FUJITSU

Achieving secure and productive database Privileged Access Management

FUJITSU

Security measures are essential for business continuity, and managing access from accounts with strong operational privileges Privileged Access Management, or PAM - is particularly crucial.

If privileged accounts are compromised by a third party, data falsification and leakage become significantly easier. Therefore, companies are required to securely manage privileged access across their entire system – including OS, network devices, and databases – in accordance with their organizational security requirements.

However, privileged access management is not easy. It requires robust security policies, including rigorous storage and updating of user credentials, and mechanisms for access monitoring. Implementation across the entire system is costly, leading many companies to adopt privileged access management products.

Centralized management of privileged accounts is also required for databases. Fujitsu Enterprise Postgres, in addition to its own database-specific user and access management features, integrates with privileged access management products. This integration enables the secure and automated management of database privileged account passwords, and by controlling and monitoring access by privileged accounts, it enables database operation and management that complies with the organization's security requirements.

Benefits of integrating Fujitsu Enterprise Postgres with Privileged Access Management products

Integrating **Fujitsu Enterprise Postgres** with **Privileged Access Management** products automates the database's privileged access management.
This maintains productivity while ensuring compliance and secure access to critical assets

Preventing misuse and malicious operations of database administrator privileges

By requiring approval for database logins, it's possible to prevent the misuse of administrator privileges and malicious actions.

Simplifying the security operation of database administrator account passwords

Passwords for privileged accounts are stored in an isolated, secure environment and are automatically updated in accordance with organizational security policies.

Preventing database administrator account password leaks

Password authentication during database connection is securely handled within the privileged access management product. Unless granted viewing privileges, passwords cannot be accessed, thus reducing the risk of leakage.

Facilitating the understanding of operations in case of misuse of database administrator privilege

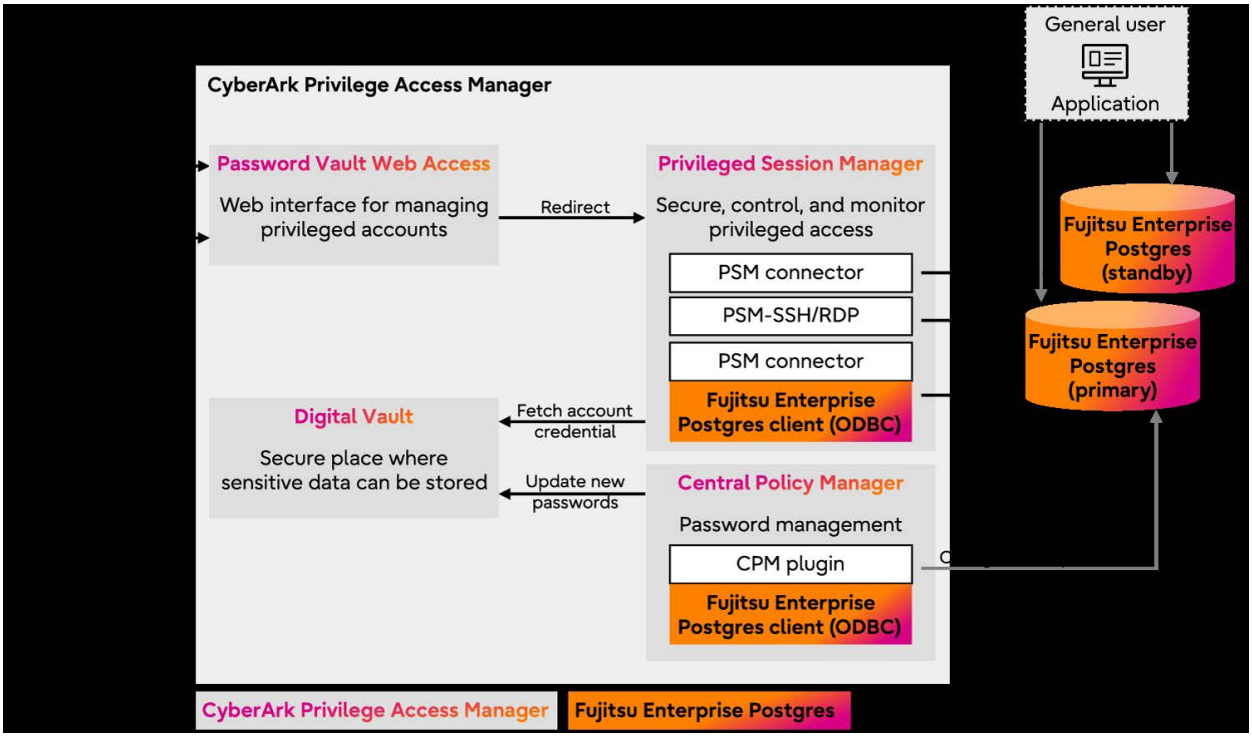
Operations performed by DB administrators can be viewed as text logs or recorded videos. Combined with Fujitsu Enterprise Postgres' Dedicated Audit Log it allows for easier and detailed understanding of malicious user activity, including misuse of administrator privilege.

Integration of Fujitsu Enterprise Postgres and CyberArk Privileged Access Manager

The following sections describe the system configuration and integration procedure when integrating with CyberArk Privileged Access Manager, one example of a privileged access management product.

System Configuration

The system configuration using Fujitsu Enterprise Postgres and CyberArk Privileged Access Manager is below.



CyberArk Privileged Access Manager consists of the following four fundamental components:

- **Digital Vault** (Vault) - Prevents password leaks

  Securely stores sensitive data associated with privileged accounts, including passwords. When connecting to the database using a privileged account, the **Privileged Session Manager** retrieves the account credentials and handles authentication, preventing privileged account password leakage.

- **Password Vault Web Access** (PVWA) - Prevents privilege abuse and malicious operations

  Web portal for managing privileged access, within which you can add Fujitsu Enterprise Postgres privileged accounts and configure password auto-updates using **Central Policy Manager** and connection settings using **Privileged Session Manager**. By using the Dual Control feature, database logins and operations can be made subject to approval, preventing the misuse of database administrator privileges and malicious actions.

- **Central Policy Manager** (CPM) - Simplifies security operation

  Password update is automated by connecting to the DB using a **Central Policy Manager** plugin that supports password management for Fujitsu Enterprise Postgres and a Fujitsu Enterprise Postgres client (ODBC driver). Automatic password updates can be configured in accordance with organizational security policies, automating the previously manual password management tasks and simplifying operations.

- **Privileged Session Manager** (PSM) - Facilitates the understanding of operation

  Using the PSM connector for Fujitsu Enterprise Postgres and the Fujitsu Enterprise Postgres client (psql), the **Privileged Session Manager** acts as a proxy for database connections. It handles authentication, enabling secure database logins without exposing passwords to the operating user. For accessing the server to execute database server commands, you can use the standard PSM connector for SSH or RDP. All operations on the PSM server are recorded in both text and video format, allowing for easy identification of actions taken in the event of database administrator privilege misuse.

How to get started - Integration Procedure

1. Fujitsu Enterprise Postgres server installation/setup

   a. Install and set up Fujitsu Enterprise Postgres.

   Refer to the **Fujitsu Enterprise Postgres Installation and Setup Guide for Server** for details.

   b. Enhance security by configuring the following:

   - Configure SSL connection setup to encrypt client/server communication.
     Refer to the **Fujitsu Enterprise Postgres Operation Guide** section *Configuring secure communication using Secure Sockets Layer* for details.
   - Restrict database administrator connections to only through CPM/PSM.
     Edit pg_hba.conf to configure accordingly. For example, to allow connections from only the **Central Policy Manager** server (`192.168.12.10`) and **Privileged Session Manager** server (`192.168.12.11`) for the database administrator (postgres):

     ```
     # TYPE   DATABASE    USER        ADDRESS              METHOD
     hostssl  all         postgres    192.168.12.10/32     scram-sha-256
     hostssl  all         postgres    192.168.12.11/32     scram-sha-256
     ```

     Refer to the **PostgreSQL documentation** section *The pg_hba.conf file* for more details on the file.

2. CyberArk Privileged Access Manager Installation and Setup

   a. Review and select the appropriate installation method and install the components in this order: **Digital Vault**, **PrivateArk Client**, **Password Vault Web Access** (PVWA), **Central Policy Manager** (CPM) and **Privileged Session Manager** (PSM).

   Refer to the **CyberArk documentation** section *Installation* for details.

   b. Install any additional solutions for management, backup, and administration.

   c. Install the Fujitsu Enterprise Postgres client, which is required on both the CPM and PSM servers.

   Refer to the **Fujitsu Enterprise Postgres Installation and Setup Guide for Client** for details.

3. Import **Central Policy Manager** plugin and **Privileged Session Manager** connector for Fujitsu Enterprise Postgres.

   Sign in to the CyberArk Marketplace, access the download the plugin and connector download pages (*here* and *here*, respectively), and import them from the **Platform Management** page in PVWA.

4. Configure the **Central Policy Manager** plugin and **Privileged Session Manager** connector

   a. Configure the **Central Policy Manager** plugin

   Verify that the product version listed in the ODBC connection string for the CPM connection is correct. This can be edited via **Fujitsu Enterprise Postgres** on the **Platform Management** page in PVWA. In the **Additional Policy Settings** section, check the Fujitsu Enterprise Postgres version specified in the **ConnectionCommand** parameter. Refer to the plugin documentation for details on available options.

   b. Configure the and **Privileged Session Manager** connector

   Verify that the psql installation path setting for the PSM connection is correct. This can be edited via **Options** on the **System Configuration** page in PVWA. Check the **ExeFullPath** parameter in the **Connection Components** section. Refer to the connector documentation for details on available options.

5. Register database administrator accounts in Privileged Access Manager.

   Select **Database** for the system type and **Fujitsu Enterprise Postgres** for the platform.

   If you are operating your database in a replication configuration, specify the primary server as the account's connection target. If the primary server changes due to failover or other reasons, you will need to update the account's connection target server.

   Refer to the **Privileged Access Manager documentation** section *Add an account* for more details on registering OS accounts for SSH or RDP access to the database server.

6. Connect to the database as a Database Administrator

   From the **Accounts View** page in PVWA, click **Connect** of the account created in the step above.

About CyberArk Privileged Access Manager

CyberArk Privileged Access Manager protects privileged accounts and credentials, providing centralized management of privileged access across your organization. This helps safeguard your business and valuable assets from both internal and external threats. The comprehensive protection offered by CyberArk Privileged Access Manager ensures security without hindering your operations.

For more information, visit the **CyberArk website**.

About Fujitsu Enterprise Postgres

Fujitsu Enterprise Postgres is the enhanced version of PostgreSQL, for enterprises seeking a more robust, secure, and fully supported edition for business-critical applications. It provides improvements to support enterprise-level workloads and improved Deployment and Management, Availability, Performance, Data Governance, and Security, above and beyond the community edition of PostgreSQL.

Visit the **Fujitsu Enterprise Postgres website**.

Notes

- When integrating with **Privileged Access Manager**, do not apply password policies using the *policy-based login security* feature of Fujitsu Enterprise Postgres to privileged accounts.
- When connecting to the database from the **Central Policy Manager/Privileged Session Manager** server, connect directly without using the Connection Manager function.
- The superuser used for Mirroring Controller's database connection settings cannot be managed through this integration.

Target versions

- CyberArk Privileged Access Manager: 12 (12.2 or later), 13, 14
- **Fujitsu Enterprise Postgres**: 15, 16 (Advanced Edition for x86)
  Please inquire if you plan to use the Advanced Edition with Cryptographic Module or a non-x86 architecture.

Support

Support for the product integration is provided by both Fujitsu and CyberArk. Therefore, it is necessary to have support contracts with both organizations

fast.fujitsu.com/
Email: enterprisepostgresql@fujitsu.com
2024-10-11 WW EN

FUJITSU