Configuration des prérequis

NetApp Solutions

NetApp
April 25, 2024

Sommaire

Configuration des prérequis

Certaines conditions préalables doivent être configurées à la fois sur site et dans le cloud avant d'exécuter des workloads de base de données de cloud hybride. La section suivante fournit un résumé de ce processus de haut niveau et les liens suivants fournissent des informations supplémentaires sur la configuration du système nécessaire.

Sur site

- Installation et configuration de SnapCenter
- Configuration du stockage du serveur de bases de données sur site
- Licences requises
- Mise en réseau et sécurité
- Automatisation

Cloud public

- Identifiant NetApp Cloud Central
- Accès au réseau à partir d'un navigateur Web vers plusieurs noeuds finaux
- Emplacement réseau d'un connecteur
- Les autorisations du fournisseur cloud
- Mise en réseau pour des services individuels

Remarques importantes :

1. Où déployer Cloud Manager Connector ?
2. Architecture et dimensionnement de Cloud volumes ONTAP
3. Un seul nœud ou une haute disponibilité ?

Vous trouverez des informations supplémentaires sur les liens suivants :

"Sur site"

"Cloud public"

Conditions préalables sur site

Pour préparer l'environnement de workload de base de données de cloud hybride SnapCenter, les tâches suivantes doivent être réalisées sur site.

Installation et configuration de SnapCenter

L'outil NetApp SnapCenter est une application Windows qui s'exécute généralement dans un environnement de domaine Windows, mais aussi dans un déploiement de groupe de travail. Elle est basée sur une architecture multiniveaux, incluant un serveur de gestion centralisée (le serveur SnapCenter) et un plug-in SnapCenter sur les hôtes du serveur de base de données pour les charges de travail de la base de données.

Voici quelques éléments à prendre en compte pour le déploiement du cloud hybride.

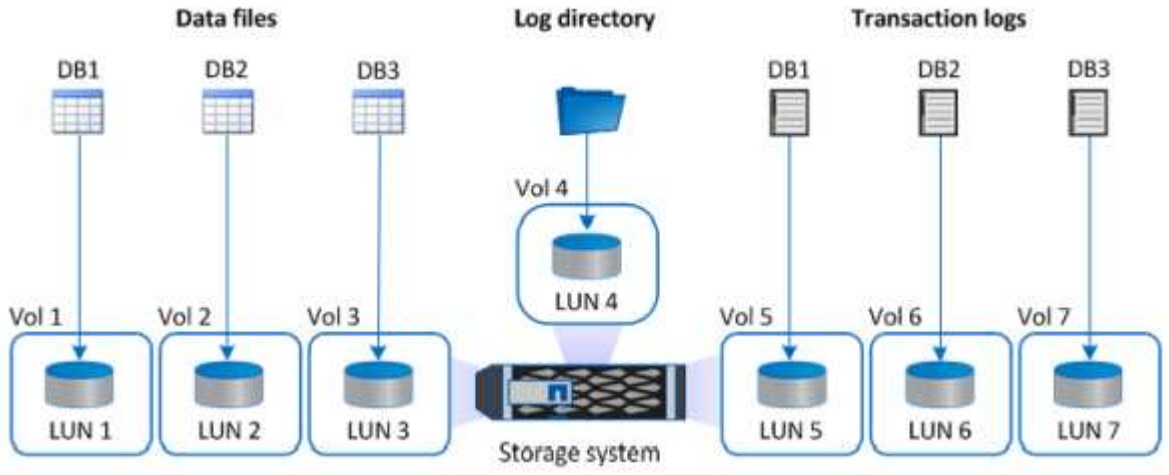
- **Déploiement d'instance unique ou de haute disponibilité.** le déploiement de haute disponibilité fournit une redondance en cas de défaillance d'un serveur d'instance SnapCenter unique.
- **Résolution du nom.** le DNS doit être configuré sur le serveur SnapCenter pour résoudre tous les hôtes de base de données ainsi que sur le SVM de stockage pour la recherche avant et arrière. Le serveur DNS doit également être configuré sur des serveurs de base de données pour résoudre le serveur SnapCenter et la SVM de stockage pour la recherche avant et arrière.
- **Configuration du contrôle d'accès basé sur les rôles (RBAC).** pour les charges de travail de bases de données mixtes, vous pouvez utiliser RBAC pour isoler la responsabilité de gestion de différentes plates-formes de bases de données telles qu'une base de données admin pour Oracle ou un administrateur pour SQL Server. Les autorisations nécessaires doivent être accordées à l'utilisateur DB admin.
- **Activer la stratégie de sauvegarde basée sur des stratégies.** pour renforcer la cohérence et la fiabilité des sauvegardes.
- **Ouvrez les ports réseau nécessaires sur le pare-feu.** pour que le serveur SnapCenter sur site communique avec les agents installés sur l'hôte DB cloud.
- **Les ports doivent être ouverts pour permettre le trafic SnapMirror entre le cloud sur site et le cloud public.** le serveur SnapCenter utilise ONTAP SnapMirror pour répliquer les sauvegardes Snapshot sur site vers les SVM de stockage Cloud volumes ONTAP.

Après avoir soigneusement étudié et planifié la pré-installation, cliquez sur ce bouton "Workflow d'installation de SnapCenter" Pour plus d'informations sur l'installation et la configuration de SnapCenter.

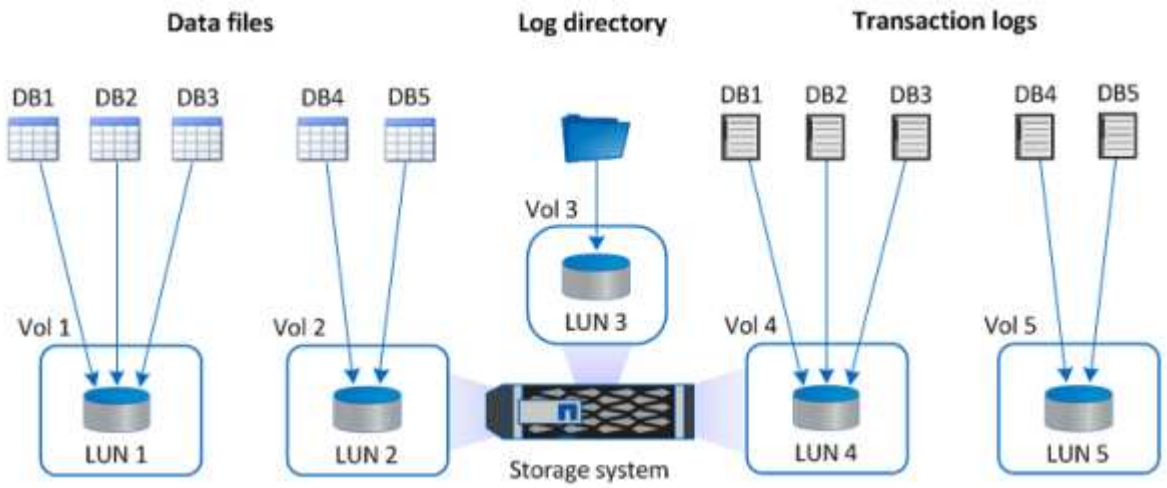
Configuration du stockage du serveur de bases de données sur site

Les performances du stockage jouent un rôle important dans les performances globales des bases de données et des applications. Une disposition de stockage bien conçue peut non seulement améliorer les performances de la base de données, mais aussi faciliter la gestion de la sauvegarde et de la restauration de la base de données. Plusieurs facteurs doivent être pris en compte lors de la définition de l'organisation du stockage, notamment la taille de la base de données, le taux de modification attendu des données pour la base de données et la fréquence avec laquelle vous effectuez des sauvegardes.

En reliant directement des LUN de stockage à la machine virtuelle invitée par NFS ou iSCSI pour les charges de travail de bases de données virtualisées, vous bénéficiez généralement de performances supérieures à celles du stockage alloué via VMDK. NetApp recommande l'organisation de stockage d'une importante base de données SQL Server sur les LUN décrits dans la figure suivante.



La figure suivante présente l'organisation de stockage recommandée par NetApp pour les bases de données SQL Server de petite ou moyenne taille sur des LUN.



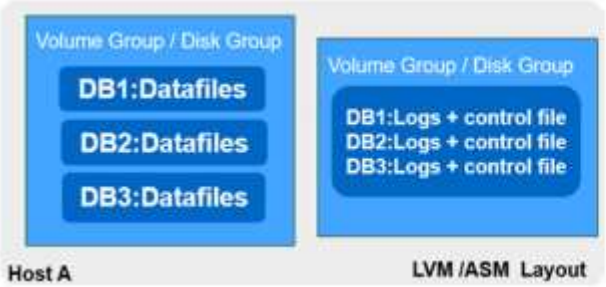
Le répertoire des journaux est dédié à SnapCenter pour effectuer une synthèse du journal des transactions pour la récupération de la base de données. Pour une base de données très volumineuse, plusieurs LUN peuvent être allouées à un volume pour améliorer les performances.

Pour les charges de travail de bases de données Oracle, SnapCenter prend en charge les environnements de bases de données bénéficiant d'un stockage ONTAP monté sur l'hôte en tant que périphériques physiques ou virtuels. Vous pouvez héberger toute la base de données sur un ou plusieurs périphériques de stockage en fonction du caractère stratégique de l'environnement. Généralement, les clients isolent les fichiers de données sur un système de stockage dédié de tous les autres fichiers comme les fichiers de contrôle, les fichiers de reprise et les fichiers journaux d'archivage. Cela permet aux administrateurs de restaurer rapidement (ONTAP Single-File SnapRestore) ou de cloner une grande base de données stratégique (de plusieurs pétaoctets) à l'aide de la technologie Snapshot en quelques secondes à quelques minutes.

Pour optimiser la latence, un volume de stockage dédié doit être déployé sur différents types de fichiers Oracle afin d'optimiser la latence. Pour une grande base de données, plusieurs LUN (NetApp recommande jusqu'à huit) par volume doivent être alloués aux fichiers de données.

Pour les bases de données Oracle plus petites, SnapCenter prend en charge les dispositions de stockage partagé dans lesquelles vous pouvez héberger plusieurs bases de données ou faire partie d'une base de

données sur le même volume de stockage ou LUN. Par exemple, vous pouvez héberger des fichiers de données pour toutes les bases de données d'un groupe de disques + DATA ASM ou d'un groupe de volumes. Le reste des fichiers (fichiers de reprise, journaux d'archivage et fichiers de contrôle) peut être hébergé sur un autre groupe de disques ou groupe de volumes dédié (LVM). Un tel scénario de déploiement est illustré ci-dessous.



Pour faciliter la relocalisation des bases de données Oracle, le binaire Oracle doit être installé sur un LUN distinct inclus dans la stratégie de sauvegarde régulière. Cela permet de garantir que, dans le cas du transfert de la base de données vers un nouvel hôte serveur, la pile Oracle peut être démarrée pour la restauration sans problèmes potentiels dus à un binaire Oracle désynchronisé.

Licences requises

SnapCenter est un logiciel sous licence de NetApp. Elle est généralement incluse dans une licence ONTAP sur site. Cependant, pour le déploiement d'un cloud hybride, une licence cloud pour SnapCenter doit également ajouter CVO à SnapCenter comme destination de réplication des données cible. Veuillez consulter les liens ci-dessous pour en savoir plus sur la licence standard basée sur la capacité SnapCenter :

"Licences standard basées sur la capacité SnapCenter"

Mise en réseau et sécurité

Dans le cas d'une base de données de production sur site nécessitant une stabilité accrue dans le cloud pour les opérations de développement/test et de reprise d'activité, la mise en réseau et la sécurité sont des facteurs essentiels à prendre en compte lors de la configuration de l'environnement et de la connexion au cloud public à partir d'un data Center sur site.

Les clouds publics utilisent généralement un cloud privé virtuel (VPC) pour isoler différents utilisateurs au sein d'une plateforme de cloud public. Au sein d'un VPC individuel, la sécurité est contrôlée à l'aide de mesures telles que des groupes de sécurité configurables en fonction des besoins des utilisateurs pour le verrouillage d'un VPC.

La connectivité entre le data Center sur site et le VPC peut être sécurisée via un tunnel VPN. Sur la passerelle VPN, la sécurité peut être renforcée à l'aide de règles NAT et de pare-feu qui bloquent les tentatives d'établissement de connexions réseau à partir d'hôtes sur Internet vers des hôtes à l'intérieur du data Center de l'entreprise.

Pour les considérations relatives au réseau et à la sécurité, consultez les règles Cloud volumes ONTAP entrantes et sortantes pour votre cloud public :

- "Règles du groupe de sécurité pour CVO - AWS"
- "Règles du groupe de sécurité pour CVO - Azure"
- "Règles de pare-feu pour CVO - GCP"

Utilisation de l'automatisation Ansible pour la synchronisation facultative des instances de BDD entre l'environnement sur site et le cloud

Pour simplifier la gestion d'un environnement de base de données de cloud hybride, NetApp vous recommande vivement, mais ne vous demande pas de déployer un contrôleur Ansible afin d'automatiser certaines tâches de gestion, comme le maintien des instances de calcul sur site et dans le cloud en mode synchrone. Cela est particulièrement important, car une instance de calcul désynchronisée dans le cloud peut entraîner l'erreur de la base de données récupérée dans le cloud en raison de l'absence de packages du noyau et d'autres problèmes.

La fonctionnalité d'automatisation d'un contrôleur Ansible peut également être utilisée pour étendre SnapCenter à certaines tâches, comme l'interruption de l'instance SnapMirror pour activer la copie de données de reprise après incident en production.

Suivez ces instructions pour configurer votre nœud de contrôle Ansible pour les machines RedHat ou CentOS : "Configuration du contrôleur Red Hat/CentOS Ansible". Suivez ces instructions pour configurer votre nœud de contrôle Ansible pour les machines Ubuntu ou Debian : "Configuration du contrôleur Ansible Ubuntu/Debian".

Conditions préalables au cloud public

Avant d'installer Cloud Manager Connector et Cloud Volumes ONTAP et de configurer SnapMirror, nous devons préparer notre environnement cloud. Cette page décrit le travail à effectuer, ainsi que les considérations relatives au déploiement de Cloud Volumes ONTAP.

Liste de contrôle des conditions préalables au déploiement de Cloud Manager et de Cloud Volumes ONTAP

- Identifiant NetApp Cloud Central
- Accès au réseau à partir d'un navigateur Web vers plusieurs noeuds finaux
- Emplacement réseau d'un connecteur
- Les autorisations du fournisseur cloud
- Mise en réseau pour des services individuels

Pour en savoir plus sur ce dont vous avez besoin pour démarrer, consultez le site "documentation cloud".

Considérations

1. Qu'est-ce qu'un connecteur Cloud Manager ?

Dans la plupart des cas, un administrateur de compte Cloud Central doit déployer un connecteur dans votre réseau cloud ou sur site. Ce connecteur permet à Cloud Manager de gérer les ressources et les processus au sein de votre environnement de cloud public.

Pour plus d'informations sur les connecteurs, visitez notre "documentation cloud".

2. Dimensionnement et architecture de Cloud Volumes ONTAP

Lors du déploiement de Cloud Volumes ONTAP, vous avez le choix entre un package prédéfini ou la création

de votre propre configuration. Bon nombre de ces valeurs peuvent être modifiées ultérieurement, sans interrompre l'activité, mais certaines décisions clés doivent être prises avant le déploiement, en fonction des charges de travail à déployer dans le cloud.

Chaque fournisseur de cloud propose différentes options de déploiement et chaque workload dispose de ses propres propriétés. NetApp a une "Outil de dimensionnement CVO" cela peut aider à dimensionner correctement les déploiements en fonction de la capacité et des performances, mais il a été conçu autour de certains concepts de base qui méritent d'être pris en compte :

- Capacité requise
- Capacité réseau de la machine virtuelle du cloud
- Les caractéristiques de performances du stockage cloud

L'essentiel est de planifier une configuration qui non seulement répond aux besoins actuels en termes de capacité et de performances, mais qui étudie également la croissance future. Ce chiffre est généralement appelé marge de capacité et marge de performance.

Si vous souhaitez des informations complémentaires, lisez la documentation sur la planification correcte "AWS", "Azure", et "GCP".

3. Un seul nœud ou haute disponibilité ?

Dans tous les clouds, il est possible de déployer Cloud volumes ONTAP dans un seul nœud ou dans une paire haute disponibilité en cluster avec deux nœuds. Selon le cas de figure, vous pouvez déployer un nœud unique pour réduire les coûts ou une paire haute disponibilité pour améliorer la disponibilité et la redondance.

Pour une reprise après incident ou l'exécution de systèmes de stockage temporaires pour le développement et le test, des nœuds uniques sont courants, car l'impact d'une panne d'infrastructure soudaine ou d'un zone est moindre. Toutefois, pour toutes les utilisations de production, et lorsque les données ne se trouvent que dans un seul emplacement ou que le dataset doit avoir plus de redondance et de disponibilité, la haute disponibilité est recommandée.

Pour plus d'informations sur l'architecture de la version haute disponibilité de chaque Cloud, consultez la documentation pour "AWS", "Azure" et "GCP".