# Data Guard durch Firewalls?

## Kein Problem mit Connection Manager!

Mathias Zarick
Principal Consultant


BASEL BERN BRUGG LAUSANNE ZÜRICH DÜSSELDORF FRANKFURT A.M. FREIBURG I.BR. HAMBURG MÜNCHEN STUTTGART WIEN



2013 © Trivadis



trivadis
makes IT easier.

# Vorstellung – Mathias Zarick

- Principal Consultant bei Trivadis Delphi GmbH in Wien
- Trainer
  - Data Guard, Architektur und Interna für fortgeschrittene DBAs, Maximum Availability Architecture Workshop
- E-Mail: Mathias.Zarick@trivadis.com
- Hauptthemen:
  - Oracle Datenbank
  - Oracle Hochverfügbarkeitsprojekte (Real Application Clusters, Data Guard, Maximum Availability Architecture, Replikation mit Streams und GoldenGate)
  - Backup/Recovery
  - Entwicklungsleiter der Trivadis Toolbox
  - Entwickler von TVD-Standby
  - Forschungsprojekte im Trivadis Technology Center (TTC)

ORACLE
Certified Master
Oracle Database 11*g*
Administrator

ORACLE
Certified Professional

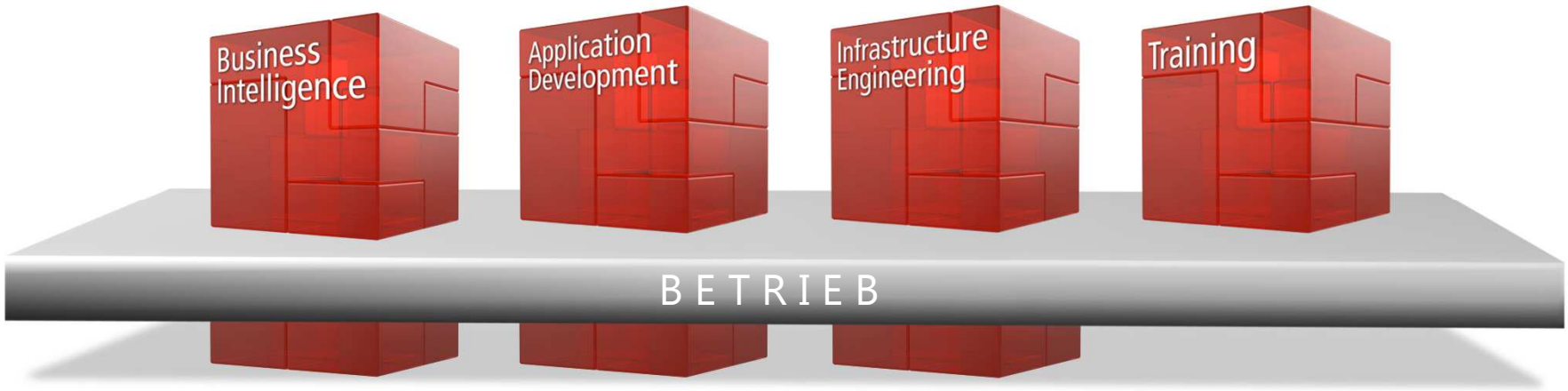

2013 © Trivadis


trivadis
makes IT easier.

# Unser Unternehmen

Trivadis ist führend bei der IT-Beratung, der Systemintegration, dem Solution-Engineering und der Erbringung von IT-Services mit Fokussierung auf ORACLE und Microsoft Technologien im D-A-CH-Raum.

Unsere Leistungen erbringen wir aus den strategischen Geschäftsfeldern:




Trivadis Services übernimmt den korrespondierenden Betrieb Ihrer IT Systeme.


2013 © Trivadis

# Mit über 600 IT- und Fachexperten bei Ihnen vor Ort


12 Trivadis Niederlassungen mit über 600 Mitarbeitenden

200 Service Level Agreements

Mehr als 4'000 Trainingsteilnehmer

Forschungs- und Entwicklungs-budget: CHF 5.0 / EUR 4 Mio.

Finanziell unabhängig und nachhaltig profitabel

Erfahrung aus mehr als 1'900 Projekten pro Jahr bei über 800 Kunden



2013 © Trivadis



Stand 12/2012

trivadis
makes IT easier.


BASEL BERN BRUGG LAUSANNE ZÜRICH DÜSSELDORF FRANKFURT A.M. FREIBURG I.BR. HAMBURG MÜNCHEN STUTTGART WIEN



2013 © Trivadis



trivadis
makes IT easier.

# Data Guard durch Firewalls

1. Einführung
2. Data Guard und Connection Manager
3. Observer
4. Fazit

# Oracle Datenbank Infrastruktur beim Kunden

- **Kunde**
  Broadcasting in Österreich
- **Technologien und Produkte**
  - Vorher:
    - 5 Databanken Oracle Enterprise Edition 11.2
    - Oracle Streams
  - Jetzt:
    - Data Guard
    - Connection Manager

- **Herausforderung**
  Vorher:
  - Errichten und Betreiben einer 5 Wege Multimaster Replikation

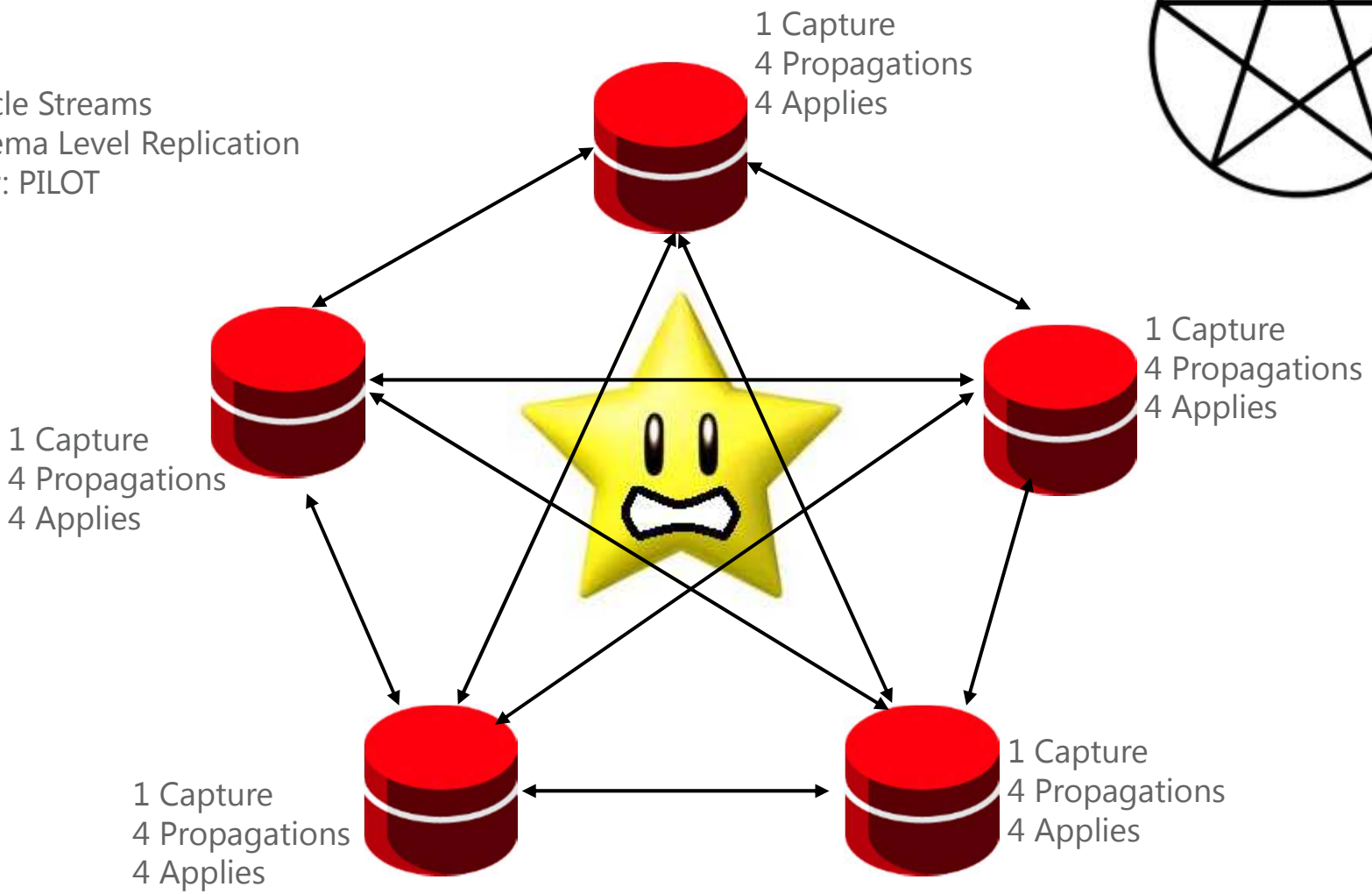
  Jetzt:
  - Clients in verschiedenen durch Firewalls abgeschotteten Netzwerksegmenten
- **Lösung**
  wird hier vorgestellt


2013 © Trivadis

trivadis
makes IT easier.

# Streams Setup war ein nettes Pentagramm

Oracle Streams
Schema Level Replication
User: PILOT




Keine Angst! ☺



trivadis
makes IT easier.

# Warum Streams hier doch ein Problem wurde

- Die Streams Replikation lief perfekt
- Konflikte konnten in der Multimaster Replikation vermieden werden
- Aber – der asynchrone Message Austausch wurde zum Problem

- Die Applikation braucht auch Advanced Queuing (AQ)
- In seltenen Fällen konnte eine AQ Message die dazugehörenden Schemadaten überholen

- AQ: “Es gibt einen neuen Datensatz in der Playlist!”
- Applikation: Query des Datensatz → no data found


2013 © Trivadis

trivadis
makes IT easier.

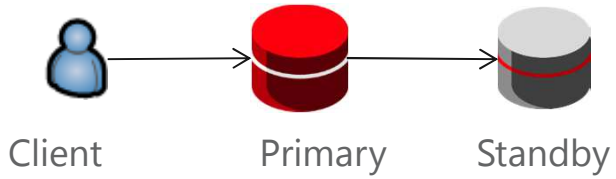
# Datenbank Charakteristiken

- Oracle Database 11.2.0.3
- Oracle Windows Patch Bundle 13 for 11.2.0.3 (Nov. 2012)
- Windows Server 2008 R2
- Oracle Data Guard
- Oracle Connection Manager (CM)
- Lizenzen:
  - Oracle Enterprise Edition
  - Keine weiteren Optionen
  - Kein Tuning / Diagnostics Pack (Keine Installation der OEM Database Console)

# Data Guard durch Firewalls

1. Einführung
2. Data Guard und Connection Manager
3. Observer
4. Fazit

# Data Guard Kommunikation (1)

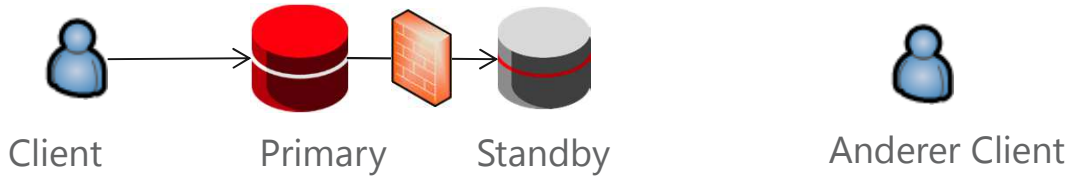



- Client verbindet zum Primärserver, z.B. Port 1521
- LNS/NSS Prozess verbindet sich zum Standby Server (RFS), z.B. Port 1521
- Nach einem Rollenwechsel muss sich der Client zum ehemaligen Standby-, jetzt Primärserver verbinden
- Die Verbindung kann durch Oracle Net Failover Mechanismen und TAF transparent verschoben werden


2013 © Trivadis

trivadis
makes IT easier.

# Data Guard Kommunikation (2)




- Eine Firewall zwischen Primär- und Standbyserver ist kein Problem für die Basis Funktionalität (Log Transport, Broker Kommunikation)
  - Wenn man bereit ist einige bekannte Verbindungen durch die Firewall zuzulassen (Firewall Holes)
- Aber
  - Was ist, wenn wir die Rolle wechseln müssen?
  - Was ist, wenn wir mehrere Clients von verschiedenen Subnetzten zugreifen lassen müssen?


2013 © Trivadis

trivadis
makes IT easier.

# Connection Manager

- Oracle Net Proxy
- Arbeitet auf Session-Level
- Benutzer verbinden sich auf den CM Listener → der CM Gateway Prozess verbindet auf die DB oder einen anderen CM
- Installation wird mit dem Client Paket gemacht: custom installation
  - Oracle Connection Manager
  - Oracle Net Listener
  - Oracle Database Utilities
- Kann für Security-Zwecke verwendet werden
  - Erlauben / Verweigern von spezifischen Clients, Servern, Services
- Kann zum Umgehen verschiedener Netzwerkeigenschaften verwendet werden, z.B. IPV4 → IPV6
- Oder um verschiedene separate Netzwerke zu verbinden

# Data Guard Setup Details

- Physical standby database Konfiguration
  - Primary Datenbank: Server1, DB_UNIQUE_NAME VIZRTDB_SITE1
  - Standby Datenbank: Server3, DB_UNIQUE_NAME VIZRTDB_SITE2
- Log Transport, lokaler Listener → Port 1522
- Maximum Availability
  - Synchroner Log Transport
  - Zero data loss
- Fast Start Failover ist aktiviert
  - Observer ist im Produktions Netzwerk (Server4)
  - Ein Backup Observer ist im Office Netzwerk vorbereitet (Server2)


2013 © Trivadis

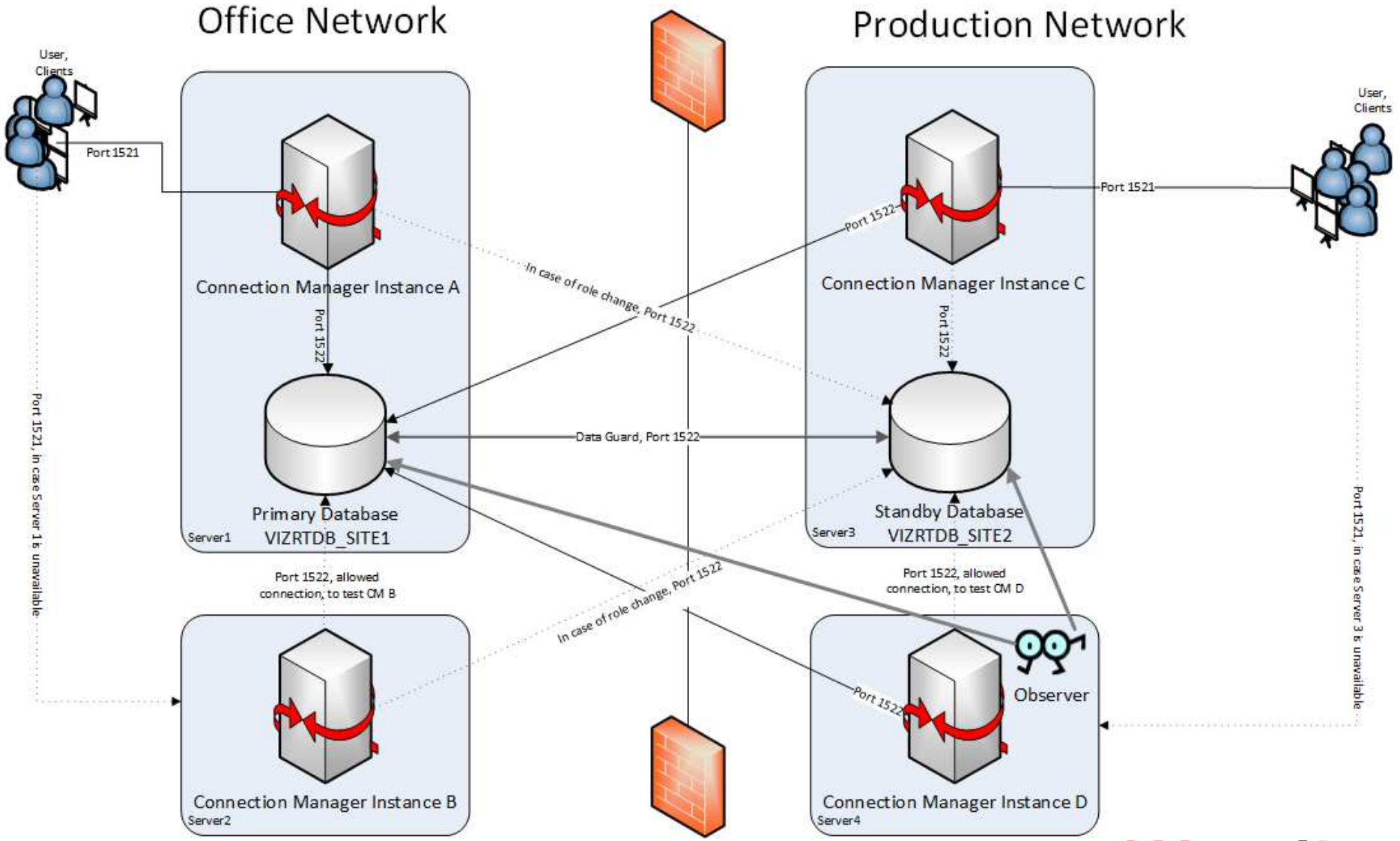
trivadis
makes IT easier.

# Data Guard durch eine Firewall

- Es gibt eine Firewall zwichen Office- und Produktionsnetzwerk

- 4 CM Instanzen sind installiert, um diese Herausforderung zu lösen:
  - Auf dem Primären Datenbank Server (Server1, Produktionsnetzwerk)
  - Auf dem Standby Datenbank (Server 3, Office-Netzwerk)
  - Auf 2 zusätzlichen Servern (Server2, Server 4) um die Verfügbarkeit pro Netzwerk zu erhöhen
- CM Listener sind auf Port 1521 konfiguriert
- Offene Ports (Firewall Holes):
  - Port 1521 und 1522 für den Primärdatenbankserver, den Standbydatenbankserver und die 2 anderen CMs (bzw. Observer)

# Infrastruktur – Big Picture






2013 © Trivadis



trivadis
makes IT easier.

# Oracle Datenbank Services für kontrollierten Zugriff (1)

- Oracle Datenbank Instanzen registrieren ihre Services auf alle 4 CMs
  - remote_listener ist folgendermaßen gesetzt

```
SQL> ALTER SYSTEM SET remote_listener = '
(ADDRESS_LIST=
  (ADDRESS=(HOST=SERVER1)(PROTOCOL=TCP)(PORT=1521))
  (ADDRESS=(HOST=SERVER2)(PROTOCOL=TCP)(PORT=1521))
  (ADDRESS=(HOST=SERVER3)(PROTOCOL=TCP)(PORT=1521))
  (ADDRESS=(HOST=SERVER4)(PROTOCOL=TCP)(PORT=1521))
)'
;
```

  - VIZRTDB ist der primäre Service
  - VIZRTDB_RO, falls die Standby read only geöffnet wird
  - VIZRTDB_SNAP, falls sie als Snapshot Standby read write geöffnet wird
- TAF ist für alle diese Services eingeschaltet
  - Failover Method BASIC, Failover Type SELECT
  - Failover Retries 3600, Failover Delay 1

# Oracle Datenbank Services für kontrollierten Zugriff (2)

- Benutzer verbinden über die CMs auf Port 1521
- Jeder CM verbindet zur Primärdatenbankinstanz über den Port 1522 (Proxy Forward)
- Der CM arbeitet also als Oracle Net Proxy
- Services und lokale Listener werden den CMs bekannt gegeben
  - VIZRTDB_SITE1:

```
SQL> ALTER SYSTEM SET
local_listener='(ADDRESS=(PROTOCOL=TCP)(HOST=SERVER1)(PORT=1522))';
```

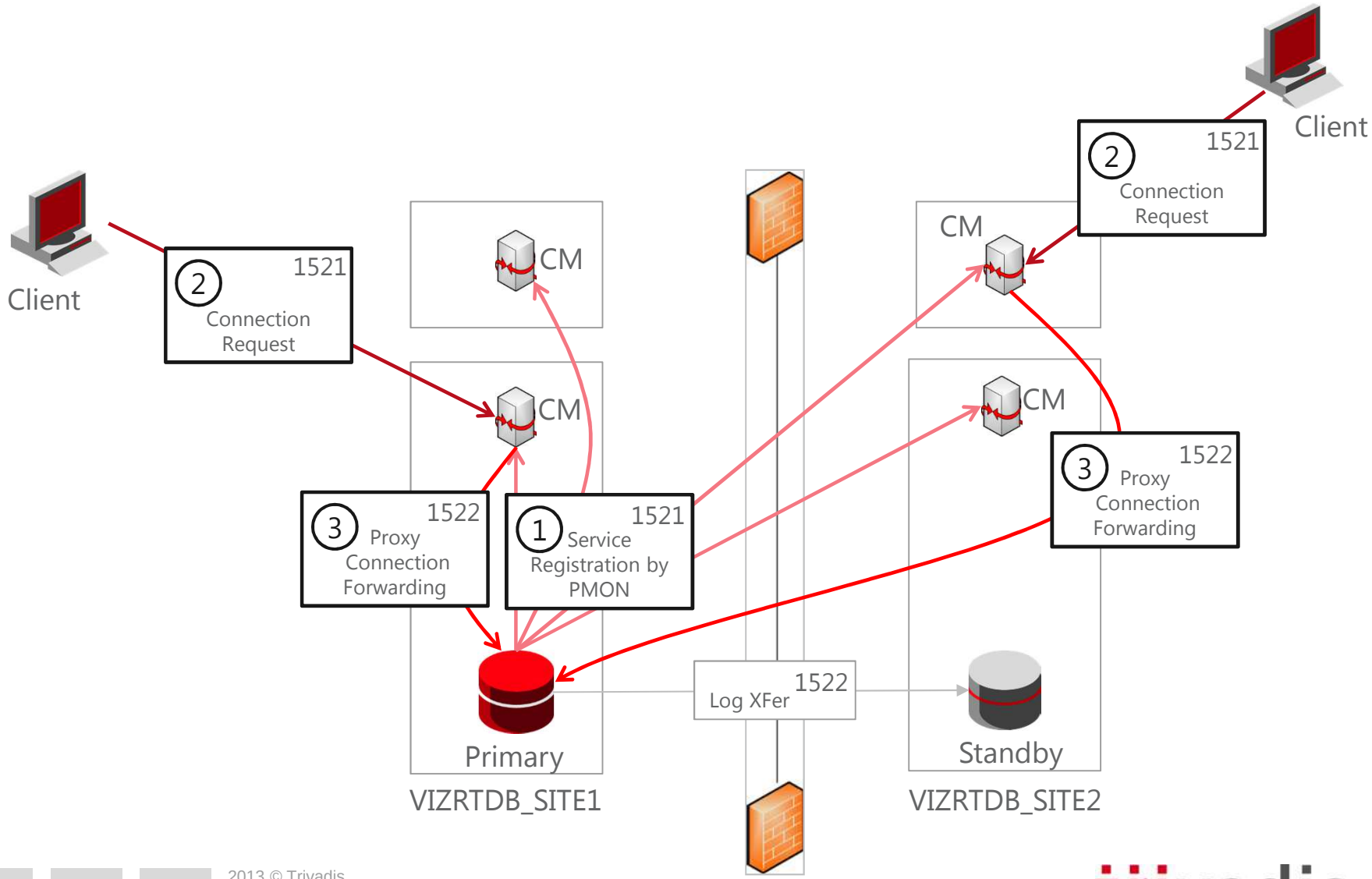
  - VIZRTDB_SITE2:

```
SQL> ALTER SYSTEM SET
local_listener='(ADDRESS=(PROTOCOL=TCP)(HOST=SERVER3)(PORT=1522))';
```


2013 © Trivadis

trivadis
makes IT easier.

# Verbindungsaufbau durch den Connection Manager






2013 © Trivadis



trivadis
makes IT easier.

# Korrekte Verbindungen sind wichtig (1)

- Die beschriebene Konnektivität ist wichtig für die Umgebung und darf nicht umgangen werden
- Daher wird das direkte Verbinden auf den DB Server verweigert
  - sqlnet.ora des Datenbankserver Listeners:

```
SQLNET.EXPIRE_TIME = 5    # Dead Connection Detection
                          # Keep Alive Packets
TCP.VALIDNODE_CHECKING=yes
TCP.INVITED_NODES=(SERVER1,SERVER2,SERVER3,SERVER4)
```

- Falls eine Verbindung von einer anderen Maschine versucht wird, wird folgender Fehler geworfen:

```
SQL> connect system@VIZRTDB_SITE1
Enter password:
ERROR:
ORA-12537: TNS:connection closed
```

# Korrekte Verbindungen sind wichtig (2)

- Der CM erlaubt nur bekannte Services, cman.ora

```
cman_SERVER1.domain =
(configuration=
  (address=(protocol=tcp)(host=SERVER1)(port=1521))
  (parameter_list =
   ...
  )
  (rule_list=
    (rule=(src=*)(dst=*)(srv=cmon)(act=accept))
    (rule=(src=*)(dst=SERVER1)(srv=VIZRTDB)(act=accept))
    (rule=(src=*)(dst=SERVER3)(srv=VIZRTDB)(act=accept))
    (rule=(src=*)(dst=SERVER1)(srv=VIZRTDB_RO)(act=accept))
    (rule=(src=*)(dst=SERVER3)(srv=VIZRTDB_RO)(act=accept))
    (rule=(src=*)(dst=SERVER1)(srv=VIZRTDB_SNAP)(act=accept))
    (rule=(src=*)(dst=SERVER3)(srv=VIZRTDB_SNAP)(act=accept))
  )
)
```

# Verbindungen aus Office- und Produktionsnetzwerk

- TNS Connect Deskriptoren

```
# office network
VIZRTDB =
  (DESCRIPTION =
    (ADDRESS_LIST=
      (LOAD_BALANCE=OFF) (CONNECT_TIMEOUT=3)
      (ADDRESS = (PROTOCOL = TCP)(HOST = SERVER1 )(PORT = 1521))
      (ADDRESS = (PROTOCOL = TCP)(HOST = SERVER3 )(PORT = 1521))
    )
    (CONNECT_DATA = (SERVICE_NAME = VIZRTDB)))

# production network
VIZRTDB =
  (DESCRIPTION =
    (ADDRESS_LIST=
      (LOAD_BALANCE=OFF) (CONNECT_TIMEOUT=3)
      (ADDRESS = (PROTOCOL = TCP)(HOST = SERVER2 )(PORT = 1521))
      (ADDRESS = (PROTOCOL = TCP)(HOST = SERVER4 )(PORT = 1521))
    )
    (CONNECT_DATA = (SERVICE_NAME = VIZRTDB)))
```

# Active Data Guard wird vermieden, Services werden dynamisch gesetzt

- Ein „After startup on database“ trigger
  - Verweigert das Read-Only-Öffnen der Standbydatenbank auf normale Art und Weise
  - Vermeidet daher die Benutzung der Real-Time Query und den Bedarf der Lizenz für die Active Data Guard Option
  - Übernimmt das Starten der korrekten Services nach Evaluierung der aktuellen Rolle (VIZRTDB, VIZRTDB_RO, VIZRTDB_SNAP)
- Für weitere Details, siehe Blog http://blog.trivadis.com/b/mathiaszarick/archive/2012/09/07/active-data-guard-s-real-time-query-avoid-usage-if-not-licensed.aspx

# Trigger Code

- Auszug / nur der Teil der Vermeidung von ADG ist hier dargestellt

```
CREATE OR REPLACE TRIGGER service_trigger_no_adg
AFTER STARTUP ON DATABASE
DECLARE
  v_sql v$sql.sql_text%TYPE;
BEGIN
  IF sys_context('userenv','database_role') = 'PHYSICAL STANDBY'  THEN
    SELECT sql_text INTO v_sql
    FROM v$sql sq, v$session se
    WHERE sq.sql_id = se.sql_id
    AND se.sid =  sys_context('userenv','sid');
    IF v_sql NOT LIKE '%FORCE%' THEN
      EXECUTE IMMEDIATE
        '/* do not open as we do not have adg licensed */ ALTER DATABASE CLOSE';
      /* restart DMON */
      EXECUTE IMMEDIATE('ALTER SYSTEM SET dg_broker_start=FALSE SCOPE=MEMORY');
      EXECUTE IMMEDIATE('ALTER SYSTEM SET dg_broker_start=TRUE SCOPE=MEMORY');
    END IF;
  END IF;
END;
/
```

# Aber es geht noch besser

- In einem Blog von Uwe Hesse wurde ein besserer Weg vorgestellt, ADG zu vermeiden
  http://uhesse.com/2013/10/01/parameter-to-prevent-license-violation-with-active-data-guard/

```
SQL> ALTER SYSTEM SET "_query_on_physical" = FALSE SCOPE=SPFILE
```

- Aber: es ist ein undokumentierter Parameter, also habe ich Oracle Support gefragt, ob es unterstützt ist.
  - „SR 3-7930233621 : support of parameter _query_on_physical”:
    Is it supported to set the _query_on_physical to false?
    NO - it is not supported.
- Ich habe im selben SR einen Enhancement Request eingegeben, um einen unterstützten Weg zu bekommen: “Work in Progress”

# Data Guard durch Firewalls

1. Einführung
2. Data Guard und Connection Manager
3. Observer
4. Fazit


2013 © Trivadis

trivadis
makes IT easier.

# Observer Konfiguration

- Server: SERVER4, SERVER2 (Observer Service ist nur vorbereitet)
- Script: observer.cmd
- SrvAny aus dem Windows Resource Kit (http://support.microsoft.com/kb/137890) wird für die Konfiguration des Windows Service verwendet

```
C:\Users\Administrator>sc qc OracleObserver
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: OracleObserver
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : C:\..\Win Resource Kits\..\srvany.exe
        TAG                : 0
        DISPLAY_NAME       : OracleObserver
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
```

# Observer CMD Script nutzt TVD-BasEnv

- observer.cmd
- Oracle Home wird mit dem CM geteilt
- Umgebung wird durch Trivadis BasEnv gesetzt

```
@ECHO OFF
REM source the environment
CALL basenv.cmd
CALL %BE_HOME%\bin\oraenv.cmd VIZRTDB
CD /D c:\oracle\admin\%ORACLE_SID%\log
REM we write the stop to another logfile as it may be locked by last run
SET LOGFILE=c:\oracle\admin\%ORACLE_SID%\log\observer_stop.log
DATE /T >>%LOGFILE%
TIME /T >>%LOGFILE%
%ORACLE_HOME%\bin\dgmgrl -silent "sys/***********@VIZRTDB" "stop observer"
>>%LOGFILE%
SLEEP 10 >>%LOGFILE% 2>&1
SET LOGFILE=c:\oracle\admin\%ORACLE_SID%\log\observer.log
ECHO observer script start >>%LOGFILE%
%ORACLE_HOME%\bin\dgmgrl -silent "sys/***********@VIZRTDB" "start observer"
>>%LOGFILE%
```

# SrvAny Konfiguration

- Service wurde folgendermaßen angelegt:

```
sc.exe create OracleObserver ^
binPath= "C:\Program Files (x86)\Windows Resource Kits\Tools\srvany.exe"
```

- SrvAny Konfiguration in der Registry:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\OracleObserver\Par
ameters]
"Application"="C:\\Windows\\System32\\cmd.exe"
"AppParameters"="/c C:\\oracle\\local\\dba\\bin\\observer.cmd"
```

# Data Guard durch Firewalls

1. Einführung
2. Data Guard und Connection Manager
3. Observer
4. Fazit

# Fazit

- Erfolgreiches Projekt → Zufriedener Kunde
  - Sparen von Lizenzkosten
  - Einsparen bei der Komplexität und im Betrieb
- Einige Herausforderungen bezüglich Netzwerk wurden mit Connection Manager gelöst

- Hochverfügbarkeit durch Data Guard
- Strenges Servicekonzept mit Zugriffsregeln
- Keine ADG Lizenz → Vermeidung der Real-Time Query
- Observer und FSFO auf Windows: kein Problem mit Microsoft Windows Resource Kit und Trivadis Toolbox

# Weitere Informationen...

- Data Guard Concepts and Administration
  http://docs.oracle.com/cd/E11882_01/server.112/e41134/toc.htm
- Net Services Administrator‘s Guide
  http://docs.oracle.com/cd/E11882_01/network.112/e41945/toc.htm

# Fragen und Antworten...

Mathias Zarick

Principal Consultant

+43 664 85 44 295

Mathias.Zarick@trivadis.com


BASEL BERN BRUGG LAUSANNE ZÜRICH DÜSSELDORF FRANKFURT A.M. FREIBURG I.BR. HAMBURG MÜNCHEN STUTTGART WIEN

# Trivadis an der DOAG

Ebene 3 - gleich neben der Rolltreppe

Wir freuen uns auf Ihren Besuch.

**Denn mit Trivadis gewinnen Sie immer.**