

1. DB 접근제어 / System 접근제어 (GS 인증, 국제 CC, 조달)
2. Gateway, Sniffing, Hybrid, Agent 운영 / 이중화 운영 / 클라우드/ NoSQL/ MAC
3. 작업결재 - 사전/사후/다단계/대리/제3자 실행 / 서버 접근 및 작업결재
4. Dynamic Data Masking / 사전사후 데이터 기록 / 콘솔로깅
5. 우회접속차단 / 로컬 접속 감시통제 / 사용자 파일저장 통제
6. 사용자 2-Fact 인증 / 가상 계정 통제 / 인증키 로그인
7. 통신구간 암호화 / 감사로그 암호화 / DB통신채널 (SSL/TLS) 암호화 연결

Chakra MAX V2 – DB & System 접근제어 솔루션

WAREVALLEY

DBMS, Database Management and Security

<http://www.warevalley.com>

1. 웨어밸리 – Innovative Data Solution



“데이터베이스 솔루션 기업”

(주)웨어밸리 – WAREVALLEY, Since 2001

<http://www.warevalley.com>

서울 마포구 상암동 누리꿈스퀘어 비지니스타워 22F
DBMS, DB보안(접근제어, 암호화, 취약점분석),
DB 운영관리 및 성능관리 솔루션 개발
전세계 3,500 고객사 / 400,000 사용자

Gartner

Hype Cycle for Application Security, 2016

🕒 13 July 2016 | ... Fortinet; HexaTier; IBM; Imperva; McAfee; Mentis; Oracle; Trustwave;

WareValley Recommended Reading: Analysis By: Jonathan Care; Avivah Litan ...

Analyst(s): Ayal Tirosch

Hype Cycle for Data Security, 2016

🕒 13 July 2016 | ... Fortinet; HexaTier; IBM; Imperva; McAfee; Mentis; Oracle; Trustwave;

WareValley Recommended Reading: Analysis By: John Girard Definition: Interoperable ...

Analyst(s): Brian Lowans

가트너 2012년 ~ 2019년 8년 연속 선정 ;

- 아시아 DB보안 선두 기업
- 전세계 7개 주요 DB보안 벤더 중 하나
- DB보안 모든 Portfolio 제공

Gartner 2012-2019

- Leader of Database Security
- One of Global Top 7 Vendors
- Owns full portfolio of Database security and management

Market Definition

Analysis

Competitive Situation and Trends

Market Trends

Market Players

The Future of Competition

Competitive Profiles

Application Security

BeyondTrust

IBM InfoSphere Guardium

Imperva

McAfee (A Division of Intel)

Oracle

WareValley

References and Methodology

Gartner Recommended Reading

1. 웨어밸리 – Innovative Data Solution

DB 솔루션	제품명	설명
DB-System 접근통제	 CHAKRA MAX	Enterprise급 규모의 DB 및 Server 접근 통제/감사
DB 암호화	 GALEA	Column-Level (Plug-in, API) 방식의 DB 암호화
DB 작업결재	 CHAKRA MAX	DB Tool, DB 종류에 상관없는 강력한 DB 작업결재
	 Trusted ORANGE	Orange 사용자 기반의 강력한 DB 작업결재
개인정보스캔 DB 취약점 분석	 CYCLONE	개인정보 모니터링, DBMS의 취약점 Scan (모의해킹 및 내부감사)
DB 관리 및 개발	 ORANGE	DB 성능 모니터링 및 개발 지원 도구
DBMS	 PetaSQL	빅데이터 분석/데이터웨어하우스/데이터 마트/실시간 로그 분석
통합 로그관리	 LOG_CATCH	개인정보 접속이력 관리 및 이상징후 감지 및 소명 관리
DB 수집 및 활용	 Peta INSIGHT	이기종 데이터베이스간 실시간 데이터 복제 및 활용

데이터보안인증(DQC-S)에 완벽대응

- 접근통제(Level 1) / 암호화(Level 2) / 작업결재(Level 3) / 취약점 분석(Level 4)
- 인증기관 : 한국 데이터베이스 진흥원

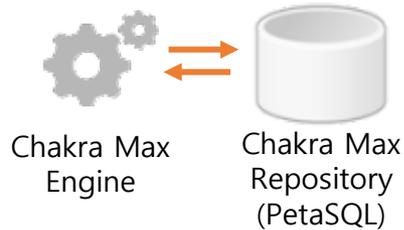
데이터보안 진단 컨설팅

- 한국데이터베이스진흥원의 데이터 품질관리 지침(Ver2.1)과 데이터 품질관리 성숙모형(Ver1.0)을 기준으로 하여 '데이터베이스 품질관리 인증서'를 받을 수 있도록 정확하고 신속하게 컨설팅 지원

2. 제품 구성 | 제품 구성

DB접근제어 서버

Chakra Max Server



보안 정책 관리 / 적용

DB & System 작업 감사 데이터 로깅

보안 시스템 운영 현황 모니터링

DB접근제어 관리자

Chakra Max Manager Program



접근제어 관리자

DB / System / 사용자 / 그룹 관리

보안 정책 설정(결재/차단/경보)

실시간 모니터/보고서 생성

DB사용자 Client

Chakra Max Client Program



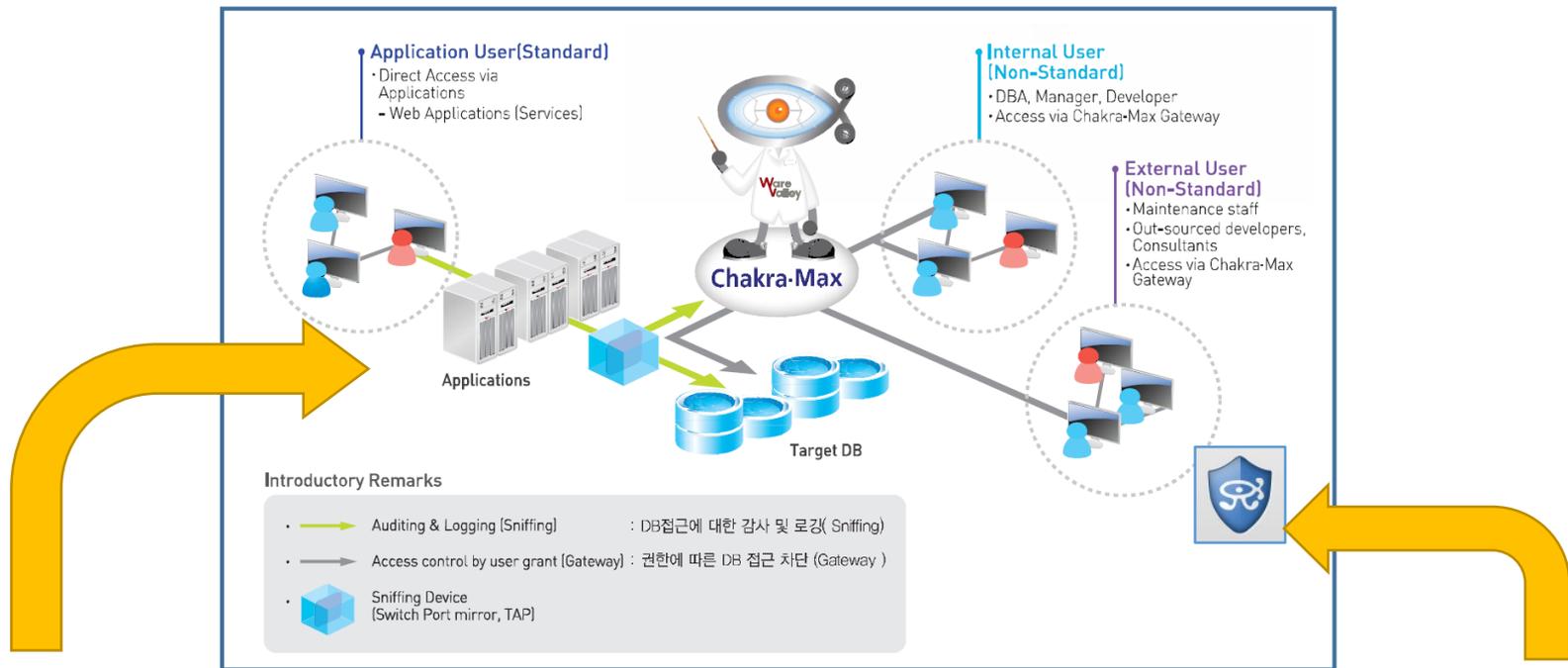
DB 사용자

DB / System 직접 접속 통제

기안 / 승인 / 진행 상태 조회 및 관리

개인 정보 관리 / 파일저장통제

2. 제품 구성 | 시스템 구성



Sniffing mode

중요 DB 접근에 대한 실시간 모니터링 및 사후감사

- 사용자 별 DB에 연결된 Session에 대한 다양한 상태 정보를 실시간 모니터링
- DB 트랜잭션 로그 데이터에 대한 분석 및 감사보고서 생성
- DB 서버 부하율 0%의 처리방식

Gateway mode

사용자 별 DB 접근에 대한 권한관리 등 접근통제

- 불법적인 개인정보 조회, 유출방지
- 사용자 정의 보안정책에 따라 경보 및 차단 기능

Hybrid : Gateway, Sniffing, Agent 구성의 혼합형태

- 정형 접근에 대한 가용성 보장 및 감사기능 제공
- 비정형 접근에 대한 강력한 권한제어 및 접근통제

3. 주요기능 | 요약



System 접근통제 (6종)

Windows
HP-UX
AIX
Solaris
Linux
Mainframe

Database 접근통제 (30종)



Oracle / Time-Stan / Exadata
Microsoft SQL Server
IBM DB2 (Mainframe, UDB)
SAP Sybase IQ/ASE
SAP HANA
Mysql / MariaDB
IBM Netezza
TeraData
PostgreSQL / Greenplum
Altibase / Tibero / Cubrid / Kairos / SunDB
Amazon RedShift / Aurora
Dameng DM7
Fujitsu Symfoware
PetaSQL
Firebird / Couch / Influx / MongoDB



- DB 및 System 접근 및 작업결재
- HA(이중화) 구성
- 데이터 마스킹 (지정/패턴방식)
- 3 Tier User Tracking
- 우회접속 통제
- 사용자 파일저장 통제
- 불법 로그 위.변조 방지
- 개인정보/민감정보 탐색
- 사전-사후 데이터 기록
- 사용자 2-Factor 인증
- DB/서버 가상 계정 통제
- Cloud 지원(AWS, MS, KT 등등)
- Client Mac OS 지원

3. 주요기능 | DB 접근통제 및 기록

DB에 접근하는 모든 사용자(및 시스템)을 식별하고, 접근이력/수행SQL/변수/결과값을 기록하고 통제합니다. (실시간 모니터링 및 로그 조회)

The screenshot shows the Chakra Max interface with various search filters and a table of search results. The search filters include Target System (oracle 11g), DBMS 계정, O/S 계정, SQL 타입, and various search criteria. The search results table shows columns for ID, DBMS, DB User, OS User, Chakra M..., User Name, Group Na..., Client Ho..., Client IP..., Application, SQL, and Start Time. The results include queries like SELECT /*+ LEADING(S) */ INST_ID, SID, SERIAL#, OSPID, OR... and ALTER SESSION SET NLS_LANGUAGE=KOREAN NLS_TERRITO...

모든 SQL커맨드에 대하여 전문을 포함하여 약 40여 가지의 정보를 추적! 원하는 조건에 맞는 검색이 가능

실행 명령어 / 접속 시각 / 종료 시각 / 대상 시스템 계정 / 클라이언트 IP 정보 확인

조회 결과를 Excel/CSV로 export

3. 주요기능 | System 접근통제 및 기록

System (Linux, Unix, Windows, Mainframe)에 접근하는 모든 사용자(및 시스템)을 식별하고, Telnet, (s)FTP, SSH, R-Login, R-Command, Windows Terminal, Mainframe 등 다양한 시스템 접근이력 및 명령어 수행을 기록하고 통제합니다. (실시간 모니터링 및 로그 조회) (시스템에서 입력된 커맨드를 포함하여 vi 편집기에서 작업된 내역도 확인 가능)

The screenshot displays the Chakra Max Manager interface. The top navigation bar includes 'Monitor', 'Policy', 'Search', 'Report', and 'System'. The 'Monitor' dropdown menu is open, showing 'Overview', 'Session', 'Trend', 'Alert', and 'Client'. The 'Session' tab is selected, showing a table of active sessions. The table has columns for No., Server Name, Client IP Address, Client Mac Address, Login Time, Server Mac Address, and Alert Count. Below the table, there is a 'SessionMonitor Detail View' section with 'Command list' and 'Alert List' tabs. The 'Command list' tab shows a list of commands executed, including 'ls', 'cd /home/chakramax', 'cd setup', and './maxsetup'. A terminal window is overlaid on the right side, showing a root shell session with various commands and their outputs, including 'ls', 'cd /home/chakramax', and './maxsetup'.

No.	Server Name	Client IP Address	Client Mac Address	Login Time	Server Mac Address	Alert Count
1	CentOS_5.5	172.17.30.50	04:7D:7B:9B:9B:C5	2013/11/29 (금) 14:08:43	00:0C:29:1E:D3:22	0
2	CentOS_5.5	172.17.30.50	04:7D:7B:9B:9B:C5	2013/11/29 (금) 14:03:46	00:0C:29:1E:D3:22	1
3	CentOS_5.5	172.17.46.50	00:0C:29:A8:06:D8	2013/11/29 (금) 13:59:01	00:0C:29:1E:D3:22	0

```
root@localhost/home/chakramax/setup
localhost.localdomain (Linux release 2.6.18-194.el5 #1 SMP Fri Apr 2 14:58:14 EDT 2010) (3)
login: root
Password:
Login incorrect
login: root
Password:
Last login: Fri Nov 29 14:00:20 on tty5
You have new mail.
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# ls
anaconda-ks.cfg  install.log  install.log.syslog
[root@localhost ~]# cd /home/chakramax
[root@localhost chakramax]# ls
bin  chakramax_setup_v2.0.1.29_r17914.tar.gz  dbclient  java  log  mdb  ozreport  patchfiles  setup  temp
[root@localhost chakramax]# cd setup
[root@localhost setup]# ./maxsetup
```

3. 주요기능 | System 접근통제 - Windows Terminal

Windows Remote Desktop (Windows Terminal) 연결 시 수행 내역 동영상으로 녹화,
 Shell에서 실행 된 명령어 감사 기록으로 저장
 원격 사용자 통제 및 실행하는 프로그램 통제
 관리자 화면에서 감사로그 명령어 조회 및 녹화 동영상 재생 기능

MaxManager

Chakra Max

Monitor Policy Search Report System

Database System RDP Alert Approval Client Work History

2013년 11월 4일 오전 11:35:17 부터 2013년 11월 6일 오전 11:35:17 까지 로그를 검색합니다. [검색조건 감추기](#)

Target System : 172.17.100.10(Terminal Service),

클라이언트 IP주소 : 사용자 이름 :

대상 시스템 계정 : 사용자 계정 :

실행 명령어 : 사용자 그룹(부서) :

Search Sniffing Log
 Search Gateway Log

RDP Session Result(1) RDP Session Result(2)

Search operation was finished successfully. : 306 SQL (1.112초) [Hide Detail Pane](#) [Object Usage Analysis](#) [Execution Trend](#)

ID	Service T...	Service N...	Client IP	Client Port	Client Ho...	Start Time	Login Result	End Time
1	Terminal ...	172.17.1...	172.17.1.1	1854	HAEDON...	2013/11/...	2013/11/...	
2	Terminal ...	172.17.1...	172.17.1.1	1855	HAEDON...	2013/11/...	2013/11/...	
3	Terminal ...	172.17.1...	172.17.1.1	4454	HAEDON...	2013/11/...	2013/11/...	
4	Terminal ...	172.17.1...	172.17.1.1	4455	HAEDON...	2013/11/...	2013/11/...	

명령어 로깅

Terminal 녹화
실행 프로그램 통제

User #1

Chakra Max Database Security Assurance

Chakra Max RDP agent

SQL Server 2008 R2

3. 주요기능 | System 접근통제 – Mainframe (TN5250, 3270)

As/400과 같은 IBM Mainframe서버에 접근하는 TN3270,5250 터미널의 사용자 식별 및 작업이력을 기록하고 통제합니다.

SessionMonitor Detail View

Command list Alert List

Command Time	Command
2015/03/27 (금) 03:...	[0,0] SESSION OPEN
2015/03/27 (금) 03:...	[6,53] TESTCONT, [7,53] (password), [7, 62] ENTER KEY
2015/03/27 (금) 03:...	[1, 1] ENTER KEY
2015/03/27 (금) 03:...	[1, 1] ENTER KEY
2015/03/27 (금) 03:...	[20,7] 1, [20, 8] ENTER KEY
2015/03/27 (금) 03:...	[20,7] 1, [20, 8] ENTER KEY
2015/03/27 (금) 03:...	[21,7] 1, [21, 8] ENTER KEY
2015/03/27 (금) 03:...	[1, 1] ENTER KEY
2015/03/27 (금) 03:...	[21, 7] F3 KEY
2015/03/27 (금) 03:...	[20, 7] F3 KEY
2015/03/27 (금) 03:...	[20,7] 6, [20, 8] ENTER KEY
2015/03/27 (금) 03:...	[20,7] 2, [20, 8] ENTER KEY
2015/03/27 (금) 03:...	[20,7] 3, [20, 8] ENTER KEY
2015/03/27 (금) 03:...	[5, 27] F3 KEY

TN5250,3270 실시간 모니터링 - 좌표와 입력 명령어 확인

Alert ID	Server N...	Command Time /	Command
16	DASAPQAS	2015/04/07 (금) 12:29...	[0,0] SESSION OPEN
17	DASAPQAS	2015/04/07 (금) 12:29...	[6,53] TWKWON, [7,53] (password), [7, 59]
18	DASAPQAS	2015/04/07 (금) 12:29...	[6, 60] ENTER KEY
19	DASAPQAS	2015/04/07 (금) 12:29...	[6, 60] ENTER KEY
20	DASAPQAS	2015/04/07 (금) 12:29...	[6,53] QSECOFR, [7,53] (password), [7, 60]
21	DASAPQAS	2015/04/07 (금) 12:30...	[20,7] wrksrpf*, [20, 15] ENTER KEY
22	DASAPQAS	2015/04/07 (금) 12:30...	[7,3] 1, [21, 7] ENTER KEY
23	DASAPQAS	2015/04/07 (금) 12:30...	[5,37] twkwon, [5, 43] ENTER KEY
24	DASAPQAS	2015/04/07 (금) 12:30...	[10,2] 2, [10, 3] ENTER KEY
25	DASAPQAS	2015/04/07 (금) 12:30...	[6,37] secofr1, [6, 43] ENTER KEY
26	DASAPQAS	2015/04/07 (금) 12:30...	[10, 2] F3 KEY
27	DASAPQAS	2015/04/07 (금) 12:30...	[7, 3] F3 KEY
28	DASAPQAS	2015/04/07 (금) 12:30...	[20, 7] F3 KEY
29	DASAPQAS	2015/04/07 (금) 12:30...	[20, 7] F3 KEY
30	DASAPQAS	2015/04/07 (금) 12:30...	[20,7] 90, [20, 9] ENTER KEY
31	DASAPQAS	2015/04/07 (금) 12:30...	[6,53] TWKWON, [7,53] SECOFR1, [7, 60] E
32	DASAPQAS	2015/04/07 (금) 12:30...	[1, 1] ENTER KEY
33	DASAPQAS	2015/04/07 (금) 12:54...	[0,0] SESSION OPEN
34	DASAPQAS	2015/04/07 (금) 12:54...	[6,53] TWKWON, [7,53] (password), [7, 60]
35	DASAPQAS	2015/04/07 (금) 12:54...	[1, 1] ENTER KEY
36	DASAPQAS	2015/04/07 (금) 12:54...	[20,7] wrksyssts, [20, 16] ENTER KEY
37	DASAPQAS	2015/04/07 (금) 12:54...	[0,0] SESSION OPEN
38	DASAPQAS	2015/04/07 (금) 12:55...	[6,53] TWKWON, [7,53] (password), [7, 60]
39	DASAPQAS	2015/04/07 (금) 12:55...	[1, 1] ENTER KEY

실행된 결과 화면 저장 기능

MAIN IBM Main Menu System: DYSAPQAS

Select one of the following:

1. User tasks
2. Office tasks
3. General system tasks
4. Files, libraries, and folders
5. Programming
6. Communications
7. Define or change the system
8. Problem handling
9. Display a menu
10. Information Assistant options
11. IBM i Access tasks

90. Sign off

Selection or command
====> r

F3=Exit F4=Prompt F9=Retrieve F12=Cancel F13=Information Assistant
F23=Set initial menu
(C) COPYRIGHT IBM CORP. 1980, 2009.

3. 주요기능 | 보안정책 구성

DB, System에 접근하는 모든 사용자(및 시스템)을 접근 및 작업 통제를 위하여, 위저드(Wizard) 방식의 손쉬운 보안정책을 구성할 수 있습니다.

데이터베이스/시스템 접근 및 실행제어 정책

-  Database Access Control Policy
데이터베이스 접근 통제 정책을 정의합니다.
-  SQL Execution Control Policy
SQL 실행 통제 정책을 정의합니다.
-  System Access Control Policy
시스템 접근 통제 정책을 정의합니다.
-  System Command Execution Control Policy
시스템 명령어 실행 통제 정책을 정의합니다.

결재정책 / 파일저장 통제 정책

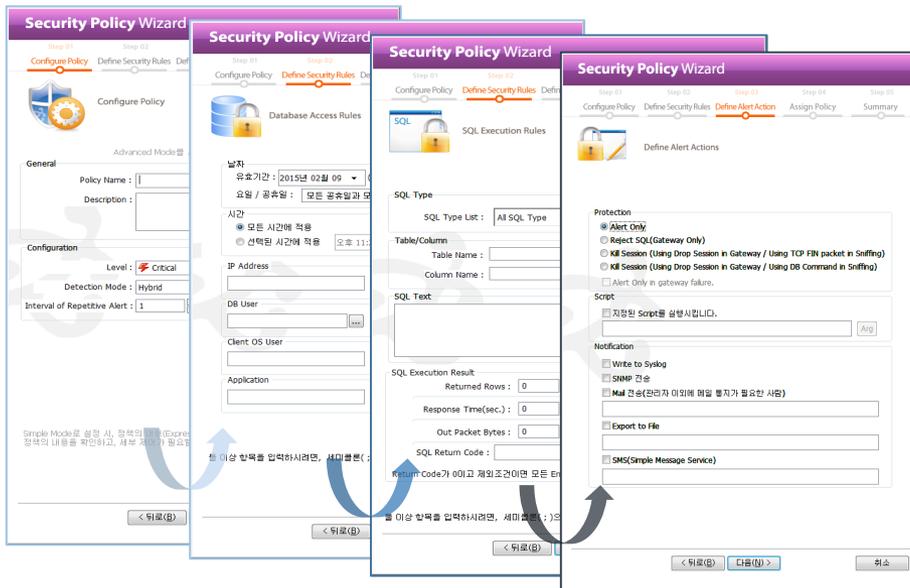
-  Database / System Access Approval Policy
접근 권한을 획득하기 위한 결재 정책을 정의합니다.
-  CMD/SQL Execution Approval Policy
CMD/SQL 실행 권한 제어를 위한 결재 정책을 정의합니다.
-  SQL Result Save Approval Policy
SQL 실행 결과 저장을 통제하기 위한 결재 정책을 정의합니다.
-  Approval Policy For Masking Exception
승인 받은 쿼리의 결과는 마스킹 되지 않는 정책을 정의합니다.

변경 전/후 데이터 저장 정책

-  Modified Data Policy
데이터베이스 변경 전/후 데이터 로깅 정책을 정의합니다.

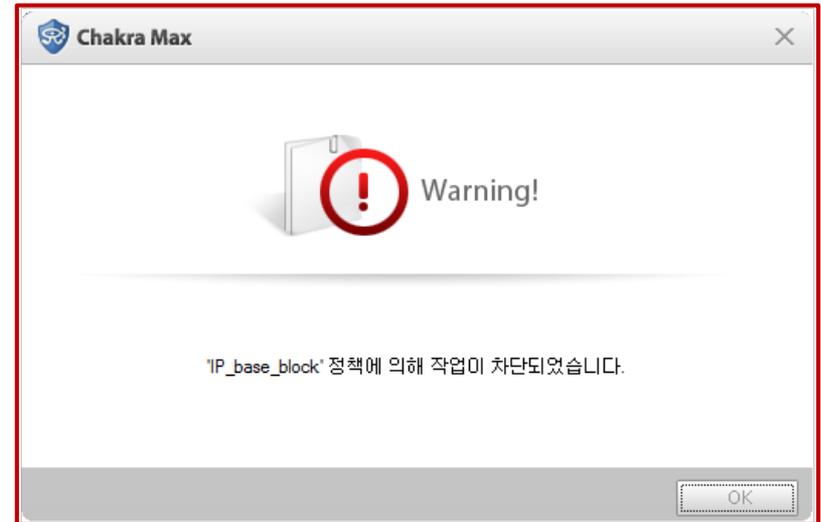
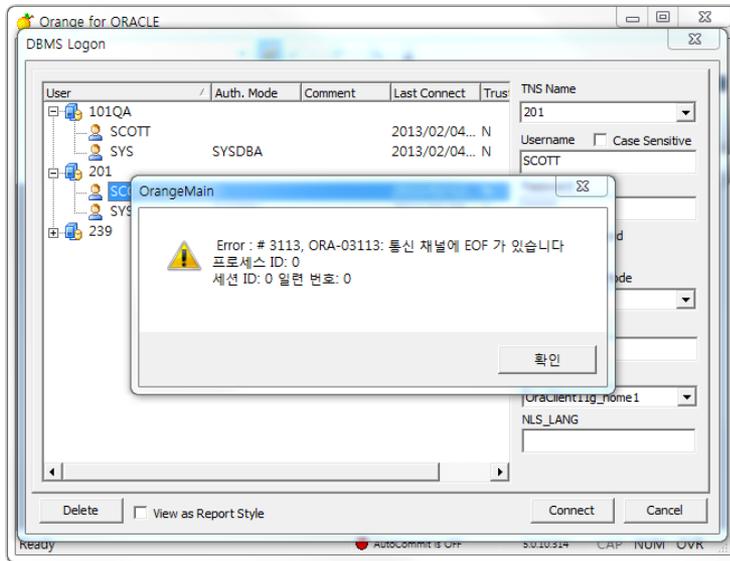
마스킹 정책

-  SQL Result Masking Policy
쿼리 결과 중 보안이 필요한 항목에 대해 Masking정책을 정의합니다.



3. 주요기능 | 보안정책에 따른 DB 접근통제

Client IP, DB user, Table, Column, SQL Command 등의 다양한 조건의 통제 정책 적용



다양한 조합으로 DB 접근을 제어

- 사용자 식별 유저 정보 : IP 주소, DB 계정, OS 로그인 유저, 접속 어플리케이션, 접속시간 등
- DB작업내용 : 테이블, 컬럼, SQL 타입(DDL/DML/DCL), 입력 커맨드 등
- 기타 : 프로토콜, 시간대, 네트워크 사용량, SQL 결과 리턴 로우

3. 주요기능 | 보안정책에 따른 System 접근통제

SSH, Telnet, FTP, Windows Terminal, TN5250 등의 시스템 접속에 대한 실시간 감시 및 통제, 접근 이력의 재분석이 가능

서버 원격 프로토콜 (ssh, telnet, ftp, 원격데스크톱 등) : 세션, 명령어 접근제어

No.	Chakra Max User	Server Name /	Client IP Address	Client Mac Address	Login Time	Server Mac Ad...	Alert Count
1	test(test)	oracle svr	192.168.0.200	00:50:56:C0:00:08	2015/03/02 (월) 13:09:21	00:0C:29:6A:F...	
2	test(test)	oracle svr	192.168.0.200	00:50:56:C0:00:08	2015/03/02 (월) 13:09:52	00:0C:29:6A:F...	
3	test(test)	oracle svr	192.168.0.200	00:50:56:C0:00:08	2015/03/02 (월) 13:19:42	00:0C:29:6A:F...	

TN5250 : 좌표와 입력 명령어 모니터링, 화면저장 등

SessionMonitor Detail View

Command Time	Command
2015/03/02 (월) 13:...	ls
2015/03/02 (월) 13:...	pwd
2015/03/02 (월) 13:...	df -Th
2015/03/02 (월) 13:...	top
2015/03/02 (월) 13:...	free -m
2015/03/02 (월) 13:...	su - oracle
2015/03/02 (월) 13:...	pwd
2015/03/02 (월) 13:...	sqlplus */as sys
2015/03/02 (월) 13:...	select * from ta

392.168.0.129 - PuTTY

```

login as: root
root@192.168.0.129's password:
    
```

PUTTY Data Drop

Server unexpectedly closed network connection

Warning!

00. ssh 접근차단 정책 정책에 의해 작업이 차단되었습니다.

3. 주요기능 | 경고 모니터

보안정책에 위배된 DB접근이나 System 접근 혹은 SQL, System 명령어 작업에 대해, 실시간으로 관리자, 사용자에게 정책 위반 및 경고 메시지를 쉽게 확인이 가능

Alert "00, ssh 접근차단 정책" on server "oracle svr" 2015년 03월 02일 13:15:40 Alert "00, ssh 접근차단 정책" on server "oracle svr"

DB Session Server Session

Limit Count Auto Refresh Session by Gateway & Sniffing

Drag a column header here to group by that column.

N..	Server	Database	SID	Serial#	DB User	Chakra Max U...	Client OS ...	Client IP Address	Application	Client Host...	Terminal
1	orade svr	oracle 11g	40	7943	SCOTT	test(test)	SHINUK	192.168.0.200	ORANGEMAI...	SHINUK-PC	SHINUK-
2	orade svr	oracle 11g	33	4391	SCOTT	test(test)	SHINUK	192.168.0.200	SQLPLUS.EXE	SHINUK-PC	SHINUK-
3	orade svr	oracle 11g	27	9565	SCOTT	test(test)	SHINUK	192.168.0.200	ORANGEMAI...	SHINUK-PC	SHINUK-
4	orade svr	oracle 11g	31	6521	SCOTT	test(test)	SHINUK				

실시간 경고 발생 알림

세션 모니터의 경고 발생 표시

Warning !

'SQL (select with insert) control' 정책에 의해 작업이 차단되었습니다.

Warning !

'scott,dept block to sys' 정책에 의해 작업이 차단되었습니다.

확인

사용자 Client 정책 위반 경고 팝업

3. 주요기능 | 경보 캘린더

발생된 경보가 월/주/일별의 달력형태로 표현하여 확인 및 추이 파악이 용이

The screenshot displays the Chakra Max Alert Calendar interface. The main calendar view shows alerts for the month of March 2015, with alerts color-coded by severity: Critical (red), Major (orange), Minor (yellow), Warn (green), and Info (blue). A callout box on the left provides detailed information for a selected alert, including Name, Time, Description, Alert Level, Server Name, Database, Service Type, Conditions, and Access Information. A callout box on the right shows a weekly summary of alerts for the week of March 2nd to 8th, 2015. Another callout box on the right shows a monthly summary of alerts for the month of March 2015.

경보를 등급색을 구분하여 표시

경고 클릭하여 상세 정보를 확인

월/주/일별 경보 현황 확인

3. 주요기능 | Security Dashboard

현재 접속현황 / 민감정보 접근자 / 경보발생IP top5 등, 경보에 관련된 정보 표시

The screenshot displays the Chakra Max Security Dashboard interface. The main dashboard includes several key metrics and charts:

- 현재 세션 수:** 2 세션 (1 IP 주소, 1 DB 사용자)
- 24시간 SQL 추이 (한달 평균):** A line graph showing SQL activity over 24 hours.
- 보안 정책 수:** 3 (사건 정의: 2, 경보: 0, 결재: 1, 마스킹: 0, 사전 사후: 0)
- 접근 가능 사용자:** 8 명 (현재 접속 중인 사용자 수: 1 명)
- 민감정보 컬럼 수:** 2 Columns
- 민감정보 접근 사용자 Top 5:** A table listing top users by sensitive information access.

The table for '민감정보 접근 사용자 Top 5' is as follows:

IP	이름(로그인 ID)	누적 건수
192.168.24...	테스트01(test01)	5304

The 'ord (ORACLE)' section features three pie charts:

- 오늘의 경보 수:** 10 경보
- 경보 발생 IP Top 5 (최근 한달):**
 - 192.168.246.50: 6
 - 192.168.246.10: 4
 - 192.168.246.20: 3
- 경보 발생 DB 사용자 Top 5 (최근 한달):**
 - SCOTT: 11
 - SYS: 2
- 경보 발생 사용자 Top 5 (최근 한달):**
 - 테스트01: 6
 - 테스트02: 4
 - 테스트03: 3

A configuration window titled 'Section' is open, showing a list of available sections and a selected section. The 'Selected Section' includes:

- 오늘의 경보 수
- 경보 발생 IP Top 5 (최근 한달)
- 경보 발생 DB 사용자 Top 5 (...)
- 경보 발생 사용자 Top 5 (최근 한달)
- 경보 발생 정책 Top 5 (최근 한달)

3. 주요기능 | 데이터 마스킹(Masking)

DB내의 민감 정보에 대한 Masking을 통한 정보를 은닉하며, DB성능 저하가 없이 Packet 분석을 통해 Masking 처리를 지원

- 1) 지정된 Table/Column에 대한 민감 정보 Masking
- 2) 개인정보를 가진 임의의 SQL 결과에 의한 패턴 Masking

테이블/컬럼 또는 패턴 지정을 선택

Define Masking Rules

Object(s)

Table, Column을 지정 Sensitive Pattern을 지정

Table	Column	Type	Format
user_info	jumin	Partial Masking	000000*

Column : 여러 칼럼을 동시에 적용하시려면 ';'을 구분자로 사용하십시오.
Type : 칼럼 데이터 전체 은닉을 원하시면 'Full Masking'을 설정 형식에 따라 일부 은닉을 원하시면 'Partial Masking'을 선택하십시오.
Format : 'Partial Masking'형식을 설정합니다.
아래 예제와 같이 '*'과 '0'을 이용하여 형식을 정의 하십시오.
(예제) 원본 데이터 : 770101-1111111
 설정 방법 : 0000000*****
 Masking 결과 : 770101-*****

Exception Object(s)

Table	Column
There are no items to show.	

마스킹 예외 테이블/컬럼 지정

Orange for ORACLE (Unicode) - [SQL Tool:SCOTT@oracle 11g_scott/SQL1 *]

DB접근제어 솔루션 Chakra Max

```
10 - SCOTT@oracle 11g_scott
```

```
SQL SQL PLRN
```

```
SQL SQL ERViewer
```

```
SQL1 *
```

```
1
```

```
2 > select * from user_info;
```

Result

NO	NAME	JUMIN	CARD_NO	TEL
1	홍길동	777777*****	4677-3281-4596-6410	803-483-8155
2	54322	000000*****	4063-5304-5745-5067	647-7480-1940
3	고민서	647545*****	3349-3060-7605-4518	262-8849-5759
4	우라온	147184*****	7330-6564-6359-7687	628-5827-5088
5	이승해	459065*****	2145-7852-5670-9069	694-500-5667
6	최혜선	986085*****	9730-6489-3367-1882	964-1496-1509
7	chakra	116355*****	2413-8032-3334-3245	311-1966-4070
8	박지혜	393117*****	5450-4772-1033-5238	880-2272-8379
9	배승호	717417*****	6580-2902-8075-1071	951-151-3404
10	서민승	018181*****	6667-9190-7227-1378	761-2725-0027
11	이지후	169012*****	3537-9029-6668-9865	369-2632-5979

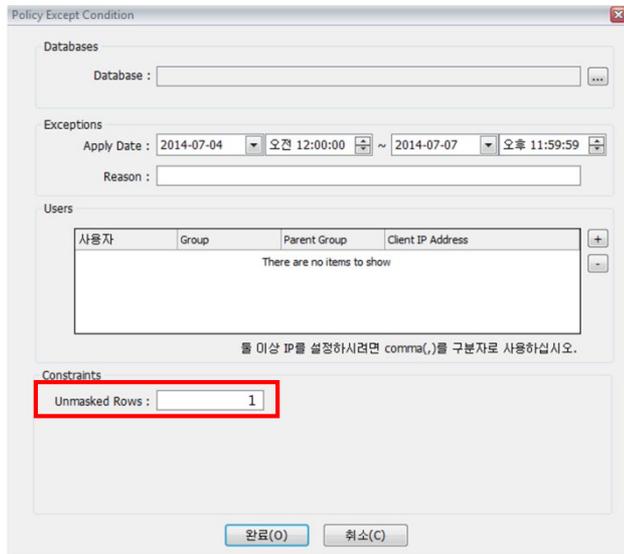
Ln 2, Col 1 0.02 sec. 100+ rows

Ready AutoCommit is Off 6.0.1.25 CAP NUM OVR

- Chakra MAX의 경우 마스킹을 위해 고객의 DB에 View를 설치하거나 SQL 변조를 일으키는 행위를 하지 않습니다.

3. 주요기능 | 고객 업무편의를 위한 선택적 마스크 해제

고객의 업무 편의를 위해 마스크 처리된 오브젝트에서 일부 선택적 마스크 해제를 지원



- 마스크가 적용된 오브젝트에서 마스크 해제되는 레코드 건수를 설정



The screenshot shows the SQL Developer interface. The SQL query is: `select user_no, card_no, concat(substr(card_no,-8, 11), hp) from user_test`. The result set is displayed in a grid, with the first row highlighted in red:

USER NO	CARD NO	CONCAT(SUBSTR(CARD NO.-8.11).HP)
1	1409 673721038133	8133321101621650762
2	1410	*****
3	1411	*****
4	1412	*****
5	1413	*****
6	1414	*****
7	1415	*****
8	1416	*****
9	1417	*****
10	1418	*****
11	1419	*****
12	1420	*****
13	1421	*****
14	1422	*****
15	1423	*****

- 설정 된 행수를 제외한 부분은 마스크 처리

3. 주요기능 | 감사로그 내의 민감정보보호를 위한 마스킹

Chakra MAX에 수집된 감사로그에 고객의 민감정보를 보호하기 위해, 로그조회나 리포트 출력에서 마스킹을 통해 고객의 정보를 보호합니다.

```

1 INSERT
2 INTO TEST_SENSITIVE(MAIN_ADDR, PHONE_NUM, USER_NAME,
3 VALUES ('TEST@WAREVALLEY.COM',
4         '01012345678',
5         'USER01',
6         'USER01')
    
```

실제 실행된 SQL



감사 로그 검색 결과에 고객 정보 포함되어 자동 마스킹

보고서 또는 로그 검색 시 Pattern 포함을 감지하고 Masking할 것인지 설정

Masking 방식을 정의. 부분 Masking이 필요하면 Rule을 정의

설정 화면

3. 주요기능 | 민감정보 관리

고객 정보와 같은 민감한 정보를 "Sensitive Object"로 관리
 미리 정의된 정보 패턴(Sensitive Pattern) 를 제공 및 사용자 정의 가능

Registered Objects

Schema	Object Name	Column	Description	Pattern
Database: allnix	test#2	test#2	test#1	Cellular Phone Number
	test#1	test#1	test#1	Foreigner Registration N
	test1	test1	test	New Passport Number
	ste	estst	t	New Passport Number
	scott	dept	name	
	scott	emp	고객정보 테이블	Cellular Phone Number
	schema test			

Sensitive Pattern

Pattern은 정규 표현식으로 입력하십시오.

Pattern Name :

Description :

Regular Expression :

Regular Expression

- ^ : 문자열의 시작 \$: 문자열의 끝
- [n, } : 전 요소가 n개 이상 매치
- [abc] : a 또는 b 또는 c 인 문자
- { n } : 전 요소가 정확히 n개 만큼 매치
- [^abc] : a, b, c 가 아닌 어떠한 문자
- () : 그룹핑, 반복 연산자들에 대해서 범위를 지정함
- [a - z] : a 부터 z 까지 영문자
- | : 대체, 왼쪽 또는 오른쪽 표현식에 매칭됨
- [0 - 9] : 0 부터 9 까지 숫자 한 문자
- ? : 전 요소가 0개 또는 1개 매치. { 0, 1 } 과 동일
- { n, m } : 전 요소(previous Element)가 적어도 n 개부터 m 개까지 매치
- + : 전 요소가 1개 이상 매치. { 1, } 과 동일
- [a - z A - Z] : a 부터 z 까지, A 부터 Z 까지 영문자 (대소문자 구분없는 영문자)
- * : 전 요소가 0개 이상 매치. { 0, } 과 동일

Masking

Using for search masking

Using for report masking

Masking Format :

Expression에 ()를 이용하여 그룹핑을 설정하면 그룹 별 부분 마스킹이 가능합니다.
 * : 모든 문자열이 마스킹됩니다.
 \$1* : 첫 번째 그룹(\$1)은 마스킹되지 않습니다.
 \$1*\$3 : 두 번째 그룹(\$2)만 마스킹 됩니다.

OK Cancel

ex) 전화번호, 신용카드번호, 이메일, 군번, 주민번호, 여권번호(신/구), 휴대전화 번호
 필요 시 민감정보 패턴을 직접 작성/수정 가능

3. 주요기능 | 결재

다양한 방식의 결재 정책 및 다단계 결재 정책 지원

Approval Procedure Wizard

Step 01: Configure Approval Procedure | **Step 02: Set Approval Steps** | Step 03: Set Options

Set Approval Steps

Approval Step: 3 step procedure

1 step procedure
2 step procedure
3 step procedure
4 step procedure
5 step procedure
6 step procedure

사전/사후 승인 선택

모든 결재자의 승인 후 실행 가능
모든 결재자의 승인 후 실행 가능
결재 없이 실행 가능

결재 단계 선택

기안자의 상위 그룹 리더

1차 결재자를 선택하십시오

==== 그룹장 =====
기안자의 소속 그룹 리더
기안자의 상위 그룹 리더
기안자의 2번째 상위 그룹 리더
특정 그룹의 리더
==== 특정 소속원 =====
기안자가 본인 그룹 소속원 중 한명을 결재자로 지정
기안자가 상위 그룹 소속원 중 한명을 결재자로 지정
기안자가 2번째 상위 그룹 소속원 중 한명을 결재자로 지정
기안자가 특정 그룹 소속원 중 한명을 결재자로 지정
특정 사용자를 결재자로 지정
==== 특정 그룹 =====
기안자와 동일한 그룹 소속원 중 한 명이 결재함
기안자의 상위 그룹 소속원 중 한 명이 결재함
기안자의 2번째 상위 그룹 소속원 중 한 명이 결재함
특정 그룹 소속원 중 한 명이 결재함

결재 대상자 선택

< 뒤로(B) | 다음(N) > | 마침 | 취소

Chakra Max

Warning!

수행한 작업은 문제가 없습니다.
로그 요청하시겠습니까?

결재정책 차단 후 기안

기안 상세정보

제목: Update 실행

설명: Update 실행

기안 상세정보

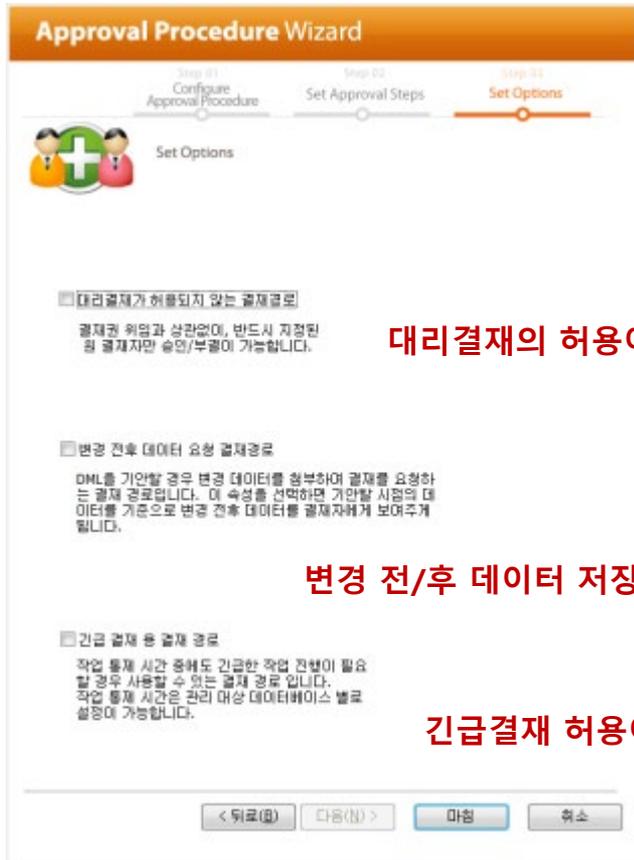
대상 DB: Oracle 11g
사용자: SCOTT
대상 그룹: SCOTT
실행 권한: None
실행 시간: 2015-03-25 12:00:00
실행 기간 시작 시간: 2015-03-25 12:00:00
실행 기간 종료 시간: 2015-03-25 12:00:00
실행 결과: 성공(100%) 실행 시간: 00:00:00

기안 완료 후 결재 대상자의 승인 후 SQL 실행

사후 결재시 기안 후 결재전 실행가능, 실행이력 감사로그로 저장 및 결재자에 이메일 통보

3. 주요기능 | 대리결재/긴급결재

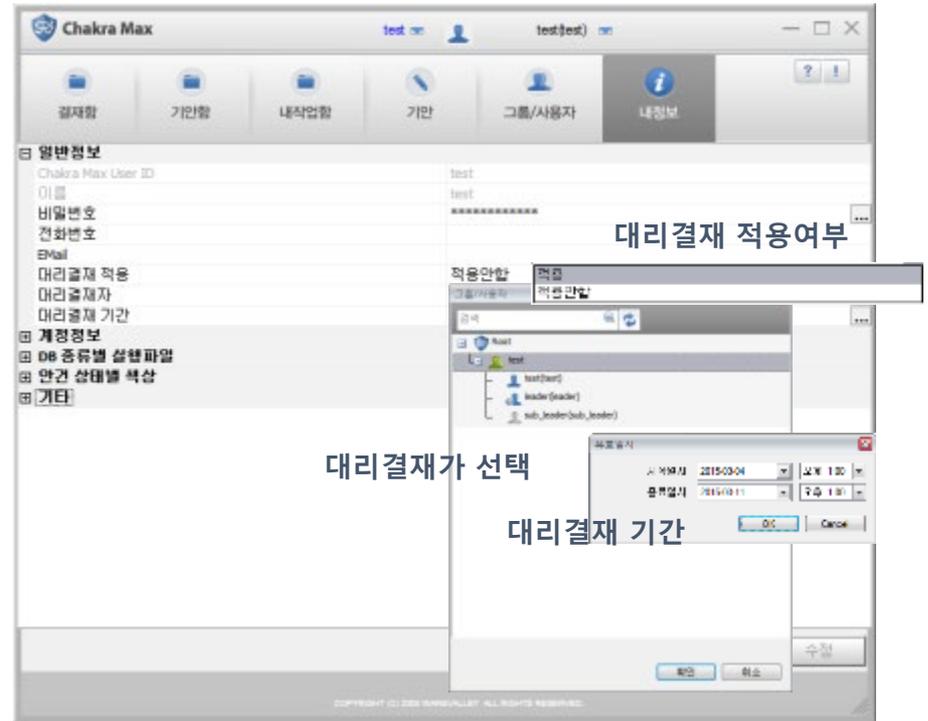
관리자의 확인이 필요한 작업에 대해 결재 프로세스를 이용한 작업 확인, 승인(결재) 기능을 제공하며, 사전/사후 결재 및 대리/긴급결재를 제공하여 업무 연속성을 보장



대리결재의 허용여부

변경 전/후 데이터 저장여부

긴급결재 허용여부



대리결재가 선택

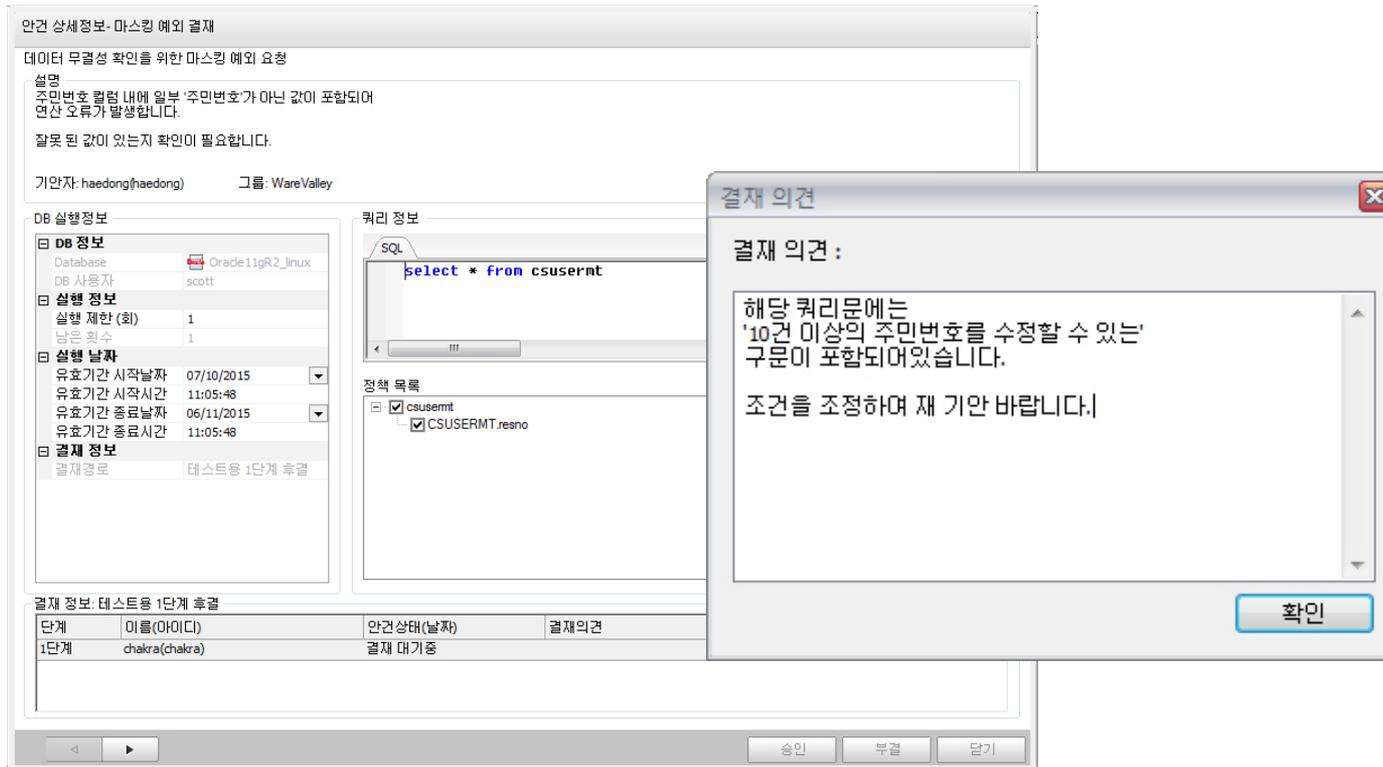
대리결재 기간

대리결재 적용 및 대리결재자/기간은 사용자가 지정

3. 주요기능 | 결재 의견

결재자의 결재 / 부결 처리 시 결재권자의 결재/부결 의견 기입

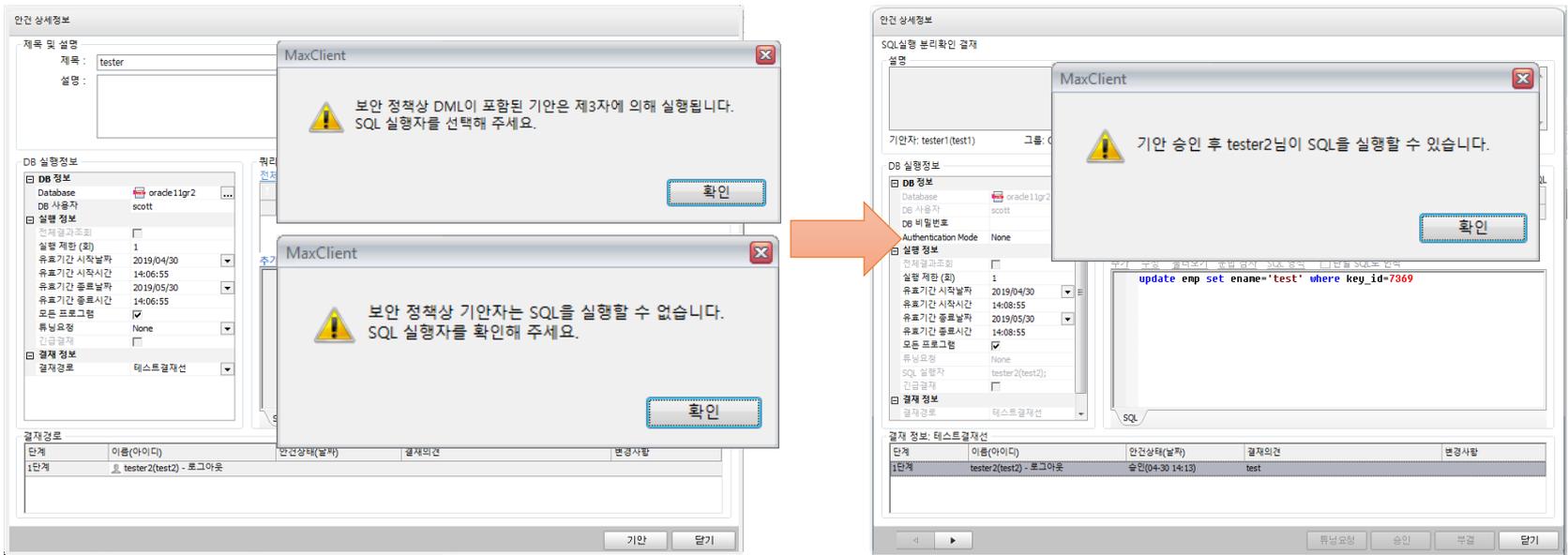
(결재자의 결재 처리 시 결재 의견 삽입을 통해 결재 / 부결 등에 대한 명확한 의견 전달)



3. 주요기능 | 제3자 실행 결재

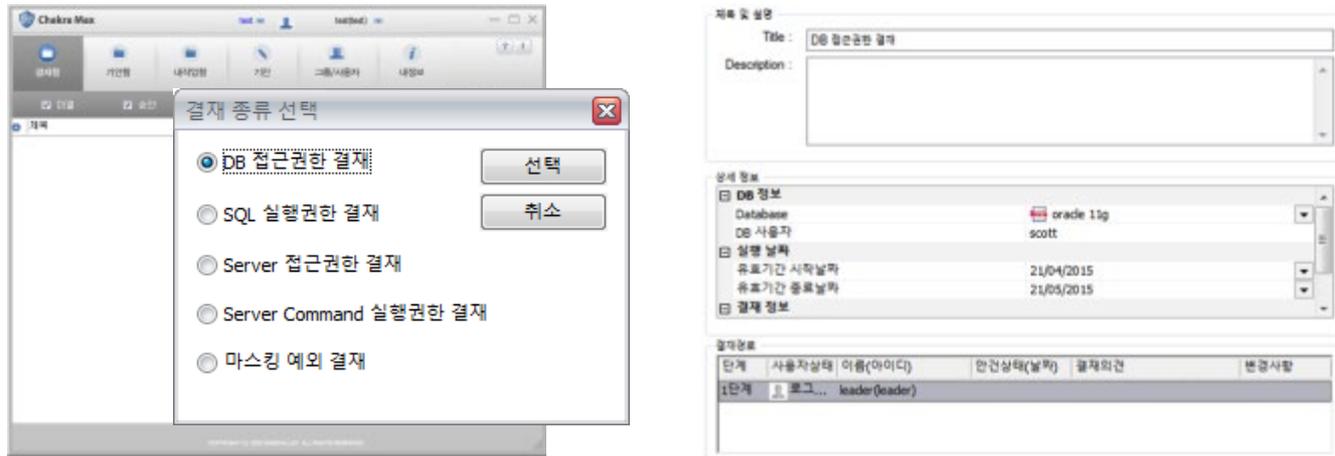
기안자와 실행자의 권한 분리 기능

결재를 요청하는 기안자와 SQL의 실행자를 분리하는 기능으로, 기안자는 기안작성 후 결재요청시 sql 실행자를 선택하여 결재를 올리고, 결재완료시 실행자가 SQL을 실행할 권한을 가진다.



3. 주요기능 | DB 접근권한 결재

접근 권한이 없는 데이터베이스에 DB 접근권한 결재 기능을 이용하여 사용자가 직접 기안 후 결재자의 승인을 통해 접속하는 기능을 제공



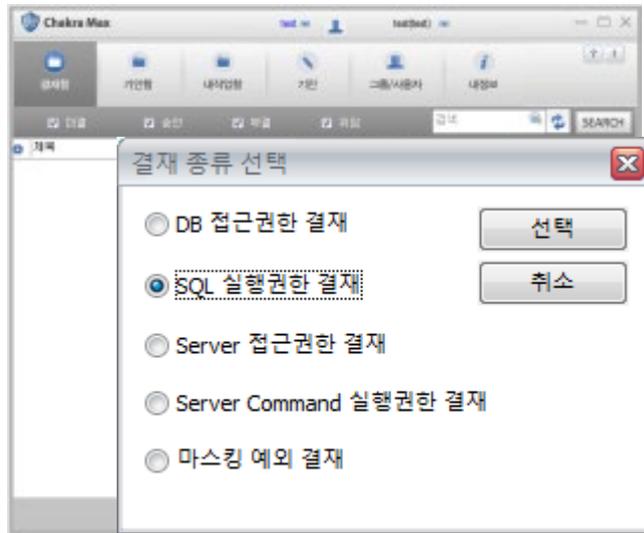
사용자가 DB 접근권한 기안, 결재자의 승인 완료 후 접속 권한 부여

Name	ID	Group	Database Account
상속레벨: Database			
test	test	/test;	scott(***:2015/04/21 ~ 2015/05/21);
sub_leader	sub_leader	/test;	

접근대상 DB에 사용계정 및 사용기간 할당

3. 주요기능 | SQL 실행권한 결재

SQL 실행 결재 정책이 적용된 SQL 실행시, SQL 실행권한 결재를 통해 사용자가 직접 기안하고 결재자의 승인 후 SQL 실행 및 이력을 감사기록으로 저장

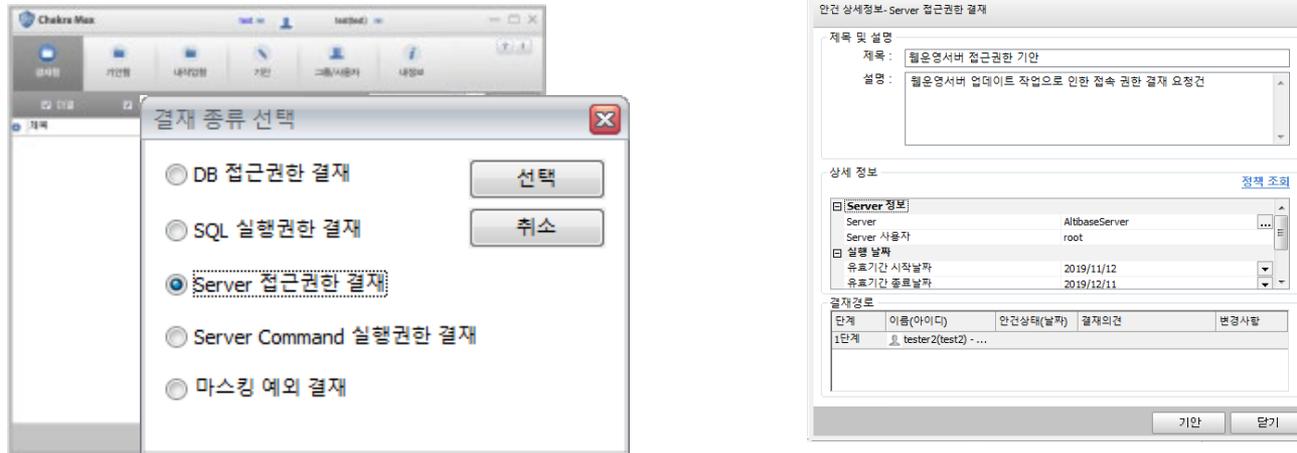


사용자가 SQL 실행권한 기안 요청, 결재자의 승인 완료 후 SQL 실행 가능

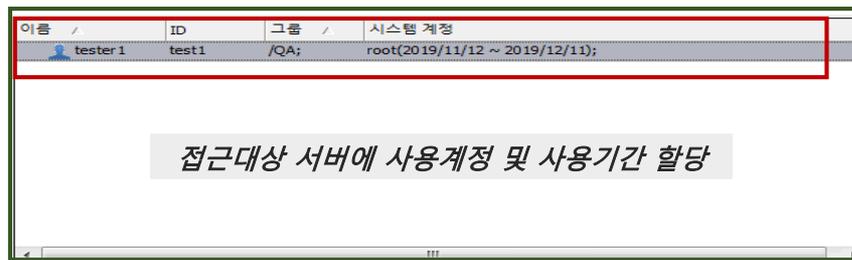


3. 주요기능 | 서버 접근권한 결재

접근 권한이 없는 SERVER에 server 접근권한 결재 기능을 이용하여 사용자가 직접 기안 후 결재자의 승인을 통해 접속하는 기능을 제공

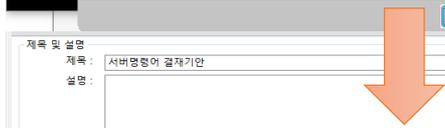
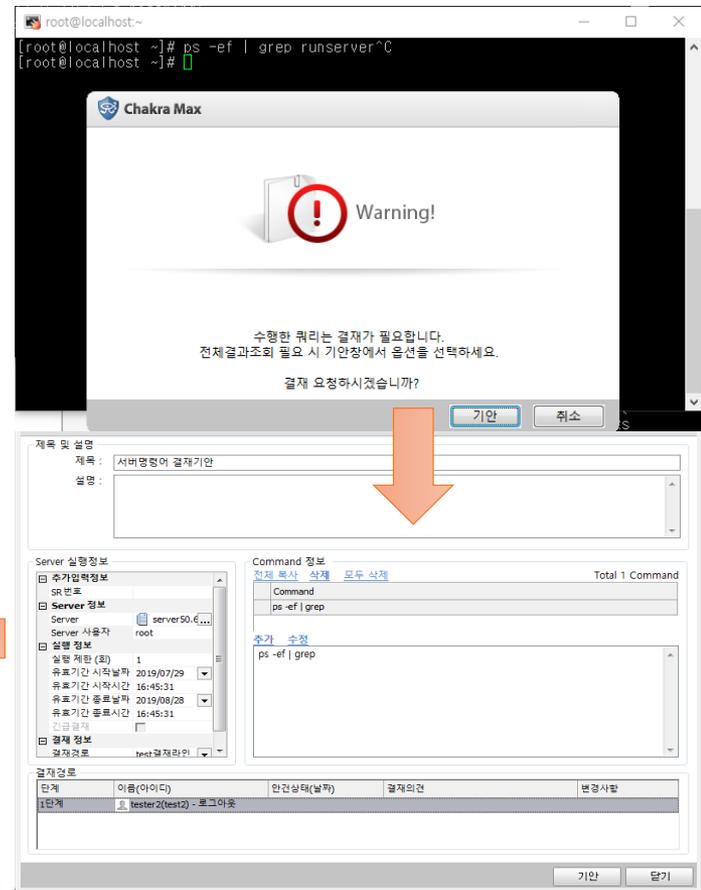
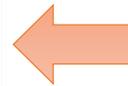
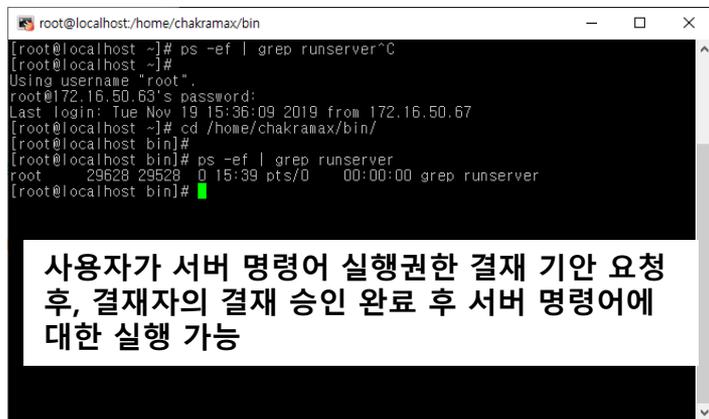
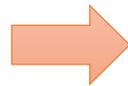
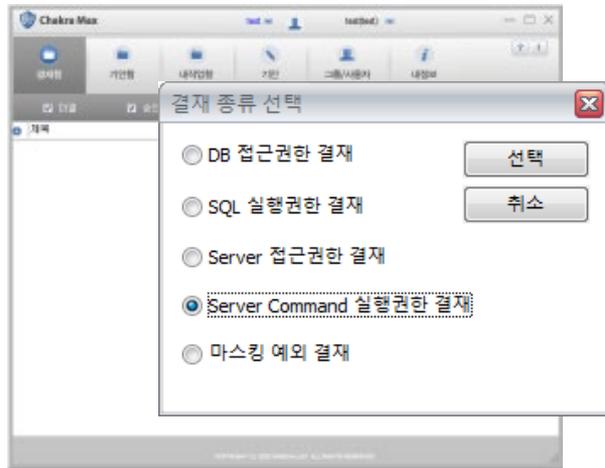


사용자가 DB 접근권한 기안, 결재자의 승인 완료 후 접속 권한 부여



3. 주요기능 | 서버 명령어 실행권한 결재

서버 명령어 결재 정책이 적용된 command 실행시, 서버 명령어 결재를 프로세스를 통해 사용자가 기안 후 결재자의 승인을 통해 서버 명령어를 실행권한을 취득하고, 명령어 실행시 이력을 감사기록으로 저장



3. 주요기능 | 마스킹 예외 결재

마스킹 지정 테이블/칼럼을 결재를 통하여 실행하는 SQL이 일정기간, 지정된 횟수에 한하여 마스킹 정책에서 예외 할 수 있는 기능 제공

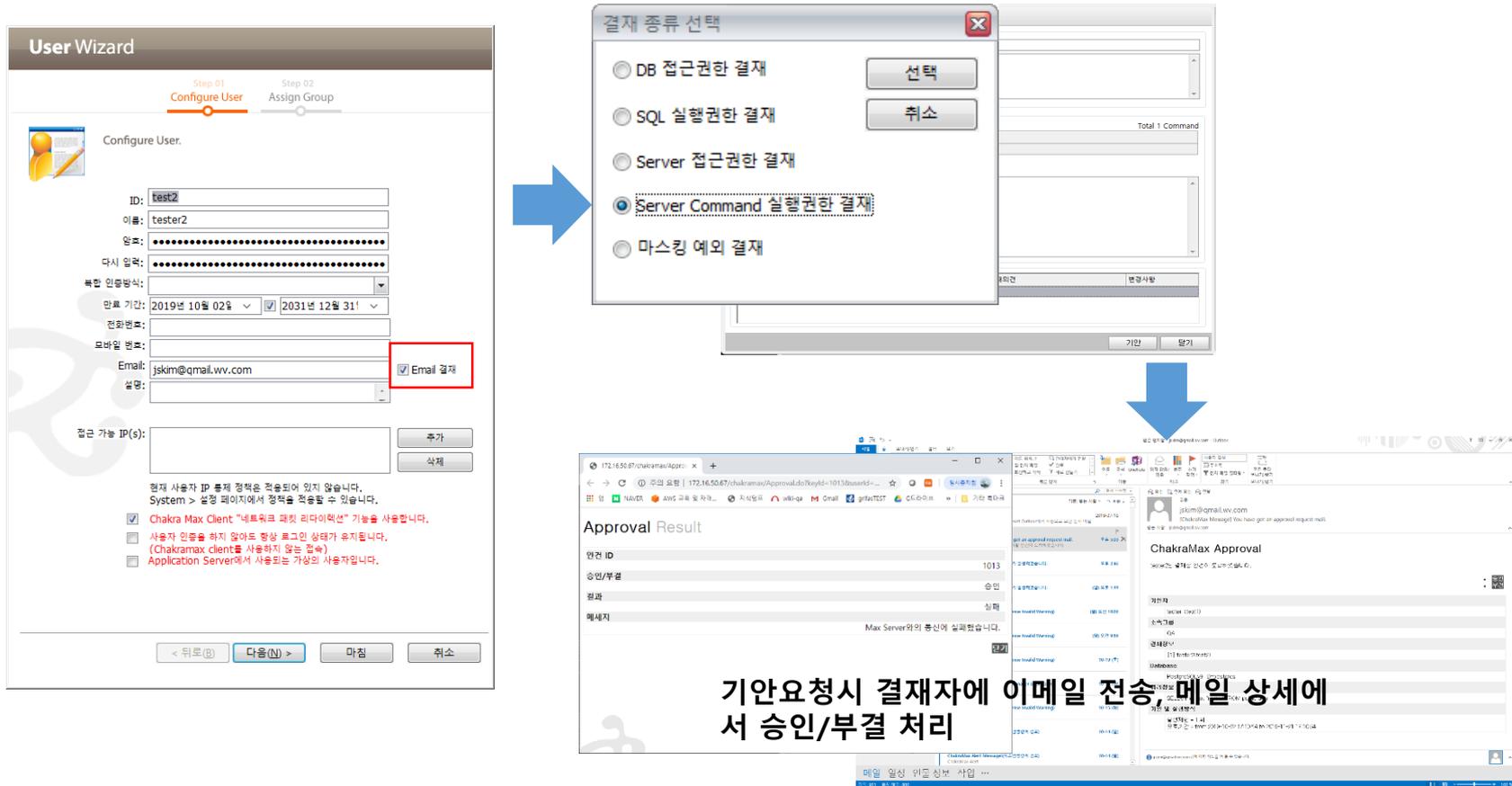
The image shows the Chakra Max interface for configuring a 'Masking Exception Approval' (마스킹 예외 결재). It consists of several parts:

- 결재 종류 선택 (Approval Type Selection):** A dialog box with radio buttons for different approval types. '마스킹 예외 결재' (Masking Exception Approval) is selected.
- 결재 안건명 (Approval Item Name):** A field for the title, set to '마스킹 예외 결재'.
- DB 실행정보 (DB Execution Info):** Fields for Database (oracle 11g), DB 사용자 (scott), 실행 정보 (모든 프로그램, 실행 제한(회) 1), 실행 날짜 (유효기간 시작날짜, 유효기간 시작시간, 유효기간 종료날짜, 유효기간 종료시간), and 결재 정보 (결재유형 테스트 결재).
- 마스킹 제외 대상 SQL 목록 (Masking Exemption SQL List):** A text area containing the SQL query: `select * from user_info`. A callout notes: 'masking 제외 대상 SQL 목록 여러 SQL 을 동시 기안 가능' (Multiple SQL queries can be submitted simultaneously for masking exemption).
- 정책 목록 (Policy List):** A list of policies with checkboxes. '마스킹 정책' (Masking Policy) is checked, and 'USER_INFO' is listed as the target.
- 결재 경로 (Approval Path):** A table showing the approval flow:

단계	사용자	이름(아이디)	안전상태(날짜)	결재의견	변경사항
1단계	부재준	leader(leader)			
- 결재 경로 확인 (Approval Path Confirmation):** A callout pointing to the approval path table.

3. 주요기능 | 이메일 결재

이메일 결재 옵션이 설정된 경우, 기안자가 기안 작성 후 결재 요청시 결재자에 이메일로 안건이 전송되고, 결재자가 이메일에서 승인/부결 처리함



3. 주요기능 | 정책 적용 권한 분리

보안정책의 등록과 적용권한을 분리하여, 적용시점에 기안-승인의 절차를 적용

Administrator Role Wizard

Step 01: Configure Administrator Role | Step 02: Grant Feature | Step 03: Assign Administrator

Configure Administrator's Role

이름: Managers
 설명: Manager Role

경보 알림 옵션: Call 등급: Critical

보안 정책:

- 보안 정책 적용 요청에 대한 결재 권한을 가집니다.
- 생성과 변경 요청은 가능하지만 적용 권한은 없습니다.

< 뒤로(B) | 다음(N) > | 마침 | 취소

보안정책 적용권
한 분리

Chakra Max

Security Information

Chakra System 정책 목록

- 정책 추가
- 정책 수정
- 정책 삭제
- 정책 복사
- 정책 활성화**
- 정책 비활성화
- 수동 무결성 체크
- 새로고침
- 들어오기
- 내보내기

해당 보안정책의 활성화를 요청합니다.

결재 관리자 : warevalley

요청 사유 :

확인 | 취소

정책을 활성화를 시도하면
자동으로 기안창이 팝업

3. 주요기능 | 변경 전/후 데이터 저장

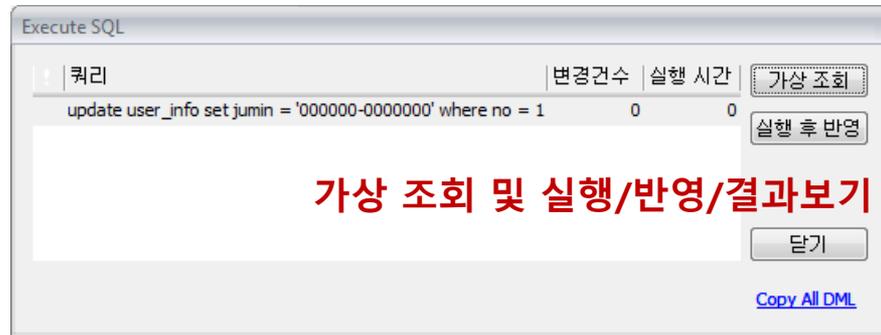
중요 정보의 수정 시 수정 전 대상 데이터 기록, 수정 후 데이터 기록
사용 툴에 관계없이 지원 (결재 & 비 결재)

```
update user_info set jumin = '000000-0000000' where no = 1;
```

update SQL 실행



정책 차단 팝업



가상 조회 및 실행/반영/결과보기



SQL Search Result(1) - 2015/03/03 ~ 2015/03/05

Found : 12 SQL (1.509초)

Application	SQL	Start Time
MAXCLIE...	UPDATE USER_INFO SET JUMIN = '000000-0000000' WHERE N...	2015/03/04 (수)
MAXCLIE...	SELECT ROWID AS "__ORACLE_JDBC_INTERAL_ROWID__", JU...	2015/03/04 (수)
MAXCLIE...	UPDATE USER_INFO SET JUMIN = '000000-0000000' WHERE N...	2015/03/04 (수)
ORANGE...	UPDATE USER_INFO SET JUMIN = '000000-0000000' WHERE N...	2015/03/04 (수)
MAXCLIE...	UPDATE USER_INFO SET JUMIN = '000000-0000000' WHERE N...	2015/03/04 (수)
MAXCLIE...	SELECT ROWID AS "__ORACLE_JDBC_INTERAL_ROWID__", JU...	2015/03/04 (수)
MAXCLIE...	SELECT ROWID AS "__ORACLE_JDBC_INTERAL_ROWID__", JU...	2015/03/04 (수)
MAXCLIE...	UPDATE USER_INFO SET JUMIN = '000000-0000000' WHERE N...	2015/03/04 (수)
MAXCLIE...	SELECT ROWID AS "__ORACLE_JDBC_INTERAL_ROWID__", JU...	2015/03/04 (수)
MAXCLIE...	UPDATE USER_INFO SET JUMIN = '000000-0000000' WHERE N...	2015/03/04 (수)
MAXCLIE...	SELECT ROWID AS "__ORACLE_JDBC_INTERAL_ROWID__", JU...	2015/03/04 (수)
MAXCLIE...	UPDATE USER_INFO SET JUMIN = '000000-0000000' WHERE N...	2015/03/04 (수)

rowid	JUMIN
1 1	777777-22222...
rowid	JUMIN
1 1	000000-00000...

변경 전/후 데이터 확인

3. 주요기능 | 보안계정 관리정책

보안계정에 대해 접속 및 패스워드 대한 다양한 정책을 제공

- 패스워드 사용기간 설정 기능
- 계정 미 사용에 따른 계정 잠김 기능 및 비밀번호 오류 시 계정 잠김
- 미 사용시 비밀번호 재 입력 기능
- 프로그램 사용 시 초기 비밀번호 설정 기능

- 패스워드 길이의 관리
- 숫자 및 특수문자를 포함한 구성
- 패스워드에 개인정보 포함 제한
- 과거 사용 비밀번호 제한
- 특정 문자열 패스워드 포함 제한

3. 주요기능 | Auto Discovery - 데이터베이스 서비스 탐색

네트워크상의 추가된 데이터베이스를 자동 검색하여 감시대상 DB로 등록 스케줄링으로 정기적인 검색을 제공

The screenshot displays the Chakra Max Service Discovery Scheduler interface. At the top, there are navigation tabs: '모니터', '정책', '검색', '보고서', '시스템', and '탐색'. The '탐색' tab is active, and a sub-tab '데이터베이스' is selected. Below this, the 'Service Discovery Scheduler' section contains a table of tasks.

Task 명	등록일	스캔 방법	탐색할 IP	탐색할 ...	설명	스캔 주기	스케줄 상태	자동 등...	최근 시작 시간	최근 종료 시간	소요 시간	진행 상태
192.168.246 스캔	2016년 01월 0...	Databa...	192.168.246.1-192...	1521-1...		즉시	만료	No	2016년 01월 08일 ...	2016년 01월 08일 ...	00:01:09	대기
mssql 스캔	2016년 01월 0...	Databa...	192.168.246.100-1...	1433		즉시	만료	No	-	-	-	진행 중

Below the table, the 'Service Discovery Wizard' is shown in two steps:

- Step 02: Define Service Discovery**
 - Discovery Method: Database Scan
 - IP Range: 192.168.246.1-192.168.246.200
 - Ping: Don't send ping Send ping
 - Ping Time-out: 2 Sec
 - Windows Computers: Don't scan Scan
 - Port Range: 1000-1500
 - Target Services:
 - ORACLE 1521
 - DB2 for Linux/Unix/... 50000
 - MSSQL Server 1433
 - Sybase ASE 4100
 - Sybase ASIQ 2638
 - MySQL 3306
- Step 03: Schedule Service Discovery**
 - Execution Date / Time:
 - Date: 2016-01-09 ~ 2016-02-07
 - Time: 오전 12:00:00
 - Frequency:
 - Every 1 주
 - Monday Tuesday Wednesday
 - Thursday Friday Saturday
 - Sunday

At the bottom, a '결과' (Results) section shows a list of discovered services. A green callout bubble points to this section with the text: "DBMS 종류 및 IP/port Range 선택".

Another green callout bubble points to the scheduling options in Step 03 with the text: "스케줄링으로 정기적인 검색".

A third green callout bubble points to the '수동 등록' (Manual Register) button in the results table with the text: "검색 결과를 바탕으로 감시대상 DB등록".

3. 주요기능 | Auto Discovery - DB 내의 민감정보 탐색

데이터베이스 테이블 및 컬럼을 패턴스캔 하여 민감정보 유무를 감지,
감지된 데이터의 샘플데이터로 민감정보 대상으로 지정하여 접근이력을 조회 / 리포팅

The screenshot shows the Chakra Max Sensitive Discovery Scheduler interface. The top navigation bar includes '탐색' (Search) and '민감정보' (Sensitive Information). The main area is divided into two wizard steps: 'Define Sensitive Data Discovery' and 'Schedule Sensitive Data Discovery'.

Define Sensitive Data Discovery: This step shows the selection of sensitive data patterns. A green callout bubble indicates '스캔할 개인정보 패턴을 선택' (Select sensitive personal information patterns to scan). The 'IT Compliance' section is checked, and a list of patterns is shown, including Credit Card Number, Email Address, Foreigner Registr..., Health Insurance..., Jumin Number, Military Number, New Passport Nu..., Old Passport Num..., and Phone Number.

Schedule Sensitive Data Discovery: This step shows the scheduling options. A green callout bubble indicates '스케줄링으로 정기적인 스캔' (Regular scan by scheduling). The 'Frequency' is set to 'Weekly', and the 'Execution Date / Time' is set to 'Date: 2016-01-08 ~ 2016-02-07' and 'Time: 오후 4:42:21'.

Task List: A table at the top shows the task configuration:

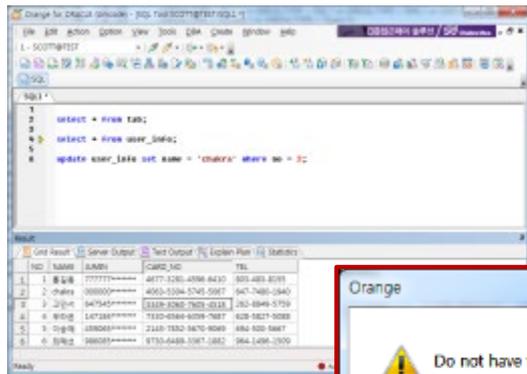
Task 명	등록일	데이터베이스	검색방법	설명	스캔 주기	스케줄 상태	자동...	최근 시작 시간	최근 종료 시간	소요 시간	진행 상태
192.168.246.1	2016년 01월 08일	ord	데이터의 패턴 검...		즉시	만료	No	2016년 01월 08일...	2016년 01월 08일...	00:00:03	대기

Results: A table at the bottom shows the results of the scan:

패턴	개수	DB 종류	개수	데이터베이스	Database ...	스키마	Table	Column	패턴	탐색 상태	샘플 데이터
Credit Card Number	1	ord	2	ord		SCOTT	USER_INFO	CARD_NO	Credit Card Nu...	등록 되지 않음	4677-3281-***...
Jumin Number	1			ord		SCOTT	USER_INFO	JUMIN	Jumin Number	등록 되지 않음	825753-*****

3. 주요기능 | 메뉴통제(오렌지연동)

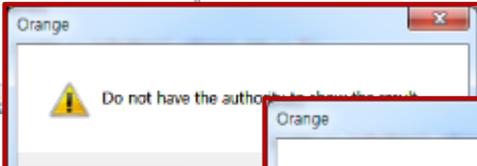
파일저장, 복사, 프린트 기능을 차단하여 중요정보의 유출을 방지하고 보안을 강화



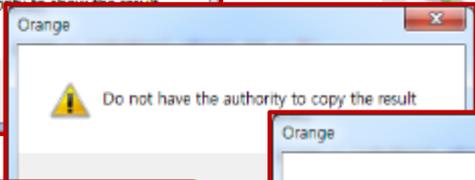
Orange 통제 연동



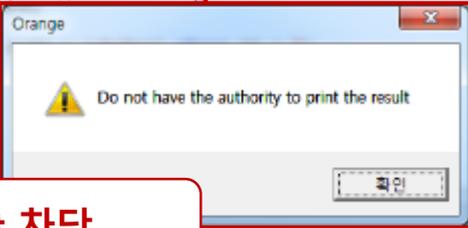
Excel export 차단



Copy 차단



Print 차단



본 기능은 WareValley Orange와 연동 시 제공되는 기능입니다.

3. 주요기능 | DB 계정은닉(오렌지연동)

가상계정 기능을 연동하여 DB 계정의 통제 및 비밀번호 은닉

Chakra Max 가상계정 설정

이 화면은 Chakra Max의 가상계정 설정 인터페이스를 보여줍니다. 상단에는 'Name', 'ID', 'Group', 'Database Account' 등의 열이 있는 테이블이 있습니다. 'test' 사용자의 설정이 표시되어 있으며, 비밀번호는 'scott****'로 은닉되어 있고, 유효기간은 '2015/03/03 ~ 2015/04/02'로 설정되어 있습니다.

아래에는 '비밀번호 저장'을 위한 옵션이 있으며, '지정된 계정만 접속을 허용'과 '사용기간을 설정'이라는 설명이 포함되어 있습니다.

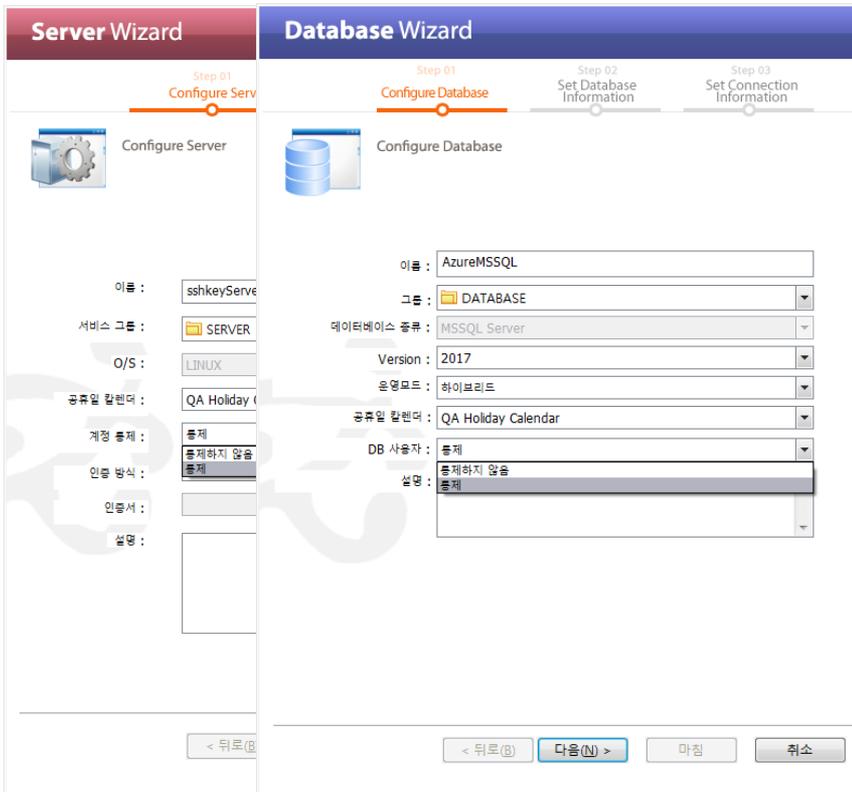
이 화면은 Oracle Enterprise Manager의 사용자 관리 인터페이스를 보여줍니다. 'User' 탭에서 'scott' 사용자가 선택되어 있으며, 'TNS Name'이 'oracle 11g_scott'로 설정되어 있습니다. '계정/비밀번호 연동'이라는 설명이 붙어 있습니다.

아래에는 '가상계정 활성화'와 '허가되지 않은 계정 접근시 차단'이라는 설명이 포함되어 있습니다. 또한, 'Warning!' 메시지가 포함된 경고 대화 상자가 표시되어 있으며, 'DB Account Not Permitted' 정책에 의해 작업이 차단되었습니다.

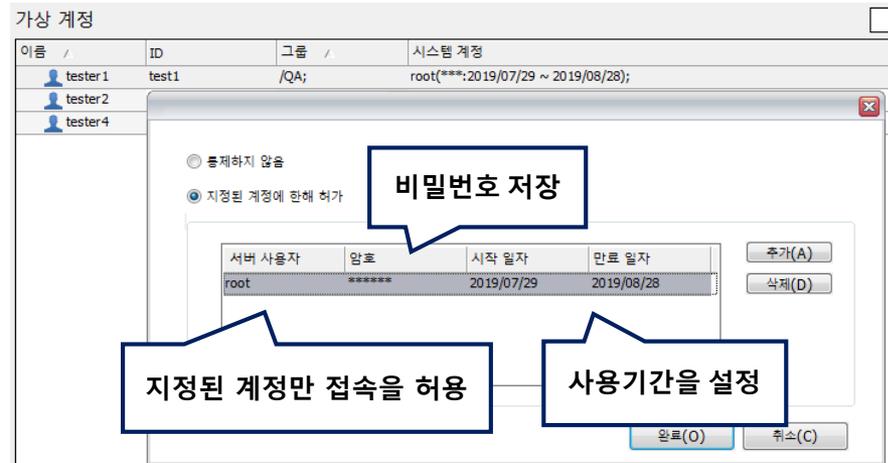
본 기능은 WareValley Orange와 연동 시 제공되는 기능입니다.

3. 주요기능 | DB / 서버 가상 계정 통제

가상계정 기능을 연동하여 사용자별로 할당된 계정에 대해서만 접속 권한을 허용하고 이외의 계정에 대해서는 통제



Chakra Max 가상계정 설정

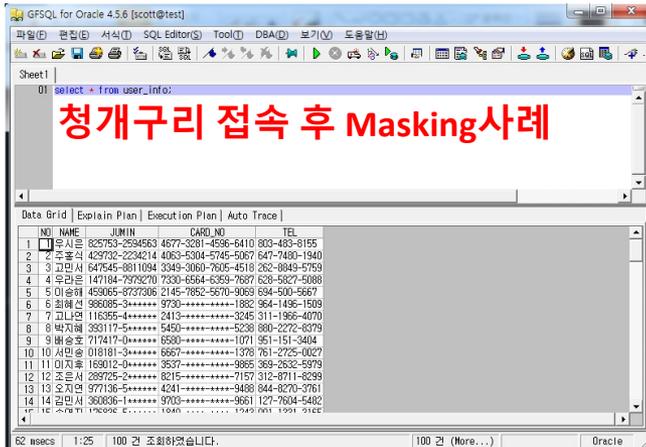
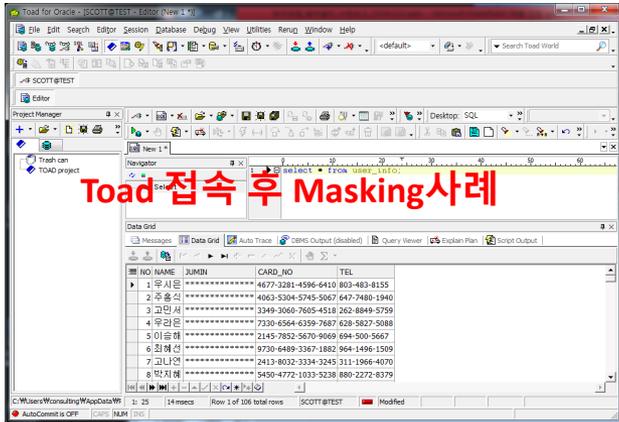


허가되지 않은 계정 접근시 차단



3. 주요기능 | 비인가 어플리케이션 접근통제

DB에 접속하는 Application의 Signature를 확인, 위변조 Application도 탐지 및 차단



- 이름
- 시간
- 설명

: Changed Application name
: 2016년 12월 23일 15:24:12

: 데이터베이스 접속 프로그램 실행 파일 이름을 임의로 변경하고 로그인 할 경우 경고를 발생립니다. 특정 프로그램에 한하여 기능이 제공됩니다. [지원 데이터베이스 : Oracle]

Detail Information

- 경보 등급 : Critical
- 서버 이름 : Linux
- 데이터베이스 이름 : Oracle
- 서비스 종류 : ORACLE
- 조건 : 사용자가 Application의 실행 파일 이름을 [UNKNOWN]에서 [GFSQL.EXE]로 수정하였습니다.
- 운영 모드 : 게이트웨이
- Policy : 상세보기

Access Information

- 클라이언트 IP 주소 : 10.180.3.2
- 응용프로그램 : GFSQL.EXE[UNKNOWN]
- 클라이언트 호스트 이름 : CONSULTING-PUB
- Chakra Max 그룹 : test
- Chakra Max 사용자 : 테스트(test)

어플리케이션 시그니처 기능을 이용한 위변조 탐지 기능 제공

3. 주요기능 | 사용자 2-Factor 인증

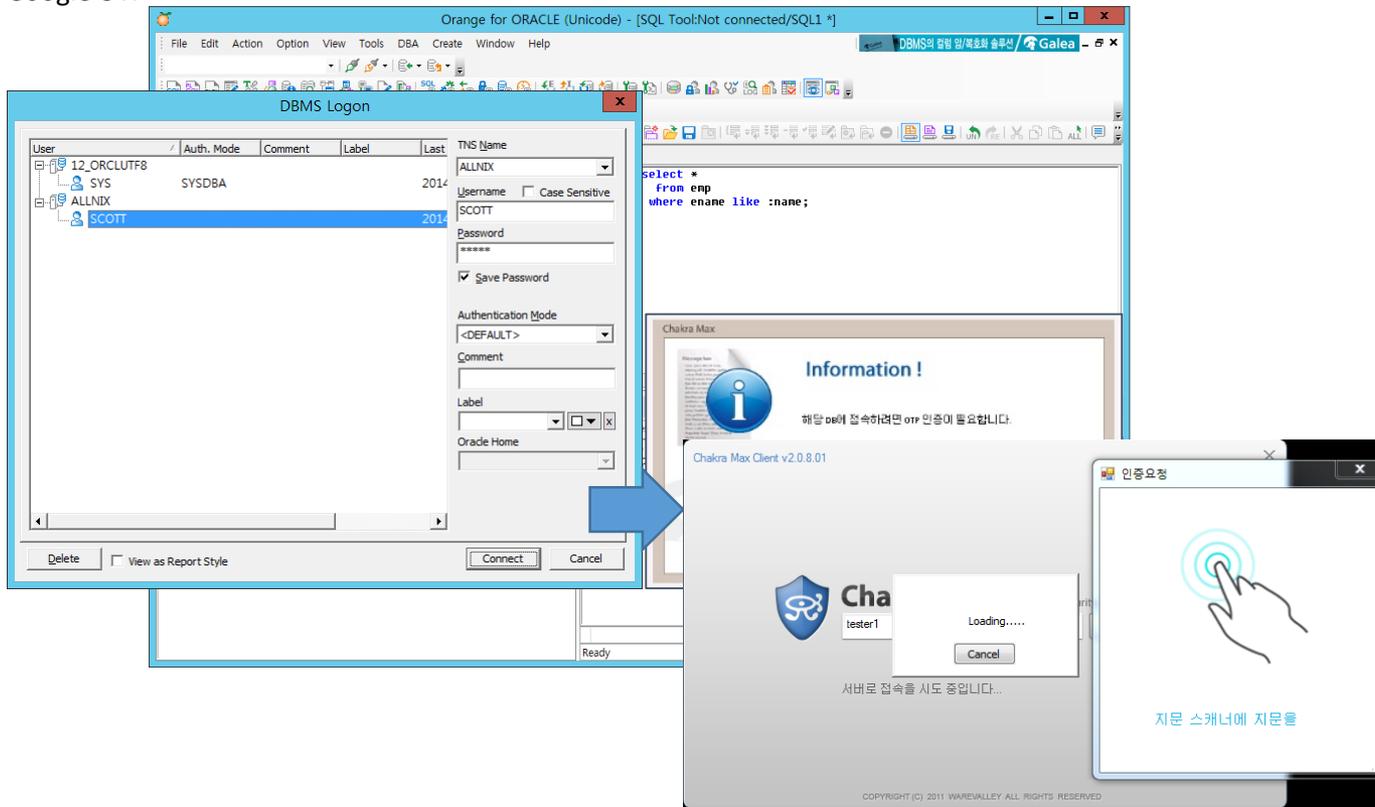
- DB접근제어 계정 및 DB접속 계정에 대한 다양한 인증 적용
- 유저 등록 화면에서 복합인증 등을 지정하여 유저 생성하여 로그인 정책 관리

- 사례

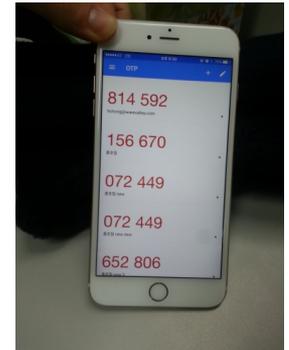
OTP 인증: 외환은행, 대우증권, KEB 하나은행, 수출입은행

인증서(PKI), Biometric(지문): KB은행

Google OTP



폐쇄 망에서도 가능한
Mobile OTP

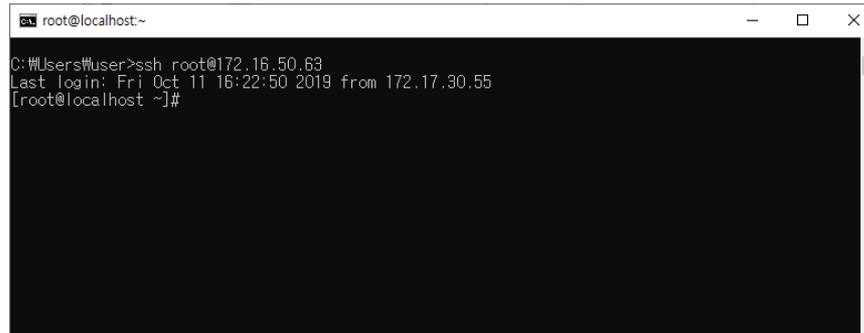
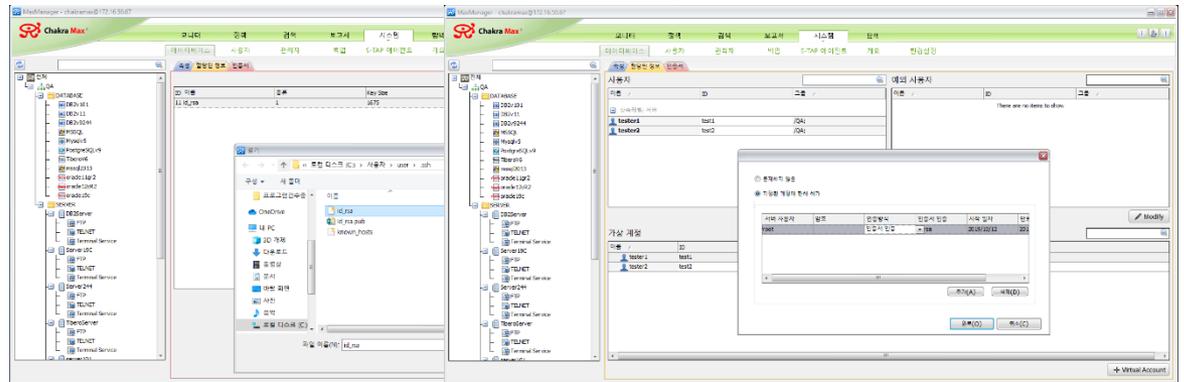


3. 주요기능 | 사용자 인증서 로그인 인증

인증서 로그인 방식은 서버 접속시 비밀번호 대신 SSH key를 제출하는 방식으로, 비밀번호 보다 높은 수준의 보안을 필요로 하거나, 비밀번호 입력 없이 자동으로 서버에 접속할 때 사용

Chakra max manager 프로그램을 통해 SSH Key의 비공개 키를 사전 등록하고 사용자의 가상계정에 할당하면, 사용자는 패스워드나 인증서 없이 권한을 할당 받은 서버에 chakra 의 인증을 거쳐 자동 로그인 할 수 있다.

지원 프로토콜 : SSH, SFTP 암호화키 지원 : RSA/DSA



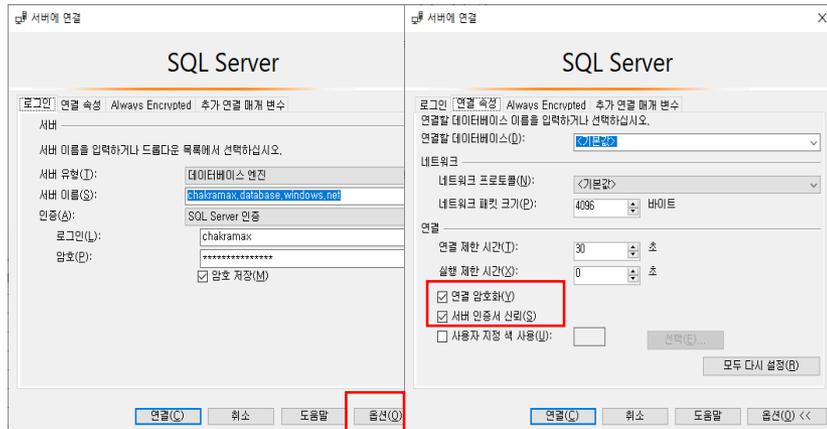
할당 받은 서버에 접속시 패스워드 입력 없이 자동 로그인 처리

3. 주요기능 | SSL/TSL 를 사용하여 암호화 연결하는 데이터베이스 지원

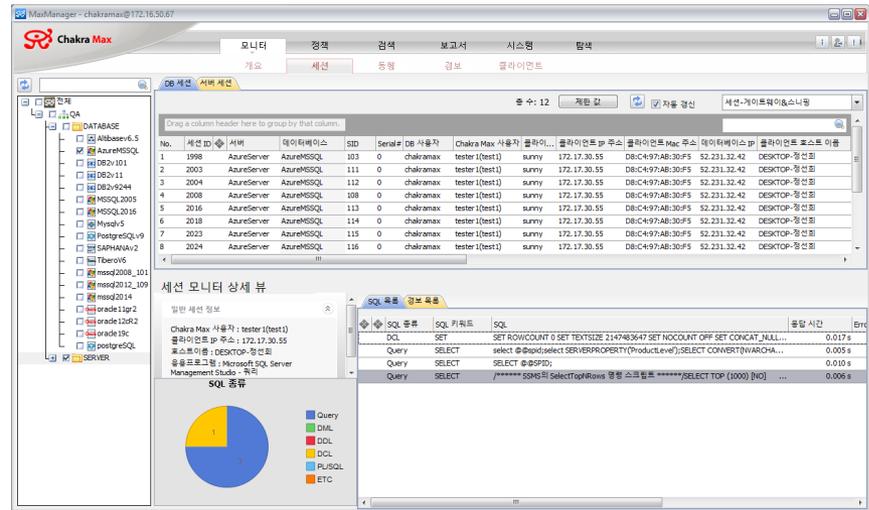
DB 접속시 TLS 암호화 통신을 하는 데이터베이스의 통신을 지원(SSL Proxy)

애플리케이션에서 SSL(Secure Socket Layer) 또는 TLS(전송 계층 보안)를 사용하여 암호화 연결하는 데이터베이스를 지원

- 지원 데이터베이스 : MSSQL, Mysql, Maria, PostgreSQL



```
[root@localhost chakramax]# tcpdump -i ens32 -X -s 0 host 52.231.32.42 and port 1433
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens32, Link-type EN10MB (Ethernet), capture size 262144 bytes
16:47:56.261042 IP 52.231.32.42.ms-sql-s > 172.16.50.67: 52724: Flags [..], seq 523564640:523564641, ack 2836901501, win 1026, length 1
0x0000: 4500 0029 34f0 4000 7406 9e7a 34e7 202a E..).4.@.t..24..+
0x0010: ac10 3243 0599 cdf4 1f34 f660 a917 ae7d ..2C.....4.....}
0x0020: 5010 0402 3765 0000 0000 0000 0000 P...7.....
16:47:56.261107 IP 172.16.50.67.52724 > 52.231.32.42.ms-sql-s: Flags [..], ack 1, win 180, options [nop,nop,TS val 4069779137 ecr 2164304565 nop,nop,sack_ (0:1)], length 0
0x0000: 4500 0040 e61c 4000 4006 2137 ac10 3243 E..@..@..@..17..2C
0x0010: 34e7 202a cdf4 0599 a917 ae7d 1f34 f661 4..+.....3..4.a
0x0020: b010 00b4 3397 0000 0101 080a f293 fbfb ...3.....
0x0030: 8108 4bd3 0101 050a 1f34 f660 1f34 f661 ..K.....4..4.a
16:47:57.224387 IP 52.231.32.42.ms-sql-s > 172.16.50.67: 52672: Flags [..], seq 3387691133:3387691134, ack 2785064306, win 1024, length 1
0x0000: 4500 0029 1442 4000 7406 bf28 34e7 202a E..).@e.t..(4..+
0x0010: ac10 3243 0599 cdc0 c9ec 107d a305 c4f2 ..2C.....3.....}
0x0020: 5010 0400 6263 0000 0000 0000 0000 P...b.....
16:47:57.224445 IP 172.16.50.67.52672 > 52.231.32.42.ms-sql-s: Flags [..], ack 1, win 191, options [nop,nop,TS val 4069770100 ecr 2184734285 nop,nop,sack_ (0:1)], length 0
0x0000: 4500 0040 9482 4000 4006 ba01 ac10 3243 E..@..@e..@..2C
0x0010: 34e7 202a cdc0 0599 a305 c4f2 c9ec 107e 4..+.....3.....t
0x0020: b010 00b4 3397 0000 0101 080a f293 c374 ...3.....
0x0030: 8239 50aa 0101 050a c9ec 107d c9ec 107e ..9P.....
16:47:57.245449 IP 52.231.32.42.ms-sql-s > 172.16.50.67: 52732: Flags [..], seq 2862313708:2862313709, ack 2939517523, win 1026, length 1
0x0000: 4500 0029 56bc 4000 7406 7cae 34e7 202a E..).V.@.t..1.4..+
```

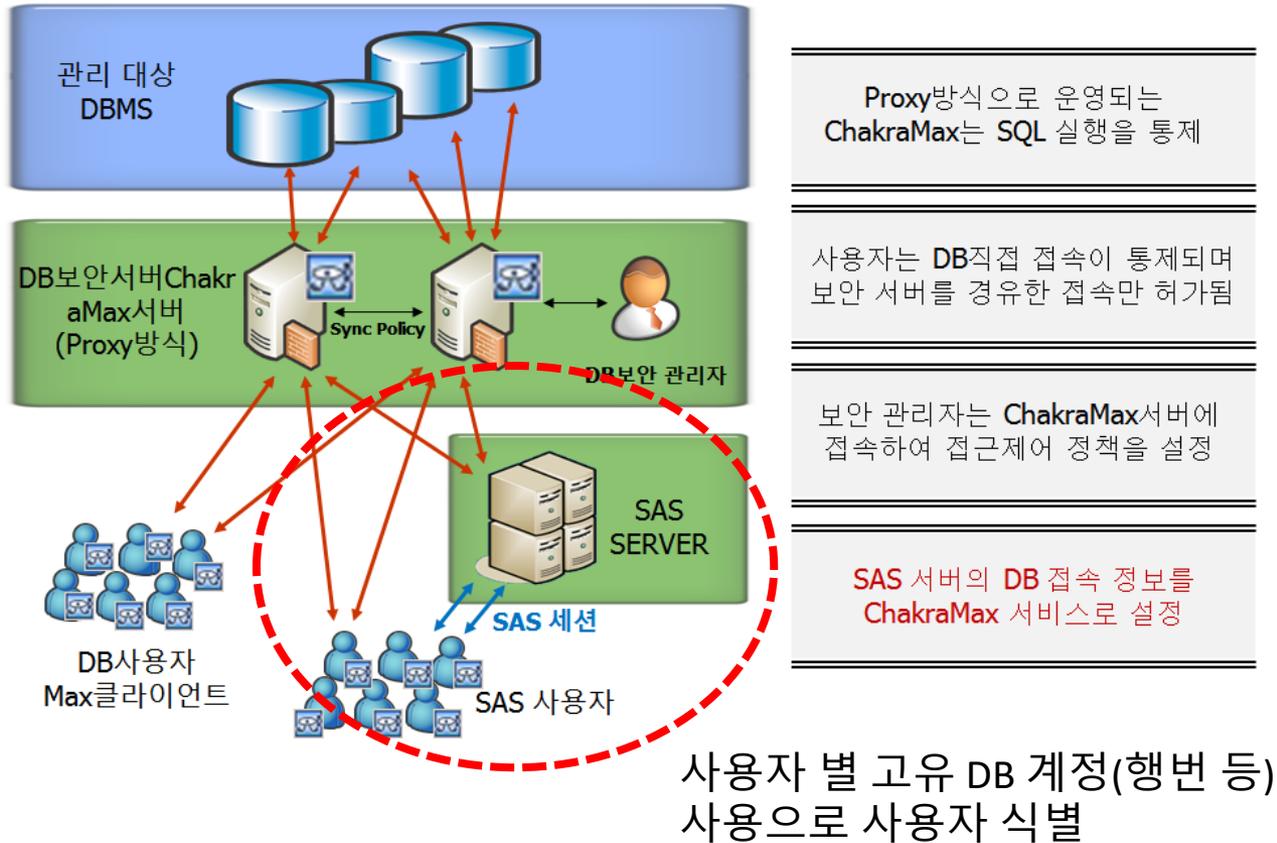


DB에 접속시 “연결 암호화” 옵션에 따라, 전송 데이터가 암호화되어 통신됨.

샤크라는 proxy 암호화 연결을 중계하여, 통제 및 감사로그를 수집

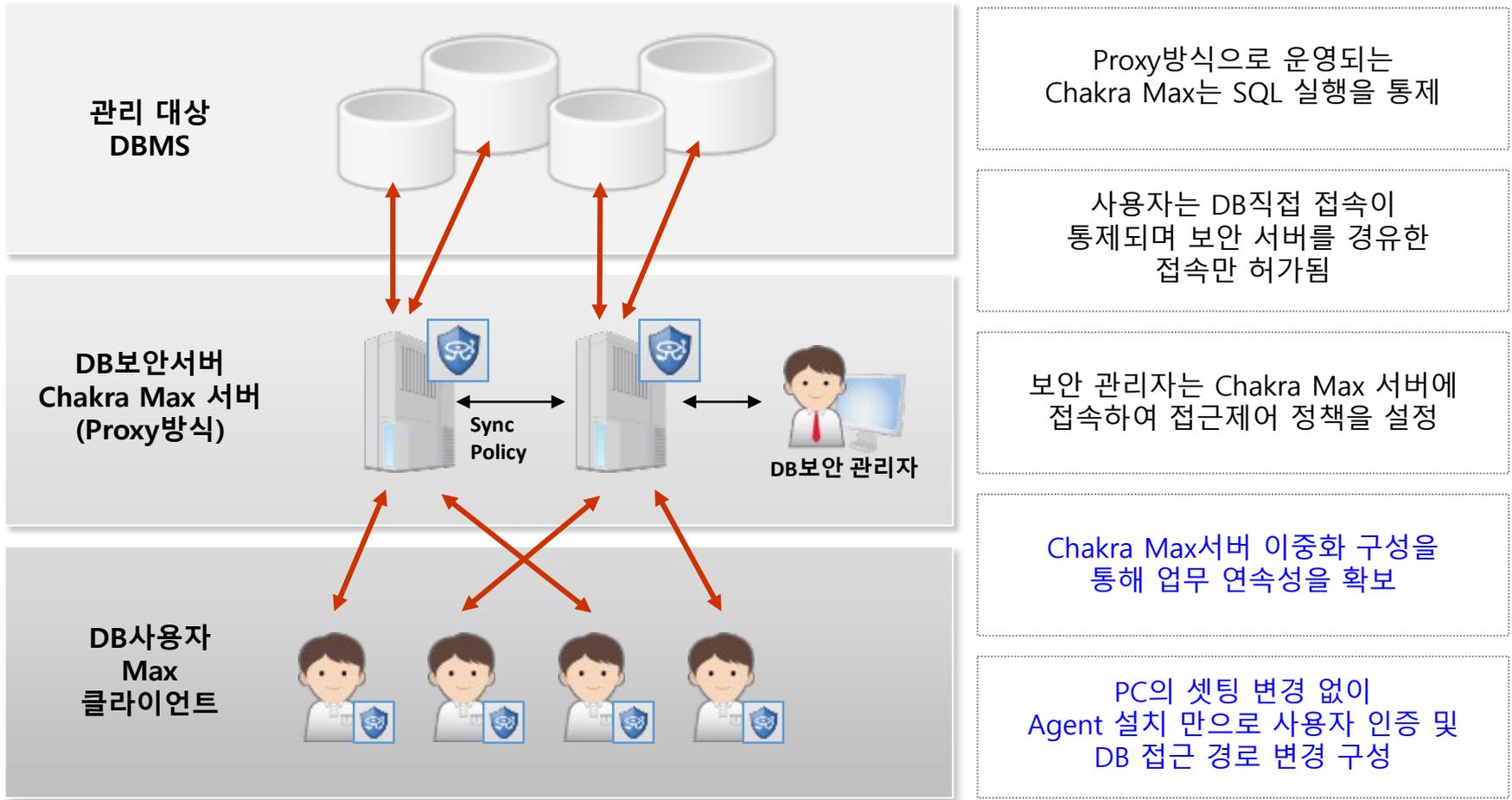
3. 주요기능 | SAS, OLAP, BO 등 3 Tier 사용자의 비정형 쿼리 통제

여러 DB의 주요정보에 접근 가능한 시스템을 Chakra Max와 연동하여 식별 및 통제



4. 관리기능 | 운영환경

Chakra Max는 고객의 DB환경 변화 없이 기존 구성 그대로 적용 가능



Proxy방식으로 운영되는 Chakra Max는 SQL 실행을 통제

사용자는 DB직접 접속이 통제되며 보안 서버를 경유한 접속만 허가됨

보안 관리자는 Chakra Max 서버에 접속하여 접근제어 정책을 설정

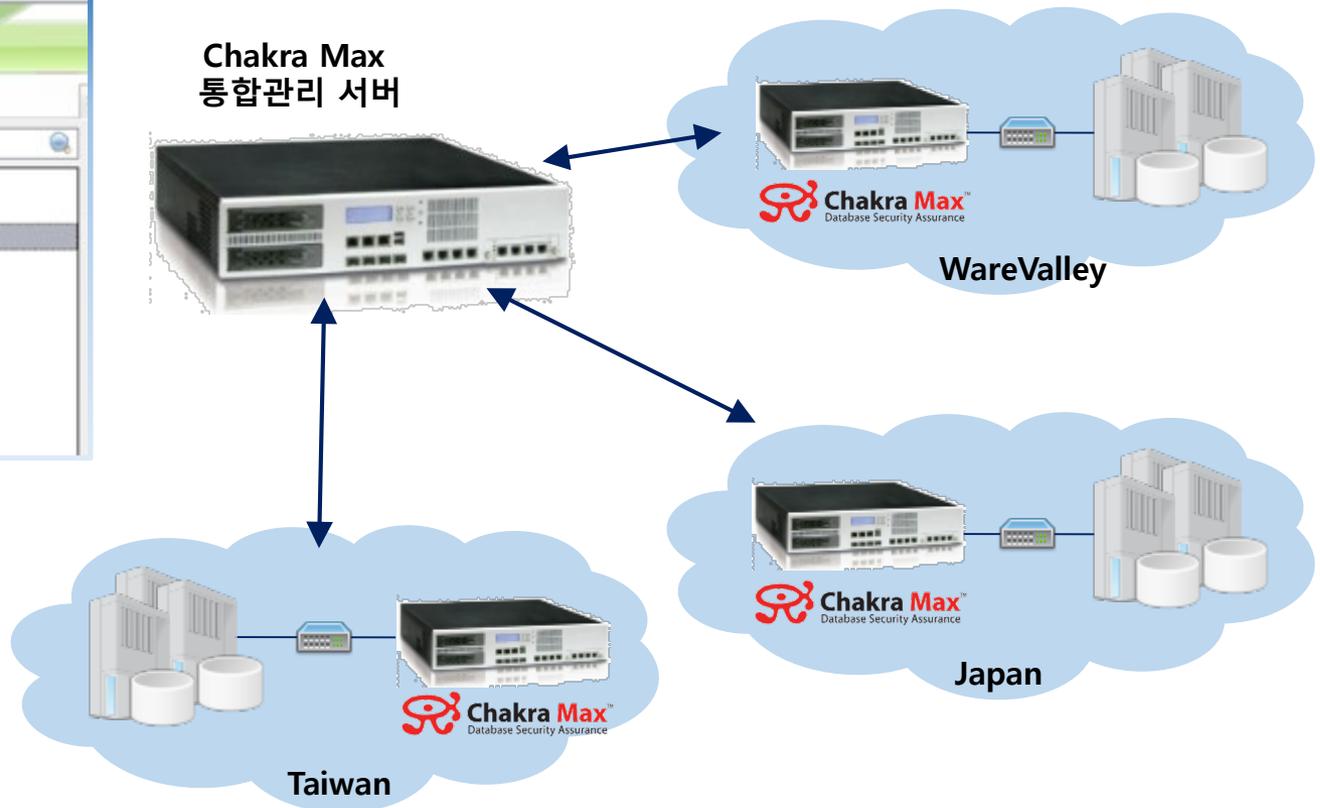
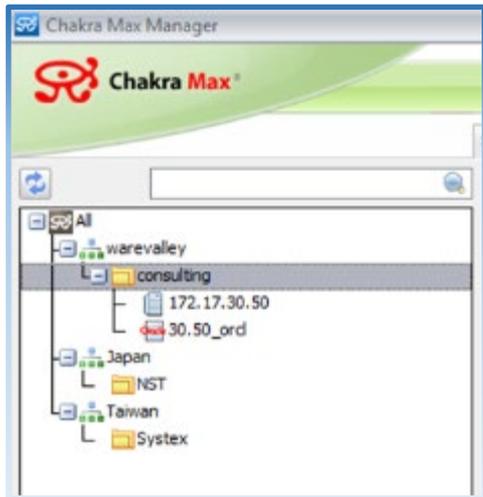
Chakra Max서버 이중화 구성을 통해 업무 연속성을 확보

PC의 셋팅 변경 없이 Agent 설치만으로 사용자 인증 및 DB 접근 경로 변경 구성

4. 관리기능 | 중앙관리기능

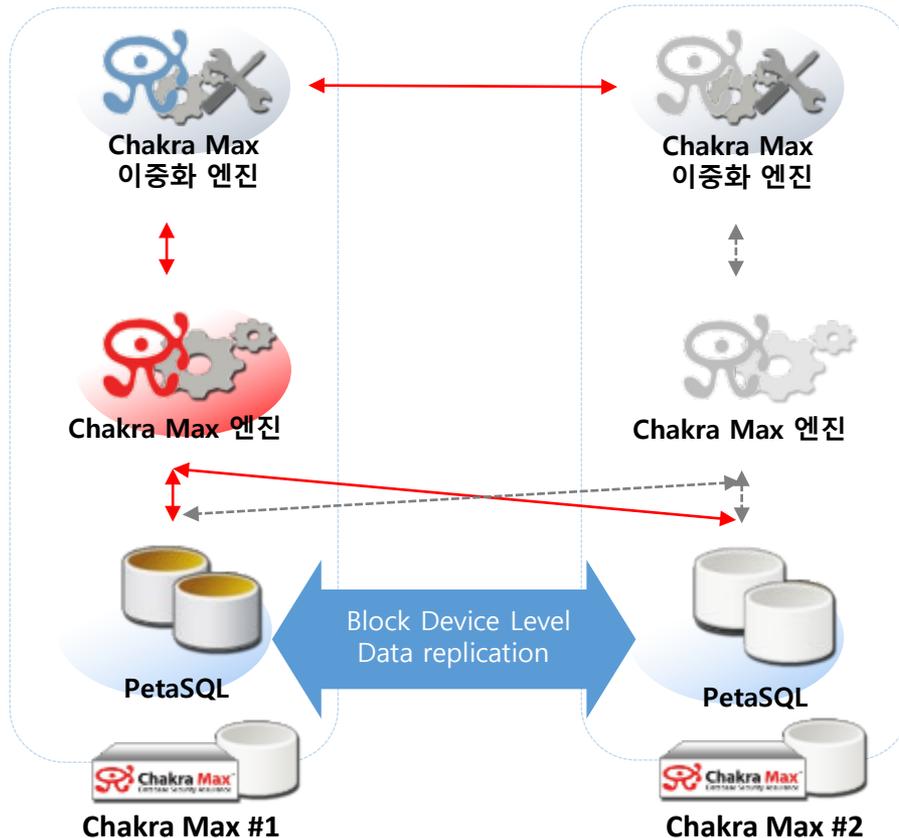
Central Management(CM)기능을 통한 중앙 모니터링

(통합 Alert 모니터링 / 보안정책 관리 / 로그 검색 / 보고서 생성이 가능)



4. 관리기능 | 이중화

Chakra Max 엔진 및 로그데이터 이중화 기능



**Partition-Level Replication 적용으로
"감사 로그 유실 방지"**

**엔진 이중화 및 PetaSQL 이중화를 통한
"업무 연속성 보장"**

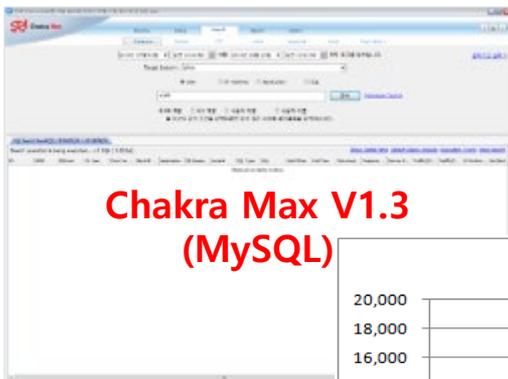
- 장애 대비를 위한 Active-Standby 구성 지원
- Load balancing을 위한 Active-Active 구성 지원

DB 접근제어서버의 엔진 이중화 및 로그용 DBMS의 이중화로 서비스의 연속성 확보 및 로그데이터 유실 방지 강화

4. 관리기능 | 고속데이터 분석용 DBMS(PetaSQL) 탑재

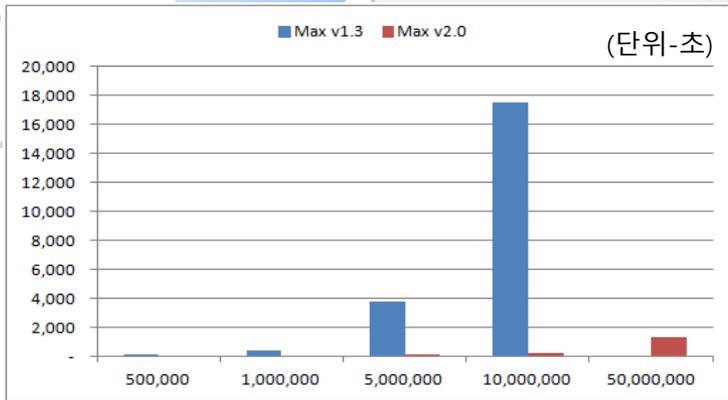
Column Stored DBMS (PetaSQL) 탑재로 더욱 빨라진 로그검색

Fast-Loading / Real-time Analysis 데이터 베이스
 Column based database로 OLAP에 특화
 기존 Chakra Max V1.3 대비 약 1600%이상의 검색 효율 증가



Chakra Max V1.3 (MySQL)

Chakra Max V2.0 (PetaSQL)



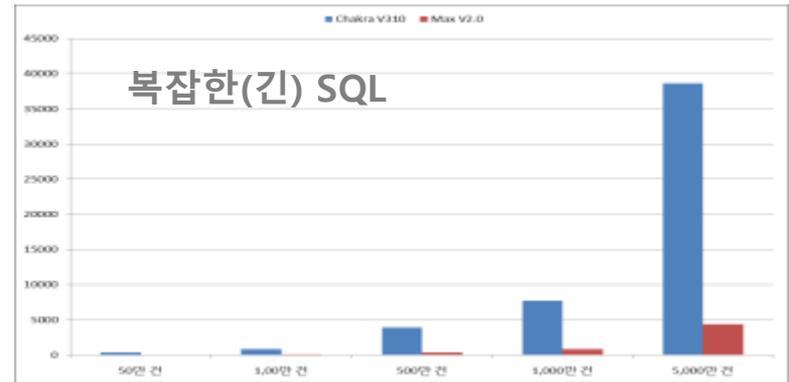
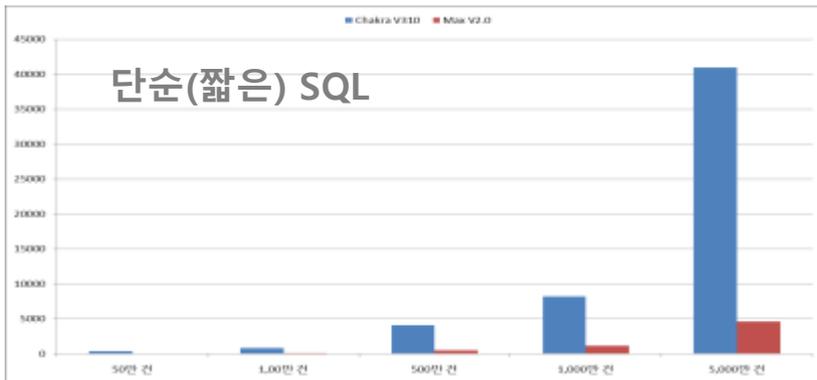
	500,000건	1,000,000건	5,000,000건	10,000,000건	50,000,000건
Max v1.3	192	472	3,794	17,580	N/A
Max v2.0	13	28	128	240	1,302

4. 관리기능 | 고속데이터 분석용 DBMS(PetaSQL) 탑재

Column Stored DBMS (PetaSQL) 탑재로 로그기록용 디스크의 효율적 운영

Dictionary 기반 중복데이터 제거를 통한 데이터 감소
기본 압축 기능 강화를 통한 디스크 사용량 감소

SQL 로그 데이터 저장 시 MySQL 대비 약 1/10 수준의 저장 공간 사용



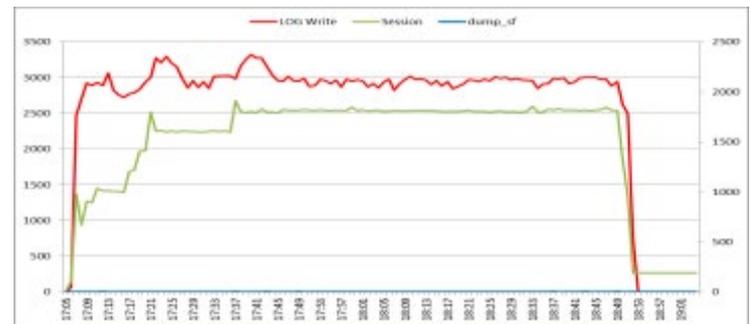
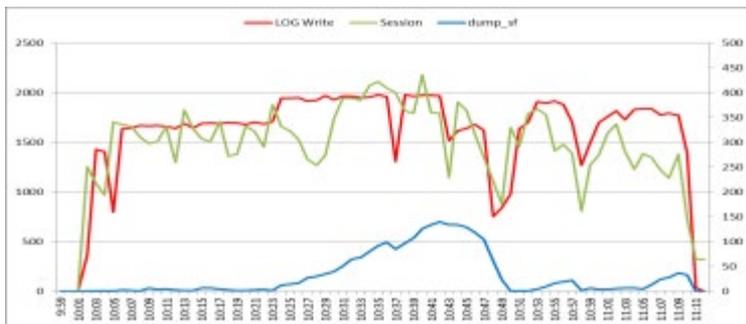
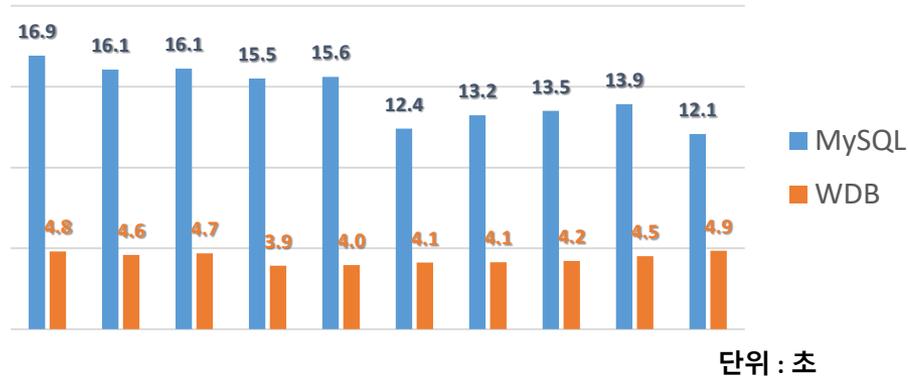
	50만 건	1,00만 건	500만 건	1,000만 건	5,000만 건	비고
Chakra V3.1	402	804	4,096	8,192	40,960	select * from dual_NUMBER where dummy_NUMBER_ = _NUMBER_
Max V2.0	54	104	491	1,135	4,616	
Chakra V310	385	797	3,890	7,716	38,619	Select * from dual where dummy = _NUMBER_
Max V2.0	52	74	388	844	4,338	

동일한 DB에 대하여 Chakra V3.1(MySQL)과 Chakra Max V2.0(PetaSQL) 를 이용하여 감사 시도 한 후 로깅 된 데이터 용량

4. 관리기능 | 고속데이터 분석용 DBMS(PetaSQL) 탑재

Column Stored DBMS (PetaSQL) 탑재로 로그기록 시간 단축 및 I/O 병목 해결

Chakra Max Repository 사용시 로그 Log write 시간
- 기존 MySQL 대비 약 200% 로그 기록 효율 증가



180byte 20만 row insert 20회 시도 후 최저, 최고 값 제외 후 10회에 대한 평균 값 산출

4. 관리기능 | 데이터 위변조 - 테이블 보호 기능

로그 데이터의 위변조 방지를 위하여 PetaSQL의 로그 저장 테이블에 Chakra Max 엔진만 쓰기 및 변경이 가능하며 사용자 접근 시 읽기로 제한

로그 위변조 방지를 위한 임의의 로그테이블 쓰기 방지 기능 (Chakra Max 엔진만 가능)

	inst_name	client_ip	db_user	date	sql_text
1	oracle	192.168.0.200	SCOTT	2015-03-04	SELECT DBMS_TRANSACTION.LOCAL_TRANSACTION_ID FROM DUAL
2	oracle	192.168.0.200	SCOTT	2015-03-04	SELECT DBMS_TRANSACTION.LOCAL_TRANSACTION_ID FROM DUAL
3	oracle	192.168.0.200	SCOTT	2015-03-04	SELECT DBMS_TRANSACTION.LOCAL_TRANSACTION_ID FROM DUAL
4	oracle	192.168.0.200	SCOTT	2015-03-04	SELECT DBMS_TRANSACTION.LOCAL_TRANSACTION_ID FROM DUAL
5	oracle	192.168.0.200	SCOTT	2015-03-04	SELECT /*+ LEADING(S) */ INST_ID, SID, SERIAL#, OSPID, ORANGE.ORANGE_FN_HOST_NAME,
6	oracle	192.168.0.200	SCOTT	2015-03-04	SELECT USERENV(♣), SYS_CONTEXT(♣,♣) FROM DUAL
7	oracle	192.168.0.200	SCOTT	2015-03-04	SELECT S.SERIAL#, P.SPID, S.SERVER FROM V\$SESSION S, V\$PROCESS P WHERE S.SID = ♣ AND
8	oracle	192.168.0.200	SCOTT	2015-03-04	SELECT * FROM V\$NLS_PARAMETERS
9	oracle	192.168.0.200	SCOTT	2015-03-04	ALTER SESSION SET NLS_LANGUAGE=♣ NLS_TERRITORY=♣ NLS_CURRENCY=♣
10	oracle	192.168.0.200	SCOTT	2015-03-04	BEGIN DBMS_APPLICATION_INFO.SET_MODULE(:Module,:Action); END;
11	oracle	192.168.0.200	SCOTT	2015-03-04	SELECT USERNAME FROM ALL_USERS
12	oracle	192.168.0.200	SCOTT	2015-03-04	SELECT OBJECT_NAME, OBJECT_TYPE FROM ALL_OBJECTS WHERE UPPER(OWNER) = UPPER(:owner)
13	oracle	192.168.0.200	SCOTT	2015-03-04	SELECT /*+ LEADING(S) */ INST_ID, SID, SERIAL#, OSPID, ORANGE.ORANGE_FN_HOST_NAME,

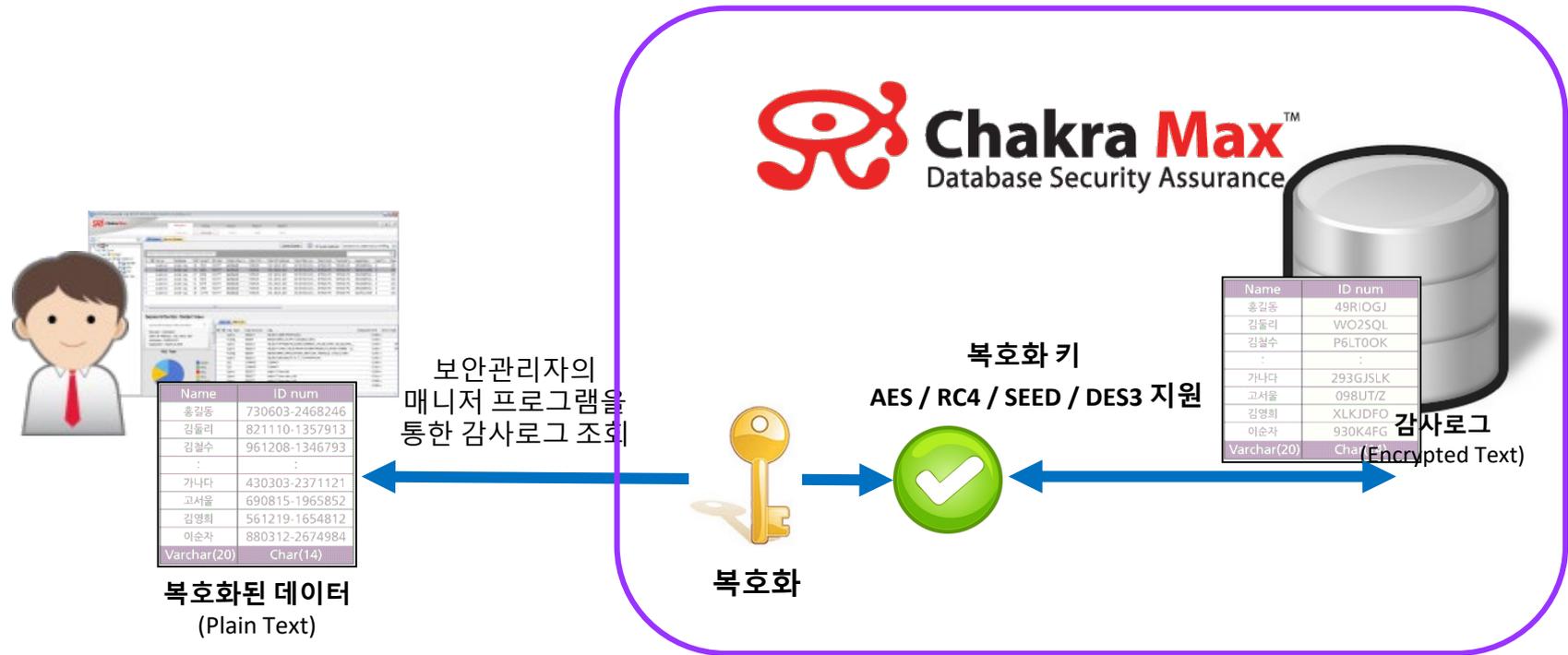
엔진에서 저장된 로그데이터

사용자가 Repository DB에 접근하여 로그 테이블에 update, delete 등을 시도하였을 테이블이 보호되어 실행을 할 수 없음

```
wdb sql> update sql_log 20150304 set sql_text = 'select * from tab;';
UPDATE: cannot update protected table 'sql_log_20150304'
wdb sql>
wdb sql> delete from sql_log 20150304;
DELETE FROM: cannot delete protected table 'sql_log_20150304'
```

4. 관리기능 | 데이터 위변조- 감사로그 암호화 지원

엔진이 감사 테이블을 생성시 암호화된 테이블로 생성하고, 로그데이터를 암호화하여 저장함으로써 실제 데이터를 식별할 수 없도록 감사로그 데이터의 보안 기능을 강화
관리자가 매니저 프로그램을 통해 로그 조회시에 복호화 키를 이용하여 복호화된 로그를 표시



** 감사 로그 테이블의 컬럼을 암호화하여, 복호화키 없는 불법적인 데이터 열람시 식별 불가

4. 관리기능 | 개인정보 보호- 감사데이터 마스킹 처리

샤크라가 수집하여 저장하는 감사로그내의 개인정보를 보호하기 위한 기능으로, 민감정보로 등록된 데이터를 자동 인식하여, 수집 저장하는 감사로그(SQL, 리턴로우)에 포함된 개인정보를 마스킹 처리

The image shows the MaxManager interface for configuring sensitive patterns. The 'Sensitive Pattern' dialog box is open, showing the following configuration:

- Pattern Name: Jumin Number
- Description: identification number ex) 800101-1987654
- Regular Expression: `^(0-9]{6})([0-9]{1-4}){0-9}{6}$`
- Ordinary Column Name: JUMIN;
- Data Check Length: 13 ~ 14

The 'Masking' section is checked for both search and report masking. The Masking Format is set to `*****$7$8$9$10$11$12$13$14`.

The main MaxManager window shows a monitoring dashboard with the following data table:

지 그룹 이름	클라이언트 호스...	클라이언트 IP 주...	응용프로그램	D...	S...	SQL...	SQL
QA	정원희입우노트북	172.17.30.55	ORANGEMAI...	0	0	Query	SELECT * FROM MASKINGTEST

The SQL query results are displayed in a table:

NO	NAME	JUMINNUM	EMAIL	CARDNO
1	tester	752222*****	tester@test.com	6360****5****7-5219
2	developer	752222*****	developer@tes...	6360****5****7-5219
3	manager	752222*****	manager@test...	6360****5****7-5219
4	director	752222*****	director@test.c...	6360****5****7-5219
5	sunnyjung	750321*****	sunnyjung@le...	6360****5****7-5219
6	tester	750321*****	tester@test.com	6360****5****7-5219
7	developer	750321*****	developer@tes...	6360****5****7-5219
8	manager	750321*****	manager@tes...	6360****5****7-5219
9	director	750321*****	director@test.c...	6360****5****7-5219

4. 관리기능 | 통신구간 암호화

Chakra Max는 사용자와 데이터베이스 서버의 구간 DB 세션 암호화를 기능을 지원하여 통신 구간의 보안성을 강화

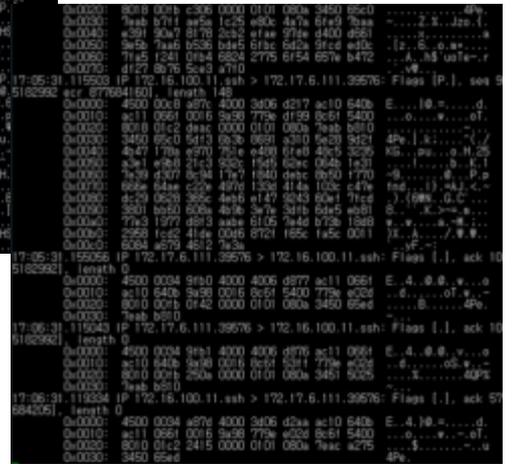
사용자 <-> Chakra Max <-> DB 서버 : 모든 구간의 암호화 통신



사용자 - Chakra Max 구간 암호화



Chakra Max - DB 서버 구간 암호화



구간 암호화 옵션 활성화, DB서버 ssh 계정/비밀번호 입력

4. 관리기능 | 통신보안 강화를 위한 GW Port 단일화

시스템 운영측면의 보안 강화기능으로 DB접근제어 시스템의 gw 운영시 서버나 데이터 베이스 별로 포트를 open 오픈하여 운영하던 방식을 변경하여, 하나의 port 로 통신할 수 있도록 지원

```
wdb sql> select * from max_config where param like '%proxy_uni%'
+-----+-----+-----+-----+-----+
| key_id | param                               | value | value_ | defa  |
|-----+-----+-----+-----+-----+
| 279    | proxy_unification_port              | 0     | 1      | 0     |
| 282    | proxy_unification_ssh_port          | 1025  | 1      | 0     |
+-----+-----+-----+-----+-----+
2 tuples (4.575ms)
```

```
root@localhost:/home
Using username "root".
root@172.16.50.63's password:
Last login: Mon Nov 18 17:37:07 2019 from 172.16.50.67
[root@localhost ~]# ls
anaconda-ks.cfg  install.log.syslog  문서          사진          다운로드
dap_svr.pid      공개              바탕화면      비디오       템플릿
install.log      다운로드
[root@localhost ~]# cd
```

사용자가 ssh 접속시, 기존의 10106 port 가 아닌 1025 port 로 통신

```
[root@localhost ~]# netstat -anp | grep 10106
[root@localhost ~]# netstat -anp | grep 1025
tcp        0      0 0.0.0.0:1025          0.0.0.0:*          LISTEN     25154/./cgw_gw
tcp        0      0 172.16.50.67:52236  172.16.50.67:1025  ESTABLISHED 27780/sshd: chakraf
tcp        0      0 172.16.50.67:1025  172.16.50.67:52236  ESTABLISHED 25154/./cgw_gw
[root@localhost ~]#
```

The screenshot shows the Chakra Max interface with the 'Server Information' window open. The 'Network Services' table is highlighted, showing the following data:

Service	Deploy Mode	Network Information IP (Service Port/Gateway Port)	Language Encoding	Response Logging
TELNET	하이브리드	172.16.50.63 (23/10105)	자동	Yes
SSH	게이트웨이	172.16.50.63 (22/10106)	자동	Yes
FTP	하이브리드	172.16.50.63 (21/10107)	자동	No

4. 관리기능 | 감사로그 백업

일일 로그데이터의 자동 백업 및 복구 복구 기능 제공

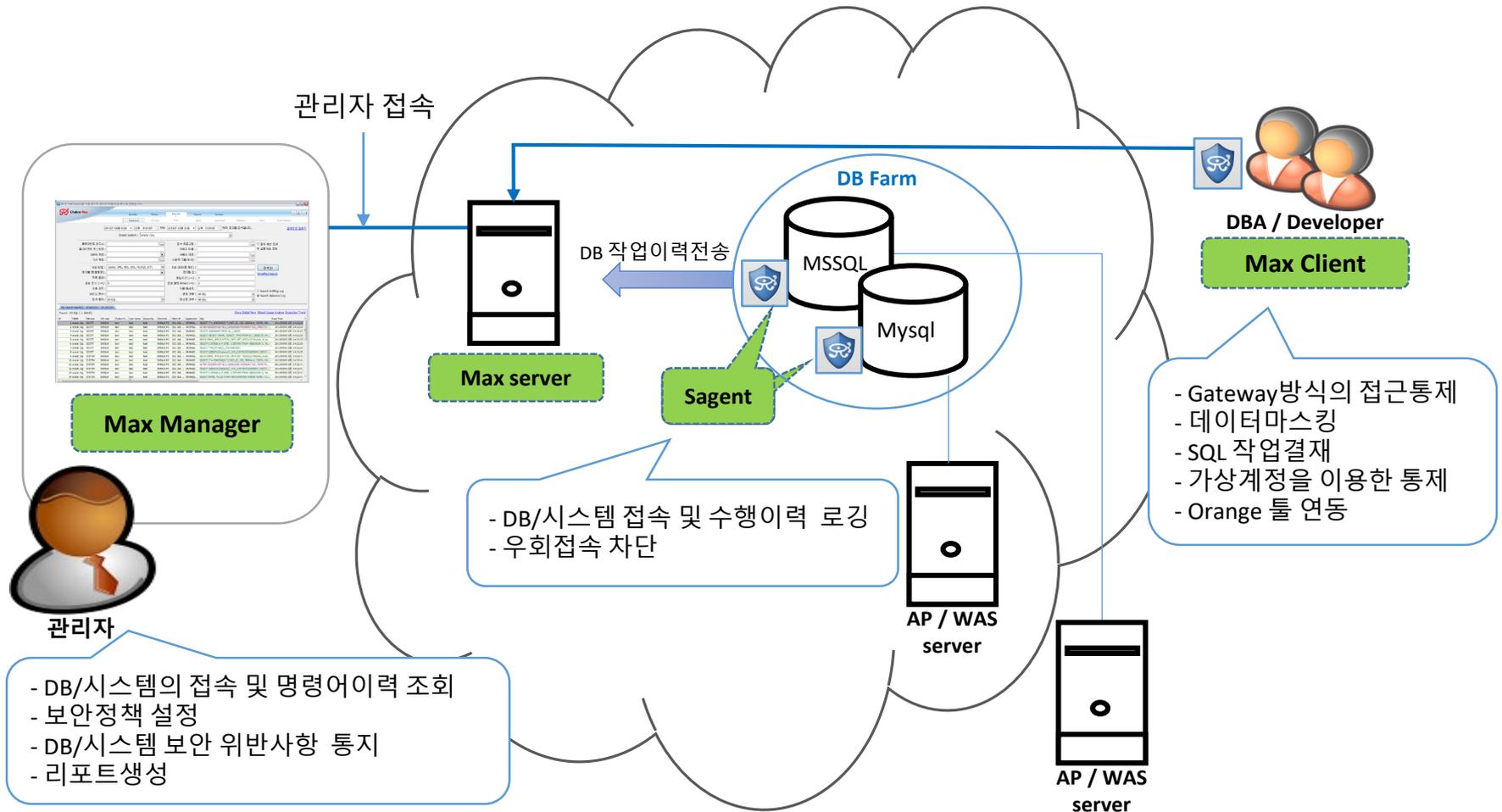
The screenshot displays the Chakra Max interface with several key sections:

- Backup History Table:** A table listing backup operations with columns for DB Status, Log Date, Execute, File Path, Backup Size, Free Sp., Start Time, End Time, Duration Time, and Description. It shows a series of successful backups for 'db_trend' and 'max_engine'.
- Backup Policy:** A calendar view for 2015, showing a daily backup schedule for 'db_trend' and 'max_engine'.
- Schedule Configuration:** A panel on the right for setting the backup schedule, including options for 'Daily Backup', 'Start Time' (01:00), 'Email Notification Options' (Notify on Failure), and 'Split File' settings.
- Backup File Location:** A table showing the file location for 'Chakra Max Database' as 'home/chakramax/log_backup'.
- Audit Log Retention Period:** A table listing retention periods for different log categories: 'Database 접속 이력 로그' (365 days), 'SQL 실행 로그' (365 days), and 'Alert' (365 days).

감사로그 및 설정 데이터 백업 및 복구 기능
 성공/실패 여부 확인
 저장위치, 시간, 용량 등의 정보 확인
 일일 백업 스케줄링 설정

4. 관리기능 | Cloud 환경 지원

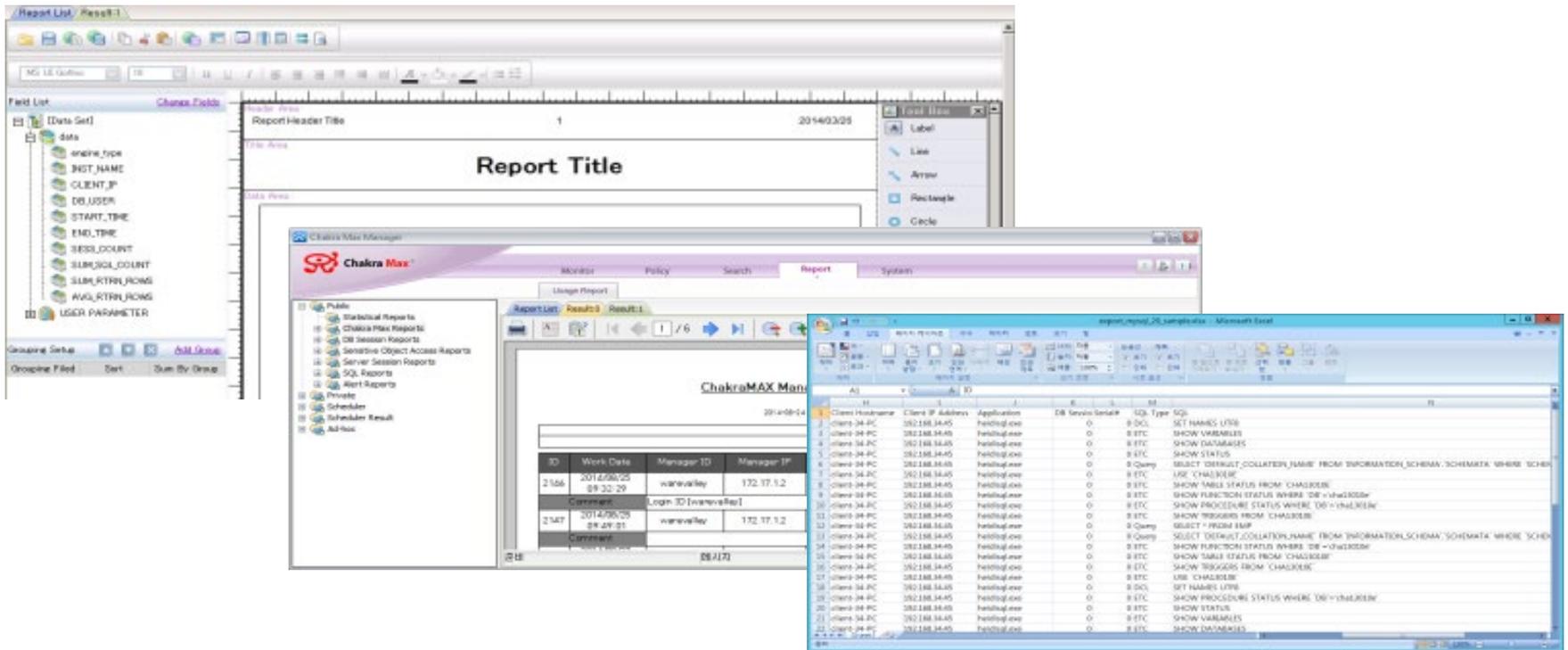
AWS, IBM, KT U cloud 등, 다양한 Cloud 환경에서 Gateway 및 Sniffing 모드 제공



4. 관리기능 | 보고서

신규 보고서 엔진(Oz Report)을 탑재하여 더욱 편리한 보고서 기능

스케줄러를 이용한 보고서 **“자동 생성과 메일 전송”**
Excel, PDF, DOC, HWP 등 다양한 문서 포맷 제공
Ad-hoc 보고서 디자이너를 제공하여 필요한 보고서 디자인이 가능
약 50여 종에 달하는 다양한 형식의 보고서 포맷 제공



4. 관리기능 | 관리자 알림 기능

DB접근제어 시스템 성능 모니터링 및 임계치 초과 알림 기능

The screenshot displays the Chakra Max monitoring interface. On the left, there are several performance charts for 'ChakraMax(0) (LDRX)' and 'Engine Status'. A 'System Overview Setting' dialog box is overlaid in the center, showing configuration options for CPU, Memory, and Disk usage alerts. On the right, the 'Administrator Wizard' is shown, with the 'Configure Administrator' step active. The 'Email' field in the wizard is highlighted with a red box, and a blue arrow points from the '확인' button in the dialog box to this field.

System Overview Setting

System Overview

Chakra Max 시스템의 자원 사용률이 임계치에 도달하면 Alert(Resource Usage of Chakra Max)을 기록하고 관리자에게 통보합니다.

관리자의 연락처는 System > Administrator 에서 설정합니다.

관련 정책이 활성화 되어 반영됩니다.

CPU : %
Memory : %
Disk : %

Administrator Wizard

Step 01: Configure Administrator | Step 02: Assign Administrator Role | Step 03: Assign Service Group

Configure Administrator

ID: warevalley
Name: Administrator
Password:
Confirm Password:
Complex Authentication: [v]
Expiration Date: 2015년 02월 13일 ~ 2031년 12월 31일
Mobile Phone: [v]
Phone: [v]
Email: consulting@warevalley.com
Description: Administrator
Acceptable IP: 192.168.0.200

< 뒤로(B) > 다음(N) > 마법 취소

**DB접근제어 시스템 자원사용률
초과시 관리자 E-Mail로 전송**

4. 관리기능 | 장애 대처 기능 강화 - 정책 복원 기능

DB접근제어 시스템 운영중 장애 또는 정책 운영 변경으로 관리자가 등록한 보안 정책에 대해 특정 시점으로 roll back 하고자 할 때, 정책을 복원하는 기능
 복원 결과는 검색의 작업내역에서 보안정책의 복원 동작 조건으로 검색 후 확인

The screenshot shows the Chakra Max Manager interface. A dialog box is displayed in the foreground with the following text:

Chakra Max Manager

※ 선택한 시점으로 모든 정책을 복원합니다.
 ※ 선택하지 않은 정책들은 변경할 시점으로 모두 복원됩니다.
 정말로 복원하시겠습니까?

Buttons: 예(Y) (highlighted), 아니오(N)

Below the dialog, a table shows the job history for policy restoration:

보안...	보안 ...	보안 정책 이름	만든 날짜	수정된 날짜	상태
1040	12	Ename사전사후정책	2019/11/12 15:46:19	2019/11/12 15:46:19	DELETE (ROLLBACK)
1040	9	Ename사전사후정책	2019/11/06 10:32:31	2019/11/12 15:42:41	CREATE (RESTORE)

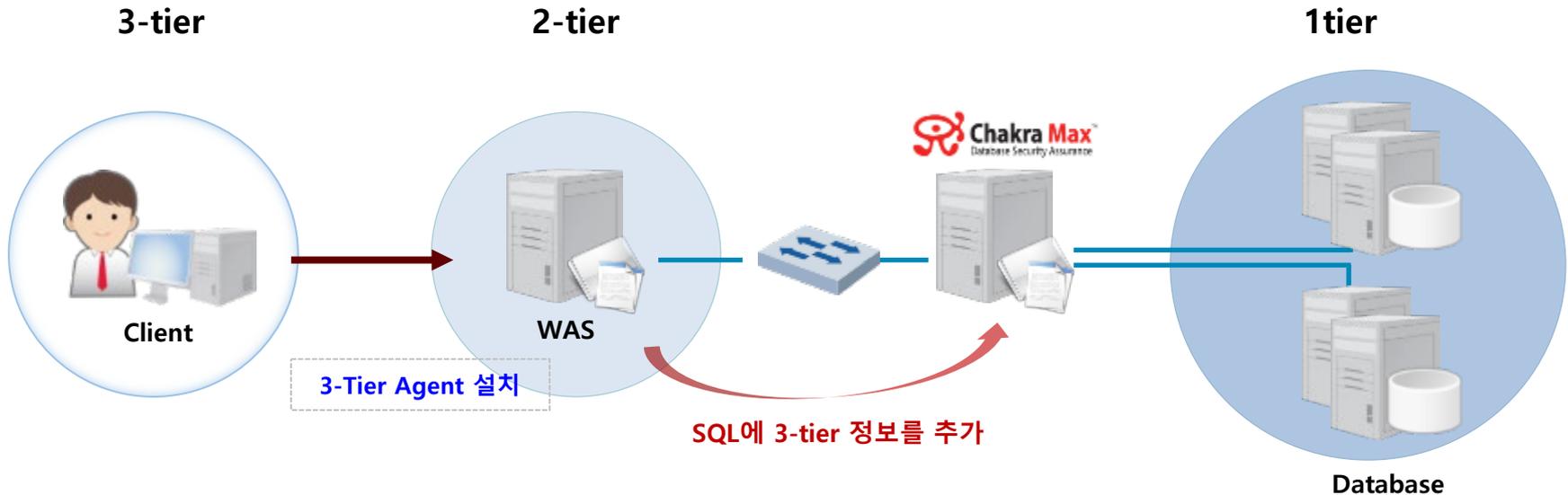
At the bottom of the dialog, there are buttons for '복원' (Restore) and '취소' (Cancel).

In the background, the main interface shows a search results table with a '복원' button highlighted in red. Below the dialog, a job history table is visible with columns for '내역(4)', '작업내역(6)', '작업내역(7)', and '작업내역(9)'. The table contains entries for policy restoration jobs performed by 'yator(chakramax)'.

작업 내역에서 보안정책의 복원 내역을 확인 가능

5. 옵션기능 | 3-Tier 추적 기능

WAS, APP Server를 경유하여 데이터베이스에 접속한 사용자 (3 Tier)의 IP / ID 추적



- 1 WAS를 경유한 End User를 추적하기 위해 "3-Tier Tracking Agent" 설치
- 2 기존 WAS Application의 수정 불필요 (Standard Java Platform 운영 시)
- 3 Tomcat, Web Sphere, Web Logic, JEUS 등 WAS를 경유한 End User 추적

• Agent 설치는 DBMS, OS, JAVA 환경에 따라 지원하지 않을 수 있으며 추가 비용이 발생할 수 있습니다

5. 옵션기능 | Local Logging Agent

LLA (Local Logging Agent)

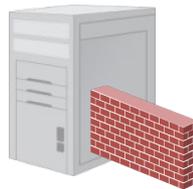
서버내의 직접접속을 감시하기 위하여 설치되는 Agent 로, 원격 또는 콘솔 등을 통한 DB의 직접접속이 발생할 경우, 모든 작업내역을 저장

※DB Collect와 연계할 경우, DB 접속차단 정책적용 지원.

※DB collector 세션 차단

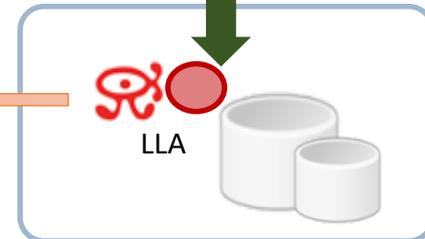
Chakra Max의 Dbcollector 가 세션을 차단 할 수 있는 관리자 권한(sys 등)으로, 항상 DB에 접속 해 있으면서 엔진 에서 분석된 차단 대상이 발견 될 경우DB 내부 명령어를 이용하여 DB 내에서 접속을 종료 하도록 함

전송된 DB작업내용을 설정된 보안정책으로 감사하여 경고발생 하고, 모든 DB작업내용은 감사 자료로 저장



로컬접속을 감지하여 DB작업내용 전송

원격접속/콘솔접속 등의 로컬접근



DB System

- **Agent 설치는 DBMS, OS, JAVA 환경에 따라 지원하지 않을 수 있으며 추가 비용이 발생할 수 있습니다**

5. 옵션기능 | Software Tap 1/2

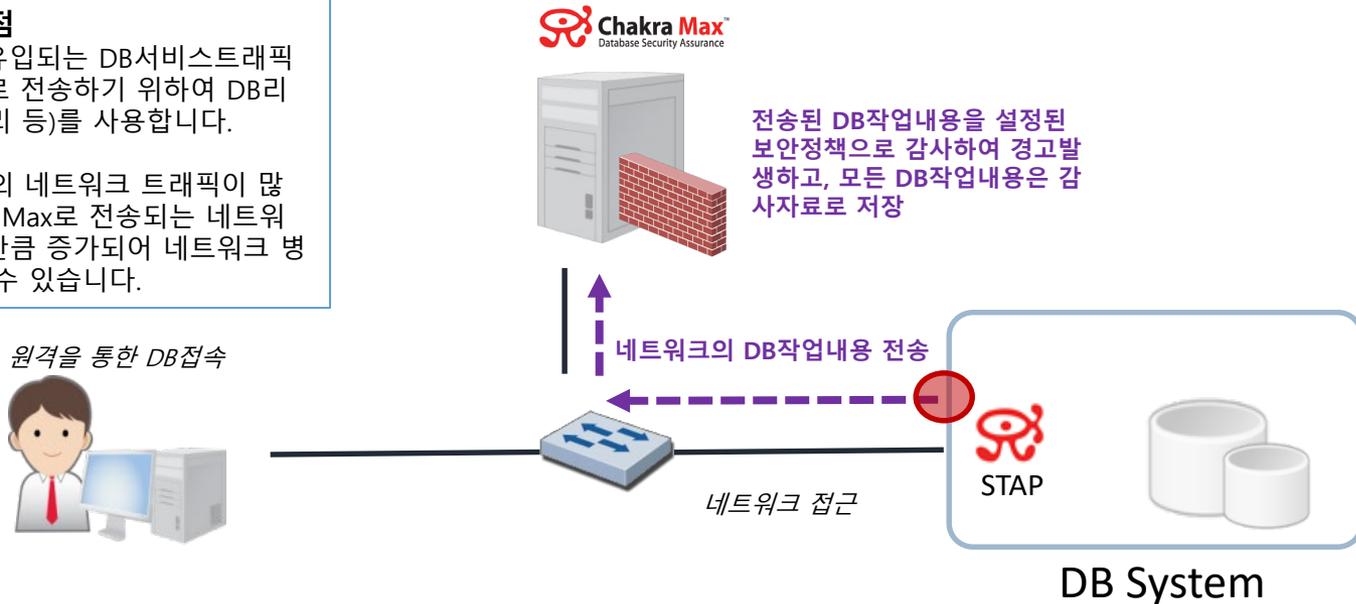
STAP (Software Tap) - 로깅

DB작업내용 감사를 위하여 스위치의 Port Mirror 혹은 TAP장비를 사용하는데, 고객사의 상황으로 이와 같은 구성이 불가능할 경우 DB서버에 설치되는 Agent로, DB 서버의 네트워크인터페이스로 유입되는 DB서비스 트래픽을 Chakra Max 서버로 전송하여, DB작업내용을 저장

STAP 의 유의점

DB시스템으로 유입되는 DB서비스트래픽을 Chakra Max로 전송하기 위하여 DB리소스(CPU, 메모리 등)를 사용합니다.

또한, DB서비스의 네트워크 트래픽이 많을 경우, Charka Max로 전송되는 네트워크 트래픽도 그만큼 증가되어 네트워크 병목의 원인이 될 수 있습니다.

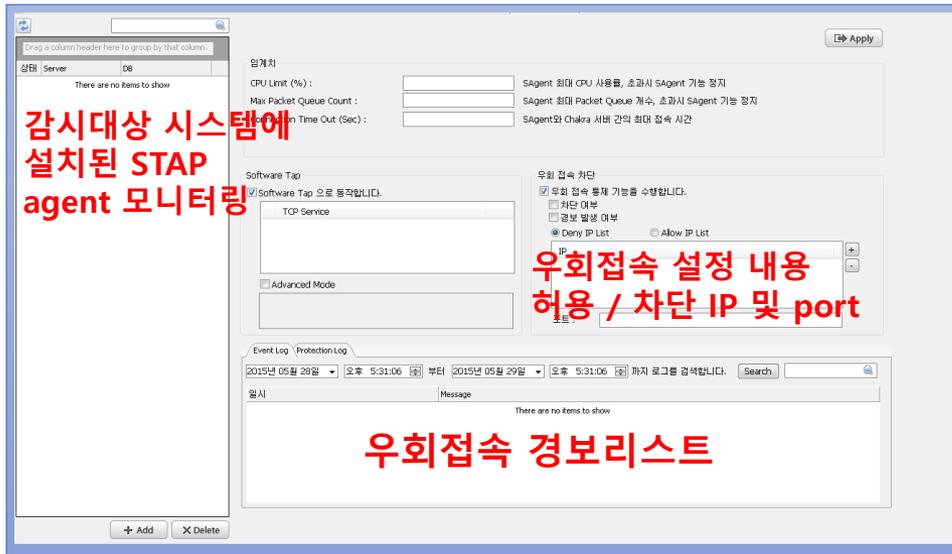


- Agent 설치는 DBMS, OS, JAVA 환경에 따라 지원하지 않을 수 있으며 추가 비용이 발생할 수 있습니다

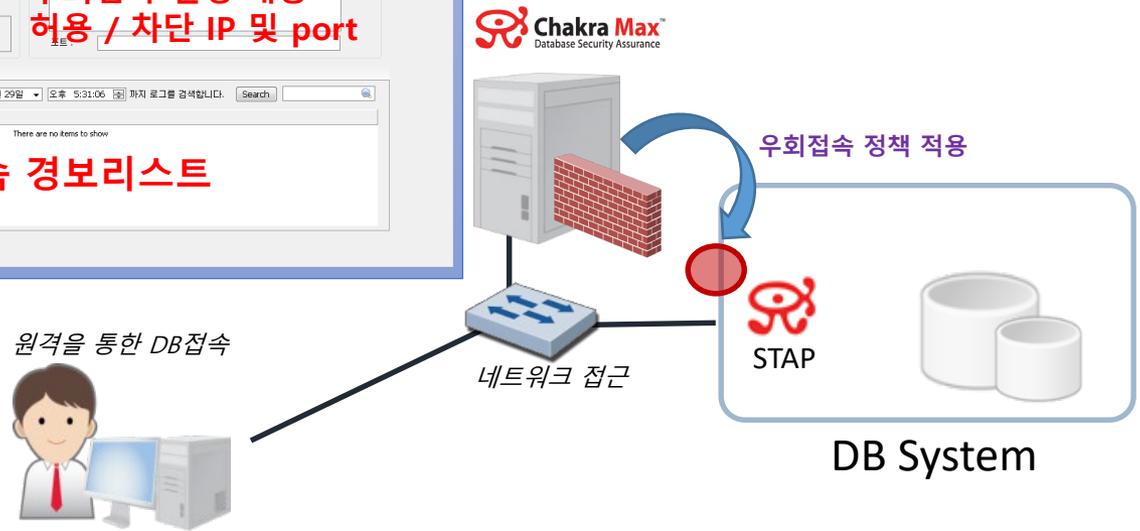
5. 옵션기능 | Software Tap 2/2

STAP (Software Tap) - 우회접속차단

허용되지 않은 유저/시스템 으로부터 제한된 서비스포트로의 우회접속에 대하여 경고/차단 기능.

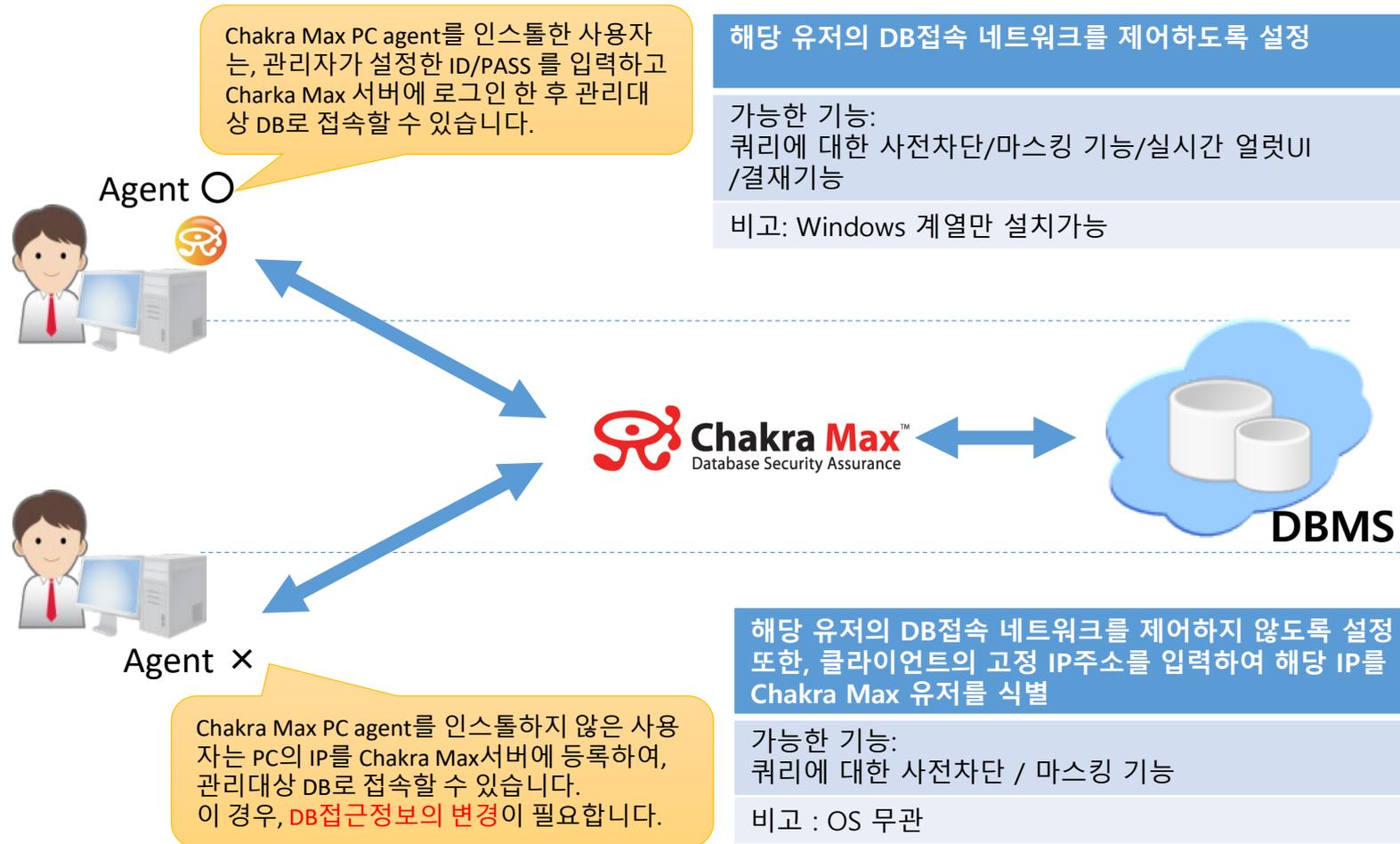


STAP 우회접속차단
DB 시스템에 설치된 STAP Agent로 접속하는 source IP 및 서비스 port 를 제어하는 방식
Chakra Max에서 모든 STAP Agent의 우회 접속 허용/차단 정책을 일괄관리



5. 옵션기능 | Agentless Gateway

Chakra Max를 proxy 게이트웨이로 사용하여 DB에 접근하는 경우, Chakra Max Client Agent의 설치 / 미설치 선택이 가능



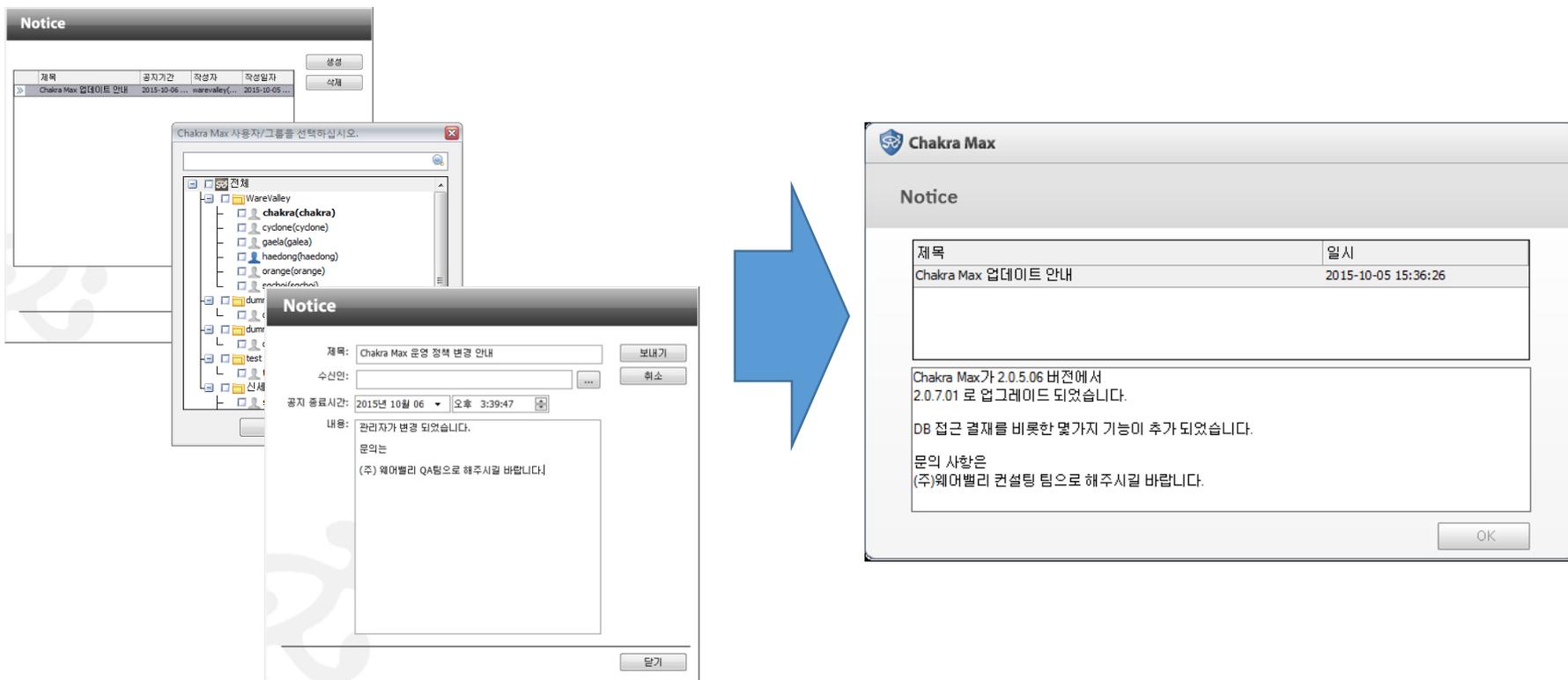
Appendix

Chakra MAX – Client 활용

Appendix. | 공지기능

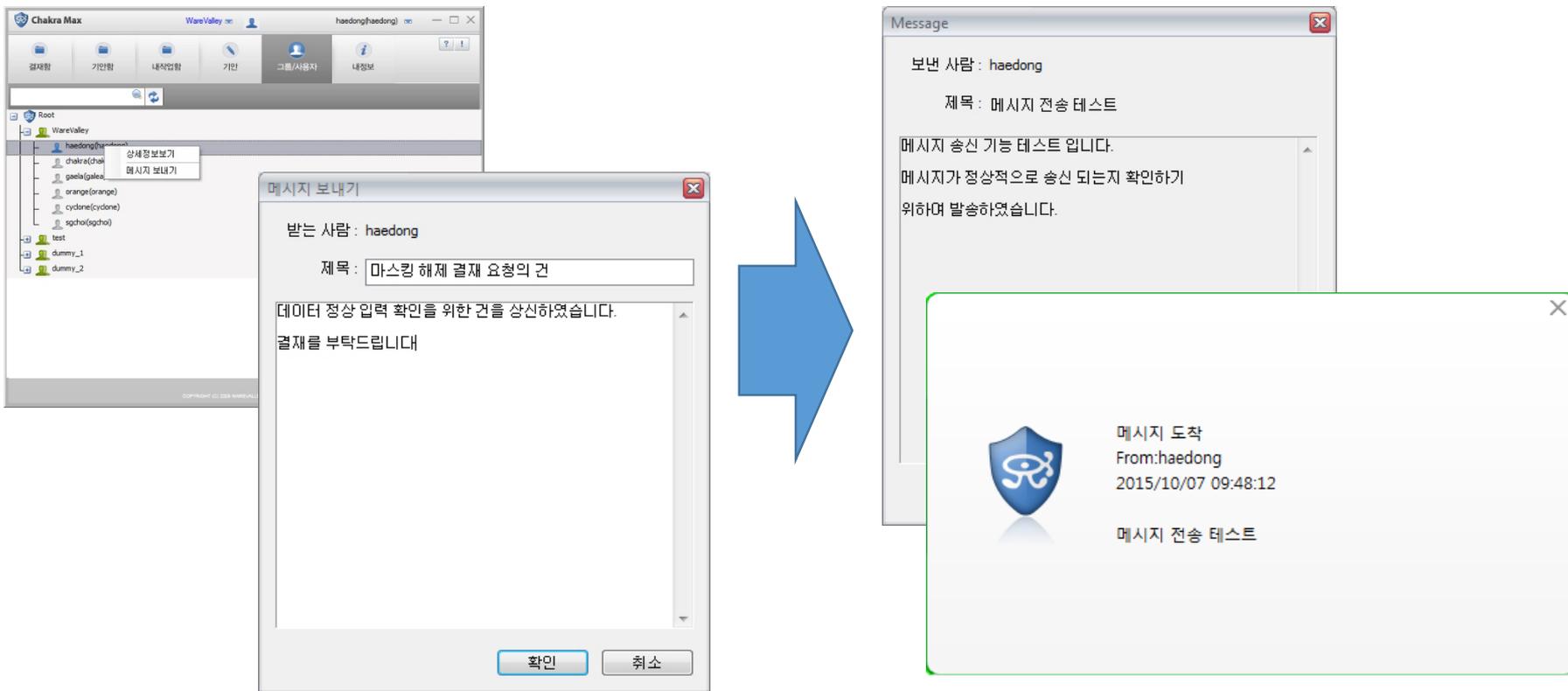
공지기능을 통한 클라이언트에 대한 알림 메시지 전송

Chakra Max 매니저를 통한 관리자의 공지 메시지 작성
공지 메시지를 수신 받을 사용자의 선별적 메시지 송신



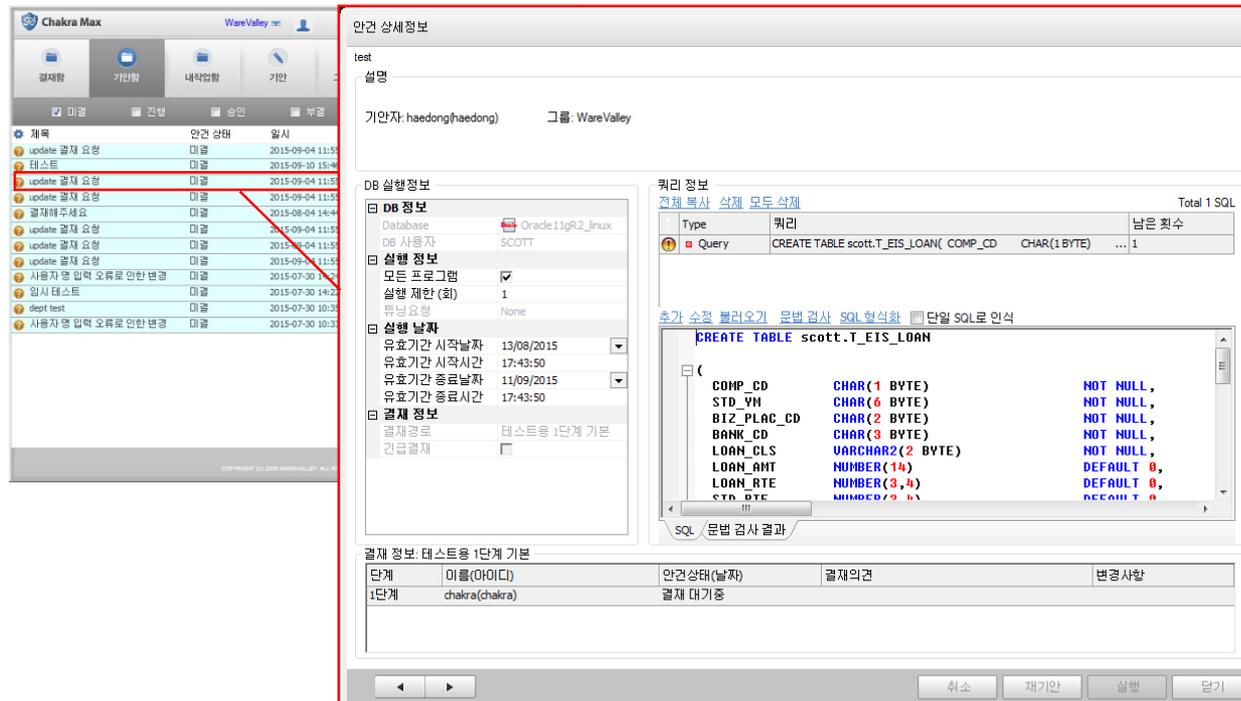
쪽지 보내기 기능을 통한 사용자 간의 메시지 전송

Chakra Max 클라이언트 사용자 간 메시지 전송
결재 / 기안 관련 건에 대한 긴급 처리 요청등의 메시지 송신



기안함의 기안문 저장 기능을 통한 과거 기안 내역 확인

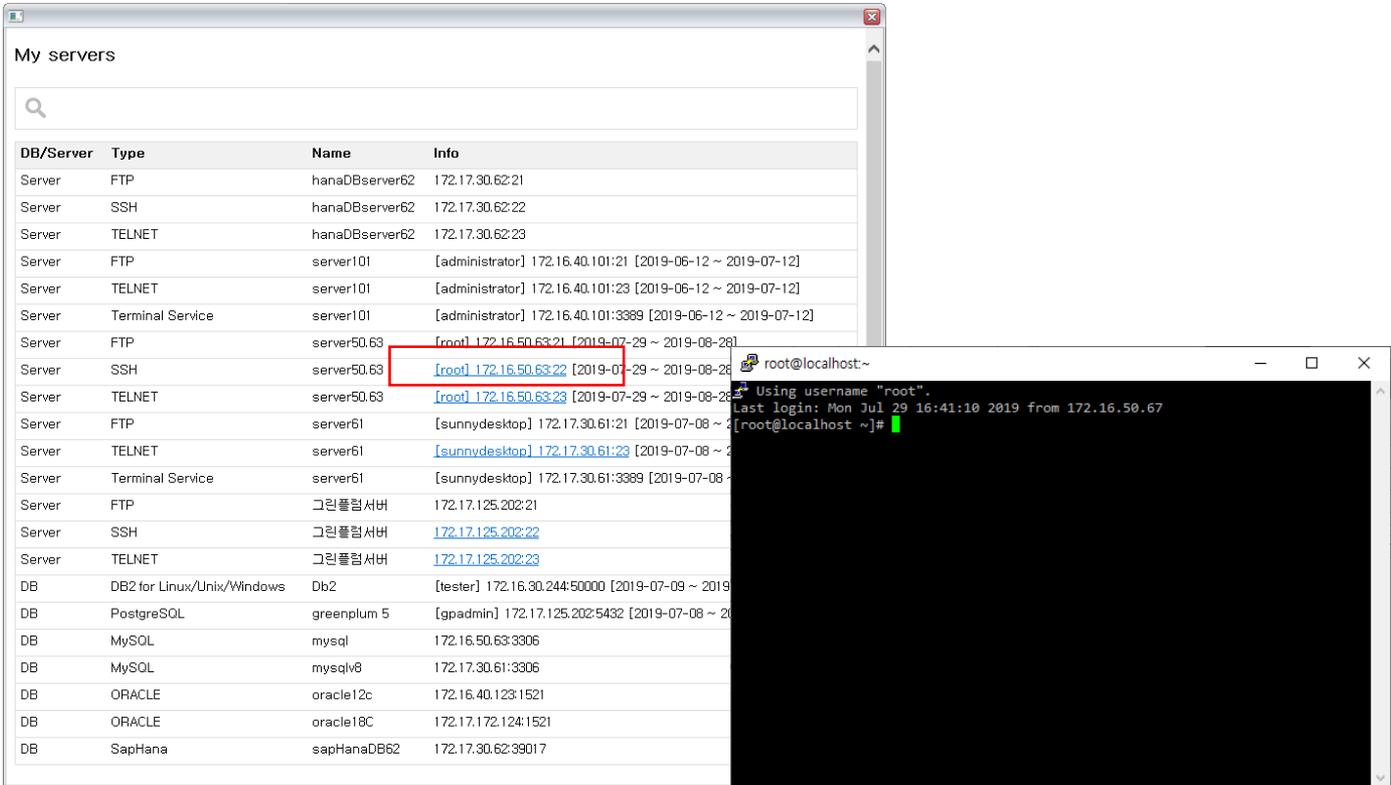
자신이 작성한 기안문에 대한 기안함 제공을 통한 기안문의 상세 내역 및 결재/부결 여부 확인



Appendix | 접속가능 서버/데이터베이스 목록

사용자가 접속 가능한 서버/데이터베이스 목록을 표시

사용자가 접속 가능한 서버/데이터베이스 목록을 표시하며, 할당된 서버 계정을 클릭하면 연결 프로그램으로 자동 접속 기능



The screenshot displays the 'My servers' window with a search bar and a table of server entries. A context menu is open over the table, showing options like '열기...', '도움말...', '서비스목록', '옵션...', '정보...', and '종료'. A terminal window is also open, showing a successful SSH connection to a server.

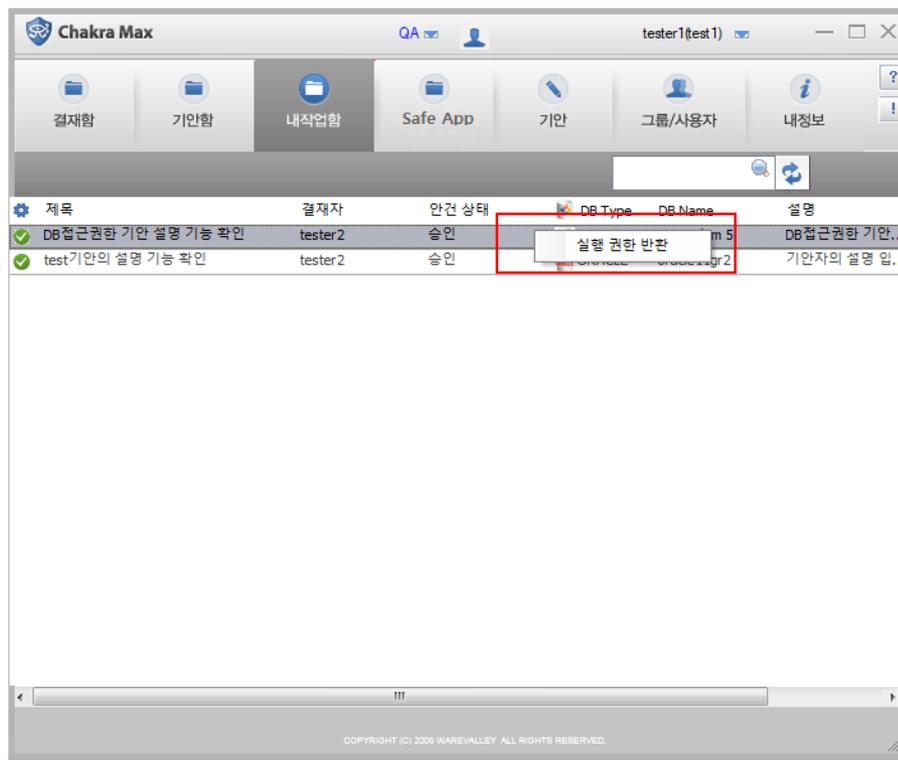
DB/Server	Type	Name	Info
Server	FTP	hanaDBserver62	172.17.30.62:21
Server	SSH	hanaDBserver62	172.17.30.62:22
Server	TELNET	hanaDBserver62	172.17.30.62:23
Server	FTP	server101	[administrator] 172.16.40.101:21 [2019-06-12 ~ 2019-07-12]
Server	TELNET	server101	[administrator] 172.16.40.101:23 [2019-06-12 ~ 2019-07-12]
Server	Terminal Service	server101	[administrator] 172.16.40.101:3389 [2019-06-12 ~ 2019-07-12]
Server	FTP	server50.63	[root] 172.16.50.63:21 [2019-07-29 ~ 2019-08-26]
Server	SSH	server50.63	[root] 172.16.50.63:22 [2019-07-29 ~ 2019-08-26]
Server	TELNET	server50.63	[root] 172.16.50.63:23 [2019-07-29 ~ 2019-08-26]
Server	FTP	server61	[sunnydesktop] 172.17.30.61:21 [2019-07-08 ~ 2019-07-12]
Server	TELNET	server61	[sunnydesktop] 172.17.30.61:23 [2019-07-08 ~ 2019-07-12]
Server	Terminal Service	server61	[sunnydesktop] 172.17.30.61:3389 [2019-07-08 ~ 2019-07-12]
Server	FTP	그린플럼서버	172.17.125.202:21
Server	SSH	그린플럼서버	172.17.125.202:22
Server	TELNET	그린플럼서버	172.17.125.202:23
DB	DB2 for Linux/Unix/Windows	Db2	[tester] 172.16.30.244:50000 [2019-07-09 ~ 2019-07-12]
DB	PostgreSQL	greenplum 5	[gpadmin] 172.17.125.202:5432 [2019-07-08 ~ 2019-07-12]
DB	MySQL	mysql	172.16.50.63:3306
DB	MySQL	mysqlv8	172.17.30.61:3306
DB	ORACLE	oracle12c	172.16.40.123:1521
DB	ORACLE	oracle18c	172.17.172.124:1521
DB	SapHana	sapHanaDB62	172.17.30.62:39017

```
root@localhost:~  
# Using username "root".  
Last login: Mon Jul 29 16:41:10 2019 from 172.16.50.67  
[root@localhost ~]#
```

Appendix | 내 작업함 - 실행 권한 반환

결재받은 안건에 대한 실행권한 반환 기능

기안 후 결재 승인 받은 안건에 대해 잔여 실행 회수가 남은 안건에 대해 더 이상 진행이 필요 없는 안건에 대해 내 작업함에서 실행권한 반환 할 수 있는 기능



사용자 편의를 위한 다양한 클라이언트 프로그램 옵션 제공

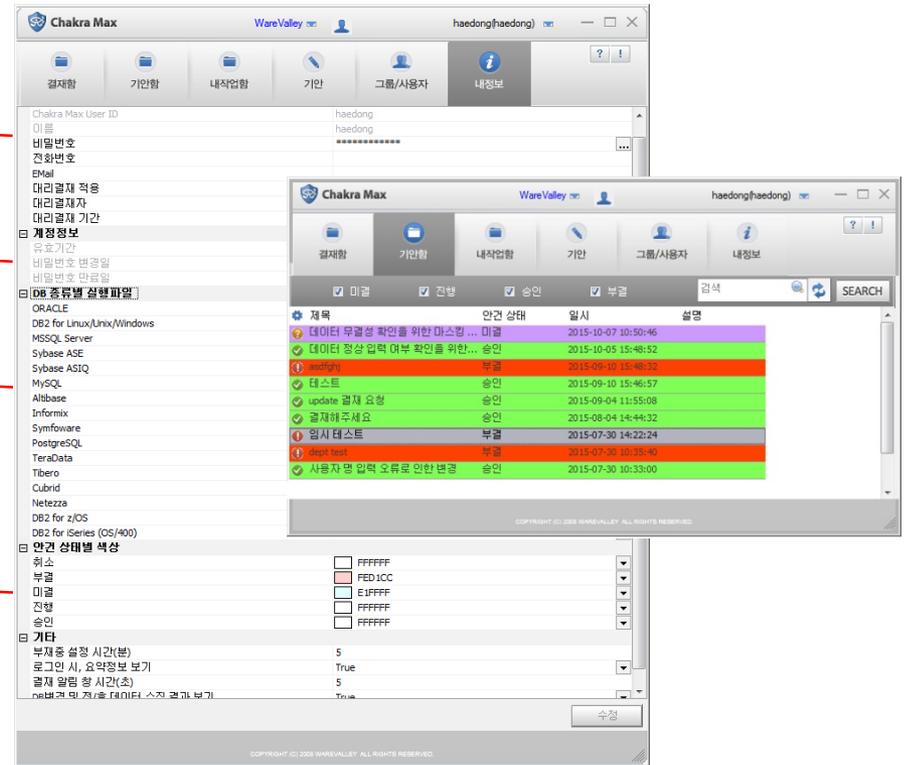
기안/결재함 진행 단계에 대한 컬러 표시
 사용자 주 사용 DB관리 프로그램 선택

사용자 패스워드
 / 연락처 / E-mail 등의 개인정보 수정

계정 유효기간 / 패스워드 변경일
 / 만료일 등의 정보

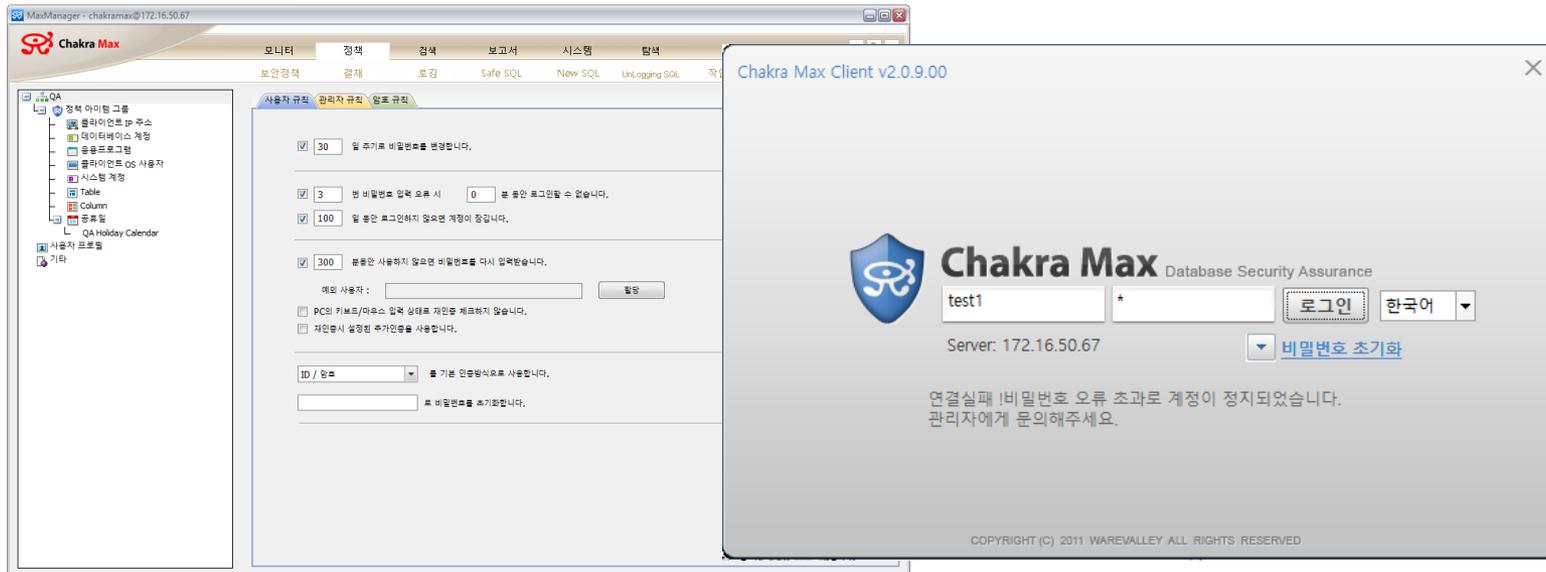
사용자의 주 사용 DB 관리 툴 지정

결재/기안함의 결재문 상태 표시 컬러



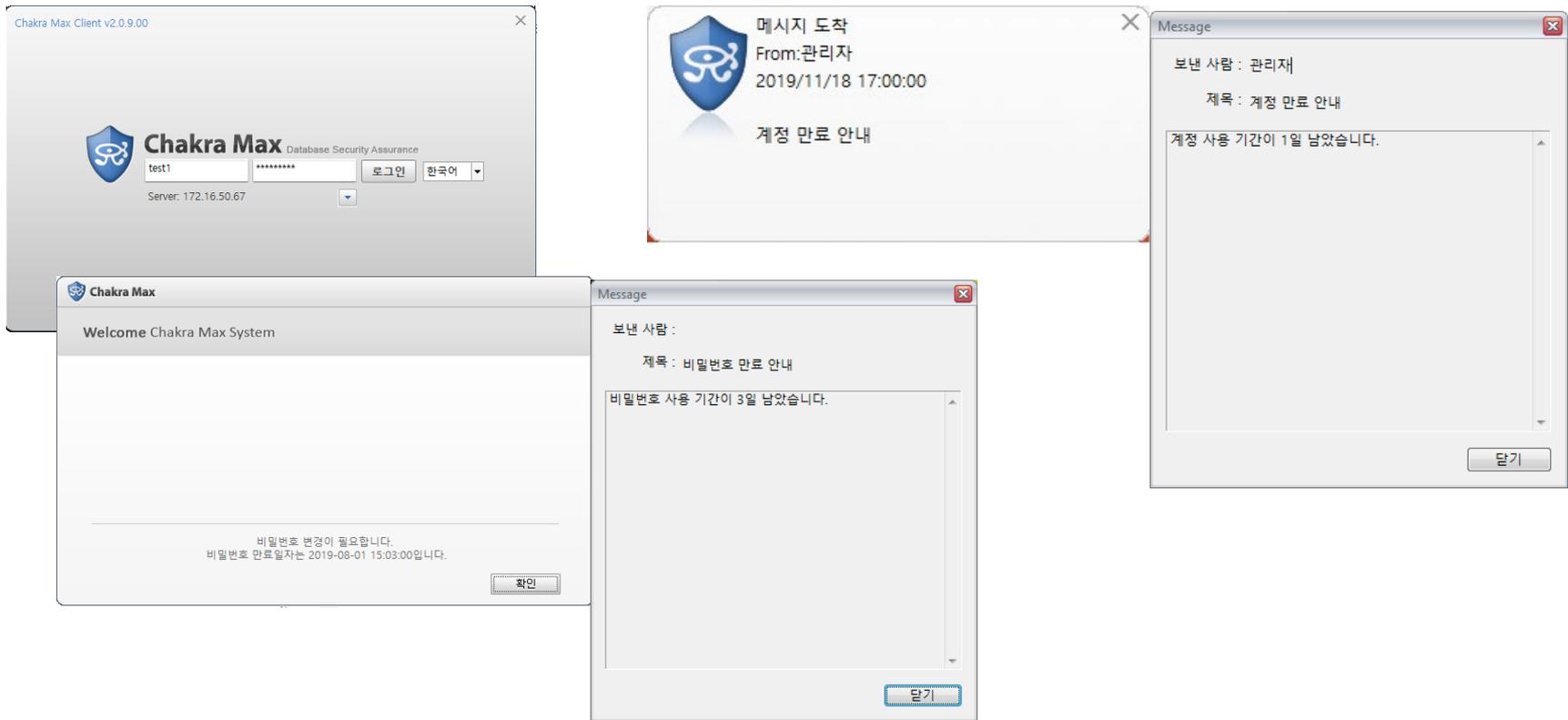
사용자 잠금 기능

사용자 로그인시 비밀번호 입력 오류 회수 초과시 설정에 따라 일정시간 로그인을 제한하는 기능에 사용자 계정을 잠금 처리하는 기능을 추가
해당 기능은 관리자가 잠금해제 처리전까지 해당 계정 사용이 불가하도록 보안 기능을 강화함.



사용자 계정만료 사전 알림 기능

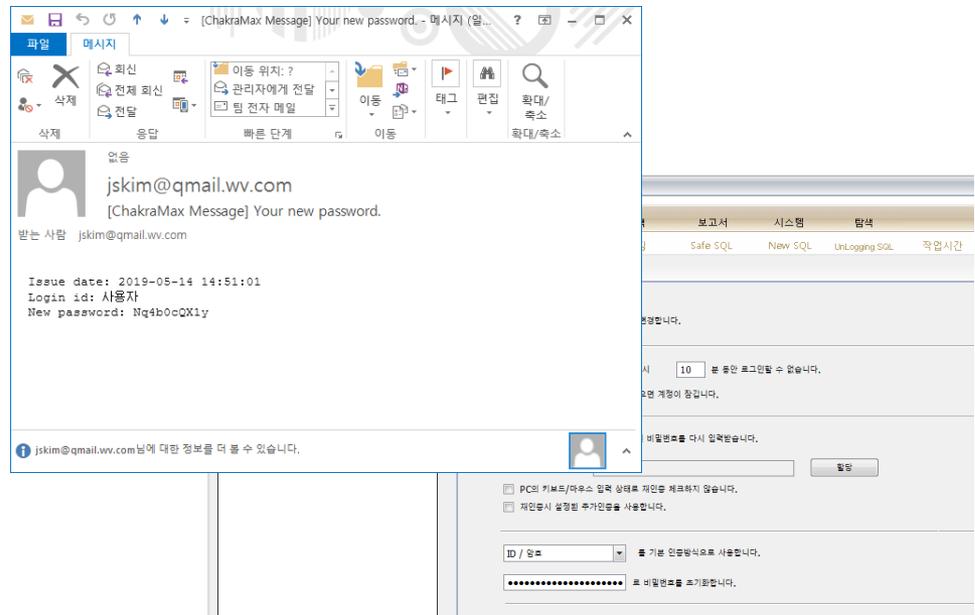
사용자 계정 및 비밀번호 만료기간이 임박함에 따라, 사용자 로그인시에 계정만료 및 패스워드 만료 안내 메시지를 출력하는 기능으로, 만료 7일전부터 알림이 표시되며 보안관리자의 설정에 따라 특정 시간에 메시지로 전송 가능



사용자 비밀번호 초기화

관리자 부재중에 사용자 계정이 잠기거나 장기 미사용 사용자에게 대해 활성화가 필요한 상태에서 사용자의 비밀번호를 초기화할 수 있는 기능 제공

- 샤크라가 생성한 임시 패스워드를 SMS, Email 로 전송하여 초기화 할 수 있도록 기능 제공
- 사용자가 비밀번호 초기화 요청시 관리자가 설정한 초기 패스워드를 사용자 임시 패스워드로 할당



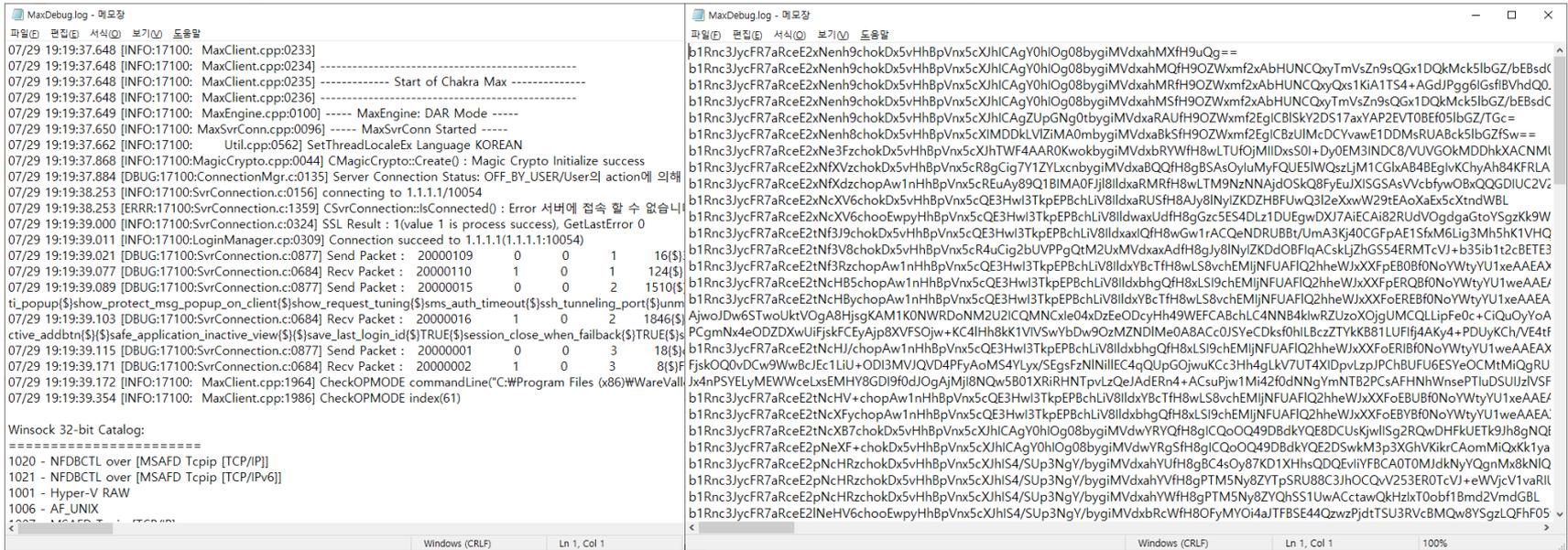
Appendix | 클라이언트 생성 로그 보안 기능 강화

클라이언트 프로그램 생성 로그의 보안 기능 강화

클라이언트가 생성하는 MaxDebug.txt 로그 생성시 사용자의 IP 주소를 그대로 저장하지 않고, 1.1.1.1로 마스킹 처리하여 저장

클라이언트가 생성하는 로그파일 암호화

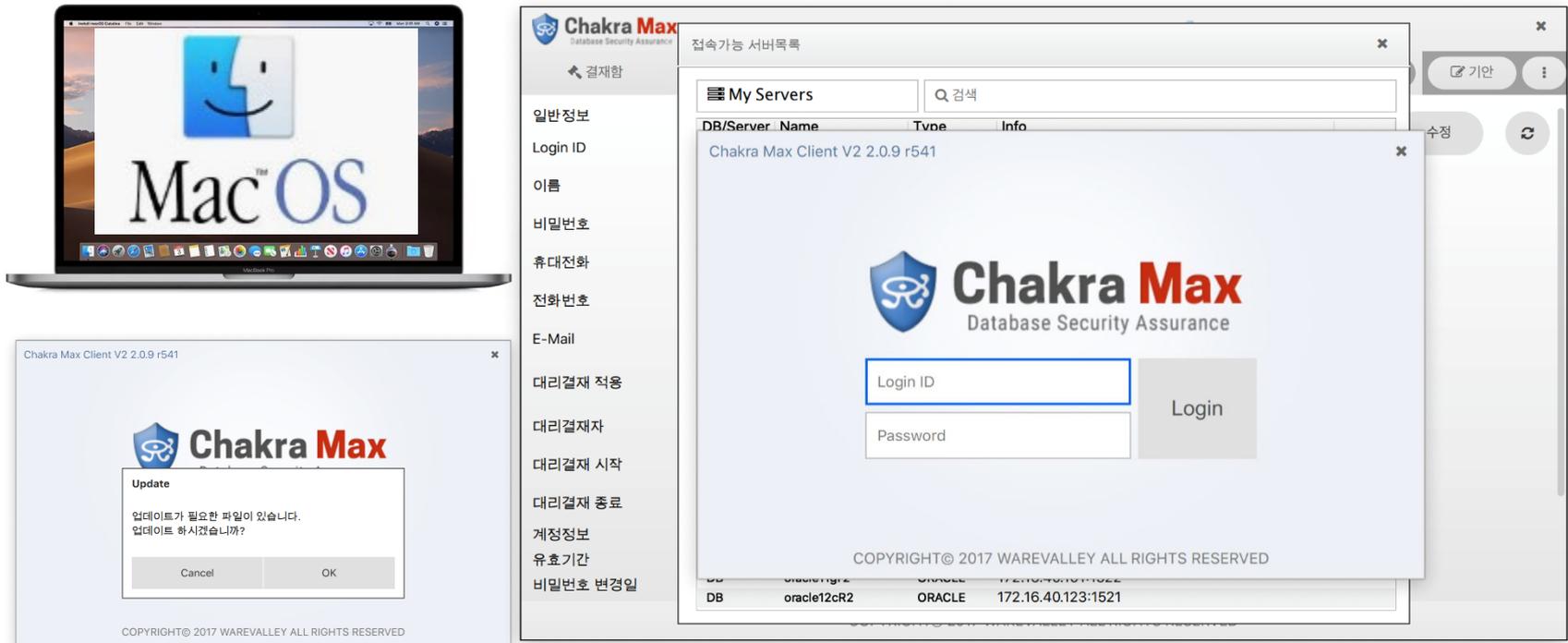
클라이언트가 생성하는 MaxDebug.txt 로그 파일을 암호화하여 생성



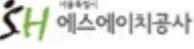
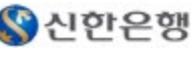
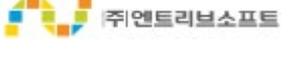
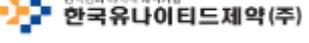
Appendix | 클라이언트 MAC OS 호환성

클라이언트 프로그램의 MAC OS 호환성 지원

- Windows OS 와 동일한 보안 기능 지원
- 자동 업데이트



6. 주요 고객사 | 주요 고객사

공공	        
	       
교육	      
금융	       
기업	       
	       
통신 / 포털서비스	      
게임	      
병원 / 제약	     
	      

Contact us.

Seoul Office :

22F, Nuritkum Square Biz Tower, 1605
Sangam-dong, Mapo-gu,
Seoul, Korea 121-795
Tel + 82.2.2132.5590

Japan Office :

Shinkasumigaseki Bldg 18F., 3-3-2,
Kasumigaseki, Chiyoda-ku, Tokyo 100-0013
Tel +81.3.5532.8801

Online Contact :

Sales@warevalley.com
<http://www.warevalley.com>

WareValley

<http://www.warevalley.com>

Database Audit and Protection [DB-System 접근통제]

Database Encryption [DB 암호화]

Database Vulnerability Assessment [개인정보 모니터링 / DB 취약점 분석]

Database SQL Query Approval [DB 작업결재]

Database Performance Monitoring and Management [DB 성능관리 및 개발]

BI / DW / OLAP DBMS [빅데이터 분석, 데이터웨어하우스]