Konfiguration der Voraussetzungen

NetApp Solutions

NetApp
January 30, 2025

Inhalt

Konfiguration der Voraussetzungen

Konfiguration der Voraussetzungen

Bestimmte Voraussetzungen müssen sowohl On-Premises als auch in der Cloud konfiguriert werden, bevor die Ausführung von Hybrid-Cloud-Datenbank-Workloads ausgeführt wird. Der folgende Abschnitt bietet einen allgemeinen Überblick über diesen Prozess und die folgenden Links führen zu weiteren Informationen über die erforderliche Systemkonfiguration.

On-Premises

- Installation und Konfiguration von SnapCenter
- Storage-Konfiguration des lokalen Datenbankservers
- Lizenzierungsanforderungen
- Networking und Sicherheit
- Automatisierung

Public Cloud

- NetApp Cloud Central Anmeldung
- Netzwerkzugriff über einen Webbrowser zu mehreren Endpunkten
- Ein Netzwerkspeicherort für einen Anschluss
- Berechtigungen für Cloud-Provider
- Vernetzung für einzelne Services

Wichtige Überlegungen:

1. Wo wird der Cloud Manager Connector bereitgestellt?
2. Sizing und Architektur für Cloud Volume ONTAP
3. Single Node oder Hochverfügbarkeit?

Die folgenden Links bieten weitere Einzelheiten:

"On-Premises"

"Public Cloud"

Voraussetzungen vor Ort

Die folgenden Aufgaben müssen vor Ort ausgeführt werden, um die SnapCenter Hybrid-Cloud-Datenbank-Workload-Umgebung vorzubereiten.

Installation und Konfiguration von SnapCenter

Das NetApp SnapCenter Tool ist eine auf Windows basierende Applikation, die normalerweise in einer Windows Domain-Umgebung ausgeführt wird, obwohl auch eine Implementierung von Arbeitsgruppen möglich ist. Sie basiert auf einer Multi-Tier-Architektur, die einen zentralen Management-Server (den SnapCenter Server) sowie ein SnapCenter-Plug-in auf den Datenbank-Server-Hosts für Datenbank-Workloads umfasst. Folgende wichtige Aspekte sollten bei der Implementierung der Hybrid Cloud beachtet werden:

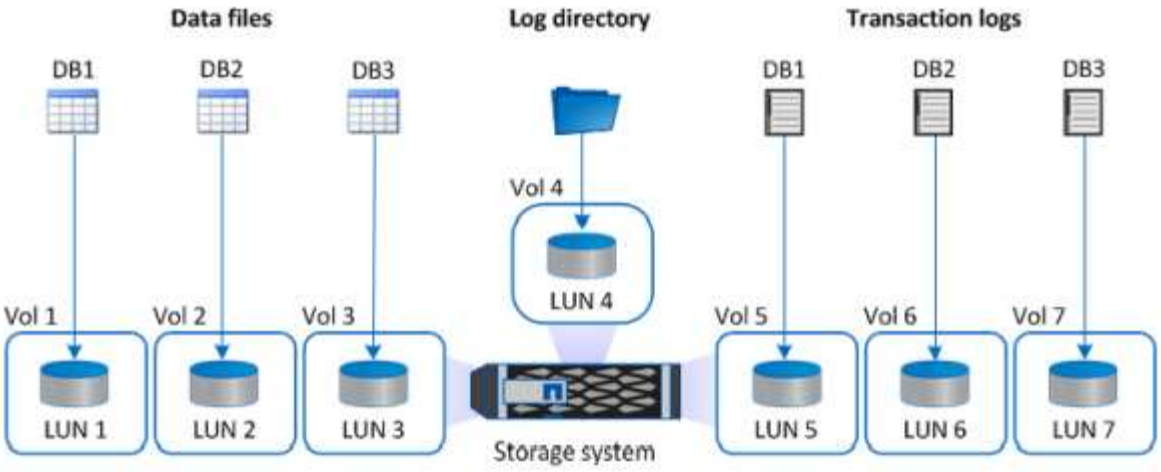
- **Single Instance oder HA-Bereitstellung.** HA-Bereitstellung bietet Redundanz bei Ausfall eines SnapCenter-Instanz-Servers.
- **Namensauflösung.** DNS muss auf dem SnapCenter-Server konfiguriert sein, um alle Datenbank-Hosts sowie auf der Speicher-SVM aufzulösen, damit die Suche vorwärts und rückwärts ausgeführt werden kann. DNS muss auch auf Datenbankservern konfiguriert werden, um den SnapCenter-Server und die Storage-SVM für die vorwärts und rückwärts Suche zu lösen.
- **Rollenbasierte Zugriffssteuerung (Role-Based Access Control, RBAC)-Konfiguration.** für gemischte Datenbank-Workloads sollten Sie die RBAC verwenden, um die Management-Verantwortung für verschiedene DB-Plattformen zu verteilen, z. B. einen Administrator für Oracle Database oder einen Administrator für SQL Server. Für den DB-Admin-Benutzer müssen die erforderlichen Berechtigungen erteilt werden.
- **Ermöglicht eine richtlinienbasierte Backup-Strategie.** zur Durchsetzung der Backup-Konsistenz und -Zuverlässigkeit.
- **Öffnen Sie erforderliche Netzwerkanschlüsse an der Firewall.** damit der On-Premise SnapCenter Server mit Agenten kommunizieren kann, die im Cloud DB-Host installiert sind.
- **Die Ports müssen offen sein, um SnapMirror Traffic zwischen On-Premises und Public Cloud zu ermöglichen.** der SnapCenter Server nutzt ONTAP SnapMirror zur Replizierung von Snapshot Backups vor Ort in Cloud-CVO Storage-SVMs.

Klicken Sie nach sorgfältiger Planung und Prüfung vor der Installation auf diese Schaltfläche "SnapCenter Installations-Workflow" Einzelheiten zur Installation und Konfiguration von SnapCenter finden Sie im Dokument.

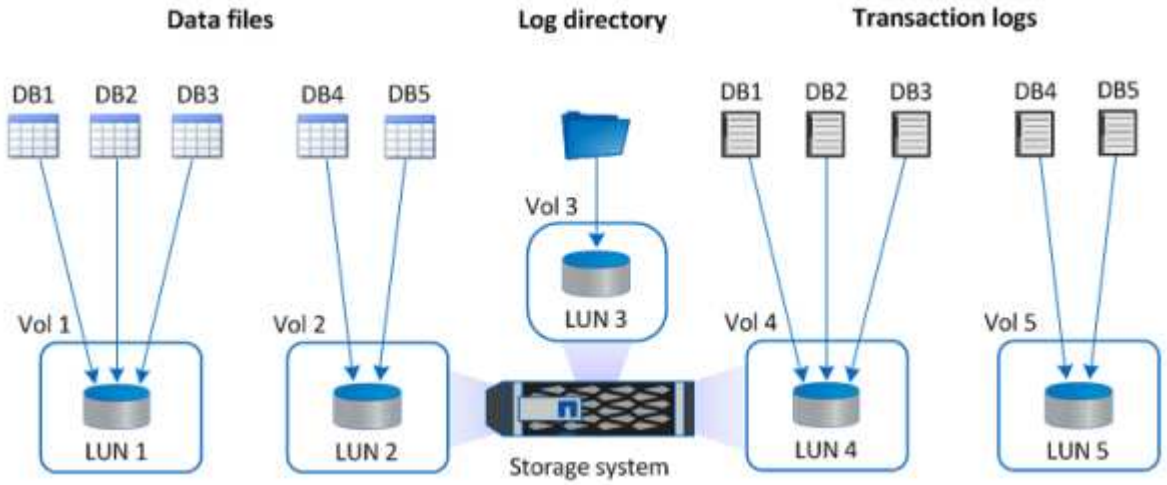
Storage-Konfiguration des lokalen Datenbankservers

Die Storage-Performance spielt für die Gesamt-Performance von Datenbanken und Applikationen eine wichtige Rolle. Mit einem gut durchdachten Storage-Layout kann nicht nur die Datenbank-Performance verbessert werden, sondern auch das Management von Datenbank-Backup und -Recovery vereinfacht wird. Bei der Definition des Storage-Layouts sind mehrere Faktoren zu berücksichtigen. Dazu gehören die Größe der Datenbank, die erwartete Datenänderung der Datenbank und die Häufigkeit der Backups.

Das direkte Anbinden von Storage-LUNs an die Gast-VM entweder über NFS oder iSCSI für virtualisierte Datenbank-Workloads liefert im Allgemeinen eine bessere Performance als über VMDK zugewiesener Storage. NetApp empfiehlt das Storage-Layout für eine große SQL Server Datenbank auf LUNs, die in der folgenden Abbildung dargestellt sind.



Die folgende Abbildung zeigt das von NetApp empfohlene Storage-Layout für kleine oder mittlere SQL Server-Datenbank auf LUNs.



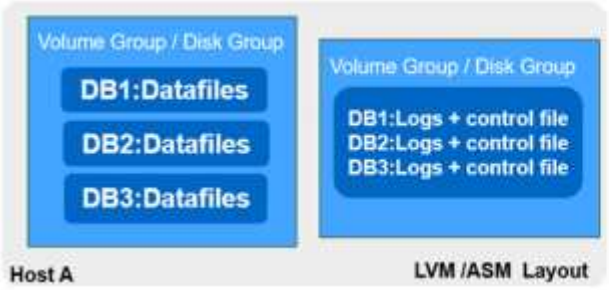
Das Log-Verzeichnis ist SnapCenter dediziert, um Transaktions-Log-Rollup für Datenbank-Recovery durchzuführen. Für eine besonders große Datenbank können einem Volume mehrere LUNs zugewiesen werden, um eine bessere Performance zu erzielen.

Bei Oracle-Datenbank-Workloads unterstützt SnapCenter Datenbankumgebungen, die über ONTAP Storage gesichert sind, die als physische oder virtuelle Geräte auf dem Host gemountet werden. Je nach Wichtigkeit der Umgebung können Sie die gesamte Datenbank auf einem einzigen oder mehreren Storage-Geräten hosten. In der Regel isolieren Kunden Datendateien im dedizierten Storage von allen anderen Dateien, z. B. Kontrolldateien, Wiederherstellungsdateien und Archivprotokolldateien. So sind Administratoren in ONTAP der Lage, in wenigen Sekunden oder Minuten eine große kritische Datenbank (Petabyte-Größe) mit Snapshot Technologie wiederherzustellen (Single-File SnapRestore) oder zu klonen.

Für geschäftskritische Workloads, die von der Latenz abhängig sind, sollte ein dediziertes Storage Volume auf verschiedene Arten von Oracle Dateien implementiert werden, um die bestmögliche Latenz zu erzielen. Bei einer großen Datenbank sollten mehrere LUNs (NetApp empfiehlt bis zu acht) pro Volume Datendateien

zugewiesen werden.

Bei kleineren Oracle Datenbanken unterstützt SnapCenter Shared-Storage-Layouts, in denen mehrere Datenbanken oder Teile einer Datenbank auf demselben Storage-Volume oder derselben LUN gehostet werden können. Als Beispiel für dieses Layout können Sie Datendateien für alle Datenbanken auf einer +DATA ASM Laufwerksgruppe oder einer Volume-Gruppe hosten. Der Rest der Dateien (Redo-, Archivprotokoll- und Kontrolldateien) kann auf einer anderen dedizierten Laufwerksgruppe oder Volume-Gruppe (LVM) gehostet werden. Ein solches Implementierungsszenario wird im Folgenden dargestellt.



Um die Verschiebung von Oracle Datenbanken zu erleichtern, sollte Oracle-Binärdatei auf einer separaten LUN installiert werden, die in der regelmäßigen Backup-Richtlinie enthalten ist. So wird sichergestellt, dass bei der Datenbankverschiebung zu einem neuen Serverhost der Oracle Stack für eine Recovery ohne potenzielle Probleme aufgrund einer aus der Synchronisierung bestehenden Oracle-Binärdatei gestartet werden kann.

Lizenzierungsanforderungen

SnapCenter ist eine lizenzierte Software von NetApp. Sie ist im Allgemeinen in einer ONTAP Lizenz vor Ort enthalten. Bei der Hybrid-Cloud-Implementierung ist jedoch auch eine Cloud-Lizenz für SnapCenter erforderlich, um CVO zu SnapCenter als Ziel-Datenreplizierungsziel zu hinzufügen. Weitere Informationen erhalten Sie unter folgenden Links zu der kapazitätsbasierten SnapCenter Standardlizenz:

"SnapCenter-Standard-kapazitätsbasierte Lizenzen"

Networking und Sicherheit

Wenn ein hybrider Datenbankbetrieb eine lokale Produktionsdatenbank benötigt, die nicht stabil in der Cloud für Entwicklung/Test und Disaster Recovery ist, müssen Netzwerke und Sicherheit beim Einrichten der Umgebung sowie die Verbindung zur Public Cloud aus einem lokalen Datacenter berücksichtigt werden.

Public Clouds verwenden in der Regel eine Virtual Private Cloud (VPC), um verschiedene Benutzer innerhalb einer Public-Cloud-Plattform zu isolieren. Innerhalb eines individuellen VPC wird die Sicherheit mithilfe von Maßnahmen wie Sicherheitsgruppen gesteuert, die je nach Benutzeranforderungen für die Sperrung eines VPC konfiguriert werden können.

Die Konnektivität vom lokalen Datacenter zur VPC kann über einen VPN-Tunnel gesichert werden. Auf dem VPN-Gateway kann die Sicherheit durch NAT- und Firewall-Regeln, die Versuche blockieren, Netzwerkverbindungen von Hosts im Internet zu Hosts im unternehmenseigenen Rechenzentrum herzustellen, abgehärtet werden.

Networking- und Sicherheitsaspekte finden Sie in den relevanten ein- und ausgehenden CVO-Regeln für die beliebige Public Cloud:

- "Regeln für Sicherheitsgruppen für CVO – AWS"
- "Regeln für Sicherheitsgruppen für CVO – Azure"
- "Firewall-Regeln für CVO - GCP"

Nutzung von Ansible-Automatisierung zur Synchronisierung von DB-Instanzen zwischen On-Premises und der Cloud – optional

Um das Management einer Hybrid-Cloud-Datenbankumgebung zu vereinfachen, empfiehlt NetApp unbedingt den Einsatz eines Ansible-Controllers, um einige Managementaufgaben zu automatisieren, z. B. um Computing-Instanzen lokal und in der Cloud synchron zu halten. Dies ist besonders wichtig, da eine Out-of-Sync-Computing-Instanz in der Cloud die wiederhergestellte Datenbank im Cloud-Fehler aufgrund fehlender Kernel-Pakete und anderer Probleme anfällig machen könnte.

Mit den Automatisierungsfunktionen eines Ansible-Controllers lässt sich SnapCenter für bestimmte Aufgaben erweitern, beispielsweise durch Aufbrechen der SnapMirror Instanz zur Aktivierung der DR-Datenkopie für die Produktion.

Befolgen Sie diese Anweisungen, um Ihren Ansible-Steuerungsknoten für RedHat- oder CentOS-Maschinen einzurichten: Einschließlich:_include/Automation_RHEL_centos_Setup.adoc[]

Befolgen Sie diese Anweisung, um Ihren Ansible-Steuerungsknoten für Ubuntu- oder Debian-Maschinen einzurichten: Include:_include/Automation_ubuntu_debian_Setup.adoc[]

Voraussetzungen für die Public Cloud

Bevor wir den Cloud Manager Connector installieren und Cloud Volumes ONTAP konfigurieren und SnapMirror konfigurieren, müssen wir einige Vorbereitungen für unsere Cloud-Umgebung durchführen. Auf dieser Seite werden die erforderlichen Arbeiten sowie die Überlegungen bei der Implementierung von Cloud Volumes ONTAP beschrieben.

Checkliste zu den Implementierungsvoraussetzungen für Cloud Manager und Cloud Volumes ONTAP

- NetApp Cloud Central Anmeldung
- Netzwerkzugriff über einen Webbrowser zu mehreren Endpunkten
- Ein Netzwerkstandort für einen Konnektor
- Berechtigungen für Cloud-Provider
- Vernetzung für einzelne Services

Weitere Informationen zu den ersten Schritten erhalten Sie auf unserer "Cloud-Dokumentation".

Überlegungen

1. Was ist ein Cloud-Manager-Konnektor?

In den meisten Fällen muss ein Cloud Central Account-Administrator einen Connector in Ihrer Cloud oder Ihrem On-Premises-Netzwerk bereitstellen. Über den Connector kann Cloud Manager Ressourcen und Prozesse in Ihrer Public-Cloud-Umgebung managen.

Weitere Informationen zu Connectors finden Sie auf unserer "Cloud-Dokumentation".

2. Dimensionierung und Architektur von Cloud Volumes ONTAP

Bei der Bereitstellung von Cloud Volumes ONTAP haben Sie die Wahl zwischen einem vordefinierten Paket oder der Erstellung Ihrer eigenen Konfiguration. Obwohl sich viele dieser Werte später unterbrechungsfrei ändern lassen, müssen vor der Implementierung auf der Grundlage der zu implementierenden Workloads in der Cloud einige wichtige Entscheidungen getroffen werden.

Jeder Cloud-Provider verfügt über unterschiedliche Implementierungsmöglichkeiten, und fast jeder Workload verfügt über eigene einzigartige Eigenschaften. NetApp hat eine "CVO-Sizing-Tool" Damit können Implementierungen auf der Basis von Kapazität und Performance korrekt ausgerichtet werden. Allerdings basieren sie auf einigen grundlegenden Konzepten, die sich lohnen:

- Erforderliche Kapazität
- Netzwerkfähigkeit der Cloud Virtual Machine
- Performance-Merkmale von Cloud-Storage

Entscheidend ist dabei die Planung einer Konfiguration, die nicht nur die aktuellen Kapazitäts- und Performance-Anforderungen erfüllt, sondern auch das künftige Wachstum berücksichtigt. Dies wird im Allgemeinen als Kapazitätsreserve und Performance Reserve bezeichnet.

Wenn Sie weitere Informationen wünschen, lesen Sie die Dokumentation zur Planung richtig für "AWS", "Azure", und "GCP".

3. Single Node oder Hochverfügbarkeit?

In allen Clouds besteht die Möglichkeit, CVO entweder in einem einzelnen Node oder in einem hochverfügbaren Cluster-Paar mit zwei Nodes zu implementieren. Je nach Anwendungsfall können Sie einen einzelnen Node implementieren, um Kosten zu sparen, oder ein HA-Paar, um weitere Verfügbarkeit und Redundanz zu ermöglichen.

Einzelne Nodes sind für einen DR-Anwendungsfall oder das Aufsetzen von temporem Storage für Entwicklung und Tests häufig vorgängig, da die Auswirkungen eines plötzlichen zonalen beziehungsweise Infrastrukturausfalls geringer sind. Wenn sich die Daten jedoch in einem Produktionsfall nur an einem einzelnen Standort befinden oder wenn der Datensatz mehr Redundanz und Verfügbarkeit haben muss, wird Hochverfügbarkeit empfohlen.

Weitere Informationen zur Architektur der Hochverfügbarkeit der einzelnen Cloud-Versionen finden Sie in der Dokumentation für "AWS", "Azure" Und "GCP".