

Fujitsu Enterprise Postgres 16

Release Notes

Linux

J2UL-2946-01PEZ0(00)
June 2024

Preface

Purpose of this document

This document provides release information for Fujitsu Enterprise Postgres.

Structure of this document

This document is structured as follows:

[Chapter 1 New Features and Improvements](#)

Explains the new features and improvements in this version.

[Chapter 2 Compatibility Information](#)

Provides information regarding compatibility.

Export restrictions

Exportation/release of this document may require necessary procedures in accordance with the regulations of your resident country and/or US export control laws.

Issue date and version

Edition 1.0: June 2024

Copyright

Copyright 2022-2024 Fujitsu Limited

Contents

Chapter 1 New Features and Improvements.....	1
1.1 Features Added in 16.....	1
1.1.1 OSS.....	1
1.1.1.1 PostgreSQL Rebase.....	1
1.1.1.2 OSS Updates Provided.....	1
1.1.2 Security.....	1
1.1.2.1 Policy-based Password Management.....	1
1.1.2.2 User Management Using an LDAP Server.....	2
1.1.2.3 Scalable Audit Log Feature.....	2
1.1.3 Performance.....	2
1.1.3.1 Fixed Statistics.....	2
Chapter 2 Compatibility Information.....	3
2.1 Installation/Setup Incompatibility.....	3
2.1.1 How max_wal_senders is calculated.....	3
2.1.2 How max_worker_processes is calculated.....	3
2.1.3 Removing Old llvm Support for JIT compilation.....	3
2.2 Application Migration Incompatibility.....	4
2.2.1 Changing the OID of the Data Type (NCHAR type) that Handles National Characters.....	4
2.3 Operation Migration Incompatibility.....	4
2.3.1 Deprecation of Some Encryption Algorithms in pgcrypto.....	4
2.3.2 Deprecation of Certificates Signed Using SHA1.....	5
2.3.3 Abolition of Message Numbers.....	5
2.3.4 Adding the key_name Column to the View pgx_tde_master_key.....	5
2.4 pgaudit Incompatibility.....	5
2.4.1 Repairing Unwanted Output in the Audit Log.....	6
2.5 pg_dbms_stats Incompatibility.....	6
2.5.1 Change in Execution Plan due to Fixed Height of Btree index.....	6
2.5.2 Incompatibility of Import Features with Fixed Height of Btree index.....	7
2.6 Confidentiality Management Incompatibility.....	7
2.6.1 Changes due to Changes in the pg_dump Specification.....	7
2.6.2 Changing Permission Settings by Changing the CREATEROLE Permission.....	7
2.6.3 Change due to Restriction of CREATEROLE Privilege.....	8
Index.....	9

Chapter 1 New Features and Improvements

This chapter explains Fujitsu Enterprise Postgres new features and improvements added in this version.

Table 1.1 New features and improvements

Version and level	Classification	Feature
16	OSS	PostgreSQL Rebase
		OSS Updates Provided
	Security	Policy-based Password Management
		User Management Using an LDAP Server
		Scalable Audit Log Feature
	Performance	Fixed Statistics

1.1 Features Added in 16

This section explains new features and improvements in Fujitsu Enterprise Postgres 16.

1.1.1 OSS

This section explains the new feature related to OSS:

- PostgreSQL Rebase
- OSS Updates Provided

1.1.1.1 PostgreSQL Rebase

The PostgreSQL version that Fujitsu Enterprise Postgres is based on is 16.2.

1.1.1.2 OSS Updates Provided

The OSS provided by Fujitsu Enterprise Postgres has been updated.



See

Refer to "OSS Supported by Fujitsu Enterprise Postgres" in the General Description for details.

1.1.2 Security

This section explains the new features and improvements related to security:

- Policy-based Password Management
- User Management Using an LDAP Server
- Scalable Audit Log Feature

1.1.2.1 Policy-based Password Management

You can now perform policy-based password operation when using password authentication as client authentication when connecting to a database.



See

.....
Refer to "Policy-based Password Management" in the Operation Guide for more information.
.....

1.1.2.2 User Management Using an LDAP Server

Using ldap2pg allows LDAP and Fujitsu Enterprise Postgres user synchronization without requiring the server administrator to be aware of the Fujitsu Enterprise Postgres user registration status.



See

.....
Refer to "ldap2pg" in the Installation Guide for Client for details.
.....

1.1.2.3 Scalable Audit Log Feature

By using the scalable audit log feature, you can now capture audit logs without performance degradation, even for systems with high application multiplicity and large amounts of audit logs.



See

.....
Refer to "Audit Log Feature" in the Security Operation Guide for details.
.....

1.1.3 Performance

This section describes new features related to Performance.

- Fixed Statistics

1.1.3.1 Fixed Statistics

The height of a Btree index can now also be fixed for statistics.

This allows all statistics used in SQL execution plans to be fixed.



See

.....
Refer to "Fixing the Height of a Btree Index" in the Operation Guide.
.....

Chapter 2 Compatibility Information

This chapter explains incompatible items and actions required when migrating from an earlier version to Fujitsu Enterprise Postgres 16. Check compatibility before migrating and take the appropriate action.

2.1 Installation/Setup Incompatibility

Item	Pre-migration version		
	14	14 SP1	15
How max_wal_senders is calculated	Y	Y	Y
How max_worker_processes is calculated	Y	Y	Y
Removing Old llvm Support for JIT compilation	Y	Y	N

Y: Incompatibility exists

N: Incompatibility does not exist

2.1.1 How max_wal_senders is calculated

Incompatibility

In Fujitsu Enterprise Postgres 16 or later, Fujitsu Enterprise Postgres uses the following values from the value set for the max_wal_senders parameter:

Policy-based password management in a streaming replication environment : Number of direct downstream hot standby servers

Action method

If necessary add a value for the max_wal_senders parameter.

2.1.2 How max_worker_processes is calculated

Incompatibility

In Fujitsu Enterprise Postgres 16 or later, Fujitsu Enterprise Postgres uses the following values from the value set for the max_worker_processes parameter:

Default value to use : 1

Policy-based password management in a streaming replication environment with a hot standby server : 1

Action method

If necessary add a value for the max_worker_processes parameter.

2.1.3 Removing Old llvm Support for JIT compilation

Incompatibility

In Fujitsu Enterprise Postgres 15, the following llvm which JIT compilation can use have been removed.

- llvm version 11

Action method

None.

2.2 Application Migration Incompatibility

Item	Pre-migration version		
	14	14 SP1	15
Changing the OID of the Data Type (NCHAR type) that Handles National Characters	Y	Y	N

Y: Incompatibility exists

2.2.1 Changing the OID of the Data Type (NCHAR type) that Handles National Characters

Incompatible

In Fujitsu Enterprise Postgres 15, OIDs for national character data types (NCHAR types) have changed.

Action method

If you are using a national character data type (NCHAR type), recompile the application and run it with Fujitsu Enterprise Postgres 15 or later clients.

2.3 Operation Migration Incompatibility

Item	Pre-migration version		
	14	14 SP1	15
Deprecation of Some Encryption Algorithms in pgcrypto	Y	Y	Y
Deprecation of Certificates Signed Using SHA1	Y	Y	Y
Abolition of Message Numbers	Y	Y	N
Adding the key_name Column to the View pgx_tde_master_key	N	Y	N

Y: Incompatibility exists

N: Incompatibility does not exist

2.3.1 Deprecation of Some Encryption Algorithms in pgcrypto

Incompatibility

In Fujitsu Enterprise Postgres 16 and later, the PostgreSQL extension pgcrypto does not support the use of the encryption algorithm, which has become a legacy algorithm in the OpenSSL3 family, by default.

The encryption algorithms that are no longer available by default are:

- BF
- CAST5
- DES-ECB
- DES-CBC
- MD4
- Whirlpool

Action method

If you use a legacy OpenSSL provider, create an OpenSSL configuration file and set the parameters in postgresql.conf. Refer to "Settings for Using Legacy OpenSSL Providers" in the Installation and Setup Guide for Server for information .

2.3.2 Deprecation of Certificates Signed Using SHA1

Incompatibility

In Fujitsu Enterprise Postgres 16 and later, you cannot connect to a database server using a certificate signed using SHA1.

Action method

Resubmit the certificate used for certificate authentication with SHA2 or higher.

2.3.3 Abolition of Message Numbers

Incompatibility

In Fujitsu Enterprise Postgres 15, the message number output at the end of the message is abolished.

Message numbers are output for messages output by Mirroring Controller.

For FUJITSU Enterprise Postgres 14 SP1 or earlier

The message number was printed at the end of the message.

[example]

```
3D000: 2017-07-10 19:41:05 JST[13899]: [1-1] user=fepuser,db=fep,remote=127.0.0.1(51902)
app=[unknown] FATAL: database "fep" does not exist (10571)
```

For Fujitsu Enterprise Postgres 15

No message number is output at the end of the message.

[example]

```
3D000: 2023-04-10 19:41:05 JST [13899]: [1-1] user = fepuser,db = fep,remote = 127.0.0.1(51902)
app = [unknown] FATAL: database "fep" does not exist
```

Action method

None.

2.3.4 Adding the key_name Column to the View pgx_tde_master_key

Incompatibility

In Fujitsu Enterprise Postgres 15, add a key_name column to the view pgx_tde_master_key.

Action method

None.

2.4 pgaudit Incompatibility

Item	Pre-migration version		
	14	14 SP1	15
Repairing Unwanted Output in the Audit Log	Y	Y	Y

2.4.1 Repairing Unwanted Output in the Audit Log

Incompatibility

In Fujitsu Enterprise Postgres 16, we changed the audit log so that it no longer contains unwanted information at the end.

Fujitsu Enterprise Postgres 15 or earlier

Some audit logs contain unwanted content at the end.

[Example]

```
Input: INSERT INTO trig_test VALUES ('new value');
Part of the audit log: NOTICE:  AUDIT:  SESSION,WRITE,,[local],,pg_regress/class,,baz,,
11,2,INSERT,,TABLE,public.trig_audit,, "INSERT INTO trig_audit SELECT 'I', now(), user, NULL,
NEW.*", (" "new value"")  trig_audit AFTER ROW INSERT 16484 trig_test trig_test public 0  f"
```

Fujitsu Enterprise Postgres 16

Prevent unwanted from being output to the audit log.

[Example]

```
Input: INSERT INTO trig_test VALUES ('new value');
Part of the audit log: NOTICE:  AUDIT:  SESSION,WRITE,,[local],,pg_regress/class,,baz,,
11,2,INSERT,,TABLE,public.trig_audit,, "INSERT INTO trig_audit SELECT 'I', now(), user, NULL,
NEW.*", (" "new value"")"
```

Action method

None.

2.5 pg_dbms_stats Incompatibility

Item	Pre-migration version		
	14	14 SP1	15
Change in Execution Plan due to Fixed Height of Btree index	Y	Y	Y
Incompatibility of Import Features with Fixed Height of Btree index	Y	Y	Y

Y: Incompatibility exists

N: Incompatibility does not exist

2.5.1 Change in Execution Plan due to Fixed Height of Btree index

Incompatibility

Fixing statistics with the following features may change the execution plan because the height of the Btree index is now fixed as well:

- dbms_stats.lock_*
- dbms_stats.restore_*
- dbms_stats.import_*

Action method

If you want to run compatibility with Fujitsu Enterprise Postgres 15 and earlier, configure the following:

- pg_dbms_stats.use_tree_height

- pg_dbms_stats.lock_tree_height

2.5.2 Incompatibility of Import Features with Fixed Height of Btree index

Incompatibility

Statistics exported by the export function in pg_dbms_stats prior to Fujitsu Enterprise Postgres 15 cannot be imported using the legacy import function.

Action method

When importing statistics exported by the export function in pg_dbms_stats prior to Fujitsu Enterprise Postgres 15, use a function with the suffix "_no_tree_height" appended to its name.

2.6 Confidentiality Management Incompatibility

Item	Pre-migration version		
	14	14 SP1	15
Changes due to Changes in the pg_dump Specification	N	N	Y
Changing Permission Settings by Changing the CREATEROLE Permission	N	N	Y
Change due to Restriction of CREATEROLE Privilege	N	N	Y

Y: Incompatibility exists

N: Incompatibility does not exist

2.6.1 Changes due to Changes in the pg_dump Specification

Incompatibility

If you are using multiple non-superuser sensitivity confidentiality management role to manage the sensitivity matrix, run the product-provided policy configuration script to define a row-level security feature policy on the table provided by the sensitivity support feature to make the sensitivity management roles independent of each other.

In Fujitsu Enterprise Postgres 15 or earlier, the effects of this script could be retained and backed up by pg_dump, but as of Fujitsu Enterprise Postgres 16, policy settings can no longer be backed up.

Action method

In Fujitsu Enterprise Postgres 16 or later, if you are managing a sensitivity matrix using more than one confidentiality management role other than superuser, then immediately after restoring a clear-text dump file using pg_dump, run the following command as superuser to reapply the confidentiality management feature policy:

```
psql -f ${install_dir}/share/extension/pgx_confidential_management_support_policy.sql
```

2.6.2 Changing Permission Settings by Changing the CREATEROLE Permission

Incompatibility

In Fujitsu Enterprise Postgres 16, if you want to use a non-superuser role as a confidentiality management role, you may need to set additional permissions for the confidentiality management role.

Action method

The confidentiality management role must already have the privileges it expects to operate on, other than the CREATEROLE privilege.

[Example]

If the confidentiality management role "manager_role" is also going to work with CREATEDB privileges, it will also set CREATEDB privileges when the role is created, like this:

```
CREATE ROLE manager_role LOGIN CREATEROLE CREATEDB;
```

If the required permissions are not set, the sensitivity management API terminates abnormally with a message similar to the following:

```
ERROR: permission denied to create role
DETAIL: Only roles with the CREATEDB attribute may create roles with the CREATEDB attribute.
```

2.6.3 Change due to Restriction of CREATEROLE Privilege

Incompatibility

In Fujitsu Enterprise Postgres 16, if you want to use a non-superuser role as a secret management role, the permissions on the roles that can be set in the secret group are different, and the roles that you set in the secret group must be granted ADMIN OPTION permission on the secret confidentiality management role before they can be used.

Action method

Take one of the following actions:

- A role created with the privileges of the confidentiality management role is to be managed in the confidential group. This creates a role that grants only the ADMIN OPTIN privilege to the sensitive confidentiality management role.
- Grant ADMIN OPTION permission on the role to the sensitive management role before setting the managed role to the sensitive group.

[Example]

You want to grant only the ADMIN OPTION privilege for role "user_role1" to the confidentiality management role "manager_role".

```
GRANT user_role1 TO manager_role WITH ADMIN TRUE, INHERIT FALSE, SET FALSE;
```

If the required permissions are not set, the sensitivity management API terminates abnormally with a message similar to the following:

```
ERROR: permission denied to alter role
DETAIL: Only roles with the CREATEROLE attribute and the ADMIN option on role "user_role1" may alter this role.
```

Index

[C]

Compatibility Information.....3

[F]

Features Added in 16.....1