

Abbildung 3.1: Schematische Darstellung eines Failover Cluster

Die Verbindung zu Clients wie Applikationsserver erfolgt über das Public Network. Dieses bildet die Netzwerkschnittstelle zur Außenwelt. Auch hier sollten pro Rechner mindestens zwei Netzwerkkarten zum Einsatz kommen, um einen SPOF zu vermeiden. Diese werden in das Unternehmensnetz eingebunden und erlauben den Zugriff auf den Failover Cluster von außen.

Cold Standby-Systeme benötigen einen gesonderten Cluster Layer, der nicht von Oracle geliefert, sondern von Drittanbietern eingekauft werden muss. So bietet Sun den Sun Cluster für Solaris. Unter AIX kann HACMP, für HP/UX der HP MC/ServiceGuard eingesetzt werden. Veritas bietet den Veritas Cluster für verschiedene Plattformen wie Sun Solaris, HP/UX und Linux an.

Notwendige Komponenten eines Cold Standby-Systems sind:

- ▶ zwei Server mit mindestens je zwei Private und zwei Public Network Interfaces
- ▶ an beide Server angeschlossener Storage (externes SCSI, SAN, iSCSI, NAS)
- ▶ Cluster Management-Software wie Sun Cluster, Veritas Cluster, HACMP oder ServiceGuard

Für Planung und Implementierung sind neben Datenbank und Netzwerk-Know-how auch Kenntnisse der Cluster Management-Software nötig. Die Oracle-Datenbank selbst wird ähnlich aufgesetzt wie ein normales Single Instance-System und anschließend über Ressourcengruppen in den Cluster eingebunden.

Vorteile eines Oracle Failover Cluster:

- ▶ Übernahme der Funktionalität bei Ausfall eines Servers ohne administrativen Eingriff

Nachteile eines Oracle Failover Cluster:

- ▶ erhöhter Zeitaufwand (im Vergleich zu Warm und Hot Standby) für Wiederanlauf
- ▶ bei Ausfall eines Rechenzentrums (z.B. durch einen Brand) fällt der gesamte Cluster aus
- ▶ redundante Hardware kann im Normalbetrieb nicht genutzt werden

Oracle Standby-Datenbanken (Warm Standby)

Auch in einem Warm Standby-System sind die Server redundant ausgelegt. Anders als beim Cold Standby ist hier jedoch der zweite Rechner bereits betriebsbereit und kann daher bei einem Ausfall des Primärserver die Funktionalität schneller übernehmen. Typische Vertreter im Oracle-Umfeld sind replizierte und Standby-Datenbanken.

In einer Standby-Datenbank wird eine transaktionskonsistente Kopie der Primärdatenbank auf einem zweiten vollständigen System gehalten. Primär- und Standby System haben dabei in der Regel ihren eigenen privaten Storage. Es gibt Ausnahmen hierzu, die in Kapitel 5 »Standby-Datenbanken und Data Guard« behandelt werden.

Initial wird die Primärdatenbank einmalig über ein Backup auf das Standby-System übertragen. Anschließend werden alle Transaktionen des Primärsystems auf das Standby-System repliziert. Die Replikation kann in Echtzeit oder auch zeitverzögert erfolgen.

Zeitverzögerte Verarbeitung wird häufig zum Abfangen von Benutzerfehlern eingesetzt. Wird in einer Standby-Datenbank eine Zeitverzögerung von 30 Minuten implementiert, so werden auch Benutzerfehler erst nach diesem Zeitraum appliziert. Fällt das Primärsystem aus, so müssen die Transaktionen der letzten 30 Minuten auf dem Standby-System nachgefahren werden, bevor dieses die Betriebsfähigkeit wiederherstellen kann.

Ab Oracle 10g ist es nicht mehr notwendig, ein solches Delay einzusetzen, um Benutzerfehler abfangen zu können. Vielmehr kann hier die Oracle Flashback-Technologie eingesetzt werden (siehe auch Kapitel 3.1.2 »Oracle und Online-Technologien«). Diese erlaubt ein vorübergehendes Zurücksetzen einer Datenbank in einen früheren konsistenten Zustand. Flashback lässt sich auch auf einer Standby-Datenbank ausführen, um von hier aus die Daten über einen Datenbank-Link zurück zur Primärdatenbank zu übertragen. Abschließend kann die Standby-Datenbank durch Wiederholung aller Transaktionen des Primärsystems wieder auf den aktuellen Zustand der Primärdatenbank vorgerollt werden.

Standby-Datenbanken können weiterhin als Disaster Recovery-Strategie eingesetzt werden. Man kann Standby-Datenbanken lokal oder auch in entfernten Rechenzentren betreiben. Beides lässt sich auch innerhalb einer Standby-Konfiguration miteinander verbinden: Eine Standby-Datenbank kann beispielsweise lokal, eine

zweite entfernt betrieben werden. Dabei sind sehr große Distanzen – auch über Kontinente hinweg – möglich. Bei Ausfall eines der Rechenzentren kann der Betrieb weiterhin aufrechterhalten werden.

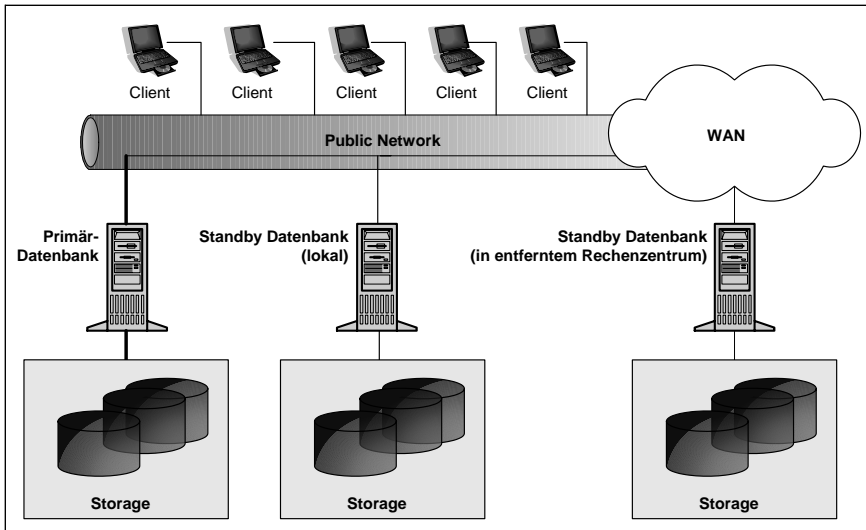


Abbildung 3.2: Schematische Darstellung einer Konfiguration mit Standby-Datenbanken

Es ist möglich, bis zu neun Standby-Datenbanken an einer Primärdatenbank zu betreiben. So bietet es sich in manchen Umgebungen an, zwei Standby-Datenbanken zu verwenden. Dies gilt insbesondere bei Verwendung spezieller Protection Modes, die garantieren, dass kein Datenverlust entsteht.

Komponenten für den Einsatz von Standby-Datenbanken sind:

- ▶ Ein Primärsystem und ein Standby-System (jeweils mit eigenem Storage)
- ▶ Eine Netzwerkverbindung zwischen Primär- und Standby-System

Vorteile einer Standby-Datenbank:

- ▶ Bei Verwendung von Oracle Data Guard: Übernahme der Funktionalität bei Ausfall eines Servers ohne administrativen Eingriff
- ▶ Bei Ausfall eines Rechenzentrums kann unter Verwendung einer entfernten Standby-Datenbank der Betrieb weiter aufrechterhalten werden
- ▶ Disaster-Schutz durch Einsatz eines Remote-Rechenzentrums möglich
- ▶ Schutz vor Benutzerfehlern (abhängig von der Verzögerungsdauer bzw. bei Einsatz von Flashback Database auf der Standby-Seite)
- ▶ Nutzung der Standby Database für das Reporting

Nachteile einer Standby-Datenbank:

- ▶ Übernahme der Betriebsfähigkeit durch Standby benötigt etwas mehr Zeit als bei Hot Standby
- ▶ Erhöhte Netzlast durch Übertragung der Redo Log Informationen zwischen Primär- und Standby System; evtl. sollte zusätzliche Bandbreite zur Verfügung gestellt werden

Oracle Real Application Cluster (Hot Standby)

Bei Nutzung des Oracle Real Application Cluster sind im Normalbetrieb zwei oder mehrere Rechnerknoten im Cluster aktiviert. Der Vorteil: Fällt ein Rechner aus, so können Clients unmittelbar und ohne Wiederanlaufzeit auf einen verbleibenden Rechnerknoten konnektieren. Zudem können Lasten auf alle Clusterknoten verteilt werden. Langlaufende Operationen können mittels Parallel Slave-Prozessen auch über den gesamten Cluster parallelisiert werden. So ist neben der erhöhten Verfügbarkeit auch das Thema Skalierung eine der Stärken des Real Application Cluster. Redundante Hardware wird nicht nur im Fehlerfall eingesetzt, sondern kann – anders als bei Failover Clustern – im Normalbetrieb genutzt werden.

Ähnlich wie in einem Oracle Failover Cluster wird auch hier ein Private Network für den Cluster Heartbeat sowie ein davon separiertes Public Network benötigt. Allerdings wird im Oracle Real Application Cluster konkurrierend auf die Datenbankdateien eines Shared Storages zugegriffen. Dies erfordert zusätzlichen Kommunikationsaufwand zwischen den Knoten, der zur Abstimmung von Sperren und veränderten Block-Images nötig ist. Diese Clusterkommunikation erfolgt über das Private Network. In Real Application Clusterumgebungen ist es daher wichtig, einen möglichst schnellen privaten Cluster Interconnect zu nutzen. Mindestens Gigabit-Ethernet sollte eingesetzt werden. Besser noch sind spezielle, oft proprietäre Lösungen mit höherer Bandbreite. Beispiele sind Memory Channel (alpha-basierte HP Cluster), Myrinet (Linux Systeme), Scalable Coherent Interconnect (SUN), Veritas LLT (verschiedene Plattformen) oder HP Hyper Fabric HMP.

Notwendige Komponenten für den Einsatz eines Oracle Real Cluster sind:

- ▶ Shared Storage für alle beteiligten Cluster Nodes (konkurrierender Zugriff)
- ▶ Verwendung von Cluster-Filesystem, ASM oder Raw Devices auf dem Shared Storage
- ▶ Für jeden Clusterknoten mindestens je zwei Private und zwei Public Network Interfaces
- ▶ Oracle Cluster Ready Services oder Cluster Management-Software eines Drittherstellers

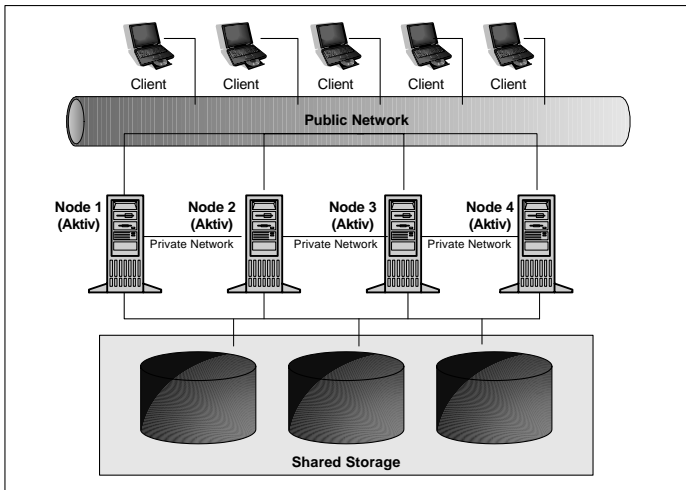


Abbildung 3.3: Schematische Darstellung des Real Application Cluster

Vorteile eines Oracle Real Application Cluster:

- ▶ Übernahme der Funktionalität bei Ausfall eines Servers ohne administrativen Eingriff
- ▶ Kein Zeitaufwand für Wiederanlauf, Client Reconnect direkt ohne Zeitversatz auf den Ersatzknoten
- ▶ Redundante Hardware kann auch während des Normalbetriebs genutzt werden
- ▶ Parallelisierung über alle Clusterknoten hinweg realisierbar
- ▶ Dynamische Zuordnung von Services möglich

Nachteile eines Oracle Real Application Cluster:

- ▶ Bei Ausfall eines Rechenzentrums (z.B. durch einen Brand) fällt der gesamte Cluster aus. Dieser Fehlerfall kann bei Bedarf durch Einsatz einer zusätzlichen Standby-Datenbank in Kombination mit Oracle Real Application Cluster abgefangen werden.

Geo Cluster, Datenbankspiegel und Hardware-Replikation

Einige Drittanbieter wie Veritas oder Libelle bieten erweiterte Möglichkeiten der Disaster-Absicherung. Geo Cluster erlauben Clustering ohne geografische Grenzen. Je nach Architektur können die Clusterknoten in Rechenzentren stehen, die von einigen wenigen bis zu mehr als hundert Kilometer entfernt sind. Manche Hersteller bieten auch Lösungen, die Spiegel- und Replikationsmechanismen über Kontinente hinweg unterstützen. Die Architekturen der einzelnen Hersteller sind ebenso unterschiedlich wie die Implementierung.

Verfahren wie Hardware-Replikation und Datenbankspiegel schützen ebenfalls vor logischen und physikalischen Ausfällen. Kernkonzept ist die Spiegelung über große Distanzen. Das Ergebnis ist von der Funktionalität her ähnlich einer Standby-Datenbank. Der Layer zur Realisierung liegt jedoch unterhalb der Datenbank-