La préparation de l'installation de MetroCluster

ONTAP MetroCluster

NetApp
April 19, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/ontap-metrocluster/install-stretch/concept_considerations_differences.html on April 19, 2024. Always check docs.netapp.com for the latest.

Sommaire

La préparation de l'installation de MetroCluster 1
Différences entre les configurations ONTAP MetroCluster 1
Peering de clusters 3
Considérations relatives à l'utilisation d'agrégats non mis en miroir 5
Utilisation du pare-feu sur les sites MetroCluster 6

La préparation de l’installation de MetroCluster

Différences entre les configurations ONTAP MetroCluster

Les différentes configurations MetroCluster présentent des différences clés au niveau des composants requis.

Dans toutes les configurations, chacun des deux sites MetroCluster est configuré en tant que cluster ONTAP. Dans une configuration MetroCluster à deux nœuds, chaque nœud est configuré en tant que cluster à un seul nœud.

Fonction	Configurations IP	Configurations intégrées à la structure		Configurations Stretch	
		Quatre ou huit noeuds	**Deux nœuds**	**Connexion pont à deux noeuds**	**Connexion directe à deux nœuds**
Nombre de contrôleurs	Quatre ou huit*	Quatre ou huit	Deux	Deux	Deux
Utilise une structure de stockage avec commutateur FC	Non	Oui.	Oui.	Non	Non
Utilise une structure de stockage avec commutateurs IP	Oui.	Non	Non	Non	Non
Utilise des ponts FC-SAS	Non	Oui.	Oui.	Oui.	Non
Utilise un stockage SAS direct	Oui (local uniquement)	Non	Non	Non	Oui.
Prend en charge ADP	Oui (à partir de ONTAP 9.4)	Non	Non	Non	Non
Prend en charge la haute disponibilité locale	Oui.	Oui.	Non	Non	Non

Prise en charge du basculement automatique non planifié avec ONTAP	Non	Oui.	Oui.	Oui.	Oui.
Prend en charge les agrégats sans miroir	Oui (à partir de ONTAP 9.8)	Oui.	Oui.	Oui.	Oui.
Prise en charge des LUN de baies	Non	Oui.	Oui.	Oui.	Oui.
Prend en charge le médiateur ONTAP	Oui (à partir de ONTAP 9.7)	Non	Non	Non	Non
Prise en charge d'MetroCluster Tiebreaker	Oui (pas en combinaison avec le médiateur ONTAP)	Oui.	Oui.	Oui.	Oui.
Supports Toutes les baies SAN	Oui.	Oui.	Oui.	Oui.	Oui.

Important

Notez les éléments suivants pour les configurations IP MetroCluster à 8 nœuds :

- Les configurations à huit nœuds sont prises en charge à partir de ONTAP 9.9.1.
- Seuls les commutateurs MetroCluster validés par NetApp (commandés auprès de NetApp) sont pris en charge.
- Les configurations utilisant des connexions back-end routées par IP (couche 3) ne sont pas prises en charge.
- Les configurations utilisant des réseaux privés partagés de couche 2 ne sont pas prises en charge.
- Les configurations utilisant un commutateur partagé Cisco 9336C-FX2 ne sont pas prises en charge.

Prise en charge de toutes les baies SAN dans les configurations MetroCluster

Certaines baies SAN (ASAS) sont prises en charge dans les configurations MetroCluster. Dans la documentation MetroCluster, les informations relatives aux modèles AFF s'appliquent au système ASA correspondant. Par exemple, tous les câbles et autres informations du système AFF A400 s'appliquent également au système ASA AFF A400.

Les configurations de plateforme prises en charge sont répertoriées dans le "NetApp Hardware Universe".

Peering de clusters

Chaque site MetroCluster est configuré comme homologue de son site partenaire. Vous devez connaître les conditions préalables et les instructions de configuration des relations de peering. C'est important lorsque vous décidez d'utiliser des ports partagés ou dédiés pour ces relations.

Informations associées

"Configuration cluster et SVM peering express"

Conditions préalables au peering de clusters

Avant de configurer le peering de cluster, vous devez vérifier que la connectivité entre le port, l'adresse IP, le sous-réseau, le pare-feu et les exigences de nommage des clusters sont respectées.

Les besoins en connectivité

Chaque LIF intercluster du cluster local doit pouvoir communiquer avec chaque LIF intercluster sur le cluster distant.

Bien qu'il ne soit pas nécessaire, il est généralement plus simple de configurer les adresses IP utilisées pour les LIF intercluster dans le même sous-réseau. Les adresses IP peuvent résider dans le même sous-réseau que les LIF de données ou dans un autre sous-réseau. Le sous-réseau utilisé dans chaque cluster doit respecter les exigences suivantes :

- Le sous-réseau doit disposer de suffisamment d'adresses IP disponibles pour allouer à une LIF intercluster par nœud.

  Par exemple, dans un cluster à quatre nœuds, le sous-réseau utilisé pour la communication intercluster doit disposer de quatre adresses IP disponibles.

Chaque nœud doit disposer d'un LIF intercluster avec une adresse IP sur le réseau intercluster.

Les LIF intercluster peuvent disposer d'une adresse IPv4 ou IPv6.

> ONTAP 9 vous permet de migrer vos réseaux de peering d'IPv4 vers IPv6 en autorisant, éventuellement, la présence simultanée des deux protocoles sur les LIF intercluster. Dans les versions précédentes, toutes les relations intercluster pour un cluster entier étaient au format IPv4 ou IPv6. Cela signifiait que le changement de protocole était potentiellement source de perturbation.

Configuration requise pour les ports

Vous pouvez utiliser des ports dédiés pour la communication intercluster ou partager les ports utilisés par le réseau de données. Les ports doivent répondre aux exigences suivantes :

- Tous les ports utilisés pour communiquer avec un cluster distant donné doivent se trouver dans le même IPspace.

  Vous pouvez utiliser plusieurs IPspaces pour gérer plusieurs clusters dans un même cluster. Une connectivité à maillage complet par paire est requise uniquement au sein d'un IPspace.

- Le broadcast domain utilisé pour les communications intercluster doit inclure au moins deux ports par nœud afin que la communication intercluster puisse basculer d'un port vers un autre.

  Les ports ajoutés à un domaine de diffusion peuvent être des ports réseau physiques, des VLAN ou des groupes d'interfaces (ifgrps).

- Tous les ports doivent être câblés.
- Tous les ports doivent être en état de santé.
- Les paramètres MTU des ports doivent être cohérents.

Exigences relatives au pare-feu

Les pare-feu et la politique de pare-feu intercluster doivent autoriser les protocoles suivants :

- Service ICMP
- TCP aux adresses IP de toutes les LIFs intercluster sur les ports 10000, 11104 et 11105
- HTTPS bidirectionnel entre les LIFs intercluster

La politique de pare-feu intercluster par défaut permet l'accès via le protocole HTTPS et à partir de toutes les adresses IP (0.0.0.0/0). Vous pouvez modifier ou remplacer la stratégie si nécessaire.

Considérations relatives à l'utilisation de ports dédiés

Pour déterminer si l'utilisation d'un port dédié pour la réplication intercluster est la bonne solution réseau intercluster, vous devez tenir compte des configurations et des exigences telles que le type de LAN, la bande passante WAN disponible, l'intervalle de réplication, le taux de changement et le nombre de ports.

Pour déterminer si l'utilisation d'un port dédié est la meilleure solution réseau intercluster, prenez en compte les aspects suivants de votre réseau :

- Si la quantité de bande passante WAN disponible est similaire à celle des ports LAN et que l'intervalle de réplication est tel que la réplication se produit pendant que l'activité client est régulière, alors vous devez dédier des ports Ethernet à la réplication intercluster pour éviter les conflits entre la réplication et les protocoles de données.
- Si l'utilisation du réseau générée par les protocoles de données (CIFS, NFS et iSCSI) est telle que l'utilisation du réseau dépasse 50 %, alors dédier des ports à la réplication pour permettre des performances non dégradées en cas de basculement sur un nœud.
- Lorsque des ports physiques 10 GbE ou plus rapides sont utilisés pour les données et la réplication, vous pouvez créer des ports VLAN pour la réplication et dédier les ports logiques à la réplication intercluster.

  La bande passante du port est partagée entre tous les VLAN et le port de base.

- Tenez compte du taux de modification des données et de l'intervalle de réplication et de l'espace requis pour déterminer si la quantité de données qui doit être répliquée sur chaque intervalle nécessite suffisamment de bande passante. Cela peut générer des conflits avec les protocoles de données en cas de partage de ports de données.

Points à prendre en compte lors du partage de ports de données

Lors de la détermination du partage d'un port de données pour la réplication intercluster est la bonne solution réseau intercluster, vous devez tenir compte des configurations et des exigences telles que le type de LAN, la bande passante WAN disponible, l'intervalle de réplication, le taux de changement et le nombre de ports.

Prenez en compte les aspects suivants de votre réseau pour déterminer si le partage de ports de données est la meilleure solution de connectivité intercluster :

- Pour un réseau haut débit, tel qu'un réseau 40 Gigabit Ethernet (40-GbE), une quantité suffisante de bande passante LAN locale peut être disponible pour effectuer la réplication sur les mêmes ports 40 GbE utilisés pour l'accès aux données.

  Dans la plupart des cas, la bande passante WAN disponible est bien inférieure à celle du réseau LAN 10 GbE.

- Le partage des ports de données peut être dû à tous les nœuds du cluster pour répliquer des données et partager la bande passante WAN disponible.
- Le partage de ports pour les données et la réplication élimine le nombre de ports supplémentaires requis pour dédier des ports à la réplication.
- La taille maximale de l'unité de transmission (MTU) du réseau de réplication sera la même que celle utilisée sur le réseau de données.
- Tenez compte du taux de modification des données et de l'intervalle de réplication et de l'espace requis pour déterminer si la quantité de données qui doit être répliquée sur chaque intervalle nécessite suffisamment de bande passante. Cela peut générer des conflits avec les protocoles de données en cas de partage de ports de données.
- Lorsque les ports de données pour la réplication intercluster sont partagés, les LIFs intercluster peuvent être migrés vers n'importe quel autre port intercluster du même nœud afin de contrôler le port de données spécifique utilisé pour la réplication.

Considérations relatives à l'utilisation d'agrégats non mis en miroir

Considérations relatives à l'utilisation d'agrégats non mis en miroir

Si votre configuration inclut des agrégats sans mise en miroir, vous devez connaître les problèmes d'accès potentiels qui suivent les opérations de basculement.

Considérations relatives aux agrégats non mis en miroir lors de tâches de maintenance nécessitant l'arrêt d'alimentation

Si vous effectuez un basculement négocié pour des raisons de maintenance requérant un arrêt de l'alimentation à l'échelle du site, vous devez d'abord mettre manuellement hors ligne les agrégats non mis en miroir qui appartiennent au site de reprise sur incident.

Si vous ne mettez pas d'agrégats non mis en miroir hors ligne, les nœuds du site survivant peuvent tomber en panne en raison de la présence de incohérences de plusieurs disques. Cela peut se produire lorsqu'un basculement sur des agrégats non mis en miroir est hors ligne ou lorsqu'ils sont manquants en raison de la perte de connectivité au stockage sur le site de secours. Cela est le résultat d'un arrêt de courant ou d'une perte de liens ISL.

Considérations relatives aux agrégats non mis en miroir et aux espaces de noms hiérarchiques

Si vous utilisez des espaces de noms hiérarchiques, vous devez configurer le chemin de jonction de sorte que tous les volumes de ce chemin soient sur des agrégats en miroir uniquement ou sur des agrégats non mis en miroir uniquement. La configuration d'agrégats non mis en miroir et en miroir dans le chemin de jonction peut

empêcher l'accès aux agrégats non mis en miroir après le basculement.

Considérations relatives aux agrégats non mis en miroir et aux volumes de métadonnées CRS et aux volumes racines des SVM de données

Le volume des métadonnées du service de réplication de la configuration (CRS) et les volumes root du SVM de données doivent se trouver sur un agrégat en miroir. Vous ne pouvez pas déplacer ces volumes vers un agrégat non mis en miroir. S'ils se trouvent sur un agrégat non mis en miroir, les opérations négociées de basculement et de rétablissement sont vetotées. La commande MetroCluster check fournit un avertissement si c'est le cas.

Considérations relatives aux SVM et aux agrégats sans miroir

Les SVM doivent être configurés sur des agrégats en miroir uniquement ou sur des agrégats sans miroir uniquement. La configuration d'une combinaison d'agrégats non mis en miroir et en miroir peut entraîner un basculement supérieur à 120 secondes et entraîner une panne des données en cas d'indisponibilité des agrégats non mis en miroir.

Considérations relatives aux agrégats sans miroir et à SAN

Dans les versions ONTAP antérieures à 9.9.1, un LUN ne doit pas être situé sur un agrégat sans miroir. La configuration d'une LUN sur un agrégat non mis en miroir peut entraîner un basculement supérieur à 120 secondes et une panne de données.

Utilisation du pare-feu sur les sites MetroCluster

Considérations relatives à l'utilisation du pare-feu sur les sites MetroCluster

Si vous utilisez un pare-feu sur un site MetroCluster, vous devez vous assurer de l'accès aux ports requis.

Le tableau suivant montre l'utilisation du port TCP/UDP dans un pare-feu externe placé entre deux sites MetroCluster.

Type de trafic	Port/services
Peering de clusters	11104 / TCP 11105 / TCP
ONTAP System Manager	443 / TCP
MetroCluster IP LIFs intercluster	65200 / TCP 10006 / TCP et UDP
Assistance matérielle	4444 / TCP

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

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

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

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

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

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

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

Informations sur les marques commerciales

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