

Introducing
EPAS15 - The
Most Secure
Postgres

Agenda

1. EDB 소개, 제품 정책
2. EDB 보안기능, Oracle 호환성
3. Transparent Data Encryption (TDE) Deep Dive
4. EPAS 15
5. PostgreSQL 15

회사 개요

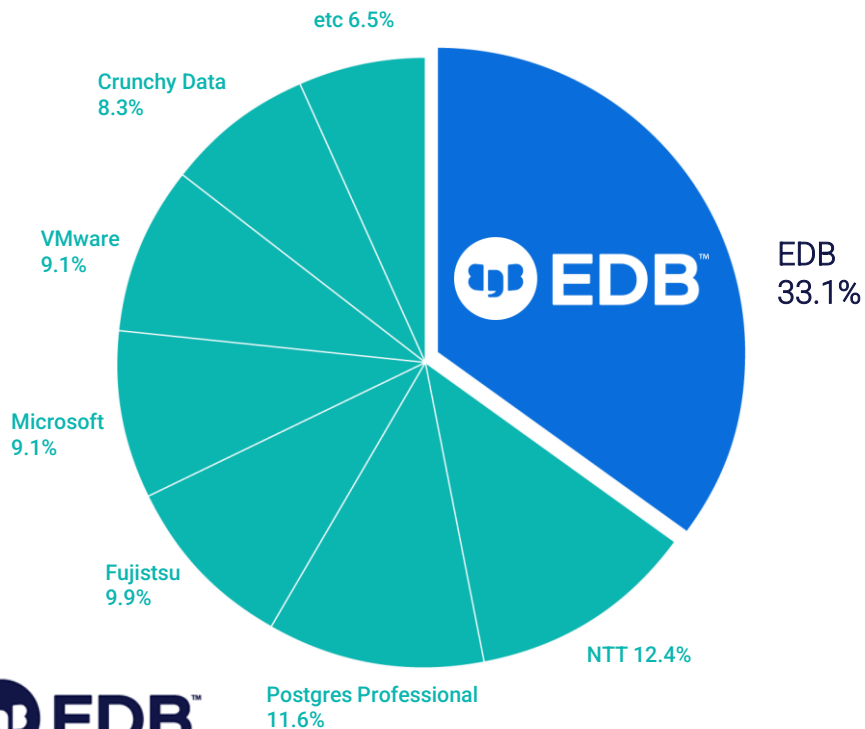
- 회사명: EnterpriseDB(이하 EDB)
- 본사: 미국 보스턴
- 회사 개요:

2004년 설립된 오픈소스 DB 전문업체로 PostgreSQL의 상용 제품인 EDB Postgres Advanced Server(이하 EPAS)를 개발 공급
2020년 유럽 PostgreSQL 상용제품 개발업체 2ndQuadrant 인수
2020년 12월 기준 전세계 5,400+ 고객 확보
2022년 전년대비 56% 매출성장(52분기 연속)
전세계 14개 지사 운영 중
한국지사는 2014년 설립



PostgreSQL 전문기업

EDB는 가장 많은 PostgreSQL 전문가와 함께하고 있는 기업입니다.



Michael Stonebraker

“Postgres의 아버지”
이자 EDB의 고문



Bruce Momjian

공동 설립자, PostgreSQL
Development Corp 및
PostgreSQL 코어 팀



Peter Eisentraut

PostgreSQL 코어
팀 멤버



Robert Haas

PostgreSQL 핵심
기여자 및 공헌자



Simon Riggs

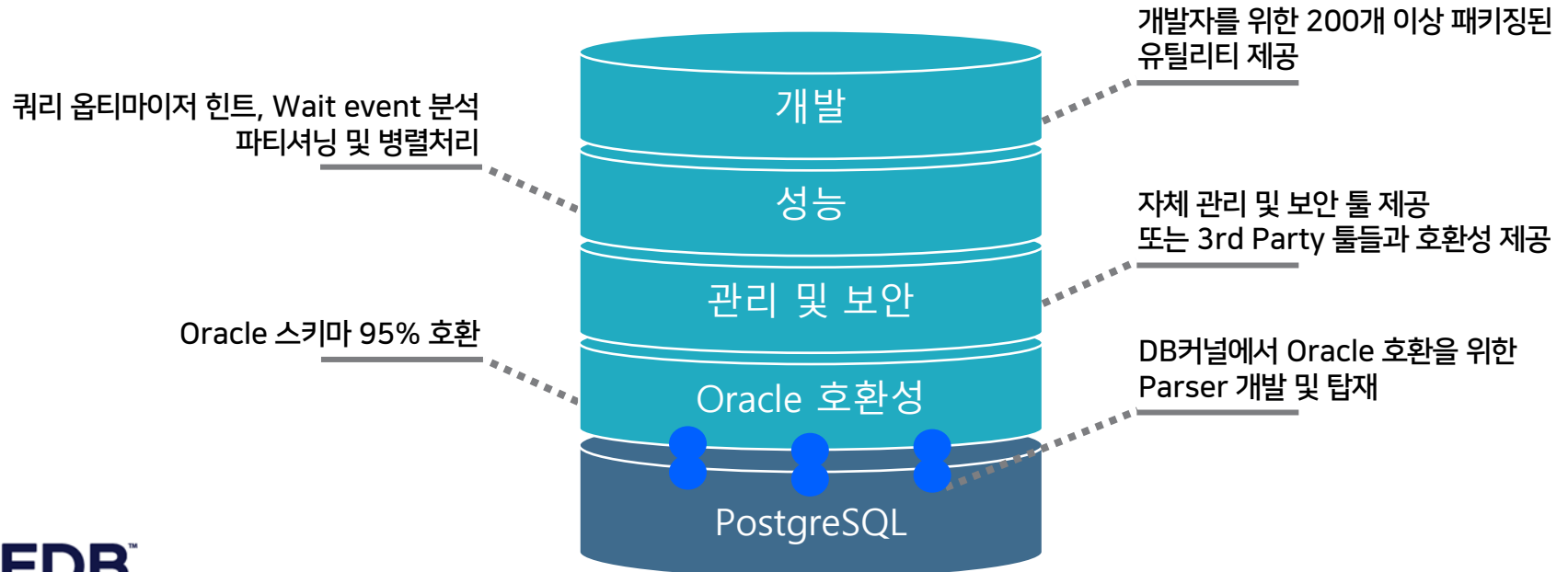
PostgreSQL 핵심 기여자,
2ndQuadrant의 창립자

EDB 제품 정책

	Community 360 PostgreSQL 전문 지식과 지원이 필요한 기업용	Standard 오픈 소스 전략이 있고 연중무휴 지원과 추가 툴이 필요한 기업용	Enterprise Oracle 호환성, 향상된 보안 및 기타 엔터프라이즈 기능이 필요한 기업용
EDB Postgres Advanced 엔터프라이즈 용, 오라클과 95% 이상의 호환되는 Postgres			○
PostgreSQL EDB 지원 오픈소스 데이터베이스		○	○
EDB 툴 관리, 백업, Failover, 마이그레이션, 복제		○	○
오픈소스 툴	○	○	○
테크니컬 서포트 24x7 365 전문인력의 지원	○	○	○
EDB Postgres Distributed (EPD) PostgreSQL에서 사용할 수 있는 가장 진보된 복제 솔루션		Optional	Optional

EDB Postgres Advanced Server(EPAS)

기업사용자의 Pain Points에 집중





보안기능

- Data 마스킹
- Profile and password 관리
- SQL Injection 보호
- Stored procedure source code 암호화
- EDB 감사



Oracle 호환성

- Oracle data types, Oracle keywords, DBA_ USER_ views
- Packages, Autonomous Transactions, Interval Partitioning, Optimizer Hints, COLLECTIONS, Hierarchical Queries
- Oracle functions
- DBMS_ packages
- UTL_ packages



EDB Postgres Advanced 15

- Merge with upstream PostgreSQL 15
 - MERGE SQL command, Logical replication, and backup and recovery capabilities
- Transparent Data Encryption
- More Oracle Compatibility
- EDB tools are tested with EDB Postgres Advanced 15
- Builds for all supported platforms

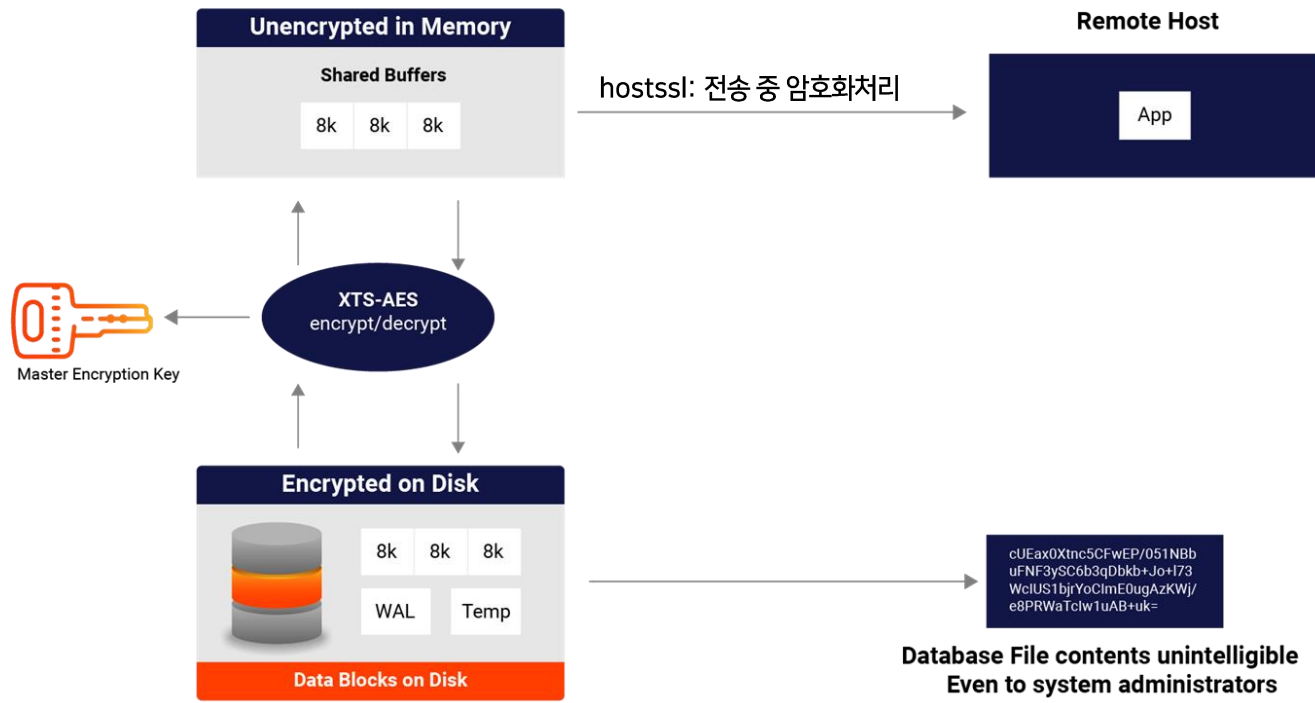
Transparent Data Encryption



Transparent Data Encryption

- 데이터베이스 서버 및 백업 저장소의 운영 체제 파일에서 데이터 무단 보기 방지
- 응용 프로그램 변경 또는 업데이트된 클라이언트 드라이버 불필요
 - EPAS에서 암호화/암호 해독 관리
- 유연한 키 관리 아키텍처

TDE with EDB Postgres



암호화 대상

- All Data files
 - Tables
 - Sequences
 - Indexes
 - TOAST tables
 - System catalogs
- Write Ahead Log (WAL)
- Temporary files
 - tuplestore
 - sort
 - hash join

비암호화 대상

- 데이터베이스 작동 내부의 메타데이터 : pg_subtrans, pg_xact, etc.
- PGDATA의 파일 이름 및 파일 시스템 구조
- 외부 테이블의 데이터 (foreign table)
- 서버 진단 로그
- 환경파일 (pg_hba.conf, postgresql.conf)

지원되는 키 저장소

HTTPS-based APIs

- Amazon AWS Key Management Service (KMS)
- Google Cloud - Cloud Key Management Service
- Microsoft Azure Key Vault

Oasis KMIP

- Thales CipherTrust Manager

Flexible Architecture

Open**SSL**

- Data Key protected by a passphrase

Wrap the Key

```
/usr/edb/as15/bin/initdb -D ${PGDATA} /  
-y /  
--key-wrap-command='openssl enc -e -aes128-  
cbc -pbkdf2 -out %p'
```

Unwrap the Key (postgresql.conf)

```
data_encryption_key_unwrap_command =  
'openssl enc -d -aes-128-cbc -pbkdf2 -in %p'
```

Flexible Architecture

- Amazon Key Management Service



Wrap the Key

```
/usr/edb/as15/bin/initdb -D ${PGDATA} /  
-y /  
--key-wrap-command='crypt encrypt aws --  
out %p --region us-east-1 --kms alias/pg-  
tde-master-1'
```

Unwrap the Key (postgresql.conf)

```
data_encryption_key_unwrap_command = 'crypt  
decrypt aws --in %p --region us-east-1'
```

Flexible Architecture

- Thales CipherTrust Manager

THALES

Wrap the Key

```
/usr/edb/as15/bin/initdb -D ${PGDATA} /  
-y /  
--key-wrap-  
command='python ./edb_tde_kmip_client.py  
encrypt --key-uid=... --out-file=%p'
```

Unwrap the Key (postgresql.conf)

```
data_encryption_key_unwrap_command =  
'python ./edb_tde_kmip_client.py decrypt --  
key-uid=... --in-file=%p'
```

Data on disk **without** TDE

```
insert into tbfoo values ('abc','123');  
INSERT 0 1
```

```
select pg_relation_filepath('tbfoo');
```

```
pg_relation_filepath  
-----  
base/5/16416
```

```
$ hexdump -C 16416 | grep abc  
00001ff0 09 61 62 63 15 31 32 33 20 20 20  
20 20 20 00 00 |.abc.123 ..|
```

```
$ hexdump -C 16416 | tail -5  
*  
00001fd0 00 00 00 00 00 00 00 00 e1 02 00  
00 00 00 00 00 |.....|  
00001fe0 00 00 00 00 00 00 00 00 01 00 02  
00 02 08 18 00 |.....|  
00001ff0 09 61 62 63 15 31 32 33 20 20 20  
20 20 20 00 00 |.abc.123 ..|  
00002000
```

Data on disk **with** TDE

```
insert into tbfoo values ('abc','123');  
INSERT 0 1
```

```
select pg_relation_filepath('tbfoo');
```

```
pg_relation_filepath  
-----  
base/5/16416
```

```
$ hexdump -C 16416 | grep abc  
$
```

```
$ hexdump -C 16416 | tail -5  
00001fc0 c8 0f 1d c8 9a 63 3d dc 7d 4e 68  
98 b8 f2 5e 0a |.....c=.)Nh...^.|  
00001fd0 9a eb 20 1d 59 ad be 94 6e fd d5  
6e ed 0a 72 8c |.. .Y...n..n..r.|  
00001fe0 7b 14 7f de 5b 63 e3 84 ba 6c e7  
b0 a3 86 aa b9 |{...[c...l.....|  
00001ff0 fe 4f 07 50 06 b7 ef 6a cd f9 84  
96 b2 4b 25 12 |.O.P...j.....K%.|  
00002000
```


EDB Postgres Advanced Server 15

Oracle Compatibility in v15

HTP and HTF

New Oracle Style Package

Consist of 88 procedures!

```
htp.address (  
  cvalue      in      varchar2  
  cnowrap    in      varchar2  DEFAULT NULL  
  cclear     in      varchar2  DEFAULT NULL  
  cattributes in      varchar2  DEFAULT NULL);  
  
htf.address (  
  cvalue, cnowrap, cclear, cattributes  
) return varchar2;
```

DBMS_UTILITY

Expanded Coverage

Now with support for 17
functions/procedures

Previously 15 functions/procedures



```
DBMS_UTILITY.FORMAT_ERROR_BACKTRACE  
return VARCHAR2
```

```
DBMS_UTILITY.FORMAT_ERROR_STACK  
return VARCHAR2
```


Oracle Compatibility

New supported SQL and
functions

- SQL
 - MERGE Syntax (where 사용가능)
 - UPDATE..SET ROW syntax support
- Functions
 - rexp_like (PostgreSQL 15)
 - from_tz
 - to_timestamp_tz
 - to_clob, to_blob, to_nchar
 - to_multi_byte, to_single_byte

PostgreSQL

15



PostgreSQL 15

EDB 커뮤니티 제공 기능

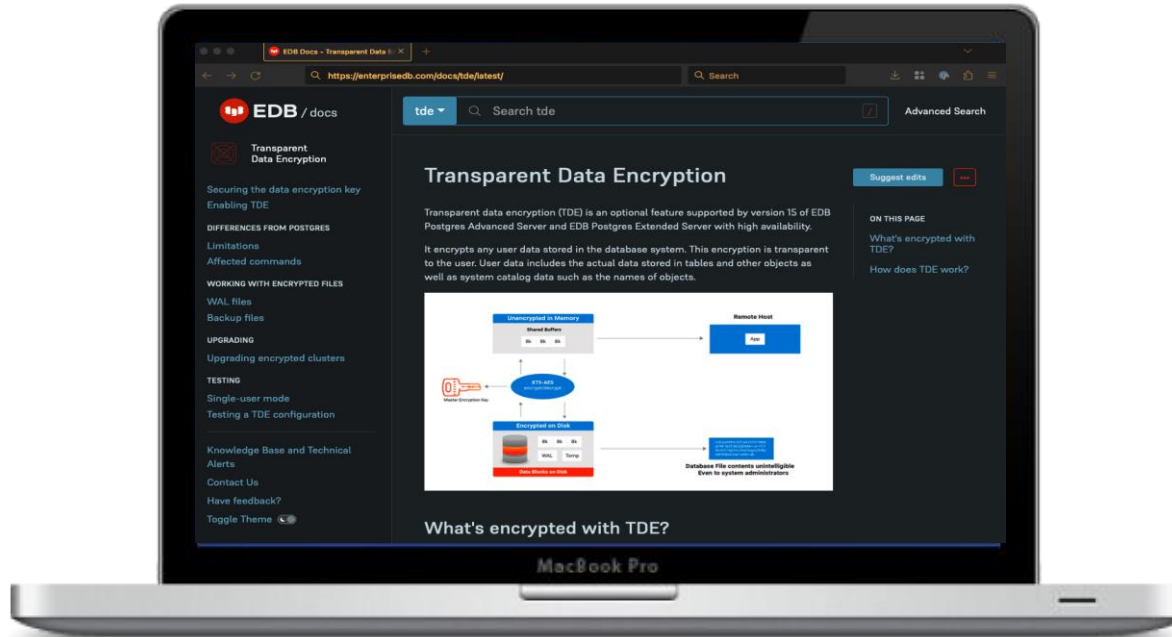
- 개발 생산성 - MERGE SQL구문
- 보안 - 슈퍼유저가 필요한 작업 축소
- 백업/복구 - 새로운 압축 옵션 및 서버 측 압축
- Lots more...

- Sorting 성능 : Order by, 분석 함수 성능개선
- Log 관련 : JSON 포맷
- Public Schema : Public 스키마에 오브젝트 생성 시 권한 필요
- 백업 명령어 : `pg_start_backup -> pg_backup_start,`
`pg_stop_backup -> pg_backup_stop`

- 압축기능 : WAL (LZ4, Zstandard) , pg_basebackup (LZ4, zstd)
- 인스턴스 통계 : 디스크 기록 -> 메모리에서 처리

EDB Docs

Detailed documentation



THANK YOU