Documentation de ASA r2

ASA r2

NetApp
September 26, 2024

Sommaire

Documentation de ASA r2 . . . 1
Notes de mise à jour . . . 2
Nouveautés de ONTAP 9.16.0 pour les systèmes ASA r2 . . . 2
Commencez . . . 4
En savoir plus sur les systèmes de stockage ASA r2 . . . 4
Démarrage rapide des systèmes de stockage ASA r2 . . . 4
Installez votre système ASA r2 . . . 5
Configurez votre système ASA r2 . . . 28
Gérez vos données avec ONTAP . . . 32
Vidéos de démonstration du système de stockage ASA r2 . . . 32
Gérez votre stockage . . . 32
Protégez vos données . . . 42
Sécurisez vos données . . . 58
Administration et contrôle . . . 61
Gestion de l’accès client aux machines virtuelles de stockage sur les systèmes de stockage ASA r2 . . . 61
Gestion de la mise en réseau des clusters sur les systèmes de stockage ASA r2 . . . 63
Surveillez l’utilisation et augmentez la capacité . . . 65
Mise à jour du firmware sur les systèmes de stockage ASA r2 . . . 68
Optimisez la sécurité et les performances du cluster grâce aux informations exploitables du système de stockage ASA r2 . . . 70
Affichage des tâches et événements de cluster sur les systèmes de stockage ASA r2 . . . 71
Gérer des nœuds . . . 72
Gestion des comptes et des rôles utilisateur sur les systèmes de stockage ASA r2 . . . 73
Gestion des certificats de sécurité sur les systèmes de stockage ASA r2 . . . 75
Vérifiez la connectivité hôte sur votre système de stockage ASA r2 . . . 77
Assurez la maintenance de votre système de stockage ASA r2 . . . 79
En savoir plus >> . . . 80
ASA r2 pour utilisateurs intensifs ONTAP . . . 80
Obtenez de l’aide . . . 91
Gérez AutoSupport sur les systèmes de stockage ASA r2 . . . 91
Envoi et consultation des dossiers de demande de support pour les systèmes de stockage ASA r2 . . . 93
Mentions légales . . . 94
Droits d’auteur . . . 94
Marques déposées . . . 94
Brevets . . . 94
Politique de confidentialité . . . 94
Source ouverte . . . 94

Documentation de ASA r2

Notes de mise à jour

Nouveautés de ONTAP 9.16.0 pour les systèmes ASA r2

Découvrez les nouvelles fonctionnalités disponibles dans ONTAP 9.16.0 pour les systèmes ASA r2.

Plateformes

Mise à jour	Description
Nouvelles plateformes	Les nouveaux systèmes NetApp ASA r2 suivants sont disponibles. Ces plateformes offrent une solution matérielle et logicielle unifiée qui offre une expérience simplifiée et adaptée aux besoins des clients qui utilisent uniquement un SAN. • ASA A1K • ASA A70 • ASA A90

System Manager

Mise à jour	Description
"Prise en charge optimisée des clients SAN uniquement"	System Manager est rationalisé pour prendre en charge les fonctionnalités SAN essentielles tout en supprimant la visibilité des fonctionnalités non prises en charge dans les environnements SAN.

Gestion du stockage

Mise à jour	Description
"Gestion du stockage simplifiée"	Pour une gestion du stockage simplifiée, les systèmes ASA r2 utilisent des unités de stockage avec des groupes de cohérence. • Une *unité de stockage* permet à vos hôtes SAN de disposer de l'espace de stockage pour les opérations de données. Une unité de stockage désigne une LUN pour les hôtes SCSI ou un namespace NVMe pour les hôtes NVMe. • *Un groupe de cohérence* est un ensemble d'unités de stockage gérées comme une seule unité.

Sécurité des données

Mise à jour	Description
"Gestionnaire de clés intégré et chiffrement double couche"	Les systèmes ASA r2 prennent en charge un gestionnaire de clés intégré et un chiffrement double couche (matériel et logiciel).

Commencez

En savoir plus sur les systèmes de stockage ASA r2

Les nouveaux systèmes NetApp ASA r2 (ASA A1K, ASA A70 et ASA A90) proposent une solution matérielle et logicielle unifiée qui simplifie l'expérience en fonction des besoins des clients qui utilisent exclusivement SAN.

Les systèmes ASA r2 prennent en charge tous les protocoles SAN (iSCSI, FC, NVMe/FC, NVMe/TCP) sur un déploiement de paire haute disponibilité unique. Les protocoles SCSI (iSCSI et FC) utilisent une architecture actif-actif symétrique pour les chemins d'accès multiples, de sorte que tous les chemins entre les hôtes et le stockage soient actifs/optimisés. Les protocoles NVMe prennent en charge les chemins directs entre les hôtes et le stockage.

Sur un système ASA r2, le logiciel ONTAP et System Manager sont optimisés pour prendre en charge les fonctionnalités SAN essentielles tout en supprimant les fonctionnalités et fonctionnalités non prises en charge dans les environnements SAN.

Les systèmes ASA r2 introduisent l'utilisation d'unités de stockage avec groupes de cohérence :

- Une *unité de stockage* permet à vos hôtes SAN de disposer de l'espace de stockage pour les opérations de données. Une unité de stockage désigne une LUN pour les hôtes SCSI ou un namespace NVMe pour les hôtes NVMe.
- *Un groupe de cohérence* est un ensemble d'unités de stockage gérées comme une seule unité.

Les systèmes ASA r2 utilisent des unités de stockage et des groupes de cohérence pour simplifier la gestion du stockage et la protection des données. 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 individuellement, vous pouvez protéger l'ensemble de la base de données en sauvegardant le groupe de cohérence.

Pour vous aider à sécuriser vos données contre les attaques malveillantes, telles que le vol ou les ransomware, les systèmes ASA r2 prennent en charge un gestionnaire de clés intégré, un chiffrement double couche, des copies Snapshot inviolables, une authentification multifacteur et la vérification multiadministrateur.

Les systèmes ASA r2 ne prennent pas en charge la combinaison de clusters avec les systèmes ASA, AFF ou FAS actuels.

Pour en savoir plus

- Pour en savoir plus sur la prise en charge et les limites des systèmes ASA r2"NetApp Hardware Universe", consultez le .
- En savoir plus sur "Nouveaux systèmes ASA r2 par rapport aux systèmes ASA".
- En savoir plus sur "NetApp ASA"le .

Démarrage rapide des systèmes de stockage ASA r2

Pour être opérationnel avec votre système ASA r2, vous installez vos composants matériels, configurez votre cluster, configurez l'accès aux données depuis vos hôtes vers le système de stockage et provisionnez votre stockage.

1 **Installez et configurez votre matériel**

"Installation et configuration" Votre système ASA r2 et déployez-le comme une paire haute disponibilité dans votre environnement ONTAP.

2 **Configurez votre cluster**

Utilisez System Manager pour vous guider tout au long d'un processus simple et rapide pour "Configurez votre cluster ONTAP".

3 **Configurez l'accès aux données**

"Connectez votre système ASA r2 à vos clients SAN".

4 **Provisionner votre stockage**

"Provisionner le stockage" Pour commencer à transmettre des données à vos clients SAN.

Et la suite ?

Vous pouvez désormais utiliser System Manager pour protéger vos données par "création d'instantanés".

Installez votre système ASA r2

Workflow d'installation et de configuration pour les systèmes de stockage ASA r2

Pour installer et configurer votre système ASA r2, vous passez en revue la configuration matérielle requise, préparez votre site, installez et câblez les composants matériels, mettez le système sous tension et configurez votre cluster ONTAP.

1 **"Vérifiez les conditions requises pour l'installation du matériel"**

Vérifiez la configuration matérielle requise pour installer votre système de stockage ASA r2.

2 **"Préparez l'installation du système de stockage ASA r2"**

Pour préparer l'installation de votre système ASA r2, vous devez préparer le site, vérifier les exigences environnementales et électriques et vous assurer qu'il y a suffisamment d'espace dans le rack. Déballez ensuite l'équipement, comparez son contenu au bordereau d'expédition et enregistrez le matériel pour bénéficier des avantages de l'assistance.

3 **"Installez le matériel du système de stockage ASA r2"**

Pour installer le matériel, installez les kits de rails pour votre système de stockage et vos tiroirs, puis installez et sécurisez votre système de stockage dans l'armoire ou le rack de télécommunications. Ensuite, faites glisser les tablettes sur les rails. Enfin, fixez des périphériques de gestion des câbles à l'arrière du système de stockage pour organiser le routage des câbles.

4 **"Reliez les contrôleurs et les tiroirs de stockage au système de stockage ASA r2"**

Pour connecter les câbles du matériel, commencez par connecter les contrôleurs de stockage à votre réseau, puis connectez les contrôleurs à vos tiroirs de stockage.

5 **"Mettez le système de stockage ASA r2 sous tension"**

Avant de mettre les contrôleurs sous tension, mettez chaque tiroir NS224 sous tension et attribuez un ID de tiroir unique pour vous assurer que chaque tiroir est identifié de manière unique dans la configuration.

Conditions requises pour l'installation des systèmes de stockage ASA r2

Vérifiez l'équipement nécessaire et les précautions de levage pour votre système de stockage ASA r2 et vos tiroirs de stockage.

Équipement nécessaire pour l'installation

Pour installer votre système de stockage ASA r2, vous avez besoin de l'équipement et des outils suivants.

- Accès à un navigateur Web pour configurer votre système de stockage
- Sangle de décharge électrostatique (ESD)
- Lampe de poche
- Ordinateur portable ou console avec connexion USB/série
- Trombone ou stylo à pointe sphérique à pointe étroite pour le réglage des ID de tablette de stockage NS224
- Tournevis Phillips n°2

Précautions de levage

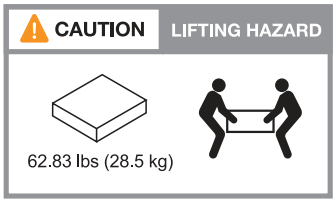
Les systèmes de stockage ASA r2 et les tiroirs de stockage NS224 sont très volumineux. Faites preuve de prudence lorsque vous soulevez et déplacez ces éléments.

Poids du système de stockage

Prenez les précautions nécessaires lors du déplacement ou du levage de votre système de stockage ASA r2.

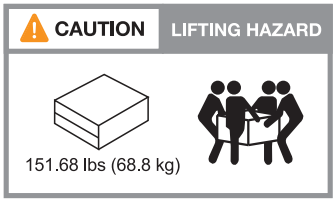
ASA A1K

Un système de stockage ASA A1K peut peser jusqu'à 28.5 kg (62.83 lb). Pour soulever le système, faire appel à deux personnes ou à un relevage hydraulique.



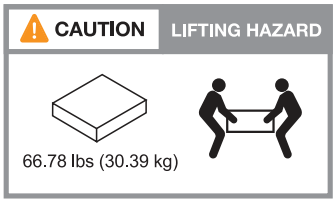
ASA A70 et ASA A90

Un système de stockage ASA A70 ou un système de stockage ASA A90 peut peser jusqu'à 68.8 kg (151.68 lb). Pour lever le système, faire appel à quatre personnes ou à un relevage hydraulique.



Poids de la tablette de stockage

Une étagère de stockage NS224 peut peser jusqu'à 30.29 kg (66.78 lb). Pour soulever la tablette de rangement, faites appel à deux personnes ou à un dispositif de levage hydraulique. Conservez tous les composants dans la tablette de stockage (avant et arrière) pour éviter de débalourer le poids de la tablette.



Informations associées

- "Informations de sécurité et avis réglementaires"

Et la suite ?

Après avoir examiné la configuration matérielle requise, vous "Préparez l'installation de votre système de stockage ASA r2".

Préparez l'installation d'un système de stockage ASA r2

Préparez l'installation de votre système de stockage ASA r2 en préparant le site, en décompressant les boîtes et en comparant le contenu des boîtes au bordereau d'expédition, puis en enregistrant le système pour accéder aux avantages du support.

Étape 1 : préparer le site

Pour installer votre système de stockage ASA r2, assurez-vous que le site et l'armoire ou le rack que vous prévoyez d'utiliser respectent les spécifications de votre configuration.

Étapes

1. Utilisez "NetApp Hardware Universe" pour vérifier que votre site répond aux exigences environnementales et électriques de votre système de stockage ASA r2.
2. Assurez-vous de disposer d'un espace de rack adéquat :
   - 4U en configuration HA pour le système de stockage
   - 2U pour chaque tiroir de stockage NS224
3. Installez les commutateurs réseau requis.

   Reportez-vous "Documentation du commutateur" au pour obtenir des instructions d'installation et "NetApp Hardware Universe" des informations sur la compatibilité.

Étape 2 : déballez les boîtes

Après avoir vérifié que le site et l'armoire ou le rack que vous prévoyez d'utiliser pour votre système de stockage ASA r2 répondent aux spécifications requises, déballez toutes les boîtes et comparez le contenu aux éléments du bordereau d'expédition.

Étapes

1. Ouvrez soigneusement toutes les boîtes et disposez le contenu de manière organisée.
2. Comparez le contenu que vous avez déballé avec la liste sur le bordereau d'expédition.

   Vous pouvez obtenir votre liste d'emballage en scannant le code QR sur le côté du carton d'expédition.

   Les éléments suivants sont quelques-uns des contenus que vous pouvez voir dans les boîtes.

   Assurez-vous que tous les éléments contenus dans les boîtes correspondent à la liste figurant sur le bordereau d'expédition. En cas d'écarts, notez-les pour prendre des mesures supplémentaires.

Matériel	Câbles	
• Panneau • Dispositif de gestion des câbles • Adieu les migrations de données onéreuses • Kits de rails avec instructions (en option) • Tiroir de stockage	• Câbles Ethernet de gestion (câbles RJ-45) • Câbles réseau • Cordons d'alimentation • Câbles de stockage (si vous avez commandé un espace de stockage supplémentaire) • Câble du port série USB-C.	

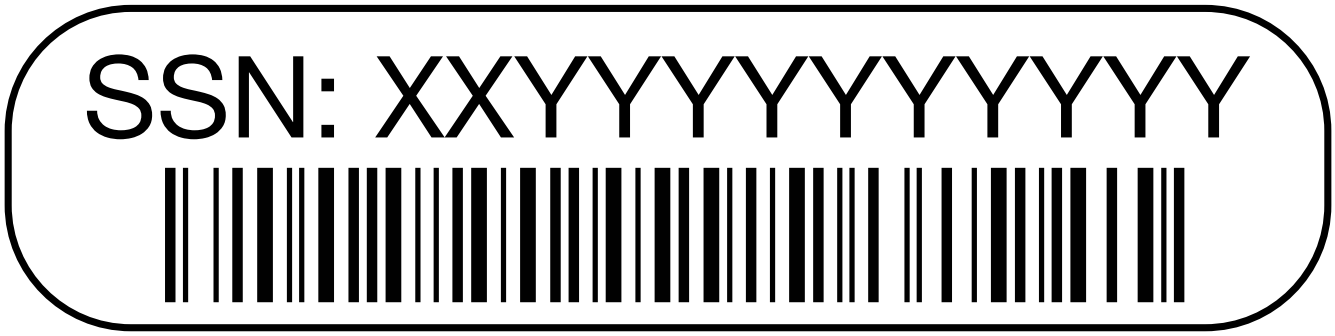
Étape 3 : enregistrez votre système de stockage

Après avoir vérifié que votre site répond aux spécifications de votre système de stockage ASA r2 et après avoir vérifié que vous disposez de toutes les pièces commandées, vous devez enregistrer votre système.

Étapes

1. Recherchez le numéro de série de votre système de stockage.

Vous trouverez le numéro sur le bordereau d'expédition, dans votre e-mail de confirmation ou sur le module de gestion du système du contrôleur après le déballage.



2. Accédez à la "Site de support NetApp".
3. Déterminez si vous devez enregistrer votre système de stockage :

Si vous êtes…	Suivez ces étapes…
Client NetApp existant	a. Connectez-vous à l'aide de votre nom d'utilisateur et de votre mot de passe. b. Sélectionnez **systèmes** > **Mes systèmes**. c. Vérifiez que le nouveau numéro de série est répertorié. d. Si ce n'est pas le cas, suivez les instructions destinées aux nouveaux clients NetApp.
Nouveau client NetApp	a. Cliquez sur **s'inscrire maintenant** et créez un compte. b. Sélectionnez **systèmes** > **Enregistrer systèmes**. c. Entrez le numéro de série du système de stockage et les détails demandés. Une fois votre inscription approuvée, vous pouvez télécharger tout logiciel requis. La procédure d'approbation peut prendre jusqu'à 24 heures.

Et la suite ?

Après avoir préparé l'installation de votre matériel ASA r2, vous "Installez le matériel de votre système de stockage ASA r2".

Installez votre système de stockage ASA r2

Après avoir préparé l'installation du système de stockage ASA r2, installez le matériel du système. Commencez par installer les kits de rails. Installez ensuite et sécurisez votre système de stockage dans une armoire ou un rack de télécommunications.

Avant de commencer

- Assurez-vous de disposer des instructions fournies avec le kit de rails.
- Soyez conscient des problèmes de sécurité associés au poids du système de stockage et de l'étagère de stockage.

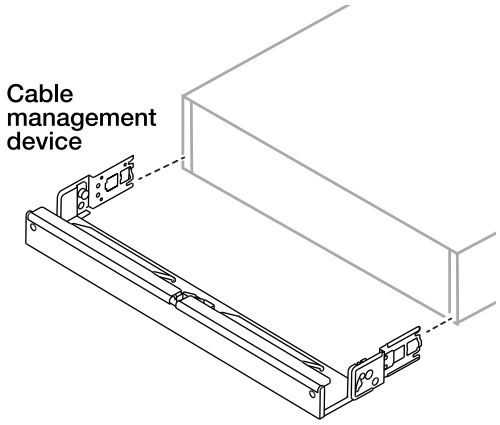
- Assurez-vous que le flux d'air qui traverse le système de stockage pénètre par l'avant où le cadre ou les embouts sont installés et sort par l'arrière où se trouvent les ports.

Étapes

1. Installez les kits de rails pour votre système de stockage et les étagères de stockage, selon les besoins, en suivant les instructions fournies avec les kits.
2. Installez et sécurisez votre système de stockage dans l'armoire ou le rack de télécommunications :
   a. Positionnez le système de stockage sur les rails au milieu de l'armoire ou du rack de télécommunications, puis soutenez le système de stockage par le bas et faites-le glisser pour le mettre en place.
   b. Fixez le système de stockage à l'armoire ou au rack de télécommunications à l'aide des vis de montage fournies.
3. Installez le tiroir de stockage :
   a. Placez l'arrière de la tablette de stockage sur les rails, puis soutenez la tablette par le bas et faites-la glisser dans l'armoire ou le rack de télécommunications.

      Si vous installez plusieurs tiroirs de stockage, placez le premier tiroir de stockage directement au-dessus des contrôleurs. Placez le second tiroir de stockage directement sous les contrôleurs. Répétez cette procédure pour toutes les étagères de stockage supplémentaires.

   b. Fixez l'étagère de stockage à l'armoire ou au rack de télécommunications à l'aide des vis de montage fournies.
4. Connectez les périphériques de gestion des câbles à l'arrière du système de stockage.



5. Fixez le panneau à l'avant du système de stockage.

Et la suite ?

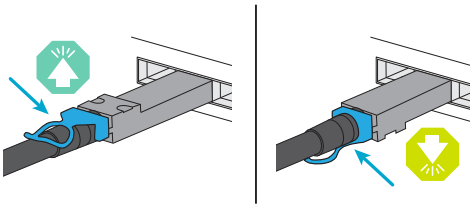
Après avoir installé le matériel de votre système ASA r2, vous "Reliez les contrôleurs et les tiroirs de stockage à votre système ASA r2".

Branchez les câbles du matériel du système de stockage ASA r2

Une fois le matériel rack du système de stockage ASA r2 installé, installez les câbles réseau des contrôleurs et connectez les câbles entre les contrôleurs et les tiroirs de stockage.

Avant de commencer

Vérifiez la flèche d'illustration dans les schémas de câblage pour connaître l'orientation correcte de la languette de retrait du connecteur de câble.



- Lorsque vous insérez le connecteur, vous devez le sentir en place. Si vous ne le sentez pas, retirez-le, retournez la tête du câble et réessayez.
- Si vous vous connectez à un commutateur optique, insérez l'émetteur-récepteur enfichable à petit facteur de forme (SFP) dans le port du contrôleur avant de le connecter au port.

Étape 1 : connectez les contrôleurs de stockage à votre réseau

Connectez vos contrôleurs directement les uns aux autres et à votre réseau hôte.

Avant de commencer

Pour plus d'informations sur la connexion du système de stockage aux commutateurs réseau de l'hôte, contactez votre administrateur réseau.

Description de la tâche

Ces procédures présentent les configurations courantes. Le câblage spécifique dépend des composants commandés pour votre système de stockage. Pour obtenir des détails complets sur la configuration et la priorité des emplacements, reportez-vous à la section "NetApp Hardware Universe".

ASA A1K

Connectez vos contrôleurs de stockage pour créer des connexions de cluster ONTAP, puis connectez les ports Ethernet de chaque contrôleur au réseau hôte.

Étapes

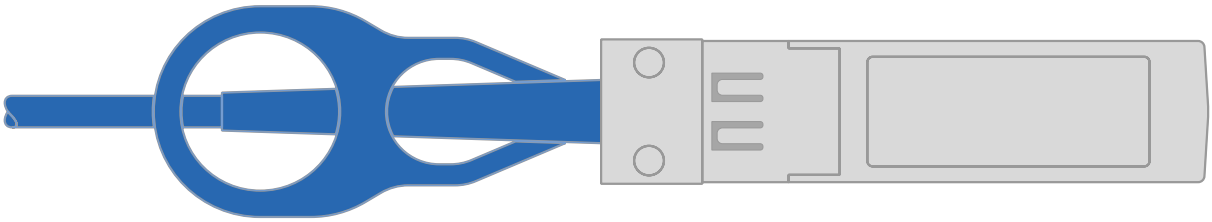
1. Utilisez le câble d'interconnexion cluster/haute disponibilité pour connecter les ports e1a à e1a et les ports e7a à e7a.

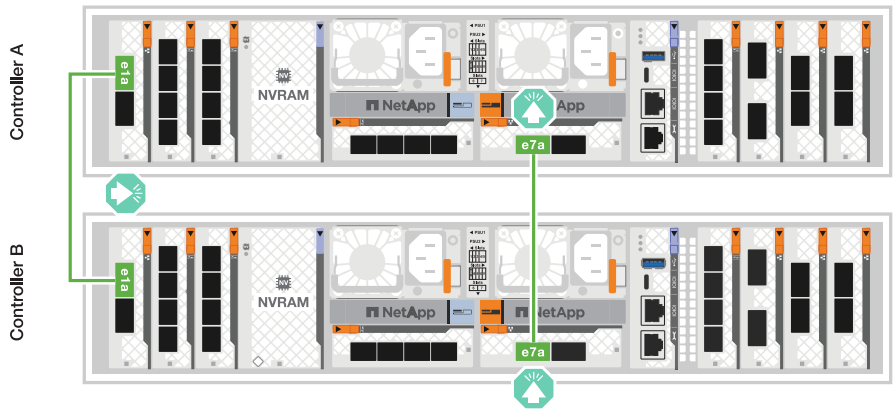
   Le trafic d'interconnexion de cluster et le trafic haute disponibilité partagent les mêmes ports physiques.

   a. Connectez le port e1a du contrôleur A au port E1A du contrôleur B.

   b. Connectez le port e7a du contrôleur A au port E1A du contrôleur B.

   Câbles d'interconnexion cluster/haute disponibilité

2. Connectez les ports du module Ethernet à votre réseau hôte.

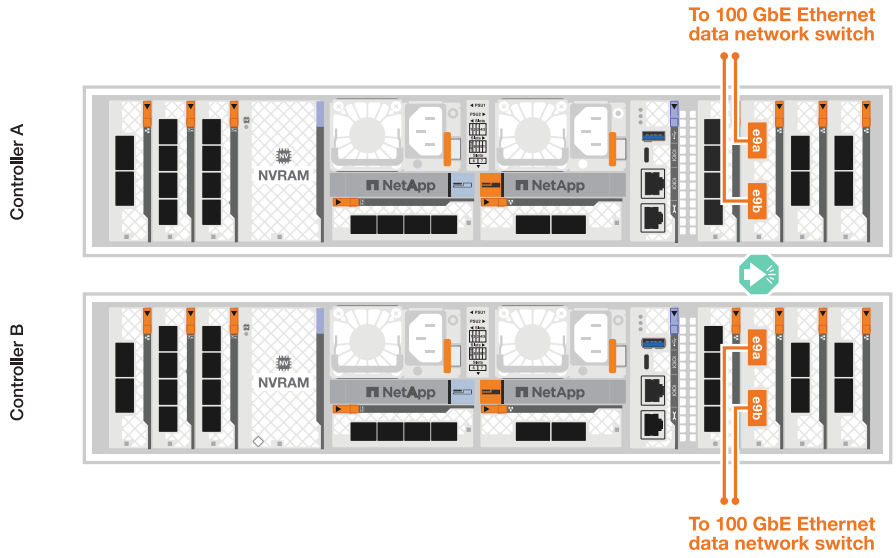
   Voici quelques exemples types de câblage réseau hôte. Reportez-vous à la section "NetApp Hardware Universe" pour connaître la configuration spécifique de votre système.

   a. Connectez les ports e9a et e9b à votre commutateur de réseau de données Ethernet, comme illustré.

   Pour optimiser les performances du système pour le trafic de cluster et haute disponibilité, n'utilisez pas les ports e1b et e7b pour les connexions réseau hôte. Utilisez une carte hôte séparée pour optimiser les performances.

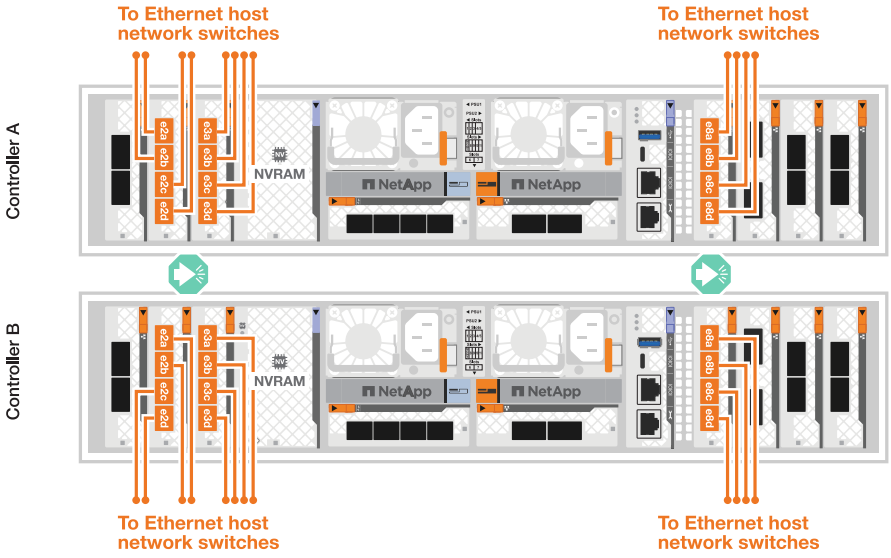
   Câble 100 GbE



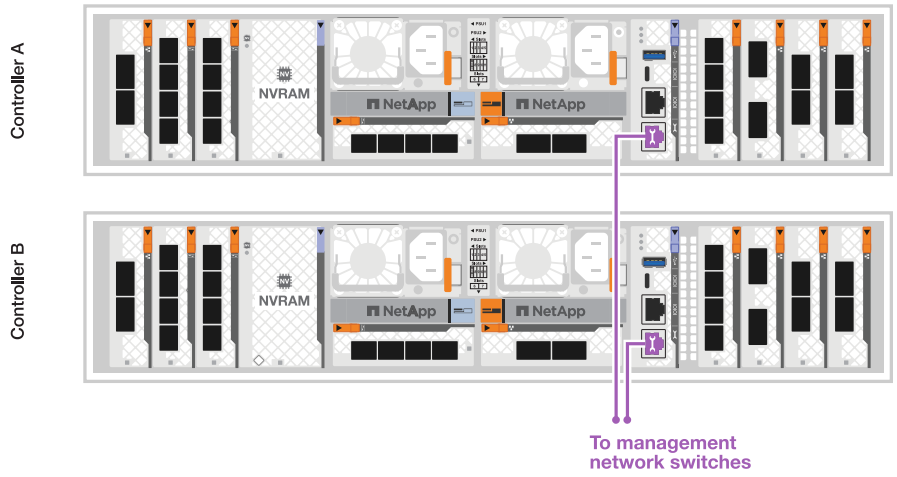
b. Connectez vos commutateurs de réseau hôte 10/25 GbE.

Hôte 10/25 GbE



3. Utilisez les câbles 1000BASE-T RJ-45 pour connecter les ports de gestion du contrôleur (clé anglaise) aux commutateurs du réseau de gestion.

CÂBLES 1000BASE-T RJ-45



Ne branchez pas encore les cordons d'alimentation.

ASA A70 et ASA A90

Connectez vos contrôleurs de stockage pour créer des connexions de cluster ONTAP, puis connectez les ports Ethernet de chaque contrôleur au réseau hôte.

Étapes

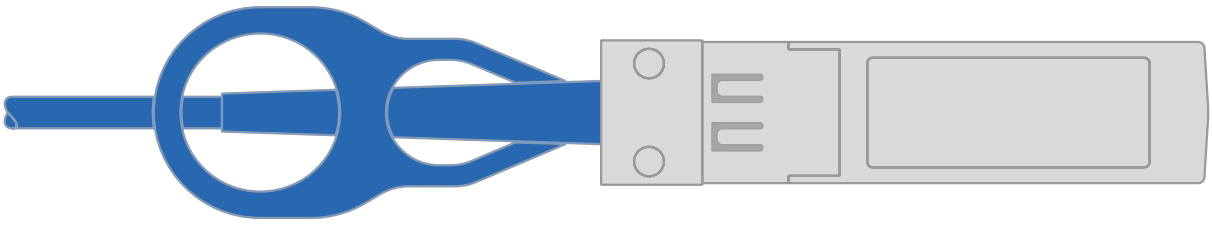
1. Utilisez le câble d'interconnexion cluster/haute disponibilité pour connecter les ports e1a à e1a et les ports e7a à e7a.

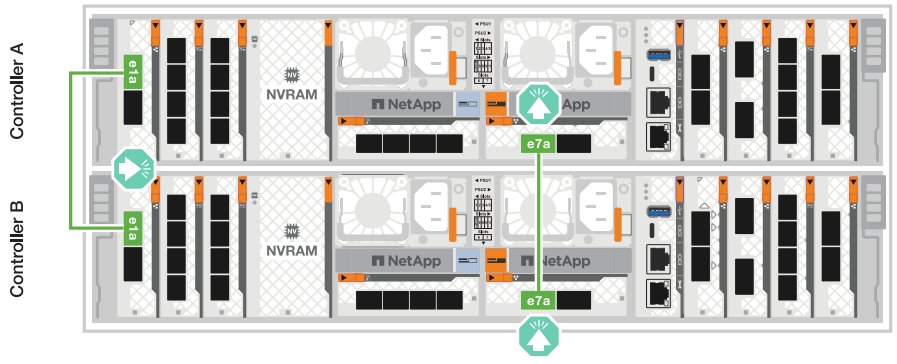
   Le trafic d'interconnexion de cluster et le trafic haute disponibilité partagent les mêmes ports physiques.

   a. Connectez le port e1a du contrôleur A au port E1A du contrôleur B.

   b. Connectez le port e7a du contrôleur A au port E1A du contrôleur B.

   Câbles d'interconnexion cluster/haute disponibilité





2. Connectez les ports du module Ethernet à votre réseau hôte.

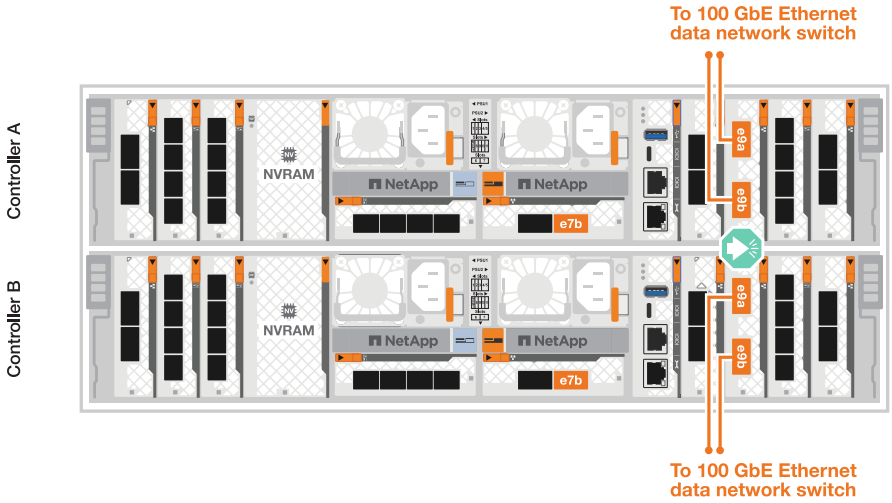
   Voici quelques exemples types de câblage réseau hôte. Reportez-vous à la section "NetApp Hardware Universe" pour connaître la configuration spécifique de votre système.

   a. Connectez les ports e9a et e9b à votre commutateur de réseau de données Ethernet, comme illustré.

   > Pour optimiser les performances du système pour le trafic de cluster et haute disponibilité, n'utilisez pas les ports e1b et e7b pour les connexions réseau hôte. Utilisez une carte hôte séparée pour optimiser les performances.

   Câble 100 GbE

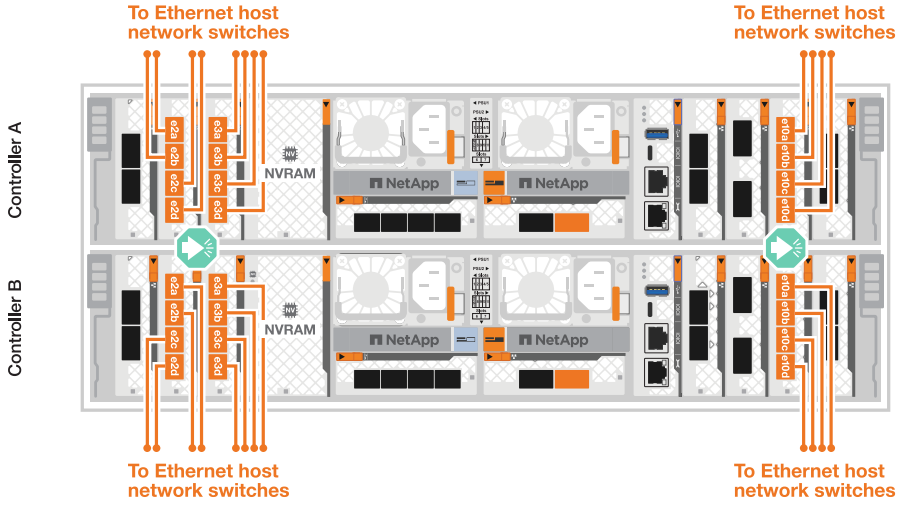
   

   b. Connectez vos commutateurs de réseau hôte 10/25 GbE.

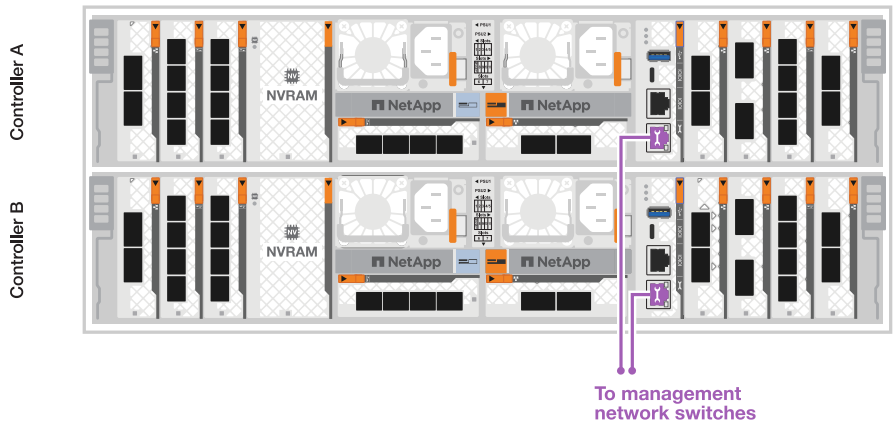
   4 ports, hôte 10/25 GbE

3. Utilisez les câbles 1000BASE-T RJ-45 pour connecter les ports de gestion du contrôleur (clé anglaise) aux commutateurs du réseau de gestion.

CÂBLES 1000BASE-T RJ-45



Ne branchez pas encore les cordons d'alimentation.

Étape 2 : connectez les contrôleurs de stockage aux tiroirs de stockage

Les procédures de câblage suivantes indiquent comment connecter les contrôleurs à un tiroir et à deux tiroirs. Vous pouvez directement connecter jusqu'à quatre tiroirs à vos contrôleurs.

ASA A1K

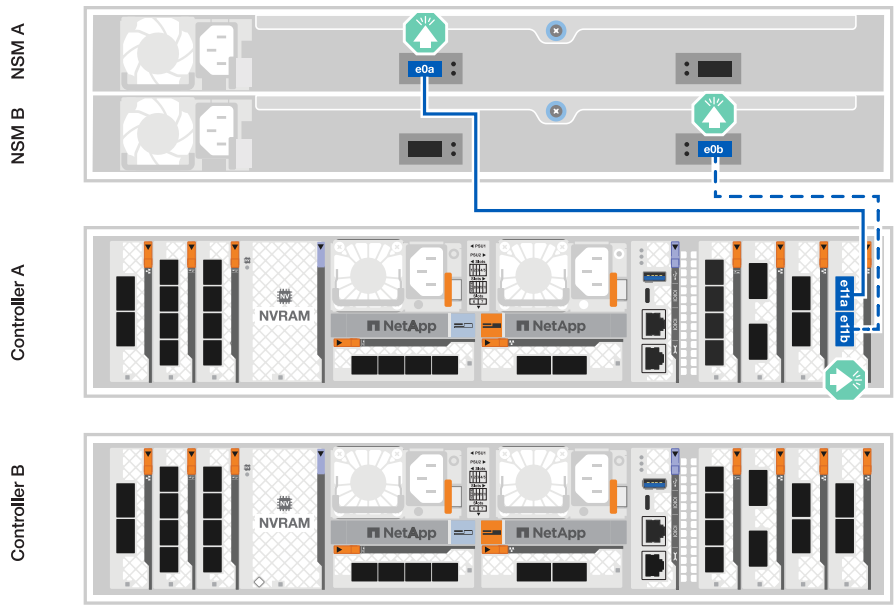
Choisissez l’une des options de câblage suivantes correspondant à votre configuration.

Option 1 : connectez les contrôleurs à un tiroir de stockage NS224

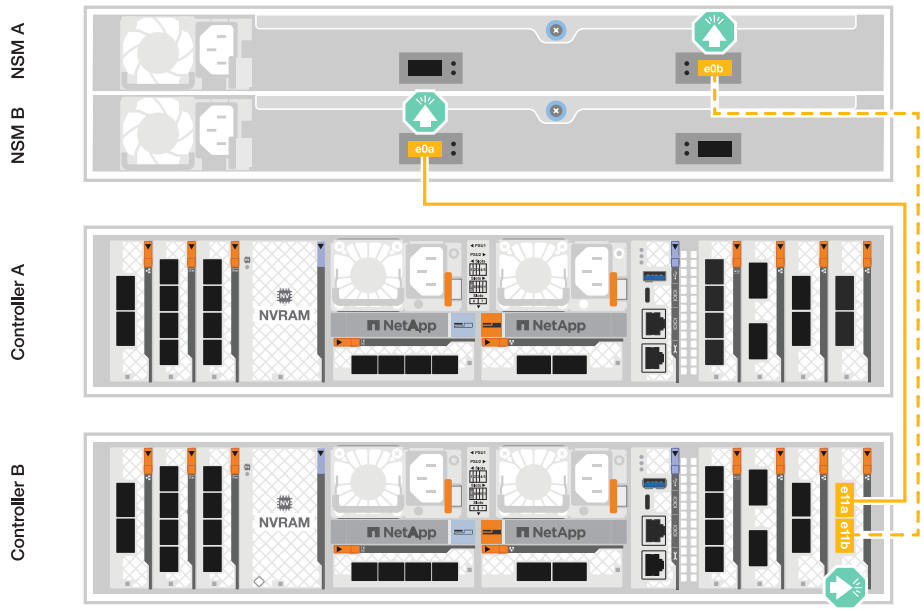
Connectez chaque contrôleur aux modules NSM du tiroir NS224. Les graphiques présentent le câblage depuis chaque contrôleur : le câblage du contrôleur A est représenté en bleu et le câblage du contrôleur B en jaune.

Étapes

1. Sur le contrôleur A, connecter les ports suivants :
   a. Connectez le port e11a au port NSM A e0a.
   b. Connectez le port e11b au port NSM B e0b.



2. Sur le contrôleur B, connecter les ports suivants :
   a. Connectez le port e11a au port NSM B e0a.
   b. Connectez le port e11b au port e0b de NSM A.

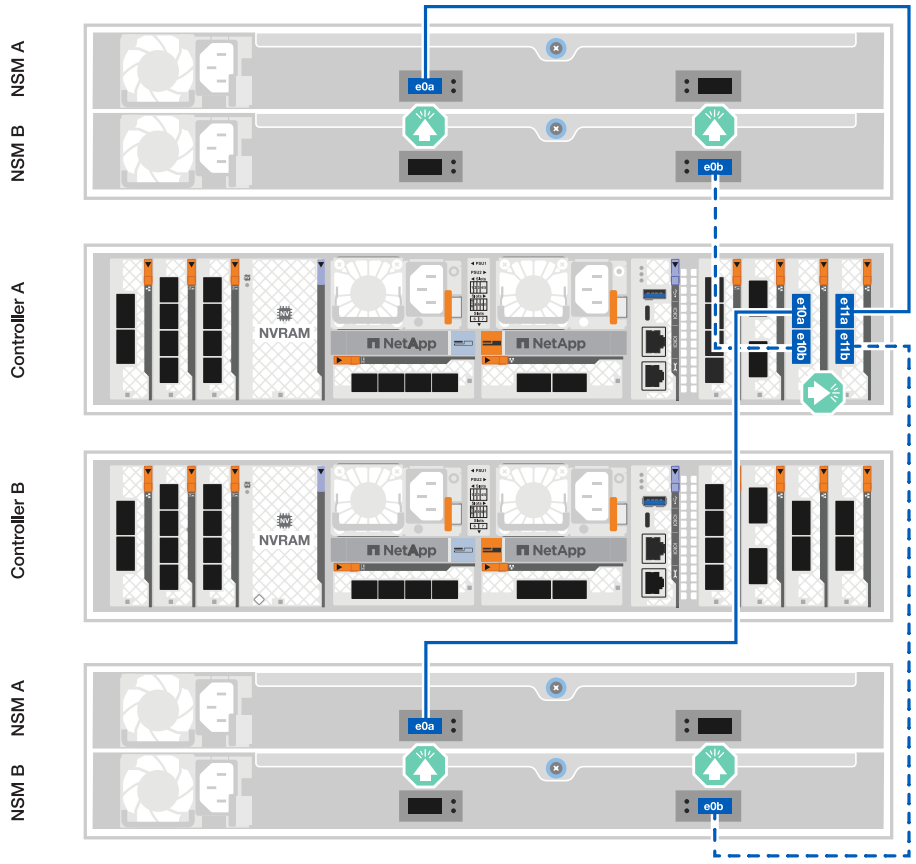


Option 2 : connectez les contrôleurs à deux tiroirs de stockage NS224

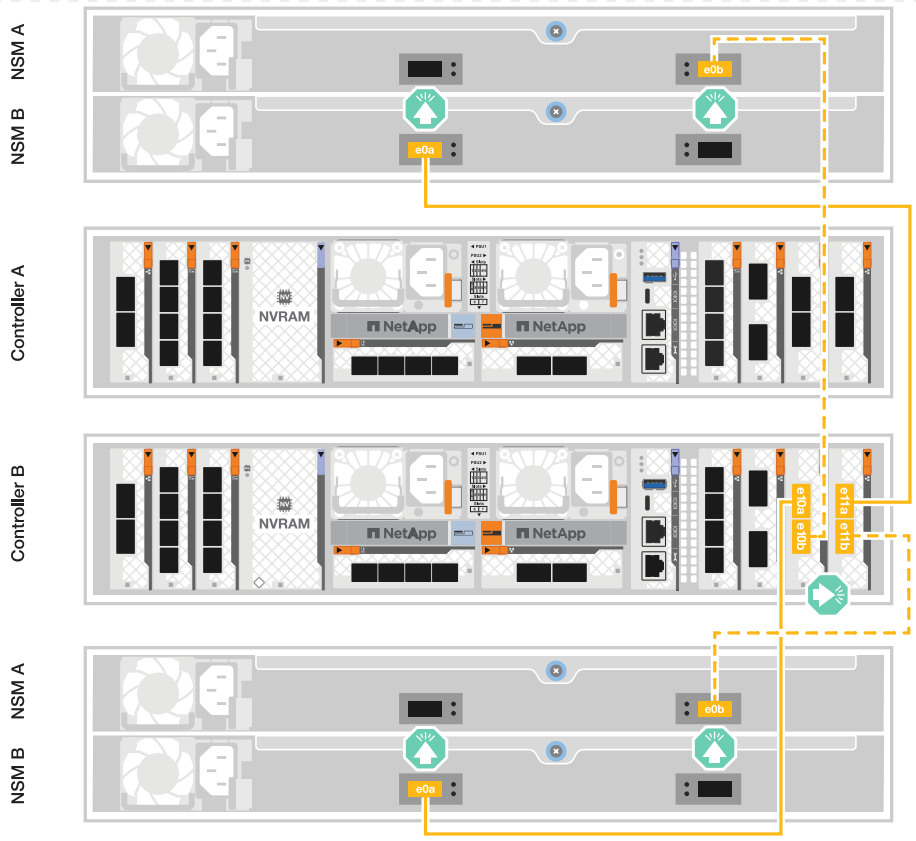
Connectez chaque contrôleur aux modules NSM des deux tiroirs NS224. Les graphiques présentent le câblage depuis chaque contrôleur : le câblage du contrôleur A est représenté en bleu et le câblage du contrôleur B en jaune.

Étapes

1. Sur le contrôleur A, connecter les ports suivants :
   a. Connectez le port e11a au port e0a NSM A du tiroir 1.
   b. Connectez le port e11b au port e0b du tiroir 2 NSM B.
   c. Connectez le port e10a au port e0a NSM A du tiroir 2.
   d. Connectez le port e10b au port e0b du tiroir 1 NSM A.



2. Sur le contrôleur B, connecter les ports suivants :
   a. Connectez le port e11a au port e0a NSM B du tiroir 1.
   b. Connectez le port e11b au port e0b du tiroir 2 NSM A.
   c. Connectez le port e10a au port e0a NSM B du tiroir 2.
   d. Connectez le port e10b au port e0b du tiroir 1 NSM A.



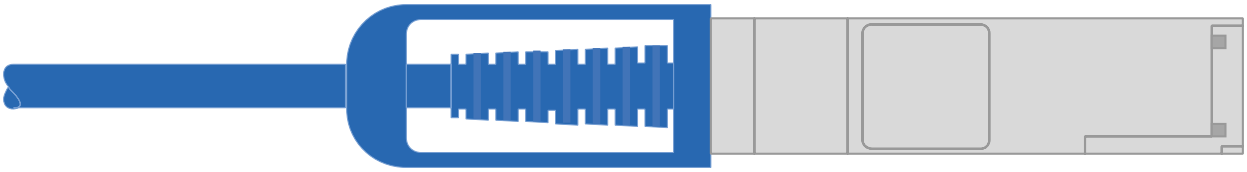
ASA A70 et ASA A90

Choisissez l'une des options de câblage suivantes correspondant à votre configuration.

Option 1 : connectez les contrôleurs à un tiroir de stockage NS224

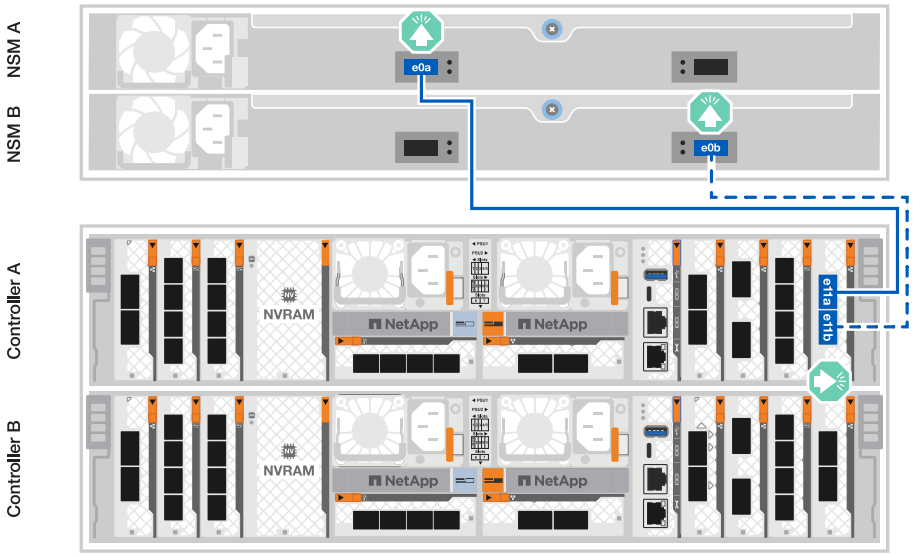
Connectez chaque contrôleur aux modules NSM du tiroir NS224. Les graphiques présentent le câblage depuis chaque contrôleur : le câblage du contrôleur A est représenté en bleu et le câblage du contrôleur B en jaune.

Câbles en cuivre QSFP28 100 GbE

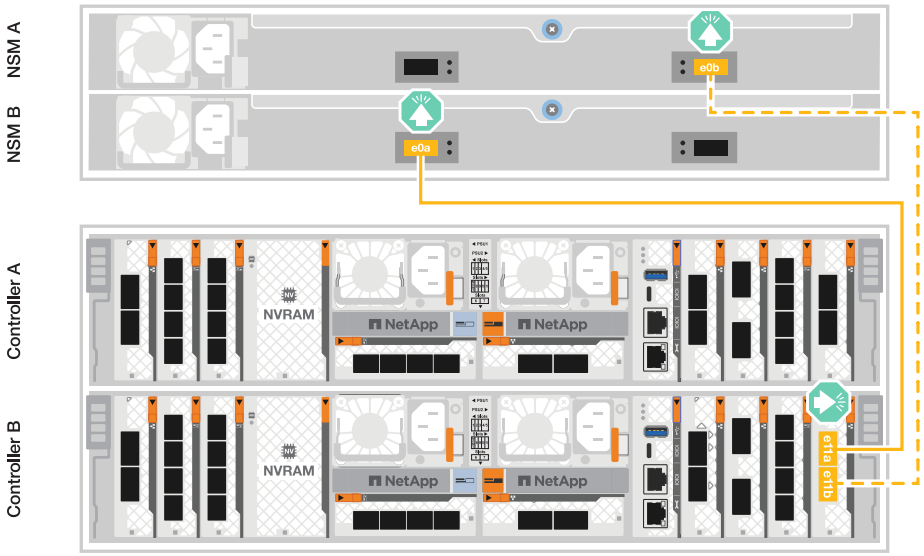


Étapes

1. Connectez le port e11a du contrôleur A au port e0a du NSM A.
2. Connectez le port e11b du contrôleur A au port NSM B e0b.



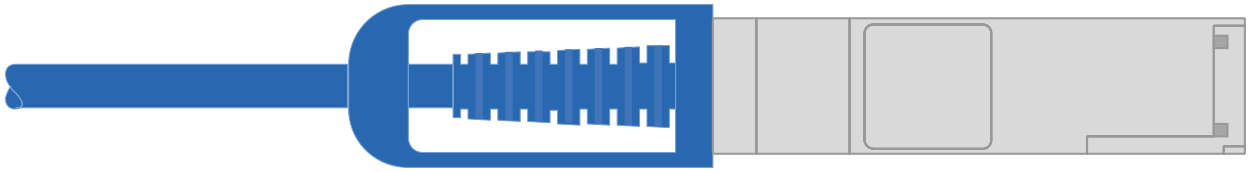
3. Connectez le port e11a du contrôleur B au port e0a du NSM B.
4. Connectez le port e11b du contrôleur B au port e0b de la carte NSM A.


NSM A
NSM B
Controller A
Controller B
e0b
e0a
NVRAM
NetApp
NVRAM
NetApp
e11a
e11b

Option 2 : connectez les contrôleurs à deux tiroirs de stockage NS224

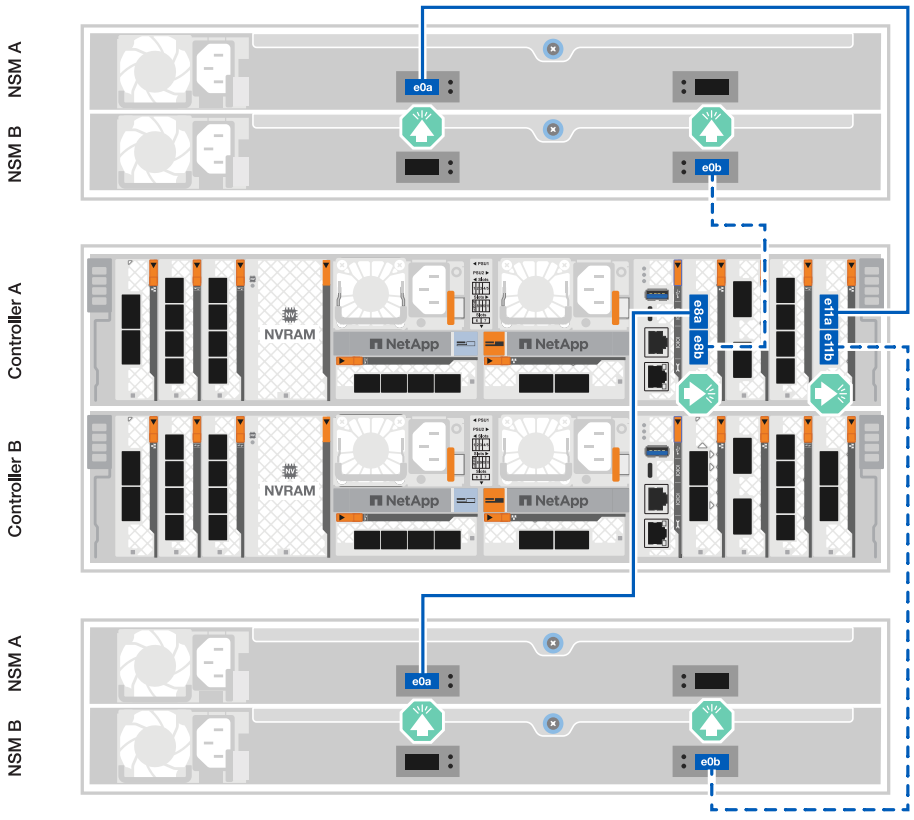
Connectez chaque contrôleur aux modules NSM des deux tiroirs NS224. Les graphiques présentent le câblage depuis chaque contrôleur : le câblage du contrôleur A est représenté en bleu et le câblage du contrôleur B en jaune.

Câbles en cuivre QSFP28 100 GbE



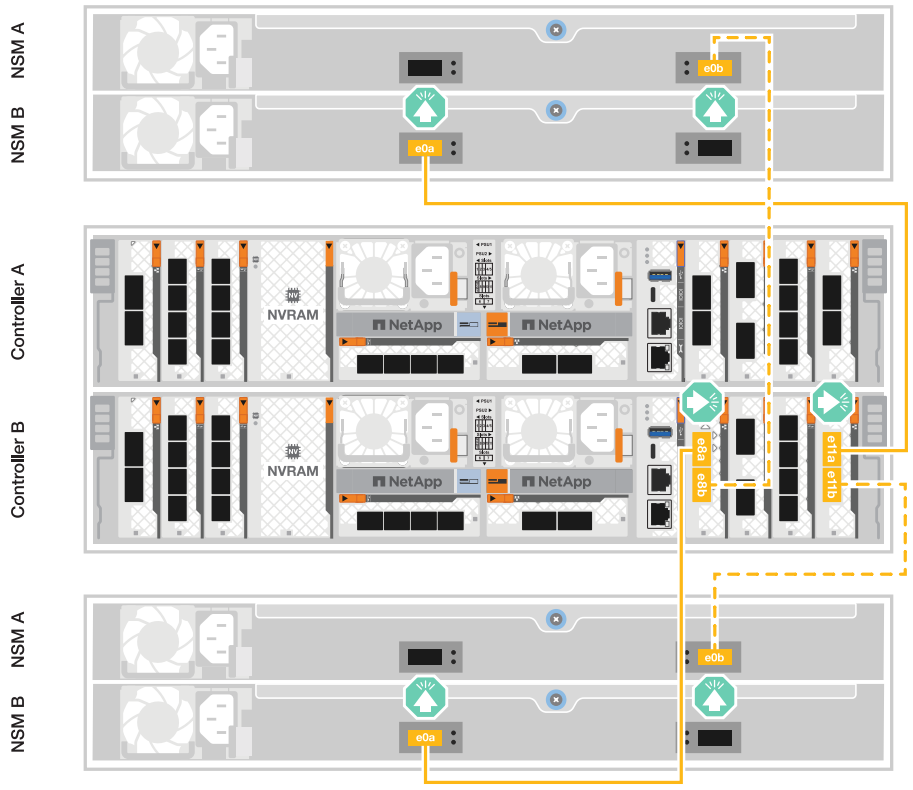
Étapes

1. Sur le contrôleur A, connecter les ports suivants :
   a. Connectez le port e11a au port e0a du tiroir 1, NSM A.
   b. Connectez le port e11b au tiroir 2, port NSM B e0b.
   c. Connectez le port e8a au port e0a du tiroir 2, NSM A.
   d. Connectez le port e8b au port e0b du tiroir 1, NSM B.



2. Sur le contrôleur B, connecter les ports suivants :
   a. Connectez le port e11a au port e0a du tiroir 1, NSM B.
   b. Connectez le port e11b au port e0b du tiroir 2, NSM A.
   c. Connectez le port e8a au port e0a du tiroir 2, NSM B.

d. Connectez le port e8b au port e0b du tiroir 1, NSM A.



Et la suite ?

Une fois que vous avez connecté les contrôleurs de stockage à votre réseau, puis connecté les contrôleurs à vos tiroirs de stockage, vous "Mettez le système de stockage ASA r2 sous tension".

Mettez le système de stockage ASA r2 sous tension

Une fois que vous avez installé le matériel en rack du système de stockage ASA r2 et que vous avez installé les câbles des contrôleurs et des tiroirs de stockage, mettez vos tiroirs et contrôleurs de stockage sous tension.

Étape 1 : mettez le tiroir sous tension et attribuez l'ID de tiroir

Chaque tiroir NS224 se distingue par un ID de tiroir unique. Cet ID garantit que le tiroir est distinct dans la configuration de votre système de stockage. Par défaut, les ID de tiroir sont attribués aux noms « 00 » et « 01 ». Toutefois, vous devrez peut-être les ajuster pour maintenir le caractère unique de votre système de stockage.

Description de la tâche

- Remarque : pour être valides, les ID de tiroir sont compris entre 00 et 99.
- Vous devez mettre un tiroir hors tension puis sous tension (débranchez les deux cordons d'alimentation, attendez la durée appropriée, puis rebranchez-les) pour que l'ID de tiroir prenne effet.

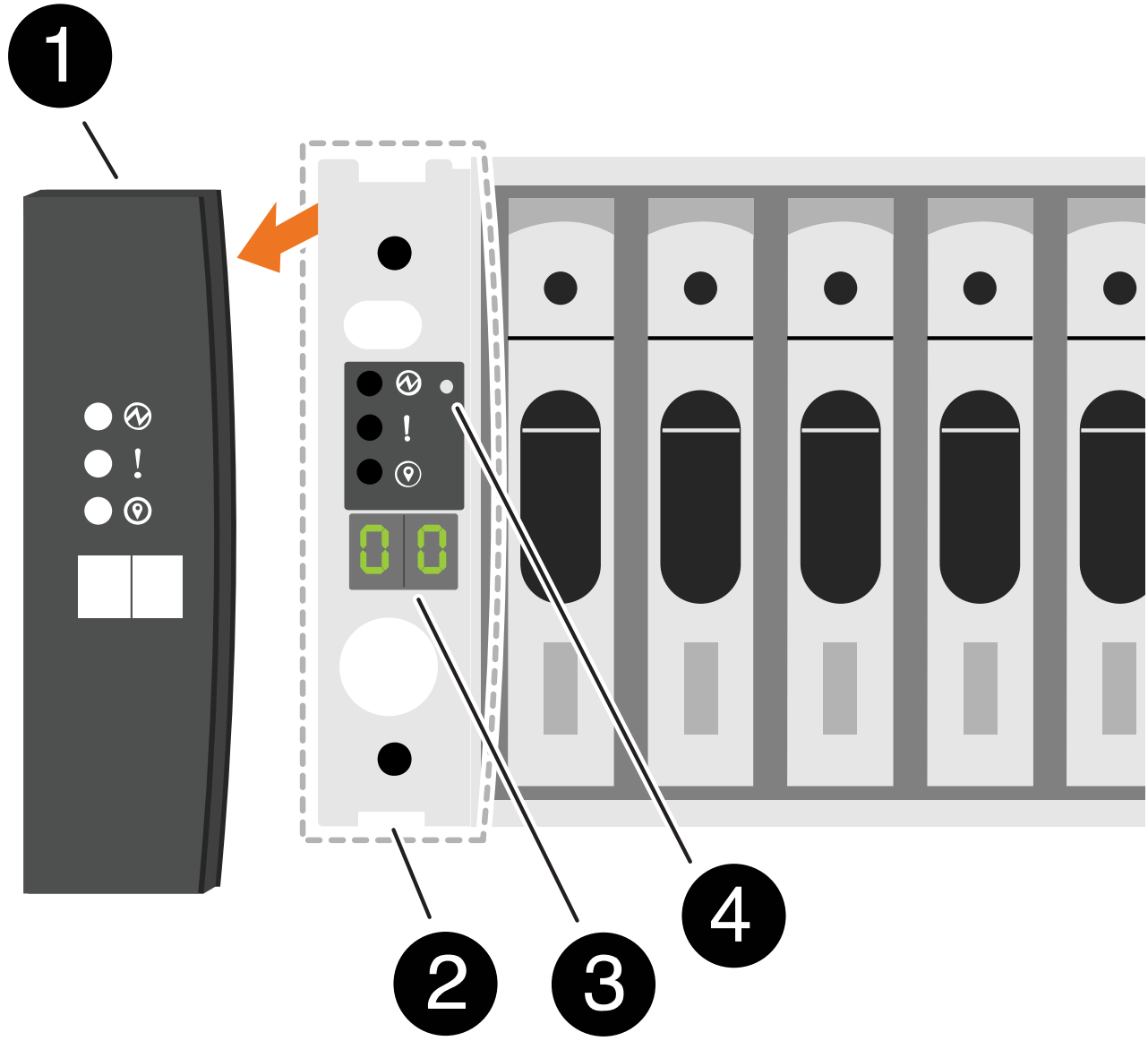
Étapes

1. Mettez le shelf sous tension en connectant d'abord les cordons d'alimentation au shelf, en les fixant à

l'aide du dispositif de retenue du cordon d'alimentation, puis en connectant les cordons d'alimentation aux sources d'alimentation de différents circuits.

Le tiroir se met sous tension et démarre automatiquement lorsqu'il est branché à la source d'alimentation.

2. Retirez le capuchon d'extrémité gauche pour accéder au bouton d'ID du shelf derrière le cache.



1	Capuchon d'extrémité de tablette

2	Plateau de tablette
3	Numéro ID du tiroir
4	Bouton de l’ID de tiroir

3. Modifier le premier numéro de l’ID de tiroir :

   a. Insérez l’extrémité droite d’un trombone ou d’un stylo à pointe sphérique à pointe étroite dans le petit trou pour appuyer sur le bouton d’identification de la tablette.

   b. Appuyez sur le bouton d’ID du tiroir et maintenez-le enfoncé jusqu’à ce que le premier chiffre de l’écran numérique clignote, puis relâchez le bouton.

      Un chiffre peut clignoter pendant 15 secondes. Cela active le mode de programmation de l’ID de tiroir.

      > Si l’ID nécessite plus de 15 secondes, appuyez de nouveau sur le bouton d’ID du tiroir et maintenez-le enfoncé, en veillant à appuyer sur le bouton.

   c. Appuyez sur le bouton d’ID du tiroir et relâchez-le pour avancer le chiffre jusqu’à ce que vous atteigniez le chiffre souhaité de 0 à 9.

      La durée de chaque pression et de chaque relâchement peut être aussi courte qu’une seconde.

   Le premier chiffre continue de clignoter.

4. Modifier le second numéro de l’ID de tiroir :

   a. Appuyez sur le bouton et maintenez-le enfoncé jusqu’à ce que le second chiffre de l’écran numérique clignote.

      Il peut prendre jusqu’à trois secondes pour que le chiffre clignote.

   Le premier chiffre de l’écran numérique cesse de clignoter.

a. Appuyez sur le bouton d'ID du tiroir et relâchez-le pour avancer le chiffre jusqu'à ce que vous atteigniez le chiffre souhaité de 0 à 9.

   Le second chiffre continue de clignoter.

5. Verrouillez le chiffre souhaité et quittez le mode de programmation en appuyant sur le bouton d'ID du tiroir et en le maintenant enfoncé jusqu'à ce que le second chiffre ne clignote plus.

   Un chiffre qui ne clignote plus pendant trois secondes peut s'arrêter.

   Les deux chiffres de l'écran numérique commencent à clignoter et le voyant orange s'allume au bout de cinq secondes environ pour vous avertir que l'ID du tiroir en attente n'a pas encore pris effet.

6. Mettez le tiroir sous tension pendant au moins 10 secondes pour valider l'ID de tiroir.
   a. Débranchez le cordon d'alimentation des deux blocs d'alimentation du shelf.
   b. Attendre 10 secondes.
   c. Rebranchez les câbles d'alimentation aux blocs d'alimentation du tiroir pour terminer la mise hors/sous tension.

      Une alimentation est mise sous tension dès que le cordon d'alimentation est branché. Son voyant bicolore doit s'allumer en vert.

7. Remettez le capuchon d'extrémité gauche en place.

Étape 2 : mettez les contrôleurs sous tension

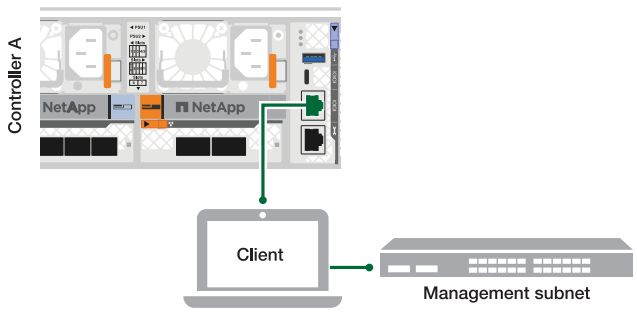
Une fois que vous avez allumé vos tiroirs de stockage et attribué des ID uniques, mettez les contrôleurs de stockage sous tension.

Étapes

1. Connectez votre ordinateur portable au port série console. Cela vous permettra de surveiller la séquence d'amorçage lorsque les contrôleurs sont sous tension.
   a. Définissez le port série console de l'ordinateur portable sur 115,200 bauds avec le N-8-1.

      Consultez l'aide en ligne de votre ordinateur portable pour obtenir des instructions sur la configuration du port série console.

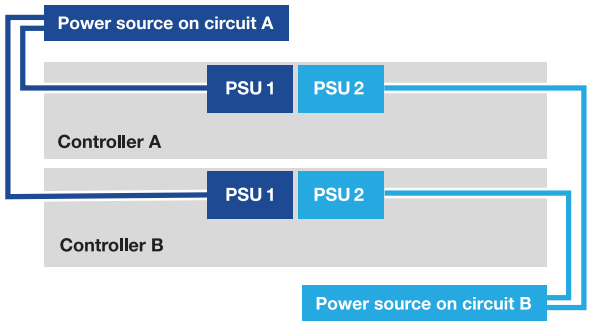
   b. Connectez le câble de la console à l'ordinateur portable et le port série console du contrôleur à l'aide du câble de console fourni avec le système de stockage.
   c. Connectez l'ordinateur portable au commutateur du sous-réseau de gestion.



   d. Attribuez une adresse TCP/IP à l'ordinateur portable, en utilisant une adresse située sur le sous-

réseau de gestion.

2. Branchez les câbles d'alimentation aux alimentations du contrôleur, puis connectez-les à des sources d'alimentation de différents circuits.



   - Le système de stockage commence à démarrer. Le démarrage initial peut prendre jusqu'à huit minutes.
   - Les LED clignotent et les ventilateurs démarrent, ce qui indique que les contrôleurs sont sous tension.
   - Les ventilateurs sont peut-être très bruyants lors du premier démarrage. Le bruit du ventilateur au démarrage est normal.

3. Fixez les câbles d'alimentation à l'aide du dispositif de fixation de chaque bloc d'alimentation.

Et la suite ?

Après avoir allumé votre système de stockage ASA r2, vous "Configuration d'un cluster ONTAP ASA r2".

Configurez votre système ASA r2

Configurez un cluster ONTAP sur votre système de stockage ASA r2

ONTAP System Manager vous guide tout au long d'un workflow simple et rapide pour la configuration d'un cluster ONTAP ASA r2.

Lors de la configuration des clusters, votre machine virtuelle de stockage de données par défaut est créée. Vous pouvez également activer le DNS (Domain Name System) pour résoudre les noms d'hôte, configurer votre cluster pour qu'il utilise le NTP (Network Time Protocol) pour la synchronisation de l'heure et activer le chiffrement des données au repos.

Avant de commencer

Rassemblez les informations suivantes :

- Adresse IP de gestion du cluster

  L'adresse IP de gestion de cluster est une adresse IPv4 unique pour l'interface de gestion de cluster utilisée par l'administrateur du cluster pour accéder à la VM de stockage d'administration et gérer le cluster. Vous pouvez obtenir cette adresse IP auprès de l'administrateur responsable de l'attribution des adresses IP dans votre organisation.

- Masque de sous-réseau réseau

  Lors de la configuration du cluster, ONTAP recommande un ensemble d'interfaces réseau adaptées à votre configuration. Vous pouvez ajuster la recommandation si nécessaire.

- Adresse IP de la passerelle réseau
- Adresse IP du nœud partenaire
- Noms de domaine DNS
- Adresses IP du serveur de noms DNS
- Adresses IP du serveur NTP
- Masque de sous-réseau de données

Étapes

1. Découvrez votre réseau en cluster
   a. Connectez votre ordinateur portable au commutateur de gestion et accédez aux ordinateurs et périphériques réseau.
   b. Ouvrez l'Explorateur de fichiers.
   c. Sélectionnez **réseau**, puis cliquez avec le bouton droit de la souris et sélectionnez **Actualiser**.
   d. Sélectionnez l'une des icônes ONTAP, puis acceptez les certificats affichés à l'écran.

      System Manager s'ouvre.

2. Sous **Mot de passe**, créez un mot de passe fort pour le compte admin.

   Le mot de passe doit comporter au moins huit caractères et doit contenir au moins une lettre et un chiffre.

3. Saisissez à nouveau le mot de passe pour confirmer, puis sélectionnez **Continuer**.
4. Sous **adresses réseau**, entrez un nom de système de stockage ou acceptez le nom par défaut.

   Si vous modifiez le nom du système de stockage par défaut, le nouveau nom doit commencer par une lettre et doit comporter moins de 44 caractères. Vous pouvez utiliser un point (.), un tiret (-) ou un trait de soulignement (_) dans le nom.

5. Entrez l'adresse IP de gestion du cluster, le masque de sous-réseau, l'adresse IP de la passerelle et l'adresse IP du nœud partenaire, puis sélectionnez **Continuer**.
6. Sous **Services réseau**, sélectionnez les options souhaitées pour **utiliser le système de noms de domaine (DNS) pour résoudre les noms d'hôte** et **utiliser le protocole NTP (Network Time Protocol) pour garder les heures synchronisées**.

   Si vous choisissez d'utiliser le DNS, entrez le domaine DNS et les serveurs de noms. Si vous choisissez d'utiliser NTP, entrez les serveurs NTP, puis sélectionnez **Continuer**.

7. Sous **Encryption**, entrez une phrase de passe pour le gestionnaire de clés intégré (OKM).

   Le chiffrement des données au repos à l'aide d'un gestionnaire de clés intégré (OKM) est sélectionné par défaut. Si vous souhaitez utiliser un gestionnaire de clés externe, mettez à jour les sélections.

   Vous pouvez également configurer votre cluster pour le chiffrement une fois l'installation du cluster terminée.

8. Sélectionnez **initialiser**.

   Une fois la configuration terminée, vous êtes redirigé vers l'adresse IP de gestion du cluster.

9. Sous **réseau**, sélectionnez **configurer les protocoles**.

Pour configurer l'IP (iSCSI et NVMe/TCP), procédez comme suit…	Pour configurer FC et NVMe/FC, procédez comme suit…
a. Sélectionnez **IP**, puis **configurer les interfaces IP**. b. Sélectionnez **Ajouter un sous-réseau**. c. Entrez un nom pour le sous-réseau, puis entrez les adresses IP de sous-réseau. d. Entrez le masque de sous-réseau et éventuellement une passerelle, puis sélectionnez **Ajouter**. e. Sélectionnez le sous-réseau que vous venez de créer, puis sélectionnez **Enregistrer**. f. Sélectionnez **Enregistrer**.	a. Sélectionnez **FC**, puis **configurer les interfaces FC** et/ou **configurer les interfaces NVMe/FC**. b. Sélectionnez les ports FC et/ou NVMe/FC, puis sélectionnez **Save**.

10. Vous pouvez également télécharger et exécuter "Active IQ Config Advisor" pour confirmer votre configuration.

    ActiveIQ Config Advisor est un outil destiné aux systèmes NetApp qui vérifie les erreurs de configuration courantes.

Et la suite ?

Vous êtes prêt à "configurez l'accès aux données"passer de vos clients SAN à votre système ASA r2.

Activez l'accès aux données depuis des hôtes SAN vers votre système de stockage ASA r2

Pour configurer l'accès aux données, vous devez vous assurer que les paramètres et paramètres spécifiques de votre client SAN qui sont essentiels au bon fonctionnement de ONTAP sont correctement configurés. Si vous utilisez VMware, vous devez migrer vos machines virtuelles.

Configurez l'accès aux données à partir d'hôtes SAN

La configuration nécessaire pour configurer l'accès aux données sur votre système ASA r2 à partir de vos hôtes SAN varie en fonction du système d'exploitation hôte et du protocole. Une configuration correcte est importante pour de meilleures performances et un basculement réussi.

Reportez-vous à la documentation de l'hôte SAN ONTAP pour "Clients SCSI VMware vSphere" "Clients NVMe VMware vSphere"et "Autres clients SAN" pour configurer correctement vos hôtes pour qu'ils se connectent à votre système ASA r2.

Migrez des machines virtuelles VMware

Si vous devez migrer votre charge de travail de machine virtuelle d'un système de stockage ASA vers un système de stockage ASA r2, NetApp vous recommande d'"VMware vSphere vMotion"effectuer une migration dynamique et sans interruption de vos données.

Et la suite ?

Vous êtes prêt à "provisionner le stockage"permettre à vos hôtes SAN de lire et d'écrire des données sur les unités de stockage.

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.

Administration et contrôle

Gestion de l'accès client aux machines virtuelles de stockage sur les systèmes de stockage ASA r2

Les unités de stockage d'un système ASA r2 sont contenues dans des machines virtuelles de stockage. Les VM de stockage sont utilisées pour transmettre des données à vos clients SAN. Utilisez ONTAP System Manager pour créer une LIF (interface réseau) pour vos clients SAN afin de se connecter à une VM de stockage et d'accéder aux données des unités de stockage. Vous pouvez également utiliser des sous-réseaux pour simplifier la création de LIF et les IPspaces afin de fournir à vos VM de stockage leur propre stockage, administration et routage sécurisés.

Créez les IPspaces

Un IPspace est un espace d'adresse IP distinct dans lequel résident les VM de stockage. Lorsque vous créez des IPspaces, vos machines virtuelles de stockage peuvent disposer de leur propre stockage, administration et routage sécurisés. Vous activez également les clients dans des domaines réseau distincts d'un point de vue administratif pour utiliser des adresses IP redondantes à partir de la même plage de sous-réseaux d'adresses IP.

Vous devez créer un IPspace avant de pouvoir créer un sous-réseau.

Étapes

1. Sélectionnez **réseau > vue d'ensemble**.
2. Sous **IPspaces**, sélectionnez + Add.
3. Entrez un nom pour l'IPspace ou acceptez le nom par défaut.

   Un nom IPspace ne peut pas être « All » car « All » est un nom réservé au système.

4. Sélectionnez **Enregistrer**.

Et la suite ?

Maintenant que vous avez créé un IPspace, vous pouvez l'utiliser pour créer un sous-réseau.

Créer des sous-réseaux

Un sous-réseau vous permet d'allouer des blocs spécifiques d'adresses IPv4 ou IPv6 à utiliser lors de la création d'une LIF (interface réseau) . Un sous-réseau simplifie la création de LIF en vous permettant de spécifier le nom de sous-réseau à la place d'une adresse IP et d'un masque réseau spécifiques pour chaque LIF.

Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- L'"broadcast-domain"IPspace et l'emplacement où vous prévoyez d'ajouter le sous-réseau doivent déjà exister.

Étapes

1. Sélectionnez **réseau > vue d'ensemble**.
2. Sélectionnez **sous-réseaux**, puis sélectionnez + Add.
3. Entrez le nom du sous-réseau.

   Tous les noms de sous-réseau doivent être uniques au sein d'un IPspace.

4. Entrez l'adresse IP du sous-réseau et le masque de sous-réseau.
5. Spécifiez la plage d'adresses IP du sous-réseau.

   Lorsque vous spécifiez la plage d'adresses IP du sous-réseau, ne faites pas chevaucher les adresses IP avec d'autres sous-réseaux. Des problèmes de réseau peuvent se produire lorsque les adresses IP de sous-réseau se chevauchent et que différents sous-réseaux ou hôtes tentent d'utiliser la même adresse IP.

6. Sélectionnez le domaine de diffusion du sous-réseau.
7. Sélectionnez **Ajouter**.

Et la suite ?

Vous avez créé un sous-réseau que vous pouvez utiliser pour simplifier la création de vos LIF.

Créer une LIF (interface réseau)

Une LIF (interface réseau) est une adresse IP associée à un port physique ou logique. Créez des LIF sur les ports que vous souhaitez utiliser pour accéder à des données. Les VM de stockage fournissent des données aux clients via une ou plusieurs LIF. En cas de défaillance d'un composant, une LIF peut basculer ou être migrée vers un autre port physique, afin que la communication réseau ne soit pas interrompue.

Lors de la création d'une LIF de données IP, celle-ci peut traiter le trafic iSCSI et NVMe/TCP par défaut. Des LIF de données distinctes doivent être créées pour le trafic FC et NVMe/FC.

Avant de commencer

- Vous devez être un administrateur de cluster pour effectuer cette tâche.
- Le port réseau physique ou logique sous-jacent doit avoir été configuré sur le `up` statut administratif.
- Si vous prévoyez d'utiliser un nom de sous-réseau pour allouer la valeur de l'adresse IP et du masque de réseau à une LIF, le sous-réseau doit déjà exister.
- Une LIF gérant le trafic intracluster entre des nœuds ne doit pas se trouver sur le même sous-réseau que le trafic de gestion d'une LIF ou encore le trafic de données géré par une LIF.

Étapes

1. Sélectionnez **réseau > vue d'ensemble**.
2. Sélectionnez **interfaces réseau**, puis sélectionnez + Add.
3. Sélectionnez le type et le protocole d'interface, puis la VM de stockage.
4. Entrez un nom pour la LIF ou acceptez le nom par défaut.
5. Sélectionnez le nœud de départ de l'interface réseau, puis entrez l'adresse IP et le masque de sous-réseau.
6. Sélectionnez **Enregistrer**.

Résultat

Vous avez créé une LIF pour l'accès aux données.

Modification d’une LIF (interfaces réseau)

Les LIF peuvent être désactivées ou renommées selon les besoins. Vous pouvez également modifier l’adresse IP et le masque de sous-réseau de la LIF.

Étapes

1. Sélectionnez **réseau > Présentation**, puis **interfaces réseau**.
2. Passez le curseur sur l’interface réseau que vous souhaitez modifier, puis sélectionnez ⋮.
3. Sélectionnez **Modifier**.
4. Vous pouvez désactiver l’interface réseau, renommer l’interface réseau, modifier l’adresse IP ou modifier le masque de sous-réseau.
5. Sélectionnez **Enregistrer**.

Résultat

Votre LIF a été modifiée.

Gestion de la mise en réseau des clusters sur les systèmes de stockage ASA r2

Vous pouvez utiliser ONTAP System Manager pour administrer le réseau de stockage de base sur votre système ASA r2. Par exemple, vous pouvez ajouter un domaine de diffusion ou réaffecter des ports à un autre domaine de diffusion.

Ajouter un domaine de diffusion

Utilisez les domaines de diffusion pour simplifier la gestion de votre réseau de clusters en regroupant les ports réseau appartenant au même réseau de couche 2. Les machines virtuelles de stockage peuvent ensuite utiliser les ports du groupe pour le trafic de données ou de gestion.

Le broadcast domain « Default » et le broadcast « Cluster » sont créés lors du setup des cluster. Le broadcast domain « Default » contient les ports inclus dans l’IPspace « Default ». Ces ports servent principalement à transmettre des données. Les ports de management des clusters et de management des nœuds sont également présents dans ce broadcast domain. Le broadcast « Cluster » contient les ports situés dans le « Cluster » IPspace. Ces ports sont utilisés pour la communication de cluster et incluent tous les ports de cluster de tous les nœuds du cluster.

Vous pouvez créer d’autres domaines de diffusion après l’initialisation de votre cluster. Lorsque vous créez un broadcast domain, un failover group contenant les mêmes ports est automatiquement créé.

Description de la tâche

L’unité de transmission maximale (MTU) des ports ajoutés à un domaine de diffusion est mise à jour vers la valeur MTU définie dans le domaine de diffusion.

Étapes

1. Dans System Manager, sélectionnez **réseau > Présentation**.
2. Sous **domaines de diffusion**, sélectionnez + Add.
3. Entrez un nom pour le domaine de diffusion ou acceptez le nom par défaut.

   Tous les noms de domaine de diffusion doivent être uniques au sein d’un IPspace.

4. Sélectionnez l'IPspace pour le broadcast domain.

   Si vous ne spécifiez pas de nom IPspace, le broadcast domain est créé dans le « Default » IPspace.

5. Entrez l'unité de transmission maximale (MTU).

   MTU est le plus grand paquet de données qui peut être accepté dans votre domaine de diffusion.

6. Sélectionnez les ports souhaités, puis sélectionnez **Enregistrer**.

Résultat

Vous avez ajouté un nouveau domaine de diffusion.

Réaffectez des ports à un autre domaine de diffusion

Les ports ne peuvent appartenir qu'à un seul domaine de diffusion. Si vous souhaitez modifier le domaine de diffusion auquel appartient un port, vous devez réaffecter le port de son domaine de diffusion existant à un nouveau domaine de diffusion.

Étapes

1. Dans System Manager, sélectionnez **réseau > Présentation**.
2. Sous **Broadcast Domains**, sélectionnez ⋮ en regard du nom de domaine, puis sélectionnez **Edit**.
3. Désélectionnez les ports Ethernet que vous souhaitez réaffecter à un autre domaine.
4. Sélectionnez le domaine de diffusion auquel vous souhaitez réaffecter le port, puis sélectionnez **réaffecter**.
5. Sélectionnez **Enregistrer**.

Résultat

Vous avez réattribué des ports à un autre domaine de diffusion.

Créer un VLAN

Un VLAN est constitué de ports de commutateur regroupés dans un domaine de diffusion. Les VLAN vous permettent d'améliorer la sécurité, d'isoler les problèmes et de limiter les chemins disponibles au sein de votre infrastructure réseau IP.

Avant de commencer

Les commutateurs déployés sur le réseau doivent soit être conformes aux normes IEEE 802.1Q, soit disposer d'une implémentation spécifique au fournisseur de VLAN.

Description de la tâche

- Un VLAN ne peut pas être créé sur un port de groupe d'interfaces ne contenant aucun port membre.
- Lorsque vous configurez un VLAN sur un port pour la première fois, le port risque de tomber en panne, entraînant une déconnexion temporaire du réseau. Les ajouts de VLAN ultérieurs au même port n'affectent pas l'état du port.
- Vous ne devez pas créer de VLAN sur une interface réseau avec le même identifiant que le VLAN natif du commutateur. Par exemple, si l'interface réseau e0b est sur un VLAN 10 natif, vous ne devez pas créer de VLAN e0b-10 sur cette interface.

Étapes

1. Dans System Manager, sélectionnez **réseau > ports Ethernet**, puis sélectionnez + VLAN.

2. Sélectionnez le nœud et le domaine de diffusion pour le VLAN.
3. Sélectionnez le port du VLAN.

   Le VLAN ne peut pas être connecté à un port hébergeant une LIF de cluster ou à des ports assignés au cluster IPspace.

4. Entrez un ID de VLAN.
5. Sélectionnez **Enregistrer**.

Résultat

Vous avez créé un VLAN pour améliorer la sécurité, isoler les problèmes et limiter les chemins disponibles au sein de votre infrastructure réseau IP.

Surveillez l'utilisation et augmentez la capacité

Surveillance des performances du cluster et de l'unité de stockage sur les systèmes de stockage ASA r2

Utilisez ONTAP System Manager pour surveiller les performances globales de votre cluster et les performances de certaines unités de stockage afin de déterminer l'impact de la latence, des IOPS et du débit sur vos applications stratégiques. Les performances peuvent être surveillées sur plusieurs périodes allant d'une heure à un an.

Supposons par exemple qu'une application stratégique connaît une latence élevée et un faible débit. Lorsque vous consultez les performances du cluster au cours des cinq derniers jours ouvrables, vous constatez une baisse des performances à la même heure chaque jour. Ces informations vous permettent de déterminer si l'application stratégique est en concurrence avec les ressources du cluster lorsqu'un processus non critique commence à s'exécuter en arrière-plan. Vous pouvez ensuite modifier votre règle de qualité de service pour limiter l'impact de la charge de travail non critique sur les ressources système et vous assurer que votre charge de travail stratégique respecte les objectifs de débit minimaux.

Contrôle des performances du cluster

Utilisez les metrics de performance du cluster pour déterminer si vous devez déplacer des charges de travail afin de minimiser la latence et d'optimiser les IOPS et le débit pour vos applications stratégiques.

Étapes

1. Dans System Manager, sélectionnez **Dashboard**.
2. Sous **Performance**, affichez la latence, les IOPS et le débit du cluster par heure, jour, semaine, mois ou année.
3. Sélectionnez pour télécharger les données de performances.

Et la suite ?

Utilisez vos metrics de performance du cluster pour déterminer si vous devez modifier vos règles de qualité de service ou effectuer d'autres ajustements de vos charges de travail applicatives afin d'optimiser les performances globales de votre cluster.

Surveiller les performances de l'unité de stockage

Utilisez les metrics de performance de l'unité de stockage pour déterminer l'impact de certaines applications sur la latence, les IOPS et le débit.

Étapes

1. Dans System Manager, sélectionnez **Storage**.
2. Sélectionnez l'unité de stockage que vous souhaitez surveiller, puis sélectionnez **Présentation**.
3. Sous **Performance**, affichez la latence, les IOPS et le débit de l'unité de stockage par heure, jour, semaine, mois ou année.
4. Sélectionnez  pour télécharger les données de performances.

Et la suite ?

Utilisez les metrics de performance de votre unité de stockage pour déterminer si vous devez modifier les règles de QoS attribuées à vos unités de stockage afin de réduire la latence et d'optimiser les IOPS et le débit.

Surveillez l'utilisation du cluster et des unités de stockage sur les systèmes de stockage ASA r2

Utilisez ONTAP System Manager pour surveiller l'utilisation du stockage et vous assurer que vous disposez de la capacité de stockage nécessaire pour gérer vos charges de travail actuelles et futures.

Surveillance de l'utilisation du cluster

Surveillez régulièrement la quantité de stockage consommée par votre cluster afin de vous assurer que, si nécessaire, vous êtes prêt à étendre la capacité du cluster avant de manquer d'espace.

Étapes

1. Dans System Manager, sélectionnez **Dashboard**.
2. Sous **capacité**, affichez la quantité d'espace physique utilisé et la quantité d'espace disponible sur votre cluster.

   Le taux de réduction des données représente l'espace économisé grâce à l'efficacité du stockage.

Et la suite ?

Si l'espace de votre cluster est insuffisant ou s'il ne dispose pas de la capacité nécessaire pour répondre à un nouveau besoin, envisagez d'"ajouter de nouveaux lecteurs"augmenter votre capacité de stockage avec votre système ASA r2.

Surveiller l'utilisation de l'unité de stockage

Surveillez la quantité de stockage consommée par une unité de stockage afin d'augmenter de manière proactive la taille de l'unité de stockage en fonction des besoins de votre entreprise.

Étapes

1. Dans System Manager, sélectionnez **Storage**.
2. Sélectionnez l'unité de stockage que vous souhaitez surveiller, puis sélectionnez **Présentation**.

3. Sous **stockage**, affichez ce qui suit :
    - Taille de votre unité de stockage
    - Quantité d'espace utilisé
    - Ratio de réduction de données

      Le taux de réduction des données représente l'espace économisé grâce à l'efficacité du stockage
    - Snapshot utilisé

      Snapshot utilisé représente la quantité de stockage utilisée par les snapshots.

Et la suite ?

Si votre unité de stockage approche de "modifier l'unité de stockage"sa capacité, vous devez augmenter sa taille.

Augmentez la capacité de stockage sur les systèmes de stockage ASA r2

Ajoutez des disques à un nœud ou à un tiroir pour augmenter la capacité de stockage de votre système ASA r2.

Utilisez NetApp Hardware Universe pour préparer l'installation d'un nouveau lecteur

Avant d'installer un nouveau disque sur un nœud ou un tiroir, vérifiez à l'aide de NetApp Hardware Universe que le disque que vous souhaitez ajouter est pris en charge par votre plateforme ASA r2 et identifiez le slot approprié pour le nouveau disque. Les emplacements appropriés pour l'ajout de disques varient en fonction du modèle de plate-forme et de la version ONTAP. Dans certains cas, vous devez ajouter des lecteurs à des emplacements spécifiques dans l'ordre.

Étapes

1. Passez à "NetApp Hardware Universe"l' .
2. Sous **produits**, sélectionnez vos configurations matérielles.
3. Sélectionnez votre plate-forme ASA r2.
4. Sélectionnez votre version ONTAP, puis **Afficher les résultats**.
5. Sous le graphique, sélectionnez **cliquez ici pour voir d'autres vues**, puis choisissez la vue qui correspond à votre configuration.
6. Utilisez l'affichage de votre configuration pour vérifier que votre nouveau lecteur est pris en charge et que le logement approprié est installé.

Résultat

Vous avez confirmé que votre nouveau lecteur est pris en charge et que vous connaissez le logement approprié pour l'installation.

Installez un nouveau lecteur sur ASA r2

Le nombre minimum de disques que vous devez ajouter en une seule procédure est de six. L'ajout d'un disque unique peut réduire les performances.

Description de la tâche

Vous devez répéter les étapes de cette procédure pour chaque lecteur.

Étapes

1. Mettez-vous à la terre.
2. Retirez délicatement le cache de l'avant de la plate-forme.
3. Insérez le nouveau lecteur dans le logement approprié.
   a. Avec la poignée de came en position ouverte, utilisez les deux mains pour insérer le nouvel entraînement.
   b. Poussez jusqu'à ce que l'entraînement s'arrête.
   c. Fermez la poignée de came de façon à ce que le lecteur soit bien en place dans le plan médian et que la poignée s'enclenche.

      Assurez-vous de fermer lentement la poignée de came de manière à ce qu'elle s'aligne correctement sur la face de l'entraînement.
4. Vérifiez que le voyant d'activité du lecteur (vert) est allumé.
   - SI le voyant est fixe, le disque est sous tension.
   - Si le voyant clignote, le lecteur est sous tension et les E/S sont en cours. Le voyant clignote également si le micrologiciel du lecteur est en cours de mise à jour.

     Le firmware des disques est automatiquement mis à jour (sans interruption) sur les nouveaux lecteurs qui ne disposent pas de versions de micrologiciel actuelles.
5. Si votre nœud est configuré pour l'affectation automatique des disques, vous pouvez attendre que ONTAP attribue automatiquement les nouveaux disques à un nœud. Si votre nœud n'est pas configuré pour l'affectation automatique des disques ou si vous préférez, vous pouvez attribuer les disques manuellement.

   Les nouveaux disques ne sont pas reconnus tant qu'ils ne sont pas attribués à un nœud.

Et la suite ?

Une fois les nouveaux disques reconnus, vérifiez qu'ils ont été ajoutés et que leur propriété est correctement spécifiée.

Mise à jour du firmware sur les systèmes de stockage ASA r2

Par défaut, ONTAP télécharge et met à jour automatiquement les fichiers système et de micrologiciel sur votre système ASA r2. Si vous souhaitez avoir la possibilité d'afficher les mises à jour recommandées avant de les télécharger et de les installer, vous pouvez utiliser ONTAP System Manager pour désactiver les mises à jour automatiques ou pour modifier les paramètres de mise à jour afin d'afficher les notifications des mises à jour disponibles avant d'effectuer une action.

Activer les mises à jour automatiques

Les mises à jour recommandées pour le micrologiciel de stockage, le micrologiciel SP/BMC et les fichiers système sont automatiquement téléchargées et installées sur votre système ASA r2 par défaut. Si les mises à jour automatiques ont été désactivées, vous pouvez les activer pour rétablir le comportement par défaut.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. En regard de **mise à jour automatique**, sélectionnez , puis **Activer**.
3. Lisez et acceptez le CLUF.
4. Acceptez les valeurs par défaut pour mettre à jour automatiquement vos fichiers système et de micrologiciel. Si vous le souhaitez, sélectionnez pour afficher les notifications ou pour ignorer automatiquement les mises à jour recommandées.
5. Sélectionnez cette option pour confirmer que vos modifications de mise à jour seront appliquées à toutes les mises à jour actuelles et futures.
6. Sélectionnez **Enregistrer**.

Résultat

Les mises à jour recommandées sont automatiquement téléchargées et installées sur votre système ASA r2 en fonction de vos sélections de mises à jour.

Désactiver les mises à jour automatiques

Désactivez les mises à jour automatiques si vous souhaitez pouvoir afficher les mises à jour recommandées avant leur installation. Si vous désactivez les mises à jour automatiques, vous devez effectuer les mises à jour du micrologiciel et des fichiers système manuellement.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. En regard de **mise à jour automatique**, sélectionnez , puis **Désactiver**.

Résultat

Les mises à jour automatiques sont désactivées. Vous devez régulièrement vérifier les mises à jour recommandées et décider si vous souhaitez effectuer une installation manuelle.

Afficher les mises à jour automatiques

Afficher la liste des mises à jour de firmware et de fichiers système qui ont été téléchargées sur le cluster et dont l'installation automatique est prévue Affichez également les mises à jour qui ont été installées automatiquement au préalable.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. En regard de **mise à jour automatique**, sélectionnez , puis **Afficher toutes les mises à jour automatiques**.

Modifier les mises à jour automatiques

Vous pouvez choisir de télécharger et d'installer automatiquement les mises à jour recommandées pour votre micrologiciel de stockage, votre micrologiciel SP/BMC et vos fichiers système sur votre cluster, ou de faire en sorte que les mises à jour recommandées soient automatiquement rejetées. Si vous souhaitez contrôler manuellement l'installation ou le rejet des mises à jour, sélectionnez pour être averti lorsqu'une mise à jour recommandée est disponible ; vous pouvez alors sélectionner manuellement l'installation ou le rejet.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.

2. En regard de **mise à jour automatique**, sélectionnez , puis **Modifier les mises à jour automatiques**.
3. Mettre à jour les sélections pour les mises à jour automatiques.
4. Sélectionnez **Enregistrer**.

Résultat

Les mises à jour automatiques sont modifiées en fonction de vos sélections.

Mettre à jour le micrologiciel manuellement

Si vous souhaitez pouvoir afficher les mises à jour recommandées avant de les télécharger et de les installer, vous pouvez désactiver les mises à jour automatiques et mettre à jour votre micrologiciel manuellement.

Étapes

1. Téléchargez votre fichier de mise à jour du micrologiciel sur un serveur ou un client local.
2. Dans System Manager, sélectionnez **Cluster > Présentation**, puis **Update**.
3. Sélectionnez **Firmware update** ; le sélectionnez + Update firmware.

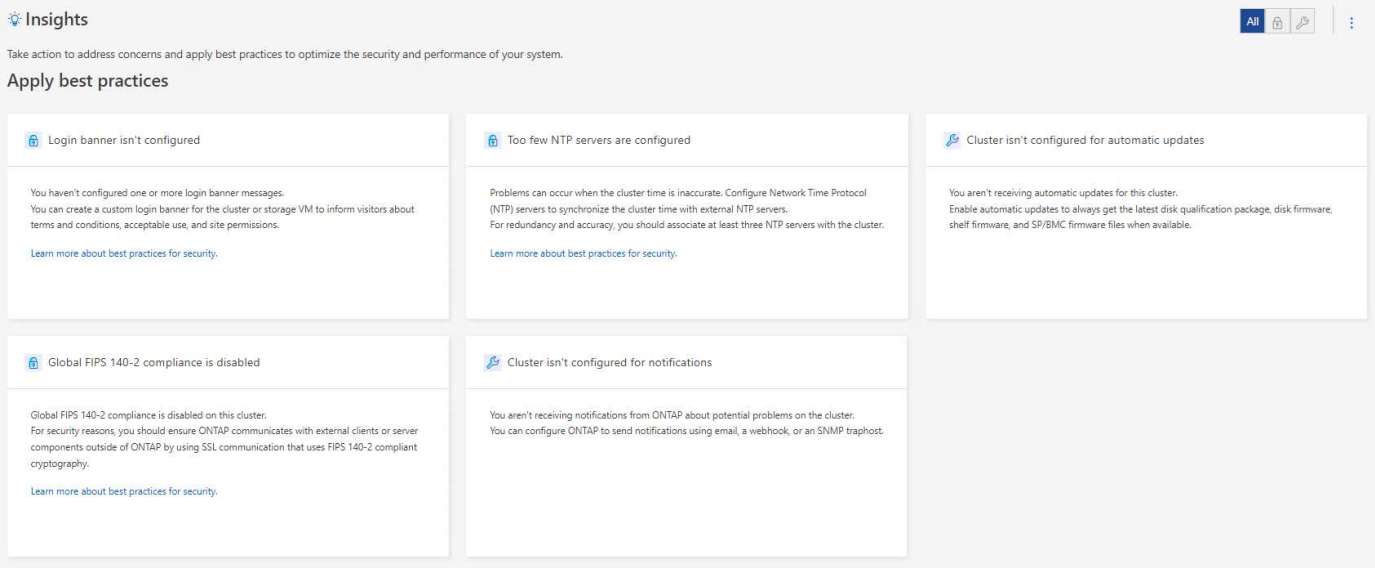
Résultat

Votre micrologiciel est mis à jour.

Optimisez la sécurité et les performances du cluster grâce aux informations exploitables du système de stockage ASA r2

Consultez *Insights* dans ONTAP System Manager pour identifier les meilleures pratiques et les modifications de configuration que vous pouvez implémenter sur votre système ASA r2 afin d'optimiser la sécurité et les performances du cluster.

Par exemple, supposons que vos serveurs NTP (Network Time Protocol) soient configurés pour votre cluster. Cependant, vous ne savez pas que le nombre de serveurs NTP requis par la gestion optimale de l'heure du cluster est inférieur à celui recommandé. Pour vous aider à prévenir les problèmes susceptibles de se produire lorsque l'heure du cluster est inexacte, Insights vous informera que vous avez configuré trop peu de serveurs NTP et vous propose des options pour en savoir plus sur ce problème, le corriger ou le rejeter.



Étapes

1. Dans System Manager, sélectionnez **Insights**.
2. Examinez les recommandations.

Et la suite

Exécutez toutes les actions nécessaires pour mettre en œuvre les meilleures pratiques et optimiser la sécurité et les performances de votre cluster.

Affichage des tâches et événements de cluster sur les systèmes de stockage ASA r2

Utilisez ONTAP System Manager pour afficher la liste des erreurs ou alertes qui se sont produites dans votre système ainsi que les actions correctives recommandées. Vous pouvez également afficher les journaux d'audit du système et la liste des tâches actives, terminées ou ayant échoué.

Étapes

1. Dans System Manager, sélectionnez **Events & Jobs**.
2. Afficher les événements et les tâches du cluster

Pour afficher ceci…	Procédez comme ça…
Événements de cluster	Sélectionnez **Events**, puis **Event log**.
Suggestions Active IQ	Sélectionnez **événements**, puis **Active IQ suggestions**.
Alertes système	a. Sélectionnez **alertes système**. b. Sélectionnez l'alerte système pour laquelle vous souhaitez effectuer l'action. c. Accuser réception ou supprimer l'alerte.

Pour afficher ceci…	Procédez comme ça…
Tâches de cluster	Sélectionnez **travaux**.
Journaux d'audit	Sélectionnez **journaux d'audit**.

Envoyez des notifications par e-mail pour les événements du cluster et les journaux d'audit

Configurez votre système pour qu'il envoie une notification à des adresses e-mail spécifiques en cas d'entrée de journal d'audit ou d'événement de cluster.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. En regard de **gestion des notifications**, sélectionnez ⋮.
3. Pour configurer une destination d'événement, sélectionnez **Afficher les destinations d'événement**, puis **destinations d'événement**. Pour configurer une destination de journal d'audit, sélectionnez **Afficher les destinations d'audit**, puis **destinations de journal d'audit**.
4. Sélectionnez + Add.
5. Entrez les informations de destination, puis sélectionnez **Ajouter**.

Résultat

L'adresse e-mail que vous avez ajoutée recevra à présent les notifications par e-mail spécifiées pour les événements du cluster et les journaux d'audit.

Gérer des nœuds

Redémarrez un nœud sur un système de stockage ASA r2

Vous devrez peut-être redémarrer un nœud pour effectuer des opérations de maintenance, de dépannage, de mise à jour logicielle ou d'autres tâches d'administration. Lorsqu'un nœud est redémarré, son partenaire haute disponibilité exécute automatiquement un basculement. Le nœud partenaire effectue ensuite un rétablissement automatique après la remise en ligne du nœud rebooté.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Présentation**.
2. Sélectionnez ⋮ en regard du nœud que vous souhaitez redémarrer, puis sélectionnez **redémarrer**.
3. Entrez la raison pour laquelle vous redémarrez le nœud, puis sélectionnez **redémarrer**.

   La raison pour laquelle vous entrez pour le redémarrage est enregistrée dans le journal d'audit du système.

Et la suite ?

Pendant le redémarrage du nœud, son partenaire haute disponibilité effectue un basculement afin qu'il n'y ait aucune interruption du service de données. Une fois le redémarrage terminé, le partenaire HA effectue un

retour.

Renommez un nœud sur un système de stockage ASA r2

Vous pouvez utiliser ONTAP System Manager pour renommer un nœud sur votre système ASA r2. Vous devrez peut-être renommer un nœud pour l'aligner sur les conventions de nommage de votre entreprise ou pour d'autres raisons d'ordre administratif.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Présentation**.
2. Sélectionnez ⋮ en regard du nœud que vous souhaitez renommer, puis sélectionnez **Renommer**.
3. Entrez le nouveau nom du nœud, puis sélectionnez **Renommer**.

Résultat

Le nouveau nom est appliqué au nœud.

Gestion des comptes et des rôles utilisateur sur les systèmes de stockage ASA r2

Utilisez System Manager pour configurer l'accès au contrôleur de domaine Active Directory, l'authentification LDAP et SAML pour vos comptes d'utilisateurs. Créez des rôles de compte utilisateur pour définir des fonctions spécifiques que les utilisateurs affectés aux rôles peuvent exécuter sur votre cluster.

Configurer l'accès au contrôleur de domaine Active Directory

Configurez l'accès du contrôleur de domaine Active Directory (AD) à votre cluster ou à votre machine virtuelle de stockage afin de pouvoir activer l'accès au compte AD.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. Dans la section **sécurité**, sous **Active Directory**, sélectionnez **configurer**.

Et la suite ?

Vous pouvez désormais activer l'accès au compte AD sur votre système ASA r2.

Configurer LDAP

Configurez un serveur LDAP (Lightweight Directory Access Protocol) pour gérer de manière centralisée les informations utilisateur à des fins d'authentification.

Avant de commencer

Vous devez avoir généré une demande de signature de certificat et ajouté un certificat numérique de serveur signé par l'autorité de certification.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.

2. Dans la section **sécurité**, en regard de **LDAP**, sélectionnez .
3. Entrez le serveur LDAP et les informations de liaison nécessaires, puis sélectionnez **Enregistrer**.

Et la suite ?

Vous pouvez désormais utiliser LDAP pour les informations utilisateur et l'authentification.

Configurez l'authentification SAML

L'authentification SAML (Security assertion Markup Language) permet aux utilisateurs d'être authentifiés par un fournisseur d'identité sécurisé (IDP) au lieu des fournisseurs de services directs tels qu'Active Directory et LDAP.

Avant de commencer

- Le IDP que vous envisagez d'utiliser pour l'authentification à distance doit être configuré.

  Pour plus d'informations sur la configuration, reportez-vous à la documentation IDP.

- Vous devez avoir l'URI du IDP.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. Sous **sécurité**, en regard de **authentification SAML**, sélectionnez .
3. Sélectionnez **Activer l'authentification SAML**.
4. Entrez l'URL de l'IDP et l'adresse IP du système hôte, puis sélectionnez **Enregistrer**.

   Une fenêtre de confirmation affiche les informations sur les métadonnées, qui ont été automatiquement copiées dans le presse-papiers.

5. Accédez au système IDP que vous avez spécifié, puis copiez les métadonnées de votre presse-papiers pour mettre à jour les métadonnées du système.
6. Revenez à la fenêtre de confirmation dans System Manager, puis sélectionnez **J'ai configuré l'IDP avec l'URI hôte ou les métadonnées**.
7. Sélectionnez **Déconnexion** pour activer l'authentification basée sur SAML.

   Le système IDP affiche un écran d'authentification.

Et la suite ?

Vous pouvez désormais utiliser l'authentification SAML pour vos comptes d'utilisateurs.

Créer des rôles de compte d'utilisateur

Les rôles des administrateurs de cluster et des administrateurs des VM de stockage sont automatiquement créés lors de l'initialisation du cluster. Créez des rôles de compte d'utilisateur supplémentaires pour définir des fonctions spécifiques que les utilisateurs affectés aux rôles peuvent exécuter sur votre cluster.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. Dans la section **sécurité**, en regard de **utilisateurs et rôles**, sélectionnez .
3. Sous **rôles**, sélectionnez + Add .

4. Sélectionnez les attributs de rôle.

   Pour ajouter plusieurs attributs, sélectionnez + Add .

5. Sélectionnez **Enregistrer**.

Résultat

Un nouveau compte utilisateur est créé et peut être utilisé sur votre système ASA r2.

Créez un compte administrateur

Créez un compte utilisateur administrateur pour permettre à l'utilisateur du compte d'effectuer des actions spécifiques sur votre cluster en fonction du rôle attribué au compte. Pour améliorer la sécurité du compte, configurez l'authentification multifacteur (MFA) lorsque vous créez le compte.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. Dans la section **sécurité**, en regard de **utilisateurs et rôles**, sélectionnez →.
3. Sous **utilisateurs**, sélectionnez + Add .
4. Entrez un nom d'utilisateur, puis sélectionnez un rôle à attribuer à l'utilisateur.
5. Sélectionnez la méthode de connexion utilisateur et la méthode d'authentification.
6. Pour activer MFA, sélectionnez + Add , puis sélectionnez une méthode de connexion secondaire et une méthode d'authentification
7. Saisissez un mot de passe pour l'utilisateur.
8. Sélectionnez **Enregistrer**.

Résultat

Un nouveau compte administrateur est créé et peut être utilisé sur votre cluster ASA r2.

Gestion des certificats de sécurité sur les systèmes de stockage ASA r2

Utilisez des certificats de sécurité numériques pour vérifier l'identité des serveurs distants.

Le protocole OCSP (Online Certificate Status Protocol) valide le statut des demandes de certificat numérique des services ONTAP à l'aide de connexions SSL et TLS (transport Layer Security).

Générer une demande de signature de certificat

Générez une requête de signature de certificat (CSR) pour créer une clé privée qui peut être utilisée pour générer un certificat public.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. Sous **sécurité**, en regard de **certificats**, sélectionnez →; puis sélectionnez + Generate CSR.
3. Saisissez le nom commun du sujet, puis sélectionnez le pays.

4. Si vous souhaitez modifier les valeurs par défaut du GSR, sélectionnez utilisation de la touche étendue ou ajoutez des noms de substitution d'objet, sélectionnez More options; puis effectuez les mises à jour souhaitées.
5. Sélectionnez **generate**.

Résultat

Vous avez généré une RSC à laquelle vous pouvez utiliser pour générer un certificat public.

Ajoutez une autorité de certification approuvée

ONTAP fournit un ensemble par défaut de certificats racine approuvés pour les applications utilisant TLS (transport Layer Security). Vous pouvez ajouter des autorités de certification approuvées supplémentaires si nécessaire.

Étapes

1. Sélectionnez **Cluster > Paramètres**.
2. Sous **sécurité**, en regard de **certificats**, sélectionnez →.
3. Sélectionnez **autorités de certification approuvées**.
4. Entrez ou importez les détails du certificat, puis sélectionnez + Add.

Résultat

Vous avez ajouté une nouvelle autorité de certification approuvée à votre système ASA r2.

Renouveler ou supprimer une autorité de certification approuvée

Les autorités de certification de confiance doivent être renouvelées chaque année. Si vous ne souhaitez pas renouveler un certificat expiré, vous devez le supprimer.

Étapes

1. Sélectionnez **Cluster > Paramètres**.
2. Sous **sécurité**, en regard de **certificats**, sélectionnez →.
3. Sélectionnez **autorités de certification approuvées**.
4. Sélectionnez l'autorité de certification de confiance que vous souhaitez renouveler ou supprimer.
5. Renouvelez ou supprimez l'autorité de certification.

Pour renouveler l'autorité de certification, procédez comme suit…	Pour supprimer l'autorité de certification, procédez comme suit…
a. Sélectionnez ⋮, puis **Renew**. b. Entrez ou importez les informations du certificat, puis sélectionnez **Renew**.	a. Sélectionnez ⋮, puis **Supprimer**. b. Confirmez que vous souhaitez supprimer, puis sélectionnez **Supprimer**.

Résultat

Vous avez renouvelé ou supprimé une autorité de certification approuvée existante sur votre système ASA r2.

Ajoutez un certificat client/serveur ou des autorités de certification locales

Ajoutez un certificat client/serveur ou des autorités de certification locales pour activer des services Web sécurisés.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. Sous **sécurité**, en regard de **certificats**, sélectionnez →.
3. Sélectionnez **certificats client/serveur** ou **autorités de certification locales**.
4. Ajoutez les informations du certificat, puis sélectionnez + Add.

Résultat

Vous avez ajouté un nouveau certificat client/serveur ou des autorités locales à votre système ASA r2.

Renouvelez ou supprimez un certificat client/serveur ou des autorités de certification locales

Les certificats client/serveur et les autorités de certification locales doivent être renouvelés chaque année. Si vous ne souhaitez pas renouveler un certificat expiré ou les autorités de certification locales, vous devez les supprimer.

Étapes

1. Sélectionnez **Cluster > Paramètres**.
2. Sous **sécurité**, en regard de certificats, sélectionnez →.
3. Sélectionnez **certificats client/serveur** ou **autorités de certification locales**.
4. Sélectionnez le certificat que vous souhaitez renouveler ou supprimer.
5. Renouvelez ou supprimez l'autorité de certification.

Pour renouveler l'autorité de certification, procédez comme suit…	Pour supprimer l'autorité de certification, procédez comme suit…
a. Sélectionnez ⋮, puis **Renew**. b. Entrez ou importez les informations du certificat, puis sélectionnez **Renew**.	Sélectionnez ⋮, puis **Supprimer**.

Résultat

Vous avez renouvelé ou supprimé un certificat client/serveur existant ou une autorité de certification locale sur votre système ASA r2.

Vérifiez la connectivité hôte sur votre système de stockage ASA r2

En cas de problème avec les opérations de données hôte, vous pouvez utiliser ONTAP System Manager pour vérifier que la connexion entre l'hôte et le système de stockage ASA r2 est active.

Étapes

1. Dans System Manager, sélectionnez **Host**.

   L'état de la connectivité hôte est indiqué en regard du nom du groupe d'hôtes comme suit :

   - **OK** : indique que tous les initiateurs sont connectés aux deux nœuds.
   - **Partiellement connecté** : indique que certains des initiateurs ne sont pas connectés aux deux nœuds.
   - **Aucun connecté** : indique qu'aucun initiateur n'est connecté.

Et la suite ?

Effectuez des mises à jour sur votre hôte pour corriger les problèmes de connectivité. ONTAP revérifie l'état de la connexion toutes les quinze minutes.

Assurez la maintenance de votre système de stockage ASA r2

Consultez le "ASA r2 maintient la documentation" pour savoir comment effectuer des procédures de maintenance sur les composants de votre système ASA r2.

En savoir plus >>

ASA r2 pour utilisateurs intensifs ONTAP

Comparez les systèmes ASA r2 aux autres systèmes ONTAP

Les systèmes ASA r2 offrent une solution matérielle et logicielle unifiée pour les environnements SAN et basée sur des plateformes 100 % Flash. Les systèmes ASA r2 sont différents des autres systèmes ONTAP (ASA, AFF et FAS) lors de l'implémentation de la couche de stockage, des protocoles pris en charge et des fonctions ONTAP.

Sur un système ASA r2, le logiciel ONTAP est optimisé pour prendre en charge les fonctionnalités SAN essentielles, tout en limitant la visibilité et la disponibilité des fonctionnalités non liées à SAN. Par exemple, System Manager exécuté sur un système ASA r2 n'affiche pas les options permettant de créer des répertoires locaux pour les clients NAS. Cette version simplifiée de ONTAP est identifiée comme la personnalité *ASA r2*. ONTAP s'exécutant sur tous les autres systèmes ONTAP (ASA, AFF, FAS) est identifié comme *personnalité ONTAP unifiée*. Les différences entre les personnalités ONTAP sont référencées dans la référence de commande ONTAP (pages man), la spécification de l'API REST et les messages EMS, le cas échéant.

Vous pouvez vérifier le profil de votre stockage ONTAP dans System Manager ou via l'interface de ligne de commande ONTAP.

- Dans le menu System Manager, sélectionnez **Cluster > Présentation**.
- Dans l'interface de ligne de commande, entrez : `san config show`

Impossible de modifier le profil de votre système de stockage ONTAP.

La couche de stockage des systèmes ONTAP exécutant la fonction ONTAP unifiée utilise des agrégats comme unité de stockage de base. Un agrégat possède un jeu spécifique des disques disponibles dans un système de stockage. L'agrégat alloue de l'espace sur les disques qu'il possède aux volumes pour les LUN et les espaces de noms. Un utilisateur de ONTAP unifié peut utiliser l'interface de ligne de commande pour créer et modifier des agrégats, des volumes, des LUN et des espaces de noms.

Dans les systèmes ASA r2, la couche stockage remplace les agrégats par une zone de disponibilité du stockage. Une zone de disponibilité de stockage est un pool de stockage commun qui a accès à tous les disques disponibles dans le système de stockage. La zone de disponibilité du stockage est visible pour les deux nœuds d'une paire HA ASA r2. Lorsqu'une unité de stockage (basée sur un LUN ou un namespace NVMe) est créée, ONTAP crée automatiquement un volume contenant une machine virtuelle de stockage (VM) dans la zone de disponibilité du stockage pour héberger l'unité de stockage. Grâce à cette approche automatisée et simplifiée de la gestion du stockage, certaines options System Manager, commandes ONTAP et terminaux d'API REST ne sont pas disponibles ou sont utilisées de façon limitée sur un système ASA r2. Par exemple, comme la création et la gestion de volumes sont automatisées pour les systèmes ASA r2, le menu **volumes** n'apparaît pas dans le Gestionnaire système et la `volume create` commande n'est pas prise en charge.

Comparatif de ASA r2 avec les autres systèmes de stockage ONTAP :

	ASA r2	**ASA**	**AFF**	**FAS**
Personnalité ONTAP	ASA r2	ASA	Unifiée	Unifiée

	ASA r2	ASA	AFF	FAS
Prise en charge du protocole SAN	Oui	Oui	Oui	Oui
Prise en charge du protocole NAS	Non	Non	Oui	Oui
Prise en charge de la couche de stockage	Zone de disponibilité du stockage	64 bits	64 bits	64 bits

Les plateformes ASA suivantes sont classées en tant que systèmes ASA r2 :

- ASA A1K
- ASA A70
- ASA A90

Pour en savoir plus

- En savoir plus sur "Systèmes matériels ONTAP".
- Consultez la prise en charge complète de la configuration et les limites des systèmes ASA et ASA r2 dans "NetApp Hardware Universe".
- En savoir plus sur "NetApp ASA"le .

Récapitulatif des différences entre les systèmes ASA r2

Les principales différences entre les systèmes ASA r2 et FAS, AFF et ASA concernant l'interface de ligne de commande et l'API REST de ONTAP sont décrites ci-dessous.

Création de SVM par défaut avec services de protocole

Les nouveaux clusters contiennent automatiquement un SVM de données par défaut lorsque les protocoles SAN sont activés. Les LIF de données IP prennent en charge les protocoles iSCSI et NVMe/TCP et utilisent la `default-data-blocks` stratégie de service par défaut.

Création automatique de volume

La création d'une unité de stockage (LUN ou espace de noms) crée automatiquement un volume à partir de la zone de disponibilité du stockage. Il en résulte un namespace commun et simplifié. La suppression d'une unité de stockage supprime automatiquement le volume associé.

Modifications du provisionnement fin et lourd

Les unités de stockage de sont toujours à provisionnement fin sur les systèmes de stockage ASA r2. Le provisionnement lourd n'est pas pris en charge.

Limitations et prise en charge du logiciel ONTAP pour les systèmes de stockage ASA r2

Bien que les systèmes ASA r2 proposent une prise en charge étendue des solutions SAN, certaines fonctionnalités du logiciel ONTAP ne sont pas prises en charge.

Les systèmes ASA r2 ne prennent pas en charge les éléments suivants :

- Basculement de LIF iSCSI
- FabricPool
- Provisionnement lourd des LUN
- MetroCluster
- Protocoles d'objet
- API ONTAP S3 SnapMirror et S3
- SnapMirror vers le cloud
- SnapMirror vers les systèmes non ASA r2
- Mappage de LUN sélectif (SLM)

Les systèmes ASA r2 prennent en charge les éléments suivants :

- SnapLock
- Chiffrement double couche

Pour en savoir plus

- "NetApp Hardware Universe"Pour plus d'informations sur la prise en charge matérielle et les limitations de ASA r2, reportez-vous au.
- "Découvrez comment verrouiller des instantanés" Sur votre système ASA r2.
- "Découvrez comment appliquer le chiffrement double couche" Aux données de votre système ASA r2.

Prise en charge de l'interface de ligne de commande ONTAP pour les systèmes de stockage ASA r2

Au lieu des agrégats traditionnels, propriétaires d'un jeu spécifique de disques disponibles dans un système de stockage, les systèmes ASA r2 utilisent une *zone de disponibilité du stockage*. Une zone de disponibilité de stockage est un pool de stockage commun qui a accès à tous les disques disponibles dans le système de stockage. La zone de disponibilité du stockage est visible pour les deux nœuds d'une paire HA ASA r2. Lors de la création d'une unité de stockage (espace de noms de LUN ou NVMe), ONTAP crée automatiquement un volume contenant une machine virtuelle de stockage (VM) dans la zone de disponibilité du stockage afin d'héberger l'unité de stockage.

Grâce à cette approche simplifiée de la gestion du stockage, les `storage aggregate` commandes ne sont pas prises en charge sur les systèmes ASA r2. La prise en charge de certaines `lun volume` commandes et paramètres est également limitée.

Les commandes et jeux de commandes suivants ne sont pas pris en charge sur ASA sous r2 :

Commandes <code> </code> non prises en charge

- `lun copy`
- `lun geometry`
- `lun import`
- `lun mapping add-reportng-nodes`
- `lun mapping-remove-reporting-nodes`
- `lun maxsize`
- `lun move`
- `lun move-in-volume`

  Cette commande est remplacée par lun rename/vserver nvme namespace rename.

- `lun transition`

Commandes et paramètres <code> </code> non pris en charge

- `volume autosize`
- `volume create`
- `volume delete`
- `volume expand`
- `volume modify`

  Cette commande n’est pas disponible lorsqu’elle est utilisée conjointement avec les paramètres suivants :

  - `-anti-ransomware-state`
  - `-autosize`
  - `-autosize-mode`
  - `-autosize-shrik-threshold-percent`
  - `-autosize-reset`
  - `-group`
  - `-is-cloud-write-enabled`
  - `-is-space-enforcement-logical`
  - `-max-autosize`
  - `-min-autosize`
  - `-offline`
  - `-online`
  - `-percent-snapshot-space`
  - `-qos*`
  - `-size`
  - `-snapshot-policy`
  - `-space-guarantee`
  - `-space-mgmt-try-first`
  - `-state`
  - `-tiering-policy`
  - `-tiering-minimum-cooling-days`
  - `-user`
  - `-unix-permisions`
  - `-vserver-dr-protection`
- `volume make-vsroot`

- volume mount
- volume move
- volume offline
- volume rehost
- volume rename
- volume restrict
- volume transition-prepare-to-downgrade
- volume unmount

Commandes <code> </code> non prises en charge

- volume clone create
- volume clone split

Commandes <code> SnapLock </code> non prises en charge

- volume snaplock modify

Commandes <code> </code> non prises en charge

- volume snapshot
- volume snapshot autodelete modify
- volume snapshot policy modify

Jeux de commandes <code> </code> non pris en charge

- `volume activity-tracking`
- `volume analytics`
- `volume conversion`
- `volume file`
- `volume flexcache`
- `volume flexgroup`
- `volume inode-upgrade`
- `volume object-store`
- `volume qtree`
- `volume quota`
- `volume reallocation`
- `volume rebalance`
- `volume recovery-queue`
- `volume schedule-style`

Commandes <code> </code> non prises en charge

- `storage failover show-takeover`
- `storage failover show-giveback`
- `storage aggregate relocation`
- `storage disk assign`
- `storage disk partition`
- `storage disk reassign`

Pour en savoir plus

"Référence des commandes ONTAP"Pour obtenir la liste complète des commandes prises en charge, reportez-vous au

Configurez un cluster ONTAP ASA r2 à l'aide de l'interface de ligne de commande

Il est recommandé que vous "Utilisez System Manager pour configurer votre cluster ONTAP ASA r2". System Manager propose un workflow guidé rapide et facile pour rendre votre cluster opérationnel. Toutefois, si vous avez l'habitude de travailler avec des commandes ONTAP, l'interface de ligne de commandes de ONTAP peut éventuellement être utilisée pour la configuration des clusters. La configuration de clusters à l'aide de l'interface de ligne de commandes n'offre aucune option ni aucun avantage supplémentaire que la configuration de clusters à l'aide de System Manager.

Lors de la configuration du cluster, votre machine virtuelle de stockage de données par défaut est créée, une unité de stockage initiale est créée et les LIF de données sont automatiquement découvertes. Vous pouvez

également activer le système DNS (Domain Name System) pour résoudre les noms d'hôte, configurer votre cluster pour qu'il utilise le protocole NTS (Network Time Protocol) pour la synchronisation de l'heure et activer le chiffrement des données au repos.

Avant de commencer

Rassemblez les informations suivantes :

- Adresse IP de gestion du cluster

  L'adresse IP de gestion de cluster est une adresse IPv4 unique pour l'interface de gestion de cluster utilisée par l'administrateur du cluster pour accéder à la VM de stockage d'administration et gérer le cluster. Vous pouvez obtenir cette adresse IP auprès de l'administrateur responsable de l'attribution des adresses IP dans votre organisation.

- Masque de sous-réseau réseau

  Lors de la configuration du cluster, ONTAP recommande un ensemble d'interfaces réseau adaptées à votre configuration. Vous pouvez ajuster la recommandation si nécessaire.

- Adresse IP de la passerelle réseau
- Adresse IP du nœud partenaire
- Noms de domaine DNS
- Adresses IP du serveur de noms DNS
- Adresses IP du serveur NTP
- Masque de sous-réseau de données

Étapes

1. Mettez sous tension les deux nœuds de la paire haute disponibilité.
2. Afficher les nœuds détectés sur le réseau local :

   ```
   system node show-discovered -is-in-cluster false
   ```

3. Démarrez l'assistant d'installation du cluster :

   ```
   cluster setup
   ```

4. Acceptez la déclaration AutoSupport.
5. Entrez les valeurs du port de l'interface de gestion du nœud, de l'adresse IP, du masque de réseau et de la passerelle par défaut.
6. Appuyez sur **entrée** pour continuer la configuration à l'aide de l'interface de ligne de commande, puis entrez **create** pour créer un nouveau cluster.
7. Acceptez les valeurs par défaut du système ou entrez vos propres valeurs.
8. Une fois la configuration du premier nœud terminée, connectez-vous au cluster.
9. Vérifier que le cluster est actif et que le premier nœud fonctionne correctement :

```
system node show-discovered
```

10. Ajouter le second nœud au cluster :

```
cluster add-node -cluster-ip <partner_node_ip_address>
```

11. Vous pouvez également synchroniser l'heure du système sur l'ensemble du cluster

Synchronisation sans authentification symétrique	`cluster time-service ntp server create -server <server_name>`
Synchronisation avec l'authentification symétrique	`cluster time-service ntp server create -server <server_ip_address> -key-id <key_id>`

    a. Vérifiez que le cluster est associé à un serveur NTP :

```
Cluster time-service ntp show
```

12. Vous pouvez également télécharger et exécuter "Active IQ Config Advisor" pour confirmer votre configuration.

Et la suite ?

Vous êtes prêt à "configurez l'accès aux données"passer de vos clients SAN à votre système.

Prise en charge de l'API REST pour ASA r2

L'API REST de ASA r2 est basée sur l'API REST fournie avec la personnalité ONTAP unifiée, avec un certain nombre de modifications adaptées aux caractéristiques et capacités uniques de la personnalité de ASA r2.

Types de modifications d'API

Il existe plusieurs types de différences entre l'API REST du système ASA r2 et l'API REST ONTAP unifiée disponible avec les systèmes FAS, AFF et ASA. Comprendre les types de modifications vous aidera à mieux utiliser la documentation de référence de l'API en ligne.

Les nouveaux terminaux ASA r2 ne sont pas pris en charge dans Unified ONTAP

Plusieurs terminaux ont été ajoutés à l'API REST ASA r2 qui ne sont pas disponibles avec Unified ONTAP.

Par exemple, un nouveau terminal volume bloc a été ajouté à l'API REST pour les systèmes ASA r2. Le

terminal du volume de bloc permet d'accéder aux objets de namespace LUN et NVMe, offrant ainsi une vue agrégée des ressources. Ceci est uniquement disponible via l'API REST.

Autre exemple : les terminaux **Storage-units** fournissent une vue agrégée des LUN et des espaces de noms NVMe. Il existe plusieurs points finaux et ils sont tous basés sur ou dérivés de `/api/storage/storage-units`. Vous devriez également revoir `/api/storage/luns` et `/api/storage/namespaces`.

Restrictions sur les méthodes HTTP utilisées pour certains noeuds finaux

Plusieurs terminaux disponibles avec ASA r2 ont des restrictions sur les méthodes HTTP pouvant être utilisées par rapport à Unified ONTAP. Par exemple, la POST et LA SUPPRESSION ne sont pas autorisées lors de l'utilisation du noeud final `/api/protocols/nvme/services` avec les systèmes ASA r2.

Modification des propriétés d'un noeud final et d'une méthode HTTP

Certaines combinaisons de noeuds finaux et de méthodes du système ASA r2 ne prennent pas en charge toutes les propriétés définies disponibles dans la personnalité ONTAP unifiée. Par exemple, lors de l'utilisation d' `/api/storage/volumes/{uuid}`un CORRECTIF avec le noeud final, plusieurs propriétés ne sont pas prises en charge par ASA r2, notamment :

- `autosize.maximum`
- `autosize.minimum`
- `autosize.mode`

Modifications apportées au traitement interne

Plusieurs modifications ont été apportées à la façon dont ASA r2 traite certaines requêtes de l'API REST. Par exemple, une demande de SUPPRESSION avec le point de terminaison `/api/storage/luns/{uuid}` est traitée de manière asynchrone.

Sécurité améliorée avec OAuth 2.0

OAuth 2.0 est le cadre d'autorisation standard de l'industrie. Elle permet de restreindre et de contrôler l'accès aux ressources protégées en fonction de jetons d'accès signés. Vous pouvez configurer OAuth 2.0 à l'aide du Gestionnaire système pour protéger les ressources système de ASA r2.

Une fois OAuth 2.0 configuré avec System Manager, l'accès par les clients de l'API REST peut être contrôlé. Vous devez d'abord obtenir un jeton d'accès à partir d'un serveur d'autorisation. Le client REST transmet ensuite le jeton au cluster ASA r2 en tant que jeton porteur à l'aide de l'en-tête de requête d'autorisation HTTP. Voir "Authentification et autorisation via OAuth 2.0" pour plus d'informations.

Accédez à la documentation de référence de l'API ASA r2 via l'interface utilisateur swagger

Vous pouvez accéder à la documentation de référence de l'API REST via l'interface utilisateur swagger de votre système ASA r2.

Description de la tâche

Pour plus d'informations sur l'API REST, accédez à la page de documentation de référence de ASA r2. Dans ce cadre, vous pouvez rechercher la chaîne **caractéristiques de la plate-forme** pour obtenir des détails sur la prise en charge du système ASA r2 pour les appels et les propriétés de l'API.

Avant de commencer

Vous devez disposer des éléments suivants :

- Adresse IP ou nom d'hôte de la LIF de gestion de cluster du système ASA r2

- Nom d’utilisateur et mot de passe pour un compte disposant des droits d’accès à l’API REST

Étapes

1. Tapez l’URL dans votre navigateur et appuyez sur **entrée**:
   `https://<ip_address>/docs/api`
2. Connectez-vous à l’aide de votre compte administrateur.

   La page de documentation de l’API ASA r2 s’affiche avec les appels d’API organisés en catégories de ressources majeures.
3. Pour voir un exemple d’appel d’API qui ne s’applique qu’aux systèmes ASA r2, faites défiler jusqu’à la catégorie **SAN** et cliquez sur **OBTENIR /stockage/unités de stockage**.

Obtenez de l’aide

Gérez AutoSupport sur les systèmes de stockage ASA r2

AutoSupport est un mécanisme qui surveille de manière proactive l’état de votre système et envoie automatiquement des messages au support technique NetApp, à votre organisation de support interne et à un partenaire de support.

Les messages AutoSupport envoyés au support technique sont activés par défaut lorsque vous configurez votre cluster. Vous devez définir les options correctes et disposer d’un hôte de messagerie valide pour que les messages soient envoyés à votre organisation de support interne. ONTAP commence à envoyer des messages AutoSupport 24 heures après leur activation.

Avant de commencer

Vous devez être administrateur du cluster pour gérer AutoSupport.

Tester la connectivité AutoSupport

Une fois le cluster configuré, testez la connectivité AutoSupport pour vérifier que le support technique recevra les messages générés par AutoSupport.

Étapes

1. Dans le gestionnaire système, sélectionnez **Cluster > Paramètres**.
2. En regard de **AutoSupport**, sélectionnez ; puis **Tester la connectivité**.
3. Saisissez un objet pour le message AutoSupport, puis sélectionnez **Envoyer le message test AutoSupport**.

Et la suite ?

Vous avez vérifié que le support technique peut recevoir des messages AutoSupport de votre système ASA r2 et dispose des données nécessaires pour vous aider en cas de problème.

Ajouter des destinataires AutoSupport

Ajoutez des membres de votre organisation de support interne à la liste des adresses e-mail qui reçoivent des messages AutoSupport.

Étapes

1. Dans le gestionnaire système, sélectionnez **Cluster > Paramètres**.
2. À côté de **AutoSupport**, sélectionnez ; puis **plus d’options**.
3. En regard de **Email**, sélectionnez ; puis sélectionnez + Add .
4. Saisissez l’adresse e-mail du destinataire, puis la catégorie de destinataire.

   Pour les partenaires, sélectionnez **partenaire** pour la catégorie de destinataires. Sélectionnez **général** pour les membres de votre organisation de soutien interne.

5. Sélectionnez enregistrer.

Et la suite ?

Les adresses e-mail que vous avez ajoutées recevront de nouveaux messages AutoSupport pour leur

catégorie de destinataire spécifique.

Envoyer des données AutoSupport

En cas de problème sur votre système ASA r2, les données AutoSupport réduisent considérablement le temps nécessaire à l'identification et à la résolution des problèmes.

Étapes

1. Dans le gestionnaire système, sélectionnez **Cluster > Paramètres**.
2. En regard de **AutoSupport**, sélectionnez ; puis **générer et envoyer**.
3. Saisissez un objet pour le message AutoSupport, puis sélectionnez **Envoyer**.

Et la suite ?

Vos données AutoSupport sont envoyées au support technique.

Supprimer la génération de dossier de support

Si vous effectuez une mise à niveau ou une maintenance sur votre système ASA r2, vous pouvez supprimer les dossiers de demande de support de la génération AutoSupport jusqu'à ce que votre mise à niveau ou votre maintenance soit terminée.

Étapes

1. Dans le gestionnaire système, sélectionnez **Cluster > Paramètres**.
2. En regard de **AutoSupport**, sélectionnez ; puis sélectionnez **Supprimer la génération de cas de support**.
3. Spécifiez le nombre d'heures pour supprimer la génération de dossiers de support, puis sélectionnez les nœuds pour lesquels vous ne souhaitez pas générer de dossiers.
4. Sélectionnez **Envoyer**.

Et la suite ?

Les dossiers AutoSupport ne seront pas générés pendant le temps que vous avez spécifié. Si vous effectuez la mise à niveau ou la maintenance avant l'expiration du délai spécifié, vous devez reprendre immédiatement la génération du dossier de support.

Reprendre la génération du dossier de support

Si vous avez supprimé la génération de dossiers de support pendant une fenêtre de mise à niveau ou de maintenance, vous devez reprendre la génération de dossiers de support immédiatement après la fin de votre mise à niveau ou de votre maintenance.

Étapes

1. Dans le gestionnaire système, sélectionnez **Cluster > Paramètres**.
2. En regard de **AutoSupport**, sélectionnez ; puis sélectionnez **reprendre la génération de cas de support**.
3. Sélectionnez les nœuds pour lesquels vous souhaitez reprendre les dossiers AutoSupport générés.
4. Sélectionnez **Envoyer**.

Résultat

Les dossiers AutoSupport sont générés automatiquement pour votre système ASA r2, si nécessaire.

Envoi et consultation des dossiers de demande de support pour les systèmes de stockage ASA r2

Si vous rencontrez un problème qui nécessite de l'aide, utilisez le Gestionnaire système ONTAP pour soumettre un dossier au support technique. Vous pouvez également utiliser ONTAP System Manager pour afficher les dossiers clos ou en cours d'exécution.

Vous devez "Enregistré auprès de Active IQ"afficher les dossiers de demande de support de votre système ASA r2.

Étapes

1. Pour soumettre un dossier d'assistance, dans le Gestionnaire système, sélectionnez **Cluster > support**, puis sélectionnez **aller au support NetApp**.
2. Pour afficher un cas soumis précédemment, dans System Manager, sélectionnez **Cluster > support**, puis **Afficher mes cas**.

Mentions légales

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

Droits d’auteur

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

Marques déposées

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

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

Brevets

Vous trouverez une liste actuelle des brevets appartenant à NetApp à l’adresse suivante :

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

Politique de confidentialité

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

Source ouverte

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