Commencer

NetApp Disaster Recovery

NetApp
February 04, 2026

Sommaire

Commencer

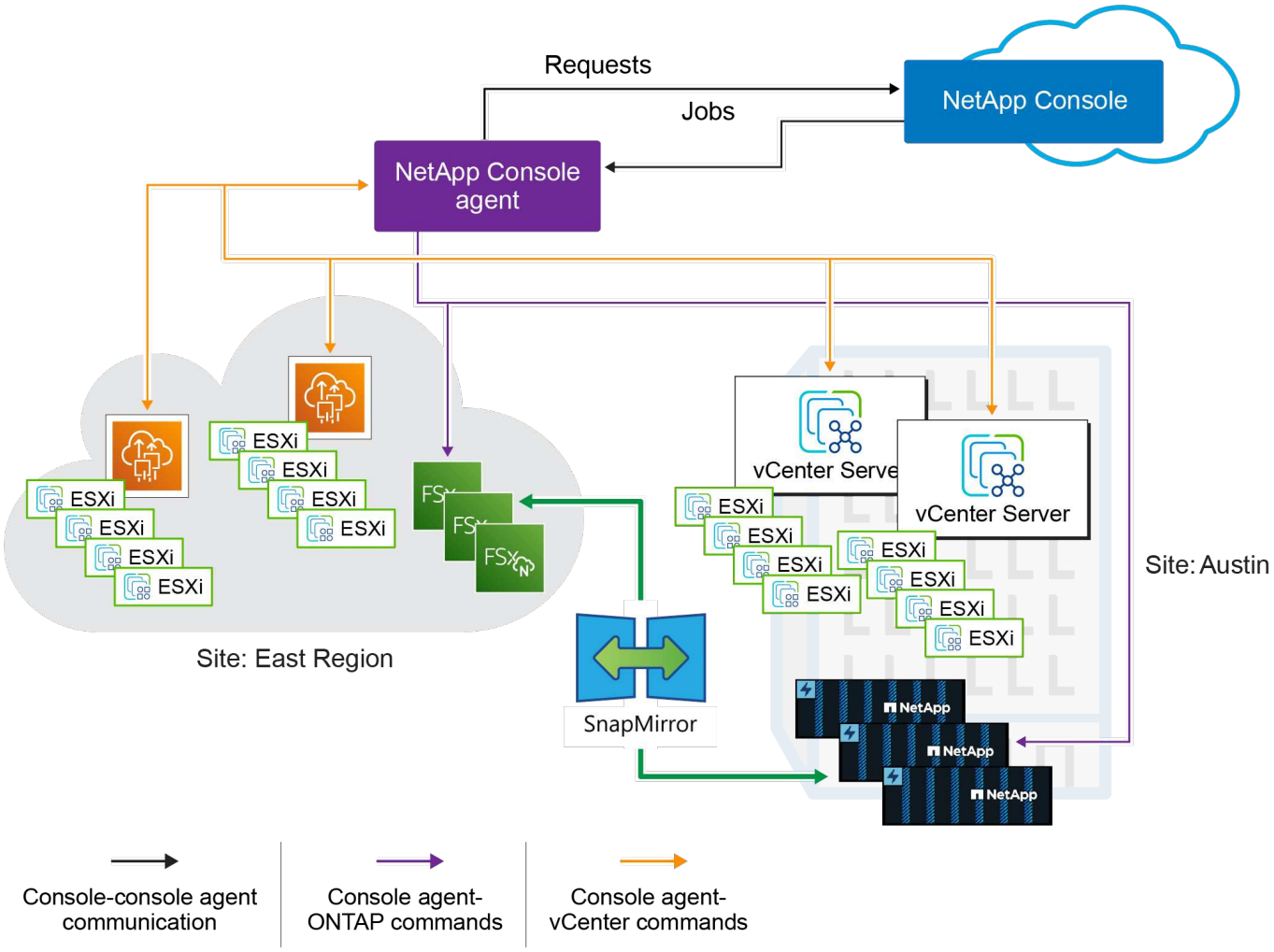
En savoir plus sur NetApp Disaster Recovery pour VMware

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

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

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

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



NetApp Console

NetApp Disaster Recovery est accessible via la NetApp Console.

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

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

Apprenez-en davantage sur le "NetApp Console" .

Avantages de l'utilisation de NetApp Disaster Recovery pour VMware

NetApp Disaster Recovery offre les avantages suivants :

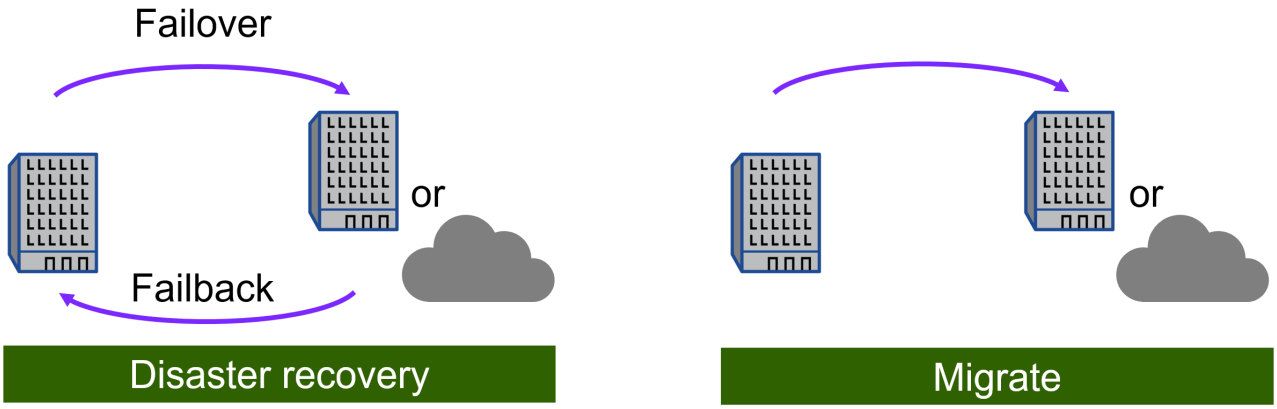
- Expérience utilisateur simplifiée pour la découverte et la récupération d'applications vCenter avec plusieurs opérations de récupération à un instant donné.

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

Ce que vous pouvez faire avec NetApp Disaster Recovery pour VMware

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

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



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

Coût

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

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

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

Licences

Vous pouvez utiliser les types de licences suivants :

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

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

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

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

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

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

Essai gratuit de 30 jours

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

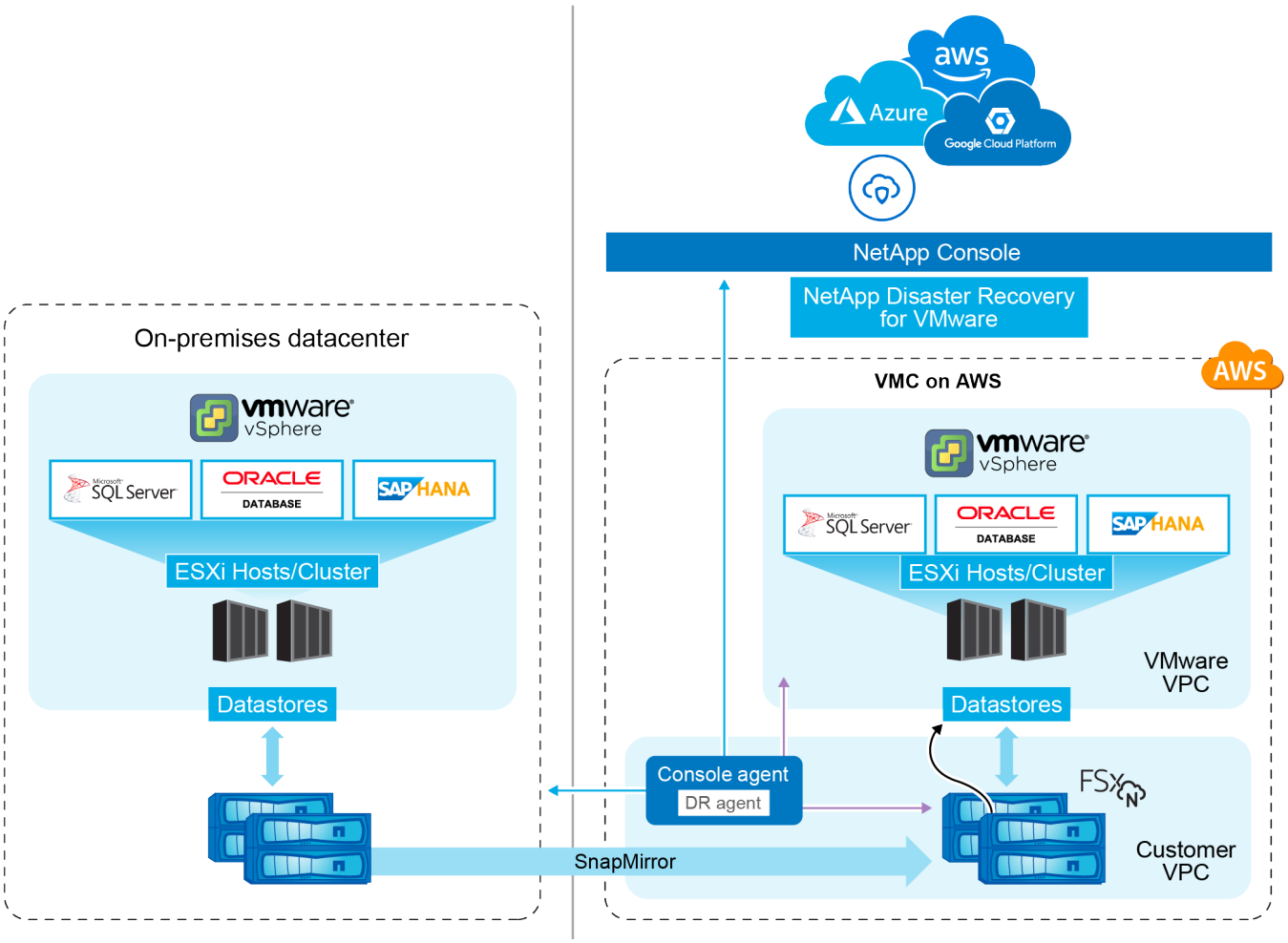
Pour continuer après l'essai de 30 jours, vous devrez obtenir un abonnement Pay-as-you-go (PAYGO) auprès de votre fournisseur de cloud ou acheter une licence BYOL auprès de NetApp.

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

Comment fonctionne la NetApp Disaster Recovery

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

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



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

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

Composants de la reprise après sinistre

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

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

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

Le flux de travail de protection de reprise après sinistre

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

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

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

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

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

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

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

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

protocole iSCSI ou FC

Cibles de protection prises en charge

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

Termes qui pourraient vous aider avec NetApp Disaster Recovery

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

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

Conditions préalables à la NetApp Disaster Recovery

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

Versions du logiciel

Composant	Version minimale
Amazon FSx for NetApp ONTAP	Dernière version disponible

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

Prérequis et considérations relatifs à Google Cloud

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

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

Considérations relatives au basculement

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

Considérations relatives aux solutions de repli

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

Autorisations Google Cloud

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

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

Autorisations de la NetApp Console

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

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

Prérequis de stockage ONTAP

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

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

Conditions préalables pour les clusters VMware vCenter

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

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

Prérequis de la NetApp Console

Démarrer avec la NetApp Console

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

Collecter les informations d'identification pour ONTAP et VMware

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

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

Créer l'agent de la NetApp Console

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

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

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

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

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

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

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

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

  Voir "Découvrez les clusters ONTAP sur site" .

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

Prérequis de charge de travail

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

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

Plus d'informations

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

Démarrage rapide pour la reprise NetApp Disaster Recovery

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

Réviser les prérequis

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

Configurer la NetApp Disaster Recovery

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

Quelle est la prochaine étape ?

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

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

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

Configurez votre infrastructure pour la NetApp Disaster Recovery

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

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

Vous pouvez utiliser NetApp Disaster Recovery dans les infrastructures suivantes :

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

Cloud hybride avec VMware Cloud et Amazon FSx for NetApp ONTAP

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

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

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

Zones de disponibilité AWS

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

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

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

Sur site vers AWS

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

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

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

Interconnexions VPC à VPC

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

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

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

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

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

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

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

Configurer AWS FSx pour NetApp ONTAP

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

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

Configurer VMware Cloud sur AWS SDDC

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

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

Cloud privé

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

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

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

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

Préparez-vous à une protection sur site vers sur site

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

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

Prise en charge de proxy intelligent

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

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

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

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

Accéder à la NetApp Disaster Recovery

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

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

Des tâches spécifiques nécessitent des rôles d'utilisateur spécifiques. "En savoir plus sur les rôles et les autorisations des utilisateurs dans NetApp Disaster Recovery". "En savoir plus sur les rôles d'accès à la NetApp Console pour tous les services".

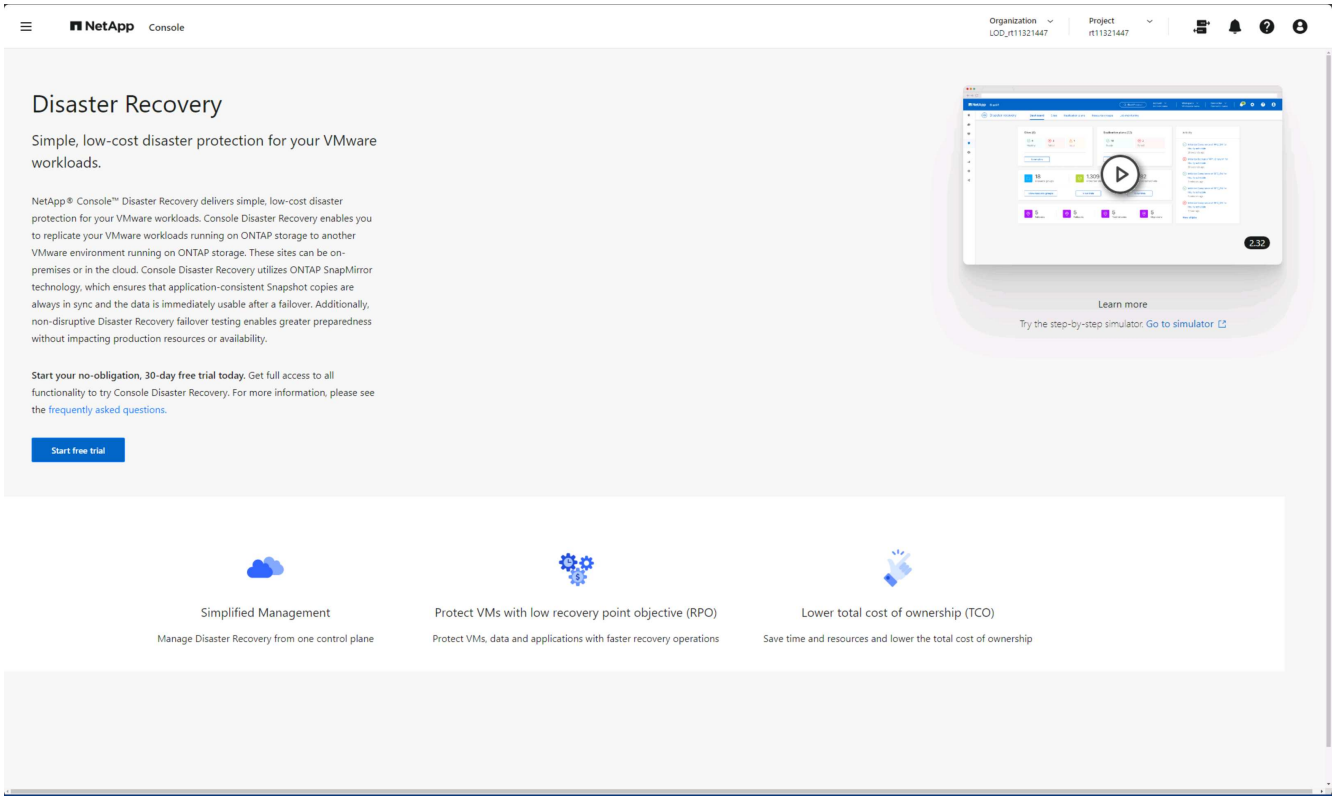
Étapes

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

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

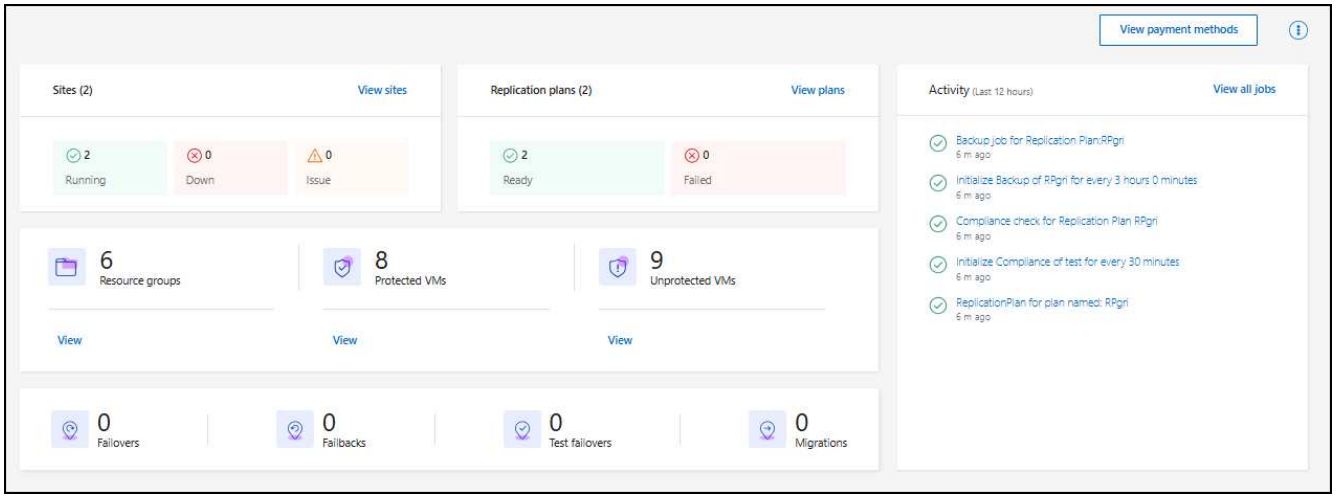
2. Connectez-vous à la NetApp Console.
3. Dans la navigation de gauche de la NetApp Console , sélectionnez **Protection** > **Reprise après sinistre**.

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



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

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



Configurer les licences pour NetApp Disaster Recovery

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

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

"En savoir plus sur les rôles et les autorisations des utilisateurs dans NetApp Disaster Recovery". "En savoir plus sur les rôles d'accès pour tous les services".

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

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

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

"En savoir plus sur les abonnements".

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

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

Essayez-le en utilisant un essai gratuit de 30 jours

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

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

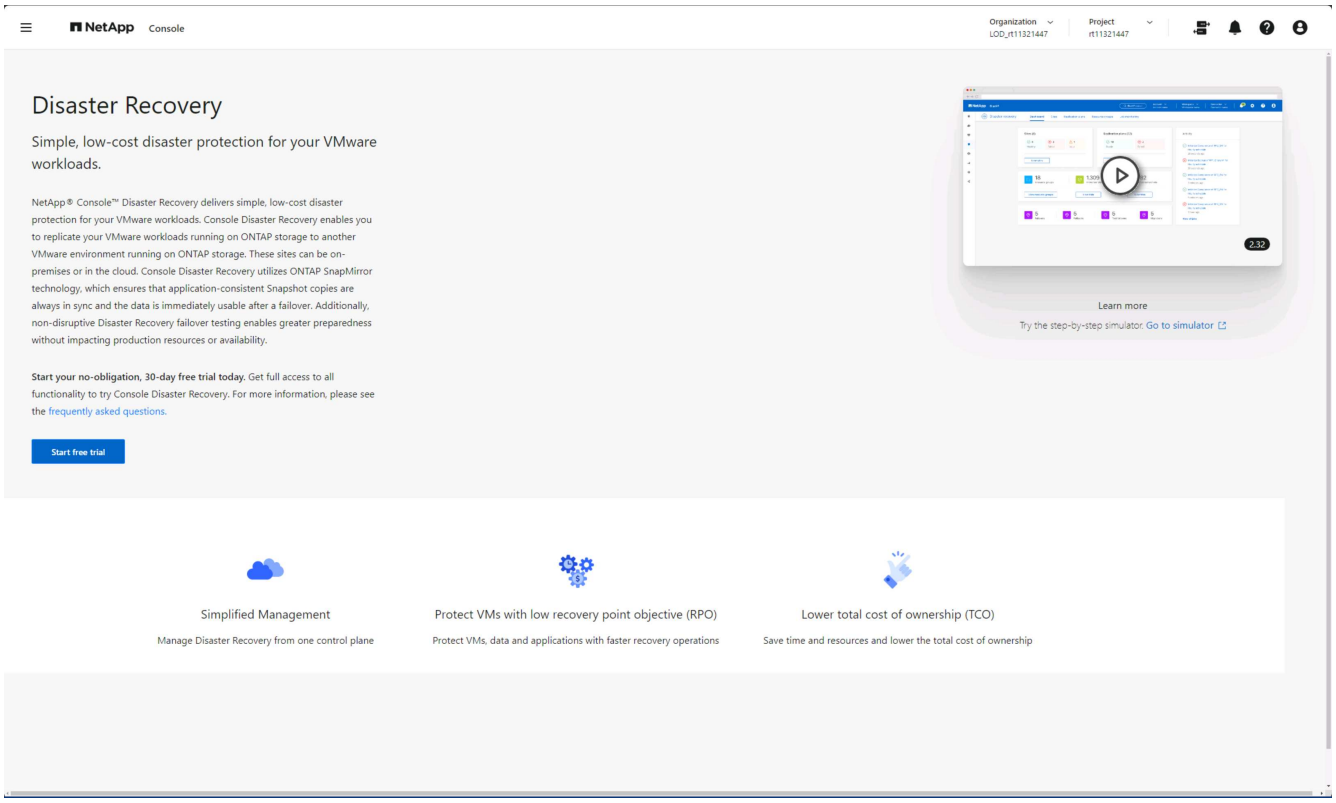
Pour continuer après l'essai, vous devrez acheter une licence BYOL ou un abonnement AWS PAYGO. Vous pouvez obtenir une licence à tout moment et vous ne serez pas facturé avant la fin de la période d'essai.

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

Étapes

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

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



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

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

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

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

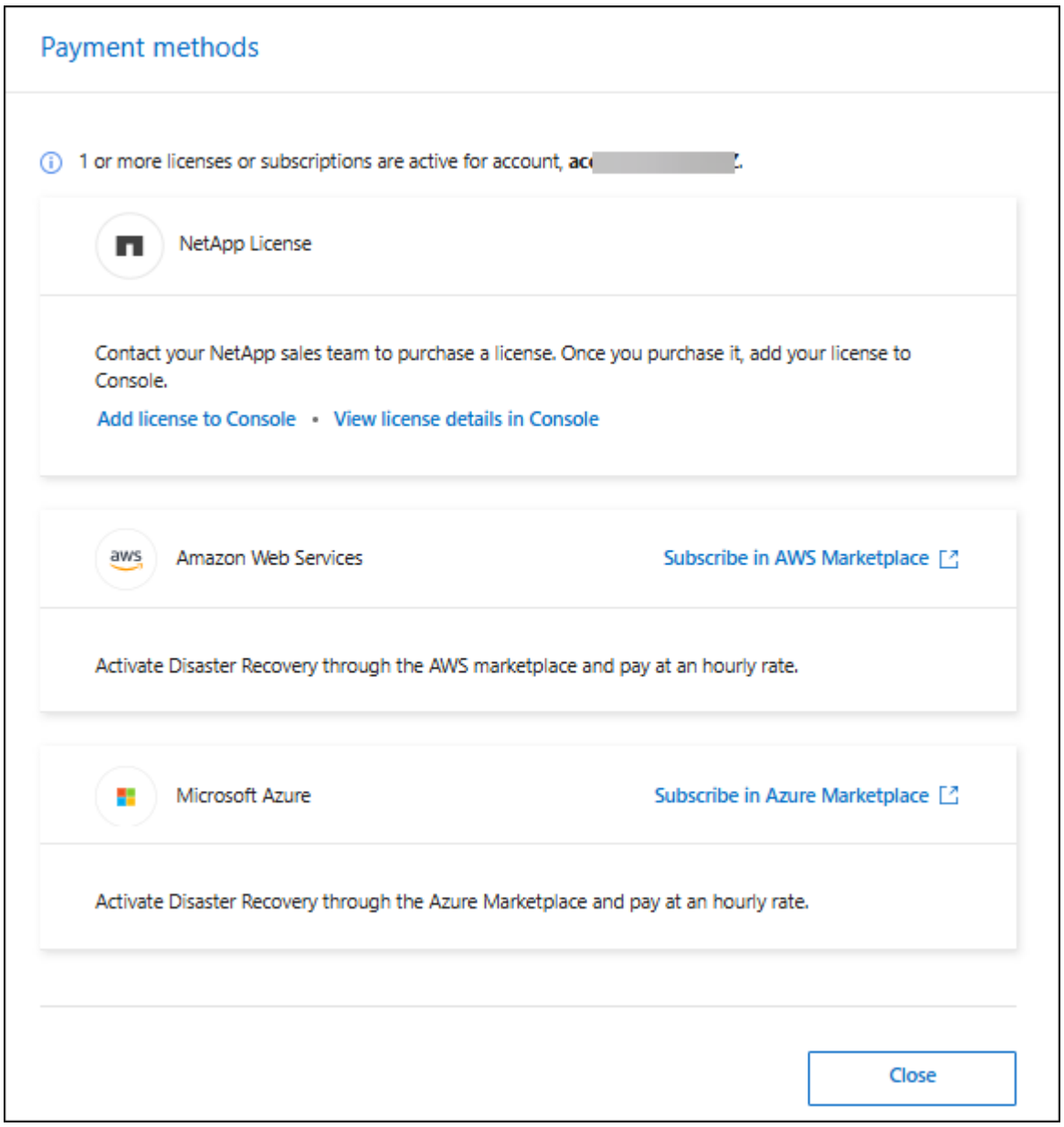
Une fois l’essai terminé, abonnez-vous via l’une des places de marché

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

Étapes

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

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



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

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

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

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

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

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

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

Mettez à jour votre licence lorsqu'elle expire

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

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

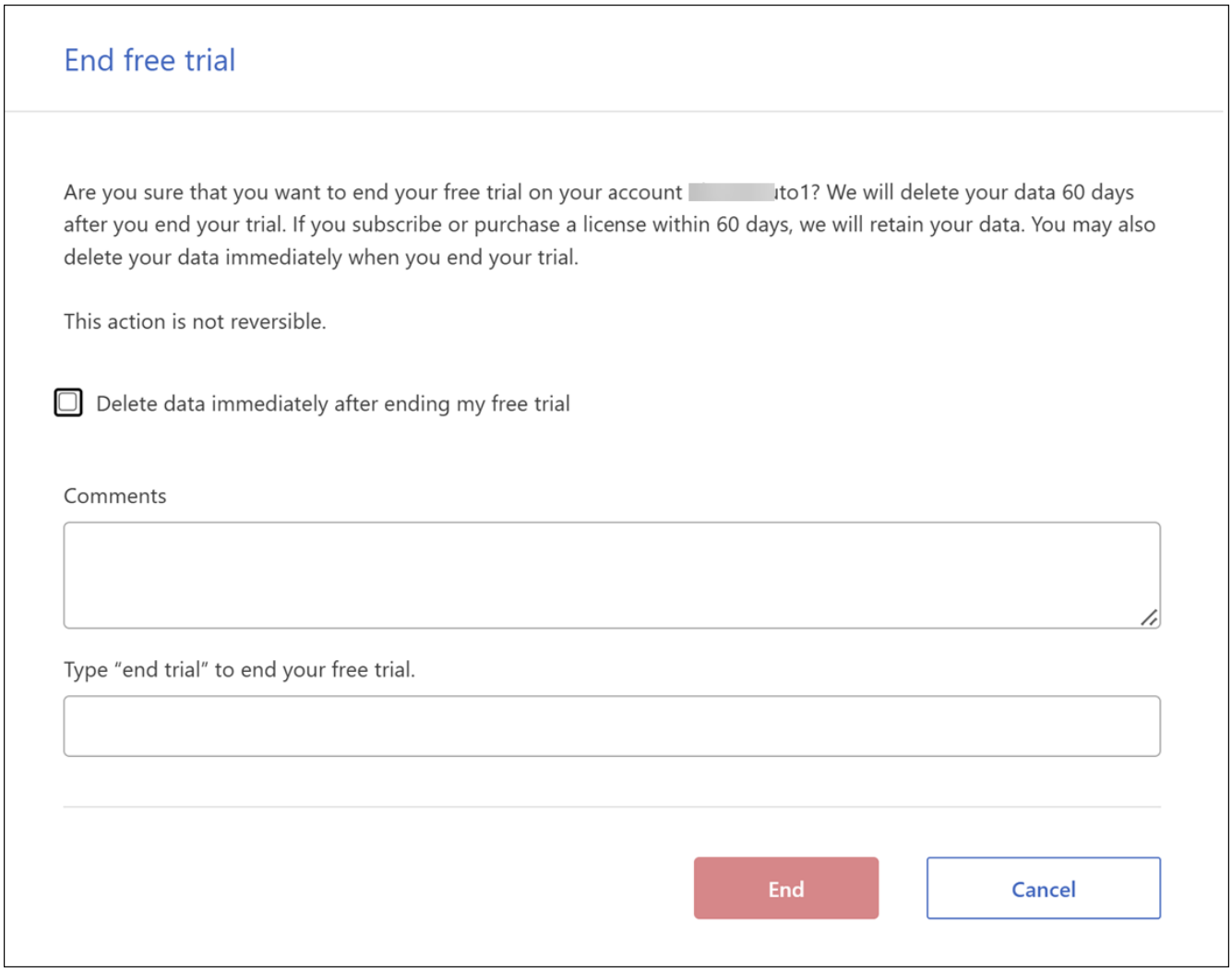
"En savoir plus sur la mise à jour des licences avec la NetApp Console".

Mettre fin à l'essai gratuit

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

Étapes

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



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

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

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

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