PostgreSQL Security. How Do We Think?

Masanori Oyama @ooyamams1987
NTT OSS Center

Who am I?

Masanori Oyama / 大山 真実
twitter @ooyamams1987

Work

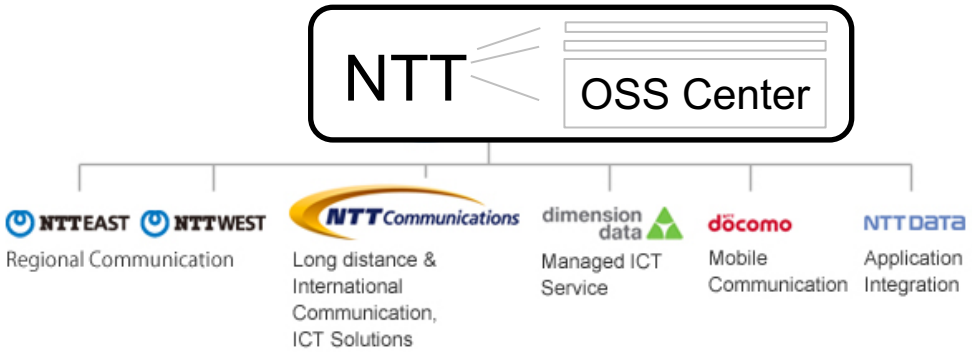
- PostgreSQL engineering support and consultation.
  - Recently focus to database security.
- Extensive quality verification of PostgreSQL releases.
  - Latest work: Parallel query evaluation.
    pgconf.asia “What’s new in 9.6, by PostgreSQL contributor” by Masahiko Sawada
    https://www.slideshare.net/masahikosawada98/whats-new-in-96-by-postgresql-contributor

Prev work

- Hadoop engineering support and consultation at NTT DATA Inc.
  - I had managed a big Hadoop cluster (1000 node, 200PB!).

About NTT

- Who we are?
  - NTT（Nippon Telegraph and Telephone Corporation）
  - National flagship carrier in Japan



NTT group
subsidiary

NTT COMWARE

NTT-TX

about 900 companies

- What NTT OSS Center is doing ?
  - Promotes the adoption of OSS by the group companies
    - Total support
      - support desk, Introduction support, Product maintenance
    - R&D
      - developing OSS and related tools with the communities
  - Deals with about 60 OSS products.




Agenda

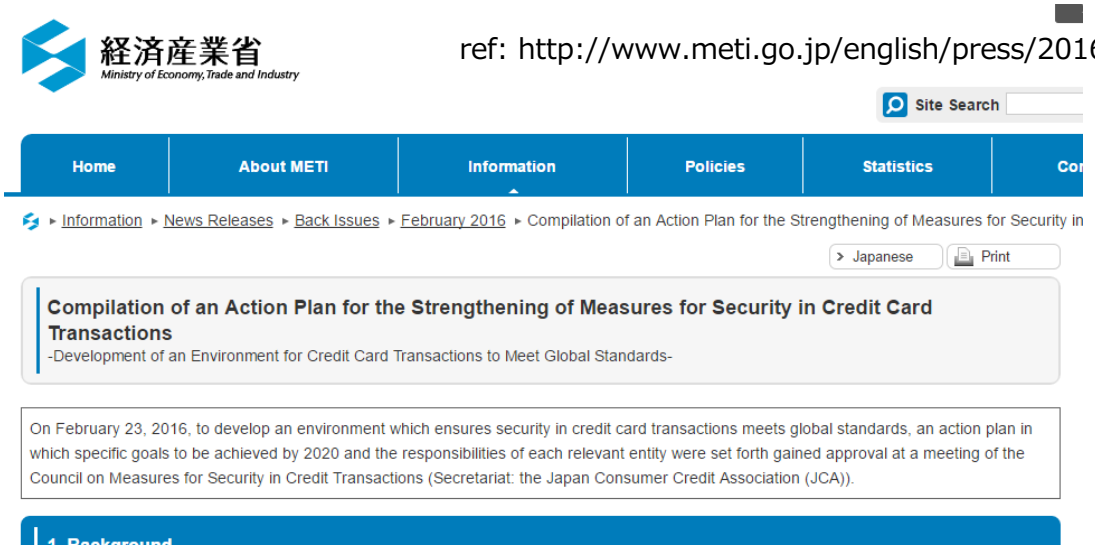
1. **Introduction**
2. **Database Security Requirements**
3. **How to Apply to PostgreSQL**

1. Introduction

The circumstances in Japan

- Japanese government aims to implement an action plan for strengthening the security of credit card transactions by 2020.
  - Make business operators holding such information conform to the PCI DSS.
  - Multi-layered measures are introduced by retailers dealing with EC transactions.

ref: http://www.meti.go.jp/english/press/2016/0223_02.html



- Some our projects try to conform to PCI DSS.

What is PCI DSS?

- PCI DSS (Payment Card Industry Data Security Standard) is credit card industry security standard.

The Council was founded in 2006 by American Express, Discover, JCB International, MasterCard and Visa Inc. They share equally in governance and execution of the Council's work.

ref: https://www.pcisecuritystandards.org/pci_security/

What is PCI DSS?

- PCI DSS (Payment Card Industry Data Security Standard) is credit card industry security standard.

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1.	Install and maintain a firewall configuration to protect cardholder data
	2.	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3.	Protect stored cardholder data
	4.	Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5.	Protect all systems against malware and regularly update anti-virus software or programs
	6.	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7.	Restrict access to cardholder data by business need to know
	8.	Identify and authenticate access to system components
	9.	Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10.	Track and monitor all access to network resources and cardholder data
	11.	Regularly test security systems and processes
Maintain an Information Security Policy	12.	Maintain a policy that addresses information security for all personnel

ref: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf

The requirements of PCI DSS related to database

Innovative R&D by NTT

Data Encryption with Key Management.

Keep your Database Secure.

CI Data Security Standard – High Level Ov

Build and Maintain a Se Network and Systems	1. Install and maintain a firewall configuratio protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Tes Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Inform Security Policy	12. Maintain a policy that addresses information security for all rsonnel

User Identification, Authentication, Authorization, Identity management.

Audit.

NTT

The requirements of PCI DSS related to database

Innovative R&D by NTT

Data Encryption and Key Management.

Keep your Database Secure.

CI Data Security Standard – High Level Ov

Build and Maintain a Sec Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data **2. Do not use vendor-supplied defaults for system passwords and other security parameters**
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs **6. Develop and maintain secure systems and applications**
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Tes Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Inform Security Policy	12. Maintain a policy that addresses information security for all rsonnel

User Identification, Authentication, Authorization, Identity management.

Audit.

NTT

i. Keep your Database Secure

PCI DSS Requirements 2 & 6 say

- Don’t use a default user account and password.
- Don’t use unnecessary modules, functions, protocols.
- Admin control accesses have to be encrypted.
- Use a latest software version.

These are not difficult.
Traditional (or basic) security practices are important!

The requirements of PCI DSS related to database

Innovative R&D by NTT

Data Encryption with Key Management.

Keep your Database Secure.

CI Data Security Standard – High Level Ov

Build and Maintain a Se… Network and Systems	1. Install and maintain a firewall configuration… protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**3. Protect stored cardholder data** **4. Encrypt transmission of cardholder data across open, public networks**
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Tes… Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Inform… Security Policy	12. Maintain a policy that addresses information security for all …rsonnel

User Identification, Authentication, Authorization, Identity management.

Audit.

NTT

ii. Encryption and Key Management

PCI DSS Requirement 3 says

- PAN (Primary account number) must be unreadable or encrypted.

irreversible

unreadable

- **One-way hashes**
  af1bcec2664906a9f587fb
- **Truncation**
  XXXX XXXX XXXX 1234

reversible

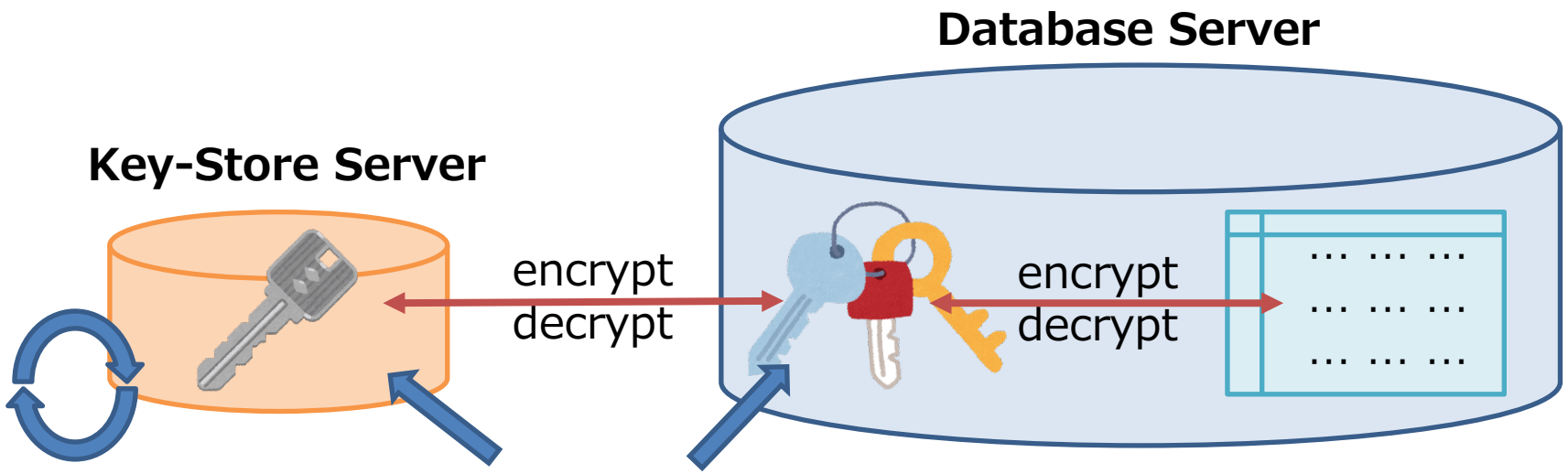
strong encryption

- **With key-management**
- **AES, TDES/TDEA, RSA**
  (see PCI DSS Glossary "Strong Cryptography")
- **Only valid user can decrypt**

ii. Encryption and Key Management

Encryption key-management Outline

- Two-tier encryption
  - **Data-encrypting key**
  - **Key-encrypting keys**



- Replace in a certain period
- Store separately
- Restricted access
- Stored in the fewest locations
- Accesses to key are Audited

see Requirements 3.5, 3.6

The requirements of PCI DSS related to database

Innovative R&D by NTT

Data Encryption and Key Management.

Keep your Database Secure.

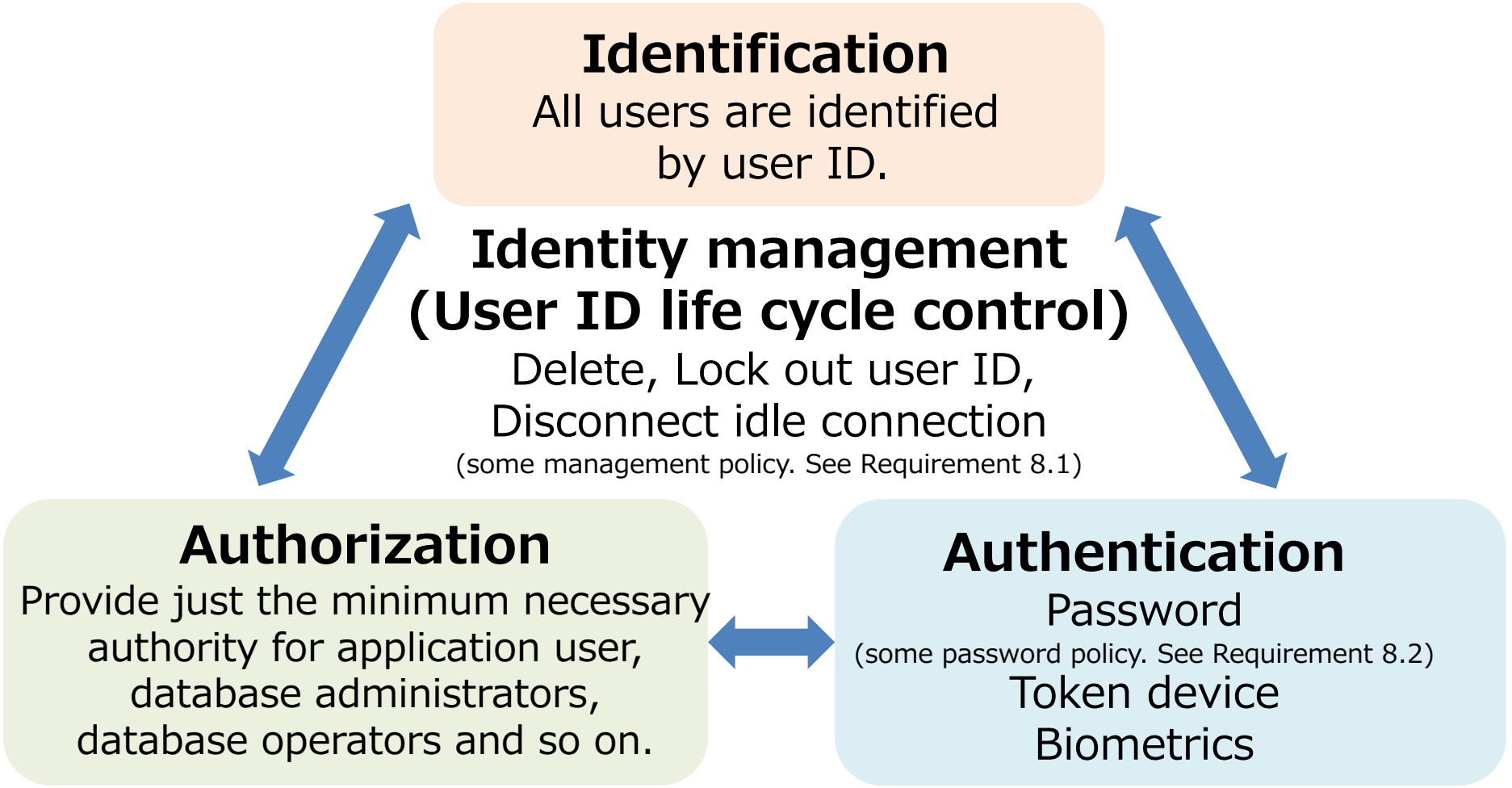
CI Data Security Standard – High Level Ov

Build and Maintain a Sec Network and Systems	1. Install and maintain a firewall configuration protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	**7. Restrict access to cardholder data by business need to know** **8. Identify and authenticate access to system components** 9. Restrict physical access to cardholder data
Regularly Monitor and Tes Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Inform Security Policy	12. Maintain a policy that addresses information security for all personnel

User Identification, Authentication, Authorization, Identity management.

NTT

PCI DSS requirements 7 & 8 say



The requirements of PCI DSS related to database

Innovative R&D by NTT

Data Encryption and Key Management.

Keep your Database Secure.

CI Data Security Standard – High Level Ov

Build and Maintain a Sec Network and Systems	1. Install and maintain a firewall configuration protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Tes Networks	**10. Track and monitor all access to network resources and cardholder data** 11. Regularly test security systems and processes
Maintain an Inform Security Policy	12. Maintain a policy that addresses information security for all rsonnel

User Identification, Authentication, Authorization, Identity management.

Audit.

NTT

iv. Audit

PCI DSS Requirement 10 says

- **These events must be audited.**

#	Requirement
10.2.1	Access to PANs
10.2.2	All operations of administrators
10.2.3	Access to audit logs
10.2.4	Invalid access
10.2.5	Operation about Identification, Authentication (DCL)
10.2.6	Change audit log setting and Stop to audit
10.2.7	DDL

iv. Audit

PCI DSS Requirement 10 says

- **Audit logs must output following information.**

#	Requirement
10.3.1	User ID
10.3.2	Event category (ex. READ, WRITE)
10.3.3	Date and time
10.3.4	Success or Failure
10.3.5	Client information (ex. IP address)
10.3.6	Object name, Object id (ex. Table name, Column name)

- **10.5 Audit logs also must be audited and protected.**

3. How to Apply to PostgreSQL

i. Keep your Database Secure.
ii. Data Encryption and Key Management.
iii. User Identification, Authentication, Authorization, Identity management.
iv. Audit.

i. Keep your Database Secure

Innovative R&D by NTT

To Do

- Don’t use postgres(default) account.
- Change 5432(default) port.
- Use openSSL connection with psql.
  - See manual.
    https://www.postgresql.org/docs/current/static/runtime-config-connection.html
- Restrict unnecessary access by pg_hba.conf
  - See manual.
    https://www.postgresql.org/docs/current/static/auth-pg-hba-conf.html
- Update binaries to latest minor version.

Again,
Traditional (or basic) security practices are important!

ii. Data Encryption and Key Management

Innovative R&D by NTT

To Do

- Use **pgcrypto**
  pgcrypto is a good encryption module.
  see manual. https://www.postgresql.org/docs/current/static/pgcrypto.html

Difficulty to apply PCI DSS to PostgreSQL.

- Manage two-tier encryption key by yourself
  - An application development is hard!

→ You should consult the PostgreSQL vendors.

● It seems to me that ...

PostgreSQL needs
TDE (Transparent Data Encryption) with
KMS (Key Management Service).

Should we start discussion in PostgreSQL community?

iii. User Identification, Authentication, Authorization, Identity management

Innovative R&D by NTT

To Do

- Don’t use superuser!
- Apply PCI DSS password policies.
- Manage each user id.

For details, next slides!

NTT

iii. User Identification, Authentication, Authorization, Identity management

Innovative R&D by NTT

To Do

- Don't use superuser!
  Superuser can do everything!
  All user id must be restricted to least privileges necessary to perform job responsibilities.
  see manual https://www.postgresql.org/docs/current/static/ddl-priv.html
  https://www.postgresql.org/docs/current/static/ddl-rowsecurity.html

Difficulties to apply PCI DSS to PostgreSQL.

Some useful SQLs ~~and functions~~ need superuser privilege.
For example,

- CREATE/ALTER EVENT TRIGGER
- CREATE FOREIGN DATA WRAPPER
- CREATE TABLESPACE
- ~~pg_reload_conf(), pg_rotate_logfile(), pg_switch_xlog()~~

-> Since PG 9.6, these can be executed by non superusers.

● It seems to me that ...

Users who are granted superuser privilege must be audited fully.

Innovative R&D by NTT

- A suggestive example?

  PostgreSQL on Amazon RDS

  rds_superuser role

  ➢ has the most privileges on the DB instance
  - add extensions
  - manage tablespaces
  - use pg_terminate_backend, pg_cancel_backend
  - grant the replication attribute onto all roles

  ref: http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_PostgreSQL.html

  But

  ➢ has no privilege to access objects owned by other users by default.

  ref: https://blog.2ndquadrant.com/the-rds_superuser-role-isnt-that-super/

● It seems to me that ...

Even in PostgreSQL, superuser should not be able to access objects owned by other users by default.

iii. User Identification, Authentication, Authorization, Identity management

- Use Default Roles!

PostgreSQL 10 new feature.

https://www.postgresql.org/docs/devel/static/default-roles.html

Role	Allowed Access
pg_read_all_settings	Read all configuration variables, even those normally visible only to superusers.
pg_read_all_stats	Read all pg_stat_* views and use various statistics related extensions, even those normally visible only to superusers.
pg_stat_scan_tables	Execute monitoring functions that may take AccessShareLocks on tables, potentially for a long time.
pg_signal_backend (Since PG 9.6)	Send signals to other backends (eg: cancel query, terminate).
pg_monitor	Read/execute various monitoring views and functions. This role is a member of pg_read_all_settings, pg_read_all_stats and pg_stat_scan_tables.

- It seems to me that ...

Are more Default Roles needed?
-> audit role (or security role).

iii. User Identification, Authentication, Authorization, Identity management

Innovative R&D by NTT

To Do

- Apply password policy
  - ➢ Use contrib/passwordchk.
    - ■ A minimum length of 8 characters.
    - ■ Not contain user/role name.
    - ■ Mix of letter and non-letter.

      see https://www.postgresql.org/docs/current/static/passwordcheck.html
  - ➢ Use “CREATE ROLE ... WITH VALID UNTIL ...;”
    - ■ The password is valid until the end of a specific date.

      see https://www.postgresql.org/docs/current/static/sql-createrole.html

Difficulties to apply PCI DSS to PostgreSQL.

- These password policies cannot be implemented in PostgreSQL.
  - 8.2.5 Do not allow a new password that is the same as any of the last 4 passwords used.
  - 8.2.6 Set passwords for first-time use and change immediately after the first use.

● It seems to me that ...

We should use a directory service.

NTT

iii. User Identification, Authentication, Authorization, Identity management

Innovative R&D by NTT

To Do

- Manage each user id.
  - ➢ Delete or Lockout user id according to PCI DSS requirements.
    Delete: DROP ROLE ...; see manual https://www.postgresql.org/docs/current/static/sql-droprole.html
    Lockout: ALTER ROLE ... WITH NOLOGIN;
    see manual https://www.postgresql.org/docs/current/static/sql-droprole.html

Difficulties to apply PCI DSS to PostgreSQL.

- To perform the following requirement is hard only in PostgreSQL.
  - 8.1.4 Inactive user accounts within 90 days.
  - 8.1.6 Repeated access attempts after not more than six attempts.
  - 8.1.8 Require the user to re-authenticate If a session has been idle for more than 15 minutes.

● It seems to me that ...

We should use a directory service.

- Use LDAP authentication.
  see https://www.postgresql.org/docs/current/static/auth-methods.html

NTT

iii. User Identification, Authentication, Authorization, Identity management

Innovative R&D by NTT

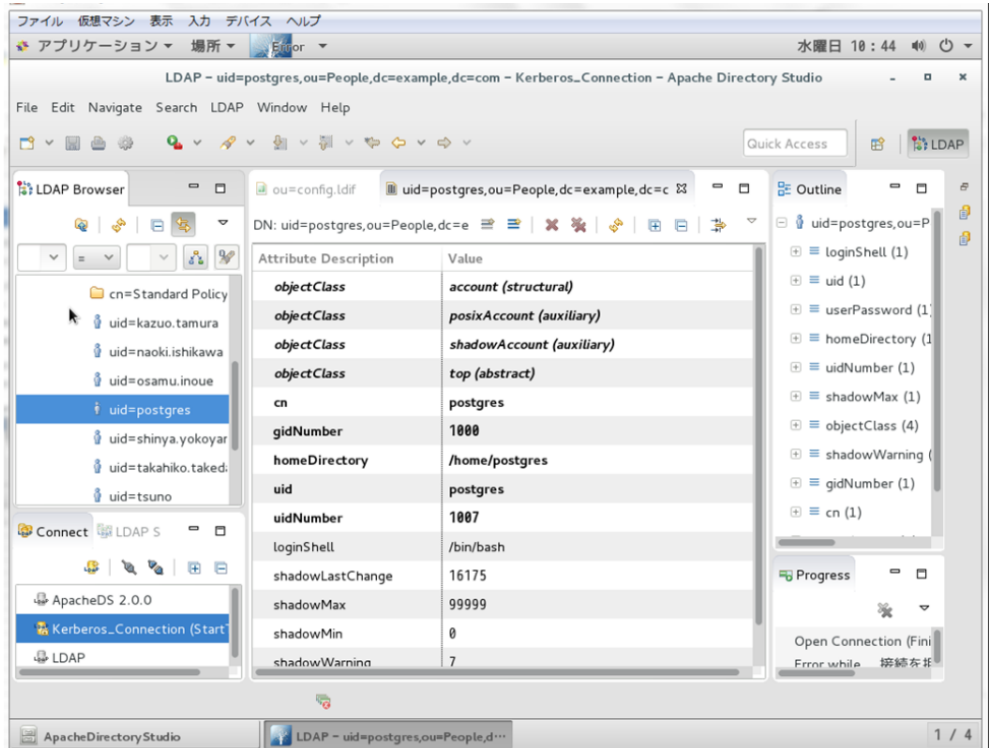
Apache DS and Apache Directory studio

- Apache DS is directory service software.
- Apache Directory studio is GUI console of directory service.

http://directory.apache.org/apacheds/

```
WELCOME TO THE APACHEDS INSTALLER PROGRAM

 _                    _            ____   ____
/ \    _ __    __ _  ___| |__    ___|  _ \ / ___|
/ _ \  | '_ \  / _` |/ __| '_ \  / _ \ | | \___ \
/ ___ \ | |_) | (_| | (__| | | |  __/ |_| |___) |
/_/   \_\ .__/ \__,_|\___|_| |_|\___|____/|____/
        |_|

ApacheDS is distributed under the Apache Software License Version 2.0.

Please, take some time to read the license terms below.

                        Apache License
                  Version 2.0, January 2004
               http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

   "License" shall mean the terms and conditions for use, reproduction,
   and distribution as defined by Sections 1 through 9 of this document.
```

https://directory.apache.org/studio/

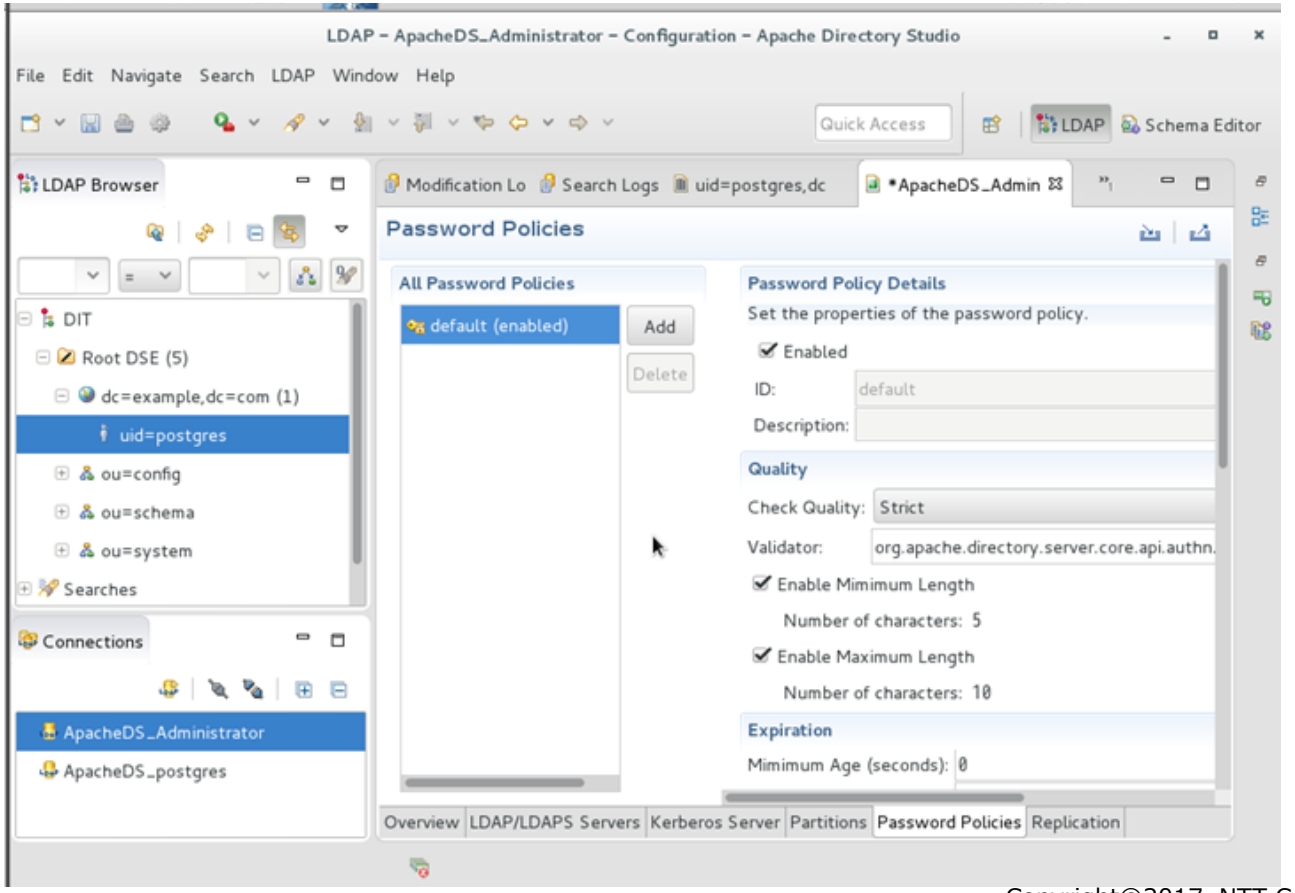


iii. User Identification, Authentication, Authorization, Identity management

Apache DS and Apache Directory studio

- Rich password policy configuration.
- Rich lock out policy configuration.
- Authentication Log

see official document.
http://directory.apache.org/apacheds/
https://directory.apache.org/studio/



Innovative R&D by NTT

Difficulties to apply PCI DSS to PostgreSQL with Apache DS.

- Apache DS can not create user accounts in PostgreSQL
  - Create a PostgreSQL user accounts then register them to Apache DS.

- Apache DS and Apache Directory studio can not control and edit authorization of PostgreSQL.
  - You need to login to PostgreSQL to edit authorization of PostgreSQL.

iv. Audit

Innovative R&D by NTT

To Do

- Use PostgreSQL server log.
  PostgreSQL server log can output the following events.
  see manual https://www.postgresql.org/docs/current/static/runtime-config-logging.html

#	Requirement	postgresql.conf parameters
10.2.1	Access to PANs	log_statement = all
10.2.2	All operations of administrators	log_statement = all
10.2.3	Access to audit logs	#Use OS module (ex. auditd)
10.2.4	Invalid access	log_connection, log_disconnection
10.2.5	Operation about Identification, Authentication (DCL)	log_statement = all
10.2.6	Change audit log setting and Stop to audit	log_statement = all #And use OS module
10.2.7	DDL	log_statement = all

see https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Security_Guide/chap-system_auditing.html

NTT

iv. Audit

Innovative R&D by NTT

To Do

- Use PostgreSQL server log.
  PostgreSQL server log can output the following information.
  see manual https://www.postgresql.org/docs/current/static/runtime-config-logging.html

#	Requirement	postgresql.conf parameters
10.3.1	User ID	log_line_prefix
10.3.2	Event category (ex. READ, WRITE)	log_line_prefix
10.3.3	Date and time	log_line_prefix
10.3.4	Success or Failure	log_line_prefix
10.3.5	Client information (ex. IP address)	log_line_prefix
10.3.6	Object name, Object id (ex. Table name)	**No such configuration params...**

- Use Syslog to send another server and use auditd.

NTT

iv. Audit

Innovative R&D by NTT

Difficulties to apply PCI DSS to PostgreSQL.

- Object name do not output.
  - Some SQLs are difficult to audit.

    For example, “DO”

    ref: https://github.com/pgaudit/pgaudit

```
testdb=# DO $$
BEGIN
  EXECUTE 'SELECT * FROM import' || 'ant_table';
END $$;
```

    server log output (log_statement=all)

```
LOG: statement: DO $$
       BEGIN
           EXECUTE 'SELECT * FROM import' || 'ant_table';
       END $$;
```

    To search SQL accessing to "important_table" is hard.

- Log size is big.
  - It does not have useful log filters.

iv. Audit

Difficulties to apply PCI DSS to PostgreSQL.

- Superuser can change server log settings easily.
  - Hard to confirm to Requirement 10.2.2

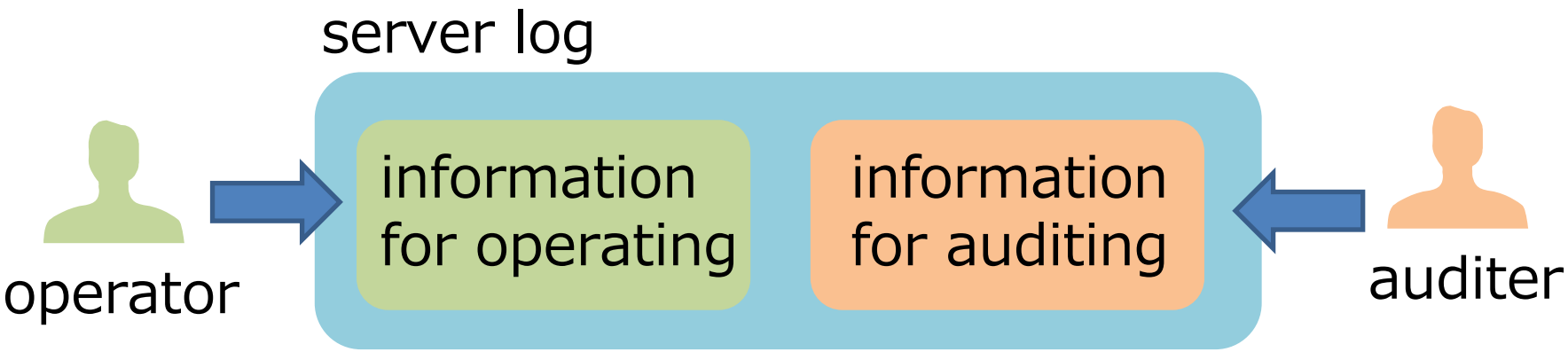
    Requirement 10.2.2

    All operations of administrators must be audited

- Can not divide a log for auditing into a log for operating.
  - Hard to confirm to Requirement 10.5

    Requirement 10.5

    Audit logs also must be protected.



iv. Audit

Innovative R&D by NTT

- It seems to me that ...

We should use **pgaudit**!

pgaudit is developed by 2ndquadrant and Crunchy Data.

https://github.com/pgaudit/pgaudit

Install pgaudit and
set shared_preload_libraries = ‘pgaudit‘ in postgresql.conf.

NTT

iv. Audit

- **pgaudit can reduce audit log size.**
  Set class name to pgaudit.log parameter in postgresql.conf.

  pgaudit.log = *class name*, ...

  pgaudit output only SQLs belonging to the class.

class name	outputted SQL
READ	SELECT, VALUES, COPY etc.
WRITE	INSERT, UPDATE, DELETE, TRUNCATE, COPY etc.
FUNCTION	DO etc.
ROLE	CREATE|ALTER|DROP USER|ROLE|GROUP, GRANT, REVOKE etc.
DDL	CREATE ... , ALTER ... , DROP ... , REINDEX, SELECT INTO etc.
MISC	VACUUM, ANALYZE, BEGIN, COMMIT, ROLLBACK, SET, LOCK etc.
ALL	ALL SQLs

iv. Audit

Innovative R&D by NTT

For example,

postgresql.conf

```
shared_preload_libraries = pgaudit
pgaudit.log = 'WRITE, DDL, MISC'
```

SQL

```
testdb=# BEGIN;
testdb=# SELECT * FROM pgbench_accounts LIMIT 1;
testdb=# UPDATE pgbench_accounts SET bid = '4' WHERE aid = '1';
testdb=# COMMIT;
```

Audit log

```
LOG:  AUDIT: SESSION,1,1,MISC,BEGIN,,,BEGIN;,<not logged>
LOG:  AUDIT: SESSION,2,1,WRITE,UPDATE,,,
             UPDATE pgbench_accounts SET bid = '4'
                    WHERE aid = '1';,<not logged>
LOG:  AUDIT: SESSION,3,1,MISC,COMMIT,,,COMMIT;,<not logged>
```

-> “SELECT” does not output.
The log size is suppressed to a minimum.

NTT

iv. Audit

- **pgaudit can output object name.**

postgresql.conf

```
shared_preload_libraries = pgaudit
pgaudit.log = 'READ'
```

SQL

```
testdb=# DO $$
BEGIN
       EXECUTE 'SELECT * FROM import' || 'ant_table';
END $$;
```

Audit log

```
LOG:  AUDIT: SESSION,2,1,READ,SELECT,TABLE,
             public.important_table,
             SELECT * FROM important_table,<none>
```

-> Table name is outputted with schema name.

To search SQL accessing to "important_table" is easy!

iv. Audit

Innovative R&D by NTT

pgaudit is good tool!

However,
pgaudit can not cover the following two PCI DSS requirements yet.

Difficulties to apply PCI DSS to PostgreSQL with pgaudit.

- Superuser can change pgaudit settings easily.
  - Hard to confirm to Requirement 10.2.2
- Can not divide a server log into a pgaudit log.
  - Hard to confirm to Requirement 10.5

It seems to me that ...

- Superuser must not be able to change pgaudit settings easily!
- Divide a server log into a pgaudit log.
  -> PostgreSQL logger should be extend for auditing!

NTT

Wrap up.

PostgreSQL can conform to PCI DSS by the following things.

- Set basic configurations and do basic security practices.
- Use pgcrypto.
- Use a directory service.
- Use pgaudit.

Should be better.

- TDE (Transparent Data Encryption) with KMS (Key Management Service).
- Operation without superuser privilege.

PostgreSQL STIG

Innovative R&D by NTT

"Announcing the PostgreSQL STIG"

http://info.crunchydata.com/blog/postgres-stig-disa-security-guide

PostgreSQL STIG provides guidance on the configuration of PostgreSQL to address requirements associated with:

- Auditing
- Logging
- Data Encryption at Rest
- Data Encryption Over the Wire
- Access Controls
- Administration
- Authentication
- Protecting against SQL Injection

END

Questions?

e-mail: oyama.masanori.1987 at gmail.com

Disk encryption

- Disk encryption is allowed by PCI DSS,
  But how to apply to PostgreSQL?

Requirement 3.4.1

If disk encryption is used (rather than file- or column-level database encryption), **logical access must be managed separately and independently of native operating system authentication and access control mechanisms** (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

Note: This requirement applies in addition to all other PCI DSS encryption and key-management requirements.