Gérez vos données avec ONTAP

ASA r2

NetApp
September 26, 2024

Sommaire

Gérez vos données avec ONTAP

Vidéos de démonstration du système de stockage ASA r2

Visionnez de courtes vidéos qui expliquent comment utiliser ONTAP System Manager pour effectuer rapidement et facilement des tâches courantes sur vos systèmes de stockage ASA r2.

Configurez les protocoles SAN sur votre système ASA r2

"Transcription vidéo"

Provisionnez le stockage SAN sur votre système ASA r2

"Transcription vidéo"

Répliquez les données sur un cluster distant à partir d'un système ASA r2

"Transcription vidéo"

Gérez votre stockage

Provisionnez le stockage SAN ONTAP sur les systèmes ASA r2

Lorsque vous provisionnez le stockage, vos hôtes SAN peuvent lire et écrire des données sur les systèmes de stockage ASA r2. Pour provisionner le stockage, vous pouvez utiliser ONTAP System Manager pour créer des unités de stockage, ajouter des initiateurs hôtes et mapper l'hôte sur une unité de stockage. Vous devez également effectuer des étapes sur l'hôte pour activer les opérations de lecture/écriture.

Créer des unités de stockage

Sur un système ASA r2, une unité de stockage met à disposition de l'espace de stockage de vos hôtes SAN pour les opérations sur les données. Une unité de stockage désigne une LUN pour les hôtes SCSI ou un namespace NVMe pour les hôtes NVMe. Si votre cluster est configuré pour prendre en charge les hôtes SCSI, vous êtes invité à créer une LUN. Si votre cluster est configuré pour prendre en charge les hôtes NVMe, vous êtes invité à créer un namespace NVMe. Une unité de stockage ASA r2 a une capacité maximale de 128 To.

Consultez le "NetApp Hardware Universe" pour connaître les limites de stockage les plus récentes pour les systèmes ASA r2.

Les initiateurs hôtes sont ajoutés et mappés sur l'unité de stockage dans le cadre du processus de création de l'unité de stockage. Vous pouvez également "ajoutez des initiateurs hôtes""carte"les et sur vos unités de stockage une fois les unités de stockage créées.

Étapes

1. Dans System Manager, sélectionnez **Storage**, puis sélectionnez + Add .
2. Entrez un nom pour la nouvelle unité de stockage.
3. Entrez le nombre d'unités que vous souhaitez créer.

Si vous créez plusieurs unités de stockage, chaque unité est créée avec la même capacité, le même système d'exploitation hôte et le même mappage d'hôte.

4. Entrez la capacité de l'unité de stockage, puis sélectionnez le système d'exploitation hôte.
5. Acceptez le **mappage d'hôte** sélectionné automatiquement ou sélectionnez un autre groupe d'hôtes pour l'unité de stockage à mapper.

   Host Mapping fait référence au groupe d'hôtes auquel la nouvelle unité de stockage sera mappée. S'il existe un groupe d'hôtes préexistant pour le type d'hôte que vous avez sélectionné pour votre nouvelle unité de stockage, le groupe d'hôtes préexistant est automatiquement sélectionné pour votre mappage d'hôtes. Vous pouvez accepter le groupe d'hôtes sélectionné automatiquement pour votre mappage d'hôtes ou sélectionner un autre groupe d'hôtes.

   S'il n'existe aucun groupe d'hôtes préexistant pour les hôtes s'exécutant sur le système d'exploitation que vous avez spécifié, un nouveau groupe d'hôtes est automatiquement créé par ONTAP.

6. Si vous souhaitez effectuer l'une des opérations suivantes, sélectionnez **plus d'options** et suivez les étapes requises.

Option	Étapes
Modifiez la règle de qualité de service (QoS) par défaut Si la stratégie QoS par défaut n'a pas été définie précédemment sur la machine virtuelle de stockage sur laquelle l'unité de stockage est créée, cette option n'est pas disponible.	a. Sous **stockage et optimisation**, à côté de **qualité de service (QoS)**, sélectionnez ⌄ . b. Sélectionnez une politique QoS existante.

Option	Étapes
Création d'une règle de QoS	a. Sous **stockage et optimisation**, à côté de **qualité de service (QoS)**, sélectionnez . b. Sélectionnez **définir une nouvelle stratégie**. c. Entrez un nom pour la nouvelle politique de QoS. d. Définissez une limite QoS, une garantie QoS, ou les deux. i. Si vous le souhaitez, sous **Limit**, entrez une limite de débit maximal, une limite d'IOPS maximale ou les deux. La définition d'un débit et d'IOPS maximum pour une unité de stockage limite son impact sur les ressources système afin qu'elles ne dégradent pas les performances des charges de travail stratégiques. ii. Si vous le souhaitez, entrez un débit minimal, un nombre minimal d'IOPS ou les deux sous **Guarantee**. La définition d'un débit et d'IOPS minimaux pour une unité de stockage garantit qu'elle satisfait aux objectifs de performance minimaux, indépendamment de la demande des charges de travail concurrentes. e. Sélectionnez **Ajouter**.
Ajoutez un nouvel hôte SCSI	a. Sous **informations sur l'hôte**, sélectionnez **SCSI** pour le protocole de connexion. b. Sélectionnez le système d'exploitation hôte. c. Sous **Host Mapping**, sélectionnez **New hosts**. d. Sélectionnez **FC** ou **iSCSI**. e. Sélectionnez des initiateurs hôtes existants ou sélectionnez **Ajouter un initiateur** pour ajouter un nouvel initiateur hôte. Un WWPN FC valide est un exemple de WWPN « 01:02:03:04:0a:0b:0C:0d ». Les noms d'initiateurs iSCSI valides sont « iqn.1995-08.com.example:string" et « eui.0123456789abcdef ».
Créez un nouveau groupe d'hôtes SCSI	a. Sous **informations sur l'hôte**, sélectionnez **SCSI** pour le protocole de connexion. b. Sélectionnez le système d'exploitation hôte. c. Sous **Host Mapping**, sélectionnez **New host group**. d. Entrez un nom pour le groupe d'hôtes, puis sélectionnez les hôtes à ajouter au groupe.

Option	Étapes
Ajoutez un nouveau sous-système NVMe	a. Sous **informations sur l'hôte**, sélectionnez **NVMe** pour le protocole de connexion. b. Sélectionnez le système d'exploitation hôte. c. Sous **Host Mapping**, sélectionnez **Nouveau sous-système NVMe**. d. Entrez un nom pour le sous-système ou acceptez le nom par défaut. e. Entrez un nom pour l'initiateur. f. Si vous souhaitez activer l'authentification intrabande ou TLS (transport Layer Security), sélectionnez , puis sélectionnez vos options. L'authentification intrabande permet une authentification bidirectionnelle et unidirectionnelle sécurisée entre vos hôtes NVMe et votre système ASA r2. TLS chiffre toutes les données envoyées sur le réseau entre vos hôtes NVMe/TCP et votre système ASA r2. g. Sélectionnez **Ajouter initiateur** pour ajouter d'autres initiateurs. Le NQN hôte doit être formaté en <nqn.yyyy-mm> suivi d'un nom de domaine complet. L'année doit être égale ou ultérieure à 1970. La longueur maximale totale doit être de 223. Exemple d'initiateur NVMe valide : nqn.2014-08.com.example:string

7. Sélectionnez **Ajouter**.

Et la suite ?

Vos unités de stockage sont créées et mappées sur vos hôtes. Vous pouvez désormais "créer des instantanés"protéger les données stockées sur votre système ASA r2.

Pour en savoir plus

En savoir plus sur "Utilisation des machines virtuelles de stockage par les systèmes ASA r2".

Ajoutez des initiateurs hôtes

Vous pouvez à tout moment ajouter de nouveaux initiateurs hôtes à votre système ASA r2. Les initiateurs rendent les hôtes éligibles pour accéder aux unités de stockage et effectuer des opérations sur les données.

Avant de commencer

Si vous souhaitez répliquer la configuration hôte sur un cluster de destination pendant le processus d'ajout de vos initiateurs hôtes, votre cluster doit faire partie d'une relation de réplication. Si vous le souhaitez, vous pouvez "créer une relation de réplication" une fois votre hôte ajouté.

Ajoutez des initiateurs hôtes pour des hôtes SCSI ou NVMe.

Hôtes SCSI

Étapes

1. Sélectionnez **hôte**.
2. Sélectionnez **SCSI**, puis + Add.
3. Entrez le nom d'hôte, sélectionnez le système d'exploitation hôte et entrez une description d'hôte.
4. Si vous souhaitez répliquer la configuration hôte vers un cluster de destination, sélectionnez **replicate host configuration**, puis sélectionnez le cluster de destination.

   Votre cluster doit faire partie d'une relation de réplication pour pouvoir répliquer la configuration hôte.

5. Ajouter des hôtes nouveaux ou existants.

Ajouter de nouveaux hôtes	Ajouter des hôtes existants
a. Sélectionnez **nouveaux hôtes**. b. Sélectionnez **FC** ou **iSCSI**, puis sélectionnez les initiateurs hôtes. c. Si vous le souhaitez, sélectionnez **configurer la proximité de l'hôte**. La configuration de la proximité des hôtes permet à ONTAP d'identifier le contrôleur le plus proche de l'hôte pour optimiser le chemin d'accès aux données et réduire la latence. Ceci s'applique uniquement si vous avez répliqué des données vers un emplacement distant. Si vous n'avez pas configuré la réplication de snapshot, vous n'avez pas besoin de sélectionner cette option. d. Si vous devez ajouter de nouveaux initiateurs, sélectionnez **Ajouter des initiateurs**.	a. Sélectionnez **hôtes existants**. b. Sélectionnez l'hôte à ajouter. c. Sélectionnez **Ajouter**.

6. Sélectionnez **Ajouter**.

Et la suite ?

Vos hôtes SCSI sont ajoutés à votre système ASA r2 et vous êtes prêt à mapper vos hôtes à vos unités de stockage.

Hôtes NVMe

Étapes

1. Sélectionnez **hôte**.
2. Sélectionnez **NVMe**, puis + Add.
3. Entrez un nom pour le sous-système NVMe, sélectionnez le système d'exploitation hôte et entrez une description.
4. Sélectionnez **Ajouter initiateur**.

Et la suite ?

Vos hôtes sont ajoutés au système ASA r2 et vous pouvez mapper vos hôtes sur vos unités de stockage.

Créer des groupes d'hôtes

Sur un système ASA r2, un *groupe d'hôtes* est le mécanisme utilisé pour donner aux hôtes l'accès aux unités de stockage. Un groupe d'hôtes désigne un groupe initiateur pour les hôtes SCSI ou un sous-système NVMe pour les hôtes NVMe. Un hôte ne peut voir que les unités de stockage qui sont mappées aux groupes d'hôtes auxquels il appartient. Lorsqu'un groupe d'hôtes est mappé sur une unité de stockage, les hôtes qui sont membres du groupe peuvent alors monter (créer des répertoires et des structures de fichiers sur) l'unité de stockage.

Les groupes d'hôtes sont créés automatiquement ou manuellement lorsque vous créez vos unités de stockage. Vous pouvez éventuellement utiliser les étapes suivantes pour créer des groupes hôtes avant ou après la création de l'unité de stockage.

Étapes

1. Dans System Manager, sélectionnez **Host**.
2. Sélectionnez les hôtes que vous souhaitez ajouter au groupe d'hôtes.

   Après avoir sélectionné le premier hôte, l'option à ajouter à un groupe d'hôtes apparaît au-dessus de la liste des hôtes.

3. Sélectionnez **Ajouter au groupe d'hôtes**.
4. Recherchez et sélectionnez le groupe d'hôtes auquel vous souhaitez ajouter l'hôte.

Et la suite ?

Vous avez créé un groupe d'hôtes et vous pouvez maintenant le mapper à une unité de stockage.

Mappez l'unité de stockage sur un hôte

Après avoir créé vos unités de stockage ASA r2 et ajouté des initiateurs hôtes, vous devez mapper vos hôtes sur vos unités de stockage pour assurer le service des données. Les unités de stockage sont mappées aux hôtes dans le cadre du processus de création de l'unité de stockage. Vous pouvez également mapper les unités de stockage existantes à tout moment sur des hôtes nouveaux ou existants.

Étapes

1. Sélectionnez **stockage**.
2. Placez le pointeur de la souris sur le nom de l'unité de stockage à mapper.
3. Sélectionnez ⋮, puis **Mapper sur les hôtes**.
4. Sélectionnez les hôtes que vous souhaitez mapper à l'unité de stockage, puis sélectionnez **Map**.

Et la suite ?

Votre unité de stockage est mappée sur vos hôtes et vous êtes prêt à terminer le processus de provisionnement sur vos hôtes.

Provisionnement complet côté hôte

Une fois que vous avez créé vos unités de stockage, ajouté vos initiateurs hôtes et mappé vos unités de stockage, vous devez effectuer certaines étapes sur vos hôtes avant de pouvoir lire et écrire des données sur

votre système ASA r2.

Étapes

1. Pour les protocoles FC et FC/NVMe, indiquez vos commutateurs FC par WWPN.

   Utilisez une zone par initiateur et incluez tous les ports cibles dans chaque zone.

2. Découvrez la nouvelle unité de stockage.
3. Initialisez l'unité de stockage et un système de création de fichiers.
4. Vérifiez que votre hôte peut lire et écrire des données sur l'unité de stockage.

Et la suite ?

Vous avez terminé le processus de provisionnement et êtes prêt à transférer des données. Vous pouvez désormais "créer des instantanés"protéger les données stockées sur votre système ASA r2.

Pour en savoir plus

Pour plus d'informations sur la configuration côté hôte, reportez-vous à "Documentation de l'hôte SAN ONTAP"la section correspondant à votre hôte spécifique.

Cloner les données sur des systèmes de stockage ASA r2

Le clonage des données crée des copies d'unités de stockage et de groupes de cohérence sur votre système ASA r2 à l'aide de ONTAP System Manager. Ces copies peuvent être utilisées pour le développement d'applications, les tests, les sauvegardes, la migration des données ou d'autres fonctions d'administration.

Cloner les unités de stockage

Lorsque vous clonez une unité de stockage, vous créez une nouvelle unité de stockage sur votre système ASA r2 qui est une copie inscriptible instantanée de l'unité de stockage que vous avez clonée.

Étapes

1. Dans System Manager, sélectionnez **Storage**.
2. Placez le curseur de la souris sur le nom de l'unité de stockage à cloner.
3. Sélectionnez ⋮, puis **Clone**.
4. Acceptez le nom par défaut de la nouvelle unité de stockage qui sera créée en tant que clone ou entrez-en un nouveau.
5. Sélectionnez le système d'exploitation hôte.

   Par défaut, un nouveau snapshot est créé pour le clone.

6. Si vous souhaitez utiliser un snapshot existant, créer un nouveau groupe d'hôtes ou ajouter un nouvel hôte, sélectionnez **plus d'options**.

Option	Étapes
Utiliser un snapshot existant	a. Sous **instantané à cloner**, sélectionnez **utiliser un instantané existant**. b. Sélectionnez le snapshot que vous souhaitez utiliser pour le clone.
Créez un nouveau groupe d'hôtes	a. Sous **Host Mapping**, sélectionnez **New host group**. b. Entrez un nom pour le nouveau groupe d'hôtes, puis sélectionnez les initiateurs hôtes à inclure dans le groupe.
Ajouter un nouvel hôte	a. Sous **Host mapping**, sélectionnez **New hosts**. b. Entrez le nom a du nouvel hôte, puis sélectionnez **FC** ou **iSCSI**. c. Sélectionnez les initiateurs hôtes dans la liste des initiateurs existants ou sélectionnez **Ajouter** pour ajouter de nouveaux initiateurs pour l'hôte.

7. Sélectionnez **Clone**.

Et la suite ?

Vous avez créé une nouvelle unité de stockage identique à l'unité de stockage que vous avez clonée. Vous êtes maintenant prêt à utiliser la nouvelle unité de stockage si nécessaire.

Cloner des groupes de cohérence

Lorsque vous clonez un groupe de cohérence, vous créez un nouveau groupe de cohérence dont la structure, les unités de stockage et les données sont identiques au groupe de cohérence que vous avez cloné. Utilisez un clone de groupe de cohérence pour tester les applications ou migrer les données. Supposons, par exemple, que vous deviez migrer une charge de travail de production à partir d'un groupe de cohérence. Vous pouvez cloner le groupe de cohérence pour créer une copie de votre charge de travail de production à conserver en tant que sauvegarde jusqu'à la fin de la migration.

Le clone est créé à partir d'un snapshot du groupe de cohérence en cours de clonage. L'instantané utilisé pour le clone est pris au moment où le processus de clonage est lancé par défaut. Vous pouvez modifier le comportement par défaut pour utiliser un instantané existant.

Les mappages d'unité de stockage sont copiés dans le cadre du processus de clonage. Les règles Snapshot ne sont pas copiées dans le cadre du processus de clonage.

Vous pouvez créer des clones à partir de groupes de cohérence stockés localement sur votre système ASA r2 ou à partir de groupes de cohérence qui ont été répliqués sur des sites distants.

Clonage à l'aide d'un snapshot local

Étapes

1. Dans System Manager, sélectionnez **protection > groupes de cohérence**.
2. Placez le curseur de la souris sur le groupe de cohérence à cloner.
3. Sélectionnez ⋮, puis **Clone**.
4. Indiquez le nom du clone de groupe de cohérence ou acceptez le nom par défaut.
5. Sélectionnez le système d'exploitation hôte.
6. Si vous souhaitez dissocier le clone du groupe de cohérence source et allouer de l'espace disque, sélectionnez **Split clone**.
7. Si vous souhaitez utiliser un snapshot existant, créer un nouveau groupe d'hôtes ou ajouter un nouvel hôte pour le clone, sélectionnez **plus d'options**.

Option	Étapes
Utiliser un snapshot existant	a. Sous **instantané à cloner**, sélectionnez **utiliser un instantané existant**. b. Sélectionnez le snapshot que vous souhaitez utiliser pour le clone.
Créez un nouveau groupe d'hôtes	a. Sous **Host Mapping**, sélectionnez **New host group**. b. Entrez un nom pour le nouveau groupe d'hôtes, puis sélectionnez les initiateurs hôtes à inclure dans le groupe.
Ajouter un nouvel hôte	a. Sous **Host mapping**, sélectionnez **New hosts**. b. Entrez le nouveau nom d'hôte, puis sélectionnez **FC** ou **iSCSI**. c. Sélectionnez les initiateurs hôtes dans la liste des initiateurs existants ou sélectionnez **Ajouter un initiateur** pour ajouter de nouveaux initiateurs pour l'hôte.

8. Sélectionnez **Clone**.

Clonage à l'aide d'un snapshot distant

Étapes

1. Dans System Manager, sélectionnez **protection > réplication**.
2. Passez le curseur sur la **Source** que vous souhaitez cloner.
3. Sélectionnez ⋮, puis **Clone**.
4. Sélectionnez le cluster source et la machine virtuelle de stockage, puis indiquez le nom du nouveau groupe de cohérence ou acceptez le nom par défaut.
5. Sélectionnez l'instantané à cloner, puis sélectionnez **Clone**.

Et la suite ?

Vous avez cloné un groupe de cohérence à partir de votre emplacement distant. Le nouveau groupe de cohérence est disponible en local sur votre système ASA r2 et peut être utilisé en fonction des besoins.

Et la suite ?

Pour protéger vos données, vous devez "créer des instantanés" utiliser le groupe de cohérence cloné.

Modification des unités de stockage sur les systèmes de stockage ASA r2

Pour optimiser les performances de votre système ASA r2, vous devrez peut-être modifier vos unités de stockage afin d'augmenter leur capacité, mettre à jour les règles de QoS ou modifier les hôtes mappés sur les unités. Par exemple, si une nouvelle charge de travail applicative stratégique est ajoutée à une unité de stockage existante, vous devrez peut-être modifier la règle de qualité de service (QoS) appliquée à l'unité de stockage afin de prendre en charge le niveau de performance requis pour la nouvelle application.

Augmentation de la capacité

Augmentez la taille d'une unité de stockage avant qu'elle n'atteigne sa pleine capacité afin d'éviter une perte d'accès aux données qui peut se produire si l'unité de stockage manque d'espace inscriptible. La capacité d'une unité de stockage peut être augmentée à 128 To, ce qui correspond à la taille maximale autorisée par ONTAP.

Modifier les mappages d'hôte

Modifiez les hôtes mappés à une unité de stockage pour faciliter l'équilibrage des charges de travail ou la reconfiguration des ressources système.

Modifiez la règle QoS

Les règles de qualité de service (QoS) garantissent que la performance des charges de travail stratégiques n'est pas dégradée par les autres charges de travail. Vous pouvez utiliser des règles de QoS pour définir un débit de QoS *limite* et un débit de QoS *garantie*.

- Limite de débit QoS

  Le débit de qualité de service *limite* limite l'impact d'une charge de travail sur les ressources système en limitant le débit de la charge de travail à un nombre maximal d'IOPS ou de Mo/sec, ou d'IOPS et de Mo/sec.

- Garantie de débit QoS

  La qualité de service *Guarantee* garantit que les charges de travail stratégiques atteignent des objectifs de débit minimaux, indépendamment de la demande des charges de travail concurrentes, en garantissant que le débit pour la charge de travail stratégique ne passe pas en dessous d'un nombre minimal d'IOPS, de Mo/sec, ou d'IOPS et de Mo/sec.

Étapes

1. Dans System Manager, sélectionnez **Storage**.
2. Placez le pointeur de la souris sur le nom de l'unité de stockage à modifier.
3. Sélectionnez ⋮, puis **Modifier**.

4. Mettez à jour les paramètres de l'unité de stockage si nécessaire pour augmenter la capacité, modifier la stratégie QoS et mettre à jour le mappage de l'hôte.

Et la suite ?

Si vous avez augmenté la taille de votre unité de stockage, vous devez relancer l'analyse de l'unité de stockage sur l'hôte pour qu'il reconnaisse le changement de taille.

Supprimez les unités de stockage sur les systèmes de stockage ASA r2

Supprimez une unité de stockage si vous n'avez plus besoin de conserver les données contenues dans l'unité. La suppression d'unités de stockage qui ne sont plus nécessaires peut vous aider à libérer de l'espace pour d'autres applications hôtes.

Avant de commencer

Si l'unité de stockage à supprimer se trouve dans un groupe de cohérence faisant partie de la relation de réplication, vous devez d'"retirez l'unité de stockage du groupe de cohérence"abord la supprimer.

Étapes

1. Dans System Manager, sélectionnez **Storage**.
2. Placez le pointeur de la souris sur le nom de l'unité de stockage à supprimer.
3. Sélectionnez ⋮, puis **Supprimer**.
4. Confirmez que la suppression ne peut pas être annulée.
5. Sélectionnez **Supprimer**.

Et la suite ?

Vous pouvez utiliser l'espace libéré de l'unité de stockage supprimée vers "augmentez la taille" des unités de stockage qui nécessitent de la capacité supplémentaire.

Limites de stockage de ASA r2

Pour optimiser les performances, la configuration et le support, vous devez tenir compte des limites de stockage de ASA r2.

Les systèmes ASA r2 prennent en charge les éléments suivants :

Nombre max. De nœuds par cluster	2
Taille max. De l'unité de stockage	128 TO

Pour en savoir plus

Pour obtenir la liste complète des limites de stockage ASA r2 les plus récentes, reportez-vous à "NetApp Hardware Universe"la section .

Protégez vos données

Créez des copies Snapshot pour sauvegarder vos données sur les systèmes de stockage ASA r2

Pour sauvegarder des données sur votre système ASA r2, vous devez créer un snapshot. Vous pouvez utiliser ONTAP System Manager pour créer un snapshot manuel d'une seule unité de stockage ou pour créer un groupe de cohérence et planifier des snapshots automatiques de plusieurs unités de stockage en même temps.

Étape 1 : créez un groupe de cohérence éventuellement

Un groupe de cohérence est un ensemble d'unités de stockage gérées comme une seule unité. Créez des groupes de cohérence pour simplifier la gestion du stockage et la protection des données pour les charges de travail applicatives sur plusieurs unités de stockage. Supposons par exemple que vous disposez d'une base de données constituée de 10 unités de stockage dans un groupe de cohérence et que vous devez sauvegarder l'ensemble de la base de données. Au lieu de sauvegarder chaque unité de stockage, vous pouvez sauvegarder l'ensemble de la base de données en ajoutant simplement la protection des données Snapshot au groupe de cohérence.

Créez un groupe de cohérence avec de nouvelles unités de stockage ou un groupe de cohérence avec des unités de stockage existantes.

Utilisez de nouvelles unités de stockage

Étapes

1. Dans System Manager, sélectionnez **protection > groupes de cohérence**.
2. Sélectionnez + Add, puis **utilisation de nouvelles unités de stockage**.
3. Entrez un nom pour la nouvelle unité de stockage, le nombre d'unités et la capacité par unité.

   Si vous créez plusieurs unités, chaque unité est créée avec la même capacité et le même système d'exploitation hôte. Pour attribuer une capacité différente à chaque unité, sélectionnez **plus d'options**, puis sélectionnez **Ajouter une capacité différente**.
4. Sélectionnez le système d'exploitation hôte et le mappage d'hôte.
5. Sélectionnez **Ajouter**.

Et la suite ?

Vous avez créé un groupe de cohérence contenant les unités de stockage que vous souhaitez protéger. Vous êtes maintenant prêt à créer un snapshot.

Utiliser les unités de stockage existantes

Étapes

1. Dans System Manager, sélectionnez **protection > groupes de cohérence**.
2. Sélectionnez + Add, puis **en utilisant des unités de stockage existantes**.
3. Indiquez le nom du groupe de cohérence, puis recherchez et sélectionnez les unités de stockage à inclure dans le groupe de cohérence.
4. Sélectionnez **Ajouter**.

Et la suite ?

Vous avez créé un groupe de cohérence contenant les unités de stockage que vous souhaitez protéger. Vous êtes maintenant prêt à créer un snapshot.

Étape 2 : créer un instantané

Un snapshot est une copie locale en lecture seule de vos données, que vous pouvez utiliser pour restaurer des unités de stockage à des points spécifiques dans le temps.

Les snapshots peuvent être créés à la demande ou automatiquement à intervalles réguliers en fonction d'un "règle snapshot et planification". La règle et la planification des snapshots indiquent quand créer les snapshots, combien de copies conserver, comment les nommer et comment les étiqueter pour la réplication. Par exemple, un système peut créer un snapshot tous les jours à 12:10, conserver les deux copies les plus récentes, les nommer « quotidien » (ajouté à un horodatage) et les étiqueter « quotidien » pour la réplication.

Types de snapshots

Vous pouvez créer un snapshot à la demande d'une unité de stockage ou d'un groupe de cohérence. Vous pouvez créer des snapshots automatisés d'un groupe de cohérence contenant plusieurs unités de stockage. Vous ne pouvez pas créer de snapshots automatisés pour une seule unité de stockage.

- Snapshots à la demande

  Un snapshot à la demande d'une unité de stockage peut être créé à tout moment. L'unité de stockage n'a pas besoin d'être membre d'un groupe de cohérence pour être protégée par un snapshot à la demande. Si

vous créez un snapshot à la demande d'une unité de stockage membre d'un groupe de cohérence, les autres unités de stockage du groupe de cohérence ne sont pas incluses dans le snapshot à la demande. Si vous créez un snapshot à la demande d'un groupe de cohérence, toutes les unités de stockage du groupe de cohérence sont incluses dans le snapshot.

- Snapshots automatisés

  Les snapshots automatisés sont créés à l'aide de règles Snapshot. Pour appliquer une règle de snapshot à une unité de stockage en vue de la création automatique de snapshots, l'unité de stockage doit être membre d'un groupe de cohérence. Si vous appliquez une règle de snapshot à un groupe de cohérence, toutes les unités de stockage du groupe de cohérence sont protégées par des snapshots automatisés.

Créez un snapshot d'un groupe de cohérence ou d'une unité de stockage.

Snapshot d'un groupe de cohérence

Étapes

1. Dans System Manager, sélectionnez **protection > groupes de cohérence**.
2. Placez le curseur de la souris sur le nom du groupe de cohérence à protéger.
3. Sélectionnez ⋮ , puis **protéger**.
4. Si vous souhaitez créer un instantané immédiat à la demande, sous **protection locale**, sélectionnez **Ajouter un instantané maintenant**.

   La protection locale crée l'instantané sur le même cluster contenant l'unité de stockage.

   a. Entrez un nom pour le snapshot ou acceptez le nom par défaut, puis saisissez une étiquette SnapMirror.

      Le libellé SnapMirror est utilisé par la destination distante.

5. Si vous souhaitez créer des instantanés automatisés à l'aide d'une stratégie d'instantanés, sélectionnez **planifier des instantanés**.

   a. Sélectionnez une règle de snapshots.

      Acceptez la règle de snapshot par défaut, sélectionnez une règle existante ou créez une nouvelle règle.

Option	Étapes
Sélectionnez une politique de snapshots existante	Sélectionnez ⌄ en regard de la stratégie par défaut, puis sélectionnez la stratégie existante que vous souhaitez utiliser.
Créer une politique de snapshots	i. Sélectionnez + Add ; puis entrez les paramètres de la règle de snapshot. ii. Sélectionnez **Ajouter une stratégie**.

6. Si vous souhaitez répliquer vos snapshots sur un cluster distant, sous **protection distante**, sélectionnez **répliquer sur un cluster distant**.
   a. Sélectionnez le cluster source et la VM de stockage, puis sélectionnez la règle de réplication.

      Le transfert initial des données pour la réplication démarre immédiatement par défaut.

7. Sélectionnez **Enregistrer**.

Instantané de l'unité de stockage

Étapes

1. Dans System Manager, sélectionnez **Storage**.
2. Placez le pointeur de la souris sur le nom de l'unité de stockage que vous souhaitez protéger.
3. Sélectionnez ⋮ , puis **protéger**. Si vous souhaitez créer un instantané immédiat à la demande, sous **protection locale**, sélectionnez **Ajouter un instantané maintenant**.

   La protection locale crée l'instantané sur le même cluster contenant l'unité de stockage.

4. Entrez un nom pour le snapshot ou acceptez le nom par défaut, puis saisissez une étiquette SnapMirror.

   Le libellé SnapMirror est utilisé par la destination distante.

5. Si vous souhaitez créer des instantanés automatisés à l'aide d'une stratégie d'instantanés, sélectionnez **planifier des instantanés**.

   a. Sélectionnez une règle de snapshots.

      Acceptez la règle de snapshot par défaut, sélectionnez une règle existante ou créez une nouvelle règle.

Option	Étapes
Sélectionnez une politique de snapshots existante	Sélectionnez ⌄ en regard de la stratégie par défaut, puis sélectionnez la stratégie existante que vous souhaitez utiliser.
Créer une politique de snapshots	i. Sélectionnez + Add ; puis entrez les paramètres de la règle de snapshot. ii. Sélectionnez **Ajouter une stratégie**.

6. Si vous souhaitez répliquer vos snapshots sur un cluster distant, sous **protection distante**, sélectionnez **répliquer sur un cluster distant**.

   a. Sélectionnez le cluster source et la VM de stockage, puis sélectionnez la règle de réplication.

      Le transfert initial des données pour la réplication démarre immédiatement par défaut.

7. Sélectionnez **Enregistrer**.

Et la suite ?

Maintenant que vos données sont protégées avec des snapshots, vous devez "configuration de la réplication snapshot"copier vos groupes de cohérence vers un site distant à des fins de sauvegarde et de reprise d'activité.

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 Snapshot à partir d'un système de stockage ASA r2 n'est prise en charge que sur un autre système de stockage ASA r2. Vous ne pouvez pas répliquer les snapshots d'un système ASA r2 vers un système ASA, AFF ou FAS actuel.

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.

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.

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 **Lauch 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 : vous pouvez éventuellement créer une règle de réplication

La règle de réplication des snapshots définit le moment où les mises à jour effectuées sur le cluster ASA r2 sont répliquées sur le site distant.

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. Sélectionnez le **Type de stratégie**.

Option	Étapes
Copiez les données sur le site distant une fois qu'elles ont été écrites sur la source.	a. Sélectionnez **Asynchronous**. b. Sous **transférer des instantanés à partir de la source**, acceptez le programme de transfert par défaut ou sélectionnez un autre programme. c. Sélectionnez cette option pour transférer tous les instantanés ou pour créer des règles afin de déterminer les snapshots à transférer. d. Activez éventuellement la compression réseau.

Option	Étapes
Écrire simultanément les données sur les sites source et distant	a. Sélectionnez **synchrone**.

6. 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

Si vous souhaitez verrouiller vos snapshots de destination, vous devez d'"Initialiser l'horloge de conformité de snapshot"abord 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	a. Sélectionnez **destinations locales**, puis sélectionnez Replicate. b. Recherchez et sélectionnez le groupe de cohérence source. Le groupe de cohérence *source* fait référence au groupe de cohérence de votre cluster local que vous souhaitez répliquer.

Option	Étapes
Sources locales	a. Sélectionnez **sources locales**, puis sélectionnez Replicate . b. Recherchez et sélectionnez le groupe de cohérence source. Le groupe de cohérence *source* fait référence au groupe de cohérence de votre cluster local que vous souhaitez répliquer. c. 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

1. Dans System Manager, sélectionnez **protection > réplication**.
2. Passez le curseur sur la relation de réplication que vous souhaitez tester, puis sélectionnez ⋮.
3. Sélectionnez **Test failover**.
4. 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.

Protégez vos applications Kubernetes sur les systèmes de stockage ASA r2

Utilisez Astra Control Center pour protéger vos applications Kubernetes. ASTRA Control Center vous permet de migrer des applications et des données d'un cluster Kubernetes à un autre, de répliquer des applications sur un système distant à l'aide de la technologie NetApp SnapMirror et de cloner des applications de la phase intermédiaire à la production.

Pour en savoir plus

"En savoir plus sur la protection des applications Kubernetes à l'aide d'Astra Control".

Restaurez les données sur les systèmes de stockage ASA r2

Les données d'un groupe de cohérence ou d'une unité de stockage protégé par des snapshots peuvent être restaurées en cas de perte ou de corruption.

Restaurez un groupe de cohérence

La restauration d'un groupe de cohérence remplace les données de toutes les unités de stockage du groupe de cohérence par les données d'un snapshot. Les modifications apportées aux unités de stockage après la création de l'instantané ne sont pas restaurées.

Vous pouvez restaurer un groupe de cohérence à partir d'un snapshot local ou distant.

Restauration à partir d'un snapshot local

Étapes

1. Dans System Manager, sélectionnez **protection > groupes de cohérence**.
2. Double-cliquez sur le groupe de cohérence contenant les données à restaurer.

   La page d'informations sur les groupes de cohérence s'ouvre.
3. Sélectionnez **instantanés**.
4. Sélectionnez l'instantané à restaurer, puis sélectionnez ⋮.
5. Sélectionnez **Restaurer le groupe de cohérence à partir de cet instantané**, puis sélectionnez **Restaurer**.

Restauration à partir d'un snapshot distant

Étapes

1. Dans System Manager, sélectionnez **protection > réplication**.
2. Sélectionnez **destinations locales**.
3. Sélectionnez la **Source** que vous souhaitez restaurer, puis sélectionnez ⋮.
4. Sélectionnez **Restaurer**.
5. Sélectionnez le cluster, la machine virtuelle de stockage et le groupe de cohérence vers lesquels vous souhaitez restaurer les données.
6. Sélectionnez l'instantané à partir duquel vous souhaitez restaurer.
7. Lorsque vous y êtes invité, entrez "restaurer", puis sélectionnez **Restaurer**.

Résultat

Votre groupe de cohérence est restauré à partir du point dans le temps du snapshot utilisé pour la restauration.

Restaurer une unité de stockage

La restauration d'une unité de stockage remplace toutes les données de l'unité de stockage par les données d'un instantané. Les modifications apportées à l'unité de stockage après la création de l'instantané ne sont pas restaurées.

Étapes

1. Dans System Manager, sélectionnez **Storage**.
2. Double-cliquez sur l'unité de stockage contenant les données à restaurer.

   La page de détails de l'unité de stockage s'ouvre.

3. Sélectionnez **instantanés**.
4. Sélectionnez l'instantané à restaurer.
5. Sélectionnez ⋮, puis **Restaurer**.
6. Sélectionnez **utiliser cet instantané pour restaurer l'unité de stockage**, puis sélectionnez **Restaurer**.

Résultat

Votre unité de stockage est restaurée au point dans le temps de l'instantané utilisé pour la restauration.

Gestion des groupes de cohérence ONTAP sur les systèmes de stockage ASA r2

Un groupe de cohérence est un ensemble d'unités de stockage gérées comme une seule unité. Utilisation de groupes de cohérence pour une gestion simplifiée du stockage. Supposons par exemple que vous disposez d'une base de données constituée de 10 unités de stockage dans un groupe de cohérence et que vous devez sauvegarder l'ensemble de la base de données. Au lieu de sauvegarder chaque unité de stockage, vous pouvez sauvegarder l'ensemble de la base de données en ajoutant simplement la protection des données Snapshot au groupe de cohérence. La sauvegarde des unités de stockage en tant que groupe de cohérence au lieu de individuellement permet également d'effectuer une sauvegarde cohérente de toutes les unités, tandis que la sauvegarde individuelle des unités pourrait créer des incohérences.

Ajouter la protection des données de snapshot à un groupe de cohérence

Lorsque vous ajoutez une protection des données de snapshot à un groupe de cohérence, des snapshots locaux du groupe de cohérence sont effectués à intervalles réguliers, selon une planification prédéfinie.

Vous pouvez utiliser des instantanés "restaurez les données"perdus ou corrompus.

Étapes

1. Dans System Manager, sélectionnez **protection > groupes de cohérence**.
2. Placez le curseur sur le groupe de cohérence à protéger.
3. Sélectionnez ⋮, puis **Modifier**.
4. Sous **protection locale**, sélectionnez **planifier les instantanés**.

5. Sélectionnez une règle de snapshots.

   Acceptez la règle de snapshot par défaut, sélectionnez une règle existante ou créez une nouvelle règle.

Option	Étapes
Sélectionnez une politique de snapshots existante	Sélectionnez en regard de la stratégie par défaut, puis sélectionnez la stratégie existante que vous souhaitez utiliser.
Créer une politique de snapshots	a. Sélectionnez + Add ; puis entrez le nouveau nom de la stratégie. b. Sélectionnez la portée de la règle. c. Sous **horaires**, sélectionnez + Add . d. Sélectionnez le nom qui apparaît sous **Nom de l'horaire**; puis sélectionnez . e. Sélectionnez la planification de la stratégie. f. Sous **nombre maximal de snapshots**, entrez le nombre maximal de snapshots que vous souhaitez conserver pour le groupe de cohérence. g. Si vous le souhaitez, sous **SnapMirror label**, saisissez un libellé SnapMirror. h. Sélectionnez **Enregistrer**.

6. Sélectionnez **Modifier**.

Et la suite

Maintenant que vos données sont protégées à l'aide de snapshots, vous devez "configuration de la réplication snapshot"copier vos groupes de cohérence vers un site distant à des fins de sauvegarde et de reprise d'activité.

Supprimez la protection des données Snapshot d'un groupe de cohérence

Lorsque vous supprimez la protection des données de snapshot d'un groupe de cohérence, les snapshots sont désactivés pour toutes les unités de stockage du groupe de cohérence.

Étapes

1. Dans System Manager, sélectionnez **protection > groupes de cohérence**.
2. Placez le curseur de la souris sur le groupe de cohérence que vous souhaitez arrêter de protéger.
3. Sélectionnez , puis **Modifier**.
4. Sous **protection locale**, désélectionnez Programmer les instantanés.
5. Sélectionnez **Modifier**.

Résultat

Aucun snapshot ne sera pris pour les unités de stockage du groupe de cohérence.

Ajouter des unités de stockage à un groupe de cohérence

Augmentez la quantité de stockage gérée par un groupe de cohérence en ajoutant des unités de stockage au groupe de cohérence.

Vous pouvez ajouter des unités de stockage existantes à votre groupe de cohérence ou créer de nouvelles unités de stockage à ajouter au groupe de cohérence.

Ajouter des unités de stockage existantes

Étapes

1. Dans System Manager, sélectionnez **protection > groupes de cohérence**.
2. Placez le curseur de la souris sur le groupe de cohérence à développer.
3. Sélectionnez ⋮, puis **développer**.
4. Sélectionnez **utilisation des unités de stockage existantes**.
5. Sélectionnez les unités de stockage à ajouter au groupe de cohérence, puis sélectionnez **expand**.

Ajouter de nouvelles unités de stockage

Étapes

1. Dans System Manager, sélectionnez **protection > groupes de cohérence**.
2. Placez le curseur de la souris sur le groupe de cohérence à développer.
3. Sélectionnez ⋮, puis **développer**.
4. Sélectionnez **utilisation de nouvelles unités de stockage**.
5. Entrez le nombre d'unités que vous souhaitez créer et la capacité par unité.

   Si vous créez plusieurs unités, chaque unité est créée avec la même capacité et le même système d'exploitation hôte. Pour attribuer une capacité différente à chaque unité, sélectionnez **Ajouter une capacité différente** pour attribuer une capacité différente à chaque unité.

6. Sélectionnez **développer**.

Et la suite

Après avoir créé une nouvelle unité de stockage, vous devez "ajoutez des initiateurs hôtes" et "mappez l'unité de stockage nouvellement créée sur un hôte". L'ajout d'initiateurs hôtes permet aux hôtes d'accéder aux unités de stockage et d'effectuer des opérations de données. Le mappage d'une unité de stockage à un hôte permet à l'unité de stockage de commencer à transmettre des données à l'hôte auquel elle est mappée.

Et la suite ?

Les snapshots existants du groupe de cohérence n'incluent pas les nouvelles unités de stockage ajoutées. "créer un instantané immédiat"Afin de protéger les unités de stockage que vous venez d'ajouter, vous devez utiliser votre groupe de cohérence jusqu'à la création automatique du prochain snapshot planifié.

Supprimer une unité de stockage d'un groupe de cohérence

Vous devez supprimer une unité de stockage d'un groupe de cohérence si vous souhaitez supprimer l'unité de stockage, si vous souhaitez la gérer dans le cadre d'un autre groupe de cohérence ou si vous n'avez plus besoin de protéger les données qu'elle contient. La suppression d'une unité de stockage d'un groupe de cohérence rompt la relation entre l'unité de stockage et le groupe de cohérence, mais ne supprime pas l'unité

de stockage.

Étapes

1. Dans System Manager, sélectionnez **protection > groupes de cohérence**.
2. Double-cliquez sur le groupe de cohérence dont vous souhaitez supprimer une unité de stockage.
3. Dans la section **vue d'ensemble**, sous **unités de stockage**, sélectionnez l'unité de stockage à supprimer, puis sélectionnez **Supprimer du groupe de cohérence**.

Résultat

L'unité de stockage n'est plus membre du groupe de cohérence.

Et la suite

Si vous devez continuer à protéger les données de l'unité de stockage, ajoutez-la à un autre groupe de cohérence.

Supprimez un groupe de cohérence

Si vous n'avez plus besoin de gérer les membres d'un groupe de cohérence comme une seule unité, vous pouvez supprimer le groupe de cohérence. Une fois un groupe de cohérence supprimé, les unités de stockage du groupe restent actives sur le cluster.

Avant de commencer

Si le groupe de cohérence à supprimer appartient à une relation de réplication, vous devez interrompre la relation avant de supprimer le groupe de cohérence. Après avoir supprimé un groupe de cohérence de réplication antérieur, les unités de stockage appartenant au groupe de cohérence restent actives sur le cluster et les copies répliquées y sont conservées.

Étapes

1. Dans System Manager, sélectionnez **protection > groupes de cohérence**.
2. Placez le curseur de la souris sur le groupe de cohérence à supprimer.
3. Sélectionnez ⋮, puis **Supprimer**.
4. Acceptez l'avertissement, puis sélectionnez **Supprimer**.

Et la suite ?

Une fois que vous avez supprimé un groupe de cohérence, les unités de stockage qui se trouvent auparavant dans ce groupe ne sont plus protégées par des snapshots. Envisagez d'ajouter ces unités de stockage à un autre groupe de cohérence pour les protéger contre la perte de données.

Gérez les stratégies et les plannings de protection des données ONTAP sur les systèmes de stockage ASA r2

Utilisez les règles de snapshot pour protéger les données de vos groupes de cohérence selon une planification automatisée. Utilisez les planifications de règles au sein des règles de snapshot pour déterminer la fréquence de création des snapshots.

Créez un nouveau planning de stratégie de protection

Une planification de règle de protection définit la fréquence à laquelle une règle de snapshots est exécutée. Vous pouvez créer des horaires à exécuter à intervalles réguliers en fonction d'un certain nombre de jours, d'heures ou de minutes. Par exemple, vous pouvez créer un programme à exécuter toutes les heures ou une

seule fois par jour. Vous pouvez également créer des horaires à exécuter à des heures spécifiques sur des jours spécifiques de la semaine ou du mois. Par exemple, vous pouvez créer un programme à exécuter à 12:15 le 20 de chaque mois.

La définition de plusieurs plannings de règles de protection vous permet d'augmenter ou de diminuer la fréquence des snapshots pour différentes applications. Vous bénéficiez ainsi d'un niveau de protection supérieur et d'un risque moindre de perte de données pour vos workloads stratégiques par rapport à ce qui pourrait être nécessaire pour les workloads moins stratégiques.

Étapes

1. Sélectionnez **protection > politiques**, puis **Programme**.
2. Sélectionnez + Add.
3. Entrez un nom pour le planning, puis sélectionnez les paramètres du planning.
4. Sélectionnez **Enregistrer**.

Et la suite ?

Maintenant que vous avez créé une nouvelle planification de règles, vous pouvez utiliser la nouvelle planification créée au sein de vos règles pour définir le moment où les snapshots sont effectués.

Création d'une règle de snapshots

Une règle définit la fréquence de création des snapshots, le nombre maximal de snapshots autorisés et la durée de conservation des snapshots.

Étapes

1. Dans System Manager, sélectionnez **protection > stratégies**, puis **règles d'instantanés**.
2. Sélectionnez + Add.
3. Entrez un nom pour la politique de snapshots.
4. Sélectionnez **Cluster** pour appliquer la stratégie à l'ensemble du cluster. Sélectionnez **Storage VM** pour appliquer la stratégie à une machine virtuelle de stockage individuelle.
5. Sélectionnez **Ajouter un planning**, puis entrez le planning de la stratégie de snapshot.
6. Sélectionnez **Ajouter une stratégie**.

Et la suite ?

Une fois que vous avez créé une politique de snapshots, vous pouvez l'appliquer à un groupe de cohérence. Des copies Snapshot du groupe de cohérence seront effectuées en fonction des paramètres définis dans la règle de copie Snapshot.

Applique une politique de snapshot à un groupe de cohérence

Appliquez une règle de snapshot à un groupe de cohérence pour créer, conserver et étiqueter automatiquement les snapshots du groupe de cohérence.

Étapes

1. Dans System Manager, sélectionnez **protection > stratégies**, puis **règles d'instantanés**.
2. Placez le pointeur de la souris sur le nom de la politique de snapshots que vous souhaitez appliquer.
3. Sélectionnez ⋮; puis **appliquer**.
4. Sélectionnez les groupes de cohérence auxquels vous souhaitez appliquer la règle de snapshot, puis sélectionnez **appliquer**.

Et la suite ?

Maintenant que vos données sont protégées avec des snapshots, vous devez "configurer une relation de réplication"copier vos groupes de cohérence vers un site distant à des fins de sauvegarde et de reprise d'activité.

Modifiez, supprimez ou désactivez une règle de snapshots

Modifiez une règle de snapshot pour modifier le nom de la règle, le nombre maximal de snapshots ou le libellé SnapMirror. Supprimez une règle pour la supprimer du cluster, ainsi que les données de sauvegarde qui y sont associées. Désactivez une règle pour arrêter temporairement la création ou le transfert de snapshots spécifiés par la règle.

Étapes

1. Dans System Manager, sélectionnez **protection > stratégies**, puis **règles d'instantanés**.
2. Placez le pointeur de la souris sur le nom de la règle de snapshot à modifier.
3. Sélectionnez ⋮, puis **Modifier**, **Supprimer** ou **Désactiver**.

Résultat

Vous avez modifié, supprimé ou désactivé la règle de snapshot.

Modifier une règle de réplication

Modifiez une règle de réplication pour modifier la description de la règle, la planification du transfert et les règles. Vous pouvez également modifier la stratégie pour activer ou désactiver la compression réseau.

Étapes

1. Dans System Manager, sélectionnez **protection > stratégies**.
2. Sélectionnez **stratégies de réplication**.
3. Passez le curseur sur la règle de réplication à modifier, puis sélectionnez ⋮.
4. Sélectionnez **Modifier**.
5. Mettez à jour la stratégie, puis sélectionnez **Enregistrer**.

Résultat

Vous avez modifié la règle de réplication.

Sécurisez vos données

Chiffrement des données au repos sur les systèmes de stockage ASA r2

Lorsque vous chiffrez les données au repos, elles ne peuvent pas être lues si un support de stockage est requalifié, perdu ou volé. Vous pouvez utiliser ONTAP System Manager pour chiffrer vos données au niveau matériel et logiciel afin de bénéficier d'une protection double couche.

NetApp Storage Encryption (NSE) prend en charge le chiffrement matériel à l'aide de disques à autochiffrement (SED). Les disques SED chiffrent les données au fur et à mesure de leur écriture. Chaque SED contient une clé de chiffrement unique. Les données chiffrées stockées sur le SED ne peuvent pas être lues sans la clé de chiffrement du SED. Les nœuds qui tentent de lire à partir d'un SED doivent être authentifiés pour accéder à la clé de cryptage du SED. Les nœuds sont authentifiés en obtenant une clé

d'authentification auprès d'un gestionnaire de clés, puis en présentant la clé d'authentification au SED. Si la clé d'authentification est valide, le SED donnera au nœud sa clé de cryptage pour accéder aux données qu'il contient.

Utilisez le gestionnaire de clés intégré ASA r2 ou un gestionnaire de clés externe pour transmettre des clés d'authentification à vos nœuds.

En plus de NSE, vous pouvez également activer le chiffrement logiciel afin d'ajouter une couche supplémentaire de sécurité à vos données.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. Dans la section **sécurité**, sous **cryptage**, sélectionnez **configurer**.
3. Configurez le gestionnaire de clés.

Option	Étapes
Configurez le gestionnaire de clés intégré	a. Sélectionnez **Onboard Key Manager** pour ajouter les serveurs de clés. b. Saisissez une phrase de passe.
Configurez un gestionnaire de clés externe	a. Sélectionnez **Gestionnaire de clés externe** pour ajouter les serveurs de clés. b. Sélectionnez + Add pour ajouter les serveurs clés. c. Ajoutez les certificats de l'autorité de certification du serveur KMIP. d. Ajoutez les certificats client KMIP.

4. Sélectionnez **chiffrement double couche** pour activer le chiffrement logiciel.
5. Sélectionnez **Enregistrer**.

Et la suite ?

Une fois que vous avez chiffré vos données au repos, si vous utilisez le protocole NVMe/TCP, vous pouvez le "chiffrez toutes les données envoyées sur le réseau" faire entre votre hôte NVMe/TCP et votre système ASA r2.

Protégez-vous contre les attaques par ransomware sur les systèmes de stockage ASA r2

Pour une protection renforcée contre les attaques par ransomware, répliquez les snapshots sur un cluster distant, puis verrouillez les snapshots de destination pour les protéger contre toute tentative d'altération. 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 n'est jamais compromise par une attaque par ransomware.

Initialiser l'horloge SnapLock Compliance

Avant de pouvoir créer des instantanés inviolables, vous devez initialiser l'horloge SnapLock Compliance sur vos clusters locaux et de destination.

Étapes

1. Sélectionnez **Cluster > Présentation**.
2. Dans la section **nœuds**, sélectionnez **initialiser horloge SnapLock Compliance**.
3. Sélectionnez **initialiser**.
4. Vérifiez que l'horloge de conformité est initialisée.
   a. Sélectionnez **Cluster > Présentation**.
   b. Dans la section **nœuds**, sélectionnez ; puis **SnapLock Compliance horloge**.

Et la suite ?

Après avoir initialisé l'horloge SnapLock Compliance sur vos clusters locaux et de destination, vous êtes prêt à "créer une relation de réplication avec des snapshots verrouillés".

Sécurisez les connexions NVMe sur vos systèmes de stockage ASA r2

Si vous utilisez le protocole NVMe, vous pouvez configurer l'authentification intrabande pour renforcer la sécurité de vos données. L'authentification intrabande permet une authentification bidirectionnelle et unidirectionnelle sécurisée entre vos hôtes NVMe et votre système ASA r2. L'authentification intrabande est disponible pour tous les hôtes NVMe. Si vous utilisez le protocole NVMe/TCP, vous pouvez renforcer encore la sécurité de vos données en configurant transport Layer Security (TLS) pour chiffrer toutes les données envoyées sur le réseau entre vos hôtes NVMe/TCP et votre système ASA r2.

Étapes

1. Sélectionnez **hosts**, puis **NVMe**.
2. Sélectionnez + Add .
3. Entrez le nom d'hôte, puis sélectionnez le système d'exploitation hôte.
4. Entrez une description d'hôte, puis sélectionnez la VM de stockage à connecter à l'hôte.
5. Sélectionnez en regard du nom d'hôte.
6. Sélectionnez **authentification intrabande**.
7. Si vous utilisez le protocole NVMe/TCP, sélectionnez **nécessite TLS (transport Layer Security)**.
8. Sélectionnez **Ajouter**.

Résultat

La sécurité de vos données est renforcée par l'authentification intrabande et/ou TLS.