Préparation du cluster et de la SVM peering

ONTAP 9

NetApp
February 13, 2026

This PDF was generated from https://docs.netapp.com/fr-fr/ontap/peering/peering-basics-concept.html on February 13, 2026. Always check docs.netapp.com for the latest.

Sommaire

Préparation du cluster et de la SVM peering . . . 1
- Principes de base du peering ONTAP . . . 1
- Conditions préalables au peering ONTAP . . . 1
  - Les besoins en connectivité . . . 2
  - Configuration requise pour les ports . . . 2
  - Exigences relatives au pare-feu . . . 2
  - Regroupement des clusters . . . 3
- Utilisez des ports ONTAP partagés ou dédiés . . . 3
  - La bande passante du réseau . . . 3
  - Intervalle de réplication . . . 4
  - Disponibilité du port . . . 4
- Utilisez des IPspaces ONTAP personnalisés pour isoler le trafic de réplication . . . 4

Préparation du cluster et de la SVM peering

Principes de base du peering ONTAP

Vous devez créer des *relations peer* entre les clusters source et de destination et entre les SVM source et de destination avant de pouvoir répliquer des snapshots à l'aide de SnapMirror. Une relation de type peer-to-peer définit les connexions réseau qui permettent aux clusters et aux SVM d'échanger les données de manière sécurisée.

Les clusters et les SVM dans des relations entre pairs communiquent sur le réseau intercluster à l'aide de *interfaces logiques (LIF) intercluster.* une LIF intercluster est une LIF qui prend en charge le service d'interface réseau « intercluster-core » et qui est généralement créée en utilisant la politique de service d'interface réseau « default-intercluster ». On doit créer des LIF intercluster sur chaque nœud des clusters en cours de peering.

Les LIFs intercluster utilisent des routes qui appartiennent au SVM système auquel elles sont assignées. ONTAP crée automatiquement un SVM système pour les communications au niveau du cluster au sein d'un IPspace.

Les topologies en mode « Fan-Out » et en cascade sont toutes deux prises en charge. Dans une topologie en cascade, il suffit de créer des réseaux intercluster entre les clusters principal et secondaire, et entre les clusters secondaire et tertiaire. Il n'est pas nécessaire de créer un réseau intercluster entre le cluster principal et le cluster tertiaire.

> Il est possible (mais pas conseillé) à un administrateur de supprimer le service intercluster de la politique de service default-intercluster. Dans ce cas, les LIFs créées à l'aide de « Default-intercluster » ne seront en fait pas des LIFs intercluster. Pour vérifier que la politique de service par défaut-intercluster contient le service intercluster-core, utiliser la commande suivante :
>
> `network interface service-policy show -policy default-intercluster`
>
> Pour en savoir plus, `network interface service-policy show` consultez le "Référence de commande ONTAP".

Conditions préalables au peering ONTAP

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

> À partir de ONTAP 9.6, Cluster peering fournit par défaut la prise en charge du chiffrement TLS 1.2 AES-256 GCM pour la réplication des données. Les chiffrements de sécurité par défaut (« PSK-AES256-GCM-SHA384 ») sont requis pour que le chiffrement de cluster fonctionne même si le chiffrement est désactivé.
>
> À partir de ONTAP 9.11.1, les chiffrements de sécurité DHE-PSK sont disponibles par défaut.
>
> À partir de ONTAP 9.15.1, Cluster peering assure par défaut la prise en charge du chiffrement TLS 1.3 pour la réplication des données.

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 appartenir au broadcast domain qui contient les ports utilisés pour la communication intercluster.
- 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 vous permet de migrer vos réseaux de peering depuis IPv4 vers IPv6 en autorisant éventuellement la présence des deux protocoles simultanément 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 la communication 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

Depuis ONTAP 9.10.1, les politiques de pare-feu sont obsolètes et intégralement remplacées par les politiques de service de LIF. Pour plus d'informations, voir "Configuration des politiques de pare-feu pour les LIF".

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

- Trafic ICMP bidirectionnel
- Le trafic TCP initié bidirectionnel vers les adresses IP de toutes les LIFs intercluster sur les ports 11104 et 11105
- HTTPS bidirectionnel entre les LIFs intercluster

  Bien que HTTPS n'est pas requis lors de la configuration du peering de clusters à l'aide de l'interface de ligne de commande, HTTPS est requis plus tard si vous utilisez System Manager pour configurer la protection des données.

La valeur par défaut `intercluster` La politique de pare-feu 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.

Regroupement des clusters

Les clusters doivent répondre aux exigences suivantes :

- Un cluster ne peut pas se trouver dans une relation entre pairs et plus de 255 clusters.

Utilisez des ports ONTAP partagés ou dédiés

Vous pouvez utiliser des ports dédiés pour la communication intercluster ou partager les ports utilisés par le réseau de données. Lors de la décision de partager des ports, vous devez tenir compte de la bande passante du réseau, de l'intervalle de réplication et de la disponibilité des ports.

Vous pouvez partager les ports sur un cluster en utilisant des ports dédiés sur l'autre.

La bande passante du réseau

Si vous disposez d'un réseau haut débit (par exemple 10 GbE), vous disposez peut-être d'une bande passante LAN locale suffisante pour effectuer la réplication à l'aide des mêmes ports 10 GbE utilisés pour l'accès aux données.

Vous devriez même comparer votre bande passante WAN disponible à celle de votre réseau local. Si la bande passante WAN disponible est bien inférieure à 10 GbE, vous devrez peut-être utiliser des ports dédiés.

À l'exception de cette règle, on peut trouver lorsque tous les nœuds du cluster répliquent des données, auquel cas l'utilisation de la bande passante est généralement répartie entre ces nœuds.

Si vous n'utilisez pas de ports dédiés, la taille de l'unité de transmission maximale (MTU) du réseau de réplication doit généralement être identique à la taille de MTU du réseau de données.

Intervalle de réplication

Si la réplication se déroule en dehors des heures de pointe, vous devriez pouvoir utiliser des ports de données pour la réplication, même sans connexion LAN 10 GbE.

Si la réplication a lieu pendant les heures de bureau, vous devez tenir compte de la quantité de données à répliquer et de la quantité de bande passante nécessaire pour créer des conflits avec les protocoles de données. Si l'utilisation du réseau par les protocoles de données (SMB, NFS, iSCSI) est supérieure à 50 %, il est recommandé d'utiliser des ports dédiés pour la communication intercluster afin de permettre des performances non dégradées en cas de basculement du nœud.

Disponibilité du port

Si vous déterminez que le trafic de réplication interfère sur le trafic de données, vous pouvez migrer des LIFs intercluster vers n'importe quel autre port partagé intercluster sur le même nœud.

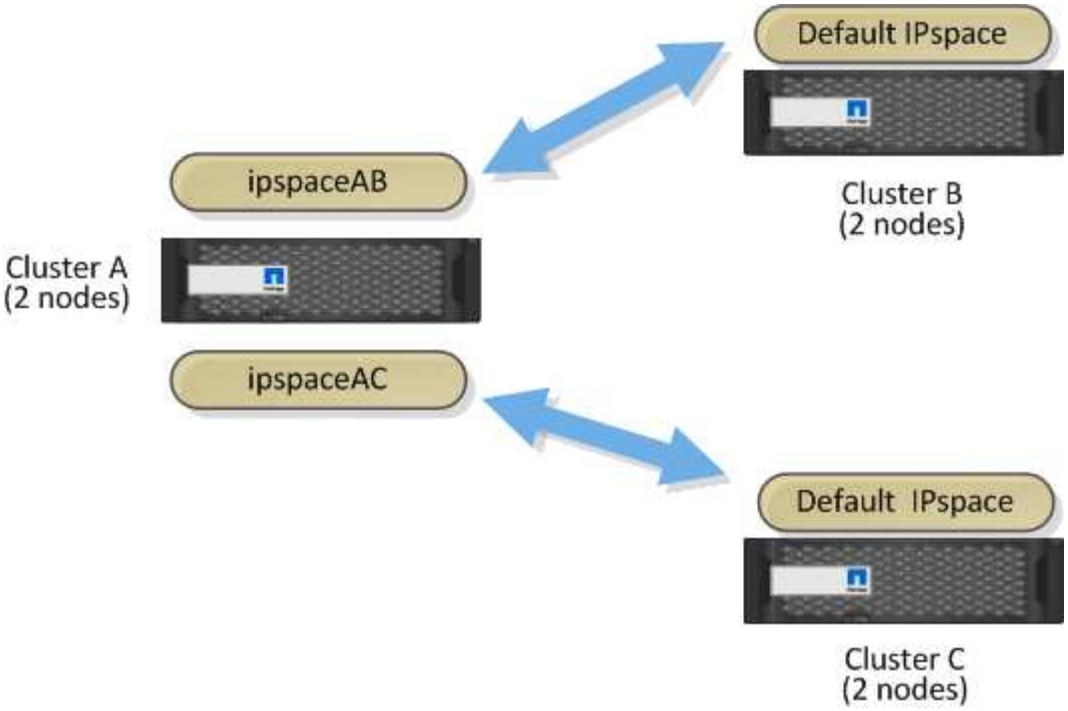
Vous pouvez également dédier des ports VLAN à la réplication. La bande passante du port est partagée entre tous les VLAN et le port de base.

Utilisez des IPspaces ONTAP personnalisés pour isoler le trafic de réplication

Vous pouvez utiliser des IPspaces personnalisés pour séparer les interactions d'un cluster avec ses pairs. Appelée *connectivité intercluster désignée*, cette configuration permet aux fournisseurs de services d'isoler le trafic de réplication dans des environnements mutualisés.

Supposons, par exemple, que vous souhaitez que le trafic de réplication entre le Cluster A et le Cluster B soit séparé du trafic de réplication entre le Cluster A et le Cluster C. Pour ce faire, vous pouvez créer deux IPspaces sur le Cluster A.

Un IPspace contient les LIF intercluster que vous utilisez pour communiquer avec le Cluster B. L'autre contient les LIFs intercluster que vous utilisez pour communiquer avec le Cluster C, comme indiqué sur l'illustration suivante.



Informations associées

- "En savoir plus sur la configuration ONTAP IPspace"

Informations sur le copyright

Copyright © 2026 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.