Standardization of the Database-Environment

Contents

[Configuration Policy 4](#_Toc402252323)

[Naming Convention 4](#_Toc402252324)

[Instance Name 4](#_Toc402252325)

[Database Name 4](#_Toc402252326)

[Communication 5](#_Toc402252327)

[SQL-Server and SQL-Browser 5](#_Toc402252328)

[Oracle Listener Port and Service Names 5](#_Toc402252329)

[Friendly-ServerName (DNS-ALIAS) 5](#_Toc402252330)

[DB Configuration/Set up 5](#_Toc402252331)

[SQL-Server 5](#_Toc402252332)

[Oracle 6](#_Toc402252333)

[Database Object Template Format 7](#_Toc402252334)

[Maintenance Procedures 8](#_Toc402252335)

[Data Retention Policy 8](#_Toc402252336)

[Maintenance Tasks 8](#_Toc402252337)

[Patching Policy 8](#_Toc402252338)

[Backup Policy 10](#_Toc402252339)

[Job Scheduling 10](#_Toc402252340)

[Incident & Change Management Procedures 10](#_Toc402252341)

[Deployment Procedures 10](#_Toc402252342)

[Script Implementation 11](#_Toc402252343)

[Script Format & Delivery Requirements 11](#_Toc402252344)

[Testing and Auditing Process 11](#_Toc402252345)

[Environments 11](#_Toc402252346)

[Lifecycle Requirements 11](#_Toc402252347)

[Decommissioning 11](#_Toc402252348)

[QA & Testing Environment Guidelines 11](#_Toc402252349)

[Compliance Procedures 11](#_Toc402252350)

[Security Access Level 11](#_Toc402252351)

[User Access Management 11](#_Toc402252352)

[External Database Access 12](#_Toc402252353)

[Security Encryption Requirements 12](#_Toc402252354)

[Version Upgrades 12](#_Toc402252355)

[Auditing 12](#_Toc402252356)

[Monitoring Procedures 13](#_Toc402252357)

[Monitoring Tools 13](#_Toc402252358)

[Metrics 13](#_Toc402252359)

[Alert Indicators 13](#_Toc402252360)

[Performance Indicators (Tuning/Optimization) 14](#_Toc402252361)

[Utilization Indicators 14](#_Toc402252362)

Required Test & Production Environments?

Environment and Application DB-Server Relationship

There are 6 Environments available.

Production, QA, Test, Development, Sandbox, User acceptance.

|  |  |
| --- | --- |
| **Environment** | **Purpose** |
| Production | This is the actual environment in which your system will run once it is deployed |
| QA | Its purpose is to provide an environment that simulates your actual production environment as closely as possible so you can test your application in conjunction with other applications |
| Test |  |
| Development |  |
| Sandbox |  |
| User-acceptance |  |

Dependent on the Workload and … Requirements on Application and

# Configuration Policy

## Communication

### SQL-Server and SQL-Browser

To mitigate Problems with JDBC-Access, it has to be used a fixed TCP Port for MSSQL Instance **1433**.

### Oracle Listener Port and Service Names

The Oracle default Listener-Port 1521 should be used.

### Friendly-ServerName (DNS-ALIAS)

To have a higher flexibility and to be independent from Server Name changes in the future, due to server migrations etc, a DNS-ALIAS (C-Name) has to be used by the application to access the database server.

EnvironmentRDBMSAPPLNAME

1 3 max(10)

Example:

|  |  |  |  |
| --- | --- | --- | --- |
| Application | Server Name | C-Name | RDBMS |
| Right Fax | Pfhlbdmsql02 | pSQLRightfax | SQL-Server |
|  |  | tSQLRightFax |  |
| SharePoiint | psharepsql01 | pSQLMoss |  |
| Calypso | pcalora01 | pORACalypso | Oracle |
| Principia | ppasora01 | pORAPrincip | Oracle |

## DB Configuration/Set up

The Requirements for a database creation will be captured with Sharepoint E-mail form.

These information are required.

Application-Name:

Application Owner:

Department:

Project:

Application-Type: DSS, OLTP, OLAP

SOX-relevant:

Data-Deletion Policy:

Application Requirements Document

DB-Requirements

DB Server

DB Database Edition (Enterprise, Std, BI)

DB Database Minimum Version

DB Type – Oracle/SQL

DB-Size Initial in MB:

yearly-DB growth in MB:

DB Supported Service Pack/Patching

Concurrent-User:

Backup: Point-In-Time

Backup-Retention: bank-standard (daily backup 10 days, monthly 5/7 years)

Security

Initial Permissions

Transparent Data Encryption

Network Encryption

The DB Edition and DB-Options are be determined by the business application and security needs.

Example Scripts see ….

SQL\_DB ENGINE, SQL\_DB ENGINE + SSIS, SQL\_DB ENGINE + SSIS + SSRS, SSRS

For additional settings after installation

## Naming Convention

Server Name

The Server Name should describe the environment and the RDBMS it is used for.

**P**FHLBDM**SQL01**

**T**FHLBDM**ORA01**

### Instance Name

#### SQL-Server

The “Default Instance” (MSSQLSERVER) should be used, except otherwise stated.

#### Oracle

The instance name should describe the environment and the application it is used for.

EnvironmentInstanceName

1. 7

Example:

|  |  |  |  |
| --- | --- | --- | --- |
| Environment | Application | Curr Instance Name | New Instance Name |
| Production | Calypso | CALTX01 | PCALTX01 |
| Test |  | CALTX01 | TCALTX01 |
| Development | Principia | PRODDB | DPRODDB |
|  |  | CALTX01 | ORA01 |

#### Database Name

##### SQL-Server

Where ever possible, the Database Name should describe the environment and the application it is used for.

EnvironmentDBName

1 32

Example:

|  |  |  |  |
| --- | --- | --- | --- |
| Environment | Application | Curr Database Name | New Database Name |
| Production | Right Fax | RightFax | RightFaxp |
| Test | Right Fax | RightFax | tRightFaxt |
| Development | Right Fax | RightFax | dRightFaxd |
|  |  |  |  |

##### Oracle

The Database Name is equal the Instance Name.

### SQL-Server

#### Recovery Settings

The Recovery Model should be set to meet the business requirements regarding the Recovery Objective Time, which is defined in the SLA.

By setting the Recovery Model to “Simple”, the database can only be recovered from a complete full backup, where as a recovery model “Full” allows to perform a point in time recovery. When Full -> appropriate TSM scheduled backup for truncate or shrink to maintain the Log file size

Furthermore it has to be to take in account, that the ETL Jobs into the current Data Warehouse are re-startable. 🡪 scheduling

If nothing is specified in the SLA, “Simple” is the default.

#### Disk Layout

|  |  |
| --- | --- |
| Parameter | Drive |
| INSTALLSHAREDDIR | C:\Program Files\Microsoft SQL Server |
| INSTANCEDIR | D:\ |
| INSTALLSQLDATADIR | D:\ |
| SQLUSERDBDIR | E:\MSSQLxx.MSSQLSERVER\MSSQL\Data |
| SQLUSERDBLOGDIR | F:\MSSQLXX.MSSQLSERVER\MSSQL\Log |
| SQLTEMPDBDIR | G:\MSSQLXX.MSSQLSERVER\MSSQL\Data |
| SQLTEMPDBLOGDIR | G:\MSSQLXX.MSSQLSERVER\MSSQL\Log |
| SQLBACKUPDIR | H:\MSSQLXX.MSSQLSERVER\MSSQL\Backup |

xx (Major Build Version, 11,12, …), where MSSQLSERVER is a defaults instance name, if it is a specified Instance Name this will change to the Instance Name

Advance Options

|  |  |
| --- | --- |
| Parameter |  |
| Database Mail XPs |  |
| xp\_cmdshell |  |
| remote admin connections |  |
| xp\_dirtree |  |
| xp\_fixeddrives |  |

### Oracle

#### Recovery Settings

The Backup and recovery Database parameters should be set to meet the business requirements regarding the Recovery Objective Time, which is defined in the SLA.

Using Oracle managed File approach for Database File Naming.

#### Disk Layout Windows

|  |  |
| --- | --- |
| Parameter | Purpose |
| ORACLE\_BASE | C:\ORACLE |
| ORACLE\_HOME | %ORACLE\_BASE%\product\xx\db\_home1 |
| DB\_CREATE\_FILE\_DEST | D:\ORADATA |
| DB\_CREATE\_ONLINE\_LOG\_DEST\_1 | D:\ORADATA |
| DB\_CREATE\_ONLINE\_LOG\_DEST\_2 | R:\ORADATA |
| DB\_RECOVERY\_FILE\_DEST | P:\ORADATA |
| LOG\_ARCHIVE\_DEST\_1 | P:\oradata\%ORACLE\_SID%\ARCHIVELOG |
| LOG\_ARCHIVE\_DEST\_2 | D:\oradata\%ORACLE\_SID%\ARCHIVELOG\ |
| DIAGNOSTIC\_DEST | C:\ORACLE |

xx (DB Version and Patchset level, 11.2.0.3, 11.2.0.4)

#### Disk Layout SUN

|  |  |
| --- | --- |
| Parameter | Purpose |
| ORACLE\_BASE | /app/oracle |
| ORACLE\_HOME | $ORACLE\_BASE/product/xx/db\_home1 |
| DB\_CREATE\_FILE\_DEST | /oradata/$ORACLE\_SID/datafiles |
| DB\_CREATE\_ONLINE\_LOG\_DEST\_1 | /oradata/$ORACLE\_SID/datafiles |
| DB\_CREATE\_ONLINE\_LOG\_DEST\_2 | /oradata/PRODDB/redo |
| DB\_RECOVERY\_FILE\_DEST | /oracle/fast\_recovery\_area |
| LOG\_ARCHIVE\_DEST\_1 | /oradata/%ORACLE\_SID/archive/ |
| LOG\_ARCHIVE\_DEST\_2 | -- |
| DIAGNOSTIC\_DEST | /app/oracle |

xx (DB Version and Patchset level, 11.2.0.3, 11.2.0.4)

## Database Object Template Format

Link to DB Developer Documentation

DB Stored Procedures

DB Views

DB Tables

# Maintenance Procedures

## Data Retention Policy

## Maintenance Tasks

Defining index fragmentation percentage for rebuild

### Patching Policy

The Goal of the patching policy is to provide a secure, stable and standardized database environment.

The Build level and Version Level for each product version should be consistent across the environments.

|  |  |  |
| --- | --- | --- |
|  | Microsoft | Oracle |
| Maintstream Support | Service Pack | PatchSet |
| Critical, business impact | Hotfix COD, GDR | CPU, Bundle, SPU |
| Non-critical | QFE, CU | PSU |

#### Terminology Microsoft SQL Server

##### Service Packs

A tested, cumulative set of all hotfixes, security updates, critical updates, and updates. Additionally, service packs may contain additional fixes for problems that are found internally since the release of the product. Service Packs are fully regression tested.

SQL Server software update packages typically fall into two major release types:

GDR (General Distribution Release)/QFE (Quick Fix Engineering)

GDR releases are reserved for those key fixes identified by SQL Server support to potentially affect a broad customer base. It includes only security related changes that have been made to the binary, including changes that are relevant to this build of the file and from any earlier security hotfix that updates the same binary.

QFE releases contains both security related changes that have been made to the binary as well as any functionality changes that have been made to it, including changes that are relevant to this build of the file and from any earlier security fix or bug fix that updates the same binary.

##### Hotfix Patches

Hotfix releases are typically for fixes to isolated issues not affecting a large customer base; while the product is in mainstream support. Hotfix are released in two major types:

*COD (Critical On Demand) or OD (On Demand)*: COD or OD releases are reserved for critical customer requests where key business functionality is impaired from the issue encountered. As the nature of the request, these releases do not follow a regular cadence.

*CU (Cumulative Update)*: CU releases are non-critical requests which provide fixes for isolated issues not affecting key business functionality. The CU releases on a two-month cadence while the product and service pack are in mainstream support. Cumulative Updates are not fully regression tested.

#### Terminology Oracle

##### Patchset Update (PSU)/ Security Patches only for Non-Windows platforms

The PSU and SPU patches released each quarter contain the same security content. Oracle recommends the PSU as it provides additional critical bug fixes. The SPU and PSU patches employ different patching mechanisms, so customers need to take into account the following information when selecting between Database SPUs and PSUs.

##### Patch Set

On a regular basis Oracle provides patch sets that include generic and port specific fixes encountered by customers since the base product was released.

##### Patch Set Exceptions (PSE)

If a customer encounters a critical problem that requires a fix prior to the next patch set becoming available, they can request that a one off fix be made available on top of the latest patch set. These Patchsets Exceptions are cumulative and includes all fixes since the current patch set.

##### Bundle Patches only for Windows

The bundle patches also include the fixes for the SPU/CPU (Critical Patch Update), DST (Daylight Saving Time), PSU (Patch Set Update) and Recommended Patch Bundles.

##### OVJM all platforms

The JavaVM Component Database PSU is delivered as a single bundle patch which can be applied to all Unix platforms; on Windows there is a separate bundle for 32-bit and x64. The Windows OJVM PSU bundle patch is delivered as an overlay patch on top of the regular Windows bundle patch, much like a one off patch.

##### Critical Patch Updates

Critical Patch Updates are collections of security fixes for Oracle products. They are available to customers with valid support contracts. They are released on the Tuesday closest to the 17th day of January, April, July and October.

#### Guideline

We are proactively monitoring patch status for vulnerabilities and business critical functionality in order to maintain compliance with defined Standards.

We are actively assessing Risk Management for the database environments and collaborating with Information Security.

Identified Hotfixes/GDR or Critical Patch Updates which are impacting the security or are impacting the key business functionality should be applied in a timely manner.

Oracle follows the Common Vulnerability Scoring System Version 2 and every identified Vulnerability with a Base Score equal or higher than 7 needs to be applied.

QFE/non-critical CU/Patch Set Exceptions should be applied if we encounter these problems.

Service Packs and Patch Sets needs to be applied to be complaint with the mainstream Support.

Since the Service Packs, Patch Sets, PSE and PSU are cumulative, it should be discussed with the Application Data Owner to apply the Service Pack/Patch Set/PSE/PSU instead of the Hotfix or CPU.

### Backup Policy

The data retention and Backup procedure has to be aligned to meet the regulatory requirements and the Recovery Time Objective/Recovery Point objective for each business application, which is defined in the Service Level Agreement.

#### Data Retention

Daily Backups are stored for 7 days. End of Month backups are stored for 7 years.

The data retention is defined within of the TSM Domain that is used for backing up.

#### Backup Procedure

Currently TSM for Databases (SQL Server) is utilized to perform the SQL-Server Backups. The Scheduling is implemented via TSM-Scheduler.

For Oracle-Backups is a 2 step Backup procedure implemented. RMAN from Oracle is utilized to backup to disk and TSM BA Client is used to back up the RMAN-Backups to the TSM Storage. The Scheduling is implemented via Windows Scheduled Task and TIDAL jobs.

Backup/Restore/Recovery Validation

A scheduled Validation Test will be performed twice a year not including the company BRC-Test.

### Job Scheduling

Currently different job scheduling tools are used (TSM-Scheduler, TIDAL, Windows Scheduled Task, SQL Maintenance Plan).

The current Job-Scheduling Policy defined Tidal as the preferred Job-Scheduling tool.

Review logging to tables for job start, end, etc.

#### Alert Notifications

#### Error Handling Guidelines

# Incident & Change Management Procedures

We are following general FHLBDM-Incident and Change management process

## Deployment Procedures

Process for Subversion

## Script Implementation

### Script Format & Delivery Requirements

### Testing and Auditing Process

# Environments

## Lifecycle Requirements

### Decommissioning

## QA & Testing Environment Guidelines

# Compliance Procedures

## Security Access Level

Security permissions will be granted following the guidelines of lowest privileged access for the database login user.

### User Access Management

Roles:

* Read/Write
* Read Only

Audit Process – Access Rights

Removal Process

### External Database Access

ODBC or JDBC based connector applications that connect to database systems including Access, Excel, Crystal Reports, SSRS, and Application Integration. These external database applications and files need to be identified and maintained in a list for reference with regards to versioning, compatibility, location, and access permissions.

The usage of ODBC or JDBC based connector applications should be standardized to only the approved tools to ensure data integrity, security and quality. The preferred method would be to utilize a standardized reporting/analytics tool company wide to minimize risk and complexity in the environment.

## Security Encryption Requirements

## Version Upgrades

All database applications to be added to the “version support matrix” with input from ADO for each application to include the following: appropriate software version listed for each version of database software, indicator for current application version and current database software version, application data owner, and date last reviewed.

## Auditing

We utilize the audit functionality of the RDBMS where necessary with guidance from the security team. The servers and areas to be audited are defined by the security team’s SOX 404 compliance list.

Currently the following applications needed to be audited.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Application | DB/Instance | Server | RDBMS | Hosted |
| BankMate | Pbankm01 |  | DB2 iSeries | FHLBDM |
| QRM | DEFAULT\_INSTANCE | Pqrmsql01 | SQL Server | FHLBDM |
| eAdvantage |  |  |  |  |
| Microsoft Dynamics | Dynamics, GP\_Interface,HLGBP, TWO | buckeye | SQL Server | FHLBDM |
| Principia | Proddb | Ppasora01 | Oracle | FHLBDM |
| FundTech (BankServ) |  |  |  |  |
| Workday |  |  |  |  |

More detailed information regarding the application is available in the [Business Master Application List](../../../../entarch/Lists/Master%20Application%20List/Business%20Applications.aspx).

For SQL Server the Enterprise Edition is necessary to utilize the audit functionality.

Audit findings are to be reviewed with the security team for risk assessment and appropriate action.

What tool?

What level of detail?

Encryption

Best Practices

* Orphaned Users
* User Permission Assessment (RSOP)
* With No Lock
* xpcmdshell
* Database Mail

Policy Enforcement

* Enforce Standard Naming convention db, table, sp, views, functions, indexes, ….
* Enforce of RiskManagement
* Enforce of Configuration
* Enforcement of Information Security

# Monitoring Procedures

The primary goal is to ensure of notification by critical alerts which are impacting the business application availability and response time.

This data is also used for capacity management and planning to provide a stable database service which meets the business requirements.

## Monitoring Tools

Currently the monitoring tool Foglight and Performance Anaylsis are used.

For monitoring audit activities Tripwire will be examined.

Other Tools ( tbd)

## Metrics

Configuration Changes

In complaint with Auditor requirements (db\_mail, xp\_cmdshell, …)

### Alert Indicators

CPU Threshold

Memory Threshold

Disk I/O Threshold (Writes per second/IOPS)

Disk Usage

* + Log file
  + Data file
  + Backup/Recovery Destination
  + Archive Destination

Network Bandwidth

Long running queries

Deadlocks and wait events

Availability (Up/Down)

Maintenance Job Failures

Scheduled Job Failures

Total Maintenance Jobs Scheduled

Total Scheduled Jobs Run

Alert Log

Sql Server Log

### Performance Indicators (Tuning/Optimization)

Response Time

Index Usage

Query Update/Optimization

### Utilization Indicators

CPU Utilization

Memory Utilization

Storage Utilization

Number of Databases

Number of Transactions

Number of Concurrent Users