

**『SEMA』 차세대 정보시스템 구축**

DBMS 아키텍처 정의서

[DA\_DA\_A\_11]

Ver. 1.02

2020.11.12



개 정 이 력

| **버전** | **작성일** | **변경 내용** | **작성자** | **승인자** |
| --- | --- | --- | --- | --- |
| 0.80 | 2020.09.25 | 최초 작성 | 양경철 | 윤화병 |
| 0.81 | 2020.09.29 | PMO 검토의견 반영 | 양경철 | 윤화병 |
| 1.00 | 2020.10.08 | 현업 검토 완료 | 양경철 | 윤화병 |
| 1.02 | 2020.11.12 | 개인정보 보안 관련 일정 현행화 | 양경철 | 윤화병 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table of Contents

[Table of Contents 3](#_Toc56085538)

[1. 목적 6](#_Toc56085539)

[1.1. 대상 6](#_Toc56085540)

[1.2. 관련 산출물 6](#_Toc56085541)

[2. 데이터베이스 서버 구성 정의 7](#_Toc56085542)

[2.1. 하드웨어 구성 7](#_Toc56085543)

[2.2. 소프트웨어 구성 7](#_Toc56085544)

[2.3. AS-IS 분석용 DBMS 8](#_Toc56085545)

[2.3.1. 설치 대상 8](#_Toc56085546)

[2.3.2. SYSTEM 및 DB 정보 8](#_Toc56085547)

[2.3.3. DBMS Default 사용 Port 8](#_Toc56085548)

[2.4. 선도장비 DBMS 9](#_Toc56085549)

[2.4.1. 설치 대상 9](#_Toc56085550)

[2.4.2. SYSTEM 및 DB 정보 9](#_Toc56085551)

[2.4.3. DBMS Default 사용 Port 9](#_Toc56085552)

[2.5. 개발기 DBMS 10](#_Toc56085553)

[2.5.1. 설치 대상 10](#_Toc56085554)

[2.5.2. SYSTEM 및 DB 정보 10](#_Toc56085555)

[2.5.3. DBMS Default 사용 Port 10](#_Toc56085556)

[2.6. 운영기 DBMS 11](#_Toc56085557)

[2.6.1. 설치 대상 11](#_Toc56085558)

[2.6.2. SYSTEM 및 DB 정보 11](#_Toc56085559)

[2.6.3. DBMS Default 사용 Port 11](#_Toc56085560)

[3. DBMS 명명 규칙 12](#_Toc56085561)

[3.1. 오브젝트 별 명명 규칙 12](#_Toc56085562)

[3.1.1. Database 명 12](#_Toc56085563)

[3.1.2. Instance 명 13](#_Toc56085564)

[3.1.3. Listener 명 13](#_Toc56085565)

[3.1.4. Profile 명 13](#_Toc56085566)

[3.1.5. Role 명 14](#_Toc56085567)

[3.1.6. ASM DiskGroup 명 14](#_Toc56085568)

[3.1.7. Partition Segment 명 15](#_Toc56085569)

[4. DBMS 구조 설계 16](#_Toc56085570)

[4.1. 파일시스템 정의 16](#_Toc56085571)

[4.2. 데이터파일 및 로그파일 정의 16](#_Toc56085572)

[4.3. DBMS 저장장치 구성 17](#_Toc56085573)

[4.4. 파라미터 설계 18](#_Toc56085574)

[4.5. DB계정 구성 정의 20](#_Toc56085575)

[5. DBMS 보안 21](#_Toc56085576)

[5.1. 보안 설계 요약 21](#_Toc56085577)

[5.2. 보안 설계 21](#_Toc56085578)

[5.2.1. 적극적인 통제의 프록시(Proxy) 운영방식 21](#_Toc56085579)

[5.2.2. 클라우드 환경을 위한 Software TAP 에이전트 구성 22](#_Toc56085580)

[5.3. DB 계정별 정책 22](#_Toc56085581)

[5.3.1. 개발기 22](#_Toc56085582)

[5.3.2. 운영기 22](#_Toc56085583)

[5.4. DBMS 서버 OS계정 22](#_Toc56085584)

[6. DBMS 백업 23](#_Toc56085585)

[6.1. 백업 정책 및 백업 주기 23](#_Toc56085586)

[6.2. 백업 방법 23](#_Toc56085587)

[6.3. 백업 계획 및 백업 구조 23](#_Toc56085588)

[6.4. 복원 계획 24](#_Toc56085589)

[6.4.1. 복구관련 확인 사항 24](#_Toc56085590)

[6.4.2. 유형별 복구 계획 24](#_Toc56085591)

[6.4.3. 유형별 복구 방법 24](#_Toc56085592)

[7. 현행시스템 분석 결과 26](#_Toc56085593)

[7.1. 현행시스템 분석 결과 26](#_Toc56085594)

[7.1.1. 총괄표 26](#_Toc56085595)

[7.1.2. 백업정책 28](#_Toc56085596)

[8. 스키마 접근 정책 및 데이터 보안 계획 30](#_Toc56085597)

[8.1. 스키마 접근 정책 30](#_Toc56085598)

[8.1.1. 기본 접근 정책 30](#_Toc56085599)

[8.1.2. Synonym 30](#_Toc56085600)

[8.1.3. Role 31](#_Toc56085601)

[8.1.4. 주요 스키마 별 계정정보 및 관련 Application 31](#_Toc56085602)

[8.2. 데이터보안 계획 33](#_Toc56085603)

[8.2.1. 데이터 암복호화 및 마스킹 처리 로직 33](#_Toc56085604)

[8.2.2. 개인정보 보안 관련 계획 34](#_Toc56085605)

# 목적

본 “아키텍처 정의서”는 SEMA차세대 정보시스템 구축 프로젝트에서 DBMS에 대한 아키텍처를 상세 설계함에 있어서 필요한 원칙과 기준을 정의하기 위하여 작성되었습니다.

## 대상

본 문서는 다음과 같은 역할을 수행하는 팀원을 대상으로 작성되었습니다.

* 과학기술인공제회 DBA/DA
* SEMA 차세대 정보시스템 구축팀 DBA/DA/모델러

## 관련 산출물

“아키텍처 정의서”에서 다루지 않는 데이터 표준과 관련된 내용이나 명영규칙, 예외사항, 데이터모델링가이드, SQL작성가이드는 “데이터 표준화 지침서”에 별도 작성하여 배포합니다.

# 데이터베이스 서버 구성 정의

## 하드웨어 구성

오라클 데이터베이스 서버는 아래의 표와 같이 구성합니다.

|  |  |  |
| --- | --- | --- |
| 구분 | 품번 | 제원 |
| 운영 | 통합 DBMS #1 | DELL R740 | * CPU : 2 \* Intel Xeon Gold 6244 (3.6 / 8C)
* MEM : 128(8 \* 16)GB Memory
* DISK : 2 \* 960GB RI SSD,
* NIC : Quad Port 1GbE rNDC, NIC(Quad Port 1GbE,
* 4 \* Dual Port 10Gb NIC (w/ GBIC)),
* HBA : 2 \* DP 16Gb FC HBA
 |
| 통합 DBMS #2 | DELL R740 | 상동 |
| 개발 | 개발 DBMS | DEL R640 | * CPU : 1 \* Intel Xeon Silver 42082 (2.1GHz / 8C)
* MEM : 64(4 \* 16)GB Memory
* DISK : 2 \* 960GB RI SSD
* NIC : 1Gb QP Base-T rNDC
* HBA : DP 16Gb FC HBA
 |
| 운영스토리지 | 유니파이드스토리지 | DELLUnity XT380F | * UNITY 380F DPE 25 X 2.5 DELL FLD RCK
* UNITY 380F DPE INSTALL KIT
* D4F 1.92TB ALL FLASH 25X2.5 SSD \* 26
* UNITY 2U 25X2.5 DAE FLD RCK AF
* UNITY CNA 4X10GBE OPT SFPS AF
* UNITY 2X4 PORT IO 16GB FC AF
* UNITY AFA BASE SOFTWARE=IC
* PROSUPPORT W/NBD-SOFTWARE SUPPORT
 |

## 소프트웨어 구성

|  |  |  |  |
| --- | --- | --- | --- |
| 구분 | 제품명 | 세부내역 | 수량 |
| DBMS | Oracle 19C | * Oracle Enterprise Edition 14PL(운영)
* Oracle RAC 16PL(운영)
* Oracle SE2 10NUP(개발)
 | 1 ea |
| 데이터표준화 | META | * WISE Meta v5.0
 | 1 ea |
| 모델링툴 | ERWIN | * Genesis ERWIN Data Modeler 2020 R1
 | Server 1 ea, Client 5 ea |
| DB 암호화 | D’Amo | * Tednet D’Amo
 |  |
| DB접근제어 | ChakraMax | * WareValley Chakra Max
 |  |
| DB모니터링 | Sherpa 4.2 | * Sherpa 4.2 for Oracle
 |  |

## AS-IS 분석용 DBMS

### 설치 대상

|  |  |  |
| --- | --- | --- |
| 구분 | 솔루션명 | 버전 |
| RDBMS | Oracle database Standard Edition | 11.2.0.4 |

### SYSTEM 및 DB 정보

|  |  |  |
| --- | --- | --- |
| 항목 | 내용 | 비고 |
| IP | 100.100.100.212 |  |
| Server Name | asisdev\_db |  |
| OS Version | CentOS 6.4 64bit |  |
| Version | 11.2.0.4.0 |  |
| Name | SEMADT | Database Name |
| Database Edition | Standard Edition |  |
| Database Home | /oracle/app/oracle/product/11g/dbhome\_1 |  |
| Inventory Location | /oracle/app/oraInventory |  |
| Block Size | 8192 |  |
| Listener Port | 1521 |  |
| Database Template | Custom Database |  |
| Base Dir | /oracle/app/oracle |  |
| Database Machines | SEMADT |  |
| Character Set | KO16MSWIN949 |  |
| National Charter Set | AL16UTF16 |  |

### DBMS Default 사용 Port

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Component | Discription | Protocol | Port | 비고 |
| Oracle Net Listener | Database Net Services | TCP | 1521 |  |
| Oracle Enterprise Manager Database Express | N/A | TCP | 5500 | EM 사용안함 |

## 선도장비 DBMS

### 설치 대상

|  |  |  |
| --- | --- | --- |
| 구분 | 솔루션명 | 버전 |
| RDBMS | Oracle database Standard Edition | 19c |

### SYSTEM 및 DB 정보

|  |  |  |
| --- | --- | --- |
| 항목 | 내용 | 비고 |
| IP | 100.100.100.222 |  |
| Server Name | tobedev\_db |  |
| OS Version | Redhat Enterprise Linux 7.8 64bit |  |
| Version | 19.0.9 |  |
| Name | SEMADT | Database Name |
| Database Edition | Standard Edition |  |
| Database Home | /oracle/app/oracle/product/19c/dbhome\_1 |  |
| Inventory Location | /oracle/app/oraInventory |  |
| Block Size | 8192 |  |
| Listener Port | 1521 |  |
| Database Template | Custom Database |  |
| Base Dir | /oracle/app/oracle |  |
| Database Machines | SEMADT |  |
| Character Set | KO16MSWIN949 |  |
| National Charter Set | AL16UTF16 |  |

### DBMS Default 사용 Port

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Component | Discription | Protocol | Port | 비고 |
| Oracle Net Listener | Database Net Services | TCP | 1521 |  |
| Oracle Enterprise Manager Database Express | N/A | TCP | 5500 | EM 사용안함 |

## 개발기 DBMS

### 설치 대상

|  |  |  |
| --- | --- | --- |
| 구분 | 솔루션명 | 버전 |
| RDBMS | Oracle database Standard Edition 2 | 19c |

### SYSTEM 및 DB 정보

|  |  |  |
| --- | --- | --- |
| 항목 | 내용 | 비고 |
| IP | 172.16.1.253 |  |
| Host Name | sdbxpd00 |  |
| OS Version | Redhat Enterprise Linux 7.8 64bit |  |
| Version | 19.8.0 |  |
| Name | SEMADT | Database Name |
| Database Edition | Standard Edition |  |
| Database Home | /app/oracle/product/19c/dbhome\_1 |  |
| Grid Home | /app/grid/19c/grid |  |
| Inventory Location | /app/oraInventory |  |
| Block Size | 8192 |  |
| Listener Port | 1521 |  |
| Database Template | Custom Database |  |
| Base Dir | /app/oracle |  |
| Grid Base Dir | /app/grid/base |  |
| Database Machines | SEMADT |  |
| Character Set | UTF-8 |  |
| National Charter Set | UTF-8 |  |

### DBMS Default 사용 Port

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Component | Discription | Protocol | Port | 비고 |
| Oracle Net Listener | Database Net Services | TCP | 1521 |  |
| Oracle Enterprise Manager Database Express | N/A | TCP | 5500 | EM 사용안함 |

## 운영기 DBMS

### 설치 대상

|  |  |  |
| --- | --- | --- |
| 구분 | 솔루션명 | 버전 |
| RDBMS | Oracle database Enterprise Edition, RAC | 19c |

### SYSTEM 및 DB 정보

|  |  |  |
| --- | --- | --- |
| 항목 | 내용 | 비고 |
| IP | 172.16.1.15 (RAC) |  |
| Server Name | sdbxpp01, sdbxpp02 |  |
| OS Version | Redhat Enterprise Linux 7.8 64bit |  |
| Version | 19.8.0 |  |
| Name | SEMADT | Database Name |
| Database Edition | Enterprise Edition |  |
| Database Home | /app/oracle/product/19c/dbhome\_1 |  |
| Grid Home | /app/grid/19c/grid |  |
| Inventory Location | /app/oraInventory |  |
| Block Size | 8192 |  |
| Listener Port | 1521 |  |
| Database Template | Custom Database |  |
| Base Dir | /app/oracle |  |
| Grid Base Dir | /app/grid/base |  |
| Database Machines | SEMADT |  |
| Character Set | UTF-8 |  |
| National Charter Set | UTF-8 |  |

### DBMS Default 사용 Port

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Component | Discription | Protocol | Port | 비고 |
| Oracle Net Listener | Database Net Services | TCP | 1521 |  |
| Oracle Enterprise Manager Database Express | N/A | TCP | 5500 |  |

# DBMS 명명 규칙

## 오브젝트 별 명명 규칙

데이터 관련 전사표준 기본 명명규칙입니다.

본 전사표준 규칙을 따를 것을 권장하고, 부득이한 경우, DBA와 협의하여 조정할 수 있습니다.

요약표는 다음과 같으며, 각 항목별로 상세 설명합니다.

Tablespace, Schema, User, Table, 등 모델과 관련있는 명명규칙은 데이터표준화지침서를 참고하시기 바랍니다.

|  |  |  |
| --- | --- | --- |
| 구분 | 리소스 /오브젝트 타입 | 내용 |
| Database | 데이터베이스 | * 전사약어명 + 시스템구분 [+ “\_” + DB환경구분(3)]
 |
| Instance | 인스턴스 | * Database명 [+ RAC노드번호]
 |
| Listener | 리스너 | * LISTENER or [“LSNR” + “\_” + Database명]
 |
| Profile | 프로파일 (Profile) | * “PROF” + "\_" + 구분약어 + "\_" + 사용자분류(3)
 |
| Role | 역할 (Role) | * “RL” + "\_" + 구분약어 + "\_" + 할당유형(3)
 |
| ASM DiskGroup | ASM Diskgroup | * “ADG” + “\_” + DB코드명 + “\_” + 볼륨그룹명 [+ 일련번호(2)]
 |
| Partition Segment | 파티션 세그먼트 | * “PS” + “\_” + 테이블명 + “\_” + 파티션유형 + 파티션분류내용
 |

### Database 명

Database명은 전사약어명(SEMA)와 시스템구분(DT)를 조합하여 명명하며, 추가적으로 환경구분에 따라 DB환경구분을 조합하여 명명이 가능합니다. (Database명은 최대 8자리까지 지원합니다.)

명명 규칙 : 전사약어명 + 시스템구분 [+ “\_” + DB환경구분(3)]

|  |  |  |  |
| --- | --- | --- | --- |
| 규칙 | 필수/옵션 | 내용 | 비고 |
| 전사약어명 | 필수 | 과학기술인공제회 전사시스템의 약어명 | SEMA |
| 시스템구분 | 필수 | Database의 구분명 | DT |
| DB환경구분 | 옵션 | 구성되는 데이터베이스의 환경 구분 | P : 운영환경D : 개발환경 |

명명 예시)

운영기 : SEMADT or SEMADT\_P

개발기 : SEMADT or SEMADT\_D

### Instance 명

Instance명은 Database명을 차용하여 사용하되, RAC로 구성하는 경우, RAC노드번호를 조합하여 명명할 수 있습니다.

명명 규칙 : Database명 [+ RAC노드번호]

|  |  |  |  |
| --- | --- | --- | --- |
| 규칙 | 필수/옵션 | 내용 | 비고 |
| Database명 | 필수 | 3.1.1.에서 명명된 Database명 |  |
| RAC노드번호 | 옵션 | RAC 노드 |  |

명명 예시)

SEMADT

SEMADT1, SEMADT2

### Listener 명

Listener명은 별도로 명명하지 않고, DBMS에서 제공하는 LISTENER를 그대로 사용하는 것을 권장합니다. 별도의 명명이 필요한 경우, 약어("LSNR")와 Database명을 조합하여 명명할 수 있습니다.

명명 규칙 : LISTENER or [“LSNR” + “\_” + Database명]

|  |  |  |  |
| --- | --- | --- | --- |
| 규칙 | 필수/옵션 | 내용 | 비고 |
| 약어 | 옵션 | LISTENER의 약어 | LSNR |
| Database명 | 필수 | 3.1.1.에서 명명된 Database명 |  |

명명 예시)

 LISTENER or LSNR\_SEMADT

### Profile 명

PROF는 Profile의 약자입니다.

명명 규칙 : “PROF” + "\_" + 구분약어 + "\_" + 사용자분류(3)

|  |  |  |  |
| --- | --- | --- | --- |
| 규칙 | 필수/옵션 | 내용 | 비고 |
| 약어 | 필수 | PROFILE의 약어 | PROF |
| 구분약어 | 필수 | 주제영역(L1) 혹은 스키마단위의 약어 등의 구분단어 |  |
| 사용자분류 | 필수 | 사용자에 대한 분류 | APP : ApplicationDEV : 개발자... |

명명 예시)

 PROF\_CORE\_APP, PROF\_CORE\_DEV

### Role 명

RL은 Role의 약자입니다.

명명 규칙 : “RL” + “\_” + 구분약어 + + “\_” + 할당유형(3)

|  |  |  |  |
| --- | --- | --- | --- |
| 규칙 | 필수/옵션 | 내용 | 비고 |
| 약어 | 필수 | ROLE의 약어 | RL |
| 구분약어 | 필수 | 주제영역(L1) 혹은 스키마단위의 약어 등의 구분단어 |  |
| 할당유형 | 필수 | 개체에 할당된 유형별 분류 | ALL : 전체권한 (CRUD)SEL : 조회Only... |

명명 예시)

 RL\_CORE\_ALL, RL\_CORE\_SEL

### ASM DiskGroup 명

ASM 구성시에만 적용합니다. ADG는 ASM Disk Group의 약자입니다.

명명 규칙 : “ADG” + “\_” + DB코드명 + “\_” + 볼륨그룹명 [+ 일련번호(2)]

|  |  |  |  |
| --- | --- | --- | --- |
| 규칙 | 필수/옵션 | 내용 | 비고 |
| DB코드명 | 필수 | 데이터베이스의 코드명 | SEMA |
| 볼륨그룹명 | 필수 | ASM 볼륨 그룹 명

|  |  |  |
| --- | --- | --- |
| 약어 | 내용 | 비고 |
| CRS | OCR/Voting Disk 정보 |  |
| DATA | 복구영역 (REDO / UNDO) | Fast Recovery Area |
| SYSTEM File 영역 |  |
| DATA 영역 |  |
| ARCH | ARCHIVE Log 영역 |  |

 |  |
| 일련번호 | 옵션 | 일련번호 2자리. 01부터 시작함 | 옵션 |

명명 예시)

 "CRS" DiskGroup 명 : ADG\_SEMA\_CRS or ADG\_SEMA\_CRS01

 "DATA" DiskGroup명 : ADG\_SEMA\_DATA or ADG\_SEMA\_DATA01

### Partition Segment 명

PS 는 Partition Segment의 약자입니다.

명명규칙 : “PS” + “\_” + 테이블명 + “\_” + 파티션유형 + 파티션분류내용

|  |  |  |  |
| --- | --- | --- | --- |
| 규칙 | 필수/옵션 | 내용 | 비고 |
| 약어 | 필수 | Partition Segment의 약어 | PS |
| 테이블명 | 필수 | 파티셔닝할 대상 테이블명 |  |
| 파티션유형 | 필수 | 파티셔닝 유형 명 | R : 범위 파티셔닝L : 목록 파티셔닝H : 해쉬 파티셔닝... |
| 파티션분류내용 | 필수 | 파티셔닝 분류에 대한 업무적인 명칭 |  |

명명 예시)

 PS\_AR\_ARR\_M\_R2009

# DBMS 구조 설계

## 파일시스템 정의

|  |  |  |
| --- | --- | --- |
| 분류 | 내용 | 비고 |
| Oracle account | oracle | DB Common |
| Oracle account ID | 301 | DB Common |
| Oracle account group | DBA | DB Common |
| Oracle group ID | 500 | DB Common |
| Oracle GRID | grid | Only when Oracle RAC is installed |
| Oracle GRID ID | 300 | Only when Oracle RAC is installed |
| Base directory | /app/oracle/ | $ORACLE\_BASE environment variable |
| Log directory | /log/oracle/ | Oracle Log location |
| Diagnostic dest | $ORACLE\_BASE |  |
| Inventory directory | /app/oraInventory | Oracle Inventory directory (orainventory) saves software inventory installed to the system Generated in the sub-directory of $ORACLE\_BASE |
| Home directory | $ORACLE\_BASE/product/19c/dbhome\_1/ | ORACLE\_HOME environment variable |
| Memory Allocation (GB) |  |  |
| :: SGA | Server Memory 40% | System Global Area |
| :: PGA | Server Memory 20% | Program Global Area |
| Character Set | UTF-8 | Supports Traditional Unicode |
| Control File | +ADG\_<DB코드명>\_DATA |  |
| Tablespace Path |  |  |
| :: UNDO | +ADG\_<DB코드명>\_DATA | UNDO\_MANAGEMENT : AUTO |
| :: SYSTEM | +ADG\_<DB코드명>\_DATA | System Area |
| :: TEMP | +ADG\_<DB코드명>\_DATA | Temp Area |
| :: DATA | +ADG\_<DB코드명>\_DATA | Data Area |
| :: INDEX | +ADG\_<DB코드명>\_DATA | Index Area |
| Archive Mode | /arch | Archive Mode |

## 데이터파일 및 로그파일 정의

데이터 파일과 인덱스 파일은 별도로 구성되며 시스템, UNDO, TEMP 테이블스페이스 영역과는 독립적인 테이블스페이스로 작성됩니다.

데이터 파일은 각 주제영역에 대해 별도의 테이블스페이스를 생성하여 관리합니다. 개발기 및 운영시스템은 모두 장애 발생시 효과적인 복구를 위하여 Archive모드로 생성됩니다.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 대분류 | 중분류 | 디스크 그룹 | ASM 파일 | 비고 |
| Log File | Redo Log | +ADG\_<DB코드명>\_DATA | <DB명>/ONLINELOG/group\_{sequence).{file}.%r |  |
| Archive Log | N/A | /arch/%t\_%s\_%r | %s : 로그일련번호%t : 쓰레드번호%r : incarnation resetlogs ID |
| Data File | Data File | +ADG\_<DB코드명>\_DATA | <DB명>/DATAFILE/{file}.%r | Data Area |
| Index File | +ADG\_<DB코드명>\_DATA | <DB명>/DATAFILE/{file}.%r | Index Area |
| Temp File | +ADG\_<DB코드명>\_DATA | <DB명>/DATAFILE/{file}.%r | Temp Area |

## DBMS 저장장치 구성

오라클에서는 Raw Device가 스토리지 장비로 지원되지 않습니다. (Oracle 12c 이후 버전)

운영기 DBMS는 RAC과 ASM이 동시에 구성됩니다. 디스크 그룹은 높은 중복성을 제공하기 위하여 멀티플렉스 구조로 설계되었습니다.

Database

Instance

Disk

O/S

**[ 개발기 DB ]**

**[ 운영기 DB ]**

RAC

Instance1

RAC

Instance2

Diskgroup1

Diskgroup2

ASM

Instance1

ASM

Instance2

RAC

## 파라미터 설계

|  |  |  |  |
| --- | --- | --- | --- |
| 종류 | 파라미터 | 권장 값 | 비고 |
| DBMS, Table & Partition | ADD\_COL\_OPTIM\_ENABLED | FALSE | column add 시 dictionary 먼저 update 하고 이후 insert시 해당 컬럼 생성 제어 |
| PARTITION\_LARGE\_EXTENTS | FALSE | Partition 생성시 Initial/Next Extent를 크게 생성1) TRUE: Extent의 크기를 8M 이상으로 생성2) FALSE: segment의 크기에 따라 64k/1M/8M/64M로 증가 |
| INDEX\_PARTITION\_LARGE\_EXTENTS | FALSE | Partition Index 의 initial/Next Extent를 크게 생성할지 지정 |
| DEFERRED\_SEGMENT\_CREATION | FALSE | Create 명령 수행 직후 table은 dictionary에만 등록되고, segment로는 만들어 지지 않으며, insert시에 segment 생성 |
| MAX\_STRING\_SIZE | standard | 12C에서 변경된 vARCHAR2, NVARTCHAR2, RAW의 maximum size of 를 변경 |
| RESOURCE\_MANAGER\_PLAN | ‘FORCE:’ | CPU, Active Session Count, PQ deg등 자원이 일별, 요일별 schedule 되는 것을 제어 |
| Critical Process | USE\_ADAPTIVE\_LOG\_FILE\_SYNC | FALSE | Log File Sync 수행 시 post/wait 과 polling 방식 선택 제어1) TRUE : post-wait과 polling 방식 중 adaprive2) FALSE : 기존 방식인 post-wait3) polling\_only : polling 방식 |
| USE\_SINGLE\_LOG\_WRITE | TRUE | Scalable LGWR 기능 제어 |
| UNDO | ROLLBACKUP\_SEGMENT\_COUNT | 1000 | Instance 구동과 동시에 Online 유지할 undo segment 개수 |
| CLEANUP\_ROLLBACK\_ENTRIES | 2000 | Transaction cleanup 수행 시 한번에 처리되는 undo entries 개수 |
| UNDO\_AUTOTUNE | TRUE | 자동으로 Tuning된 Undo Retention값의 사용여부를 결정 |
| HIGHTHRESHOLD\_UNDORETENTION | 4294967294 | Undo\_autotune=TRUE 설정 시 자동으로 조정되는 undo retention의 최대 값을 지정 |
| TEMP\_UNDO\_ENABLED | TRUE | Temporary object가 temporary undo를 사용 하도록 설정 |
| SGA | PX\_USE\_LARGE\_POOL | TRUE | Parallel query 수행 시 large pool 사용 여부 제어 |
| MEMORY\_IMM\_MODE\_WITHOUT\_AUTOSGA | TRUE | AMM/ASMM 기능을 disable한 경우라도 ORA-4031이 발생할 상황(immediate mode resize)에서 memory resize를 허용할지를 지정 |
| RESULT\_CAHCE\_MAX\_SIZE | Server Memory40% 지정 | SGA 내에 result cache가 사용할 메모리 총량을 바이트로 지정 |
| PGA\_AGGREGATE\_LIMIT | Memory부족으로hard limit필요시 설정 | instance의 PGA 사용량의 hard limit |
| RAC | PARALLEL\_FORCE\_LOCAL | TRUE | RAC환경에서 SQL 문장을 병렬 처리할 때, Cluster 전체 수준에서 처리를 할 것인지, 아니면 local instance에서만 수행할 것인지 지정- TRUE: local node에서만 사용 (instance\_groups, parallel\_instance\_group 제거- FALSE: instance\_groups, parallel\_instance\_group 설정 |
| Security | SYS\_LOGON\_DELAY | 1 | Brute force password attack을 방지하기 위해 login시에 비밀번호가 틀리면 일정시간 delay를 주는 기능 |
| AUDIT\_TRAIL | NONE | 권한, 문장 등에 대한 audit 설정 |
| Diag & Dump | NONFATALPROCESS\_REDO\_DUMP\_TIME\_LIMIT | 0 | Non fatal process, 즉 user process들에 의한 diagnostic redo dump 수행에 대한 시간 제어 |

## DB계정 구성 정의

오브젝트 소유자와 오브젝트 접근자는 별도로 관리합니다. 오브젝트 접근 권한은 Role로 부여되고 역할은 Application user에게 부여됩니다. 원칙적으로 개발자는 운영기에 접근할 수 없으며, 관리자도 운영기에서 조회만 가능합니다.

|  |  |  |
| --- | --- | --- |
| 분류 | 내용 | 비고 |
| 오브젝트 소유자 | Object 소유자 계정 |  |
| 응용프로그램 | 실제 응용프로그램에서 접근하는 계정. DDL 및 DCL권한 없음

|  |  |  |
| --- | --- | --- |
| 구분 | 권한 | 비고 |
| 전체권한자 | CRUD권한부여 | 응용프로그램 소유자 |
| 조회권한자 | 조회권한만 부여 | 타 응용프로그램 |

 | Role 기반으로 권한 관리 |
| 관리자 | 운영기 및 개발기에서 관리자에게 부여된 계정 | Role 기반으로 권한 관리 |
| 개발자 | 개발기에서 개발자에게 부여된 계정 | Role 기반으로 권한 관리 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 계정유형권한 | SYS /SYSTEM | DBA | 오브젝트소유자 | 응용프로그램 | 관리자개발자 |
| ALTER | O | O | O |  |  |
| CREATE | O | O | O |  |  |
| CREATE TMEPORARY TABLES | O | O | O |  |  |
| CREATE VIEW | O | O | O |  |  |
| DROP | O | O | O |  |  |
| EXECUTE | O | O | O | O |  |
| DELETE | O | O | O | O | O |
| INSERT | O | O | O | O | O |
| SELECT | O | O | O | O | O |
| UPDATE | O | O | O | O | O |
| TRIGGER | O | O | O |  |  |
| GRANT OPTION | O | O |  |  |  |
| ALL [PRIVILEGES] | O | O |  |  |  |
| CREATE USER | O | O |  |  |  |
| PACKAGE | O | O | O |  |  |
| FUNCTION | O | O | O |  |  |
| SHUTDOWN | O | O |  |  |  |

# DBMS 보안

## 보안 설계 요약

데이터베이스와 서버에 대한 네트워크 트래픽 분석 기반의 감사와 접근 통제 기능을 제공하고, 동시에 서버 측 보안 에이전트를 통해 콘솔 작업이나 원격지를 우회한 로컬 작업에 대한 통제도 가능합니다.

일반적으로 정형화된 접근이 이뤄지는 애플리케이션과 데이터베이스 구간은 서비스 운영에 부하가 없도록 스니핑을 통한 감사 환경을 구성하며, 적극적인 통제가 필수적인 비정형 사용자와 데이터베이스 구간은 프록시를 통한 접근제어를 제공합니다.

이와 같이 **에이전트, 스니핑, 프록시**의다양한 운영방식을 지원하여 효과적인 정보보안 활동이 가능합니다

## 보안 설계

### 적극적인 통제의 프록시(Proxy) 운영방식

클라이언트에서 전송된 입/출력 데이터는 모두 프록시 서버의 검증을 받아 사전 통제가 가능하며,

서버로부터 클라이언트로 전송되는 데이터는 중요 정보를 마스킹하거나 조회 시도를 제어하는 구성으로 설계됩니다.

* 네트워크 방화벽을 이용한 우회 접속 통제
* 데이터베이스와 서버 운영체제의 소프트웨어 방화벽을 이용한 우회 접속 통제
* Chakra Max 스니핑 서버의 통제 기능을 활용한 우회 접속 통제



### 클라우드 환경을 위한 Software TAP 에이전트 구성

네트워크 구간의 Sniffing 구성이 용이하지 않는 경우, 보호대상 서버에 Chakra Max Software TAP 에이전트를 설치하여 통신 내역을 확보하고 분석하는 구성을 적용하며, 해당 에이전트는 네트워크 TAP 장비와 같이 데이터베이스 또는 서버의 통신 내역을 Chakra Max 서버로 전송하는 역할을 수행합니다.

## DB 계정별 정책

### 개발기

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 분류 | 정책 | 권한 | 변경주기 | 비고 |
| 개발자 계정 | 개발자별 발급 | Data CRUD | N/A |  |
| 관리자 계정 | 관리자별 발급 | Table CUD / Data CRUD | N/A |  |
| AP 계정 | AP별 발급 | Table CUD / Data CRUD | N/A | AP별 차등 적용 가능 |
| 운영자 계정 | DBMS별 1개 발급 | DB/Table/Data CRUD | N/A |  |
| 암호 | 각 계정별로 유일하게 발급 | N/A | N/A |  |

### 운영기

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 분류 | 정책 | 권한 | 변경주기 | 비고 |
| 개발자 계정 | 발급 불가 | N/A | N/A |  |
| 관리자 계정 | 각 업무별 1개 발급 | Data Read | N/A |  |
| AP 계정 | AP별 발급 | Data CRU | N/A | AP별 차등 적용 가능 |
| 운영자 계정 | DBMS별 1개 발급 | DB/Table/Data CRUD | N/A |  |
| 암호 | 각 계정별로 유일하게 발급 | N/A | 3 개월 |  |

## DBMS 서버 OS계정

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| OS계정 | Uid | GroupName | Gid | Shell | 보안 | 비고 |
| oracle | 3001 | dba | 301 | /bin/hash | 원격접속 불가 |  |

# DBMS 백업

## 백업 정책 및 백업 주기

데이터 변경에 대한 양과 빈도에 따라서 DB백업 방법과 주기를 결정해야 합니다. 중요 데이터의 실시간 백업을 유지하고 DB의 장애 이후 최소시간 내에 데이터를 완벽하게 복구할 수 있도록 구성해야 합니다.

|  |  |  |
| --- | --- | --- |
| 분류 | 백업 미디어 및 방법 | 백업 주기 |
| 데이터 | 백업소프트웨어를 사용하여 온라인 RMAN 백업 | 일단위, 주단위 |
| 아카이브 로그 | 백업소프트웨어를 사용하여 RMAN 백업 | 일단위, 주단위 |
| 덤프 파일 | 백업영역에서 덤프작업후 소프트웨어를 사용하여 백업 | 일단위, 주단위 |

## 백업 방법

|  |  |  |
| --- | --- | --- |
| 백업 유형 | 백업 범위 | 비고 |
| Export 백업 | 전체 백업, 특정 스키마, 특정 테이블 | 논리적 백업 |
| RMAN 백업 | Control 파일, 데이터 파일, 아카이브 파일, 등 | 물리적 백업 |

## 백업 계획 및 백업 구조

주요 비즈니스 데이터베이스는 비즈니스 서버에 부하를 주지 않는 방식으로 백업해야 합니다. 현재 정확한 백업 시간을 계산할 수 없으므로, 백업 방법, 목표 시간, 실행 시간은 나중에 확정해야 합니다.

**백업솔루션을 이용한
RMAN BACKUP**

**SEMIS DB**

**VTL**

**Clone**

## 복원 계획

### 복구관련 확인 사항

|  |  |  |
| --- | --- | --- |
| 분류 | 체크 포인트 | 비고 |
| 복구 전 체크 | - 시스템 장애 또는 시스템 업그레이드시 전체 백업 수행- 정확한 고장 발생 시간 기록- 현재 백업 버전, 최신 백업 버전 및 아카이브 확인- 장애유형 파악 및 적절한 복구계획 수립 |  |
| 복구 후 체크 | - 복구 완료 후 정상적으로 DB를 종료하고 재시작하여 DB를 확인함- 데이터 및 스키마 확인과 함께 현재 DB 전체 백업 수행 |  |

### 유형별 복구 계획

#### 사용자 실수로 인한 장애

|  |  |  |
| --- | --- | --- |
| 복구 유형 | 복구 조치 방법 | 복구 계획 |
| DROP | - Recyclebin 기능을 이용하여 테이블 복구- 이중화 처리된 데이터를 이용하여 데이터베이스 복구 | FlashBack시점 복구 |
| DELETE | - FlashBack 기능을 이용하여 손실된 데이터를 복구(Undo 상태에 따라서 복구가 불가능 할 수 있음)- 이중화 처리된 데이터를 이용하여 데이터베이스 복구 | FlashBack시점 복구 |

### 유형별 복구 방법

#### ControlFile 복구

|  |  |  |
| --- | --- | --- |
| 분류 | 복구 방법 | 비고 |
| DB ControlFile 복구 | - DB nomount 상태로 전환 |  |
| - Networker 로 받은 ControlFile 복구 |  |

#### DataFile 복구

|  |  |  |
| --- | --- | --- |
| 분류 | 복구 방법 | 비고 |
| DB Data File 복구 | - DB 재 마운트 |  |
| - RMAN 모드에서 DB 데이터 확인 |  |
| - 시점 복구시 SET UNTIL TIME "TO\_DATA 옵션 추가- restore datafile : 데이터 파일 별로 복구시 사용- DataFile 복구 |  |

#### Archive 복구

|  |  |  |
| --- | --- | --- |
| 분류 | 복구 방법 | 비고 |
| DB Archive 복구 | - RMAN 모드 진입 후 필요한 Archivelog 의 시퀀스 번호를 확인 |  |
| - Archivelog 시퀀스 번호 xx 부터 xx 까지 복구 실행 |  |
| - DB recover 진행 |  |

# 현행시스템 분석 결과

분석 단계 감리 권고 및 필수사항으로 현행시스템 총괄표 및 데이터 보안계획을 첨부합니다.

자세한 내용은 “DA\_DA\_A\_01\_현행시스템분석서.docx”를 참고하세요.

## 현행시스템 분석 결과

### 총괄표

현행시스템 분석 결과 총괄 사항은 아래와 같으며,
자세한 이슈사항 및 현황은 “DA\_DA\_A\_01\_현행시스템분석서.docx”를 참고하세요.

#### DBMS Hardware 상세 내역

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 시스템명 | CPU | 메모리 | 디스크 | IP | 비고 |
| 통합DB01 | IBM POWER7 3108 MHz \* 8 | 20 GB | 146GB \* 2EA600GB \* 2EA | 203.250.240.71 |  |
| 통합DB02 | IBM POWER7 3108 MHz \* 8 | 20 GB | 146GB \* 2EA600GB \* 2EA | 203.250.240.72 |  |

#### DBMS Software 상세 내역

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 시스템명 | 항목 | 제품명 | 설치경로 | 비고 |
| 통합DB01 | Cluster | HACMP 6.1 | /usr/es/sbin/cluster |  |
|  | DBMS | Oracle 11 R2 | /engn001/product/11.2 |  |
|  | 백업SW | EMC Networker V8.1 | /opt/nsr |  |
|  | OS보안 | RedCastle v2.0 | /usr/local/redcastle/ |  |
|  | 보안 | D’amo | /home/maxgauge |  |
| 통합DB02 | Cluster | HACMP 6.1 | /usr/es/sbin/cluster |  |
|  | DBMS | Oracle 11 R2 | /engn001/product/11.2 |  |
|  | 백업SW | EMC Networker V8.1 | /opt/nsr |  |
|  | OS보안 | RedCastle v2.0 | /usr/local/redcastle/ |  |

#### 테이블스페이스

|  |  |  |  |
| --- | --- | --- | --- |
| 테이블스페이스 | 관련파일명 | 관련 주요 스키마 | 비고 |
| BIZI\_DATA | bizi\_data.dbf |  |  |
| BIZI\_IDXES | bizi\_idxes.dbf |  |  |
| BIZI\_LOGS | bizi\_logs.dbf |  |  |
| ITSM\_CLOB | itsm\_clob.dbf | ITSM |  |
| ITSM\_DT | itsm\_dt.dbf | ITSM |  |
| ITSM\_IX | itsm\_ix.dbf | ITSM |  |
| SHERPA\_TBS | sherpa\_tbs.dbf |  |  |
| SYSAUX | sysaux01.dbf |  | Oracle |
| SYSTEM | system01.dbf |  | Oracle |
| TS\_DAM01 | ts\_dam01.dbf | SEMA\_OWN |  |
| TS\_DAMO | ts\_damo.dbf | DAMO |  |
| TS\_DCMS01 | ts\_dcms01.dbf | SEMA\_CMS |  |
| TS\_DCO01 | ts\_dco01.dbf | SEMA\_MSG, SEMA\_OWN |  |
| TS\_DEX01 | ts\_dex01.dbf | SEMA\_OWN, SEMA\_WCMS |  |
| TS\_DFI01 | ts\_dfi01.dbf | SEMA\_OWN |  |
| TS\_DFSS | ts\_dfss.dbf | SEMA\_FSS |  |
| TS\_DHOME01 | ts\_dhome01.dbf |  |  |
| TS\_DHP01 | ts\_dhp01.dbf |  |  |
| TS\_DHR01 | ts\_dhr01.dbf | SEMA\_OWN |  |
| TS\_DIM01 | ts\_dim01.dbf | SEMA\_OWN |  |
| TS\_DKFB | ts\_dkfb.dbf | SEMA\_KFB |  |
| TS\_DML01 | ts\_dml01.dbf | MAIL |  |
| TS\_DMT01 | ts\_dmt01.dbf, ts\_dmt01\_1.dbf | SEMA\_KT, SEMA\_OWN |  |
| TS\_DPT01 | ts\_dpt01.dbf | PORTAL |  |
| TS\_DRP01 | ts\_drp01.dbf, ts\_drp01\_1.dbf | SEMA\_OWN |  |
| TS\_DRP02 | ts\_drp02.dbf, ts\_drp02\_1.dbf | SEMA\_OWN |  |
| TS\_DSHOME01 | ts\_dshome01.dbf | SEMA\_SHOME |  |
| TS\_ERP\_DATA | ts\_erp\_data.dbf |  |  |
| TS\_ERP\_IDX | ts\_erp\_idx.dbf |  |  |
| TS\_GSITM | ts\_gsitm.dbf |  |  |
| TS\_IAM01 | ts\_iam01.dbf |  |  |
| TS\_ICMS01 | ts\_icms01.dbf |  |  |
| TS\_ICO01 | ts\_ico01.dbf |  |  |
| TS\_IEX01 | ts\_iex01.dbf |  |  |
| TS\_IFI01 | ts\_ifi01.dbf |  |  |
| TS\_IHOME01 | ts\_ihome01.dbf |  |  |
| TS\_IHP01 | ts\_ihp01.dbf |  |  |
| TS\_IHR01 | ts\_ihr01.dbf |  |  |
| TS\_IIM01 | ts\_iim01.dbf |  |  |
| TS\_IML01 | ts\_iml01.dbf |  |  |
| TS\_IMT01 | ts\_imt01.dbf |  |  |
| TS\_IPT01 | ts\_ipt01.dbf |  |  |
| TS\_IRP01 | ts\_irp01.dbf | SEMA\_OWN |  |
| TS\_IRP02 | ts\_irp02.dbf |  |  |
| TS\_ITSM | ts\_itsm.dbf |  |  |
| TS\_SECOM01 | ts\_secom01.dbf | SEMA\_SECOM |  |
| UNDOTBS1 | undotbs1.dbf |  | Oracle |
| USERS | users01.dbf |  | Oracle |

#### 스키마정보

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 스키마 | 테이블수 | 내용 | 특이사항 | 비고 |
| DAMO |  |  |  |  |
| ERP | 159 | ERP |  |  |
| ITSM | 194 | IT서비스관리 |  |  |
| MAIL | 66 | 메일 |  |  |
| PORTAL | 291 | SSO, 포탈 |  |  |
| SEMA\_CMS | 26 | 금감원 CMS연계 |  |  |
| SEMA\_FSS | 7 | 연금포털 |  |  |
| SEMA\_HOME | 47 | 홈페이지(구) |  |  |
| SEMA\_KFB | 5 | 은행연합회 연계 |  |  |
| SEMA\_KT | 18 | SMS, MMS, FMS, VMS 연계 |  |  |
| SEMA\_MSG | 3 | 카카오톡, SNS용 |  |  |
| SEMA\_OWN | 1093 | 업무시스템용 |  |  |
| SEMA\_SECOM | 4 | SECOM |  |  |
| SEMA\_SHOME | 126 | 홈페이지(신) |  |  |
| SEMA\_WCMS | 2 | 우리은행 CMS 연계 |  |  |

### 백업정책

#### 백업장비 및 소프트웨어 현황

|  |  |  |
| --- | --- | --- |
| 구분 | 내용 | 도입시기 |
| 가상 백업 장비 | VTL : EMC DL4106 30TB | 2009.11 |
| 물리 백업 장비 | PTL : Overland NEO4000e - LTO-5, 2 Drive, 60 Slot | 2012.05 |
| 백업 솔루션 | EMC Networker - Host data, NAS, Database 백업용 | 2013.12 |

#### 대상 자료별 백업 방법

|  |  |  |  |
| --- | --- | --- | --- |
| 구분 | 내용 | 용도 | 보관주기 |
| Database | RMAN / Networker | Instance 단위 복원 | 1개월 |
| Hot Backup / Networker | Instance 단위 복원 | 1개월 |
| Export, data pump / Networker | 일부 데이터 확인 및 복원 | 로그 : 3년백업 : 1개월 |
| File System | Networker | File 단위 복원 | 1개월 |
| Rsync | 재해복구 | 최근 파일 |
| Networker | File 단위 복원 | 1개월 |
| Xcopy / TiSync | 재해복구 | 최근파일 / 1개월 |

#### 데이터 동기화 도구 및 방법

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 대상 | 동기화 도구 | 동기화 주기 | 동기화 용량 | 복원방법 | 복원시간 |
| Oracle | Export | 1일 / Full | 12GB / 30GB | Import | 2시간 / 30분 |
| NFS | Rsync | 1일 / Incremental | 3.5 TB / 1.6 TB / 250 GB | NFS mount | 10분 이내 |
| CIFS | Xcopy / TiSync | 1일 / incremental | 3 TB | 볼륨 mount | 10분 이내 |

# 스키마 접근 정책 및 데이터 보안 계획

## 스키마 접근 정책

### 기본 접근 정책

기본적으로 오브젝트를 소유한 계정은 Application에게 제공하지 않으며, DML권한을 소유한 계정을 추가로 생성하여 Application이 그 계정을 기반으로만 접근이 가능토록 하게 합니다.

(단, 메타시스템이나 보안솔루션 등 단위 솔루션이나 제품 등은 해당 솔루션의 정책을 따릅니다.)

예를 들어, ‘회원사업’의 시스템 약어가 CORE라면, 스키마는 SEMA\_CORE로 생성되게 되며, CRUD가 가능한 전체권한자는 CORE, 조회만 가능한 조회권한자는 CORE\_VWR으로 구성되게 됩니다. 조회권한자 생성은 필수가 아니며, 필요시 생성할 수 있습니다.

보통 Application 별 1개의 스키마를 소유하며, Application에서는 “전체권한자” 계정으로 엑세스하게 됩니다.

과학기술인공제회 내의 다른 Application은 “조회권한자” 계정으로 엑세스하여 조회만 가능하도록 합니다.

조회권한만

부여

(테이블)

(스키마) SEMA\_CORE

(테이블)

(테이블)

**(소유자)**

**SEMA\_CORE**

**(전체권한자)**

**CORE**

**(조회권한자)**

**CORE\_VWR**

**(Application)**

**회원사업**

**과학기술인공제회**

**다른 (Application)**

접근

접근

CRUD권한

부여

CRUD

조회

### Synonym

DB오브젝트는 각자 고유한 이름이 존재합니다. 이 오브젝트들을 위와 같은 여러 종류의 계정을 주고, 개별 접근 정책을 용이하게 할 수 있는 것이 Synonym입니다.

GRANT와 PRIVATE Synonym을 사용하여, 임의사용자에 대한 참조를 방지하고, GRANT와 PUBLIC Synonym을 이용하여, 복잡한 데이터연계를 방지합니다.

본 프로젝트에서는 GRANT와 Synonym을 이용하여, 데이터를 보다 유연하게 접근할 수 있으면서 개선된 보안이 적용될 수 있도록 합니다.

(테이블)

(스키마) SEMA\_CORE

(테이블)

(테이블)

**회원사업**

**(전체권한자)**

**CORE**

**Synonym**

PRIVATE Synonym

(테이블)

(스키마) SEMA\_ERP

(테이블)

(테이블)

**경영지원**

**(전체권한자)**

**ERP**

**Synonym**

PRIVATE Synonym

**Synonym**

PUBLIC Synonym

### Role

Role이란 하나 이상의 권한으로 이루어진 권한그룹입니다.

스키마별 전체권한자 및 조회권한자에 대한 사용자Role을 정의하여, 복잡해진 데이터베이스 권한관리에 대한 권한부여와 회수를 용이하도록 구성합니다.

### 주요 스키마 별 계정정보 및 관련 Application

현재 도출된 주요 스키마 별 계정정보 및 관련 Application입니다.

별도의 솔루션 및 제품군은 제외하였습니다.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 스키마 | 소유자 | 전체권한자 | 조회권한자 | 관련 Application | 비고 |
| SEMA\_WEB | SEMA\_WEB | WEB | n/a | 홈페이지 |  |
| SEMA\_ORG | SEMA\_ORG | ORG | n/a | 기관포털 | 폐기 |
| SEMA\_CORE | SEMA\_CORE | CORE | CORE\_VWR | 회원사업 |  |
| SEMA\_NF14 | SEMA\_NF14 | NF14 | NF14\_VWR | 자산운용 |  |
| SEMA\_ERP | SEMA\_ERP | ERP | ERP\_VWR | 경영지원 |  |
| SEMA\_STAT | SEMA\_STAT | STAT | STAT\_VWR | 통계 |  |
| SEMA\_ADUIT | SEMA\_ADUIT | ADUIT | ADUIT\_VWR | 감사 |  |
| SEMA\_EDMS | SEMA\_EDMS | EDMS | n/a | EDMS | 별도 솔루션 |
| SEMA\_SECOM | SEMA\_SECOM | SECOM | n/a | SECOM | 별도 솔루션 |
| SEMA\_GRP | SEMA\_GRP | n/a | n/a | 그룹웨어 | 별도 솔루션 |
| SEMA\_SSO | SEMA\_SSO | SSO | n/a | 통합인증 | 별도 솔루션 |
| SEMA\_CRM | SEMA\_CRM | CRM | n/a | 회원상담 |  |
| SEMA\_MCA | SEMA\_MCA | MCA | n/a | 기준정보 |  |
| SEMA\_META | SEMA\_META | META | n/a | 메타시스템 | 별도 솔루션 |
| SEMA\_ERWIN | SEMA\_ERWIN | ERWIN | n/a | 모델링 | 별도 솔루션 |
| SEMA\_DAMO | SEMA\_DAMO | DAMO | n/a | 암복호화 | 별도 솔루션 |
| SEMA\_ADPM | SEMA\_ADPM | ADPM | n/a | 성능모니터링 | 별도 솔루션 |
| SEMA\_BATCH | SEMA\_BATCH | BATCH | n/a | 배치 |  |
| SEMA\_EAI | SEMA\_EAI | EAI | n/a | 전사통합 | 별도 솔루션 |
| SEMA\_MSG | SEMA\_MSG | MSG | n/a | SNS,SMS |  |
| SEMA\_LGUFAX | SEMA\_LGUFAX | n/a | n/a | LG U+ 웹팩스 | 별도 솔루션 |

## 데이터보안 계획

### 데이터 암복호화 및 마스킹 처리 로직

데이터 암복호화는 D’amo API서비스를 이용하여 프레임워크 측에서 암복호화 처리를 진행하며, 데이터베이스상에서는 암복호화 처리를 하지 않습니다.

**Application**

**Frame**

**Work**

(테이블)

고객정보가 포함된 테이블

(테이블)

해제요청

정보

암/복호화 기준 정보

표준속성

정보

Service

Bean

DAO

1.2. 암호화 또는 마스킹 리턴

**1.1. 일반 정보 요청**

**2.1. 마스킹 해제 요청 조회**

2.2. 마스킹 해제 정보 리턴

372-\*\*\*\*\*\*\*-02

372-1234567-02

*25cfe946c9ec8020bf83a9a9e304d2e0*

*25cfe946c9ec8020bf83a9a9e304d2e0*

*25cfe946c9ec8020bf83a9a9e304d2e0*

내부단말

해제

암/복호화 작업은 Framework에서 처리하며, 암복호화되어 저장된 데이터를 복호화하여 평문으로 복원하거나 마스킹 유형에 따라 평문을 마스킹 처리된 값으로 변경하는 작업을 합니다.

서버와 UI 업무개발자는 대상 컬럼 대한 암/복호화 처리에 관여하지 않습니다.

다만, 암복호화 처리를 위한 대상 컬럼과 기준정보를 Configuration Portal에 등록합니다.

#### Framework에서 암/복호화 및 마스킹 처리 절차

1. In/Out 항목 중 표준속성에 ‘암호화, 마스킹’ 대상 컬럼이 있는지 조사
2. 암호화, 마스킹 처리 대상이 존재한다면,
	1. 요청헤더에 해제요청 정보가 있는지 확인하고,
		1. 해제요청 정보가 있다면, 복호화 후 마스킹 처리 안함 (평문 리턴)
		2. 해제요청 정보가 없다면, 복호화 후 마스킹 처리 수행 (마스킹된 값 리턴)
3. 암호화, 마스킹 처리 대상이 아니라면,
	1. 암/복호화 로직 SKIP (아무 처리 안 함)

### 개인정보 보안 관련 계획

개인정보 보안과 관련하여 암/복호화 대상 컬럼과 암호화 방법은 선정하고, 대상 컬럼에 대한 물리ERD및 물리 테이블을 조정한 후 암/복호화 모듈 설계 및 개발을 진행합니다. 이후 암/복호화 관련 단위테스트를 진행하고 사후모니터링을 진행하며, 통합테스트는 업무팀의 통합테스트와 맞물려 같이 진행하도록 하겠습니다.

11월초에 개발장비가 도입되고, 개발장비의 환경이 준비되는 동안, 암호화 모듈과 개인정보영향평가가 진행됩니다. 이후 암호화 대상 및 방법을 선정하고 암복호화 모듈을 설계합니다. 개발장비가 정상적으로 준비되어 업무팀의 개발환경을 제공을 완료한 후 프레임워크에서 암/복호화 모듈을 개발하는 일정으로 진행합니다. 예상 일정은 다음과 같습니다.

**2020년 12월**

**2021년 02월**

**2020년 1월**

3

4

5

1

2

3

4

1

2

3

4

암호화 대상 컬럼 선정

암호화

방법 선정

ERD 모델

조정

암/복호화

모듈 설계

암/복호화

모듈 개발

단위테스트

**암호화 대상**

**컬럼 선정**

**암호화**

**방법 선정**

**모델 조정**

**암/복호화**

**모듈 설계**

**암/복호화**

**모듈 개발**

**테스트**

|  |  |  |  |
| --- | --- | --- | --- |
| 단계 | 예상 일정 | 방법 | 담당자 |
| 암호화 대상 컬럼 선정 | 12월 3주차 (1주)(2020.12.14 ~ 2020.12.18) | 현행 암호화컬럼의 TO-BE 이행컬럼을 포함하여,신규 대상 컬럼 추출 후 검토 | DA /SEMA |
| 암호화 방법 선정 | 12월 4주차 (1주)(2020.12.21 ~ 2020.12.24) | 선정된 암호화 컬럼에 대하여,암호화 방법을 선정 | SEMA |
| 모델 조정 | 12월 5주차 (1주)(2020.12.28 ~ 2020.12.31) | 암호화 방법별 변경되는 모델을 체크하고,물리ERD, 메타시스템, DBMS 조정 | DA |
| 암/복호화 모듈 설계 | 1월 1주차 (1주)(2021.01.04 ~ 2021.01.08) | 암/복호화 대상에 대한 범위 및 방법을 확인하고,적합한 구성 및 설계 진행 | AA |
| 암/복호화 모듈 개발 | 1월 2주차 (5주)(2021.01.11 ~ 2020.02.10) | 프레임워크에 암/복호화 모듈 개발 | 인프라 |
| 암/복호화 단위테스트 | 2월 3주차 (2주)(2021.02.15 ~ 2021.02.26) | 암/복호화 모듈에 대한 단위테스트 실시 | 인프라 |
| 사후관리 | 이후 계속 |  | 인프라 |
| 통합테스트 | 업무팀 통합테스트 포함 | 업무팀 통합테스트시 포함하여 테스트 진행 | 전체 |