**HSSBC Database Services**

**Reference Architecture**

**Version 1.2**

**October 29, 2010**

# Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Created/Updated By** | **Reviewed by** | **Summary of Change** |
| 1.0 | Oct 29 / 2010 | Marcus Robb |  | initial draft |
| 1.1 | Nov 4/2010 | Marcus Robb |  | Updates post HPAS review |
| 1.2 | Nov 8/2010 | Marcus Robb/Brinder Lally |  | Updates including Oracle/Post Cross Over Meeting |

Table of Contents

[Revision History 2](#_Toc280260874)

[1. Architecture Overview 5](#_Toc280260875)

[2. Design Principles 5](#_Toc280260876)

[3. Summary of Key Decisions 5](#_Toc280260877)

[4. Architectural Design 6](#_Toc280260878)

[4.1 Architectural Design Introduction 6](#_Toc280260879)

[4.2 Business/Technology Requirements 6](#_Toc280260880)

[4.4 Design Section 6](#_Toc280260881)

[4.4.1 MSSQL Server 6](#_Toc280260882)

[4.4.1.1 Base Physical Specifications 6](#_Toc280260883)

[4.4.1.2 Use of SQL Instances: 7](#_Toc280260884)

[4.4.1.3 Disk Layout: 7](#_Toc280260885)

[4.4.1.4 Service Accounts: 8](#_Toc280260886)

[4.4.1.5 SQL Collation: 8](#_Toc280260887)

[4.4.1.6 Account Provisioning: 8](#_Toc280260888)

[4.4.1.7 Network Configuration: 9](#_Toc280260889)

[4.4.1.8 Production vs. QA/DEV/Test/Training 9](#_Toc280260890)

[4.4.1.9 Monitoring and Trending: 9](#_Toc280260891)

[4.4.1.10 High Availability: 11](#_Toc280260892)

[4.4.1.11 Backup and Recovery: 11](#_Toc280260893)

[4.4.2 Oracle 11](#_Toc280260894)

[4.4.2.1 Base Physical Specifications: 11](#_Toc280260895)

[4.4.2.2 Disk Layout: 11](#_Toc280260896)

[4.4.2.3 Service Accounts: 11](#_Toc280260897)

[4.4.2.4 Account Provisioning: 12](#_Toc280260898)

[4.4.2.5 Network Configuration: 12](#_Toc280260899)

[4.4.2.7 Monitoring and Trending: 12](#_Toc280260900)

[4.4.2.8 High Availability: 12](#_Toc280260901)

[4.4.2.9 Backup and Recovery: 12](#_Toc280260902)

[4.5 Security & Administration 13](#_Toc280260903)

[4.5.1 Network Isolation: 13](#_Toc280260904)

[4.5.2 Database Auditing: 13](#_Toc280260905)

[4.6 Risks/Constraints 13](#_Toc280260906)

[5. Appendices 13](#_Toc280260907)

[6. Reference Section 13](#_Toc280260908)

# 1. Architecture Overview

The primary objective of HSSBC Database Services is to provide secure, scalable and robust database services to all our Health Authorities while minimizing licensing sprawl and maximizing our hardware's potential.

This document's objective is to outline the standardized requirements for both Microsoft SQL Database servers, Oracle Database servers and their associated bundled software. Unless otherwise specified in the document, these are the only database technologies supported by HSSBC Database Services. The areas discussed will cover deployment and security.

## 2. Design Principles

Design principles will follow industry best practices for RDBMS:

* Principle of least privileges
* Standardized, repeatable installations
* Automation when possible
* Monitoring and trending for capacity

## 3. Summary of Key Decisions

* Microsoft SQL server is the primary RDBMS technology of HSSBC
* Oracle is the secondary supported RDBMS of HSSBC to be used only when business needs do not present a Microsoft SQL server option. This is due to Oracle licensing cost and availability of Oracle DBA’s at HSSBC.
* HSSBC Database Services will support versions of RDBMS actively supported by the originating vendors and encourage vendors and the business units in this direction.
* HSSBC Database Services will retain sole possession of any Systems Administration level accounts or roles at the instance level of each RDBMS installation.
* Application Owners will retain Database Owner Privileges.
* Virtualization technology is the primary choice for hardware as it provides abstraction from physical hardware for ease of maintenance and upgrades while also providing fail over capability similar to clustering without the added complexity at the guest level.
* Reduction of licensing for RDBMS
* Policy Based Management will be used to audit and when appropriate enforce server configuration
* Assumptions from the HSSBC Storage Services group will apply to the selection of disk tier for databases. Example: Tier 1 storage (5 9’s uptime) will be used for Tier 1 business applications (PCIS Systems); Tier 2 storage (4 9’s uptime) will be used for Dev/Test systems and some business systems that do not require 5 9’s; Tier 3 storage (highly available but with no defined SLA) will be used for backup/archive.
* Backup/Archive files should live on separate physical storage from the data/log files.

# 4. Architectural Design

# 4.1 Architectural Design Introduction

There will be two primary classifications of RDBMS, Managed Instance and Managed Hosted installations.

Managed Hosted systems will provide shared resources for utilization. Each Managed Hosted system will service only the originating HA. The primary ownership and management of these systems will always remain with HSSBC Database Services regardless of where the originating funding is provided. Projects will be encouraged to leverage shared systems as a first choice to reduce licensing and administrative footprint.

Managed Instance systems are RDBMS that are dedicated to a particular application based on performance or business needs.

Each classification will follow the standardized build practice of HSSBC Database Services and keep the fundamental design principles consistent between the two implementation types.

## 4.2 Business/Technology Requirements

HSSBC Database Services primary objective is to reduce database sprawl and ultimately consolidate installations and licensing.

In order to facilitate this business objective it is imperative to have accurate trending information in order to scale consolidated instances. We will rely on the HSSBC Operations team to deploy central monitoring software that will gather the extended system information required.

# 4.4 Design Section

## 4.4.1 MSSQL Server

### 4.4.1.1 Base Physical Specifications

The assumption is there will be a dedicated farm of VM Servers to handle the load of production databases, much are there is for exchange. In this farm there will be capability and capacity to fail instances to a physically separate blade chassis in a separate physical rack to ensure redundancy and maximize the ability to maintain hardware independent of host downtimes.

Base Specifications for Database Servers (subject to change based on requirements):

VMWare VSphere 4.0

Windows 2008 R2 64 Bit

SQL 2008 R2 64 Bit Enterprise with SSIS (Standard to be used when the installation is on physical hardware)

2 CPUs

4 GB Memory

To meet specifications of larger RDBMS we have the ability to go a 1:1 ratio of host to guest when needed.

Where architecture deems virtualization isn’t an option we will follow the WinTel Server architecture:

* + The HSSBC Virtual Services Reference Architecture outlines the benefits for server virtualization and where it meets the requirements of the WinTel Server platform requirements it will be the preferred deployment choice.
  + Physical server will be deployed as required on blade technology to best make utilization of computer room facility.
  + Rack physical servers will be implemented where virtual and blade servers do not meet the requirement

### 4.4.1.2 Use of SQL Instances:

The primary reason for multiple instances is when a security restriction does not allow databases to be hosted from the same instance or to maximize clustered hardware. Multiple instances of SQL on a single VM are to be discouraged. In a physical cluster scenario active/passive and active/active nodes are supported with a max of two instances on an active/active cluster. Instance root directories will remain at C:\Program Files\Microsoft SQL Server

SSIS will be deployed to each instance as a requirement for maintenance plans.

SSAS will be deployed only when required.

SSRS will be deployed only when required. HSSBC will provide a Managed Host solution for shared SSRS that will consist of two or more SSRS servers behind a hardware load balancer.

### 4.4.1.3 Disk Layout:

The assumption is disk tier will follow the business requirements of the SQL Instance.

Data/Log and TempDB drives for Tier 1 applications including all shared servers should reside on Tier 1 disk.

Each SQL Server must have the following disks dedicated to SQL Server service, recommended disk sizes are based on the total disk space required for data files:

* H (Data): 100%
* I (Log): 25% of Data
* J (TempDB): 25% of Data
* K (Backup): 150% of Data - (TBD pending review of Net Backup Agents)

In order to separate SQL related files from other files that might accidentally be saved on above disk drives; the folders below must be created prior to begin SQL setup:

* H:\SQL\_Data
* I:\SQL\_Log
* J:\SQL\_TempDB
* K:\SQL\_Backup
  + K:\SQL\_Backup\Maintenance Logs
  + K:\SQL\_Backup\System Databases
  + K:\SQL\_Backup\User Databases

In case we are planning to install a second instance the next four disk drives will be:

* L (Data): 100%
* M (Log): 25% of Data
* N (TempDB): 25% of Data
* O (Backup): 150% of Data

### 4.4.1.4 Service Accounts:

Service accounts will be dedicated to each SQL Instance Install with a randomly generated service account password.

SQL Server Agent and all Instance Services will run under the same service account and set to Automatic Start.

### 4.4.1.5 SQL Collation:

Standard North American Database Collation settings will be utilized unless there is a business need otherwise. SQL\_Latin1\_General\_CP1\_CI\_AS for the database engine and Latin1\_General\_CI\_AS for analysis services.

### 4.4.1.6 Account Provisioning:

Mixed mode authentication is supported but access through windows groups is the preferred authentication method for all SQL Installations.

SA Account passwords are to be randomly generated and unique for each instance.

Built-in local administrative accounts are to be removed from sysadmin roles during installation and replaced with HSSBC Database Services AD Group.

### 4.4.1.7 Network Configuration:

TCP/IP port configurations of instances will be configured in the following pattern:

Default Instance - port 1433

First Named Instance - port 1533

Second Named Instance - port 1633

### 4.4.1.8 Production vs. QA/DEV/Test/Training

Production systems will live on the primary SQL VM farm.

QA/Dev/Test/Training systems will live on lower tier systems or VM farm where uptime expectations are not as critical.

### 4.4.1.9 Monitoring and Trending:

Every instance will require monitoring using the preferred tool from HSSBC Operations, SCOM.

Thresholds and alert patterns will be determined at a future date.

Monitoring will be provided by HSSBC Operations and include:

Logical Disk

Disk Free Space

Logical Disk Read Latency Analysis

Logical Disk Write Latency Analysis

Logical Disk Transfers/sec

Memory

Memory Leak Detection

Handle Leak Detection

Process Thread Count

Process Working Set

Available MBytes

Free System Page Table Entries

Pool Non-Paged Bytes

Pool Paged Bytes

Memory Pages/sec

Memory System Cache Resident Bytes

Memory Percent Committed Bytes In Use

Network

% Network Utilization

Output Queue Length

Paging File

Paging File % Usage

PhysicalDisk

Physical Disk Read Latency Analysis

Physical Disk Write Latency Analysis

Process

Process % Privileged Time

High Virtual Memory Usage

Processor

Excessive Processor Use by Processes

% Processor Time

Privileged Mode CPU Analysis

Processor Queue Length

High Context Switching

Interrupt Time

SQLServer:Access Methods

SQLServer:Access Methods Forwarded Records/sec

SQLServer:Access Methods FreeSpace Scans/sec

SQLServer:Access Methods Full Scans/sec

SQLServer:Access Methods Page Splits/sec

SQLServer:Access Methods Scan Point Revalidations/sec

SQLServer:Access Methods Workfiles Created/sec

SQLServer:Access Methods Worktables Created/sec

SQLServer:Access Methods Index Searches/sec

SQLServer:Buffer Manager

SQLServer:Buffer Manager Buffer cache hit ratio

SQLServer:Buffer Manager Free pages

SQLServer:Buffer Manager Lazy writes/sec

SQLServer:Buffer Manager Page life expectancy

SQLServer:Buffer Manager Page lookups/sec

SQLServer:Buffer Manager Page reads/sec

SQLServer:Buffer Manager Page writes/sec

SQLServer:General Statistics

SQLServer:General Statistics Logins/sec

SQLServer:General Statistics Logouts/sec

SQLServer:General Statistics User Connections

SQLServer:Latches

SQLServer:Latches Latch Waits/sec

SQLServer:Latches\Total Latch Wait Time (ms)

SQLServer:Locks

SQLServer:Locks Lock Requests/sec

SQLServer:Locks Lock Waits/sec

SQLServer:Locks Lock Wait Time (ms)

SQLServer:Locks Lock Timeouts/sec

SQLServer:Locks Number of Deadlocks/sec

SQLServer:Memory Manager

SQLServer:Memory Manager Memory Grants Pending

SQLServer:Memory Manager Target Server Memory(KB)

SQLServer:SQL Statistics

SQLServer:SQL Statistics Batch Requests/sec

SQLServer:SQL Statistics SQL Compilations/sec

SQLServer:SQL Statistics SQL Re-Compilations/sec

### 4.4.1.10 High Availability:

With the capabilities of V-Motion in the virtual farm and the added security of snapshots before applying operating system updates, Virtualization is the preferred method of deploying SQL Servers. With the ability to utilize a 1:1 host/guest ratio in the SQL VM farm, we’re able to provide the performance of a dedicated cluster node while removing the complexity and limitations of a hardware bound cluster.

In situations where required, HSSBC Database Services will support clustered instances of MSSQL.

##### Mirroring, replication and log shipping are also supported DR solutions where required.

### 4.4.1.11 Backup and Recovery:

Flat file backups are currently the supported backup strategy at HSSBC, subject to change based on evaluation of a comparison between Netbackup SQL Agents vs. disk storage costs from the HSSBC Storage and Backup team.

Daily backups coupled with 15 minute transaction log backups are the standard backup policy at HSSBC. Simple recover mode of databases is only supported on a case by case basis with understanding and agreement from application owners of the limits to recoverability.

## 4.4.2 Oracle

### 4.4.2.1 Base Physical Specifications:

Subject to requirements and core factor licensing of Oracle.

### 4.4.2.2 Disk Layout:

/U01 – Binaries – 20 GB

/U02 – Data Files/Control File 01 – 100% of required

/U03 – Redo Logs – 25% of data

/U04 – Archive/Backups/ Control File 02 – 150% of data

A mirror copy of the Redo Logs and U04 should reside on a separate physical SAN from U02/U03. The mirror copy Redo Logs should reside on disk equally as fast as U03.

### 4.4.2.3 Service Accounts:

Oracle UNIX Account – password will be randomly generated

ORInstall UNIX Group – will own the Oracle binaries

DBA UNIX Group – will own the Oracle data files

Service accounts on Windows will be dedicated to each Oracle Instance Install with a randomly generated service account password. SQLNet Services will run under the same service account and set to Automatic Start.

### 4.4.2.4 Account Provisioning:

Account passwords are to be randomly generated and unique for each instance for the following accounts:

SYSDBA

SYSOPR

System

### 4.4.2.5 Network Configuration:

Primary Instance:

1521 – Oracle Listener

3876 – Oracle Enterprise Manager (Grid Control Agent)

**When separation of instances required:**

Secondary Instance:

1523 – Oracle Listener

3876 – Oracle Enterprise Manager (Grid Control Agent)

Third Instance:

1525 – Oracle Listener

3876 – Oracle Enterprise Manager (Grid Control Agent)

Central Grid Control Server:

1158/1159 – Grid Control

### 4.4.2.7 Monitoring and Trending:

Oracle Enterprise Manager Grid Control is the preferred method for monitoring and managing all production Oracle Instances. Where cost is prohibitive, Dev/Test systems may be monitored by SCCM or Orion for basic metrics.

### 4.4.2.8 High Availability:

##### RAC, Data Guard and Unix/Windows clustering are supported DR solutions where required.

### 4.4.2.9 Backup and Recovery:

Hot Backups are taken daily via RMAN.

Archive Logs and a mirrored copy of the Redo logs and control file will reside on separate physical storage from the Data and main Redo logs.

Cold Backup’s performed on a case by case basis and need.

Physical files will be picked up via NetBackup per the Backup and Storage team’s policy.

## 4.5 Security & Administration

### 4.5.1 Network Isolation:

In alignment with Security Services guidelines, database systems will be logically separated from other systems through use of IDS/IPS and firewalls.

HSSBC production Managed Host instances will reside in a network segment secured by firewalls. Direct inbound connection to the servers will only be available via the standardized ports from outside systems. Outbound connections from this zone will be restricted to server subnets. Inbound exceptions will be restricted to IPs and ports of identified monitoring and management servers.

A management terminal server will reside inside this zone for the purpose of RDP management access for HSSBC Windows Server Services and HSSBC Database Services. Direct RDP to the SQL Servers will not be permitted. Network IDS will monitor traffic to this zone and the exposed ports.

Managed Instance installations will follow the same port standards, and based on the application tier live in appropriate network zones.

QA/DEV/Test/Training systems will be restricted by firewalls from accessing production database zones.

### 4.5.2 Database Auditing:

Per section 6.3 Logging and Auditing of the Security Services Architecture, all database servers capable of native auditing (SQL 2008, Oracle 11G) will have instance and database auditing configured to log to remote Security Services central logging servers. Access to raw logs and modification of log settings will be restricted to the security group.

## 4.6 Risks/Constraints

Oracle 9i/10g are in use and there will be no upgrade while migration. We will however correct any disk layout or memory/server configurations to maximize recovery on the target infrastructure.

# 5. Appendices

# 6. Reference Section

Security Services Architecture

Windows Server Services Architecture

Storage Services Architecture