce

NETAPP, le logo NETAPP et les marques répertoriées sur la page Marques NetApp sont des marques commerciales de NetApp, Inc. Les autres noms de sociétés et de produits peuvent être des marques commerciales de leurs propriétaires respectifs.

"https://www.netapp.com/company/legal/trademarks/"

Brevets

Une liste actuelle des brevets détenus par NetApp est disponible à l'adresse suivante :

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Politique de confidentialité

"https://www.netapp.com/company/legal/privacy-policy/"

Open source

Les fichiers d'avis fournissent des informations sur les droits d'auteur et les licences tiers utilisés dans les logiciels NetApp .

"Avis concernant la NetApp Disaster Recovery"

Informations sur le copyright

Informations sur les marques commerciales