Documentation de ASA r2

ASA r2

NetApp
February 11, 2026

Sommaire

Documentation de ASA r2

Notes de mise à jour

Nouveautés d' ONTAP 9.18.1 pour les systèmes ASA r2

Découvrez les nouvelles fonctionnalités disponibles dans ONTAP 9.18.1 pour les systèmes ASA r2.

Protection des données

Mise à jour	Description
"Prise en charge accrue des configurations de synchronisation active SnapMirror"	La prise en charge de la synchronisation active SnapMirror est étendue des clusters à deux nœuds aux clusters à quatre nœuds.

Réseautage

Mise à jour	Description
"Déchargement matériel IPsec, prise en charge d'IPv6"	La prise en charge du déchargement matériel IPsec est étendue à IPv6.
"Algorithmes PQC d'OpenSSL"	ONTAP prend en charge les algorithmes cryptographiques post-quantiques pour SSL. Ces algorithmes offrent une protection supplémentaire contre d'éventuelles futures attaques informatiques quantiques et sont disponibles lorsque le mode SSL FIPS est désactivé.

Migration de données SAN

Mise à jour	Description
"Prise en charge de la migration des machines virtuelles de stockage"	Vous pouvez migrer sans interruption une machine virtuelle de stockage (VM) d'un cluster ASA vers un cluster ASA r2. Cela permet de déplacer les charges de travail par blocs vers les systèmes ASA r2 tout en préservant l'intégrité des données et en garantissant l'absence d'impact sur les applications. Le processus de migration est conçu pour maintenir les mappages hôtes et les configurations LUN existants, réduisant ainsi les efforts opérationnels et les risques pendant la migration.

Sécurité

Mise à jour	Description
"Prise en charge de l'activation automatique ARP/AI"	Lorsque vous initialisez un nouveau cluster ASA r2 9.18.1 ou que vous mettez à niveau votre cluster vers 9.18.1, ARP/AI est automatiquement activé par défaut sur toutes les nouvelles unités de stockage après un délai de grâce de 12 heures. Si vous ne désactivez pas ARP/AI pendant le délai de grâce, il est activé à l'échelle du cluster pour les nouvelles unités de stockage créées lorsque le délai de grâce prend fin.

Efficacité du stockage

Mise à jour	Description
"Prise en charge du déchargement de copie NVMe"	La fonction de déchargement de copie NVMe permet à un hôte NVMe de décharger les opérations de copie de son processeur vers le processeur du contrôleur de stockage ONTAP . L'hôte peut copier des données d'un espace de noms NVMe à un autre tout en réservant ses ressources CPU pour les charges de travail applicatives.
"Prise en charge de la modification de la réserve d'instantanés et de la suppression automatique des instantanés"	Vous pouvez modifier la réserve de snapshots et activer la suppression automatique des snapshots pour limiter l'espace utilisé pour les snapshots dans vos unités de stockage ASA r2. Lorsque la réserve d'instantanés est configurée avec la suppression automatique des instantanés, les instantanés les plus anciens sont automatiquement supprimés lorsque l'espace utilisé par les instantanés dépasse la réserve d'instantanés. Cela évite les interruptions d'application en empêchant les instantanés de consommer de l'espace dans votre unité de stockage destiné aux données utilisateur.

Nouveautés d' ONTAP 9.17.1 pour les systèmes ASA r2

Découvrez les nouvelles fonctionnalités disponibles dans ONTAP 9.17.1 pour les systèmes ASA r2.

Migration de données SAN

Mise à jour	Description
"Prise en charge de la migration de données à partir d'un système de stockage tiers"	La migration de données SAN via l'importation de LUN étrangers (FLI) est prise en charge pour les systèmes ASA r2. FLI permet de migrer des données d'un LUN d'un système de stockage tiers vers un système ASA r2.

Protection des données

Mise à jour	Description
"Prise en charge de la protection autonome contre les ransomwares avec intelligence artificielle (ARP/AI)"	ARP/AI peut être activé sur les unités de stockage ASA r2. ARP/AI offre une protection supplémentaire des données en détectant et en signalant les attaques potentielles de ransomware sans période d'apprentissage.
"Prise en charge de SnapMirror Active Sync pour les protocoles NVMe"	SnapMirror Active Sync prend désormais en charge les charges de travail VMware avec accès hôte NVMe/TCP et NVMe/FC pour les clusters ONTAP à deux nœuds. La prise en charge des charges de travail VMware pour NVMe/TCP dépend de la résolution du bug VMware n° TR1049746.

Mise à jour	Description
"Prise en charge des modifications géométriques des groupes de cohérence dans les relations de réplication"	Les systèmes ASA r2 prennent en charge les modifications de géométrie apportées aux groupes de cohérence dans une synchronisation active SnapMirror ou une relation de réplication asynchrone sans supprimer la relation de synchronisation active SnapMirror ni rompre la relation asynchrone. Lorsqu'une modification de géométrie se produit sur le groupe de cohérence principal, la modification est répliquée sur le groupe de cohérence secondaire.
"Prise en charge de la réplication asynchrone des groupes de cohérence enfants"	Les politiques de réplication asynchrone peuvent être appliquées aux groupes de cohérence dans des relations hiérarchiques.

Gestion du stockage

Mise à jour	Description
"Prise en charge de l'équilibrage automatique de la charge de travail"	Les charges de travail sont automatiquement équilibrées entre les nœuds d'une paire HA pour optimiser les performances et l'utilisation des ressources.

Nouveautés de ONTAP 9.16.1 pour les systèmes ASA r2

Découvrez les nouvelles fonctionnalités disponibles dans ONTAP 9.16.1 pour les systèmes ASA r2.

Systèmes

Mise à jour	Description
Systèmes	Les systèmes NetApp ASA r2 suivants sont pris en charge à partir d' ONTAP 9.16.1. Ces systèmes offrent une solution matérielle et logicielle unifiée qui crée une expérience simplifiée adaptée aux besoins spécifiques des clients utilisant exclusivement un SAN. • ASA A50 • ASA A30 • ASA A20 • ASA C30

Protection des données

Mise à jour	Description
"Prise en charge de la migration des clés de chiffrement entre les gestionnaires de clés"	Lorsque vous basculez du gestionnaire de clés intégré ONTAP vers un gestionnaire de clés externe au niveau du cluster, vous pouvez utiliser l'interface de ligne de commandes ONTAP pour migrer facilement les clés de chiffrement d'un gestionnaire de clés vers un autre.

Mise à jour	Description
"Prise en charge des groupes de cohérence hiérarchiques"	Les groupes de cohérence hiérarchiques vous permettent de créer un groupe de cohérence parent contenant plusieurs groupes de cohérence enfant. Cela simplifie la protection et la gestion des données pour les structures de données complexes.

Protocoles pris en charge

Mise à jour	Description
"Prise en charge de NVMe pour les chemins d'accès multiples symétriques actif-actif"	NVMe/FC et NVMe/TCP prennent désormais en charge l'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.

Efficacité du stockage

Mise à jour	Description
"Prise en charge du rééquilibrage automatique des unités de stockage"	ONTAP rééquilibre automatiquement les unités de stockage dans vos zones de disponibilité du stockage pour une utilisation optimale des performances et de la capacité.
"La désallocation d'espace NVMe est activée par défaut"	La désallocation d'espace (également appelée « perforation » et « unmap ») est activée par défaut pour les espaces de noms NVMe. La désallocation d'espace permet à un hôte de désallouer les blocs inutilisés à partir des espaces de noms pour libérer de l'espace. Cela améliore considérablement l'efficacité globale du stockage, en particulier avec les systèmes de fichiers dont le volume de données est élevé.

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.

Systèmes

Mise à jour	Description
Systèmes	Les systèmes NetApp ASA r2 suivants sont disponibles. Ces systèmes offrent une solution matérielle et logicielle unifiée qui crée une expérience simplifiée adaptée aux besoins spécifiques des clients utilisant exclusivement 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).

Modifications des limites ONTAP et des valeurs par défaut affectant les systèmes ASA r2

En savoir plus sur les modifications des limites et des valeurs par défaut affectant les systèmes ASA r2. NetApp s'efforce d'aider ses clients à comprendre les valeurs par défaut les plus importantes et à limiter les modifications apportées à chaque version de ONTAP.

Modifications des limites ONTAP

Fonction	Modification de limite	Modifié dans la version…
Machines virtuelles de stockage par cluster	Le nombre maximal de machines virtuelles de stockage prises en charge (VM) par paire HA passe de 32 à 256.	ONTAP 9.18.1
SnapMirror activ sync	La prise en charge de la synchronisation active SnapMirror est étendue des clusters à deux nœuds aux clusters à quatre nœuds.	ONTAP 9.18.1

Fonction	Modification de limite	Modifié dans la version…
Nœuds par cluster	Le nombre maximum de nœuds par cluster est passé de 2 à 12. Si vous exécutez ONTAP 9.16.1 avec plus de 2 nœuds dans un cluster, vous ne pouvez pas revenir à ONTAP 9.16.0.	ONTAP 9.16.1
Unités de stockage	Le nombre maximal d'unités de stockage est augmenté de 2500 par paire haute disponibilité à 10,000 par paire haute disponibilité.	ONTAP 9.16.1

Commencez

En savoir plus sur les systèmes de stockage ASA r2

Les systèmes NetApp ASA r2 apportent une solution matérielle et logicielle unifiée qui simplifie l'expérience et répond parfaitement aux besoins des clients SAN.

Les éléments suivants sont classés comme systèmes ASA r2 :

- ASA A1K
- ASA A90
- ASA A70
- ASA A50
- ASA A30
- ASA A20
- ASA C30

Les systèmes ASA r2 prennent en charge tous les protocoles SAN (iSCSI, FC, NVMe/FC, NVMe/TCP). Les protocoles iSCSI, FC, NVMe/FC et NVMe/TCP prennent en charge l'architecture active-active symétrique pour le multivoie afin que tous les chemins entre les hôtes et le stockage soient actifs/optimisés. Les protocoles iSCSI et NVMe/TCP prennent en charge la connexion directe entre les hôtes et le stockage. Pour les protocoles Fibre Channel et NVMe/FC, la connexion directe n'est pas prise en charge.

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 avec des groupes de cohérence pour simplifier la gestion du stockage et la protection des données. Par exemple, supposons que vous disposez d'une base de données composée de 10 unités de stockage dans un groupe de cohérence et que vous devez sauvegarder l'intégralité de la base de données. Au lieu de sauvegarder chaque unité de stockage individuellement, vous pouvez protéger l'intégralité de la base de données en sauvegardant le groupe de cohérence.

Pour protéger vos données contre les attaques malveillantes telles que le vol ou les rançongiciels, les systèmes ASA r2 prennent en charge un gestionnaire de clés intégré, un chiffrement double couche, une authentification multifacteur et une vérification multi-administrateur. Les instantanés inviolables sont également pris en charge sur les systèmes ASA r2 secondaires.

Les systèmes ASA r2 ne prennent pas en charge le mixage de clusters avec les systèmes ASA, AFF ou FAS .

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 "Les 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 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 la mise en place des ID de tablette de stockage
- Tournevis Phillips n°2

Précautions de levage

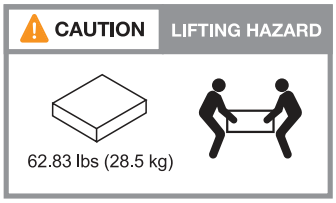
Les systèmes de stockage et tiroirs de stockage ASA r2 sont très lourds. Faites preuve de prudence lorsque vous soulevez et déplacez ces éléments.

Poids du système de stockage

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

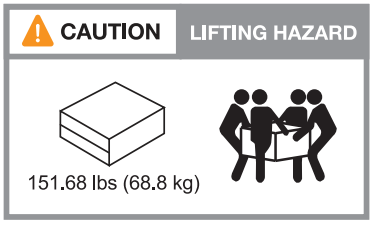
A1K

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



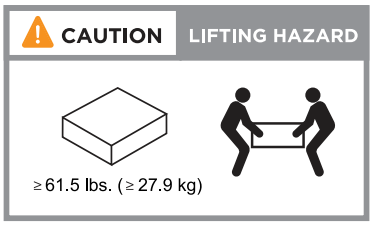
A70 et A90

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



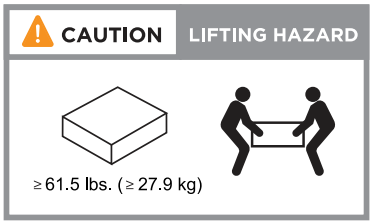
A20, A30 ET A50

Un système de stockage ASA A20, ASA A30 ou ASA A50 peut peser jusqu'à 27.9 kg (61.5 lb). Pour soulever le système de stockage, faire appel à deux personnes ou à un relevage hydraulique.



C30

Un système de stockage ASA C30 peut peser jusqu'à 61,5 lb (27,9 kg). Pour soulever le système de stockage, faire appel à deux personnes ou à un relevage hydraulique.

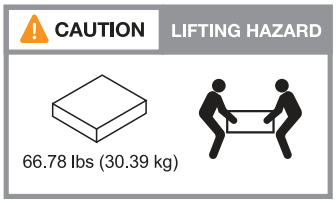


Poids des étagères de stockage

Prenez les précautions nécessaires lorsque vous déplacez ou soulevez votre tablette.

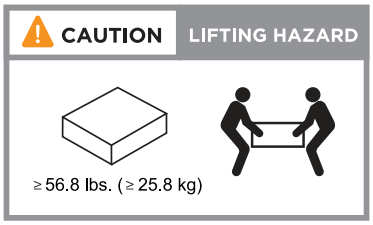
Tiroir NS224

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



Tiroir NS224 avec modules NSM100B

Une étagère NS224 avec modules NSM100B peut peser jusqu'à 25.8 kg (56.8 lb). Pour soulever la tablette, faites appel à deux personnes ou à un dispositif de levage hydraulique. Conservez tous les composants dans la tablette (à l'avant et à l'arrière) pour éviter de rééquilibrer 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.
2. Assurez-vous de disposer d'une armoire ou d'un espace rack adapté à votre système de stockage, à vos tiroirs et aux commutateurs :

A1K

- 4U en configuration HA
- 2U pour chaque tiroir de stockage NS224
- 1U pour la plupart des commutateurs

A70 et A90

- 4U en configuration HA
- 2U pour chaque tiroir de stockage NS224
- 1U pour la plupart des commutateurs

A20, A30 ET A50

- 2U pour un système de stockage
- 2U pour chaque tiroir de stockage NS224
- 1U pour la plupart des commutateurs

C30

- 2U pour un système de stockage
- 2U pour chaque tiroir de stockage NS224
- 1U pour la plupart des commutateurs

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. En cas d'écarts, notez-les pour prendre des mesures supplémentaires.

   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.

Matériel	Câbles	

• Panneau • Adieu les migrations de données onéreuses • Kits de rails avec instructions (en option) • Tiroir de stockage (si vous avez commandé du stockage supplémentaire)	• 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

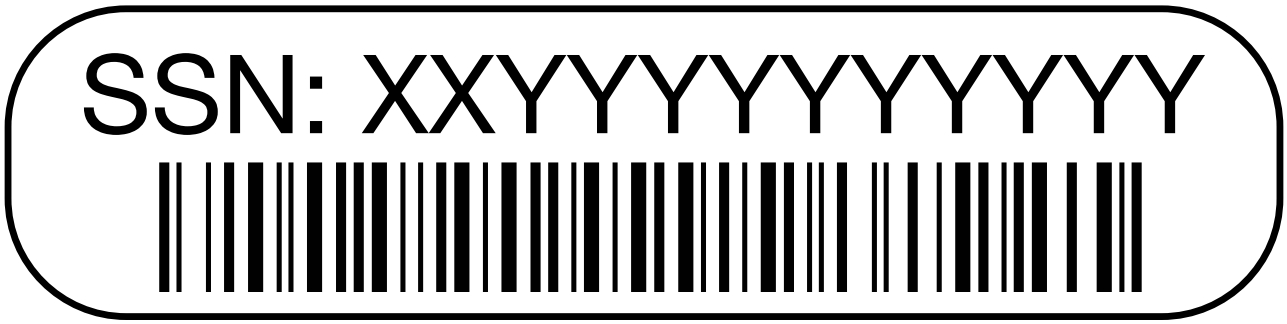
Après avoir vérifié que votre site répond aux spécifications de votre système de stockage ASA r2 et après avoir vérifié que vous disposez de toutes les pièces commandées, vous devez enregistrer votre système.

Étapes

1. Recherchez les numéros de série de votre système de stockage.

   Les numéros de série sont indiqués aux emplacements suivants :

   - Sur le bordereau d'expédition
   - Dans votre e-mail de confirmation
   - Sur chaque contrôleur ou pour certains systèmes, sur le module de gestion du système de chaque contrôleur

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 le numéro de série n'est pas répertorié, suivez les instructions pour les nouveaux clients NetApp.

Si vous êtes…	Suivez ces étapes…
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

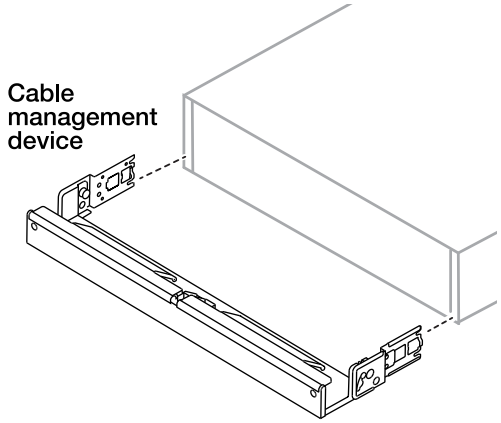
Après avoir préparé l'installation du système de stockage ASA r2, installez le matériel du système. Commencez par installer les kits de rails. Installez ensuite et sécurisez votre système de stockage dans une armoire ou un rack de télécommunications.

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. Assurez-vous que les broches de guidage de l'armoire ou du rack Telco s'insèrent parfaitement dans les fentes de guidage du système de stockage.
   c. Fixez le système de stockage à l'armoire ou au rack de télécommunications à l'aide des vis de montage fournies.
3. Fixez le panneau à l'avant du système de stockage.
4. Si votre système ASA r2 est fourni avec un dispositif de gestion des câbles, connectez-le à l'arrière du système de stockage.



5. Installez et fixez 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.

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

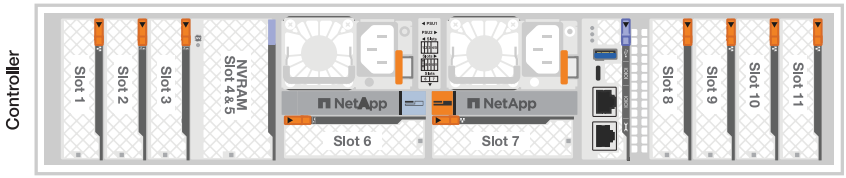
Pour plus d'informations sur la connexion du système de stockage aux commutateurs réseau, contactez votre administrateur réseau.

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".
- Les procédures de câblage du réseau hôte/cluster/haute disponibilité présentent les configurations courantes.

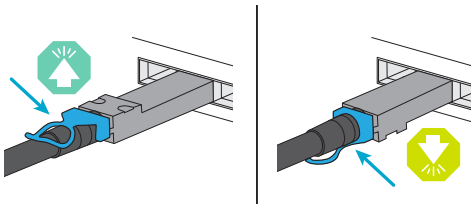
  Si vous ne voyez pas votre configuration dans les procédures de câblage, accédez à "NetApp Hardware Universe" pour une configuration complète et des informations sur la priorité des emplacements afin de câbler correctement votre système de stockage.

- Si vous disposez d'un système de stockage ASA A1K, ASA A70 ou ASA A90, les emplacements d'E/S sont numérotés de 1 à 11.



- Les graphiques de câblage sont dotés d'icônes de flèche indiquant l'orientation correcte (vers le haut ou vers le bas) de la languette du connecteur de câble lors de l'insertion d'un connecteur dans un port.

  Lorsque vous insérez le connecteur, vous devez le sentir en place ; si vous ne le sentez pas, retirez-le, retournez-le et réessayez.



- Si vous effectuez un câblage vers un commutateur optique, insérez l'émetteur-récepteur optique dans le port du contrôleur avant de le connecter au port du commutateur.

Étape 1 : câblez les connexions du cluster/haute disponibilité

Connectez les contrôleurs au cluster ONTAP. Cette procédure varie en fonction du modèle de votre système de stockage et de la configuration de votre module d'E/S.

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

A1K

Créez les connexions du cluster ONTAP. Dans le cas de clusters sans commutateur, connectez les contrôleurs les uns aux autres. Pour les clusters commutés, connectez les contrôleurs aux commutateurs de réseau du cluster.

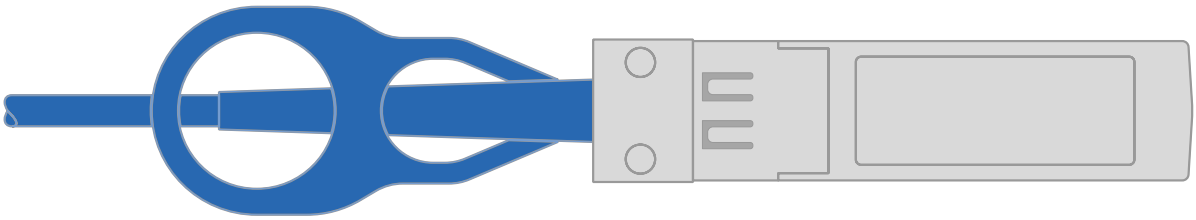
Câblage switchless cluster Cabling

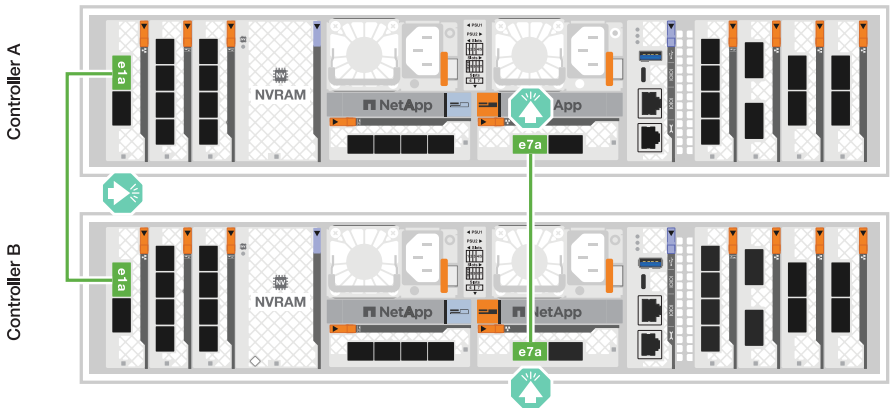
Utilisez le câble d'interconnexion cluster/haute disponibilité pour connecter les ports e1a à e1a et les ports e7a à e7a.

Étapes

1. Connectez le port e1a du contrôleur A au port e1a du contrôleur B.
2. Connectez le port e7a du contrôleur A au port e1a du contrôleur B.

Câbles d'interconnexion cluster/haute disponibilité





Câblage commuté du cluster

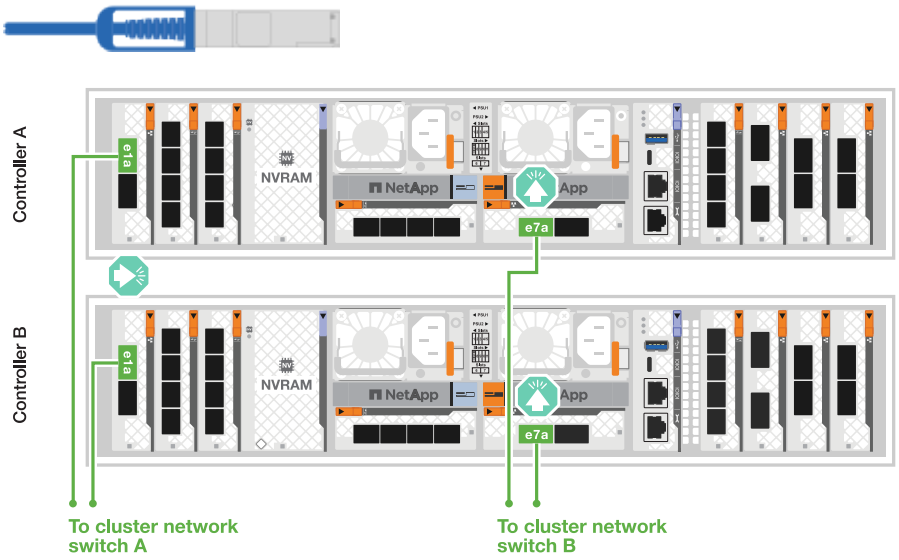
Utilisez le câble 100 GbE pour connecter les ports e1a à e1a et les ports e7a à e7a.

> Les configurations de cluster commuté sont prises en charge dans la version 9.16.1 et les versions ultérieures.

Étapes

1. Connectez le port e1a du contrôleur A et le port e1a du contrôleur B au commutateur a du réseau du cluster
2. Connectez le port e7a du contrôleur A et le port e7a du contrôleur B au commutateur de réseau du cluster B.

Câble 100 GbE



A70 et A90

Créez les connexions du cluster ONTAP. Dans le cas de clusters sans commutateur, connectez les contrôleurs les uns aux autres. Pour les clusters commutés, connectez les contrôleurs aux commutateurs de réseau du cluster.

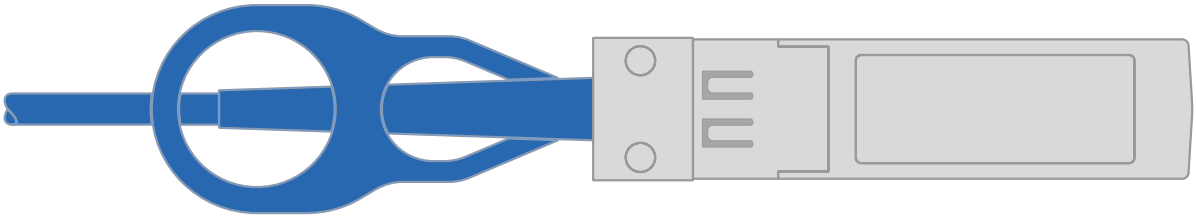
Câblage switchless cluster Cabling

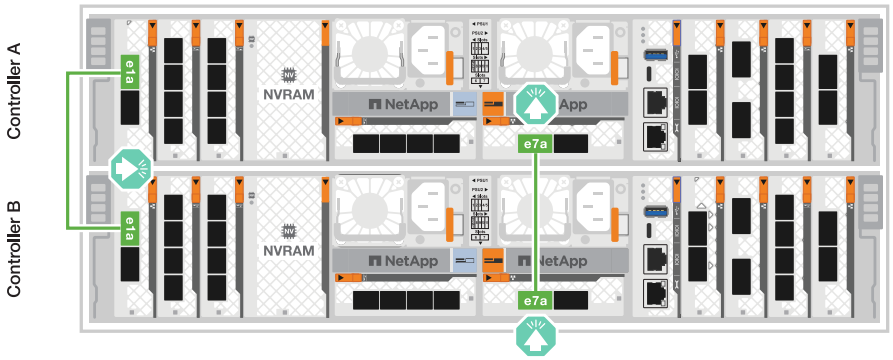
Utilisez le câble d'interconnexion cluster/haute disponibilité pour connecter les ports e1a à e1a et les ports e7a à e7a.

Étapes

1. Connectez le port e1a du contrôleur A au port e1a du contrôleur B.
2. Connectez le port e7a du contrôleur A au port e1a du contrôleur B.

Câbles d'interconnexion cluster/haute disponibilité





Câblage commuté du cluster

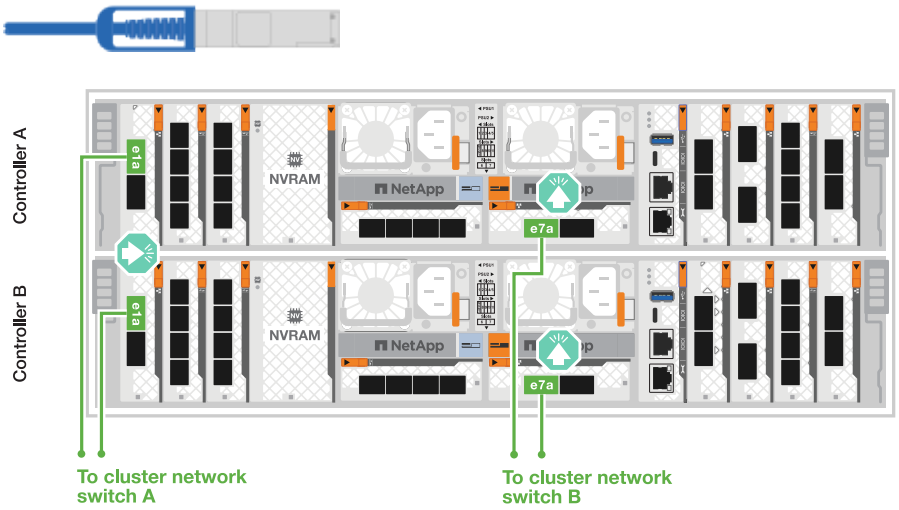
Utilisez le câble 100 GbE pour connecter les ports e1a à e1a et les ports e7a à e7a.

Les configurations de cluster commuté sont prises en charge dans la version 9.16.1 et les versions ultérieures.

Étapes

1. Connectez le port e1a du contrôleur A et le port e1a du contrôleur B au commutateur a du réseau du cluster
2. Connectez le port e7a du contrôleur A et le port e7a du contrôleur B au commutateur de réseau du cluster B.

Câble 100 GbE



A20, A30 ET A50

Créez les connexions du cluster ONTAP. Dans le cas de clusters sans commutateur, connectez les contrôleurs les uns aux autres. Pour les clusters commutés, connectez les contrôleurs aux commutateurs de réseau du cluster.

Les exemples de câblage cluster/HA montrent des configurations courantes.

Si vous ne voyez pas votre configuration ici, accédez à "NetApp Hardware Universe" pour obtenir des informations complètes sur la configuration et la priorité des emplacements pour câbler votre système de stockage.

Câblage de cluster sans commutateur

Connectez les contrôleurs l'un à l'autre pour créer des connexions de cluster ONTAP.

ASA A30 et ASA A50 avec deux modules d'E/S 40/100 GbE à 2 ports

Étapes

1. Connectez les connexions d'interconnexion cluster/haute disponibilité :

   Le trafic d'interconnexion de cluster et le trafic haute disponibilité partagent les mêmes ports physiques (sur les modules d'E/S des connecteurs 2 et 4). Les ports sont 40/100 GbE.

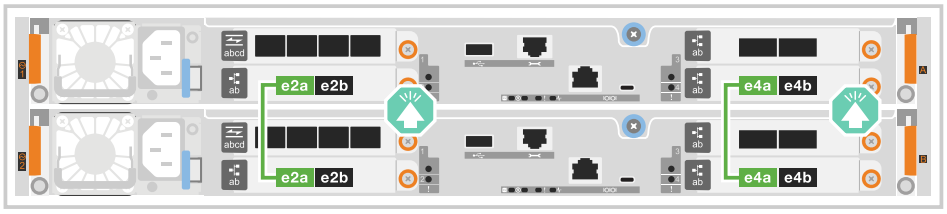
   a. Brancher le port e2a du contrôleur A sur le port e2a du contrôleur B.

   b. Connectez le port e4a du contrôleur A au port e4a du contrôleur B.

   Les ports de module d'E/S e2b et e4b sont inutilisés et disponibles pour la connectivité réseau de l'hôte.

Câbles d'interconnexion cluster/haute disponibilité 100 GbE

Controller A



Controller B

ASA A30 et ASA A50 avec un module d'E/S 40/100 GbE à 2 ports

Étapes

1. Connectez les connexions d'interconnexion cluster/haute disponibilité :

> Le trafic d'interconnexion de cluster et le trafic haute disponibilité partagent les mêmes ports physiques (sur le module d'E/S du slot 4). Les ports sont 40/100 GbE.

a. Connectez le port e4a du contrôleur A au port e4a du contrôleur B.

b. Connectez le port e4b du contrôleur A au port e4b du contrôleur B.

Câbles d'interconnexion cluster/haute disponibilité 100 GbE

Controller A

Controller B

ASA A20 avec un module d'E/S 10/25 GbE à 2 ports

Étapes

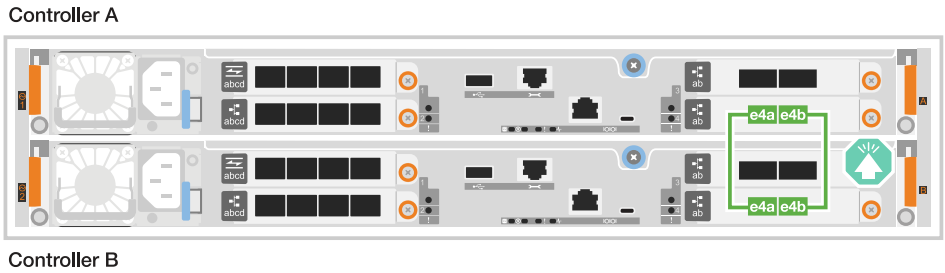
1. Connectez les connexions d'interconnexion cluster/haute disponibilité :

> Le trafic d'interconnexion de cluster et le trafic haute disponibilité partagent les mêmes ports physiques (sur le module d'E/S du slot 4). Les ports sont 10/25 GbE.

a. Connectez le port e4a du contrôleur A au port e4a du contrôleur B.

b. Connectez le port e4b du contrôleur A au port e4b du contrôleur B.

Câbles d'interconnexion cluster/haute disponibilité 25 GbE



Câblage de cluster commuté

Connectez les contrôleurs aux commutateurs de réseau du cluster pour créer les connexions de cluster ONTAP.

ASA A30 ou ASA A50 avec deux modules d'E/S 40/100 GbE à 2 ports

Étapes

1. Reliez les connexions d'interconnexion cluster/haute disponibilité :

> Le trafic d'interconnexion de cluster et le trafic haute disponibilité partagent les mêmes ports physiques (sur les modules d'E/S des connecteurs 2 et 4). Les ports sont 40/100 GbE.

a. Connectez le port e4a du contrôleur A au commutateur réseau du cluster A.

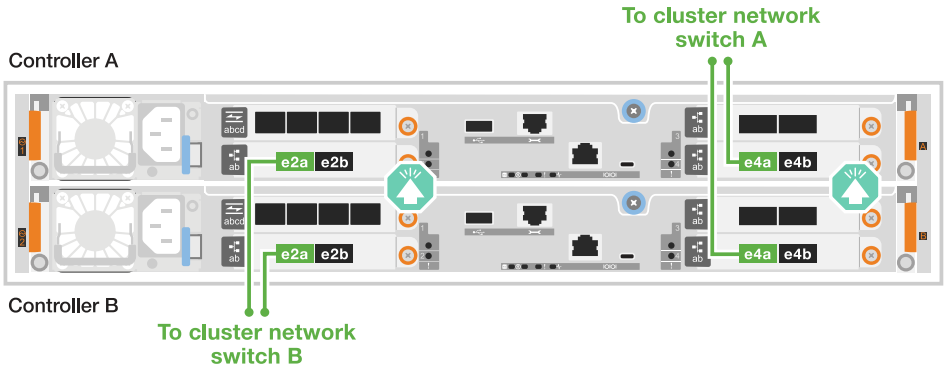
b. Connectez le port e2a du contrôleur A au commutateur réseau du cluster B.

c. Connectez le port e4a du contrôleur B au commutateur réseau du cluster A.

d. Connectez le port e2a du contrôleur B au commutateur réseau du cluster B.

> Les ports de module d'E/S e2b et e4b sont inutilisés et disponibles pour la connectivité réseau de l'hôte.

Câbles d'interconnexion cluster/haute disponibilité 40/100 GbE



ASA A30 ou ASA A50 avec un module d'E/S 40/100 GbE à 2 ports

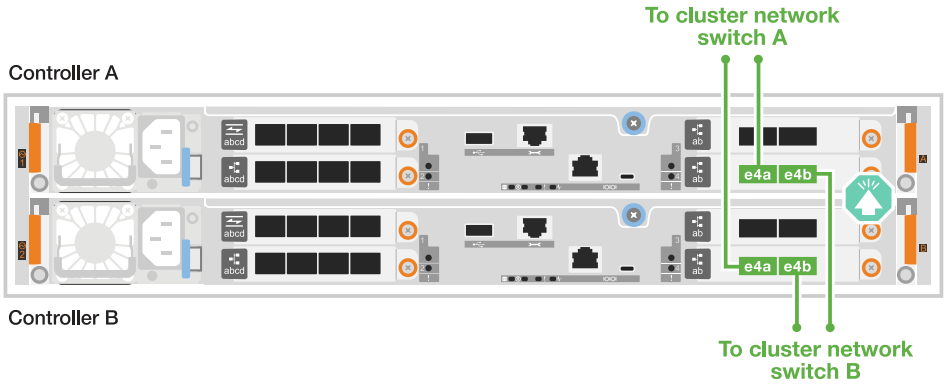
Étapes

1. Reliez les contrôleurs aux commutateurs du réseau du cluster :

> Le trafic d'interconnexion de cluster et le trafic haute disponibilité partagent les mêmes ports physiques (sur le module d'E/S du slot 4). Les ports sont 40/100 GbE.

a. Connectez le port e4a du contrôleur A au commutateur réseau du cluster A.
b. Connectez le port e4b du contrôleur A au commutateur réseau du cluster B.
c. Connectez le port e4a du contrôleur B au commutateur réseau du cluster A.
d. Connectez le port e4b du contrôleur B au commutateur réseau du cluster B.

Câbles d'interconnexion cluster/haute disponibilité 40/100 GbE



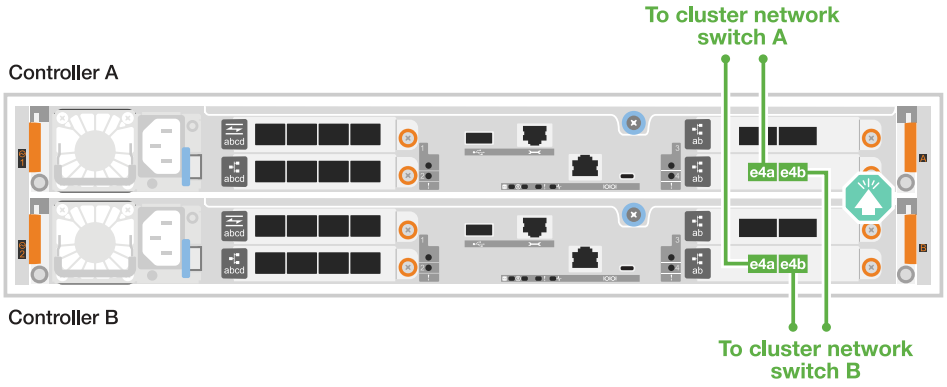
ASA A20 avec un module d'E/S 10/25 GbE à 2 ports

1. Reliez les contrôleurs aux commutateurs du réseau du cluster :

   Le trafic d'interconnexion de cluster et le trafic haute disponibilité partagent les mêmes ports physiques (sur le module d'E/S du slot 4). Les ports sont 10/25 GbE.

   a. Connectez le port e4a du contrôleur A au commutateur réseau du cluster A.
   b. Connectez le port e4b du contrôleur A au commutateur réseau du cluster B.
   c. Connectez le port e4a du contrôleur B au commutateur réseau du cluster A.
   d. Connectez le port e4b du contrôleur B au commutateur réseau du cluster B.

   Câbles d'interconnexion cluster/haute disponibilité 10/25 GbE



Créez les connexions du cluster ONTAP. Dans le cas de clusters sans commutateur, connectez les contrôleurs les uns aux autres. Pour les clusters commutés, connectez les contrôleurs aux commutateurs de réseau du cluster.

Les exemples de câblage cluster/HA montrent des configurations courantes.

Si vous ne voyez pas votre configuration ici, accédez à "NetApp Hardware Universe" pour obtenir des informations complètes sur la configuration et la priorité des emplacements pour câbler votre système de stockage.

Câblage de cluster sans commutateur

Connectez les contrôleurs l'un à l'autre pour créer des connexions de cluster ONTAP.

ASA C30 avec deux modules d'E/S 40/100 GbE à 2 ports

Étapes

1. Reliez les connexions d'interconnexion cluster/haute disponibilité :

   Le trafic d'interconnexion de cluster et le trafic haute disponibilité partagent les mêmes ports physiques (sur les modules d'E/S des connecteurs 2 et 4). Les ports sont 40/100 GbE.

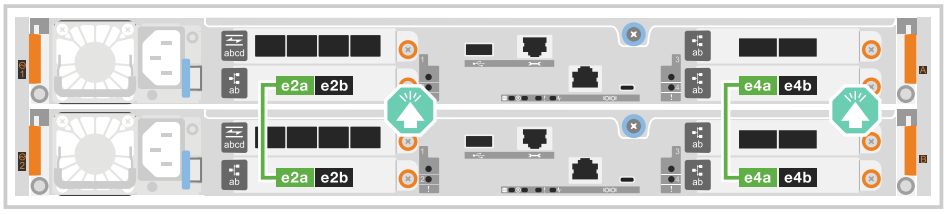
   a. Brancher le port e2a du contrôleur A sur le port e2a du contrôleur B.

   b. Connectez le port e4a du contrôleur A au port e4a du contrôleur B.

   Les ports de module d'E/S e2b et e4b sont inutilisés et disponibles pour la connectivité réseau de l'hôte.

Câbles d'interconnexion cluster/haute disponibilité 100 GbE

Controller A



Controller B

ASA C30 avec un module d'E/S 40/100 GbE à 2 ports

Étapes

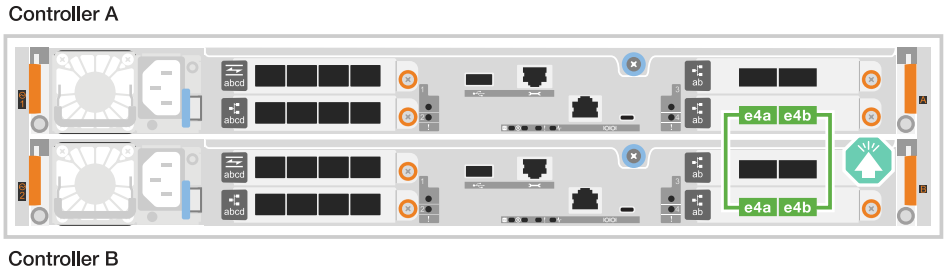
1. Reliez les connexions d'interconnexion cluster/haute disponibilité :

> Le trafic d'interconnexion de cluster et le trafic haute disponibilité partagent les mêmes ports physiques (sur le module d'E/S du slot 4). Les ports sont 40/100 GbE.

a. Connectez le port e4a du contrôleur A au port e4a du contrôleur B.

b. Connectez le port e4b du contrôleur A au port e4b du contrôleur B.

Câbles d'interconnexion cluster/haute disponibilité 100 GbE



Câblage de cluster commuté

Connectez les contrôleurs aux commutateurs de réseau du cluster pour créer les connexions de cluster ONTAP.

ASA C30 avec deux modules d'E/S 40/100 GbE à 2 ports

Étapes

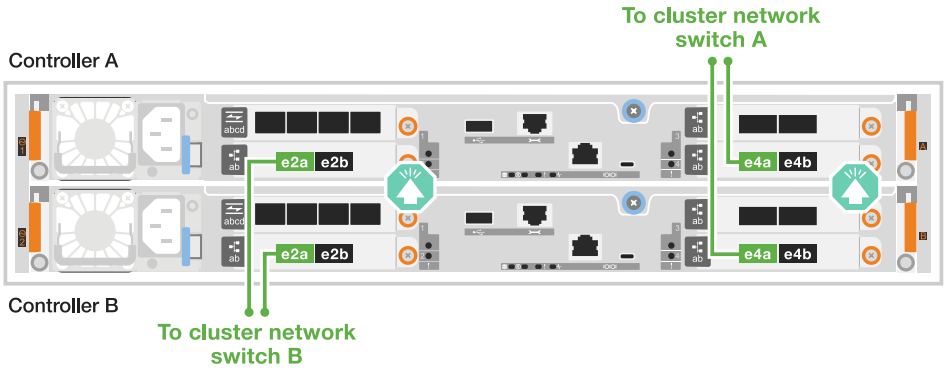
1. Reliez les connexions d'interconnexion cluster/haute disponibilité :

> Le trafic d'interconnexion de cluster et le trafic haute disponibilité partagent les mêmes ports physiques (sur les modules d'E/S des connecteurs 2 et 4). Les ports sont 40/100 GbE.

a. Connectez le port e4a du contrôleur A au commutateur réseau du cluster A.
b. Connectez le port e2a du contrôleur A au commutateur réseau du cluster B.
c. Connectez le port e4a du contrôleur B au commutateur réseau du cluster A.
d. Connectez le port e2a du contrôleur B au commutateur réseau du cluster B.

> Les ports de module d'E/S e2b et e4b sont inutilisés et disponibles pour la connectivité réseau de l'hôte.

Câbles d'interconnexion cluster/haute disponibilité 40/100 GbE



ASA C30 avec un module d'E/S 40/100 GbE à 2 ports

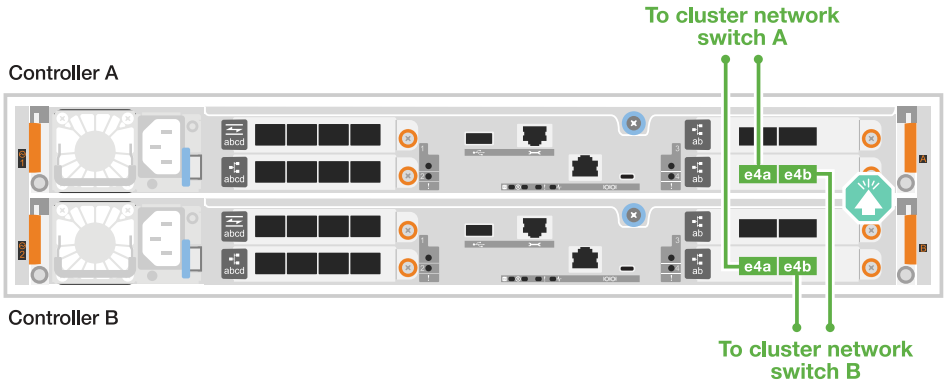
Étapes

1. Connectez les contrôleurs aux commutateurs réseau du cluster :

> Le trafic d'interconnexion de cluster et le trafic haute disponibilité partagent les mêmes ports physiques (sur le module d'E/S du slot 4). Les ports sont 40/100 GbE.

a. Connectez le port e4a du contrôleur A au commutateur réseau du cluster A.
b. Connectez le port e4b du contrôleur A au commutateur réseau du cluster B.
c. Connectez le port e4a du contrôleur B au commutateur réseau du cluster A.
d. Connectez le port e4b du contrôleur B au commutateur réseau du cluster B.

Câbles d'interconnexion cluster/haute disponibilité 40/100 GbE



Étape 2 : câblez les connexions réseau de l'hôte

Connectez les contrôleurs à votre réseau hôte.

Cette procédure varie en fonction du modèle de votre système de stockage et de la configuration de votre module d'E/S.

A1K

Connectez les ports du module Ethernet à votre réseau hôte.

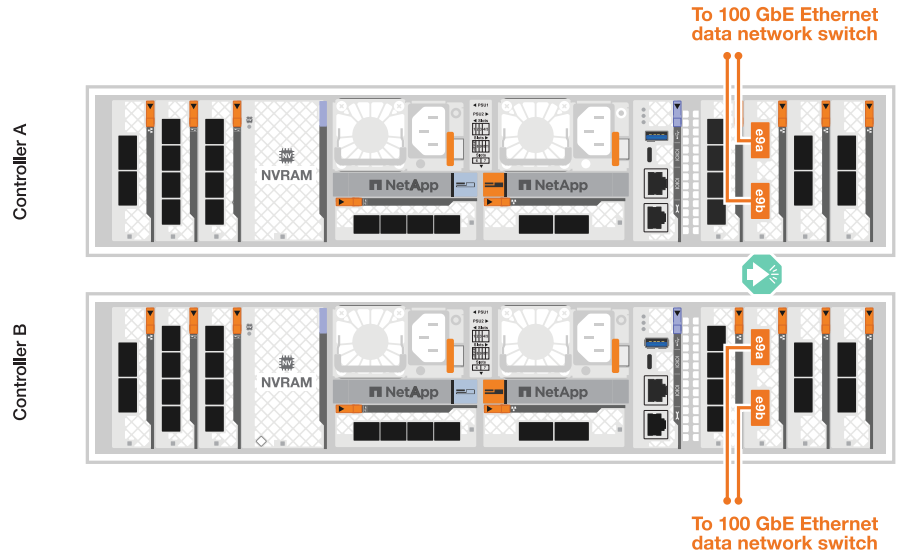
Voici quelques exemples types de câblage réseau hôte. Reportez-vous à la section "NetApp Hardware Universe" pour connaître la configuration spécifique de votre système.

Étapes

1. Connectez les ports e9a et e9b à votre commutateur de réseau de données Ethernet.

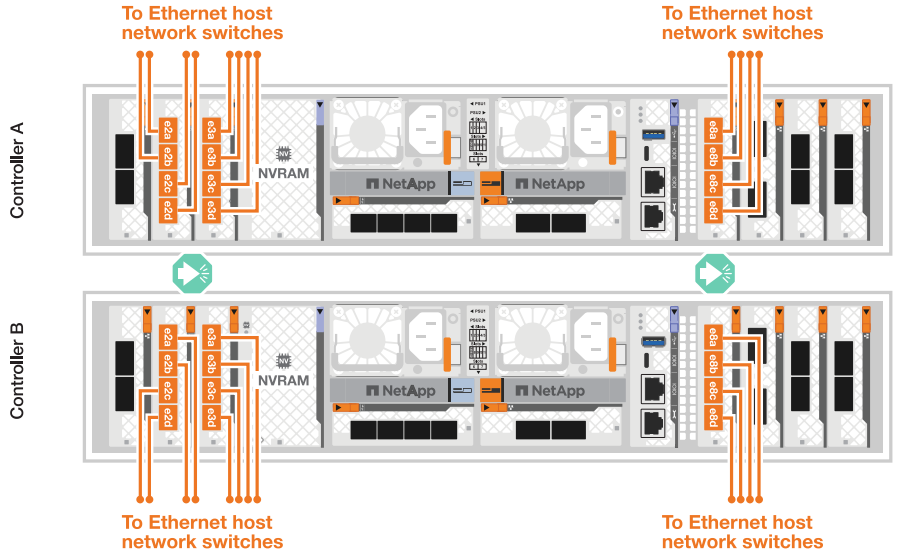
> Pour optimiser les performances du système pour le trafic de cluster et haute disponibilité, n'utilisez pas les ports e1b et e7b pour les connexions réseau hôte. Utilisez une carte hôte séparée pour optimiser les performances.

Câble 100 GbE



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

Hôte 10/25 GbE



A70 et A90

Connectez les ports du module Ethernet à votre réseau hôte.

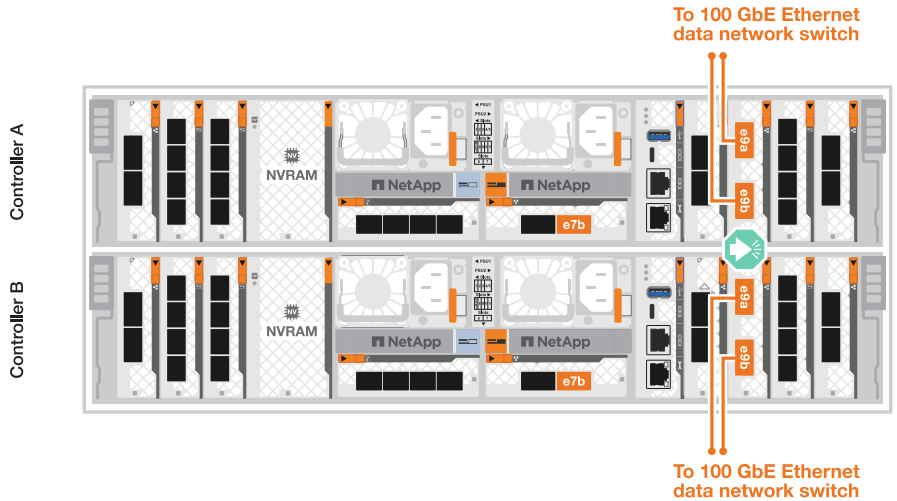
Voici quelques exemples types de câblage réseau hôte. Reportez-vous à la section "NetApp Hardware Universe" pour connaître la configuration spécifique de votre système.

Étapes

1. Connectez les ports e9a et e9b à votre commutateur de réseau de données Ethernet.

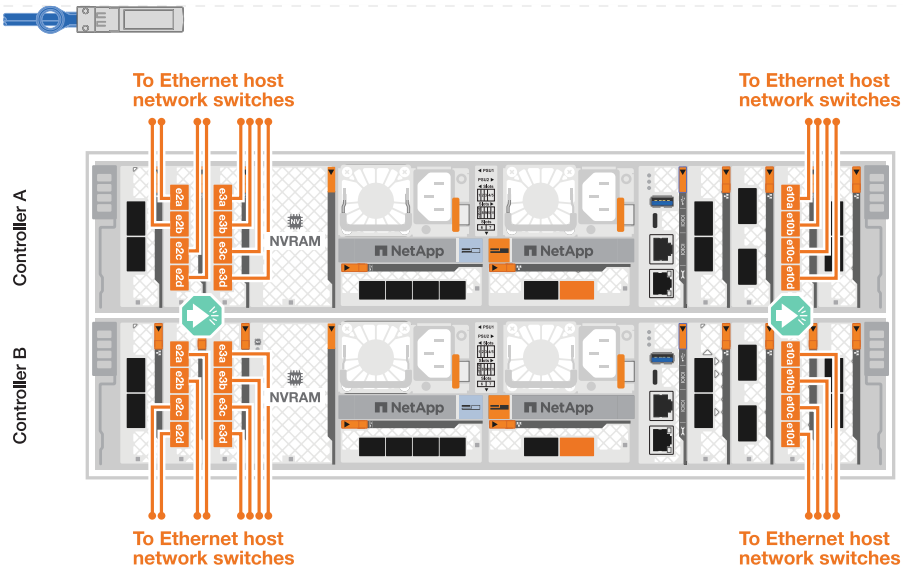
> Pour optimiser les performances du système pour le trafic de cluster et haute disponibilité, n'utilisez pas les ports e1b et e7b pour les connexions réseau hôte. Utilisez une carte hôte séparée pour optimiser les performances.

Câble 100 GbE



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

4 ports, hôte 10/25 GbE



A20, A30 ET A50

Connectez les ports de module Ethernet ou Fibre Channel (FC) à votre réseau hôte.

Les exemples de câblage du réseau hôte montrent des configurations courantes.

Si vous ne voyez pas votre configuration ici, accédez à "NetApp Hardware Universe" pour obtenir des informations complètes sur la configuration et la priorité des emplacements pour câbler votre système de stockage.

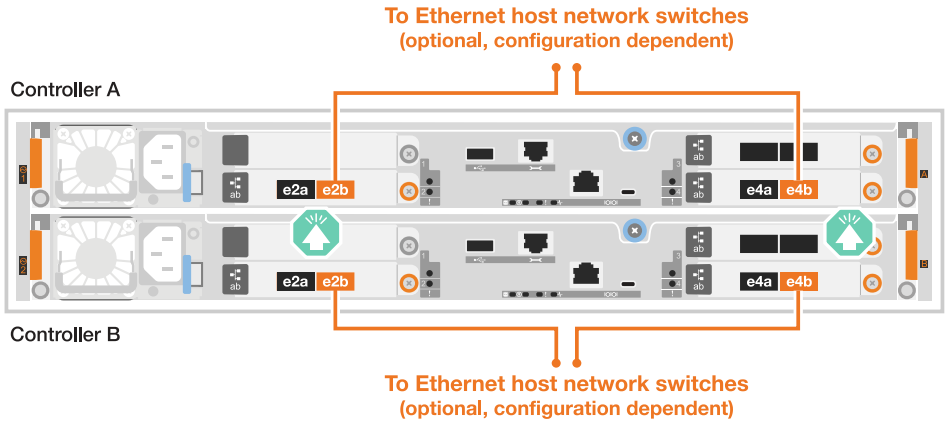
Câblage hôte Ethernet

ASA A30 et ASA A50 avec deux modules d'E/S 40/100 GbE à 2 ports

Sur chaque contrôleur, connectez les ports e2b et e4b aux commutateurs réseau hôte Ethernet.

> Les ports des modules d'E/S des connecteurs 2 et 4 sont 40/100 GbE (connectivité hôte 40/100 GbE).

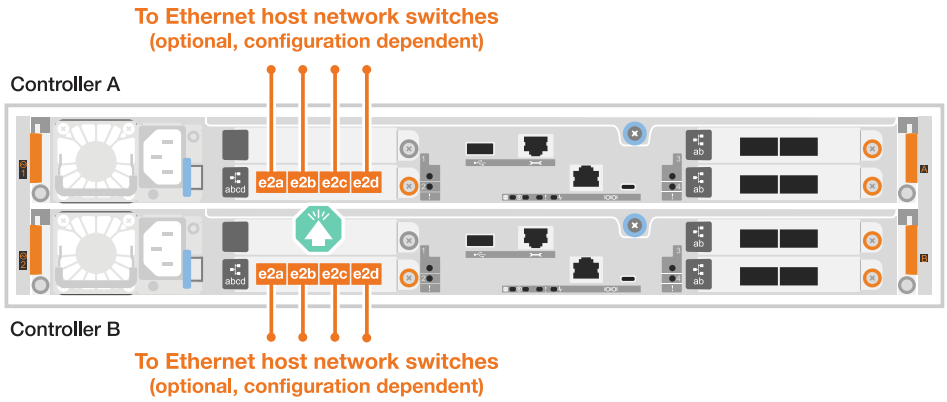
Câbles 40/100 GbE



ASA A20, A30 et A50 avec un module d'E/S 10/25 GbE à 4 ports

Sur chaque contrôleur, connectez les ports e2a, e2b, e2c et e2d aux commutateurs de réseau hôte Ethernet.

Câbles 10/25 GbE

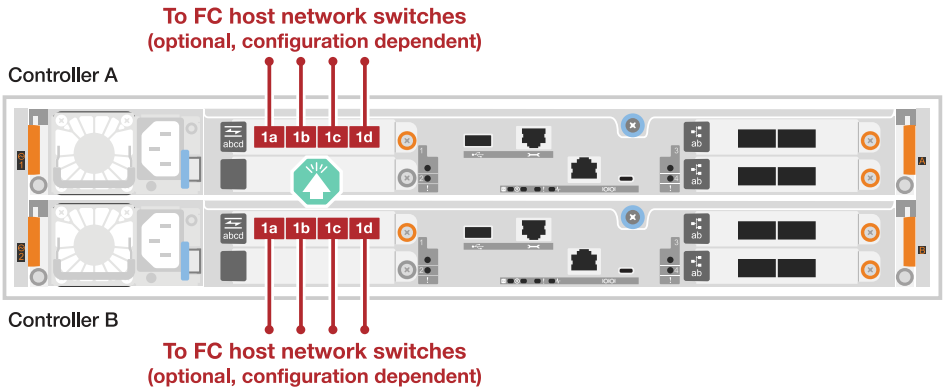


Câblage hôte FC

ASA A20, A30 et A50 avec un module d'E/S FC 64 Gb/s à 4 ports

Sur chaque contrôleur, connectez les ports 1a, 1b, 1c et 1D aux commutateurs réseau hôte FC.

Câbles FC 64 Gbit/s



Connectez les ports de module Ethernet ou Fibre Channel (FC) à votre réseau hôte.

Les exemples de câblage du réseau hôte montrent des configurations courantes.

Si vous ne voyez pas votre configuration ici, accédez à "NetApp Hardware Universe" pour obtenir des informations complètes sur la configuration et la priorité des emplacements pour câbler votre système de stockage.

Câblage hôte Ethernet

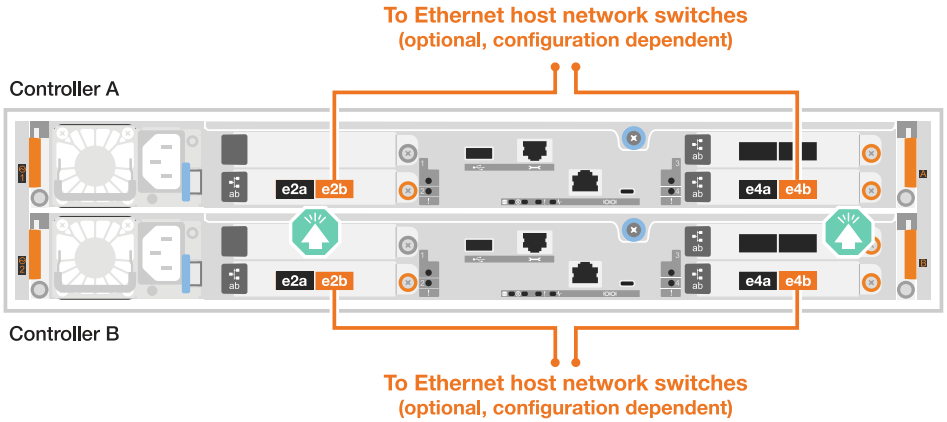
ASA C30 avec deux modules d'E/S 40/100 GbE à 2 ports

Étapes

1. Sur chaque contrôleur, reliez les ports e2b et e4b aux commutateurs réseau hôte Ethernet.

> Les ports des modules d'E/S des connecteurs 2 et 4 sont 40/100 GbE (connectivité hôte 40/100 GbE).

Câbles 40/100 GbE

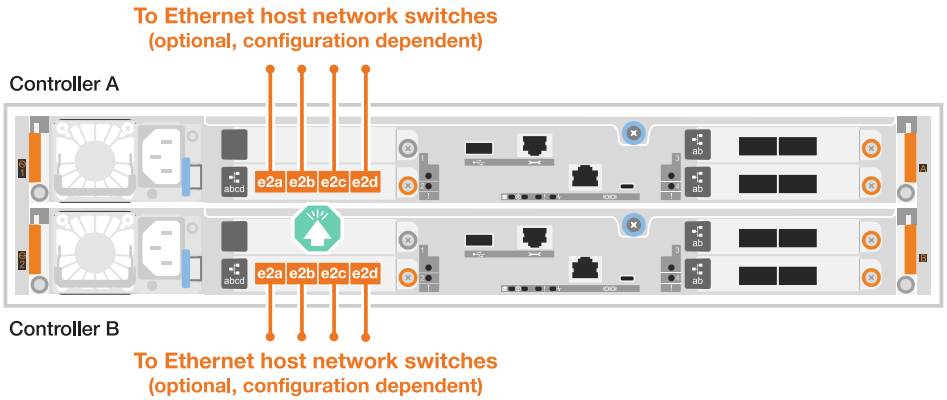


ASA C30 avec un module d'E/S 10/25 GbE à 4 ports

Étapes

1. Sur chaque contrôleur, reliez les ports e2a, e2b, e2c et e2d aux commutateurs de réseau hôte Ethernet.

   Câbles 10/25 GbE

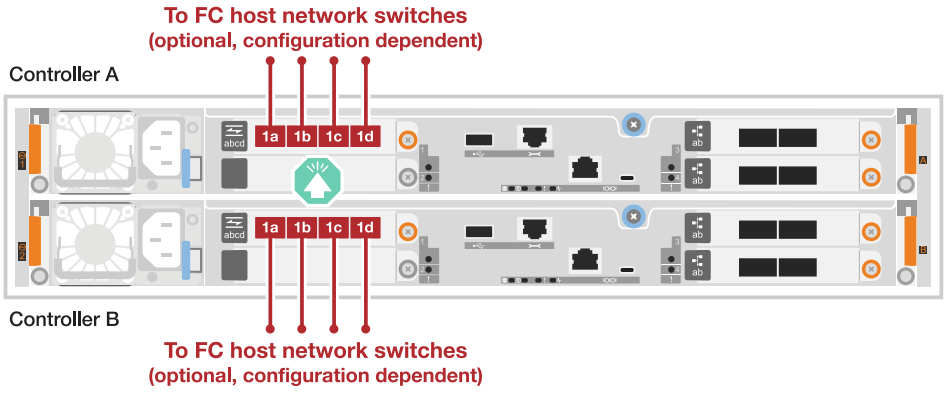


ASA C30 avec un module d'E/S FC 64 Gb/s à 4 ports

Étapes

1. Sur chaque contrôleur, reliez les ports 1a, 1b, 1c et 1D aux commutateurs réseau hôte FC.

   Câbles FC 64 Gbit/s



Étape 3 : branchement des câbles du réseau de gestion

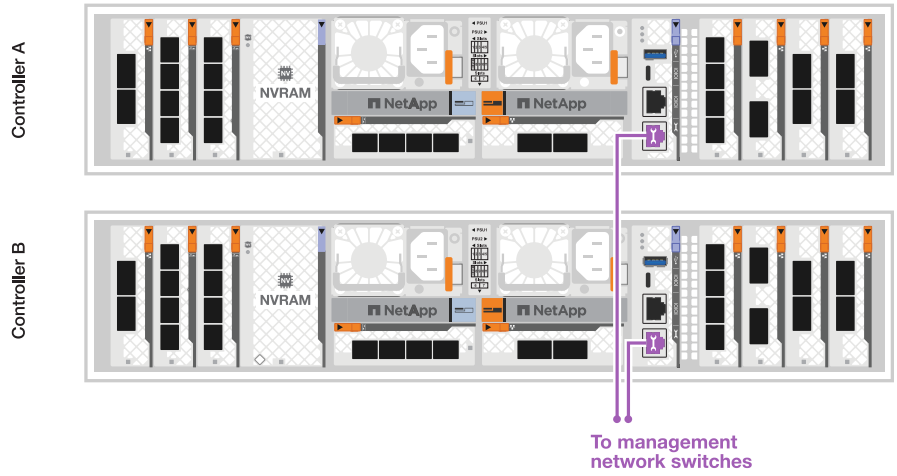
Connectez les contrôleurs à votre réseau de gestion.

Pour plus d’informations sur la connexion du système de stockage aux commutateurs du réseau de gestion, contactez votre administrateur réseau.

A1K

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

CÂBLES 1000BASE-T RJ-45

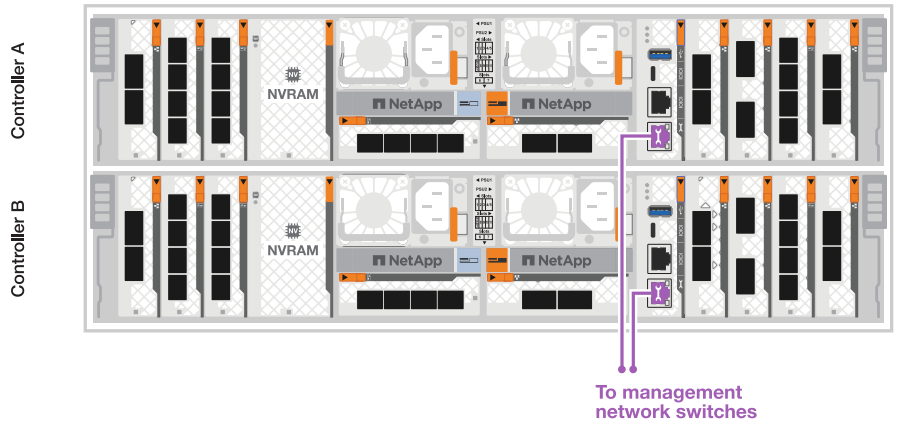


Ne branchez pas encore les cordons d'alimentation.

A70 et A90

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

CÂBLES 1000BASE-T RJ-45

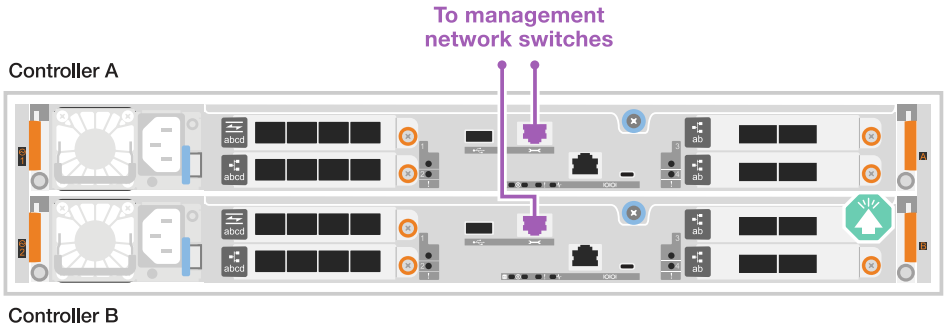


Ne branchez pas encore les cordons d'alimentation.

A20, A30 ET A50

Connectez les ports de gestion (clé anglaise) de chaque contrôleur aux switchs réseau de gestion.

CÂBLES 1000BASE-T RJ-45

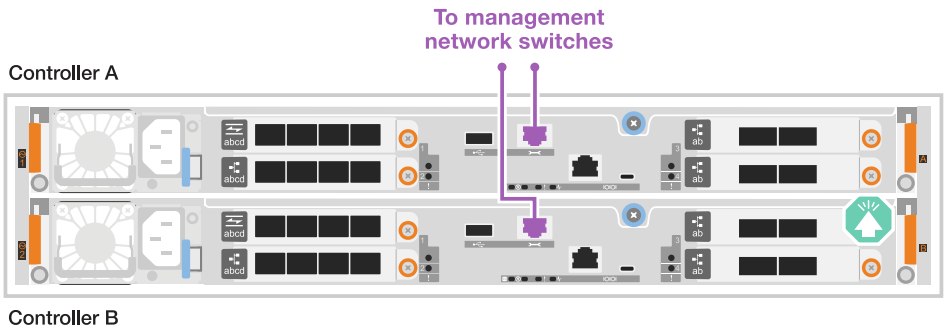


Ne branchez pas encore les cordons d'alimentation.

C30

Connectez les ports de gestion (clé anglaise) de chaque contrôleur aux switchs réseau de gestion.

CÂBLES 1000BASE-T RJ-45



Ne branchez pas encore les cordons d'alimentation.

Étape 4 : branchement des tiroirs sur le câble

Les procédures de câblage suivantes indiquent comment connecter les contrôleurs à un tiroir de stockage.

Pour connaître le nombre maximum de tiroirs pris en charge par votre système de stockage et pour toutes vos options de câblage, telles que les options optiques et connectées par commutateur, reportez-vous à "NetApp Hardware Universe"la section .

A1K

Les systèmes de stockage AFF A1K prennent en charge les étagères NS224 avec le module NSM100 ou NSM100B. Les principales différences entre les modules sont les suivantes :

- Les modules d'étagère NSM100 utilisent les ports intégrés e0a et e0b.
- Les modules d'étagère NSM100B utilisent les ports e1a et e1b dans l'emplacement 1.

L'exemple de câblage suivant montre les modules NSM100 dans les étagères NS224 en faisant référence aux ports des modules d'étagère.

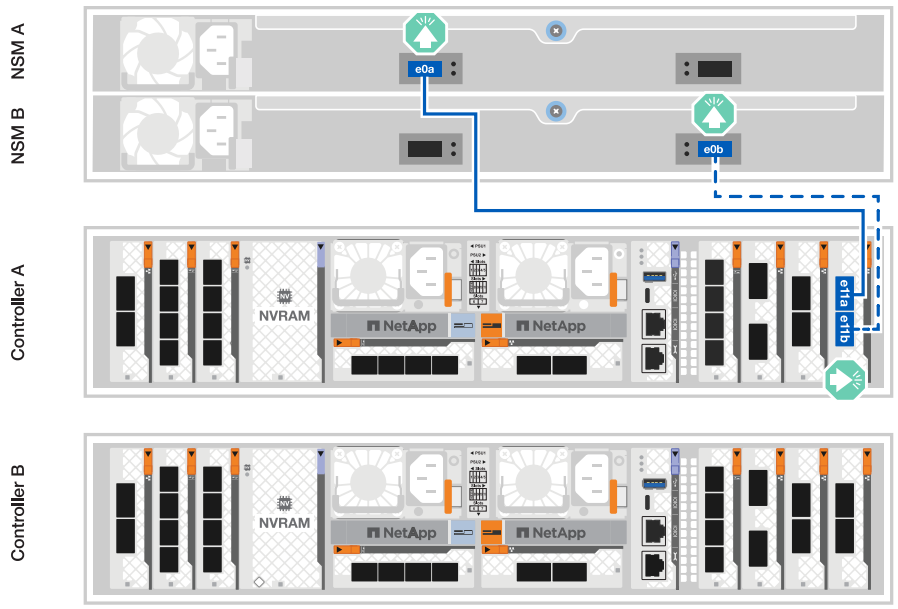
Choisissez l'une des options de câblage suivantes correspondant à votre configuration.

Option 1 : un tiroir de stockage NS224

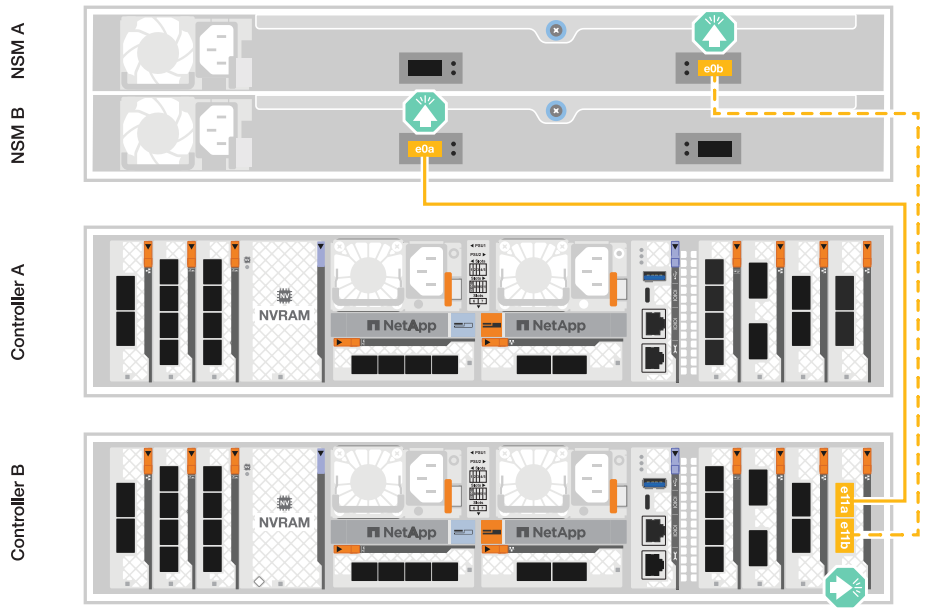
Connectez chaque contrôleur aux modules NSM du tiroir NS224. Les graphiques présentent le câblage depuis chaque contrôleur : le câblage du contrôleur A est représenté en bleu et le câblage du contrôleur B en jaune.

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.

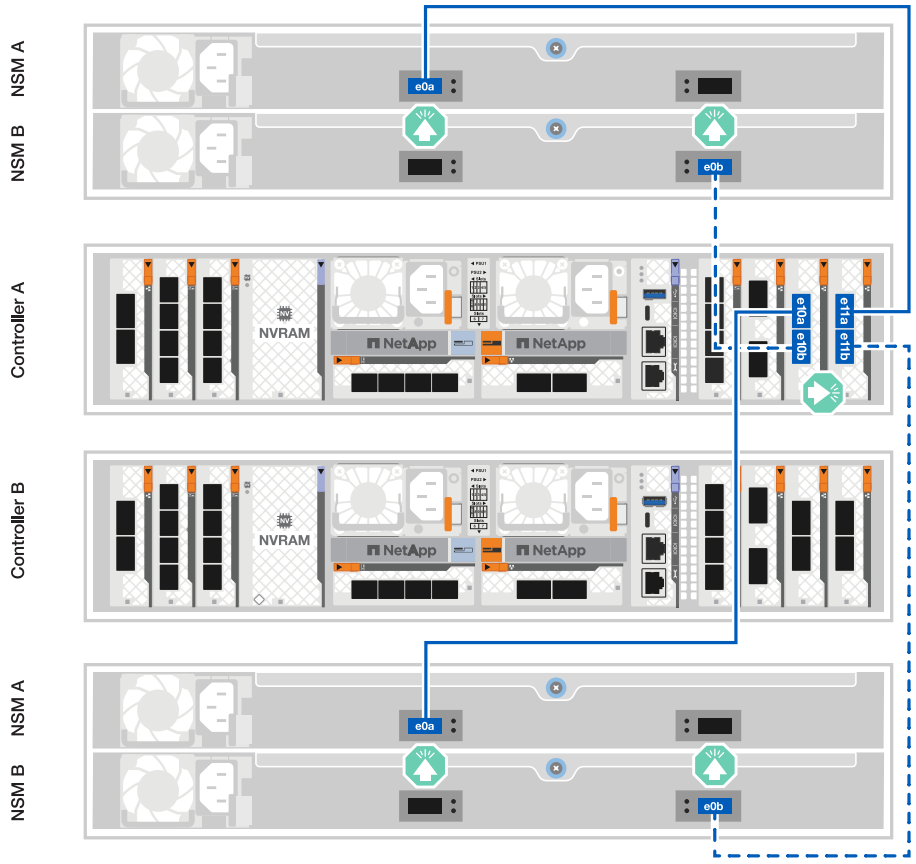


Option 2 : deux tiroirs de stockage NS224

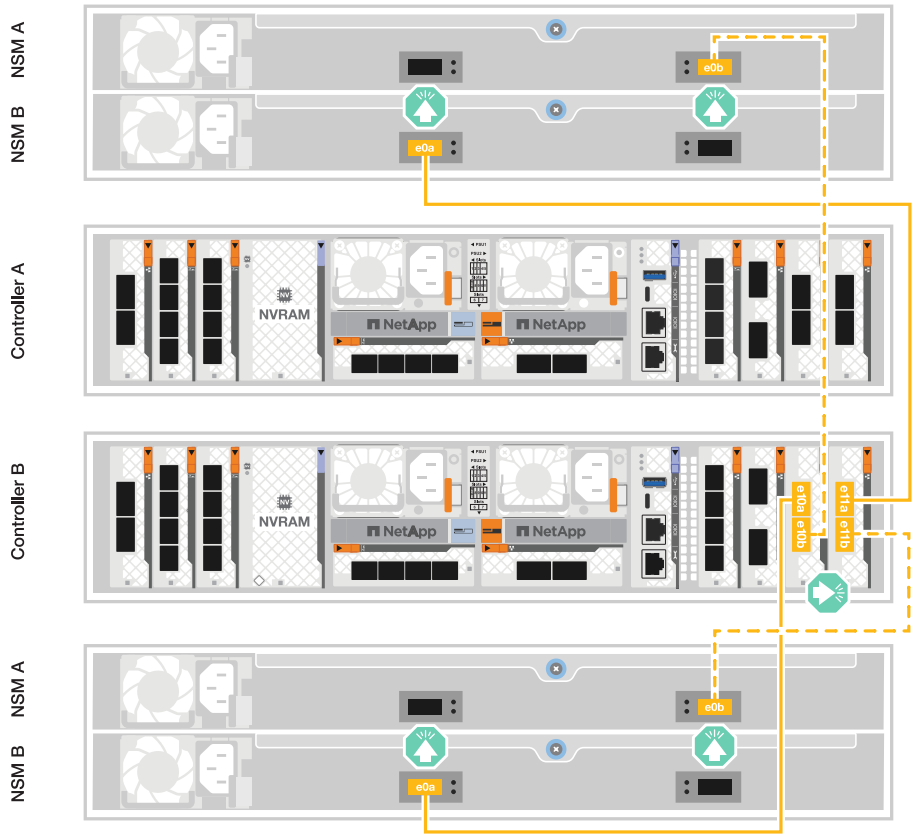
Connectez chaque contrôleur aux modules NSM des deux tiroirs NS224. Les graphiques présentent le câblage depuis chaque contrôleur : le câblage du contrôleur A est représenté en bleu et le câblage du contrôleur B en jaune.

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.



A70 et A90

Les systèmes de stockage AFF A70 et 90 prennent en charge les étagères NS224 avec le module NSM100 ou NSM100B. Les principales différences entre les modules sont les suivantes :

- Les modules d'étagère NSM100 utilisent les ports intégrés e0a et e0b.
- Les modules d'étagère NSM100B utilisent les ports e1a et e1b dans l'emplacement 1.

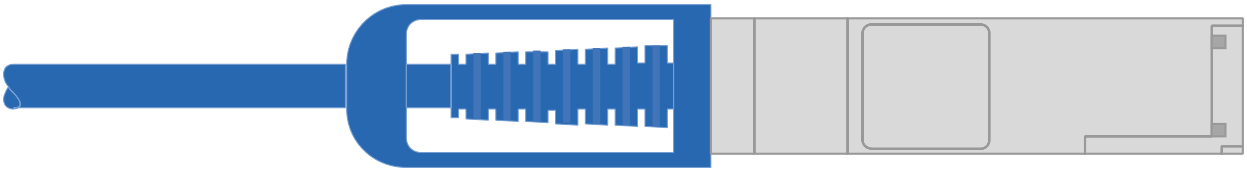
L'exemple de câblage suivant montre les modules NSM100 dans les étagères NS224 en faisant référence aux ports des modules d'étagère.

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

Option 1 : un tiroir de stockage NS224

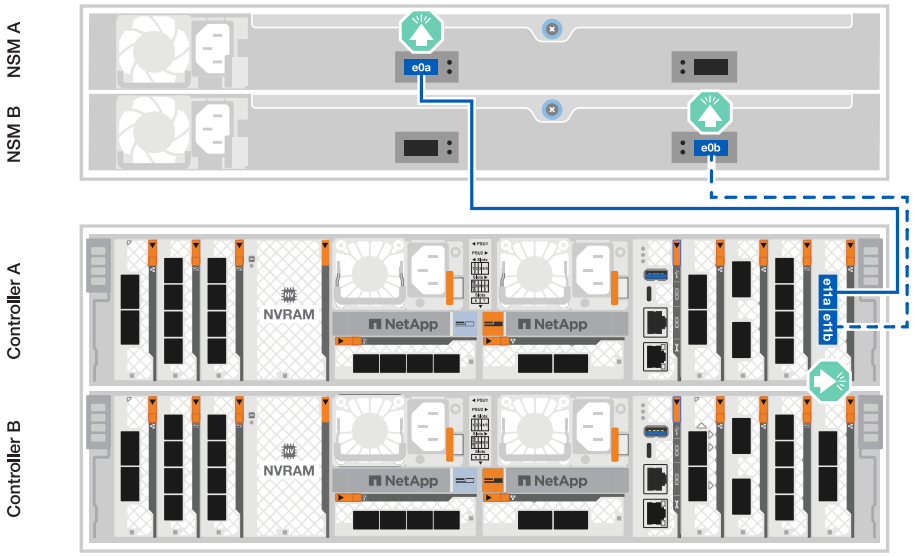
Connectez chaque contrôleur aux modules NSM du tiroir NS224. Les graphiques présentent le câblage depuis chaque contrôleur : le câblage du contrôleur A est représenté en bleu et le câblage du contrôleur B en jaune.

Câbles en cuivre QSFP28 100 GbE

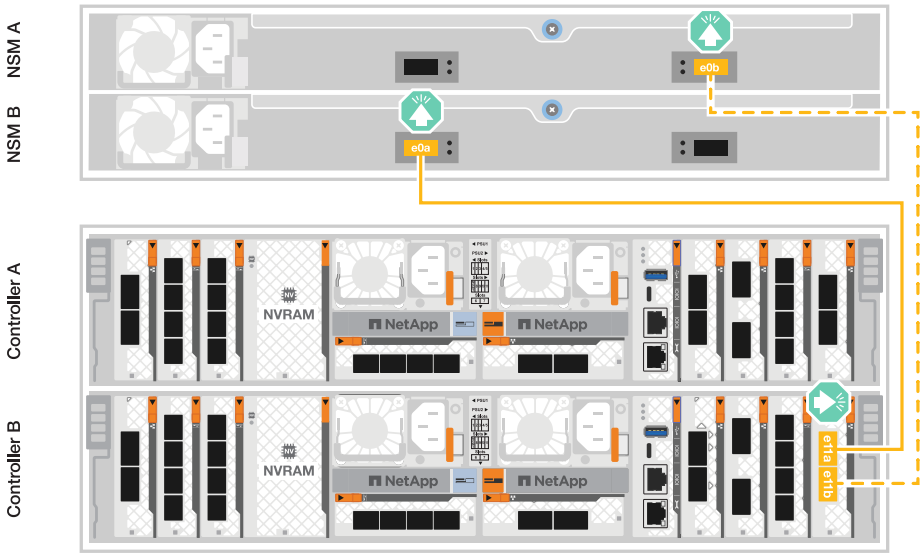


Étapes

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.



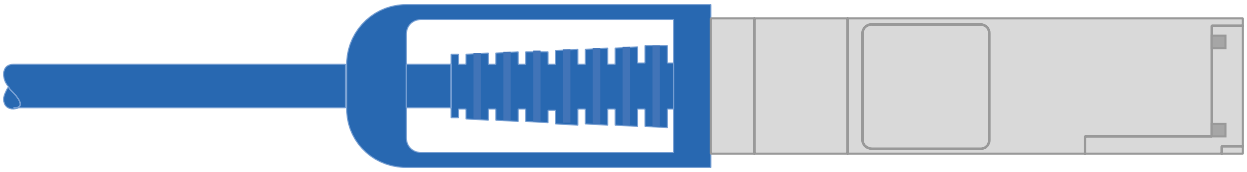
3. Connectez le port e11a du contrôleur B au port e0a du NSM B.
4. Connectez le port e11b du contrôleur B au port e0b de la carte NSM A.


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

Option 2 : deux tiroirs de stockage NS224

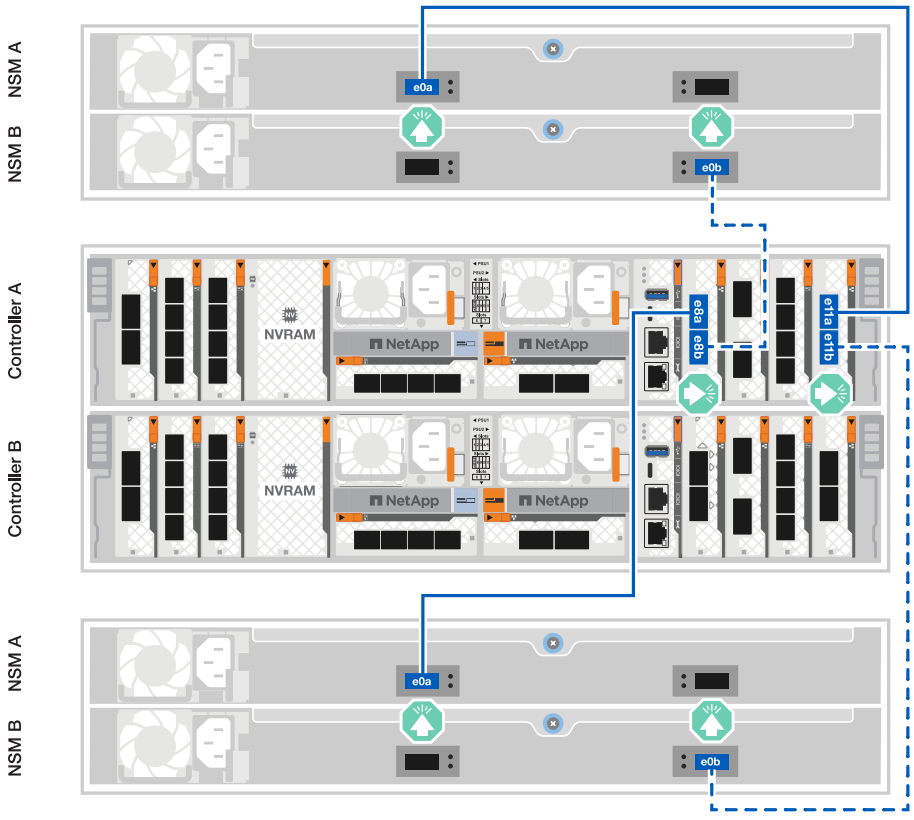
Connectez chaque contrôleur aux modules NSM des deux tiroirs NS224. Les graphiques présentent le câblage depuis chaque contrôleur : le câblage du contrôleur A est représenté en bleu et le câblage du contrôleur B en jaune.

Câbles en cuivre QSFP28 100 GbE



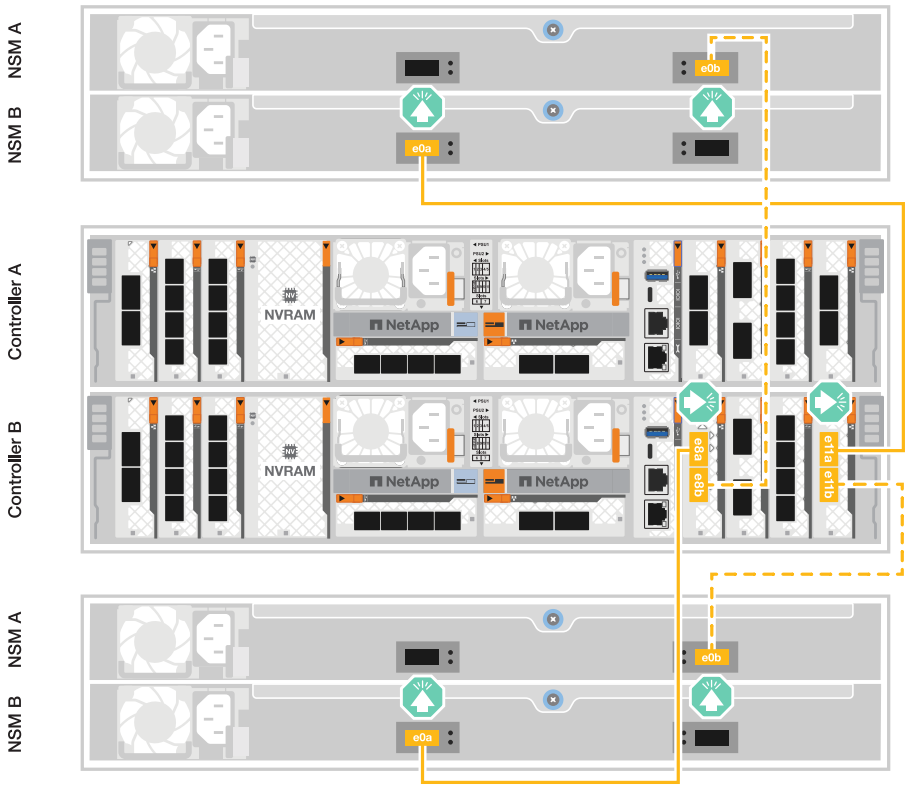
Étapes

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.



A20, A30 ET A50

La procédure de câblage du plateau NS224 utilise des modules NSM100B au lieu de modules NSM100. Le câblage est identique quel que soit le type de modules NSM utilisé ; seuls les noms de ports diffèrent :

- Les modules NSM100B utilisent les ports e1a et e1b sur un module d'E/S dans l'emplacement 1.
- Les modules NSM100 utilisent les ports intégrés (à bord) e0a et e0b.

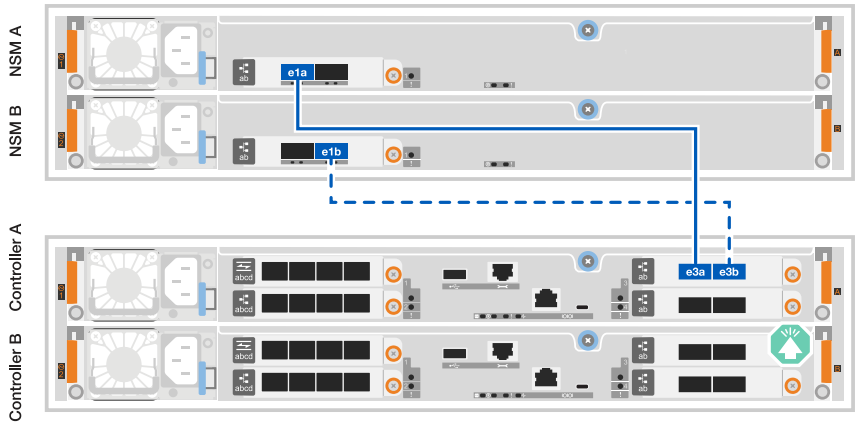
Vous câblez chaque contrôleur à chaque module NSM sur l'étagère NS224 à l'aide des câbles de stockage fournis avec votre système de stockage, qui peuvent être du type de câble suivant :

Câbles en cuivre QSFP28 100 GbE

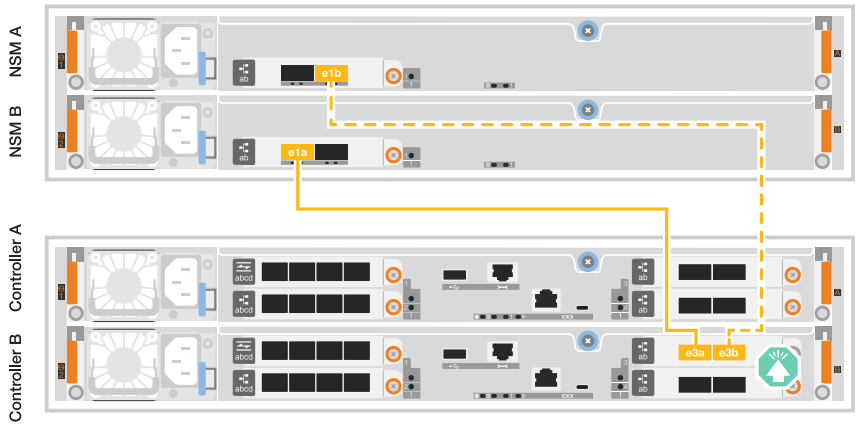
Les graphiques présentent le câblage du contrôleur A en bleu et le câblage du contrôleur B en jaune.

Étapes

1. Brancher le contrôleur A sur le tiroir :
   a. Connectez le port e3a du contrôleur A au port e1a du NSM A.
   b. Connectez le port e3b du contrôleur A au port NSM B e1b.



2. Connectez le contrôleur B au tiroir :
   a. Connectez le port e3a du contrôleur B au port e1a du NSM B.
   b. Connectez le port e3b du contrôleur B au port e1b de la carte NSM A.



C30

La procédure de câblage du plateau NS224 utilise des modules NSM100B au lieu de modules NSM100. Le câblage est identique quel que soit le type de modules NSM utilisé ; seuls les noms de ports diffèrent :

- Les modules NSM100B utilisent les ports e1a et e1b sur un module d'E/S dans l'emplacement 1.
- Les modules NSM100 utilisent les ports intégrés (à bord) e0a et e0b.

Vous câblez chaque contrôleur à chaque module NSM sur l'étagère NS224 à l'aide des câbles de stockage fournis avec votre système de stockage, qui peuvent être du type de câble suivant :

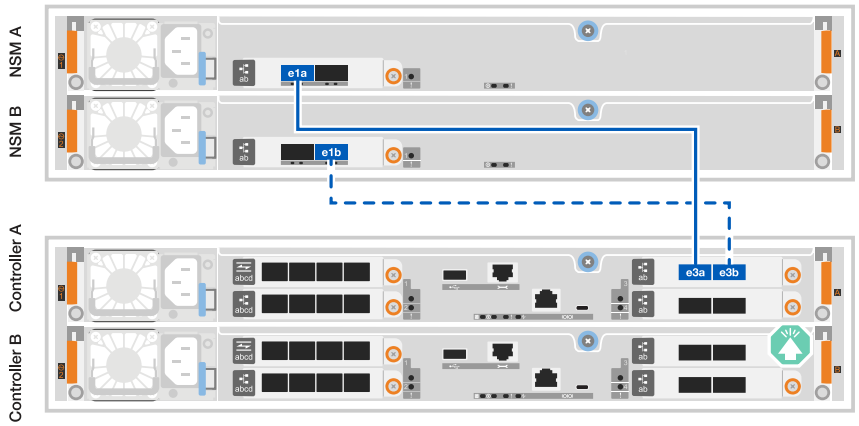
Câbles en cuivre QSFP28 100 GbE

Les graphiques présentent le câblage du contrôleur A en bleu et le câblage du contrôleur B en jaune.

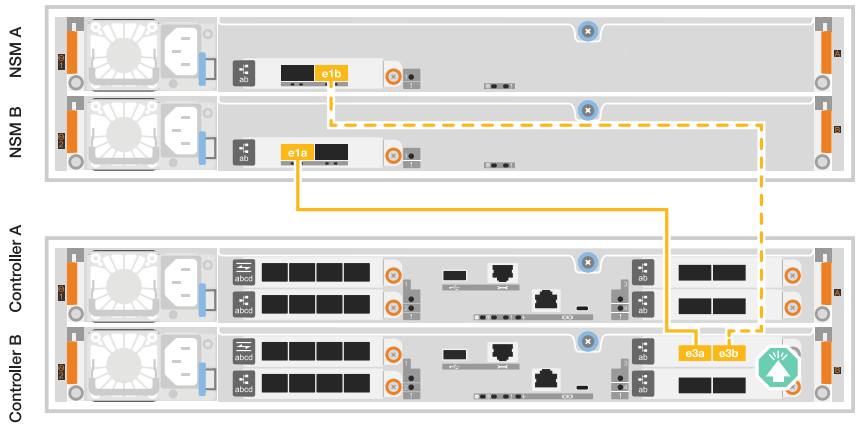
Étapes

1. Brancher le contrôleur A sur le tiroir :
   a. Connectez le port e3a du contrôleur A au port e1a du NSM A.

b. Connectez le port e3b du contrôleur A au port NSM B e1b.



2. Connectez le contrôleur B au tiroir :
   a. Connectez le port e3a du contrôleur B au port e1a du NSM B.
   b. Connectez le port e3b du contrôleur B au port e1b de la carte 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 se distingue par un ID de tiroir unique. Cet ID garantit que le tiroir est distinct dans la configuration de votre système de stockage.

Description de la tâche

- Remarque : pour être valides, les ID de tiroir sont compris entre 01 et 99.

  Si vous disposez de tiroirs internes (de stockage) intégrés aux contrôleurs, l'ID de tiroir fixe est 00.

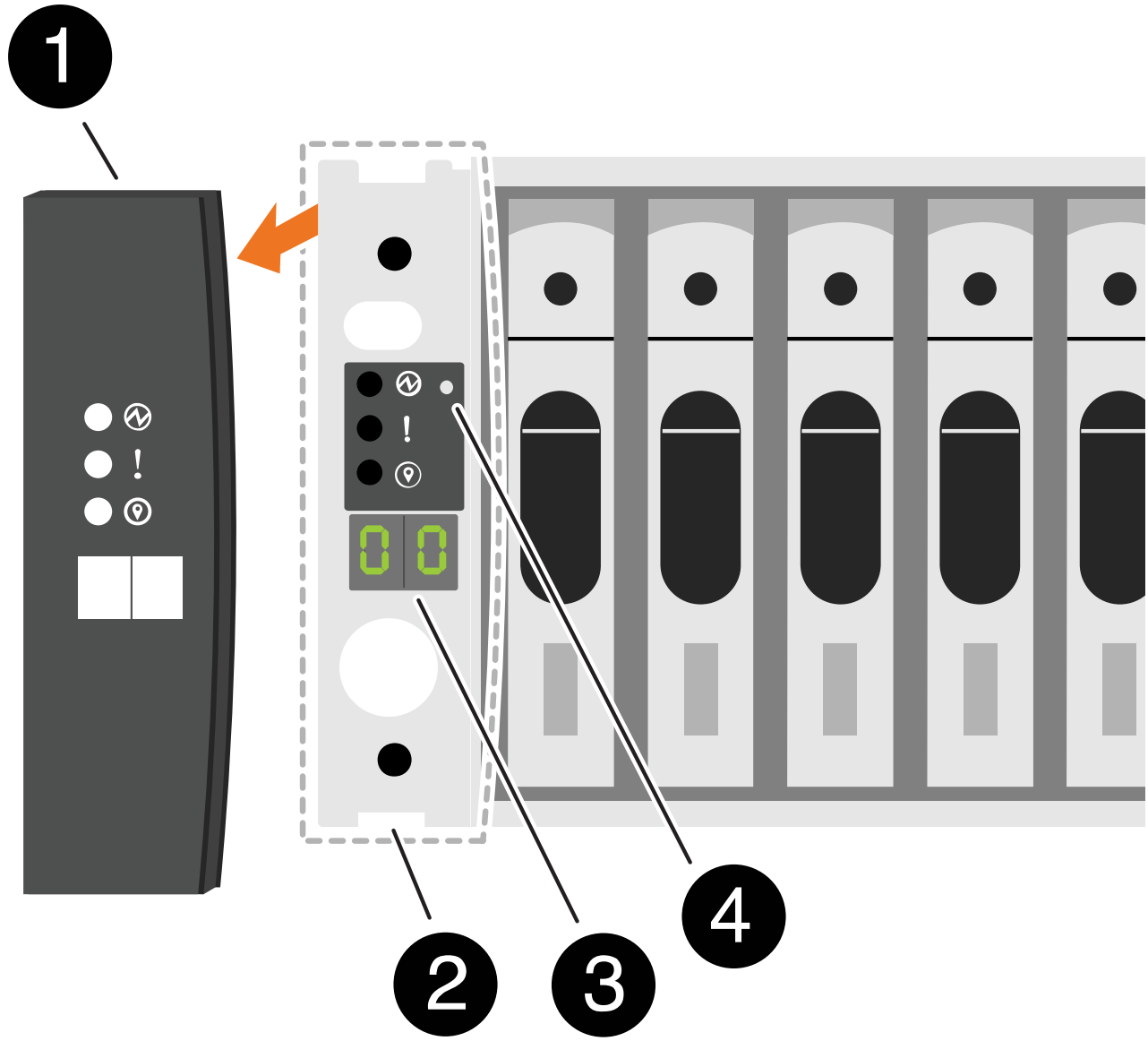
- Vous devez mettre un tiroir hors tension puis sous tension (débranchez les deux cordons d'alimentation, attendez la durée appropriée, puis rebranchez-les) pour que l'ID de tiroir prenne effet.

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.

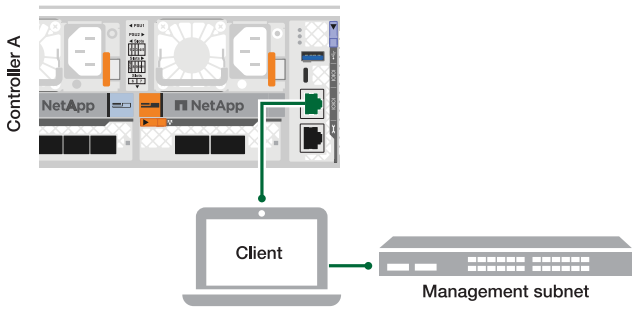
Étapes

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.

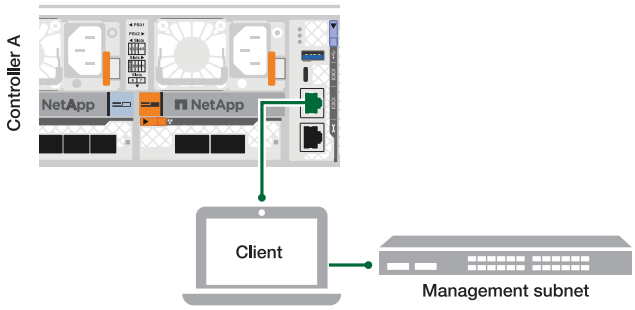
      Consultez l’aide en ligne de votre ordinateur portable pour obtenir des instructions sur la configuration du port série console.

   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.

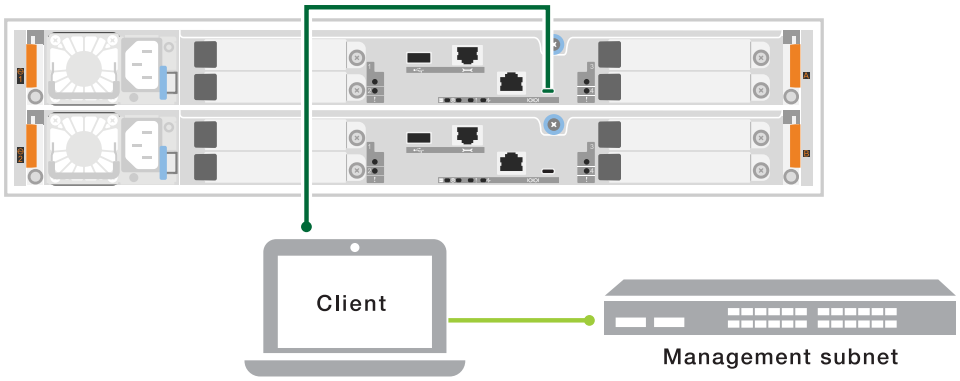
A1K



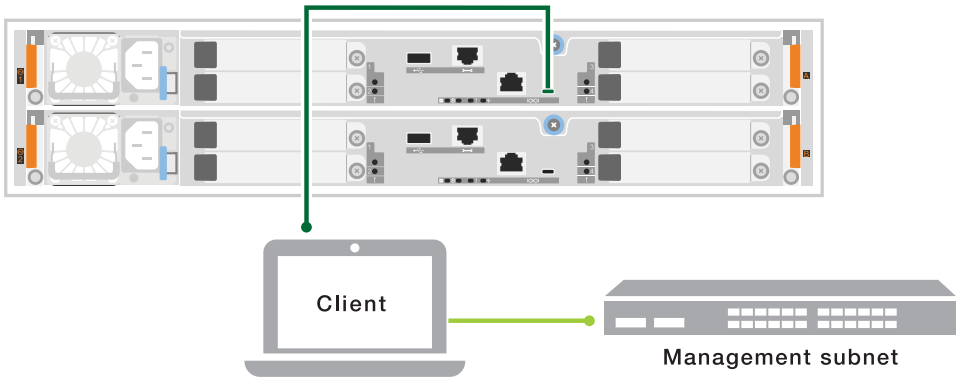
A70 et A90



A20, A30 ET A50



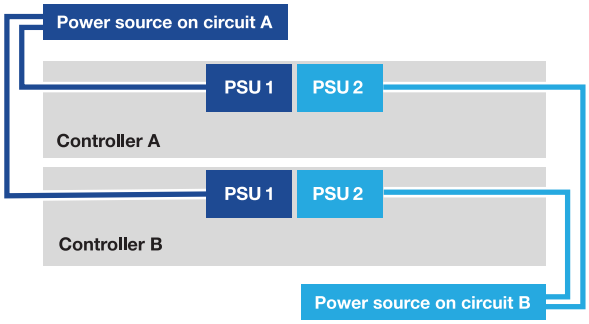
C30



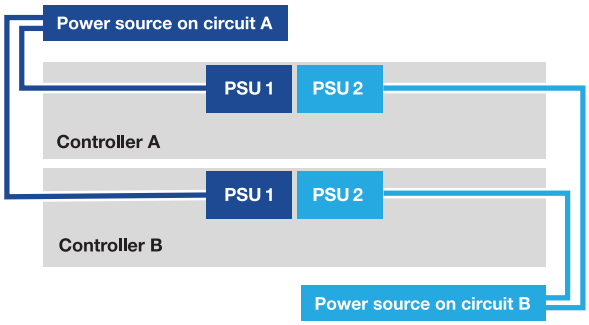
2. Attribuez une adresse TCP/IP à l'ordinateur portable, en utilisant une adresse située sur le sous-réseau de gestion.

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

A1K



A70 et A90



A20, A30 ET A50

C30

   - Le système lance le processus de démarrage. La séquence de démarrage initiale peut prendre jusqu'à huit minutes.
   - Pendant le processus de démarrage, vous verrez les voyants clignoter et les ventilateurs s'activer, indiquant que les contrôleurs sont en cours de mise sous tension.
   - N'oubliez pas que les ventilateurs peuvent émettre un niveau de bruit élevé lors de leur premier démarrage. Le bruit du ventilateur au démarrage est normal.
   - Pour les systèmes de stockage ASA A20, A30, A50 et ASA C30, l'affichage de l'ID d'étagère à l'avant du châssis du système ne s'allume pas.
4. Fixez les cordons 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.

Dans certains cas, vous pourriez avoir besoin de "Utilisez l'interface de ligne de commande (CLI) ONTAP pour configurer votre cluster.". Vous devriez utiliser l'interface de ligne de commande (CLI), par exemple, si vos protocoles de sécurité ne vous permettent pas de connecter un ordinateur portable à vos commutateurs de gestion, ou si vous utilisez un système d'exploitation autre que Windows.

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. Découverte de votre réseau de clusters
   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.

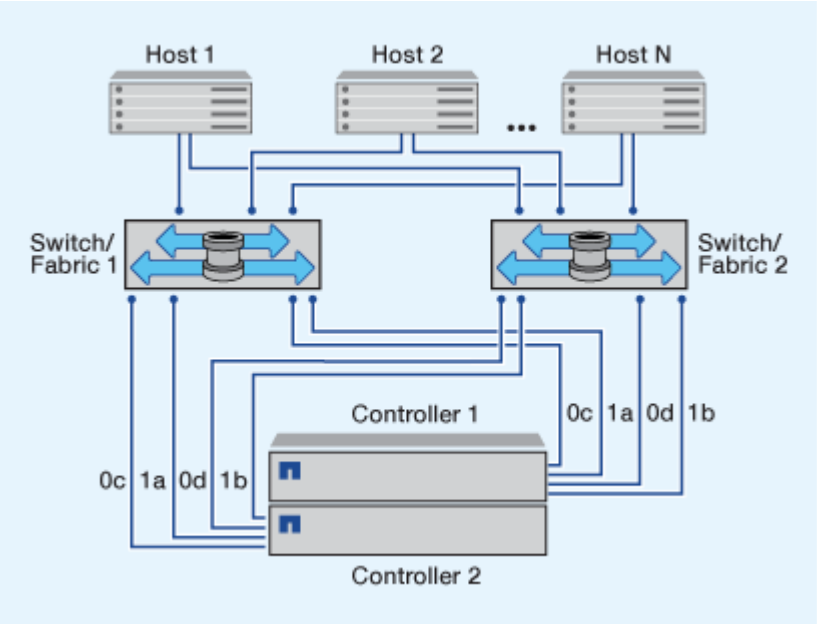
Configuration d’hôtes SAN avec les systèmes ASA r2

Les systèmes ASA r2 suivent les mêmes recommandations et instructions pour la configuration des hôtes SAN que tous les autres systèmes ONTAP.

Il est recommandé d’utiliser au moins deux commutateurs pour connecter votre système de stockage à un ou plusieurs hôtes SAN. Pour les configurations iSCSI, la topologie réseau reliant vos hôtes, commutateurs et systèmes de stockage est appelée *network*. Pour les configurations FC et FC-NVMe, cette même topologie réseau est appelée *fabric*.

Les configurations multiréseau et multistructure (qui utilisent au moins deux commutateurs) sont recommandées, car elles assurent la redondance au niveau des couches de switch et de stockage. Cette redondance rend votre système de stockage plus tolérant aux pannes et assure la continuité de l’activité.

L’illustration suivante est un exemple de configuration FC avec plusieurs hôtes utilisant deux fabrics pour accéder à une seule paire HA. Les numéros de port cible FC (0c, 0d, 1a, 1b) sont également des exemples. Les numéros de port réels varient en fonction du modèle de votre système et de l’utilisation ou non d’adaptateurs d’extension.



En savoir plus sur "Configuration SAN pour hôtes iSCSI". En savoir plus sur "Configuration SAN pour les hôtes FC et FC/NVMe".

Recommandation de segmentation pour les hôtes FC

Vous devez configurer vos hôtes FC pour qu’ils utilisent la segmentation. Les systèmes ASA r2 suivent les mêmes recommandations et instructions de segmentation des hôtes FC que tous les autres systèmes ONTAP.

Une zone est un regroupement logique d’un ou de plusieurs ports au sein d’une structure. Pour que les périphériques puissent se découvrir, établir des sessions entre eux et communiquer, les deux ports doivent avoir une appartenance à une zone commune.

En savoir plus sur "Segmentation FC/FC-NVMe".

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 critiques de votre client SAN pour un fonctionnement correct avec ONTAP sont configurés correctement. Si vous fournissez du stockage à votre environnement VMware, vous devez installer OTV 10.3 pour simplifier la gestion de votre stockage ASA r2.

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’utiliser"VMware vSphere vMotion" pour effectuer une migration en direct et sans interruption de vos données.

Les unités de stockage ASA r2 sont provisionnées dynamiquement par défaut. Lors de la migration de votre charge de travail VM, les disques virtuels (VMDK) doivent également être provisionnés de manière fine.

Informations associées

- En savoir plus sur "les avantages de l’utilisation ONTAP pour vSphere" .
- En savoir plus sur"Récupération de site VMware Live avec ONTAP" .
- En savoir plus sur"solutions de disponibilité continue pour les environnements vSphere" .
- En savoir plus sur"Comment configurer Broadcom VMware ESXi iSCSI MPIO avec les systèmes de stockage ONTAP SAN ASA" .

Migrer des données à partir d’un système de stockage tiers

À partir d' ONTAP 9.17.1, vous pouvez utiliser l’importation de LUN étrangers (FLI) pour migrer des données d’un LUN d’un système de stockage tiers vers un système ASA r2. L’utilisation de FLI pour la migration de vos données peut vous aider à réduire les risques de perte de données et d’interruption de service pendant le processus de migration.

FLI prend en charge les migrations en ligne et hors ligne. Lors d’une migration en ligne, le système client reste en ligne pendant la copie des données du système de stockage tiers vers le système de stockage ONTAP . Les migrations en ligne sont prises en charge par les systèmes d’exploitation hôtes Windows, Linux et ESXi. Lors d’une migration hors ligne, le système client est mis hors ligne, les données LUN sont copiées du système de stockage tiers vers le système de stockage ONTAP , puis le système client est remis en ligne.

- Apprenez à effectuer une "Migration hors ligne FLI" .
- Apprenez à effectuer une "Migrations en ligne FLI" .

Configurez votre système ASA r2 en tant que fournisseur de stockage dans votre environnement VMware

Vous pouvez utiliser les outils ONTAP pour VMware afin de mettre en place votre système ASA r2 en tant que fournisseur de stockage dans votre environnement VMware.

Les outils ONTAP pour VMware vSphere sont un ensemble d'outils compatibles avec VMware vCenter Server Virtual Appliance (vCSA) pour une gestion simplifiée des machines virtuelles sur vos hôtes VMware ESXi.

Les systèmes ASA r2 sont pris en charge par "Outils ONTAP pour VMware vSphere 10.3" et les versions ultérieures.

Découvrez comment "Déployez les outils ONTAP pour VMware"puis utilisez-le pour :

- "Ajouter des instances vCenter Server"
- "Configurez les paramètres de l'hôte ESXi"
- "Découvrez votre système de stockage et vos hôtes ASA r2"

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 de l'espace de stockage à la disposition de vos hôtes SAN pour les opérations de données. Une unité de stockage désigne un LUN pour les hôtes SCSI ou un espace de noms NVMe pour les hôtes NVMe. Si votre cluster est configuré pour prendre en charge les hôtes SCSI, vous serez invité à créer un LUN. Si votre cluster est configuré pour prendre en charge les hôtes NVMe, vous serez invité à créer un espace de noms NVMe.

Une unité de stockage ASA r2 a une capacité maximale de 128 To. Voir le"NetApp Hardware Universe" pour connaître les limites de stockage les plus récentes pour les systèmes ASA r2.

Vous ajoutez et associez les initiateurs hôtes à l'unité de stockage dans le cadre du processus de création de l'unité de stockage. Vous pouvez également"ajouter" et"carte" Les initiateurs hôtes après la création des unités de stockage.

À partir d' ONTAP 9.18.1, vous pouvez modifier la réserve de snapshots et activer la suppression automatique des snapshots lors de la création d'une unité de stockage. La réserve de snapshots correspond à l'espace de l'unité de stockage réservé spécifiquement aux snapshots. Lorsque la réserve d'instantanés est configurée avec la suppression automatique des instantanés, les instantanés les plus anciens sont automatiquement supprimés lorsque l'espace utilisé par les instantanés dépasse la réserve d'instantanés.

"Découvrez plus d'informations sur la réserve de snapshots sur les systèmes ASA r2".

Les unités de stockage sont provisionnées dynamiquement par défaut. Le provisionnement fin permet à l'unité de stockage d'atteindre la taille allouée, mais ne réserve pas l'espace à l'avance. L'espace est alloué dynamiquement en fonction des besoins, à partir de l'espace libre disponible. Cela vous permet d'obtenir une plus grande efficacité de stockage en *surdimensionnant* votre espace disponible. Par exemple, supposons que vous disposiez de 1 To d'espace libre et que vous deviez créer quatre unités de stockage de 1 To. Au lieu d'ajouter immédiatement 3 To de capacité de stockage supplémentaire à votre système, vous pouvez créer les unités de stockage, surveiller l'utilisation de l'espace et augmenter votre capacité de stockage au fur et à mesure que les unités de stockage consomment de l'espace réel. En savoir plus sur"provisionnement fin" .

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.

   Pour optimiser l'équilibrage de la charge de travail dans la zone de disponibilité du stockage, créez un nombre pair d'unités de stockage.

4. Entrez la capacité de l'unité de stockage, puis sélectionnez le système d'exploitation hôte.

   Si vous créez plusieurs unités de stockage, chaque unité aura la même capacité. Multipliez le nombre d'unités de stockage que vous créez par la capacité souhaitée pour vous assurer de disposer d'un espace utilisable suffisant. Si vous ne disposez pas de suffisamment d'espace libre et que vous avez choisi de surdimensionner votre stockage, surveillez attentivement son utilisation afin d'éviter toute rupture d'espace et toute perte de données.

5. Acceptez le **mappage d'hôte** sélectionné automatiquement ou sélectionnez un autre groupe d'hôtes pour l'unité de stockage à mapper.

   Mappage d'hôte fait référence au groupe d'hôtes sur lequel 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'hôte. Vous pouvez accepter le groupe d'hôtes sélectionné automatiquement ou sélectionner un autre groupe d'hôtes.

   S'il n'existe pas de groupe d'hôtes préexistant pour les hôtes exécutés sur le système d'exploitation que vous avez spécifié, ONTAP crée automatiquement un nouveau groupe d'hôtes.

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.
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 de QoS, une garantie de 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**.
Modifiez le niveau de service de performances par défaut.	a. Sous **stockage et optimisation**, en regard du niveau de service **Performance**, sélectionnez . b. Sélectionnez **Performance**. Les systèmes ASA r2 offrent deux niveaux de performances. Le niveau de performance par défaut est **Extrême**, qui est le niveau le plus élevé disponible. Vous pouvez abaisser le niveau à **Performance**.
Modifiez la réserve de snapshots par défaut et activez la suppression automatique des snapshots.	a. Sous **% de réserve de snapshots**, saisissez la valeur numérique du pourcentage de l'espace de l'unité de stockage que vous souhaitez allouer aux snapshots. b. Sélectionnez **Supprimer automatiquement les anciens instantanés**.

Option	Étapes
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. Formatez le NQN de l'hôte comme <nqn.yyyy-mm> suivi d'un nom de domaine pleinement qualifié. L'année doit être égale ou postérieure à 1970. La longueur maximale totale doit être de 223. Un exemple d'initiateur NVMe valide est 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.

Mappez l'unité de stockage sur un hôte

Après avoir créé des unités de stockage ASA r2 et ajouté des initiateurs hôtes, associez les hôtes aux unités de stockage pour commencer à diffuser les données. Les unités de stockage sont associées à des hôtes dans le cadre du processus de création des unités de stockage. Vous pouvez également associer à tout moment des unités de stockage existantes à 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.

Séparer le clone du groupe de cohérence

Lorsque vous fractionnez un clone de groupe de cohérence, vous dissociez le clone du groupe de cohérence source et allouez de l'espace disque au clone. Le clone devient un groupe de cohérence autonome pouvant être utilisé indépendamment du groupe de cohérence source.

Étapes

1. Dans System Manager, sélectionnez **protection > groupes de cohérence**.
2. Placez le curseur de la souris sur le clone de groupe de cohérence à diviser.
3. Sélectionnez **Split clone**.
4. Sélectionnez **Fractionner**.

Résultat

Le clone est dissocié du groupe de cohérence source et l'espace disque est alloué au clone.

Gérer les groupes d'hôtes

Créez des groupes d'hôtes sur votre système ASA r2

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 désormais "mappez-le à une unité de stockage" .

Supprimer un groupe d'hôtes sur votre système ASA r2

Sur un système ASA r2, un groupe d'hôtes est le mécanisme permettant aux hôtes d'accéder aux unités de stockage. Un groupe d'hôtes fait référence à un igroup pour les hôtes SCSI ou à un sous-système NVMe pour les hôtes NVMe. Un hôte ne peut voir que les unités de stockage mappées aux groupes d'hôtes auxquels il appartient. Vous pouvez supprimer un groupe d'hôtes si vous ne souhaitez plus que les hôtes qui le composent aient accès aux unités de stockage mappées à ce groupe.

Étapes

1. Dans System Manager, sélectionnez **Storage**.
2. Sous **Mappage d'hôte**, sélectionnez le groupe d'hôtes que vous souhaitez supprimer.
3. Sélectionnez **Stockage mappé**.
4. Sélectionnez **Plus**, puis sélectionnez **Supprimer**.
5. Sélectionnez pour vérifier que vous souhaitez continuer, puis sélectionnez **Supprimer**.

Et la suite ?

Le groupe d'hôtes est supprimé. Les hôtes qui le composaient n'ont plus accès aux unités de stockage qui y étaient mappées.

Gérer les unités de stockage

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.

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

Si l'espace d'une zone de disponibilité du stockage est insuffisant, vous pouvez déplacer des unités de stockage vers une autre zone de disponibilité du stockage afin d'équilibrer l'utilisation du stockage dans le cluster.

Vous pouvez déplacer une unité de stockage pendant que celle-ci est en ligne et qu'elle assure l'accès aux données. L'opération de déplacement est sans interruption.

Avant de commencer

- Vous devez exécuter ONTAP 9.16.1 ou une version ultérieure.
- Votre cluster doit être composé d'au moins quatre nœuds.

Étapes

1. Dans System Manager, sélectionnez **Storage**, puis sélectionnez l'unité de stockage à déplacer.
2. Sélectionnez ⋮, puis **déplacer**.
3. Sélectionnez la zone de disponibilité de stockage vers laquelle vous souhaitez déplacer l'unité de stockage, puis sélectionnez **déplacer**.

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 que vous souhaitez supprimer se trouve dans un groupe de cohérence en relation de réplication, vous devez"retirez l'unité de stockage du groupe de cohérence" avant de le 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.

Migrer les machines virtuelles de stockage

Migrer une machine virtuelle de stockage d'un cluster ASA vers un cluster ASA r2

À partir d' ONTAP 9.18.1, vous pouvez migrer sans interruption une machine virtuelle de stockage (VM) de n'importe quel cluster ASA vers n'importe quel cluster ASA r2. La migration d'un cluster ASA vers un cluster ASA r2 vous permet d'adopter l'architecture simplifiée et rationalisée des systèmes ASA r2 pour les environnements SAN uniquement.

La migration des machines virtuelles de stockage entre les systèmes de stockage ASA et ASA r2 est prise en charge comme suit :

À partir de l'un des systèmes ASA suivants :	À l'un des systèmes ASA r2 suivants :
• ASA C800 • ASA C400 • ASA C250 • ASA A900 • ASA A800 • ASA A400 • ASA A250 • ASA A150 • ASA AFF A800 • ASA AFF A700 • ASA AFF A400 • ASA AFF A250 • ASA AFF A220	• ASA A1K • ASA C30 • ASA A90 • ASA A70 • ASA A50 • ASA A30 • ASA A20

Pour obtenir la liste la plus récente des systèmes ASA et ASA r2, consultez"NetApp Hardware Universe" . Les systèmes ASA r2 sont répertoriés dans NetApp Hardware Universe sous le nom de «ASA série A/série C (nouveau) ».

Vous pouvez migrer une machine virtuelle de stockage vers un cluster ASA r2 uniquement à partir d'un cluster ASA . La migration depuis tout autre type de système ONTAP n'est pas prise en charge.

Avant de commencer

Tous les nœuds du cluster ASA r2 et du cluster ASA doivent exécuter ONTAP 9.18.1 ou une version ultérieure. Les versions des correctifs ONTAP 9.18.1 sur les nœuds du cluster peuvent varier.

Étape 1 : Vérifier l'état de la machine virtuelle de stockage ASA

Avant de migrer une VM de stockage depuis un système ASA , aucun espace de noms NVMe ni vVols ne doit être présent et chaque volume de la VM de stockage ne doit contenir qu'un seul LUN. La migration des espaces de noms NVMe et des vVols n'est pas prise en charge. L'architecture des systèmes ASA r2 exige que les volumes contiennent un seul LUN.

Étapes

1. Vérifiez qu'aucun espace de noms NVMe n'est présent dans la machine virtuelle de stockage :

   ```
   vserver nvme namespace show -vserver <storage_VM>
   ```

   Si des entrées sont affichées, les objets NVMe doivent être"converti" aux LUN ou supprimés. Voir le `vserver nvme namespace delete` et le `vserver nvme subsystem delete` commandes dans le"Référence des commandes ONTAP" pour plus d'informations.

2. Vérifiez qu'aucun vVols n'est présent dans la machine virtuelle de stockage :

```
lun show -verser <storage_VM> -class protocol-endpoint,vvol
```

Si des vVols sont présents, ils doivent être copiés sur une autre machine virtuelle de stockage, puis supprimés de la machine virtuelle de stockage à migrer. Voir le `lun copy` et `lun delete` commandes dans le"Référence des commandes ONTAP" pour plus d'informations.

3. Vérifiez que chaque volume de la machine virtuelle de stockage contient un seul LUN :

```
lun show -verser <storage_VM>
```

Si un volume contient plusieurs LUN, utilisez le `volume create` et `lun move` commandes pour créer un ratio volume/LUN de 1:1. Voir le"Référence des commandes ONTAP" pour plus d'informations.

Et la suite ?

Vous êtes prêt à créer une relation de pair à pair entre vos clusters ASA et ASA r2.

Étape 2 : Créez une relation de pair à pair entre vos clusters ASA et ASA r2

Avant de pouvoir migrer une machine virtuelle de stockage d'un cluster ASA vers un cluster ASA r2, vous devez créer une relation de pair à pair. Une relation d'égal à égal définit les connexions réseau qui permettent aux clusters ONTAP et aux machines virtuelles de stockage d'échanger des données en toute sécurité.

Avant de commencer

Vous devez avoir créé des LIF inter-clusters sur chaque nœud des clusters appariés en utilisant l'une des méthodes suivantes.

- "Configurer les LIF inter-clusters sur les ports de données partagés"
- "Configurez les LIF inter-clusters sur des ports de données dédiés"
- "Configurer les LIF inter-clusters dans des espaces IP personnalisés"

Étapes

1. Sur le cluster ASA r2, créez une relation de pair avec le cluster ASA et générez une phrase secrète :

```
cluster peer create -peer-addrs <ASA_cluster_LIF_IPs> -generate
-passphrase
```

L'exemple suivant crée une relation d'homologue entre le cluster 1 et le cluster 2 et crée une phrase secrète générée par le système :

```
cluster1::> cluster peer create -peer-addrs 10.98.191.193 -generate
-passphrase
Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
            Peer Cluster Name: cluster2
            Initial Allowed Vserver Peers: -
            Expiration Time: 6/7/2017 09:16:10 +5:30
            Intercluster LIF IP: 10.140.106.185
Warning: make a note of the passphrase - it cannot be displayed again.
```

2. Copiez la phrase secrète générée.
3. Sur le cluster ASA , créez une relation de pair avec le cluster ASA r2 :

```
cluster peer create -peer-addrs <ASA_r2_LIF_IPs>
```

4. Saisissez la phrase secrète générée sur le cluster ASA r2.
5. Vérifiez que la relation entre pairs du cluster est bien créée :

```
cluster peer show
```

L'exemple suivant illustre le résultat attendu pour des clusters appariés avec succès.

```
cluster1::> cluster peer show

Peer Cluster Name   Cluster Serial Number   Availability
Authentication
-----------------   ---------------------   --------------
--------------
cluster2             1-80-123456             Available      ok
```

Résultat

Les clusters ASA et ASA r2 sont appariés et les données des machines virtuelles de stockage peuvent être transférées en toute sécurité.

Et la suite ?

Vous êtes prêt à préparer votre machine virtuelle de stockage ASA pour la migration.

Étape 3 : Préparer la migration des machines virtuelles de stockage d'un ASA vers un cluster ASA r2

Avant de migrer une machine virtuelle de stockage (VM) d'un cluster ASA vers un cluster ASA r2, vous devez effectuer une vérification préalable de la migration et corriger les problèmes éventuels. Vous ne pouvez pas effectuer la migration tant que la vérification préalable n'a pas été réussie.

Étape

1. Depuis votre cluster ASA r2, exécutez la vérification préalable de la migration :

```
vserver migrate start -vserver <storage_VM> -source-cluster
<asa_cluster> -check-only true
```

Si vous devez résoudre des problèmes pour préparer votre cluster ASA à la migration, le problème et la solution corrective sont affichés. Corrigez le problème et répétez la vérification préalable jusqu'à ce qu'elle se termine avec succès.

Et la suite ?

Vous êtes prêt à migrer votre machine virtuelle de stockage de votre cluster ASA vers un cluster ASA r2.

Étape 4 : Migrer une machine virtuelle de stockage ASA vers un cluster ASA r2

Une fois votre cluster ASA préparé et la relation de pair de cluster nécessaire créée avec le cluster ASA r2, vous pouvez commencer la migration de la VM de stockage.

Lors de la migration d'une machine virtuelle de stockage, il est recommandé de laisser une marge de 30 % sur le processeur, tant sur le cluster ASA que sur le cluster ASA r2, afin de permettre l'exécution de la charge de travail du processeur.

Description de la tâche

Après la migration de la machine virtuelle de stockage, les clients sont automatiquement basculés vers le cluster ASA r2 et la machine virtuelle de stockage sur le cluster ASA est automatiquement supprimée. La bascule automatique et la suppression automatique des machines virtuelles de stockage sont activées par défaut. Vous pouvez également les désactiver tous les deux et effectuer manuellement la bascule et la suppression de la machine virtuelle de stockage.

Avant de commencer

- Le cluster ASA r2 doit disposer d'un espace libre suffisant pour accueillir la machine virtuelle de stockage migrée.
- Si la machine virtuelle de stockage ASA contient des volumes chiffrés, le gestionnaire de clés intégré ou le gestionnaire de clés externe du système ASA r2 doit être configuré au niveau du cluster.
- Les opérations suivantes ne peuvent pas être exécutées sur le cluster ASA source :
  - Opérations de basculement
  - WAFLIRON
  - Empreinte digitale
  - Déplacement de volume, réhébergement, clonage, création, conversion ou analyse

Étapes

1. Depuis le cluster ASA r2, lancez la migration de la machine virtuelle de stockage :

```
vserver migrate start -vserver <storage_VM_name> -source-cluster
<ASA_cluster>
```

Pour désactiver la bascule automatique, utilisez le `-auto-cutover false` paramètre. Pour désactiver la suppression automatique de la machine virtuelle de stockage ASA , utilisez le `-auto-source-cleanup`

`false` paramètre.

2. Surveillez l'état de la migration

```
vserver migrate show -vserver <storage_VM_name>
```

Une fois la migration terminée, le **statut** s'affiche comme **migration-terminée**.

> Si vous devez suspendre ou annuler la migration avant le début du basculement automatique, utilisez la `vserver migrate pause` et le `vserver migrate abort` commandes. Vous devez suspendre la migration avant de l'annuler. Vous ne pouvez pas annuler la migration une fois la transition commencée.

Résultat

La machine virtuelle de stockage est migrée du cluster ASA vers le cluster ASA r2. Le nom et l'UUID de la machine virtuelle de stockage, le nom de l'interface logique de données, l'adresse IP et les noms des objets, tels que le nom du volume, restent inchangés. L'UUID des objets migrés dans la machine virtuelle de stockage est mis à jour.

Et la suite ?

Si vous avez désactivé la bascule automatique et la suppression automatique des machines virtuelles de stockage,"Basculez manuellement vos clients ASA vers votre cluster ASA r2 et supprimez la machine virtuelle de stockage du cluster ASA." .

Basculer les clients et nettoyer la machine virtuelle de stockage source après la migration vers un système ASA r2

Après la migration d'une machine virtuelle de stockage (VM) d'un cluster ASA vers un cluster ASA r2, par défaut, les clients sont automatiquement basculés vers le cluster ASA r2 et la VM de stockage sur le cluster ASA est automatiquement supprimée. Si vous avez choisi de désactiver le basculement automatique et la suppression de la machine virtuelle de stockage ASA pendant la migration, vous devrez effectuer ces étapes manuellement une fois la migration terminée.

Basculer manuellement les clients vers un système ASA r2 après une migration de machine virtuelle de stockage

Si vous désactivez la bascule automatique du client lors de la migration d'une machine virtuelle de stockage d'un cluster ASA vers un cluster ASA r2, une fois la migration terminée avec succès, effectuez la bascule manuellement afin que la machine virtuelle de stockage ASA r2 puisse fournir des données aux clients.

Étapes

1. Sur le cluster ASA r2, exécutez manuellement la bascule du client :

```
vserver migrate cutover -vserver <storage_VM_name>
```

2. Vérifiez que l'opération de basculement est terminée :

```
vserver migrate show
```

Résultat

Les données sont fournies à vos clients depuis la machine virtuelle de stockage de votre cluster ASA r2.

Et la suite ?

Vous êtes maintenant prêt à supprimer la machine virtuelle de stockage du cluster ASA source.

Supprimer manuellement une machine virtuelle de stockage ASA après la migration vers un cluster ASA r2

Si vous désactivez le nettoyage automatique de la source lors de la migration d'une machine virtuelle de stockage d'un cluster ASA vers un cluster ASA r2, une fois la migration terminée, supprimez la machine virtuelle de stockage du cluster ASA pour libérer l'espace de stockage.

Avant de commencer

Vos clients doivent diffuser des données provenant du cluster ASA r2.

Étapes

1. Depuis le cluster ASA , vérifiez que l'état de la machine virtuelle de stockage ASA est **Prêt pour le nettoyage de la source** :

```
vserver migrate show
```

2. Supprimez la machine virtuelle de stockage ASA :

```
vserver migrate source-cleanup -vserver <storage_VM_name>
```

Résultat

La machine virtuelle de stockage de votre cluster ASA a été supprimée.

Limites de stockage de ASA r2

Pour des performances, une configuration et une assistance optimales, vous devez connaître les limites de stockage de l'ASA r2.

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

Les systèmes ASA r2 prennent en charge les limites de stockage suivantes :

	Maximum par paire d'aides auditives	Maximum par groupe
Groupes de cohérence	256	256
Applications d'entreprise	100	350

	Maximum par paire d'aides auditives	Maximum par groupe
Nœuds	2	12
Groupes de réplication	50	50
Taille de la zone de disponibilité de stockage	2 PB	2 PB
Unités de stockage	10 000	30 000
Taille de l'unité de stockage	128 TO	128 TO
Unités de stockage par groupe de cohérence	256	256
Groupes de cohérence enfant par groupe de cohérence parent	64	64
machines virtuelles de stockage	• 256 (ONTAP 9.18.1 et versions ultérieures) • 32 (ONTAP 9.17.1 et versions antérieures)	• 256 (ONTAP 9.18.1 et versions ultérieures) • 32 (ONTAP 9.17.1 et versions antérieures)
Machines virtuelles	800	1200

Limites des relations asynchrones SnapMirror

Les limites suivantes s'appliquent aux unités de stockage et aux groupes de cohérence dans une relation de réplication asynchrone SnapMirror . Pour obtenir la liste complète des limites de stockage les plus récentes ASA r2,"NetApp Hardware Universe" .

Limite maximale	Par paire HA	Par cluster
Groupes de cohérence	250	750
Unités de stockage	4 000	6 000

Limites de la relation de synchronisation active SnapMirror

Les limites suivantes s'appliquent aux unités de stockage et aux groupes de cohérence dans une relation de réplication de synchronisation active SnapMirror . La synchronisation active SnapMirror est prise en charge à partir d' ONTAP 9.17.1 uniquement sur les clusters à deux nœuds. À partir d' ONTAP 9.18.1, la synchronisation active SnapMirror est prise en charge sur les clusters à quatre nœuds.

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

Limite maximale	Par paire HA
Groupes de cohérence	50
Unités de stockage	400

Protégez vos données

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

Créez un instantané pour sauvegarder les données de votre système ASA r2. Utilisez ONTAP System Manager pour créer un instantané manuel d'une seule unité de stockage, ou pour créer un groupe de cohérence et planifier des instantanés automatiques de plusieurs unités de stockage simultanément.

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.

À partir d' ONTAP 9.18.1, vous pouvez définir le pourcentage de réserve de snapshots et activer la suppression automatique des snapshots lors de la création d'un groupe de cohérence avec de nouvelles unités de stockage. La réserve d'instantanés correspond à l'espace de l'unité de stockage réservé spécifiquement aux instantanés. Lorsque la réserve d'instantanés est configurée avec la suppression automatique des instantanés, les instantanés les plus anciens sont automatiquement supprimés lorsque l'espace utilisé par les instantanés dépasse la réserve d'instantanés. Si la réservation d'instantanés et la suppression automatique des instantanés sont activées sur un groupe de cohérence parent, elles le sont également sur tous les groupes de cohérence enfants existants. Si de nouveaux groupes de cohérence enfants sont ajoutés, ils n'héritent pas des paramètres de réservation et de suppression des instantanés du groupe parent.

"Découvrez-en plus sur la réserve de snapshots sur les systèmes de stockage ASA r2".

À partir d' ONTAP 9.16.1, lorsque vous créez des groupes de cohérence à l'aide de nouvelles unités de stockage, vous pouvez configurer jusqu'à cinq groupes de cohérence enfants. "Apprenez-en davantage sur les groupes de cohérence des enfants sur les systèmes ASA r2".

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 par défaut. Vous pouvez éventuellement attribuer une capacité différente à chaque unité.

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

Option	Étapes
Attribuez une capacité différente à chaque unité de stockage	Sélectionnez **Ajouter une capacité différente**.
Modifiez le niveau de service de performances par défaut	Sous **niveau de service Performance**, sélectionnez un niveau de service différent. Les systèmes ASA r2 offrent deux niveaux de performance. Le niveau de performance par défaut est **Extrême**, qui est le niveau le plus élevé disponible. Vous pouvez abaisser le niveau de performance à **Performance**.
Modifier la réserve de snapshots par défaut et activer la suppression automatique des snapshots	a. Sous **% de réserve de snapshots**, saisissez la valeur numérique du pourcentage de l'espace de l'unité de stockage que vous souhaitez allouer aux snapshots. b. Sélectionnez **Supprimer automatiquement les anciens instantanés**.
Créer un groupe de cohérence enfant	Sélectionnez **Ajouter un groupe de cohérence enfant**.

5. Sélectionnez le système d'exploitation hôte et le mappage d'hôte.
6. Sélectionnez **Ajouter**.

Et la suite ?

Vous avez créé un groupe de cohérence contenant les unités de stockage que vous souhaitez protéger. Vous pouvez maintenant créer un instantané.

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 pouvez maintenant créer un instantané.

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

  Vous pouvez créer à tout moment un instantané à la demande d'une unité de stockage. L'unité de stockage n'a pas besoin d'appartenir à un groupe de cohérence pour être protégée par un instantané à la demande. Si vous créez un instantané 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 l'instantané à la demande. Si vous créez un instantané à la demande d'un groupe de cohérence, toutes les unités de stockage du groupe de cohérence sont incluses dans l'instantané.

- 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.

Gérer la réserve d'instantanés

Découvrez la réservation de snapshots ONTAP sur le stockage ASA r2

La réserve de snapshots correspond à l'espace de l'unité de stockage réservé spécifiquement aux snapshots. Lorsque la réserve d'instantanés est configurée avec la suppression automatique des instantanés, les instantanés les plus anciens sont automatiquement supprimés lorsque l'espace utilisé par les instantanés dépasse la réserve d'instantanés. Cela empêche les instantanés de consommer de l'espace dans votre unité de stockage destiné aux données utilisateur.

La réserve instantanée est définie en pourcentage de la taille totale de l'unité de stockage. Par exemple, si l'unité de stockage est de 50 Go et que vous définissez la réserve d'instantanés à 10 %, l'espace réservé aux instantanés est de 5 Go. Lorsque l'espace utilisé par les instantanés atteint 5 Go, les instantanés les plus anciens sont automatiquement supprimés pour faire de la place aux nouveaux. Si la taille de l'unité de

stockage passe à 100 Go, la réserve de snapshots passe à 10 Go. La réserve maximale de snapshots que vous pouvez définir est de 200 %. Si votre unité de stockage atteint la taille maximale de 128 To, une réserve de snapshots de 200 % vous permet de prendre 2 snapshots complets.

Par défaut, la réserve de snapshots est fixée à 0 % et la suppression automatique des snapshots n'est pas activée.

À partir d' ONTAP 9.18.1, vous pouvez modifier la réserve de snapshot par défaut pendant ou après la création d'unités de stockage et pendant la création de groupes de cohérence. Vous pouvez également modifier la réserve de snapshots par défaut sur les machines virtuelles de stockage existantes (VM). Dans ONTAP 9.17.1 et versions antérieures, vous ne pouvez pas modifier ces paramètres.

La réserve d'instantané est définie sur le même pourcentage pour toutes les unités de stockage d'un groupe de cohérence au moment de la création de ce groupe. La réserve d'instantané doit être définie individuellement pour chaque unité de stockage ajoutée ultérieurement.

Modifier la réserve de snapshots sur un système de stockage ASA r2

La réserve d'instantanés correspond à l'espace de l'unité de stockage réservé spécifiquement aux instantanés. Par défaut, la réserve de snapshots est fixée à 0 %. À partir d' ONTAP 9.18.1, vous pouvez modifier la réserve de snapshots par défaut de l'unité de stockage et activer la suppression automatique des snapshots. La suppression automatique des instantanés est désactivée par défaut. Lorsqu'une valeur de réserve pour les instantanés est définie et que la suppression automatique des instantanés est activée, les instantanés les plus anciens sont automatiquement supprimés lorsque l'espace utilisé par les instantanés dépasse la réserve d'instantanés. Cela empêche les instantanés de consommer de l'espace dans votre unité de stockage destiné aux données utilisateur.

"Découvrez-en plus sur la réserve de snapshots sur les systèmes de stockage ASA r2".

Modifier la réserve d'instantané sur les unités de stockage

Pour définir des valeurs de réserve de snapshots différentes, configurez chaque unité de stockage individuellement. Pour utiliser la même valeur pour toutes les unités de stockage, modifiez la réserve d'instantanés sur la machine virtuelle de stockage.

Étapes

1. Dans System Manager, sélectionnez **Storage**.
2. Survolez le nom de l'unité de stockage pour laquelle vous souhaitez définir la réserve d'instantanés.
3. Sélectionner ⋮ , puis sélectionnez **Modifier**.
4. Sous **% de réserve de snapshots**, saisissez la valeur numérique du pourcentage de l'espace de l'unité de stockage que vous souhaitez allouer aux snapshots.
5. Vérifiez que l'option **Supprimer automatiquement les anciens instantanés** est sélectionnée.
6. Sélectionnez **Enregistrer**.

Résultat

La réserve d'instantanés est définie sur le pourcentage que vous avez spécifié. Si l'espace occupé par les instantanés atteint la réserve, les instantanés les plus anciens sont automatiquement supprimés.

Modifier la réserve de snapshot sur une machine virtuelle de stockage

Pour définir la même réserve de snapshots pour toutes les unités de stockage d'une VM de stockage, appliquez le pourcentage souhaité à la VM de stockage. . Lorsque la réserve d'instantané est appliquée à la machine virtuelle de stockage, elle est appliquée à toutes les unités de stockage nouvellement créées au sein de cette machine virtuelle. Cela ne s'applique pas aux unités de stockage créées avant que vous ne modifiiez ce paramètre.

Étapes

1. Dans le Gestionnaire système, sélectionnez **Cluster > Machines virtuelles de stockage** ; puis sélectionnez **Paramètres**.
2. Sous **Politiques**, à côté de **Instantanés**, sélectionnez ⋮ ; puis sélectionnez **Définir/modifier la valeur par défaut de la réserve d'instantanés**.
3. Sous **% de réserve de snapshots**, saisissez la valeur numérique du pourcentage de l'espace de l'unité de stockage que vous souhaitez allouer aux snapshots.
4. Vérifiez que l'option **Supprimer automatiquement les anciens instantanés** est sélectionnée.
5. Sélectionnez **Enregistrer**.

Résultat

La réserve d'instantanés pour les unités de stockage nouvellement créées est définie sur le pourcentage que vous avez spécifié. Si l'espace occupé par les instantanés dans ces unités de stockage atteint la réserve, les instantanés les plus anciens sont automatiquement supprimés.

Créer une relation homologue de machine virtuelle de stockage intercluster sur les systèmes de stockage ASA r2

Une relation d'homologue définit les connexions réseau permettant aux clusters et aux machines virtuelles de stockage (VM) d'échanger des données en toute sécurité. Créez des relations d'homologue entre les VM de stockage de différents clusters pour assurer la protection des données et la reprise après sinistre grâce à SnapMirror.

"En savoir plus sur les relations entre pairs" .

Avant de commencer

Vous devez avoir établi une relation d'homologue de cluster entre les clusters locaux et distants avant de pouvoir créer une relation d'homologue de machine virtuelle de stockage. "Créer une relation entre pairs de cluster" si vous ne l'avez pas déjà fait.

Étapes

1. Dans le Gestionnaire système, sélectionnez **Protection > Présentation**.
2. Sous **Homologations de machines virtuelles de stockage**, sélectionnez **Ajouter une homologation de machines virtuelles de stockage**.
3. Sélectionnez la machine virtuelle de stockage sur le cluster local, puis sélectionnez la machine virtuelle de stockage sur le cluster distant.
4. Sélectionnez **Ajouter un homologue de machine virtuelle de stockage**.

Configuration de la réplication Snapshot

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

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

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

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

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

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

Étape 1 : créer une relation entre clusters

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

Avant de commencer

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

Étapes

1. Sur le cluster local, dans System Manager, sélectionnez **Cluster > Paramètres**.
2. Sous **intercluster Settings** en regard de **Cluster peers**, sélectionnez , puis **Ajouter un homologue de cluster**.
3. Sélectionnez **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 : (facultatif) Créez une politique de réplication personnalisée

La politique de réplication définit quand les mises à jour effectuées sur le cluster ASA r2 sont répliquées sur le

site distant. ONTAP inclut diverses politiques de protection des données prédéfinies que vous pouvez utiliser pour vos relations de réplication. Si les politiques prédéfinies ne répondent pas à vos besoins, vous pouvez créer une politique de réplication personnalisée.

En savoir plus sur"politiques de protection des données ONTAP prédéfinies" .

Étapes

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

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

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

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

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

Et la suite ?

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

Pour en savoir plus

En savoir plus sur "Machines virtuelles de stockage pour l'accès client".

Étape 3 : création d'une relation de réplication

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

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

Avant de commencer

- "En savoir plus sur les politiques de réplication" .

  Lorsque vous créez une relation de réplication, vous devez sélectionner la stratégie de réplication

appropriée pour votre relation de réplication. Vous pouvez utiliser une politique prédéfinie ou créer une politique personnalisée.

- Si vous souhaitez verrouiller vos snapshots de destination, vous devez d'"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. 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.

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

La politique de réplication définit quand les mises à jour effectuées sur le cluster ASA r2 sont répliquées sur le site distant. ONTAP inclut diverses politiques de protection des

données prédéfinies que vous pouvez utiliser pour vos relations de réplication.

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

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

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

Politique	Description	Type de politique
Asynchrone	Une politique asynchrone et de coffre-fort SnapMirror unifiée pour la mise en miroir du dernier système de fichiers actif et des instantanés quotidiens et hebdomadaires avec un calendrier de transfert horaire.	Asynchrone
Basculement automatique duplex	Politique pour SnapMirror synchrone avec garantie RTO nulle et réplication de synchronisation bidirectionnelle.	Synchronisation active de SnapMirror
CloudBackupDefault	Politique de coffre-fort avec règle quotidienne.	Asynchrone
Sauvegarde quotidienne	Politique de coffre-fort avec une règle quotidienne et un calendrier de transfert quotidien.	Asynchrone
DPDéfaut	Politique asynchrone SnapMirror pour la mise en miroir de tous les instantanés et du dernier système de fichiers actif.	Asynchrone
MirrorAllSnapshots	Politique asynchrone SnapMirror pour la mise en miroir de tous les instantanés et du dernier système de fichiers actif.	Asynchrone
MiroirTous les instantanésSupprimer le réseau	Politique asynchrone SnapMirror pour la mise en miroir de tous les instantanés et du dernier système de fichiers actif, à l'exclusion des configurations réseau.	Asynchrone
Miroir et coffre-fort	Une politique asynchrone et de coffre-fort SnapMirror unifiée pour la mise en miroir du dernier système de fichiers actif et des instantanés quotidiens et hebdomadaires.	Asynchrone
MirrorAndVaultDiscardNetwork	Une politique asynchrone et de coffre-fort SnapMirror unifiée pour la mise en miroir du dernier système de fichiers actif et des instantanés quotidiens et hebdomadaires à l'exclusion des configurations réseau.	Asynchrone
MirrorLatest	Politique asynchrone SnapMirror pour la mise en miroir du dernier système de fichiers actif.	Asynchrone
Unified7year	Politique SnapMirror unifiée avec conservation de 7 ans.	Asynchrone

Politique	Description	Type de politique
XDP par défaut	Politique de coffre-fort avec règles quotidiennes et hebdomadaires.	Asynchrone

Rompre une relation de réplication asynchrone sur votre système ASA r2

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

Étapes

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

Résultat

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

Configurer la synchronisation active de SnapMirror

Flux de travail de configuration de la synchronisation active de SnapMirror

La protection des données ONTAP SnapMirror Active Sync permet aux services métier de continuer à fonctionner même en cas de panne totale du site, en permettant le basculement transparent des applications via une copie secondaire. Aucune intervention manuelle ni script personnalisé ne sont requis pour déclencher un basculement avec SnapMirror Active Sync.

Bien que les procédures du gestionnaire système pour la configuration de SnapMirror Active Sync soient différentes sur les systèmes ASA r2 et sur les systèmes NetApp FAS, AFF et ASA exécutant la personnalité ONTAP unifiée, les exigences, l'architecture et le fonctionnement de SnapMirror Active Sync sont les mêmes.

"En savoir plus sur les personnalités ONTAP" .

> ⓘ À partir d' ONTAP 9.18.1, la synchronisation active SnapMirror est prise en charge sur les configurations à quatre nœuds. Dans ONTAP 9.17.1, la synchronisation active SnapMirror est prise en charge uniquement sur les configurations à deux nœuds.

"En savoir plus sur la synchronisation active de SnapMirror" .

"En savoir plus sur la reprise après sinistre avec SnapMirror Active Sync sur votre système ASA r2"

Sur les systèmes ASA r2, SnapMirror Active Sync prend en charge les configurations symétriques actives/actives. Dans une telle configuration, les deux sites peuvent accéder au stockage local pour les E/S actives.

En savoir plus sur "configurations symétriques actives/actives" .

1. **Préparez-vous à configurer la synchronisation active de SnapMirror .**

À "préparer la configuration de SnapMirror Active Sync" sur votre système ASA r2, vous devez examiner les conditions préalables de configuration, confirmer la prise en charge de vos systèmes d'exploitation hôtes et être conscient des limites d'objets susceptibles d'avoir un impact sur une configuration spécifique.

2. **Confirmez la configuration de votre cluster.**

Avant de configurer la synchronisation active de SnapMirror , vous devez "confirmez que vos clusters ASA r2 sont dans les relations de peering appropriées et répondent aux autres exigences de configuration" .

3. **Installez ONTAP Mediator.**

Vous pouvez utiliser ONTAP Mediator ou ONTAP Cloud Mediator pour surveiller l'état de votre cluster et assurer la continuité de vos activités. Si vous utilisez ONTAP Mediator, vous devez "installez-le" sur votre hôte. Si vous utilisez ONTAP Cloud Mediator, vous pouvez ignorer cette étape.

4. **Configurez ONTAP Mediator ou ONTAP Cloud Mediator à l'aide de certificats auto-signés.**

Vous devez "configurer le médiateur ONTAP ou le médiateur cloud ONTAP" avant de pouvoir commencer à l'utiliser avec SnapMirror Active Sync pour la surveillance des clusters.

5. **Configurer la synchronisation active de SnapMirror .**

"Configurer la synchronisation active de SnapMirror" pour créer une copie de vos données sur un site secondaire et permettre à vos applications hôtes de basculer automatiquement et de manière transparente en cas de sinistre.

Préparez-vous à configurer SnapMirror Active Sync sur les systèmes ASA r2

Pour préparer la configuration de SnapMirror Active Sync sur votre système ASA r2, vous devez examiner les conditions préalables de configuration, confirmer la prise en charge des systèmes d'exploitation de vos hôtes et être conscient des limites d'objets susceptibles d'avoir un impact sur une configuration spécifique.

Étapes

1. Revoir la synchronisation active de SnapMirror "prérequis" .
2. "Confirmez que vos systèmes d'exploitation hôtes sont pris en charge" pour la synchronisation active SnapMirror .
3. Passez en revue le "limites de l'objet" cela pourrait avoir un impact sur votre configuration.
4. Vérifiez la prise en charge du protocole hôte pour la synchronisation active SnapMirror sur votre système ASA r2.

   La prise en charge de la synchronisation active SnapMirror sur les systèmes ASA r2 varie en fonction de la version ONTAP et du protocole hôte.

En commençant par ONTAP…	La synchronisation active de SnapMirror prend en charge…
9.17.1	• iSCSI • FC • NVMe/FC • NVMe/TCP
9.16.0	• iSCSI • FC

Limitations du protocole NVMe avec la synchronisation active SnapMirror sur les systèmes ASA r2

Avant de configurer SnapMirror Active Sync sur un système ASA r2 avec des hôtes NVMe, vous devez connaître certaines limitations du protocole NVMe.

Toutes les unités de stockage NVMe du sous-système NVMe doivent être membres du même groupe de cohérence et doivent toutes faire partie de la même relation de synchronisation active SnapMirror .

Les protocoles NVMe/FC et NVMe/TCP sont pris en charge avec SnapMirror Active Sync comme suit :

- Uniquement sur les clusters à 2 nœuds
- Uniquement sur les hôtes ESXi
- Uniquement avec des configurations symétriques actives/actives

  Les configurations actives/actives asymétriques ne sont pas prises en charge avec les hôtes NVMe.

La synchronisation active de SnapMirror avec NVMe ne prend pas en charge les éléments suivants :

- Sous-systèmes mappés à plusieurs groupes de cohérence

  Un groupe de cohérence peut être mappé avec plusieurs sous-systèmes, mais chaque sous-système ne peut être mappé qu'à un seul groupe de cohérence.

- Extension des groupes de cohérence dans une relation de synchronisation active SnapMirror
- Mappage des unités de stockage NVMe qui ne sont pas dans une relation de synchronisation active SnapMirror vers des sous-systèmes répliqués
- Suppression d'une unité de stockage d'un groupe de cohérence
- Changement de géométrie du groupe de cohérence
- "Transfert de données déchargées Microsoft (ODX)"

Et la suite ?

Après avoir terminé la préparation nécessaire pour activer la synchronisation active de SnapMirror , vous devez "confirmer la configuration de votre cluster" .

Confirmez la configuration de votre cluster ASA r2 avant de configurer SnapMirror Active Sync

SnapMirror Active Sync s'appuie sur des clusters appairés pour protéger vos données en cas de basculement. Avant de configurer SnapMirror Active Sync, vous devez vérifier que vos clusters ASA r2 sont dans une relation d'appairage prise en charge et répondent aux autres exigences de configuration.

Étapes

1. Confirmez qu'une relation d'appairage de cluster existe entre les clusters.

   > L'espace IP par défaut est requis par SnapMirror Active Sync pour les relations entre homologues de cluster. Un espace IP personnalisé n'est pas pris en charge.

   "Créer une relation entre pairs de cluster" .

2. Confirmez qu'une relation homologue existe entre les machines virtuelles de stockage (VM) sur chaque cluster.

   "Créer une relation homologue de machine virtuelle de stockage intercluster" .

3. Confirmez qu'au moins un LIF est créé sur chaque nœud du cluster.

   "Créer un FRV".

4. Confirmez que les unités de stockage nécessaires sont créées et mappées aux groupes d'hôtes.

   "Créer une unité de stockage" et "mapper l'unité de stockage à un groupe d'hôtes" .

5. Réanalysez l'hôte de l'application pour découvrir de nouvelles unités de stockage.

Et la suite ?

Après avoir confirmé la configuration de votre cluster, vous êtes prêt à "installer ONTAP Mediator" .

Installer ONTAP Mediator sur les systèmes ASA r2

Pour installer ONTAP Mediator pour votre système ASA r2, vous devez suivre la même procédure utilisée pour installer ONTAP Mediator pour tous les autres systèmes ONTAP .

L'installation ONTAP Mediator comprend la préparation de l'installation, l'activation de l'accès aux référentiels, le téléchargement du package ONTAP Mediator, la vérification de la signature du code, l'installation du package sur l'hôte et l'exécution des tâches de post-installation.

Pour installer ONTAP Mediator, suivez "ce flux de travail"

Et la suite

Une fois ONTAP Mediator installé, vous devez "configurer ONTAP Mediator à l'aide de certificats auto-signés" .

Configurer ONTAP Mediator ou ONTAP Cloud Mediatior sur les systèmes ASA r2

Vous devez configurer ONTAP Mediator ou ONTAP Cloud Mediator avant de pouvoir utiliser SnapMirror Active Sync pour la surveillance des clusters. ONTAP Mediator et ONTAP Cloud Mediator fournissent tous deux un stockage persistant et clôturé pour les

métadonnées haute disponibilité (HA) utilisées par les clusters ONTAP dans une relation SnapMirror Active Sync. De plus, les deux médiateurs offrent une fonctionnalité de requête synchrone sur l'état des nœuds pour faciliter la détermination du quorum et servent de proxy ping pour la détection de la vivacité des contrôleurs.

Avant de commencer

Si vous utilisez ONTAP Cloud Mediator, vérifiez que votre système ASA r2 répond aux exigences nécessaires "prérequis" .

Étapes

1. Dans le Gestionnaire système, sélectionnez **Protection > Présentation**.
2. Dans le volet de droite, sous **Médiateurs**, sélectionnez **Ajouter un médiateur**.
3. Sélectionnez le **type de médiateur**.
4. Pour un médiateur **Cloud**, saisissez l'ID d'organisation, l'ID client et le secret client. Pour un médiateur **On-premises**, saisissez l'adresse IP, le port, le nom d'utilisateur et le mot de passe du médiateur.
5. Sélectionnez le pair de cluster dans la liste des pairs de cluster éligibles ou sélectionnez **Ajouter un pair de cluster** pour en ajouter un nouveau.
6. Ajoutez les informations du certificat
   - Si vous utilisez un certificat auto-signé, copiez le contenu du `intermediate.crt` fichier et collez-le dans le champ **Certificat**, ou sélectionnez **Importer** pour accéder au `intermediate.crt` fichier et importer les informations du certificat.
   - Si vous utilisez un certificat tiers, saisissez les informations du certificat dans le champ **Certificat**.
7. Sélectionnez **Ajouter**.

Et la suite ?

Après avoir initialisé le médiateur, vous pouvez "configurer la synchronisation active de SnapMirror" pour créer une copie de vos données sur un site secondaire et permettre à vos applications hôtes de basculer automatiquement et de manière transparente en cas de sinistre.

Configurer la synchronisation active SnapMirror sur les systèmes ASA r2

Configurez la synchronisation active SnapMirror pour créer une copie de vos données sur un site secondaire et permettre à vos applications hôtes de basculer automatiquement et de manière transparente en cas de sinistre.

Sur les systèmes ASA r2, SnapMirror Active Sync prend en charge les configurations symétriques actives/actives. Dans une telle configuration, les deux sites peuvent accéder au stockage local pour les E/S actives.

Si vous utilisez le protocole iSCSI ou FC et utilisez les outils ONTAP pour VMware Sphere, vous pouvez éventuellement "utilisez ONTAP Tools pour VMware pour configurer SnapMirror Active Sync" .

Avant de commencer

"Créer un groupe de cohérence" sur le site principal avec de nouvelles unités de stockage. Si vous souhaitez créer une configuration active/active symétrique non uniforme, créez également un groupe de cohérence sur le site secondaire avec de nouvelles unités de stockage.

En savoir plus sur "non uniforme" configurations symétriques actives/actives.

Étapes

1. Dans System Manager, sélectionnez **protection > groupes de cohérence**.
2. Passez la souris sur le nom du groupe de cohérence que vous souhaitez protéger avec la synchronisation active SnapMirror .
3. Sélectionner ⋮ puis sélectionnez **Protéger**.
4. Sous **protection distante**, sélectionnez **répliquer sur un cluster distant**.
5. Sélectionnez un homologue de cluster existant ou choisissez d'**en ajouter un nouveau**.
6. Sélectionnez la machine virtuelle de stockage.
7. Pour la politique de réplication, sélectionnez **AutomatedFailOverDuplex**.
8. Si vous créez une configuration active/active symétrique non uniforme, sélectionnez **Paramètres de destination** ; puis saisissez le nom du nouveau groupe de cohérence de destination que vous créez avant de commencer cette procédure.
9. Sélectionnez **Enregistrer**.

Résultat

La synchronisation active de SnapMirror est configurée pour protéger vos données afin que vous puissiez poursuivre vos opérations avec un objectif de point de récupération (RPO) proche de zéro et un objectif de temps de récupération (RTO) proche de zéro en cas de sinistre.

Gérer la synchronisation active de SnapMirror

Reconfigurer ONTAP Mediator ou ONTAP Cloud Mediator pour utiliser un certificat tiers sur les systèmes ASA r2

Si vous configurez ONTAP Mediator ou ONTAP Cloud Mediator avec un certificat auto-signé, vous pouvez reconfigurer le médiateur pour utiliser un certificat tiers. Les certificats tiers peuvent être préférés ou exigés par votre organisation pour des raisons de sécurité.

Étape 1 : Supprimer la configuration du médiateur

Pour reconfigurer le médiateur, vous devez d'abord supprimer sa configuration actuelle du cluster.

Étapes

1. Dans le Gestionnaire système, sélectionnez **Protection > Présentation**.
2. Dans le volet de droite, sous **Médiateurs**, sélectionnez ⋮ à côté du pair de cluster avec la configuration de médiateur que vous souhaitez supprimer ; puis sélectionnez **Supprimer**.

   Si vous avez plusieurs médiateurs installés et que vous souhaitez supprimer toutes les configurations, sélectionnez ⋮ à côté de **Médiateurs** ; puis sélectionnez **Supprimer**.

3. Sélectionnez **Supprimer** pour confirmer que vous souhaitez supprimer la configuration du médiateur.

Étape 2 : supprimer le certificat auto-signé

Une fois la configuration du médiateur supprimée, vous devez supprimer le certificat auto-signé associé du cluster.

Étapes

1. Sélectionnez **Cluster > Paramètres**.
2. Sous **Sécurité**, sélectionnez **Certificats**.
3. Sélectionnez le certificat que vous souhaitez supprimer.
4. Sélectionnez ⋮, puis **Supprimer**.

Étape 3 : Réinstaller le médiateur avec un certificat tiers

Après avoir supprimé le certificat auto-signé associé, vous pouvez reconfigurer le médiateur avec le certificat tiers.

Étapes

1. Sélectionnez **Protection > Présentation**.
2. Dans le volet de droite, sous **Médiateurs**, sélectionnez **Ajouter un médiateur**.
3. Sélectionnez le **type de médiateur**.
4. Pour un médiateur **Cloud**, saisissez l'ID d'organisation, l'ID client et le secret client. Pour un médiateur **sur site**, saisissez l'adresse IP, le port, le nom d'utilisateur du médiateur et le mot de passe du médiateur.
5. Sélectionnez un homologue de cluster dans la liste des homologues de cluster éligibles ou sélectionnez **Ajouter un homologue de cluster** pour en ajouter un nouveau.
6. Sous **Certificat**, saisissez les informations du certificat tiers.
7. Sélectionnez **Ajouter**.

Résultat

Le médiateur ONTAP ou le médiateur cloud ONTAP est reconfiguré pour utiliser le certificat tiers. Vous pouvez désormais utiliser le médiateur pour gérer les relations de synchronisation active de SnapMirror .

Effectuer un basculement planifié des clusters ASA r2 dans une relation de synchronisation active SnapMirror

La synchronisation active SnapMirror assure une disponibilité continue des applications critiques en créant une copie de vos données sur un site secondaire et en permettant à vos applications hôtes de basculer automatiquement et de manière transparente en cas de sinistre. Vous devrez peut-être effectuer un basculement planifié de votre relation de synchronisation active SnapMirror pour tester le processus de basculement ou effectuer une maintenance sur le site principal.

Avant de commencer

- La relation de synchronisation active SnapMirror doit être synchronisée.
- Vous ne pouvez pas lancer un basculement planifié lorsqu'une opération non perturbatrice, telle qu'un déplacement d'unité de stockage, est en cours.
- ONTAP Mediator ou ONTAP Cloud Mediator doit être configuré, connecté et en quorum.

Étapes

1. Sélectionnez **Protection > Réplication**.
2. Sélectionnez la relation de synchronisation active SnapMirror que vous souhaitez basculer.
3. Sélectionner ⋮ ; puis sélectionnez **Failover**.

Et la suite

Utilisez le `snapmirror failover show` commande dans l'interface de ligne de commande ONTAP (CLI) pour surveiller l'état du basculement.

Rétablir la relation de synchronisation active SnapMirror après un basculement imprévu de vos clusters ASA r2

Sur les systèmes ASA r2, SnapMirror active sync prend en charge les configurations actives/actives symétriques. Dans une configuration active/active symétrique, les deux sites peuvent accéder au stockage local pour les E/S actives. Si le cluster source tombe en panne ou est isolé, le médiateur déclenche un basculement automatique non planifié (AUFO) et prend en charge toutes les E/S depuis le cluster de destination jusqu'à la récupération du cluster source.

Si vous rencontrez une AUFO de votre SnapMirror active sync relationship, vous devez rétablir la relation et reprendre les opérations sur le cluster source d'origine une fois celui-ci remis en ligne.

Avant de commencer

- La relation de synchronisation active SnapMirror doit être synchronisée.
- Vous ne pouvez pas lancer un basculement planifié lorsqu'une opération non perturbatrice, telle qu'un déplacement d'unité de stockage, est en cours.
- Le médiateur ONTAP doit être configuré, connecté et en quorum.
- Pour récupérer les chemins d'E/S perdus ou mettre à jour l'état des chemins d'E/S sur vos hôtes, vous devez effectuer une nouvelle analyse du stockage/des adaptateurs sur les hôtes après la reprise du fonctionnement du cluster de stockage principal.

Étapes

1. Sélectionnez **Protection > Réplication**.
2. Sélectionnez la relation de synchronisation active SnapMirror que vous devez rétablir.
3. Attendez que le statut de la relation affiche **InSync**.
4. Sélectionner ⋮ ; puis sélectionnez **Failover** pour reprendre les opérations sur le cluster principal d'origine.

Supprimer une relation de synchronisation active SnapMirror sur votre système ASA r2

Si vous n'avez plus besoin d'un RPO et d'un RTO proches de zéro pour une application métier, vous devez supprimer la protection de synchronisation active SnapMirror en supprimant la relation de synchronisation active SnapMirror associée. Si vous exécutez ONTAP 9.16.1 sur un système ASA r2, vous devrez peut-être également supprimer la relation de synchronisation active SnapMirror avant de pouvoir apporter certaines modifications de géométrie aux groupes de cohérence dans une relation de synchronisation active SnapMirror .

Étape 1 : Terminer la réplication de l'hôte

Si le groupe d'hôtes du cluster source est répliqué vers le cluster de destination et que les groupes de cohérence de destination sont mappés au groupe d'hôtes répliqué, vous devez terminer la réplication de l'hôte sur le cluster source avant de pouvoir supprimer la relation de synchronisation active SnapMirror .

Étapes

1. Dans System Manager, sélectionnez **Host**.
2. À côté d'un hôte contenant le groupe d'hôtes dont vous souhaitez arrêter la réplication, sélectionnez , puis sélectionnez **Modifier**.
3. Désélectionnez **Répliquer la configuration de l'hôte**, puis sélectionnez **Mettre à jour**.

Étape 2 : Supprimer la relation de synchronisation active SnapMirror

Pour supprimer la protection de synchronisation active SnapMirror d'un groupe de cohérence, vous devez supprimer la relation de synchronisation active SnapMirror .

Étapes

1. Dans System Manager, sélectionnez **protection > réplication**.
2. Sélectionnez **Destinations locales** ou **Sources locales**.
3. À côté de la relation de synchronisation active SnapMirror que vous souhaitez supprimer, sélectionnez ; puis sélectionnez **Supprimer**.
4. Sélectionnez **Libérer les instantanés de base du groupe de cohérence source**.
5. Sélectionnez **Supprimer**.

Résultat

La relation de synchronisation active SnapMirror est supprimée et les instantanés de base du groupe de cohérence source sont libérés. Les unités de stockage du groupe de cohérence ne sont plus protégées par la synchronisation active SnapMirror .

Et la suite ?

"Configuration de la réplication Snapshot"pour copier le groupe de cohérence vers un emplacement géographiquement distant à des fins de sauvegarde et de reprise après sinistre.

Supprimez ONTAP Mediator ou ONTAP Cloud Mediator de votre système ASA r2

Vous ne pouvez utiliser qu'un seul type de médiateur à la fois pour la synchronisation active SnapMirror sur votre système ASA r2. Si vous choisissez de modifier votre type de médiateur, vous devez supprimer votre instance actuelle avant d'installer une autre instance.

Étapes

Vous devez utiliser l'interface de ligne de commande ONTAP (CLI) pour supprimer ONTAP Mediator ou ONTAP Cloud Mediator.

Médiateur ONTAP

1. Supprimer ONTAP Mediator :

   ```
   snapmirror mediator remove -mediator-address <address> -peer-cluster
   <peerClusterName>
   ```

   Exemple:

   ```
   snapmirror mediator remove -mediator-address 12.345.678.90 -peer
   -cluster cluster_xyz
   ```

Médiateur cloud ONTAP

1. Supprimer ONTAP Cloud Mediator :

   ```
   snapmirror mediator remove -peer-cluster <peerClusterName> -type cloud
   ```

   Exemple:

   ```
   snapmirror mediator remove -peer-cluster cluster_xyz -type cloud
   ```

Informations associées

- "supprimer le médiateur SnapMirror"

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.

Gérer les groupes de cohérence

En savoir plus sur les 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. Utilisez des groupes de cohérence pour une gestion simplifiée du stockage.

Par exemple, supposons que vous disposez d'une base de données composée de 10 unités de stockage dans un groupe de cohérence et que vous devez sauvegarder l'intégralité de la base de données. Au lieu de sauvegarder chaque unité de stockage, vous pouvez sauvegarder l'intégralité de la base de données en ajoutant simplement une protection des données de snapshot au groupe de cohérence. La sauvegarde des unités de stockage en tant que groupe de cohérence plutôt qu'individuellement fournit également une sauvegarde cohérente de toutes les unités, tandis que la sauvegarde des unités individuellement peut potentiellement créer des incohérences.

À partir d' ONTAP 9.16.1, vous pouvez utiliser System Manager pour créer des groupes de cohérence hiérarchiques sur votre système ASA r2. Dans une structure hiérarchique, un ou plusieurs groupes de cohérence sont configurés comme enfants sous un groupe de cohérence parent.

Les groupes de cohérence hiérarchiques vous permettent d'appliquer des règles de snapshot individuelles à chaque groupe de cohérence enfant et de répliquer les snapshots de tous les groupes de cohérence enfant sur un cluster distant en tant qu'unité unique en répliquant le parent. Cela simplifie la protection et la gestion des données pour les structures de données complexes. Supposons par exemple que vous créez le groupe de cohérence parent appelé `SVM1_app` qui contient deux groupes de cohérence enfant : `SVM1app_data` pour les données d'application et `SVM1app_logs` pour les journaux d'application. Des instantanés de `SVM1app_data` sont pris toutes les 15 minutes et des instantanés de `SVM1app_logs` sont pris toutes les heures. Le groupe de cohérence parent, `SVM1_app`, dispose d'une règle SnapMirror qui réplique les snapshots de `SVM1app_data` et `SVM1app_logs` sur un cluster distant toutes les 24 heures. Le groupe de cohérence parent `SVM1_app` est géré comme une seule unité et les groupes de cohérence enfant sont gérés comme des unités distinctes.

Groupes de cohérence dans les relations de réplication

À partir d' ONTAP 9.17.1, vous pouvez apporter les modifications de géométrie suivantes aux groupes de cohérence dans une relation de réplication asynchrone ou dans une relation de synchronisation active SnapMirror sans interrompre ou supprimer la relation. Lorsqu'un changement de géométrie se produit sur le groupe de cohérence principal, le changement est répliqué sur le groupe de cohérence secondaire.

- "Modifier la taille d'une unité de stockage"en ajoutant ou en supprimant des unités de stockage.
- "Promouvoir un groupe de cohérence unique"à un groupe de cohérence parent.
- "Rétrograder un groupe de cohérence parent"à un seul groupe de cohérence.
- "Détacher un groupe de cohérence enfant"d'un groupe de cohérence parent.
- "Créer un groupe de cohérence enfant"en utilisant un groupe de cohérence existant.

Dans ONTAP 9.16.1, vous devez"rompre la relation de réplication asynchrone" et"supprimer la relation de synchronisation active SnapMirror" avant d'apporter des modifications géométriques au groupe de cohérence.

Protégez les groupes de cohérence sur votre système ASA r2 avec des instantanés

Créez des instantanés des groupes de cohérence dans votre système de stockage ASA r2 pour protéger les données dans les unités de stockage qui font partie du groupe de cohérence. Si vous n'avez plus besoin de protéger les données dans l'une des unités de

stockage du groupe de cohérence, vous pouvez supprimer la protection des snapshots du groupe de cohérence.

Si vous n'avez plus besoin de protéger les données d'unités de stockage spécifiques dans le groupe de cohérence, vous pouvez supprimer ces unités de stockage du groupe de cohérence.

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 **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.

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.

Modifier la taille des groupes de cohérence sur votre système ASA r2

Augmentez ou diminuez la taille d'un groupe de cohérence en modifiant le nombre d'unités de stockage dans le groupe de cohérence.

Ajouter des unités de stockage à un groupe de cohérence

Augmentez la capacité de stockage gérée par un groupe de cohérence en ajoutant des unités de stockage nouvelles ou existantes à ce groupe.

À partir d' ONTAP 9.18.1, vous pouvez configurer la réserve de snapshots et la suppression automatique des snapshots pour limiter la quantité d'espace utilisée par les snapshots dans vos unités de stockage. Lorsque vous ajoutez une unité de stockage à un groupe de cohérence existant, la réserve d'instantanés et la suppression automatique des instantanés sont configurées comme suit par défaut.

Si vous ajoutez…	Le pourcentage de réserve pour les instantanés est fixé à…	La suppression automatique des instantanés est…
Nouveaux entrepôts	0	Désactivées
Unités de stockage existantes	Inchangé	Inchangé

Vous pouvez modifier les paramètres par défaut des nouvelles unités de stockage lors de leur création. Vous pouvez également"modifier les unités de stockage existantes" pour mettre à jour leurs paramètres actuels.

"Découvrez-en plus sur la réserve de snapshots sur les systèmes de stockage ASA r2".

Avant de commencer

Si vous exécutez ONTAP 9.16.1 et que le groupe de cohérence que vous souhaitez développer se trouve dans une relation de synchronisation active SnapMirror , vous devez"supprimer la relation de synchronisation active SnapMirror" avant de pouvoir ajouter des unités de stockage. Si vous exécutez ONTAP 9.16.1 et que le groupe de cohérence est dans une relation de réplication asynchrone, vous devez"rompre la relation" avant de pouvoir développer le groupe de cohérence. La suppression de la relation de synchronisation active SnapMirror ou la rupture de la relation asynchrone avant l'extension d'un groupe de cohérence n'est pas requise dans ONTAP 9.17.1 et les versions ultérieures.

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 sera 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**.

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

Retirez une unité de stockage d'un groupe de cohérence pour la supprimer, la gérer dans le cadre d'un autre groupe de cohérence ou cesser de protéger ses données. 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.

Supprimer les groupes de cohérence sur votre système ASA r2

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 précédemment présentes dans le groupe restent actives sur le cluster. Si le groupe de cohérence était dans une relation de réplication, les copies répliquées restent sur le cluster distant.

Avant de commencer

Si vous exécutez ONTAP 9.16.1 et que le groupe de cohérence que vous souhaitez supprimer se trouve dans une relation de synchronisation active SnapMirror , vous devez"supprimer la relation de synchronisation active SnapMirror" avant de supprimer le groupe de cohérence. La suppression de cette relation avant de modifier un groupe de cohérence n'est pas requise dans ONTAP 9.17.1 et les versions ultérieures.

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 groupes de cohérence hiérarchique sur votre système ASA r2

À partir d' ONTAP 9.16.1, vous pouvez utiliser System Manager pour créer des groupes de cohérence hiérarchiques sur votre système ASA r2. Dans une structure hiérarchique, un ou plusieurs groupes de cohérence sont configurés comme enfants sous un groupe de cohérence parent. Vous pouvez appliquer des stratégies de snapshot individuelles à chaque groupe de cohérence enfant et répliquer les snapshots de tous les groupes de cohérence enfant sur un cluster distant en tant qu'unité unique en répliquant le parent. Cela simplifie la protection et la gestion des données pour les structures de données complexes.

Promouvoir un groupe de cohérence existant en groupe de cohérence parent

Si vous promouvez un groupe de cohérence existant en parent, un nouveau groupe de cohérence enfant est créé et les unités de stockage appartenant au groupe de cohérence promu sont déplacées vers le nouveau groupe de cohérence enfant. Les unités de stockage ne peuvent pas être directement associées à un groupe de cohérence parent.

Avant de commencer

Si vous exécutez ONTAP 9.16.1 et que le groupe de cohérence que vous souhaitez promouvoir est dans une relation de synchronisation active SnapMirror , vous devez"supprimer la relation de synchronisation active SnapMirror" avant que le groupe de cohérence puisse être promu. Si vous exécutez ONTAP 9.16.1 et que le groupe de cohérence est dans une relation de réplication asynchrone, vous devez"rompre la relation" avant de pouvoir promouvoir le groupe de cohérence. La suppression de la relation de synchronisation active SnapMirror ou la rupture de la relation asynchrone avant la promotion d'un groupe de cohérence n'est pas requise dans ONTAP 9.17.1 et les versions ultérieures.

Étapes

1. Dans System Manager, sélectionnez **protection > groupes de cohérence**.
2. Placez le curseur de la souris sur le groupe de cohérence à convertir en groupe de cohérence parent.
3. Sélectionnez ⋮, puis **promouvoir vers le groupe de cohérence parent**.
4. Saisissez un nom pour le nouveau groupe de cohérence enfant ou acceptez le nom par défaut, puis sélectionnez le type de composant du groupe de cohérence.
5. Sélectionnez **promouvoir**.

Et la suite ?

Vous pouvez créer des groupes de cohérence enfants supplémentaires sous le groupe de cohérence parent. Vous pouvez également"configuration de la réplication snapshot" pour copier les groupes de cohérence parents et enfants vers un emplacement géographiquement distant à des fins de sauvegarde et de reprise après sinistre.

Rétrograder un groupe de cohérence parent en un seul groupe de cohérence

Lorsque vous rétrogradez un groupe de cohérence parent en un groupe de cohérence unique, les unités de stockage des groupes de cohérence enfants associés sont ajoutées au groupe de cohérence parent. Les groupes de cohérence enfants sont supprimés et le parent est alors géré comme un groupe de cohérence unique.

Avant de commencer

Si vous exécutez ONTAP 9.16.1 et que le groupe de cohérence que vous souhaitez rétrograder est dans une relation de synchronisation active SnapMirror , vous devez"supprimer la relation de synchronisation active SnapMirror" avant que le groupe de cohérence puisse être rétrogradé. Si vous exécutez ONTAP 9.16.1 et que le groupe de cohérence est dans une relation de réplication asynchrone, vous devez"rompre la relation" avant de pouvoir rétrograder le groupe de cohérence. La suppression de la relation de synchronisation active SnapMirror ou la rupture de la relation asynchrone avant l'extension d'un groupe de cohérence n'est pas requise dans ONTAP 9.17.1 et les versions ultérieures.

Étapes

1. Dans System Manager, sélectionnez **protection > groupes de cohérence**.
2. Placez le pointeur de la souris sur le groupe de cohérence parent à rétrograder.
3. Sélectionnez ⋮, puis **Rétrograder à un seul groupe de cohérence**.
4. Sélectionnez **Rétrograder**

Et la suite ?

"Ajouter une règle de snapshots" au groupe de cohérence rétrogradé afin de protéger les unités de stockage précédemment gérées par les groupes de cohérence enfant.

Créer un groupe de cohérence enfant

La création de groupes de cohérence enfants vous permet d'appliquer des stratégies d'instantanés individuelles à chaque enfant. À partir d' ONTAP 9.17.1, vous pouvez également appliquer des stratégies de réplication individuelles directement à chaque enfant. Dans ONTAP 9.16.1, les politiques de réplication ne peuvent être appliquées qu'au niveau parent.

Vous pouvez créer un groupe de cohérence enfant à partir d'un groupe de cohérence nouveau ou existant.

D'un nouveau 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 parent auquel vous souhaitez ajouter un groupe de cohérence enfant.
3. Sélectionnez ⋮, puis **Ajouter un nouveau groupe de cohérence enfant**.
4. Indiquez le nom du groupe de cohérence enfant ou acceptez le nom par défaut, puis sélectionnez le type de composant du groupe de cohérence.
5. Sélectionnez cette option pour ajouter des unités de stockage existantes au groupe de cohérence enfant ou pour créer de nouvelles unités de stockage.

   Si vous créez de nouvelles unités de stockage, entrez le nombre d'unités que vous souhaitez créer et la capacité par unité, puis entrez les informations sur l'hôte.

   Si vous créez plusieurs unités de stockage, 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**.

6. Sélectionnez **Ajouter**.

À partir d'un groupe de cohérence existant

Avant de commencer

Si le groupe de cohérence que vous souhaitez utiliser est déjà l'enfant d'un autre groupe de cohérence, vous devez"le détacher du groupe de cohérence parent existant" avant de pouvoir le déplacer vers un nouveau groupe de cohérence parent.

Étapes

1. Dans System Manager, sélectionnez **protection > groupes de cohérence**.
2. Sélectionnez le groupe de cohérence existant que vous souhaitez créer.
3. Sélectionnez ⋮, puis **déplacer sous un autre groupe de cohérence**.
4. Indiquez un nouveau nom pour le groupe de cohérence enfant ou acceptez le nom par défaut, puis sélectionnez le type de composant du groupe de cohérence.
5. Sélectionnez le groupe de cohérence existant que vous souhaitez créer le groupe de cohérence parent ou sélectionnez pour créer un nouveau groupe de cohérence parent.

   Si vous choisissez de créer un nouveau groupe de cohérence parent, indiquez le nom du groupe de cohérence parent ou acceptez le nom par défaut, puis sélectionnez le type de composant d'application de cohérence.

6. Sélectionnez **déplacer**.

Et la suite

Après avoir créé un groupe de cohérence enfant, vous pouvez"appliquez des règles de protection de snapshots individuelles" à chaque groupe de cohérence enfant. Vous pouvez également"configurer des politiques de réplication" sur les groupes de cohérence parents et enfants pour répliquer les groupes de cohérence vers un emplacement distant.

Détachez un groupe de cohérence enfant d'un groupe de cohérence parent

Lorsque vous détachez un groupe de cohérence enfant d'un groupe de cohérence parent, le groupe de cohérence enfant est supprimé du groupe de cohérence parent et est géré comme un groupe de cohérence unique. La politique de réplication appliquée au parent n'est plus appliquée au groupe de cohérence enfant détaché.

Avant de commencer

Si vous exécutez ONTAP 9.16.1 et que le groupe de cohérence que vous souhaitez détacher est dans une relation de synchronisation active SnapMirror , vous devez"supprimer la relation de synchronisation active SnapMirror" avant que le groupe de cohérence puisse être détaché. Si vous exécutez ONTAP 9.16.1 et que le groupe de cohérence est dans une relation de réplication asynchrone, vous devez"rompre la relation" avant de pouvoir détacher le groupe de cohérence. La suppression de la relation de synchronisation active SnapMirror ou la rupture de la relation asynchrone avant l'extension d'un groupe de cohérence n'est pas requise dans ONTAP 9.17.1 et les versions ultérieures.

Étapes

1. Dans System Manager, sélectionnez **protection > groupes de cohérence**.
2. Sélectionnez le groupe de cohérence parent.
3. Sélectionnez sur le groupe de cohérence enfant à détacher.
4. Sélectionnez ⋮; puis sélectionnez **détacher du parent**.
5. Indiquez le nouveau nom du groupe de cohérence que vous souhaitez détacher ou acceptez le nom par défaut, puis sélectionnez le type d'application du groupe de cohérence.
6. Sélectionnez **détacher**.

Et la suite ?

"Configuration d'une règle de réplication"pour répliquer les instantanés du groupe de cohérence enfant détaché vers un cluster distant.

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.

ⓘ Dans les systèmes ASA r2, les SED ne sont pris en charge que pour les SSD basés sur NVMe.

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.

Migrez les clés de chiffrement des données ONTAP entre les gestionnaires de clés de votre système ASA r2

Vous pouvez gérer vos clés de chiffrement des données à l'aide du gestionnaire de clés intégré ONTAP sur votre système ASA r2 ou d'un gestionnaire de clés externe (ou les deux). Les gestionnaires de clés externes ne peuvent être activés qu'au niveau des VM de stockage. Au niveau du cluster ONTAP, vous pouvez activer le gestionnaire de clés intégré ou un gestionnaire de clés externe.

Si vous activez votre gestionnaire de clés sur…	Vous pouvez utiliser…
Au niveau du cluster uniquement	Gestionnaire de clés intégré ou gestionnaire de clés externe
Niveau de machine virtuelle de stockage uniquement	Gestionnaire de clés externe uniquement

Si vous activez votre gestionnaire de clés sur…	Vous pouvez utiliser…
Le niveau de la machine virtuelle du cluster et du stockage	Une des combinaisons de gestionnaire de clés suivantes : • Option 1 Niveau cluster : gestionnaire de clés intégré Niveau de la machine virtuelle de stockage : Gestionnaire de clés externe • Option 2 Niveau cluster : gestionnaire de clés externe Niveau de la machine virtuelle de stockage : Gestionnaire de clés externe

Migration des clés entre les gestionnaires de clés au niveau du cluster ONTAP

Depuis la version ONTAP 9.16.1, vous pouvez utiliser l'interface de ligne de commande ONTAP pour migrer les clés entre les gestionnaires de clés au niveau du cluster.

De la carte intégrée à la carte externe

Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Créez une configuration de gestionnaire de clés externe inactive :

```
security key-manager external create-config
```

3. Passer au gestionnaire de clés externe :

```
security key-manager keystore enable -vserver <storage_vm_name>
-type KMIP
```

4. Supprimez la configuration du gestionnaire de clés intégré :

```
security key-manager keystore delete-config -vserver
<storage_vm_name> -type OKM
```

5. Définissez le niveau de privilège sur admin :

```
set -privilege admin
```

De l’externe à l’embarqué

Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Créez une configuration de gestionnaire de clés intégré inactive :

```
security key-manager onboard create-config
```

3. Activez la configuration du gestionnaire de clés intégré :

```
security key-manager keystore enable -vserver <storage_vm_name>
-type OKM
```

4. Supprimez la configuration du gestionnaire de clés externe

```
security key-manager keystore delete-config -vserver
<storage_vm_name> -type KMIP
```

5. Définissez le niveau de privilège sur admin :

```
set -privilege admin
```

Migration des clés entre les gestionnaires de clés au niveau du cluster ONTAP et des VM de stockage

Vous pouvez utiliser l'interface de ligne de commandes ONTAP pour migrer les clés entre le gestionnaire de clés au niveau du cluster et un gestionnaire de clés au niveau de la machine virtuelle de stockage.

Étapes

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Migration des clés :

```
security key-manager key migrate -from-vserver <storage_vm_name> -to
-vserver <storage_vm_name>
```

3. Définissez le niveau de privilège sur admin :

```
set -privilege admin
```

Protégez-vous contre les attaques par ransomware

Créez des instantanés inviolables pour vous protéger contre les attaques de 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".

Activez la protection autonome contre les ransomwares avec l'IA sur vos systèmes de stockage ASA r2

À partir d' ONTAP 9.17.1, vous pouvez utiliser la protection autonome contre les ransomwares avec intelligence artificielle (ARP/AI) pour protéger les données de votre système ASA r2. ARP/AI détecte rapidement les menaces potentielles de ransomware, crée automatiquement un instantané ARP pour protéger vos données et affiche un message d'avertissement dans le Gestionnaire système pour vous avertir de toute activité suspecte.

ARP améliore la cyber-résilience en adoptant un modèle d'apprentissage automatique pour l'analyse anti-ransomware qui détecte les formes de ransomware en constante évolution avec une précision de 98 % dans les environnements SAN. Le modèle d'apprentissage automatique d'ARP est pré-entraîné sur un vaste ensemble de fichiers, à la fois avant et après une attaque par ransomware simulée. Cet entraînement gourmand en ressources est effectué en dehors d'ONTAP, et le modèle pré-entraîné résultant de cet entraînement est inclus sur la boîte avec ONTAP. Ce modèle n'est pas accessible ni modifiable. ARP/AI est actif immédiatement après l'activation ; il n'y a pas "période d'apprentissage".

> Aucun système de détection ou de prévention des ransomwares ne peut complètement garantir la sécurité contre une attaque de ransomware. Bien qu'une attaque puisse passer inaperçue, ARP/AI agit comme une couche de défense supplémentaire importante si le logiciel antivirus ne parvient pas à détecter une intrusion.

Description de la tâche

- Le support ARP/AI est inclus avec le "Licence ONTAP One" .
- ARP/AI n'est pas pris en charge sur les unités de stockage protégées par SnapMirror active sync, SnapMirror synchrone ou SnapLock.
- À partir de ONTAP 9.18.1, ARP/AI est activé par défaut sur toutes les nouvelles unités de stockage créées 12 heures après la mise à niveau vers ONTAP 9.18.1 ou l'initialisation d'un nouveau cluster ONTAP 9.18.1

ASA r2.

- Après avoir activé ARP/AI, vous devez "activer les mises à jour automatiques de vos fichiers de sécurité" pour recevoir automatiquement les nouvelles mises à jour de sécurité.

Activez ARP/AI sur toutes les unités de stockage du cluster

Si vous utilisez ONTAP 9.17.1, vous pouvez activer ARP/AI sur toutes les unités de stockage créées dans le cluster par défaut.

Dans ONTAP 9.18.1 et versions ultérieures, ARP/AI est activé par défaut sur toutes les nouvelles unités de stockage. Si vous avez des unités de stockage créées dans ONTAP 9.17.1 pour lesquelles ARP/AI n'est pas activé, vous pouvez l'activer manuellement.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. À côté de **Anti-ransomware**, sélectionnez ⋮ puis sélectionnez **Activer sur toutes les unités de stockage existantes**.
3. Sélectionnez **Activer**.

Activez ARP/AI sur toutes les unités de stockage d'une machine virtuelle de stockage.

Si vous utilisez ONTAP 9.17.1, vous pouvez activer ARP/AI par défaut sur toutes les unités de stockage créées dans une storage virtual machine (VM). Cela signifie que toute nouvelle unité de stockage créée dans la storage VM aura ARP/AI activé automatiquement. Vous pouvez également appliquer ARP/AI aux unités de stockage existantes dans la storage VM.

Dans ONTAP 9.18.1 et versions ultérieures, ARP/AI est activé par défaut sur toutes les nouvelles unités de stockage. Si vous avez des unités de stockage créées dans ONTAP 9.17.1 pour lesquelles ARP/AI n'est pas activé, vous pouvez l'activer manuellement.

Étapes

1. Dans le Gestionnaire système, sélectionnez **Cluster > Machines virtuelles de stockage**.
2. Sélectionnez la machine virtuelle de stockage sur laquelle vous souhaitez activer ARP/AI.
3. Dans la section **Sécurité**, à côté de **Anti-ransomware**, sélectionnez ⋮ ; puis sélectionnez **Modifier les paramètres anti-ransomware**.
4. Sélectionnez **Activer l'anti-ransomware**.

   Cela active ARP/AI sur toutes les futures unités de stockage créées sur la machine virtuelle de stockage sélectionnée par défaut.

5. Pour appliquer ARP aux unités de stockage existantes sur la machine virtuelle de stockage sélectionnée, sélectionnez **Appliquer cette modification à toutes les unités de stockage existantes applicables sur cette machine virtuelle de stockage**.
6. Sélectionnez **Enregistrer**.

Résultat

Toutes les nouvelles unités de stockage que vous créez sur la machine virtuelle de stockage sont protégées par défaut contre les attaques de ransomware, et toute activité suspecte vous est signalée dans le Gestionnaire système.

Activer ARP/AI sur des unités de stockage spécifiques dans une machine virtuelle de stockage

Si vous utilisez ONTAP 9.17.1 et que vous ne souhaitez pas activer ARP/AI sur toutes les unités de stockage dans une storage VM, vous pouvez sélectionner les unités spécifiques que vous souhaitez activer.

Dans ONTAP 9.18.1 et versions ultérieures, ARP/AI est activé par défaut sur toutes les nouvelles unités de stockage. Si vous avez des unités de stockage créées dans ONTAP 9.17.1 pour lesquelles ARP/AI n'est pas activé, vous pouvez l'activer manuellement.

Étapes

1. Dans System Manager, sélectionnez **Storage**.
2. Sélectionnez les unités de stockage pour lesquelles vous souhaitez activer ARP/AI.
3. Sélectionner ⋮ ; puis sélectionnez **Activer l'anti-ransomware**.
4. Sélectionnez **Activer**.

Résultat

Les unités de stockage que vous avez sélectionnées sont protégées contre les attaques de ransomware et toute activité suspecte vous est signalée dans le Gestionnaire système.

Désactivez la protection autonome par défaut contre les ransomwares sur vos systèmes de stockage ASA r2

Lorsque vous initialisez un nouveau cluster ONTAP 9.18.1 ASA r2 ou que vous mettez à niveau votre cluster vers ONTAP 9.18.1, ARP/AI est automatiquement activé par défaut sur toutes les nouvelles unités de stockage après un délai de grâce de 12 heures. Si vous ne désactivez pas ARP/AI pendant le délai de grâce, il est activé pour l'ensemble du cluster pour les nouvelles unités de stockage à la fin du délai de grâce.

Les unités de stockage créées dans ONTAP 9.17.1 doivent être "activé manuellement" pour ARP/AI.

Étapes

Vous pouvez désactiver l'activation par défaut pendant ou après le délai de grâce initial de 12 heures.

System Manager

1. Sélectionnez **Cluster > Paramètres**.
2. Désactiver ARP:
   - Pour désactiver pendant le délai de grâce de 12 heures :
     i. Sous **Anti-ransomware**, sélectionnez **Ne pas activer** puis sélectionnez **Désactiver**.
   - Pour désactiver après le délai de grâce de 12 heures :
     i. Sous **Anti-ransomware**, sélectionnez puis désélectionnez **Enable for new storage units**.
     ii. Sélectionnez **Save**

CLI

1. Vérifiez l'état d'activation par défaut :

```
security anti-ransomware auto-enable show
```

2. Désactiver l'activation par défaut pour les volumes existants et nouveaux :

```
security anti-ransomware auto-enable modify -default-existing-volume
-state false -default-new-volume-state false
```

Modifier les périodes de conservation des snapshots ARP/AI sur les systèmes de stockage ASA r2

Si la protection autonome contre les ransomwares avec intelligence artificielle (ARP/IA) détecte une activité anormale sur une ou plusieurs unités de stockage de votre système ASA r2, elle crée automatiquement un snapshot ARP pour protéger les données de l'unité. En fonction de votre capacité de stockage et des besoins de votre entreprise en matière de données, vous pouvez augmenter ou réduire la période de conservation par défaut du snapshot ARP. Par exemple, vous pouvez augmenter la période de conservation des applications critiques afin de bénéficier, si nécessaire, de périodes de conservation plus longues pour la récupération des données, ou réduire celle des applications non critiques pour économiser de l'espace de stockage.

La période de conservation par défaut de l'instantané ARP varie en fonction de l'action que vous entreprenez en réponse à l'activité anormale.

Si vous effectuez cette action…	Les instantanés ARP sont conservés par défaut pendant…
Marquer comme faux positif	12 heures
Marquer comme attaque potentielle par ransomware	7 jours
Ne prenez pas de mesures immédiates	10 jours

Les périodes de conservation par défaut peuvent être modifiées à l'aide de l'interface de ligne de commande (CLI) ONTAP . Voir "Modifier les options pour les instantanés automatiques ONTAP" pour connaître les étapes à suivre pour modifier la période de conservation par défaut.

Répondez à la protection autonome contre les ransomwares avec des alertes IA sur les systèmes de stockage ASA r2

Si la protection autonome contre les ransomwares avec intelligence artificielle (ARP/IA) détecte une activité anormale sur une ou plusieurs unités de stockage de votre système ASA r2, un avertissement s'affiche sur le tableau de bord du Gestionnaire système. Consultez l'avertissement, vérifiez l'activité et, si nécessaire, prenez les mesures nécessaires pour contrer toute menace potentielle pesant sur vos données.

Si un message d'avertissement ARP/AI s'affiche, avant d'agir, utilisez le vérificateur d'intégrité des applications approprié pour vérifier l'intégrité des données sur l'unité de stockage. Vérifier l'intégrité des données de l'unité de stockage vous permet de déterminer si l'activité est acceptable ou s'il s'agit d'une attaque potentielle par rançongiciel.

Si l'activité anormale est…	Alors fais ceci…
Acceptable	Marquer l'activité comme un faux positif.
Une attaque potentielle de ransomware	Marquez l'activité comme une attaque potentielle de ransomware.
Indéterminé	N'agissez pas immédiatement. Surveillez l'unité de stockage pendant 7 jours maximum. Si l'unité de stockage continue de fonctionner normalement, signalez l'activité comme un faux positif. Si l'unité de stockage continue de présenter une activité anormale, signalez-la comme une attaque potentielle par rançongiciel.

Étapes

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

   Si ARP a détecté une activité anormale sur une ou plusieurs unités de stockage, un message apparaît sous **Avertissements**.

2. Sélectionnez le message d'avertissement.
3. Sous **Aperçu des événements**, sélectionnez le message **Avertissements** qui indique le nombre d'unités de stockage présentant une activité anormale.
4. Sous **Unités de stockage avec activité anormale**, sélectionnez l'unité de stockage.
5. Sélectionnez **Sécurité**.

   S'il y a une activité anormale sur l'unité de stockage, un message s'affiche sous **Anti-ransomware**.

6. Sélectionnez **Choisir une action**.
7. Sélectionnez **Marquer comme faux positif** ou sélectionnez **Marquer comme attaque potentielle par ransomware**.

Et la suite ?

Si vous constatez des pics d'activité dans votre unité de stockage, qu'il s'agisse de pics ponctuels ou d'une augmentation caractéristique d'une nouvelle norme, vous devez les signaler comme étant sans danger. Le signalement manuel de ces pics comme étant sans danger contribue à améliorer la précision des évaluations des menaces d'ARP. Découvrez comment "signaler les pics connus d'ARP/IA".

Suspendez ou reprenez la protection autonome contre les ransomwares avec l'IA sur vos systèmes de stockage ASA r2

À partir d' ONTAP 9.17.1, vous pouvez utiliser la protection autonome contre les ransomwares avec intelligence artificielle (ARP/AI) pour protéger les données de votre système ASA r2. Si vous prévoyez un événement de charge de travail inhabituel, vous pouvez suspendre temporairement l'analyse ARP/AI afin d'éviter les détections de faux positifs d'attaques de ransomware. Une fois l'événement de charge de travail terminé, vous pouvez reprendre l'analyse ARP/AI.

Mettre en pause ARP/AI

Avant de commencer un événement de charge de travail inhabituel, vous devrez peut-être suspendre temporairement l'analyse ARP/AI pour éviter les détections faussement positives d'attaques de ransomware.

Étapes

1. Dans System Manager, sélectionnez **Storage**.
2. Sélectionnez les unités de stockage pour lesquelles vous souhaitez suspendre ARP/AI.
3. Sélectionnez **Pause anti-ransomware**.

Résultat

L'analyse ARP/AI est suspendue pour les unités de stockage sélectionnées et aucune activité suspecte ne vous est signalée dans le Gestionnaire système jusqu'à ce que vous repreniez ARP/AI.

Reprendre ARP/AI

Si vous suspendez ARP/AI pendant une charge de travail inhabituelle, une fois votre charge de travail terminée, vous devez la reprendre pour protéger vos données contre les attaques de ransomware.

Étapes

1. Dans System Manager, sélectionnez **Storage**.
2. Sélectionnez les unités de stockage pour lesquelles vous souhaitez reprendre ARP/AI.
3. Sélectionnez **Reprendre l'anti-ransomware**.

Résultat

L'analyse des attaques potentielles de ransomware reprend et les activités suspectes vous sont signalées dans le Gestionnaire système.

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.

Sécurisez les connexions IP sur vos systèmes de stockage ASA r2

Si vous utilisez le protocole IP sur votre système ASA r2, vous pouvez configurer la sécurité IP (IPsec) pour améliorer la sécurité de vos données. IPSec est une norme Internet qui fournit un chiffrement des données à la volée, une authentification pour le trafic circulant entre les terminaux réseau au niveau IP et une protection contre les attaques par réexécution et les attaques de l'homme du milieu malveillantes sur vos données.

Pour les systèmes ASA r2, IPSec est disponible pour les hôtes iSCSI et NVMe/TCP.

Sur certains systèmes ASA r2, plusieurs opérations cryptographiques, telles que le cryptage et les contrôles d'intégrité, peuvent être déchargées sur une carte réseau (NIC) prise en charge. Le débit pour les opérations déchargées sur la carte NIC est d'environ 5 % ou moins. Cela peut considérablement améliorer les performances et le débit du trafic réseau protégé par IPsec.

À partir d' ONTAP 9.18.1, le déchargement matériel IPsec pris en charge est étendu au trafic IPv6.

Les cartes réseau suivantes sont prises en charge pour le déchargement matériel sur les systèmes ASA r2 et les versions ONTAP suivants :

Carte réseau prise en charge	Systèmes ASA r2	Version ONTAP
X50135A (contrôleur Ethernet 2p, 40G/100G)	• ASA A1K • ASA A90 • ASA A70	ONTAP 9.17.1 et versions ultérieures

Carte réseau prise en charge	Systèmes ASA r2	Version ONTAP
X60135A (contrôleur Ethernet 2p, 40G/100G)	• ASA A50 • ASA A30 • ASA A20	ONTAP 9.17.1 et versions ultérieures
X50131A - (contrôleur Ethernet 2p, 40G/100G/200G/400G)	• ASA A1K • ASA A90 • ASA A70	ONTAP 9.16.1 et versions ultérieures
X60132A - (contrôleur Ethernet 4p, 10G/25G)	• ASA A50 • ASA A30 • ASA A20	ONTAP 9.16.1 et versions ultérieures

Voir le"NetApp Hardware Universe" pour plus d'informations sur les systèmes et cartes compatibles.

Et la suite ?

La configuration d'IPsec sur votre système ASA r2 est identique à celle des autres systèmes ONTAP . Pour plus d'informations, voir "Préparez-vous à configurer la sécurité IP pour le réseau ONTAP".

Administration et contrôle

Mettre à niveau et rétablir ONTAP

Mise à niveau de ONTAP sur les systèmes de stockage ASA r2

Lorsque vous mettez à niveau votre logiciel ONTAP sur votre système ASA r2, vous pouvez bénéficier des nouvelles fonctionnalités ONTAP améliorées pour réduire les coûts, accélérer les charges de travail stratégiques, améliorer la sécurité et étendre la portée de la protection des données disponible pour votre entreprise.

Les mises à niveau du logiciel ONTAP pour les systèmes ASA r2 suivent le même processus que pour les autres systèmes ONTAP. Si vous avez un contrat SupportEdge actif pour le conseiller numérique Active IQ (également appelé conseiller numérique), vous devez "Préparez la mise à niveau avec Upgrade Advisor". Upgrade Advisor fournit des informations intelligentes qui vous aident à minimiser l'incertitude et les risques en évaluant votre cluster et en créant un plan de mise à niveau propre à votre configuration. Si vous n'avez pas de contrat SupportEdge actif pour le conseiller numérique Active IQ, vous devez "Préparez la mise à niveau sans Upgrade Advisor".

Après avoir préparé votre mise à niveau, il est recommandé d'effectuer les mises à niveau à l'aide de "Mise à niveau automatisée sans interruption (ANDU) depuis System Manager". ANDU exploite la technologie de basculement haute disponibilité d'ONTAP pour assurer le service des données sans interruption lors de la mise à niveau.

En savoir plus sur "Mises à niveau du logiciel ONTAP".

Rétablir ONTAP sur les systèmes de stockage ASA r2

Les restaurations du logiciel ONTAP pour les systèmes ASA r2 suivent le même processus que les restaurations pour les autres systèmes ONTAP .

La restauration d'un cluster ONTAP est perturbatrice. Vous devez mettre le cluster hors ligne pendant toute la durée de la restauration. Vous ne devez pas restaurer un cluster de production sans l'aide du support technique. Vous pouvez restaurer un nouveau cluster ou un cluster de test sans assistance. Si la restauration d'un nouveau système ou d'un cluster de test échoue ou réussit, mais que vous n'êtes pas satisfait des performances du cluster dans votre environnement de production, contactez le support technique pour obtenir de l'aide.

"Rétablir un cluster ONTAP" .

Rétablir les exigences pour les systèmes ASA r2

Certaines configurations de cluster ASA r2 nécessitent que vous preniez des mesures spécifiques avant de commencer une restauration du logiciel ONTAP .

Retour à ONTAP 9.17.1

Si vous revenez à ONTAP 9.17.1 sur un système ASA r2, vous devez effectuer les actions suivantes avant de commencer la restauration :

"équilibrage dynamique de l'espace"est activé par défaut 14 jours après la mise à niveau vers ONTAP 9.17.1 ou l'initialisation d'un nouveau cluster ONTAP 9.17.1 ASA r2. Vous ne pouvez pas revenir à la version ONTAP 9.17.1 sur votre système ASA r2 après l'activation de l'équilibrage dynamique de l'espace.

Si vous avez…	Avant de revenir en arrière, vous devriez…
Groupes de cohérence hiérarchique dans une relation de synchronisation active SnapMirror	"Supprimer la relation de synchronisation active SnapMirror".
Relations d'importation actives	Supprimez les relations d'importation actives. "Découvrez les relations d'importation".
Protection anti-ransomware activée	"Suspendre la protection anti-ransomware".

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. Sous **Mises à jour logicielles**, sélectionnez **Activer**.
3. Lisez le CLUF.
4. Acceptez les paramètres par défaut pour **Afficher la notification** des mises à jour recommandées. Vous pouvez également choisir de **Mettre à jour automatiquement** ou de **Rejeter 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 uniquement si vous souhaitez gérer entièrement les mises à jour vous-même. Avec les mises à jour automatiques désactivées, le système ne vous notifiera pas, ne téléchargera pas et n'installera pas de mises à jour. Vous êtes responsable de surveiller, télécharger, planifier

et installer toutes les mises à jour manuellement.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Paramètres**.
2. Sous **Mises à jour logicielles**, sélectionnez **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. À côté de **Mises à jour logicielles**, sélectionnez → , puis sélectionnez **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. À côté de **Mises à jour logicielles**, sélectionnez → , puis sélectionnez **Toutes les autres mises à jour**.
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 le Gestionnaire système, sélectionnez **Cluster > Présentation**, puis sélectionnez **Toutes les autres mises à jour**.
3. Sous **Mises à jour manuelles**, sélectionnez **Ajouter des fichiers de micrologiciel** ; puis sélectionnez **Télécharger depuis le serveur** ou **Télécharger depuis le client local**.

4. Installez le fichier de mise à jour du firmware.

Résultat

Votre micrologiciel est mis à jour.

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 une machine virtuelle de stockage

Lors de la configuration des clusters, votre machine virtuelle de stockage de données par défaut est créée. Toutes les nouvelles unités de stockage sont créées à l'intérieur de votre VM de stockage de données par défaut, sauf si vous créez et sélectionnez une autre VM de stockage. Vous pouvez créer une VM de stockage supplémentaire pour séparer vos unités de stockage pour différentes applications, différents services ou clients. Par exemple, vous pouvez créer une VM de stockage pour votre environnement de développement et une autre VM de stockage pour votre environnement de production, ou bien créer une VM de stockage pour votre département financier et une autre VM de stockage pour votre département marketing.

Étapes

1. Sélectionnez **Cluster > VM de stockage**.
2. Sélectionnez + Add.
3. Entrez un nom pour la machine virtuelle de stockage ou acceptez le nom par défaut.
4. Sous **configurer les protocoles**, sélectionnez les protocoles pour la machine virtuelle de stockage.

   Sélectionnez **IP** pour iSCSI et NVMe/TCP. Sélectionnez **FC** pour Fibre Channel ou NVMe/FC.

5. Sous **Storage VM administration**, sélectionnez **Manage Administrator account**, puis entrez le nom d'utilisateur et le mot de passe du compte administrateur.
6. Ajouter une interface réseau pour la VM de stockage
7. Sélectionnez **Enregistrer**.

Et la suite ?

Vous avez créé une VM de stockage. Vous pouvez maintenant utiliser la machine virtuelle de stockage pour "provisionner le stockage".

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.

Sur un système ASA r2, vous pouvez créer des LIF IP, FC et NVMe/FC. Une LIF de données IP 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.

Si vous souhaitez activer le basculement automatique de LIF iSCSI, vous devez créer une LIF IP pour le trafic iSCSI uniquement. Lorsque le basculement automatique de LIF iSCSI est activé, en cas de basculement du stockage, la LIF iSCSI IP est automatiquement migrée de son nœud ou port de rattachement vers son nœud ou port partenaire haute disponibilité, puis de nouveau une fois le basculement terminé. Ou, si le port d'une LIF iSCSI IP est défectueux, la LIF est automatiquement migrée vers un port sain de son nœud de rattachement actuel, puis revient sur son port d'origine une fois le port refonctionnel.

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 

.
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.

Et la suite ?

Vous pouvez utiliser l'interface de ligne de commande (CLI) ONTAP pour créer un LIF iSCSI uniquement avec basculement automatique.

Créer une stratégie de service LIF iSCSI uniquement personnalisée

Si vous souhaitez créer des LIF iSCSI uniquement avec basculement LIF automatique, vous devez d'abord créer une stratégie de service LIF iSCSI uniquement personnalisée.

Vous devez utiliser l'interface de ligne de commande (CLI) ONTAP pour créer la stratégie de service personnalisée.

Étape

1. Définissez le niveau de privilège sur avancé :

```
set -privilege advanced
```

2. Créer une stratégie de service LIF iSCSI uniquement personnalisée :

```
network interface service-policy create -vserver <storage_VM_name>
-policy <service_policy_name> -services data-core,data-iscsi
```

3. Vérifiez que la politique de service a été créée :

```
network interface service-policy show -policy <service_policy_name>
```

4. Renvoyer le niveau de privilège à l'administrateur :

```
set -privilege admin
```

Créer des LIF uniquement iSCSI avec basculement automatique des LIF

Si des LIF iSCSI présentes sur la VM de stockage ne sont pas activées pour le basculement automatique des LIF, vos LIF nouvellement créées ne seront pas non plus activées pour le basculement automatique des LIF. Si le basculement automatique des LIF n'est pas activé et qu'un événement de basculement se produit, vos LIF iSCSI ne migreront pas.

Avant de commencer

Vous devez avoir créé une stratégie de service LIF iSCSI uniquement personnalisée.

Étapes

1. Créez des LIF uniquement iSCSI avec basculement automatique des LIF :

```
network interface create -vserver <storage_VM_name> -lif
<iscsi_lif_name> -service-policy <service_policy_name> -home-node
<home_node> -home-port <port_name> -address <ip_address> -netmask
<netmask> -failover-policy sfo-partner-only -status-admin up
```

   - Il est recommandé de créer deux LIF iSCSI sur chaque nœud, un pour la structure A et l'autre pour la structure B. Cela assure la redondance et l'équilibrage de charge de votre trafic iSCSI. Dans l'exemple suivant, quatre LIF iSCSI sont créés : deux sur chaque nœud et un pour chaque structure.

```
network interface create -vserver svm1 -lif iscsi-lif-01a -service
-policy custom-data-iscsi -home-node node1 -home-port e2b -address
<node01-iscsi-a-ip> -netmask 255.255.255.0 -failover-policy sfo-
partner-only -status-admin up

network interface create -vserver svm1 -lif iscsi-lif-01b -service
-policy custom-data-iscsi -home-node node1 -home-port e4b -address
<node01-iscsi-b-ip> -netmask 255.255.255.0 -failover-policy sfo-
partner-only -status-admin up

network interface create -vserver svm1 -lif iscsi-lif-02a -service
-policy custom-data-iscsi -home-node node2 -home-port e2b -address
<node02-iscsi-a-ip> -netmask 255.255.255.0 -failover-policy sfo-
partner-only -status-admin up

network interface create -vserver svm1 -lif iscsi-lif-02b -service
-policy custom-data-iscsi -home-node node2 -home-port e4b -address
<node02-iscsi-b-ip> -netmask 255.255.255.0 -failover-policy sfo-
partner-only -status-admin up
```

- Si vous utilisez des VLAN, ajustez le `home-port` paramètre pour inclure les informations de port VLAN pour la structure iSCSI respective, par exemple, `-home-port e2b-<iSCSI-A-VLAN>` pour la structure iSCSI A et `-home-port e4b-<iSCSI-B-VLAN>` .
- Si vous utilisez des groupes d'interfaces (ifgroups) avec des VLAN, ajustez le `home-port` paramètre pour inclure le port VLAN approprié, par exemple, `-home-port a0a-<iSCSI-A-VLAN>` pour la structure iSCSI A et `-home-port a0a-<iSCSI-B-VLAN>` pour la structure iSCSI B où `a0a` est le ifgroup et a0a-<iSCSI-A-VLAN> et a0a-<iSCSI-B-VLAN> sont les ports VLAN respectifs pour la structure iSCSI A et la structure iSCSI B.

2. Vérifiez que les LIF iSCSI ont été créés :

```
network interface show -lif iscsi*
```

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.

Description de la tâche

ONTAP utilise le protocole NTP (Network Time Protocol) pour synchroniser l'heure sur le cluster. Après avoir modifié les adresses IP LIF, vous devrez peut-être mettre à jour la configuration NTP pour éviter les échecs de synchronisation. Pour plus d'informations, reportez-vous à l'article de la base de connaissances"La synchronisation NTP échoue après le changement d'IP 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 remarquez 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 la zone de disponibilité du stockage

Chaque paire haute disponibilité d'un système ASA r2 utilise un pool de stockage commun appelé *zone de disponibilité du stockage*. La zone de disponibilité du stockage a accès à tous les disques disponibles dans le système de stockage et est visible pour les deux nœuds de la paire haute disponibilité.

Si votre cluster comporte 4 nœuds ou plus, vous pouvez afficher la quantité d'espace utilisée par la zone de disponibilité du stockage pour chaque paire haute disponibilité. Cette métrique n'est pas disponible pour les clusters à 2 nœuds.

Étapes

1. Dans System Manager, sélectionnez **Cluster**, puis **Présentation**.

   Un récapitulatif de l'utilisation de la zone de disponibilité du stockage s'affiche pour chaque paire HA dans le cluster.

2. Si vous souhaitez obtenir des mesures plus détaillées, sélectionnez une disponibilité spécifique du stockage.

   Sous **vue d'ensemble**, la capacité de la zone de disponibilité du stockage, la quantité d'espace utilisé et le

taux de réduction des données sont affichés.

Sous **unités de stockage**, une liste de toutes les unités de stockage de la zone de disponibilité de stockage s'affiche.

Et la suite ?

Si le niveau d'espace de votre zone de disponibilité du stockage est faible, envisagez "déplacer les unités de stockage"d'utiliser une autre zone de disponibilité du stockage pour équilibrer l'utilisation du stockage dans le cluster.

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 une étagère, utilisez NetApp Hardware Universe pour vérifier que le disque que vous souhaitez ajouter est pris en charge par votre système ASA r2 et pour identifier l'emplacement approprié pour le nouveau disque. Les emplacements appropriés pour l'ajout de disques varient en fonction du modèle du système et de la version ONTAP . Dans certains cas, il est nécessaire d'ajouter les disques 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 système 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 cadre de la face avant du système.
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.

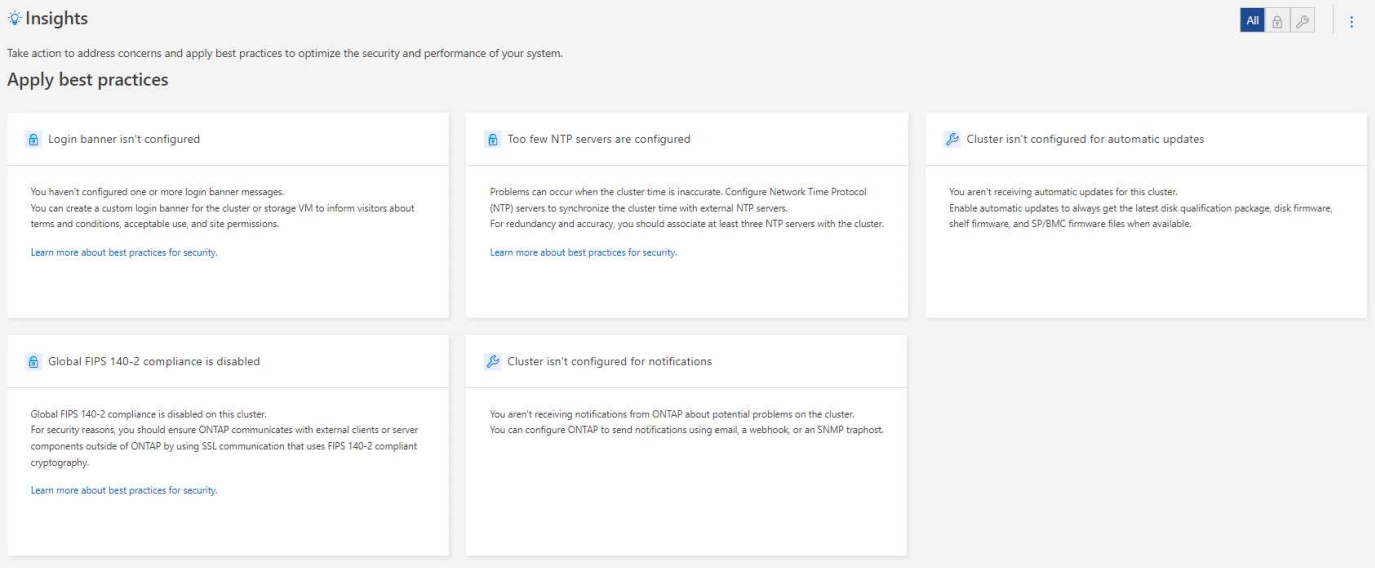
Et la suite ?

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

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.
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

Ajoutez des nœuds ASA r2 à un cluster ONTAP

À partir d' ONTAP 9.16.1, les systèmes de stockage ASA r2 prennent en charge jusqu'à 12 nœuds par cluster. Une fois les nouveaux nœuds d'une paire HA câblés et mis sous tension, vous devez les joindre au cluster.

Avant de commencer

Rassemblez les informations suivantes :

- Adresse IP du nœud
- Adresse IP de l'interface réseau intercluster
- Le masque de sous-réseau intercluster
- La passerelle réseau intercluster
- Pour configurer le gestionnaire de clés intégré OKM, vous devez disposer de la phrase de passe OKM.

Étapes

1. Dans System Manager, sélectionnez **Cluster > Présentation**.
2. Sélectionnez ⋮ en regard du nœud que vous souhaitez joindre au cluster, puis sélectionnez **Ajouter un nœud**
3. Entrez l'adresse IP de chaque nœud.
4. Indiquez l'adresse IP, le masque de sous-réseau et la passerelle de l'interface réseau intercluster.
5. Si vous souhaitez configurer le gestionnaire de clés intégré OKM, entrez la phrase de passe OKM.

   Configurer le gestionnaire de clés intégré pour le chiffrement est sélectionné par défaut.

6. Sélectionnez **Ajouter**.

Résultat

La nouvelle paire haute disponibilité est jointe au cluster.

Et la suite ?

Une fois que vous avez ajouté la nouvelle paire haute disponibilité au cluster, vous pouvez "Activez l'accès aux données à partir de vos hôtes SAN" accéder à vos nouveaux 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 "Documentation de maintenance de ASA r2" 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 pour les environnements SAN uniquement, construits sur des solutions 100 % flash. ASA se distinguent des autres systèmes ONTAP (ASA, AFF et FAS) par la mise en œuvre de leur personnalité ONTAP , de leur couche de stockage et des protocoles pris en charge.

Les éléments suivants sont classés comme systèmes ASA r2 :

- ASA A1K
- ASA A90
- ASA A70
- ASA A50
- ASA A30
- ASA A20
- ASA C30

Différences de personnalité

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 exécuté sur des systèmes ASA est identifié comme *ASA ONTAP Personality*. ONTAP exécuté sur des systèmes AFF et FAS ONTAP 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**.
- Depuis la CLI, entrez : `system node show -personality -is-disaggregated`

Pour les systèmes ASA r2, la *personnalité* est *ASA r2* et le statut *is-disaggregated* est *true*.

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

Différences entre les couches de stockage

Les systèmes ASA r2 utilisent une couche de stockage simplifiée qui est différente de la couche de stockage utilisée par les systèmes FAS, AFF et ASA .

Systèmes FAS, AFF et ASA

La couche de stockage des systèmes FAS, AFF et ASA utilise les agrégats comme unité de base. Un agrégat possède un ensemble spécifique de disques disponibles dans un système de stockage. Il alloue l'espace sur les disques qu'il possède aux volumes pour les LUN et les espaces de noms. Avec ces systèmes, les utilisateurs ONTAP peuvent créer et modifier des agrégats, des volumes, des LUN et des espaces de noms.

Systèmes ASA r2

Au lieu d'agrégats, la couche de stockage des systèmes ASA r2 utilise des zones de disponibilité de stockage. Une zone de disponibilité de stockage est un pool commun de stockage accessible aux deux nœuds d'une même paire HA. Les deux nœuds de la paire HA ont accès à tous les disques disponibles dans leur zone de disponibilité de stockage partagée. Par exemple, dans un cluster ONTAP ASA r2 à deux nœuds, il existe une zone de disponibilité de stockage, accessible aux deux nœuds du cluster. Dans un cluster ONTAP ASA r2 à quatre nœuds, il existe deux zones de disponibilité de stockage. Chaque paire HA du cluster a accès à l'une des zones de disponibilité de stockage.

Lorsqu'une unité de stockage (basée sur un LUN ou un espace de noms NVMe) est créée, ONTAP crée automatiquement un volume dans la zone de disponibilité de stockage appropriée pour l'héberger. Le volume nouvellement créé est automatiquement placé dans la zone de disponibilité de stockage pour des performances optimales et une utilisation équilibrée de la capacité. L'utilisation de la capacité est équilibrée au sein de la zone de disponibilité du stockage en fonction de votre version d' ONTAP. "Découvrez comment équilibrer la capacité dans un cluster ASA r2".

Résumé des différences du système ASA r2

Les systèmes ASA r2 diffèrent des systèmes FAS, AFF et ASA des manières suivantes :

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

En raison de cette approche automatisée et simplifiée de la gestion du stockage, certaines options de System Manager, commandes ONTAP et points de terminaison de l'API REST ne sont pas disponibles ou ont une utilisation limitée sur un système ASA r2. Par exemple, la création et la gestion des volumes étant automatisées pour les systèmes ASA r2, le menu « Volumes » n'apparaît pas dans System Manager et le `volume create` la commande n'est pas prise en charge. "En savoir plus sur les commandes ASA r2 non prises en charge" .

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 VM de stockage par défaut avec services de protocole

Les nouveaux clusters contiennent automatiquement une machine virtuelle (VM) de stockage de données par défaut avec les protocoles SAN activés. Les interfaces logiques de données IP prennent en charge les protocoles iSCSI et NVMe/TCP et utilisent le `default-data-blocks` politique 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 sont toujours à provisionnement fin sur les systèmes de stockage ASA r2. Le provisionnement lourd n'est pas pris en charge.

Modifications de la compression des données

L'efficacité du stockage sensible à la température n'est pas appliquée aux systèmes ASA r2. Sur les systèmes ASA r2, la compression n'est pas basée sur des données *hot* (fréquemment utilisées) ou *Cold* (rarement consultées). La compression commence sans attendre que les données soient inactives.

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 .

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 automatique de LIF iSCSI par défaut

  Sur les systèmes ASA r2, la LIF réseau par défaut est partagée entre les hôtes NVMe et SCSI, de sorte que le basculement automatique ne soit pas pris en charge. Pour activer le basculement automatique de LIF iSCSI, vous devez "Créez une LIF iSCSI uniquement". Le basculement automatique est activé par défaut sur les LIF iSCSI uniquement.

  Lorsque le basculement automatique de LIF iSCSI est activé, si un basculement du stockage se produit, la LIF iSCSI est automatiquement migrée de son nœud ou port de rattachement vers son nœud ou port partenaire haute disponibilité, puis de nouveau une fois le basculement terminé. Ou, si le port d'une LIF iSCSI est défectueux, la LIF est automatiquement migrée vers un port sain de son nœud de rattachement actuel, puis revient sur son port d'origine une fois le port refonctionnel.

- FabricPool
- Provisionnement lourd des LUN

- MetroCluster
- Protocoles d'objet
- API ONTAP S3 SnapMirror et S3

Les systèmes ASA r2 prennent en charge les éléments suivants :

- SnapLock

  "Découvrez comment verrouiller des instantanés" Sur votre système ASA r2.

- Chiffrement double couche

  "Découvrez comment appliquer le chiffrement double couche" Aux données de votre système ASA r2.

Prise en charge de la réplication SnapMirror

La réplication SnapMirror est prise en charge sur les systèmes ASA r2 avec les limitations suivantes :

- La réplication synchrone SnapMirror n'est pas prise en charge.
- La synchronisation active SnapMirror est prise en charge uniquement entre deux systèmes ASA r2.

  En savoir plus sur"Synchronisation active SnapMirror sur les systèmes ASA r2" .

- La réplication asynchrone SnapMirror est prise en charge uniquement entre deux systèmes ASA r2. La réplication asynchrone SnapMirror n'est pas prise en charge entre un système ASA r2 et un système ASA, AFF ou FAS ou le cloud.

  En savoir plus sur"Les politiques de réplication SnapMirror sont prises en charge sur les systèmes ASA r2." .

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.

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

Au lieu d'agrégats, la couche de stockage des systèmes ASA r2 utilise des zones de disponibilité de stockage. Une zone de disponibilité de stockage est un pool commun de stockage accessible à une seule paire HA. Les deux nœuds de la paire HA ont accès à tous les disques disponibles dans leur zone de disponibilité de stockage partagée. Lorsqu'une unité de stockage (LUN ou espace de noms NVMe) est créée, ONTAP crée automatiquement un volume dans la zone de disponibilité de stockage appropriée pour l'héberger.

En raison de cette approche simplifiée de la gestion du stockage, `storage aggregate` Les commandes ne sont pas prises en charge sur les systèmes ASA r2. Prise en charge de certaines `lun` , `storage` et `volume` les commandes et les paramètres sont également limités.

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 maxsize`
- `lun move`
- `lun move-in-volume`

> Le `lun move-in-volume` la commande est remplacée par la `lun rename` et le `vserver nvme namespace rename` commandes.

- `lun transition`

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`

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

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

  Le `volume modify` La commande n'est pas disponible lorsqu'elle est utilisée 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`

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**.

Fonctionnalités ONTAP courantes prises en charge sur les systèmes ASA r2

Étant donné que les systèmes ASA r2 exécutent une version simplifiée d' ONTAP, de nombreuses tâches ONTAP courantes et fonctions du gestionnaire de système sont exécutées de la même manière sur les systèmes ASA r2 que sur les autres systèmes ONTAP .

Pour plus d'informations sur les fonctionnalités et fonctions courantes, consultez la documentation ONTAP suivante.

Protection des données

Découvrez plus d'informations sur les fonctionnalités de protection des données courantes prises en charge par les systèmes ASA r2.

Serveurs de clés externes en cluster

Vous pouvez configurer la connectivité à des serveurs de gestion de clés externes en cluster sur une machine virtuelle de stockage. Avec les serveurs de clés en cluster, vous pouvez désigner des serveurs de clés primaires et secondaires sur une machine virtuelle de stockage. Lors de l'enregistrement des clés, ONTAP tentera d'abord d'accéder à un serveur de clés primaire avant de tenter successivement d'accéder aux serveurs secondaires jusqu'à ce que l'opération se termine avec succès, empêchant ainsi la duplication des clés.

"Apprenez à configurer des serveurs de clés externes en cluster".

Gestion externe des clés pour le chiffrement au repos

Vous pouvez utiliser un ou plusieurs serveurs KMIP pour sécuriser les clés utilisées par le cluster pour accéder aux données chiffrées.

- "Activer la gestion des clés externes".
- "Activer la gestion des clés externes (NVE)" .

Sécurité des données

Découvrez plus d'informations sur les fonctionnalités de sécurité des données courantes prises en charge par les systèmes ASA r2.

Gestion des accès administrateur

Le rôle attribué à un administrateur détermine les fonctions qu'il peut effectuer. Le gestionnaire système fournit des rôles prédéfinis pour les administrateurs de cluster et les administrateurs de machines virtuelles de stockage. Vous attribuez le rôle lors de la création du compte administrateur, ou vous pouvez attribuer un rôle différent ultérieurement.

- "Apprenez à gérer les accès administrateur avec System Manager".

Authentification et autorisation du client

ONTAP utilise des méthodes standard pour sécuriser l'accès des clients et des administrateurs au stockage et pour se protéger contre les virus. Des technologies avancées sont disponibles pour le chiffrement des données au repos et pour le stockage WORM. ONTAP authentifie une machine cliente et un utilisateur en vérifiant leur identité auprès d'une source fiable. ONTAP autorise un utilisateur à accéder à un fichier ou à un répertoire en comparant ses informations d'identification avec les autorisations configurées sur le fichier ou le répertoire.

"En savoir plus sur l'authentification et l'autorisation des clients" .

Authentification OAuth 2.0

Vous pouvez utiliser le framework Open Authorization (OAuth 2.0) pour contrôler l'accès à vos clusters ONTAP . OAuth 2.0 restreint et contrôle l'accès aux ressources protégées à l'aide de jetons d'accès signés.

"En savoir plus sur l'authentification OAuth 2.0" .

Authentification SAML et accès administrateur

Vous pouvez configurer et activer l'authentification SAML (Security Assertion Markup Language) pour les services Web. SAML authentifie les utilisateurs par l'intermédiaire d'un fournisseur d'identité externe (IdP) au lieu des fournisseurs de services d'annuaire tels qu'Active Directory et LDAP.

"Apprenez à configurer l'authentification SAML" .

Réseautage

Découvrez plus d'informations sur les fonctionnalités réseau courantes prises en charge par les systèmes ASA r2.

Conformité FIPS

ONTAP est conforme aux normes fédérales de traitement de l'information (FIPS) 140-2 pour toutes les connexions SSL. Vous pouvez activer et désactiver le mode SSL FIPS, définir les protocoles SSL globalement et désactiver les chiffrements faibles tels que RC4 dans ONTAP.

À partir d' ONTAP 9.18.1, les algorithmes cryptographiques de calcul post-quantique sont pris en charge pour SSL. Ces algorithmes offrent une protection supplémentaire contre d'éventuelles futures attaques informatiques quantiques et sont disponibles lorsque le mode SSL FIPS est désactivé.

- "Apprenez à configurer FIPS pour toutes les connexions SSL".

Groupes d'agrégation de liens (LAG)

Un groupe d'interfaces, également appelé groupe d'agrégation de liens (LAG), est créé en combinant deux ou plusieurs ports physiques sur le même nœud en un seul port logique. Le port logique offre une résilience

accrue, une disponibilité accrue et un partage de charge.

"Découvrez les groupes d'agrégation de liens".

Protocoles SAN

Les systèmes ASA r2 prennent en charge tous les protocoles SAN (iSCSI, FC, NVMe/FC, NVMe/TCP).

- "Apprenez-en davantage sur le protocole iSCSI".
- "Apprenez-en davantage sur le protocole Fibre Channel (FC).".
- "Découvrez le protocole NVMe".
  - "Apprenez à configurer le déchargement de copie NVMe".

    À partir d' ONTAP 9.18.1, le déchargement de copie NVMe est pris en charge. La fonction de déchargement de copie NVMe permet à un hôte NVMe de décharger les opérations de copie de son processeur vers le processeur du contrôleur de stockage ONTAP . L'hôte peut copier des données d'un espace de noms NVMe à un autre tout en réservant ses ressources CPU pour les charges de travail applicatives.

  - "Apprenez-en davantage sur l'allocation d'espace (désallocation) pour NVMe".

    À partir d' ONTAP 9.16.1, la désallocation d'espace (également appelée « perforation de trous » et « démappage ») est activée par défaut pour les espaces de noms NVMe. La désallocation d'espace permet à un hôte de désallouer les blocs inutilisés des espaces de noms pour récupérer de l'espace.

System Manager

Vous pouvez rechercher diverses actions, objets et sujets d'information dans le Gestionnaire système. Vous pouvez également rechercher des entrées spécifiques dans les données du tableau.

"Apprenez à rechercher, filtrer et trier les informations dans System Manager".

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 System Manager, 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 confirmé que le support technique peut recevoir des messages AutoSupport de votre système ASA r2, en vous assurant qu’ils disposent 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 System Manager, 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 System Manager, 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 System Manager, 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 System Manager, 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 être "Enregistré auprès de Active IQ" pour consulter les demandes d'assistance concernant 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.

ONTAP

"Avis pour ONTAP 9.16.1"

Informations sur le copyright

Informations sur les marques commerciales