



Documentation sur la reprise d'activité **BlueXP**

BlueXP disaster recovery

NetApp
August 08, 2025

Sommaire

Documentation sur la reprise d'activité BlueXP	1
Notes de mise à jour	2
Nouveautés de la reprise d'activité BlueXP	2
04 août 2025	2
14 juillet 2025	2
30 juin 2025	3
23 juin 2025	4
9 juin 2025	4
13 mai 2025	4
16 avril 2025	6
10 mars 2025	6
19 février 2025	7
30 octobre 2024	7
20 septembre 2024	9
2 août 2024	10
17 juillet 2024	10
5 juillet 2024	11
15 mai 2024	12
5 mars 2024	12
1er février 2024	13
11 janvier 2024	14
20 octobre 2023	14
27 septembre 2023	14
1er août 2023	15
18 mai 2023	16
Limitations de la récupération après sinistre BlueXP	16
Attendez la fin du retour arrière avant d'exécuter la détection	16
BlueXP ne découvre peut-être pas Amazon FSX pour NetApp ONTAP	16
Commencez	18
Découvrez la reprise d'activité BlueXP pour VMware	18
Avantages de l'utilisation de la reprise d'activité BlueXP pour VMware	19
Les possibilités de la reprise d'activité BlueXP pour VMware	19
Le coût	20
Licences	20
essai gratuit de 30 jours	21
Fonctionnement de la reprise d'activité BlueXP	21
Des conditions qui peuvent vous aider dans la reprise d'activité BlueXP	23
Conditions préalables à la reprise d'activité BlueXP	23
Conditions préalables au stockage ONTAP	23
Prérequis pour les clusters VMware vCenter	23
Prérequis de BlueXP	24
Prérequis des charges de travail	25
Démarrage rapide de la reprise d'activité BlueXP	25

Configurez votre infrastructure pour la reprise d'activité BlueXP	26
Préparez-vous à la reprise d'activité BlueXP pour la protection des données sur site à sur site	26
Préparez-vous à la reprise d'activité BlueXP pour une protection sur site dans le cloud avec AWS	27
Accédez à la reprise d'activité BlueXP	27
Configurez les licences pour la reprise d'activité BlueXP	29
Essayez-le gratuitement pendant 30 jours	30
Une fois l'essai terminé, abonnez-vous via l'une des places de marché	31
Une fois la version d'évaluation terminée, achetez une licence BYOL par l'intermédiaire de NetApp	31
Mettez à jour votre licence BlueXP lorsqu'elle expire	32
Terminez l'essai gratuit	32
Forum aux questions sur la reprise d'activité BlueXP	33
Utilisez la reprise d'activité BlueXP	35
Utilisez la présentation de la reprise d'activité BlueXP	35
Consultez l'état de vos plans de reprise après sinistre BlueXP sur le tableau de bord	35
Ajouter des vCenters à un site dans la récupération après sinistre BlueXP	37
Ajoutez le mappage de sous-réseau pour un site vCenter	39
Modifiez le site du serveur vCenter et personnalisez la planification de la découverte	41
Actualisez la découverte manuellement	43
Créer un groupe de ressources pour organiser les machines virtuelles ensemble dans la reprise après sinistre BlueXP	44
Créer un plan de réplication dans la reprise après sinistre BlueXP	47
Créez le plan	48
Modifiez les plannings pour tester la conformité et vous assurer que les tests de basculement fonctionnent	57
Répliquer des applications vers un autre site avec la récupération après sinistre BlueXP	59
Migrer des applications vers un autre site avec la récupération après sinistre BlueXP	60
Basculer les applications vers un site distant avec la récupération après sinistre BlueXP	60
Tester le processus de basculement	61
Nettoyez l'environnement de test après un test de basculement	62
Basculez le site source vers un site de reprise après incident	62
Restaurez les applications à leur source d'origine avec la récupération après sinistre BlueXP	63
Gérez les sites, les groupes de ressources, les plans de réplication, les banques de données et les informations des machines virtuelles avec la reprise après sinistre BlueXP	64
Gestion des sites vCenter	65
Gérer les groupes de ressources	65
Gérer les plans de réplication	65
Afficher les informations sur les datastores	68
Afficher les informations sur les machines virtuelles	69
Surveiller les tâches de récupération après sinistre BlueX	69
Afficher les travaux	69
Annuler un travail	69
Créer des rapports de reprise après sinistre BlueXP	70
Référence	71
Privilèges vCenter requis pour la reprise d'activité BlueXP	71
Accès aux fonctionnalités de BlueXP disaster recovery basé sur les rôles	73

Utiliser la reprise après sinistre BlueXP avec Amazon EVS	74
Introduction à la reprise après sinistre BlueXP à l'aide d'Amazon Elastic VMware Service et d'Amazon FSx pour NetApp ONTAP	74
Présentation de la solution de reprise après sinistre BlueXP utilisant Amazon EVS et Amazon FS pour NetApp ONTAP	75
Installer le connecteur BlueXP pour la reprise après sinistre BlueXP	77
Configurer la reprise après sinistre BlueXP pour Amazon EVS	77
Créer des plans de réplication pour Amazon EVS	89
Exécuter des opérations de plan de réplication avec la reprise après sinistre BlueXP	102
Connaissances et support	115
S'inscrire pour obtenir de l'aide	115
Présentation de l'inscription au support	115
Enregistrez BlueXP pour bénéficier du support NetApp	115
Associer les informations d'identification NSS pour le support Cloud Volumes ONTAP	118
Obtenez de l'aide	119
Bénéficiez du support pour les services de fichiers d'un fournisseur cloud	119
Utilisation d'options de support en libre-service	120
Créez un dossier de demande de support auprès du support NetApp	120
Gestion de vos dossiers de demande de support (aperçu)	122
Mentions légales	125
Droits d'auteur	125
Marques déposées	125
Brevets	125
Politique de confidentialité	125
Source ouverte	125

Documentation sur la reprise d'activité BlueXP

Notes de mise à jour

Nouveautés de la reprise d'activité BlueXP

Découvrez les nouveautés de la reprise d'activité BlueXP.

04 août 2025

Version 4.2.5P2

Mises à jour de BlueXP disaster recovery

Cette version comprend 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 "[Licence de BlueXP disaster recovery](#)" et "[Configurez les licences pour la reprise d'activité BlueXP](#)".

14 juillet 2025

Version 4.2.5

Rôles des utilisateurs dans la BlueXP disaster recovery

La BlueXP 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 la BlueXP disaster recovery.

- **Administrateur de récupération après sinistre** : effectuez toutes les actions dans la BlueXP disaster recovery.
- **Administrateur de basculement de reprise après sinistre** : effectuez des actions de basculement et de migration dans la BlueXP 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 la BlueXP disaster recovery,

mais ne pouvez effectuer aucune action.

Si vous cliquez sur le service de BlueXP disaster recovery et le configurez pour la première fois, vous devez disposer de l'autorisation **SnapCenterAdmin** ou du rôle **Administrateur d'organisation**.

Pour plus de détails, voir "[Rôles et autorisations des utilisateurs dans la BlueXP disaster recovery](#)".

["En savoir plus sur les rôles d'accès BlueXP pour tous les services"](#).

Autres mises à jour de la BlueXP 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 vCenter SDK et de la gestion des pools
- Gestion des données obsolètes lors de la prochaine découverte planifiée ou manuelle :
 - Lorsqu'une machine virtuelle est supprimée dans vCenter, la BlueXP disaster recovery la supprime désormais automatiquement du plan de réplication.
 - Lorsqu'une banque de données ou un réseau est supprimé dans vCenter, la BlueXP 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, la BlueXP disaster recovery le supprime désormais du plan de réplication et du groupe de ressources.
- Vous pouvez désormais accéder à la documentation Swagger en mode navigation privée. Vous pouvez y accéder depuis la BlueXP disaster recovery via Paramètres > Documentation API ou directement à l'URL suivante en mode navigation privée : "[Documentation Swagger](#)".
- Dans certains cas, après une restauration automatique, l'iGroup était conservé une fois l'opération terminée. Cette mise à jour supprime l'iGroup s'il est obsolète.
- Si le nom de domaine complet NFS était utilisé dans le plan de réplication, la BlueXP disaster recovery le résout désormais en 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-réseaux » avec une nouvelle fonctionnalité de recherche. Vous pouvez désormais trouver rapidement des sous-réseaux spécifiques en saisissant des termes de recherche, ce qui simplifie la gestion des mappages de sous-réseaux.

9 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 administrateur local sur Active Directory.

Vous pouvez désormais sélectionner les options de mappage de sous-réseau et cocher l'option LAPS en fournissant les informations du contrôleur de domaine. Grâce à cette option, vous n'avez pas besoin de fournir de 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

Mappage de sous-réseau

Avec cette version, vous pouvez gérer les adresses IP en cas de basculement de manière nouvelle à l'aide du mappage de sous-réseau, qui vous permet d'ajouter des sous-réseaux pour chaque vCenter. Dans ce cas, vous définissez le CIDR IPv4, la passerelle par défaut et le DNS pour chaque réseau virtuel.

Lors du basculement, la reprise après incident BlueXP 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 :

- Réseau a = 10.1.1.0/24
- Réseau B = 192.168.1.0/24

VM1 dispose d'une vNIC (10.1.1.50) connectée au réseau A. NetworkA est mappé sur le réseau B dans les paramètres du plan de réplication.

En cas de basculement, la reprise après incident BlueXP 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, BlueXP Disaster Recovery examine les paramètres CIDR du réseau B et utilise cette partie du réseau 192.168.1 tout en conservant la partie hôte (.50) pour créer la nouvelle adresse IP du VM1. La nouvelle adresse 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

d'adresses IP en cas de basculement, notamment si vous avez des centaines de réseaux et des milliers de machines virtuelles à gérer.

Pour plus d'informations sur l'inclusion du mappage de sous-réseau dans vos sites, reportez-vous à la section ["Ajoutez des sites de serveur vCenter"](#) .

Ignorer la protection

Vous pouvez maintenant ignorer la protection afin que le service ne crée pas automatiquement une relation de protection inverse après un basculement de plan de réplication. Cette fonction est utile si vous souhaitez effectuer des opérations supplémentaires sur le site restauré avant de le remettre en ligne dans le cadre de la reprise sur incident BlueXP .

Lorsque vous initiez 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 entre le site cible et le site source. Par ailleurs, le service inverse automatiquement la relation SnapMirror lorsque vous initiez un retour arrière.

Lorsque vous lancez un basculement, vous pouvez maintenant choisir une option **Ignorer la protection**. Avec cela, le service n'inverse pas automatiquement la relation SnapMirror. Il laisse le volume inscriptible des deux côtés du plan de réplication.

Une fois le site source d'origine remis en ligne, vous pouvez établir une protection inverse en sélectionnant **protéger les ressources** dans le menu actions du plan de réplication. Cette opération tente de créer une relation de réplication inverse pour chaque volume du plan. Vous pouvez exécuter cette tâche plusieurs fois jusqu'à ce que la protection soit restaurée. Une fois la protection restaurée, vous pouvez lancer un rétablissement de la manière habituelle.

Pour plus de détails sur le fait d'ignorer la protection, reportez-vous à la ["Basculement des applications vers un site distant"](#).

SnapMirror planifie les mises à jour dans le plan de réplication

La reprise sur incident BlueXP prend désormais en charge l'utilisation de solutions de gestion externe des snapshots, comme le planificateur de règles ONTAP SnapMirror natif ou les intégrations tierces avec ONTAP. Si chaque datastore (volume) du plan de réplication dispose déjà d'une relation SnapMirror gérée par un autre emplacement, vous pouvez utiliser ces snapshots comme points de restauration dans la reprise d'activité BlueXP .

Pour configurer, dans la section Replication Plan > Resource Mapping, cochez la case **utiliser les sauvegardes gérées par la plate-forme et les plannings de rétention** lors de la configuration du mappage des datastores.

Lorsque cette option est sélectionnée, la reprise sur incident BlueXP ne configure pas de programme de sauvegarde. Toutefois, vous devez toujours configurer un planning de conservation, car les snapshots peuvent toujours être créés pour les opérations de test, de basculement et de restauration.

Une fois configuré, le service ne prend pas de snapshots planifiés régulièrement, mais s'appuie plutôt sur l'entité externe pour prendre et mettre à jour ces snapshots.

Pour plus d'informations sur l'utilisation de solutions d'instantanés externes dans le plan de réplication, reportez-vous à la section ["Créer un plan de réplication"](#) .

16 avril 2025

Version 4.2.2

Découverte planifiée pour les VM

La reprise sur incident BlueXP effectue une détection 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 la 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 que wan planifie 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 ["Ajoutez des sites de serveur vCenter"](#) .

Prise en charge des datastores de groupes de ressources

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

Vous pouvez créer un groupe de ressources avec un datastore de l'une des manières suivantes :

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

Pour plus de détails, reportez-vous à ["Créer un plan de réplication"](#).

Notifications d'expiration de licence ou d'essai gratuit

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

Notification des mises à jour de service

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

10 mars 2025

Version 4.2.1

Prise en charge de proxy intelligent

Le connecteur BlueXP prend en charge le proxy intelligent. Le proxy intelligent est un moyen léger, sécurisé et efficace de connecter votre environnement sur site au service BlueXP. Il fournit une connexion sécurisée entre votre environnement et le service BlueXP sans VPN ni accès direct à Internet. Cette mise en œuvre de proxy optimisée décharge le trafic API au sein du réseau local.

Lorsqu'un proxy est configuré, la reprise après incident BlueXP tente de communiquer directement avec VMware ou ONTAP et utilise le proxy configuré en cas d'échec de la communication directe.

La mise en œuvre du proxy de reprise après incident BlueXP nécessite une communication sur le port 443 entre le connecteur et tous les serveurs vCenter et baies ONTAP utilisant un protocole HTTPS. L'agent de reprise après incident BlueXP intégré au connecteur communique directement avec VMware vSphere, VC ou ONTAP lors de l'exécution de toute action.

Pour plus d'informations sur le proxy intelligent pour la reprise après incident BlueXP, reportez-vous à la section "[Configurez votre infrastructure pour la reprise d'activité BlueXP](#)".

Pour plus d'informations sur la configuration générale du proxy dans BlueXP, reportez-vous à la section "[Configurez un connecteur pour utiliser un serveur proxy](#)".

Terminez l'essai gratuit à tout moment

Vous pouvez arrêter l'essai gratuit à n'importe quelle date ou vous pouvez attendre jusqu'à ce qu'il expire.

Voir "[Terminez l'essai gratuit](#)".

19 février 2025

Version 4.2

Prise en charge de ASA r2 pour les machines virtuelles et les datastores sur stockage VMFS

Cette version de BlueXP Disaster Recovery prend en charge ASA r2 pour les machines virtuelles et les datastores 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 groupes de cohérence pour le stockage primaire (groupe de cohérence plat uniquement, c'est-à-dire un seul niveau sans structure hiérarchique)
- Opérations de sauvegarde (groupe de cohérence) incluant l'automatisation SnapMirror

La prise en charge de ASA r2 dans la reprise sur incident BlueXP utilise ONTAP 9.16.1.

Les datastores peuvent être montés sur un volume ONTAP ou une unité de stockage ASA r2, mais un groupe de ressources dans BlueXP Disaster Recovery ne peut pas inclure à la fois un datastore depuis ONTAP et un datastore depuis ASA r2. Vous pouvez sélectionner un datastore à partir de ONTAP ou un datastore à partir de ASA r2 dans un groupe de ressources.

30 octobre 2024

Création de rapports

Vous pouvez désormais générer et télécharger des rapports pour vous aider à analyser votre environnement. Des rapports prédéfinis résumant les basculements et les basculements, affichent les détails de réplication sur tous les sites et affichent les détails des tâches des sept derniers jours.

Reportez-vous à la "[Créez des rapports de reprise d'activité](#)".

essai gratuit de 30 jours

Vous pouvez désormais vous inscrire pour bénéficier d'un essai gratuit de 30 jours de reprise d'activité BlueXP . Auparavant, les essais gratuits étaient de 90 jours.

Reportez-vous à la "[Configuration des licences](#)".

Désactivez et activez les plans de réplication

Une version précédente incluait des mises à jour de la structure de planification des tests de basculement, qui devait prendre en charge les planifications quotidiennes et hebdomadaires. Cette mise à jour exige que vous désactiviez et réactiviez tous les plans de réplication existants afin de pouvoir utiliser les nouveaux programmes de tests de basculement quotidiens et hebdomadaires. Il s'agit d'une exigence ponctuelle.

Voici comment :

1. Dans le menu supérieur, 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 que vous mappez des ressources de calcul, vous pouvez désormais mapper des dossiers de sorte que les machines virtuelles soient restaurées 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 sur les machines virtuelles disponibles pour le basculement, la restauration et le basculement de test

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

Reportez-vous à la "[Basculement des 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 maintenant définir un délai de démarrage pour chaque machine virtuelle du plan. Cela vous permet de définir une séquence pour que les machines virtuelles commencent à s'assurer que toutes vos machines virtuelles prioritaires sont en cours d'exécution avant que les machines virtuelles prioritaires suivantes ne soient démarrées.

Pour plus de détails, reportez-vous à "[Créer un plan de réplication](#)".

Informations sur le système d'exploitation des machines virtuelles

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

Pour plus de détails, reportez-vous à ["Créer un plan de réplication"](#).

Alias de nom de VM

Lorsque vous créez un plan de réplication, vous pouvez à présent ajouter un préfixe et un suffixe aux noms des machines virtuelles sur le SIT de reprise après incident. Cela vous permet d'utiliser un nom plus descriptif pour les VM du plan.

Pour plus de détails, reportez-vous à ["Créer un plan de réplication"](#).

Nettoyez les anciens snapshots

Vous pouvez supprimer tous les snapshots qui ne sont plus nécessaires au-delà du nombre de conservation spécifié. Les snapshots peuvent s'accumuler au fil du temps lorsque vous réduisez le nombre de conservation des snapshots 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 ["Gérez les sites, les groupes de ressources, les plans de réplication, les datastores et les informations sur les machines virtuelles"](#).

Réconcilier les instantanés

Vous pouvez désormais réconcilier les instantanés qui sont désynchronisés entre la source et la cible. Cela peut se produire si des snapshots sont supprimés sur une cible en dehors de la reprise sur incident BlueXP. Le service supprime automatiquement le snapshot sur la source toutes les 24 heures. Cependant, vous pouvez effectuer cette opération à la demande. Cette fonction vous permet de vous assurer que les snapshots 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 datastores VMware VMFS sur site et sur site

Cette version inclut la prise en charge des machines virtuelles montées sur des datastores VMFS (Virtual machine File System) VMware vSphere pour iSCSI et FC protégées sur le stockage sur site. Auparavant, le service fournissait un *aperçu de la technologie* prenant en charge les datastores VMFS pour iSCSI et FC.

Voici quelques considérations supplémentaires concernant à la fois les protocoles iSCSI et FC :

- La prise en charge de FC concerne les protocoles client frontaux, pas la réplication.
- La reprise d'activité BlueXP ne prend en charge qu'une seule 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 VM protégées. Par exemple, si la source utilise un protocole FC, la destination doit également utiliser FC.

2 août 2024

Prise en charge des datastores VMware VMFS pour FC sur site vers sur site

Cette version inclut un *aperçu de la technologie* de la prise en charge des machines virtuelles montées sur des datastores VMFS (Virtual machine File System) VMware vSphere pour la protection FC sur un stockage sur site. Auparavant, le service offrait un aperçu de la technologie prenant en charge les datastores VMFS pour iSCSI.



NetApp ne vous facture pas pour la capacité de workloads prévisualisée.

Annulation du travail

Avec cette version, vous pouvez maintenant annuler un travail dans l'interface utilisateur de Job Monitor.

Reportez-vous à la "[Surveiller les tâches](#)".

17 juillet 2024

Planifications de tests de basculement

Cette version inclut des mises à jour de la structure de planification des tests de basculement, qui était nécessaire 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 programmes de tests de basculement quotidiens et hebdomadaires. Il s'agit d'une exigence ponctuelle.

Voici comment :

1. Dans le menu supérieur, 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 de « snapshot introuvable ». Pour ce faire, vous devez définir le nombre de rétention dans tous les plans de réplication sur 1 et lancer un instantané à la demande. Ce processus crée une nouvelle sauvegarde et supprime toutes les anciennes sauvegardes.

Voici comment :

1. Dans le menu supérieur, sélectionnez **plans de réplication**.
2. Sélectionnez le plan de réplication, cliquez sur l'onglet **mappage de basculement**, puis cliquez sur l'icône crayon **Modifier**.
3. Cliquez sur la flèche **datastores** pour la développer.
4. Notez la valeur du nombre de rétention dans le plan de réplication. Vous devrez rétablir cette valeur d'origine lorsque vous aurez terminé ces étapes.
5. Réduisez le compte à 1.

6. Lancez un snapshot à la demande. Pour ce faire, sur la page Plan de réplication, sélectionnez le plan, cliquez sur l'icône actions et sélectionnez **prendre instantané maintenant**.
7. Une fois la procédure de snapshot terminée, 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.

5 juillet 2024

Cette version de reprise d'activité de BlueXP inclut les mises à jour suivantes :

Prise en charge de AFF A-Series

Cette version prend en charge les plateformes matérielles NetApp AFF A-Series.

Prise en charge des datastores VMware VMFS sur site et sur site

Cette version inclut un *aperçu technologique* de la prise en charge des machines virtuelles montées sur des datastores VMFS (Virtual machine File System) VMware vSphere protégés sur le stockage sur site. Avec cette version, la reprise après incident est prise en charge dans un aperçu technologique pour les workloads VMware sur site vers un environnement VMware sur site avec des datastores VMFS.



NetApp ne vous facture pas pour la capacité de workloads prévisualisée.

Mises à jour du plan de réplication

Vous pouvez ajouter un plan de réplication plus facilement en filtrant les machines virtuelles par datastore sur la page applications et en sélectionnant plus de détails sur les cibles sur la page mappage des ressources. Reportez-vous à la "[Créer un plan de réplication](#)".

Modifier les plans de réplication

Avec cette version, la page mappages de basculement a été améliorée pour plus de clarté.

Reportez-vous à la "[Gérer les plans](#)".

Modifier les VM

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

Reportez-vous à la "[Gestion des VM](#)".

Basculement des mises à jour

Avant d'initier un basculement, vous pouvez maintenant déterminer l'état des machines virtuelles et leur mise sous tension ou hors tension. Le processus de basculement vous permet maintenant de prendre un instantané ou de choisir les snapshots.

Reportez-vous à la "[Basculement des applications vers un site distant](#)".

Planifications de tests de basculement

Vous pouvez désormais modifier les tests de basculement et définir des plannings quotidiens, hebdomadaires et mensuels pour le test de basculement.

Reportez-vous à la ["Gérer les plans"](#).

Mise à jour des informations de prérequis

Les informations sur les conditions préalables à la reprise sur incident de BlueXP ont été mises à jour.

Reportez-vous à la ["Conditions préalables à la reprise d'activité BlueXP"](#).

15 mai 2024

Cette version de reprise d'activité de BlueXP inclut les mises à jour suivantes :

Réplication des charges de travail VMware du stockage sur site vers le stockage sur site

Il est maintenant disponible en tant que fonctionnalité de disponibilité générale. Auparavant, il s'agissait d'un aperçu technologique avec des fonctionnalités limitées.

Mises à jour des licences

Avec la solution de reprise après incident BlueXP, vous pouvez vous inscrire à un essai gratuit de 90 jours, acheter un abonnement PAYGO avec Amazon Marketplace ou BYOL (Bring Your Own License), un fichier de licence NetApp que vous obtenez auprès de votre ingénieur commercial NetApp ou auprès du site de support NetApp (NSS).

Pour plus d'informations sur la configuration des licences pour la reprise d'activité BlueXP, reportez-vous à la section ["Configuration des licences"](#).

["En savoir plus sur la reprise d'activité BlueXP"](#).

5 mars 2024

Il s'agit de la version General Availability de BlueXP Disaster Recovery, qui comprend les mises à jour suivantes.

Mises à jour des licences

Avec BlueXP Disaster Recovery, vous pouvez vous inscrire à un essai gratuit de 90 jours ou BYOL (Bring Your Own License), un fichier de licence NetApp que vous obtenez auprès de votre ingénieur commercial NetApp. Vous pouvez utiliser le numéro de série de licence pour activer la fonction BYOL dans le portefeuille digital BlueXP. Les frais de reprise d'activité BlueXP sont calculés en fonction de la capacité provisionnée des datastores.

Pour plus d'informations sur la configuration des licences pour la reprise d'activité BlueXP, reportez-vous à la section ["Configuration des licences"](#).

Pour plus d'informations sur la gestion des licences pour **tous** services BlueXP, reportez-vous à la section ["Gérez les licences de tous les services BlueXP"](#).

Modifier les horaires

Avec cette version, vous pouvez désormais définir des plannings de test de conformité et de basculement afin de vous assurer qu'ils fonctionneront correctement si vous en avez besoin.

Pour plus de détails, reportez-vous à ["Créez le plan de réplication"](#).

1er février 2024

Cette version de préversion de la reprise d'activité de BlueXP inclut les mises à jour suivantes :

Amélioration du réseau

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

- DHCP : si vous choisissez cette option, vous fournissez les informations d'identification de la machine virtuelle.
- IP statique : vous pouvez sélectionner les mêmes informations ou des informations différentes à partir de la machine virtuelle source. Si vous choisissez la même chose que la source, vous n'avez pas besoin d'entrer les informations d'identification. En revanche, 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 la 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 les scripts personnalisés, la reprise d'activité BlueXP peut 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 ["Basculez vers un site distant"](#).

Relation SnapMirror

Il est désormais possible de créer une relation SnapMirror pendant le développement du plan de réplication. Auparavant, vous deviez créer la relation en dehors de la reprise d'activité BlueXP.

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 SVM. La reprise d'activité BlueXP crée une copie Snapshot de groupe de cohérence en incluant tous les volumes et en mettant à jour tous les sites 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 Resource Groups, vous pouvez définir un délai sur chaque machine virtuelle afin qu'elle se met sous tension en séquence différée.

Pour plus de détails, reportez-vous à ["Créer un plan de réplication"](#).

Copies Snapshot cohérentes au niveau des applications

Vous pouvez spécifier de créer des copies Snapshot cohérentes au niveau des applications. Le service arrête l'application, puis prend un Snapshot 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 la reprise d'activité de BlueXP inclut les mises à jour suivantes :

Tableau de bord plus rapide

Cette version vous permet d'accéder plus rapidement aux informations d'autres pages du tableau de bord.

["Découvrez la reprise d'activité BlueXP"](#).

20 octobre 2023

Cette version préliminaire de la reprise d'activité de BlueXP inclut les mises à jour suivantes.

Protégez les workloads VMware sur site basés sur NFS

Désormais, avec la reprise d'activité BlueXP, vous pouvez protéger vos workloads VMware sur site basés sur NFS contre les incidents vers un autre environnement VMware sur site et NFS en plus du cloud public. La reprise d'activité BlueXP orchestre l'achèvement des plans de reprise d'activité.



Avec cette offre de prévisualisation, 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 reprise d'activité BlueXP"](#).

27 septembre 2023

Cette version préliminaire de la reprise d'activité de BlueXP inclut les mises à jour suivantes :

Mises à jour du tableau de bord

Vous pouvez maintenant cliquer sur les options du tableau de bord, ce qui vous permet de passer rapidement en revue les informations. De plus, le tableau de bord affiche désormais l'état des basculements et des migrations.

Reportez-vous à la section ["Consultez l'état de vos plans de reprise sur incident dans le tableau de bord"](#).

Mises à jour du plan de réplication

- **RPO** : vous pouvez maintenant saisir l'objectif de point de récupération (RPO) et le nombre de rétention dans la section datastores du plan de réplication. Indique la quantité de données qui doit exister et qui n'est pas antérieure à l'heure définie. Si, par exemple, vous le configurez à 5 minutes, le système peut

perdre jusqu'à 5 minutes de données en cas d'incident sans affecter les besoins stratégiques de l'entreprise.

Reportez-vous à la section "[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 machines virtuelles du plan de réplication, BlueXP 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. En outre, vous pouvez maintenant saisir des informations d'identification pour les machines virtuelles.

Reportez-vous à la section "[Créer un plan de réplication](#)".

- **Modifier les plannings** : vous pouvez maintenant mettre à jour les plannings de plans de réplication.

Reportez-vous à la section "[Gérer les ressources](#)".

- **SnapMirror automation** : lors de la création du 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
 - De plusieurs à 1 en tant que groupe de cohérence
 - De plusieurs à plusieurs

Reportez-vous à la section "[Créer un plan de réplication](#)".

1er août 2023

Aperçu de la reprise d'activité BlueXP

La préversion de la reprise d'activité BlueXP est un service de reprise après incident basé dans le cloud qui automatise les workflows de reprise après incident. À l'aide de la préversion de la reprise d'activité BlueXP, vous pouvez protéger vos workloads VMware sur site basés sur NFS exécutant le stockage NetApp vers VMware Cloud (VMC) sur AWS avec Amazon FSX pour ONTAP.



Avec cette offre de prévisualisation, 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 reprise d'activité BlueXP"](#).

Cette version comprend 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 incident ou de réplication, vous pouvez ajouter des machines virtuelles à des groupes de ressources fonctionnelles. 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 restauration. Avec cette version, chaque groupe de ressources peut inclure une ou plusieurs machines virtuelles. Les machines virtuelles s'allument en fonction de l'ordre dans lequel vous les incluez dans le plan. Reportez-vous à la "[Sélectionnez les applications à répliquer et attribuez des groupes de ressources](#)".

Vérification de la réplication

Après avoir créé le plan de reprise sur incident ou de réplication, identifiez la récurrence dans l'assistant et lancez une réplication vers un site de reprise sur incident, la reprise sur incident BlueXP vérifie toutes les 30 minutes que la réplication se produit réellement conformément au plan. Vous pouvez surveiller la progression dans la page moniteur des tâches. Reportez-vous à la ["Réplication d'applications vers un autre site"](#).

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

Lorsque vous créez un plan de réplication ou de reprise d'activité, vous sélectionnez les machines virtuelles. Dans cette version, vous pouvez désormais afficher la SnapMirror associée à chacun des volumes associés au datastore ou à la machine virtuelle. Vous pouvez également consulter les planifications de transfert RPO associées à la planification SnapMirror. L'objectif de point de récupération vous permet de déterminer si votre planification de sauvegarde est suffisante pour permettre une reprise après incident. Reportez-vous à la ["Créer un plan de réplication"](#).

Mise à jour de Job Monitor

La page surveillance des travaux comprend désormais une option Actualiser qui vous permet d'obtenir un état à jour des opérations. Reportez-vous à la ["Surveiller les tâches de reprise après incident"](#).

18 mai 2023

Il s'agit de la version initiale de la reprise d'activité de BlueXP.

Service de reprise après incident basé sur le cloud

BlueXP est un service de reprise après incident basé dans le cloud qui automatise les workflows de reprise après incident. À l'aide de la préversion de la reprise d'activité BlueXP, vous pouvez protéger vos workloads VMware sur site basés sur NFS exécutant le stockage NetApp vers VMware Cloud (VMC) sur AWS avec Amazon FSX pour ONTAP.

["En savoir plus sur la reprise d'activité BlueXP"](#).

Limitations de la récupération après sinistre BlueXP

Les limitations connues identifient les plates-formes, les périphériques ou les fonctions qui ne sont pas pris en charge par cette version du service ou qui ne fonctionnent pas correctement avec celui-ci.

Attendez la fin du retour arrière avant d'exécuter la détection

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

BlueXP ne découvre peut-être pas Amazon FSX pour NetApp ONTAP

Il peut arriver que BlueXP ne détecte pas les clusters Amazon FSX pour 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 pour NetApp ONTAP dans BlueXP et actualisez régulièrement le cluster pour afficher les modifications éventuelles.

Si vous devez supprimer le cluster ONTAP FSX du service de reprise d'activité BlueXP, effectuez les opérations suivantes :

1. Dans le connecteur BlueXP, utilisez les options de connectivité de votre fournisseur cloud, connectez-vous à la VM Linux sur laquelle le connecteur s'exécute, redémarrez le service « occm » à l'aide du `docker restart occm` commande.

Reportez-vous à la section "[Gérer les connecteurs existants](#)".

2. Dans le canevas BlueXP, ajoutez de nouveau l'environnement Amazon FSX pour ONTAP et fournissez les informations d'identification FSX.

Reportez-vous à la section "[Créer un système de fichiers Amazon FSX pour NetApp ONTAP](#)".

3. Depuis la reprise d'activité BlueXP, sélectionnez **sites**, sur la ligne vCenter, sélectionnez l'option **actions**



, Et dans le menu actions, sélectionnez **Refresh** pour actualiser la découverte FSX dans la reprise d'activité BlueXP.

Le datastore, ses machines virtuelles et sa relation de destination sont alors redécouverts.

Commencez

Découvrez la reprise d'activité BlueXP pour VMware

La reprise d'activité dans le cloud est un moyen résilient et économique de protéger les workloads contre les pannes sur site et les corruptions de données. Avec la reprise d'activité BlueXP pour VMware, vous pouvez répliquer vos workloads de VM ou de datastores VMware sur site exécutant le stockage ONTAP vers un data Center Software-defined VMware dans un cloud public à l'aide du stockage cloud NetApp ou vers un autre environnement VMware sur site avec un stockage ONTAP comme site de reprise d'activité.

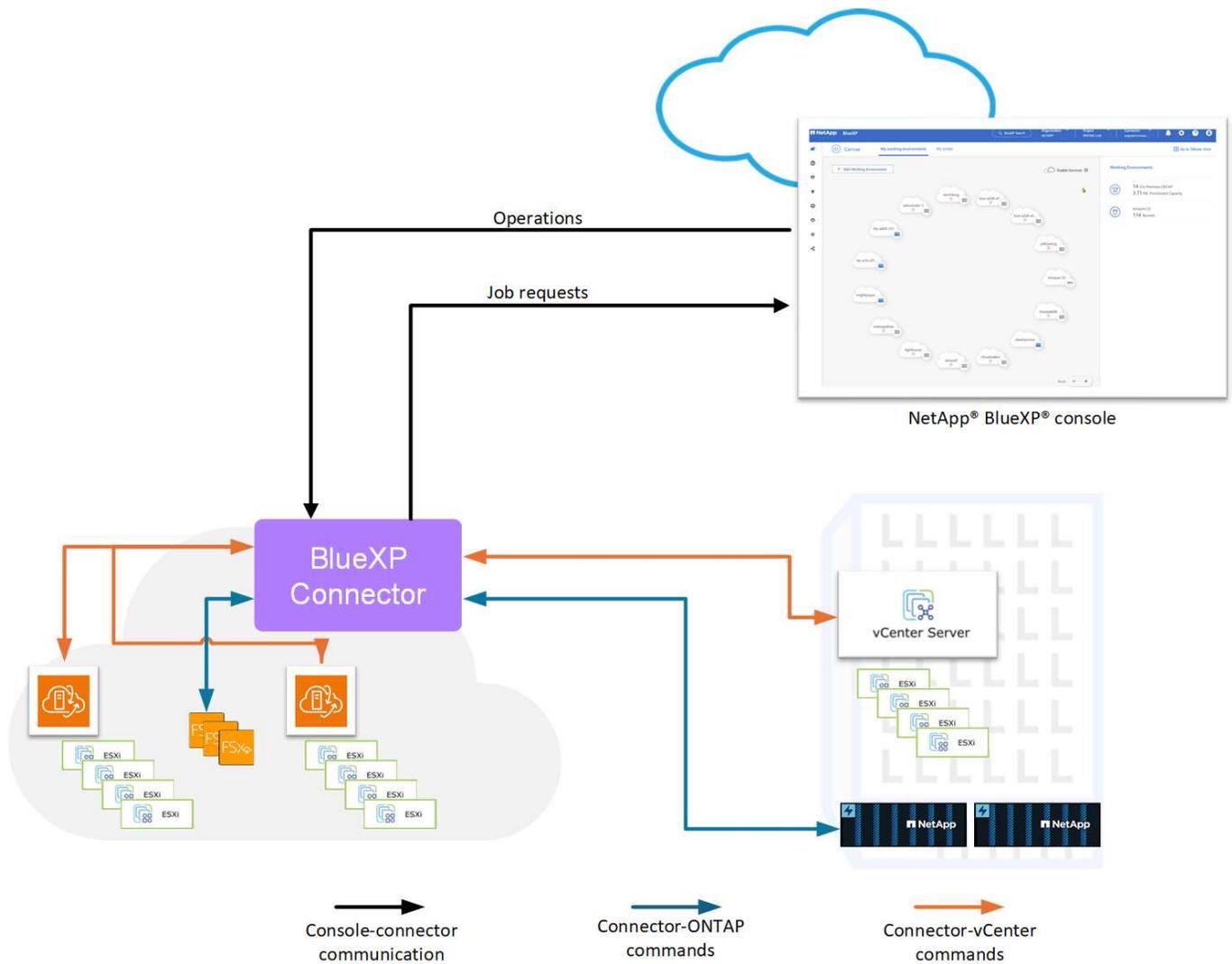
BlueXP est un service de reprise après incident basé dans le cloud qui automatise les workflows de reprise après incident. Le service de reprise après incident BlueXP protège vos workloads sur site basés sur NFS et vos datastores VMFS (Virtual machine File System) VMware vSphere pour iSCSI et FC exécutant un stockage NetApp vers l'un des éléments suivants :

- VMware Cloud (VMC) sur AWS avec Amazon FSX pour NetApp ONTAP ou
- Un autre environnement VMware sur site basé sur NFS avec stockage ONTAP



CETTE DOCUMENTATION CONCERNANT AWS EVS EST FOURNIE À TITRE D'APERÇU TECHNOLOGIQUE. Avec cette offre de présentation, NetApp se réserve le droit de modifier les détails, le contenu et le calendrier de l'offre avant la disponibilité générale. Pour plus de détails, voir ["Introduction à la reprise après sinistre BlueXP à l'aide d'Amazon Elastic VMware Service et d'Amazon FSx pour NetApp ONTAP"](#).

La reprise d'activité BlueXP utilise la technologie ONTAP SnapMirror pour le transport de réplication vers le site de reprise d'activité. Cela permet d'optimiser l'efficacité du stockage (compression et déduplication) sur les sites primaires et secondaires.



Avantages de l'utilisation de la reprise d'activité BlueXP pour VMware

La reprise d'activité BlueXP offre les avantages suivants :

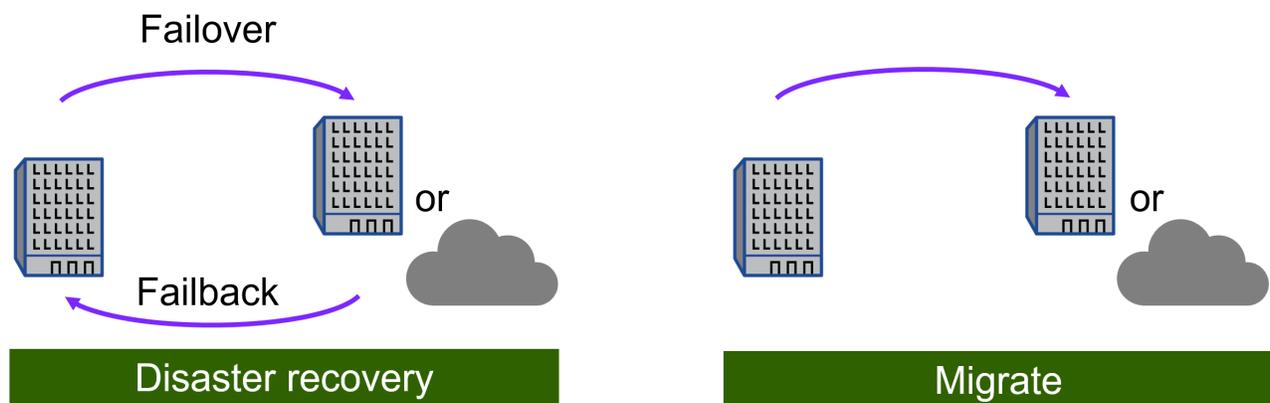
- Expérience utilisateur simplifiée pour la découverte et la restauration vCenter des applications avec plusieurs opérations de restauration à un point dans le temps
- Réduisez le coût total de possession tout en réduisant le coût des opérations et en créant et en adaptant des plans de reprise après incident avec des ressources minimales
- Disponibilité continue de la reprise après incident grâce à des tests de basculement virtuel qui ne perturbent pas les opérations
- Retour sur investissement plus rapide grâce aux modifications dynamiques de votre environnement IT et à la capacité à les gérer dans vos plans de reprise d'activité

Les possibilités de la reprise d'activité BlueXP pour VMware

Grâce à la reprise d'activité BlueXP, vous exploitez pleinement plusieurs technologies NetApp pour atteindre ces objectifs :

- Répliquez les applications VMware de votre site de production sur un site distant de reprise d'activité dans le cloud ou sur site à l'aide de la réplication SnapMirror.

- Migrez les workloads VMware de votre site d'origine vers un autre site.
- Effectuez un test de basculement ; les machines virtuelles sont créées temporairement. La reprise d'activité BlueXP crée un nouveau volume FlexClone à partir de l'instantané sélectionné, et un datastore temporaire sur lequel le volume FlexClone est installé est mappé aux hôtes ESXi. Ce processus ne consomme pas de capacité physique supplémentaire dans le stockage ONTAP sur site ou FSX pour le stockage NetApp ONTAP dans AWS. Le volume source d'origine n'est pas modifié et les tâches de réplica peuvent se poursuivre même en cas de reprise après sinistre.
- En cas d'incident, basculez votre site principal à la demande vers le site de reprise d'activité, qui peut être VMware Cloud on AWS avec Amazon FSX for NetApp ONTAP ou un environnement VMware sur site avec ONTAP.
- Une fois le sinistre résolu, basculez à la demande du site de reprise sur incident vers le site principal.
*Regrouper les machines virtuelles ou les datastores en groupes de ressources logiques pour une gestion efficace.



La configuration du serveur vSphere s'effectue en dehors de la reprise d'activité BlueXP dans vSphere Server.

Le coût

NetApp ne vous facture pas pour l'utilisation de la version d'évaluation de la reprise d'activité de BlueXP.

Le service de reprise d'activité BlueXP peut être utilisé avec une licence NetApp ou avec un plan d'abonnement annuel via Amazon Web Services.



Certaines versions incluent un aperçu de la technologie. NetApp ne vous facture pas pour la capacité de workloads prévisualisée. Voir "[Nouveautés de la reprise d'activité BlueXP](#)" pour plus d'informations sur les dernières innovations technologiques.

Licences

Vous pouvez utiliser les types de licence suivants :

- Inscrivez-vous pour bénéficier d'un essai gratuit de 30 jours.
- Achetez un abonnement à la carte (PAYGO) à * NetApp Intelligent Services* avec Amazon Web Services

(AWS) Marketplace et Microsoft Azure Marketplace.

- BYOL (Bring Your Own License), un fichier de licence NetApp (NLF) que vous obtenez auprès de votre ingénieur commercial NetApp. Vous pouvez utiliser le numéro de série de licence pour activer la fonction BYOL dans le portefeuille digital BlueXP.

Les licences de tous les services BlueXP sont gérées par le service de portefeuille digital BlueXP. Une fois que vous avez configuré votre modèle BYOL, une licence active s'affiche pour le service dans le portefeuille digital BlueXP.



Les frais de reprise sur incident BlueXP sont basés sur la capacité utilisée des datastores sur le site source lorsqu'au moins une machine virtuelle possède un plan de réplication. La capacité d'un datastore ayant subi un basculement n'est pas incluse dans l'allocation de capacité. Pour les modèles BYOL, si les données dépassent la capacité autorisée, les opérations du service sont limitées jusqu'à ce que vous obteniez une licence de capacité supplémentaire ou mettiez à niveau la licence dans le portefeuille digital BlueXP.

Pour plus d'informations sur la configuration des licences pour la reprise d'activité BlueXP, reportez-vous à la section "[Configurez la licence de reprise d'activité BlueXP](#)".

essai gratuit de 30 jours

Essayez la reprise d'activité BlueXP avec un essai gratuit de 30 jours.

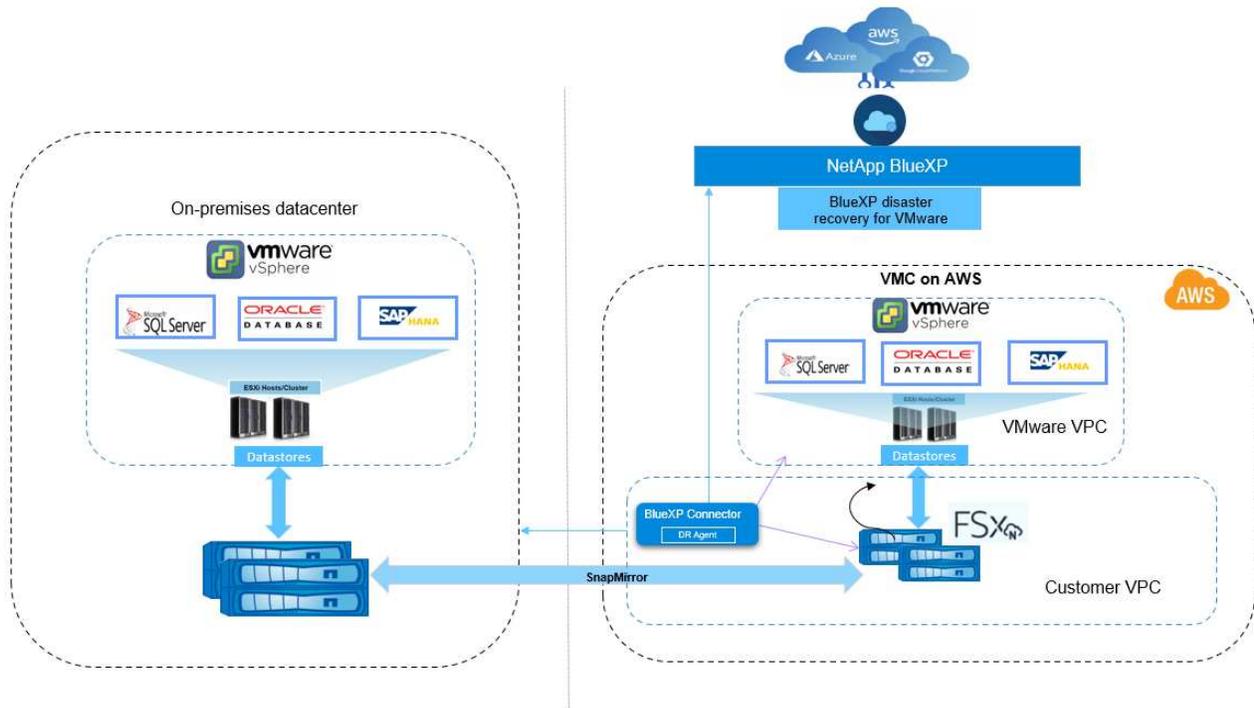
Pour continuer après l'essai de 30 jours, vous devez souscrire un abonnement PAYGO (paiement basé sur l'utilisation) auprès de votre fournisseur de cloud ou acheter une licence BYOL auprès de NetApp.

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

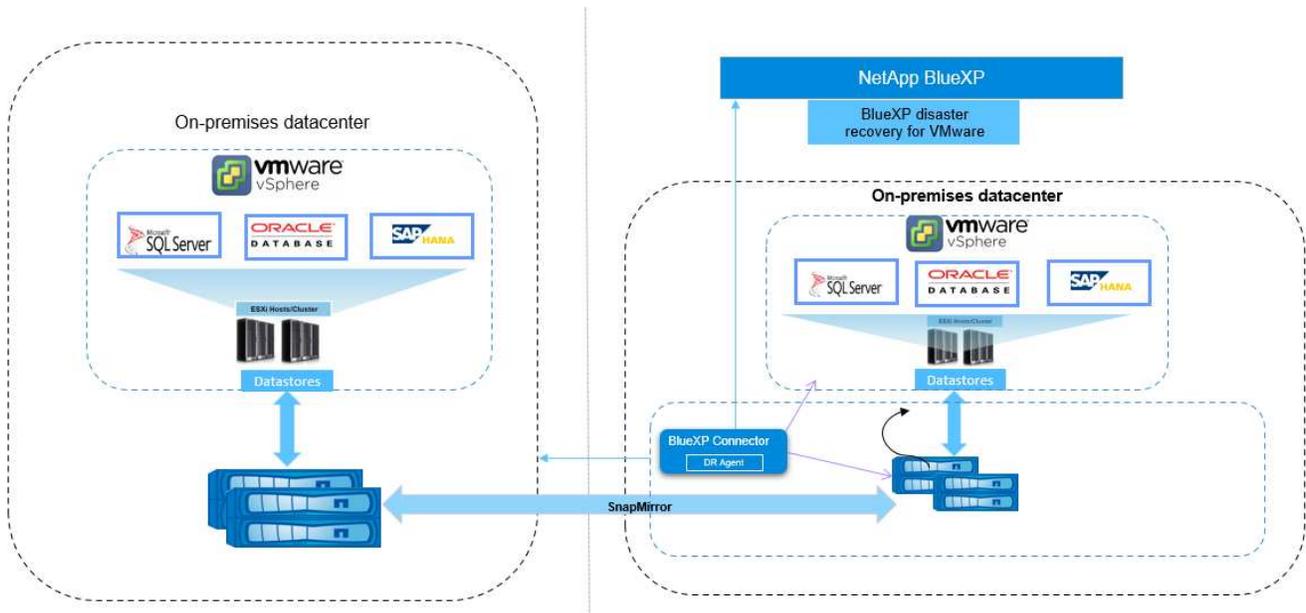
Fonctionnement de la reprise d'activité BlueXP

La reprise d'activité BlueXP permet de restaurer des workloads répliqués depuis un site sur site vers Amazon FSX pour ONTAP ou un autre site sur site. Ce service automatise la restauration à partir du niveau SnapMirror, via l'enregistrement des machines virtuelles vers Virtual machine Cloud (VMC) et les mappages du réseau directement sur la plateforme de sécurité et de virtualisation du réseau VMware, NSX-T. Cette fonctionnalité est incluse dans tous les environnements Virtual machine Cloud.

La reprise d'activité BlueXP s'appuie sur la technologie ONTAP SnapMirror, qui offre une réplication ultra-efficace et préserve l'efficacité des copies Snapshot incrémentielles à l'infini de ONTAP. La réplication SnapMirror garantit que les copies Snapshot cohérentes au niveau des applications sont toujours synchronisées et que les données sont utilisables immédiatement après un basculement.



Le schéma suivant présente l'architecture des plans de reprise d'activité sur site à sur site.



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

- Le service vous permet également de rétablir les machines virtuelles à l'emplacement source d'origine.
- Vous pouvez tester le processus de basculement de reprise après incident sans interrompre les machines virtuelles d'origine. Le test restaure 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 dernier instantané (par défaut) ou le dernier instantané sélectionné à partir duquel restaurer votre machine virtuelle.

Des conditions qui peuvent vous aider dans la reprise d'activité BlueXP

Il est parfois utile de comprendre la terminologie relative à la reprise sur incident.

- **Site** : conteneur logique généralement associé à un centre de données physique ou à un fournisseur de cloud.
- **Resource group** : conteneur logique qui vous permet de gérer plusieurs machines virtuelles en tant qu'unité unique.
- **Plan de réplication** : ensemble de règles sur la fréquence des sauvegardes et sur la manière de gérer les événements de basculement. Les plans sont affectés à un ou plusieurs groupes de ressources.

Conditions préalables à la reprise d'activité BlueXP

Avant d'utiliser la reprise d'activité BlueXP, vérifiez que votre environnement répond aux exigences de stockage ONTAP, de cluster VMware vCenter et de BlueXP.

Conditions préalables au stockage ONTAP

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

- Les clusters source et cible doivent avoir une relation de pairs.
- Le SVM qui hébergera les volumes de reprise d'activité doit exister sur le cluster destination.
- Le SVM source et le SVM destination doivent avoir une relation entre pairs.



La création des volumes de reprise d'activité dans le SVM ou SVM de destination n'est pas anticipée. La reprise d'activité BlueXP crée les volumes de destination selon les besoins du plan de réplication.

- En cas de déploiement avec Amazon FSX pour NetApp ONTAP, la condition préalable suivante s'applique :
 - Une instance Amazon FSX pour NetApp ONTAP pour héberger les datastores VMware DR doit exister dans votre VPC. Reportez-vous à la documentation d'Amazon FSX pour ONTAP sur "[guide d'utilisation](#)".

Prérequis pour les clusters VMware vCenter

Ces conditions préalables s'appliquent à la fois aux clusters vCenter sur site et au Software-Defined Data Center (SDDC) de VMware Cloud for AWS.

- Tous les clusters VMware que vous souhaitez gérer avec BlueXP Disaster Recovery doivent être hébergés sur des volumes ONTAP.
- Tous les datastores VMware à gérer par la reprise d'activité BlueXP doivent utiliser l'un des protocoles suivants :
 - NFS
 - VMFS avec protocole iSCSI ou FC
- VMware vSphere version 7.0 mise à jour 3 (7.0v3) ou ultérieure
- Si vous utilisez un SDDC de VMware Cloud, les conditions préalables suivantes s'appliquent.

- Dans VMware Cloud Console, utilisez les rôles de service Administrateur et Administrateur Cloud NSX. Utilisez également le propriétaire de l'organisation pour le rôle Organisation. Reportez-vous à la ["Utilisation de la documentation VMware Cloud Foundations avec AWS FSX for NetApp ONTAP"](#).
- Associez le SDDC dans le cloud VMware à l'instance Amazon FSX pour NetApp ONTAP. Reportez-vous à la ["Intégration de VMware Cloud on AWS avec Amazon FSX for NetApp ONTAP"](#).

Prérequis de BlueXP

Lancez-vous avec BlueXP

Si vous ne l'avez pas déjà fait, ["Inscrivez-vous à BlueXP et créez une entreprise"](#)

Collectez les informations d'identification pour ONTAP et VMware

- Les identifiants Amazon FSX pour ONTAP et AWS doivent être ajoutés à l'environnement de travail dans le projet BlueXP qui sera utilisé pour gérer la reprise d'activité BlueXP .
- La reprise d'activité BlueXP nécessite des informations d'identification vCenter. Vous entrez les informations d'identification vCenter lorsque vous ajoutez un site dans le cadre de la reprise d'activité BlueXP.

Pour obtenir la liste des privilèges vCenter nécessaires, reportez-vous ["Privilèges vCenter requis pour la reprise d'activité BlueXP"](#) à la section . Pour obtenir des instructions sur l'ajout d'un site, reportez-vous à la section ["Ajouter un site"](#).

Créer un connecteur BlueXP

Un connecteur BlueXP doit être configuré dans BlueXP. Lorsque vous utilisez le connecteur BlueXP, il inclut les fonctionnalités appropriées pour le service de reprise d'activité.

- La reprise d'activité BlueXP fonctionne uniquement avec le déploiement de connecteur de mode standard. Voir ["Mise en route de BlueXP en mode standard"](#).
- Assurez-vous que les vCenters source et de destination utilisent le même connecteur BlueXP.
- Type de connecteur BlueXP requis :
 - **Reprise d'activité sur site et sur site** : installez le connecteur sur site BlueXP sur le site de reprise d'activité. Reportez-vous à la ["Installez et configurez un connecteur sur site"](#).
 - **Sur site vers AWS** : installez le connecteur BlueXP pour AWS dans votre VPC AWS. Reportez-vous à la ["Options d'installation des connecteurs dans AWS"](#).



Du site aux environnements sur site, utilisez le connecteur sur site BlueXP. Pour les environnements sur site ou AWS, utilisez le connecteur BlueXP AWS Connector, qui permet d'accéder au vCenter sur site source et au vCenter sur site de destination.

- Le connecteur BlueXP installé doit pouvoir accéder à tout cluster VMware que la reprise d'activité BlueXP va gérer.
- Toutes les baies ONTAP devant être gérées par BlueXP Disaster Recovery doivent être ajoutées à tout environnement de travail du projet BlueXP qui sera utilisé pour gérer BlueXP Disaster Recovery.

Voir ["Découvrez les clusters ONTAP sur site"](#).

- Pour plus d'informations sur la configuration d'un proxy intelligent pour la reprise après incident BlueXP ,

reportez-vous à la section ["Configurez votre infrastructure pour la reprise d'activité BlueXP"](#).

Prérequis des charges de travail

Pour garantir la cohérence des processus au niveau des applications, appliquez les conditions préalables suivantes :

- 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 ou Oracle Database ou les deux, leurs enregistreurs VSS doivent être activés pour les bases de données.
- L'authentification utilisateur du système d'exploitation doit être activée pour le rôle SYSDBA de la base de données Oracle pour les bases de données Oracle qui s'exécutent sur un système d'exploitation Linux.

Démarrage rapide de la reprise d'activité BlueXP

Voici un aperçu des étapes à suivre pour démarrer avec la reprise d'activité BlueXP. Les liens de chaque étape vous mènent à une page qui fournit plus de détails.

1

Passer en revue les prérequis

["Assurez-vous que votre environnement répond à ces exigences"](#).

2

Configurez le service de reprise d'activité BlueXP

- ["Configurer l'infrastructure du service"](#).
- ["Configuration des licences"](#).

3

Et la suite ?

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

- ["Ajoutez vos sites vCenter à la reprise d'activité BlueXP"](#).
- ["Créez votre premier groupe de ressources"](#).
- ["Créez votre premier plan de réplication"](#).
- ["Réplication d'applications vers un autre site"](#).
- ["Basculement des applications vers un site distant"](#).
- ["Rétablir les applications sur le site source d'origine"](#).
- ["Gérer les sites, les groupes de ressources et les plans de réplication"](#).
- ["Contrôler les opérations de reprise après incident"](#).

Configurez votre infrastructure pour la reprise d'activité BlueXP

Pour utiliser la reprise d'activité BlueXP, effectuez quelques étapes de configuration dans Amazon Web Services (AWS) et BlueXP.



Révision "prérequis" pour vous assurer que votre environnement est prêt.

Préparez-vous à la reprise d'activité BlueXP pour la protection des données sur site à sur site

Assurez-vous que les exigences suivantes sont respectées avant de configurer la reprise d'activité BlueXP pour la protection sur site à sur site :

- Le stockage ONTAP
 - Vérifiez que vous disposez des informations d'identification ONTAP.
 - Créez ou vérifiez votre site de reprise sur incident.
 - Créez ou vérifiez votre SVM ONTAP de destination.
 - Vérifiez que vos SVM ONTAP source et destination sont bien peering.
- Clusters vCenter
 - Assurez-vous que les machines virtuelles que vous souhaitez protéger sont hébergées sur des datastores NFS (en utilisant des volumes NFS ONTAP) ou des datastores VMFS (en utilisant des LUN iSCSI NetApp).
 - Examen "[vCenter Privileges](#)" requis pour BlueXP DR.
 - Créez un compte d'utilisateur de reprise après incident (pas le compte d'administrateur vCenter par défaut) et attribuez le vCenter Privileges au compte.

Prise en charge de proxy intelligent

Le connecteur BlueXP prend en charge le proxy intelligent. Le proxy intelligent est un moyen léger, sécurisé et efficace de connecter votre environnement sur site au service BlueXP. Il fournit une connexion sécurisée entre votre environnement et le service BlueXP sans VPN ni accès direct à Internet. Cette mise en œuvre de proxy optimisée décharge le trafic API au sein du réseau local.

Lorsqu'un proxy est configuré, la reprise après incident BlueXP tente de communiquer directement avec VMware ou ONTAP et utilise le proxy configuré en cas d'échec de la communication directe.

La mise en œuvre du proxy de reprise après incident BlueXP nécessite une communication sur le port 443 entre le connecteur et tous les serveurs vCenter et baies ONTAP utilisant un protocole HTTPS. L'agent de reprise après incident BlueXP intégré au connecteur 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 BlueXP, reportez-vous à la section "[Configurez un connecteur pour utiliser un serveur proxy](#)".

Préparez-vous à la reprise d'activité BlueXP pour une protection sur site dans le cloud avec AWS

Pour configurer la reprise d'activité BlueXP pour la protection des données sur site vers le cloud avec AWS, vous devez configurer les éléments suivants :

- Configurez AWS FSX pour NetApp ONTAP
- Configurez VMware Cloud sur un SDDC AWS

Configurez AWS FSX pour NetApp ONTAP

- Créez un système de fichiers Amazon FSX pour NetApp ONTAP.
 - Provisionnez et configurez FSX pour ONTAP. Amazon FSX pour NetApp ONTAP est un service entièrement géré qui fournit un stockage de fichiers extrêmement fiable, évolutif, haute performance et riche en fonctionnalités, basé sur le système de fichiers NetApp ONTAP.
 - Suivez les étapes "[Rapport technique 4938 : montez Amazon FSX ONTAP en tant que datastore NFS avec VMware Cloud sur AWS](#)" des et pour provisionner et "[Démarrage rapide d'Amazon FSX pour NetApp ONTAP](#)" configurer FSX pour ONTAP.
- Ajoutez Amazon FSX pour ONTAP à l'environnement de travail et les identifiants AWS pour FSX pour ONTAP.
- Créez ou vérifiez votre SVM ONTAP de destination dans l'instance AWS FSX pour ONTAP.
- Configurez la réplication entre votre cluster ONTAP source sur site et votre instance FSX pour ONTAP dans BlueXP .

Reportez-vous "[Comment configurer un environnement de travail FSX pour ONTAP](#)" à la pour obtenir des instructions détaillées.

Configurez VMware Cloud sur un SDDC AWS

"[VMware Cloud sur AWS](#)" Offre une expérience cloud native pour les charges de travail VMware dans l'écosystème AWS. Chaque data Center Software-defined VMware (SDDC) s'exécute dans un cloud privé virtuel Amazon et fournit une pile VMware complète (y compris vCenter Server), une mise en réseau Software-defined NSX-T, un stockage Software-defined 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 de la section "[Déploiement et configuration de l'environnement de virtualisation sur AWS](#)". Un cluster pilote peut également être utilisé à des fins de reprise après incident.

Accédez à la reprise d'activité BlueXP

NetApp BlueXP vous permet de vous connecter au service de reprise d'activité BlueXP.

Pour vous connecter à BlueXP, vous pouvez utiliser vos identifiants du site de support NetApp ou vous inscrire à une connexion au cloud NetApp à l'aide de votre e-mail et de votre mot de passe. "[En savoir plus sur la connexion](#)".

Des tâches spécifiques nécessitent des rôles d'utilisateur BlueXP spécifiques. "[En savoir plus sur les rôles et les autorisations des utilisateurs dans la BlueXP disaster recovery](#)". "[En savoir plus sur les rôles d'accès BlueXP pour tous les services](#)".

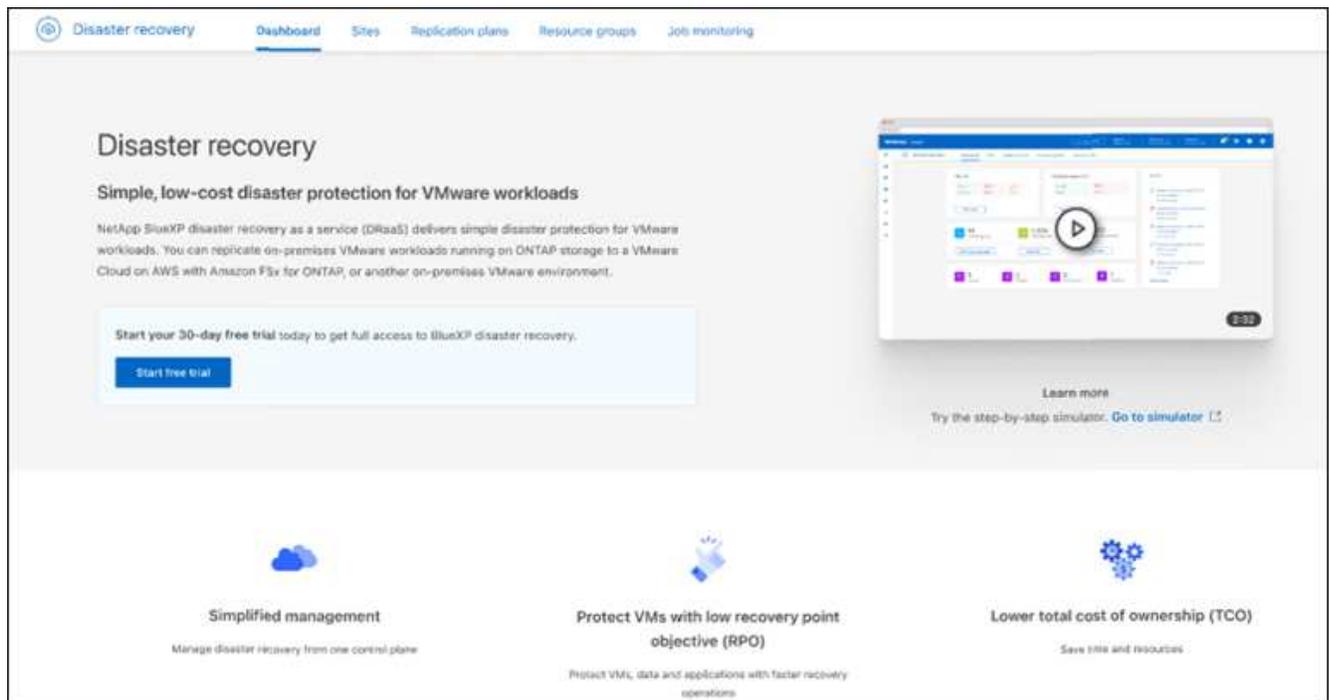
Étapes

1. Ouvrez un navigateur Web et accédez au ["Console BlueXP"](#).

La page de connexion NetApp BlueXP s'affiche.

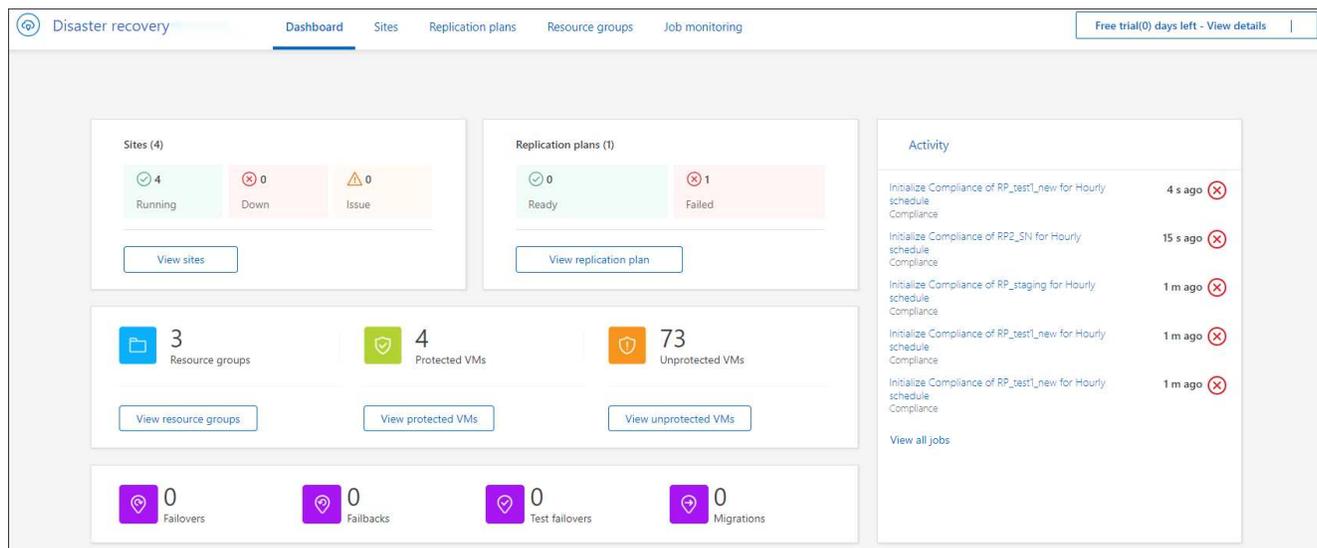
2. Connectez-vous à BlueXP.
3. Dans le menu de navigation de gauche de BlueXP, sélectionnez **protection > Disaster Recovery**.

Si vous vous connectez pour la première fois à ce service, la page d'accueil s'affiche et vous pouvez vous inscrire pour un essai gratuit.



Sinon, le tableau de bord de reprise d'activité BlueXP s'affiche.

- Si vous n'avez pas encore ajouté de connecteur BlueXP, vous devez ajouter un connecteur. Pour ajouter un connecteur, voir ["En savoir plus sur les connecteurs"](#).
- Si vous utilisez BlueXP avec un connecteur existant, lorsque vous sélectionnez « reprise après incident », un message s'affiche pour vous inscrire.
- Si vous utilisez déjà le service, le tableau de bord s'affiche lorsque vous sélectionnez « récupération après sinistre ».



Configurez les licences pour la reprise d'activité BlueXP

Avec la reprise d'activité BlueXP, vous pouvez utiliser différents plans de licence, notamment un essai gratuit, un abonnement avec paiement à l'utilisation ou l'utilisation de votre propre licence.

Rôle BlueXP requis Rôle d'administrateur d'organisation, d'administrateur de dossier ou de projet, d'administrateur de récupération après sinistre ou d'administrateur d'application de récupération après sinistre.

["En savoir plus sur les rôles et les autorisations des utilisateurs dans la BlueXP disaster recovery"](#). ["En savoir plus sur les rôles d'accès BlueXP pour tous les services"](#).

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

- Inscrivez-vous pour bénéficier d'un essai gratuit de 30 jours.
- Achetez un abonnement à la carte (PAYGO) à * NetApp Intelligent Services* avec Amazon Web Services (AWS) Marketplace ou à Microsoft Azure Marketplace.
- BYOL (Bring Your Own License), un fichier de licence NetApp (NLF) que vous obtenez auprès de votre ingénieur commercial NetApp. Vous pouvez utiliser le numéro de série de licence pour activer la fonction BYOL dans le portefeuille digital BlueXP.



Les frais de reprise sur incident BlueXP sont basés sur la capacité utilisée des datastores sur le site source lorsqu'au moins une machine virtuelle possède un plan de réplication. La capacité d'un datastore ayant subi un basculement n'est pas incluse dans l'allocation de capacité. Pour les modèles BYOL, si les données dépassent la capacité autorisée, les opérations du service sont limitées jusqu'à ce que vous obteniez une licence de capacité supplémentaire ou mettiez à niveau la licence dans le portefeuille digital BlueXP.

["En savoir plus sur le portefeuille digital"](#).

Après la fin de la période d'essai gratuite ou l'expiration de la licence, vous pouvez toujours effectuer les opérations suivantes dans le service :

- Afficher 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 gratuitement pendant 30 jours

Essayez la reprise d'activité BlueXP avec un essai gratuit de 30 jours.



Aucune limite de capacité n'est appliquée pendant l'essai.

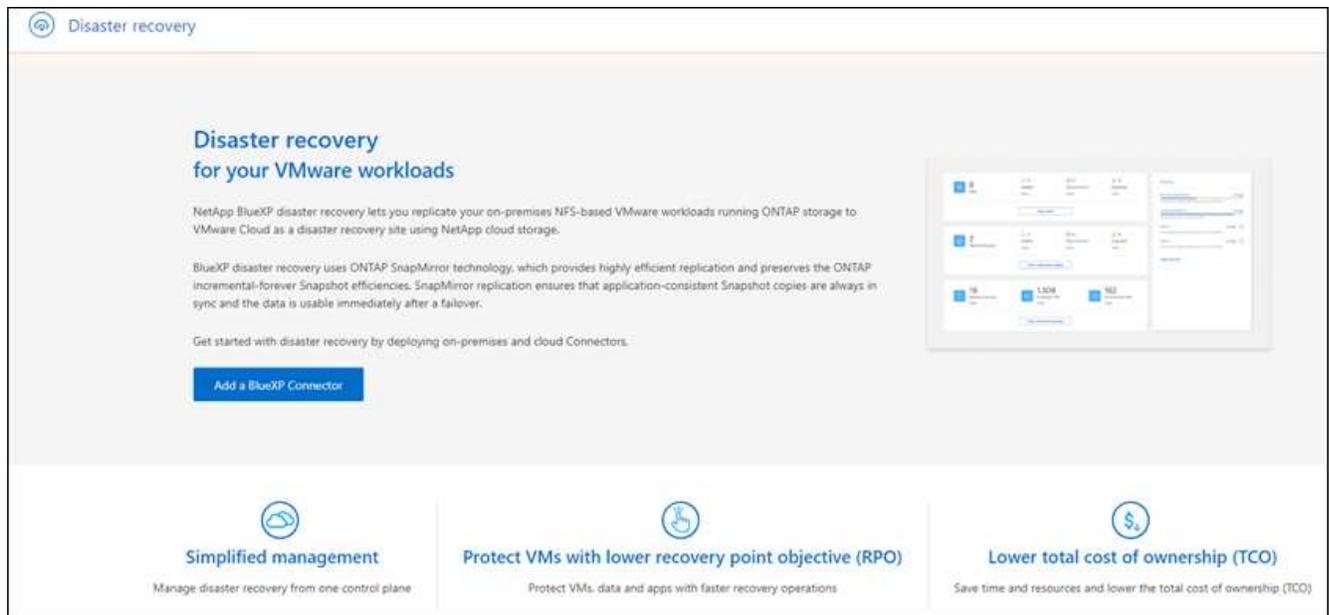
Après la période d'essai, vous devez acheter une licence BYOL ou un abonnement PAYGO AWS. Vous pouvez obtenir une licence à tout moment et vous ne serez pas facturé avant la fin de la période d'essai.

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

Étapes

1. Accédez au ["Console BlueXP"](#).
2. Connectez-vous à BlueXP.
3. Dans le menu de navigation de gauche de BlueXP, sélectionnez **protection > Disaster Recovery**.

S'il s'agit de votre première connexion à ce service, la page d'accueil s'affiche.



4. Si vous n'avez pas encore ajouté de connecteur pour d'autres services, ajoutez-en un.

Pour ajouter un connecteur, voir ["En savoir plus sur les connecteurs"](#).

5. Une fois que vous avez configuré un connecteur, sur la page d'accueil de la reprise d'activité BlueXP, le bouton pour ajouter des modifications de connecteur à un bouton et lancer un essai gratuit. Sélectionnez **Démarrer essai gratuit**.

6. Commencez par ajouter des vCenters.

Pour plus de détails, voir ["Ajoutez des sites vCenter"](#).

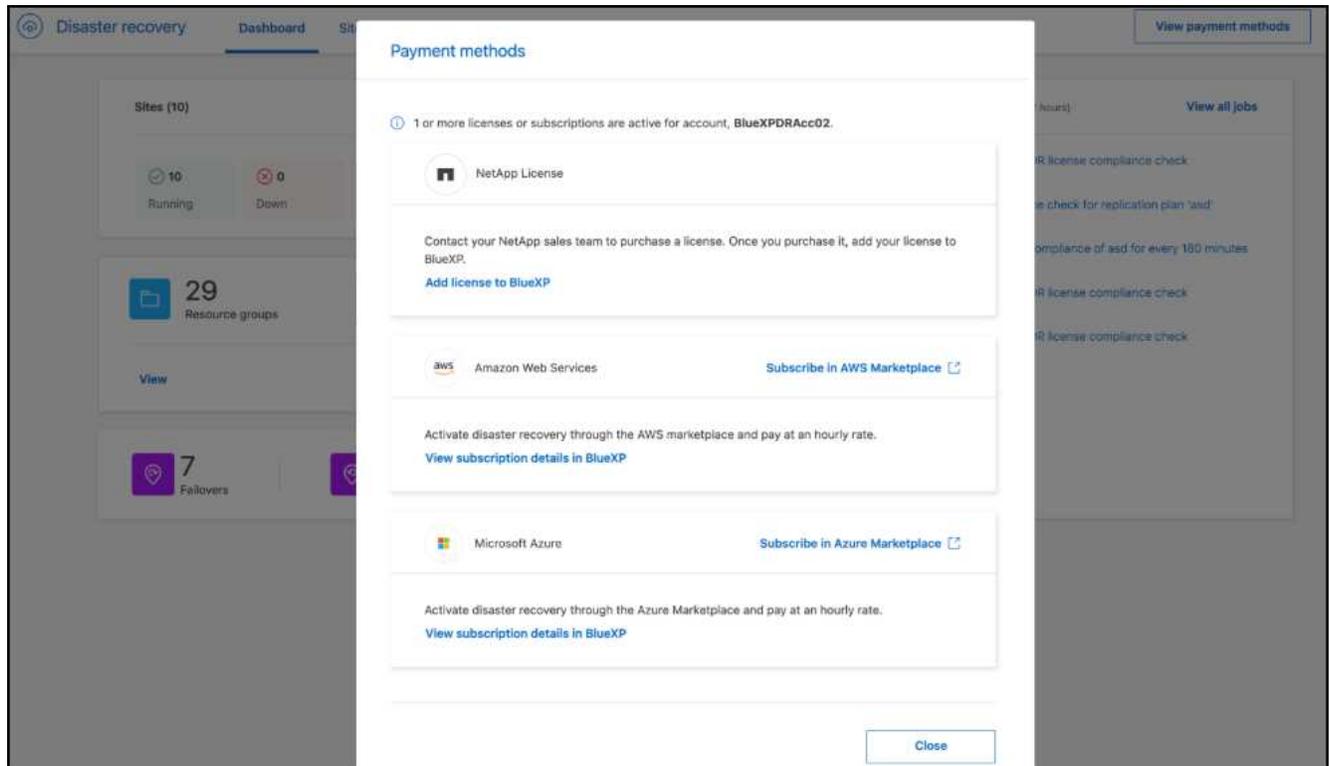
Une fois l'essai terminé, abonnez-vous via l'une des places de marché

Une fois l'essai gratuit terminé, vous pouvez acheter une licence auprès de NetApp ou vous abonner à * NetApp Intelligent Services* 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. Lors de la reprise d'activité de BlueXP, un message vous indique que la version d'essai gratuite arrive à expiration. Dans le message, sélectionnez **s'abonner ou acheter une licence**.

Ou, en haut à droite, 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 Intelligent Services* et à * BlueXP disaster recovery*.
4. Lorsque vous revenez à la reprise d'activité BlueXP, un message indique que vous êtes abonné.

Vous pouvez afficher les détails de l'abonnement dans le portefeuille digital BlueXP . ["En savoir plus sur la gestion des abonnements avec le portefeuille digital"](#).

Une fois la version d'évaluation terminée, achetez une licence BYOL par l'intermédiaire de NetApp

Une fois la version d'évaluation terminée, vous pouvez acheter une licence auprès de votre représentant commercial NetApp

Si vous apportez votre propre licence (BYOL), la configuration inclut l'achat de la licence, l'obtention du fichier de licence NetApp (NLF) et l'ajout de la licence au portefeuille digital BlueXP.

Ajouter la licence au portefeuille numérique BlueXP * après avoir acheté votre licence de reprise après sinistre BlueXP auprès de votre représentant commercial NetApp, vous pouvez gérer la licence dans le portefeuille numérique.

["Découvrez comment ajouter des licences avec le portefeuille digital"](#).

Mettez à jour votre licence BlueXP lorsqu'elle expire

Si votre période de licence approche la date d'expiration ou si votre capacité sous licence atteint la limite, vous serez informé dans l'interface utilisateur de reprise d'activité BlueXP. Vous pouvez mettre à jour votre licence de reprise d'activité BlueXP avant son expiration afin que vous puissiez accéder à vos données numérisées sans interruption.



Ce message apparaît également dans le portefeuille digital BlueXP et dans ["Notifications"](#).

["En savoir plus sur la mise à jour des licences avec le portefeuille digital"](#).

Terminez l'essai gratuit

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

Étapes

1. Dans la reprise d'activité BlueXP, en haut à droite, sélectionnez **essai gratuit - Afficher les détails**.
2. Dans la liste déroulante des détails, sélectionnez **Terminer l'essai gratuit**.

End free trial

Are you sure that you want to end your free trial on your account BlueXPAuto1? We will delete your data 60 days after you end your trial. If you subscribe or purchase a license within 60 days, we will retain your data. You may also delete your data immediately when you end your trial.

This action is not reversible.

Delete data immediately after ending my free trial

Comments

Type "end trial" to end your free trial.

End

Cancel

3. Si vous voulez supprimer toutes les données, cochez **Supprimer les données immédiatement après avoir mis fin à mon essai gratuit**.

Ceci supprimera tous les plannings, 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 vie du produit.



Si vous avez mis fin à l'essai gratuit, n'avez pas demandé de supprimer des données et n'avez pas acheté de licence ou d'abonnement, BlueXP Disaster Recovery supprime toutes vos données 60 jours après la fin de l'essai gratuit.

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

Forum aux questions sur la reprise d'activité BlueXP

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

Quelle est l'URL de reprise d'activité BlueXP ?

Pour l'URL, dans un navigateur, entrez : "<https://console.bluexp.netapp.com/>" Pour accéder à la console BlueXP.

Avez-vous besoin d'une licence pour utiliser la reprise d'activité BlueXP ?

Une licence de reprise d'activité BlueXP est requise pour un accès complet. Cependant, vous pouvez essayer gratuitement.

Pour plus d'informations sur la configuration des licences pour la reprise d'activité BlueXP, reportez-vous à la section "[Configurez la licence de reprise d'activité BlueXP](#)".

Comment accédez-vous à la récupération après sinistre de BlueXP ? La reprise d'activité BlueXP ne nécessite aucune activation. L'option de reprise d'activité s'affiche automatiquement dans le menu de navigation de gauche de BlueXP.

Utilisez la reprise d'activité BlueXP

Utilisez la présentation de la reprise d'activité BlueXP

La reprise d'activité BlueXP vous permet d'atteindre les objectifs suivants :

- ["Consultez l'état de vos plans de reprise d'activité"](#).
- ["Ajoutez des sites vCenter"](#).
- ["Créer des groupes de ressources pour organiser les VM ensemble"](#)
- ["Création d'un plan de reprise d'activité"](#).
- ["Répliquez des applications VMware"](#) Sur votre site principal vers un site distant de reprise d'activité dans le cloud, grâce à la réplication SnapMirror
- ["Migrez vos applications VMware"](#) sur votre site principal vers un autre site.
- ["Tester le basculement"](#) sans interrompre les machines virtuelles d'origine.
- En cas d'incident, ["basculez votre site principal"](#) À VMware Cloud on AWS avec FSX for NetApp ONTAP.
- Une fois le sinistre résolu, ["retour arrière"](#) du site de reprise sur incident au site principal.
- ["Contrôler les opérations de reprise après incident"](#) Sur la page surveillance des travaux.

Consultez l'état de vos plans de reprise après sinistre BlueXP sur le tableau de bord

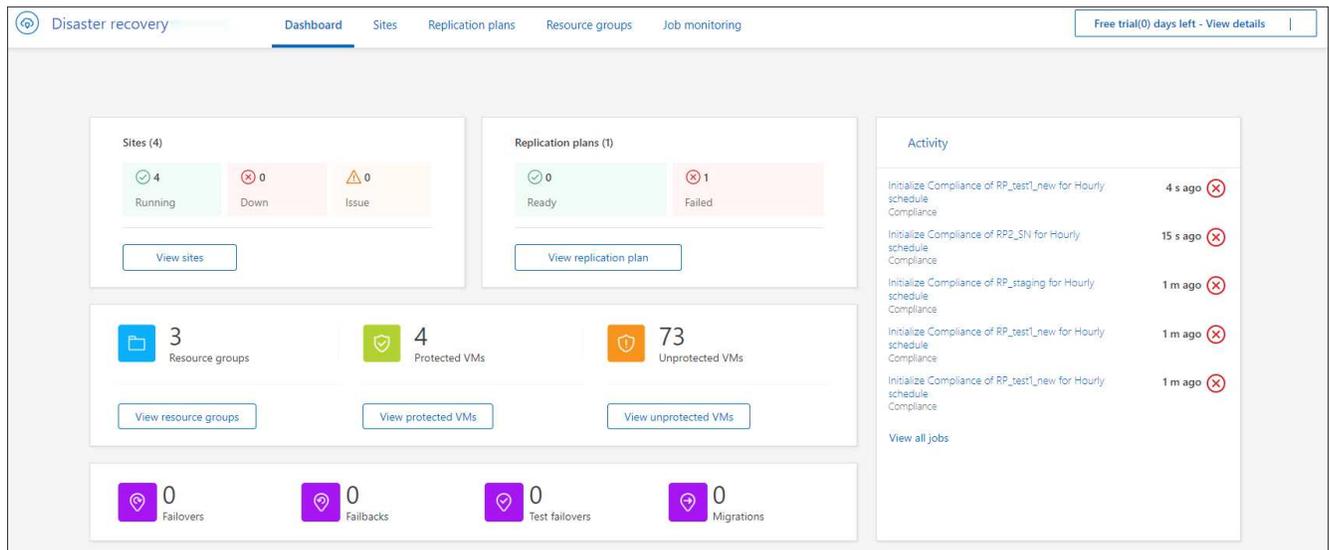
Le tableau de bord de reprise d'activité BlueXP vous permet de déterminer l'état de vos sites de reprise d'activité et de vos plans de réplication. Vous pouvez rapidement déterminer quels sites et plans sont sains, déconnectés ou dégradés.

Rôle BlueXP requis Administrateur d'organisation, administrateur de dossier ou de projet, administrateur de récupération après sinistre, administrateur d'application de récupération après sinistre ou rôle de visualiseur de récupération après sinistre.

["En savoir plus sur les rôles et les autorisations des utilisateurs dans la BlueXP disaster recovery"](#). ["En savoir plus sur les rôles d'accès BlueXP pour tous les services"](#).

Étapes

1. Dans le menu de navigation gauche de BlueXP, sélectionnez **protection > reprise après sinistre**.
2. Dans le menu supérieur de reprise d'activité BlueXP, sélectionnez **Tableau de bord**.



3. 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 États suivants :
 - **En cours d'exécution** : le vCenter est connecté, sain et en cours d'exécution.
 - **Down** : le vCenter n'est pas accessible ou présente des problèmes de connectivité.
 - **Problème** : le vCenter est inaccessible ou présente des problèmes de connectivité.

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

- **Plans de réplication** : permet d'afficher l'état de santé de vos plans. Un plan peut avoir l'un des États suivants :
 - **Prêt**
 - **Échec**

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

- **Groupes de ressources** : permet d'afficher l'état de santé de vos groupes de ressources. Un groupe de ressources peut avoir l'un des États suivants :
- **MV protégées** : les VM font partie d'un groupe de ressources.
- **Machines virtuelles non protégées** : les machines virtuelles ne font pas partie d'un groupe de ressources.

Pour consulter les détails, cliquez sur le lien **Afficher** situé en dessous de chaque.

- 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 ».

4. Vérifiez toutes les opérations dans le volet activité. Pour afficher toutes les opérations sur le moniteur des tâches, sélectionnez **Afficher tous les travaux**.

Ajouter des vCenters à un site dans la récupération après sinistre BlueXP

Avant de créer un plan de reprise sur incident, vous devez ajouter un serveur vCenter principal à un site et un site de reprise sur incident vCenter cible dans BlueXP .



Assurez-vous que les vCenters source et de destination utilisent le même connecteur BlueXP.

Une fois les vCenter ajoutés, la reprise après incident BlueXP effectue une découverte approfondie des environnements vCenter, notamment des clusters vCenter, des hôtes ESXi, des datastores, l'empreinte du stockage, les détails des machines virtuelles, des répliques SnapMirror et des réseaux de machines virtuelles.

Rôle BlueXP 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 la BlueXP disaster recovery"](#). ["En savoir plus sur les rôles d'accès BlueXP pour tous les services"](#).

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



La reprise sur incident BlueXP effectue une détection toutes les 24 heures. Après avoir configuré un site, vous pouvez modifier vCenter ultérieurement pour personnaliser le planning 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 la découverte de sorte 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 à jour sur votre environnement. Ensuite, vous pouvez définir la planification pour qu'elle s'exécute automatiquement.

Les machines virtuelles récemment 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 :

- À vos marques
- Rétablissement validé
- Le basculement de test a été validé

Étapes

1. Connectez-vous à BlueXP et dans le menu de navigation de gauche, sélectionnez **protection > récupération après sinistre**.

Accédez à la page du tableau de bord de reprise d'activité BlueXP. Lorsque vous commencez par utiliser le service, vous devez ajouter des informations vCenter. Plus tard, le tableau de bord affiche les données relatives à vos sites et à vos plans de réplication.



Différents champs s'affichent en fonction du type de site que vous ajoutez.

2. **Source** : sélectionnez **découvrir les serveurs vCenter** pour entrer des informations sur le site vCenter source.



Si certains sites vCenter existent déjà et que vous souhaitez en ajouter d'autres, sélectionnez **sites** dans le menu supérieur, puis **Ajouter**.

- Ajoutez un site, sélectionnez le connecteur BlueXP et fournissez les informations d'identification vCenter.
- (S'applique uniquement aux sites sur site) 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 serveur vCenter est configuré avec des certificats d'autorité de certification (CA) **NON**, cochez cette case ; sinon, la connexion au serveur vCenter ne fonctionnera pas.

3. Sélectionnez **Ajouter**.

Vous allez ensuite ajouter un vCenter cible.

4. **Cible** :

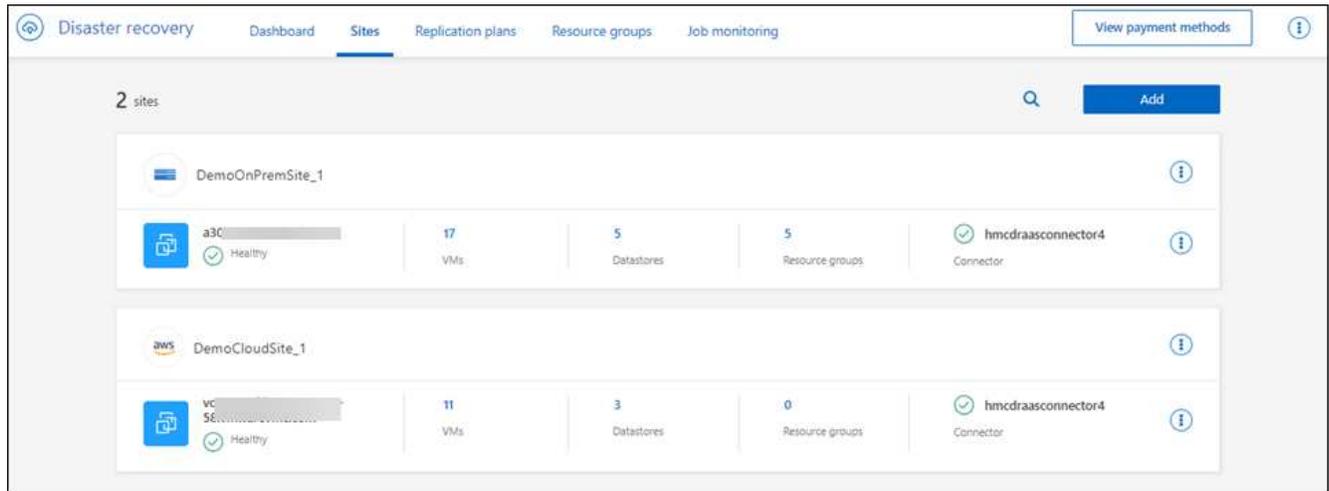
- a. Choisissez le site cible et l'emplacement. Si la cible est Cloud, sélectionnez **AWS**.

- (S'applique uniquement aux sites clouds) **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 console BlueXP .

b. Sélectionnez **Ajouter**.

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



5. Pour voir la progression de l'opération, dans le menu supérieur, sélectionnez **surveillance des tâches**.

Ajoutez le mappage de sous-réseau pour un site vCenter

Gérer les adresses IP lors du basculement de manière nouvelle à l'aide du mappage de sous-réseau, qui vous permet d'ajouter des sous-réseaux pour chaque vCenter. Dans ce cas, vous définissez le CIDR IPv4, la passerelle par défaut et le DNS pour chaque réseau virtuel.

Lors du basculement, la reprise après incident BlueXP 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 :

- Réseau a = 10.1.1.0/24
- Réseau B = 192.168.1.0/24

VM1 dispose d'une vNIC (10.1.1.50) connectée au réseau A. NetworkA est mappé sur le réseau B dans les paramètres du plan de réplication.

En cas de basculement, la reprise après incident BlueXP 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, BlueXP Disaster Recovery examine les paramètres CIDR du réseau B et utilise cette partie du réseau 192.168.1 tout en conservant la partie hôte (.50) pour créer la nouvelle adresse IP du VM1. La nouvelle adresse 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 d'adresses IP en cas de basculement, notamment si vous avez des centaines de réseaux et des milliers de machines virtuelles à gérer.

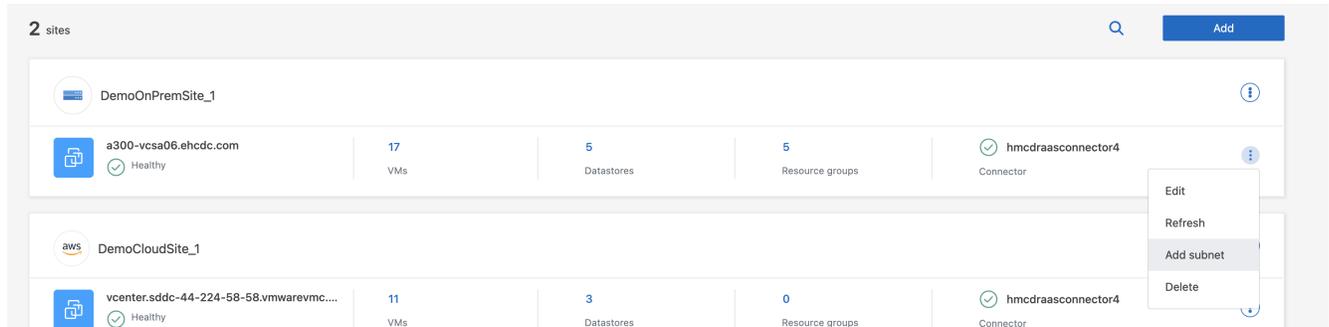
L'utilisation du mappage de sous-réseau est un processus en deux étapes facultatif :

- Commencez par ajouter 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 supérieur de récupération après sinistre de BlueXP , sélectionnez **sites**.
2. Dans l'icône actions  située à droite, sélectionnez **Ajouter un sous-réseau**.



La page configurer le sous-réseau s'affiche :

The 'Configure subnet' page displays a table with the following columns: Network Name, Datacenter Name, Subnet, Gateway, and DNS. The table contains five rows of network configurations. At the bottom, there are two buttons: 'Add subnet mapping' and 'Cancel'.

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

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

3. Sur la page configurer le sous-réseau, entrez les informations suivantes :
 - a. Subnet : saisissez le CIDR IPv4 du sous-réseau jusqu'à /32.



La notation CIDR est une méthode de spécification des adresses IP et de leurs masques de réseau. /24 indique le masque de réseau. Le numéro se compose d'une adresse IP dont le numéro se trouve après le signe « / » indiquant le nombre de bits de l'adresse IP qui indiquent le réseau. Par exemple, 192.168.0.50/24, l'adresse IP est 192.168.0.50 et le nombre total de bits de l'adresse réseau est 24. 192.168.0.50 255.255.255.0 devient 192.168.0.0/24.

- b. Passerelle : entrez la passerelle par défaut pour le sous-réseau.

c. DNS : entrez le DNS du sous-réseau.

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

Sélectionnez 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 en deux étapes facultatif :

- Commencez par ajouter 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 supérieur de reprise d'activité BlueXP, sélectionnez **plans de réplication**.
2. Sélectionnez **Ajouter** pour ajouter un plan de réplication.
3. Complétez les champs de la manière habituelle en ajoutant les serveurs vCenter, en sélectionnant les groupes de ressources ou les applications et en effectuant les mappages.
4. Dans la page Replication plan > Resource mapping, sélectionnez la section **Virtual machines**.

The screenshot shows the 'Virtual machines' configuration section. It includes a dropdown for 'IP address type' (set to 'Static') and a dropdown for 'Target IP' (with 'Use subnet mapping' selected). There are also checkboxes for 'Use the same credentials for all VMs' and 'Use the same script for all VMs'. Below these are input fields for 'Target VM prefix' and 'Target VM suffix', both labeled as 'Optional'. A preview of a sample VM name is visible on the right.

5. Dans le champ **Target IP**, 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 Windows), les informations d'identification sont nécessaires uniquement pour Windows.

6. Poursuivez la création du plan de réplication.

Modifiez le site du serveur vCenter et personnalisez la planification de la découverte

Vous pouvez modifier le site du serveur vCenter pour personnaliser le planning de découverte. Par exemple, si vous disposez d'un grand nombre de machines virtuelles, vous pouvez définir la planification de la découverte de sorte 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 avez ajouté des vCenters dans les versions précédentes et que vous souhaitez personnaliser le planning de découverte, vous devez modifier le site du serveur vCenter et définir le planning.

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 de récupération après sinistre de BlueXP , sélectionnez **sites**.
2. Sélectionnez le site à modifier.
3. Sélectionnez l'icône actions  sur la droite et sélectionnez **Modifier**.
4. Dans la page Modifier le serveur vCenter, modifiez les champs selon vos besoins.
5. Pour personnaliser le planning de découverte, cochez la case **Activer la découverte planifiée** et sélectionnez la date et l'intervalle de temps souhaités.

Edit vCenter server

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

Site	BlueXP Connector
<input type="text" value="Source"/>	<input type="text" value="SecLab_Connector_4"/>
vCenter IP address	port
<input type="text" value="172.26.212.218"/>	<input type="text" value="443"/>
vCenter user name	vCenter password
<input type="text"/>	<input type="text"/>

Use self-signed certificates ⓘ

Enable scheduled discovery

Start discovery from ⓘ : ⓘ

Run discovery once every Hour(s) Minute(s)

6. Sélectionnez **Enregistrer**.

Actualisez la découverte manuellement

Vous pouvez actualiser la détection manuellement à tout moment. Cette fonction est utile si vous avez ajouté ou supprimé des machines virtuelles et si vous souhaitez mettre à jour les informations dans la reprise sur incident BlueXP .

Étapes

1. Dans le menu de récupération après sinistre de BlueXP , sélectionnez **sites**.
2. Sélectionnez le site à actualiser.

3.

Sélectionnez l'icône actions



sur la droite et sélectionnez **Actualiser**.

Créer un groupe de ressources pour organiser les machines virtuelles ensemble dans la reprise après sinistre BlueXP

Après avoir ajouté des sites vCenter, vous pouvez créer des groupes de ressources qui regroupent des machines virtuelles par machines virtuelles ou par datastores. 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 des applications disposant de niveaux similaires. Comme autre exemple, les groupes peuvent contenir des ordres de démarrage retardés qui peuvent être exécutés lors de la récupération.

Rôle BlueXP requis Rôle d'administrateur d'organisation, d'administrateur de dossier ou de projet, d'administrateur de récupération après sinistre ou d'administrateur d'application de récupération après sinistre.

["En savoir plus sur les rôles et les autorisations des utilisateurs dans la BlueXP disaster recovery"](#). ["En savoir plus sur les rôles d'accès BlueXP pour tous les services"](#).

Vous pouvez regrouper les machines virtuelles elles-mêmes ou les machines virtuelles dans des datastores.

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

- Dans l'onglet groupes de ressources
- Pendant que vous créez une reprise d'activité ou un *plan de réplication*. Si un grand nombre de machines virtuelles sont hébergées par un cluster vCenter source, il peut être plus facile de créer les groupes de ressources lors de la création du plan de réplication. Pour obtenir des instructions sur la création de groupes de ressources lors de la création d'un plan de réplication, reportez-vous à la section ["Créer un plan de réplication"](#).



Chaque groupe de ressources peut inclure une ou plusieurs machines virtuelles ou datastores. Les machines virtuelles se mettra sous tension en fonction de l'ordre dans lequel vous les incluez dans le plan de réplication. Vous pouvez modifier l'ordre en faisant glisser les VM ou les datastores vers le haut ou vers le bas de la liste des groupes de ressources.

A propos des groupes de ressources

Les groupes de ressources vous permettent de combiner des machines virtuelles ou des datastores qui incluent des machines virtuelles liées aux opérations et qui doivent être protégées comme une seule unité.

Par exemple, une application de point de vente peut consister en plusieurs machines virtuelles hébergeant des bases de données, plusieurs machines virtuelles hébergeant la gestion des règles de logique applicative et plusieurs machines virtuelles agissant en tant que boutique basée sur un serveur Web. Il peut être avantageux de gérer la disponibilité de l'ensemble de l'application avec un processus de protection unique en plaçant ces VM dans un seul groupe de ressources.

Une fois les groupes de ressources configurés, vous pouvez appliquer les règles du plan de réplication pour un ordre de démarrage correct des machines virtuelles, une connexion réseau, etc. Afin d'assurer une

récupération correcte de toutes les machines virtuelles requises pour l'application.

Comment cela fonctionne-t-il ?

La reprise d'activité BlueXP protège les machines virtuelles en répliquant les volumes ONTAP sous-jacents et les LUN qui hébergent les machines virtuelles dans le groupe de ressources. Pour ce faire, le système demande à vCenter le nom de chaque magasin de données hébergeant des machines virtuelles dans un groupe de ressources. La fonction de reprise après incident BlueXP identifie ensuite le volume ONTAP source ou le LUN hébergeant ce datastore. Toutes les protections sont effectuées au niveau du volume ONTAP à l'aide de la réplication SnapMirror.

Si les machines virtuelles du groupe de ressources sont hébergées dans différents magasins de données, la reprise d'activité BlueXP utilise l'une des méthodes suivantes pour créer un snapshot cohérent avec les données des volumes ou des LUN ONTAP.

Emplacement relatif des volumes FlexVol	Processus de réplica d'instantané
Plusieurs datastores - volumes FlexVol sur même SVM	<ul style="list-style-type: none">• Groupe de cohérence ONTAP créé• Snapshots du groupe de cohérence pris• Réplication SnapMirror volume-scoped effectuée
Plusieurs magasins de données - volumes FlexVol dans plusieurs SVM	<ul style="list-style-type: none">• API ONTAP : <code>cg_start</code>. Quieces tous les volumes pour que des instantanés puissent être pris et lance des instantanés avec une portée de volume de tous les volumes de groupe de ressources.• API ONTAP : <code>cg_end</code>. Reprise des E/S sur tous les volumes et activation de la réplication SnapMirror étendue par volume après la création de snapshots.

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

- Avant d'ajouter des datastores à des groupes de ressources, commencez par lancer une découverte manuelle ou une découverte planifiée des machines virtuelles. Cela permet de s'assurer que les VM sont découvertes et répertoriées dans le groupe de ressources. Si vous ne lancez pas de découverte manuelle, il se peut que les machines virtuelles ne soient pas répertoriées dans le groupe de ressources.
- Assurez-vous qu'il y a au moins une machine virtuelle dans le datastore. S'il n'y a pas de VM dans le datastore, celui-ci ne sera pas découvert.
- Un datastore unique 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 datastore. Si des machines virtuelles protégées et non protégées sont hébergées sur le même datastore, les problèmes suivants peuvent se produire :
 - Étant donné que la reprise d'activité BlueXP utilise SnapMirror et que le système réplique des volumes ONTAP entiers, la capacité utilisée de ce volume est utilisée pour gérer les licences. 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 les datastores associés doivent être basculés vers le site de reprise d'activité, toutes les machines virtuelles non protégées (qui ne font pas partie du groupe de ressources mais sont hébergées sur le volume ONTAP) n'existeront plus sur le site source depuis le processus de basculement, entraînant ainsi la défaillance de machines virtuelles non protégées sur le site source.

Par ailleurs, la reprise sur incident BlueXP ne démarre pas ces machines virtuelles non protégées sur le site vCenter de basculement.

- Pour que la machine virtuelle soit protégée, elle doit être incluse dans un groupe de ressources.

MEILLEURE PRATIQUE : organisez vos machines virtuelles avant de déployer la reprise sur incident BlueXP pour limiter la « prolifération des datastores ». Placez les machines virtuelles qui ont besoin d'une protection sur un sous-ensemble de datastores et placez-les sur des machines virtuelles qui ne seront pas protégées dans un sous-ensemble différent de datastores. Assurez-vous que les machines virtuelles d'un datastore donné ne sont pas protégées par des plans de réplication différents.

Étapes

1. Dans le menu de récupération après sinistre de BlueXP , sélectionnez **groupes de ressources**.
2. Sélectionnez **Ajouter**.
3. Entrez un nom pour le groupe de ressources.
4. Sélectionnez le cluster vCenter source où se trouvent les VM.
5. Sélectionnez **machines virtuelles** ou **datastores** en fonction de la façon dont vous souhaitez effectuer la recherche.
6. Sélectionnez l'onglet **Ajouter des groupes de ressources**. Le système répertorie tous les datastores ou machines virtuelles du cluster vCenter sélectionné. Si vous avez sélectionné **datastores**, le système répertorie tous les datastores du cluster vCenter sélectionné. Si vous avez sélectionné **machines virtuelles**, le système répertorie toutes les machines virtuelles du cluster vCenter sélectionné.
7. Dans la partie gauche de la page Ajouter des groupes de ressources, sélectionnez les machines virtuelles que vous souhaitez protéger.

Add resource group

Name: DemoRG

vCenter: [Dropdown]

Virtual machines Datastores

Select virtual machines

Search all datastores

Select virtual machines	Selected VMs (3)
<input checked="" type="checkbox"/> VMFS_Centos_vm1_ds4	VMFS_Centos_vm1_ds4 X
<input checked="" type="checkbox"/> VMFS_Centos_vm1_ds5	VMFS_Centos_vm1_ds5 X
<input checked="" type="checkbox"/> VMFS_RHEL_vm2_ds1	VMFS_RHEL_vm2_ds1 X
<input type="checkbox"/> VMFS_RHEL_vm2_ds2	
<input type="checkbox"/> VMFS_RHEL_vm2_ds3	
<input type="checkbox"/> VMFS_RHEL_vm2_ds4	
<input type="checkbox"/> VMFS_RHEL_vm2_ds5	

Add Cancel

8. Vous pouvez également modifier l'ordre des machines virtuelles à droite en faisant glisser chaque machine virtuelle vers le haut ou le bas de la liste. Les machines virtuelles se mettra sous tension en fonction de l'ordre dans lequel vous les incluez.
9. Sélectionnez **Ajouter**.

Créer un plan de réplication dans la reprise après sinistre BlueXP

Une fois que vous avez ajouté des sites vCenter, vous pouvez créer un plan de reprise après incident ou de réplication. Sélectionnez les vCenters source et de destination, choisissez les groupes de ressources et définissez le mode de restauration et de mise sous tension des applications. Par exemple, vous pouvez regrouper des machines virtuelles (VM) associées à une application ou vous pouvez regrouper des applications disposant de niveaux similaires.

Ces plans sont parfois appelés *plans*.

Rôle BlueXP requis Administrateur d'organisation, administrateur de dossier ou de projet, administrateur de récupération après sinistre, administrateur de basculement de récupération après sinistre ou administrateur d'application de récupération après sinistre.

["En savoir plus sur les rôles et les autorisations des utilisateurs dans la BlueXP disaster recovery"](#). ["En savoir plus sur les rôles d'accès BlueXP pour tous les services"](#).

Vous pouvez créer un plan de réplication et modifier des plannings pour la conformité et les tests.

Vous pouvez protéger plusieurs machines virtuelles sur plusieurs datastores. La reprise d'activité BlueXP crée des groupes de cohérence ONTAP pour tous les volumes ONTAP hébergeant des datastores de machines virtuelles protégés.

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

- À vos marques
- Rétablissement validé
- Le basculement de test a été validé

Créez le plan

Un assistant vous guide tout au long de la procédure suivante :

- Sélectionnez serveurs vCenter.
- Sélectionnez les machines virtuelles ou datastores à répliquer et attribuez des groupes de ressources.
- Mappez la façon dont les ressources de l'environnement source sont mappées à la destination.
- Identifiez la récurrence, exécutez un script hébergé par l'invité, définissez l'ordre de démarrage et sélectionnez l'objectif du point de récupération.
- Revoir le plan.

Lorsque vous créez le plan, vous devez suivre les directives suivantes :

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

Avant de commencer

Si vous souhaitez créer une relation SnapMirror dans ce service, le cluster et son peering de SVM doivent avoir déjà été configurés en dehors de la reprise d'activité BlueXP.

Sélectionnez serveurs vCenter

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

Étapes

1. Dans le menu de navigation gauche de BlueXP, sélectionnez **protection > reprise après sinistre**.
2. Dans le menu supérieur de récupération après sinistre de BlueXP, sélectionnez **plans de réplication** et sélectionnez **Ajouter**. Ou, si vous commencez juste à utiliser le service, sélectionnez **Ajouter un plan de réplication** dans le tableau de bord.

Add replication plan

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

Replication plan > Add plan

vCenter servers and plan name

Provide the plan name and select source and target vCenter servers

Replication plan name
onprem to cloud GRI

i A source vCenter is where the production data exists; it gets replicated to a target vCenter

Source vCenter
a300-vcsa06.e

Target vCenter
vcenter.sc

Replicate

Cancel Next

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

Sélectionnez les applications à répliquer et attribuez des groupes de ressources

L'étape suivante consiste à regrouper les VM ou datastores requis en groupes de ressources fonctionnelles. Les groupes de ressources vous permettent de protéger un ensemble de machines virtuelles ou de datastores avec un snapshot commun.

Lorsque vous sélectionnez des applications dans le plan de réplication, vous pouvez voir le système d'exploitation pour chaque VM ou datastore du plan. Ceci est utile pour décider comment regrouper des VM ou des datastores dans un groupe de ressources.



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

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

- Avant d'ajouter des datastores à des groupes de ressources, commencez par lancer une découverte manuelle ou une découverte planifiée des machines virtuelles. Cela permet de s'assurer que les VM sont découvertes et répertoriées dans le groupe de ressources. Si vous ne lancez pas de découverte manuelle, il se peut que les machines virtuelles ne soient pas répertoriées dans le groupe de ressources.
- Assurez-vous qu'il y a au moins une machine virtuelle dans le datastore. S'il n'y a pas de VM dans le datastore, celui-ci ne sera pas découvert.
- Un datastore unique 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 datastore. Si des machines virtuelles protégées et non protégées sont hébergées sur le même datastore, les problèmes suivants peuvent se produire :

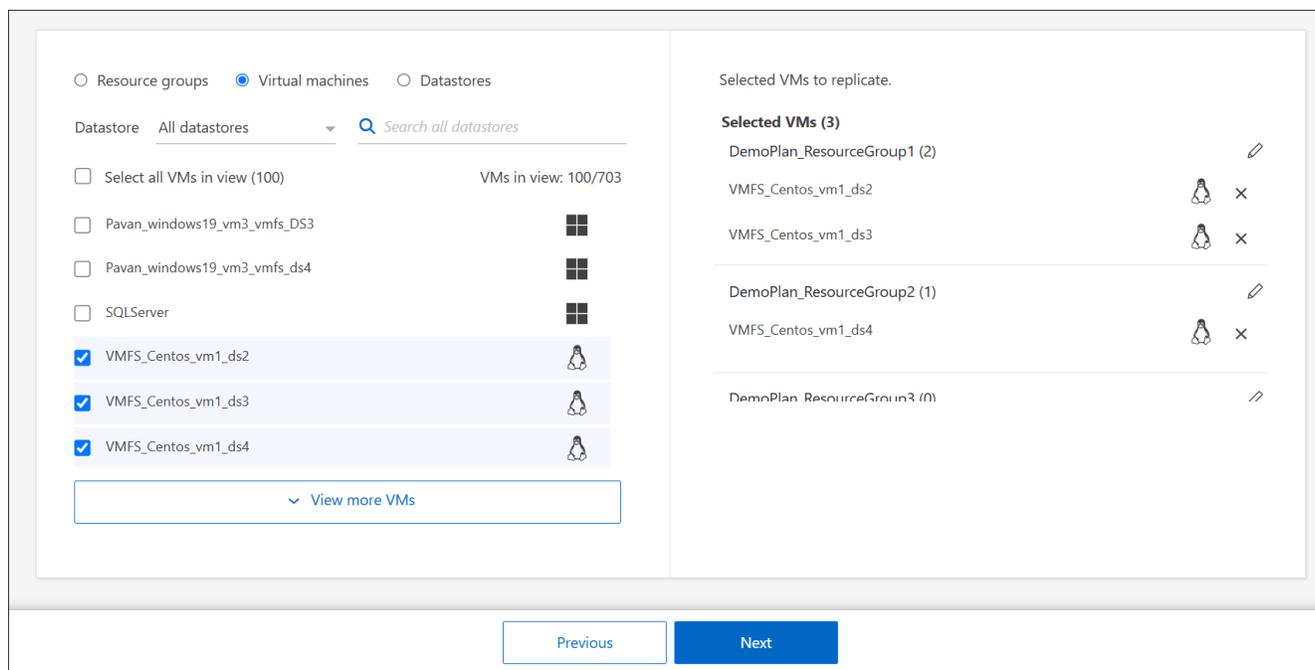
- Étant donné que la reprise d'activité BlueXP utilise SnapMirror et que le système réplique des volumes ONTAP entiers, la capacité utilisée de ce volume est utilisée pour gérer les licences. Dans ce cas, l'espace de volume consommé par les machines virtuelles protégées et non protégées serait inclus dans ce calcul.
 - Si le groupe de ressources et les datastores associés doivent être basculés vers le site de reprise d'activité, toutes les machines virtuelles non protégées (qui ne font pas partie du groupe de ressources mais sont hébergées sur le volume ONTAP) n'existeront plus sur le site source depuis le processus de basculement, entraînant ainsi la défaillance de machines virtuelles non protégées sur le site source. Par ailleurs, la reprise sur incident BlueXP ne démarre pas ces machines virtuelles non protégées sur le site vCenter de basculement.
- Pour que la machine virtuelle soit protégée, elle doit être incluse dans un groupe de ressources.

MEILLEURE PRATIQUE : organisez vos machines virtuelles avant de déployer la reprise sur incident BlueXP pour limiter la « prolifération des datastores ». Placez les machines virtuelles qui ont besoin d'une protection sur un sous-ensemble de datastores et placez-les sur des machines virtuelles qui ne seront pas protégées dans un sous-ensemble différent de datastores. Utilisez la protection basée sur les datastores pour vous assurer que les machines virtuelles de n'importe quel datastore donné sont protégées.

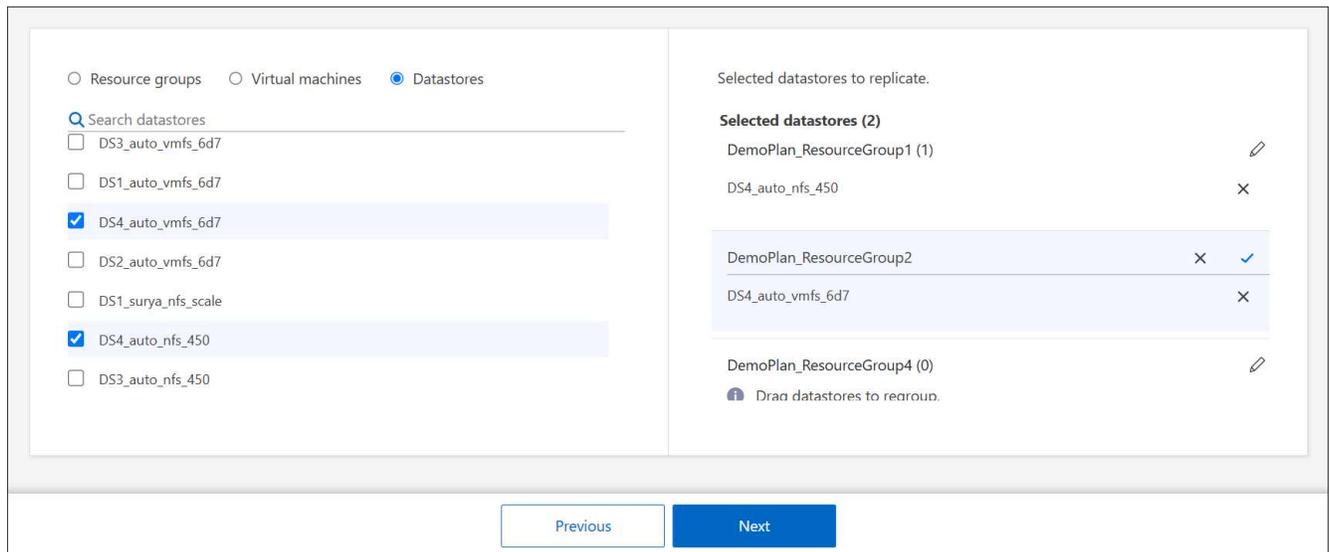
Étapes

1. Sélectionnez **machines virtuelles** ou **datastores**.
2. Vous pouvez également rechercher par nom une machine virtuelle ou un datastore spécifique.
3. Dans la partie gauche de la page applications, sélectionnez les machines virtuelles ou datastores à protéger et à affecter au groupe sélectionné.

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



Ou, pour les datastores :



4. Si vous le souhaitez, effectuez l'une des opérations suivantes :

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



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

5. Sélectionnez **Suivant**.

Mappez les ressources source à la cible

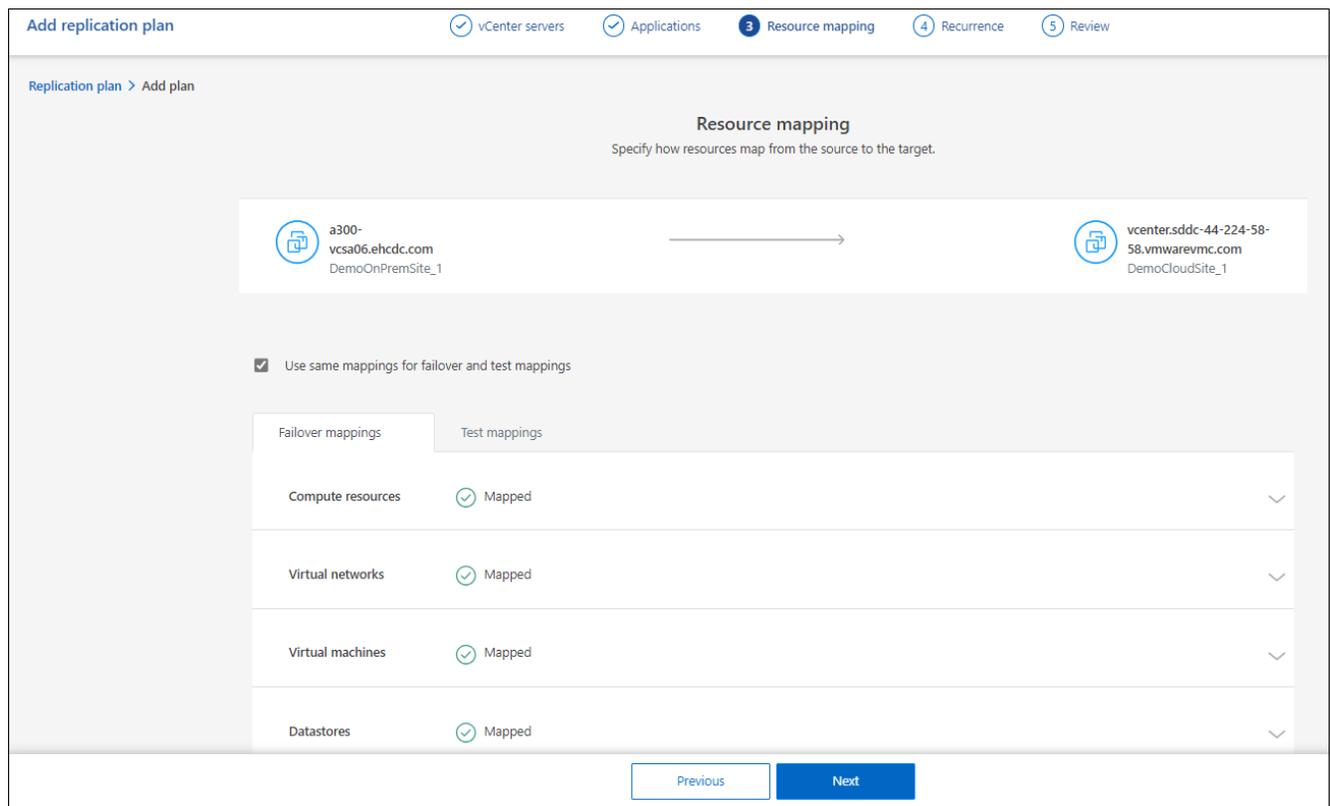
Dans l'étape mappage des ressources, spécifiez la façon dont les ressources de l'environnement source doivent être mappées sur la cible. Lorsque vous créez un plan de réplication, vous pouvez définir un délai de démarrage et un ordre pour chaque machine virtuelle du plan. Vous pouvez ainsi définir une séquence de démarrage des machines virtuelles.

Avant de commencer

Si vous souhaitez créer une relation SnapMirror dans ce service, le cluster et son peering de SVM doivent avoir déjà été configurés en dehors de la reprise d'activité BlueXP.

Étapes

1. Dans la page 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 de chacune.

Mapper les ressources > calculer les ressources

Sélectionnez la flèche vers le bas en regard de **calculer les ressources**.

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



Si un vCenter dispose d'un DRS (Distributed Resource Scheduler) configuré pour gérer plusieurs hôtes d'un cluster, vous n'avez pas besoin de sélectionner un hôte. Si vous sélectionnez un hôte, BlueXP Disaster Recovery place toutes les machines virtuelles sur l'hôte sélectionné. * **Dossier VM cible** (facultatif) : créez un nouveau dossier racine pour stocker les machines virtuelles sélectionnées.

Mapper la section ressources > réseaux virtuels

Dans l'onglet mappages de basculement, sélectionnez la flèche vers le bas en regard 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 configurés. Sélectionnez donc le réseau local virtuel approprié pour mapper la machine virtuelle.

Mapper les ressources > machines virtuelles

Dans l'onglet mappages de basculement, sélectionnez la flèche vers le bas en regard de **machines virtuelles**.

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

Si vous modifiez les paramètres par défaut, vous devez modifier le champ IP cible pour qu'il soit 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 différents champs en fonction de votre sélection.

- **Type d'adresse IP** : reconfigurez la configuration des machines virtuelles pour qu'elle corresponde aux exigences du réseau virtuel cible. La reprise sur incident BlueXP propose deux options : DHCP ou IP statique. Pour les adresses IP statiques, configurez le masque de sous-réseau, la passerelle et les serveurs DNS. De plus, entrez 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 ne fournissez que les informations d'identification de la machine virtuelle.
 - **Static IP** : 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 d'entrer les informations d'identification. En revanche, 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 la passerelle. Les informations d'identification du système d'exploitation invité de la machine virtuelle doivent être fournies au niveau global ou au niveau de chaque machine virtuelle.

Cela peut s'avérer très utile lors de la restauration d'environnements volumineux sur des clusters cibles plus petits ou lors de tests de reprise après incident sans devoir provisionner une infrastructure VMware physique individuelle.

Virtual machines

IP address type: Target IP:

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

Use the same credentials for all VMs

Use Windows LAPS *Use Windows LAPS*

Domain controller: Account name: Password:
Required

Domain:

Use the same script for all VMs

Target VM prefix: Optional Target VM suffix: Optional
Preview: Sample VM name

- Dans le champ **IP cible**, sélectionnez l'une des options suivantes :
 - **Identique à la source**
 - **Différent de la source**
 - Mappage de sous-réseau : sélectionnez cette option pour mapper le sous-réseau source à un autre sous-réseau cible. Vous pouvez sélectionner le sous-réseau source, puis le sous-réseau cible. Cette option est utile pour modifier l'adresse IP de la machine virtuelle dans l'environnement cible.



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 dans l'onglet Sites. Deuxièmement, dans le plan de réplication, indiquez que vous souhaitez utiliser le mappage de sous-réseau.



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

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

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

- **Scripts** : vous pouvez inclure des scripts personnalisés au format .sh, .bat ou .ps1 comme processus de post-basculement. Avec les scripts personnalisés, la reprise d'activité BlueXP peut 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.

- **Préfixe et suffixe de la machine virtuelle cible** : sous les détails des machines virtuelles, vous pouvez éventuellement ajouter un préfixe et un suffixe au nom de la machine virtuelle.
- **CPU et RAM de la machine virtuelle source** : sous les détails des machines virtuelles, vous pouvez éventuellement redimensionner les paramètres CPU et RAM de la machine virtuelle.

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

- **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 en parallèle ; toutefois, vous pouvez effectuer des modifications à ce stade. Ceci est utile pour vous assurer que toutes vos machines virtuelles prioritaires sont exécutées avant le démarrage des machines virtuelles prioritaires suivantes.

Toutes les machines virtuelles ayant le même numéro d'ordre de démarrage seront démarrées en parallèle.

- 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 nombre 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** : réglez le délai en minutes de l'action de démarrage.



Pour rétablir l'ordre de démarrage par défaut, sélectionnez **Réinitialiser les paramètres VM par défaut**, puis choisissez les paramètres que vous souhaitez rétablir par défaut.

- **Créer des répliques cohérentes avec l'application** : indiquer si vous devez créer des copies snapshot cohérentes avec l'application. Le service arrête l'application, puis effectue un instantané pour obtenir un état cohérent de l'application. Cette fonctionnalité est prise en charge par Oracle fonctionnant sous Windows et Linux et SQL Server sous Windows.

Mapper la section ressources > datastores

Sélectionnez la flèche vers le bas en regard de **datastores**. En fonction de la sélection des machines virtuelles, les mappages des datastores sont sélectionnés automatiquement.

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

The screenshot shows the 'Datastores' configuration interface. At the top, there is a title 'Datastores' and a back arrow. Below this, there is a section for backup and retention settings. A checkbox labeled 'Use platform managed backups and retention schedules' is checked. Below it, the 'Start running retention from' field is set to '2025-05-13' with a calendar icon, and the time is set to '12 : 00 AM'. The 'Run retention once every' field is set to '03 Hour(s) 00 Minute(s)'. The 'Retention count for all datastores' field is set to '30'. There are two sections for mapping datastores: 'Source datastore' and 'Target datastore', both showing 'DS_Testing_Staging (Temp_3510_N1:DR_Vol_Staging)'. Below these, there are two dropdown menus: 'Preferred NFS LIF' and 'Export policy', both showing 'Select preferred NFS LIF' and 'Select export policy' respectively.

- **Utiliser des sauvegardes gérées par la plateforme et des calendriers de conservation** : si vous utilisez une solution de gestion des snapshots externes, cochez cette case. BlueXP Disaster Recovery prend en charge l'utilisation de solutions externes de gestion des snapshots, telles que le planificateur de règles ONTAP SnapMirror natif ou les intégrations tierces. Si chaque datastore (volume) du plan de réplication dispose déjà d'une relation SnapMirror gérée par un autre emplacement, vous pouvez utiliser ces snapshots comme points de restauration dans la reprise d'activité BlueXP .

Lorsque cette option est sélectionnée, la reprise sur incident BlueXP ne configure pas de programme de sauvegarde. Toutefois, vous devez toujours configurer un planning de conservation, car les snapshots peuvent toujours être créés pour les opérations de test, de basculement et de restauration.

Une fois configuré, le service ne prend pas de snapshots planifiés régulièrement, mais s'appuie plutôt sur l'entité externe pour prendre et mettre à jour ces snapshots.

- **Heure de début** : saisissez la date et l'heure auxquelles vous souhaitez que les sauvegardes et la rétention commencent à s'exécuter.
- **Intervalle d'exécution** : saisissez l'intervalle de temps en heures et en minutes. Par exemple, si vous saisissez 1 heure, le service prend un instantané toutes les heures.
- **Retention count** : entrez le nombre d'instantanés que vous souhaitez conserver.
- **Datastores source et cible** : si plusieurs relations SnapMirror (fan-out) existent, vous pouvez sélectionner la destination à utiliser. Si une relation SnapMirror est déjà établie sur un volume, les datastores source et cible correspondants s'affichent. Si un volume ne possède pas de relation SnapMirror, vous pouvez en créer une en sélectionnant un cluster cible, en sélectionnant un SVM cible et en fournissant un nom de volume. Le service créera la relation volume et SnapMirror.



Si vous souhaitez créer une relation SnapMirror dans ce service, le cluster et son peering de SVM doivent avoir déjà été configurés en dehors de la reprise d'activité BlueXP.

- Si les machines virtuelles proviennent du même volume et du même SVM, le service exécute un snapshot ONTAP standard et met à jour les destinations secondaires.
- Si les machines virtuelles proviennent d'un autre volume et d'un même SVM, le service crée un snapshot de groupe de cohérence en incluant tous les volumes et met à jour les destinations secondaires.
- Si les machines virtuelles proviennent d'un autre volume et d'un autre SVM, le service exécute une phase de démarrage du groupe de cohérence et un Snapshot de phase de validation en incluant tous les volumes du même cluster ou d'un autre cluster, et met à jour les destinations secondaires.
- Pendant le basculement, vous pouvez sélectionner n'importe quel snapshot. Si vous sélectionnez le dernier snapshot, le service crée une sauvegarde à la demande, met à jour la destination et utilise ce snapshot pour le basculement.

Ajoutez des mappages de basculement de test

Étapes

1. Pour définir différents mappages pour l'environnement de test, décochez la case et sélectionnez l'onglet **Tester les mappages**.
2. Passez en revue chaque onglet comme précédemment, mais cette fois pour l'environnement de test.

Dans l'onglet Tester les mappages, les mappages des ordinateurs virtuels et des datastores sont désactivés.



Vous pouvez tester ultérieurement l'intégralité du plan. Vous configurez actuellement les mappages pour l'environnement de test.

Vérifiez le plan de réplication

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



Vous pouvez par la suite désactiver ou supprimer le plan de réplication.

Étapes

1. Consultez les informations de chaque onglet : Détails du plan, mappage du basculement sur incident et machines virtuelles.
2. Sélectionnez **Ajouter un plan**.

Le plan est ajouté à la liste des plans.

Modifiez les plannings pour tester la conformité et vous assurer que les tests de basculement fonctionnent

Il peut être utile de définir des plannings pour tester les tests de conformité et de basculement afin de vous assurer 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 programme de conformité par défaut. Le temps de conformité par défaut est de 30 minutes. Pour modifier cette heure, vous pouvez utiliser l'option modifier la planification dans le plan de réplication.
- **Impact du basculement de test** : vous pouvez tester un processus de basculement à la demande ou selon un planning. Cela vous permet de tester le basculement des machines virtuelles vers une destination

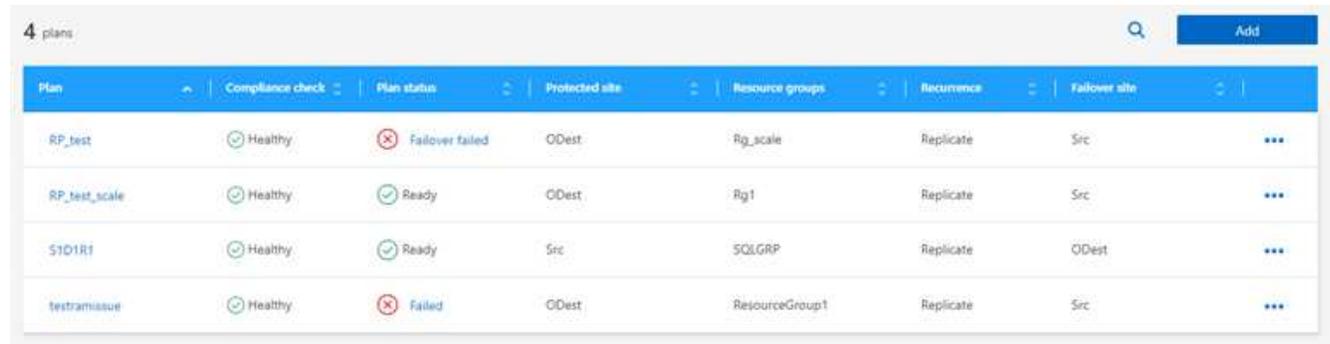
spécifiée dans un plan de réplication.

Un basculement de test crée un volume FlexClone, monte le datastore et déplace la charge de travail sur ce datastore. Un 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 de la planification, le test de basculement s'exécute et s'assure que les charges de travail sont déplacées vers la destination spécifiée par le plan de réplication.

Étapes

1. Dans le menu supérieur de reprise d'activité BlueXP, sélectionnez **plans de réplication**.



Plan	Compliance check	Plan status	Protected site	Resource groups	Recurrence	Failover site	
RP_test	Healthy	Failover failed	ODest	Rg_scale	Replicate	Src	...
RP_test_scale	Healthy	Ready	ODest	Rg1	Replicate	Src	...
S1D1R1	Healthy	Ready	Src	SQLGRP	Replicate	ODest	...
testramisue	Healthy	Failed	ODest	ResourceGroup1	Replicate	Src	...

2. Sélectionnez **actions** **...** Et sélectionnez **Modifier les horaires**.
3. Indiquez la fréquence en minutes à laquelle vous souhaitez que la reprise d'activité BlueXP vérifie la conformité des tests.
4. Pour vérifier que vos tests de basculement sont en bon état, cochez **Exécuter les basculements selon un planning mensuel**.
 - a. Sélectionnez le jour du mois et l'heure d'exécution de ces tests.
 - b. Saisissez la date au format `aaaa-mm-jj` lorsque vous souhaitez que le test commence.

Edit schedules: RP_DRAAS

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

Compliance check

Frequency (min) ⓘ

Test failover

Run test failovers on a schedule ⓘ

Use on-demand snapshot for scheduled test failover ⓘ

Repeat

Hour : Minute AM/PM Start date ⓘ
 :

Automatically cleanup minutes after test failover ⓘ

5. **Utiliser l'instantanéé ondemand pour le basculement de test planifié** : cochez cette case pour prendre un nouvel instantanéé avant de lancer le basculement de test automatisé.
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 démarrage du nettoyage.



Ce processus annule l'enregistrement des machines virtuelles temporaires à partir de l'emplacement de test, supprime le volume FlexClone créé et démonte les datastores temporaires.

7. Sélectionnez **Enregistrer**.

Répliquer des applications vers un autre site avec la récupération après sinistre BlueXP

Avec la reprise d'activité BlueXP, vous pouvez répliquer les applications VMware sur votre site source vers un site distant de reprise d'activité dans le cloud à l'aide de la réplication SnapMirror.

Rôle BlueXP 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 la BlueXP disaster recovery"](#). ["En savoir plus sur les rôles d'accès BlueXP pour tous les services"](#).



Une fois le plan de reprise d'activité créé, identifiez la récurrence dans l'assistant et lancez une réplication vers un site de reprise d'activité, la reprise d'activité BlueXP vérifie toutes les 30 minutes que la réplication se produit réellement conformément au plan. Vous pouvez surveiller la progression dans la page moniteur des tâches.

Avant de commencer

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

Étapes

1. Dans le menu de navigation gauche de BlueXP, sélectionnez **protection > reprise après sinistre**.
2. Dans le menu supérieur, sélectionnez **plans de réplication**.
3. Sélectionnez le plan de réplication.
4. Sur la droite, sélectionnez l'option **actions**  Et sélectionnez **répliquer**.

Migrer des applications vers un autre site avec la récupération après sinistre BlueXP

En utilisant la reprise d'activité BlueXP, vous pouvez migrer les applications VMware de votre site source vers un autre site.



Après avoir créé le plan de réplication, identifiez la récurrence dans l'assistant et lancez la migration, la reprise d'activité BlueXP vérifie toutes les 30 minutes que la migration a effectivement lieu conformément au plan. Vous pouvez surveiller la progression dans la page moniteur des tâches.

Avant de commencer

Avant de lancer la migration, vous devez avoir créé un plan de réplication et choisi de migrer les applications. L'option **migrer** apparaît alors dans le menu actions.

Étapes

1. Dans le menu de navigation gauche de BlueXP, sélectionnez **protection > reprise après sinistre**.
2. Dans le menu supérieur, sélectionnez **plans de réplication**.
3. Sélectionnez le plan de réplication.
4. Sur la droite, sélectionnez l'option **actions**  Et sélectionnez **migrer**.

Basculer les applications vers un site distant avec la récupération après sinistre BlueXP

En cas d'incident, basculez votre site VMware primaire sur site vers un autre site VMware sur site ou VMware Cloud sur AWS. Vous pouvez tester le processus de basculement

pour vous assurer qu'il est efficace au moment où vous en avez besoin.

Rôle BlueXP 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 la BlueXP disaster recovery"](#). ["En savoir plus sur les rôles d'accès BlueXP pour tous les services"](#).

Lors d'un basculement, la copie Snapshot SnapMirror la plus récente est utilisée. Vous pouvez également sélectionner un snapshot spécifique à partir d'un snapshot instantané (conformément à la règle de conservation de SnapMirror). L'option instantanée peut être utile si vous êtes confronté à une corruption, telle qu'une attaque par ransomware, où les répliques les plus récentes sont déjà compromises ou chiffrées. La reprise d'activité BlueXP affiche tous les points disponibles dans le temps.

Ce processus diffère selon que le site de production fonctionne correctement et que vous effectuez un basculement vers le site de reprise d'activité pour des raisons autres qu'une défaillance critique de l'infrastructure :

- Défaillance critique du site de production lorsque le cluster vCenter ou ONTAP source n'est pas accessible : la reprise d'activité BlueXP vous permet de sélectionner les snapshots disponibles à partir desquels effectuer la restauration.
- L'environnement de production est sain : vous pouvez « prendre un snapshot maintenant » ou sélectionner un snapshot créé précédemment.

Cette procédure rompt la relation de réplication, met hors ligne les machines virtuelles source vCenter, enregistre les volumes en tant que datastores dans le vCenter de reprise après incident, redémarre les machines virtuelles protégées à l'aide des règles de basculement du plan et active la lecture/l'écriture sur le site cible.

Tester le processus de basculement

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

Lors d'un test de basculement, les machines virtuelles sont créées temporairement. La reprise d'activité BlueXP ne mappe pas le volume cible. Elle crée un nouveau volume FlexClone à partir de l'instantané sélectionné et un datastore temporaire sur lequel le volume FlexClone est pris en compte est mappé sur les hôtes ESXi.

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

Lorsque vous avez terminé le test, vous devez réinitialiser les machines virtuelles avec l'option **Clean up test**. Bien que cela soit recommandé, il n'est pas nécessaire.

Un 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.

Étapes

1. Dans le menu de navigation gauche de BlueXP, sélectionnez **protection > reprise après sinistre**.
2. Dans le menu supérieur de reprise d'activité BlueXP, sélectionnez **plans de réplication**.
3. Sélectionnez le plan de réplication.

4. Sur la droite, sélectionnez l'option **actions**  Et sélectionnez **Test failover**.
5. Sur la page Test failover, entrez "Test failover" et sélectionnez **Test fail over**.
6. Une fois le test terminé, nettoyez l'environnement de test.

Nettoyez l'environnement de test après un test de basculement

Une fois le test de basculement terminé, nettoyez l'environnement de test. Ce processus supprime les VM temporaires de l'emplacement de test, les FlexClones et les datastores temporaires.

Étapes

1. Dans le menu supérieur de reprise d'activité BlueXP, sélectionnez **plans de réplication**.
2. Sélectionnez le plan de réplication.
3. Sur la droite, sélectionnez l'option **actions**  Et sélectionnez **Clean up failover test**.
4. Dans la page Test failover, entrez "Clean up failover" et sélectionnez **Clean up failover test**.

Basculez le site source vers un site de reprise après incident

En cas d'incident, basculez votre site VMware primaire sur site à la demande 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 :

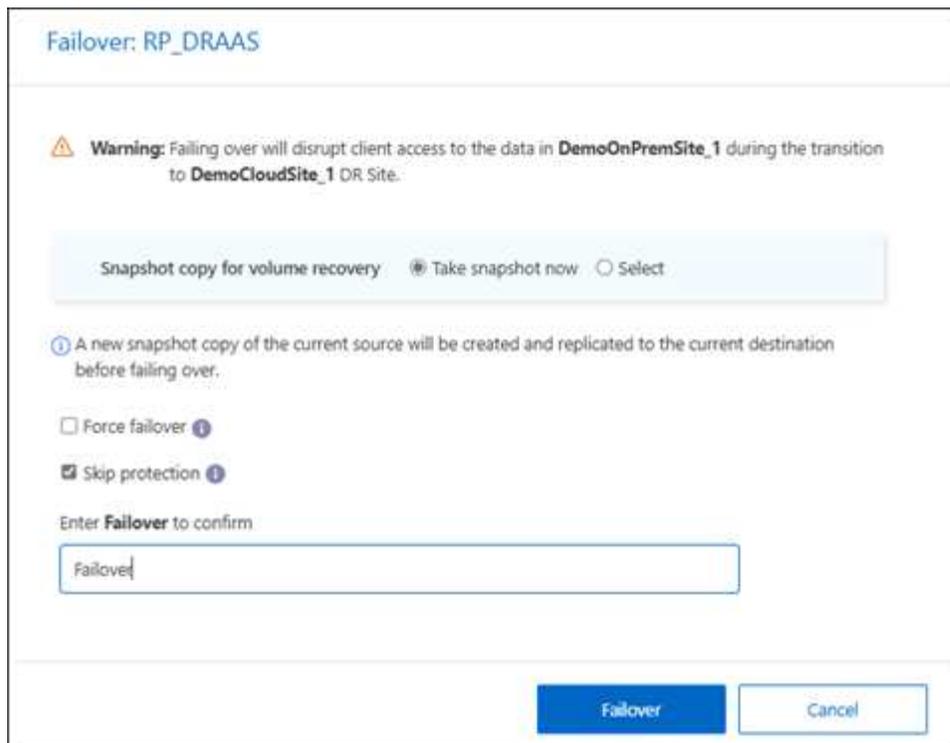
- Si vous avez sélectionné le dernier snapshot, la mise à jour SnapMirror est effectuée pour répliquer les dernières modifications.
- Les machines virtuelles source sont hors tension.
- La relation SnapMirror est rompue et le volume cible est réalisé en lecture/écriture.
- En fonction de la sélection du snapshot, le système de fichiers actif est restauré sur le snapshot spécifié (dernier ou sélectionné)
- Les datastores sont créés et montés sur le cluster ou l'hôte VMware ou VMC en fonction des informations capturées dans le plan de réplication.
- Les machines virtuelles cibles sont enregistrées et sous tension en fonction de l'ordre saisi dans la page groupes de ressources.
- La relation SnapMirror est inversée entre la machine virtuelle cible et la machine virtuelle source.



Une fois le basculement lancé, les VM restaurées sont visibles dans le vCenter du site de reprise d'activité (machines virtuelles, réseaux et datastores). Par défaut, les machines virtuelles sont restaurées dans le dossier charge de travail.

Étapes

1. Dans le menu de navigation gauche de BlueXP, sélectionnez **protection > reprise après sinistre**.
2. Dans le menu supérieur de reprise d'activité BlueXP, sélectionnez **plans de réplication**.
3. Sélectionnez le plan de réplication.
4. Sur la droite, sélectionnez l'option **actions**  Et sélectionnez **basculement**.



5. Dans la page basculement, vous pouvez soit lancer un instantané maintenant, soit choisir l'instantané du datastore à partir duquel effectuer la restauration. La valeur par défaut est la dernière.

Un instantané de la source actuelle est pris et répliqué vers la destination actuelle avant le basculement.

6. Vous pouvez également sélectionner **forcer le basculement** si vous souhaitez que le basculement se produise même si une erreur est détectée, ce qui empêcherait normalement le basculement.
7. Si vous le souhaitez, sélectionnez **Ignorer la protection** si vous souhaitez que le service ne crée pas automatiquement une relation de protection SnapMirror inverse après un basculement de plan de réplication. Cette fonction est utile si vous souhaitez effectuer des opérations supplémentaires sur le site restauré avant de le remettre en ligne dans le cadre de la reprise sur incident BlueXP .



Vous pouvez établir une protection inverse en sélectionnant **protéger les ressources** dans le menu actions du plan de réplication. Cette opération tente de créer une relation de réplication inverse pour chaque volume du plan. Vous pouvez exécuter cette tâche plusieurs fois jusqu'à ce que la protection soit restaurée. Une fois la protection restaurée, vous pouvez lancer un rétablissement de la manière habituelle.

8. Saisissez « basculement » dans la zone.
9. Sélectionnez **basculement**.
10. Pour vérifier la progression, dans le menu supérieur, sélectionnez **surveillance des travaux**.

Restaurez les applications à leur source d'origine avec la récupération après sinistre BlueXP

Une fois l'incident résolu, rebasculez le système du site de reprise sur incident vers le site source pour rétablir les opérations normales. Vous pouvez sélectionner l'instantané à partir duquel effectuer la restauration.

Rôle BlueXP 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 la BlueXP disaster recovery"](#). ["En savoir plus sur les rôles d'accès BlueXP pour tous les services"](#).

Dans ce workflow, BlueXP Disaster Recovery réplique (resyncs) toutes les modifications apportées à la machine virtuelle source d'origine avant d'inverser le sens de la réplication. Ce processus commence à partir d'une relation qui a terminé le basculement vers une cible et implique les étapes suivantes :

- Sur le site cible, les machines virtuelles sont hors tension et non enregistrées, et les volumes sont démontés.
- La relation SnapMirror sur la source d'origine est rompue pour la lecture/l'écriture.
- La relation SnapMirror est resynchronisée pour inverser la réplication.
- Les machines virtuelles source sont sous tension et enregistrées, et les volumes sont montés sur la source.

Étapes

1. Dans le menu de navigation gauche de BlueXP, sélectionnez **protection > reprise après sinistre**.
2. Dans le menu supérieur de reprise d'activité BlueXP, sélectionnez **plans de réplication**.
3. Sélectionnez le plan de réplication.
4. Sur la droite, sélectionnez l'option **actions**  Et sélectionnez **Retour arrière**.
5. Entrez le nom du plan de réplication pour confirmer et démarrer le retour arrière.
6. Choisissez le snapshot du datastore à partir duquel effectuer la restauration. La valeur par défaut est la dernière.
7. Pour vérifier la progression, dans le menu supérieur, sélectionnez **surveillance des travaux**.

Gérez les sites, les groupes de ressources, les plans de réplication, les banques de données et les informations des machines virtuelles avec la reprise après sinistre BlueXP

Vous pouvez obtenir un aperçu rapide de toutes vos ressources de récupération après sinistre BlueXP ou examiner chacune d'elles en détail :

- Sites
- Groupes de ressources
- Plans de réplication
- Datastore
- Ordinateurs virtuels

Les tâches nécessitent différents rôles BlueXP . Pour plus de détails, consultez la section « Rôle BlueXP requis » de chaque tâche.

["En savoir plus sur les rôles et les autorisations des utilisateurs dans la BlueXP disaster recovery"](#). ["En savoir plus sur les rôles d'accès BlueXP pour tous les services"](#).

Gestion des sites vCenter

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

Rôle BlueXP 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 supérieur, 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

Bien que vous puissiez ajouter un groupe de ressources dans le cadre de la création d'un plan de réplication, il peut être plus pratique d'ajouter les groupes séparément et d'utiliser ces groupes ultérieurement dans le plan. Vous créez des groupes de ressources par machines virtuelles ou par datastores.

Rôle BlueXP requis Rôle d'administrateur d'organisation, d'administrateur de dossier ou de projet, d'administrateur de récupération après sinistre ou d'administrateur d'application de récupération après sinistre.

Vous pouvez créer un groupe de ressources par datastores de l'une des manières suivantes :

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

Vous pouvez également modifier et supprimer des groupes de ressources.

Étapes

1. Dans le menu supérieur, sélectionnez **groupes de ressources**.
2. Pour ajouter un groupe de ressources, sélectionnez **Ajouter un groupe**.
3. Pour effectuer des actions avec le groupe de ressources, sélectionnez l'option **actions**  À droite et sélectionnez l'une des options, telles que **Modifier le groupe de ressources** ou **Supprimer le groupe de ressources**.

Gérer les plans de réplication

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

Rôle BlueXP requis Administrateur d'organisation, administrateur de dossier ou de projet, administrateur de récupération après sinistre, administrateur de basculement de récupération après sinistre ou administrateur d'application de récupération après sinistre.

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

Étapes

1. Dans le menu supérieur, sélectionnez **plans de réplication**.

Plan	Compliance check	Plan status	Protected site	Resource groups	Recurrence	Failover site	
Customer1	Healthy	Ready	ScaleOnPremSrc	Cust1RG	Replicate	ScaleFsXDest	...
Customer2	Healthy	Ready	ScaleOnPremSrc	Cust2RG	Replicate	ScaleFsXDest	...
Customer3	Healthy	Ready	ScaleOnPremSrc	Cust3RG	Replicate	ScaleFsXDest	...
Customer4	Healthy	Ready	ScaleOnPremSrc	Cust4RG	Replicate	ScaleFsXDest	...
Customer5	Healthy	Ready	ScaleOnPremSrc	Cust5RG	Replicate	ScaleFsXDest	...

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 en haut 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 plannings**, **Tester le basculement**, **basculement**, **Retour**, **migrer**, **prendre instantané**, **nettoyer les anciens snapshots**, **Désactiver**, **Activer**, **Supprimer** ou **Supprimer**.

6. Pour définir ou modifier un planning 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 planifications**.

- Dans la page Modifier les planifications, entrez la fréquence en minutes à laquelle vous souhaitez que la vérification de conformité du basculement se produise.
- Vérifier **Exécuter les basculements de test sur un planning**.
- Dans l'option répéter, sélectionnez l'horaire quotidien, hebdomadaire ou mensuel.
- Sélectionnez **Enregistrer**.

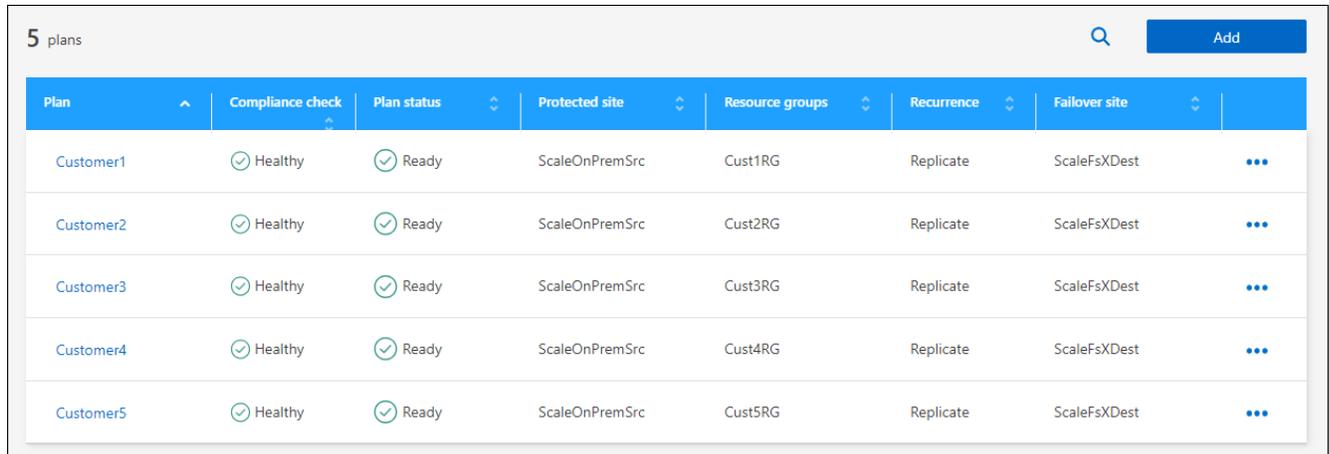
Réconcilier les snapshots à la demande

Vous pouvez réconcilier les instantanés qui sont désynchronisés entre la source et la cible. Cela peut se produire si des snapshots sont supprimés sur une cible en dehors de la reprise sur incident BlueXP . Le service supprime automatiquement le snapshot sur la source toutes les 24 heures. Cependant, vous pouvez effectuer cette opération à la demande. Cette fonction vous permet de vous assurer que les snapshots sont cohérents sur tous les sites.

Rôle BlueXP requis Administrateur d'organisation, administrateur de dossier ou de projet, administrateur de récupération après sinistre, administrateur de basculement de récupération après sinistre ou administrateur d'application de récupération après sinistre.

Étapes

1. Dans le menu supérieur, sélectionnez **plans de réplication**.



Plan	Compliance check	Plan status	Protected site	Resource groups	Recurrence	Failover site	
Customer1	Healthy	Ready	ScaleOnPremSrc	Cust1RG	Replicate	ScaleFsXDest	...
Customer2	Healthy	Ready	ScaleOnPremSrc	Cust2RG	Replicate	ScaleFsXDest	...
Customer3	Healthy	Ready	ScaleOnPremSrc	Cust3RG	Replicate	ScaleFsXDest	...
Customer4	Healthy	Ready	ScaleOnPremSrc	Cust4RG	Replicate	ScaleFsXDest	...
Customer5	Healthy	Ready	ScaleOnPremSrc	Cust5RG	Replicate	ScaleFsXDest	...

2. Dans la liste des plans de réplication, sélectionnez l'option **actions** ... à droite du plan et sélectionnez **réconcilier instantanés**.
3. Passez en revue les informations de rapprochement.
4. Sélectionnez **Synchroniser**.

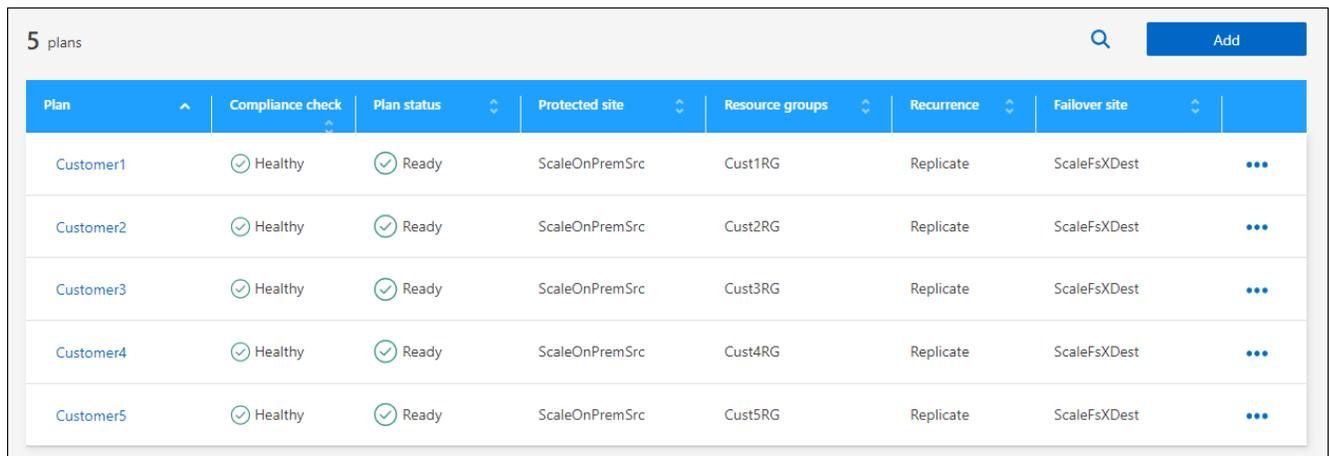
Supprimer un plan de réplication

Vous pouvez supprimer un plan de réplication si vous n'en avez plus besoin. Si vous supprimez un plan de réplication, vous pouvez également supprimer les instantanés principal et secondaire créés par le plan.

Rôle BlueXP requis Administrateur d'organisation, administrateur de dossier ou de projet, administrateur de récupération après sinistre, administrateur de basculement de récupération après sinistre ou administrateur d'application de récupération après sinistre.

Étapes

1. Dans le menu supérieur, sélectionnez **plans de réplication**.



Plan	Compliance check	Plan status	Protected site	Resource groups	Recurrence	Failover site	
Customer1	Healthy	Ready	ScaleOnPremSrc	Cust1RG	Replicate	ScaleFsXDest	...
Customer2	Healthy	Ready	ScaleOnPremSrc	Cust2RG	Replicate	ScaleFsXDest	...
Customer3	Healthy	Ready	ScaleOnPremSrc	Cust3RG	Replicate	ScaleFsXDest	...
Customer4	Healthy	Ready	ScaleOnPremSrc	Cust4RG	Replicate	ScaleFsXDest	...
Customer5	Healthy	Ready	ScaleOnPremSrc	Cust5RG	Replicate	ScaleFsXDest	...

2. Sélectionnez l'option **actions** ... à droite du plan et sélectionnez **Supprimer**.
3. Indiquez si vous souhaitez supprimer les snapshots primaires, secondaires ou uniquement les métadonnées créées par le plan.

4. Tapez « DELETE » pour confirmer la suppression.
5. Sélectionnez **Supprimer**.

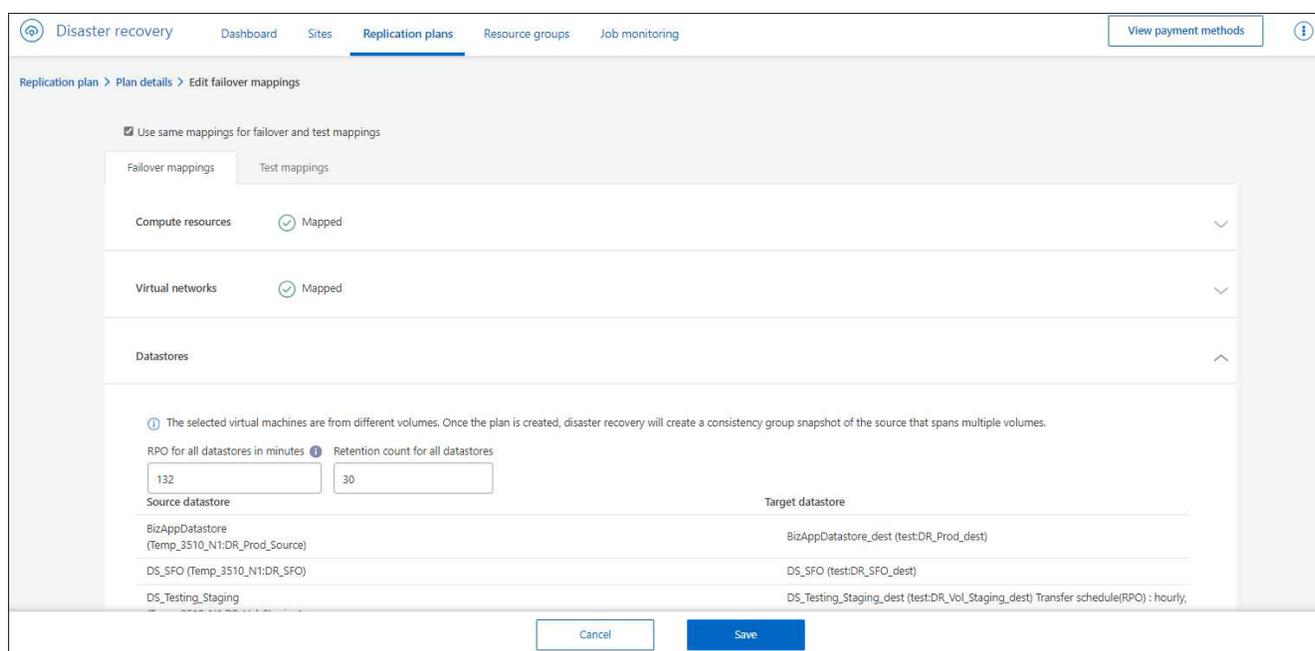
Modifier le nombre de rétention pour les planifications de basculement

Vous pouvez modifier le nombre de datastores conservés.

Rôle BlueXP requis Administrateur d'organisation, administrateur de dossier ou de projet, administrateur de récupération après sinistre, administrateur de basculement de récupération après sinistre ou administrateur d'application de récupération après sinistre.

Étapes

1. Dans le menu supérieur, sélectionnez **plans de réplication**.
2. Sélectionnez le plan de réplication, cliquez sur l'onglet **mappage de basculement**, puis cliquez sur l'icône crayon **Modifier**.
3. Cliquez sur la flèche **datastores** pour la développer.



4. Modifiez la valeur du nombre de rétention dans le plan de réplication.
5. Une fois le plan de réplication sélectionné, sélectionnez le menu actions, 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 datastores

Vous pouvez afficher des informations sur le nombre de datastores présents sur la source et sur la cible.

Rôle BlueXP requis Administrateur d'organisation, administrateur de dossier ou de projet, administrateur de récupération après sinistre, administrateur de basculement de récupération après sinistre, administrateur d'application de récupération après sinistre ou rôle de visualiseur de récupération après sinistre.

Étapes

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

2. Sélectionnez le vCenter dans la ligne site.
3. Sélectionnez **datastores**.
4. Afficher les informations sur les datastores.

Afficher les informations sur les machines virtuelles

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

Rôle BlueXP requis Administrateur d'organisation, administrateur de dossier ou de projet, administrateur de récupération après sinistre, administrateur de basculement de récupération après sinistre, administrateur d'application de récupération après sinistre ou rôle de visualiseur de récupération après sinistre.

Étapes

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

Surveiller les tâches de récupération après sinistre BlueX

Vous pouvez surveiller toutes les tâches de récupération après sinistre BlueXP et déterminer leur progression.

Afficher les travaux

Rôle BlueXP requis Administrateur d'organisation, administrateur de dossier ou de projet, administrateur de récupération après sinistre, administrateur d'application de récupération après sinistre ou rôle de visualiseur de récupération après sinistre.

["En savoir plus sur les rôles et les autorisations des utilisateurs dans la BlueXP disaster recovery"](#). ["En savoir plus sur les rôles d'accès BlueXP pour tous les services"](#).

Étapes

1. Dans le menu de navigation gauche de BlueXP, sélectionnez **protection > reprise après sinistre**.
2. Dans le menu supérieur, sélectionnez **surveillance des travaux**.
3. Explorez tous les travaux liés aux opérations et vérifiez leurs horodatages et leur état.
4. Pour afficher les détails d'un travail particulier, sélectionnez cette ligne.
5. Pour actualiser les informations, sélectionnez **Actualiser**.

Annuler un travail

Si un travail est en cours ou en file d'attente et que vous ne souhaitez pas qu'il continue, vous pouvez l'annuler. Vous pouvez annuler un travail s'il est bloqué dans le même état et que vous souhaitez libérer l'opération suivante dans la file d'attente. Vous pouvez annuler un travail avant qu'il ne soit trop tard.

Rôle BlueXP requis Administrateur d'organisation, administrateur de dossier ou de projet, administrateur de récupération après sinistre, administrateur de basculement de récupération après sinistre ou administrateur

d'application de récupération après sinistre.

["En savoir plus sur les rôles et les autorisations des utilisateurs dans la BlueXP disaster recovery"](#). ["En savoir plus sur les rôles d'accès BlueXP pour tous les services"](#).

Étapes

1. Dans le menu de navigation gauche de BlueXP, sélectionnez **protection > reprise après sinistre**.
2. Dans le menu supérieur, sélectionnez **surveillance des travaux**.
3. Sur la page moniteur de travaux, notez l'ID du travail que vous souhaitez annuler.

Le travail doit être à l'état « en cours » ou « en file d'attente ».

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

Créer des rapports de reprise après sinistre BlueXP

L'examen des rapports de reprise après sinistre BlueXP peut vous aider à analyser votre état de préparation à la reprise après sinistre. Les rapports préconçus incluent un récapitulatif 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 Télécharger est valide pendant six heures.

Étapes

1. Dans la navigation de gauche de BlueXP, sélectionnez **protection > récupération après sinistre > plans de réplication**.
2. En haut de la page, sélectionnez **Créer un rapport**.
3. Sélectionnez le type de format de fichier et la période comprise dans les 7 derniers jours.
4. Sélectionnez **Créer**.



L'affichage du rapport peut prendre quelques minutes.

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

Référence

Privilèges vCenter requis pour la reprise d'activité BlueXP

Le compte vCenter doit disposer d'un ensemble minimal de privilèges vCenter pour permettre à BlueXP Disaster Recovery d'exécuter ses services, tels que l'enregistrement et le désenregistrement des datastores, le démarrage et l'arrêt des machines virtuelles et la reconfiguration des machines virtuelles (VM). Le tableau suivant répertorie tous les privilèges requis pour l'interface de la reprise après incident BlueXP avec un cluster vCenter.

Type	Nom de privilège	Description
Datastore	Datastore. Configurer le datastore	Permet de configurer un datastore.
	Datastore. Supprimer le datastore	Utilisez pour supprimer un datastore.
Machine virtuelle	Machine virtuelle.Configuration.Modifier les paramètres	Permet de modifier les paramètres généraux de la machine virtuelle.
	Machine virtuelle.Configuration.Modifier les paramètres du périphérique	Permet de modifier les propriétés d'un périphérique existant.
	Machine virtuelle.Configuration.recharger à partir du chemin	Permet de modifier un correctif de configuration de machine virtuelle tout en préservant l'identité de la machine virtuelle. Des solutions telles que VMware vCenter Site Recovery Manager permettent de gérer l'identification des machines virtuelles lors du basculement et du retour arrière.
	Machine virtuelle.Configuration.Renommer	Permet de renommer une machine virtuelle ou de modifier les nœuds associés d'une machine virtuelle.
	Machine virtuelle.Configuration.Réinitialiser les informations sur l'invité	Permet de modifier les informations du système d'exploitation invité d'une machine virtuelle.
	Machine virtuelle.Configuration.Modifier la mémoire	Permet de modifier la quantité de mémoire allouée à la machine virtuelle.

Type	Nom de privilège	Description
	Machine virtuelle.Configuration.Modifier le nombre de CPU	Permet de modifier le nombre de processeurs virtuels.
Invité de machine virtuelle	Machine virtuelle. Opérations clients. Modifications apportées à l'opération client	Permet les opérations des invités de machine virtuelle qui impliquent des modifications du système d'exploitation invité d'une machine virtuelle, telles que le transfert d'un fichier vers cette dernière.
Interaction de la machine virtuelle	Machine virtuelle.interaction.mise hors tension	Permet de mettre hors tension une machine virtuelle sous tension. Cette opération met le système d'exploitation invité hors tension.
	Machine virtuelle.interaction.mise sous tension	Permet de mettre sous tension une machine virtuelle hors tension et de reprendre une machine virtuelle suspendue.
	Machine virtuelle.interaction.installation de VMware Tools	Utilisez pour monter et démonter le CD d'installation de VMware Tools en tant que CD-ROM du système d'exploitation invité.
Inventaire des machines virtuelles	Machine virtuelle.Inventaire.Créer nouveau	Permet de créer une machine virtuelle et d'allouer des ressources pour son exécution.
	Machine virtuelle.Inventory.Register	Permet d'ajouter une machine virtuelle existante à un serveur vCenter ou à un inventaire d'hôtes.
	Machine virtuelle.Inventaire.désenregistrer	Utilisez pour annuler l'enregistrement d'une machine virtuelle à partir d'un serveur vCenter ou d'un inventaire d'hôtes.
Etat de la machine virtuelle	Machine virtuelle. Gestion des snapshots. Créer un Snapshot	Permet de créer un snapshot à partir de l'état actuel de la machine virtuelle.
	Machine virtuelle. Gestion des snapshots. Supprimer l'instantané	Permet de supprimer un instantané de l'historique des instantanés.
	Machine virtuelle. Gestion des snapshots. Revenir au snapshot	Utiliser pour définir la machine virtuelle à l'état dans lequel elle se trouvait au niveau d'un snapshot donné.

Accès aux fonctionnalités de BlueXP disaster recovery basé sur les rôles

La BlueXP disaster recovery utilise 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 la BlueXP disaster recovery.

- **Administrateur de récupération après sinistre** : effectuez toutes les actions dans la BlueXP disaster recovery.
- **Administrateur de basculement de reprise après sinistre** : effectuez des actions de basculement et de migration dans la BlueXP 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 la BlueXP disaster recovery, mais ne pouvez effectuer aucune action.

Ces rôles sont spécifiques à la BlueXP disaster recovery et ne sont pas les mêmes que les rôles de plate-forme utilisés dans BlueXP. Pour plus de détails sur tous les rôles de plate-forme BlueXP, voir "[Documentation d'installation et d'administration de BlueXP](#)".

Le tableau suivant indique les actions que chaque rôle de BlueXP disaster recovery peut effectuer.

Fonction et action	Administrateur de reprise après sinistre	Administrateur de basculement de reprise après sinistre	Administrateur d'application de reprise après sinistre	Visionneuse de reprise après sinistre
Afficher le tableau de bord et tous les onglets	Oui	Oui	Oui	Oui
Essayer gratuitement	Oui	Non	Non	Non
Lancez la découverte des charges de travail	Oui	Non	Non	Non
Afficher les informations de licence	Oui	Oui	Oui	Oui
Activer la licence	Oui	Non	Oui	Non
Dans l'onglet Sites :				
Voir les sites	Oui	Oui	Oui	Oui
Ajouter, modifier ou supprimer des sites	Oui	Non	Non	Non
Dans l'onglet Plans de réplication :				
Afficher les plans de réplication	Oui	Oui	Oui	Oui

Fonction et action	Administrateur de reprise après sinistre	Administrateur de basculement de reprise après sinistre	Administrateur d'application de reprise après sinistre	Visionneuse de reprise après sinistre
Afficher les détails du plan de réplication	Oui	Oui	Oui	Oui
Créer ou modifier des plans de réplication	Oui	Oui	Oui	Non
Créer des rapports	Oui	Non	Non	Non
Voir les instantanés	Oui	Oui	Oui	Oui
Effectuer des tests de basculement	Oui	Oui	Oui	Non
Effectuer des basculements	Oui	Oui	Non	Non
Effectuer des restaurations automatiques	Oui	Oui	Non	Non
Effectuer des migrations	Oui	Oui	Non	Non
Dans l'onglet Groupes de ressources :				
Afficher les groupes de ressources	Oui	Oui	Oui	Oui
Créer, modifier ou supprimer des groupes de ressources	Oui	Non	Oui	Non
Dans l'onglet Suivi des tâches :				
Afficher les travaux	Oui	Non	Oui	Oui
Annuler les emplois	Oui	Oui	Oui	Non

Utiliser la reprise après sinistre BlueXP avec Amazon EVS

Introduction à la reprise après sinistre BlueXP à l'aide d'Amazon Elastic VMware Service et d'Amazon FSx pour NetApp ONTAP

Les clients dépendent de plus en plus des infrastructures virtualisées pour leurs charges de travail de production, comme celles basées sur VMware vSphere. Ces machines virtuelles (VM) étant devenues plus critiques pour leurs entreprises, les clients doivent les protéger des mêmes types de sinistres que leurs ressources de calcul physiques. Les solutions de reprise après sinistre (DR) actuellement proposées sont complexes, coûteuses et gourmandes en ressources. NetApp, principal fournisseur de stockage pour les infrastructures virtualisées, a tout intérêt à garantir la protection des VM de ses clients, de la même manière que nous protégeons les données hébergées sur le

stockage ONTAP, quel que soit leur type. Pour atteindre cet objectif, NetApp a créé le service de reprise après sinistre BlueXP.



CETTE DOCUMENTATION CONCERNANT AMAZON EVS EST FOURNIE À TITRE D'APERÇU TECHNOLOGIQUE. Avec cette offre de présentation, NetApp se réserve le droit de modifier les détails, le contenu et le calendrier de l'offre avant la disponibilité générale.

L'un des principaux défis de toute solution de reprise après sinistre est la gestion des coûts supplémentaires liés à l'achat, à la configuration et à la maintenance de ressources de calcul, de réseau et de stockage supplémentaires, nécessaires à la mise en place d'une infrastructure de réplication et de reprise après sinistre. Une option courante pour protéger les ressources virtuelles critiques sur site consiste à utiliser des ressources virtuelles hébergées dans le cloud comme infrastructure de réplication et de reprise après sinistre. Amazon est un exemple de solution offrant des ressources économiques et compatibles avec les infrastructures de machines virtuelles hébergées NetApp ONTAP.

Amazon a lancé Amazon Elastic VMware Service (Amazon EVS), qui permet d'intégrer VMware Cloud Foundation à votre cloud privé virtuel (VPC). Amazon EVS offre la résilience et les performances d'AWS, ainsi que les logiciels et outils VMware habituels, permettant ainsi l'intégration des vCenters Amazon EVS comme extension de votre infrastructure virtualisée sur site.

Bien qu'Amazon EVS soit fourni avec des ressources de stockage incluses, l'utilisation d'un stockage natif peut réduire son efficacité pour les entreprises dont les charges de travail nécessitent un stockage important. Dans ce cas, l'association d'Amazon EVS avec Amazon FSx for NetApp ONTAP Storage (Amazon FSxN) peut offrir 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 vous permet de bénéficier d'une interopérabilité et de fonctionnalités de protection des données optimales entre vos infrastructures sur site et hébergées dans le cloud.

Pour plus d'informations sur Amazon FSX pour NetApp ONTAP, reportez-vous à la section "[Mise en route avec Amazon FSX pour NetApp ONTAP](#)".

Présentation de la solution de reprise après sinistre BlueXP utilisant Amazon EVS et Amazon FS pour NetApp ONTAP

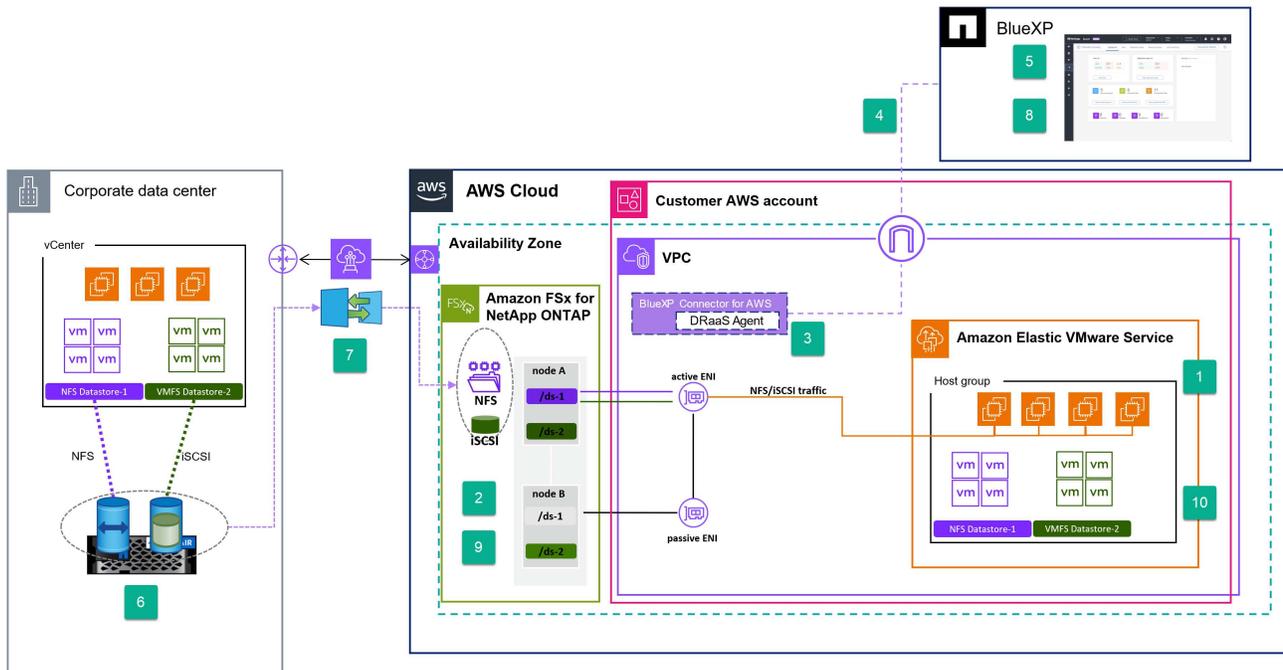
La reprise après sinistre BlueXP est un service à valeur ajoutée hébergé dans l'environnement SaaS BlueXP, qui repose sur l'architecture BlueXP. Plusieurs composants principaux composent le service de reprise après sinistre pour la protection VMware au sein de BlueXP.

Pour un aperçu complet de la solution de reprise après sinistre BlueXP, consultez "[Découvrez la reprise d'activité BlueXP 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 pour NetApp ONTAP.

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

Présentation de la reprise après sinistre BlueXP 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 for ONTAP est déployé dans la même zone de disponibilité que le déploiement Amazon EVS. Le système de fichiers se connecte à Amazon EVS directement via une interface réseau élastique (ENI), une connexion homologue VPC ou une passerelle AmazonTransit.
3. Le connecteur NetApp BlueXP est installé sur votre VPC. Il héberge plusieurs services de gestion des données (appelés agents), dont l'agent de reprise après sinistre BlueXP qui gère la reprise après sinistre de l'infrastructure VMware sur vos centres de données physiques locaux et vos ressources hébergées sur Amazon AWS.
4. L'agent de reprise après sinistre BlueXP communique en toute sécurité avec le service hébergé dans le cloud BlueXP 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 BlueXP 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 les banques de données vCenter hébergeant les machines virtuelles protégées et les volumes ONTAP qui les hébergent. Si les volumes n'existent pas encore sur le cluster FSx for ONTAP, la reprise après sinistre BlueXP 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 console BlueXP et sélectionne une sauvegarde à utiliser comme point de restauration.
9. L'agent de récupération après sinistre BlueXP 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 le connecteur BlueXP pour la reprise après sinistre BlueXP

Un connecteur BlueXP est un logiciel NetApp exécuté sur votre réseau cloud ou sur site. Il exécute les actions nécessaires à BlueXP pour gérer votre infrastructure de données. Le connecteur interroge en permanence le logiciel de reprise d'activité BlueXP en tant que couche de service pour connaître les actions nécessaires.

Pour le service de reprise après sinistre BlueXP, les actions exécutées orchestrent les clusters VMware vCenter et les instances de stockage ONTAP à l'aide d'API natives pour chaque service afin de protéger les machines virtuelles de production exécutées sur site. Bien que le connecteur puisse être installé sur n'importe quel emplacement réseau, pour la reprise après sinistre BlueXP, nous recommandons de l'installer sur le site de reprise après sinistre. Ainsi, en cas de panne du site principal, l'interface utilisateur de la console cloud BlueXP reste en contact avec le connecteur et peut orchestrer le processus de reprise sur ce site.

Pour utiliser le service, installez le connecteur en mode standard. Pour en savoir plus sur les différents types d'installation du connecteur, consultez la page ["En savoir plus sur les modes de déploiement BlueXP | Documentation NetApp"](#) .

Bien que le connecteur soit essentiel à l'utilisation du service, ses étapes d'installation dépendent de vos besoins et de la configuration de votre réseau. Ces informations ne fournissent pas d'instructions spécifiques pour l'installation.

La méthode la plus simple pour installer un connecteur avec Amazon AWS est d'utiliser AWS Marketplace. Pour plus d'informations sur l'installation d'un connecteur via AWS Marketplace, consultez la page ["Créer un connecteur depuis AWS Marketplace | Documentation NetApp"](#) .

Configurer la reprise après sinistre BlueXP pour Amazon EVS

Présentation de la configuration de la reprise après sinistre BlueXP pour Amazon EVS

Après avoir installé le connecteur BlueXP, vous devez intégrer toutes les ressources de stockage ONTAP et VMware vCenter qui participeront au processus de récupération après sinistre avec la récupération après sinistre BlueXP.

- ["Conditions préalables pour la reprise après sinistre Amazon EVS avec BlueXP"](#)
- ["Ajoutez des baies de stockage ONTAP à la reprise après sinistre BlueXP"](#)
- ["Activer la reprise après sinistre BlueXP pour Amazon EVS"](#)
- ["Ajouter des sites vCenter à la récupération après sinistre BlueXP"](#)
- ["Ajouter des clusters vCenter à la reprise après sinistre BlueXP"](#)

Conditions préalables pour la reprise après sinistre Amazon EVS avec BlueXP

Vous devez vous assurer que plusieurs conditions préalables sont remplies avant de continuer à configurer Amazon EVS avec la reprise après sinistre BlueXP.

Plus précisément, procédez comme suit :

- Créez un compte utilisateur vCenter avec les privilèges VMware spécifiques requis pour la récupération

après sinistre BlueXP pour effectuer les opérations nécessaires.



Nous ne recommandons pas d'utiliser le compte administrateur par défaut « administrator@vsphere.com ». Il est préférable de créer un compte utilisateur BlueXP dédié à la reprise après sinistre sur tous les clusters vCenter participant au processus de reprise après sinistre. Pour obtenir la liste des privilèges spécifiques requis, consultez la section "[Privilèges vCenter requis pour la reprise d'activité BlueXP](#)".

- Assurez-vous que tous les magasins de données vCenter qui hébergeront les machines virtuelles protégées par la reprise après sinistre BlueXP sont situés sur des ressources de stockage NetApp ONTAP.

Le service prend en charge NFS et VMFS sur iSCSI (et non FC) lors de l'utilisation d'Amazon FSx sur NetApp ONTAP. Bien que le service prenne en charge FC, Amazon FSx pour NetApp ONTAP ne le prend pas en charge.

- 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 via une méthode de connexion approuvée par Amazon. Nous vous recommandons d'utiliser AWS Direct Connect, AWS Private Link ou un VPN site à site AWS.

Ajoutez des baies sur site à l'environnement de travail BlueXP pour Amazon EVS avec la reprise après sinistre BlueXP

Avant d'utiliser la récupération après sinistre BlueXP, vous devez ajouter des instances de stockage sur site et hébergées dans le cloud à l'environnement de travail BlueXP.

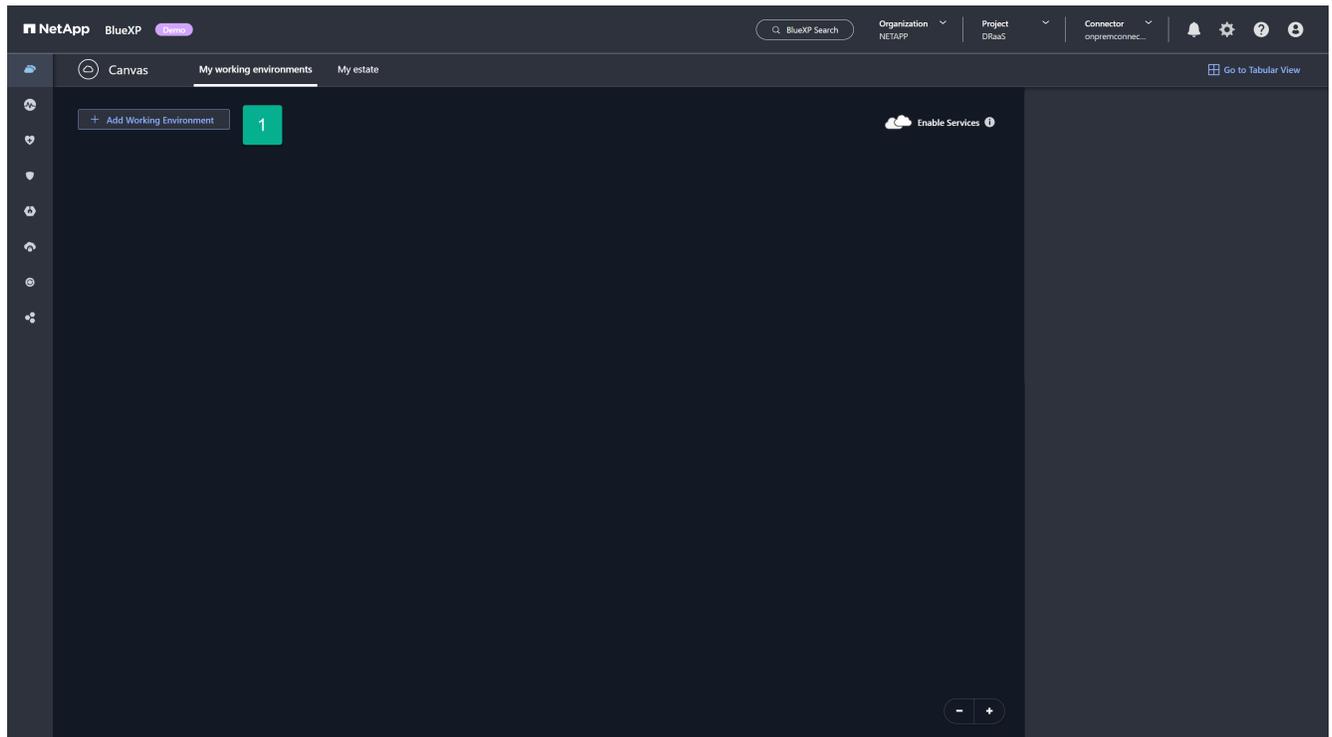
Vous devez effectuer les opérations suivantes :

- Ajoutez des baies sur site à votre environnement de travail BlueXP.
- Ajoutez des instances Amazon FSx for NetApp ONTAP (FSx for ONTAP) à votre environnement de travail BlueXP.

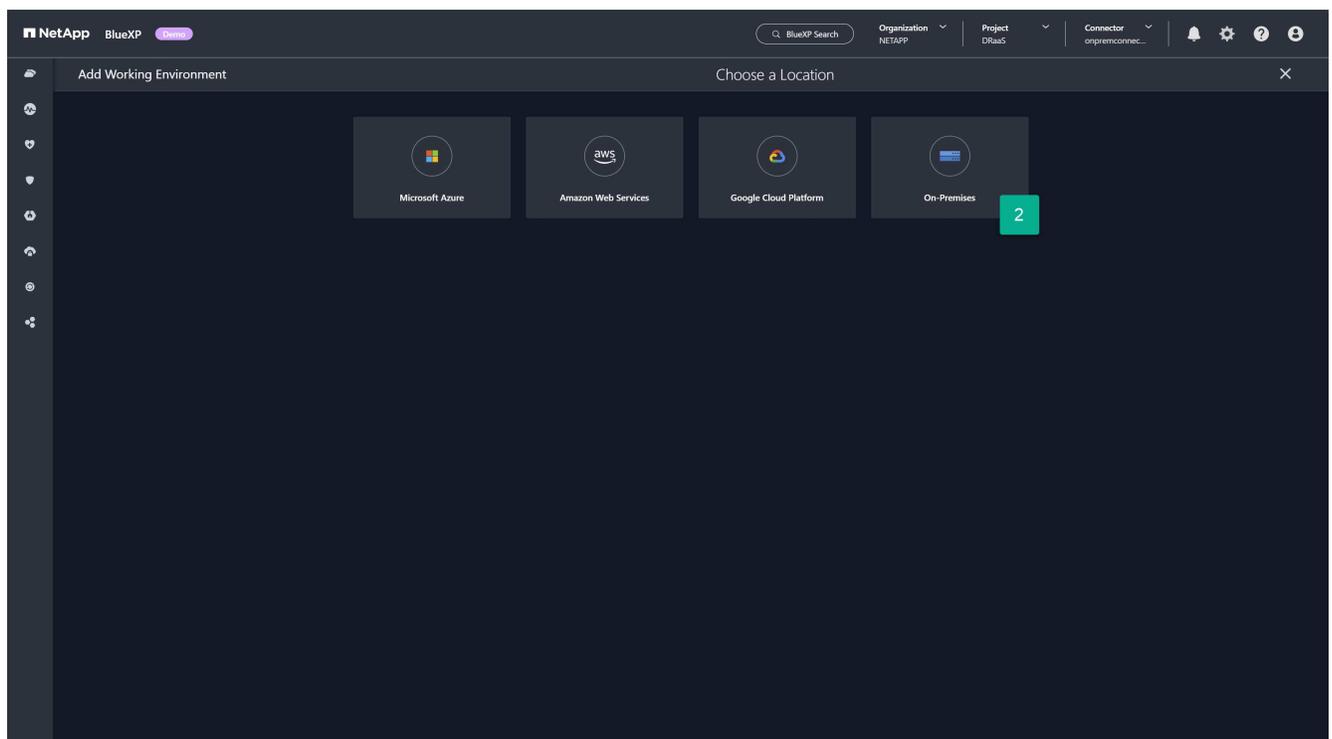
Ajouter des baies de stockage sur site à l'environnement de travail BlueXP

Ajoutez des ressources de stockage ONTAP sur site à votre environnement de travail BlueXP.

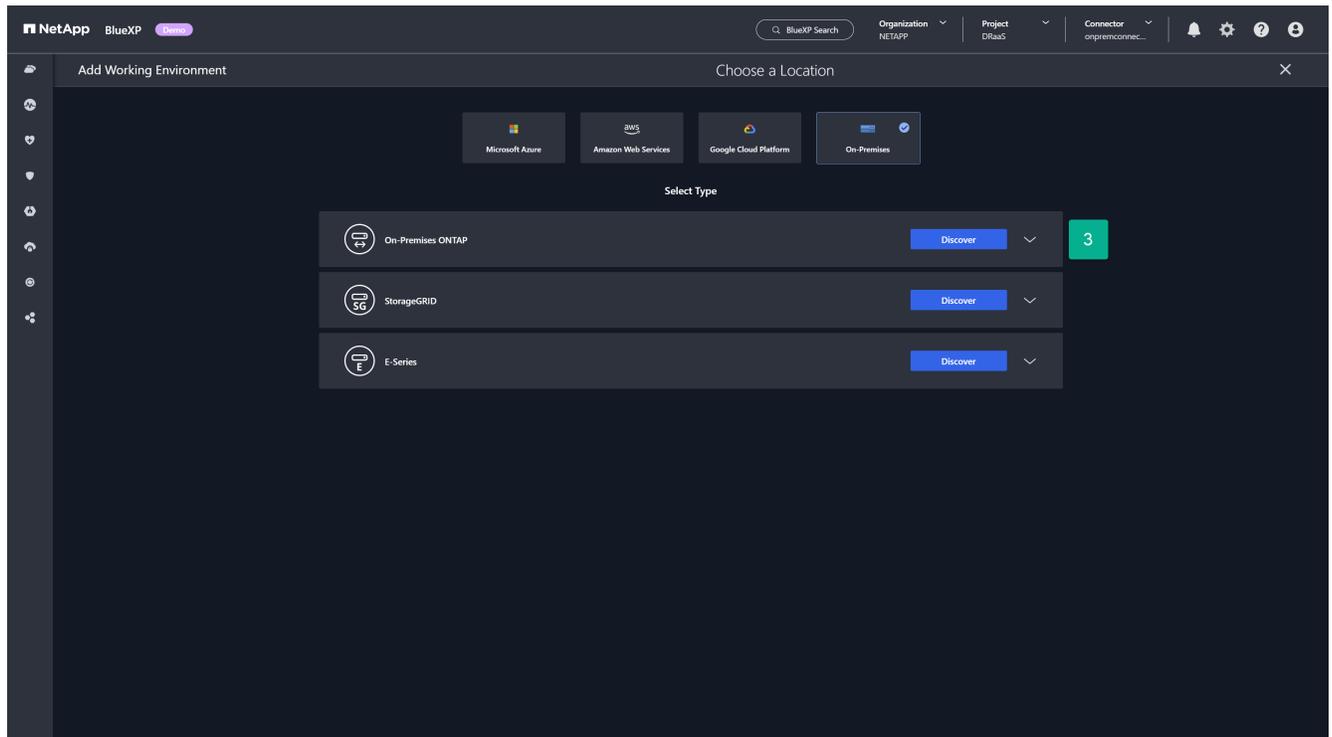
1. Depuis le canevas BlueXP, sélectionnez **Ajouter un environnement de travail**.



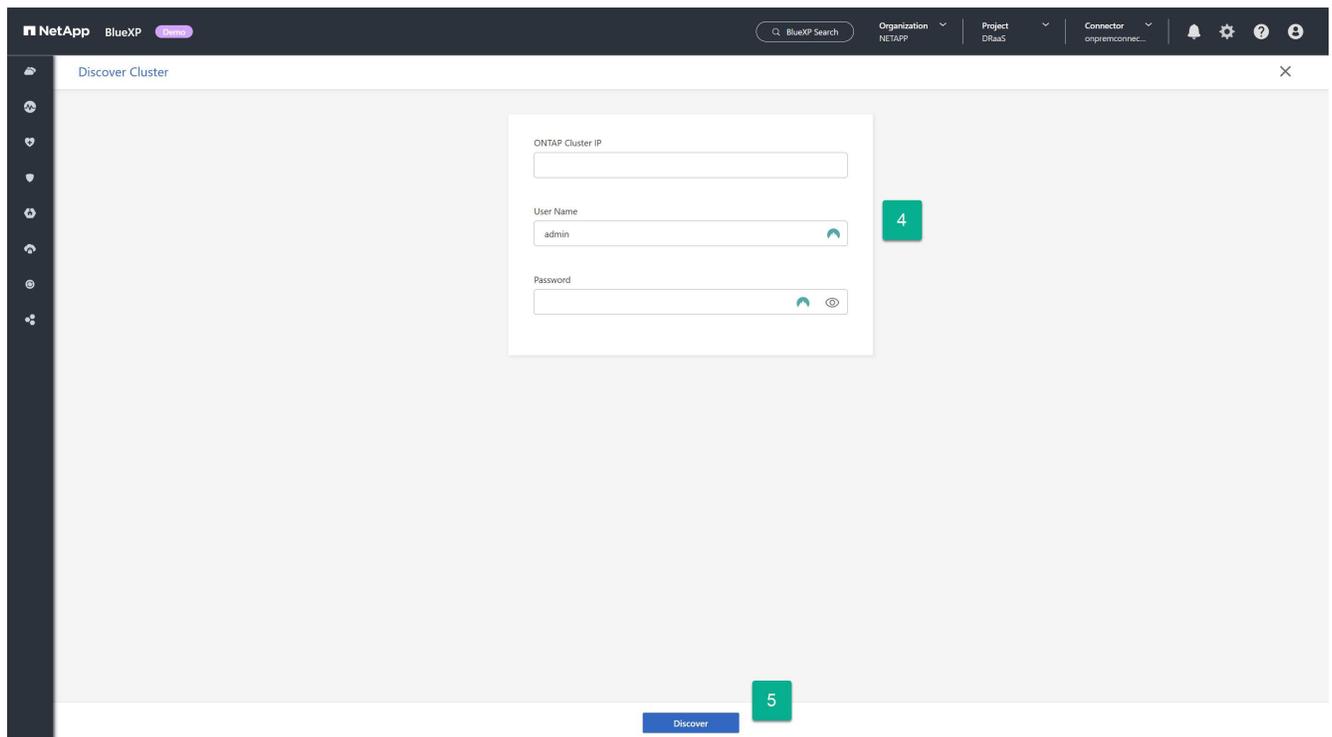
2. Depuis la page Ajouter un environnement de travail, sélectionnez la carte **Sur site**.



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 baies ONTAP
 - b. Le nom d'utilisateur de l'administrateur
 - c. Le mot de passe administrateur
5. Sélectionnez **Découvrir** au bas de la page.

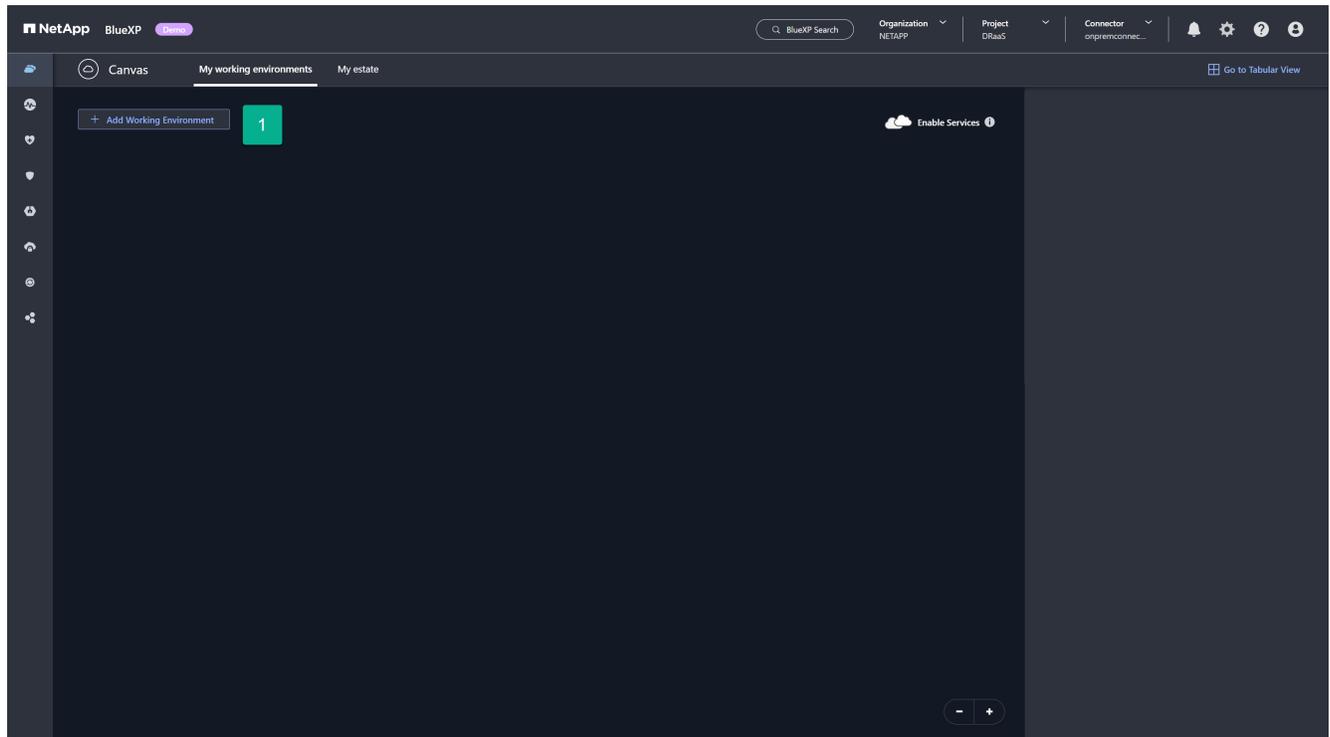


6. Répétez les étapes 1 à 5 pour chaque baie ONTAP qui hébergera les banques de données vCenter.

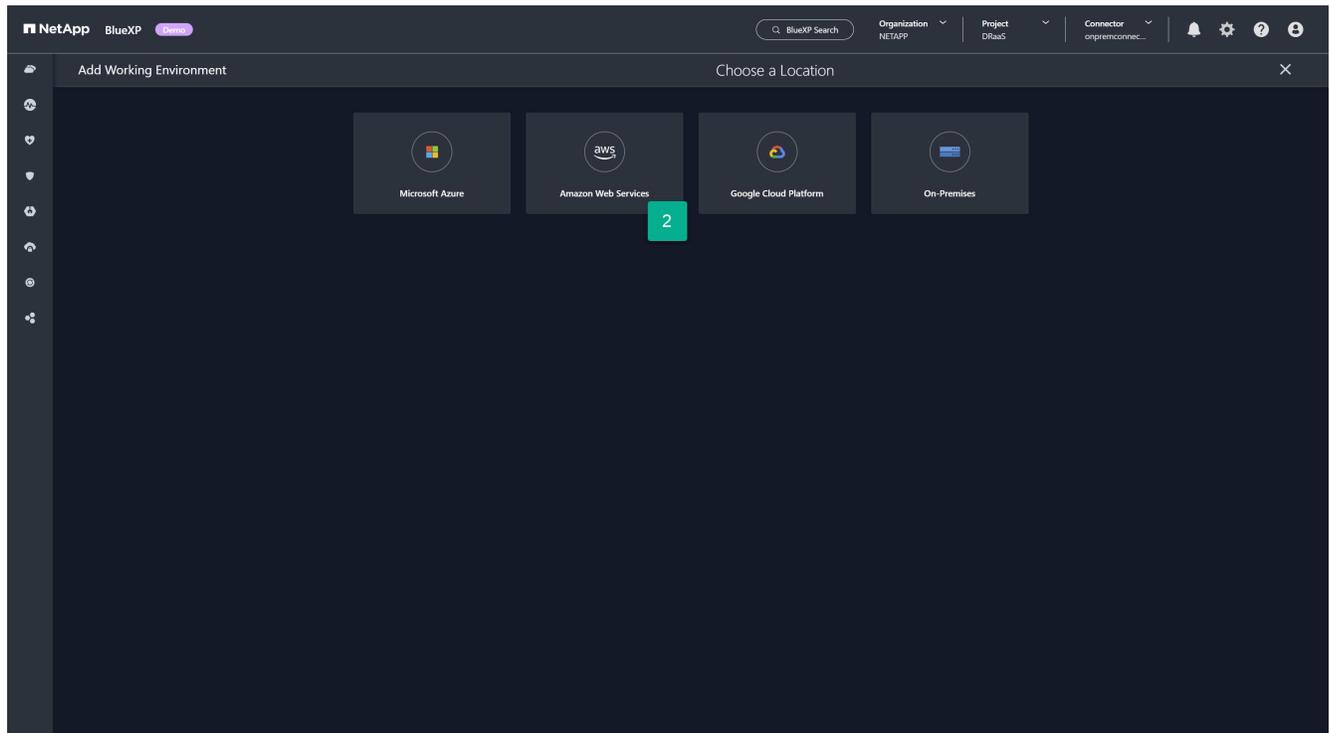
Ajoutez des instances de stockage Amazon FSx pour NetApp ONTAP à l'environnement de travail BlueXP

Ensuite, ajoutez des ressources de stockage Amazon FSx pour NetApp ONTAP à votre environnement de travail BlueXP.

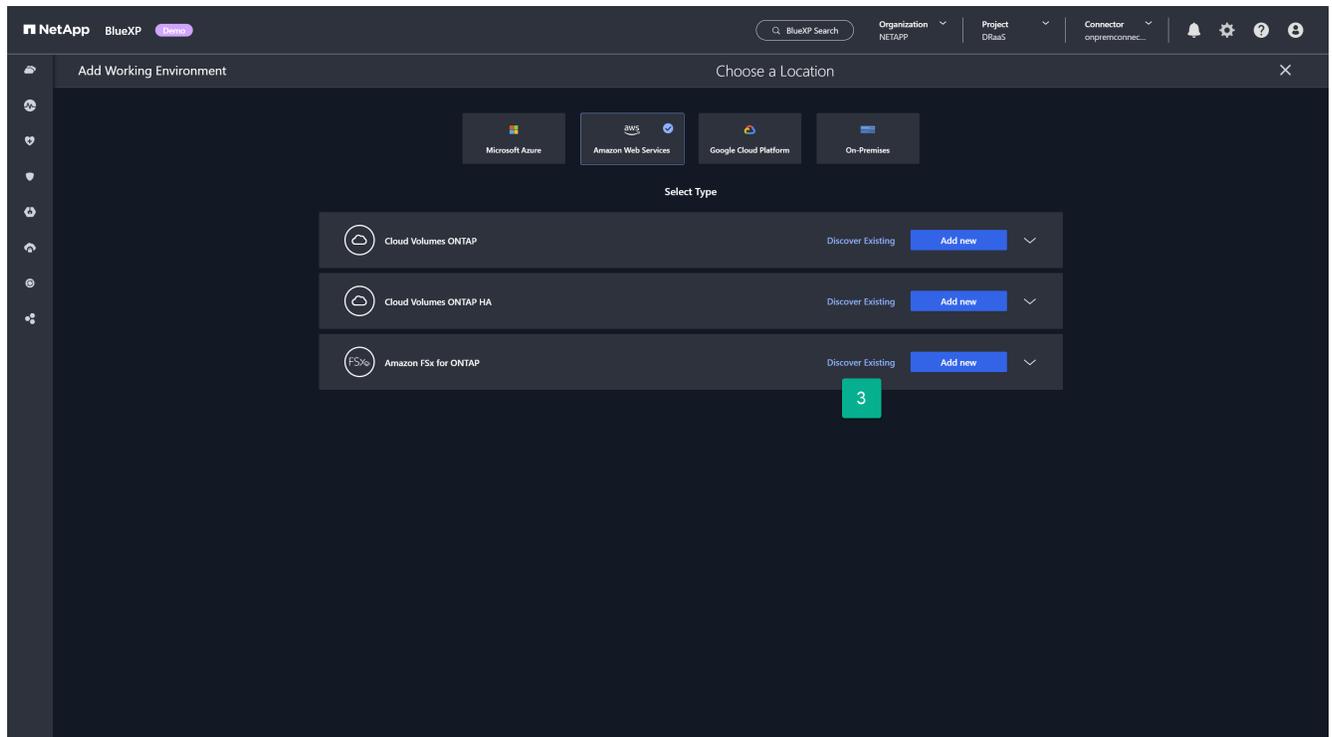
1. Depuis le canevas BlueXP, sélectionnez **Ajouter un environnement de travail**.



2. Depuis la page Ajouter un environnement de travail, sélectionnez la carte **Amazon Web Services**.



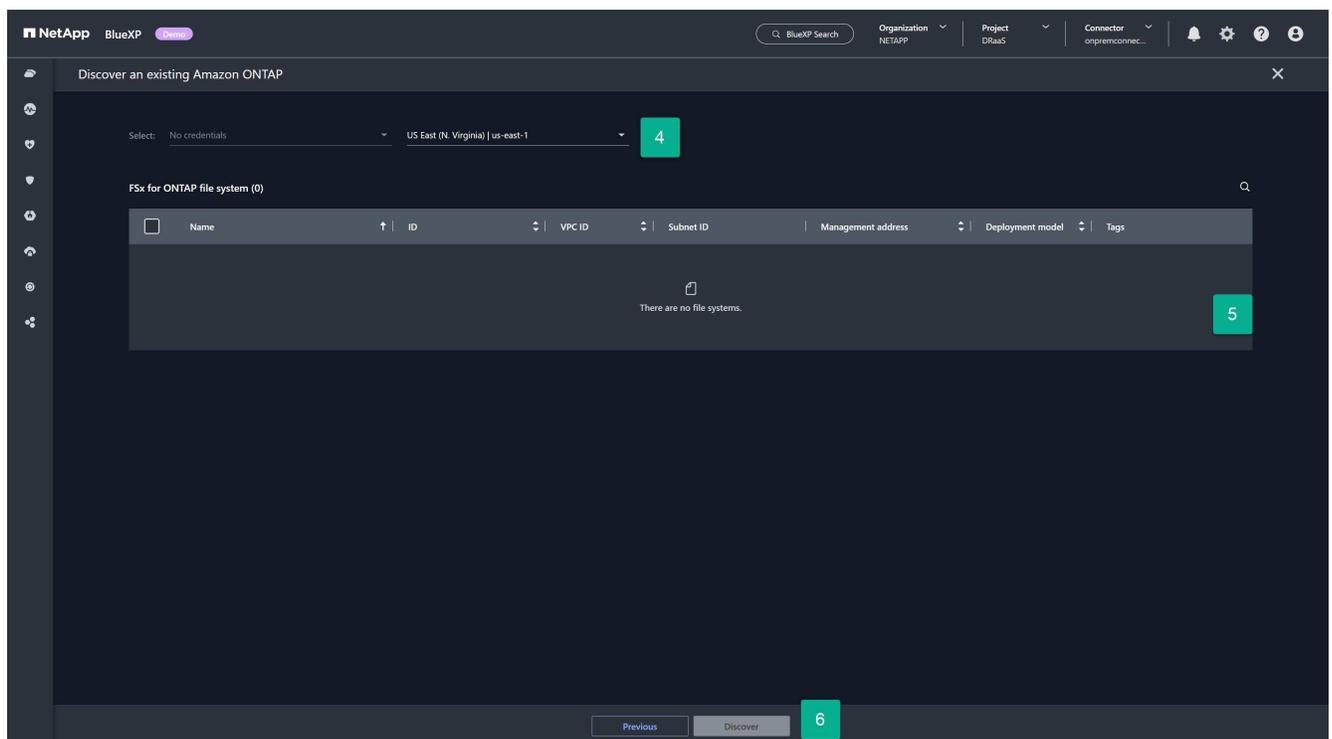
3. Sélectionnez le lien **Découvrir l'existant** sur la carte Amazon FSx for ONTAP.



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 de reprise après sinistre BlueXP à votre compte BlueXP pour Amazon EVS

BlueXP Disaster Recovery est un produit sous licence dont l'achat est obligatoire. Il existe plusieurs types de licences et différentes manières de les acquérir. Une licence vous permet de protéger une quantité spécifique de données pendant une durée déterminée.

Pour plus d'informations sur les licences de reprise après sinistre BlueXP, consultez ["Configurez les licences pour la reprise d'activité BlueXP"](#).

Types de licence

Il existe deux principaux types de licences :

- NetApp propose un ["Licence d'essai de 30 jours"](#) Vous pouvez l'utiliser pour évaluer la reprise après sinistre BlueXP avec vos ressources ONTAP et VMware. Cette licence offre 30 jours d'utilisation pour une capacité protégée illimitée.
- Achetez une licence de production si vous souhaitez une protection après sinistre au-delà de la période d'essai de 30 jours. Cette licence est disponible sur les marketplaces de tous les partenaires cloud de NetApp. Cependant, pour ce guide, nous vous recommandons d'acheter votre licence **NetApp Intelligent Services** pour la reprise après sinistre BlueXP via la marketplace Amazon AWS. Pour en savoir plus sur l'achat d'une licence sur la marketplace Amazon, consultez la page ["Abonnez-vous sur AWS Marketplace"](#).

Évaluez vos besoins en matière de capacité de reprise après sinistre

Avant d'acheter votre licence, vous devez connaître la capacité de stockage ONTAP à protéger. L'un des avantages du stockage NetApp ONTAP réside dans la grande efficacité avec laquelle NetApp stocke vos données. Toutes les données stockées sur un volume ONTAP (comme une banque de données VMware hébergeant des machines virtuelles) bénéficient d'une grande efficacité. 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. NetApp offre d'ailleurs une ["garantie d'efficacité de stockage"](#) pour certaines charges de travail.

Cela peut vous être bénéfique, car la reprise après sinistre BlueXP calcule la capacité à des fins de licence après application de toutes les améliorations d'efficacité du stockage ONTAP. Par exemple, imaginons que vous ayez provisionné une banque de données NFS de 100 téraoctets (Tio) dans vCenter pour héberger 100 machines virtuelles que vous souhaitez protéger via ce service. De plus, supposons que, lors de l'écriture des données sur le volume ONTAP, les techniques d'efficacité du stockage appliquées automatiquement entraînent une consommation de seulement 33 Tio par ces machines virtuelles (efficacité de stockage de 3:1). La reprise après sinistre BlueXP ne nécessite une licence que pour 33 Tio, et non 100 Tio. Cela peut représenter un avantage considérable sur le coût total de possession de votre solution de reprise après sinistre par rapport à d'autres solutions de reprise après sinistre.

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 CLI ONTAP 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 la solution de reprise après sinistre BlueXP doit protéger, et c'est cette valeur qui déterminera la capacité nécessaire pour l'acquisition de licences.

Ajouter des sites dans la reprise après sinistre BlueXP pour Amazon EVS

Avant de protéger votre infrastructure de machines virtuelles, identifiez les clusters VMware vCenter qui hébergent les machines virtuelles à protéger et leur emplacement. La première étape consiste à créer un site représentant les centres de données source et de destination. Un site est un domaine de défaillance ou de reprise.

Vous devez créer les éléments suivants :

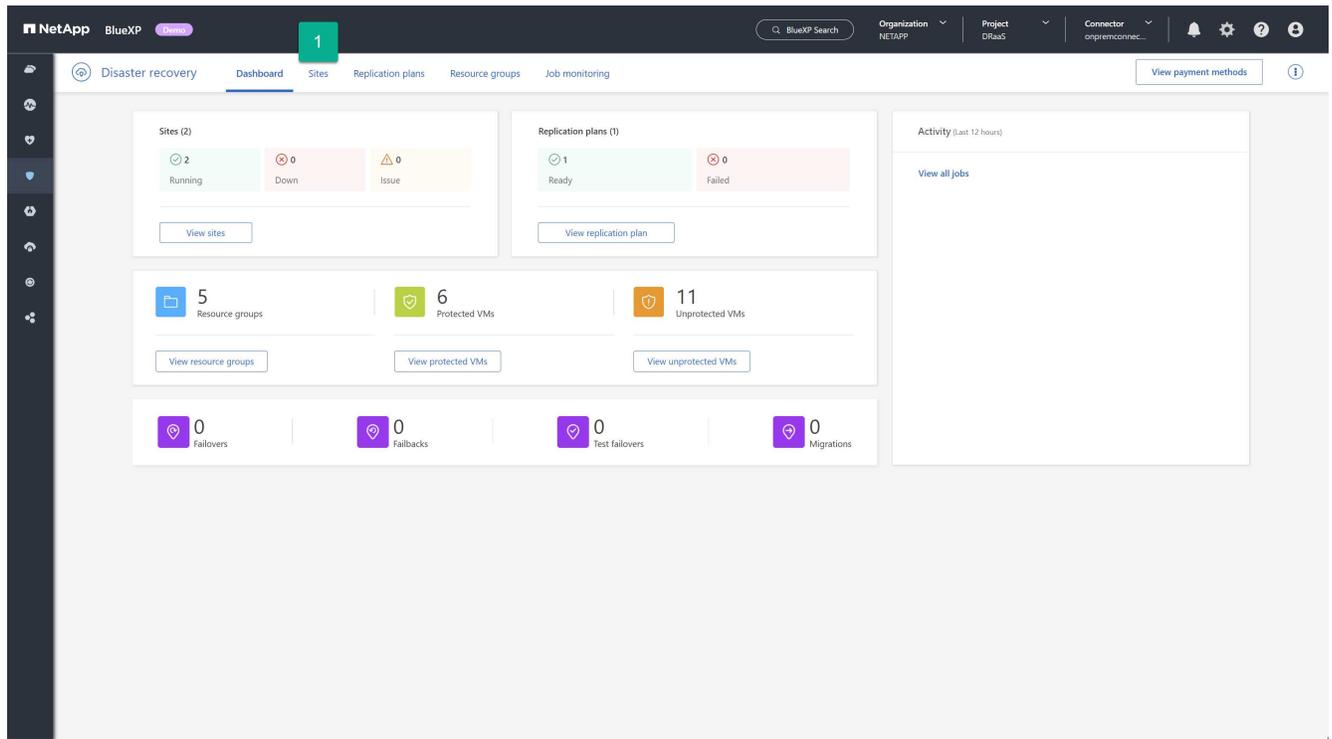
- Un site pour représenter chaque centre de données de production où résident vos clusters vCenter de production
- Un site pour votre centre de données cloud Amazon EVS/Amazon FSx pour NetApp ONTAP

Créer des sites sur site

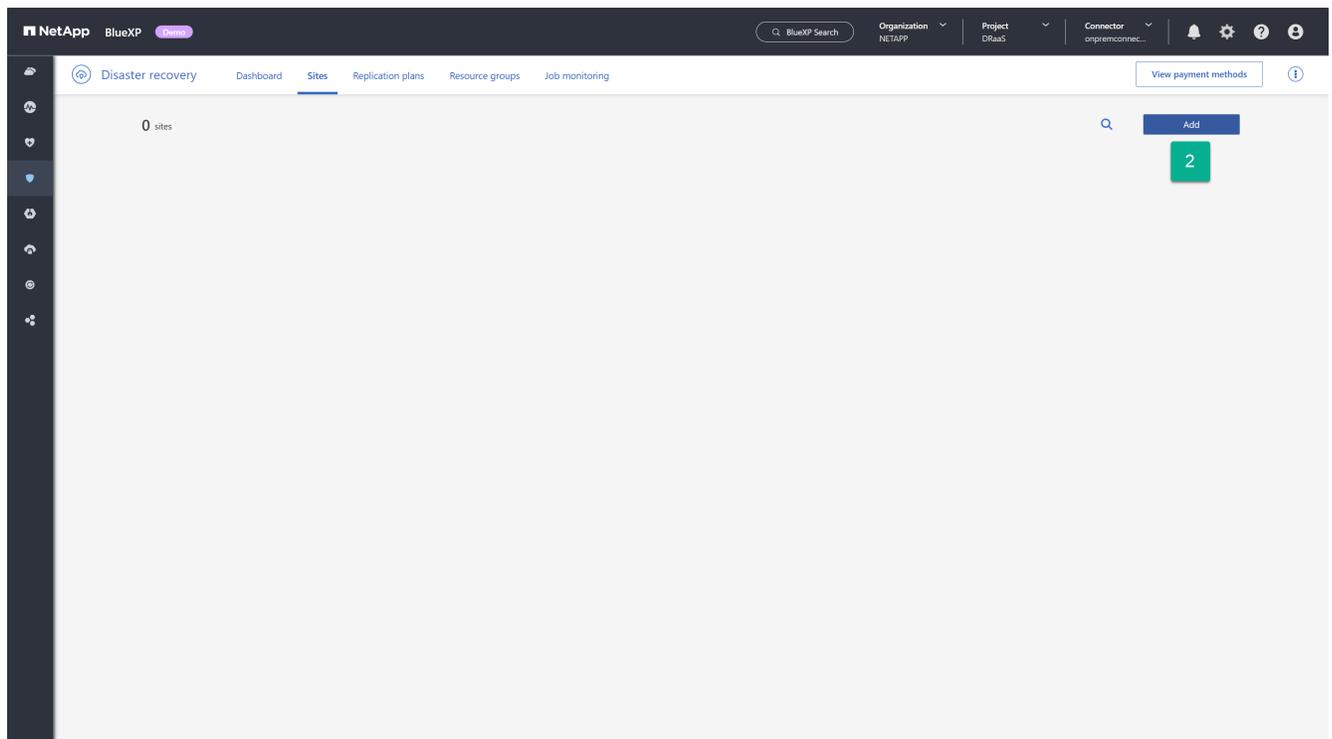
Créez un site vCenter de production.

Étapes

1. Dans la navigation de gauche de BlueXP, sélectionnez **Protection > Reprise après sinistre**.
2. Depuis n'importe quelle page de la récupération après sinistre BlueXP, sélectionnez l'onglet **Sites**.



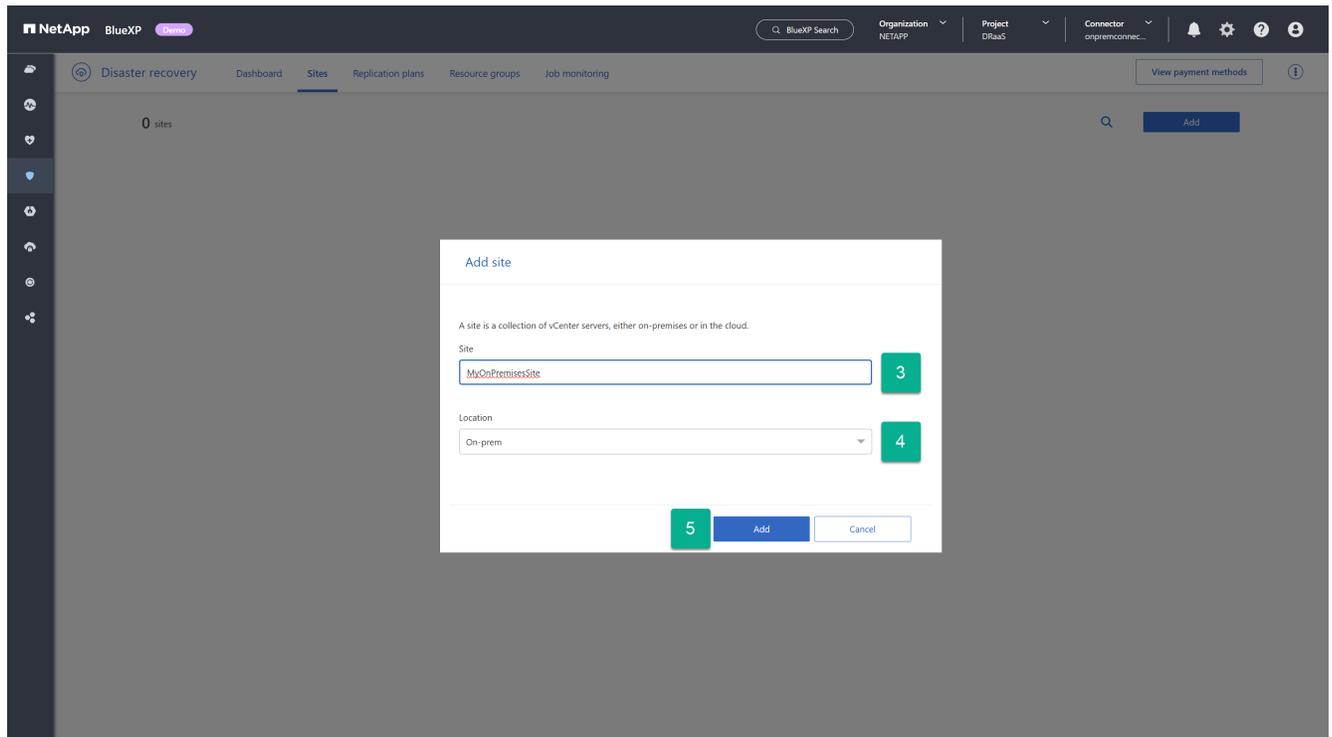
3. Dans l'onglet Sites, sélectionnez **Ajouter**.



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

5. Sélectionnez « Sur site » comme emplacement.

6. Sélectionnez **Ajouter**.

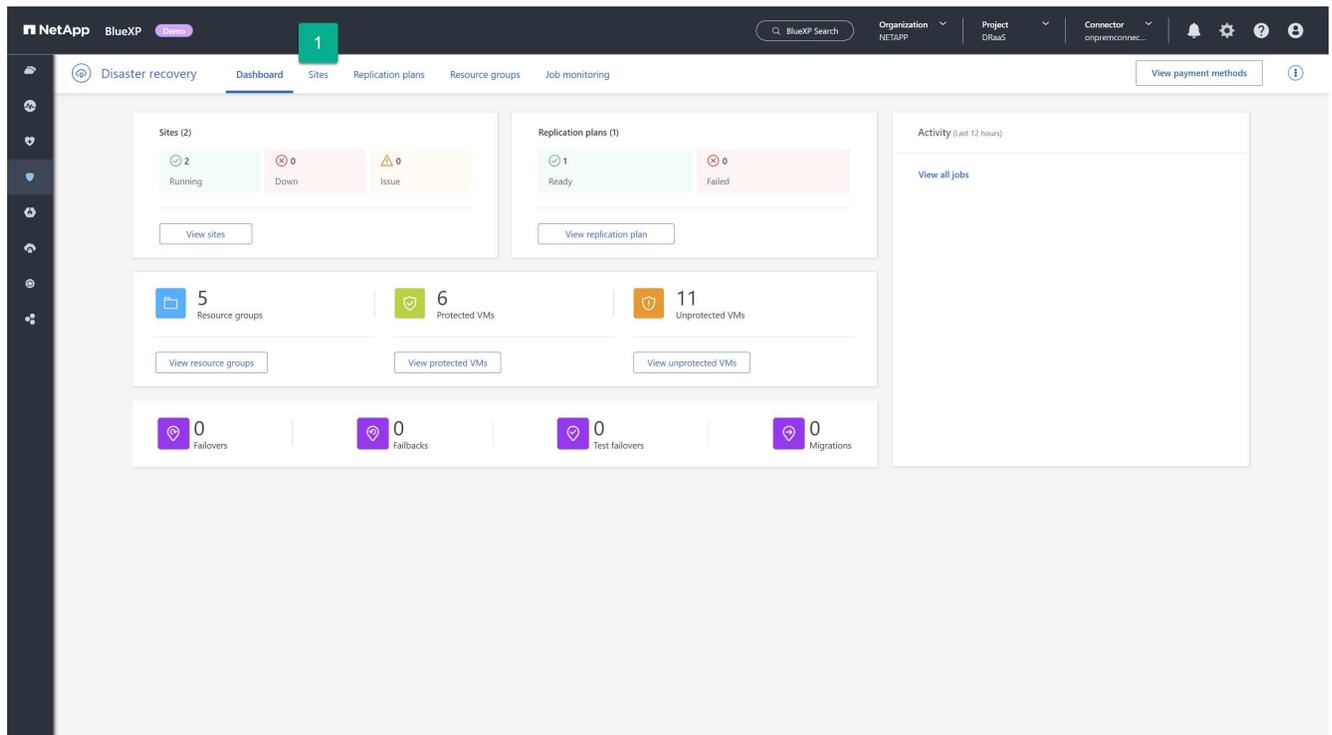


Si vous disposez d'autres sites vCenter de production, vous pouvez les ajouter en suivant les mêmes étapes.

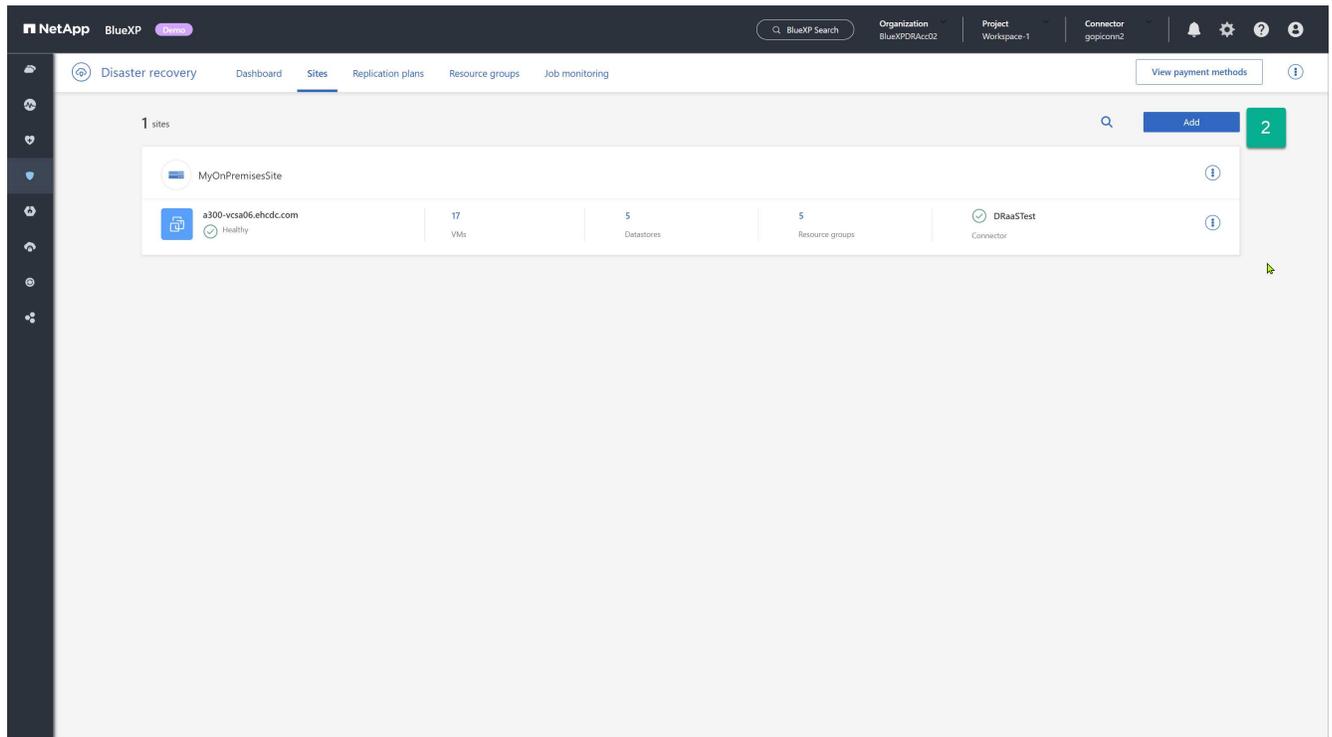
Créer des sites cloud Amazon

Créez un site DR pour Amazon EVS à l'aide d'Amazon FSx pour le stockage NetApp ONTAP.

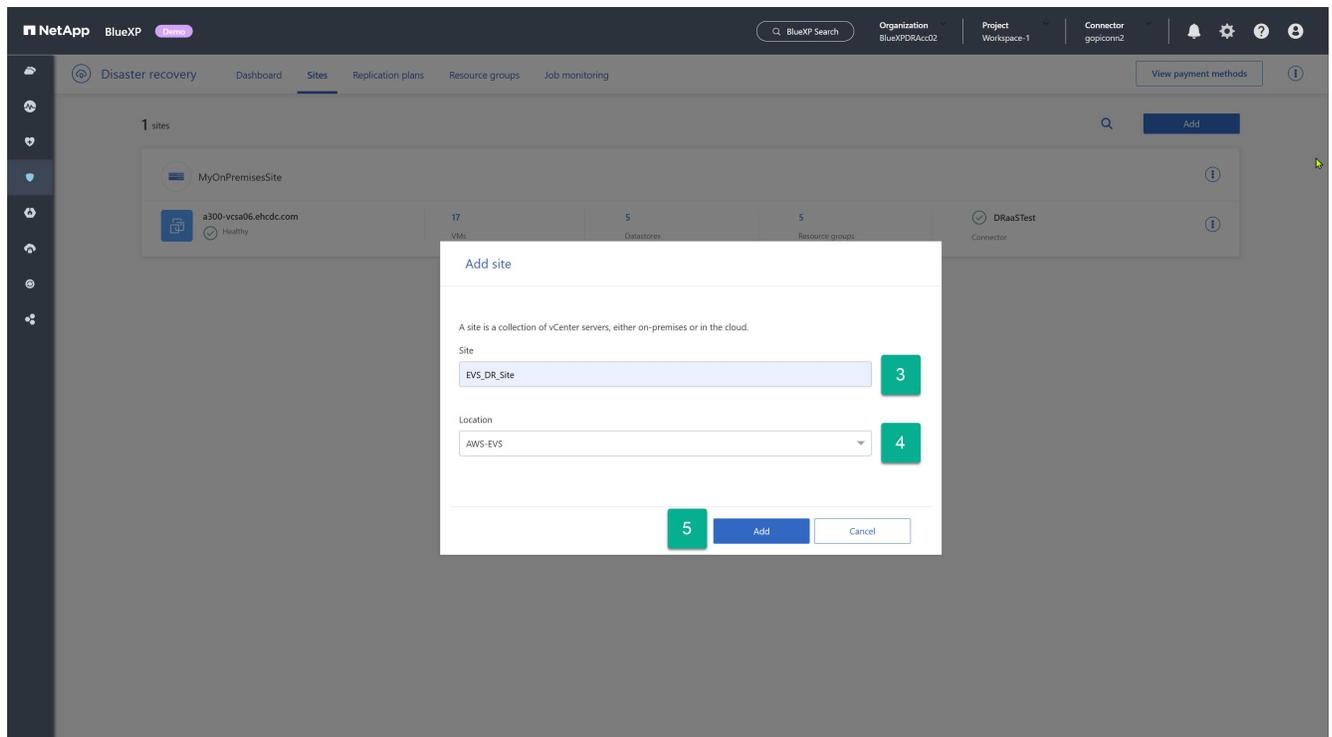
1. Depuis n'importe quelle page de la récupération après sinistre BlueXP, sélectionnez l'onglet **Sites**.



2. Dans l'onglet 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

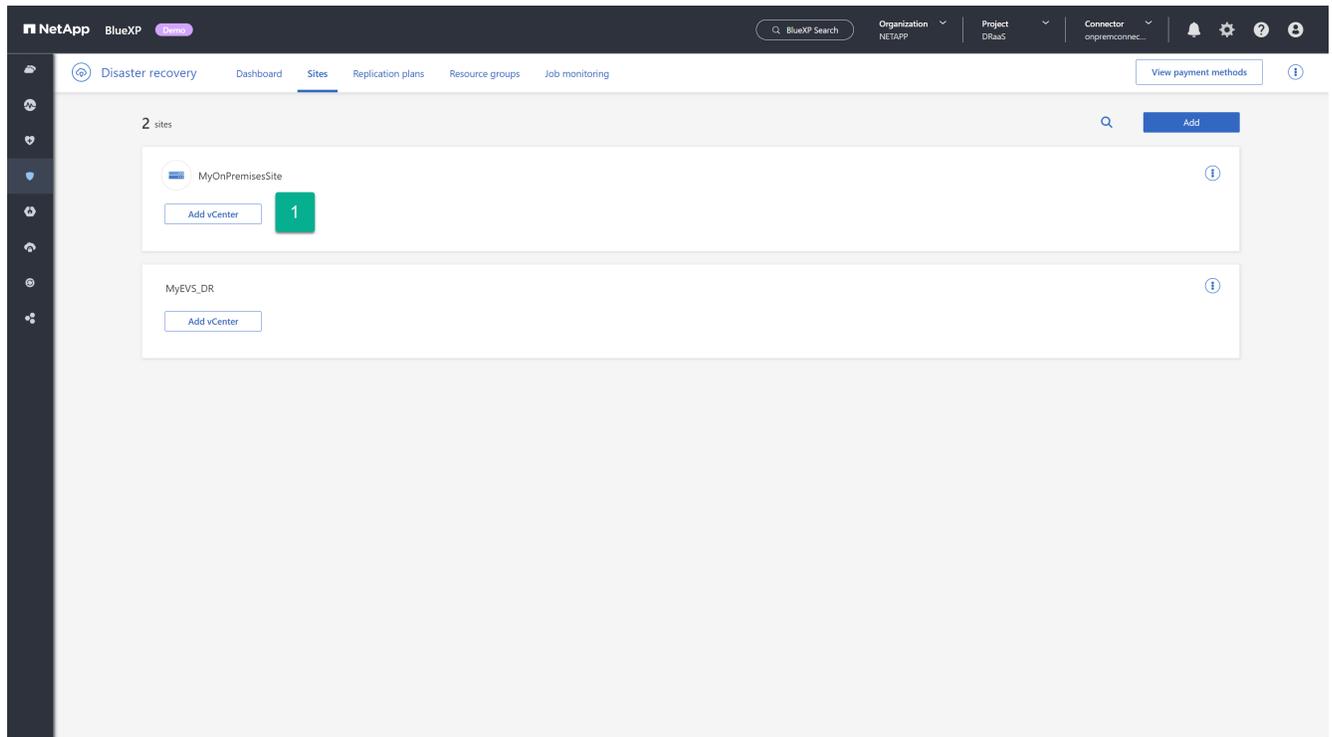
Vous disposez désormais d'un site de production (source) et d'un site DR (destination) créés.

Ajoutez des clusters vCenter sur site et Amazon EVS dans la reprise après sinistre BlueXP

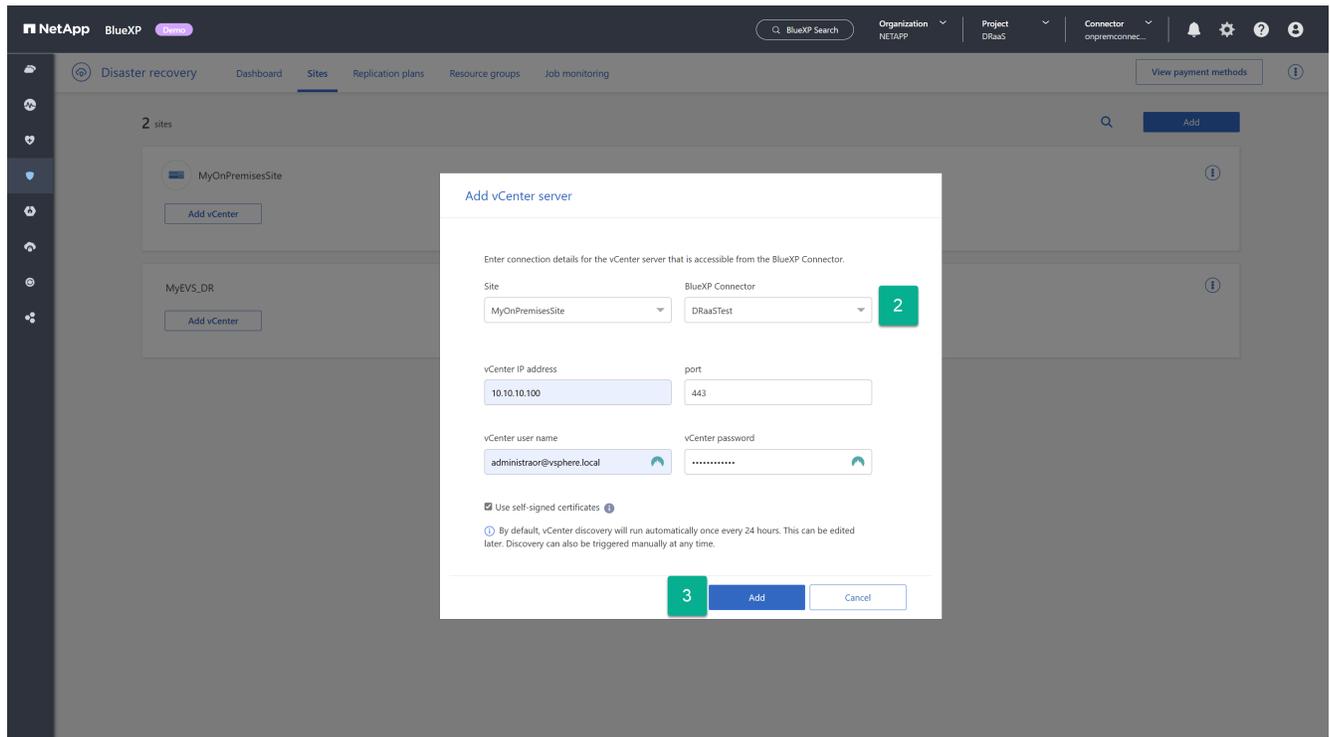
Une fois les sites créés, vous pouvez désormais ajouter vos clusters vCenter à chaque site dans la reprise après sinistre BlueXP. Lors de la création de chaque site, nous avons indiqué chaque type de site. Cela indique à la reprise après sinistre BlueXP le type d'accès requis pour les vCenters hébergés sur chaque type de site. L'un des avantages d'Amazon EVS est qu'il n'y a aucune distinction réelle 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. Dans l'onglet **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. Le connecteur BlueXP 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 la récupération après sinistre BlueXP pour gérer le vCenter.
 - e. Le mot de passe vCenter pour le nom d'utilisateur fourni.
 - f. Si votre entreprise utilise une autorité de certification externe ou le magasin de certificats vCenter Endpoint pour accéder à vos vCenters, décochez la case « Utiliser des certificats auto-signés ». Sinon, laissez la case cochée.
3. Sélectionnez **Ajouter**.



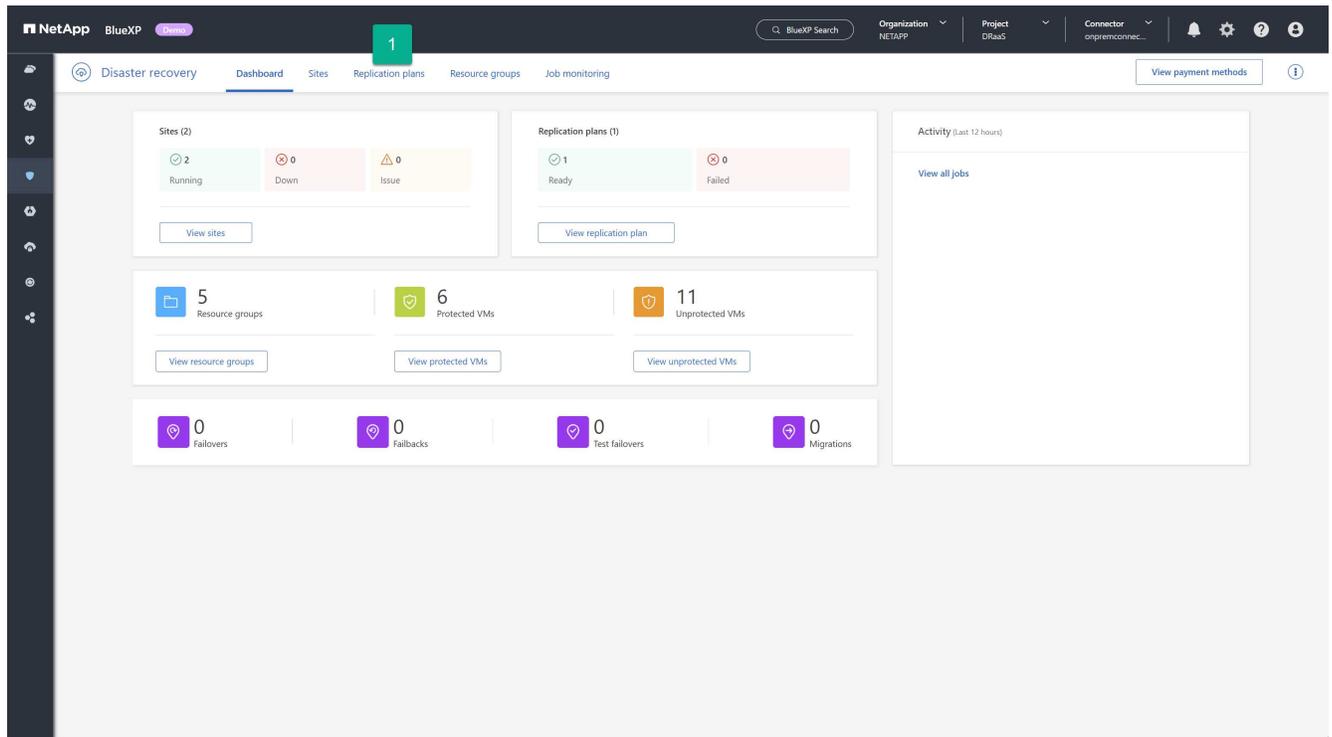
Créer des plans de réplication pour Amazon EVS

Créer des plans de réplication dans la vue d'ensemble de la reprise après sinistre BlueXP

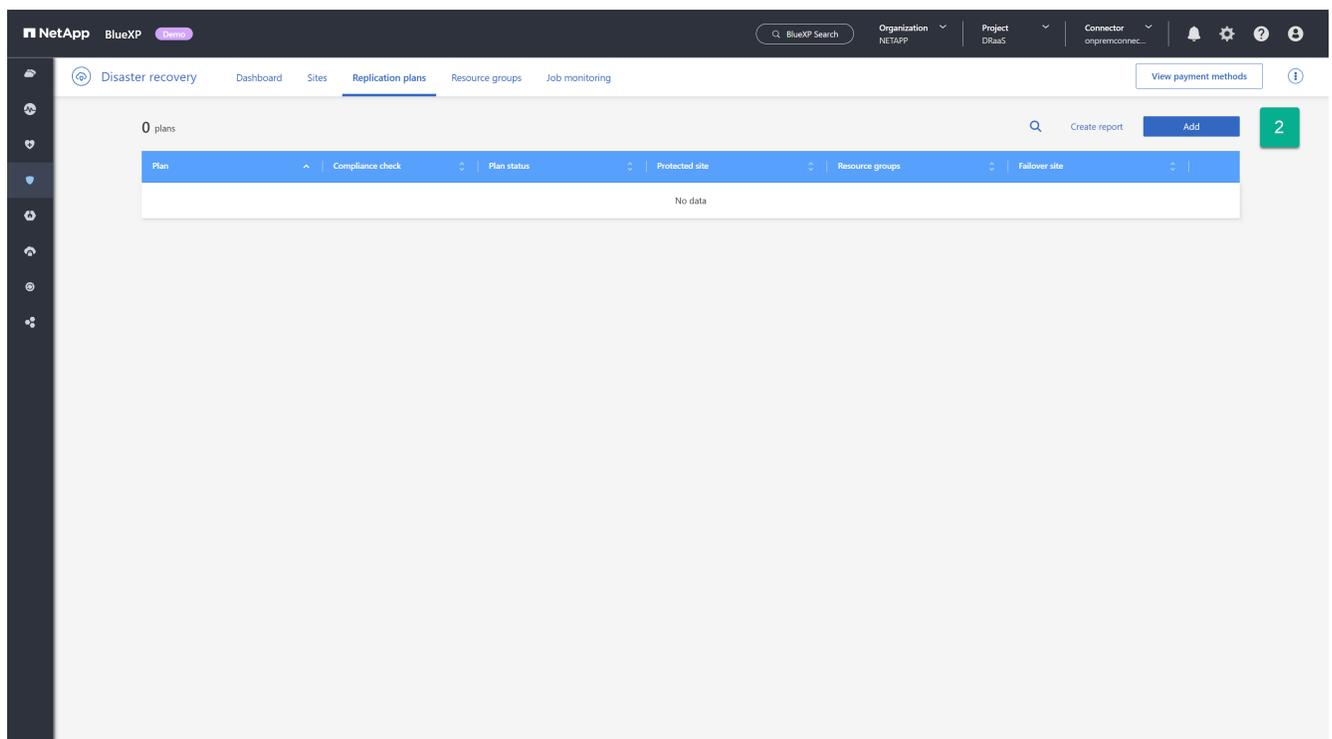
Une fois que vous avez des vCenters à protéger sur le site local et que vous disposez d'un site Amazon EVS configuré pour utiliser Amazon FSx for NetApp ONTAP que vous pouvez utiliser comme destination de reprise après sinistre, vous pouvez créer un plan de réplication (RP) pour protéger tout ensemble 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 récupération après sinistre BlueXP, sélectionnez l'onglet **Plans de réplication**.



2. Dans l'écran 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 la récupération après sinistre BlueXP

Tout d'abord, à l'aide de la récupération après sinistre BlueXP, indiquez un nom de plan de réplication et sélectionnez les vCenters source et de destination pour la réplication.

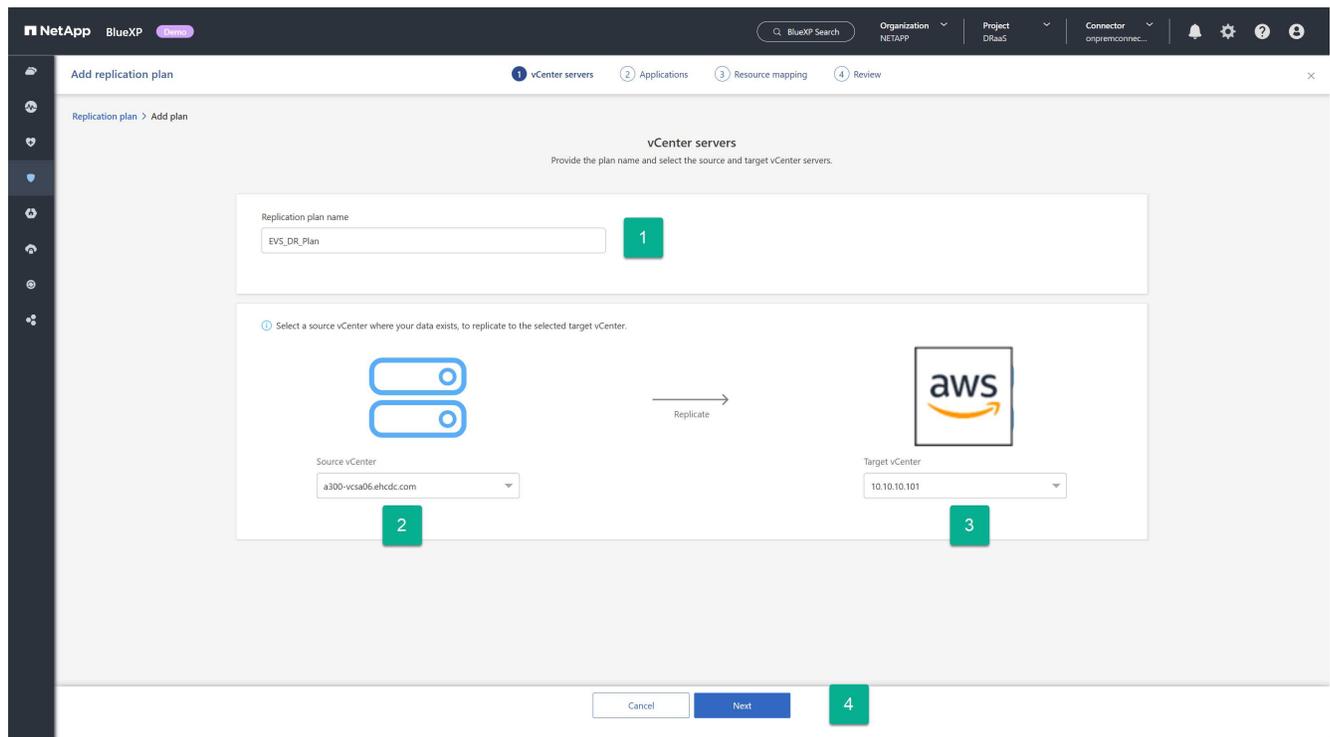
1. Saisissez un nom unique pour le plan de réplication.

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 la récupération après sinistre BlueXP

Sélectionnez les machines virtuelles à protéger à l'aide de la récupération après sinistre BlueXP.

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 les machines virtuelles à protéger. À chaque sélection, le service ajoute une machine virtuelle à un groupe de ressources par défaut situé à droite de l'écran.
- **Sélectionner des groupes de ressources précédemment créés** : Vous pouvez créer des groupes de ressources personnalisés au préalable via l'onglet Groupe de ressources en haut de l'interface de reprise

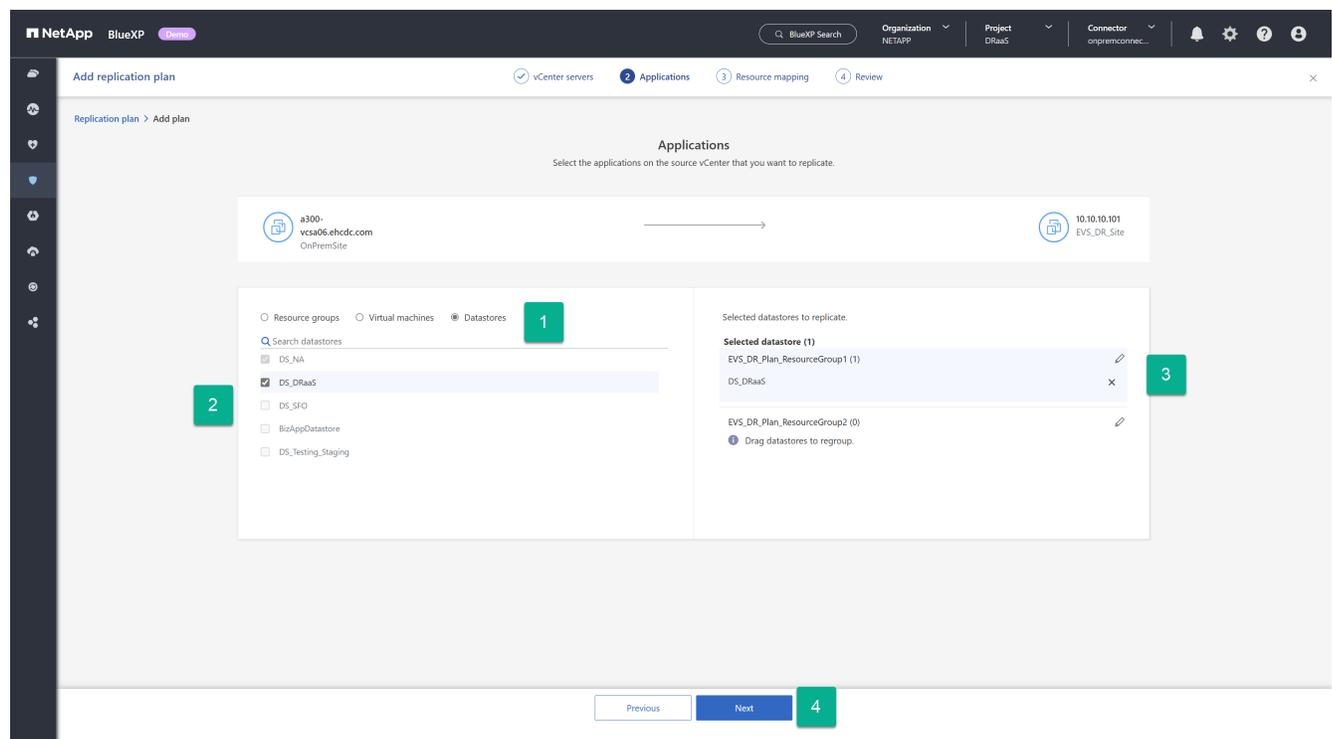
après sinistre de BlueXP. Ce n'est pas obligatoire, car vous pouvez utiliser les deux autres méthodes pour créer un groupe de ressources dans le cadre du plan de réplication. Pour plus de détails, voir "[Créer un plan de réplication](#)".

- **Sélectionner l'intégralité des datastores vCenter** : Si vous avez beaucoup de machines virtuelles à protéger avec ce plan de réplication, sélectionner des machines virtuelles individuelles peut s'avérer moins efficace. Étant donné que la reprise après sinistre BlueXP utilise la réplication SnapMirror basée sur les volumes pour protéger les machines virtuelles, toutes les machines virtuelles résidant sur un datastore seront répliquées au sein du volume. Dans la plupart des cas, la reprise après sinistre BlueXP doit protéger et redémarrer toutes les machines virtuelles situées sur le datastore. Utilisez cette option pour indiquer au service d'ajouter toutes les machines virtuelles hébergées sur un datastore sélectionné 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 la reprise après sinistre BlueXP

Une fois que vous disposez d'une liste de machines virtuelles que vous souhaitez protéger à l'aide de la récupération après sinistre BlueXP, 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 du magasin de données

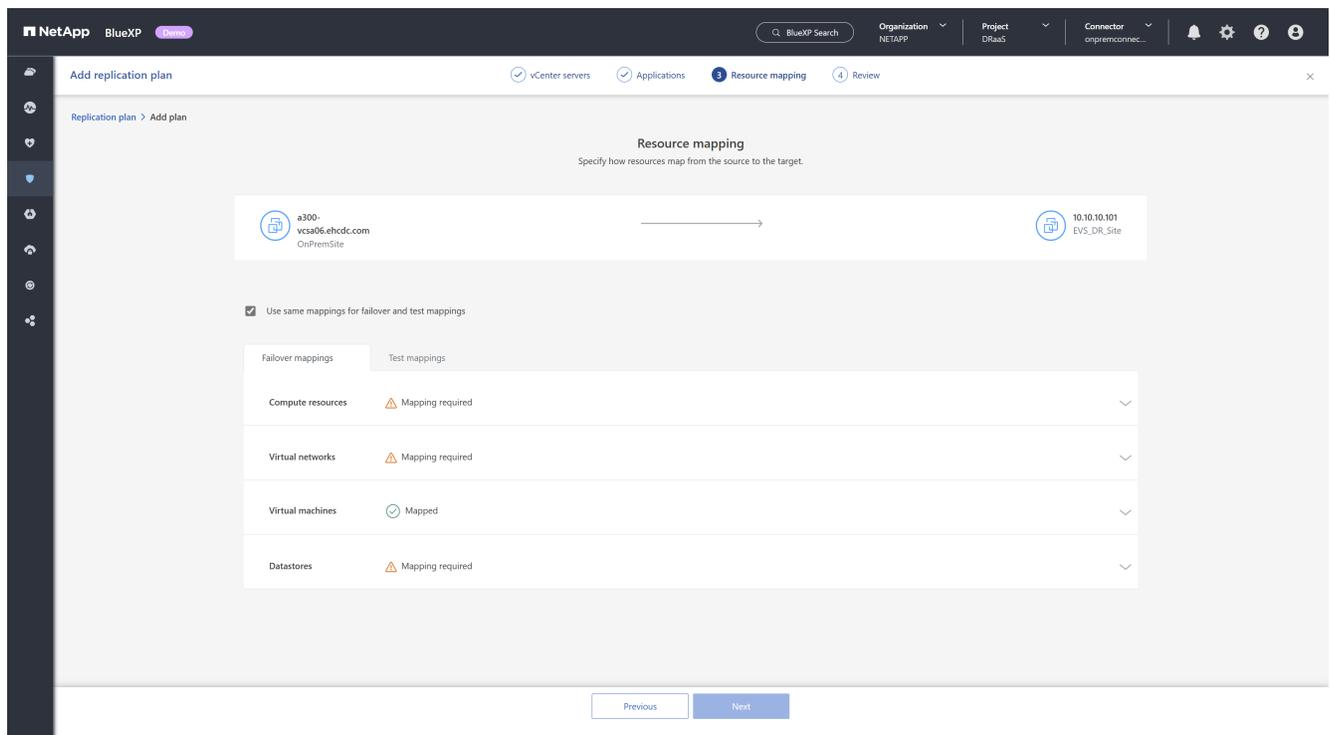
Chaque machine virtuelle nécessite les trois premiers types d'informations. Le mappage des banques de données est requis pour chaque banque de données hébergeant les machines virtuelles à protéger.

- 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 possèdent des mappages par défaut. Vérifiez-les 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 **Mappage des ressources** qui s'ouvre.



The screenshot displays the NetApp BlueXP web interface during the 'Resource mapping' step of a replication plan configuration. The breadcrumb trail shows 'Replication plan > Add plan'. The main heading is 'Resource mapping' with the subtext 'Specify how resources map from the source to the target'. The source is identified as 'a300-vcsa06.ehcdc.com OnPremSite' and the target as '10.10.10.101 EVS_DR_Site'. A checkbox 'Use same mappings for failover and test mappings' is checked. Below this, there are two tabs: 'Failover mappings' (active) and 'Test mappings'. A table lists resource types and their mapping status:

Resource Type	Status
Compute resources	Mapping required
Virtual networks	Mapping required
Virtual machines	Mapped
Datstores	Mapping required

At the bottom, there are 'Previous' and 'Next' navigation buttons.

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.

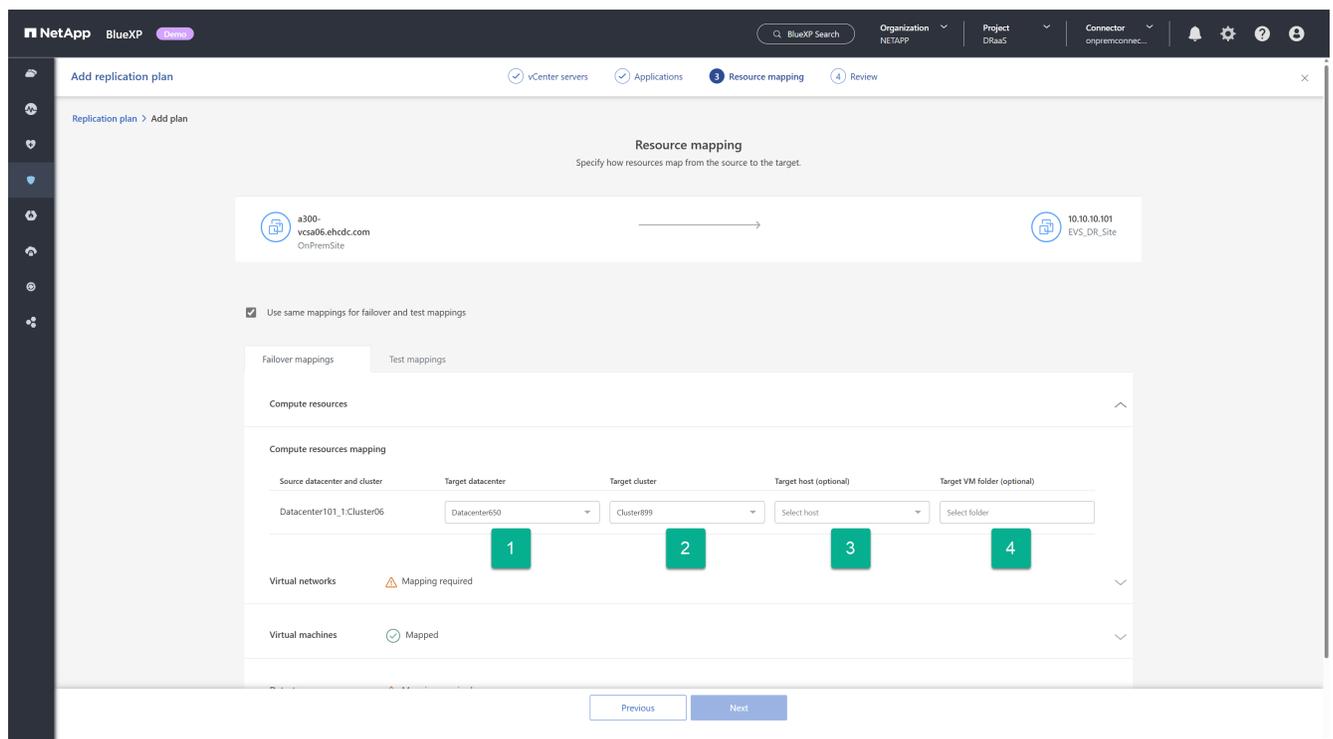
Étapes pour cartographier les ressources de calcul

1. Sélectionnez le centre de données virtuel dans la liste des centres de données situés sur le site DR.
2. Sélectionnez le cluster pour héberger 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 nécessaire, car la reprise après sinistre BlueXP 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.



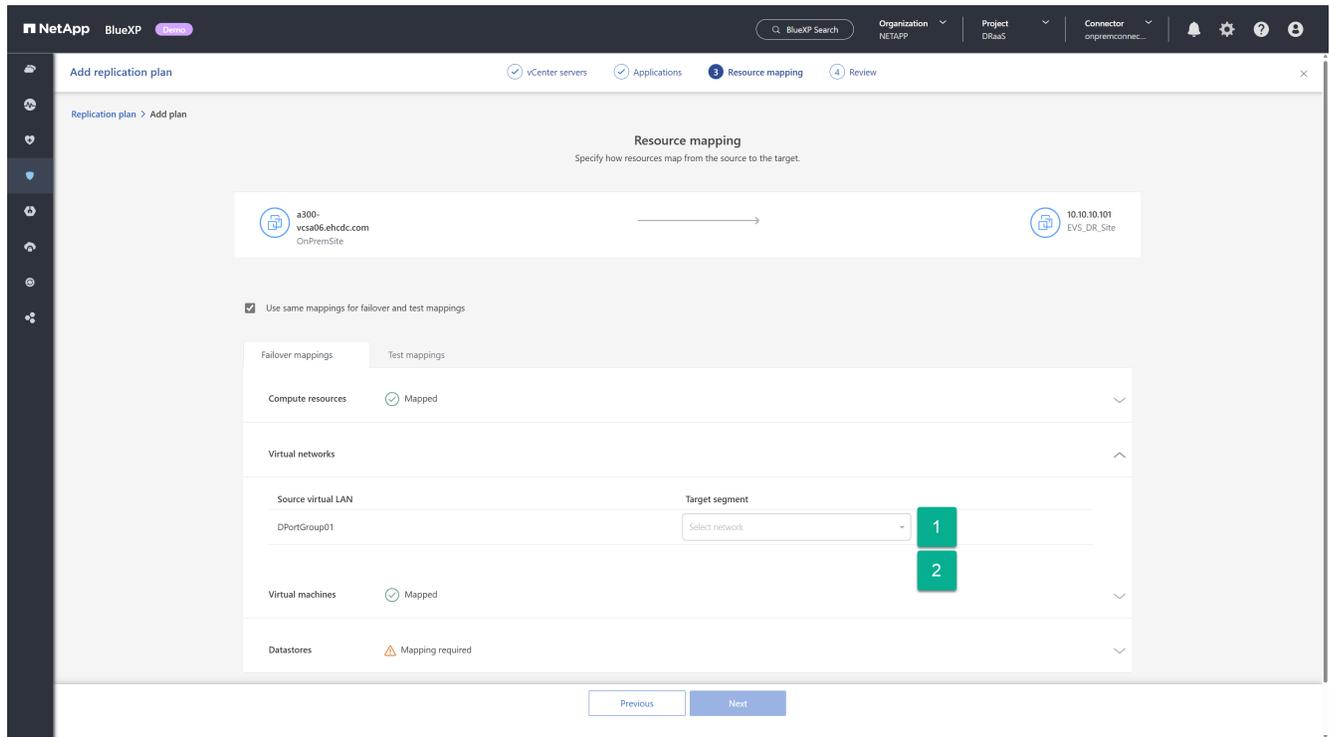
Cartographier les ressources du réseau virtuel

Chaque machine virtuelle peut disposer d'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 de reprise après sinistre, identifiez les réseaux virtuels du site de reprise après sinistre auxquels ces machines virtuelles doivent être connectées. Pour ce faire, mappez chaque réseau virtuel du site sur site à un réseau associé sur le site de reprise après

sinistre.

Sélectionnez le réseau virtuel de destination sur lequel 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 vCenter de reprise après sinistre. La section « Machines virtuelles » vous permet d'effectuer les modifications nécessaires.

Par défaut, la reprise après sinistre BlueXP utilise les mêmes paramètres pour chaque machine virtuelle que ceux utilisés sur le site source sur site. Cela suppose que les machines virtuelles utilisent la même adresse IP, le même processeur virtuel et la même configuration de DRAM virtuelle.

Reconfiguration du réseau

Les types d'adresses IP pris en charge sont les adresses IP statiques et DHCP. Pour les adresses IP statiques, les paramètres IP cibles sont les 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 de configurer les réseaux virtuels mappés à l'étape précédente avec les mêmes paramètres de sous-réseau.
- **Différent de la source** : Le service fournit un ensemble de champs d'adresse IP pour chaque machine virtuelle (VM) qui doivent être configurés pour le sous-réseau approprié utilisé sur le réseau virtuel de destination, mappé dans la section précédente. Pour chaque VM, vous devez fournir une adresse IP, un masque de sous-réseau, un DNS et une passerelle par défaut. Vous pouvez également utiliser les mêmes paramètres de masque de sous-réseau, DNS et passerelle pour toutes les VM afin de simplifier le processus lorsque toutes les VM sont connectées au même sous-réseau.

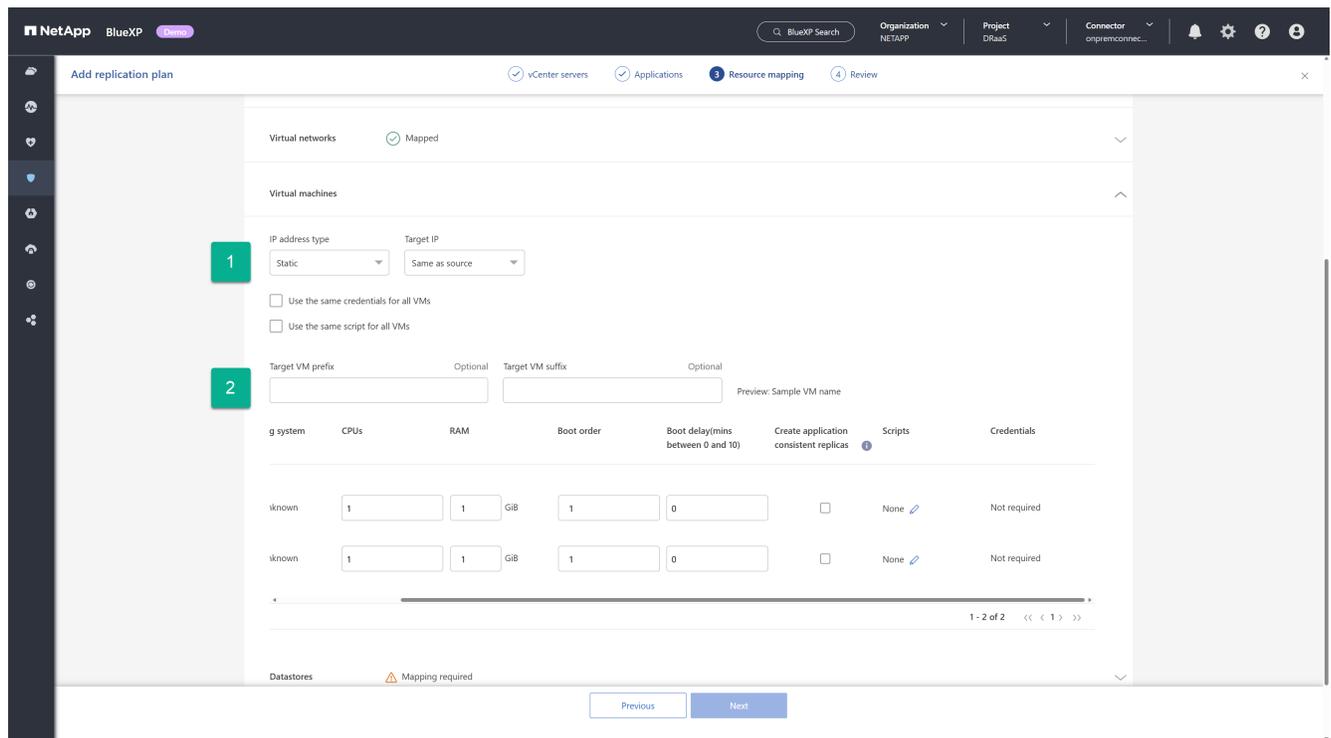
- **Mappage de sous-réseau** : cette option reconfigure l'adresse IP de chaque machine virtuelle en fonction de la configuration CIDR du réseau virtuel de destination. Pour utiliser cette fonctionnalité, assurez-vous que chaque réseau virtuel vCenter dispose d'un paramètre CIDR défini au sein du service,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

Après avoir configuré les sous-réseaux, le mappage de sous-réseaux utilise le même composant d'unité de l'adresse IP pour la configuration des machines virtuelles 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 des machines virtuelles. La reprise après sinistre BlueXP prend en charge la modification du nombre de processeurs virtuels, de la quantité de DRAM virtuelle et du nom de la machine virtuelle.

Spécifiez 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 vCenter de reprise après sinistre ne disposent pas d'autant de cœurs de processeur que le cluster vCenter source.

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

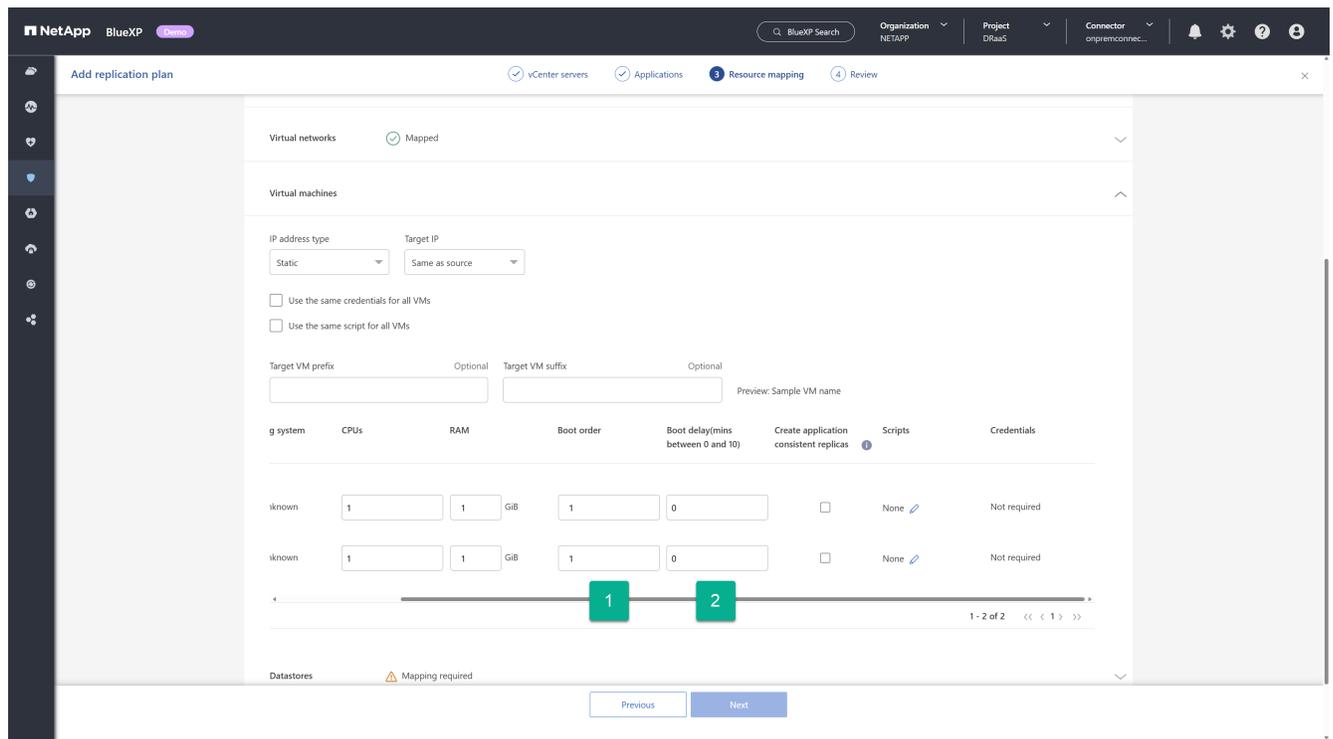
The screenshot shows the 'Add replication plan' wizard in NetApp BlueXP. The 'Resource mapping' step is selected, displaying a table of virtual machines. The table has columns for 'g system', 'CPUs', 'RAM', 'Boot order', 'Boot delay (mins between 0 and 10)', 'Create application consistent replicas', 'Scripts', and 'Credentials'. Two rows are shown, both with '1' in the 'Boot order' column and '0' in the 'Boot delay' column. The 'RAM' column shows '1 GiB'. Below the table, there are 'Previous' and 'Next' buttons. A 'Mapping required' warning is visible at the bottom left.

Ordre de démarrage

La reprise après sinistre BlueXP prend en charge le redémarrage ordonné des machines virtuelles selon un champ d'ordre de démarrage. Ce champ indique le mode de démarrage des machines virtuelles de chaque groupe de ressources. Les machines virtuelles dont le champ d'ordre de démarrage contient la même valeur démarrent en parallèle.

Modifier les paramètres de l'ordre de démarrage

- (Facultatif) Modifiez l'ordre de redémarrage de vos machines virtuelles. Ce champ prend n'importe quelle valeur numérique. La reprise après sinistre BlueXP tente de redémarrer en parallèle les machines virtuelles ayant la même valeur numérique.
- (Facultatif) Indiquez un délai à utiliser entre chaque redémarrage de machine virtuelle. Ce délai est injecté après le redémarrage de cette machine virtuelle et avant celui des machines virtuelles dont le numéro d'ordre de démarrage est supérieur. Ce délai est exprimé en minutes.



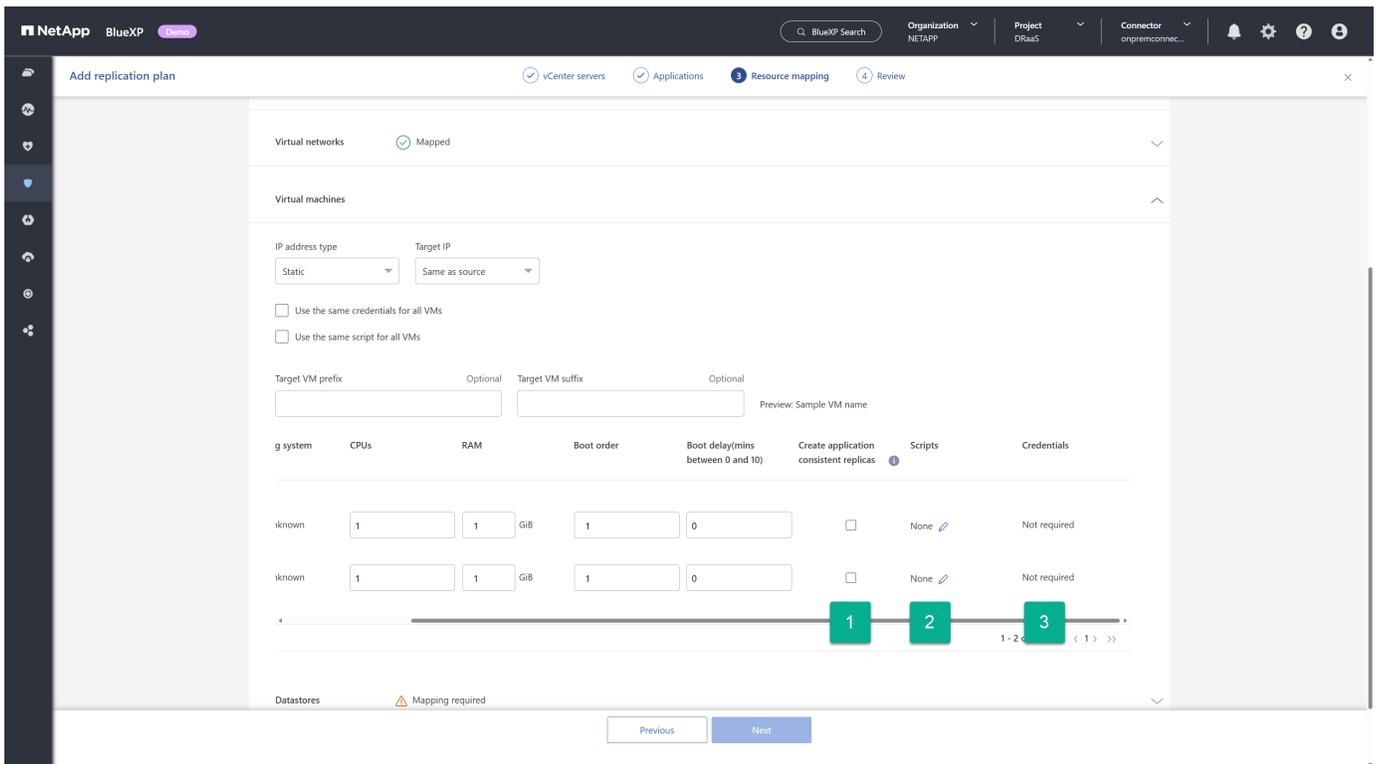
Opérations personnalisées du système d'exploitation invité

La récupération après sinistre BlueXP prend en charge l'exécution de certaines opérations du système d'exploitation invité pour chaque machine virtuelle :

- La récupération après sinistre BlueXP peut effectuer des sauvegardes cohérentes avec les applications des machines virtuelles pour les machines virtuelles exécutant des bases de données Oracle et des bases de données Microsoft SQL Server.
- La solution de reprise après sinistre BlueXP peut exécuter des scripts personnalisés adaptés au système d'exploitation invité de chaque machine virtuelle. L'exécution de ces scripts nécessite des identifiants utilisateur compatibles avec le système d'exploitation invité, avec des privilèges suffisants pour exécuter les opérations listées 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 l'application** si la machine virtuelle héberge une base de données Oracle ou SQL Server.
2. (Facultatif) Pour exécuter des actions personnalisées sur le système d'exploitation invité lors du démarrage, téléchargez un script pour chaque machine virtuelle. Pour exécuter un script unique sur toutes les machines virtuelles, cochez la case en surbrillance et renseignez les champs.
3. Certaines modifications de configuration nécessitent des identifiants utilisateur disposant des autorisations adéquates pour effectuer les opérations. Fournissez vos identifiants 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 de réplication des volumes ONTAP hébergés par chaque banque de données vCenter.

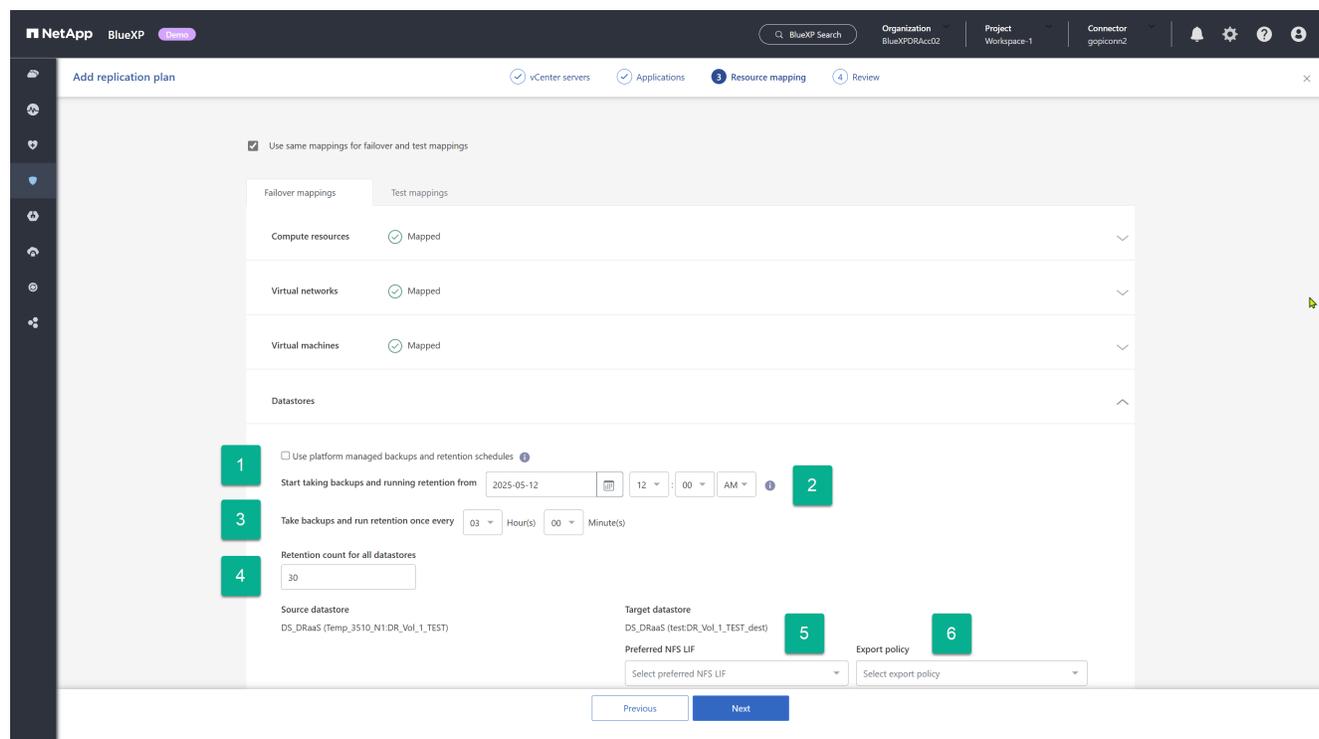
Par défaut, la récupération après sinistre BlueXP gère sa propre planification de réplication de snapshots ; toutefois, vous pouvez éventuellement spécifier que vous souhaitez utiliser la planification de stratégie de réplication SnapMirror existante pour la protection de la banque de données.

De plus, vous pouvez personnaliser les interfaces logiques (LIF) de données et la stratégie d'exportation à utiliser. Si vous ne spécifiez pas ces paramètres, la reprise après sinistre BlueXP utilise toutes les interfaces logiques de données associées au protocole approprié (NFS, iSCSI ou FC) et la stratégie d'exportation par défaut pour les volumes NFS.

Pour configurer le mappage du magasin de données (volume)

1. (Facultatif) Décidez si vous souhaitez utiliser une planification de réplication ONTAP SnapMirror existante ou si vous souhaitez que la récupération après sinistre BlueXP gère 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 les clusters de stockage source et de destination.
5. (Facultatif) Sélectionnez une interface logique par défaut (LIF de données) pour chaque volume. Si aucune n'est sélectionnée, toutes les LIF de données de la SVM de destination prenant en charge le protocole d'accès au volume sont configurées.
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 de récupération après sinistre BlueXP

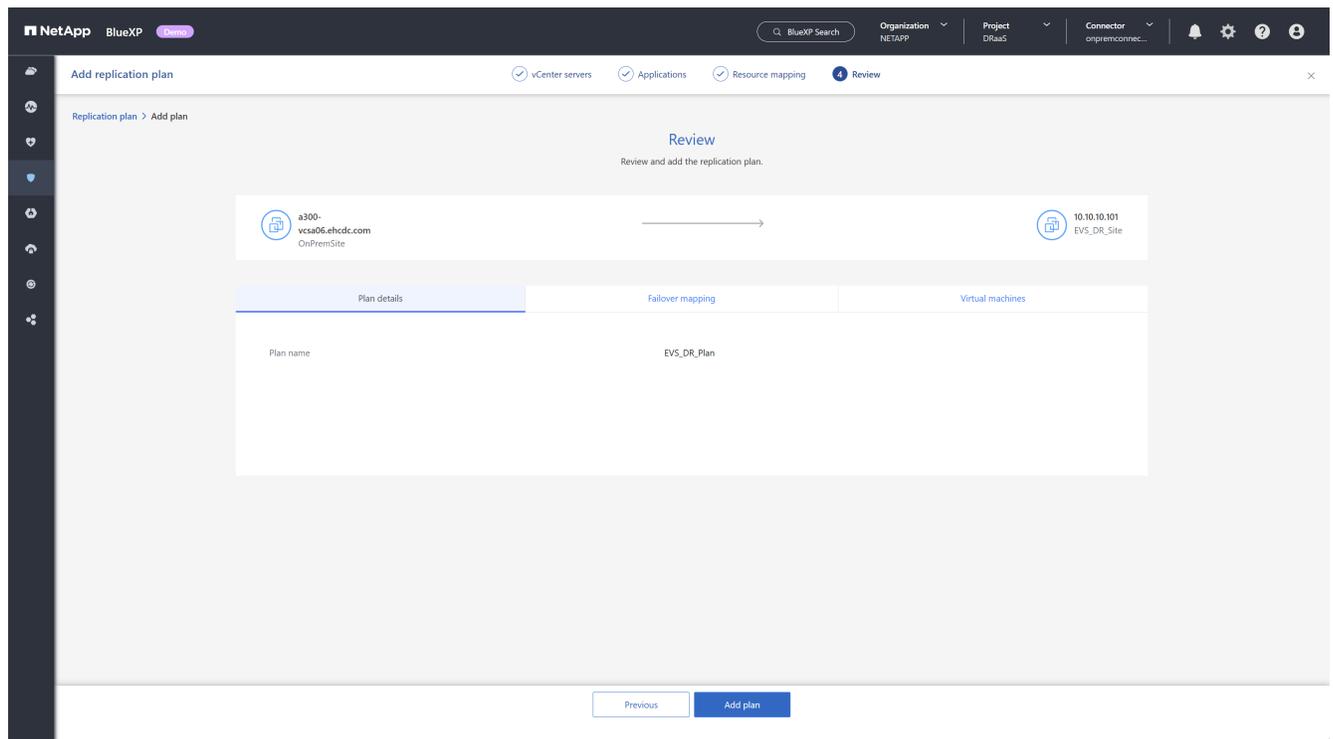
Après avoir ajouté les informations du plan de réplication dans la récupération après sinistre BlueXP, vérifiez que les informations que vous avez saisies sont correctes.

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



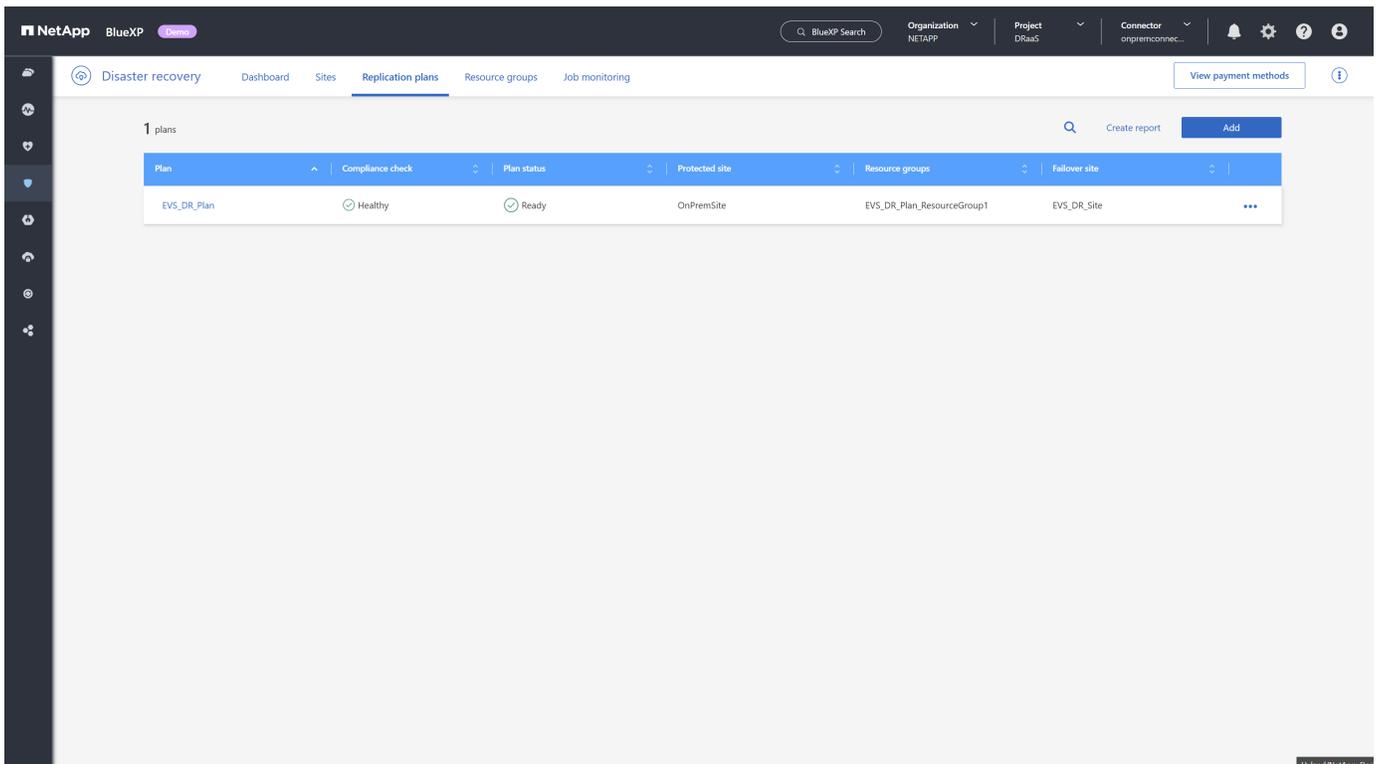
2. Lorsque vous êtes satisfait que tous les paramètres sont corrects, sélectionnez **Ajouter un plan** en bas de l'écran.

Continuer avec "[Vérifier le plan de réplication](#)".

Vérifiez que tout fonctionne dans la récupération après sinistre BlueXP

Après avoir ajouté le plan de réplication à la reprise après sinistre BlueXP, vous revenez à la page Plans de réplication où vous pouvez consulter vos plans de réplication et leur état. Vérifiez que le plan de réplication est à l'état « Sain ». Dans le cas contraire, vérifiez son état et corrigez les problèmes avant de continuer.

Figure : Page des plans de réplication



La reprise après sinistre BlueXP effectue une série de tests pour vérifier que tous les composants (cluster ONTAP, clusters vCenter et machines virtuelles) sont accessibles et en bon état pour que le service puisse protéger les machines virtuelles. Ce contrôle de conformité 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 la reprise après sinistre BlueXP

Utilisez la récupération après sinistre BlueXP avec Amazon EVS et Amazon FSx pour 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.

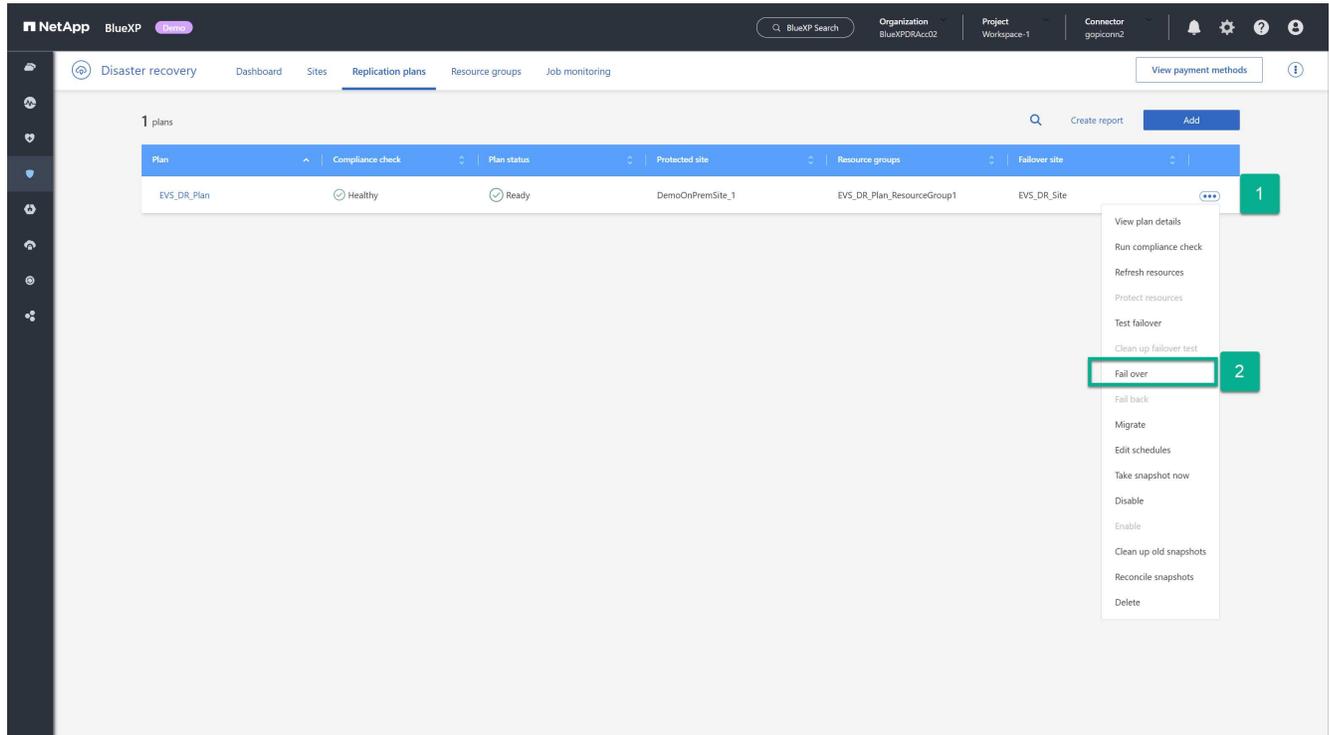
Le basculement est un processus lancé manuellement.

Étapes pour accéder à l'opération de basculement

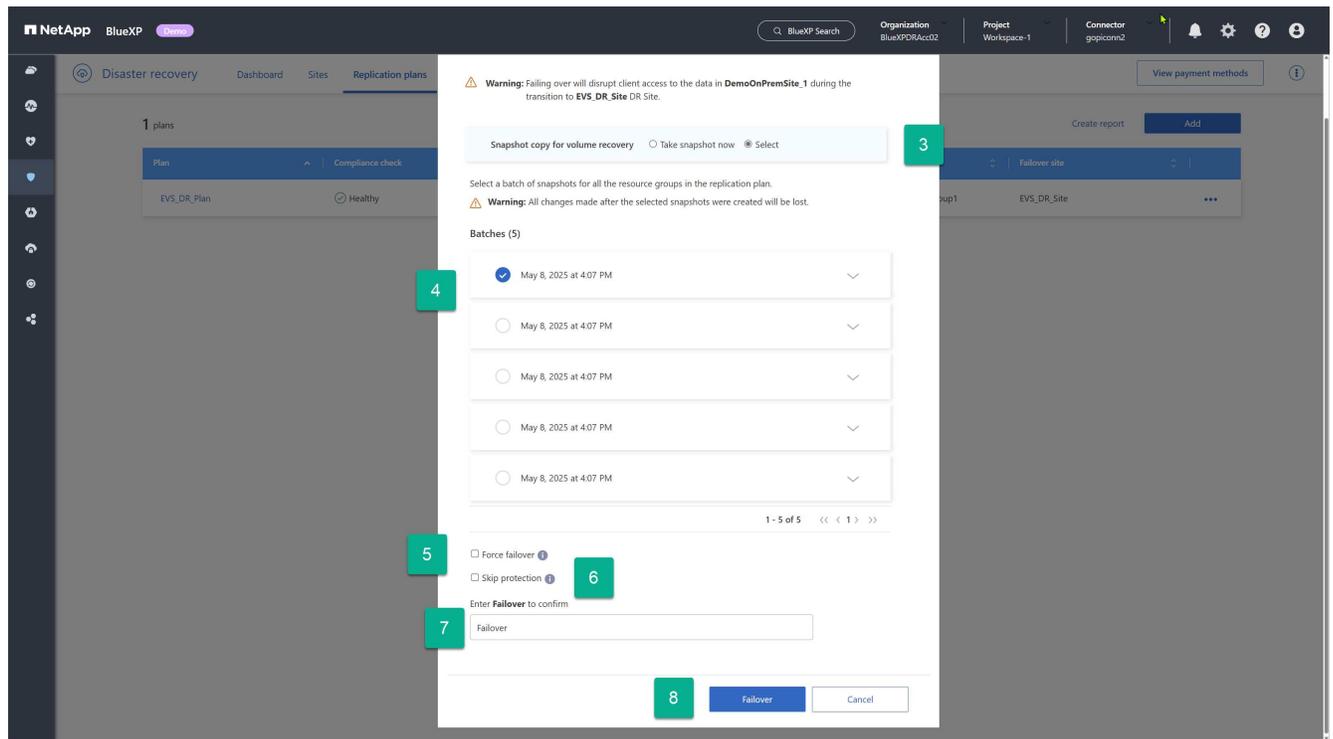
1. Dans la navigation de gauche de BlueXP, sélectionnez **Protection > Reprise après sinistre**.
2. Dans le menu de récupération après sinistre BlueXP, sélectionnez **Plans de réplication**.

Étapes pour effectuer un basculement

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



3. Si le site de production (protégé) n'est pas accessible, sélectionnez un snapshot précédemment créé comme image de récupération. Pour cela, sélectionnez **Sélectionner**.
4. Sélectionnez la sauvegarde à utiliser pour la récupération.
5. (Facultatif) Indiquez si vous souhaitez que la reprise après sinistre BlueXP force le basculement, quel que soit l'état du plan de réplication. Cette option ne doit être utilisée qu'en dernier recours.
6. (Facultatif) Sélectionnez si vous souhaitez que la récupération après sinistre BlueXP 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 **Basculement**.



Tester le basculement

Un basculement de test est similaire à un basculement, à deux différences près.

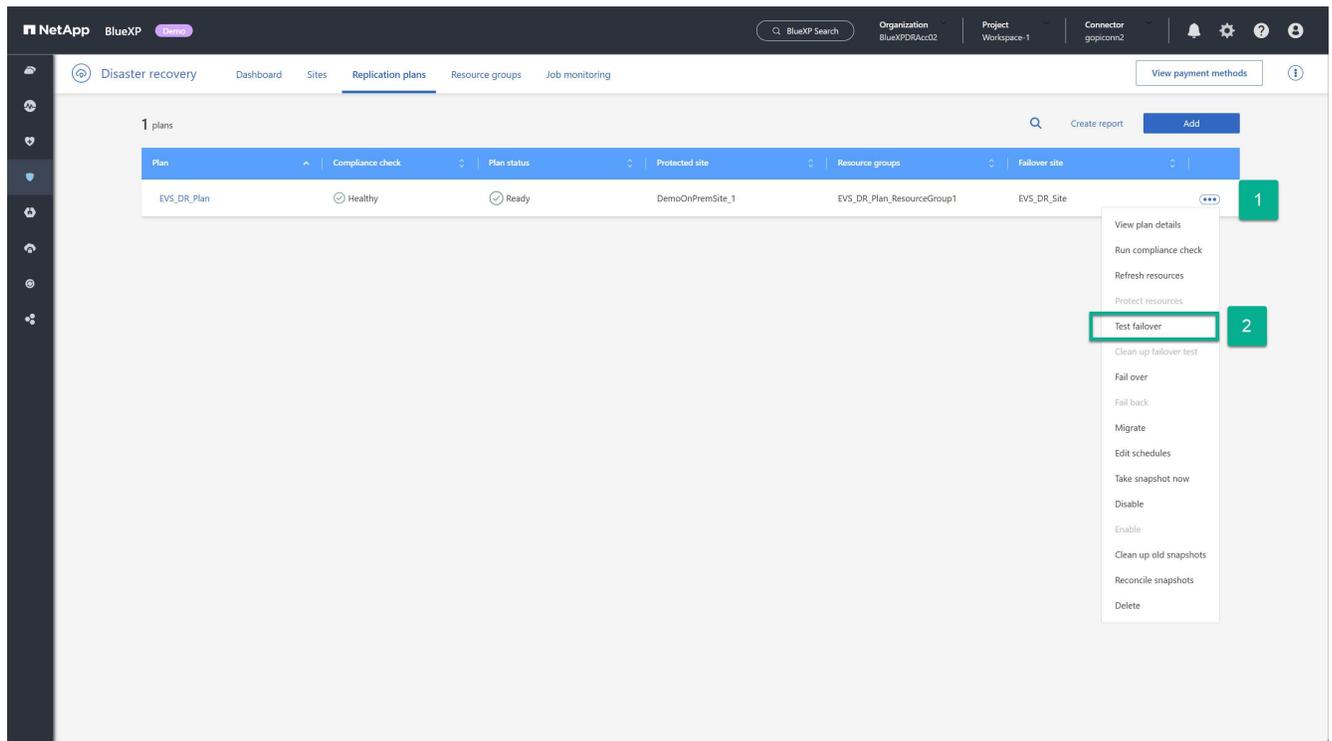
- Le site de production est toujours actif et toutes les machines virtuelles fonctionnent toujours comme prévu.
- La protection de reprise après sinistre BlueXP des machines virtuelles de production se poursuit.

Ceci est réalisé en utilisant des volumes FlexClone ONTAP natifs sur le site de destination. Pour en savoir plus sur le test de basculement, consultez la section "[Basculer des applications vers un site distant | Documentation NetApp](#)".

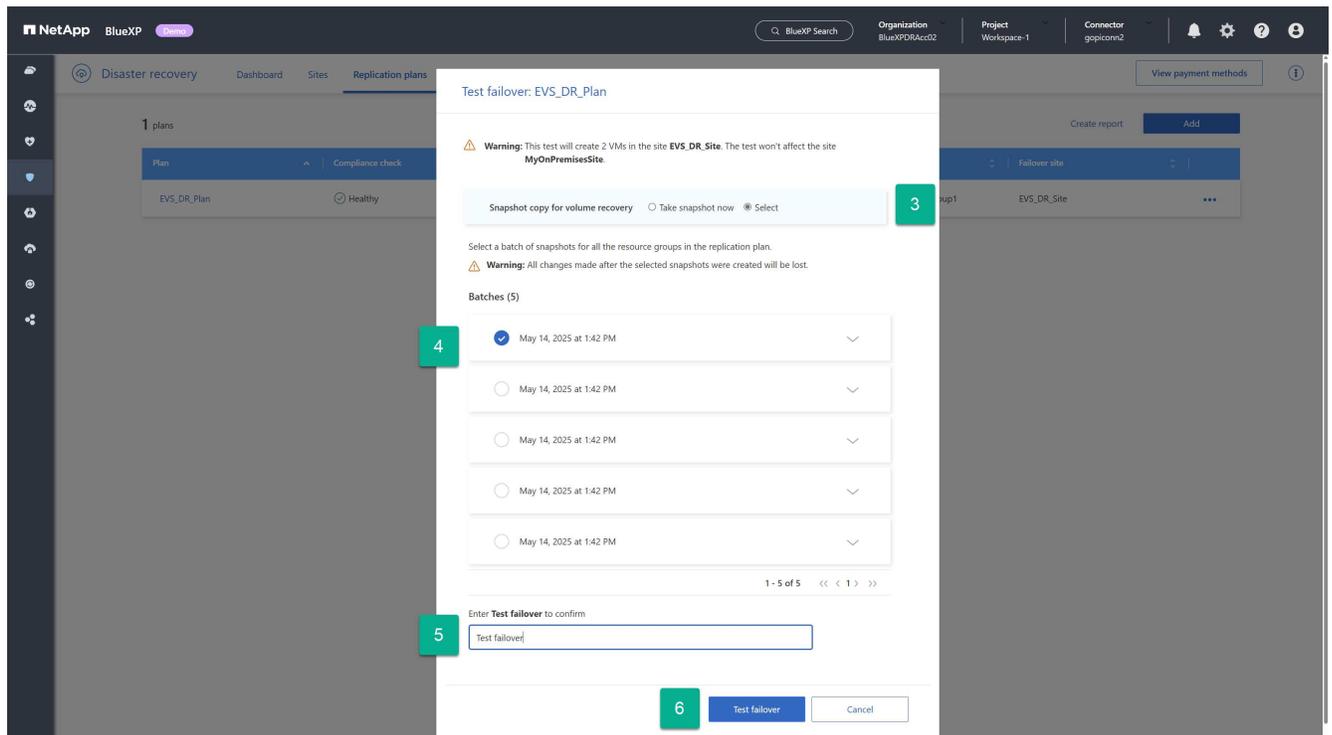
Les étapes d'exécution d'un basculement de test sont identiques à celles utilisées pour exécuter un basculement réel, sauf que vous utilisez l'opération de basculement de test dans le menu contextuel du plan de réplication.

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 créée précédemment (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 **Test failover**.

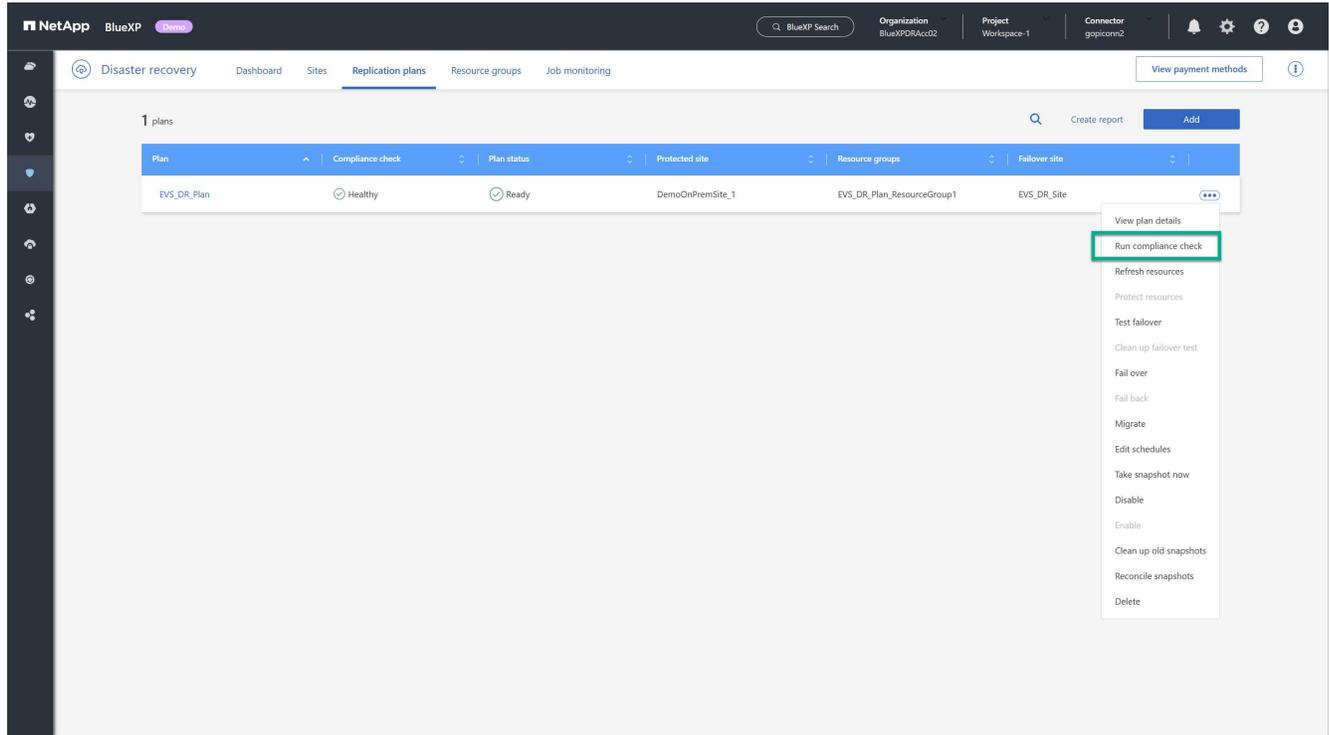


Effectuer un contrôle de conformité

Les contrôles de conformité sont exécutés toutes les trois heures par défaut. Vous pouvez effectuer un contrôle de conformité manuellement à tout moment.

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 :



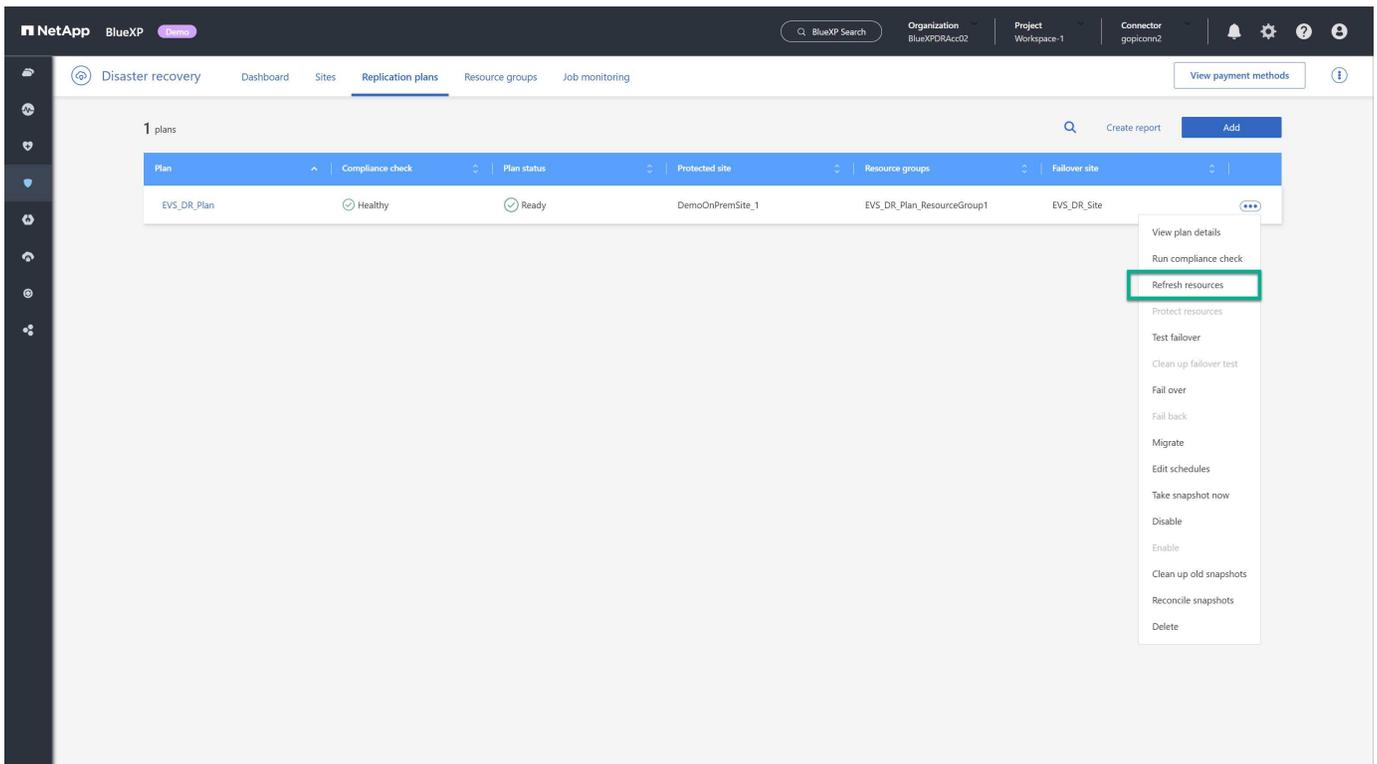
3. Pour modifier la fréquence à laquelle la récupération après sinistre BlueXP exécute automatiquement les contrôles de conformité, sélectionnez l'option **Modifier les planifications** dans le menu Actions du plan de réplication.

Actualiser les ressources

Chaque fois que vous apportez des modifications à votre infrastructure virtuelle (ajout ou suppression de machines virtuelles, ajout ou suppression de banques de données, ou déplacement de machines virtuelles entre banques de données), vous devez actualiser les clusters vCenter concernés dans le service de reprise après sinistre BlueXP. Par défaut, le service effectue cette actualisation automatiquement toutes les 24 heures, mais une actualisation manuelle garantit que les informations les plus récentes sur l'infrastructure virtuelle sont disponibles et prises en compte pour la protection après sinistre.

Il existe deux cas où une actualisation est nécessaire :

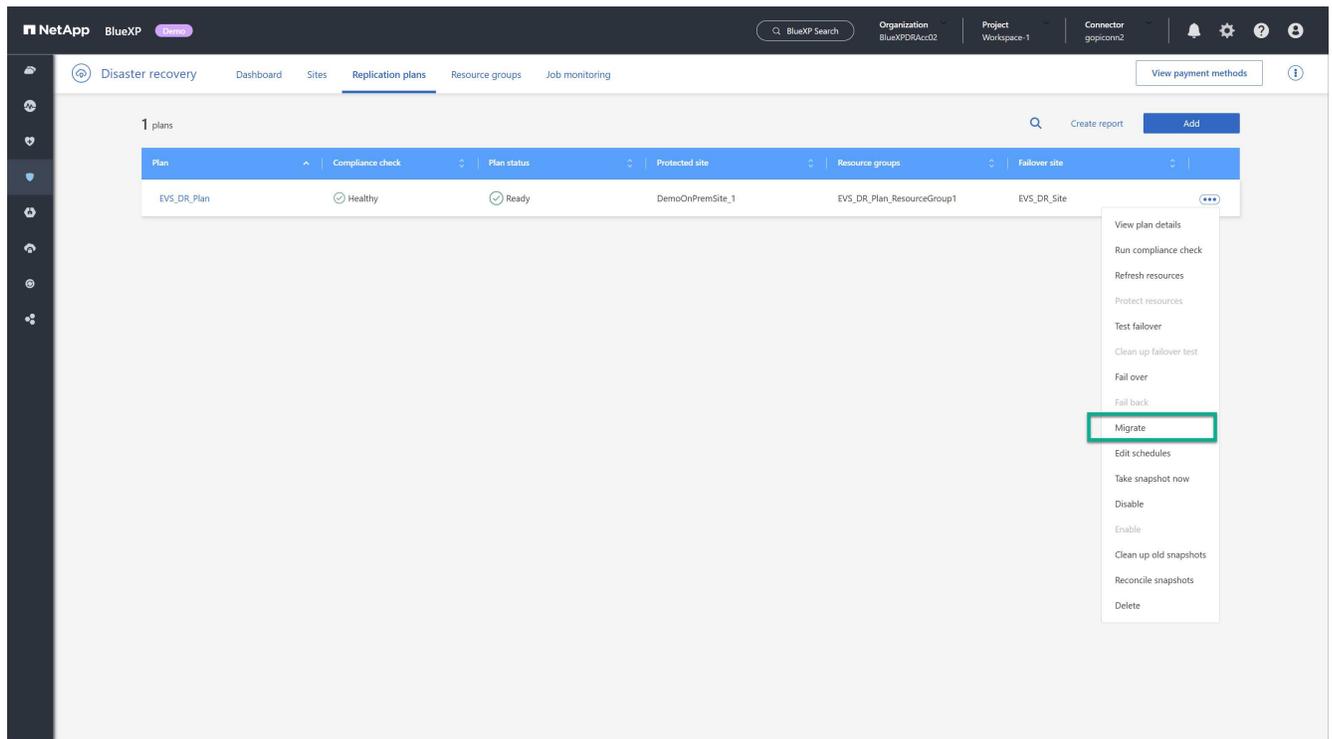
- Actualisation de vCenter : effectuez une actualisation de vCenter à chaque fois que des machines virtuelles sont ajoutées, supprimées ou déplacées hors d'un cluster vCenter :
- Actualisation du plan de réplication : effectuez une actualisation du plan de réplication à chaque fois qu'une machine virtuelle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



Migrer

Bien que la solution de reprise après sinistre BlueXP soit principalement utilisée pour les cas d'utilisation de reprise après sinistre, elle permet également de déplacer ponctuellement un ensemble de machines virtuelles du site source vers le site de destination. Cela peut être le cas pour un projet de migration concertée vers le cloud ou pour éviter des sinistres, tels que des intempéries, des conflits politiques ou d'autres événements catastrophiques temporaires.

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 :

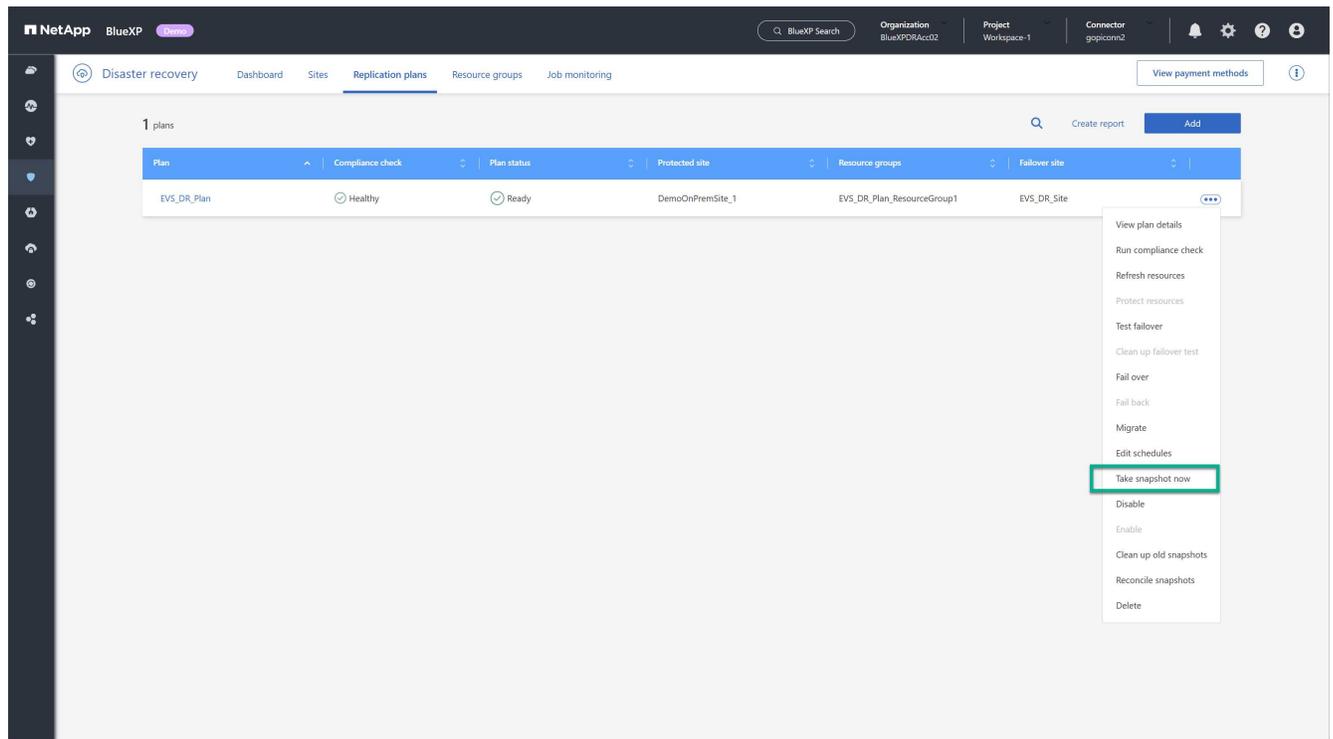


3. Saisissez les informations dans la boîte de dialogue Migrer.

Prenez un instantané maintenant

À tout moment, vous pouvez prendre un instantané du plan de réplication. Cet instantané est inclus dans les considérations de reprise après sinistre BlueXP 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 :

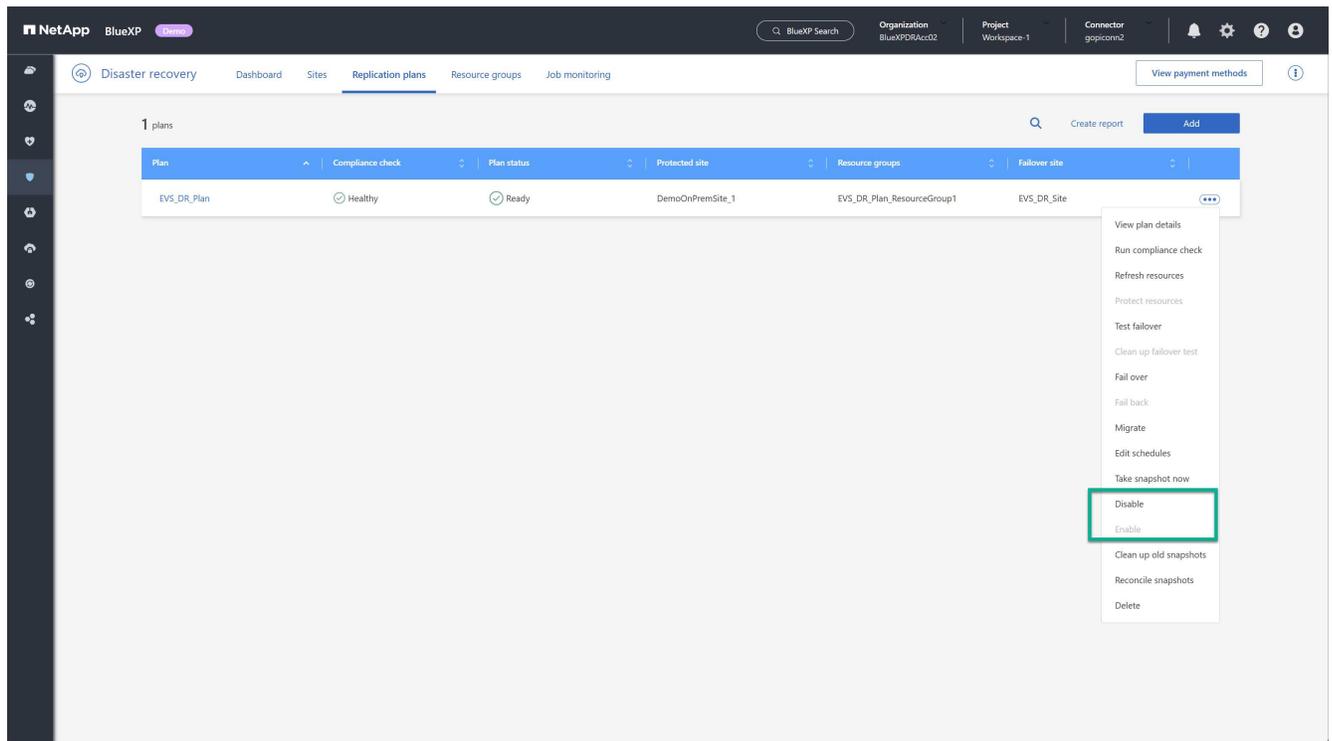


Désactiver ou activer le plan de réplication

Vous devrez peut-être interrompre temporairement le plan de réplication pour effectuer une opération ou une maintenance susceptible d'impacter 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.

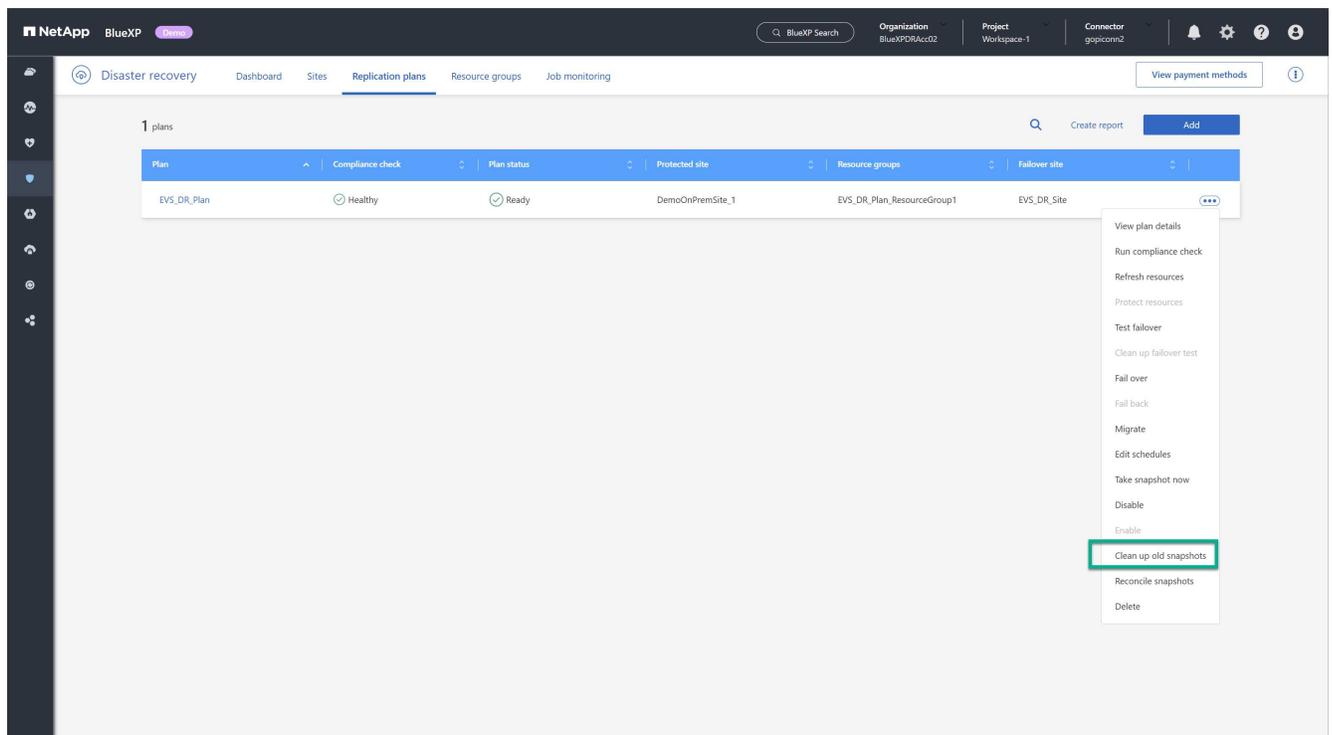
Lorsque le plan de réplication est actif, la commande **Activer** est grisée. Lorsqu'il est désactivé, la commande **Désactiver** est grisée.



Nettoyez les anciens snapshots

Vous souhaitez peut-être nettoyer les anciens snapshots conservés sur les sites source et de destination. Cela peut se produire si le nombre de snapshots conservés dans le plan de réplication est modifié.

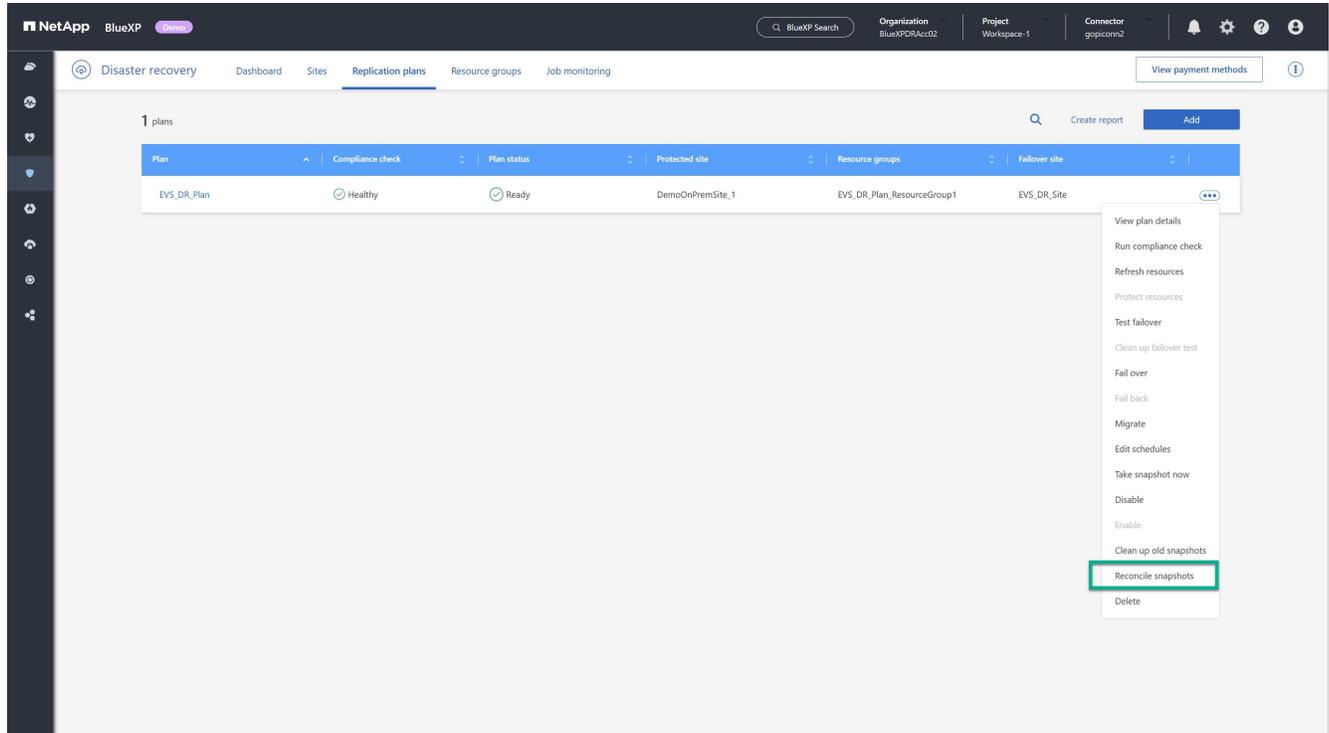
1. Sélectionnez l'option **Actions** **...** à côté du plan de réplication.
2. Pour supprimer manuellement ces anciens instantanés, sélectionnez **Nettoyer les anciens instantanés** dans le menu Actions du plan de réplication.



Réconcilier les instantanés

Étant donné que le service orchestre les snapshots de volumes ONTAP, un administrateur de stockage ONTAP peut supprimer directement ces snapshots à l'aide d'ONTAP System Manager, de l'interface de ligne de commande ONTAP ou des API REST ONTAP, sans que le service en soit informé. Le service supprime automatiquement, toutes les 24 heures, tous les snapshots du cluster source qui ne se trouvent pas sur le cluster de destination. Cependant, vous pouvez effectuer cette opération à la demande. Cette fonction vous permet de vous assurer que les snapshots sont cohérents sur tous les sites.

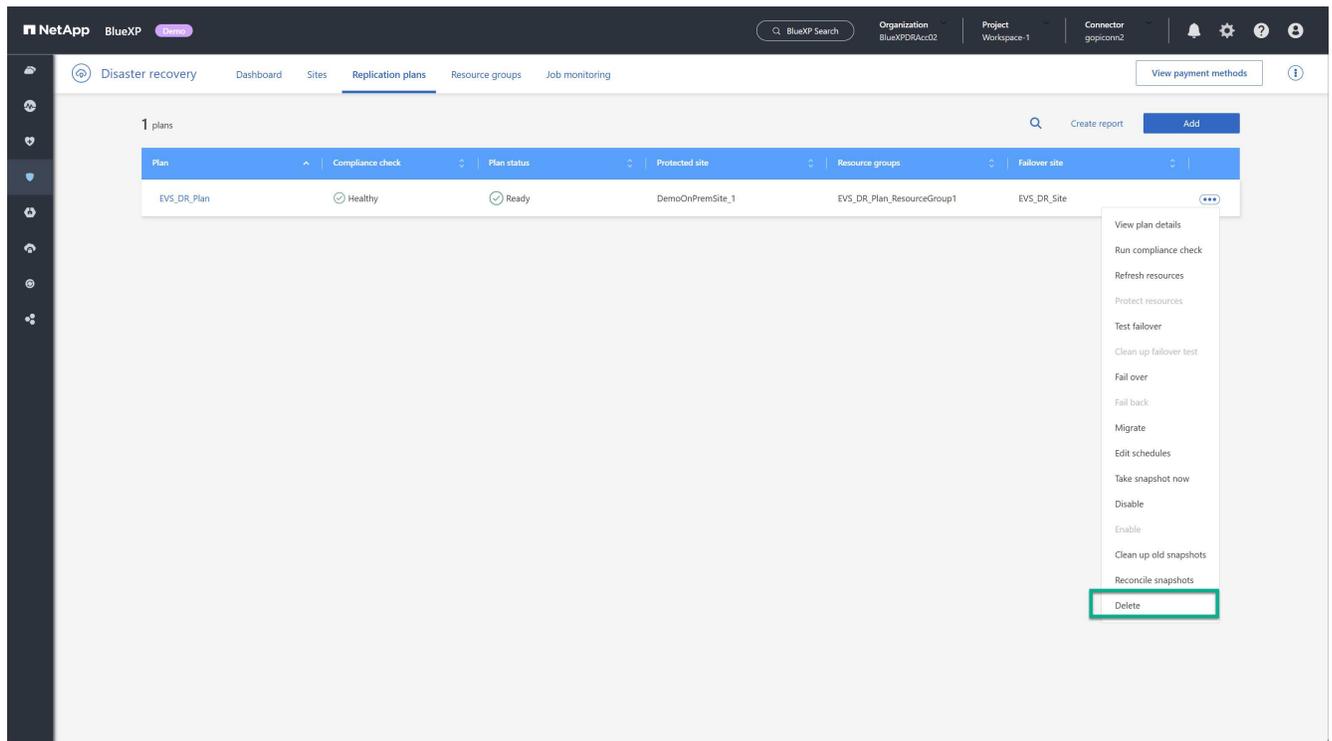
1. Sélectionnez l'option **Actions** ... à côté du plan de réplication.
2. Pour supprimer les snapshots du cluster source qui n'existent pas sur le cluster de destination, sélectionnez **Réconcilier les snapshots** dans le menu Actions du plan de réplication.



Supprimer le plan de réplication

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

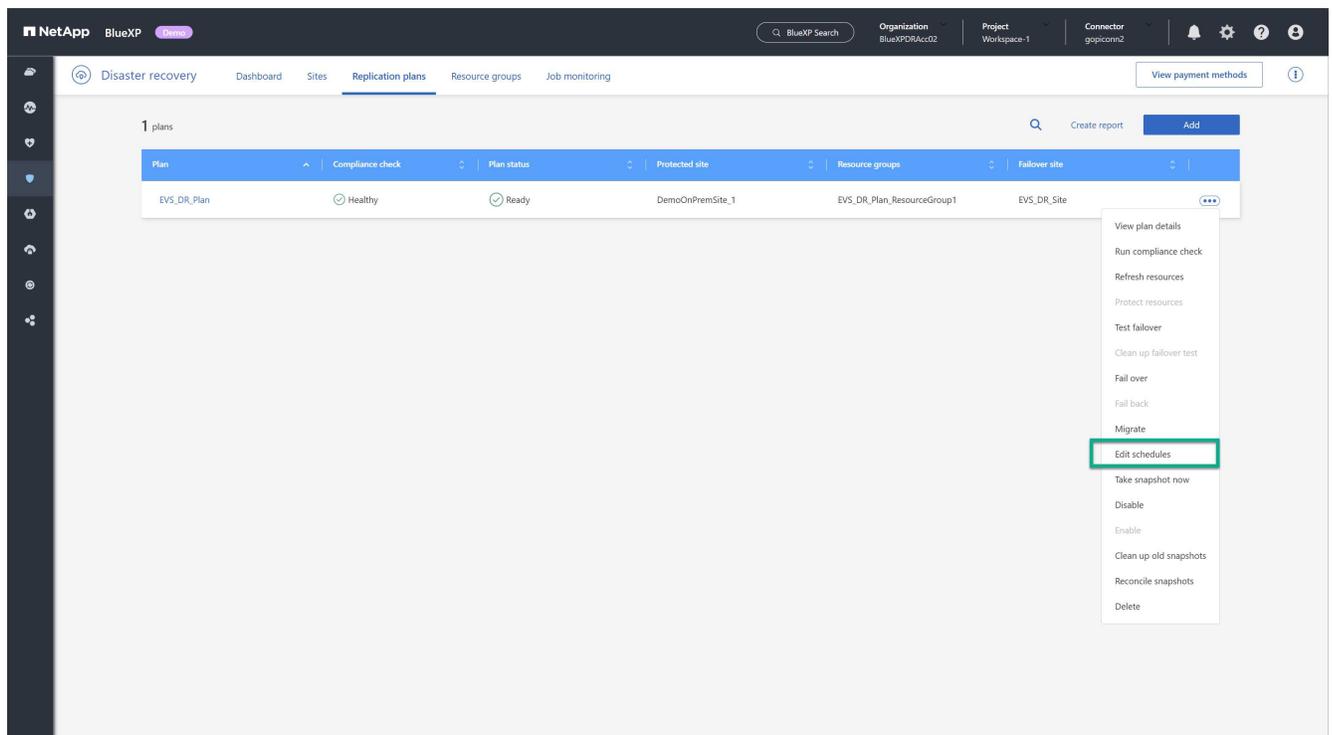
1. Sélectionnez l'option **Actions** ... à côté du plan de réplication.
2. Pour supprimer le plan de réplication, sélectionnez **Supprimer** dans le menu contextuel du plan de réplication.



Modifier les horaires

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

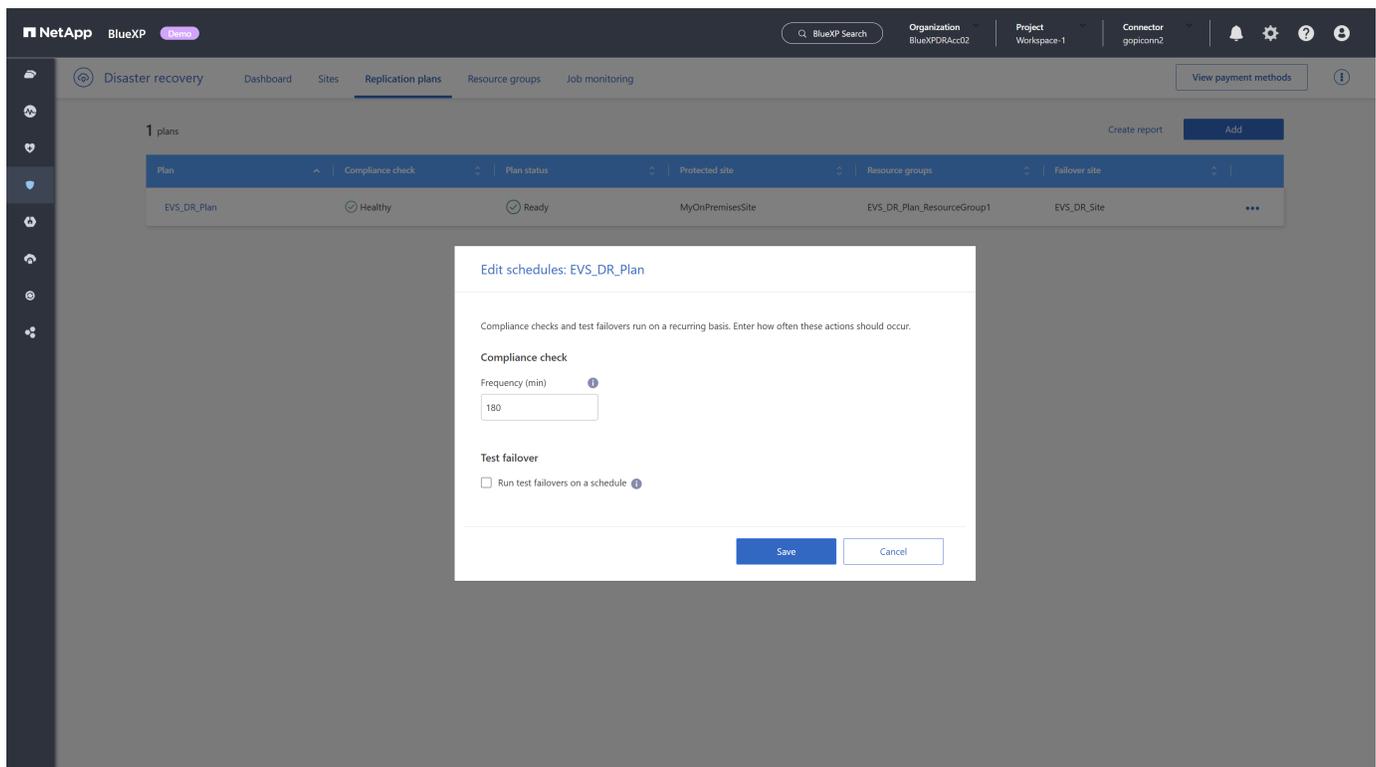
1. Sélectionnez l'option **Actions** **...** à côté du plan de réplication.
2. Pour modifier ces planifications pour l'une de ces deux opérations, sélectionnez **Modifier les planifications** pour le plan de réplication.



Modifier l'intervalle de vérification de la conformité

Par défaut, les contrôles de conformité sont effectués toutes les trois heures. Vous pouvez modifier cet intervalle 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 automatisés, ce qui garantit le bon fonctionnement de vos plans de réplication. Pour en savoir plus sur le processus de basculement de test, consultez la section "[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.

The screenshot displays the NetApp BlueXP interface for editing disaster recovery schedules. A modal window titled "Edit schedules: EVS_DR_Plan" is open, showing configuration options for a replication plan. The background shows a list of plans with "EVS_DR_Plan" selected and a "Healthy" status. The modal window includes the following sections and fields:

- Compliance check:** A text prompt states "Compliance checks and test failovers run on a recurring basis. Enter how often these actions should occur." Below this is a "Frequency (min)" input field set to "180".
- Test failover:** A section with a checked checkbox "Run test failovers on a schedule" and an unchecked checkbox "Use on-demand snapshot for scheduled test failover".
- Repeat:** A dropdown menu set to "Weekly".
- Day of the week:** A dropdown menu set to "Saturday".
- Time and Date:** Fields for "Hour" (02), "Minute" (00), "AM/PM" (AM), and "Start date" (2025-05-15).
- Automatically cleanup:** A checked checkbox "Automatically cleanup" followed by an input field set to "10" minutes after test failover.
- Buttons:** "Save" and "Cancel" buttons at the bottom right of the modal.

Green numbered callouts (1-8) are overlaid on the interface to highlight specific elements: 1 points to the plan name, 2 to the "Run test failovers on a schedule" checkbox, 3 to the "Repeat" dropdown, 4 to the "Day of the week" dropdown, 5 to the "Hour" dropdown, 6 to the "Start date" field, 7 to the "Automatically cleanup" checkbox, and 8 to the "Save" button.

Connaissances et support

S'inscrire pour obtenir de l'aide

L'enregistrement au support est requis pour recevoir le support technique spécifique à BlueXP et à ses solutions et services de stockage. L'enregistrement au support est également requis pour activer les principaux workflows des systèmes Cloud Volumes ONTAP.

L'inscription au support n'active pas le support NetApp pour un service de fichiers de fournisseur cloud. Pour obtenir de l'aide concernant un service de fichiers d'un fournisseur cloud, son infrastructure ou toute solution utilisant le service, consultez la section « obtention d'aide » de la documentation BlueXP associée à ce produit.

- ["Amazon FSX pour ONTAP"](#)
- ["Azure NetApp Files"](#)
- ["Google Cloud NetApp Volumes"](#)

Présentation de l'inscription au support

Il existe deux types d'inscription pour activer les droits d'assistance :

- Enregistrement du numéro de série de votre compte BlueXP (votre numéro de série 960xxxxxxxxx à 20 chiffres, disponible sur la page des ressources de support de BlueXP).

Il sert d'ID d'abonnement unique pour tous les services de BlueXP. Chaque abonnement au support BlueXP au niveau du compte doit être enregistré.

- Enregistrement des numéros de série Cloud Volumes ONTAP associés à un abonnement sur le marché de votre fournisseur cloud (numéros de série à 20 chiffres 909201xxxxxxxx).

Ces numéros de série sont généralement appelés *PAYGO - numéros de série* et sont générés par BlueXP au moment du déploiement de Cloud Volumes ONTAP.

L'enregistrement des deux types de numéros de série offre des fonctionnalités telles que l'ouverture de tickets de support et la génération automatique de tickets. L'inscription est terminée en ajoutant des comptes du site de support NetApp (NSS) à BlueXP, comme décrit ci-dessous.

Enregistrez BlueXP pour bénéficier du support NetApp

Pour vous inscrire au support et activer votre droit de support, un utilisateur de votre entreprise (ou compte) BlueXP doit associer un compte du site de support NetApp à ses identifiants BlueXP . Le fait de vous inscrire au support NetApp dépend de la présence ou non d'un compte sur le site de support NetApp (NSS).

Client existant avec un compte NSS

Si vous êtes client NetApp avec un compte NSS, il vous suffit de vous inscrire pour obtenir du support dans BlueXP.

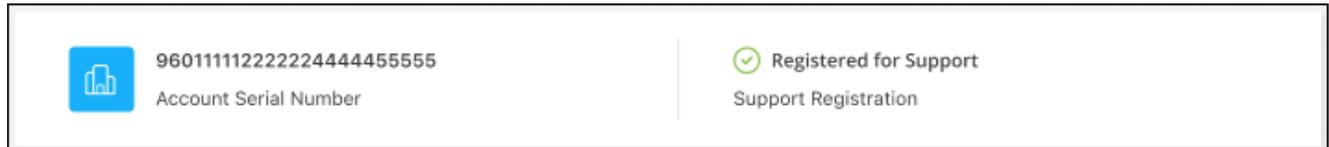
Étapes

1. Dans le coin supérieur droit de la console BlueXP, sélectionnez l'icône Paramètres, puis sélectionnez

informations d'identification.

2. Sélectionnez **informations d'identification utilisateur**.
3. Sélectionnez **Ajouter des informations d'identification NSS** et suivez l'invite authentification du site de support NetApp (NSS).
4. Pour confirmer que le processus d'enregistrement a réussi, sélectionnez l'icône aide et sélectionnez **support**.

La page **Ressources** doit indiquer que votre organisation BlueXP est enregistrée pour le support.



Notez que les autres utilisateurs BlueXP ne verront pas ce même statut d'enregistrement de support s'ils n'ont pas associé de compte sur le site de support NetApp à leur identifiant BlueXP. Cependant, cela ne signifie pas que votre entreprise BlueXP n'est pas enregistrée pour le support. Tant qu'un utilisateur de l'organisation a suivi ces étapes, votre organisation a été enregistrée.

Client existant mais aucun compte NSS

Si vous possédez déjà des licences et des numéros de série NetApp, mais que vous possédez un compte NSS, vous devez créer un compte NSS et l'associer à votre connexion BlueXP.

Étapes

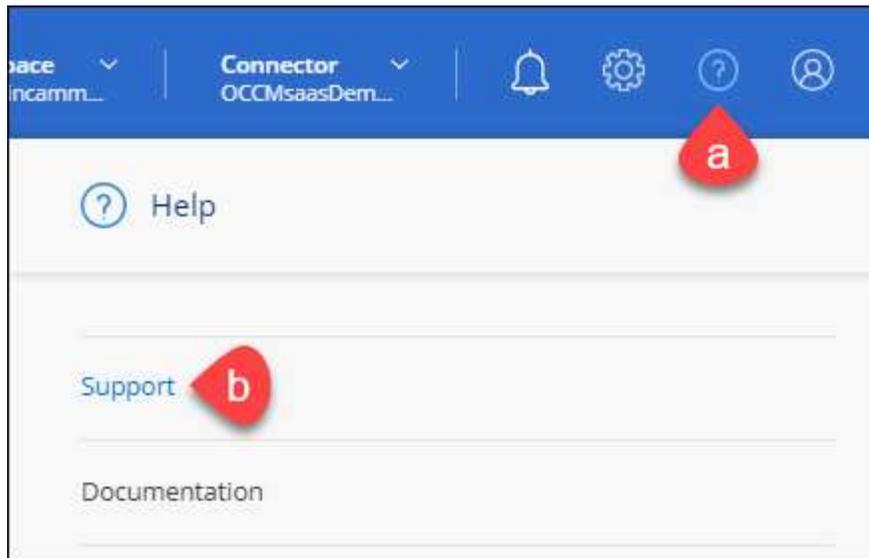
1. Créez un compte sur le site de support NetApp en complétant le "[Formulaire d'inscription de l'utilisateur du site de support NetApp](#)"
 - a. Veillez à sélectionner le niveau d'utilisateur approprié, qui est généralement **client/utilisateur final NetApp**.
 - b. Veillez à copier le numéro de série du compte BlueXP (960xxxx) utilisé ci-dessus pour le champ Numéro de série. Le traitement du compte sera ainsi accéléré.
2. Associez votre nouveau compte NSS à votre connexion BlueXP en suivant les étapes décrites sous [Client existant avec un compte NSS](#).

Découvrez la toute nouvelle gamme NetApp

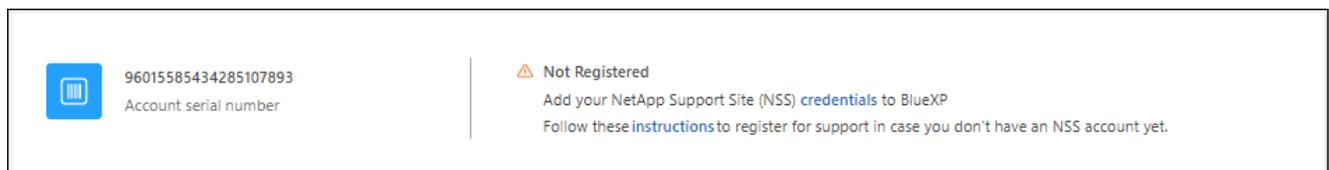
Si vous êtes nouveau chez NetApp et que vous ne disposez pas d'un compte NSS, effectuez chacune des étapes ci-dessous.

Étapes

1. Dans le coin supérieur droit de la console BlueXP, sélectionnez l'icône aide, puis sélectionnez **support**.



2. Recherchez le numéro de série de l'ID de compte sur la page d'inscription au support.



3. Accédez à "[Site d'inscription au support 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 **Product Line**, sélectionnez **Cloud Manager**, puis votre fournisseur de facturation applicable.
6. Copiez le numéro de série de votre compte à l'étape 2 ci-dessus, vérifiez sa sécurité, puis lisez la Déclaration de confidentialité des données NetApp.

Un e-mail est immédiatement envoyé à la boîte aux lettres fournie pour finaliser cette transaction sécurisée. Assurez-vous de vérifier vos dossiers de courrier indésirable si l'e-mail de validation n'arrive pas dans quelques minutes.

7. Confirmez l'action à partir de l'e-mail.

La confirmation de la soumission de 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 complétant le "[Formulaire d'inscription de l'utilisateur du site de support NetApp](#)"
 - a. Veillez à sélectionner le niveau d'utilisateur approprié, qui est généralement **client/utilisateur final NetApp**.
 - b. Veillez à copier le numéro de série du compte (960xxxx) utilisé ci-dessus pour le champ Numéro de série. Cela accélère le traitement.

Une fois que vous avez 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 possédez votre compte sur le site de support NetApp, associez-le à votre connexion BlueXP en suivant les étapes décrites sous [Client existant avec un compte NSS](#).

Associer les informations d'identification NSS pour le support Cloud Volumes ONTAP

L'association des informations d'identification du site de support NetApp à votre organisation BlueXP est nécessaire pour activer les flux de travail clés suivants pour Cloud Volumes ONTAP :

- Enregistrement des systèmes Cloud Volumes ONTAP avec paiement à l'utilisation pour bénéficier d'une assistance

Vous devez fournir votre compte NSS afin d'activer le support pour votre système et d'accéder aux ressources du support technique NetApp.

- Déploiement d'Cloud Volumes ONTAP avec modèle BYOL (Bring Your Own License)

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

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

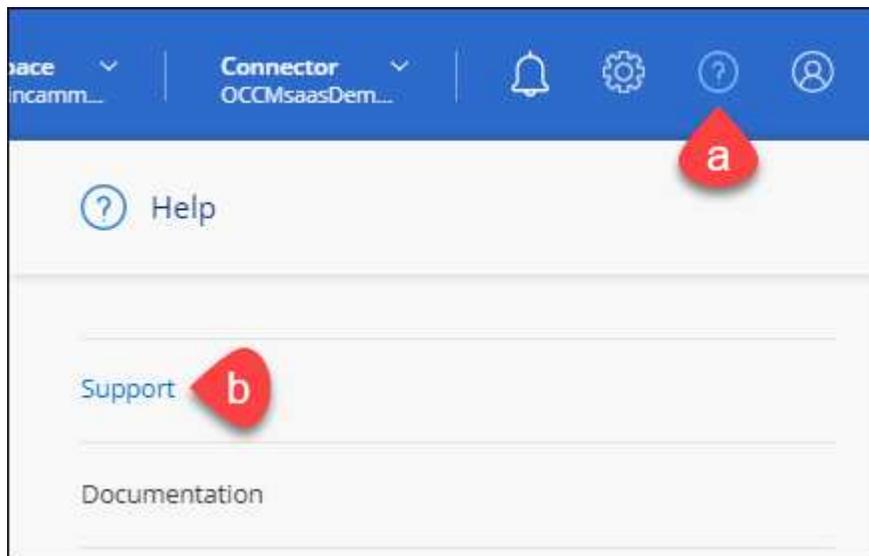
L'association des informations d'identification NSS à votre organisation BlueXP est différente du compte NSS associé à une connexion utilisateur BlueXP .

Ces informations d'identification NSS sont associées à votre identifiant d'organisation BlueXP spécifique. Les utilisateurs qui appartiennent à l'organisation BlueXP peuvent accéder à ces informations d'identification à partir de **support > gestion NSS**.

- Si vous avez un compte au niveau du client, vous pouvez ajouter un ou plusieurs comptes NSS.
- Si vous avez un compte partenaire ou revendeur, vous pouvez ajouter un ou plusieurs comptes NSS, mais ils ne peuvent pas être ajoutés en même temps que les comptes au niveau du client.

Étapes

1. Dans le coin supérieur droit de la console BlueXP, 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 à la prise en charge et à l'octroi de licences.

4. Sur la page de connexion, indiquez l'adresse e-mail et le mot de passe que vous avez enregistrés sur le site de support NetApp pour réaliser le processus d'authentification.

Ces actions permettent à BlueXP d'utiliser votre compte NSS pour des opérations telles que le téléchargement de licences, la vérification de la mise à niveau logicielle et les inscriptions de support futures.

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 de 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 de niveau client et qu'un compte de niveau partenaire existe, le message d'erreur suivant s'affiche :

"Le type de client NSS n'est pas autorisé pour ce compte car il existe déjà des utilisateurs NSS de type différent."

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

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

Il s'agit d'un ID généré par le système qui correspond à votre courrier électronique. Sur la page **NSS Management**, vous pouvez afficher votre courriel 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.

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.

Obtenez de l'aide

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

Bénéficiez du support pour les services de fichiers d'un fournisseur cloud

Pour obtenir de l'aide concernant un service de fichiers d'un fournisseur cloud, son infrastructure ou toute solution utilisant le service, consultez la section « obtention d'aide » de la documentation BlueXP associée à ce produit.

- ["Amazon FSX pour ONTAP"](#)
- ["Azure NetApp Files"](#)
- ["Google Cloud NetApp Volumes"](#)

Pour bénéficier du support technique spécifique à BlueXP et à ses solutions et services de stockage, utilisez les options de support décrites ci-dessous.

Utilisation d'options de support en libre-service

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

- Documentation

La documentation BlueXP que vous consultez actuellement.

- ["Base de connaissances"](#)

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

- ["Communautés"](#)

Rejoignez la communauté BlueXP pour suivre des discussions en cours ou en créer de nouveaux.

Créez un dossier de demande de support auprès du support NetApp

Outre les options d'auto-support mentionnées ci-dessus, vous pouvez travailler avec un spécialiste du support NetApp pour résoudre tous les problèmes après avoir activé le service de support.

Avant de commencer

- Pour utiliser la fonctionnalité **Créer un cas**, vous devez d'abord associer vos informations d'identification du site de support NetApp à votre connexion BlueXP. ["Découvrez comment gérer les identifiants associés à votre connexion BlueXP"](#).
- 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 BlueXP, 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 avec quelqu'un au téléphone. Vous serez dirigé vers une page netapp.com qui répertorie les numéros de téléphone que vous pouvez appeler.
 - b. Sélectionnez **Créer un cas** pour ouvrir un ticket avec un spécialiste du support NetApp :
 - **Service** : sélectionnez le service auquel le problème est associé. Par exemple, BlueXP lorsqu'il est spécifique à un problème de support technique avec des flux de travail ou des fonctionnalités au sein du service.
 - **Environnement de travail** : si applicable au stockage, sélectionnez **Cloud Volumes ONTAP** ou **sur site**, puis l'environnement de travail associé.

La liste des environnements de travail s'applique à l'organisation (ou au compte), au projet (ou à l'espace de travail) et au connecteur BlueXP que vous avez sélectionnés dans la bannière

supérieure du service.

- **Priorité du cas** : choisissez la priorité du cas, qui peut être faible, Moyen, élevé ou critique.

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

- **Description du problème** : fournir une description détaillée de votre problème, y compris les messages d'erreur ou les étapes de dépannage applicables que vous avez effectués.
- **Adresses e-mail supplémentaires**: Entrez 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 fichier suivantes sont prises en charge : txt, log, PDF, jpg/JPEG, rtf, doc/docx, xls/xlsx et csv.

ntapitdemo 

NetApp Support Site Account

Service Working Environment

Select Select

Case Priority 

Low - General guidance

Issue Description

Provide detailed description of problem, applicable error messages and troubleshooting steps taken.

Additional Email Addresses (Optional) 

Type here

Attachment (Optional) Upload 

No files selected 

Une fois que vous avez terminé

Une fenêtre contextuelle contenant votre numéro de dossier de support s'affiche. Un spécialiste du support NetApp va étudier votre dossier et vous recontacterons très rapidement.

Pour un historique de vos dossiers de support, vous pouvez sélectionner **Paramètres > Chronologie** et rechercher les actions nommées "Créer un dossier de support". Un bouton situé à l'extrême droite vous permet de développer l'action pour afficher les détails.

Il est possible que vous rencontriez le message d'erreur suivant lors de la création d'un dossier :

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

Cette erreur peut signifier que le compte NSS et la société d'enregistrement auquel il est associé n'est pas la même société d'enregistrement pour le numéro de série du compte BlueXP (par exemple 960xxxx) ou le numéro de série de l'environnement de travail. Vous pouvez demander de l'aide en utilisant l'une des options suivantes :

- Utilisez le chat du produit
- Soumettre un dossier non technique à <https://mysupport.netapp.com/site/help>

Gestion de vos dossiers de demande de support (aperçu)

Vous pouvez afficher et gérer les dossiers de support actifs et résolus directement à partir de BlueXP. Vous pouvez gérer les dossiers associés à votre compte NSS et à votre entreprise.

La gestion des dossiers est disponible en tant qu'aperçu. Nous prévoyons d'affiner cette expérience et d'ajouter des améliorations dans les prochaines versions. Envoyez-nous vos commentaires à l'aide de l'outil de chat In-Product.

Notez ce qui suit :

- Le tableau de bord de gestion des dossiers en haut de la page propose deux vues :
 - La vue de gauche affiche le nombre total de dossiers ouverts au cours des 3 derniers mois par le compte NSS utilisateur 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 NSS utilisateur.

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 offrent uniquement des fonctions de tri.

Pour plus d'informations, consultez les étapes ci-dessous.

- Au niveau de chaque dossier, nous offrons la possibilité de mettre à jour les notes de dossier ou de fermer un dossier qui n'est pas déjà à l'état fermé ou en attente fermée.

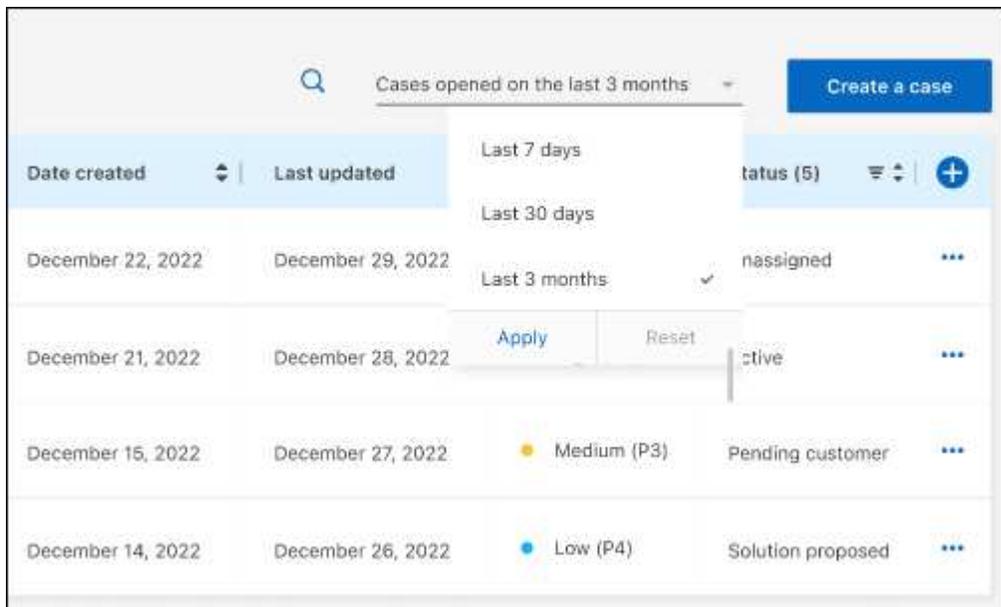
Étapes

1. Dans BlueXP, sélectionnez **aide > support**.
2. Sélectionnez **case Management** et si vous y êtes invité, ajoutez votre compte NSS à BlueXP.

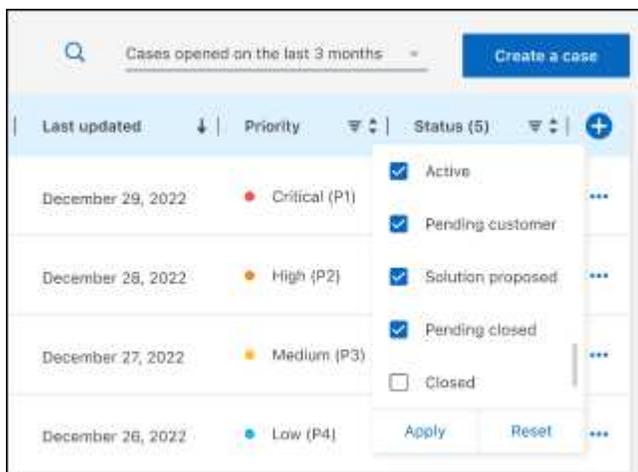
La page **gestion des cas** affiche les cas ouverts associés au compte NSS associé à votre compte utilisateur BlueXP. Il s'agit du même compte NSS qui apparaît en haut de la page **gestion NSS**.

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 société.

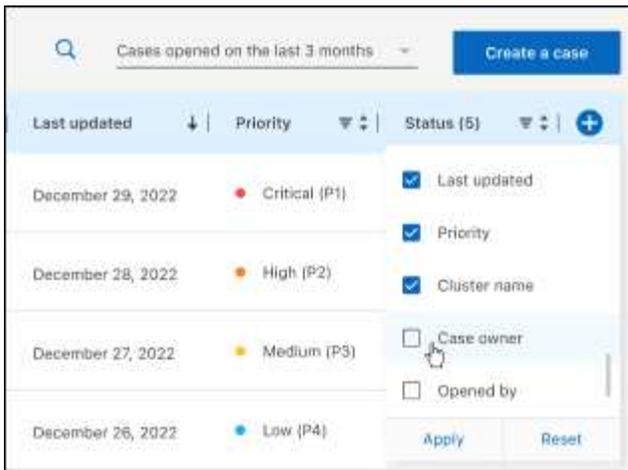
- Modifiez la plage de dates en choisissant une plage de dates exacte ou en choisissant une autre période.



- Filtrez le contenu des colonnes.



- Modifiez les colonnes qui apparaissent dans le tableau en sélectionnant  puis choisissez les colonnes que vous souhaitez afficher.

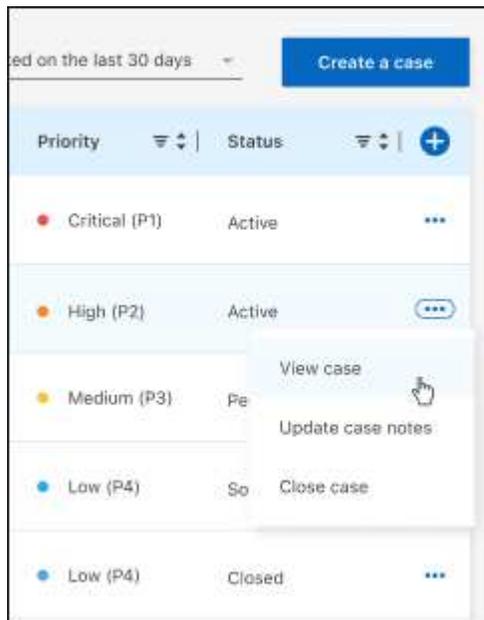


4. Gérer un dossier existant en sélectionnant **...** et en sélectionnant l'une des options disponibles :

- **Voir cas**: Afficher tous les détails sur un cas spécifique.
- **Mettre à jour les notes de cas** : fournir des détails supplémentaires sur votre problème ou sélectionner **Télécharger les fichiers** pour joindre jusqu'à cinq fichiers.

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

- **Fermer le cas** : fournissez des détails sur la raison pour laquelle vous fermez le cas et sélectionnez **Fermer le cas**.



Mentions légales

Les mentions légales donnent accès aux déclarations de copyright, aux marques, aux brevets, etc.

Droits d'auteur

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

Marques déposées

NetApp, le logo NETAPP et les marques mentionnées sur la page des marques commerciales 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/"](https://www.netapp.com/company/legal/trademarks/)

Brevets

Vous trouverez une liste actuelle des brevets appartenant à NetApp 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/"](https://www.netapp.com/company/legal/privacy-policy/)

Source ouverte

Les fichiers de notification fournissent des informations sur les droits d'auteur et les licences de tiers utilisés dans le logiciel NetApp.

["Notez la reprise d'activité BlueXP"](#)

Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

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

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

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

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

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

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

Informations sur les marques commerciales

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