



Configuration de la réplication Snapshot

ASA r2

NetApp
February 11, 2026

Sommaire

- Configuration de la réplication Snapshot 1
 - Répliquez des snapshots sur un cluster distant à partir des systèmes de stockage ASA r2 1
 - Étape 1 : créer une relation entre clusters 1
 - Étape 2 : (facultatif) Créez une politique de réplication personnalisée 2
 - Étape 3 : création d'une relation de réplication 2
 - Étape 4 : test du basculement de réplication 5
 - En savoir plus sur les politiques de protection des données ONTAP prédéfinies 6
 - Rompre une relation de réplication asynchrone sur votre système ASA r2 7

Configuration de la réplication Snapshot

Répliquez des snapshots sur un cluster distant à partir des systèmes de stockage ASA r2

La réplication Snapshot est un processus au cours duquel les groupes de cohérence de votre système ASA r2 sont copiés sur un site distant. Après la réplication initiale, les modifications apportées aux groupes de cohérence sont copiées vers l'emplacement distant en fonction d'une règle de réplication. Les groupes de cohérence répliqués peuvent être utilisés pour la reprise après incident ou la migration des données.



La réplication de snapshots pour un système de stockage ASA r2 est uniquement prise en charge vers et depuis un autre système de stockage ASA r2. Vous ne pouvez pas répliquer des snapshots d'un système ASA r2 vers un système ASA, AFF ou FAS ou d'un système ASA, AFF ou FAS vers un système ASA r2.

Pour configurer la réplication Snapshot, vous devez établir une relation de réplication entre votre système ASA r2 et l'emplacement distant. La relation de réplication est régie par une règle de réplication. Une règle par défaut permettant de répliquer tous les snapshots est créée lors de la configuration du cluster. Vous pouvez utiliser la règle par défaut ou, si vous le souhaitez, créer une nouvelle règle.

À partir d' ONTAP 9.17.1, vous pouvez appliquer des stratégies de réplication asynchrone aux groupes de cohérence dans une relation hiérarchique. La réplication asynchrone n'est pas prise en charge pour les groupes de cohérence dans les relations hiérarchiques dans ONTAP 9.16.1.

["En savoir plus sur les groupes de cohérence hiérarchiques \(parent/enfant\)"](#) .



Étape 1 : créer une relation entre clusters

Avant de pouvoir protéger vos données en les répliquant sur un cluster distant, vous devez créer une relation entre les pairs de cluster entre le cluster local et distant.

Avant de commencer

Les conditions préalables à l'appairage de cluster sont les mêmes pour les systèmes ASA r2 que pour les autres systèmes ONTAP . ["Passez en revue les conditions préalables à l'appairage de clusters"](#) .

Étapes

1. Sur le cluster local, dans System Manager, sélectionnez **Cluster > Paramètres**.
2. Sous **intercluster Settings** en regard de **Cluster peers**,  sélectionnez , puis **Ajouter un homologue de cluster**.
3. Sélectionnez **Launch remote cluster** ; ceci génère une phrase de passe que vous utiliserez pour vous authentifier auprès du cluster distant.
4. Une fois la phrase de passe du cluster distant générée, collez-la sous **Passphrase** sur le cluster local.
5. Sélectionner  **Add** , puis entrer l'adresse IP de l'interface réseau intercluster.
6. Sélectionnez **Initiate cluster peering**.

Et la suite ?

Vous avez effectué un peering pour le cluster ASA r2 local avec un cluster distant. Il est maintenant possible

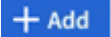
de créer une relation de réplication.

Étape 2 : (facultatif) Créez une politique de réplication personnalisée

La politique de réplication définit quand les mises à jour effectuées sur le cluster ASA r2 sont répliquées sur le site distant. ONTAP inclut diverses politiques de protection des données prédéfinies que vous pouvez utiliser pour vos relations de réplication. Si les politiques prédéfinies ne répondent pas à vos besoins, vous pouvez créer une politique de réplication personnalisée.

En savoir plus sur ["politiques de protection des données ONTAP prédéfinies"](#) .

Étapes

1. Dans System Manager, sélectionnez **protection > stratégies**, puis **règles de réplication**.
2. Sélectionnez  **Add** .
3. Entrez un nom pour la règle de réplication ou acceptez le nom par défaut, puis entrez une description.
4. Sélectionnez **étendue de la stratégie**.

Si vous souhaitez appliquer la règle de réplication à l'ensemble du cluster, sélectionnez **Cluster**. Si vous souhaitez que la règle de réplication s'applique uniquement aux unités de stockage d'une machine virtuelle de stockage spécifique, sélectionnez **Storage VM**.

5. Pour le **type de politique**, sélectionnez **Asynchrone**.



Avec la politique asynchrone, les données sont copiées sur le site distant après avoir été écrites à la source. La réplication synchrone n'est pas prise en charge pour les systèmes ASA r2.

6. Sous **transférer des instantanés à partir de la source**, acceptez le programme de transfert par défaut ou sélectionnez un autre programme.
7. Sélectionnez cette option pour transférer tous les instantanés ou pour créer des règles afin de déterminer les snapshots à transférer.
8. Activez éventuellement la compression réseau.
9. Sélectionnez **Enregistrer**.

Et la suite ?

Vous avez créé une règle de réplication et êtes maintenant prêt à créer une relation de réplication entre votre système ASA r2 et votre emplacement distant.

Pour en savoir plus

En savoir plus sur ["Machines virtuelles de stockage pour l'accès client"](#).

Étape 3 : création d'une relation de réplication

Une relation de réplication de snapshot établit une connexion entre le système ASA r2 et un emplacement distant afin que vous puissiez répliquer des groupes de cohérence vers un cluster distant. Les groupes de cohérence répliqués peuvent être utilisés pour la reprise après incident ou la migration des données.

Pour une protection contre les attaques par ransomware, lorsque vous configurez votre relation de réplication, vous pouvez choisir de verrouiller les snapshots de destination. Les snapshots verrouillés ne peuvent pas être supprimés accidentellement ou de manière malveillante. Vous pouvez utiliser des snapshots verrouillés pour restaurer des données si une unité de stockage est compromise par une attaque par ransomware.

Avant de commencer

- ["En savoir plus sur les politiques de réplication"](#) .


Lorsque vous créez une relation de réplication, vous devez sélectionner la stratégie de réplication appropriée pour votre relation de réplication. Vous pouvez utiliser une politique prédéfinie ou créer une politique personnalisée.

- Si vous souhaitez verrouiller vos snapshots de destination, vous devez d'abord ["Initialiser l'horloge de conformité de snapshot"](#) avant de créer la relation de réplication.

Créer une relation de réplication avec ou sans snapshots de destination verrouillés.

Avec instantanés verrouillés

Étapes

1. Dans System Manager, sélectionnez **protection > groupes de cohérence**.
2. Sélectionnez un groupe de cohérence.
3. Sélectionnez , puis **protéger**.
4. Sous **protection distante**, sélectionnez **répliquer sur un cluster distant**.
5. Sélectionnez la **règle de réplication**.

Vous devez sélectionner une règle de réplication *vault*.

6. Sélectionnez **Paramètres de destination**.
7. Sélectionnez **Verrouiller les instantanés de destination pour empêcher la suppression**.
8. Entrez la période de conservation maximale et minimale des données.
9. Pour retarder le début du transfert de données, désélectionnez **Démarrer immédiatement le transfert**.

Le transfert de données initial commence immédiatement par défaut.

10. Si vous le souhaitez, sélectionnez **Paramètres de destination** pour remplacer le programme de transfert par défaut, puis **remplacer le programme de transfert**.


Votre planning de transfert doit être d'au moins 30 minutes pour être pris en charge.


11. Sélectionnez **Enregistrer**.

Sans snapshots verrouillés

Étapes

1. Dans System Manager, sélectionnez **protection > réplication**.
2. Sélectionnez cette option pour créer la relation de réplication avec la destination locale ou la source locale.

Option	Étapes
Destinations locales	<ol style="list-style-type: none">a. Sélectionnez destinations locales, puis sélectionnez .b. Recherchez et sélectionnez le groupe de cohérence source. <p>Le groupe de cohérence <i>source</i> fait référence au groupe de cohérence de votre cluster local que vous souhaitez répliquer.</p>

Option	Étapes
Sources locales	<ol style="list-style-type: none"> Sélectionnez sources locales, puis sélectionnez  . Recherchez et sélectionnez le groupe de cohérence source. Sous destination de la réplication, sélectionnez le cluster vers lequel effectuer la réplication, puis sélectionnez la machine virtuelle de stockage.

3. Sélectionnez une règle de réplication.

4. Pour retarder le début du transfert de données, sélectionnez **Paramètres de destination**, puis désélectionnez **Démarrer immédiatement le transfert**.

Le transfert de données initial commence immédiatement par défaut.

5. Si vous le souhaitez, sélectionnez **Paramètres de destination** pour remplacer le programme de transfert par défaut, puis **remplacer le programme de transfert**.

Votre planning de transfert doit être d'au moins 30 minutes pour être pris en charge.

6. Sélectionnez **Enregistrer**.


Et la suite ?

Maintenant que vous avez créé une règle de réplication et une relation, votre transfert de données initial commence comme défini dans votre règle de réplication. Vous pouvez également tester votre basculement de réplication pour vérifier qu'il peut se produire si votre système ASA r2 est hors ligne.

Étape 4 : test du basculement de réplication

Vous pouvez également vérifier que vous pouvez transmettre les données à partir d'unités de stockage répliquées sur un cluster distant si le cluster source est hors ligne.

Étapes

- Dans System Manager, sélectionnez **protection > réplication**.
- Passez le curseur sur la relation de réplication que vous souhaitez tester, puis sélectionnez .
- Sélectionnez **Test failover**.
- Entrez les informations de basculement, puis sélectionnez **Test failover**.

Et la suite ?

Maintenant que vos données sont protégées par la réplication Snapshot à des fins de reprise sur incident, vous devez "[chiffrement de vos données au repos](#)" empêcher leur lecture si un disque de votre système ASA r2 est requalifié, renvoyé, perdu ou volé.

En savoir plus sur les politiques de protection des données ONTAP prédéfinies

La politique de réplication définit quand les mises à jour effectuées sur le cluster ASA r2 sont répliquées sur le site distant. ONTAP inclut diverses politiques de protection des données prédéfinies que vous pouvez utiliser pour vos relations de réplication.

Si les politiques prédéfinies ne répondent pas à vos besoins, vous pouvez ["créer une politique de réplication personnalisée"](#) .



Les systèmes ASA r2 ne prennent pas en charge la réplication synchrone.

Les systèmes ASA r2 prennent en charge les politiques de protection prédéfinies suivantes.


Politique	Description	Type de politique
Asynchrone	Une politique asynchrone et de coffre-fort SnapMirror unifiée pour la mise en miroir du dernier système de fichiers actif et des instantanés quotidiens et hebdomadaires avec un calendrier de transfert horaire.	Asynchrone
Basculement automatique duplex	Politique pour SnapMirror synchrone avec garantie RTO nulle et réplication de synchronisation bidirectionnelle.	Synchronisation active de SnapMirror
CloudBackupDefault	Politique de coffre-fort avec règle quotidienne.	Asynchrone
Sauvegarde quotidienne	Politique de coffre-fort avec une règle quotidienne et un calendrier de transfert quotidien.	Asynchrone
DPDéfaut	Politique asynchrone SnapMirror pour la mise en miroir de tous les instantanés et du dernier système de fichiers actif.	Asynchrone
MirrorAllSnapshots	Politique asynchrone SnapMirror pour la mise en miroir de tous les instantanés et du dernier système de fichiers actif.	Asynchrone
MiroirTous les instantanésSupprimer le réseau	Politique asynchrone SnapMirror pour la mise en miroir de tous les instantanés et du dernier système de fichiers actif, à l'exclusion des configurations réseau.	Asynchrone
Miroir et coffre-fort	Une politique asynchrone et de coffre-fort SnapMirror unifiée pour la mise en miroir du dernier système de fichiers actif et des instantanés quotidiens et hebdomadaires.	Asynchrone
MirrorAndVaultDiscardNetwork	Une politique asynchrone et de coffre-fort SnapMirror unifiée pour la mise en miroir du dernier système de fichiers actif et des instantanés quotidiens et hebdomadaires à l'exclusion des configurations réseau.	Asynchrone

Politique	Description	Type de politique
MirrorLatest	Politique asynchrone SnapMirror pour la mise en miroir du dernier système de fichiers actif.	Asynchrone
Unified7year	Politique SnapMirror unifiée avec conservation de 7 ans.	Asynchrone
XDP par défaut	Politique de coffre-fort avec règles quotidiennes et hebdomadaires.	Asynchrone

Rompre une relation de réplication asynchrone sur votre système ASA r2

Dans certaines situations, vous devrez peut-être rompre une relation de réplication asynchrone. Par exemple, si vous exécutez ONTAP 9.16.1 et que vous souhaitez augmenter la taille d'un groupe de cohérence qui se trouve dans une relation de réplication asynchrone, vous devez rompre la relation avant de pouvoir modifier la taille du groupe de cohérence.

Étapes

1. Dans System Manager, sélectionnez **protection > réplication**.
2. Sélectionnez **Destinations locales** ou **Sources locales**.
3. À côté de la relation que vous souhaitez rompre, sélectionnez  ; puis sélectionnez **Pause**.
4. Sélectionnez **Pause**.

Résultat

La relation asynchrone entre le groupe de cohérence primaire et secondaire est rompue.

Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

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

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

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

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

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

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

Informations sur les marques commerciales

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