FlexPod datacenter avec NetApp SnapMirror Business Continuity et ONTAP 9.10

FlexPod

NetApp
March 25, 2024

Sommaire

FlexPod datacenter avec NetApp SnapMirror Business Continuity et ONTAP 9.10

Tr-4920 : continuité de l'activité pour FlexPod Datacenter avec NetApp SnapMirror et ONTAP 9.10

Jyh-shing Chen, NetApp

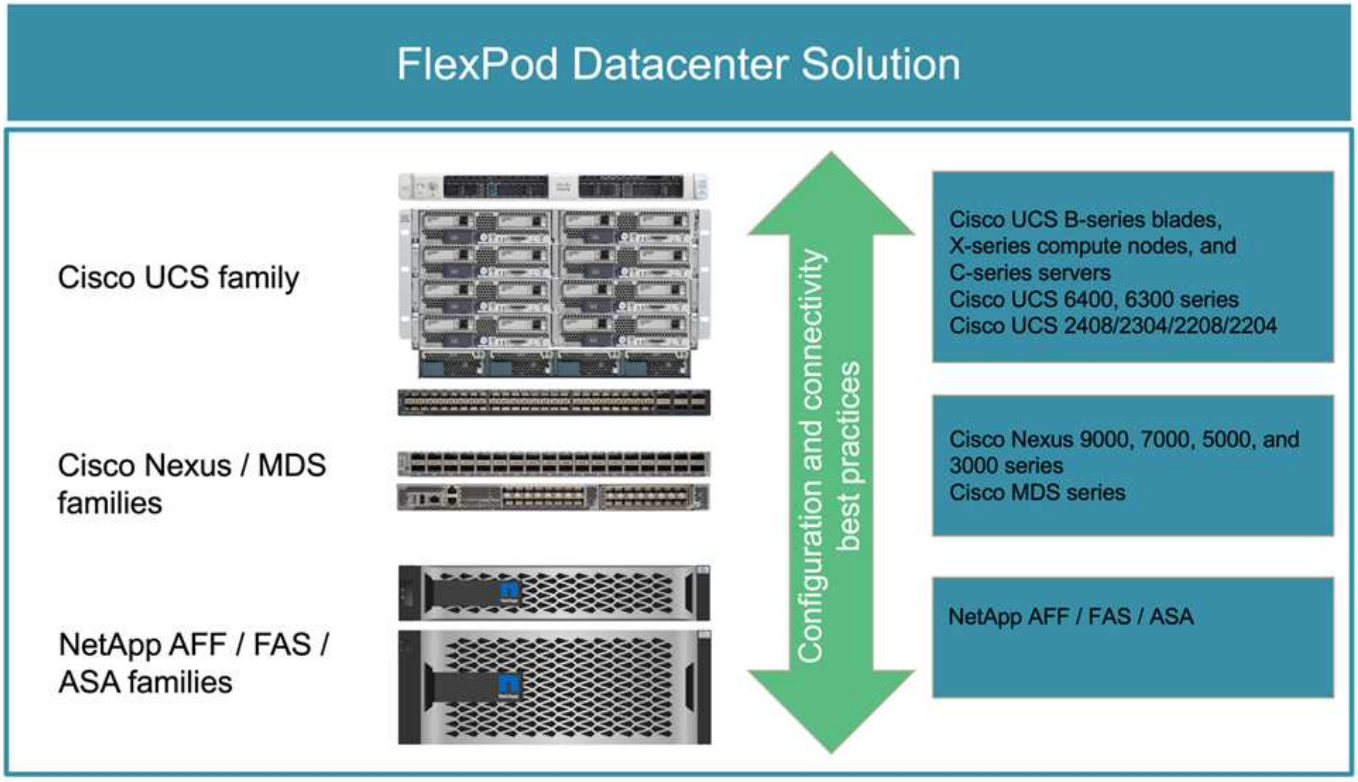
Introduction

Solution FlexPod

FlexPod est une architecture de data Center basée sur les bonnes pratiques. Elle inclut les composants suivants de Cisco et NetApp :

- Serveurs Cisco Unified Computing System (Cisco UCS)
- Gammes de commutateurs Cisco Nexus et MDS
- Systèmes NetApp FAS, NetApp AFF et ASA

La figure suivante décrit certains des composants utilisés pour créer des solutions FlexPod. Ces composants sont connectés et configurés conformément aux meilleures pratiques recommandées par Cisco et NetApp pour fournir une plateforme idéale pour exécuter en toute confiance une variété de charges de travail d'entreprise.



Un large portefeuille de conceptions validées Cisco (CVD) et d'architectures vérifiées NetApp (NVA) est disponible. Ces CVD et NVA couvrent l'ensemble des charges de travail majeures des data centers et résultent

d’une collaboration et d’innovations continues entre NetApp et Cisco sur les solutions FlexPod.

En intégrant des tests et des validations déjà exhaustifs dans le processus de création, les conformément aux CVD et aux NVA de FlexPod fournissent des conceptions d’architecture de solutions de référence et des guides de déploiement détaillés pour aider les partenaires et les clients à déployer et à adopter les solutions FlexPod. En utilisant ces CVD et les NVA comme guides de conception et d’implémentation, les entreprises peuvent réduire les risques, réduire les temps d’indisponibilité de la solution et augmenter la disponibilité, l’évolutivité, la flexibilité et la sécurité des solutions FlexPod qu’elles déploient.

Chacune des familles de composants FlexPod présentées (Cisco UCS, commutateurs Cisco Nexus/MDS et stockage NetApp) offre des options de plateforme et de ressources pour faire évoluer l’infrastructure de manière verticale ou horizontale, tout en prenant en charge les fonctionnalités requises selon les meilleures pratiques de configuration et de connectivité de FlexPod. FlexPod peut également évoluer horizontalement pour les environnements nécessitant plusieurs déploiements cohérents en déployant des piles FlexPod supplémentaires.

Assurer une reprise après incident rapide et la continuité de l’activité

Plusieurs méthodes permettent aux entreprises de récupérer rapidement leurs applications et services de données en cas d’incident. La mise en place d’un plan de reprise après incident et de continuité de l’activité, l’implémentation d’une solution qui répond aux objectifs métier et l’exécution de tests réguliers des scénarios d’incident permettent aux entreprises de bénéficier d’une reprise après incident et de continuer les services stratégiques après une situation d’incident.

Les exigences en matière de reprise après incident et de continuité de l’activité peuvent être différentes pour les types de services d’applications et de données. Certaines applications et données ne sont pas nécessaires en cas d’urgence ou d’incident, alors que d’autres doivent être disponibles en continu pour répondre aux exigences de l’entreprise.

Pour les applications stratégiques et les services de données qui risquent de perturber votre activité alors qu’ils ne sont pas disponibles, une évaluation minutieuse est nécessaire pour répondre à des questions telles que le type de maintenance et les scénarios d’incident auxquels l’entreprise doit tenir compte, quelle quantité de données l’entreprise peut se permettre de perdre en cas d’incident, et la rapidité à laquelle la reprise peut et doit avoir lieu.

Pour les entreprises qui ont recours à des services de données pour générer du chiffre d’affaires, les services de données doivent être protégés par une solution capable de résister à plusieurs scénarios de défaillance unique, mais aussi à un scénario de panne sur site dans le but d’assurer la continuité de l’activité.

Objectifs de point de restauration et de délai de restauration

L’objectif de point de restauration (RPO) mesure la quantité de données générée, en termes de temps, vous pouvez vous permettre de perdre ou bien le point auquel vous pouvez récupérer vos données. Avec un plan de sauvegarde quotidien, une entreprise risque de perdre une journée de données, car les modifications apportées aux données depuis la dernière sauvegarde pourraient être perdues en cas d’incident. Pour les services de données stratégiques et stratégiques, vous avez besoin d’un RPO nul et d’un plan et d’infrastructures associés pour protéger vos données sans aucune perte.

L’objectif de délai de restauration (RTO) mesure le temps que vous pouvez vous permettre d’éviter que les données ne soient disponibles ou la rapidité à laquelle les services de données doivent être mis en service. Par exemple, une entreprise peut disposer d’une implémentation de la sauvegarde et de la restauration qui utilise des bandes traditionnelles pour certains jeux de données en raison de sa taille. Par conséquent, la restauration des données à partir des bandes de sauvegarde peut prendre plusieurs heures, voire des jours, en cas de défaillance de l’infrastructure. Il faut également comprendre le temps nécessaire pour sauvegarder l’infrastructure et restaurer les données. Pour les services de données stratégiques, vous pourriez avoir besoin

d'un RTO très faible et vous ne pouvez tolérer qu'un temps de basculement de quelques secondes ou minutes pour remettre en ligne les services de données pour assurer la continuité de l'activité.

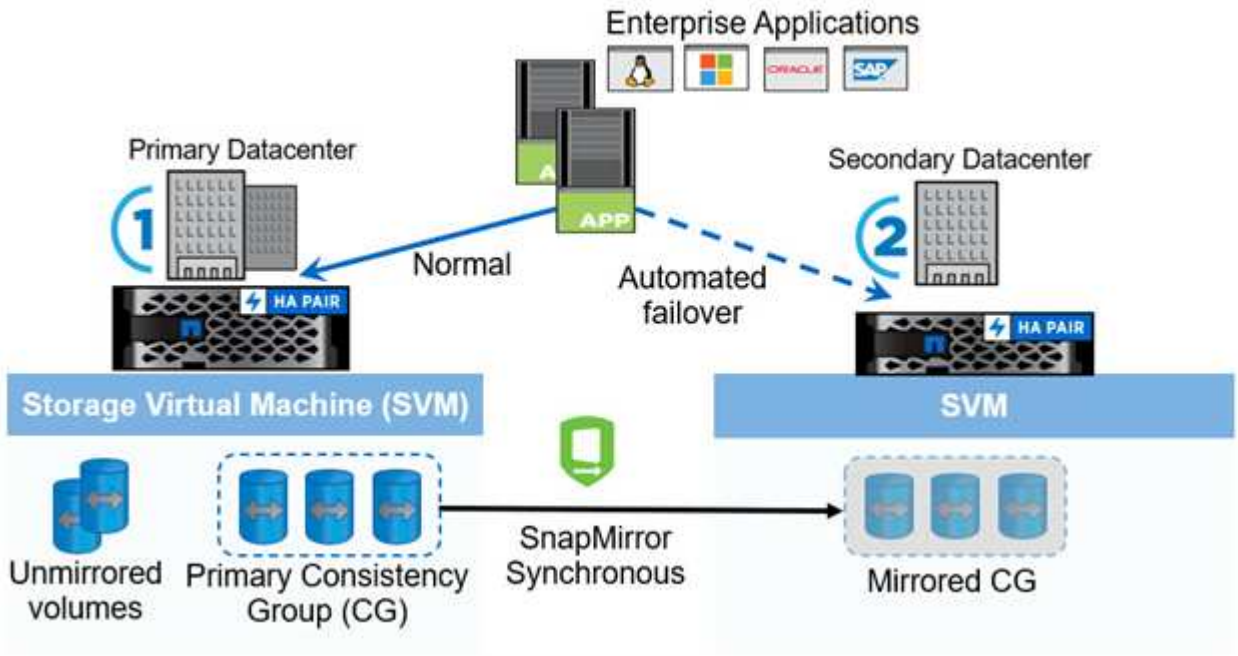
SM-BC

Depuis ONTAP 9.8, vous pouvez protéger les charges de travail SAN pour un basculement transparent des applications avec NetApp SM-BC. Vous pouvez créer des relations de groupes de cohérence entre deux clusters AFF ou deux clusters ASA pour la réplication des données afin d'atteindre un RPO nul et un RTO proche de zéro.

La solution SM-BC réplique les données à l'aide de la technologie SnapMirror synchrone sur un réseau IP. Elle offre une granularité au niveau des applications et un basculement automatique pour protéger vos services de données stratégiques, tels que Microsoft SQL Server, Oracle, etc. Avec des LUN SAN basées sur des protocoles iSCSI ou FC. Un médiateur ONTAP déployé sur un troisième site surveille la solution SM-BC et active le basculement automatique en cas d'incident sur site.

Un groupe de cohérence est une collection de volumes FlexVol qui offre une garantie de cohérence de l'ordre d'écriture pour la charge de travail applicative qui doit être protégée pour la continuité de l'activité. Elle permet d'effectuer simultanément des copies Snapshot cohérentes après panne d'un ensemble de volumes à un point dans le temps. Une relation SnapMirror, également appelée relation de groupe de cohérence, est établie entre un groupe de cohérence source et un groupe de cohérence de destination. Le groupe de volumes sélectionnés pour faire partie d'un groupe de cohérence peut être mappé à une instance d'application, à un groupe d'instances d'applications ou à une solution complète. En outre, les relations de groupe de cohérence SM-BC peuvent être créées ou supprimées à la demande en fonction des exigences et des changements de l'entreprise.

Comme illustré dans la figure suivante, les données du groupe de cohérence sont répliquées sur un second cluster ONTAP pour la reprise sur incident et la continuité de l'activité. Les applications disposent d'une connectivité aux LUN des deux clusters ONTAP. Les E/S sont généralement servies par le cluster primaire et reprises automatiquement à partir du cluster secondaire si un incident se produit sur le cluster primaire. Lors de la conception d'une solution SM-BC, les nombres d'objets pris en charge pour les relations CG (par exemple, un maximum de 20 CGS et un maximum de 200 noeuds finaux) doivent être observés pour éviter de dépasser les limites prises en charge.



"Suivant : solution FlexPod SM-BC."

Solution FlexPod SM-BC

"Précédent : introduction."

Présentation de la solution

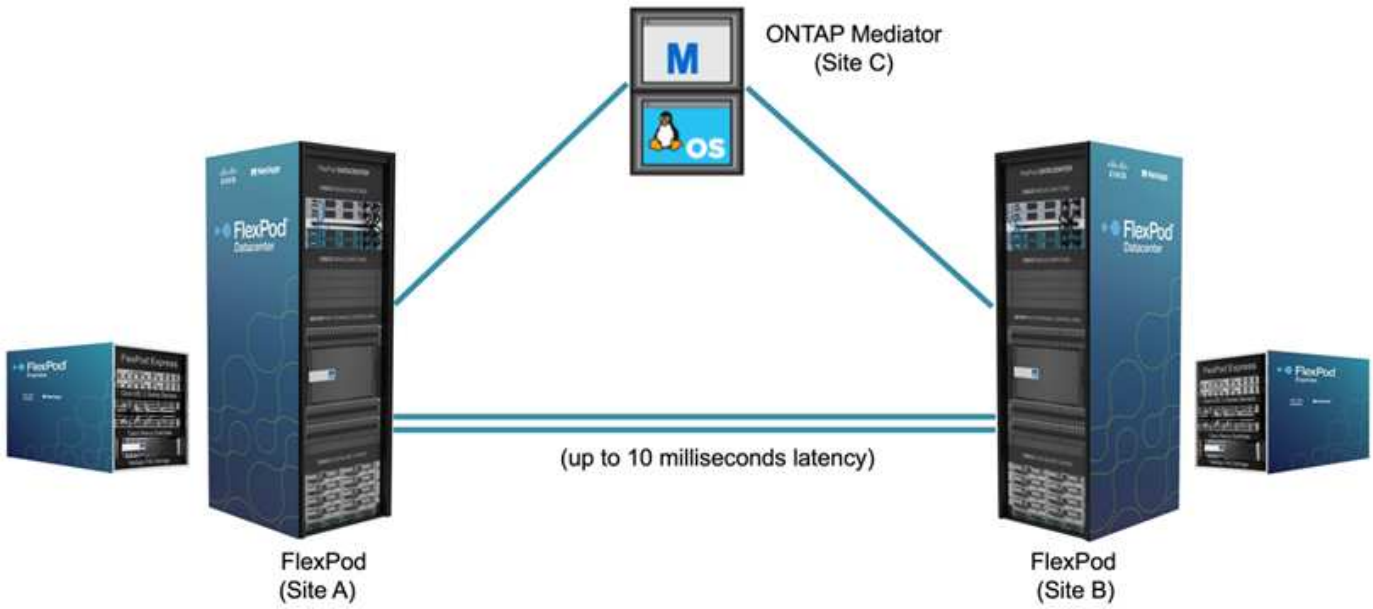
À un haut niveau, la solution FlexPod SM-BC est composée de deux systèmes FlexPod, situés sur deux sites séparés par une certaine distance, connectés et associés, afin d'offrir une solution de data Center hautement disponible, extrêmement flexible et extrêmement fiable, capable d'assurer la continuité de l'activité malgré une défaillance sur un site.

Outre le déploiement de deux nouvelles infrastructures FlexPod pour créer une solution FlexPod SM-BC, la solution peut également être implémentée sur deux infrastructures FlexPod existantes compatibles avec SM-BC ou en ajoutant un nouveau FlexPod pour être homologue avec un FlexPod existant.

Les deux systèmes FlexPod d'une solution FlexPod SM-BC n'ont pas besoin d'être identiques dans les configurations. Cependant, les deux clusters ONTAP doivent être des mêmes familles de stockage, deux systèmes AFF ou deux systèmes ASA, mais pas nécessairement du même modèle matériel. La solution SM-BC ne prend pas en charge les systèmes FAS.

Les deux sites FlexPod nécessitent une connectivité réseau qui répond aux exigences de bande passante et de qualité de service de la solution. Ils offrent une latence aller-retour inférieure à 10 millisecondes (10 ms) entre les sites, comme l'exige la solution ONTAP SM-BC. Pour la validation de cette solution FlexPod SM-BC, les deux sites FlexPod sont interconnectés via un réseau de couche 2 étendu dans le même laboratoire.

La solution NetApp ONTAP SM-BC assure une réplication synchrone entre les deux clusters de stockage NetApp pour une haute disponibilité et la reprise après incident dans un campus ou une zone métropolitaine. Le médiateur ONTAP déployé sur un troisième site surveille la solution et permet un basculement automatique en cas d'incident sur site. La figure suivante fournit une vue d'ensemble des composants de la solution.



Avec la solution FlexPod SM-BC, vous pouvez déployer un cloud privé basé sur VMware vSphere sur une infrastructure distribuée mais intégrée. La solution intégrée permet de coordonner plusieurs sites en tant qu'infrastructure unique afin de protéger les services de données contre différents scénarios de point de

défaillance unique et une défaillance complète du site.

Ce rapport technique met en évidence certaines des considérations de conception de bout en bout de la solution FlexPod SM-BC. Les professionnels sont encouragés à obtenir des informations de référence disponibles dans les CVD et les NVA d'FlexPod pour d'autres détails d'implémentation de la solution FlexPod.

Bien que la solution ait été validée en déployant deux systèmes FlexPod basés sur les meilleures pratiques de FlexPod, comme décrit dans les CVD, elle tient compte des exigences de la solution SM-BC. La solution FlexPod SM-BC déployée décrite dans ce rapport a été validée pour la résilience et la tolérance aux pannes dans différents scénarios de défaillance, ainsi qu'une simulation de défaillance d'un site.

De la solution

La solution FlexPod SM-BC est conçue pour répondre aux exigences clés suivantes :

- Continuité de l'activité pour les applications et les services de données stratégiques en cas de défaillance complète du data Center
- Placement flexible des workloads distribués avec mobilité des workloads dans l'ensemble des data centers
- Affinité avec les sites dans lesquels les données des machines virtuelles sont accessibles localement, à partir du même site de data Center, pendant les opérations normales
- Restaurez rapidement vos données sans aucune perte en cas de défaillance d'un site

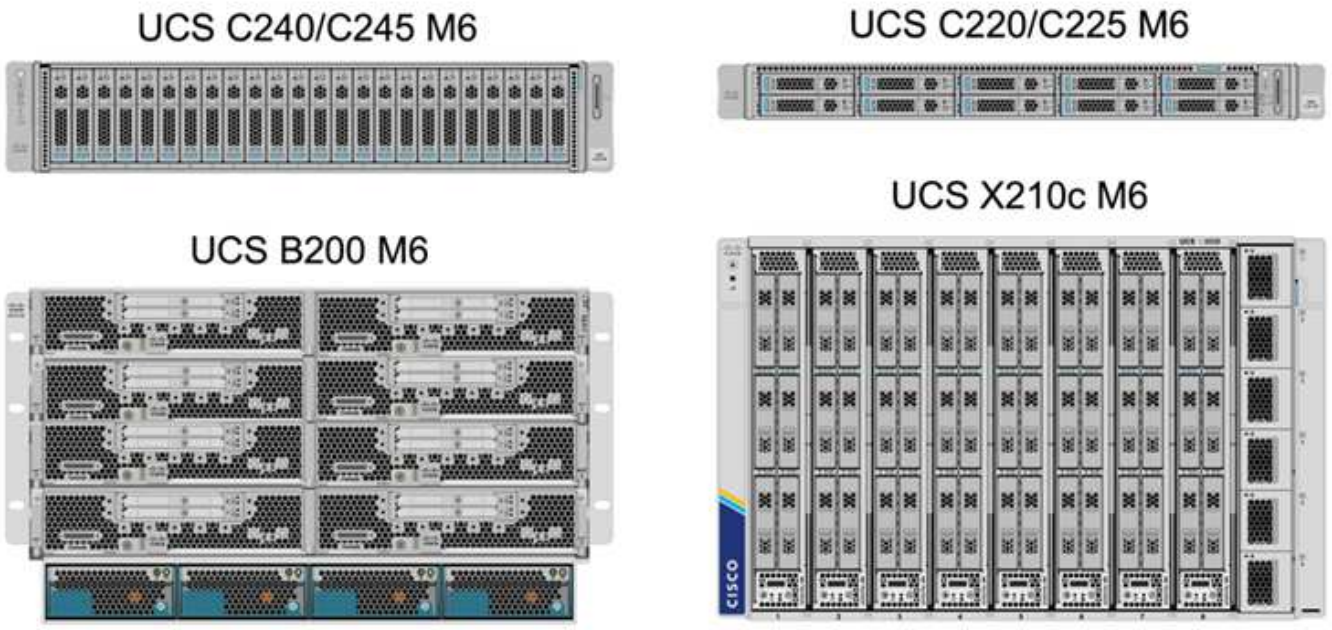
Composants de la solution

Composants de calcul Cisco

Cisco UCS est une infrastructure informatique intégrée qui offre des ressources informatiques unifiées, une structure unifiée et une gestion unifiée. Elle permet aux entreprises d'automatiser et d'accélérer le déploiement des applications, y compris la virtualisation et les charges de travail sans système d'exploitation. Cisco UCS prend en charge de nombreuses utilisations dans le cadre du déploiement, notamment les bureaux distants, les succursales, les data centers et le cloud hybride. Selon les exigences spécifiques de la solution, la mise en œuvre des ressources de calcul FlexPod et Cisco peut utiliser différents composants à différentes échelles. Les sous-parties suivantes fournissent des informations supplémentaires sur certains composants UCS.

Serveur UCS et nœud de calcul

La figure suivante présente quelques exemples de composants de serveur UCS, dont des serveurs en rack UCS C-Series, des châssis UCS 5108 avec serveurs lames B-Series et le nouveau châssis UCS X9508 avec nœuds de calcul X-Series. Les serveurs en rack Cisco UCS C-Series sont disponibles dans un ou deux formats d'unité de rack (RU), avec processeurs Intel et AMD, ainsi que dans plusieurs vitesses de CPU, cœurs, mémoire et options d'E/S. Les serveurs lames Cisco UCS B-Series et les nouveaux nœuds de calcul X-Series sont également disponibles avec plusieurs options de processeur, de mémoire et d'E/S, et tous sont pris en charge dans l'architecture FlexPod pour répondre aux diverses exigences de l'entreprise.



En plus des serveurs rack M6 nouvelle génération C220/C225/C240/C245, des serveurs lames B200 M6 et des nœuds de calcul X210c illustrés dans cette figure, les générations précédentes de serveurs rack et lame peuvent également être utilisées si elles sont toujours prises en charge.

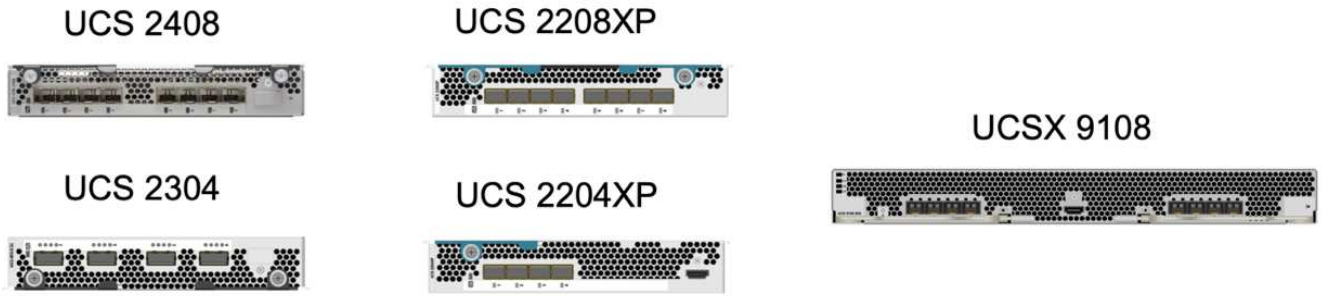
Module d'E/S et module de structure intelligente

Le module d'E/S (IOM)/Fabric Extender et le module de structure intelligente (IFM) offrent une connectivité de structure unifiée pour le châssis de serveurs lames Cisco UCS 5108 et le châssis Cisco UCS X9508 X-Series, respectivement.

La quatrième génération d'UCS IOM 2408 possède huit ports Ethernet unifiés 25 G pour la connexion du châssis UCS 5108 avec Fabric Interconnect (FI). Chaque 2408 dispose de quatre ports Ethernet de fond de panier 10 G par le biais du fond de panier central à chaque serveur lame du châssis.

Le contrôleur UCSTM X 9108 25G IFM est doté de huit ports Ethernet unifiés 25-G pour la connexion des serveurs lames dans le châssis UCS X9508 avec des interconnexions de fabric. Chaque 9108 dispose de quatre connexions 25-G vers chaque nœud de calcul UCS X210c dans le châssis X9108. Le 9108 IFM fonctionne également de concert avec le Fabric Interconnect pour gérer l'environnement du châssis.

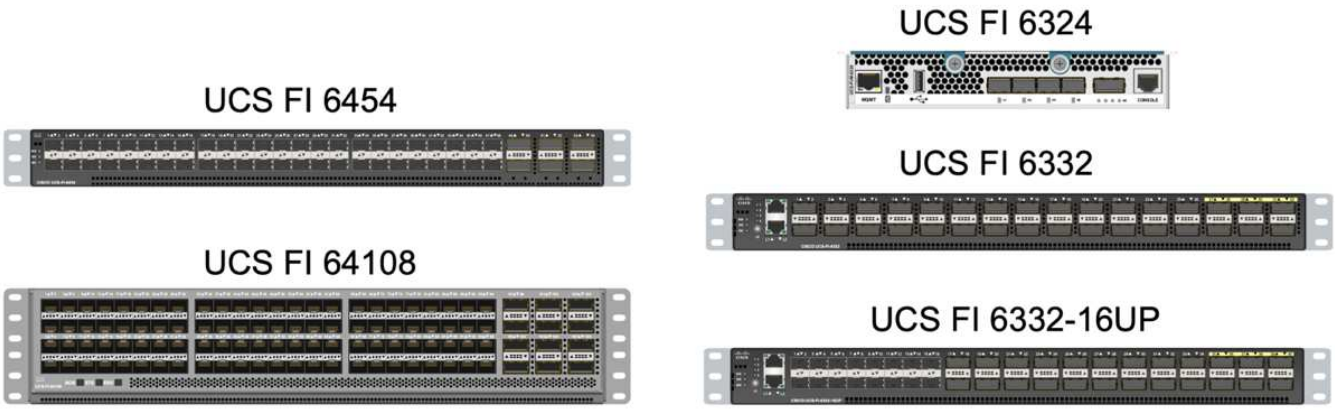
La figure suivante représente les générations d'IOM UCS 2408 et antérieures pour le châssis UCS 5108 et le module 9108 IFM pour le châssis X9508.



Interconnexions de fabric UCS

Les interconnexions de fabric Cisco UCS (IF) offrent une connectivité et une gestion à l'ensemble du système Cisco UCS. Généralement déployées en tant que paire active/active, les interfaces de contrôle de la qualité du système intègrent tous les composants dans un domaine de gestion unique et hautement disponible, contrôlé par Cisco UCS Manager ou Cisco Intersight. Il s'agit d'une structure unifiée unique pour le système avec une faible latence et sans perte, des commutateurs coupe-circuit qui prennent en charge le trafic LAN, SAN et de gestion à l'aide d'un seul jeu de câbles.

Il existe deux variantes pour les IFI Cisco UCS de quatrième génération : UCS FI 6454 et 64108. Ils comprennent la prise en charge de ports Ethernet 10/25 Gbit/s, de ports Ethernet 1/10/25 Gbit/s, de ports Ethernet UP-link 40/100 Gbit/s et de ports unifiés prenant en charge les ports Ethernet 10/25 Gbit/s ou Fibre Channel 8/16/32 Gbit/s. La figure suivante montre les IFI Cisco UCS de quatrième génération, ainsi que les modèles de troisième génération également pris en charge.

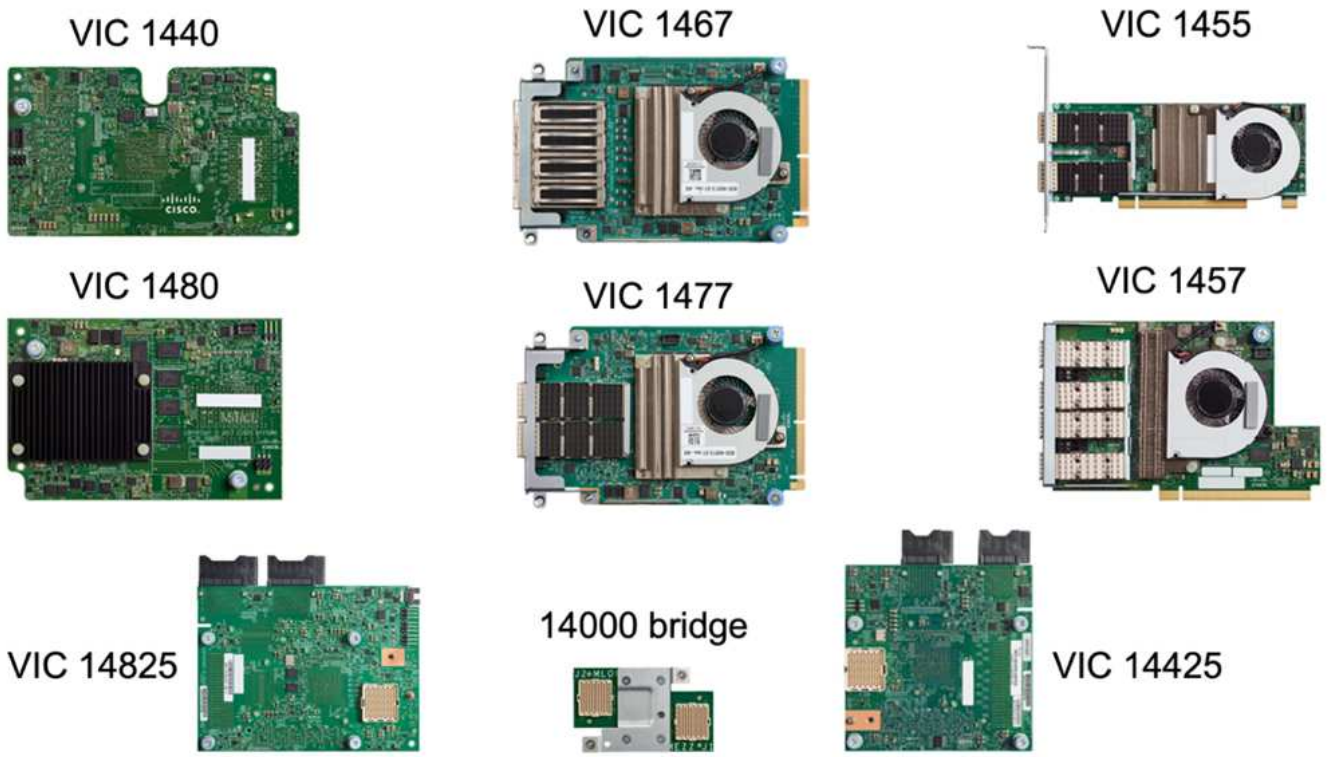


> Pour prendre en charge le châssis Cisco UCS X-Series, des interconnexions de fabric de quatrième génération configurées en mode géré InterSight (IMM) sont requises. Cependant, le châssis Cisco UCS 5108 B-series peut être pris en charge aussi bien en mode IMM qu'en mode géré UCSM.

> Le système UCS FI 6324 utilise le format de module d'E/S et est intégré dans un châssis UCS Mini pour les déploiements qui requièrent uniquement un petit domaine UCS.

Cartes d'interface virtuelle UCS

Les cartes d'interface virtuelle Cisco UCS (VICS) unifient la gestion des systèmes et la connectivité LAN et SAN pour les serveurs rack et lames. Il prend en charge jusqu'à 256 périphériques virtuels, soit en tant que cartes d'interface réseau virtuelles (vNIC), soit en tant que cartes de bus hôte virtuelles (vHBA) utilisant la technologie Cisco SingleConnect. Suite à la virtualisation, les cartes VIC simplifient considérablement la connectivité réseau et réduisent le nombre d'adaptateurs réseau, de câbles et de ports de commutation nécessaires au déploiement de la solution. La figure suivante présente certaines des Cisco UCS VICS disponibles pour les serveurs B-Series et C-Series, ainsi que les nœuds de calcul X-Series.



Les différents modèles d'adaptateurs prennent en charge différents serveurs lame et rack avec différents nombres de ports, vitesses de port et formats de LAN modulaire sur la carte mère (mLOM), cartes mezzanine et interfaces PCIe. Les adaptateurs prennent en charge certaines combinaisons de Ethernet 10/25/40/100-G et FCoE (Fibre Channel over Ethernet). Ils intègrent la technologie CNA (Converged Network adapter) de Cisco, prennent en charge un ensemble complet de fonctionnalités et simplifient la gestion des adaptateurs et le déploiement des applications. Par exemple, le VIC prend en charge la technologie VM-FEX (Data Center Virtual machine Fabric Extender) de Cisco, qui étend les ports d'interconnexion de structure Cisco UCS aux machines virtuelles, simplifiant ainsi le déploiement de la virtualisation des serveurs.

Avec une combinaison de Cisco VIC dans les configurations mLOM, mezzanine, module d'extension de port et carte pont, vous pouvez tirer pleinement parti de la bande passante et de la connectivité disponibles pour les serveurs lames. Par exemple, en utilisant les deux liaisons 25 G sur le VIC 14825 (mLOM) et 14425 (mezzanine) et le 14000 (carte de pont) pour le nœud de calcul X210c, la bande passante combinée VIC est de 2 x 50-G + 2 x 50-G, Ou 100 G par fabric/IFM et 200 G au total par serveur avec la configuration IFM double.

Pour plus d'informations sur les gammes de produits Cisco UCS, les spécifications techniques et la documentation, consultez le "Cisco UCS" site web pour information.

Composants de commutation Cisco

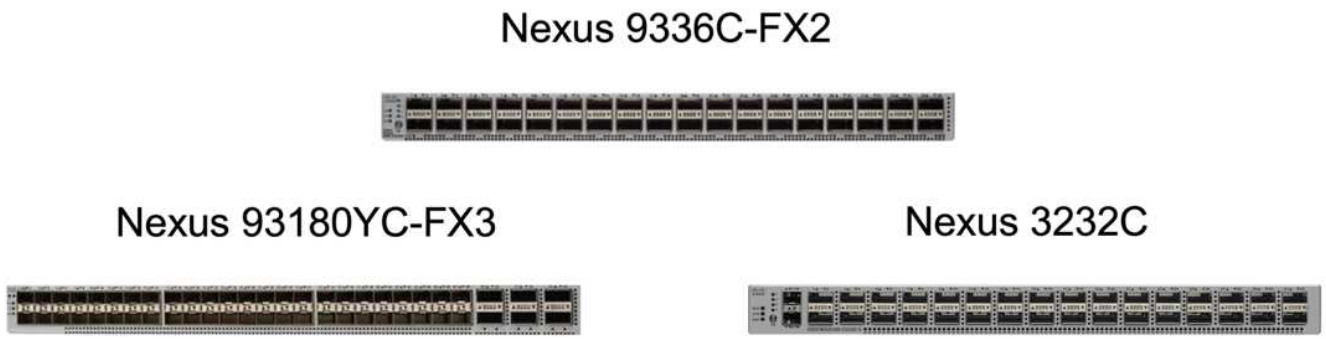
Commutateurs Nexus

FlexPod utilise des commutateurs Cisco Nexus Series afin de fournir une structure de commutation Ethernet pour les communications entre Cisco UCS et les contrôleurs de stockage NetApp. Tous les modèles de commutateurs Cisco Nexus actuellement pris en charge, y compris les gammes Cisco Nexus 3000, 5000, 7000 et 9000, sont pris en charge pour le déploiement de FlexPod.

Dans le choix d'un modèle de switch pour un déploiement FlexPod, de nombreux facteurs sont à prendre en compte, notamment les performances, la vitesse de port, la densité de port, la latence de commutation, Et des protocoles tels que la prise en charge ACI et VXLAN, pour vos objectifs de conception ainsi que la durée de

prise en charge des commutateurs.

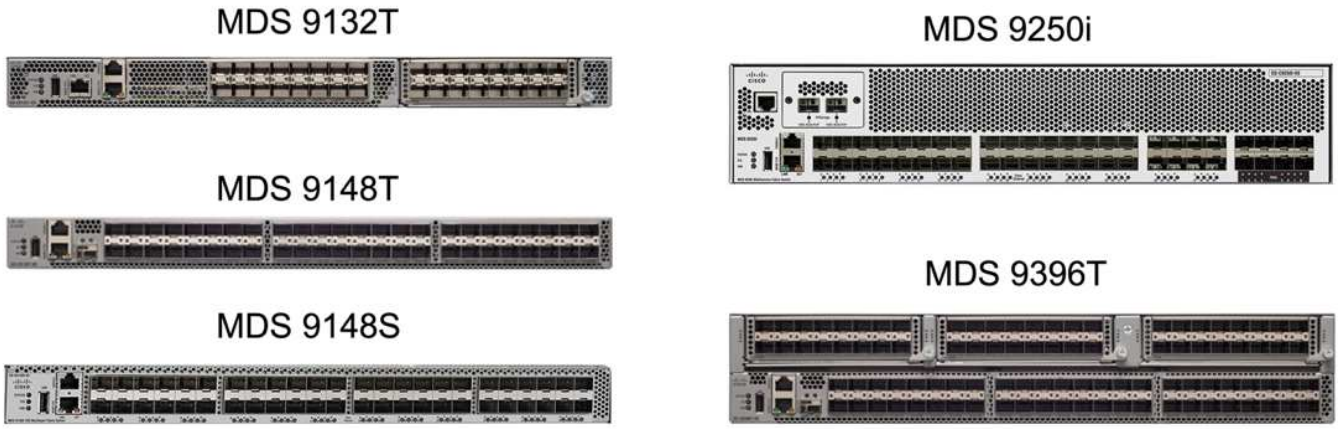
La validation de nombreux CVD récents de FlexPod utilise des commutateurs Cisco Nexus 9000, tels que les Nexus 9336C-FX2 et Nexus 93180YC-FX3. Ils offrent des ports haute performance 40/100G et 10//25G, une faible latence et une efficacité énergétique exceptionnelle dans un format compact 1U. Des vitesses supplémentaires sont prises en charge via des ports de liaison ascendante et des câbles de dérivation. La figure ci-dessous présente quelques switchs Cisco Nexus 9k et 3K, notamment les Nexus 9336C-FX2 et Nexus 3232C utilisés pour cette validation.



Voir "Commutateurs pour data Center Cisco" Pour plus d'informations sur les commutateurs Nexus disponibles ainsi que leurs spécifications et leurs documentations.

Switchs MDS

Les switchs de fabric Cisco MDS 9100/9200/9300 sont des composants facultatifs pour l'architecture FlexPod. Ces commutateurs sont extrêmement fiables, hautement flexibles, sécurisés et offrent une visibilité sur le flux du trafic dans le maillage. La figure suivante présente quelques exemples de commutateurs MDS qui peuvent être utilisés pour créer des structures SAN FC redondantes pour une solution FlexPod, afin de répondre aux besoins des applications et de l'entreprise.



Les commutateurs Cisco MDS 9132T/9148T/9396T haute performance 32G Multilayer Fabric sont économiques et extrêmement fiables, flexibles et évolutifs. Les fonctionnalités avancées du réseau de stockage facilitent la gestion et sont compatibles avec l'ensemble de la gamme Cisco MDS 9000 pour une implémentation SAN fiable.

Ces fonctionnalités de télémétrie et d'analytique SAN dernière génération sont intégrées à cette plateforme matérielle nouvelle génération. Les données de télémétrie extraites de l'inspection des en-têtes de trame peuvent être transmises à une plateforme de visualisation analytique, y compris Cisco Data Center Network

Manager. Les commutateurs MDS qui prennent en charge Fibre Channel 16 Gbit/s, comme le MDS 9148S, sont également pris en charge dans FlexPod. De plus, les commutateurs multiservice MDS, comme le MDS 9250i, qui prend en charge les protocoles FCoE et FCIP en plus du protocole FC, font également partie de la gamme de solutions FlexPod.

Sur les commutateurs MDS semi-modulaires tels que le 9132T et le 9396T, des licences de port et de module d'extension de port supplémentaires peuvent être ajoutées pour prendre en charge la connectivité de périphérique supplémentaire. Sur les commutateurs fixes comme le 9148T, des licences de port supplémentaires peuvent être ajoutées si nécessaire. Cette flexibilité de facturation à l'utilisation fournit une composante des dépenses d'exploitation qui permet de réduire les dépenses d'investissement relatives à la mise en œuvre et à l'exploitation d'une infrastructure SAN de commutateur MDS.

Voir "Commutateurs de structure Cisco MDS" Pour plus d'informations sur les commutateurs MDS Fabric disponibles, consultez le "NetApp IMT" et "Liste de compatibilité matérielle et logicielle Cisco" Pour obtenir la liste complète des commutateurs SAN pris en charge.

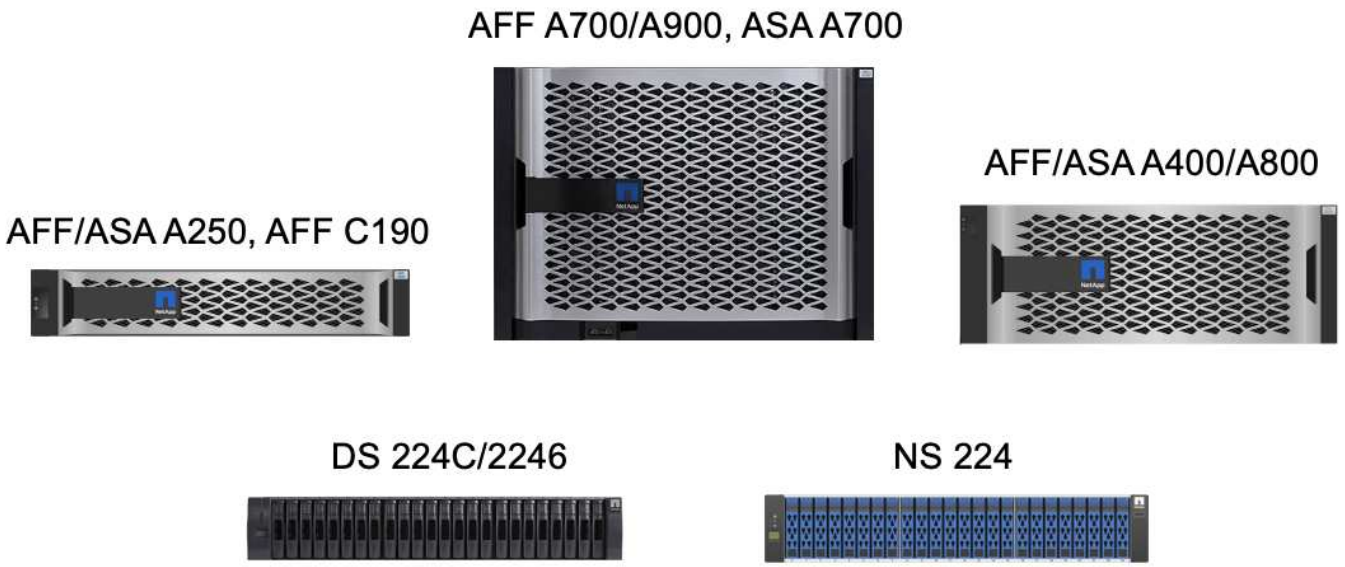
Composants NetApp

Les contrôleurs NetApp AFF ou ASA redondants qui exécutent le logiciel ONTAP 9.8 ou des versions ultérieures sont requis pour créer une solution FlexPod SM-BC. La dernière version d'ONTAP, actuellement 9.10.1, est recommandée pour le déploiement de SM-BC afin de tirer parti des innovations, des performances et des améliorations de qualité continues de ONTAP, ainsi que du nombre maximal d'objets pour la prise en charge de SM-BC.

Les contrôleurs NetApp AFF et ASA, dotés de performances et d'innovations de pointe, assurent la protection des données d'entreprise et proposent des fonctionnalités avancées de gestion des données. Les systèmes AFF et ASA prennent en charge les technologies NVMe de bout en bout, y compris les disques SSD connectés via NVMe et la connectivité hôte front-end NVMe over Fibre Channel (NVMe/FC). Vous pouvez améliorer le débit des workloads et réduire la latence d'E/S en adoptant une infrastructure SAN NVMe/FC. Toutefois, les datastores NVMe/FC ne peuvent actuellement être utilisés que pour les charges de travail qui ne sont pas protégées par SM-BC, car la solution SM-BC ne prend actuellement en charge que les protocoles iSCSI et FC.

NetApp AFF et les contrôleurs de stockage ASA fournissent également une base solide pour le cloud hybride qui permet aux clients de profiter des avantages de la mobilité transparente des données grâce à NetApp Data Fabric. Data Fabric vous permet d'accéder facilement aux données de la périphérie jusqu'au cœur, où elles sont générées, ainsi qu'au cloud, pour exploiter l'élasticité de calcul, d'IA et DE ML des informations exploitables à la demande.

Comme le montre la figure suivante, NetApp propose différents contrôleurs de stockage et tiroirs disques afin de répondre à vos exigences en termes de performances et de capacité. Pour plus d'informations sur les fonctionnalités et les spécifications des contrôleurs NetApp AFF et ASA, consultez le tableau suivant et consultez les liens vers les pages produits.

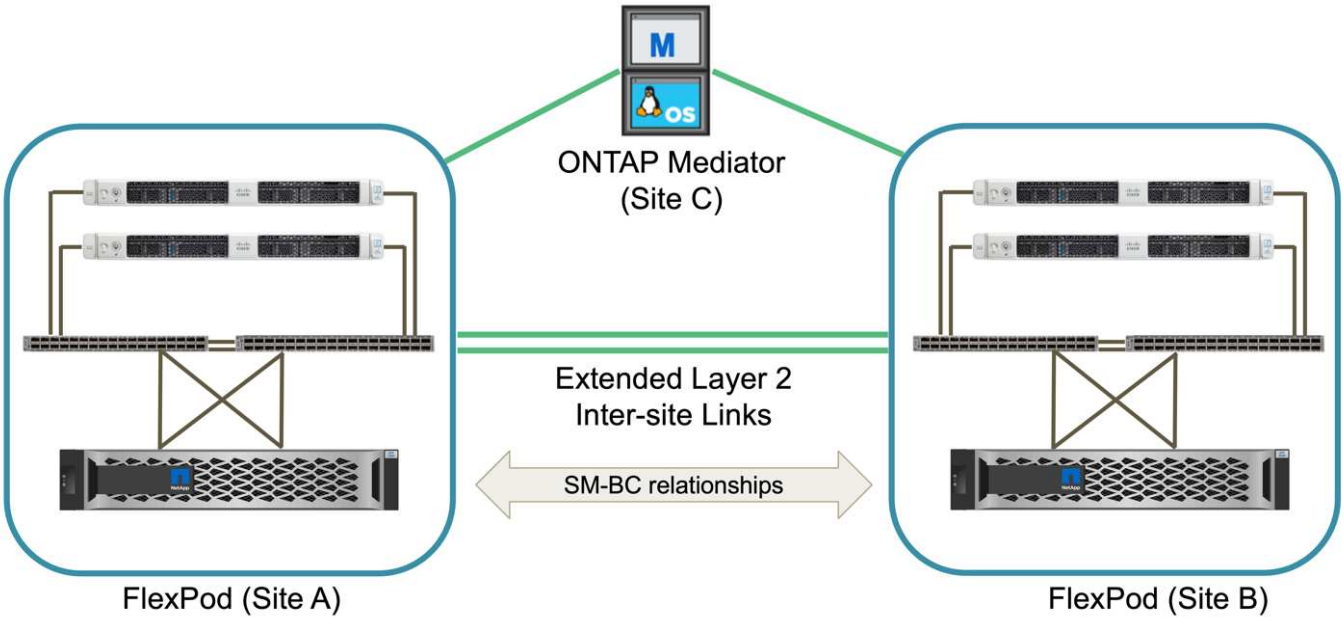


Famille de produits	Caractéristiques techniques
Gamme AFF	"Documentation sur la gamme AFF"
Gamme ASA	"Documentation sur la gamme ASA"

Consulter le "Documentation relative aux tiroirs disques et aux supports de stockage NetApp" et "NetApp Hardware Universe" pour en savoir plus sur les tiroirs disques et les tiroirs disques pris en charge pour chaque modèle de contrôleur de stockage.

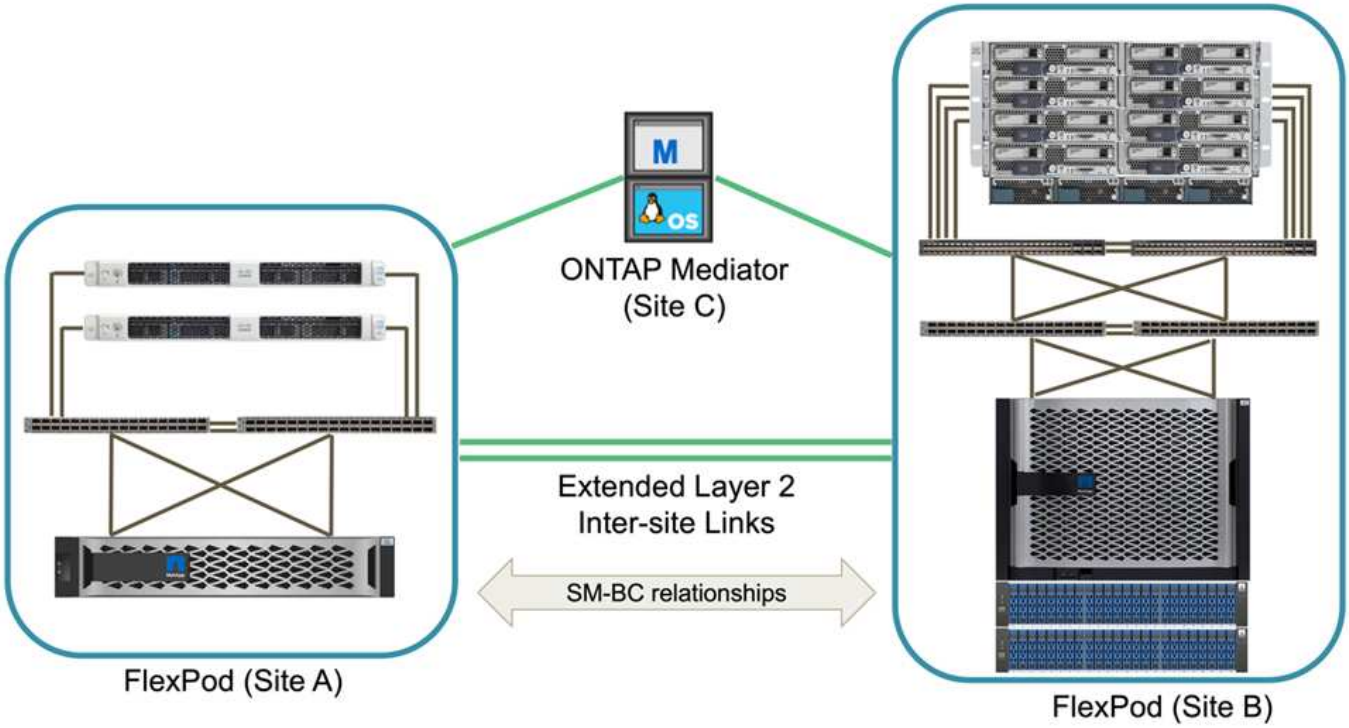
Topologies de solution

Les solutions FlexPod sont flexibles en topologie et peuvent évoluer verticalement ou horizontalement pour répondre à différents besoins. Une solution qui exige une protection de continuité de l'activité et qui ne contient que des ressources minimales de calcul et de stockage peuvent exploiter une topologie de la solution simple, comme l'illustre la figure suivante. Cette topologie simple utilise les serveurs rack UCS C-Series et les contrôleurs AFF/ASA avec des disques SSD dans le contrôleur sans tiroirs disques supplémentaires.



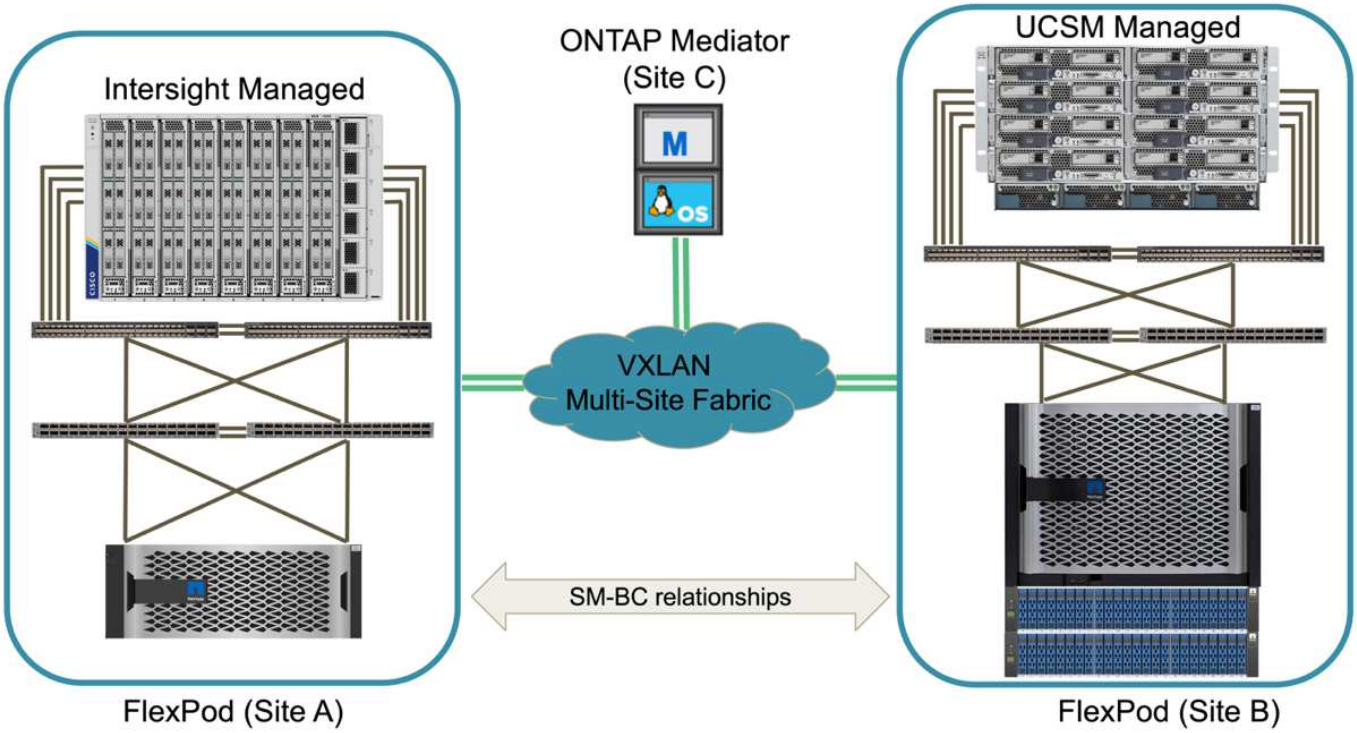
Ses composants redondants de calcul, de réseau et de stockage sont interconnectés par la connectivité redondante entre les composants. Ce design haute disponibilité assure la résilience de la solution et permet de résister à un seul point de défaillance. La conception multisite et les relations de réplication de données synchrone ONTAP SM-BC fournissent des services de données stratégiques, malgré un risque de défaillance d'un stockage sur un seul site.

Une topologie de déploiement asymétrique qui pourrait être utilisée par les entreprises entre un data Center et une succursale dans une zone métropolitaine pourrait ressembler à la figure suivante. Pour ce design asymétrique, le data Center requiert un FlexPod plus performant avec davantage de ressources de calcul et de stockage. Cependant, les besoins de la succursale sont moins importants et peuvent être satisfaits par un FlexPod beaucoup plus petit.

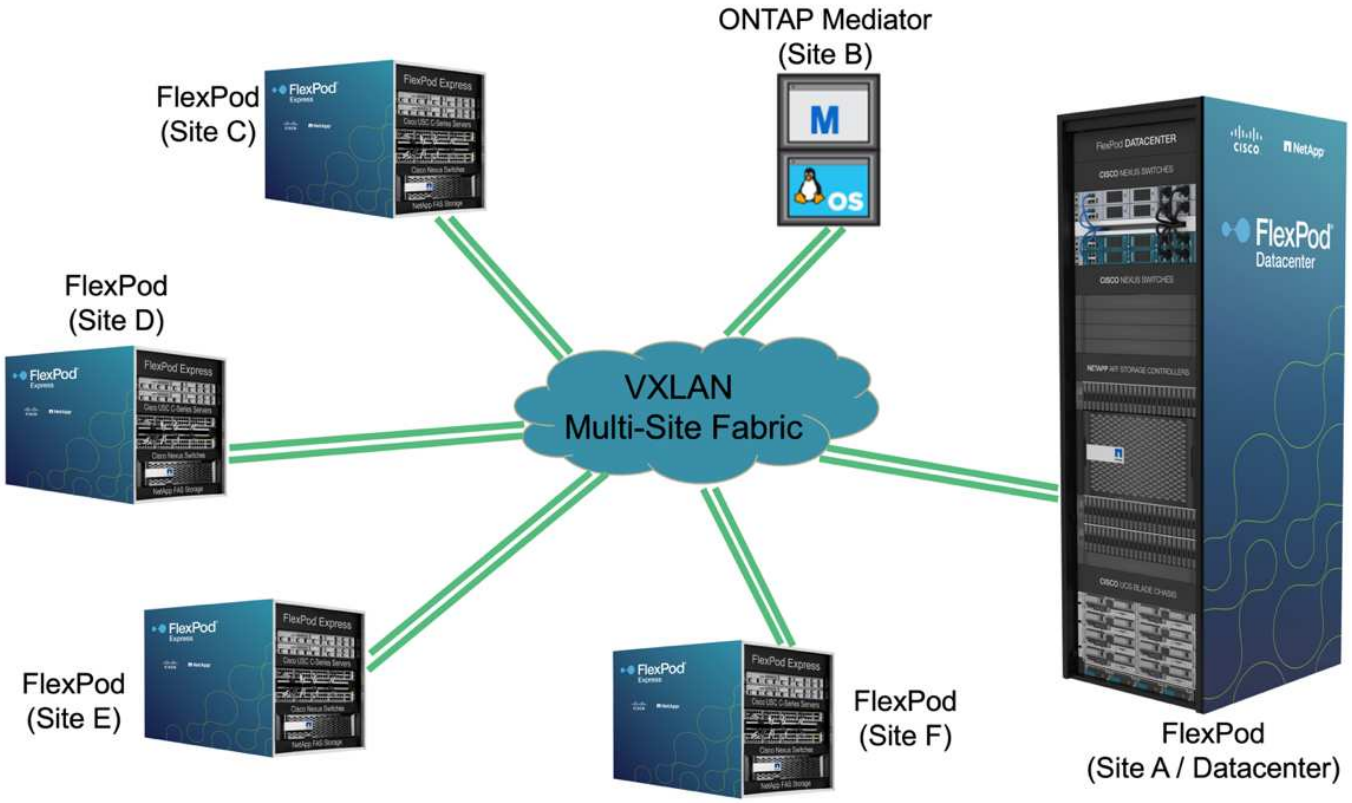


Pour les entreprises dont les besoins en ressources de calcul et de stockage sont plus importants et sur plusieurs sites, une structure multisite basée sur VXLAN permet à plusieurs sites d'avoir une structure réseau transparente afin de faciliter la mobilité des applications et de servir une application depuis n'importe quel site.

Il peut y avoir une solution FlexPod existante au moyen de châssis Cisco UCS 5108 et de serveurs lames B-Series qui doivent être protégés par une nouvelle instance FlexPod. La nouvelle instance FlexPod peut utiliser le tout dernier châssis UCS X9508 avec des nœuds de calcul X210c gérés par Cisco Intersight, comme l'illustre la figure suivante. Dans ce cas, les systèmes FlexPod de chaque site sont connectés à une structure de data Center plus vaste, et les sites sont connectés via un réseau d'interconnexion pour former une structure multisite VXLAN.



Pour les entreprises disposant d'un data Center et de plusieurs succursales dans une zone métropolitaine, qui doivent tous être protégées afin d'assurer la continuité de l'activité, La topologie de déploiement FlexPod SM-BC illustrée dans la figure suivante peut être mise en œuvre pour protéger les services d'applications et de données stratégiques afin d'atteindre un RPO nul et un RTO proche de zéro pour toutes les succursales.



Pour ce modèle de déploiement, chaque succursale établit les relations SM-BC et les groupes de cohérence dont elle a besoin avec le centre de données. Vous devez tenir compte des limites d'objets SM-BC prises en charge, de sorte que les relations de groupes de cohérence et le nombre de points de terminaison globaux ne dépassent pas les valeurs maximales prises en charge au niveau du datacenter.

"Ensuite : présentation de la validation de la solution."

Validation des solutions

Validation des solutions : présentation

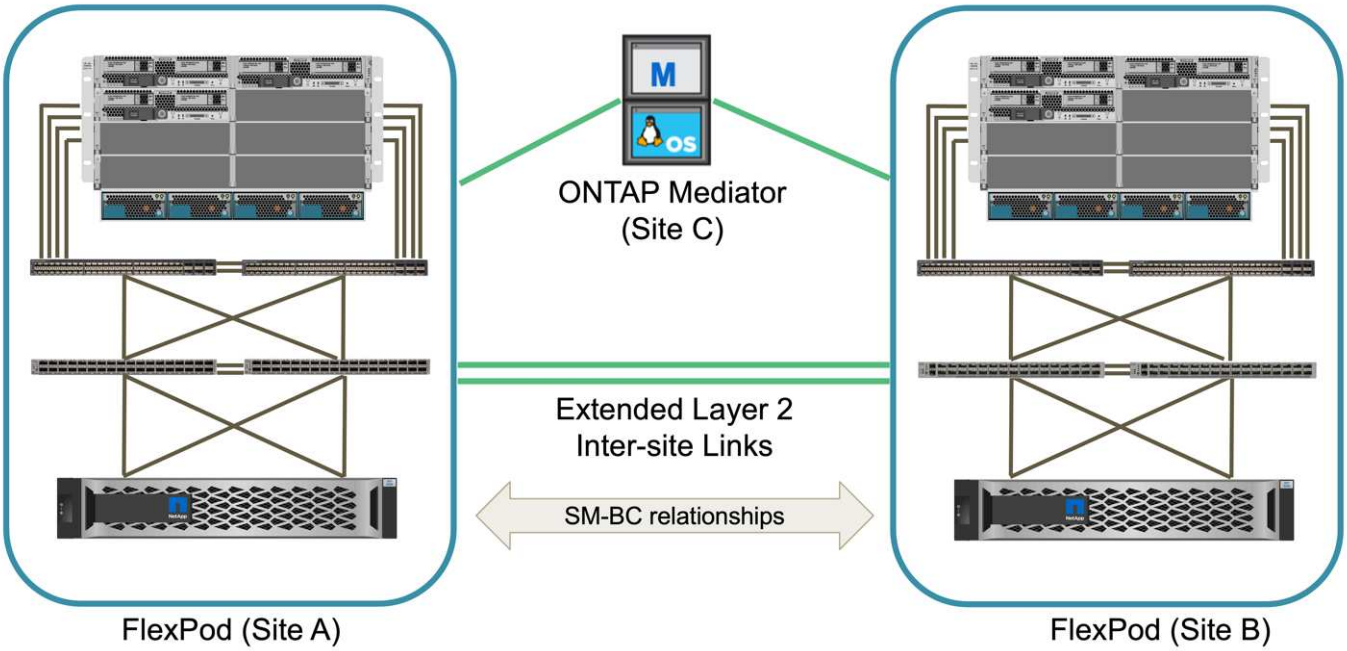
"Précédent : solution FlexPod SM-BC."

Les détails de la conception et de l'implémentation de la solution FlexPod SM-BC dépendent des objectifs spécifiques de la configuration et de la solution FlexPod. Une fois les exigences générales de continuité de l'activité définies, la solution FlexPod SM-BC peut être créée en implémentant une toute nouvelle solution avec deux nouveaux systèmes FlexPod, en ajoutant un nouveau système FlexPod sur un autre site pour une paire avec un FlexPod existant, ou en associant deux systèmes FlexPod existants.

Les solutions FlexPod étant par nature flexibles dans ses configurations, tous les composants et configurations FlexPod pris en charge peuvent être utilisés. Le reste de cette section fournit des informations sur les validations d'implémentation effectuées pour une solution d'infrastructure virtuelle basée sur VMware. À l'exception des aspects liés à SM-BC, l'implémentation suit les processus standard de déploiement FlexPod. Pour en savoir plus sur l'implémentation FlexPod, consultez les CVD et les NVA FlexPod disponibles, en fonction de vos configurations spécifiques.

Topologie de validation

À des fins de validation de la solution FlexPod SM-BC, les composants technologiques pris en charge par NetApp, Cisco et VMware sont utilisés. La solution comprend des paires HA AFF A250 de NetApp exécutant ONTAP 9.10.1, deux switchs Cisco Nexus 9336C-FX2 sur le site A et deux switchs Cisco Nexus 3232C sur le site B, ou Cisco UCS 6454 Fi sur les deux sites, Et trois serveurs Cisco UCS B200 M5 sur chaque site exécutant VMware vSphere 7.0u2 et gérés par UCS Manager et le serveur VMware vCenter. La figure suivante montre la topologie de validation de solution au niveau des composants avec deux systèmes FlexPod s'exécutant sur le site A et le site B connectés par des liens inter-sites étendus de couche 2 et un médiateur ONTAP s'exécutant sur le site C.



Matériel et logiciels

Le tableau suivant répertorie le matériel et les logiciels utilisés pour la validation de la solution. Il est important de noter que Cisco, NetApp et VMware disposent de matrices d'interopérabilité permettant de déterminer la prise en charge de toute implémentation spécifique de FlexPod :

- "http://support.netapp.com/matrix/"
- "Outil d'interopérabilité matérielle et logicielle Cisco UCS"
- "http://www.vmware.com/resources/compatibility/search.php"

Catégorie	Composant	Version logicielle	Quantité
Calcul	Fabric Interconnect Cisco UCS 6454	4.2(1f)	4 (2 par site)
	Serveurs Cisco UCS B200 M5	4.2(1f)	6 (3 par site)
	MODULE D'E/S CISCO UCS 2204XP	4.2(1f)	4 (2 par site)
	CISCO VIC 1440 (PID : UCSTM-MLOM-40G-04)	5.2(1a)	2 (1 par site)

Catégorie	Composant	Version logicielle	Quantité
	CISCO VIC 1340 (PID : UCSTM-MLOM-40G-03)	4.5(1a)	4 (2 par site)
Le réseau	Cisco Nexus 9336C-FX2	9.3(6)	2 (site A)
	Cisco Nexus 3232C	9.3(6)	2 (site B)
Stockage	NetApp AFF A250	9.10.1	4 (2 par site)
	NetApp System Manager	9.10.1	2 (1 par site)
	NetApp Active IQ Unified Manager	9.10	1
	Outils NetApp ONTAP pour VMware vSphere	9.10	1
	Plug-in NetApp SnapCenter pour VMware vSphere	4.6	1
	Médiateur ONTAP	1.3	1
	Boîte NAbox	3.0.2	1
	Récolte NetApp	21.11.1-1	1
Virtualisation	VMware ESXi	7.0U2	6 (3 par site)
	Pilote Ethernet nenic VMware ESXi	1.0.35.0	6 (3 par site)
	VMware vCenter	7.0U2	1
	Plug-in NetApp NFS pour VMware VAAI	2.0	6 (3 par site)
Test	Microsoft Windows	2022	1
	Microsoft SQL Server	2019	1
	Microsoft SQL Server Management Studio	18.10	1
	HammerDB	4.3	1
	Microsoft Windows	10	6 (3 par site)
	Iometer	1.1.0	6 (3 par site)

"Validation de la solution - calcul."

Validation des solutions : calcul

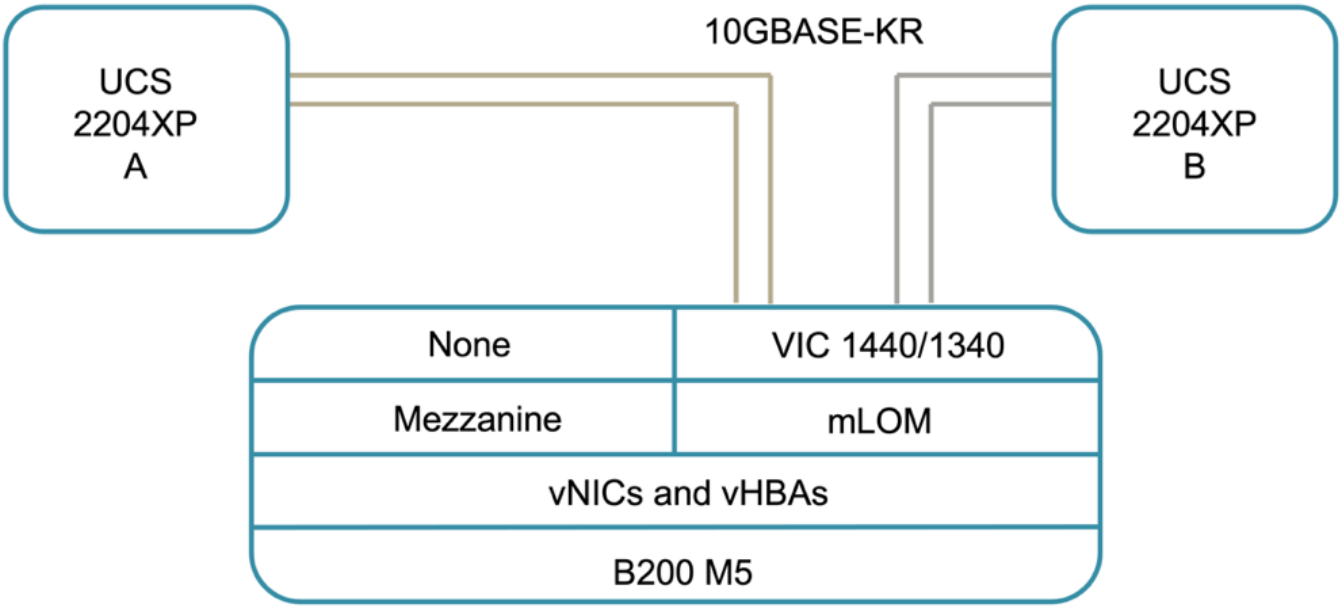
"Preivous : validation de la solution - Présentation."

La configuration de calcul de la solution FlexPod SM-BC suit les bonnes pratiques des solutions FlexPod classiques. Les sections suivantes mettent en évidence certaines des connexions et configurations utilisées pour la validation. Certaines des considérations

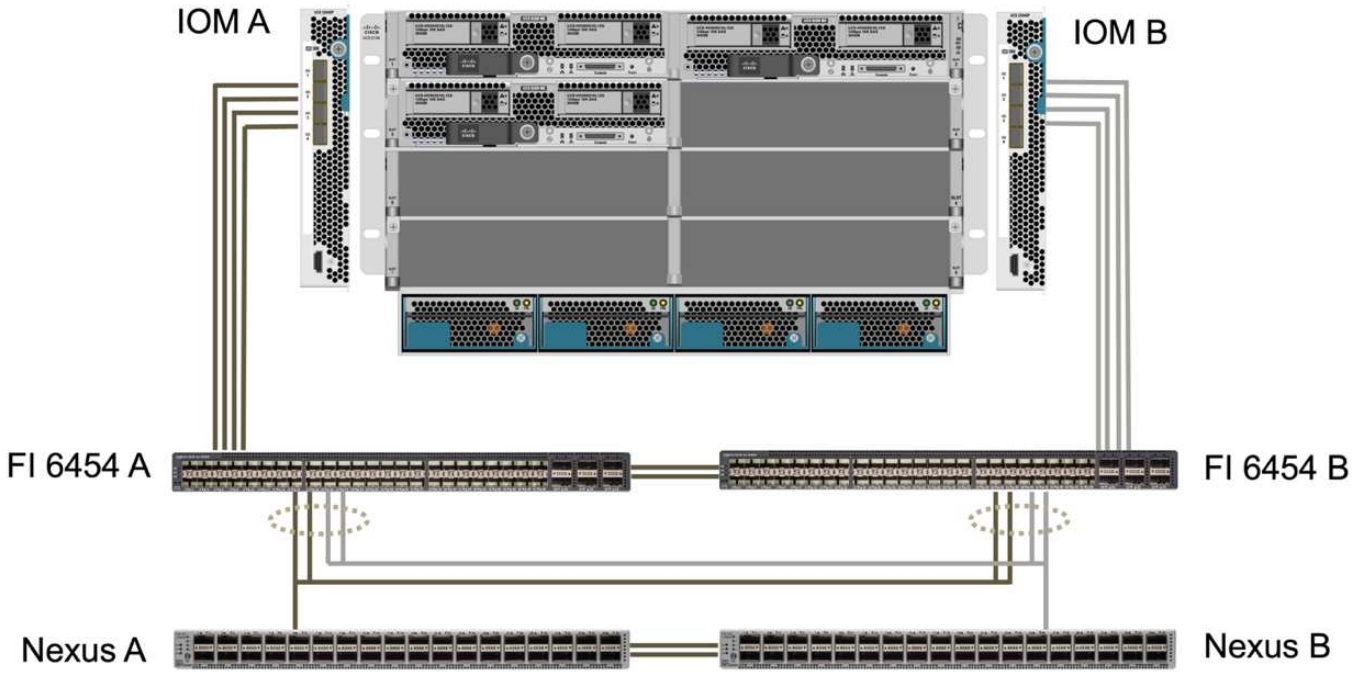
liées au SM-BC sont également mises en évidence pour fournir des références et des conseils sur la mise en œuvre.

Connectivité

La connectivité entre les serveurs lames UCS B200 et les IOM est fournie par la carte VIC UCS 5108 via les connexions de fond de panier du châssis UCS. UCS 2204XP Fabric Extender utilisé pour la validation possède 16 ports 10G chacun pour la connexion aux huit serveurs lames demi-largeur, par exemple deux pour chaque serveur. Pour augmenter la bande passante de connectivité du serveur, vous pouvez ajouter un VIC supplémentaire basé sur mezzanine pour connecter le serveur au module UCS 2408 IOM alternatif qui fournit quatre connexions 10G à chaque serveur.



La connectivité entre le châssis UCS 5108 et les IF UCS 6454 utilisés pour la validation sont assurées par le module IOM 2204XP qui utilise quatre connexions 10G. Les ports FI 1 à 4 sont configurés comme ports serveur pour ces connexions. Les ports FI 25 à 28 sont configurés en tant que ports de liaison ascendante du réseau vers les commutateurs Nexus A et B du site local. Les figures et tableaux suivants présentent le schéma de connectivité et les détails de connexion des ports pour les serveurs UCS 6454 IFF permettant de se connecter au châssis UCS 5108 et aux switchs Nexus.



Périphérique local	Port local	Périphérique distant	Port distant
UCS 6454 FI A	1	MODULE D’E/S A	1
	2		2
	3		3
	4		4
	25	Nexus A	24/13/1
	26		24/13/2
	27	Nexus B	24/13/3
	28		24/13/4
	L1	UCS 6454 FI B	L1
	L2		L2
UCS 6454 FI B	1	MODULE D’E/S B	1
	2		2
	3		3
	4		4
	25	Nexus A	24/13/3
	26		24/13/4
	27	Nexus B	24/13/1
	28		24/13/2
	L1	UCS 6454 FI A	L1

Périphérique local	Port local	Périphérique distant	Port distant
	L2		L2

Les connexions ci-dessus sont similaires pour les deux sites A et B, malgré l'utilisation du site A avec des switchs Nexus 9336C-FX2et du site B avec des switchs Nexus 3232C. Des câbles de dérivation 40G à 4x10G sont utilisés pour les connexions Nexus vers FI. Les connexions FI au Nexus utilisent le canal de port et les canaux de port virtuel sont configurés sur les commutateurs Nexus afin d'agréger les connexions à chaque FI.

Si vous utilisez une autre combinaison de composants IOM, FI et Nexus, veillez à utiliser les câbles et la vitesse de port appropriés pour la combinaison d'environnement.

Une bande passante supplémentaire peut être obtenue en utilisant des composants qui prennent en charge des connexions plus rapides ou plus de connexions. Pour assurer une redondance supplémentaire, il est possible d'ajouter des connexions supplémentaires avec des composants qui les prennent en charge.

Profils de services

Un châssis de serveur lame avec des Fabric Interconnect gérés par UCS Manager (UCSM) ou Cisco Intersight peut extraire les serveurs à l'aide des profils de service disponibles dans UCSM et les profils de serveurs. Cette validation utilise UCSM et les profils de service pour simplifier la gestion des serveurs. Avec les profils de service, il est possible de remplacer ou mettre à niveau un serveur simplement en associant le profil de service d'origine au nouveau matériel.

Les profils de service créés prennent en charge les éléments suivants pour les hôtes VMware ESXi :

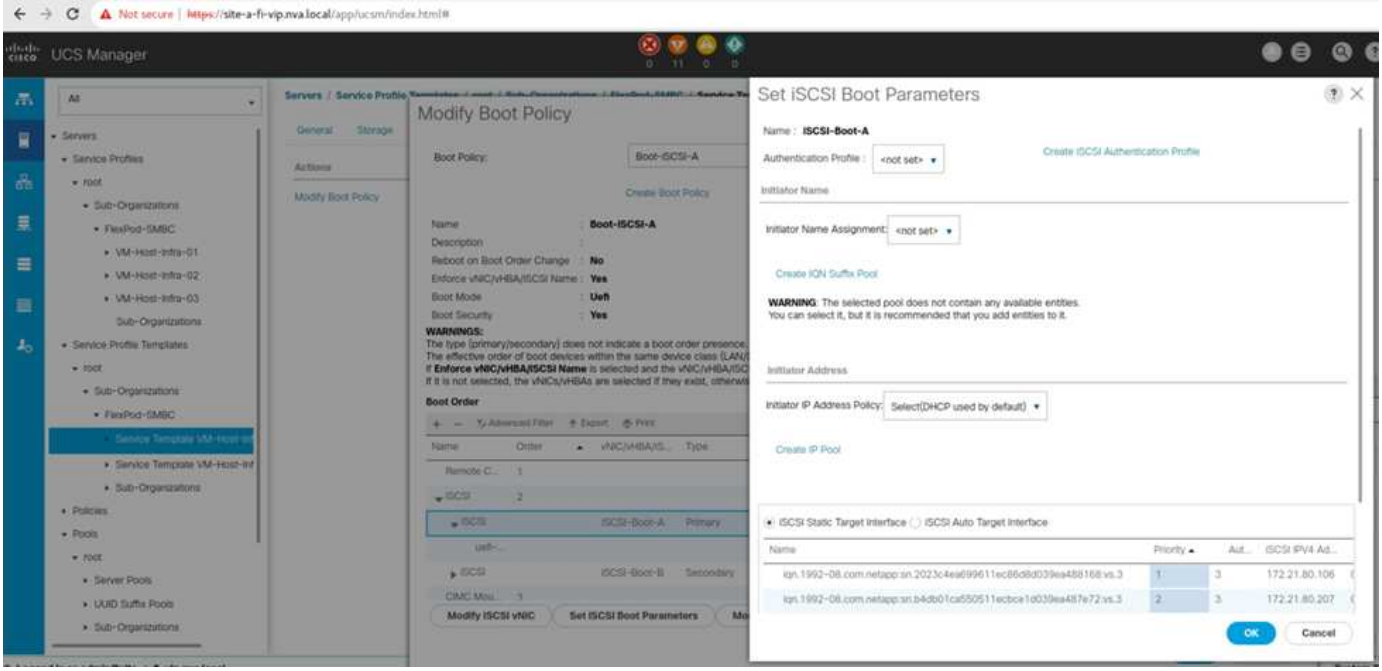
- Démarrage SAN depuis le système de stockage AFF A250 sur n'importe quel site, au moyen du protocole iSCSI.
- Six vNIC sont créés pour les serveurs où :
  - Deux cartes vNIC redondantes (vSwitch0-A et vSwitch0-B) transportent le trafic de gestion sur bande. Éventuellement, ces vNIC peuvent également être utilisés par des données de protocole NFS qui ne sont pas protégées par SM-BC.
  - Deux vNIC redondants (VDS-A et VDS-B) sont utilisés par le commutateur distribué vSphere pour supporter le trafic VMware vMotion et d'autres applications.
  - ISCSI-A vNIC utilisé par iSCSI-A vSwitch pour fournir un accès au chemin iSCSI-A.
  - VNIC iSCSI-B utilisé par le vSwitch iSCSI-B pour fournir un accès au chemin iSCSI-B.

Démarrage SAN

Dans le cas de la configuration de démarrage SAN iSCSI, les paramètres de démarrage iSCSI sont définis pour autoriser le démarrage iSCSI à partir des deux matrices iSCSI. Pour prendre en charge le scénario de basculement SM-BC dans lequel une LUN de démarrage SAN iSCSI est desservie à partir du cluster secondaire lorsque le cluster principal n'est pas disponible, la configuration cible statique iSCSI doit inclure des cibles à partir du site A et du site B. De plus, pour optimiser la disponibilité des LUN de démarrage, configurez les paramètres de démarrage iSCSI pour qu'ils démarrent à partir de tous les contrôleurs de stockage.

La cible statique iSCSI peut être configurée dans la stratégie d'amorçage des modèles de profil de service sous la boîte de dialogue définir le paramètre d'amorçage iSCSI, comme illustré dans la figure suivante. La

configuration recommandée des paramètres d'amorçage iSCSI est indiquée dans le tableau suivant, qui implémente la stratégie d'amorçage décrite ci-dessus pour obtenir une haute disponibilité.



Structure iSCSI	Priorité	Cible iSCSI	LIF iSCSI
ISCSI A	1	Site Une cible iSCSI	Site A Controller 1 iSCSI A LIF
	2	Cible iSCSI du site B	Contrôleur B 2 iSCSI A LIF
ISCSI B	1	Cible iSCSI du site B	Contrôleur B 1 LIF iSCSI B du site B
	2	Site Une cible iSCSI	Site A contrôleur 2 iSCSI B LIF

"Suivant : validation de la solution - réseau."

Validation de la solution : réseau

"Précédente : validation de la solution - calcul."

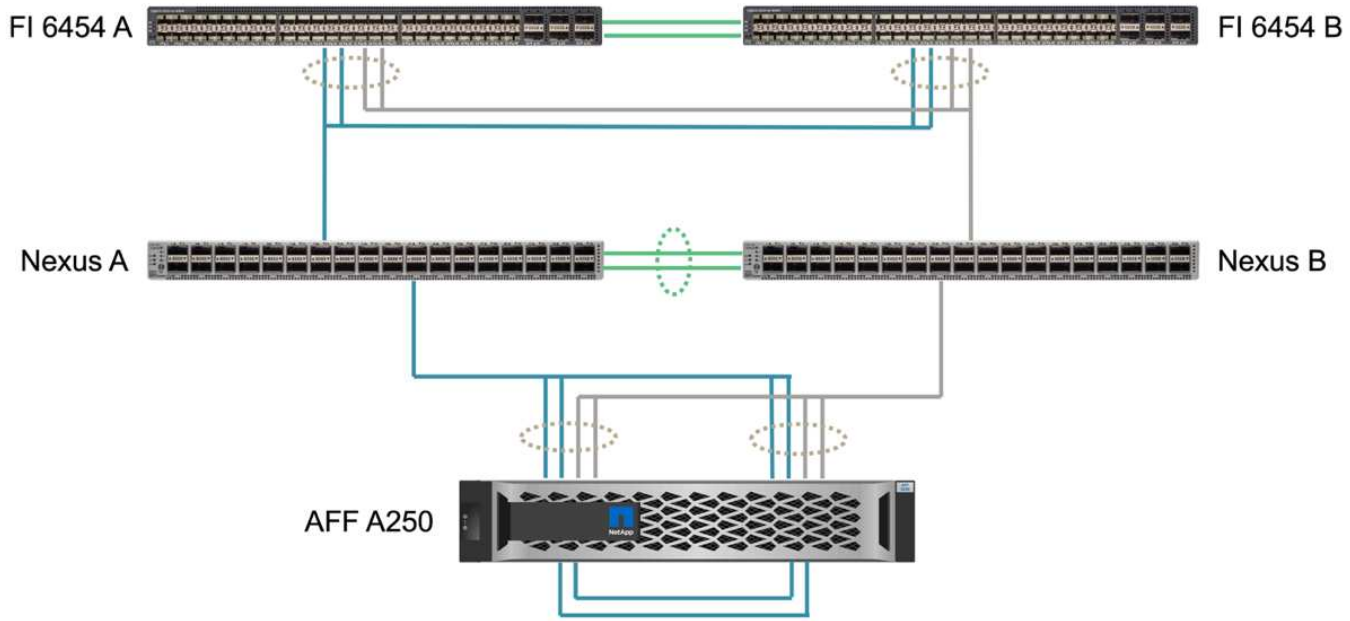
La configuration réseau de la solution FlexPod SM-BC suit les meilleures pratiques typiques des solutions FlexPod sur chaque site. Pour la connectivité entre sites, la configuration de validation de la solution connecte les switchs FlexPod Nexus sur les deux sites afin d'assurer une connectivité entre sites qui étend les VLAN entre les deux sites. Les sections suivantes mettent en évidence certaines des connexions et configurations utilisées pour la validation.

Connectivité

Les switchs FlexPod Nexus de chaque site procurent une connectivité locale entre le calcul UCS et le stockage ONTAP dans une configuration haute disponibilité. Les composants redondants et la connectivité

redondante offrent la résilience aux scénarios de point de défaillance unique.

Le schéma suivant présente la connectivité locale du commutateur Nexus sur chaque site. Outre ce qui est illustré dans le schéma, il existe aussi des connexions au réseau de gestion et de console pour chaque composant qui ne sont pas affichés. Les câbles de dérivation 40G à 4 x 10G sont utilisés pour connecter les commutateurs Nexus aux serveurs d'accès UCS ainsi qu'aux contrôleurs de stockage ONTAP AFF A250. Il est également possible d'utiliser des câbles de dérivation 100G à 4 x 25G pour accroître la vitesse de communication entre les commutateurs Nexus et les contrôleurs de stockage AFF A250. Pour plus de simplicité, les deux contrôleurs AFF A250 sont présentés côte à côte pour illustrer le câblage. Les deux connexions entre les deux contrôleurs de stockage permettent au système de stockage de former un cluster sans commutateur.

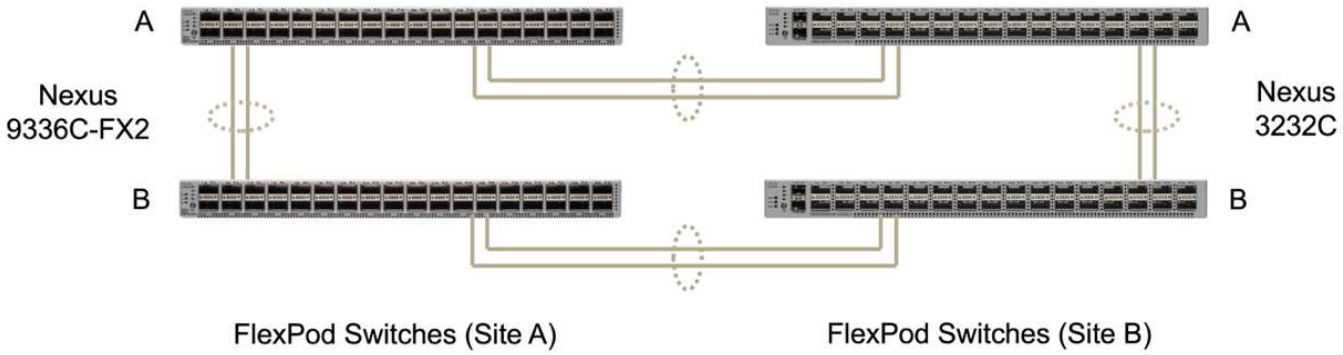


Le tableau suivant montre la connectivité entre les switchs Nexus et les contrôleurs de stockage AFF A250 sur chaque site.

Périphérique local	Port local	Périphérique distant	Port distant
Nexus A	24/10/1	AFF A250 A	e1a
	24/10/2		e1b
	24/10/3	AFF A250 B	e1a
	24/10/4		e1b
Nexus B	24/10/1	AFF A250 A	e1c
	24/10/2		e1d
	24/10/3	AFF A250 B	e1c
	24/10/4		e1d

La connectivité entre les commutateurs FlexPod du site A et du site B est illustrée dans la figure suivante avec les détails de câblage répertoriés dans le tableau ci-dessous. Les connexions entre les deux commutateurs de chaque site correspondent aux liaisons VPC Peer. D'autre part, les connexions entre les commutateurs entre les sites fournissent les liaisons intersites. Les liaisons étendent les VLAN sur plusieurs sites pour la

communication intercluster, la réplication des données SM-BC, la gestion intrabande et l'accès aux données pour les ressources des sites distants.



Périphérique local	Port local	Périphérique distant	Port distant
Commutateur a du site	33	Commutateur a du site B	31
	34		32
	25	Commutateur du site A B	25
	26		26
Commutateur du site A B	33	Commutateur du site B	31
	34		32
	25	Commutateur a du site	25
	26		26
Commutateur a du site B	31	Commutateur a du site	33
	32		34
	25	Commutateur du site B	25
	26		26
Commutateur du site B	31	Commutateur du site A B	33
	32		34
	25	Commutateur a du site B	25
	26		26

Le tableau ci-dessus répertorie la connectivité du point de vue de chaque commutateur FlexPod. Par conséquent, le tableau contient des informations dupliquées pour leur lisibilité.

Canal de port et canal de port virtuel

Le canal de port active l'agrégation de liens à l'aide du protocole LACP (Link Aggregation Control Protocol) pour l'agrégation de la bande passante et la résilience des pannes de liaison. Le canal de port virtuel (VPC) permet que les connexions des canaux de port entre deux commutateurs Nexus apparaissent logiquement comme une seule. Ceci améliore davantage la résilience des pannes pour les situations telles qu'une panne de liaison unique ou une défaillance de commutateur unique.

Le trafic du serveur UCS vers le système de stockage chemins entre l'E/S A et LES E/S B et LA FI B avant d'atteindre les commutateurs Nexus. Au fur et à mesure que les connexions FI aux commutateurs Nexus utilisent le canal de port du côté FI et le canal de port virtuel du côté du commutateur Nexus, le serveur UCS peut utiliser efficacement les chemins via les deux commutateurs Nexus et résister aux scénarios de défaillance unique. Entre les deux sites, les commutateurs Nexus sont interconnectés, comme illustré dans la figure précédente. Il y a deux liaisons pour connecter les paires de commutateurs entre les sites et ils utilisent également une configuration de canal de port.

La connectivité des protocoles de stockage des données intrabande, inter-cluster et iSCSI/NFS est assurée par l'interconnexion des contrôleurs de stockage de chaque site aux switchs Nexus locaux dans une configuration redondante. Chaque contrôleur de stockage est relié à deux commutateurs Nexus. Les quatre connexions sont configurées en tant que partie d'un groupe d'interface sur le stockage pour une résilience améliorée. Du côté du commutateur Nexus, ces ports font également partie d'un VPC entre les commutateurs.

Le tableau suivant répertorie l'ID et l'utilisation du canal de port sur chaque site.

ID de canal de port	Du stockage
10	Lien homologue Nexus local
15	Fabric Interconnect A liens
16	Liaisons Fabric Interconnect B
27	Le contrôleur de stockage A relie
28	Liaisons du contrôleur de stockage B
100	Liaisons a du commutateur inter-site
200	Liaisons du commutateur intersite B

VLAN

Le tableau suivant répertorie les réseaux VLAN configurés pour la configuration de l'environnement de validation de la solution FlexPod SM-BC et leur utilisation.

Nom	ID VLAN	Du stockage
VLAN natif	2	VLAN 2 utilisé comme VLAN natif au lieu du VLAN par défaut (1)
OOB-MGMT-VLAN	3333	VLAN de gestion hors bande pour les périphériques
IB-MGMT-VLAN	3334	VLAN de gestion intrabande pour les hôtes ESXi, la gestion des VM, etc
NFS-VLAN	3335	VLAN NFS facultatif pour le trafic NFS
ISCSI-A-VLAN	3336	San iSCSI-A Fabric pour le trafic iSCSI
ISCSI-B-VLAN	3337	San fabric iSCSI-B pour le trafic iSCSI

Nom	ID VLAN	Du stockage
VMotion-VLAN	3338	VLAN pour le trafic VMware vMotion
VM-trafic-VLAN	3339	VLAN pour le trafic des machines virtuelles VMware
VLAN-intercluster	3340	VLAN intercluster pour les communications entre clusters ONTAP

Bien que SM-BC ne prend pas en charge les protocoles NFS ou CIFS pour la continuité de l'activité, vous pouvez les utiliser pour les workloads qui n'ont pas besoin d'être protégés pour la continuité de l'activité. Les datastores NFS n'ont pas été créés pour cette validation.

"Suivant : validation de la solution - stockage."

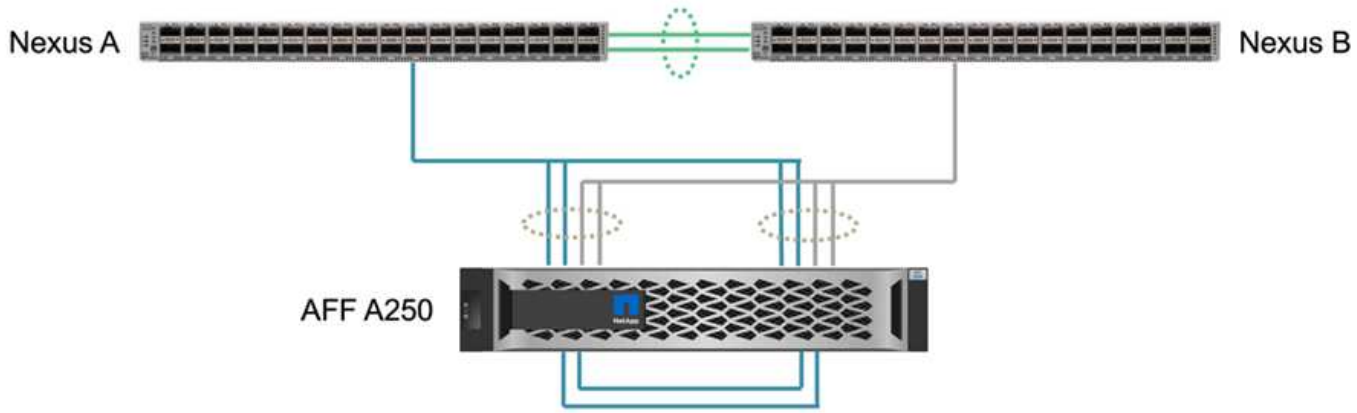
Validation de la solution : stockage

"Précédent : validation de la solution - réseau."

La configuration du stockage pour la solution FlexPod SM-BC suit les meilleures pratiques typiques des solutions FlexPod sur chaque site. Pour le peering de clusters et la réplication des données de SM-BC, ils utilisent les liaisons intersites établies entre les commutateurs FlexPod sur les deux sites. Les sections suivantes mettent en évidence certaines des connexions et configurations utilisées pour la validation.

Connectivité

La connectivité de stockage aux IF et aux serveurs lames UCS locaux est fournie par les commutateurs Nexus sur le site local. La connectivité du switch Nexus entre les sites permet au stockage d'être accessible par les serveurs lames UCS distants. La figure et le tableau ci-dessous présentent le schéma de connectivité du stockage et une liste des connexions des contrôleurs de stockage de chaque site.



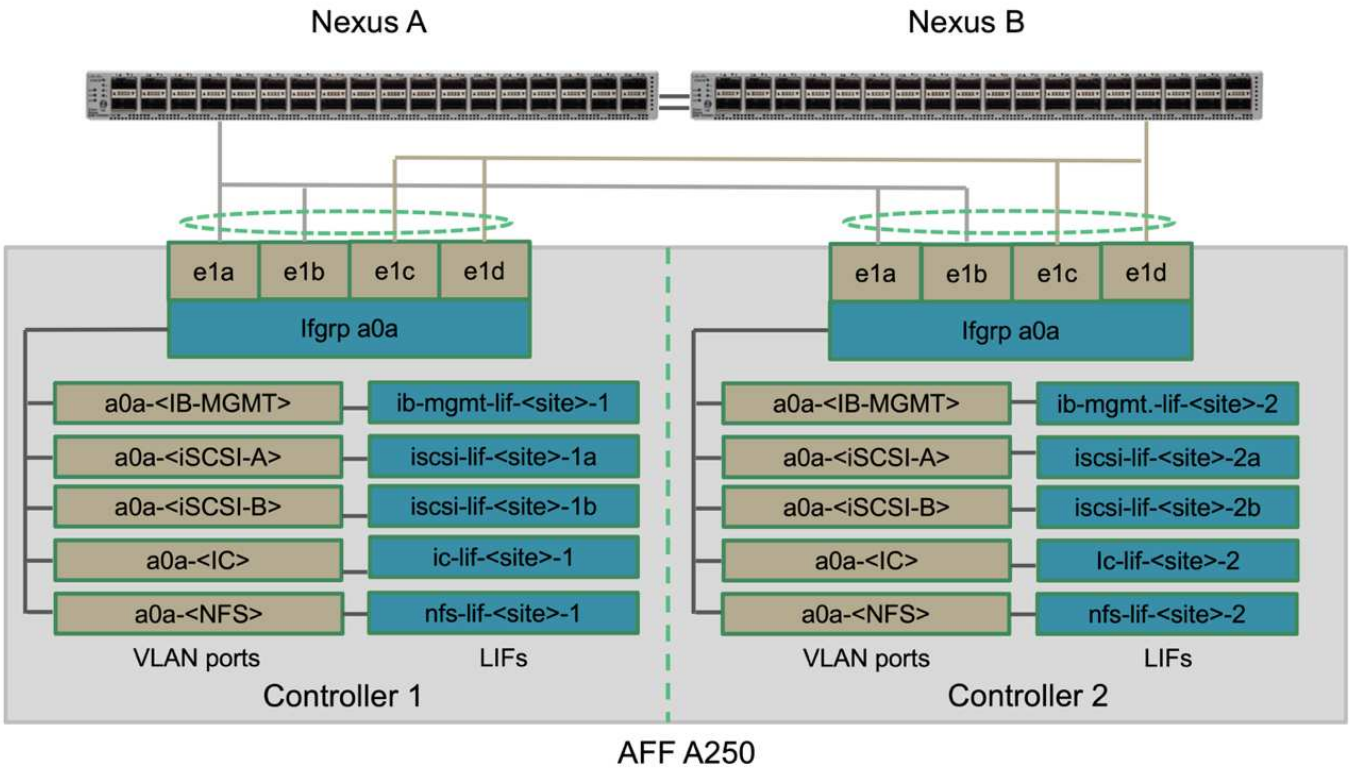
Périphérique local	Port local	Périphérique distant	Port distant
AFF A250 A	e0c	AFF A250 B	e0c

Périphérique local	Port local	Périphérique distant	Port distant
	e0d		e0d
	e1a	Nexus A	24/10/1
	e1b		24/10/2
	e1c	Nexus B	24/10/1
	e1d		24/10/2
AFF A250 B	e0c	AFF A250 A	e0c
	e0d		e0d
	e1a	Nexus A	24/10/3
	e1b		24/10/4
	e1c	Nexus B	24/10/3
	e1d		24/10/4

Connexions et interfaces

Deux ports physiques de chaque contrôleur de stockage sont connectés à chaque commutateur Nexus afin d'assurer l'agrégation de la bande passante et la redondance pour cette validation. Ces quatre connexions participent à une configuration de groupe d'interface sur le système de stockage. Les ports correspondants des commutateurs Nexus font partie d'un VPC pour assurer l'agrégation de liens et la résilience.

Les protocoles de stockage des données intrabande et inter-cluster et NFS/iSCSI utilisent des VLAN. Les ports VLAN sont créés sur le groupe d'interface pour isoler les différents types de trafic. Les interfaces logiques (LIF) des fonctions respectives sont créées en plus des ports VLAN correspondants. La figure suivante montre la relation entre les connexions physiques, les groupes d'interfaces, les ports VLAN et les interfaces logiques.

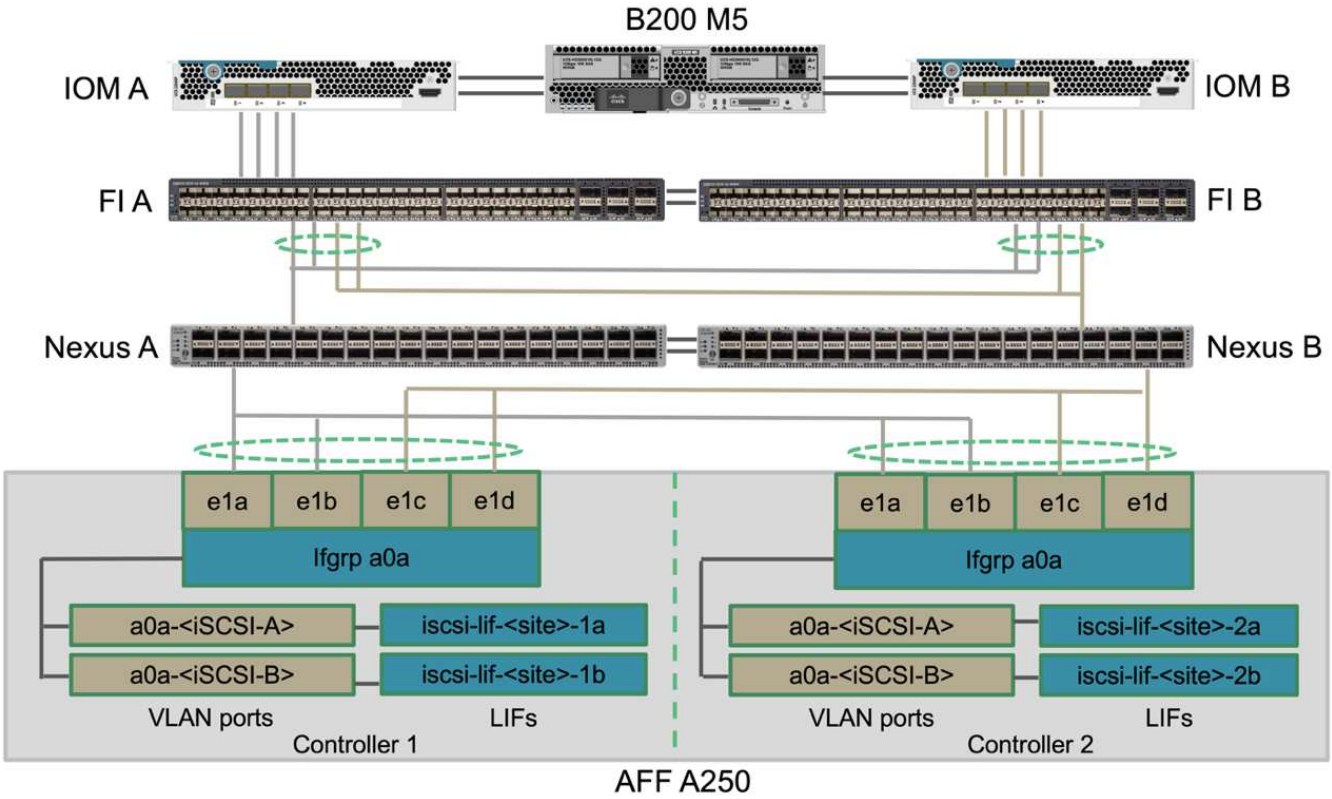


Démarrage SAN

NetApp recommande l'implémentation d'un démarrage SAN pour les serveurs Cisco UCS dans la solution FlexPod. L'implémentation du démarrage SAN vous permet de sécuriser le système d'exploitation au sein du système de stockage NetApp, vous offrant ainsi de meilleures performances et une plus grande flexibilité. Pour cette solution, le démarrage SAN iSCSI a été validé.

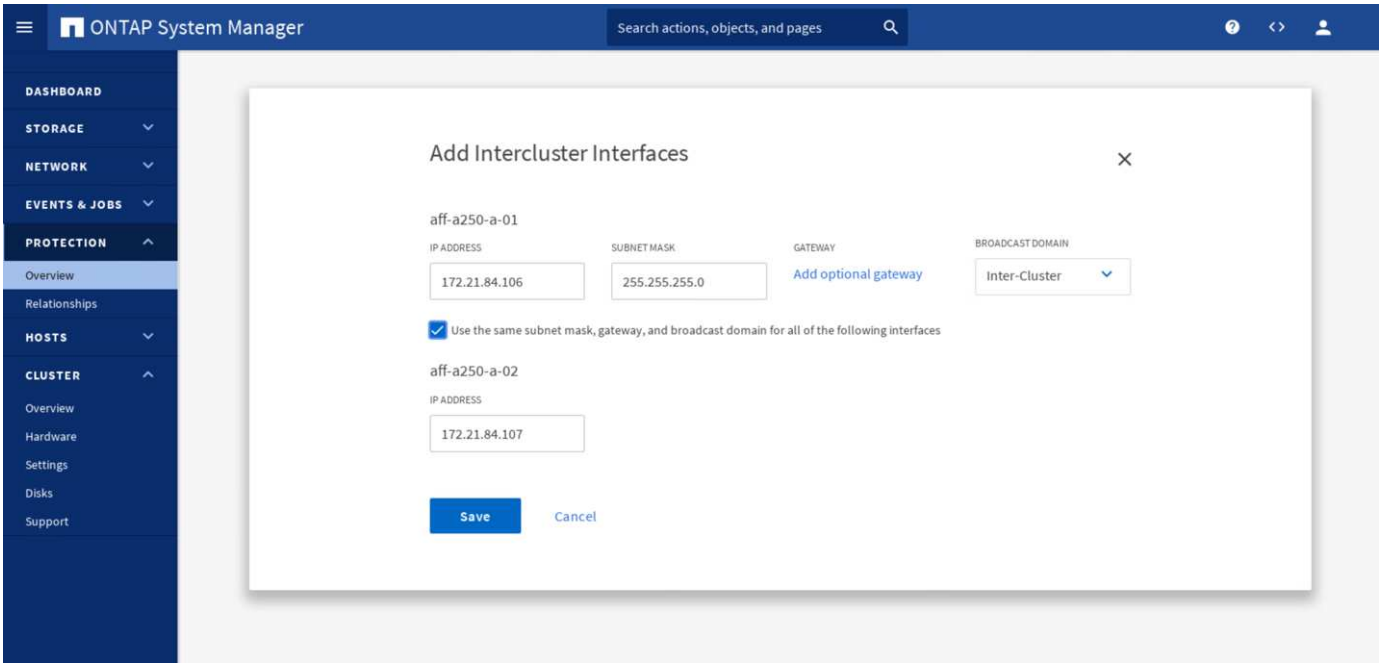
La figure suivante décrit la connectivité du démarrage SAN iSCSI du serveur Cisco UCS du stockage NetApp. Lors du démarrage SAN iSCSI, chaque serveur Cisco UCS est affecté à deux vNIC iSCSI (une pour chaque structure SAN) qui fournissent une connectivité redondante depuis le serveur jusqu'au stockage. Les ports de stockage Ethernet 10/25-G connectés aux commutateurs Nexus (dans cet exemple e1a, e1b, e1c et e1d) sont regroupés pour former un groupe d'interface (ifgrp) (dans cet exemple, a0A). Les ports VLAN iSCSI sont créés sur le ifgrp et les LIFs iSCSI sont créés sur les ports VLAN iSCSI.

Chaque LUN de démarrage iSCSI est mappée sur le serveur qui s'amorce à partir de celle-ci via les LIFs iSCSI en associant la LUN de démarrage aux noms qualifiés iSCSI (IQN) du serveur dans son groupe initiateur de démarrage. Le groupe initiateur d'initialisation du serveur contient deux IQN, un pour chaque structure vNIC/SAN. Cette fonctionnalité permet uniquement au serveur autorisé d'accéder à la LUN de démarrage créée spécifiquement pour ce serveur.



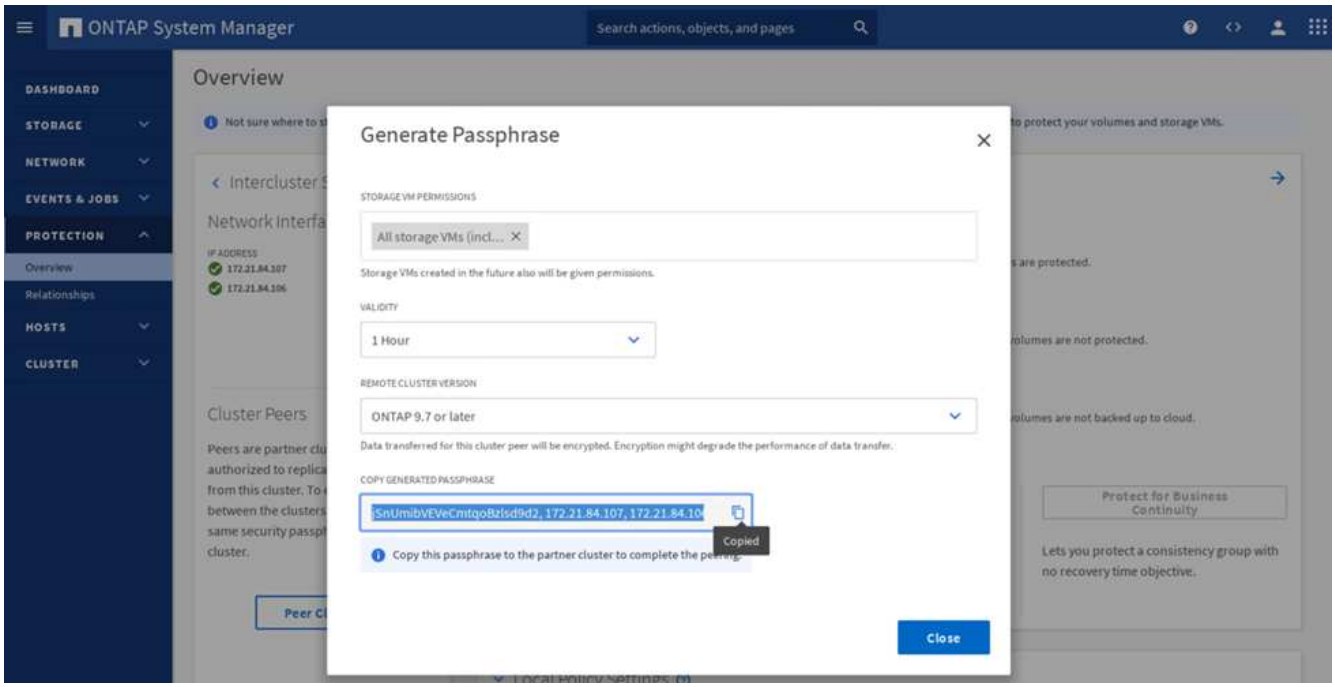
Peering de clusters

Les pairs de cluster ONTAP communiquent via les LIFs intercluster. En utilisant ONTAP System Manager pour les deux clusters, vous pouvez créer les LIF intercluster nécessaires sous le volet protection > Présentation.

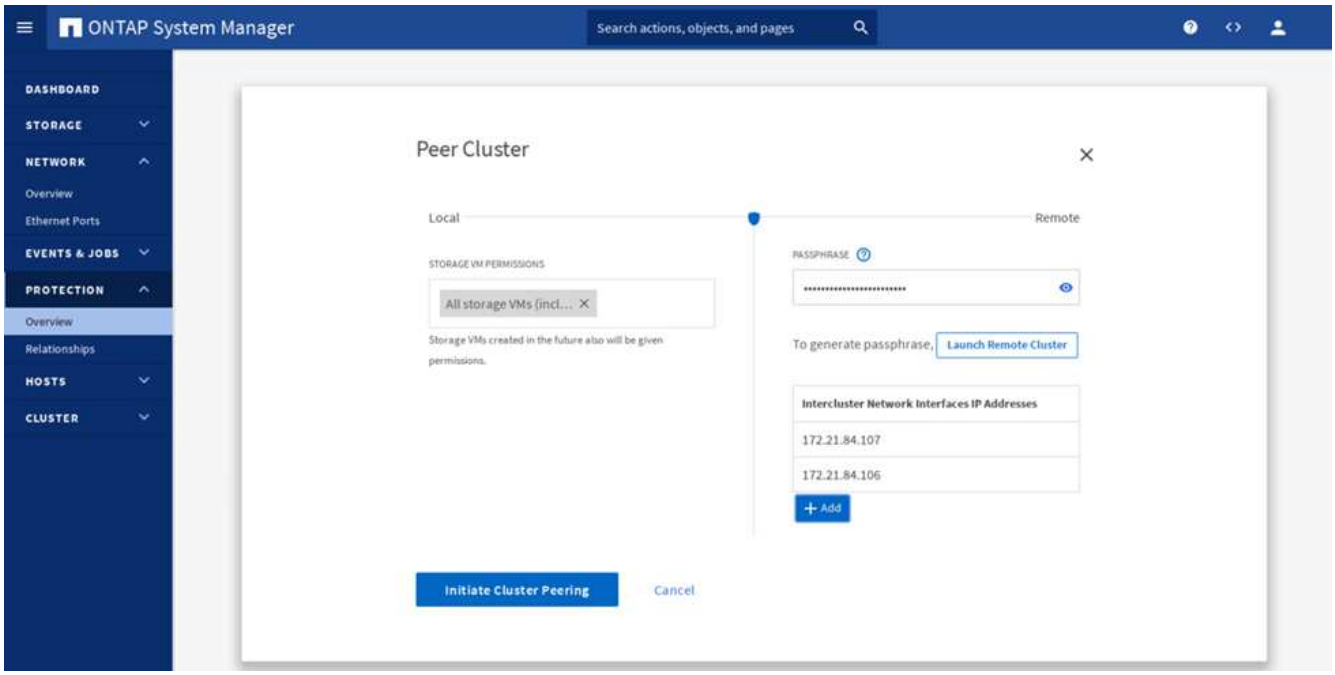


Pour pairs les deux clusters, effectuez la procédure suivante :

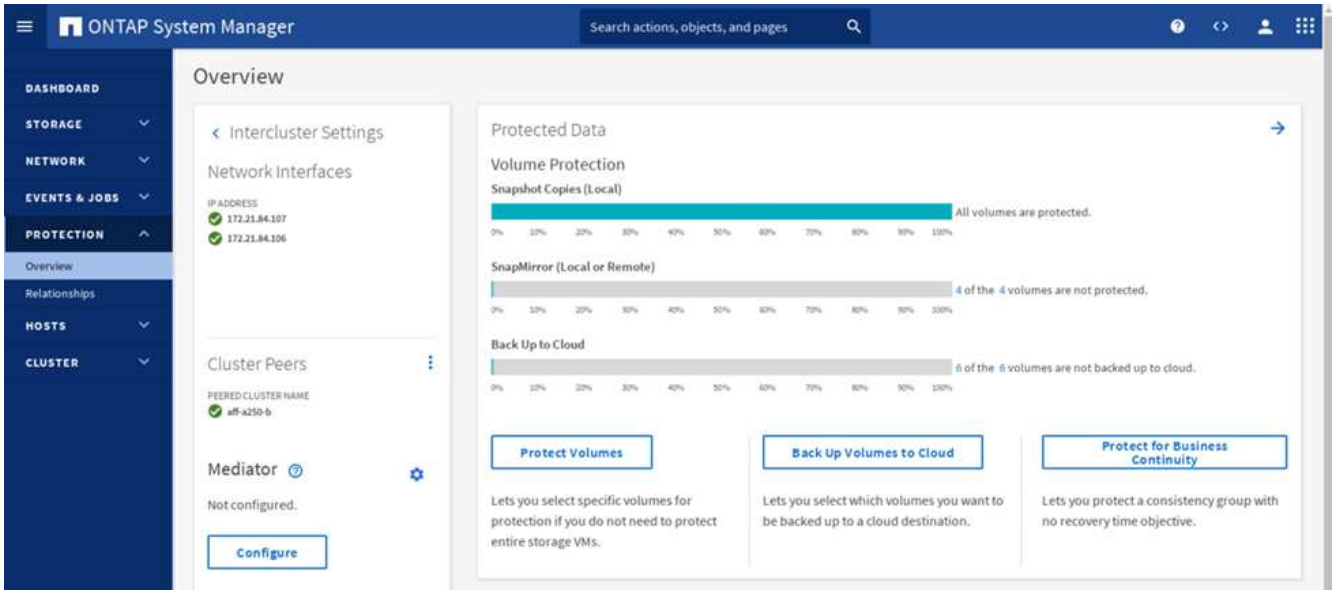
1. Générer la phrase de passe de peering de cluster dans le premier cluster.



2. Appeler l'option Peer Cluster dans le second cluster et fournir la phrase de passe et les informations LIF intercluster



3. Le volet protection > Présentation de System Manager affiche les informations sur les pairs de cluster.

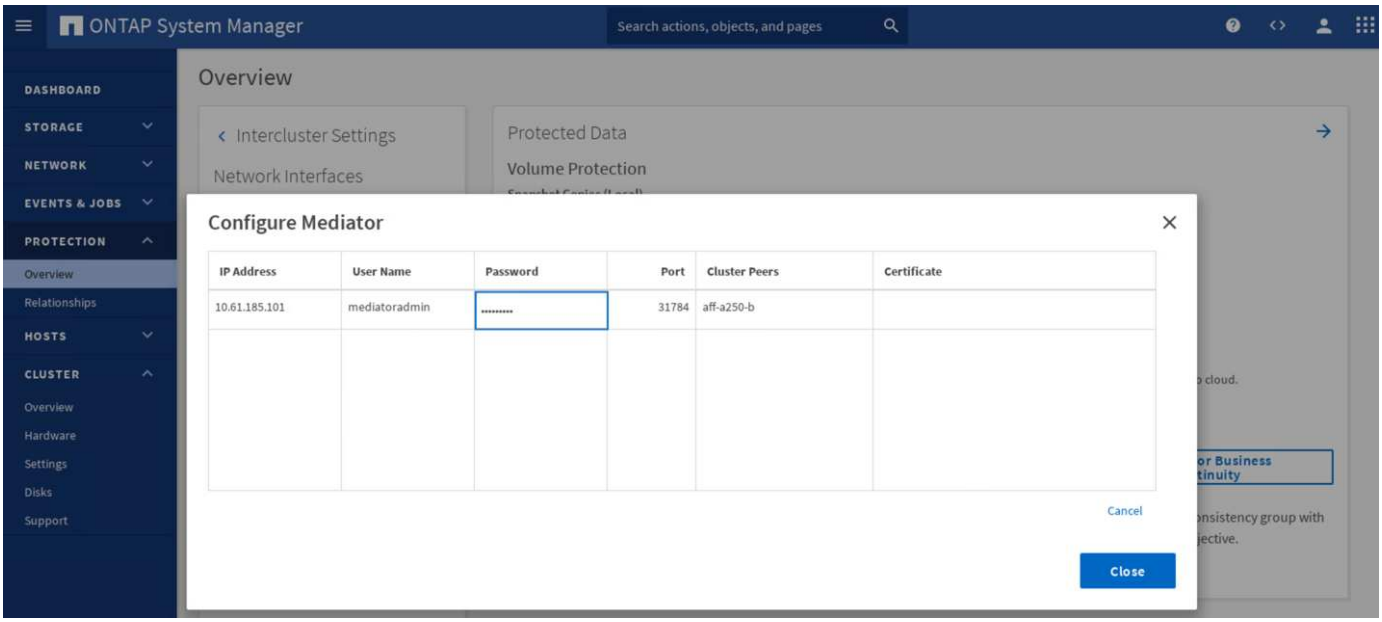


Installation et configuration du médiateur ONTAP

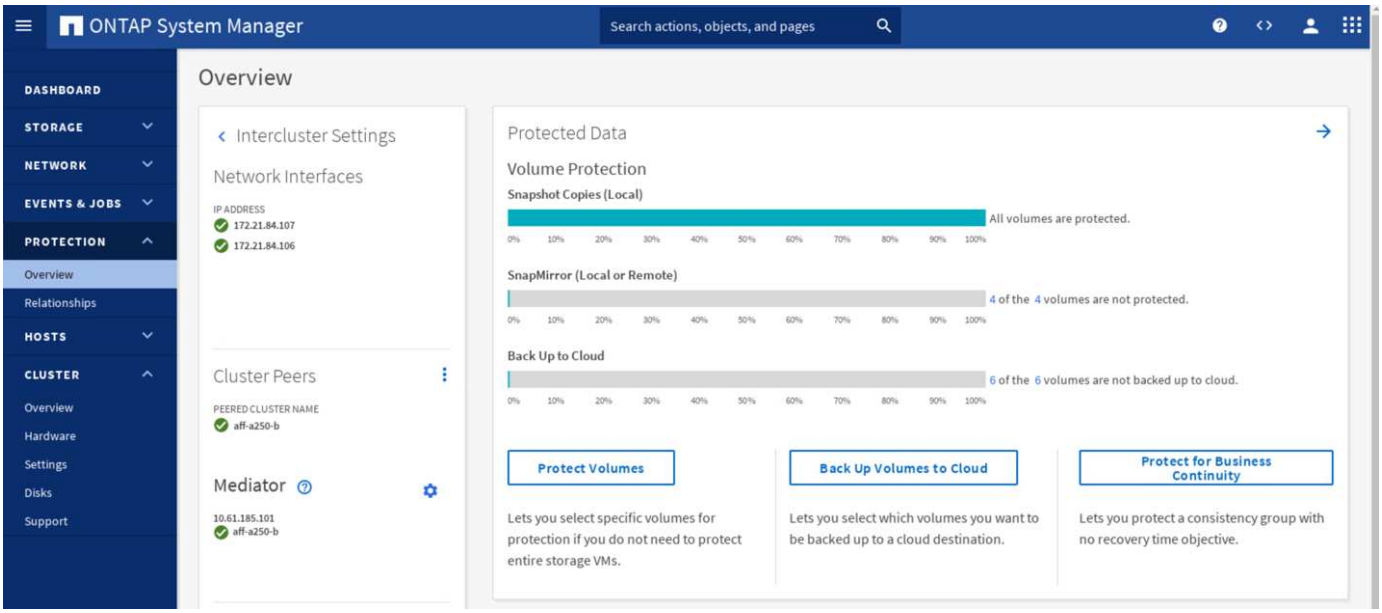
Le médiateur ONTAP établit un quorum pour les clusters ONTAP dans une relation SM-BC. Il coordonne le basculement automatique en cas de défaillance et aide à éviter les scénarios où chaque cluster tente simultanément d'établir le contrôle en tant que cluster principal.

Avant d'installer le médiateur ONTAP, consultez le "Installez ou mettez à niveau le service ONTAP Mediator" Page pour les prérequis, les versions Linux prises en charge et les procédures d'installation sur les différents systèmes d'exploitation Linux pris en charge.

Une fois le médiateur ONTAP installé, vous pouvez ajouter le certificat de sécurité du médiateur ONTAP aux clusters ONTAP, puis configurer le médiateur ONTAP dans le volet protection du gestionnaire système > vue d'ensemble. La capture d'écran suivante montre l'interface graphique de configuration du médiateur ONTAP.



Après avoir indiqué les informations nécessaires, le médiateur ONTAP configuré apparaît dans le volet protection du gestionnaire de système > vue d'ensemble.



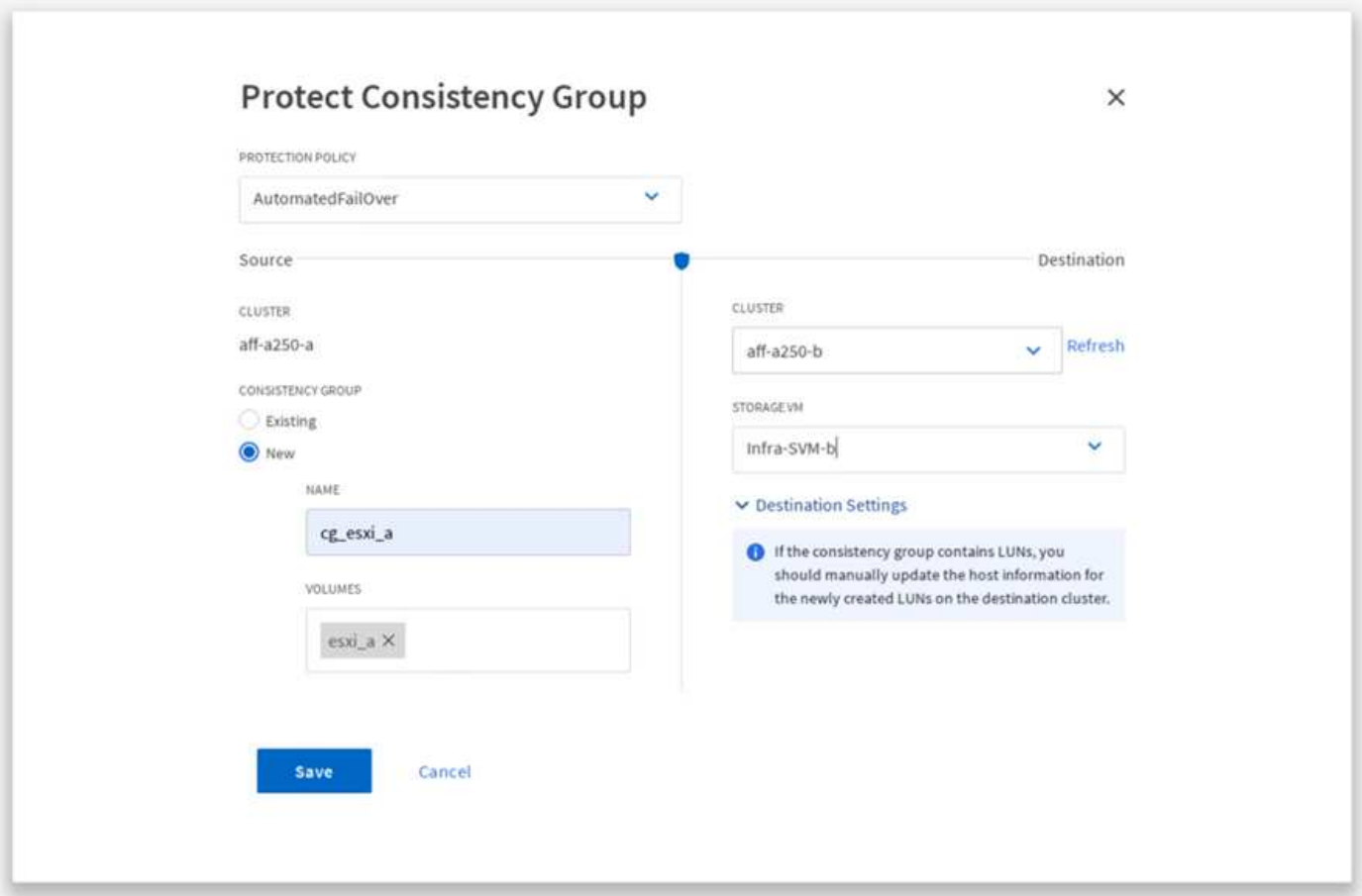
Groupe de cohérence SM-BC

Un groupe de cohérence assure la cohérence d'ordre d'écriture d'une charge de travail d'application couvrant un ensemble de volumes spécifiés. Pour ONTAP 9.10.1, voici quelques-unes des restrictions importantes.

- Le nombre maximal de relations de groupe de cohérence SM-BC dans un cluster est de 20.
- Le nombre maximal de volumes pris en charge par relation SM-BC est de 16.
- Le nombre maximal de terminaux source et de destination dans un cluster est de 200.

Pour plus de détails, consultez la documentation du SM-BC de ONTAP sur le "restrictions et limites".

Pour la configuration de validation, ONTAP System Manager a été utilisé pour créer les groupes de cohérence afin de protéger à la fois les LUN de démarrage ESXi et les LUN de datastore partagé pour les deux sites. La boîte de dialogue de création de groupes de cohérence est accessible en sélectionnant protection > Présentation > protection pour la continuité de l'activité > protéger le groupe de cohérence. Pour créer un groupe de cohérence, fournissez les volumes source, le cluster de destination et les informations de machine virtuelle de stockage de destination nécessaires à la création.

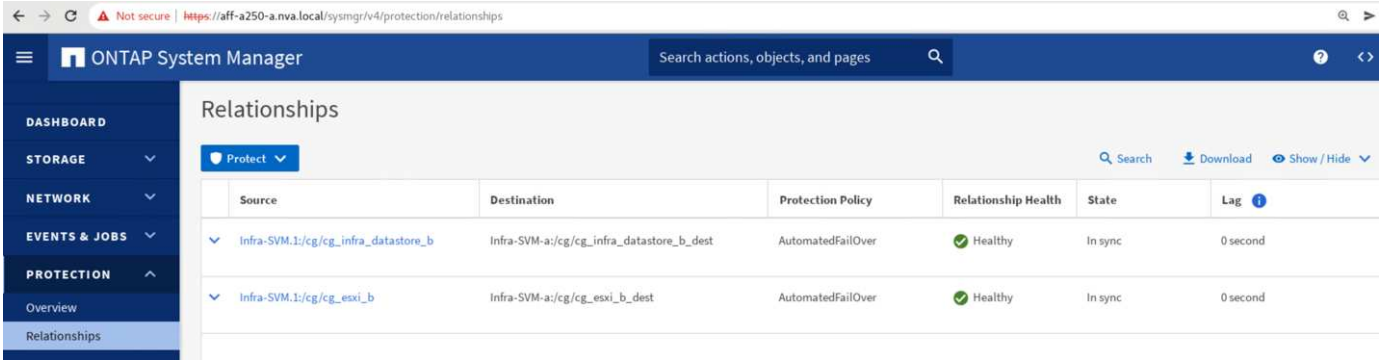


Le tableau suivant répertorie les quatre groupes de cohérence créés et les volumes inclus dans chaque groupe de cohérence pour le test de validation.

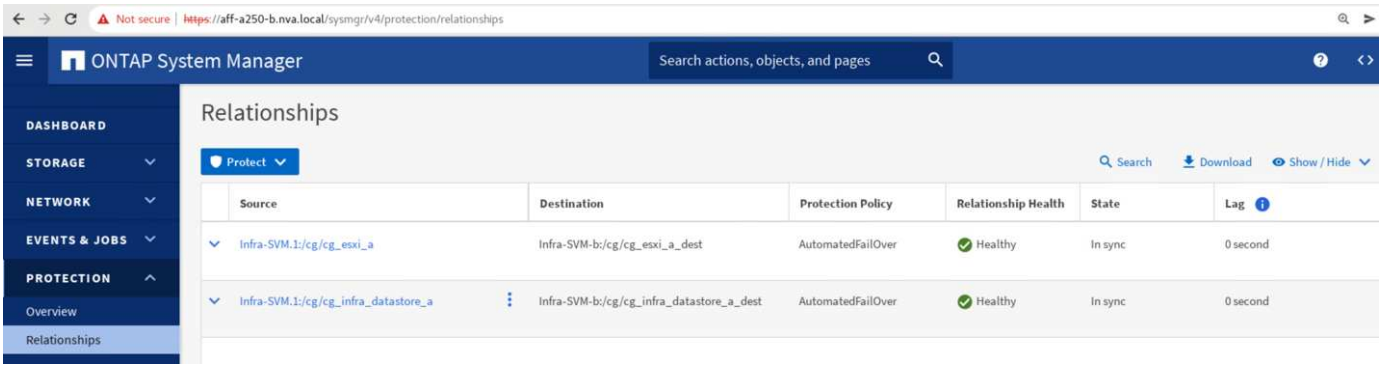
System Manager	Groupe de cohérence	Volumes
Site A	cg_esxi_a	esxi_a
Site A	cg_infra_datastore_a	infra_datastore_a_01 infra_datastore_a_02
Site B	cg_esxi_b	esxi_b
Site B	cg_infra_datastore_b	infra_datastore_b_01 infra_datastore_b_02

Une fois les groupes de cohérence créés, ils s’affichent sous les relations de protection respectives sur le site A et sur le site B.

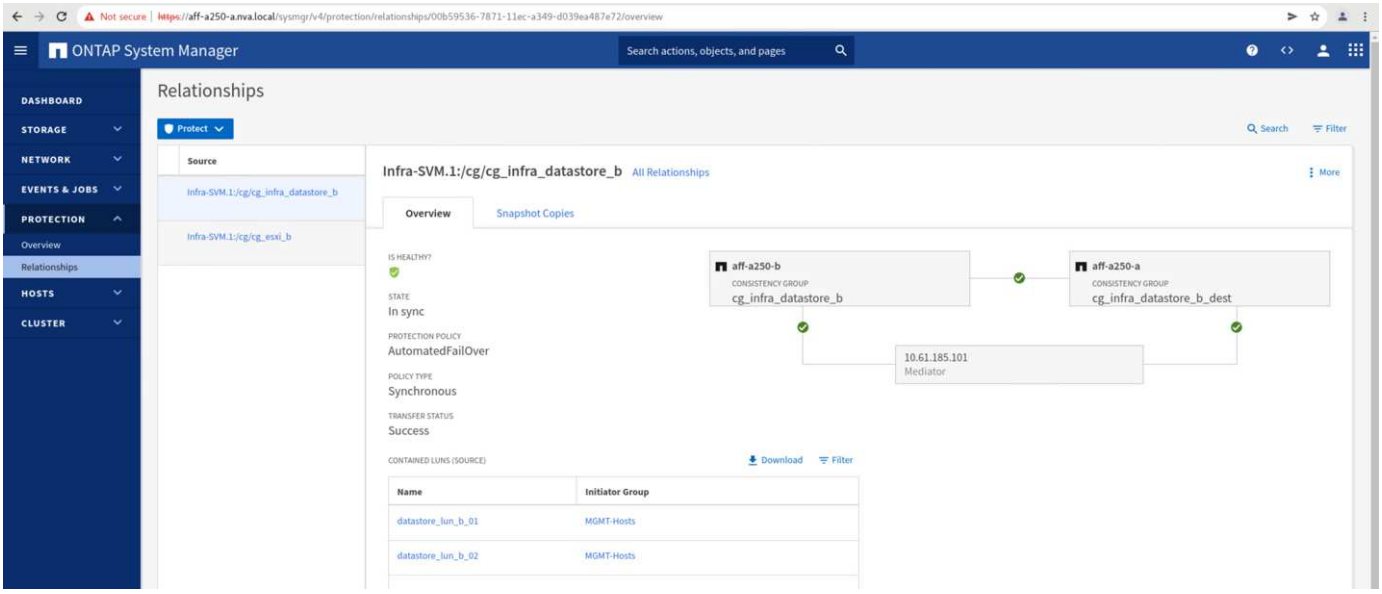
Cette capture d’écran affiche les relations de groupe de cohérence sur le site A.



Cette capture d'écran affiche les relations de groupe de cohérence sur le site B.



Cette capture d'écran affiche les détails de la relation de groupe de cohérence pour le groupe cg_infra_datastore_b.



Volumes, LUN et mappages d'hôtes

Une fois les groupes de cohérence créés, SnapMirror synchronise les volumes source et de destination pour que les données soient toujours synchronisées. Les volumes de destination du site distant portent les noms des volumes avec la fin _dest. Par exemple, pour le volume esxi_a du site Un cluster, il existe un volume ESXi_a_dest de protection des données (DP) correspondant sur le site B.

Cette capture d'écran affiche les informations de volume du site A.

```
aff-a250-a::> vol show -vserver Infra-SVM-a
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
Infra-SVM-a esxi_a     aggr1_aff_a250_a_01 online RW     320GB    315.9GB    1%
Infra-SVM-a esxi_b_dest aggr1_aff_a250_a_02 online DP   3.86GB    638.4MB   83%
Infra-SVM-a infra_datastore_a_01 aggr1_aff_a250_a_01 online RW 1TB 717.6GB  29%
Infra-SVM-a infra_datastore_a_02 aggr1_aff_a250_a_02 online RW 1TB 828.4GB  19%
Infra-SVM-a infra_svm_root aggr1_aff_a250_a_01 online RW   1GB    966.5MB    0%
Infra-SVM-a infra_svm_root_m01 aggr1_aff_a250_a_01 online LS 1GB  966.6MB    0%
Infra-SVM-a infra_svm_root_m02 aggr1_aff_a250_a_02 online LS 1GB  966.6MB    0%
Infra-SVM-a vol_infra_datastore_b_01_dest aggr1_aff_a250_a_01 online DP 138.7GB 31.52GB  76%
Infra-SVM-a vol_infra_datastore_b_02_dest aggr1_aff_a250_a_01 online DP 49.37GB 9.03GB  80%
9 entries were displayed.
```

Cette capture d'écran affiche les informations de volume du site B.

```
aff-a250-b::> vol show -vserver Infra-SVM-b
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
Infra-SVM-b esxi_a_dest aggr1_aff_a250_b_02 online DP   4.10GB    768.2MB   80%
Infra-SVM-b esxi_b     aggr1_aff_a250_b_01 online RW     320GB    315.8GB    1%
Infra-SVM-b infra_datastore_b_01 aggr1_aff_a250_b_01 online RW 1TB 911.9GB  10%
Infra-SVM-b infra_datastore_b_02 aggr1_aff_a250_b_02 online RW 1TB 964.0GB   5%
Infra-SVM-b infra_svm_root aggr1_aff_a250_b_01 online RW   1GB    966.9MB    0%
Infra-SVM-b infra_svm_root_m01 aggr1_aff_a250_b_01 online LS 1GB  967.0MB    0%
Infra-SVM-b infra_svm_root_m02 aggr1_aff_a250_b_02 online LS 1GB  967.0MB    0%
Infra-SVM-b vol_infra_datastore_a_01_dest aggr1_aff_a250_b_02 online DP 270.0GB 27.39GB  89%
Infra-SVM-b vol_infra_datastore_a_02_dest aggr1_aff_a250_b_02 online DP 202.8GB 28.20GB  85%
9 entries were displayed.
```

Pour faciliter le basculement transparent des applications, les LUN SM-BC en miroir doivent également être mappés sur les hôtes à partir du cluster de destination. Cela permet aux hôtes de voir correctement les chemins d'accès aux LUN depuis les clusters source et de destination. Le `igroup show` et `lun show` Les sorties du site A et du site B sont saisies dans les deux captures d'écran suivantes. Avec les mappages créés, chaque hôte ESXi du cluster voit son propre LUN de démarrage SAN comme ID 0 et les quatre LUN de datastore iSCSI partagés.

Cette capture d'écran montre les groupes initiateurs hôtes et le mappage de LUN pour le site A cluster.

```
aff-a250-a::> igroup show
Vserver   Igroup       Protocol OS Type  Initiators
--------- ------------ -------- -------- ------------------------------------
Infra-SVM-a MGMT-Hosts iscsi    vmware   iqn.2010-11.com.flexpod:ucs-smbc-a:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:3
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:3
Infra-SVM-a VM-Host-Infra-a-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:1
Infra-SVM-a VM-Host-Infra-a-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:2
Infra-SVM-a VM-Host-Infra-a-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:3
Infra-SVM-a VM-Host-Infra-b-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:1
Infra-SVM-a VM-Host-Infra-b-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:2
Infra-SVM-a VM-Host-Infra-b-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:3
7 entries were displayed.

aff-a250-a::> lun show -m
Vserver    Path                                      Igroup   LUN ID  Protocol
---------- ----------------------------------------  -------  ------  --------
Infra-SVM-a /vol/esxi_a/VM-Host-Infra-a-01           VM-Host-Infra-a-01  0  iscsi
Infra-SVM-a /vol/esxi_a/VM-Host-Infra-a-02           VM-Host-Infra-a-02  0  iscsi
Infra-SVM-a /vol/esxi_a/VM-Host-Infra-a-03           VM-Host-Infra-a-03  0  iscsi
Infra-SVM-a /vol/esxi_a/swap_lun_a                   MGMT-Hosts   13  iscsi
Infra-SVM-a /vol/esxi_b_dest/VM-Host-Infra-b-01      VM-Host-Infra-b-01  0  iscsi
Infra-SVM-a /vol/esxi_b_dest/VM-Host-Infra-b-02      VM-Host-Infra-b-02  0  iscsi
Infra-SVM-a /vol/esxi_b_dest/VM-Host-Infra-b-03      VM-Host-Infra-b-03  0  iscsi
Infra-SVM-a /vol/esxi_b_dest/swap_lun_b              MGMT-Hosts   23  iscsi
Infra-SVM-a /vol/infra_datastore_a_01/datastore_lun_a_01  MGMT-Hosts  11  iscsi
Infra-SVM-a /vol/infra_datastore_a_02/datastore_lun_a_02  MGMT-Hosts  12  iscsi
Infra-SVM-a /vol/vol_infra_datastore_b_01_dest/datastore_lun_b_01  MGMT-Hosts  21  iscsi
Infra-SVM-a /vol/vol_infra_datastore_b_02_dest/datastore_lun_b_02  MGMT-Hosts  22  iscsi
12 entries were displayed.
```

Cette capture d’écran montre les groupes initiateurs hôtes et le mappage de LUN pour le cluster du site B.

```
aff-a250-b::> igroup show
Vserver   Igroup       Protocol OS Type  Initiators
--------- ------------ -------- -------- ------------------------------------
Infra-SVM-b MGMT-Hosts iscsi    vmware   iqn.2010-11.com.flexpod:ucs-smbc-b:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:3
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:3
Infra-SVM-b VM-Host-Infra-a-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:1
Infra-SVM-b VM-Host-Infra-a-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:2
Infra-SVM-b VM-Host-Infra-a-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:3
Infra-SVM-b VM-Host-Infra-b-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:1
Infra-SVM-b VM-Host-Infra-b-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:2
Infra-SVM-b VM-Host-Infra-b-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:3
7 entries were displayed.

aff-a250-b::> lun show -m
Vserver    Path                                        Igroup   LUN ID  Protocol
---------- ------------------------------------------  -------  ------  --------
Infra-SVM-b /vol/esxi_a_dest/VM-Host-Infra-a-01      VM-Host-Infra-a-01  0  iscsi
Infra-SVM-b /vol/esxi_a_dest/VM-Host-Infra-a-02      VM-Host-Infra-a-02  0  iscsi
Infra-SVM-b /vol/esxi_a_dest/VM-Host-Infra-a-03      VM-Host-Infra-a-03  0  iscsi
Infra-SVM-b /vol/esxi_a_dest/swap_lun_a              MGMT-Hosts   13  iscsi
Infra-SVM-b /vol/esxi_b/VM-Host-Infra-b-01           VM-Host-Infra-b-01  0  iscsi
Infra-SVM-b /vol/esxi_b/VM-Host-Infra-b-02           VM-Host-Infra-b-02  0  iscsi
Infra-SVM-b /vol/esxi_b/VM-Host-Infra-b-03           VM-Host-Infra-b-03  0  iscsi
Infra-SVM-b /vol/esxi_b/swap_lun_b                   MGMT-Hosts   23  iscsi
Infra-SVM-b /vol/infra_datastore_b_01/datastore_lun_b_01  MGMT-Hosts  21  iscsi
Infra-SVM-b /vol/infra_datastore_b_02/datastore_lun_b_02  MGMT-Hosts  22  iscsi
Infra-SVM-b /vol/vol_infra_datastore_a_01_dest/datastore_lun_a_01  MGMT-Hosts  11  iscsi
Infra-SVM-b /vol/vol_infra_datastore_a_02_dest/datastore_lun_a_02  MGMT-Hosts  12  iscsi
12 entries were displayed.
```

"Validation de la solution - virtualisation."

Validation de la solution : virtualisation

"Précédente : validation de la solution - stockage."

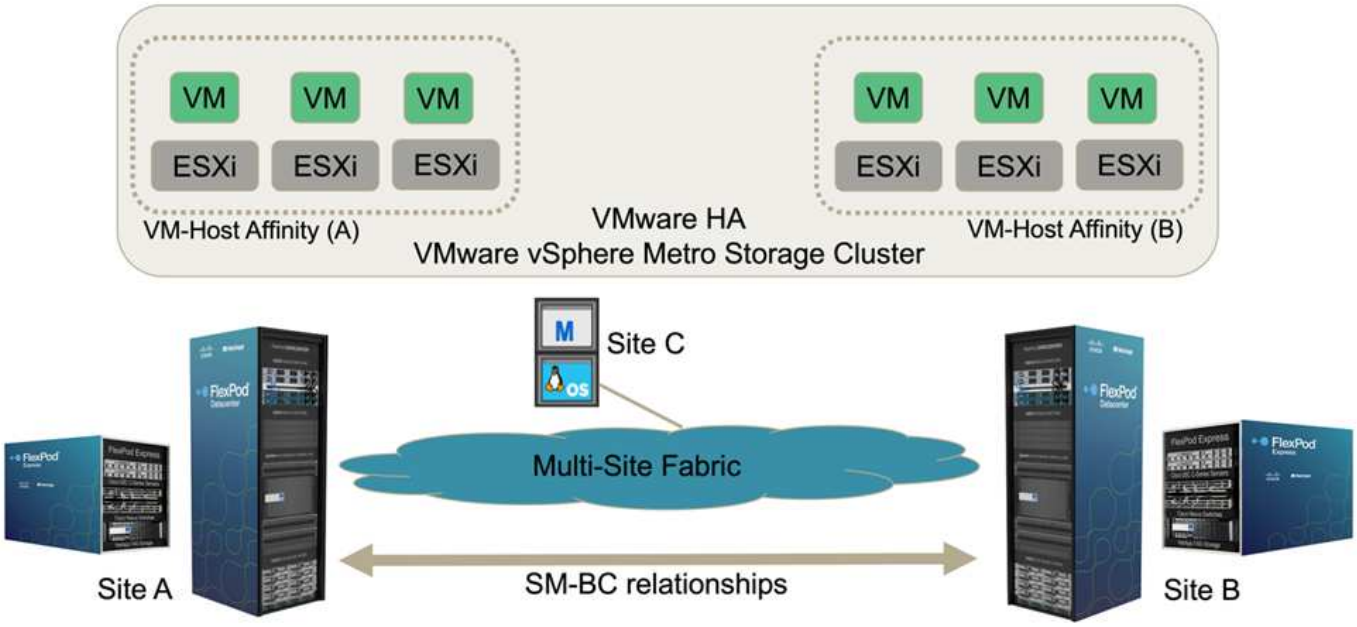
Dans la solution multisite FlexPod SM-BC, un seul VMware vCenter gère les ressources de l'infrastructure virtuelle pour l'ensemble de la solution. Les hôtes des deux data centers font partie du cluster haute disponibilité VMware unique qui s'étend sur les deux data centers. Les hôtes ont accès à la solution NetApp SM-BC où le stockage avec des relations SM-BC définies est accessible depuis les deux sites.

Le stockage de la solution SM-BC est conforme au modèle d'accès uniforme de la fonctionnalité VMware vSphere Metro Storage Cluster (vMSC) afin d'éviter les incidents et les temps d'indisponibilité. Pour des performances optimales des machines virtuelles, les disques de ces machines doivent être hébergés sur les systèmes locaux AFF A250 de NetApp. La latence et le trafic sur les liaisons WAN doivent ainsi être minimisés en cas de fonctionnement normal.

Dans le cadre de la mise en œuvre de la conception, il est nécessaire de déterminer la répartition des machines virtuelles entre les deux sites. Vous pouvez déterminer l'affinité de site et la distribution des applications de cette machine virtuelle sur les deux sites en fonction des préférences de votre site et des exigences de vos applications. Les groupes VM/hôtes du cluster VMware et les règles VM/hôte sont utilisés pour configurer l'affinité VM/hôte afin de s'assurer que les VM s'exécutent sur les hôtes du site souhaité.

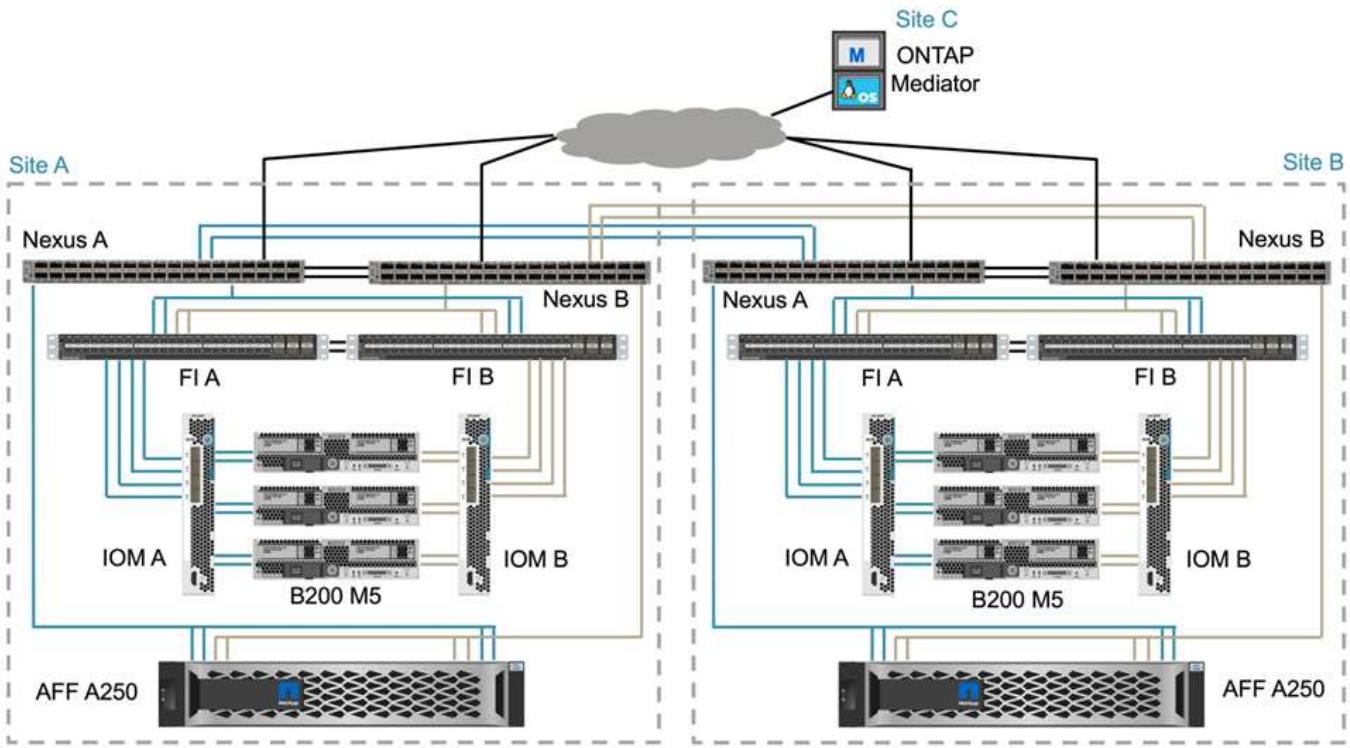
Toutefois, les configurations permettant d'exécuter des machines virtuelles sur les deux sites garantissent la résilience de la solution pour redémarrer les ordinateurs virtuels sur les hôtes du site distant. Pour que les machines virtuelles s'exécutent sur les deux sites, tous les datastores iSCSI partagés doivent être montés sur tous les hôtes ESXi afin de garantir un fonctionnement vMotion fluide des machines virtuelles entre les sites.

La figure suivante montre une vue de virtualisation de la solution FlexPod SM-BC haut de gamme incluant à la fois des fonctionnalités VMware HA et vMSC afin d'offrir la haute disponibilité des services de calcul et de stockage. L'architecture de solution de data Center actif-actif permet la mobilité de la charge de travail entre les sites et assure la reprise après incident et la continuité de l'activité.



Connectivité réseau de bout en bout

La solution FlexPod SM-BC comprend des infrastructures FlexPod sur chaque site, une connectivité réseau entre les sites et un médiateur ONTAP déployé sur un troisième site afin d'atteindre les objectifs RPO et RTO requis. La figure suivante montre une connectivité réseau de bout en bout entre les serveurs Cisco UCS B200M5 sur chaque site et le système de stockage NetApp disposant de fonctionnalités SM-BC sur un site et sur plusieurs sites.



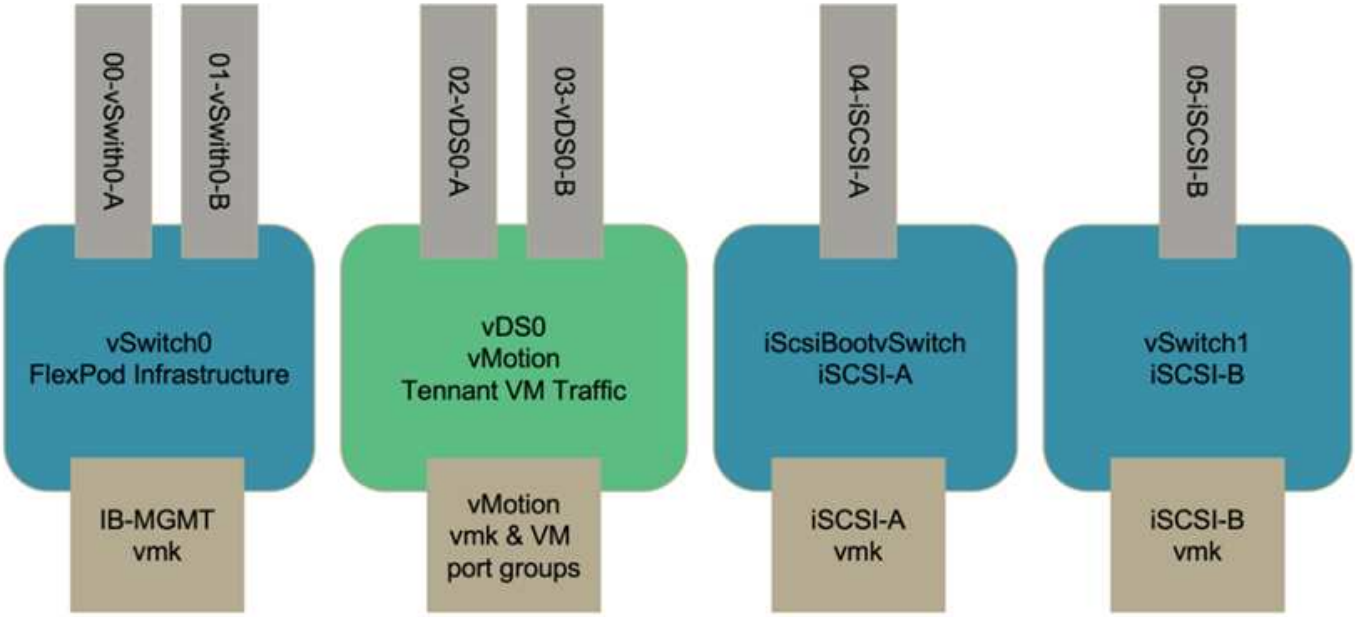
L'architecture de déploiement FlexPod est identique sur chaque site pour la validation de cette solution. Cependant, elle prend en charge les déploiements asymétriques et peut également être ajoutée aux solutions FlexPod existantes s'ils répondent aux exigences.

Une architecture étendue couche 2 est utilisée pour une Data Fabric multisite transparente qui offre une connectivité entre les ressources de calcul Cisco UCS et le stockage NetApp bâbord dans chaque data Center, ainsi que la connectivité entre les data centers. La configuration du canal de port et la configuration du canal de port virtuel, le cas échéant, sont utilisées pour l'agrégation de la bande passante et la tolérance aux pannes entre les couches de calcul, de réseau et de stockage, ainsi que pour les liens intersites. Par conséquent, les serveurs lames UCS offrent une connectivité et un accès multivoie aux systèmes de stockage NetApp locaux et distants.

La mise en réseau virtuelle

Chaque hôte du cluster est déployé à l'aide d'une mise en réseau virtuelle identique, quel que soit son emplacement. La conception sépare les différents types de trafic à l'aide de commutateurs virtuels VMware (vSwitch) et de switchs virtuels VMware (VDS). Le vSwitch VMware est utilisé principalement pour les réseaux d'infrastructure FlexPod et VDS pour les réseaux d'applications, mais il n'est pas nécessaire.

Les commutateurs virtuels (vSwitch, VDS) sont déployés avec deux liaisons ascendantes par commutateur virtuel. Les liaisons ascendantes au niveau de l'hyperviseur ESXi sont appelées vmnics et vNIC virtuels (vNIC) sur le logiciel Cisco UCS. Les vNIC sont créés sur l'adaptateur Cisco UCS VIC de chaque serveur en utilisant des profils de service Cisco UCS. Six vNIC sont définis, deux pour vSwitch0, deux pour vDS0, deux pour vSwitch1 et deux pour les liaisons montantes iSCSI, comme illustré dans la figure suivante.



VSwitch0 est défini lors de la configuration hôte VMware ESXi. Il contient le VLAN de gestion de l'infrastructure FlexPod et les ports VMK (hôte ESXi) pour la gestion. Un groupe de ports de machine virtuelle de gestion d'infrastructure est également placé sur vSwitch0 pour les machines virtuelles de gestion d'infrastructure stratégiques requises.

Il est important de placer ces machines virtuelles d'infrastructure de gestion sur vSwitch0 plutôt que dans le VDS, car si l'infrastructure FlexPod est arrêtée ou mise hors tension et que vous tentez d'activer cette machine virtuelle de gestion sur un hôte autre que l'hôte sur lequel elle était exécutée à l'origine, Il démarre très bien sur le réseau sur vSwitch0. Ce processus est particulièrement important si VMware vCenter est la machine virtuelle de gestion. Si vCenter se trouvaient sur le VDS et était déplacé vers un autre hôte puis démarré, il ne serait pas connecté au réseau après le démarrage.

Deux vswitches de démarrage iSCSI sont utilisés dans cette conception. Le démarrage iSCSI Cisco UCS nécessite des vNIC distincts pour le démarrage iSCSI. Ces vNIC utilisent le VLAN iSCSI de la structure appropriée en tant que VLAN natif et sont connectés au vSwitch de démarrage iSCSI approprié. Vous pouvez également déployer des réseaux iSCSI sur VDS en déployant un nouveau VDS ou en utilisant une existante.

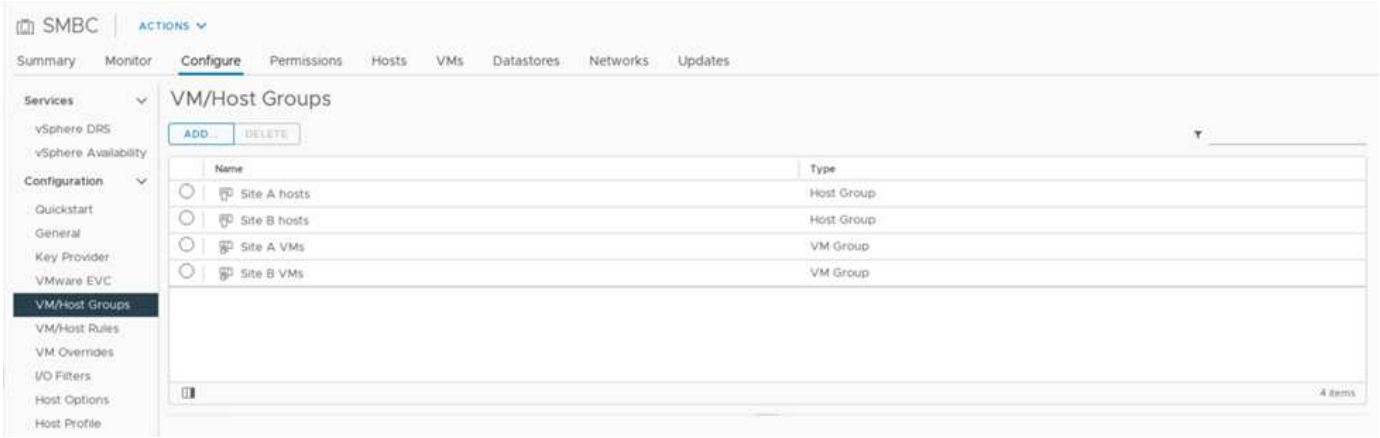
Règles et groupes d'affinité VM-Host

Pour que les machines virtuelles s'exécutent sur n'importe quel hôte ESXi des deux sites SM-BC, tous les hôtes ESXi doivent monter les datastores iSCSI des deux sites. Si les datastores des deux sites sont correctement montés par tous les hôtes ESXi, vous pouvez migrer une machine virtuelle entre tous les hôtes avec vMotion et la machine virtuelle conserve toujours l'accès à tous ses disques virtuels créés à partir de ces datastores.

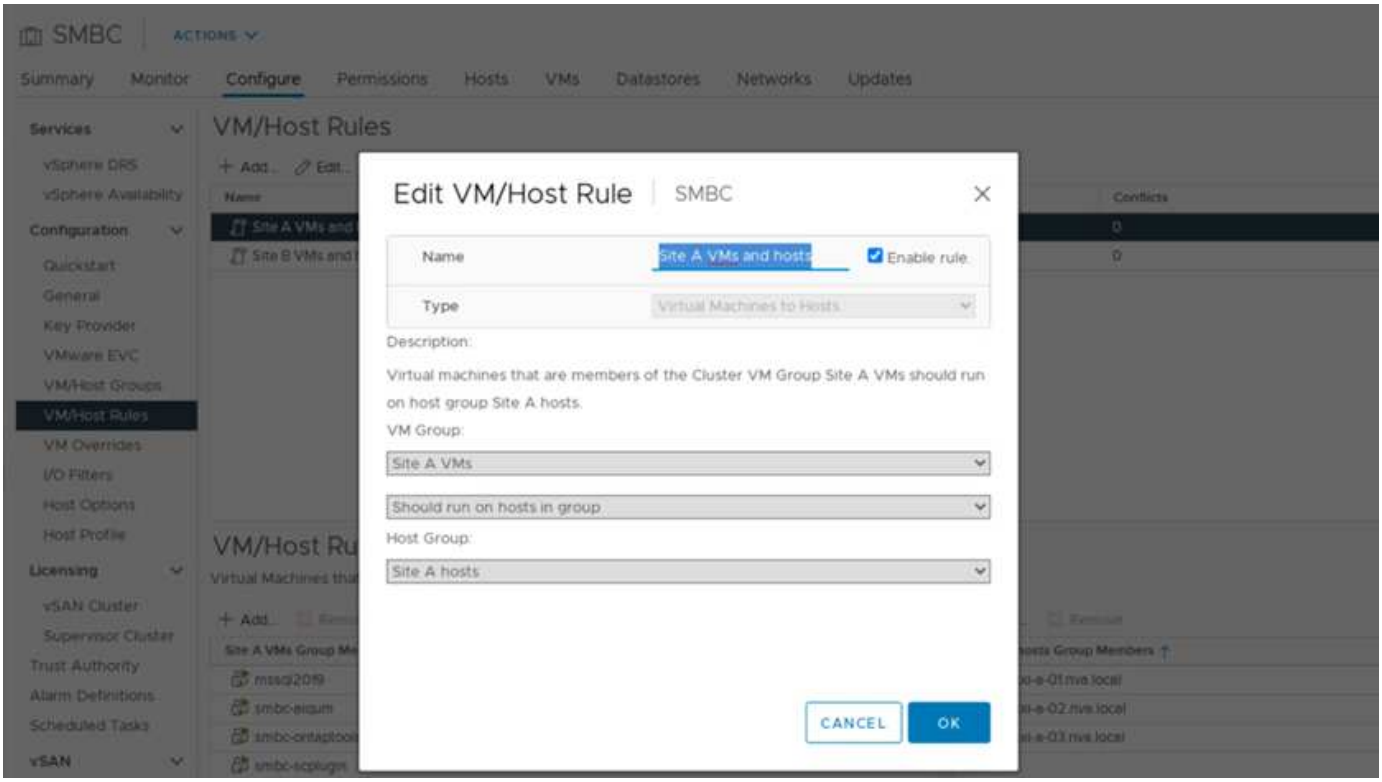
Dans le cas d'une machine virtuelle utilisant des datastores locaux, son accès aux disques virtuels devient distant s'il est migré vers un hôte du site distant et augmente ainsi la latence des opérations de lecture en raison de la distance physique entre les sites. Par conséquent, il est recommandé de conserver les machines virtuelles sur les hôtes locaux et d'utiliser le stockage local sur le site.

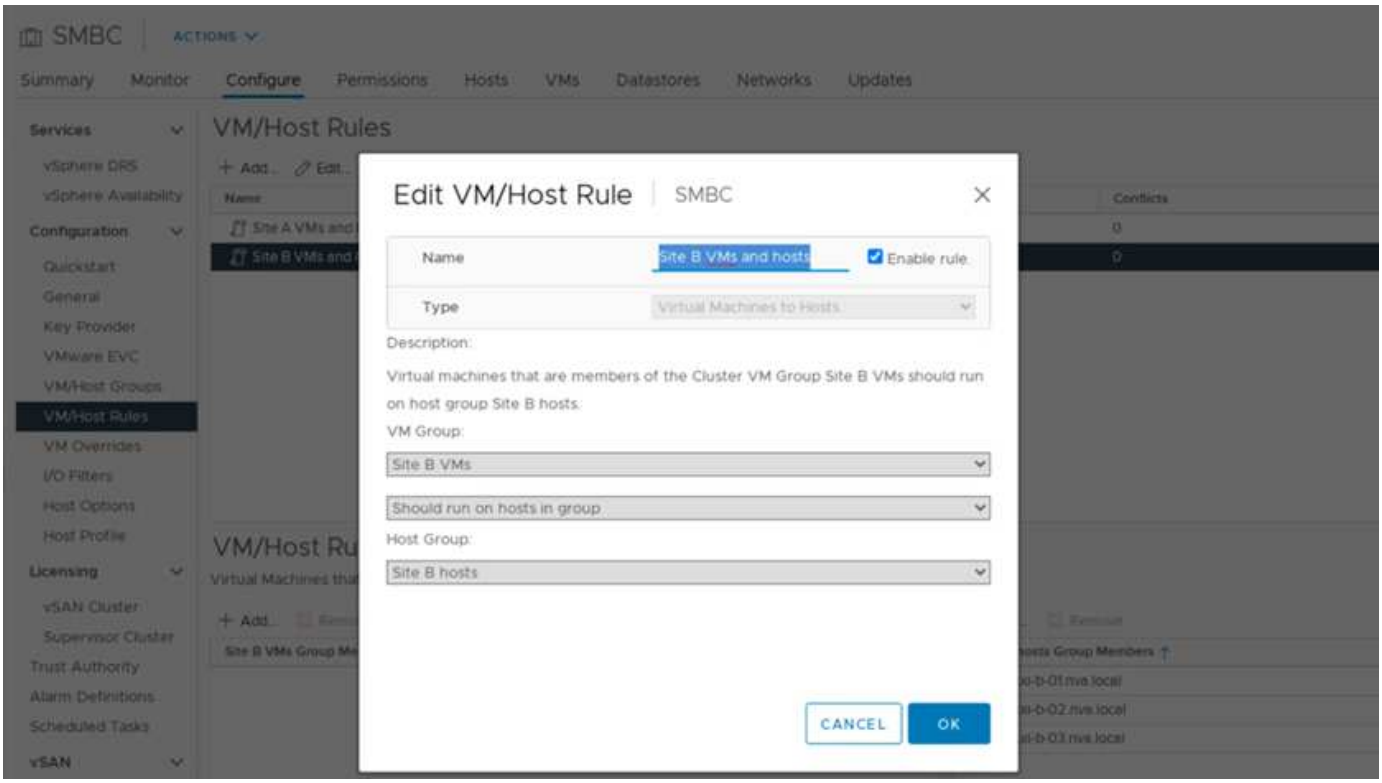
En utilisant un mécanisme d'affinité VM/hôte, vous pouvez utiliser des groupes VM/hôtes pour créer un groupe de VM et un groupe d'hôtes pour les machines virtuelles et les hôtes situés sur un site particulier. Les règles VM/hôte vous permettent de spécifier la règle à suivre pour les VM et les hôtes. Pour permettre la migration de la machine virtuelle entre les sites pendant un scénario de maintenance de site ou de sinistre, utilisez la spécification de stratégie « devrait s'exécuter sur les hôtes du groupe » pour cette flexibilité.

La capture d'écran suivante montre que deux groupes d'hôtes et deux groupes de machines virtuelles sont créés pour les hôtes et les machines virtuelles du site A et du site B.



En outre, les deux figures suivantes montrent les règles VM/hôte créées pour les machines virtuelles du site A et du site B à exécuter sur les hôtes de leurs sites respectifs à l'aide de la stratégie « devrait s'exécuter sur les hôtes du groupe ».

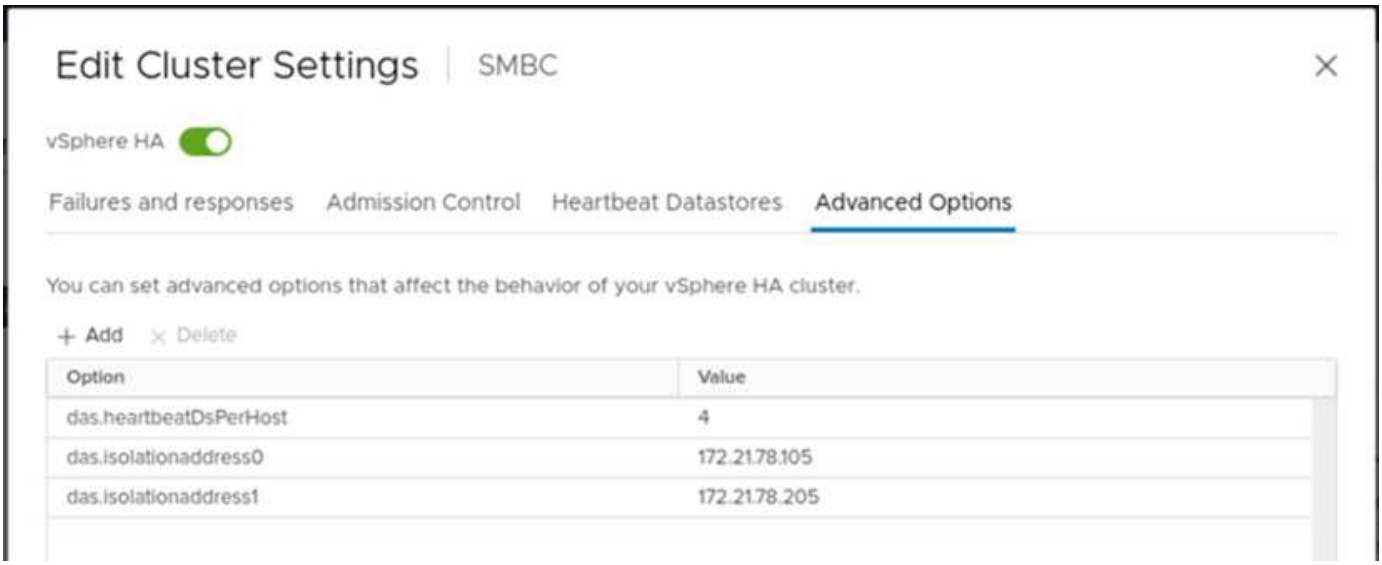




Pulsation vSphere HA

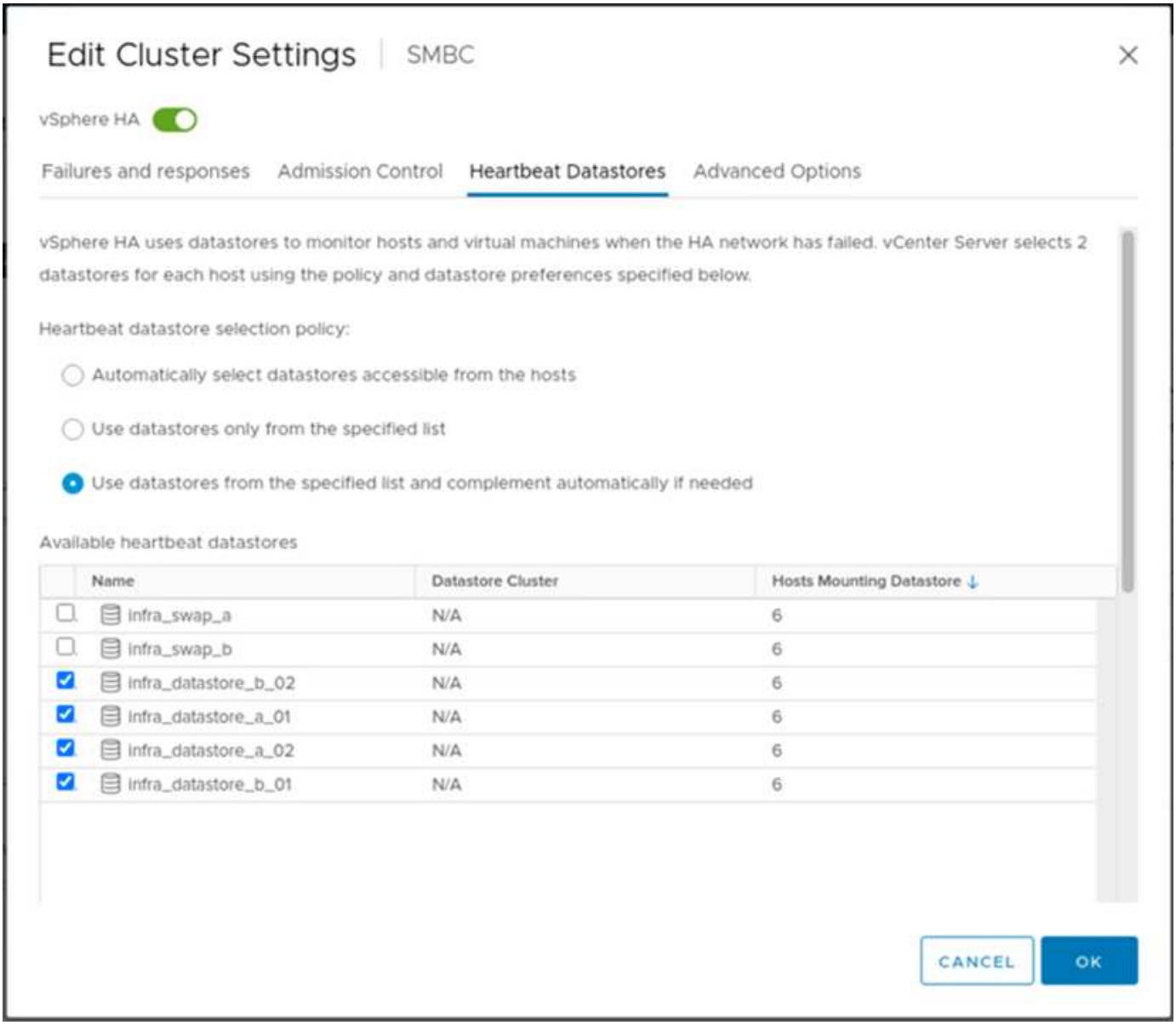
VMware vSphere HA dispose d'un mécanisme de pulsation pour la validation de l'état hôte. Le mécanisme de pulsation principal passe par le réseau, tandis que le mécanisme de pulsation secondaire se fait par l'intermédiaire du datastore. Si les signaux ne sont pas reçus, il décide alors s'ils sont isolés du réseau en envoyant une commande ping à la passerelle par défaut ou aux adresses d'isolation configurées manuellement. Pour le signal de détection du datastore, VMware recommande d'augmenter les datastores de signal de détection de deux à quatre pour un cluster étendu.

Pour la validation de la solution, les deux adresses IP de gestion de cluster ONTAP sont utilisées comme adresse d'isolation. En outre, l'option avancée vSphere HA est recommandée `ds.heartbeatDsPerHost` avec une valeur de 4 a été ajoutée comme indiqué dans la figure suivante.



Pour le datastore de signal de détection, spécifiez les quatre datastores partagés du cluster et complétez

automatiquement, comme illustré dans la figure suivante.



Pour connaître les meilleures pratiques et les configurations pour VMware HA Cluster et VMware vSphere Metro Storage Cluster, consultez "Création et utilisation de clusters HA vSphere", "Cluster de stockage Metro VMware vSphere (vMSC)" Et VMware KB pour "NetApp ONTAP avec NetApp SnapMirror Business Continuity (SM-BC) et VMware vSphere Metro Storage Cluster (vMSC)".

"La validation des solutions : scénarios validés"

Validation des solutions : scénarios validés

"Validation de la solution - virtualisation."

La solution FlexPod Datacenter SM-BC protège les services de données dans de nombreux scénarios de point de défaillance unique et en cas d'incident sur site. La conception redondante implémentée sur chaque site assure une haute disponibilité et l'implémentation de SM-BC avec réplication synchrone des données sur plusieurs sites

protège les services de données d'un incident sur l'ensemble d'un site. La solution déployée est validée pour les fonctions de la solution ainsi que pour les différents scénarios de défaillance pour lesquels la solution est conçue pour la protection.

Validation des fonctions de la solution

Différents cas de test sont utilisés pour vérifier le fonctionnement de la solution et simuler des scénarios de défaillance partielle et complète du site. Pour réduire au minimum la duplication avec les tests déjà effectués dans les solutions de data Center FlexPod existantes dans le cadre du programme de conception validée par Cisco, ce rapport se concentre sur les aspects liés à SM-BC de la solution. Certaines validations FlexPod générales sont incluses pour que les praticiens puissent passer en revue leurs validations de mise en œuvre.

Pour la validation de la solution, une machine virtuelle Windows 10 par hôte ESXi a été créée sur tous les hôtes ESXi des deux sites. L'outil IOMeter a été installé et utilisé pour générer des E/S sur deux disques de données virtuels mappés à partir des datastores iSCSI locaux partagés. Les paramètres de la charge de travail IOMeter configurés étaient à 8 Ko d'E/S, à 75 % de lecture et à 50 % aléatoires, et 8 commandes d'E/S en attente pour chaque disque de données. Dans la plupart des scénarios de test réalisés, la suite des E/S IOMeter montre que le scénario n'a pas provoqué de panne du service de données.

Étant donné que SM-BC est critique pour les applications métier telles que les serveurs de base de données, L'instance Microsoft SQL Server 2019 d'une machine virtuelle Windows Server 2022 a également été incluse dans le cadre des tests pour confirmer que l'application continue à s'exécuter lorsque le stockage sur son site local n'est pas disponible et que le service de données est repris sur le système de stockage du site distant sans application perturbation.

Test de démarrage SAN iSCSI de l'hôte ESXi

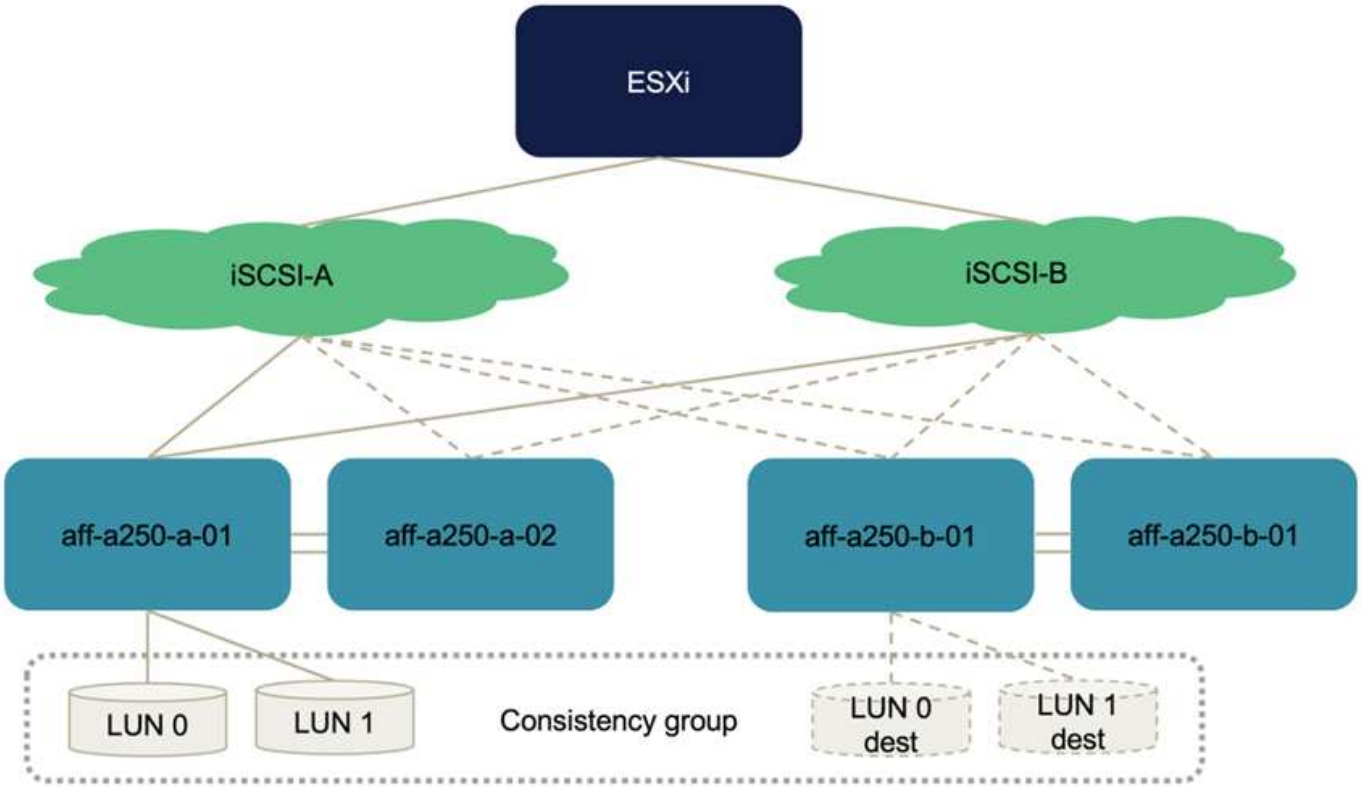
Les hôtes ESXi de la solution sont configurés pour démarrer à partir du SAN iSCSI. L'utilisation du démarrage SAN simplifie la gestion du serveur lors du remplacement d'un serveur car le profil de service du serveur peut être associé à un nouveau serveur pour qu'il démarre sans apporter de modifications de configuration supplémentaires.

En plus de démarrer un hôte ESXi situé sur un site à partir de sa LUN de démarrage iSCSI locale, un test a également été effectué pour démarrer l'hôte ESXi lorsque son contrôleur de stockage local est en état de basculement ou lorsque son cluster de stockage local est totalement indisponible. Ces scénarios de validation garantissent la configuration correcte des hôtes ESXi par conception et peuvent démarrer lors d'une maintenance du stockage ou d'un scénario de reprise après incident afin d'assurer la continuité de l'activité.

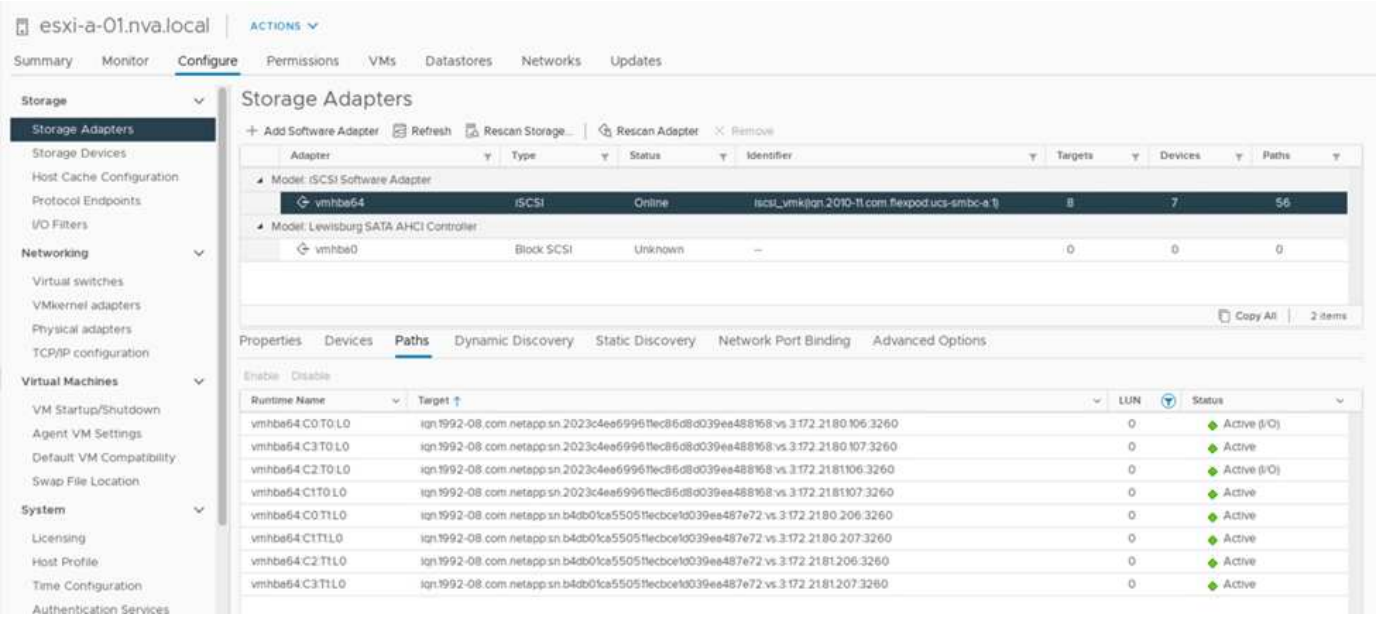
Avant de configurer la relation de groupe de cohérence SM-BC, une LUN iSCSI hébergée par une paire haute disponibilité de contrôleur de stockage dispose de quatre chemins, deux par le biais de chaque structure iSCSI, selon l'implémentation des meilleures pratiques. Un hôte peut passer au LUN via les deux VLAN/fabrics iSCSI vers le contrôleur hôte LUN, ainsi via le partenaire haute disponibilité du contrôleur.

Une fois la relation de groupe de cohérence SM-BC configurée et les LUN en miroir correctement mappées sur les initiateurs, le nombre de chemins d'accès de la LUN double. Pour cette implémentation, il s'agit de disposer de deux chemins actifs/optimisés et de deux chemins actifs/non optimisés, d'avoir deux chemins actifs/optimisés et six chemins actifs/non optimisés.

La figure suivante illustre les chemins qu'un hôte ESXi peut prendre pour accéder à une LUN, par exemple LUN 0. Comme la LUN est connectée au site A contrôleur 01, seuls les deux chemins qui accèdent directement à la LUN via ce contrôleur sont actifs/optimisés et les six chemins restants sont actifs/non optimisés.



La capture d'écran suivante des informations sur le chemin du périphérique de stockage montre comment l'hôte ESXi voit les deux types de chemins de périphérique. Les deux chemins actifs/optimisés sont indiqués comme ayant `active (I/O)` l'état du chemin, alors que les six chemins actifs/non optimisés sont affichés uniquement comme `active`. Notez également que la colonne cible affiche les deux cibles iSCSI et les adresses IP LIF iSCSI respectives pour obtenir les cibles.



Lorsqu'un des contrôleurs de stockage est en panne pour cause de maintenance ou de mise à niveau, les deux chemins qui atteignent le contrôleur de panne ne sont plus disponibles et affichent le chemin d'accès à `dead` à la place.

Si un basculement de groupe de cohérence se produit sur le cluster de stockage principal, soit en raison de

tests de basculement manuels, soit d'un basculement automatique en cas d'incident, le cluster de stockage secondaire continue à fournir les services de données pour les LUN du groupe de cohérence SM-BC. Comme les identités de LUN sont préservées et que les données ont été répliquées de manière synchrone, toutes les LUN de démarrage de l'hôte ESXi protégées par les groupes de cohérence SM-BC restent disponibles depuis le cluster de stockage distant.

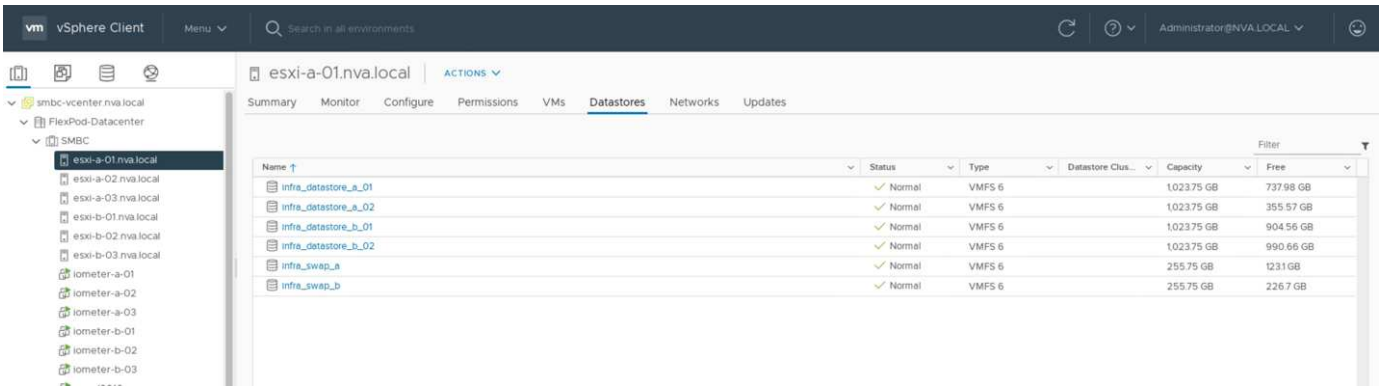
Test d'affinité avec les VM/hôtes VMware vMotion

Bien qu'une solution générique FlexPod VMware Datacenter prenne en charge plusieurs protocoles, tels que FC, iSCSI, NVMe et NFS, la fonctionnalité de la solution FlexPod SM-BC prend en charge les protocoles SAN FC et iSCSI généralement utilisés pour les solutions stratégiques. Cette validation utilise uniquement les datastores basés sur protocole iSCSI et le démarrage SAN iSCSI.

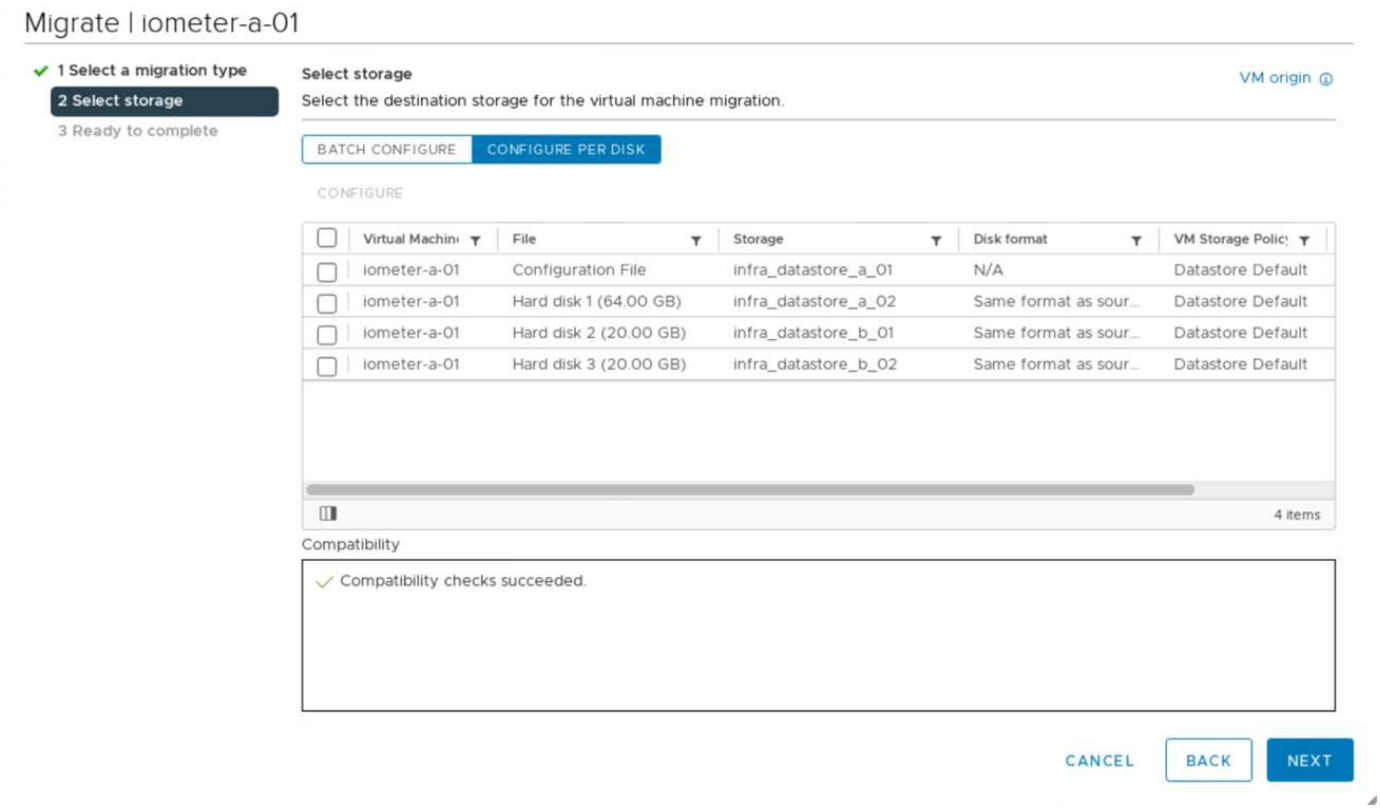
Pour permettre aux machines virtuelles d'utiliser les services de stockage depuis l'un des sites SM-BC, les datastores iSCSI des deux sites doivent être montés par tous les hôtes du cluster afin de permettre la migration des machines virtuelles entre les deux sites et dans le cadre de scénarios de basculement en cas d'incident.

Il est également possible d'utiliser le protocole NFS et les datastores NFS pour les applications exécutées sur l'infrastructure virtuelle qui ne nécessitent pas la protection des groupes de cohérence SM-BC entre les sites. Dans ce cas, il convient d'observer une attention particulière lors de l'allocation du stockage pour les VM afin que les applications stratégiques utilisent correctement les datastores SAN protégés par le groupe de cohérence SM-BC pour assurer la continuité de l'activité.

La capture d'écran suivante montre que les hôtes sont configurés pour monter des datastores iSCSI à partir des deux sites.



Vous pouvez migrer des disques de machines virtuelles entre des datastores iSCSI disponibles depuis les deux sites, comme le montre la figure suivante. Pour considérations de performances, il est optimal de disposer de serveurs virtuels qui utilisent le stockage de leur cluster de stockage local afin de réduire les latences d'E/S des disques. Ceci est particulièrement vrai lorsque les deux sites sont situés à certaines distances, en raison de la latence de distance de aller-retour physique d'environ 1 ms par 100 km de distance.



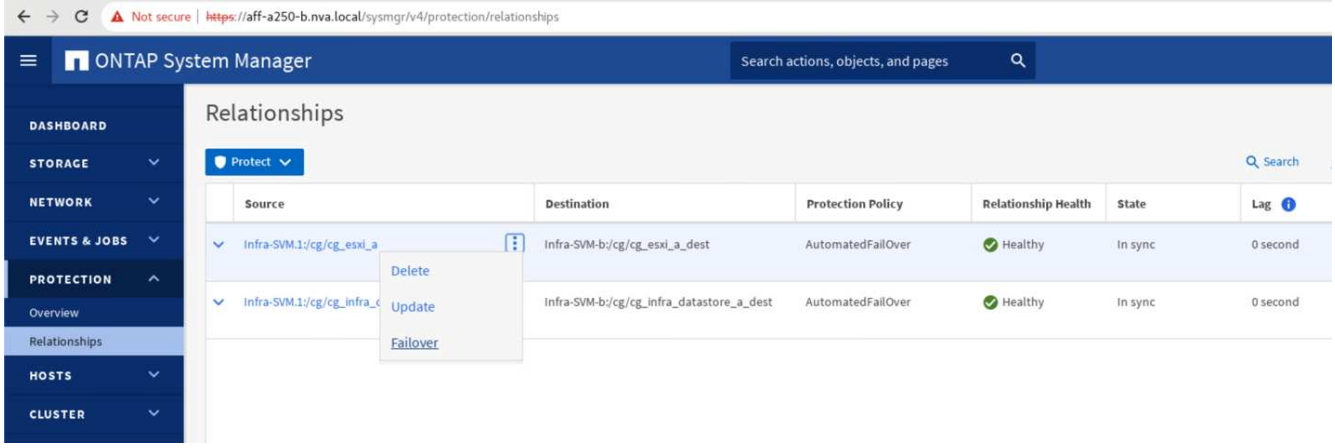
Des tests de vMotion d'machines virtuelles sur un hôte différent au niveau du même site, ainsi que sur plusieurs sites ont été réalisés et ont abouti. Après avoir migré manuellement une machine virtuelle sur plusieurs sites, la règle d'affinité VM/hôte s'active et retransfère la machine virtuelle au groupe où elle appartient dans la condition normale.

Basculement planifié du stockage

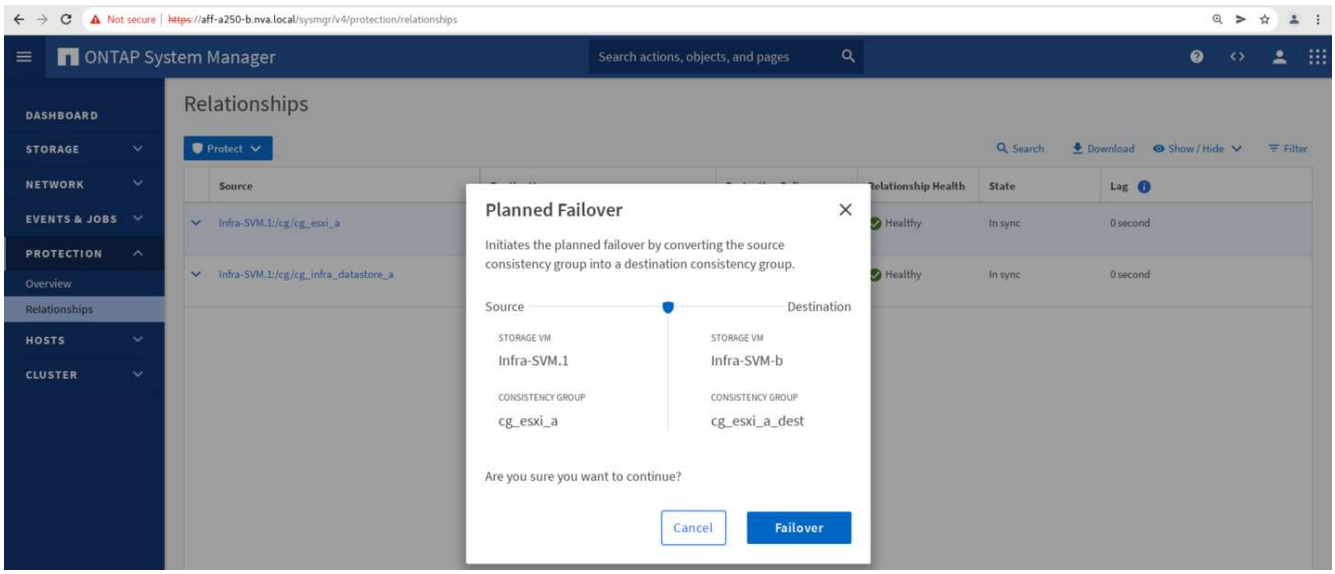
Les opérations planifiées de basculement du stockage doivent être réalisées sur la solution après la configuration initiale afin de déterminer si la solution fonctionne correctement après le basculement du stockage. Ce test peut aider à identifier tout problème de connectivité ou de configuration susceptible d'entraîner des interruptions d'E/S. Les tests et la résolution réguliers de tout problème de connectivité ou de configuration permettent de fournir des services de données sans interruption en cas d'incident sur site réel. Le basculement planifié du stockage peut également être utilisé avant une maintenance planifiée du stockage afin que les services de données puissent être assurés depuis le site non affecté.

Pour lancer un basculement manuel des services de données de stockage du site A vers le site B, vous pouvez utiliser le site B ONTAP System Manager pour effectuer l'action.

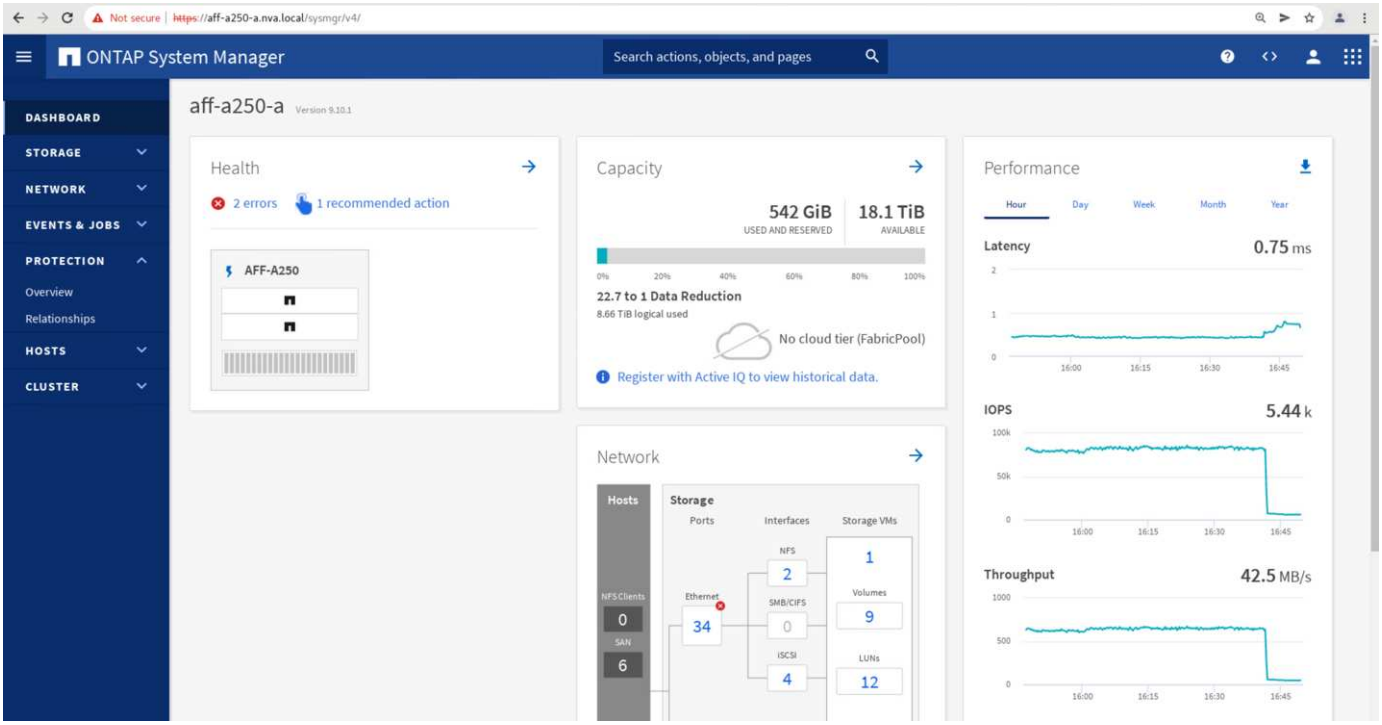
1. Accédez à l'écran protection > relations pour confirmer que l'état de la relation de groupe de cohérence est `In Sync`. S'il se trouve toujours dans le `Synchronizing` attendez que l'état devienne `In Sync` avant d'effectuer un basculement.
2. Développez les points en regard du nom de la source et cliquez sur basculement.



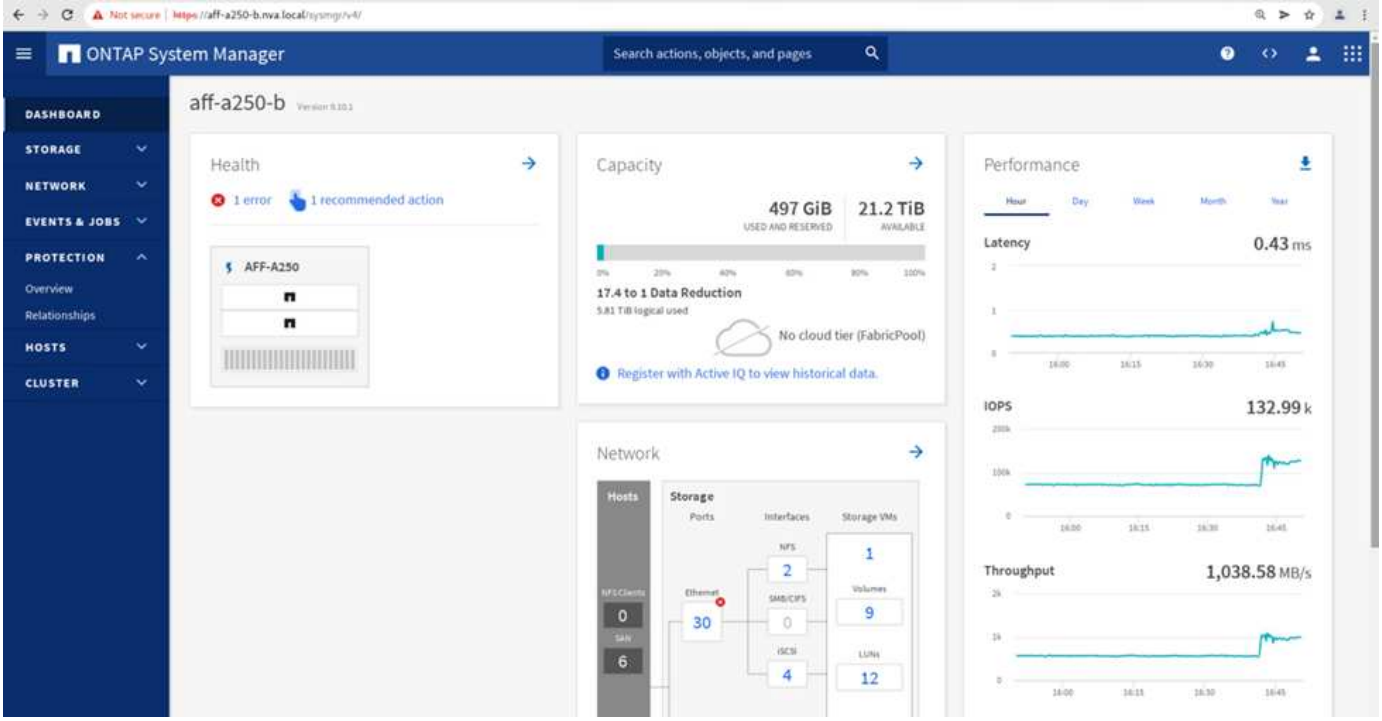
3. Confirmer le basculement pour que l'action démarre.



Peu de temps après le lancement du basculement des deux groupes de cohérence, `cg_esxi_a` et `cg_infra_datastore_a`, Sur l'interface graphique System Manager du site B, les E/S du site A servant à traiter les deux groupes de cohérence déplacés vers le site B. Ainsi, les E/S sur le site A sont considérablement réduites comme indiqué sur le site A volet performances de System Manager.

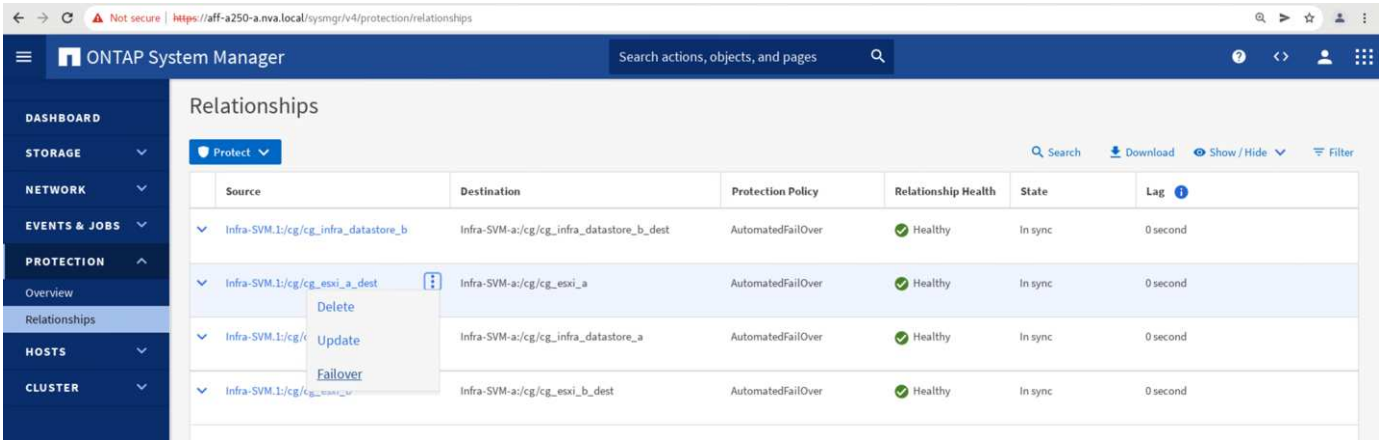


Par contre, le volet performances du tableau de bord du site B System Manager affiche une augmentation significative des IOPS, en raison de la transmission des E/S supplémentaires transférées du site A à environ 130 000 IOPS, De plus, nous avons atteint un débit d'environ 1 Gbit/s, tout en maintenant une latence d'E/S inférieure à la milliseconde.



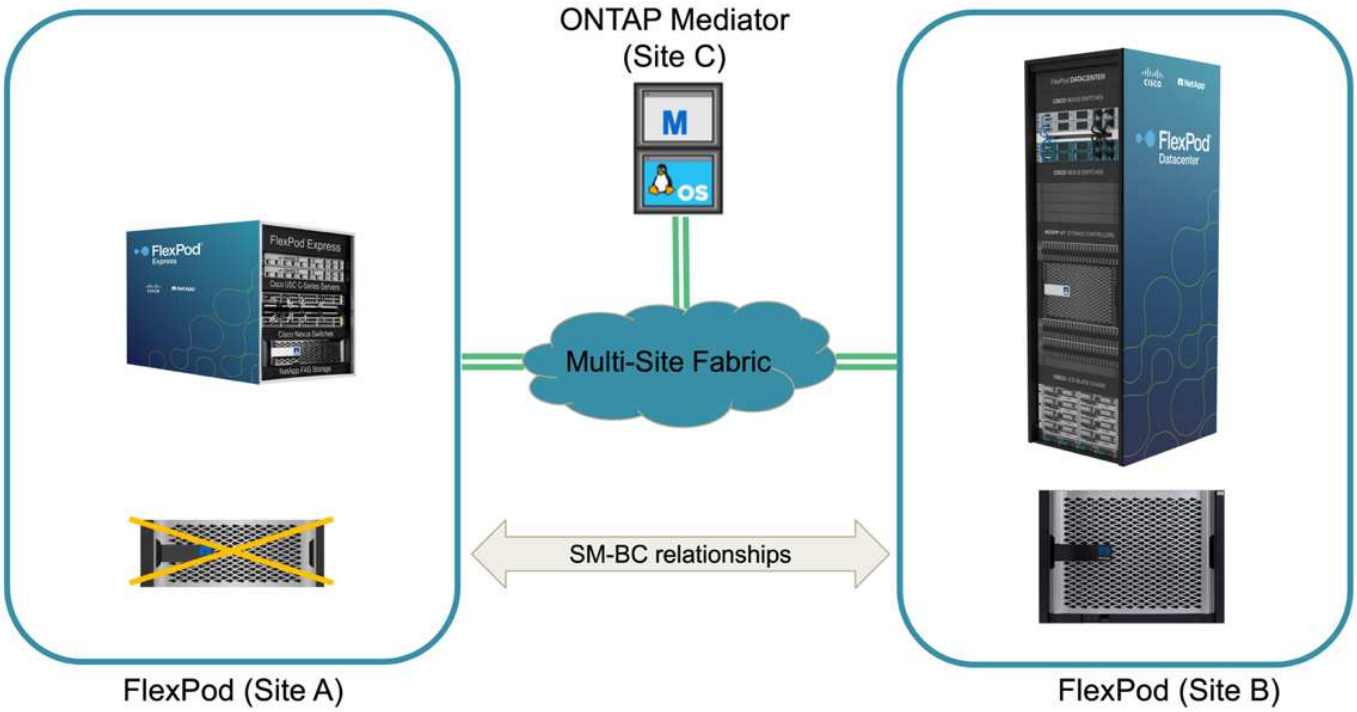
Grâce à la migration transparente des E/S du site A vers le site B, les contrôleurs de stockage du site A peuvent désormais être mis en service afin de planifier la maintenance. Une fois le travail de maintenance ou le test terminé et que le cluster de stockage d'un site est réexécuté et opérationnel, vérifiez et attendez que l'état de protection du groupe de cohérence soit revenir à `In sync` Avant d'effectuer un basculement pour renvoyer les E/S de basculement du site B vers le site A. Notez que plus un site est arrêté pour les opérations de maintenance ou de test, plus il faut de temps pour synchroniser les données et que le groupe de cohérence

est renvoyé au `In sync` état.



Basculement de stockage non planifié

Un basculement de stockage non planifié peut se produire en cas d'incident réel ou lors d'une simulation d'incident. Par exemple, consultez la figure suivante dans laquelle le système de stockage sur le site A subit une panne de courant, un basculement de stockage non planifié est déclenché et les services de données pour les LUN du site A, protégés par les relations SM-BC, continuent à partir du site B.



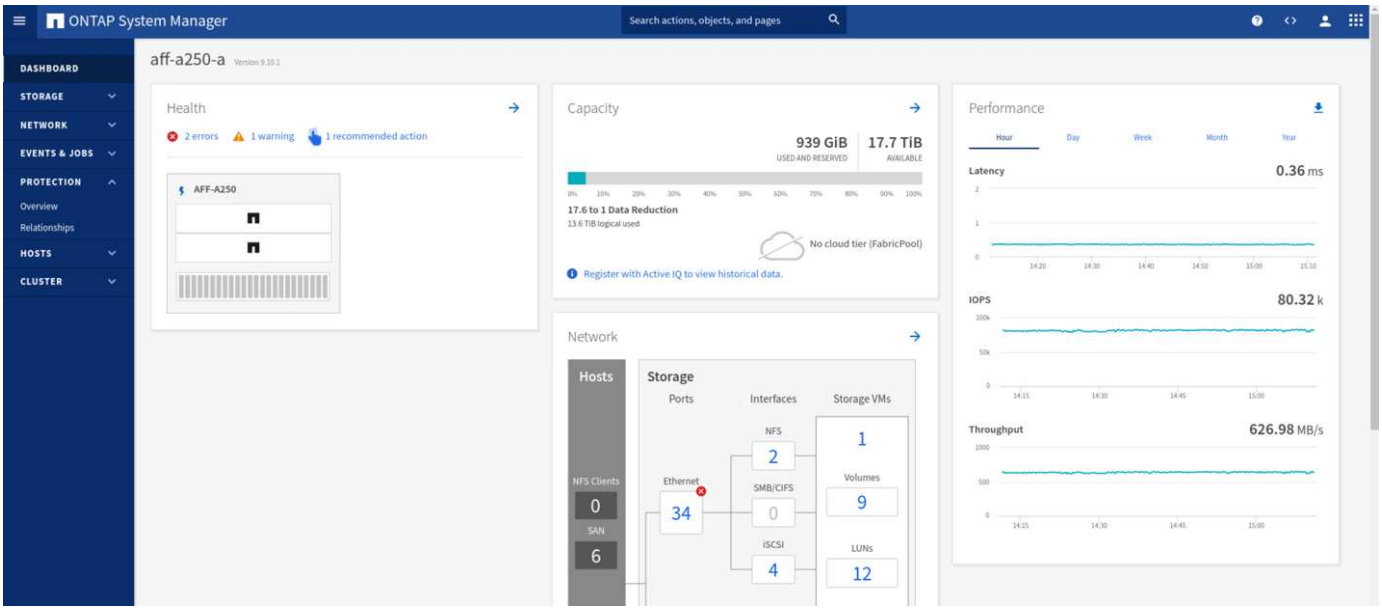
Pour simuler un incident de stockage au niveau du site A, les deux contrôleurs de stockage du site A peuvent être mis hors tension en mettant physiquement l'interrupteur afin de mettre fin à l'alimentation des contrôleurs, ou en utilisant la commande de gestion de l'alimentation système des processeurs de service du contrôleur de stockage pour mettre les contrôleurs hors tension.

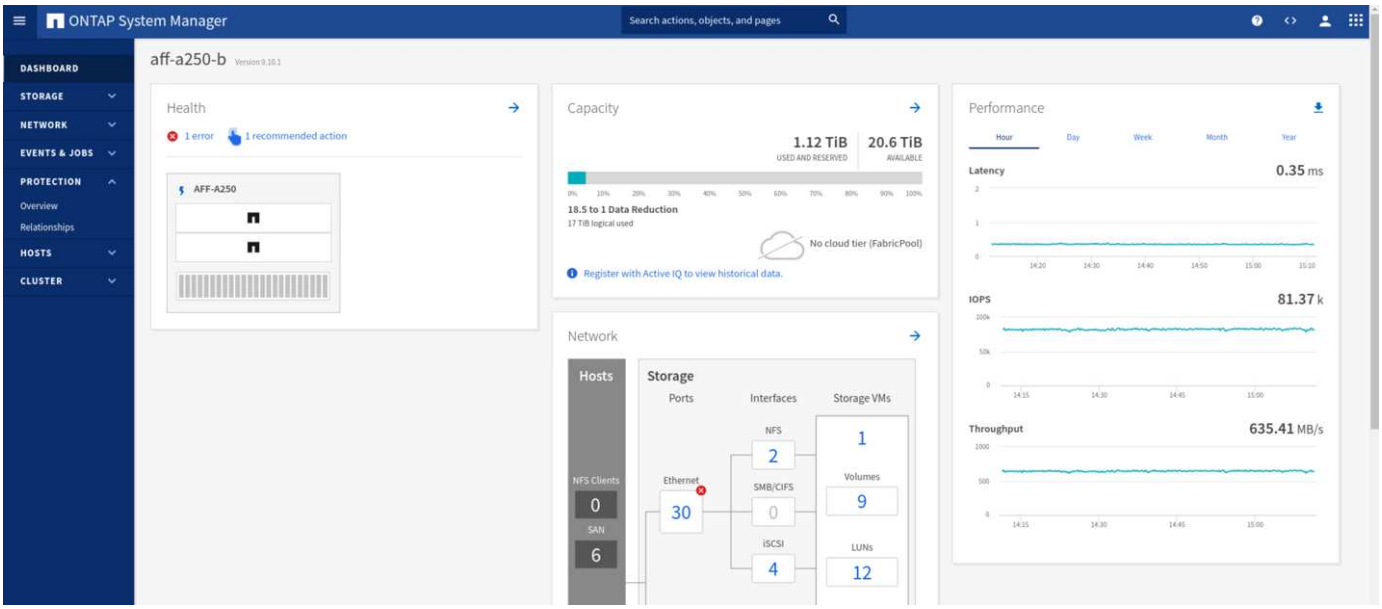
Lorsque le cluster de stockage du site a une perte de puissance, les services de données fournis par le site A du cluster de stockage sont stoppés soudainement. Ensuite, le médiateur ONTAP, qui surveille la solution SM-BC à partir d'un troisième site, détecte une condition de défaillance de stockage du site et permet à la solution SM-BC d'effectuer un basculement non planifié automatisé. Cela permet aux contrôleurs de stockage du site B de continuer les services de données pour les LUN configurés dans les relations du groupe de cohérence SM-

BC avec le site A.

Du point de vue des applications, les services de données font une pause brève fois que le système d'exploitation vérifie l'état du chemin des LUN, puis reprend les E/S sur les chemins disponibles vers les contrôleurs de stockage du site B survivants.

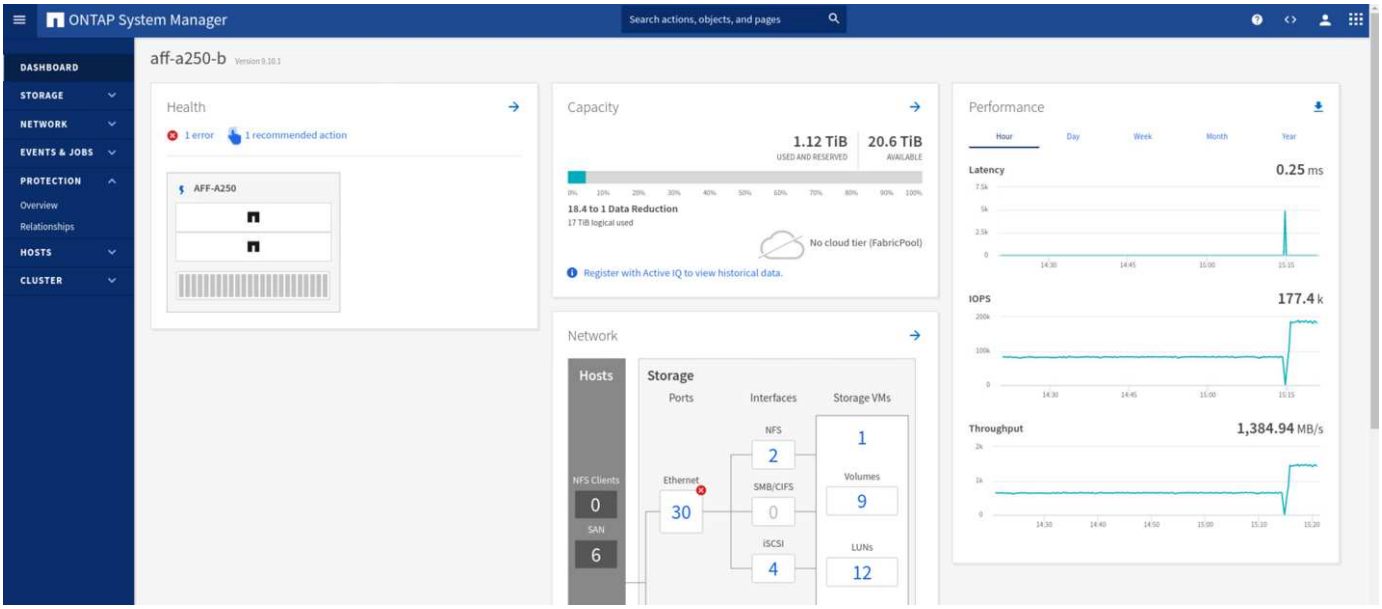
Lors des tests de validation, l'outil IOMeter installé sur les machines virtuelles des deux sites génère des E/S dans leurs datastores locaux. Après la mise hors tension du site D'Un cluster, les E/S sont suspendues brièvement et ont repris ensuite. Reportez-vous aux deux figures suivantes pour les tableaux de bord du cluster de stockage sur le site A et le site B, respectivement avant le sinistre qui montrent environ 80 000 IOPS et un débit de 600 Mo/s sur chaque site.



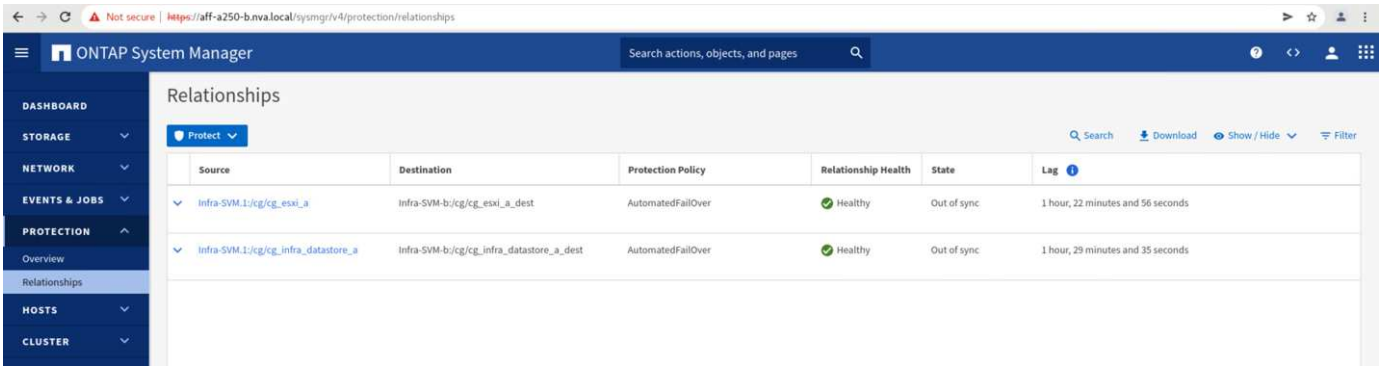


Après la mise hors tension des contrôleurs de stockage sur le site A, nous pouvons vérifier que les E/S du contrôleur de stockage du site B ont nettement augmenté pour fournir des services de données supplémentaires pour le compte du site A (voir la figure suivante). En outre, l'interface graphique des machines virtuelles IOMeter a également démontré la continuité des E/S malgré la panne du cluster de stockage sur le site. Notez que si d'autres datastores sont sauvegardés par des LUN non protégées par des relations SM-BC, ces datastores ne seront plus accessibles en cas d'incident de stockage. Par conséquent, il

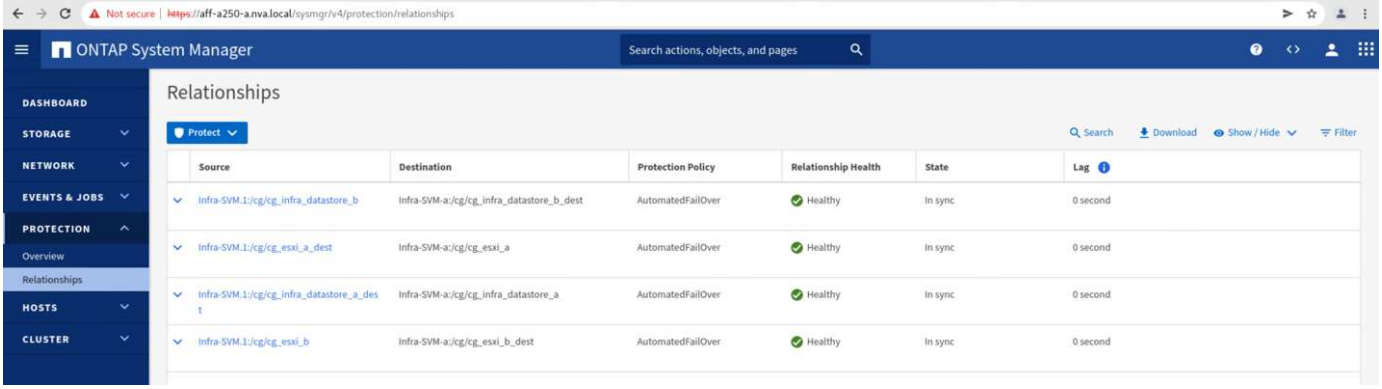
est important d'évaluer les besoins métier des diverses données d'application et de les placer correctement dans des datastores protégés par des relations SM-BC pour assurer la continuité de l'activité.



Le site D'Un cluster ne fonctionne pas, mais les relations des groupes cohérents s'affichent `Out of sync` état comme indiqué dans la figure suivante. Une fois que le système est de nouveau sous tension pour les contrôleurs de stockage du site A, le cluster de stockage démarre et la synchronisation des données entre le site A et le site B se produit automatiquement.



Avant de renvoyer les services de données du site B vers le site A, vous devez consulter le site A System Manager et vérifier que les relations SM-BC sont bien établies et que leur état est de nouveau synchronisé. Après avoir confirmé que les groupes de cohérence sont en cours de synchronisation, une opération de basculement manuel peut être lancée pour renvoyer les services de données dans les relations de groupe de cohérence vers le site A.



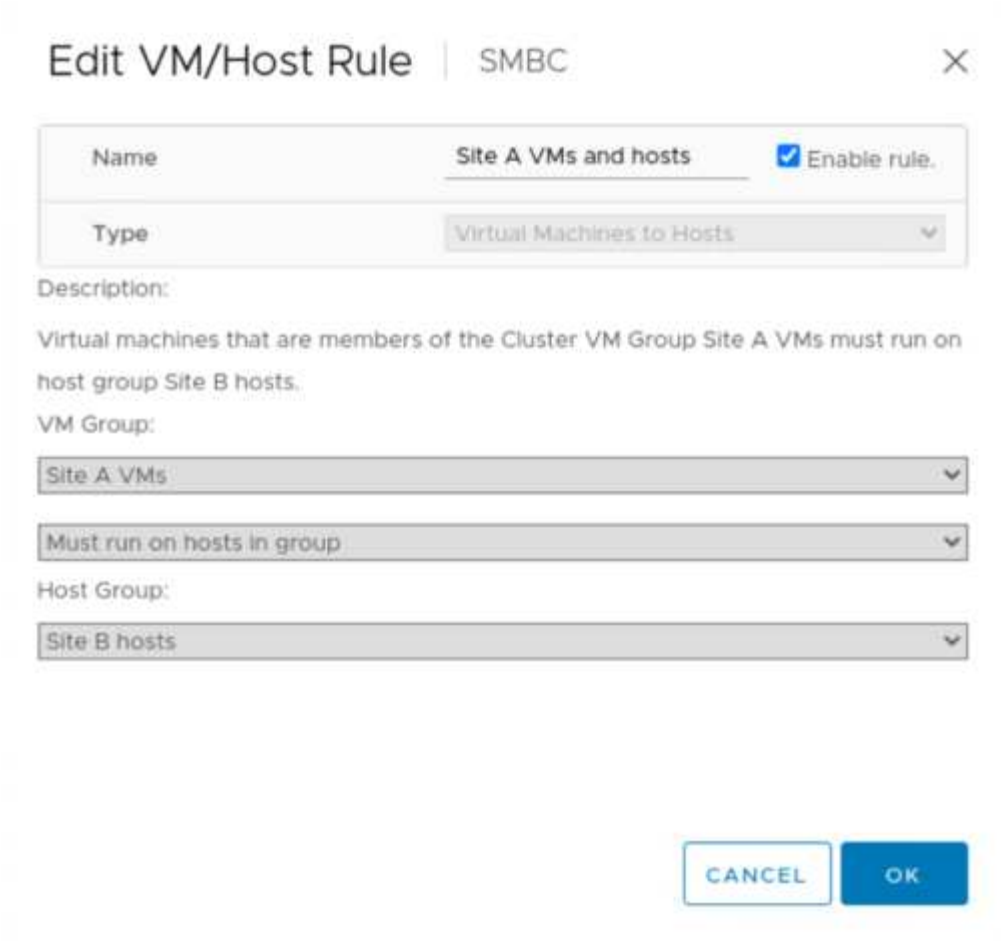
Effectuez les opérations de maintenance du site ou les pannes du site

Un site peut avoir besoin d'une maintenance de site, subir des pannes d'électricité ou être touché par une catastrophe naturelle comme un ouragan ou un tremblement de terre. Par conséquent, il est essentiel que vous pratiiez des scénarios d'échec de site planifiés et non planifiés pour vous assurer que votre solution FlexPod SM-BC est correctement configurée pour résister à de telles défaillances pour l'ensemble de vos applications et services de données stratégiques. Les scénarios suivants relatifs au site ont été validés.

- Scénario de maintenance de site planifié par la migration des machines virtuelles et des services de données critiques vers l'autre site
- Scénario de panne imprévue à l'échelle du site en mettant hors tension les serveurs et les contrôleurs de stockage à des fins de simulation d'incident

Pour préparer un site pour la maintenance planifiée des sites, une combinaison de migration des machines virtuelles concernées hors du site avec vMotion et d'un basculement manuel des relations de groupes de cohérence SM-BC est nécessaire pour migrer les machines virtuelles et les services de données critiques vers l'autre site. Les tests ont été réalisés en deux commandes différentes : VMotion a d'abord été suivi par les basculements SM-BC et SM-BC, puis vMotion, afin de confirmer que les machines virtuelles continuent à fonctionner et que les services de données ne sont pas interrompus.

Avant d'effectuer la migration planifiée, mettez à jour la règle d'affinité VM/hôte afin que les machines virtuelles actuellement exécutées sur le site soient automatiquement migrées hors du site en cours de maintenance. La capture d'écran suivante montre un exemple de modification de la règle d'affinité VM/hôte du site A pour que les machines virtuelles migrent automatiquement du site A vers le site B. Au lieu de spécifier que les VM doivent maintenant s'exécuter sur le site B, il est également possible de désactiver temporairement la règle d'affinité pour que les VM puissent être migrées manuellement.



Une fois les ordinateurs virtuels et les services de stockage migrés, vous pouvez mettre hors tension les serveurs, les contrôleurs de stockage, les tiroirs disques et les commutateurs, et réaliser les activités de maintenance du site nécessaires. Une fois la maintenance du site terminée et l'instance FlexPod renvoyée, vous pouvez modifier l'affinité des groupes d'hôtes pour que les VM reprennent leur site d'origine. Ensuite, vous devez modifier la règle d'affinité VM/site hôte "doit être exécuté sur des hôtes dans un groupe" en "devrait s'exécuter sur des hôtes dans un groupe" afin que les machines virtuelles soient autorisées à fonctionner sur des hôtes de l'autre site en cas d'incident. Pour les tests de validation, toutes les machines virtuelles ont été migrées avec succès vers l'autre site et les services de données se sont poursuivis sans problèmes après avoir effectué un basculement pour les relations SM-BC.

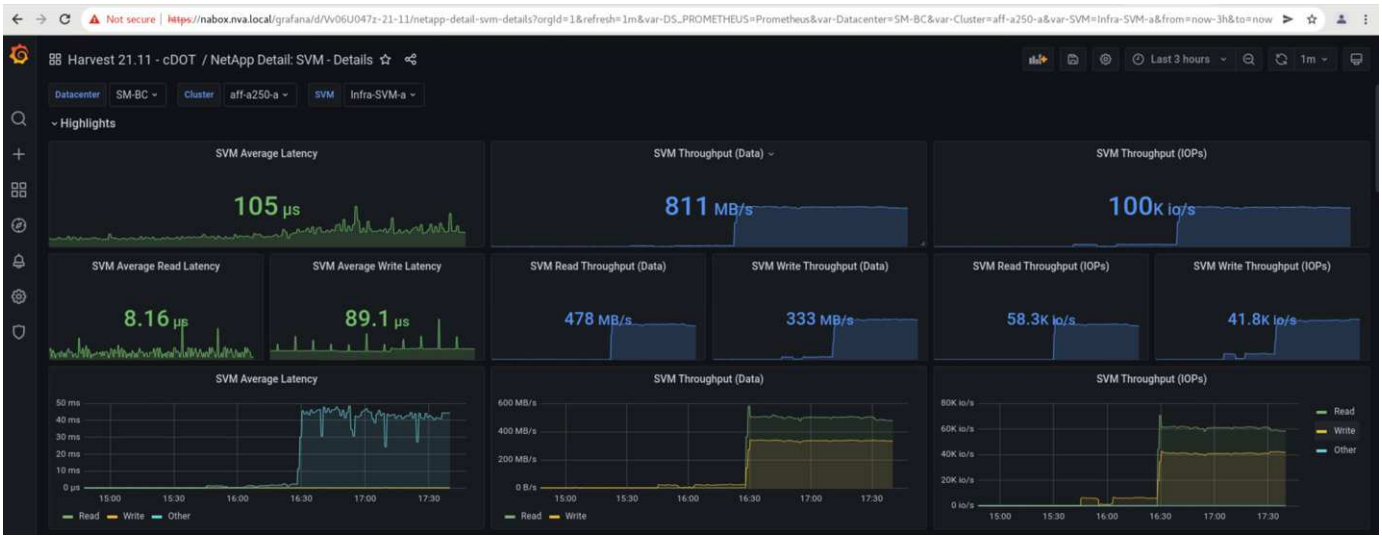
Pour la simulation d'incident imprévue à l'échelle du site, les serveurs et les contrôleurs de stockage ont été mis hors tension afin de simuler un incident de site. La fonction VMware HA détecte les machines virtuelles qui sont arrêté et redémarre ces machines virtuelles sur le site survivant. En outre, le médiateur ONTAP fonctionnant sur un troisième site détecte la panne du site et le site survivant lance un basculement et commence à fournir des services de données pour le site en panne comme prévu.

La capture d'écran suivante montre que l'interface de ligne de commande du processeur de service des contrôleurs de stockage a été utilisée pour mettre hors tension le site D'Un cluster brusquement afin de simuler un incident de stockage sur le site.

```
[BMC aff-a250-a-01>
[BMC aff-a250-a-01>
[BMC aff-a250-a-01>
[BMC aff-a250-a-01>system power off
 Chassis Power Control: Down/Off
 BMC aff-a250-a-01>
```

```
[BMC aff-a250-a-02>
[BMC aff-a250-a-02>
[BMC aff-a250-a-02>
[BMC aff-a250-a-02>system power off
 Chassis Power Control: Down/Off
 BMC aff-a250-a-02>
```

Les tableaux de bord des machines virtuelles de stockage des clusters, tels que capturés par l'outil NetApp Harvest Data et affichés dans le tableau de bord Grafana dans l'outil de surveillance NAbox, sont présentés dans les deux captures d'écran suivantes. Comme l'indique les graphiques à droite des IOPS et des débits, le cluster du site B récupère les charges de travail de stockage du cluster immédiatement après la panne du site A.

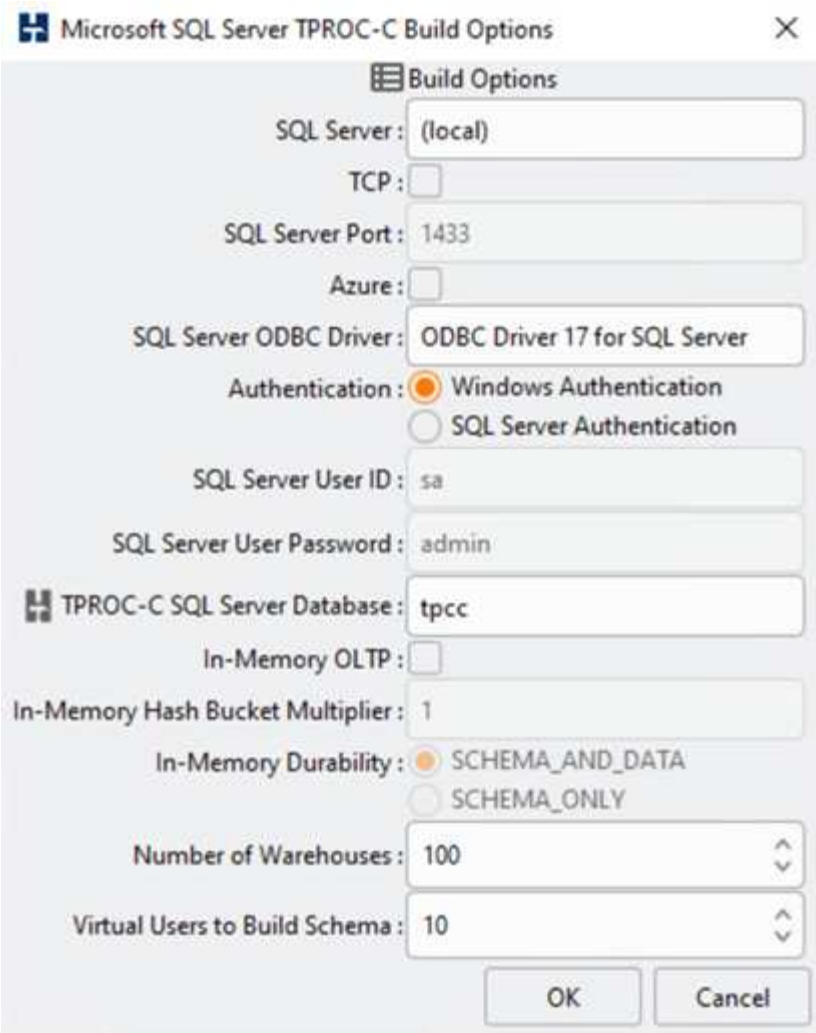


Microsoft SQL Server

Microsoft SQL Server est une plateforme de base de données adoptée et déployée pour LE DÉPARTEMENT INFORMATIQUE de l'entreprise. La version Microsoft SQL Server 2019 apporte beaucoup de nouvelles fonctionnalités et améliorations à ses moteurs relationnels et analytiques. Ce logiciel prend en charge les workloads avec des applications exécutées sur site, dans le cloud et dans un environnement hybride. En outre, il peut être déployé sur plusieurs plateformes, notamment Windows, Linux et les conteneurs.

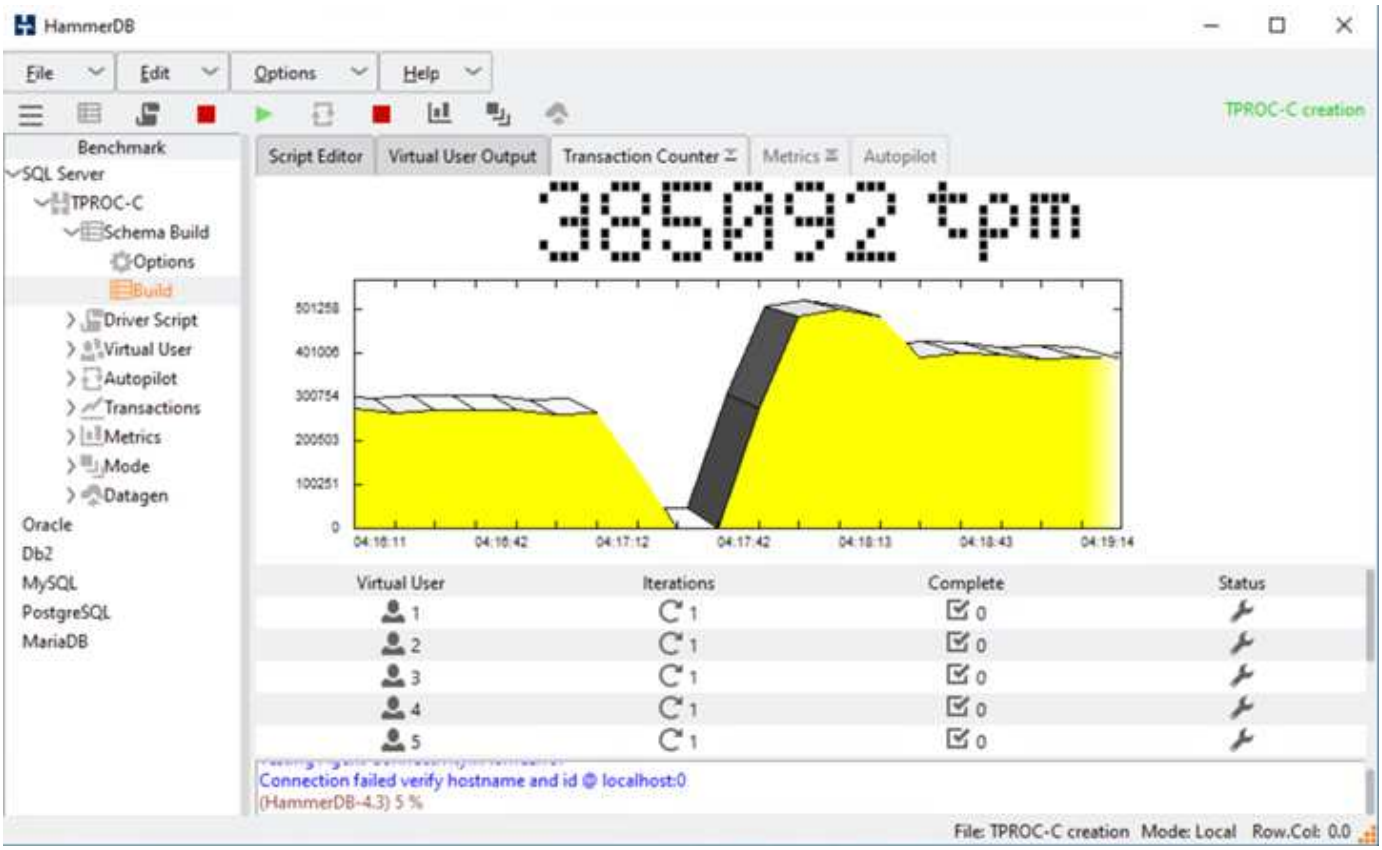
Dans le cadre de la validation des charges de travail stratégiques pour la solution FlexPod SM-BC, Microsoft SQL Server 2019 installé sur une machine virtuelle Windows Server 2022 est inclus avec les machines virtuelles IOMeter pour les tests de basculement du stockage planifiés et non planifiés de SM-BC. Sur la machine virtuelle Windows Server 2022, SQL Server Management Studio est installé pour gérer le serveur SQL. Pour les tests, l'outil base de données HammerDB est utilisé pour générer des transactions de base de données.

L'outil de test de la base de données HammerDB a été configuré pour les tests avec la charge de travail TPROC-C de Microsoft SQL Server. Pour les configurations de construction de schéma, les options ont été mises à jour pour utiliser 100 entrepôts avec 10 utilisateurs virtuels comme indiqué dans la capture d'écran suivante.



Une fois les options de création de schéma mises à jour, le processus de création de schéma a démarré. Quelques minutes plus tard, une erreur simulée de cluster de stockage du site B a été introduite en mettant hors tension les deux nœuds du cluster de stockage AFF A250 à environ la même heure à l'aide des commandes CLI du processeur système.

Après une courte pause des transactions de base de données, le basculement automatique pour la correction des sinistres a débuté et les transactions ont repris. La capture d'écran ci-dessous montre la capture d'écran du compteur de transactions HammerDB. Étant donné que la base de données de Microsoft SQL Server réside généralement dans le cluster de stockage du site B, la transaction a été interrompue brièvement lorsque le stockage sur le site B s'est arrêté, puis reprise après le basculement automatisé.



Les metrics du cluster de stockage ont été capturées à l'aide de l'outil NAbox et de l'outil de surveillance de récolte NetApp installé. Les résultats sont affichés dans les tableaux de bord prédéfinis de Grafana pour la machine virtuelle de stockage et autres objets de stockage. Le tableau de bord fournit des schémas de latence, de débit et d'IOPS, ainsi que des détails supplémentaires avec des statistiques de lecture et d'écriture séparées pour le site B et le site A.

Cette capture d'écran présente le tableau de bord des performances NAbox Grafana pour cluster de stockage site B.

Le cluster de stockage du site B était d'environ 100 000 IOPS avant l'introduction de l'incident. Ensuite, les mesures de performances ont montré une baisse nette de zéro à droite des graphiques dus à l'incident. Comme le cluster de stockage du site B était en panne, aucun élément ne pouvait être collecté à partir du

cluster du site B après l'introduction du sinistre.

À l'inverse, les IOPS du cluster de stockage du site A ont récupéré les charges de travail supplémentaires depuis le site B après le basculement automatisé. La charge de travail supplémentaire est facilement affichée à droite des graphiques IOPS et débit dans la capture d'écran suivante, qui montre le tableau de bord des performances de NAbox Grafana pour site De cluster de stockage.

Le scénario de test d'incident de stockage ci-dessus a confirmé que la charge de travail de Microsoft SQL Server peut survivre à une panne complète du cluster de stockage sur le site B où réside la base de données. Une fois l'incident détecté et le basculement effectué, l'application a utilisé de manière transparente les services de données du site De cluster De stockage.

Au niveau de la couche de calcul, lorsque les machines virtuelles qui s'exécutent sur un site particulier souffrent d'une défaillance d'hôte, les machines virtuelles sont conçues pour être redémarrée automatiquement par la fonctionnalité de haute disponibilité VMware. En cas de panne de calcul de l'ensemble du site, les règles d'affinité VM/hôte permettent de redémarrer les machines virtuelles sur le site survivant. Cependant, pour qu'une application stratégique puisse fournir des services sans interruption, une solution de mise en cluster basée sur des applications telles que Microsoft Failover Cluster ou l'architecture applicative basée sur des conteneurs Kubernetes doit éviter les temps d'indisponibilité des applications. Veuillez vous reporter au document relatif à l'implémentation de la mise en cluster basée sur l'application, qui va au-delà du périmètre de ce rapport technique.

"Suivant: Conclusion."

Conclusion

"Précédent : validation des solutions - scénarios validés"

Le FlexPod Datacenter avec SM-BC utilise une conception de data Center actif-actif afin d'assurer la continuité de l'activité et la reprise après incident pour les workloads stratégiques. La solution interconnecte généralement deux data centers déployés dans des sites séparés géographiquement dispersés dans une zone métropolitaine. La solution NetApp SM-BC utilise une réplication synchrone pour protéger les services de données stratégiques contre une panne sur site. La solution requiert que les deux sites de déploiement FlexPod offrent une latence réseau aller-retour inférieure à 10

millisecondes.

Le médiateur NetApp ONTAP déployé sur un site tiers surveille la solution SM-BC et permet un basculement automatisé en cas d'incident sur site. VMware vCenter avec VMware HA et étendu la configuration du cluster de stockage Metro VMware vSphere fonctionne en toute transparence avec NetApp SM-BC, afin de permettre à la solution de respecter le RPO nul et les objectifs de durée de restauration proches de zéro.

La solution FlexPod SM-BC peut également être déployée sur les infrastructures FlexPod existantes s'ils répondent aux exigences ou en ajoutant une solution FlexPod supplémentaire à un FlexPod existant pour atteindre les objectifs de continuité de l'activité. Des outils supplémentaires de gestion, de contrôle et d'automatisation tels que Cisco InterSight, Ansible et HashiCorp Terraform Automation sont disponibles auprès de NetApp et Cisco. Vous pouvez facilement surveiller la solution, obtenir des informations sur ses opérations et automatiser son déploiement et ses opérations.

Du point de vue d'une application stratégique telle que Microsoft SQL Server, une base de données résidant sur un datastore VMware protégé par une relation de groupe de cohérence ONTAP SM-BC reste disponible malgré une panne du stockage sur site. Comme vérifié lors du test de validation, après une panne de courant du cluster de stockage où réside la base de données, un basculement de la relation SM-BC CG CG CG se produit et les transactions Microsoft SQL Server reprennent sans interruption des applications.

Grâce à la protection granulaire des données des applications, vous pouvez créer des relations ONTAP SM-BC CG pour vos applications stratégiques afin de répondre aux exigences RPO zéro et RTO quasi nul. Afin que le cluster VMware sur lequel l'application Microsoft SQL Server s'exécute puisse survivre à une panne de stockage de site, les LUN de démarrage des hôtes ESXi de chaque site sont également protégées par une relation SM-BC CG CG CG CG.

La flexibilité et l'évolutivité de FlexPod vous permettent de démarrer avec une infrastructure correctement dimensionnée qui peut évoluer et évoluer en fonction des exigences de votre entreprise. Cette conception validée vous permet de déployer de manière fiable un cloud privé VMware vSphere sur une infrastructure intégrée et distribuée. Vous bénéficiez ainsi d'une solution résiliente à de nombreux scénarios de défaillance unique, ainsi qu'une défaillance d'un site, pour protéger les services de données stratégiques.

"Suivant : où trouver des informations supplémentaires et l'historique des versions ?"

Où trouver des informations supplémentaires et l'historique des versions

"Précédent: Conclusion."

Pour en savoir plus sur les informations données dans ce livre blanc, consultez ces documents et/ou sites web :

FlexPod

- Page d'accueil de FlexPod

  "https://www.flexpod.com"

- Guides de conception et de déploiement validés par Cisco pour FlexPod

  "https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html"

- Serveurs Cisco - Unified Computing System (UCS)

  "https://www.cisco.com/c/en/us/products/servers-unified-computing/index.html"

- Documentation produit NetApp

  "https://www.netapp.com/support-and-training/documentation/"

- FlexPod Datacenter avec Cisco UCS 4.2(1) en mode géré UCS, VMware vSphere 7.0 U2 et NetApp ONTAP 9.9 : Guide de conception

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_m6_esxi7u2_design.html"

- Guide de déploiement de FlexPod Datacenter avec Cisco UCS 4.2(1) en mode géré UCS, VMware vSphere 7.0 U2 et NetApp ONTAP 9.9

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_m6_esxi7u2.html"

- Guide de design de FlexPod Datacenter avec Cisco UCS X-Series, VMware 7.0 U2 et NetApp ONTAP 9.9

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_esxi7u2_design.html"

- Guide de déploiement de FlexPod Datacenter avec Cisco UCS X-Series, VMware 7.0 U2 et NetApp ONTAP 9.9

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_vmware_7u2.html"

- Guide de design de FlexPod Express pour VMware vSphere 7.0 avec Cisco UCS Mini et baies NetApp AFF/FAS NVA

  https://www.netapp.com/pdf.html?item=/media/22621-nva-1154-DESIGN.pdf

- Guide de déploiement de FlexPod Express pour VMware vSphere 7.0 avec Cisco UCS Mini et NVA AFF/FAS de NetApp

  https://www.netapp.com/pdf.html?item=/media/21938-nva-1154-DEPLOY.pdf

- FlexPod MetroCluster IP avec structure front-end multisite VXLAN

  "https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/flexpod-metrocluster-ip-vxlan-multi-site-wp.pdf"

- Boîte NAbox

  "https://nabox.org"

- Récolte NetApp

  "https://github.com/NetApp/harvest/releases"

SM-BC

- SM-BC

  "https://docs.netapp.com/us-en/ontap/smbc/index.html"

- Tr-4878 : continuité de l'activité SnapMirror (SM-BC) ONTAP 9.8

  https://www.netapp.com/pdf.html?item=/media/21888-tr-4878.pdf

- Comment supprimer correctement une relation SnapMirror ONTAP 9

  "https://kb.netapp.com/Advice_and_Troubleshooting/Data_Protection_and_Security/SnapMirror/How_to_correctly_delete_a_SnapMirror_relationship_ONTAP_9"

- Principes de base de la reprise après incident synchrone de SnapMirror

  "https://docs.netapp.com/us-en/ontap/data-protection/snapmirror-synchronous-disaster-recovery-basics-concept.html"

- Principes de base de la reprise sur incident asynchrone SnapMirror

  "https://docs.netapp.com/us-en/ontap/data-protection/snapmirror-disaster-recovery-concept.html#data-protection-relationships"

- Protection des données et reprise d'activité

  "https://docs.netapp.com/us-en/ontap/data-protection-disaster-recovery/index.html"

- Installez ou mettez à niveau le service ONTAP Mediator

  "https://docs.netapp.com/us-en/ontap/mediator/index.html"

VMware vSphere HA et vSphere Metro Storage Cluster

- Création et utilisation de clusters HA vSphere

  "https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.avail.doc/GUID-5432CA24-14F1-44E3-87FB-61D937831CF6.html"

- Cluster de stockage Metro VMware vSphere (vMSC)

  "https://core.vmware.com/resource/vmware-vsphere-metro-storage-cluster-vmsc"

- Bonnes pratiques pour VMware vSphere Metro Storage Cluster

  "https://core.vmware.com/resource/vmware-vsphere-metro-storage-cluster-recommended-practices"

- NetApp ONTAP avec NetApp SnapMirror Business Continuity (SM-BC) avec VMware vSphere Metro Storage Cluster (vMSC). (83370)

  "https://kb.vmware.com/s/article/83370"

- Protégez les bases de données et les applications de niveau 1 avec VMware vSphere Metro Storage Cluster et ONTAP

"https://community.netapp.com/t5/Tech-ONTAP-Blogs/Protect-tier-1-applications-and-databases-with-VMware-vSphere-Metro-Storage/ba-p/171636"

Microsoft SQL et HammerDB

- Microsoft SQL Server 2019

  "https://www.microsoft.com/en-us/sql-server/sql-server-2019"

- Guide des meilleures pratiques de conception de Microsoft SQL Server sur VMware vSphere

  "https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/solutions/sql-server-on-vmware-best-practices-guide.pdf"

- Site Web HammerDB

  "https://www.hammerdb.com"

Matrice de compatibilité

- Matrice de compatibilité matérielle Cisco UCS

  "https://ucshcltool.cloudapps.cisco.com/public/"

- Matrice d'interopérabilité NetApp

  "https://support.netapp.com/matrix/"

- NetApp Hardware Universe

  "https://hwu.netapp.com"

- Guide de compatibilité VMware

  "http://www.vmware.com/resources/compatibility/search.php"

Historique des versions

Version	Date	Historique des versions du document
Version 1.0	Avril 2022	Version initiale.