Preface

Purpose of this document
This document describes system configuration, design, installation, setup, and operational procedures of the Fujitsu Enterprise Postgres for Kubernetes.

Intended readers
This document is intended for people who are:
- Considering installing Fujitsu Enterprise Postgres for Kubernetes
- Using Fujitsu Enterprise Postgres for Kubernetes for the first time
- Wanting to learn about the concept of Fujitsu Enterprise Postgres for Kubernetes
- Wanting to see a functional overview of Fujitsu Enterprise Postgres for Kubernetes

Readers of this document are also assumed to have general knowledge of:
- Linux
- Kubernetes
- Containers
- Operators

Structure of this document
This document is structured as follows:

Chapter 1 System Requirements
Describes the system requirements.

Chapter 2 Overview of Operator Design
Describes an overview of the operator design.

Chapter 3 Operator Installation
Describes the installation of the FEP operator.

Chapter 4 Deployment Container
Describes container deployment.

Chapter 5 Post-Deployment Operations
Describes the operation after deploying the container.

Chapter 6 Maintenance Operations
Describes the maintenance operation after deploying the container.

Chapter 7 Abnormality
Describes the actions to take when an error occurs in the database or an application.

Appendix A Quantitative Values and Limitations
Describes the quantitative values and limitations.

Appendix B Adding Custom Annotations to FEPCluster Pods using Operator
Describes instructions for adding custom annotations to a FEPCluster pod.

Appendix C Utilize Shared Storage
Describes how to build a FEPCluster when using shared storage.
Appendix C Utilize Shared Storage

Describes how to build a FEPCluster when using shared storage.

Appendix D Key Management System Available for Transparent Data Encryption

Describes the key management system available for transparent data encryption.

Abbreviations

The following abbreviations are used in this manual:

<table>
<thead>
<tr>
<th>Full Name</th>
<th>Abbreviations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fujitsu Enterprise Postgres for Kubernetes</td>
<td>FEP</td>
</tr>
<tr>
<td>Fujitsu Enterprise Postgres</td>
<td></td>
</tr>
<tr>
<td>Vertical Clustered Index</td>
<td>VCI</td>
</tr>
<tr>
<td>Transparent Data Encryption</td>
<td>TDE</td>
</tr>
<tr>
<td>Point in time recovery</td>
<td>PITR</td>
</tr>
<tr>
<td>Custom Resource</td>
<td>CR</td>
</tr>
<tr>
<td>Custom Resource Definition</td>
<td>CRD</td>
</tr>
<tr>
<td>Persistent Volume</td>
<td>PV</td>
</tr>
<tr>
<td>Universal Base Image</td>
<td>UBI</td>
</tr>
<tr>
<td>OpenShift Container Platform</td>
<td>OCP</td>
</tr>
<tr>
<td>Mutual TLS</td>
<td>MTLS</td>
</tr>
</tbody>
</table>

Abbreviations of manual titles

The following abbreviations are used in this manual as manual titles:

<table>
<thead>
<tr>
<th>Full Manual Title</th>
<th>Abbreviations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fujitsu Enterprise Postgres for Kubernetes Release Notes</td>
<td>Release Notes</td>
</tr>
<tr>
<td>Fujitsu Enterprise Postgres for Kubernetes Overview</td>
<td>Overview</td>
</tr>
<tr>
<td>Fujitsu Enterprise Postgres for Kubernetes Reference</td>
<td>Reference</td>
</tr>
</tbody>
</table>

Trademarks

- Linux is a registered trademark or trademark of Mr. Linus Torvalds in the U.S. and other countries.
- Red Hat and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc. in the United States and other countries.
- S/390 is a registered trademark of International Business Machines Corporation in the United States or other countries or both.
Other product and company names mentioned in this manual are the trademarks or registered trademarks of their respective owners.

Export restrictions

If this document is to be exported or provided overseas, confirm legal requirements for the Foreign Exchange and Foreign Trade Act as well as other laws and regulations, including U.S. Export Administration Regulations, and follow the required procedures.
<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1 System Requirements</td>
<td></td>
</tr>
<tr>
<td>1.1 Components Embedded</td>
<td>1</td>
</tr>
<tr>
<td>1.2 CPU</td>
<td>1</td>
</tr>
<tr>
<td>1.3 Supported Platform</td>
<td>1</td>
</tr>
<tr>
<td>1.4 Collaboration Tool</td>
<td>2</td>
</tr>
<tr>
<td>Chapter 2 Overview of Operator Design</td>
<td></td>
</tr>
<tr>
<td>2.1 Design Task</td>
<td>3</td>
</tr>
<tr>
<td>2.2 System Configuration Design</td>
<td>3</td>
</tr>
<tr>
<td>2.2.1 Server Configuration</td>
<td>3</td>
</tr>
<tr>
<td>2.2.2 User Account</td>
<td>5</td>
</tr>
<tr>
<td>2.2.3 Basic Information of the Container</td>
<td>5</td>
</tr>
<tr>
<td>2.3 Design Perspective for Each Feature</td>
<td>10</td>
</tr>
<tr>
<td>2.3.1 Deployment</td>
<td>11</td>
</tr>
<tr>
<td>2.3.2 High Availability</td>
<td>11</td>
</tr>
<tr>
<td>2.3.3 Configurable Volume per Cluster</td>
<td>11</td>
</tr>
<tr>
<td>2.3.4 Deploying Ppool-II and Connect to FEPCluster from Operator</td>
<td>13</td>
</tr>
<tr>
<td>2.3.5 Scheduling Backup from Operator</td>
<td>13</td>
</tr>
<tr>
<td>2.3.5.1 Important Setting Items</td>
<td>14</td>
</tr>
<tr>
<td>2.3.5.2 Parameters that cannot be Set</td>
<td>14</td>
</tr>
<tr>
<td>2.3.5.3 Restricted Parameters</td>
<td>17</td>
</tr>
<tr>
<td>2.3.5.4 About Sections in the Config File</td>
<td>17</td>
</tr>
<tr>
<td>2.3.6 Perform PTR and Latest Backup Restore from Operator</td>
<td>17</td>
</tr>
<tr>
<td>2.3.7 FEP Unique Feature Enabled by Default</td>
<td>17</td>
</tr>
<tr>
<td>2.3.8 Monitoring &amp; Alert (FEPExporter)</td>
<td>18</td>
</tr>
<tr>
<td>2.3.8.1 FEPExporter Custom Resource</td>
<td>18</td>
</tr>
<tr>
<td>2.3.8.2 Change to FEPCluster CR - metrics user</td>
<td>18</td>
</tr>
<tr>
<td>2.3.8.3 FEPExporter CR auto-create for FEPCluster</td>
<td>18</td>
</tr>
<tr>
<td>2.3.9 Scaling Replicas</td>
<td>19</td>
</tr>
<tr>
<td>2.3.9.1 Change to FEPCluster CR - auto scale out</td>
<td>20</td>
</tr>
<tr>
<td>2.3.10 Disaster Recovery</td>
<td>20</td>
</tr>
<tr>
<td>2.3.11 Transparent Data Encryption Using a Key Management System</td>
<td>20</td>
</tr>
<tr>
<td>2.3.12 Database Role Management</td>
<td>21</td>
</tr>
<tr>
<td>2.3.12.1 Creating Roles Related to Database Operation</td>
<td>21</td>
</tr>
<tr>
<td>2.3.12.1.1 Quarantine SUPERUSER</td>
<td>21</td>
</tr>
<tr>
<td>2.3.12.1.2 Database Administrator Role</td>
<td>21</td>
</tr>
<tr>
<td>2.3.12.1.3 Confidential Administrator Role</td>
<td>22</td>
</tr>
<tr>
<td>2.3.12.2 Expiration Management of Database Roles with Login Privileges</td>
<td>22</td>
</tr>
<tr>
<td>Chapter 3 Operator Installation</td>
<td>24</td>
</tr>
<tr>
<td>3.1 Using the OperatorHub</td>
<td>24</td>
</tr>
<tr>
<td>3.1.1 Pre-requisite</td>
<td>24</td>
</tr>
<tr>
<td>3.1.2 Deploying Operator</td>
<td>25</td>
</tr>
<tr>
<td>3.2 Using the Helm Chart</td>
<td>27</td>
</tr>
<tr>
<td>3.2.1 Deploying Operator</td>
<td>27</td>
</tr>
<tr>
<td>3.2.2 Upgrading Operators</td>
<td>27</td>
</tr>
<tr>
<td>3.3 Using the Rancher UI</td>
<td>27</td>
</tr>
<tr>
<td>3.3.1 Pre-requisite</td>
<td>28</td>
</tr>
<tr>
<td>3.3.2 Register Helm Chart Repository</td>
<td>29</td>
</tr>
<tr>
<td>3.3.3 Deploying Operator</td>
<td>31</td>
</tr>
<tr>
<td>3.4 Implement Collaborative Monitoring Tools</td>
<td>32</td>
</tr>
<tr>
<td>3.4.1 Implement GAP Stack</td>
<td>32</td>
</tr>
<tr>
<td>3.4.2 Implement Elastic Cloud on Kubernetes</td>
<td>33</td>
</tr>
<tr>
<td>3.4.2.1 Deploy ECK Operator</td>
<td>33</td>
</tr>
<tr>
<td>3.4.2.2 Deploy Elasticsearch Cluster</td>
<td>35</td>
</tr>
<tr>
<td>3.4.2.3 Deploy Enterprise Search</td>
<td>36</td>
</tr>
</tbody>
</table>

- iv -
Chapter 4 Deployment Container...........................................................................................................................................41

4.1 Deploying FEPClusters using Operator.................................................................41
4.2 Deploying a Highly Available FEPCluster...........................................................45
4.3 Deploying FEPExporter.......................................................................................46
4.4 FEPExporter in Standalone Mode........................................................................48
4.5 Deploying FEPClusters with Cloud Secret Management.................................51
   4.5.1 Installing Secret Store CSI Driver Using Helm Charts...............................51
   4.5.2 Installing and Configuring Azure Provider for Secret Store CSI Driver........52
      4.5.2.1 Install Azure Provider drivers using helm chart.................................52
      4.5.2.2 Create Secret to Access Azure Key vault...........................................52
      4.5.2.3 Store Secret in Azure Key Vault.........................................................52
      4.5.2.4 Store Certificate in Azure Key Vault................................................52
   4.5.3 Installing and Configuring AWS Provider for Secret Store CSI Driver........54
      4.5.3.1 Install AWS Provider drivers using helm chart.................................54
      4.5.3.2 Setup EKS cluster along with service account with necessary IAM roles and permission to access Secret Manager......54
      4.5.3.3 Store Secret in AWS Secrets Manager.............................................55
      4.5.3.4 Store Cert in AWS Secrets Manager...............................................55
   4.5.4 Installing GCP Provider for Secret Store CSI Driver....................................55
      4.5.4.1 Install GCP Provider drivers using helm chart.................................55
      4.5.4.2 Configure GCP secret manager and IAM.........................................55
      4.5.4.3 Create Secret to access GCP Secret manager...................................56
      4.5.4.4 Store secret in GCP Secret manager...............................................56
      4.5.4.5 Store Cert in GCP Secret manager..................................................56
   4.5.5 Installing HashiCorp Vault Provider for Secret Store CSI Driver................56
      4.5.5.1 Install HashiCorp Provider drivers using helm chart.........................56
      4.5.5.2 Configure Kubernetes Authentication for HashiCorp Vault...............56
      4.5.5.3 Store Secret in HashiCorp Vault......................................................56
      4.5.5.4 Store Cert in HashiCorp Vault.........................................................56
      4.5.5.5 Create policy and role to access the secrets from HashiCorp Vault.......57
   4.5.6 Configuring FEPClusters to use Provider for Secret Store Driver...............57
      4.5.6.1 Azure Provider for Secret Store CSI Driver.......................................57
      4.5.6.2 AWS Provider for Secret Store CSI Driver.......................................58
      4.5.6.3 GCP Provider for Secret Store CSI Driver........................................59
      4.5.6.4 HashiCorp Vault Provider for Secret Store CSI Driver.....................60
   4.6 Deploying a customized FEP server container image....................................60
      4.6.1 Requirements..........................................................................................60
      4.6.2 Build custom FEP image with extension..............................................60
      4.6.3 Adding SQLite Foreign Data Wrapper to FEP Server Container..............61
      4.6.4 Create FEP Cluster with custom image..............................................62
   4.7 Configuration FEP to Perform MTLS..............................................................62
      4.7.1 Manual Certificate Management.........................................................63
      4.7.2 Automatic Certificate Management....................................................67
      4.7.3 Deploy FEPClusters with MTLS support............................................71
      4.7.4 Configurable Parameters.....................................................................78
   4.8 Replication Slots...............................................................................................80
      4.8.1 Setting Up Logical Replication using MTLS.......................................80
   4.9 FEP Logging....................................................................................................83
      4.9.1 FEPLogging Configuration..................................................................84
         4.9.1.1 FEPLogging Custom Resources - spec.........................................84
            4.9.1.1.1 Define fepLogging image.........................................................86
            4.9.1.1.2 Define fepLogging mcSpec......................................................86
            4.9.1.1.3 Define fepLogging restartRequired.......................................86
Chapter 5 Post-Deployment Operations...............................................................................................................................102
5.1 How to Connect to a FEP Cluster .................................................................................................................................102
5.2 Configuration Change......................................................................................................................................................103
5.3 FEPCluster Resource Change.......................................................................................................................................104
5.3.1 Changing CPU and Memory Allocation Resources..................................................................................................104
5.3.2 Resizing PVCs...............................................................................................................................................................104
5.4 FEPPGPool2 Configuration Change................................................................................................................................104
5.5 Scheduling Backup from Operator................................................................................................................................106
5.6 Configure MTLS Setting.....................................................................................................................................................107
5.6.1 Certification Rotation.....................................................................................................................................................107
5.7 Monitoring........................................................................................................................................................................107
5.7.1 Monitoring FEP Operator and Operands......................................................................................................................108
5.7.2 Monitoring FEP Server..................................................................................................................................................108
5.7.2.1 Architecture.................................................................................................................................................................109
5.7.2.2 Default Server Metrics Monitoring .............................................................................................................................109
5.7.2.3 Default Alerts...............................................................................................................................................................111
5.7.2.4 Graphical user interface...............................................................................................................................................112
5.7.3 Monitoring FEP Backup................................................................................................................................................112
5.7.3.1 pgbackrest_info_backup view..................................................................................................................................113
5.7.4 Monitoring FEP PGPool2...............................................................................................................................................113
5.7.4.1 pgpool2_stat_load_balance view.................................................................................................................................113
5.7.4.2 pgpool2_stat_conn_pool view..................................................................................................................................114
5.7.4.3 pgpool2_stat_sql_command view.................................................................................................................................114
5.8 Event Notification
5.8.1 Events raised
5.8.2 Events that Occur when Custom Resources are Updated
5.8.3 Viewing the Custom Events
5.9 Scaling Replicas
5.9.1 Automatic Scale Out
5.9.2 Manual Scale In/Out
5.10 Backing Up to Object Storage
5.10.1 Pre-creation of Resources
5.10.1.1 Storing CA Files (Root Certificates)
5.10.1.2 Storing Repository Key
5.10.2 Defining a FEPCluster Custom Resource
5.11 Disaster Recovery
5.11.1 Disaster Recovery Prerequisites
5.11.2 Performing Disaster Recovery
5.11.2.1 Pre-creation of Resources
5.11.2.1.1 Storing CA Files (Root Certificates)
5.11.2.1.2 Storing Repository Key
5.11.2.2 Defining a FEPCluster Custom Resource
5.12 Operation of Transparent Data Encryption Using Key Management System
5.12.1 Updating Custom Resource Parameters
5.12.2 Update Credentials
5.12.3 Encrypting a Tablespace
5.12.4 Backup/Restore
5.12.5 Changing Key Management System Definitions
5.13 Confidential Management Support Feature
5.13.1 Enabling Confidential Management Support Feature
5.13.2 Monitoring Confidential Management Support Feature

Chapter 6 Maintenance Operations
6.1 Minor Version Upgrade
6.2 Cluster Master Switchover
6.3 Perform PITR and the Latest Backup Restore from Operator
6.3.1 Setting Item
6.3.2 After Restore
6.4 Major Version Upgrade
6.4.1 Pre-work on the Data Source FEP Cluster
6.4.2 Operator Upgrade
6.4.2.1 Uninstalling the Old Operator
6.4.2.2 Installing a New Version of the Operator
6.4.3 Major Version Upgrade of FEP
6.4.3.1 Creating a New FEPCluster CR
6.4.3.2 Verifying FEP Major Upgrade Complete
6.4.4 Updating Each Custom Resource
6.4.4.1 Removing a FEPClusterCR for a Data Source
6.4.4.2 FEPpools
6.4.4.3 FEPExporter Built in Standalone Mode
6.5 Assigned Resources for Operator Containers
6.5.1 How to Change Assigned Resources
6.5.1.1 When installing using OperatorHub
6.5.1.2 When installing using Helm Chart or RancherUI
6.6 Using SUPERUSER Privilege
6.6.1 CREATE EXTENSION
6.6.2 Change Password of SUPERUSER
6.6.3 Using SUPERUSER

Chapter 7 Abnormality
7.1 Handling of Data Abnormalities
7.2 Handling when the Capacity of the Data Storage Destination or Transaction Log Storage Destination is Insufficient................. 134
7.3 What to do when the Capacity of the Backup Data Storage Area is Insufficient................................................................. 134
7.4 Handling Access Abnormalities When Instance Shutdown Fails............................................................................................... 134
7.5 Collection of Failure Investigation Information......................................................................................................................... 134

Appendix A Quantitative Values and Limitations................................................................................................................................. 136
A.1 Quantitative Values......................................................................................................................................................................... 136
A.2 Limitations...................................................................................................................................................................................... 136

Appendix B Adding Custom Annotations to FEPCluster Pods using Operator.................................................................................... 137

Appendix C Utilize Shared Storage......................................................................................................................................................... 139
C.1 Creating a StorageClass................................................................................................................................................................. 139
C.2 Creating a PersistentVolume...................................................................................................................................................... 139
C.3 Creating FEPCluster........................................................................................................................................................................ 140

Appendix D Key Management System Available for Transparent Data Encryption................................................................. 141
D.1 KMIP Server................................................................................................................................................................................... 141
D.2 AWS Key Management Service.................................................................................................................................................. 141
  D.2.1 Available Services................................................................................................................................................................... 141
  D.2.2 Available AWS KMS Keys............................................................................................................................................... 141
  D.2.3 Required Privileges............................................................................................................................................................... 141
  D.2.4 Key ID...................................................................................................................................................................................... 141
D.3 Azure Key Management Service.................................................................................................................................................... 141
  D.3.1 Available Services................................................................................................................................................................... 141
  D.3.2 Available Keys......................................................................................................................................................................... 142
  D.3.3 Available Algorithms...................................................................................................................................................... 142
  D.3.4 Key Operation.......................................................................................................................................................................... 142
  D.3.5 Key ID...................................................................................................................................................................................... 142
  D.3.6 Sign In...................................................................................................................................................................................... 142
Chapter 1 System Requirements

This chapter describes the system requirements.

1.1 Components Embedded

The FEP Server container embeds following components. However it is understood that these components are bound to be upgraded in the maintenance phase.

<table>
<thead>
<tr>
<th>No</th>
<th>Component</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Red Hat UBI minimal</td>
<td>8</td>
<td>Meant to provide base OS image for the container</td>
</tr>
<tr>
<td>2</td>
<td>Fujitsu Enterprise Postgres Server</td>
<td>15.0</td>
<td>To provide server capabilities</td>
</tr>
<tr>
<td>3</td>
<td>Patroni</td>
<td>2.1.7</td>
<td>To provide HA capabilities and other management to the Cluster</td>
</tr>
</tbody>
</table>

1.2 CPU

It should be noted that it provides supports to both the following CPU Architectures to meet the scope of work.

<table>
<thead>
<tr>
<th>No</th>
<th>CPU architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>x86</td>
</tr>
<tr>
<td>2</td>
<td>s390x</td>
</tr>
<tr>
<td>3</td>
<td>ppc64le</td>
</tr>
</tbody>
</table>

1.3 Supported Platform

It supports running on the following platforms.

<table>
<thead>
<tr>
<th>No</th>
<th>Platform</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>OpenShift Container Platform</td>
<td>4.8, 4.9, 4.10, 4.11</td>
</tr>
<tr>
<td>2</td>
<td>OpenShift Container Storage</td>
<td>4.8</td>
</tr>
<tr>
<td>3</td>
<td>Kubernetes</td>
<td>1.24, 1.25, 1.26</td>
</tr>
</tbody>
</table>

Support environments are as follows:
- Azure Kubernetes Service
- Amazon Elastic Kubernetes Service
- Rancher Kubernetes Engine (on Linux hosts)
- Alibaba Cloud Container Service for Kubernetes
- Google Kubernetes Engine
- IBM Cloud Kubernetes Service
- Tanzu Kubernetes Grid

Supports storage supported by OpenShift or Kubernetes (AKS, EKS, RKE, ACK, GKE, IKS and TKG).

However, you need shared storage, like NFS, or object storage for backup and archive WAL volumes. Object storage supports Amazon Simple Storage Service, Azure Blob Storage, and Google Cloud Storage.
## 1.4 Collaboration Tool

Supports integration with the following tools.

<table>
<thead>
<tr>
<th>No</th>
<th>Tool</th>
<th>Version</th>
<th>How to obtain</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Prometheus</td>
<td>- OpenShift&lt;sup&gt;1&lt;/sup&gt; The version installed OpenShift</td>
<td>- OpenShift Preinstalled with OpenShift</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Kubernetes v0.61.1 and later</td>
<td>- Kubernetes prometheus-operator <a href="https://github.com/prometheus-operator/prometheus-operator">https://github.com/prometheus-operator/prometheus-operator</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Rancher The version provided by Rancher Monitoring Chart</td>
<td>- Rancher Using the Rancher Monitoring Chart</td>
</tr>
<tr>
<td>2</td>
<td>AlertManager</td>
<td>- OpenShift&lt;sup&gt;1&lt;/sup&gt; The version installed OpenShift</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Kubernetes v0.61.1 and later</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Rancher The version provided by Rancher Monitoring Chart</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Grafana</td>
<td>- OpenShift and Kubernetes 4.7.1 and later</td>
<td>- OpenShift Provided by OperatorHub</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Rancher The version provided by Rancher Monitoring Chart</td>
<td>- Kubernetes grafana-operator <a href="https://github.com/grafana-operator/grafana-operator">https://github.com/grafana-operator/grafana-operator</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Rancher Using the Rancher Monitoring Chart</td>
</tr>
<tr>
<td>4</td>
<td>Helm</td>
<td>3.10.0 and later</td>
<td>- Kubernetes only Helm Web Site <a href="https://helm.sh/docs/intro/install/">https://helm.sh/docs/intro/install/</a></td>
</tr>
<tr>
<td>5</td>
<td>Rancher</td>
<td>v2.7 and later</td>
<td>Rancher Web Site <a href="https://rancher.com/">https://rancher.com/</a></td>
</tr>
<tr>
<td>6</td>
<td>Prometheus Adapter</td>
<td>- OpenShift and Kubernetes Confirmed the operation with v0.10.0.</td>
<td>- OpenShift and Kubernetes Prometheus Adapter <a href="https://github.com/kubernetes-sigs/prometheus-adapter">https://github.com/kubernetes-sigs/prometheus-adapter</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Rancher The version provided by Rancher Monitoring Chart</td>
<td>- Rancher Using the Rancher Monitoring Chart</td>
</tr>
<tr>
<td>7</td>
<td>Elastic Search</td>
<td>8.5.2 and later</td>
<td>- OpenShift Provided by OperatorHub</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Kubernetes <a href="https://github.com/elastic/helm-charts/tree/main/elasticsearch">https://github.com/elastic/helm-charts/tree/main/elasticsearch</a></td>
</tr>
</tbody>
</table>

<sup>1</sup> Prometheus, AlertManager, and Rancher can also be installed using Helm.
Chapter 2 Overview of Operator Design

This chapter describes an overview of the operator design.

2.1 Design Task

Installation/operation using an operator and necessity of design are shown below.

<table>
<thead>
<tr>
<th>Task</th>
<th>Design required to operate FEP</th>
<th>Where to find</th>
</tr>
</thead>
<tbody>
<tr>
<td>FEP setup</td>
<td>Required.</td>
<td>2.3.1 Deployment</td>
</tr>
<tr>
<td>High availability configuration</td>
<td>Recommended. (When checking or changing the behavior of high availability, however, even by default, constant high availability operation is possible.)</td>
<td>2.3.2 High Availability</td>
</tr>
<tr>
<td>Volume settings</td>
<td>Recommended. (When setting the volume. However, even by default, allocate a fixed volume.)</td>
<td>2.3.3 Configurable Volume per Cluster</td>
</tr>
<tr>
<td>Pgpool-II setup</td>
<td>Recommended. (When using Pgpool-II.)</td>
<td>2.3.4 Deploying Pgpool-II and Connect to FEP Cluster from Operator</td>
</tr>
<tr>
<td>Backup/restore settings</td>
<td>Recommended. (When using a backup and restore.)</td>
<td>2.3.5 Scheduling Backup from Operator</td>
</tr>
<tr>
<td>Monitoring &amp; Alert(FEPExporter)</td>
<td>Recommended. (When using Monitoring and Alert)</td>
<td>2.3.6 Perform PITR and Latest Backup Restore from Operator</td>
</tr>
<tr>
<td>Scaling Replicas</td>
<td>Recommended. (When using scaling feature)</td>
<td>2.3.7 Scaling Replicas</td>
</tr>
<tr>
<td>Key management system</td>
<td>Recommended. (When the key management system manages the master encryption key for transparent data encryption)</td>
<td>2.3.11 Transparent Data Encryption Using a Key Management System</td>
</tr>
</tbody>
</table>

2.2 System Configuration Design

This section describes the system configuration.

2.2.1 Server Configuration

The following is an overview diagram of the server configuration:
System component
Describes various system resources.

<table>
<thead>
<tr>
<th>Configuration server type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FEP operator</td>
<td>A container that accepts user requests and is responsible for automating database construction and operational operations.</td>
</tr>
<tr>
<td>FEP server container</td>
<td>A container for the FEP server.</td>
</tr>
<tr>
<td>FEP backup container</td>
<td>A container that performs scheduled backup operations. Created on the same Pod as the FEP server container.</td>
</tr>
<tr>
<td>FEP Fluentbit container</td>
<td>A container that collect FEP database CSV log and forward to fluentd container for processing.</td>
</tr>
<tr>
<td>FEP pgpool2 container</td>
<td>A container that uses Pgpool-II to provide load balancing and connection pooling. If you do not use it, you do not need to create it.</td>
</tr>
<tr>
<td>FEP restore container</td>
<td>A container that performs the restore operation. Temporarily created during a restore operation.</td>
</tr>
<tr>
<td>FEP Exporter container</td>
<td>A container that exposes http/https endpoint for monitoring stats scraping.</td>
</tr>
<tr>
<td>FEP Fluentd container</td>
<td>A container that summarise FEP log severity as metrics for Prometheus to consume. Optionally, forward log entries to Elasticsearch for detailed log analysis.</td>
</tr>
<tr>
<td>FEP upgrade container</td>
<td>A container that executes the major version upgrade process of the server container. A container created temporarily during the upgrade process.</td>
</tr>
<tr>
<td>FEP Cronjob container</td>
<td>A container that is started when the regular processing of each feature of the operator is executed.</td>
</tr>
<tr>
<td>FEP Utilis container</td>
<td>A container for cloud secret management.</td>
</tr>
<tr>
<td>Backup storage</td>
<td>Storage where backup data is stored. If you do not need to obtain a backup, you do not need to create one.</td>
</tr>
</tbody>
</table>
### Configuration server type

<table>
<thead>
<tr>
<th>Configuration server type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FEPCluster</td>
<td>Parent CR for FEP Cluster definition and configuration.</td>
</tr>
<tr>
<td>FEPBackup</td>
<td>Child CR for backup configuration.</td>
</tr>
<tr>
<td>FEPVolume</td>
<td>Child CR for volumes.</td>
</tr>
<tr>
<td>FEPConfig</td>
<td>Child CR for FEP configurations.</td>
</tr>
<tr>
<td>FEPCert</td>
<td>Child CR for system certificates.</td>
</tr>
<tr>
<td>FEPUser</td>
<td>Child CR for database users.</td>
</tr>
<tr>
<td>FEPAction</td>
<td>CR for performing actions.</td>
</tr>
<tr>
<td>FEPExporter</td>
<td>CR for monitoring configuration.</td>
</tr>
<tr>
<td>FEPUpgrade</td>
<td>CR for major upgrade.</td>
</tr>
<tr>
<td>Master service</td>
<td>A service to connect to the master FEP server.</td>
</tr>
<tr>
<td>Replica service</td>
<td>A service to connect to the replica FEP server.</td>
</tr>
<tr>
<td>Pgpool2 service</td>
<td>A service for connecting to Pgpool-II.</td>
</tr>
<tr>
<td>Fepexporter service</td>
<td>A service to scrape metrics from all FEPCluster nodes.</td>
</tr>
</tbody>
</table>

### 2.2.2 User Account

The user accounts used by this product are as follows.

<table>
<thead>
<tr>
<th>User type</th>
<th>User name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure administrator</td>
<td>Mandatory</td>
<td>A system administrator (superuser) who has root privileges on all the servers that make up this product.</td>
</tr>
<tr>
<td>Database administrator</td>
<td>Mandatory</td>
<td>Install, set up, start, stop, and perform operation and maintenance of this product.</td>
</tr>
<tr>
<td>Confidential administrator</td>
<td>Mandatory</td>
<td>An administrator who sets appropriate privileges for each database resource for database users.</td>
</tr>
<tr>
<td>Application developer</td>
<td>Mandatory</td>
<td>Develops and executes database applications.</td>
</tr>
</tbody>
</table>

### 2.2.3 Basic Information of the Container

This section describes the basic information of the container.

**FEP server container**

The naming convention for the FEP server container is as below.


For each *Version*, specify the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>OS</em></td>
<td>ubi8</td>
<td></td>
</tr>
<tr>
<td><em>FEPBaseVersion</em></td>
<td>15</td>
<td></td>
</tr>
<tr>
<td><em>MajorVersion</em></td>
<td>1,2, ...</td>
<td>To be used when major change in image, including server patch application</td>
</tr>
<tr>
<td><em>MinorVersion</em></td>
<td>0,1,2 ...</td>
<td>To be used when minor changes in image, e.g. bug fix in container script</td>
</tr>
</tbody>
</table>
The first publishing will expect following names / tagging (Manifest and Child images).

- fujitsu-enterprise-postgres-15-server:ubi8-15-1.0

- fujitsu-enterprise-postgres-15-server:ubi8-15-1.0-amd64

- fujitsu-enterprise-postgres-15-server:ubi8-15-1.0-s390x

- fujitsu-enterprise-postgres-15-server:ubi8-15-1.0-ppc64le

FEP backup container

Use the same naming convention for FEP backup containers as for FEP server containers.


For each Version, specify the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</td>
<td>ubi8</td>
<td></td>
</tr>
<tr>
<td>FEPBaseVersion</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>MajorVersion</td>
<td>1,2, ...</td>
<td>To be used when major change in image, including server patch application</td>
</tr>
<tr>
<td>MinorVersion</td>
<td>0,1,2 ...</td>
<td>To be used when minor changes in image, e.g. bug fix in container script</td>
</tr>
</tbody>
</table>

The first publishing will expect following names / tagging (Manifest and Child images)

- fujitsu-enterprise-postgres-15-backup:ubi8-15-1.0

- fujitsu-enterprise-postgres-15-backup:ubi8-15-1.0-amd64

- fujitsu-enterprise-postgres-15-backup:ubi8-15-1.0-s390x

- fujitsu-enterprise-postgres-15-backup:ubi8-15-1.0-ppc64le

FEP restore container

Use the same naming convention for FEP restore containers as for FEP server containers.


For each Version, specify the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</td>
<td>ubi8</td>
<td></td>
</tr>
<tr>
<td>FEPBaseVersion</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>MajorVersion</td>
<td>1,2, ...</td>
<td>To be used when major change in image, including server patch application</td>
</tr>
<tr>
<td>MinorVersion</td>
<td>0,1,2 ...</td>
<td>To be used when minor changes in image, e.g. bug fix in container script</td>
</tr>
</tbody>
</table>

The first publishing will expect following names / tagging (Manifest and Child images)

- fujitsu-enterprise-postgres-15-restore:ubi8-15-1.0

- fujitsu-enterprise-postgres-15-restore:ubi8-15-1.0-amd64
- fujitsu-enterprise-postgres-15-restore:ubi8-15-1.0-s390x
- fujitsu-enterprise-postgres-15-restore:ubi8-15-1.0-ppc64le

**FEP pgpool2 container**

Use the same naming convention for FEP pgpool2 containers as for FEP server containers.

**FEP pgpool2**: OS-FEPBaseVersion-MajorVersion.MinorVersion-ARCH

For each **Version**, specify the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</td>
<td>ubi8</td>
<td></td>
</tr>
<tr>
<td>FEPBaseVersion</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>MajorVersion</td>
<td>1,2, ...</td>
<td>To be used when major change in image, including server patch application</td>
</tr>
<tr>
<td>MinorVersion</td>
<td>0,1,2 ...</td>
<td>To be used when minor changes in image, e.g. bug fix in container script</td>
</tr>
</tbody>
</table>

The first publishing will expect following names / tagging (Manifest and Child images)

- fujitsu-enterprise-postgres-15-pgpool2:ubi8-15-1.0
  - fujitsu-enterprise-postgres-15-pgpool2:ubi8-15-1.0-amd64
  - fujitsu-enterprise-postgres-15-pgpool2:ubi8-15-1.0-s390x
  - fujitsu-enterprise-postgres-15-pgpool2:ubi8-15-1.0-ppc64le

**FEP Exporter container**

FEP Exporter container as for FEP server containers.

**FEP Exporter**: OS-FEPBaseVersion-MajorVersion.MinorVersion-ARCH

For each **Version**, specify the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</td>
<td>ubi8</td>
<td></td>
</tr>
<tr>
<td>FEPBaseVersion</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>MajorVersion</td>
<td>1,2, ...</td>
<td>To be used when major change in image, including server patch application</td>
</tr>
<tr>
<td>MinorVersion</td>
<td>0,1,2 ...</td>
<td>To be used when minor changes in image, e.g. bug fix in container script</td>
</tr>
</tbody>
</table>

The first publishing will expect following names / tagging (Manifest and Child images)

- fujitsu-enterprise-postgres-exporter:ubi8-15-1.0
  - fujitsu-enterprise-postgres-exporter:ubi8-15-1.0-amd64
  - fujitsu-enterprise-postgres-exporter:ubi8-15-1.0-s390x
  - fujitsu-enterprise-postgres-exporter:ubi8-15-1.0-ppc64le
FEP Fluentd container

FEP Fluentd container as for FEP server containers.


For each Version, specify the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</td>
<td>ubi8</td>
<td></td>
</tr>
<tr>
<td>FEPBaseVersion</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>MajorVersion</td>
<td>1,2, ...</td>
<td>To be used when major change in image, including server patch application</td>
</tr>
<tr>
<td>MinorVersion</td>
<td>0,1,2 ...</td>
<td>To be used when minor changes in image, e.g bug fix in container script</td>
</tr>
</tbody>
</table>

The first publishing will expect following names / tagging (Manifest and Child images)
- fujitsu-enterprise-postgres-fluentd:ubi8-15-1.0
  - fujitsu-enterprise-postgres-fluentd:ubi8-15-1.0-amd64
  - fujitsu-enterprise-postgres-fluentd:ubi8-15-1.0-s390x
  - fujitsu-enterprise-postgres-fluentd:ubi8-15-1.0-ppc64le

FEP Fluentbit container

FEP Fluentbit container as for FEP server containers.


For each Version, specify the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</td>
<td>ubi8</td>
<td></td>
</tr>
<tr>
<td>FEPBaseVersion</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>MajorVersion</td>
<td>1,2, ...</td>
<td>To be used when major change in image, including server patch application</td>
</tr>
<tr>
<td>MinorVersion</td>
<td>0,1,2 ...</td>
<td>To be used when minor changes in image, e.g bug fix in container script</td>
</tr>
</tbody>
</table>

The first publishing will expect following names / tagging (Manifest and Child images)
- fujitsu-enterprise-postgres-fluentbit:ubi8-15-1.0
  - fujitsu-enterprise-postgres-fluentbit:ubi8-15-1.0-amd64
  - fujitsu-enterprise-postgres-fluentbit:ubi8-15-1.0-s390x
  - fujitsu-enterprise-postgres-fluentbit:ubi8-15-1.0-ppc64le

FEP Cronjob container

FEP Cronjob container as for FEP server containers.

For each Version, specify the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</td>
<td>ubi8</td>
<td></td>
</tr>
<tr>
<td>FEPBaseVersion</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>MajorVersion</td>
<td>1,2, ...</td>
<td>To be used when major change in image, including server patch application</td>
</tr>
<tr>
<td>MinorVersion</td>
<td>0,1,2 ...</td>
<td>To be used when minor changes in image, e.g bug fix in container script</td>
</tr>
</tbody>
</table>

The first publishing will expect following names / tagging (Manifest and Child images)

- fujitsu-enterprise-postgres-cronjob:ubi8-15-1.0
  - fujitsu-enterprise-postgres-cronjob:ubi8-15-1.0-amd64
  - fujitsu-enterprise-postgres-cronjob:ubi8-15-1.0-s390x
  - fujitsu-enterprise-postgres-cronjob:ubi8-15-1.0-ppc64le

FEP upgrade container

FEP upgrade container as for FEP server containers.


For each Version, specify the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</td>
<td>ubi8</td>
<td></td>
</tr>
<tr>
<td>FEPBaseVersion</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>MajorVersion</td>
<td>1,2, ...</td>
<td>To be used when major change in image, including server patch application</td>
</tr>
<tr>
<td>MinorVersion</td>
<td>0,1,2 ...</td>
<td>To be used when minor changes in image, e.g bug fix in container script</td>
</tr>
</tbody>
</table>

The first publishing will expect following names / tagging (Manifest and Child images)

- fujitsu-enterprise-postgres-15-upgrade:ubi8-15-1.0
  - fujitsu-enterprise-postgres-15-upgrade:ubi8-15-1.0-amd64
  - fujitsu-enterprise-postgres-15-upgrade:ubi8-15-1.0-s390x
  - fujitsu-enterprise-postgres-15-upgrade:ubi8-15-1.0-ppc64le

FEP Utils container

FEP Utils container as for FEP server containers.


For each Version, specify the following:
<table>
<thead>
<tr>
<th>Field</th>
<th>Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FEBBaseVersion</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>MajorVersion</td>
<td>1, 2, ...</td>
<td>To be used when major change in image, including server patch application</td>
</tr>
<tr>
<td>MinorVersion</td>
<td>0.1, 2, ...</td>
<td>To be used when minor changes in image, e.g. bug fix in container script</td>
</tr>
</tbody>
</table>

The first publishing will expect following names / tagging (Manifest and Child images)

- fujitsu-enterprise-postgres-15-utils:ubi8-15-1.0
  - fujitsu-enterprise-postgres-15-utils:ubi8-15-1.0-amd64
  - fujitsu-enterprise-postgres-15-utils:ubi8-15-1.0-s390x
  - fujitsu-enterprise-postgres-15-utils:ubi8-15-1.0-ppc64le

### 2.3 Design Perspective for Each Feature

This section describes the design of each feature.

**postgresql-cfg format**

A postgresql-cfg represent ConfigMap for containing postgresql parameters. The file is used to contain the parameters which need to be reflected in postgresql.conf of the instance. Since patroni ignores all parameters which are not known by OSS postgresql.conf, an approach is defined to treat FEP Parameters in a special way.

The content of the ConfigMap is defined by key=value format. The following table shows the detail:

<table>
<thead>
<tr>
<th>Spec</th>
<th>Example</th>
<th>Comment</th>
</tr>
</thead>
</table>
| The content may have multiple key/value pairs | foo=bar  
foo1=bar1             | -                                            |
| The value cannot have space unless quoted. | foo=bar bar2  | Invalid                                       |
| The quoted value cannot have another value after | foo='bar bar2' something | Invalid                                      |
| The key value pair must have a `=` sign | -                                   | -                                             |
| White spaces are allowed before/after/between the key value pair | foo = bar | -                                             |
| Any content after `#` will be ignored | # this is a comment  
foo=bar #this is a comment    | -                                             |
| The value may be quoted by single quotes | foo='bar bar2' | -                                             |
| Single quote can be escaped by two single quotes | foo='It''s ok' | Note: single quotes are not supported by Patroni edit-config command |
| Backslash `\` will be replaced by `\\` when invoking patronictl edit-config command | - | To avoid command line escape |
When a key value pair is invalid, it will be ignored. The update continues to process the next pair.

<table>
<thead>
<tr>
<th>Spec</th>
<th>Example</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

The container script does not validate the key and value as long as they are in the correct format.

<table>
<thead>
<tr>
<th>Spec</th>
<th>Example</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

It is recommended to use the `psql`'s `show` command to verify parameters are set correctly.

### 2.3.1 Deployment

**Information for the FEPCluster**

Equivalent Kubernetes command: `kubectl apply -f FEPClusterCR.yaml`

This operation will create a FEPCluster with supplied information in `FEPClusterCR.yaml`

Refer to "FEPCluster parameter" in the Reference for details.

#### Arbitration

Patroni is used to control and monitor FEP instance startup, shutdown, status and trigger failover if the master instance fails. It plays a significant role in the solution. If the Patroni process dies, especially on the master POD, without notice, the Pod will not update the Patroni cluster lock. This may trigger an unwanted failover to one of the replica, without corresponding corrective action on the running master.

This can create a split brain issue. It is important to monitor Patroni's status to make sure it is running. This is done using liveliness probe. Important to note that this is not expected to be configured by end user.

```yaml
livenessProbe:
  httpGet:
    scheme: HTTP
    path: /liveness
    port: 25001
  initialDelaySeconds: 30
  periodSeconds: 6
  timeoutSeconds: 5
  successThreshold: 1
  failureThreshold: 3
```

### 2.3.3 Configurable Volume per Cluster

Cluster node (Pod) volumes are created according to the values set in the storage section of `fepChildCrVal` in the FEPCluster custom resource.

**Note**

- After you create the FEPCluster for the first time, you cannot add new volumes later or modify the storageClass or accessModes.
- You can resize the initially created volume only if the underlying storageClass supports dynamic resizing.

The following is the schema for the storage section of the FEPCluster custom resource:

<table>
<thead>
<tr>
<th>Field</th>
<th>Mandatory</th>
<th>Sub-Field</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>archivewalVol</td>
<td>No</td>
<td>size</td>
<td>1Gi</td>
<td>Volume size of the archive log.</td>
</tr>
<tr>
<td>Field</td>
<td>Mandatory</td>
<td>Sub-Field</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------</td>
<td>-----------</td>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>storageClass</td>
<td>Defaults to platform default if omitted</td>
</tr>
<tr>
<td>accessModes</td>
<td></td>
<td></td>
<td>Defaults to ReadWriteOnce if omitted</td>
<td>Access mode is only set at start</td>
</tr>
<tr>
<td>backupVol</td>
<td>No</td>
<td>size</td>
<td>2Gi</td>
<td>Volume size of the backup. Estimate based on the following formula: (full backup generations + incr backup generations + 1) * dataVol size</td>
</tr>
<tr>
<td>storageClass</td>
<td></td>
<td></td>
<td>Defaults to platform default if omitted</td>
<td>SC is only set at start</td>
</tr>
<tr>
<td>accessModes</td>
<td></td>
<td></td>
<td>Defaults to ReadWriteOnce if omitted</td>
<td>Access mode is only set at start</td>
</tr>
<tr>
<td>dataVol</td>
<td>Yes</td>
<td>size</td>
<td>2Gi</td>
<td>Volume size of the data. Refer to &quot;Estimating Database Disk Space Requirements&quot; in the Fujitsu Enterprise Postgres Installation and Setup Guide for Server and base the design on table/index size.</td>
</tr>
<tr>
<td>storageClass</td>
<td></td>
<td></td>
<td>Defaults to platform default if omitted</td>
<td>SC is only set at start</td>
</tr>
<tr>
<td>accessModes</td>
<td></td>
<td></td>
<td>Defaults to ReadWriteOnce if omitted</td>
<td>Access mode is only set at start</td>
</tr>
<tr>
<td>logVol</td>
<td>No</td>
<td>size</td>
<td>1Gi</td>
<td>Volume size of the log. If you change the log output level (default: WARNING), measure the actual amount of log output in a test environment.</td>
</tr>
<tr>
<td>storageClass</td>
<td></td>
<td></td>
<td>Defaults to platform default if omitted</td>
<td>SC is only set at start</td>
</tr>
<tr>
<td>accessModes</td>
<td></td>
<td></td>
<td>Defaults to ReadWriteOnce if omitted</td>
<td>Access mode is only set at start</td>
</tr>
<tr>
<td>tablespaceVol</td>
<td>No</td>
<td>size</td>
<td>512Mi</td>
<td>Volume size of the tablespace. When using tablespaces, as with dataVol, you should refer to &quot;Estimating Database Disk Space Requirements&quot; in the Fujitsu Enterprise Postgres Installation and Setup Guide for Server for information on sizing.</td>
</tr>
<tr>
<td>storageClass</td>
<td></td>
<td></td>
<td>Defaults to platform default if omitted</td>
<td>SC is only set at start</td>
</tr>
</tbody>
</table>
Field | Mandatory | Sub-Field | Default | Description
---|---|---|---|---
accessModes | | | Defaults to ReadWriteOnce if omitted | Access mode is only set at start
walVol | Yes | size | 1200Mi | Volume size of the transaction log. Refer to "Estimating Database Disk Space Requirements" in the Fujitsu Enterprise Postgres Installation and Setup Guide for Server to help you design the size. Note that the default value for max_wal_size is 1 GB.
storageClass | | | Defaults to platform default if omitted | SC is only set at start
accessModes | | | Defaults to ReadWriteOnce if omitted | Access mode is only set at start

The 'accessMode' is been incorporated for the inclusion of pgBadger layer later. Giving it a shared volume capability will allow pgBadger Container to read logs from multiple server instance (master / replica) and expose it via a WebServer.

### 2.3.4 Deploying Pgpool-II and Connect to FEPCluster from Operator

Equivalent Kubernetes command: kubectl create FEPpgpool2

This operation will create a FEP pgpool2 container with supplied information. Refer to “FEPpgpool2 Custom Resource Parameters” in the “Reference” for more information.

### 2.3.5 Scheduling Backup from Operator

When creating a FEPCluster, users can obtain scheduled backups by setting up backup definitions. Users can also modify the backup schedule by modifying the Backup custom resource that was created.

A backup definition includes the following:
- Acquisition time (Specify in crontab format)
- Backup type (Full or incremental backups)

Backup is taken on master Pod only.

Backup processing is performed by pgBackRest.

Parameter can be set to pgbackrestParams in CR definition.

The maximum number of backup schedules is 5.

See the pgBackRest User's Guide for details on the parameters.

However, some parameters are limited. Details are given below.

- 2.3.5.1 Important Setting Items
- 2.3.5.2 Parameters that cannot be Set
- 2.3.5.3 Restricted Parameters
- 2.3.5.4 About Sections in the Config File
### 2.3.5.1 Important Setting Items

Here are the important parameters for setting pgBackRest. This parameter sets the retention period of backup information. If automatic backup is set and this parameter is not set, the risk of overflowing the backup area increases.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Overview of parameters</th>
<th>Setting value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Retention Option (repo retention -full)</td>
<td>Specify number of full backups to keep No default (should be set according to user backup policy)</td>
<td>natural number</td>
</tr>
<tr>
<td>Full Retention Type Option (repo retention-full-type)</td>
<td>spec.retention -full Specifies whether the setting is a number of retention days (time) or a number of retention generations (count) No default (should be set according to user backup policy)</td>
<td>time/count</td>
</tr>
</tbody>
</table>

The following is a sample CR example of changing the backup retention period (How long the PITR is valid) to 30 days after a FEPCluster deployment by setting the above parameters.

```yaml
apiVersion: fep.fujitsu.io/v1
d kind: FEPBackup
metadata:
  name: fepcluster-backup
spec:
  pgBackrestParams: |
# define custom pgbackrest.conf parameters below to override defaults.
[global]
  repo-retention-full = 30
  repo-retention-full-type = time
...
```

### 2.3.5.2 Parameters that cannot be Set

The following parameters in the pgBackRest Configuration Reference are not configurable.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Overview of parameters</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy Archive Option (--archive-copy)</td>
<td>Copy the WAL segments needed for consistency to the backup</td>
<td>To use internal fixed values</td>
</tr>
<tr>
<td>Check Archive Mode Option (--archive-mode-check)</td>
<td>Check the PostgreSQL archive_mode setting.</td>
<td>Limited to backup from master</td>
</tr>
<tr>
<td>Backup from Standby Option (--backup-standby)</td>
<td>Back up from the standby cluster</td>
<td>Limited to backup from master</td>
</tr>
<tr>
<td>Stop Auto Option (--stop-auto)</td>
<td>Stops a previously failed backup on a new backup.</td>
<td>Because they are 9.6 not supported in</td>
</tr>
<tr>
<td>pgBackRest Command Option (--cmd)</td>
<td>pgBackRest command</td>
<td>To use internal fixed values</td>
</tr>
<tr>
<td>SSH client command Option (--cmd-ssh)</td>
<td>Path to ssh client executable</td>
<td>Not using ssh</td>
</tr>
<tr>
<td>Compress Option (--compress)</td>
<td>Use File Compression</td>
<td>For obsolete options (Use compress-type option instead)</td>
</tr>
<tr>
<td>Config Option (--config)</td>
<td>pgBackRest configuration file.</td>
<td>To use internal fixed values</td>
</tr>
<tr>
<td>Parameter</td>
<td>Overview of parameters</td>
<td>Reason</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------</td>
<td>--------</td>
</tr>
<tr>
<td>Config Include Path Option (--config-include-path)</td>
<td>Path to additional pgBackRest configuration files.</td>
<td>To use internal fixed values</td>
</tr>
<tr>
<td>Config Path Option (--config-path)</td>
<td>Base path of pgBackRest configuration files.</td>
<td>To use internal fixed values</td>
</tr>
<tr>
<td>Delta Option (--delta)</td>
<td>Restore or Backup with Checksum</td>
<td>For new restores only</td>
</tr>
<tr>
<td>Dry Run Option (--dry-run)</td>
<td>Execute a dry-run for the command.</td>
<td>Command-line only option</td>
</tr>
<tr>
<td>Lock Path Option (--lock-path)</td>
<td>Path where the lock file is stored</td>
<td>To use internal fixed values</td>
</tr>
<tr>
<td>Keep Alive Option (--sck-keep-alive)</td>
<td>Enable keep-alive messages on socket connections</td>
<td>To use internal fixed values</td>
</tr>
<tr>
<td>Spool Path Option (--spool-path)</td>
<td>Path to store temporary data for asynchronous archive-push and archive-get commands</td>
<td>For automatic determination from FEPCluster CR values</td>
</tr>
<tr>
<td>Stanza Option (--stanza)</td>
<td>Defines the stanza.</td>
<td>To use internal fixed values</td>
</tr>
<tr>
<td>Console Log Level Option (--log-level-console)</td>
<td>Console Log Level</td>
<td>It is not expected to operate on Pod.</td>
</tr>
<tr>
<td>Std Error Log Level Option (--log-level-stderr)</td>
<td>Stderr log level</td>
<td>It is not expected to operate on Pod.</td>
</tr>
<tr>
<td>Log Path Option (--log-path)</td>
<td>Log File Destination</td>
<td>For automatic determination from FEPCluster CR values</td>
</tr>
<tr>
<td>Repository Host Option (--repo-host)</td>
<td>Repository host for remote operations via SSH</td>
<td>Repository Host is not used</td>
</tr>
<tr>
<td>Repository Host Command Option (--repo-host-cmd)</td>
<td>Path of pgBackRest on Repository Host</td>
<td></td>
</tr>
<tr>
<td>Repository Host Configuration Option (--repo-host-config)</td>
<td>Repository Host Configuration File Path</td>
<td></td>
</tr>
<tr>
<td>Repository Host Configuration Include Path Option (--repo-host-config-include-path)</td>
<td>Repository hosts configuring include path</td>
<td></td>
</tr>
<tr>
<td>Repository Host Configuration Path Option (--repo-host-config-path)</td>
<td>Repository Host Configuration Path</td>
<td></td>
</tr>
<tr>
<td>Repository Host Port Option (--repo-host-port)</td>
<td>Repository host port when &quot;repo-host&quot; is configured</td>
<td></td>
</tr>
<tr>
<td>Repository Host User Option (--repo-host-user)</td>
<td>Repository host user when &quot;repo-host&quot; is configured</td>
<td></td>
</tr>
<tr>
<td>Repository Path Option (--repo-path)</td>
<td>Path where backups and archives are stored</td>
<td>For automatic determination from FEPCluster CR values</td>
</tr>
<tr>
<td>Archive Retention Option (--repo-retention-archive)</td>
<td>The number of consecutive WAL backups to keep.</td>
<td>This option is not recommended, and WAL retention is controlled by the Full Retention Option and Full Retention Type Option.</td>
</tr>
<tr>
<td>Archive Retention Type Option (--repo-retention-archive-type)</td>
<td>Backup Type for WAL Retention</td>
<td>It is recommended not to change from the default.</td>
</tr>
<tr>
<td>Differential Retention Option (--repo-retention-diff)</td>
<td>Number of incremental backups to keep</td>
<td>No incremental backups</td>
</tr>
<tr>
<td>Parameter</td>
<td>Overview of parameters</td>
<td>Reason</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Archive Mode Option (--archive-mode)</td>
<td>Retains or disables the archive for the restored cluster.</td>
<td>To use internal fixed values</td>
</tr>
<tr>
<td>Exclude Database Option (--db-exclude)</td>
<td>Restore excluding the specified databases.</td>
<td>To restore the entire FEP cluster, including all databases</td>
</tr>
<tr>
<td>Include Database Option (--db-include)</td>
<td>Restore only the specified database</td>
<td>To restore the entire FEP cluster, including all databases</td>
</tr>
<tr>
<td>Link All Option (--link-all)</td>
<td>Restore all symbolic links.</td>
<td>To use internal fixed values</td>
</tr>
<tr>
<td>Link Map Option (--link-map)</td>
<td>Changes the destination of a symbolic link.</td>
<td>To use internal fixed values</td>
</tr>
<tr>
<td>Recovery Option Option (--recovery-option)</td>
<td>Setting options in postgresQL recovery.conf</td>
<td>To use internal fixed values</td>
</tr>
<tr>
<td>Tablespace Map Option (--tablespace-map)</td>
<td>Restoring tablespace to a specified directory</td>
<td>For automatic determination from FEPCluster CR values</td>
</tr>
<tr>
<td>Map All Tablespaces Option (--tablespace-map-all)</td>
<td>Restores all tablespaces to the specified directory</td>
<td>No tablespace required because there is only one tablespace per FEPCluster</td>
</tr>
<tr>
<td>TLS Server Address Option (--tls-server-address)</td>
<td>TLS server address.</td>
<td>TLS server not used</td>
</tr>
<tr>
<td>TLS Server Authorized Clients Option (--tls-server-auth)</td>
<td>TLS server authorized clients.</td>
<td></td>
</tr>
<tr>
<td>TLS Server Certificate Authorities Option (--tls-server-ca-file)</td>
<td>TLS server certificate authorities.</td>
<td></td>
</tr>
<tr>
<td>TLS Server Key Option (--tls-server-key-file)</td>
<td>TLS server key file.</td>
<td></td>
</tr>
<tr>
<td>TLS Server Port Option (--tls-server-port)</td>
<td>TLS server port.</td>
<td></td>
</tr>
<tr>
<td>PostgreSQL Database Option (--pg-database)</td>
<td>PostgreSQL database.</td>
<td>To use internal fixed values</td>
</tr>
<tr>
<td>PostgreSQL Host Option (--pg-host)</td>
<td>PostgreSQL host for remote operations via SSH</td>
<td>No SSH connection required</td>
</tr>
<tr>
<td>PostgreSQL Host Command Option (--pg-host-cmd)</td>
<td>Path of pgBackRest exe on the PostgreSQL host</td>
<td>To use internal fixed values</td>
</tr>
<tr>
<td>PostgreSQL Host Configuration Option (--pg-host-config)</td>
<td>Path of the pgBackRest configuration file</td>
<td>To use internal fixed values</td>
</tr>
<tr>
<td>PostgreSQL Host Configuration Include Path Option (--pg-host-config-include-path)</td>
<td>Setting pgBackRest on PostgreSQL host include path</td>
<td>To use internal fixed values</td>
</tr>
<tr>
<td>PostgreSQL Host Configuration Path Option (--pg-host-config-path)</td>
<td>Path to configure pgBackRest on the PostgreSQL host</td>
<td>To use internal fixed values</td>
</tr>
<tr>
<td>PostgreSQL Host Port Option (--pg-host-port)</td>
<td>SSH Port Specification</td>
<td>No SSH connection required</td>
</tr>
</tbody>
</table>
### 2.3.5.3 Restricted Parameters

Of the parameters in the pgBackRest Configuration Reference, the following parameters limit the configurable values.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Overview of parameters</th>
<th>Possible Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>repoX-gcs-key-type</td>
<td>The type of key file you specify when using Google Cloud Storage</td>
<td>service</td>
</tr>
<tr>
<td>Repository Type Option (--repotype)</td>
<td>Type of storage to use for the repository</td>
<td>posix/s3</td>
</tr>
</tbody>
</table>

### 2.3.5.4 About Sections in the Config File

In FEPBackup CR, you can write the contents of pgbackrest.conf, but the setting for stanza (Backup space for pgBackRest) is specified internally.

The following sections are not allowed;  
[stanza: command] , [stanza]  

### 2.3.6 Perform PITR and Latest Backup Restore from Operator

There are two types of restore: one is to restore backup data to an existing FEPCluster, and the other is to create a new FEPCluster and restore backup data.

The former retains the attributes of the FEPCluster, such as IP address and name, while the latter is created from scratch.

The restore process deploys a FEP restore container. The FEP restore container performs the pgBackRest restore operation from the backup data to be restored to the master server of the FEPCluster. After the data is restored to the master server, the FEPCluster is created by synchronizing the data to two replica servers.

If user create a new FEPCluster, the newly created FEPCluster will inherit the settings of the source cluster, unless otherwise specified. User can also create a cluster with different settings from the source cluster by including the settings in FEPRestore CR.

### Switching connections to the new cluster

The restore creates a new FEPCluster. If necessary, you need to set up PgpooII and change the access point of the application to the new cluster or the new Pgpool-II.

### About recovering a failed FEPCluster

Even if the existing FEPCluster fails and the FEP is not running, if the volume of the backup area is safe, it is possible to restore from the backup data.

### 2.3.7 FEP Unique Feature Enabled by Default

Enable the following FEP features:
- Data masking
- Transparent Data Encryption (TDE)

**Data masking**

The Data masking is enabled by default in the example FEPCluster CR (in openshift UI). The postgresql.conf in container contains the following parameters:

```
shared_preload_libraries = 'pgx_datamasking,pg_prewarm'
session_preload_libraries = 'pg_prewarm'
max_worker_processes= 20
```

The user can overwrite these values in config map.

**TDE**

TDE is enabled by default. Select one of the following as the keystore to store the master encryption key used for transparent data encryption.

- File-based keystore
- External key management service

If you use a key management service as your keystore, you can change the keystore to another key management service even after you deploy the FEP cluster. You cannot change from a file-based keystore to a key management service, or from a key management service to a file-based keystore.

Refer to "2.3.11 Transparent Data Encryption Using a Key Management System" for the design perspective when using a key management system.

### 2.3.8 Monitoring & Alert (FEPExporter)

As the operator is level 5 certified, the system expose various metrics about its operand i.e. FEP containers.

FEP generates lot of useful database statistics via various views. The default statistics can be further augmented by using extensions like `pg_stat_statements`.

FEPExporter container by default is configured to extract useful database statistics and make the metrics available to Prometheus on the platform. External components and utilities can be used to visualise, analyse, trigger alerts and take operational decision based on exposed metrics.

FEPExporter also sets default alert rules based on Prometheus metrics which are useful for active monitoring of FEP cluster.

#### 2.3.8.1 FEPExporter Custom Resource

Refer to "FEPExporter Custom Resource" in the Reference for FEPExporter Custom Resource parameters.

- Custom queries to scrape metrics can be added in CR in optional section.
- Custom Prometheus alert rules are created by user manually.

#### 2.3.8.2 Change to FEPCluster CR - metrics user

User may define pgMetricsUser, pgMetricsPassword and pgMetricsUserTls in target FEPCluster. If it is defined, FEPExporter will use metrics user details to connect to FEP cluster machines. All metrics user fields are optional and can be omitted in FEPCluster.

Refer to "FEPCluster Parameter" in the Reference for FEPCluster parameters.

#### 2.3.8.3 FEPExporter CR auto-create for FEPCluster

User may define enableMonitoring flag as part of FEPCluster CR to monitor FEPCluster. It will automatically create FEPCluster specific FEPExporter so metrics scraping for FEPCluster will work.

Refer to "FEPCluster Parameter" in the Reference for FEPCluster parameters.

- FEPExporter will be named as <cluster-name>-fepexporter.
- Once FEPExporter created automatically, user can modify it manually from FEPExporter CR.
- If FEPCluster will be deleted, it will delete dependent FEPExporter as well.
- MTLS for FEPExporter will only supported when tls configuration defined for both Prometheus & FEPExporter specs.

### 2.3.9 Scaling Replicas

Auto scale out occurs when the average database CPU utilization or number of connections exceeds the threshold. Select whether the criteria for auto scale out is CPU usage or the number of connections, depending on the resource that is the bottleneck of the database.

The maximum number of replica containers, excluding the master container, is 15.

#### Scale out based on CPU utilization

Performs a scale out if the average CPU utilization of all pods (primary pods and all replica pods) in the FEPCluster exceeds the threshold for a period of time.

CPU utilization is calculated with the value specified in spec.fep.mcSpec.requests.cpu specified for the FEPCluster custom resource as the denominator.

#### Scale out based on the number of connections

Performs a scale out if the average number of connections for all pods (primary pods and all replica pods) in the FEPCluster exceeds the threshold for a period of time.

Specify the threshold for the number of connections to perform automatic scale-out with a value less than or equal to the max_connections parameter of the FEP server.

The prerequisites for using the scale out feature based on the number of connections are as follows.

- The monitoring feature (see "2.3.8 Monitoring & Alert (FEPExporter)") is enabled.
- Metrics for the number of FEP server connections are collected by the monitoring feature.
- A custom metrics server is installed in the OCP/Kubernetes cluster.
- The custom metrics server publishes the average number of connections collected by the monitoring feature.

When using the scale out feature based on the number of connections, the auto scale out feature requests the custom metrics server for metrics associated with the following Kubernetes resources.

- kind: FEPCluster
- apiVersion: fep.fujitsu.io/v2
- name: Name of FEPCluster
- namespace: The name of the namespace in which FEPCluster is deployed

The name of the requested metric is the name specified in the metricName parameter.

This metric should represent the average number of connections for each pod in the specified FEPCluster.

#### Limitations

- If you want to use the scale out feature based on the number of connections, deploy FEPExporter according to the procedure of "4.3 Deploying FEPExporter".
- If FEPCluster metrics are collected by FEPExporter in standalone mode (see "4.4 FEPExporter in Standalone Mode"), the scale out feature based on the number of connections is not available.

**Note**

When using the auto scale out feature, the FEPCluster sync mode should be "off".
Precautions when designing auto scale out

- The auto scale out feature adds replicas one at a time. In addition, additional replicas take time to service, depending on the environment and the amount of data stored. As a result, replica growth may not be able to keep up with the increased load.

- Even if the auto scale out feature increases the number of replicas, incoming requests are not given priority to those replicas. As a result, existing FEP instances may continue to be temporarily overloaded after the number of replicas increases.

- The auto scale out feature increases the number of replica requests that can be handled only by reference requests to the database. Requests with updates continue to be processed on the primary FEP instance. Therefore, the auto scale out feature may not reduce the load on the primary FEP instance.

- Currently, the auto scale out feature does not delete replicas (reduce the number of replicas). If the load decreases after the number of replicas increases due to a temporary increase in load, the number of replicas remains increased. If necessary, manually change the number of replicas.

2.3.9.1 Change to FEPCluster CR - auto scale out

If you want to use Auto Scale Out, set the parameter to FEPClusterCR.

Refer to "FEPCluster Parameter" in the Reference for FEPCluster parameters.

2.3.10 Disaster Recovery

By using OSS (pg_backrest) functionality to store backup data in object storage, data can be migrated to a database cluster in a different OCP environment.

Even if it is difficult to operate in an OCP environment with a database cluster due to a disaster, it is possible to continue operating in a different OCP environment.

2.3.11 Transparent Data Encryption Using a Key Management System

Fujitsu Enterprise Postgres provides unique features that enhance the security of PostgreSQL. These security features help users keep their data safe from unauthorized access. One such security feature is Transparent Data Encryption (TDE), which encrypts data at rest, i.e. data stored on disk/persistent volume.

In contrast, TDE's default format stores the master encryption key in a password-protected file. A key management system allows you to store your master encryption key (MEK) in a cloud-based keystore, taking your security to the next level.

The key management system that can be used with transparent data encryption is one of the following:

- Key management server using KMIP protocol
- AWS key management service (x86 only)
- Azure key management service (x86 only)

Refer to "Appendix D Key Management System Available for Transparent Data Encryption" for detailed key management system requirements.

Transparent data encryption using a key management system can only be configured when the FEPCluster is first created. Users cannot configure an existing FEPCluster for transparent data encryption using a key management system.

If the master encryption key on the key management system is lost, the encrypted/backup data cannot be decrypted. As long as the data encrypted with the master encryption key remains valid, the master encryption key must also be available and maintained on a key management system.

If you have encrypted backups with old encryption key, you must keep the old encryption key available after the master encryption key is rotated. Otherwise, you will not be able to open the database restored from backup.

In addition, the key custodian must retain the referenced master encryption key for as long as the data encrypted under the old master encryption key remains valid.
2.3.12 Database Role Management

In order to manage data access control, you can easily implement database role privilege and expiration management.

Operators can easily create roles related to database operations, assign privileges, and manage the expiration dates of database roles with login privileges in order to manage data access control.

Databases contain important data such as personal information, and data protection is important.

Data protection is defined in security protocols and is an important aspect of operations.

In order to protect data from being viewed by a third party, it is necessary to properly set the access control of database roles.

In this feature, it is recommended to divide into the following database roles.

- Database administrator: Construction/operation of database system
- Confidential administrator: Set appropriate privileges for each database resource
- General users: End users of the database

By preparing multiple database operators/administrators and assigning privileges to each, it is possible to distribute privileges. This makes it possible to prevent data from being referenced or tampered with by users with strong privileges.

This section describes the roles of database roles created by this feature.

Database administrators can perform operations related to database operations, such as referencing system tables and canceling back-end queries.

Confidential administrators grant appropriate privileges to tables and roles to prevent third parties from viewing data. With this feature, it is possible to grant the confidential administrator the privilege to use the confidential management support feature, and to grant the appropriate privilege to each database resource.

In addition, it is not recommended to use roles with SUPERUSER or BYPASSRLS privilege that can see all data for data protection. Therefore, in this feature, the SUPERUSER (postgres) password is isolated by hiding it, and the SUPERUSER and BYPASSRLS privileges are not granted to the created database role.

2.3.12.1 Creating Roles Related to Database Operation

2.3.12.1.1 Quarantine SUPERUSER

Create a database role "postgres" with SUPERUSER privileges for the operator when building the database.

By omitting "spec.fepChildCrVal.sysUsers.pgAdminPassword" in the FEPCluster custom resource, the postgres role password is created with a random value, making it impossible for general users to use SUPERUSER privileges. However, a separate method is provided to use the "postgres" role when the administrator needs SUPERUSER privileges for database operations. Therefore, monitor for unexpected usage using the audit feature of pgAudit.

2.3.12.1.2 Database Administrator Role

Database role for database management. Defining this role is mandatory.

The user name and password are defined in "pguser" and "pgpassword" under spec.fepChildCrVal.sysUsers in the FEPCluster custom resource. Has CREATE DATABASE privilege and can see system tables/cancel backend queries.

The database administrator role has the following privileges.

- NOSUPERUSER
- NOREPLICATION
- NOBYPASSRLS
- CREATEDB
- INHERIT
- LOGIN
- CREATEROLE
However, NOCREATEROLE privileges are granted when the confidential administrator role is created.

I also belong to the following roles:

- pg_monitor
- pg_signal_backend

2.3.12.1.3 Confidential Administrator Role

A database role that uses the confidential management support feature to set appropriate privileges for each database resource for database users. Creating this role is optional.

User name and password are defined in "pgSsecurityUser" and "pgSsecurityPassword" under "spec.fepChildCrVal.sysUsers" of FEPCluster custom resource.

Confidential administrator roles can be defined after building FEPCluster. However, you cannot change the role name or delete the role after defining this role.

This role holds the following privileges.

- LOGIN
- CREATEROLE
- NOSUPERUSER
- NOREPLICATION
- NOBYPASSRLS
- NOCREATEDB
- NOINHERIT

The Confidential administrator role has ALL privileges for the database defined in the FEPCluster custom resource "spec.fepChildCrVal.sysUsers.pgdb", and can create database objects such as tables in the target database.

Confidential administrator roles are assigned the following privileges necessary to operate the confidential management support feature of Fujitsu Enterprise Postgres, so the confidential management support feature can be used immediately after the role is created.

- CREATEROLE privilege
- SELECT privilege, INSERT privilege, UPDATE privilege, and DELETE privilege to all tables included in the extension of confidential management support feature

Grant ownership to the confidential administrator role for the database objects managed by the confidential management support feature.

In addition, by granting the privileges required for the confidential administrator role to operate the confidential management support feature to other database roles, the number of users who perform confidential management can be increased and the privileges can be distributed.

2.3.12.2 Expiration Management of Database Roles with Login Privileges

You can manage password expiration for database roles with login privileges.

When defining passwords for database roles with login privileges in the CREATE ROLE or ALTER ROLE statements, it is possible to force them to expire within a specified period.

Specify the following parameters in the FEPCluster custom resource to enable this feature.

- Specify "fsep_operator_security" in shared_preload_libraries of spec.fepChildCrVal.customPgParams
- "spec.fepChildCrVal.sysUsers.passwordValid.days" specifies the number of days that can be specified from the time the password is changed to the expiration date

FEPCluster custom resource definition example

```yaml
fepChildCrVal:
  customPgParams: |
    shared_preload_libraries='pgx_datamasking,pg_prewarm,pg_stat_statements,fsep_operator_security'
```
When this feature is enabled, the password expiration for pgpassword and pgSecurityPassword, as defined in spec.fepChildCrVal.sysUsers in the FEPCluster custom resource, is defined after the length of time specified in spec.fepChildCrVal.sysUsers.passwordValid.days since the password was changed.

However, passwords defined in pgAdminPassword, pgreplpassword, pgRewindUserPassword, and pgMetricsUserPassword are database role passwords required for database operation management, so their expiration dates are not managed.

In addition, if the CREATE ROLE or ALTER ROLE statement defines/changes the password for a database role that has login privileges, and the password for the database role does not expire or is longer than the length of time specified by spec.fepChildCrVal.sysUsers.passwordValid.days, the executed SQL will fail.

spec.fepChildCrVal.sysUsers.passwordValid.days can be defined or changed after building the FEPCluster. Changing this parameter updates the password expiration period for all managing database roles that have not expired.

Removing spec.fepChildCrVal.sysUsers.passwordValid.days or setting it to 0 will stop password expiration management.

By using the FEPExporter custom resource feature, it is possible to monitor the password expiration date of database roles and send an alert using AlertManager when there is a database role that is about to expire or has passed.
Chapter 3 Operator Installation

This chapter describes how to install FEP operator.

Refer to "6.5 Assigned Resources for Operator Containers" for more information about the resources assigned to installed operator containers and how to change them.

3.1 Using the OperatorHub

Describes how to use OperatorHub to install FEP operators into a new namespace on OpenShift.

3.1.1 Pre-requisite

A project on openshift is essentially a namespace. It is a good practice to install FEP in a separate name space. On the RedHat OpenShift platform, click "Home" under "Projects" main menu and hence click on "Create Project".

(Screen Shot 1 and 2 - Create Project on OCP - for ref.)

In the dialog box, specify a unique name for your namespace and an optional display name and description.

Create Project

Name *

fep-install-test

Display name

fep-install-test

Description

test installation for fep

Note

Operator installation needs Prometheus to be pre-installed in the OpenShift cluster.
3.1.2 Deploying Operator

Once operator is certified by RedHat, it is made available on OperatorHub on all RedHat OpenShift container platform.

On OpenShift platform, logon with credentials that has privileges to install operator. Click on OperatorHub on menu item under Operators and type filter keyword “Fujitsu Enterprise Postgres Operator” to find Fujitsu Enterprise Postgres Operator.

Click on Fujitsu Enterprise Postgres Operator to install operator. It will bring up details page with install button as below.
Fujitsu Enterprise Postgres Operator 1.5 delivers an enterprise-grade PostgreSQL on OpenShift Container Platform.

This solution provides the flexibility of a hybrid cloud solution while delivering an enhanced distribution of PostgreSQL to support enterprise-level workloads and provide improved deployment and management, availability, performance, data governance and security.

Available as a multi-architecture container built for both amd64, s390x and ppc64le.

The download and Use of the Product is strictly subject to the terms of the End User License Agreement with Fujitsu Limited found at https://www.fast.fujitsu.com/fujitsu-enterprise-postgres-license-agreements. Where the Product that has been embedded as a whole or part into a third party program, only Authorised Customers may download and use the Product.

---

<table>
<thead>
<tr>
<th>Latest version</th>
<th>Fujitsu Enterprise Postgres 1.5 delivers an enterprise-grade PostgreSQL on OpenShift Container Platform.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capability level</td>
<td>This solution provides the flexibility of a hybrid cloud solution while delivering an enhanced distribution of PostgreSQL to support enterprise-level workloads and provide improved deployment and management, availability, performance, data governance and security.</td>
</tr>
<tr>
<td>Source</td>
<td>Certified</td>
</tr>
<tr>
<td>Provider</td>
<td>Fujitsu</td>
</tr>
<tr>
<td>Repository</td>
<td>N/A</td>
</tr>
<tr>
<td>Container image</td>
<td>quay.io/fujitsu/fujitsu-enterprise-postgres-operator</td>
</tr>
</tbody>
</table>

Click on “Install” button, to bring up following screen to choose namespace and approval strategy. Select ”A specific namespace on the cluster” and choose desired namespace. Leave everything else to default and click install.
3.2 Using the Helm Chart

Describes how to install FEP operators into a new namespace on Kubernetes using the Helm feature.

3.2.1 Deploying Operator

1. Add a Helm Chart repository for the operator.
   
   ```bash
   helm repo add fep-repo https://fujitsu.github.io/fep-operator-helm/v1
   ```

2. Create a namespace to install the operator.
   
   ```bash
   kubectl create namespace fep-operator
   ```

   **Note**
   
   Operator installation needs Prometheus to be installed in the Kubernetes cluster in advance.

3. Run the helm command to install the operator.
   
   ```bash
   helm install fep-operator-release fep-repo/fujitsu-enterprise-postgres-operator --namespace fep-operator
   ```

3.2.2 Upgrading Operators

1. Refresh Helm Chart repository information.
   
   ```bash
   helm repo update
   ```

2. Check the Helm Chart version of the latest operator.
   
   ```bash
   helm search repo fujitsu-enterprise-postgres-operator
   ```

3. Run the helm command to upgrade the operator.
   
   ```bash
   helm upgrade fep-operator-release fep-repo/fujitsu-enterprise-postgres-operator --namespace fep-operator
   ```

3.3 Using the Rancher UI

Describes how to install FEP operators into a new namespace on Rancher UI.
3.3.1 Pre-requisite

Create a project and its associated namespace on the Rancher UI. We recommend that you install FEP in a different namespace. In the Rancher UI, click [Projects/Namespaces], then click [Create Project] that appears.

Specify a unique name for the project and click [Create].

Click [Create Namespace] displayed on the specified project.
Specify a unique name in the namespace and click [Create].

3.3.2 Register Helm Chart Repository

Register the Helm Chart repository of the operator feature on the Rancher UI.

In the Rancher UI, click [Apps & Marketplace], then click [Repositories] that appears.
Click [Create] to create the Helm Chart repository.

Enter the unique name of the catalog and the URL of the catalog below, and click [Create].

https://fujitsu.github.io/fep-operator-helm/v1
3.3.3 Deploying Operator

On the Rancher UI, apply the operator function Helm Chart to the project / namespace created in "3.3.1 Pre-requisite" and install the operator.

From the leftmost tab, click [Charts], then click [fujitsu-enterprise-postgres-operator].

Click Install on the screen that appears.
Change the [Namespace] item to the name created in "3.3.1 Pre-requisite", enter the release name in the [Name] item, click [Next], and then click [Install] on the next screen.

The operator is deployed on the target namespace.

3.4 Implement Collaborative Monitoring Tools

3.4.1 Implement GAP Stack

There is a pre-requisite for running FEPExporter.

- GAP(Grafana, AlertManager, Prometheus) stack is installed on host OpenShift or Kubernetes cluster
- FEPCluster that needs to be scraped is deployed and running properly
FEPCluster has following setting postgresql.conf:
- pg_stats_statements library pre-loaded
- track_activities and track_counts are turned on

For Prometheus and AlertManager, use the monitoring stack preinstalled on OpenShift. Please refer to the following for deployment information.
(https://docs.openshift.com/container-platform/4.11/monitoring/monitoring-overview.html#understanding-the-monitoring-stack_monitoring-overview)

For Grafana, install and use the GrafanaOperator provided by OperatorHub. Grafana is not exposed by OperatorHub in s390x and ppc64le, so use Helm to build Grafana. Detailed instructions are available at the following site for your reference.

Grafana comes pre-installed on OpenShift, but it is recommended to use Grafana published in OperatorHub to customize the dashboard and monitor FEP performance information.

You can also use the sample dashboards published below.

### 3.4.2 Implement Elastic Cloud on Kubernetes

#### 3.4.2.1 Deploy ECK Operator

1. Create namespace(project) elastic-system.
2. In OperatorHub, install Elasticsearch (ECK) Operator provided by Elastic.
3. Click Install to start proceed.
4. Change the Installation mode to "A specific namespace on the cluster" and select namespace "elastic-system". Click Install to complete the installation.

3.4.2.2 Deploy Elasticsearch Cluster

1. In Installed Operators, select "Elasticsearch (ECK) Operator".

2. Select “Elasticsearch Cluster” and "Create Elasticsearch".

3. In YAML view, enter the following details and click "Create".

```yaml
apiVersion: elasticsearch.k8s.elastic.co/v1
kind: Elasticsearch
metadata:
    name: quickstart
```
3.4.2.3 Deploy Enterprise Search

1. In Installed Operators, select “Elasticsearch (ECK) Operator”.
2. Select “Enterprise Search” and “Create EnterpriseSearch”.

3. In YAML view, enter the following details and click “Create”.

```yaml
apiVersion: enterprisesearch.k8s.elastic.co/v1
kind: EnterpriseSearch
metadata:
  name: enterprise-search-quickstart
spec:
  version: 8.5.2
  count: 1
  elasticsearchRef:
    name: quickstart
```

3.4.2.4 Deploy Kibana

1. In Installed Operators, select “Elasticsearch (ECK) Operator”.
2. Select “Kibana” and “Create Kibana”.
3. In YAML view, enter the following details and click "Create".

```yaml
piVersion: kibana.k8s.elastic.co/v1
kind: Kibana
metadata:
  name: quickstart
spec:
  count: 1
  elasticsearchRef:
    name: quickstart
  enterpriseSearchRef:
    name: enterprise-search-quickstart
  version: 8.5.2
```

### 3.4.2.5 Expose Kibana using OpenShift Route

1. Obtain CA certificate that signs Kibana certificate.

Locate the secret quickstart-kb-http-certs-public.

![Secrets](image-url)
Copy the content of ca.crt.

2. Create route for Internet access.

   Navigate to Networking -> Route and select "Create Route".

   - Fill in the details

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>kibana</td>
</tr>
<tr>
<td>Hostname</td>
<td>Leave empty</td>
</tr>
<tr>
<td>Path</td>
<td>/</td>
</tr>
<tr>
<td>Service</td>
<td>quickstart-kb-http</td>
</tr>
<tr>
<td>Target port</td>
<td>5601 -&gt; 5601 (TCP)</td>
</tr>
<tr>
<td>Secure Route</td>
<td>selected</td>
</tr>
<tr>
<td>TLS termination</td>
<td>Re-encrypt</td>
</tr>
<tr>
<td>Insecure traffic</td>
<td>Redirect</td>
</tr>
<tr>
<td>Destination CA certificate</td>
<td>Content of ca.crt in previous step</td>
</tr>
</tbody>
</table>
3.4.2.6 Login to Kibana

1. Obtain the Elasticsearch/Kibana login details

   Locate the secret quickstart-es-elastic-user

   ![Secrets Table]

2. Observe the login details from the secret

   ![Data]

3. Visit the URL as created in the Route above and use the above credential to login
4. Select the collapsed menu icon on top left corner and select Enterprise Search -> Content

![Elasticsearch Interface](image)

5. If fluentd is forwarding logs to this elastic cluster, you will find the indexes here.

### 3.5 Implement Client

To use the FEP client, use the media or download the rpm module from the following site.

https://www.postgresql.fastware.com/fujitsu-enterprise-postgres-client-download
Chapter 4 Deployment Container

This chapter describes container deployment.

---

Note

Each volume of a Pod created by a FEPCluster deployment is sized by default for the following operations:

- Data size: 1 GB
- Daily update: about 50 MB

Refer to "2.3.3 Configurable Volume per Cluster" to design each volume size according to actual operation.

---

4.1 Deploying FEPCluster using Operator

To deploy a FEPCluster in given namespace, follow these steps:

---

Note

If you are deploying on a Kubernetes cluster, Refer to "Custom Resource Parameters" in the Reference to create and apply a yaml file.

---

1. Under "Operators" menu item, click on "Installed Operators". You would see the installed FEP operator deployed in "Chapter 3 Operator Installation". Click on the name of operator.

2. It will display a page with all CRs this operator supports. FEPCluster is the main CR and all others are child CR. We would create the main CR and all other CRs will be created automatically by Operator.
   To create Cluster CR, either
   (1) Click on "Create Instance" under FEPCluster.
OR

(2) Click on "FEPCluster" on top and then click on "Create FEPCluster" on the next page.

3. This will bring to "Create FEPCluster" page. Here you have two options to configure. The first one is Form View. At the moment, in Form View, one can change only the name of cluster being deployed. The default name is ‘new-fep’.

This name must be unique within a namespace.
4. In YAML View, starting value of CR is visible and one can choose to modify parameters before creating CR. Refer to the Reference for details of parameters.

5. When "Create" is clicked on either of the two pages above, the operator creates FEPCluster CR, and there after one by one FEPBackup, FEPConfig, FEPVolume, FEPUser, and FEPCert child CRs are created automatically. The starting values for child CRs are taken from the "fepChildCrVal" section of the FEPCluster CR YAML file. Modifying value in FEPCluster "fepChildCrVal" section. Operator reflects changes from FEPCluster parent CR to respective child CRs. Only allowable changes are reflected in child CRs. Child CRs are marked internal objects and hence will not be visible on the OCP console. However, you can check child CRs using command-line tools.
6. In FEPCluster CR, annotations are added to indicate that child CRs are created successfully and has initialised properly. It may take some time to complete.

7. Once child CRs are marked done in annotations, operator creates StatefulSet for the cluster.

8. StatefulSet will start one FEP instance at one time and will wait it to be ready before starting next one.
9. Once all instances of FEP servers are started, the operator marks a flag “fepClusterReady” under “status.fepStatus” section of CR to be `true`, indicating that FEPCluster is ready for use. Looking at YAML of FEPCluster CR, it would look like as below:

![FEPCluster CR](image)

10. Operator also masks the sensitive fields like passwords, passphrase, certificates and keys in FEPCluster fepChildCrVal and also in respective child CRs.

### 4.2 Deploy a Highly Available FEPCluster

In a highly available FEP cluster, load balancing is possible by distributing read queries to replica instances.

In addition, if the master instance fails, the user can switch to the replica instance immediately to localize the business interruption period. In a highly available configuration, you can select the synchronization mode for the replica instance. Synchronous replication is recommended for systems that cannot tolerate data loss in the event of a master instance failure.

Because multiple instances are created in a highly available configuration, licenses are required for each.

To deploy a highly available FEPCluster in given namespace, follow these steps:

**[Prerequisites]**

If the FEP cluster is running in HA mode, the backup and archive WAL volumes must be configured with shared storage (NFS, etc.) that supports ReadWriteMany. See the Openshift documentation for instructions on setting up shared storage. Also, the reference procedure is described in "Appendix C Utilize Shared Storage", so please check if necessary.

If you do not have shared storage, you can remove the backup section and the backup and archive volume sections to disable the backup feature and deploy the FEP cluster.

**Note**

If you are deploying on a Kubernetes cluster, Refer to "Custom Resource Parameters" in the Reference to create and apply a yaml file.

1. It is the same as the procedure from step 1 to step 3 in "4.1 Deploying FEPCluster using Operator".
2. Instead of step 4 in "4.1 Deploying FEPCluster using Operator", change to the YAML view and specify '3' for the "instances" parameter of "fep" in "spec". Specify the storage class for the prepared shared storage for the backup and archive WAL volumes.

3. It is the same as the procedure from step 5 to step 10 in "4.1 Deploying FEPCluster using Operator".

4. Three pods deployed and ready for a highly available FEPCluster.

---

### Information

You can determine whether the master or replica pod is the master or replica pod by issuing the following command:

```sh
c$ oc get pod -L feprole
```

<table>
<thead>
<tr>
<th>NAME</th>
<th>READY</th>
<th>STATUS</th>
<th>RESTARTS</th>
<th>AGE</th>
<th>FEPROLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>fep-ansible-operator-88f7fb4b-5jh85</td>
<td>1/1</td>
<td>Running</td>
<td>0</td>
<td>24m</td>
<td></td>
</tr>
<tr>
<td>new-fep-sts-0</td>
<td>2/2</td>
<td>Running</td>
<td>0</td>
<td>17m</td>
<td>master</td>
</tr>
<tr>
<td>new-fep-sts-1</td>
<td>2/2</td>
<td>Running</td>
<td>0</td>
<td>15m</td>
<td>replica</td>
</tr>
<tr>
<td>new-fep-sts-2</td>
<td>2/2</td>
<td>Running</td>
<td>0</td>
<td>13m</td>
<td>replica</td>
</tr>
</tbody>
</table>

### 4.3 Deploying FEPEXporter

To deploy a FEPEXporter, follow these steps:
1. In order to deploy FEPExporter managed by Operator, it is as easy as setting `fep.monitoring.enable` to true in FEPCluster CR at the time of deployment.

   ![FEPCluster CR](image1)

2. FEPExporter will be created automatically under the name `<cluster-name>-fepexporter`. And it will list show all the database with statistics of specified FEPcluster.

   ![FEPExporter](image2)

3. FEPExporter spawned by FEP Operator in aforementioned way will scrape metrics by default from the Master and standby instances and make it available to Prometheus.

   ![FEP Operators](image3)
4. User can configure MTLS to be used for HTTP endpoint used by Prometheus for metrics scraping as well as connection from FEP Exporter to database.
   a. If pgMetricsUser, pgMetricsPassword and pgMetricsUserTls is defined in FEPCluster; FEPExporter will hence use these for securing connection to the postgres instances. In absence of these parameters, FEPExporter will use pgAdminUser (i.e. super user).
   b. User can configure Prometheus.tls and FEPExporter.tls to ensure that metrics end point (/metrics) by FEPExporter is also used with MTLS (Refer to "FEPExporter Custom Resource" in the Reference for details of fields)

5. User can also configure basic authentication by specifying a secret that contains username & password. (Refer to “FEPExporter Custom Resource” in the Reference for details of fields)

6. Now user can see scrape FEPExporter specific metrics on Openshift Platform in monitoring section area using PROMQL to specify a metrics of interest

Note
- User can set fep.monitoring.enable to true or false on an already instantiated cluster as well to achieve desired results
- pgMetricsUser can be defined later on a running FEPCluster with monitoring enabled and can force FEPExporter to use pgMetricsUser by mere restarting it (refer restartRequired ). However, MTLS can not be configured in this case and user is expected to grant specific permission to pgMetricsUser for all the database objects which are expected to be use while scraping information.
- For MTLS to be forced, ensure usePodName and pg_hba.conf is been set appropriately.
- FEPExporter default metrics expects few following in postgresql.conf
  - pg_stats_statements library pre-loaded
  - track_activities and track_counts are turned on
  - Monitoring user needs permission on pg_stat_* views
- FEPExporter pod specification related to CPU memory can be changed. After changing resources specification, set restartRequired flag to true. FEPExporter will be restarted with new specifications
- FEP Monitoring is closely integrated with Prometheus available on platform. User should ensure that on openshift platform monitoring is enabled for user-defined projects (Refer: https://docs.openshift.com/container-platform/4.11/monitoring/enabling-monitoring-for-user-defined-projects.html ). For platforms other than openshift, ensure Prometheus is installed before deployment of FEP operator

4.4 FEPExporter in Standalone Mode

FEPExporter is an independent CR; hence it does not necessarily depend on main FEPCluster CR. To deploy a FEPExporter in given namespace follow the below step.
1. To create FEPExporter CR, either
   (1) Click on “Create Instance” under FEPExporter.
   OR
   (2) Click on "FEPExporter" on top and then click on "Create FEPExporter" on the next page.

2. In Form View, one can change only the name of cluster being deployed. The default name is "new-fep-exporter". This name must be unique within a namespace.

3. FEPExporter scrapes metrics for FEPCluster within same namespace.
4. In YAML View, starting value of FEPExporter CR is visible and one can choose to modify parameters before creating CR. Refer to the Reference for details of parameters.

5. When clicked on the "Create" button, it will create FEPExporter pod with other resource like secret, service, configmap for data source queries.
6. Specify the name of the FEPCluster in spec.fepExporter.fepClusterList of FEPExporter. Before targeting cluster, Check the FEPCluster status and FEP StatefulSet are in running condition.

7. It will recreate FEPExporter pod with a new dataresource secret. It will list down all the database with statistics of specified FEPCluster in monitoring section.

8. If fepClusterList has more than one clusters listed, current exporter will collect metrics for all of those listed.

9. Multiple FEPExporters can be deployed within one namespace with their own cluster list to collect metrics from.

4.5 Deploying FEPClusters with Cloud Secret Management

Note

The cloud secret management feature cannot be used together with the following parameters.

- spec.fepChildCrVal.sysUsers.pgSecurityUser
- spec.fepChildCrVal.sysTde.tdek
- spec.fepChildCrVal.sysUsers.passwordValid.days

4.5.1 Installing Secret Store CSI Driver Using Helm Charts

Install Secret Store CSI Driver from Helm chart.

Add helm chart repository.

```
```

Install with helm command.

```
helm install csi-secrets-store secrets-store-csi-driver/secrets-store-csi-driver --namespace kube-system --set enableSecretRotation=true --set rotationPollInterval=30s
```

Information

- Setting enableSecretRotation=true enables auto rotation of secret. i.e if value of secret gets changed in one of the external secret store (Azure/AWS/GCP/HashiCorp vault) then the updated value will be reflected in the FEPCluster as well.
- Setting rotationPollInterval=30s enables rotation poll interval which checks how frequently the mounted secrets for all pods need to be resynced to the latest.

- For OpenShift cluster to allow CSI type volumes to be mounted in container, system Security Context Constraints needs to be patched. Patch the volumes section to include CSI for providers( nonroot, anyuid, hostmount-anyuid, machine-api-termination-handler, hostaccess.node-exporter, privileged, privileged-genevalogging, restricted).

- In scenarios where existing OpenShift is upgraded kindly verify that CSI is included in system Security Context Constraints for the above mentioned providers.

### 4.5.2 Installing and Configuring Azure Provider for Secret Store CSI Driver

#### 4.5.2.1 Install Azure Provider drivers using helm chart

```bash
```

Note: By default when installing Azure Provider ; secret-store-csi-driver installation is set to true by default. If secret-store-csi-driver is already installed as per steps in "4.5.1 Installing Secret Store CSI Driver Using Helm Charts" execute below command.

```bash
helm install csi csi-secrets-store-provider-azure/csi-secrets-store-provider-azure --namespace kube-system --set secrets-store-csi-driver.install=false
```

Note: If secret-store-csi-driver is not installed as per step "4.5.1 Installing Secret Store CSI Driver Using Helm Charts". Execute below command to install provider along with secret-store-csi-driver.

```bash
```

#### 4.5.2.2 Create Secret to Access Azure Key vault

```yaml
kind: Secret
apiVersion: v1
metadata:
  name: <Secret Name>
  namespace: <WHERE FEP CLUSTER TO BE INSTALLED>
  labels:
    secrets-store.csi.k8s.io/used: 'true'
data:
  clientid: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
  clientsecret: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

type: Opaque
```

Clientid: clientid is SERVICE_PRINCIPAL_CLIENT_ID

Clientsecret: clientsecret is SERVICE_PRINCIPAL_CLIENT_SECRET

#### 4.5.2.3 Store Secret in Azure Key Vault

```bash
az keyvault secret set --vault-name <Vault Name> --name <Secret Name> --value <Secret value>
```

#### 4.5.2.4 Store Certificate in Azure Key Vault

Certificate should be in below format before uploading cert to Azure Key Vault i.e it should be one .pem file (key, crt and CA in one file)

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBABCAQEAx1rSblocR8pR5h5d2D3kuryT7Ru6DAR8arxSwrAaSdvy1yU
KA7Q+Zg41waGwkt3cE2vX6cH4z3jwz+X0Vj0x03jVh8tvfuxQDuNpFEWCRRX1xt
3S8xc80CzbnHRWQAkdxRWhfPSWd1pPe7uNcVe86SUVWjYzBmoJnFnmK3
5EoxKrcl3sG174YhWdsGalsNzBh2pdR+11heE2KJUc65d113KJx9cDh1c81cwK
-----END RSA PRIVATE KEY-----
```
4.5.3 Installing and Configuring AWS Provider for Secret Store CSI Driver

4.5.3.1 Install AWS Provider drivers using helm chart

```

helm install -n kube-system secrets-provider-aws aws-secrets-manager/secrets-store-csi-driver-provider-aws --name namespaces/secret-store-csi-driver-provider-aws
```

4.5.3.2 Setup EKS cluster along with service account with necessary IAM roles and permission to access Secret Manager

Follow below link to setup IAM roles and EKS for CSI.

https://github.com/aws/secrets-store-csi-driver-provider-aws

Create IAM role trust policy to access Secret Manager

```
Create IAM role trust policy to access Secret Manager
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
```
4.5.3.3 Store Secret in AWS Secrets Manager

```bash
aws secretsmanager create-secret --name <Secret Name> --secret-string <Secret Value>
```

4.5.3.4 Store Cert in AWS Secrets Manager

Certificate should be in below format before uploading cert to AWS Secrets Manager i.e it should be one .pem file (key, crt and CA in one file)

(Refer "mycert.pem" for sample certificate format)

```bash
aws secretsmanager create-secret --name <Secret Name> --secret-binary fileb://<File Name>
```

**Note**

Only single key value for secret to be stored in Secret Manager.

4.5.4 Installing GCP Provider for Secret Store CSI Driver

4.5.4.1 Install GCP Provider drivers using Kubernetes

```bash

kubectl apply -f provider-gcp-plugin.yaml -namespace kube-system
```

4.5.4.2 Configure GCP secret manager and IAM

Create Service Account:

```bash
gcloud iam service-accounts create my-secret-acc;
```

Attach SecretManagerAdmin policy to the new service account

```bash
gcloud projects add-iam-policy-binding $PROJECT_ID \ 
   --member="serviceAccount: my-secret-acc @PROJECT_ID.iam.gserviceaccount.com" \ 
   --role="roles/secretmanager.admin" \ 
   --condition="None";
```

Generate a key for your new service account
4.5.4.3 Create Secret to access GCP Secret manager

Use keys generated from "4.5.4.2 Configure GCP secret manager and IAM" (iam-key.json file)

```bash
kubectl create secret generic <secret-name> --from-file=<iam-key.json>
```

4.5.4.4 Store secret in GCP Secret manager

```bash
gcloud secrets create <secret name> --data-file="/path/to/file"
```

4.5.4.5 Store Cert in GCP Secret manager

Certificate should be in below format before uploading cert to GCP Secret Manager i.e it should be one .pem file (key, crt and CA in one file)

(Refer "mycert.pem" for sample certificate format)

```bash
gcloud secrets create <secret name> --data-file="/path/to/file"
```

Note
Only single key value for secret to be stored in Secret Manager.

4.5.5 Installing HashiCorp Vault Provider for Secret Store CSI Driver

4.5.5.1 Install HashiCorp Provider drivers using helm chart

```bash
helm repo add hashicorp https://helm.releases.hashicorp.com
helm install vault hashicorp/vault --set "server.enabled=false" --set "injector.enabled=false" --set "csi.enabled=true"
```

4.5.5.2 Configure Kubernetes Authentication for HashiCorp Vault

```bash
vault auth enable kubernetes
vault write auth/kubernetes/config
  token_reviewer_jwt="$(cat /var/run/secrets/kubernetes.io/serviceaccount/token)"
  kubernetes_host="https://$KUBERNETES_PORT_443_TCP_ADDR:443"
  kubernetes_ca_cert="/var/run/secrets/kubernetes.io/serviceaccount/ca.crt"
```

4.5.5.3 Store Secret in HashiCorp Vault

```bash
vault kv put secret/<path> <secret name>=<secret value>
```

4.5.5.4 Store Cert in HashiCorp Vault

Certificate should be in below format before uploading cert to HashiCorp Vault i.e it should be one .pem file (key, crt and CA in one file)

(Refer "mycert.pem" for sample certificate format)
Vault kv put secret/<path> <secret name>@<path to cert.pem>

4.5.5 Create policy and role to access the secrets from HashiCorp Vault

Policy:

```bash
vault policy write <policy name> - <<EOF
path "secret/database/credentials" {
capabilities = ["read", "write", "update","delete"]
}
EOF
```

Role:

```bash
vault write auth/kubernetes/role/<role name> \
bound_service_account_names=* \
bound_service_account_namespaces=*\npolicies=<policy name> \nttl=24h
```

Note: access can be restricted by assigning <fep-cluster>-sa service account to bound_service_account_names and also can be namespace restricted by assigning value to bound_service_account_namespaces

Note

Only single key value for secret to be stored in HashiCorp vault.

4.5.6 Configuring FEPCluster to use Provider for Secret Store Driver

To enable use of Secret Store CSI driver, a new parameter "secretStore" under spec.fepChildCrVal section in the FEPCluster CR. Under secretStore.csi user should define the details to connect to external Secret store(Azure,AWS,GCP and HashiCorp Vault) and the list of secrets in that secret store. The definition of spec.fepChildCrVal.secretStore parameter will differ depending on the type of provider that is used.

4.5.6.1 Azure Provider for Secret Store CSI Driver

```yaml
spec:
    .....  
    fepChildCrVal:
        secretStore:
            method: csi
            csi:
                providerName: azure
                azureProvider:
                    keyvaultname:
                    tenantid:
                    credentials:
                        fepSecrets:
                        - pgadminpassword: pgadminpassword
                        - tdepassphrase: passphrase
                        - systemCertificates: systemCerts
                        - pguser: pgusername
                        - pgpassword: pgpwd
                        - pgdb: pgdbsecret
                        - pgrepluser: pgrepluser
                        - pgreplpassword: pgreplpassword
                        - pgRewinduser: pgRewinduser
                        - pgRewindpassword: pgRewindpassword
                        - pgmetricsusername: metricsuser
                        - pgmetricspwd: metricspwd
                        - patronitls: patronicrt
```
Note: The parameters which are in black in fepSecrets are mandatory.

4.5.6.2 AWS Provider for Secret Store CSI Driver

```yaml
spec:
  ...
  fepChildCrVal:
    secretStore:
      method: csi
      csi:
        awsProvider:
          region:
            roleName:
              fepSecrets:
                - pgadminpassword: pgadminpassword
                - tdepassphrase: passphrase
                - systemCertificates: systemCerts
                - pguser: pgusername
                - pgpassword: pgpwd
                - pgdb: pgdbsecret
                - pgrepluser: pgrepluser
                - pgreplpassword: pgreplpassword
                - pgRewinduser: pgRewinduser
                - pgRewindpassword: pgRewindpassword
                - pgmetricsusername: metricsuser
                - pgmetricspwd: metricspwd
                - patronitls: patronicrt
                - patronitlscacrt: patronica
                - postgrestls: postgrescrt
                - postgreslscacrt: postgresca
                - pgAdminTls: admincrt
                - pgAdminTlscacrt: adminca
                - pgAdminTls_privateKeyPassword: adminpvtkey
                - pgRewindUserTls: rewindcrt
                - pgRewindUserTls_lscacrt: rewindca
                - pgRewindUserTls_privateKeyPassword: rwndpvtkey
                - pgrepluserTls: replcrt
                - pgrepluserTls_lscacrt: replca
                - pgrepluserTls_privateKeyPassword: replpvtkey
                - pgMetricsUserTls: metricscrt
                - pgMetricsUserTls_lscacrt: metricsca
                - pgMetricsUserTls_privateKeyPassword: adminpvtkey
                - userName: user1
                  userCrt: user1crt
                  userCa: user1ca
                - userName: mydbuser
                  userCrt: mydbusercrt
                  userCa: mydbuserca
```

- patronitlscacrt: patronica
- postgrestls: postgrescrt
- postgreslscacrt: postgresca
- pgAdminTls: admincrt
- pgAdminTlscacrt: adminca
- pgAdminTls_privateKeyPassword: adminpvtkey
- pgRewindUserTls: rewindcrt
- pgRewindUserTls_lscacrt: rewindca
- pgRewindUserTls_privateKeyPassword: rwndpvtkey
- pgrepluserTls: replcrt
- pgrepluserTls_lscacrt: replca
- pgrepluserTls_privateKeyPassword: replpvtkey
- pgMetricsUserTls: metricscrt
- pgMetricsUserTls_lscacrt: metricsca
- pgMetricsUserTls_privateKeyPassword: adminpvtkey

fepCustomCerts:
  - userName:user1
    userCrt: user1crt
    userCa: user1ca
  - userName: mydbuser
    userCrt: mydbusercrt
    userCa: mydbuserca
Note: The parameters which are in black in fepSecrets are mandatory.

### 4.5.6.3 GCP Provider for Secret Store CSI Driver

```yaml
spec:
  fepChildCrVal:
    secretStore:
      method: csi
      csi:
        gcpProvider:
          credentials:
            fepSecrets:
              - pgadminpassword: pgadminpassword
              - tdepassphrase: passphrase
              - systemCertificates: systemCerts
              - pguser: pgusername
              - pgpassword: pgpwd
              - pgdb: pgdbsecret
              - pgrepluser: pgrepluser
              - pgreplpassword: pgreplpassword
              - pgRewinduser: pgRewinduser
              - pgRewindpassword: pgRewindpassword
              - pgmetricsusername: metricsuser
              - pgmetricspwd: metricspwd
              - patronitls: patronicrt
              - patronitlscacrt: patronica
              - postgresqltls: postgrescrt
              - postgresqltscacrt: postgresca
              - pgAdminTls: admincrt
              - pgAdminTlsacrt: adminca
              - pgAdminTls_privateKeyPassword: adminpvtkey
              - pgRewindUserTls: rewindcrt
              - pgRewindUserTlsacrt: rewindca
              - pgRewindUserTls_privateKeyPassword: rwdpvtkey
              - pgrepluserTls: replcrt
              - pgrepluserTlsacrt: replca
              - pgrepluserTls_privateKeyPassword: replpvtkey
              - pgMetricsUserTls: metricscrt
              - pgMetricsUserTlsacrt: metricsca
              - pgMetricsUserTls_privateKeyPassword: adminpvtkey
            fepCustomCerts:
              - userName:user1
                userCrt: user1crt
                userCa: user1ca
              - userName: mydbuser
                userCrt: mydbusercrt
                userCa: mydbuserca
```

Note: The parameters which are in black in fepSecrets are mandatory.
4.5.6.4 HashiCorp Vault Provider for Secret Store CSI Driver

```yaml
spec:
  fepChildCrVal:
    secretStore:
      method: csi
      csi:
        providerName: vault
        vaultProvider:
          roleName: "database"
        vaultAddress: "http://vault-url-addr:8765"
      fepSecrets:
        - pgadminpassword: pgadminpassword
        - tdepassphrase: passphrase
        - systemCertificates: systemCerts
        - pguser: pgusername
        - pgpassword: pgpwd
        - pgdb: pgdbsecret
        - pgrepluser: pgrepluser
        - pgreplpassword: pgreplpassword
        - pgRewinduser: pgRewinduser
        - pgRewindpassword: pgRewindpassword
        - pgmetricsusername: metricsuser
        - pgmetricspwd: metricspwd
        - patronitus: patronicrt
        - patronitlsacrt: patronica
        - postgreslts: postgrescrt
        - postgresltsacrt: postgresca
        - pgAdminTls: admincrt
        - pgAdminTlsacrt: adminca
        - pgAdminTls_privateKeyPassword: adminpvtkey
        - pgRewindUserTls: reprindcrt
        - pgRewindUserTlsacrt: reprindca
        - pgRewindUserTls_privateKeyPassword: rwndpvtkey
        - pgrepluserTls: reprlcrt
        - pgrepluserTlsacrt: replca
        - pgrepluserTls_privateKeyPassword: replpvtkey
        - pgMetricsUserTls: metricscrt
        - pgMetricsUserTlsacrt: metricsca
        - pgMetricsUserTls_privateKeyPassword: metrnpvtkey
      fepCustomCerts:
        - userName:user1
          userCrt: user1crt
          userCa: user1ca
        - userName: myDbuser
          userCrt: myDbusercrt
          userCa: myDbuserca
```

Note: The parameters which are in black in fepSecrets are mandatory.

4.6 Deploying a customized FEP server container image

4.6.1 Requirements

The procedures documented below assume the use of docker command to build container image. Building container images using alternative tools such as podman is beyond the scope of this document.

4.6.2 Build custom FEP image with extension

Before building a new custom FEP Server container image, it is important to understand several build instructions specific to that image.
- FEP server container image is built on top of UBI8 minimal image, ubi-minimal
- USER is default to 26

UBI8 minimal image uses microdnf as package manager. Microdnf does not support installing RPM packages from remote URL or local file, only from a YUM repository. If you want to install RPM package that is not in YUM repository, first download the package and install it with rpm. However, rpm has the drawback that it does not resolve dependencies. The only way to resolve this problem is to install dnf first and use dnf to install packages from remote URL or local file.

As USER is default to 26, it does not have the permission to install RPM packages or write files to system directory such as /usr/bin, /usr/local/bin, etc. To workaround this issue, first set USER to root to continue the customization and set it back to 26.

USER root
RUN ...(customization)
USER 26

### 4.6.3 Adding SQLite Foreign Data Wrapper to FEP Server Container

We will demonstrate adding the SQLite Foreign Data Wrapper module to FEP Server container.

1. Create Dockerfile

```bash
#use FEP 15 image as a base to compile sqlite_fdw
FROM quay.io/fujitsu/fujitsu-enterprise-postgres-15-server:ubi8-15-1.0 as compile-sqlite_fdw
#change the user with root privilege
USER root

# install build tools
RUN microdnf -y install cmake gcc-c++ libtool clang which openssl-devel git llvm gettext

# Install sqlite_fdw build require
RUN microdnf install -y sqlite-devel

# Download sqlite_fdw source
RUN curl -sSL https://github.com/pgspider/sqlite_fdw/archive/refs/tags/v2.3.0.tar.gz | tar -zxf -

# Compile sqlite_fdw
RUN cd /sqlite_fdw-2.3.0 && \
    make install USE_PGXS=1

#Use base image is from FEPContainer to build the custom image
FROM quay.io/fujitsu/fujitsu-enterprise-postgres-15-server:ubi8-15-1.0

#change the user with root privilege
USER root

#copy the prepared OSS extension binaries to FEP server lib folder
COPY --from=compile-sqlite_fdw /opt/fsepv15server64/lib/sqlite_fdw.so /opt/fsepv15server64/lib/
COPY --from=compile-sqlite_fdw /opt/fsepv15server64/lib/bitcode/sqlite_fdw /opt/fsepv15server64/lib/bitcode/
COPY --from=compile-sqlite_fdw /opt/fsepv15server64/share/extension/sqlite_fdw* /opt/fsepv15server64/share/extension/

# Install sqlite_fdw run time dependencies
RUN microdnf install -y sqlite-libs

#change the user to postgresql
USER postgresql
```
2. Build custom image

```bash
docker build -f Dockerfile -t my.registry/my-repo/fep-15-server-sqlite_fdw:ubi8-15-1.0
```

3. Push image to custom container registry

```bash
docker push my.registry/my-repo/fep-15-server-sqlite_fdw:ubi8-15-1.0
```

### 4.6.4 Create FEP Cluster with custom image

If the custom container registry requires authentication, create a pull secret with the name quay-pull-secret. FEP Operator will this pull secret to download container image.

```yaml
custom
kind: Secret
apiVersion: v1
metadata:
  name: quay-pull-secret
  namespace: fep-container-ct
data:
  .dockerconfigjson: xxxxxbCI6ICIiCiAgICB9CiAgfQp9
  type: kubernetes.io/dockerconfigjson
```

Create FEP Cluster CR

```yaml
apiVersion: fep.fujitsu.io/v2
kind: FEPCluster
metadata:
  name: sqlite-fdw
  namespace: fep-container-ct
spec:
  fep:
    forceSsl: true
    ...
  image:
  ...
  instances: 1
```

Deploy FEPCluster

```bash
oc apply -f sqlite_fdw.yaml
```

Create extension

```bash
postgres# CREATE EXTENSION sqlite_fdw;
CREATE EXTENSION
postgres=#
```

### 4.7 Configuration FEP to Perform MTLS

All three traffic can be secured by using TLS connection protected by certificates:

- Postgres traffic from Client Application to FEPCluster
- Patroni RESTAPI within FEPCluster
- Postgres traffic within FEPCluster (e.g. replication, rewind)

Here, we provide two methods to create certificates for securing the TLS connection and provide mutual authentication. The first method is to create and renew certificate manually. The second method is to use CertManager to create an automatically renew certificate.

**Note**

The following considerations apply to client connections to a database cluster in an MTLS configuration:

- Distribute the Root certificate for server (validation) that you specified when you created the MTLS database cluster to the client machines.
- Create and use a new client certificate.
- If the server root certificate and the client root certificate are different, a server-side configuration update is required.

### 4.7.1 Manual Certificate Management

**Overview of Procedures**

The procedures to enable MTLS communication are listed below:

1. Create a self signed certificate as CA
2. Create Configmap to store CA certificate
3. Create a password for protecting FEP Server private key (optional)
4. Create FEP Server private key
5. Create FEP Server certificate signing request
6. Create FEP Server certificate signed by CA
7. Create TLS Secret to store FEP Server certificate and key
8. Create private key for Patroni
9. Create certificate signing request for Patroni
10. Create certificate signed by CA for Patroni
11. Create TLS secret to store Patroni certificate and key
12. Create private key for "postgres" user client certificate
13. Create certificate signing request for "postgres" user client certificate
14. Create client certificate for "postgres" user
15. Create TLS secret to store "postgres" certificate and key
16. Repeat step 12-15 for "repluser" and "rewinduser"

**Note**

- The information in the manual is only an example, and in operation, use a certificate signed by a certificate authority (CA) that the user can trust.
- When working on a Kubernetes cluster, replace the oc command with the kubectl command.
Creating a CA Certificate

1. Create a self signed certificate as CA

```
openssl genrsa -aes256 -out myca.key 4096
Generating RSA private key, 4096 bit long modulus (2 primes)
................................................+++ ........................................................++++
e is 65537 (0x010001)
Enter pass phrase for myca.key: 0okm9ijn8uhb7ygv
Verifying - Enter pass phrase for myca.key: 0okm9ijn8uhb7ygv

cat << EOF > ca.cnf
[req]
distinguished_name=req_distinguished_name
x509_extensions=v3_ca
[v3_ca]
 basicConstraints = critical, CA:true
 keyUsage=critical,keyCertSign,digitalSignature,cRLSign
 [req_distinguished_name]
 commonName=Common Name
EOF
```

```
openssl req -x509 -new -nodes -key myca.key -days 3650 -out myca.pem -subj "/O=My Organization/OU=CA /CN=My Organization Certificate Authority" -config ca.cnf
Enter pass phrase for myca.key: 0okm9ijn8uhb7ygv
```

2. Create Configmap to store CA certificate

```
oc create configmap cacert --from-file=ca.crt=myca.pem -n my-namespace
```

3. Create a password for protecting FEP Server private key (optional)

```
oc create secret generic mydb-fep-private-key-password --from-literal=keypassword=abcdefghijk -n my-namespace
```

Creating a Server Certificate

4. Create FEP Server private key

```
openssl genrsa -aes256 -out fep.key 2048
Generating RSA private key, 2048 bit long modulus
................................................+++ ..............................................+++
e is 65537 (0x10001)
Enter pass phrase for fep.key: abcdefghijk
Verifying - Enter pass phrase for fep.key: abcdefghijk
```

5. Create FEP Server certificate signing request

```
cat << EOF > san.cnf
[SAN]
subjectAltName = @alt_names
[alt_names]
DNS.1 = *.my-namespace.pod
DNS.2 = *.my-namespace.pod.cluster.local
DNS.3 = mydb-primary-svc
DNS.4 = mydb-primary-svc.my-namespace
DNS.5 = mydb-primary-svc.my-namespace.svc
EOF
```
DNS.6 = mydb-primary-svc.my-namespace.svc.cluster.local
DNS.7 = mydb-replica-svc
DNS.8 = mydb-replica-svc.my-namespace
DNS.9 = mydb-replica-svc.my-namespace.svc
DNS.10 = mydb-replica-svc.my-namespace.svc.cluster.local
EOF

```
openssl req -new -key fep.key -out fep.csr -subj "/CN=mydb-headless-svc" -reqexts SAN -config 
<(cat /etc/pki/tls/openssl.cnf <(cat san.cnf))
Enter pass phrase for fep.key: abcdefghijk
```

---

**Note**

The cluster name and namespace must be changed appropriately.

If you are connecting from outside the OCP cluster, you must also include the host name used for that connection.

---

6. Create FEP Server certificate signed by CA

```
openssl x509 -req -in fep.csr -CA myca.pem -CAkey myca.key -out fep.pem -days 365 -extfile 
<(cat /etc/pki/tls/openssl.cnf <(cat san.cnf)) -extensions SAN -CAcreateserial # all in one line
```

Signature ok
subject=/CN=mydb-headless-svc
Getting CA Private Key
Enter pass phrase for myca.key: 0okm9iijn8uhb7ygv

7. Create TLS Secret to store FEP Server certificate and key

```
oc create secret generic mydb-fep-cert --from-file=tls.crt=fep.pem --from-file=tls.key=fep.key -n 
my-namespace
```

8. Create private key for Patroni

At the moment, FEP container does not support password protected private key for Patroni.

```
openssl genrsa -out patroni.key 2048
Generating RSA private key, 2048 bit long modulus
...............................................+++.......+++e is 65537 (0x10001)
```

9. Create certificate signing request for Patroni

```
cat << EOF > san.cnf
[SAN]
subjectAltName = @alt_names
[alt_names]
DNS.1 = *.my-namespace.pod
DNS.2 = *.my-namespace.pod.cluster.local
DNS.3 = mydb-primary-svc
DNS.4 = mydb-primary-svc.my-namespace
DNS.5 = mydb-replica-svc
DNS.6 = mydb-replica-svc.my-namespace
DNS.7 = mydb-headless-svc
DNS.8 = mydb-headless-svc.my-namespace
EOF
```

- 65 -
openssl req -new -key patroni.key -out patroni.csr -subj "/CN=mydb-headless-svc" -reqexts SAN -config <(cat /etc/pki/tls/openssl.cnf <(cat san.cnf)) # all in one line

Note

The cluster name and namespace must be changed appropriately.
If you are connecting from outside the OCP cluster, you must also include the host name used for that connection.

10. Create certificate signed by CA for Patroni

openssl x509 -req -in patroni.csr -CA myca.pem -CAkey myca.key -out patroni.pem -days 365 -extfile <(cat /etc/pki/tls/openssl.cnf <(cat san.cnf)) -extensions SAN -CAcreateserial # all in one line
Signature ok
subject=/CN=mydb-headless-svc
Getting CA Private Key
Enter pass phrase for myca.key: 0okm9ijn8uhb7ygv

11. Create TLS secret to store Patroni certificate and key

oc create secret tls mydb-patroni-cert --cert=patroni.pem --key=patroni.key -n my-namespace

Creating a User Certificate

12. Create private key for "postgres" user client certificate

At the moment, SQL client inside FEP server container does not support password protected certificate.

openssl genrsa -out postgres.key 2048
Generating RSA private key, 2048 bit long modulus
...............................................+++
.......+++ e is 65537 (0x10001)

13. Create certificate signing request for "postgres" user client certificate

openssl req -new -key postgres.key -out postgres.csr -subj "/CN=postgres"

14. Create client certificate for "postgres" user

openssl x509 -req -in postgres.csr -CA myca.pem -CAkey myca.key -out postgres.pem -days 365
Signature ok
subject=CN = postgres
Getting CA Private Key
Enter pass phrase for myca.key: 0okm9ijn8uhb7ygv

15. Create TLS secret to store "postgres" certificate and key

oc create secret tls mydb-postgres-cert --cert=postgres.pem --key=postgres.key -n my-namespace

16. Repeat step 12-15 for "repluser" and "rewinduser"
4.7.2 Automatic Certificate Management

There are many Certificate Management tools available in the public. In this example, we will use cert-manager for the purpose.

**Note**

- Note that certificates created in this example are not password protected.
- When working on a Kubernetes cluster, replace the `oc` command with the `kubectl` command.

Install `cert-manager`

```bash
oc create namespace cert-manager
oc apply -f https://github.com/jetstack/cert-manager/releases/download/v1.3.0/cert-manager.yaml
```

Create a Self Signed Issuer (This can be namespace specific or cluster wise)

This example creates an Issuer, that can create self signed certificate, in namespace my-namespace.

```bash
cat << EOF | oc apply -f -
apiVersion: cert-manager.io/v1
kind: Issuer
metadata:
  name: selfsigned-issuer
  namespace: my-namespace
spec:
  selfSigned: {}
EOF
```

Create a Self Signed CA certificate using `selfsigned-issuer`

```bash
cat << EOF | oc apply -f -
apiVersion: cert-manager.io/v1
kind: Certificate
metadata:
  name: cacert
  namespace: my-namespace
spec:
  subject:
    organizations:
    - My Organization
    organizationalUnits:
    - CA
  commonName: "My Organization Certificate Authority"
  duration: 87600h
  isCA: true
  secretName: cacert
  issuerRef:
    name: selfsigned-issuer
EOF
```

The above command will create a self signed Root certificate and private key stored in the Kubernetes secret “cacert” in namespace my-namespace.
Create a CA Issuer with above certificate

```
cat << EOF | oc apply -f -
apiVersion: cert-manager.io/v1
kind: Issuer
metadata:
  name: ca-issuer
  namespace: my-namespace
spec:
  ca:
    secretName: cacert
EOF
```

Create FEP Server certificate using above CAIssuer

Assuming FEPCluster name is mydb in namespace my-namespace.

```
cat << EOF | oc apply -f -
apiVersion: cert-manager.io/v1
kind: Certificate
metadata:
  name: mydb-fep-cert
  namespace: my-namespace
spec:
  subject:
    commonName: "mydb-headless-svc"
  dnsNames:
  - "**.my-namespace.pod"
  - "**.my-namespace.pod.cluster.local"
  - "mydb-primary-svc"
  - "mydb-primary-svc.my-namespace"
  - "mydb-primary-svc.my-namespace.svc"
  - "mydb-primary-svc.my-namespace.svc.cluster.local"
  - "mydb-replica-svc"
  - "mydb-replica-svc.my-namespace"
  - "mydb-replica-svc.my-namespace.svc"
  - "mydb-replica-svc.my-namespace.svc.cluster.local"
  duration: 8760h
usages:
  - server auth
secretName: mydb-fep-cert
issuerRef:
  name: ca-issuer
EOF
```

Create Patroni certificate using above CA Issuer

Assuming FEPCluster name is mydb in namespace my-namespace.

```
cat << EOF | oc apply -f -
apiVersion: cert-manager.io/v1
kind: Certificate
metadata:
  name: mydb-patroni-cert
  namespace: my-namespace
spec:
  subject:
    commonName: "mydb-headless-svc"
  dnsNames:
  - "**.my-namespace.pod"
  - "**.my-namespace.pod.cluster.local"
  - "mydb-primary-svc"
  - "mydb-primary-svc.my-namespace"
EOF
```
Create postgres user client certificate

```bash
cat << EOF | oc apply -f -
apiVersion: cert-manager.io/v1
kind: Certificate
metadata:
  name: mydb-postgres-cert
  namespace: my-namespace
spec:
  subject:
    commonName: "postgres"
  duration: 8760h
  usages:
    - client auth
  secretName: mydb-postgres-cert
  issuerRef:
    name: ca-issuer
EOF
```

Create repluser user client certificate

```bash
cat << EOF | oc apply -f -
apiVersion: cert-manager.io/v1
kind: Certificate
metadata:
  name: mydb-repluser-cert
  namespace: my-namespace
spec:
  subject:
    commonName: "repluser"
  duration: 8760h
  usages:
    - client auth
  secretName: mydb-repluser-cert
  issuerRef:
    name: ca-issuer
EOF
```

Create FEPLogging(Fluentd) server certificate using above CA Issuer

Assuming FEPLogging name is nfl in namespace feplogging-dev.

```bash
cat << EOF | oc apply -f -
apiVersion: cert-manager.io/v1
kind: Certificate
metadata:
  name: fluentd-cert
  namespace: feplogging-dev
spec:
EOF
```
subject:
  commonName: "nfl-fluentd-headless-service"
dnsNames:
- 'nfl-fluentd-headless-service'
- 'nfl-fluentd-headless-service.feplogging-dev'
- 'nfl-fluentd-headless-service.feplogging-dev.svc'
- 'nfl-fluentd-headless-service.feplogging-dev.svc.cluster.local'
duration: 8760h
usages:
  - server auth
secretName: fluentd-cert
issuerRef:
  name: ca-issuer

EOF

Create FEPLogging client(prometheus) certificate

```bash
cat << EOF | oc apply -f -
apiVersion: cert-manager.io/v1
kind: Certificate
metadata:
  name: prometheus-cert
  namespace: feplogging-dev
spec:
  subject:
    commonName: "prometheus"
  duration: 8760h
  usages:
    - client auth
  secretName: prometheus-cert
  issuerRef:
    name: ca-issuer
EOF
```

Create FEPLogging client(fluentbit) certificate

```bash
cat << EOF | oc apply -f -
apiVersion: cert-manager.io/v1
kind: Certificate
metadata:
  name: fluentbit-cert
  namespace: feplogging-dev
spec:
  subject:
    commonName: "fluentbit"
  duration: 8760h
  usages:
    - client auth
  secretName: fluentbit-cert
  issuerRef:
    name: ca-issuer
EOF
```

Create FEPExporter certificate using above CA Issuer

Assuming FEP Exporter name is `exp1` in namespace `my-namespace`.

```bash
cat << EOF | oc apply -f -
apiVersion: cert-manager.io/v1
kind: Certificate
metadata:
  name: exp1-cert
  namespace: my-namespace
spec:
  subject:
    commonName: "exp1"
  duration: 8760h
  usages:
    - client auth
  secretName: exp1-cert
  issuerRef:
    name: ca-issuer
EOF
```
Create FEPExporter user client(prometheus) certificate

```yaml
cat << EOF | oc apply -f -
apiVersion: cert-manager.io/v1
kind: Certificate
metadata:
  name: prometheus-cert
  namespace: my-namespace
spec:
  subject:
    commonName: "prometheus"
  duration: 8760h
  usages:
  - client auth
  secretName: prometheus-cert
  issuerRef:
    name: ca-issuer
EOF
```

4.7.3 Deploy FEPCluster with MTLS support

Deploy FEPCluster with manual certificate management

Use the following yaml as an example to deploy a FEPCluster with Manual Certificate Management. MTLS related parameters are highlighted in Red.

```yaml
apiVersion: fep.fujitsu.io/v2
kind: FEPCluster
metadata:
  name: mydb
  namespace: my-namespace
spec:
  fep:
    usePodName: true
  patroni:
    tls:
      certificateName: mydb-patroni-cert
      caName: cacert
  postgres:
    tls:
      certificateName: mydb-fep-cert
      caName: cacert
```
privateKeyPassword: mydb-fep-private-key-password
forceSsl: true
podAntiAffinity: false
mcSpec:
  limits:
    cpu: 500m
    memory: 700Mi
  requests:
    cpu: 200m
    memory: 512Mi
customAnnotations:
  allDeployments: {}
servicePort: 27500
image:
pullPolicy: IfNotPresent
sysExtraLogging: false
podDisruptionBudget: false
instances: 3
syncMode: 'on'
fepChildCrVal:
customPgAudit:
  # define pg audit custom params here to override defaults.
  # if log volume is not defined, log_directory should be
  # changed to '/database/userdata/data/log'
  [output]
  logger = 'auditlog'
  log_directory = '/database/log/audit'
  [rule]
  # define pg_hba custom rules here to be merged with default rules.
  # TYPE     DATABASE        USER        ADDRESS        METHOD
  hostssl all all 0.0.0.0/0 cert
  hostssl replication all 0.0.0.0/0 cert
customPgParams:
  # define custom postgresql.conf parameters below to override defaults.
  # Current values are as per default FEP deployment
  shared_preload_libraries='pgx_datamasking,vci,pgaudit,pg_prewarm'
  session_preload_libraries='vci,pg_prewarm'
  max_prepared_transactions = 100
  max_worker_processes = 30
  max_connections = 100
  work_mem = 1MB
  maintenance_work_mem = 12MB
  shared_buffers = 128MB
  effective_cache_size = 384MB
  checkpoint_completion_target = 0.8
  # tcp parameters
  tcp_keepalives_idle = 30
  tcp_keepalives_interval = 10
  tcp_keepalives_count = 3
  # logging parameters in default fep installation
  # if log volume is not defined, log_directory should be
  # changed to '/database/userdata/data/log'
  log_directory = '/database/log'
  log_filename = 'logfile-%a.log'
  log_file_mode = 0600
  log_rotation_on_rotation = on
  log_rotation_age = 1d
  log_rotation_size = 0
  log_checkpoints = on
log_line_prefix = '%e %t [%p]: [%l-1] user=%u,db=%d,app=%a,client=%h'
log_lock_waits = on
log_autovacuum_min_duration = 60s
logging_collector = on
pgaudit.config_file='/opt/app-root/src/pgaudit-cfg/pgaudit.conf'
log_replication_commands = on
log_min_messages = WARNING
log_destination = stderr

# vci parameters in default fep installation
vci.enable = on
vci.maintenance_work_mem = 256MB
vci.max_local_ros = 64MB
vci.force_max_parallelism = off

# wal_archive parameters in default fep installation
archive_mode = on
archive_command = '/bin/true'
wal_level = replica
max_wal_senders = 12
wal_keep_segments = 64

storage:
dataVol:
  size: 2Gi
  storageClass: nfs-client
walVol:
  size: 1200Mi
  storageClass: nfs-client
logVol:
  size: 1Gi
  storageClass: nfs-client

sysUsers:
pgAdminPassword: admin-password
pgdb: mydb
pgpassword: mydbpassword
pguser: mydbuser
pgrepluser: repluser
pgreplpassword: repluserpwd
pgRewindUser: rewinduser
pgRewindPassword: rewinduserpwd

pgAdminTls:
  certificateName: mydb-postgres-cert
  caName: cacert
  sslMode: prefer

pgrepluserTls:
  certificateName: mydb-repluser-cert
  caName: cacert
  sslMode: prefer

pgRewindUserTls:
  certificateName: mydb-rewinduser-cert
  caName: cacert
  sslMode: prefer

tdepassphrase: tde-passphrase

systemCertificates:

key: |-
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA0DFkImha8CIJjVcwXbBPlL+/DmS9/6pRhQQHxfO5x7jSOonse
IHdFde+Gx8XKAlAhVykf6kfacwBYTATU1xDgwWTm82KVRPh+k2Dj2wPCjrl4m
mTP6l6aZmavUgDhezHc9F8/dchYj3cw81X0kU6xamqzKQY1xQd48NkI0qcwhO6aK

---BEGIN RSA PRIVATE KEY-----
Deploy FEPCluster with automatic certificate management

Use the following yaml as an example to deploy a FEPCluster with Automatic Certificate Management. MTLS related parameters are highlighted in Red.

```yaml
apiVersion: fep.fujitsu.io/v2
kind: FEPCluster
metadata:
  name: mydb
  namespace: my-namespace
spec:
  fep:
    usePodName: true
  patroni:
    tls:
      certificateName: mydb-patroni-cert
  postgres:
    tls:
      certificateName: mydb-fep-cert
    forceSsl: true
    podAntiAffinity: false
  mcSpec:
    limits:
      cpu: 500m
      memory: 700Mi
    requests:
      cpu: 200m
      memory: 512Mi
  customAnnotations:
    allDeployments: {}
  servicePort: 27500
  image:
    pullPolicy: IfNotPresent
  sysExtraLogging: false
  podDisruptionBudget: false
  instances: '3'
  syncMode: 'on'
  fepChildCrVal:
    customPgAudit:
      # define pg audit custom params here to override defaults.
      # if log volume is not defined, log_directory should be changed to '/database/userdata/data/log'
      # [output]
      logger = 'auditlog'
      log_directory = '/database/log/audit'
      # [rule]
      customPgHba:
        # define pg_hba custom rules here to be merged with default rules.
        # TYPE DATABASE USER ADDRESS METHOD
        hostssl all all 0.0.0.0/0 cert
        hostssl replication all 0.0.0.0/0 cert
      customPgParams:
        # define custom postgresql.conf parameters below to override defaults.
        # Current values are as per default FEP deployment
        shared_preload_libraries='pgx_datamasking, vci, pgaudit, pg_prewarm'
        session_preload_libraries='vci, pg_prewarm'
```

--- END CERTIFICATE ---
max_prepared_transactions = 100
max_worker_processes = 30
max_connections = 100
work_mem = 1MB
maintenance_work_mem = 12MB
shared_buffers = 128MB
effective_cache_size = 384MB
checkpoint_completion_target = 0.8

# tcp parameters
tcp_keepalives_idle = 30
tcp_keepalives_interval = 10
tcp_keepalives_count = 3

# logging parameters in default fep installation
# if log volume is not defined, log_directory should be changed to '/database/userdata/data/log'
log_directory = '/database/log'
log_filename = 'logfile-%a.log'
log_file_mode = 0600
log_truncate_on_rotation = on
log_rotation_age = 1d
log_rotation_size = 0
log_checkpoints = on
log_line_prefix = '%e %t [%p]: [%l-1] user=%u, db=%d, app=%a, client=%h'
log_lock_waits = on
log_autovacuum_min_duration = 60s
logging_collector = on
pgaudit.config_file='/opt/app-root/src/pgaudit-cfg/pgaudit.conf'
log_replication_commands = on
log_min_messages = WARNING
log_destination = stderr

# vci parameters in default fep installation
vci.enable = on
vci.maintenance_work_mem = 256MB
vci.max_local_ros = 64MB
vci.force_max_parallelism = off

# wal_archive parameters in default fep installation
archive_mode = on
archive_command = '/bin/true'
wal_level = replica
max_wal_senders = 12
wal_keep_segments = 64

storage:
dataVol:
  size: 2Gi
  storageClass: nfs-client
walVol:
  size: 1200Mi
  storageClass: nfs-client
logVol:
  size: 1Gi
  storageClass: nfs-client
sysUsers:
  pgAdminPassword: admin-password
  pgdb: mydb
  pgpassword: mydbpassword
  pguser: mydbuser
  pgrepluser: repluser
pgreplpassword: repluserpwd
pgRewindUser: rewinduser
pgRewindPassword: rewinduserpwd
pgAdminTls:
certificateName: mydb-postgres-cert
sslMode: verify-full
pgrepluserTls:
certificateName: mydb-repluser-cert
sslMode: verify-full
pgRewindUserTls:
certificateName: mydb-rewinduser-cert
sslMode: verify-full
tdepassphrase: tde-passphrase
systemCertificates:
crt: |-
-----BEGIN CERTIFICATE-----
MIID2DCCAsCgAwIBAgIQDfFYteD4kZj4Sko2iy1IJTANBgkqhkiG9w0BAQsFADBX
MRgwFqYDVQQKEw9NeSBPcmdhbml6YXRpb24gQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4X
DTIxMDQyMDAwMDQ1OVoXDTIxMDQyMDAxMDQ1OVowGDEWMBQGA1UEAwwNKi5jaGctcHRj
LmxvY2FsghMqLm15ZGItaGVhZGxlc3Mtc3ZjghsqLm15ZGItaGVhZGxlc3Mtc3Zjghsq
LmNoZy1wdGOCHyoubXlkYi1oZWFkbGVzcy1zdmMuY2hnLXB0Yy5zdmOCLSoubXlkYi1o
ZWFkbGVzcy1zdmMuY2x1c3Rlci5sb2NhbDANBgkqhkiG9w0BAQsFAAOCAQEALEnhliDflu+BHp5conq4dXBwD/Ti2YR5TWQixM/0a6OD4KecZ
-----END CERTIFICATE-----
### 4.7.4 Configurable Parameters

To enable MTLS, make changes to the following parameters.

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>spec.fep.usePodName</td>
<td>True</td>
<td>For MTLS, this key must be defined and set to true. For TLS connection without MTLS, it can be omitted. However, it is recommended to set this to true as well.</td>
</tr>
<tr>
<td>spec.fep.patroni.tls.certificateName</td>
<td>&lt;secret-name&gt;</td>
<td>Name of Kubernetes secret that contains the certificate in tls.crt and private key in tls.key for Patroni REST API. For MTLS Patroni REST API communication, this key must be defined. The private key cannot be password protected. When using cert-manager, the secret also contains the CA bundle in ca.crt.</td>
</tr>
<tr>
<td>spec.fep.patroni.tls.caName</td>
<td>&lt;configmap-name&gt;</td>
<td>Name of Kubernetes secret that contains the certificate in tls.crt and private key in tls.key for Postgres</td>
</tr>
<tr>
<td>Key</td>
<td>Value</td>
<td>Details</td>
</tr>
<tr>
<td>-----</td>
<td>-------</td>
<td>---------</td>
</tr>
<tr>
<td>server. For MTLS Postgres communication, this key must be defined. The private key can be password protected. When using cert-manager, the secret also contains the CA bundle in ca.crt.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>spec.fep.postgres.tls.caName</td>
<td>&lt;configmap-name&gt;</td>
<td>Name of Kubernetes configmap that contains the CA bundle. If using cert-manager, the ca.crt is already included in the secret above. In this situation, this key can be omitted.</td>
</tr>
<tr>
<td>spec.fep.postgres.tls.privateKeyPassword</td>
<td>&lt;secret-name&gt;</td>
<td>Name of Kubernetes secret that contains the password for the private key for Postgres Server.</td>
</tr>
<tr>
<td>spec.fepChildCrVal.sysUsers.pgAdminTls.certificateName</td>
<td>&lt;secret-name&gt;</td>
<td>Name of Kubernetes secret that contains the certificate in tls.crt and private key in tls.key for &quot;postgres&quot; user. For MTLS Postgres communication, this key must be defined. The private key cannot be password protected. When using cert-manager, the secret also contains the CA bundle in ca.crt.</td>
</tr>
<tr>
<td>spec.fepChildCrVal.sysUsers.pgAdminTls.caName</td>
<td>&lt;configmap-name&gt;</td>
<td>Name of Kubernetes configmap that contains the CA bundle. If using cert-manager, the ca.crt is already included in the secret above. In this situation, this key can be omitted.</td>
</tr>
<tr>
<td>spec.fepChildCrVal.sysUsers.pgAdminTls.sslMode</td>
<td>verify-full</td>
<td>For MTLS, this value must be set to verify-full. If only TLS is required, this can be set to verify-ca or prefer.</td>
</tr>
<tr>
<td>spec.fepChildCrVal.sysUsers.pgrepluserTls.certificateName</td>
<td>&lt;secret-name&gt;</td>
<td>Name of Kubernetes secret that contains the certificate in tls.crt and private key in tls.key for &quot;repluser&quot; user. For MTLS Postgres communication, this key must be defined. The private key cannot be password protected. When using cert-manager, the secret also contains the CA bundle in ca.crt.</td>
</tr>
<tr>
<td>spec.fepChildCrVal.sysUsers.pgrepluserTls.caName</td>
<td>&lt;configmap-name&gt;</td>
<td>Name of Kubernetes configmap that contains the CA bundle. If using cert-manager, the ca.crt is already included in the secret above. In this situation, this key can be omitted.</td>
</tr>
<tr>
<td>spec.fepChildCrVal.sysUsers.pgrepluserTls.sslMode</td>
<td>verify-full</td>
<td>For MTLS, this value must be set to verify-full. If only TLS is required, this can be set to verify-ca or prefer.</td>
</tr>
<tr>
<td>Key</td>
<td>Value</td>
<td>Details</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>spec.fepChildCrVal.sysUsers.pgRewindUserTls.certificateName</td>
<td>&lt;secret-name&gt;</td>
<td>Name of Kubernetes secret that contains the certificate in tls.crt and private key in tls.key for “rewinduser” user. For MTLS Postgres communication, this key must be defined. The private key cannot be password protected. When using cert-manager, the secret also contains the CA bundle in ca.crt.</td>
</tr>
<tr>
<td>spec.fepChildCrVal.sysUsers.pgRewindUserTls.caName</td>
<td>&lt;configmap-name&gt;</td>
<td>Name of Kubernetes configmap that contains the CA bundle. If using cert-manager, the ca.crt is already included in the secret above. In this situation, this key can be omitted.</td>
</tr>
<tr>
<td>spec.fepChildCrVal.sysUsers.pgRewindUserTls.sslMode</td>
<td>verify-full</td>
<td>For MTLS, this value must be set to verify-full. If only TLS is required, this can be set to verify-ca or prefer.</td>
</tr>
</tbody>
</table>

It is also required to customize pg_hba.conf to perform MTLS. Below are two possible settings.

```
| spec.fep.customPgHba     | hostssl all 0.0.0.0/0 cert
|                          | hostssl replication all 0.0.0.0/0 cert
```

The above setting will force FEP server to perform certification authentication. At the same time verify the authenticity of client certificate.

```
| spec.fep.customPgHba     | hostssl all 0.0.0.0/0 md5 clientcert=verify-full
|                          | hostssl replication repluser 0.0.0.0/0 md5 clientcert=verify-full
```

The above setting will force FEP server to perform md5 authentication as well as verifying the authenticity of client certificate.

### 4.8 Replication Slots

#### 4.8.1 Setting Up Logical Replication using MTLS

This section describes setup of logical replication.

To setup logical replication using MTLS, follow these steps:

1. Create two FEPClusters - to act as Publisher and Subscriber) and ensure that they can communicate with each other. You can see the creation of FEPCluster in the "4.1 Deploying FEPCluster using Operator".
2. To setup Publisher, make following changes to the FEPCluster yaml of the cluster that you want to use as publisher:

a. Add section replicationSlots under spec.fep to create replication slots.

   The "database" should be the name of the database for which we are setting up logical replication.

   ```yaml
   spec:
   fep:
     forceSel: true
     replicationSlots:
       myslot1:
         type: logical
database: db1
plugin: pgoutput
myslot2:
  type: logical
database: db1
plugin: pgoutput
podAntiAffinity: false
   ```

b. Add section postgres under spec.fep as shown below.

   caName = enter the name of configmap created for the CA

certificateName = secret created by the end user that contains server certificate

   ```yaml
   customAnnotations:
   allDeployments: {}  
   servicePort: 27500
   postgres:
   tls:
   caName: cacert
certificateName: my-fep-cert
   ```

c. Change the value of wal_level parameter under spec.fepChildCrVal.customPgParams from replica to logical.

   ```yaml
   wal_level = logical
   ```

d. Add entry under spec.fepChildCrVal.customPgHba as shown below.

   This requires the client to present a certificate and only certificate authentication is allowed.

   Replace "SubClusterName" and "SubNamespace" with the appropriate values as per the Subscriber FEPCluster.

   ```yaml
   [rule]
cestname = all
  ```
3. To setup Subscriber, make following changes to the FEPCluster yaml of the cluster that you want to use as subscriber:
   a. Add customCertificates under spec.fepChildCrVal as shown below.

   caName = enter the name of configmap created for the CA (i.e. The CA certificate which is used to sign/authenticate the server/client certificates is mounted as a configMap called ‘cacert’)

   certificateName = secret created by end user that contains a client certificate which can be verified by the server

   username = name of the role created on publisher cluster for logical replication

4. Connect to the pod terminal of the Publisher FEPCluster and then connect to the postgres database as shown below.

5. Next, on the publisher side, connect to the database that contains the tables you want to replicate and create a role e.g., logicalrepluser and give the required permissions to this role.

   Consider the below image as example only, the privileges to grant may differ as per the requirements.

6. At the Publisher side, create a publication and alter the publication to add the tables that need to be replicated.
7. At the subscriber side, the custom certificates added in the above step 3.a will be mounted at the path /tmp/custom_certs/ as shown:

```
sh-4.4$ ls -rlt /tmp/custom_certs
total 0
drwxr-xr-t. 3 1001190000 root 10 18 10:08 logicalrepluser
sh-4.4$ ls -rlt /tmp/custom_certs/logicalrepluser
total 0
lrwxrwxrwx. 1 1001190000 root 10 18 10:08 tls.key -> ..data/tls.key
sh-4.4$
```

8. The structure of the table to be replicated should be present in the subscriber cluster since logical replication only replicates the data and not the table structure.

Create a subscription as shown below:

```
doi-4# CREATE SUBSCRIPTION my_subscription CONNECTION 'host=fepcluster-publisher-primary-svc.ns-a.svc.cluster.local port=27500 sslcert=/tmp/custom_certs/logicalrepluser/tls.crt sslkey=/tmp/custom_certs/logicalrepluser/tls.key sslrootcert=/tmp/custom_certs/logicalrepluser/ca.crt sslmode=verify-full password=my_password user=logicalrepluser dbname=db1' PUBLICATION my_publication WITH (slot_name=myslot1, create_slot=false);
```

The command in the above example is:

```
CREATE SUBSCRIPTION my_subscription CONNECTION 'host=fepcluster-publisher-primary-svc.ns-a.svc.cluster.local port=27500 sslcert=/tmp/custom_certs/logicalrepluser/tls.crt sslkey=/tmp/custom_certs/logicalrepluser/tls.key sslrootcert=/tmp/custom_certs/logicalrepluser/ca.crt sslmode=verify-full password=my_password user=logicalrepluser dbname=db1' PUBLICATION my_publication WITH (slot_name=myslot1, create_slot=false);
```

Where
- Host = primary service of the publisher FEP Cluster
- sslcert, sslkey, sslrootcert = path to certificates mounted on the Subscriber FEP Cluster
- user= Role created on the Publisher side
- password= password for the role
- dbname= database which contains the tables to be replicated

```
CREATE SUBSCRIPTION
```

4.9 FEP Logging

FEP Cluster generates log files and auditlog files, if configured, over the lifetime of execution. These log files can be useful for understanding cluster healthiness and debugging purpose. By default, the log files are stored on persistent volume of the container. User can enable log monitoring feature by forwarding those log files and auditlog files to a analytics platform such as Elasticsearch.

There are two steps to enable monitoring and forwarding.

1. FEPLogging Configuration - Creating FEP Logging instance
2. FEPCluster configuration - Enabling logging in FEPCluster

The FEP Logging instance is a standalone container running fluentd. It accepts log forwarded from FEP Clusters and aggregate data according to log entries severity and present that to Prometheus for monitoring and alerting purpose. It can optionally be configured to forward those logs to an Elasticsearch instance for detail analysis.
When logging is enabled on FEPCluster, a sidecar, containing fluentbit, will be deployed alongside the FEP server container. This fluentbit sidecar will monitor the FEP server log files and auditlog files on persistent volume and forward to the FEP Logging instance.

Multiple FEPClusters can forward logs to single FEPLogging instance.

User can have two types of connection between FEPCluster & FEPLogging

- Insecure connection: Without TLS/MTLS certificates
- Secure connection: With TLS/MTLS certificates

For the secure connections between the components, User have two options:

- User can use their own certificates
- User can generate self signed certificates (see "4.7.2 Automatic Certificate Management")

The FEP Logging instance can run standalone without additional component. For detail log analysis, the user can configure the FEP Logging instance to forward logs to Elastic Stack or Elastic Cloud. Please consult the Elastic Document on how to deploy a Elastic Stack or sign up to Elastic Cloud.

### 4.9.1 FEPLogging Configuration

This section describes how to deploy and configure FEP Logging instance via the FEPLogging custom resource. FEPLogging is a separate CR which will accept logs sent from FEPCluster and forwards them to Elasticsearch or Prometheus for raising alarm. User must create FEPLogging CR before enabling FEPCluster logging feature.

#### 4.9.1.1 FEPLogging Custom Resources - spec

The fepLogging section needs to be added under spec to define required parameters for FEPLogging configuration.

Following is a sample template:

```yaml
spec:
  fepLogging:
    elastic:
      authSecret:
        secretName: elastic-auth
        passwordKey: password
        userKey: username
        host: elastic-passthrough.apps.openshift.com
        logstashPrefix: postgres
        port: 443
        scheme: https
        sslVerify: true
        tls:
          certificateName: elastic-cert
          caName: elastic-cacert
      image:
        pullPolicy: IfNotPresent
    mcSpec:
      limits:
        cpu: 500m
        memory: 700Mi
      requests:
        cpu: 200m
        memory: 512Mi
      restartRequired: false
      sysExtraLogging: false
      scrapeInterval: 30s
      scrapeTimeout: 30s
      tls:
        certificateName: fluentd-cert
        caName: cacert
```
Below is the list of all parameters defined in the fepLogging section, along with their brief description:

<table>
<thead>
<tr>
<th>Custom Resource spec</th>
<th>Required/Optional</th>
<th>Change Effect</th>
<th>Updating value allowed</th>
</tr>
</thead>
<tbody>
<tr>
<td>spec.fepLogging.image.image</td>
<td>Optional</td>
<td>Fluentd Image of FEPLogging</td>
<td>Yes</td>
</tr>
<tr>
<td>spec.fepLogging.image.pullPolicy</td>
<td>Required</td>
<td>Fluentd Image pull policy of FEPLogging</td>
<td>Yes</td>
</tr>
<tr>
<td>spec.fepLogging.mcSpec.limits.cpu</td>
<td>Required</td>
<td>Max CPU allocated to fluentd container</td>
<td>Yes</td>
</tr>
<tr>
<td>spec.fepLogging.mcSpec.limits.memory</td>
<td>Required</td>
<td>Max memory allocated to fluentd container</td>
<td>Yes</td>
</tr>
<tr>
<td>spec.fepLogging.mcSpec.requests.cpu</td>
<td>Required</td>
<td>CPU allocation at start for fluentd container</td>
<td>Yes</td>
</tr>
<tr>
<td>spec.fepLogging.mcSpec.requests.memory</td>
<td>Required</td>
<td>Memory allocation at start for fluentd container</td>
<td>Yes</td>
</tr>
<tr>
<td>spec.fepLogging.sysExtraLogging</td>
<td>Required</td>
<td>To turn on extra debugging messages for operator, set value to true. It can be turned on/off at any time</td>
<td>Yes</td>
</tr>
<tr>
<td>spec.fepLogging.restartRequired</td>
<td>Required</td>
<td>To restart FEPLogging instance for applying any new configuration for example after certificate rotation</td>
<td>Yes</td>
</tr>
<tr>
<td>spec.fepLogging.scrapeInterval</td>
<td>Optional</td>
<td>Scrape interval for Prometheus to fetch metrics from FEPLogging instance</td>
<td>Yes</td>
</tr>
<tr>
<td>spec.fepLogging.scrapeTimeout</td>
<td>Optional</td>
<td>Scrape Timeout for Prometheus to fetch metrics from FEPLogging instance</td>
<td>Yes</td>
</tr>
<tr>
<td>spec.fepLogging.elastic.host</td>
<td>Optional</td>
<td>Target Elasticsearch host name</td>
<td>Yes</td>
</tr>
<tr>
<td>spec.fepLogging.elastic.port</td>
<td>Optional</td>
<td>Target Elasticsearch port number</td>
<td>Yes</td>
</tr>
<tr>
<td>spec.fepLogging.elastic.authSecret.secretName</td>
<td>Optional</td>
<td>Secret name which contains Elasticsearch authentication username &amp; password</td>
<td>Yes</td>
</tr>
<tr>
<td>spec.fepLogging.elastic.authSecret.userKey</td>
<td>Optional</td>
<td>Username key specified in Elasticsearch authentication secret</td>
<td>Yes</td>
</tr>
<tr>
<td>spec.fepLogging.elastic.authSecret.passwordKey</td>
<td>Optional</td>
<td>Password key specified in Elasticsearch authentication secret</td>
<td>Yes</td>
</tr>
<tr>
<td>spec.fepLogging.elastic.logstashPrefix</td>
<td>Optional</td>
<td>Logstash prefix to differentiate index pattern in Elasticsearch. Default value is postgres</td>
<td>Yes</td>
</tr>
<tr>
<td>spec.fepLogging.elastic.auditLogstashPrefix</td>
<td>Optional</td>
<td>Logstash prefix to differentiate index pattern in Elasticsearch for auditlog. If not specified, it will default to the same value as ‘logstashPrefix’.</td>
<td>Yes</td>
</tr>
<tr>
<td>spec.fepLogging.elastic.scheme</td>
<td>Optional</td>
<td>Connection scheme between FEPLogging &amp; Elasticsearch. Possible options http &amp; https</td>
<td>Yes</td>
</tr>
<tr>
<td>spec.fepLogging.elastic.sslVerify</td>
<td>Optional</td>
<td>Set to true if you want to verify ssl certificate. If set to false then will not consider TLS certificate</td>
<td>Yes</td>
</tr>
<tr>
<td>spec.fepLogging.elastic.tls.certificateName</td>
<td>Optional</td>
<td>Kubernetes secret name which holds fluentd certificate</td>
<td>Yes</td>
</tr>
<tr>
<td>spec.fepLogging.elastic.tls.caName</td>
<td>Optional</td>
<td>Kubernetes configmap which holds cacert of Elasticsearch to verify Elasticsearch TLS connection</td>
<td>Yes</td>
</tr>
<tr>
<td>Custom Resource spec</td>
<td>Required/Optional</td>
<td>Change Effect</td>
<td>Updating value allowed</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------</td>
<td>--------------------------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>spec.fepLogging.tls.certificateName</td>
<td>Optional</td>
<td>Kubernetes secret name which holds Fluentd certificate</td>
<td>Yes</td>
</tr>
<tr>
<td>spec.fepLogging.tls.caName</td>
<td>Optional</td>
<td>Kubernetes configmap which holds cacert of Fluentd to configure MTLS between FEPLogging &amp; Prometheus</td>
<td>Yes</td>
</tr>
<tr>
<td>spec.prometheus.tls.certificateName</td>
<td>Optional</td>
<td>Kubernetes secret name which holds Prometheus certificate</td>
<td>Yes</td>
</tr>
<tr>
<td>spec.prometheus.tls.caName</td>
<td>Optional</td>
<td>Kubernetes configmap which holds cacert of Fluentd to configure MTLS between FEPLogging &amp; Prometheus</td>
<td>Yes</td>
</tr>
</tbody>
</table>

4.9.1.1.1 Define fepLogging image

The image property is used to specify other than default Fluentd image and it’s pullPolicy from FEPLogging CR.

If not specified it will use default image provided by Operator.

Example)
```
spec:
  fepLogging:
    image:
      image: 'quay.io/fujitsu/fujitsu-enterprise-postgres-fluentbit:ubi8-15-1.0'
      pullPolicy: IfNotPresent
```

4.9.1.1.2 Define fepLogging mcSpec

FEPLogging container Memory & CPU configuration can be provided by mcSpec properties.

Example)
```
spec:
  fepLogging:
    mcSpec:
      limits:
        cpu: 500m
        memory: 700Mi
      requests:
        cpu: 200m
        memory: 512Mi
```

4.9.1.1.3 Define fepLogging restartRequired

If FEPLogging required to be restarted to apply any new change, for example, after certificate rotation, FEPLogging container can be restarted by setting restartRequired flag as true. Default value of this flag is False. This flag will change back to false once the pod is restarted.

Example)
```
spec:
  fepLogging:
    restartRequired: true
```
4.9.1.1.4 Define fepLogging scrapeInterval and scrapeTimeout

scrapeInterval and scrapeTimeout properties of FEPLogging are optional. These properties are used by Prometheus Servicemonitor to configure metrics fetching interval(scrapeInterval) and timeout of request.

Example)

```yaml
spec:
  fepLogging:
    scrapeInterval: 30s
    scrapeTimeout: 30s
```

4.9.1.1.5 Define fepLogging elastic

To forward logs from FEPLogging(Fluentd) to Elasticsearch, need to configure elastic property. This is optional property. Elasticsearch server and certificates will be configured by user.

To configure log forwarding to Elasticsearch, the following properties are required.

- authSecret
- host
- port
- logstashPrefix
- auditLogstashPrefix
- scheme
- sslVerify
- tls(if sslVerify set to true)

Configure Elasticsearch server and use it’s host name and port.

Here tls property is optional and works with sslVerify flag. To enable secure connection and tls verification set sslVerify true and provide valid certificateName & caName.

Elasticsearch caName is mandatory which holds CA cert of elastic search server.

Example)

```yaml
spec:
  fepLogging:
    elastic:
      authSecret:
        passwordKey: password
        secretName: elastic-auth
        userKey: username
      host: elastic-passthrough.apps.openshift.com
      logstashPrefix: postgres
      auditLogstashPrefix: postgres
      port: 443
      scheme: https
      sslVerify: false
      tls:
        certificateName: fluentd-cert
        caName: elastic-cacert
```

4.9.1.1.6 Define authSecret for elastic

authSecret is the secret which contains username & password in base64 format for elastic search authentication
4.9.1.1.7 Define fepLogging TLS

FEPLogging has optional TLS property. If user wants to forward logs from FEPCluster to FEPLogging instance over a secure connection, the TLS configuration for FEPCluster(remoteLogging section) and the TLS configuration for FEPLogging and Prometheus are mandatory. Configuring TLS configuration on just fepLogging or Prometheus will not work.

When a self signed certificate is used, caName can be skipped.

Example)

```yaml
spec:
  fepLogging:
    tls:
      certificateName: fluentd-cert
      caName: cacert
```

4.9.1.1.8 Define Prometheus TLS

If secured connection between FEPLogging and FEPCluster is required, then TLS configuration for FEPLogging and Prometheus are mandatory. Configuring TLS on just fepLogging or Prometheus will not work.

When a self signed certificate is used, caName can be skipped.

Example)

```yaml
spec:
  fepLogging:
    ...  
  prometheus:
    tls:
      certificateName: prometheus-cert
      caName: cacert
```

4.9.2 FEPCluster Configuration

This section describes how to enable logging in FEPCluster. FEP cluster provides a feature to forward logs to remote Fluentd(FEPLogging) and FEPLogging instance will forward the same logs to Elasticsearch(Optional) & Prometheus.

4.9.2.1 FEP Custom Resources - spec.fep.remoteLogging

The remoteLogging section needs to be added under fep to define required parameters for remoteLogging configuration.

Following is a sample template:

```yaml
spec:
  fep
  ...
remoteLogging:
  enable: true
  fluentdName: new-fep-logging
tls:
    certificateName: fluentbit-cert
caNMe: cacert
...

Below is the list of all parameters defined in the remoteLogging section, along with their brief description:

<table>
<thead>
<tr>
<th>Custom Resource spec</th>
<th>Required/Optional</th>
<th>Change Effect</th>
<th>Updating value allowed</th>
</tr>
</thead>
<tbody>
<tr>
<td>remoteLogging.enable</td>
<td>Required</td>
<td>The ‘enable’ is set to true for enabling Logging feature</td>
<td>No</td>
</tr>
<tr>
<td>remoteLogging.fluentdName</td>
<td>Required</td>
<td>The ‘fluentdName’ is the name of the FEPLogging CR where logs will be forwarded</td>
<td>Yes</td>
</tr>
<tr>
<td>remoteLogging.tls.secretName</td>
<td>Optional</td>
<td>Secret name which contains MTLS certs of fluentbit</td>
<td>No</td>
</tr>
<tr>
<td>remoteLogging.tls.caName</td>
<td>Optional</td>
<td>Cacert of Fluentd for ssl verification</td>
<td>No</td>
</tr>
<tr>
<td>remoteLogging.image</td>
<td>Optional</td>
<td>Fluentbit image for remoteLogging</td>
<td>Yes</td>
</tr>
<tr>
<td>remoteLogging.pullPolicy</td>
<td>Optional</td>
<td>Fluentbit image pull policy</td>
<td>Yes</td>
</tr>
<tr>
<td>remoteLogging.mcSpec.limits.cpu</td>
<td>Optional</td>
<td>CPU allocation limit for fluentbit</td>
<td>Yes</td>
</tr>
<tr>
<td>remoteLogging.mcSpec.limits.memory</td>
<td>Optional</td>
<td>Memory allocation limit for fluentbit</td>
<td>Yes</td>
</tr>
<tr>
<td>remoteLogging.mcSpec.requests.cpu</td>
<td>Optional</td>
<td>CPU allocation request for fluentbit</td>
<td>Yes</td>
</tr>
<tr>
<td>remoteLogging.mcSpec.requests.memory</td>
<td>Optional</td>
<td>Memory allocation request for fluentbit</td>
<td>Yes</td>
</tr>
<tr>
<td>remoteLogging.fluentbitParam.s.memBufLimit</td>
<td>Optional</td>
<td>Defines the Mem_Buf Limit in Fluentbit. This will affect all sections that use this parameter</td>
<td>Yes</td>
</tr>
</tbody>
</table>

4.9.2.1.1 Define remoteLogging enable and fluentdName

The enable flag is used to describe that FEPCluster will enable log monitoring feature if set as true.

If enable flag set as true then fluentdName is the mandatory field. It will describe the FEPLogging CR name to which FEPCluster will forwards the logs.

If the enable flag is set as false, the FEPCluster will not enable logging feature.

Example

```yaml
fep:
  remoteLogging:
    enable: true
    fluentdName: new-fep-logging
```

If user wants to update existing FEPCluster with log monitoring feature then FEPCluster log_destination configuration must be set as csvlogs. For new cluster it will be already set.

Example

```yaml
fep:
  ... # Old configuration
  remoteLogging:
    enable: true
    fluentdName: new-fep-logging
```
4.9.2.1.2 Define remoteLogging tls

When FEPCluster uses secure connection for remoteLogging, then TLS section is mandatory.

In the TLS section, provide the secret name that contains certificate and private key that is used for ssl verification.

For MTLS connection caName is required to mutually validate certificate.

Example)

```yaml
fep:
  remoteLogging:
    enable: true
    fluentdName: new-fep-logging
    tls:
      certificateName: fluentbit-cert-secret
      caName: ca-cert
```

**Note**

The Elasticsearch server is configured by user and it is NOT part of FEPLogging deployment by operator.

4.9.2.1.3 Define remoteLogging image

The image property is used to specify other than default Fluentbit image and it’s pullPolicy.

If not specified it will use default image provided by Operator.

Example)

```yaml
spec:
  fep:
    remoteLogging:
      image: 'quay.io/fujitsu/fujitsu-enterprise-postgres-fluentbit:ubi8-15-1.0'
      pullPolicy: IfNotPresent
```

4.9.3 FEPLogging Operations

4.9.3.1 Log Forwarding to Elasticsearch

If the user has provided Elasticsearch configuration in the FEPLogging CR, and FEPCluster is configured to send server log files and auditlog files to that FEPLogging instance, those logs will be visible on Elasticsearch stack or Elastic Cloud. Assuming Elasticsearch has been configured with Kibana then logs will be visible in Kibana Dashboard. User can use fep log csv fields to create various Dashboard in Kibana as well. LogstashPrefix and auditLogstashPrefix will be used to filter logs of specific FEPLogging instance.

User can verify if FEPLogging feature is configured properly or not by checking real time FEP logs are populating to the destination.
4.9.3.2 Log severity based Alarms/Metrics

FEPLogging feature is used for raising alarm/alert based on postgres severity counts as well. While user creates FEPLogging CR, Operator will forward real-time counts of various postgres severity metrics to Openshift managed Prometheus. Openshift managed Alertmanager can access these metrics counters and user can use them to create alerts/alarm rules. There are four default alert rules already created as part of FEPLogging implementation as listed below:

- FEPLogErrorMessage
- FEPLogFatalMessage
- FEPLogPanicMessage
- FEPLogWarningMessage

Prometheus will scrape postgres_severity counter at every 30s as default scrape interval is 30s. User can modify this scrape interval from FEPLogging CR. After each scrape interval, if any change/increment found in postgres_severity counter then alert rule will be fired. User can check counts of postgres_severity metrics anytime from Prometheus dashboard as well.

4.9.3.3 Forwarding auditlog to Elasticsearch

In order to forward auditlog to Elasticsearch, update the FEPCluster to enable creating auditlog.
Example)

```yaml
spec:
  fep:
    fepChildCrVal:
      customPgAudit: |
        [output]
          logger = 'auditlog'
          log_directory = '/database/log/audit'
      customPgParams: |
        shared_preload_libraries='...,pgaudit'
        session_preload_libraries='...,pgaudit'
```

4.9.4 Limitations

- Only postgres_severity including ERROR, PANIC, FATAL and WARNING are monitored.
- External fluentd can not be used for log monitoring and log forwarding.
- External Elasticsearch is required for log forwarding.
- User must decide at deployment time whether secured connection between FEPCluster and FEPLogging is required or not. After deployment, one can switch connection from insecure to secure but can not switch from secure to insecure connection.
- User must configure FEPLogging CR first then only FEPCluster can forward logs to particular FEPLogging otherwise Logging feature will not work.
- User must set log_destination in FEPCluster CR.

4.10 Configuring pgBadger

This section describes how to configure pgBadger. FEP cluster provides a feature to create pgbadger report on defined schedule and upload the report to a web server outside.

4.10.1 FEP Custom Resources - spec.fep.pgBadger

<table>
<thead>
<tr>
<th>Custom Resource spec</th>
<th>Change Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>pgBadger.schedules.create</td>
<td>The 'create' schedule to create report and upload it to endpoint</td>
</tr>
<tr>
<td>pgBadger.schedules.cleanup</td>
<td>The 'cleanup' schedule to delete the report left in container</td>
</tr>
<tr>
<td>pgBadger.options.incremental</td>
<td>Default: false; When set to True: create incremental report in pgbadger</td>
</tr>
<tr>
<td>pgBadger.endpoint.authentication</td>
<td>a secret to contain authentication info to access endpoint support basic auth only</td>
</tr>
<tr>
<td>pgBadger.endpoint.customCertificateName</td>
<td>Client certificate reference in customCertificate CR</td>
</tr>
<tr>
<td>pgBadger.endpoint.fileUploadParameter</td>
<td>The file upload parameter defined by the web server Default: 'file'</td>
</tr>
<tr>
<td>pgBadger.endpoint.insecure</td>
<td>equivalent to curl -insecure option, default to false</td>
</tr>
<tr>
<td>pgBadger.endpoint.url</td>
<td>Web server url to upload the report file</td>
</tr>
</tbody>
</table>

4.10.2 Define pgBdager Schedules

The schedules are used to create and run a job periodically, written in Cron format.

If the schedule format is invalid, the cronjob will not be created, so no pgBadger report will be created and uploaded.

Example)
4.10.3 Define pgBdager Options

When the incremental option is set to false, pgbadger will create normal html report and upload the html file to the web server. When the incremental option is set to true, pgbadger will create incremental report and upload a zip file to the web server.

Example)

```yaml
pgBadger:
  schedules:
    cleanup: '10 * * * *'
    create: '50 * * * *'
  options:
    incremental: true
```

4.10.4 Define Endpoint for Uploading Report

Web server url

Both http and https are supported.

Example)

```yaml
pgBadger:
  endpoint:
    url: 'https://webserver-svc:4443/cgi-bin/upload.php'
```

Web Server authentication

Only basic auth is supported

To configure web server authentication:
Create a base64 encoded text from username:password

Example)

```bash
$ echo -ne "myuser:mypass" | base64
amFzb253Omphc29udw==
```

Wrap the output with base64 for creating a secret

Example)

```bash
$ echo -ne "amFzb253Omphc29udw==" | base64
YW1GemIyNTNPbXBoYzI5dWR3PT0=
```

Create a secret by using the wrapped text. The key must be 'basic_auth'.

Example)

```yaml
kind: Secret
apiVersion: v1
metadata:
  name: pgbadger-endpoint-auth
  namespace: fep-container-ct
data:
```
Add the secret name in the endpoint definition.

Example)

```yaml
pgBadger:
  endpoint:
    authentication: pgbadger-endpoint-auth
```

**Web Server certificates**

When certificate files are required by the web server, FEP cluster provides customCertificate CR to mount the certificates files in container.

To use certificates for web server.

Create a secret based on the cert and key files.

Example)

```bash
oc create secret tls webserver-cert --cert=webserver.pem --key=webserver.key
```

The webserver.pem and webserver.key are certificate files for accessing web server.

Create a configmap based on the CA cert.

Example)

```bash
oc create configmap webserver-cacert --from-file=ca.crt=webca.pem
```

The webca.pem is the CA certificate file for accessing web server.

Define custom certificates in FEPCluster CR.

Example)

```yaml
spec:
  fepChildCrVal:
    customCertificates:
    - userName: pgbadger-custom
      certificateName: webserver-cert
      caName: webserver-cacert
```

The userName is a reference in the pgBadger endpoint.

The certificateName is the secret created above.

The caName is the configmap created above.

Refer the custom certificate name in pgbadger endpoint.

Example)

```yaml
pgBadger:
  endpoint:
    customCertificateName: pgbadger-custom
```

**Insecure access to web server**

The pgbadger CR provides an option to the web server endpoint when secure connection is not required:

Example)
pgBadger:
  endpoint:
    insecure: true

File upload parameter
This parameter specify the request parameter for uploading a file to a web server. The value of this parameter is depended on the web server implementation.
Example)

pgBadger:
  endpoint:
    fileUploadParameter: uploadfile

curl command and parameters
FEP cluster uses curl command to upload the generated report to a web server endpoint. The CR in endpoint section will be converted to curl command parameters. The following table shows the mapping:

<table>
<thead>
<tr>
<th>curl command parameter</th>
<th>User configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>[URL]</td>
<td>Endpoint url</td>
</tr>
<tr>
<td>--cert</td>
<td>webserver.pem</td>
</tr>
<tr>
<td></td>
<td>included in the secret referred in customCertificateName</td>
</tr>
<tr>
<td>--key</td>
<td>webserver.key</td>
</tr>
<tr>
<td></td>
<td>included in the secret referred in customCertificateName</td>
</tr>
<tr>
<td>--cacert</td>
<td>webca.pem</td>
</tr>
<tr>
<td></td>
<td>included in the configmap referred in customCertificateName</td>
</tr>
<tr>
<td>--form &quot;uploadfile=@/path/to/report&quot;</td>
<td>Endpoint fileUploadParameter</td>
</tr>
<tr>
<td>--header &quot;Authorization: Basic passxxxx&quot;</td>
<td>Endpoint authentication configmap</td>
</tr>
<tr>
<td>--insecure</td>
<td>When endpoint.insecure is set to true</td>
</tr>
</tbody>
</table>

4.10.5 Uploaded File on Web Server
The FEP cluster uploads the pgbadger report according to the incremental mode:

<table>
<thead>
<tr>
<th>incremental mode</th>
<th>Uploaded file name</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>True</td>
<td>[fep cluster name]-sts-[pod index].zip</td>
<td>pgbadger-test3-sts-0.zip pgbadger-test3-sts-1.zip</td>
</tr>
<tr>
<td>False</td>
<td>[fep cluster name]-sts-[pod index].html</td>
<td>pgbadger-test3-sts-0.html pgbadger-test3-sts-1.html</td>
</tr>
</tbody>
</table>

The zip file contains a folder of pgbadger incremental report.
Example)

\database
  \log
  \pgbadger-report
  \{years\}
Note

- The web server is NOT included in the FEP cluster solution.
- The web server is responsible to the uploaded files according to the customer’s business logic.

4.11 Automating Audit Log Operations

Simplifies the operation of your audit logs to implement operations that meet security requirements such as audits.

1) Simplified parameter setting
Simplifies parameter settings for audit logs to reduce initial setup costs.

2) Alerting
Detects unauthorized access or misoperation and respond quickly to alerts that you set arbitrarily.

3) Store in cloud storage
Ability to store audit logs in object storage in cloud. Easier to control log retention based on your requirements.

4.11.1 Simplifies Parameter Setting

Simplify audit log parameter settings and reduce initial setup costs. The only setting required is enabling the enable parameter. The pgaudit module is loaded when the FEP server starts and audit logs are stored in the logs directory.

By customizing the audit log configuration file as necessary, it is also possible to make settings according to operational requirements.

```
spec:
  fep:
    pgAuditLog:
      enable: true
```

4.11.2 Alerting

According to preset alert conditions, unauthorized access and erroneous operations can be detected at an early stage, enabling rapid response.

Audit logs are sent to Fluentd using the remotelogging function, and audit logs are monitored by setting alerts in Prometheus according to sqlstate conditions.

The alert is triggered when the 1 minute average of sqlstate(28P01) (invalid password) exceeds 50.
4.11.3 Store in Cloud Storage

Long-term retention of audit logs may be required in accordance with system or industry standard security policy requirements. However, long-term storage of logs requires the continuation of complicated operations such as disk management and rotation management. Therefore, with this function, by saving audit logs to cloud object storage, you can easily control the saving of logs based on your requirements.

```yaml
spec:
  fep:
    pgAuditLog:
      enable: true
      endpoint:
        protocol: s3
        url: s3://pgaudit/cluster1
        authentication: s3-secret
      schedules:
        upload: '30 * * * *'
```

4.12 Transparent Data Encryption Using a Key Management System

Describes how to configure transparent data encryption using a key management system.

Transparent data encryption using a key management system can only be configured when the FEPCluster is first created. Users cannot configure an existing FEPCluster for transparent data encryption using a key management system.
4.12.1 Registration of Authentication Information

4.12.1.1 When Using a KMIP Server

Save the certificate used for TLS communication between KMIP server in Secret or ConfigMap.

The Secret or ConfigMap you created gives the FEPCluster custom resource a resource name and mounts it in the FEP container.

Create a Secret to store the client certificate and private key for connecting to KMIP server.

Also, optionally create a ConfigMap to store the root certificate.

An example of registering credentials using the credentials file below is explained.

| kmip.pem   | # Client certificate for connecting to KMIP server |
| kmip.key   | # Private key                                     |
| myca.pem   | # Root certificate                                |

Create a Secret to store the client certificate and private key.

Specify tls.crt and tls.key as file names when mounting the client certificate and private key, respectively.

$ oc create secret generic kmip-cert --from-file=tls.crt=kmip.pem --from-file=tls.key=kmip.key -n kmip-demo

Optionally create a ConfigMap to store your root certificates.

Specify ca.crt as the file name to be mounted.

$ oc create configmap kmip-cacert --from-file=ca.crt=myca.pem -n my-namespace

4.12.1.2 When Using AWS Key Management Service

Save credentials and other settings required to connect to AWS key management services in Secrets and ConfigMaps.

Prepare two files, credentials and config, which describe credentials and other settings according to the format specified by the AWS client interface. Specifying access_key_id and secret_access_key in the credentials file is mandatory.

An example of registering authentication information using the following configuration file is explained.

| credentials | # credentials file |
| config      | # config file      |

Create a ConfigMap to store config files. Specify config for the key name. The name of the ConfigMap is arbitrary (here aws-kms-config).

$ oc create configmap aws-kms-config --from-file=config=config -n my-namespace

Create a secret to save the credentials file. Specify credentials for the key name. The name of the Secret is arbitrary (here aws-kms-credentials).

$ oc create secret generic aws-kms-credentials --from-file=credentials=credentials -n my-namespace

See

Refer to below for AWS client interface configuration files.

https://docs.aws.amazon.com/cli/latest/userguide/cli-configure-files.html

4.12.1.3 When using Azure Key Management Service

Save the credentials required to connect to Azure's key management service in Secret.
The available authentication methods are either authentication using passwords or authentication using client certificates.

For password-based authentication, create a YAML format file that defines a secret like the one below. The secret name is arbitrary (here azure-key-vault-passphrase). data.clientsecret contains a base64-encoded password.

```yaml
kind: Secret
apiVersion: v1
metadata:
  name: azure-key-vault-passphrase
  namespace: my-namespace
data:
  clientsecret: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX=
  type: Opaque
```

Create a secret based on the created YAML file. Here we are using a YAML file named azure-client-secret.yaml.

```
$ kubectl apply -f azure-client-secret.yaml -n my-namespace
```

For authentication using a client certificate, store the client certificate file and private key in Secret. Here is an example of creating a Secret using the certificate file below.

```
azuremycert.pem    # PEM file containing client certificate and private key
```

Create a secret to store the client certificate. Specify azure-key-vault.crt for the key name. The secret name is arbitrary (here azure-key-vault-secret).

```
$ oc create secret generic azure-key-vault-secret --from-file=azure-key-vault.crt=azuremycert.pem -n my-namespace
```

### 4.12.2 Configuring FEPCluster Custom Resources

To enable TDE using a key management system, you need to set “spec.fepChildCrVal.customPgParams” and “spec.fepChildCrVal.sysTde”.

#### 4.12.2.1 Define spec.fepChildCrVal.customPgParams

The fepChildCrVal.customPgParams section must define the following parameters:

**shared_preload_libraries**

Add the 'tde_kms' library to the list of libraries in shared_preload_libraries.

Example)

```yaml
spec:
  fep:
    ...
  fepChildCrVal:
    ...
  customPgParams:
    shared_preload_libraries='pgx_datamasking,pg_prewarm,pg_stat_statements,tde_kms'
```

Do not remove 'tde_kms' library from 'shared_preload_libraries' list after cluster creation.

#### 4.12.2.2 Define spec.fepChildCrVal.sysTde

Add a sysTde section under spec.fepChildCrVal to define the parameters required to connect to your key management system. Under sysTde there are two parameters defined:
Define `spec.fepChildCrVal.sysTde.tdeType`

`sysTde` itself is an optional parameter (if `sysTde` is not defined, use a file-based keystore). However, if `sysTde` is defined by the user, `sysTde.tdeType` must also be defined.

If configuring TDE with a key management system, set `sysTde.tdeType` to "tdek".

Example)

```
sysTde:
  tdeType: tdek
```

Define `spec.fepChildCrVal.sysTde.tdek.kmsDefinition`

If you set `sysTde.tdeType` to "tdek", you must also define `sysTde.tdek`.

Define the connection information of the key management system in `sysTde.tdek.kmsDefinition`. Based on the information defined here, the operator creates the key management system connection information file used by Fujitsu Enterprise Postgres.

Information for multiple key management systems can be defined in `kmsDefinition`. For `type`, specify the type of key management system (either kmip, awskms, or azurekeyvault).

Example)

```
sysTde:
  tdeType: tdek
  tdek:
    targetKmsName: kms_conninfo1
    kmsDefinition:
      - name: kms_conninfo1
        type: kmip
```

Refer to the Reference for details of each parameter.

Specify the name of the Secret or ConfigMap created in "4.12.1 Registration of Authentication Information" in the corresponding parameter under `kmsDefinition`. If `type` is awskms, `profile` specifies the name of the profile to use from the profile in the AWS client interface configuration file.

Example)

```
spec:
  fep:
    ...
  fepChildCrVal:
    ...
  sysTde:
    ...
  tdeType: tdek
  tdek:
    targetKmsName: kms_conninfo1
    targetKeyId: xxxyyyzzz
    kmsDefinition:
      - name: kms_conninfo1
        type: kmip
        address: xxx.xxx.xxx.xxx
        port: 100
        authMethod: cert
        sslpassphrase: ssl-password
        cert:
          certificateName: kmip-cert
```
Define spec.fepChildCrVal.sysTde.tdek.targetKeyId, spec.fepChildCrVal.sysTde.tdek.targetKmsName

Specify one of the key management system names defined in kmsDefinition in sysTde.tdek.targetKmsName as the name of the key management system to use as the keystore. sysTde.tdek.targetKeyId specifies the key ID of the encryption key within that key management system to use as the master encryption key.
Chapter 5 Post-Deployment Operations

This chapter describes the operation after deploying the container.

5.1 How to Connect to a FEP Cluster

When connecting from within the same project of the OpenShift system

Service resources are used to connect to FEPCluster and FEPPgpool2 from within the same project.

A service resource provides a single endpoint for communicating with containers.

Service resources are created with the following naming conventions.

FEPCluster service
- `<FEPCluster name>-primary-svc`
- `<FEPCluster name>-replica-svc`
- `<FEPCluster name>-headless-svc`

FEPPGPool2 service
- `<FEPPgpool2 name>-feppgpool2-svc`

Example of checking service resources of FEPCluster container and FEPPgpool2 container

$ oc get all

Check where the resource type is Service (Begin with "svc/").

You can also check with the oc get svc command. The following is an example.

<table>
<thead>
<tr>
<th>NAME</th>
<th>TYPE</th>
<th>CLUSTER-IP</th>
<th>EXTERNAL-IP</th>
<th>PORT(S)</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;FEPCluster name&gt;-headless-svc</code></td>
<td>ClusterIP</td>
<td>None</td>
<td>&lt;none&gt;</td>
<td>27500/TCP,25001/TCP</td>
<td>24h</td>
</tr>
<tr>
<td><code>&lt;FEPCluster name&gt;-primary-svc</code></td>
<td>ClusterIP</td>
<td>xxx.xxx.xxx.xxx</td>
<td>&lt;none&gt;</td>
<td>27500/TCP,25001/TCP</td>
<td>24h</td>
</tr>
<tr>
<td><code>&lt;FEPCluster name&gt;-replica-svc</code></td>
<td>ClusterIP</td>
<td>yyy.yyy.yyy.yyy</td>
<td>&lt;none&gt;</td>
<td>27500/TCP,25001/TCP</td>
<td>24h</td>
</tr>
<tr>
<td><code>&lt;FEPPgpool2 name&gt;-feppgpool2-svc</code></td>
<td>NodePort</td>
<td>zzz.zzz.zzz.zzz</td>
<td>&lt;none&gt;</td>
<td>9999:31707/TCP,9998:31906/TCP</td>
<td>24h</td>
</tr>
</tbody>
</table>

Example of accessing FEPPgpool2 container

$ psql -h `<FEPPgpool2 name>-feppgpool2-svc` -p 9999 -c "select version();"

When connecting from outside the OpenShift system

Automatically creating a service with ClusterIP to connect to the deployed container. You can connect to FEP or FEPPgpool2 services from the OpenShift system’s internal network. To access from outside the OpenShift system, you need to know the address of the OpenShift node.

For example, “Access the FEP pgpool2 container from an application server that is running outside the OpenShift system but is part of the Internal network”.

An example of how to check the node IP in OpenShift.

$ oc get nodes

<table>
<thead>
<tr>
<th>NAME</th>
<th>STATUS</th>
<th>ROLES</th>
<th>AGE</th>
<th>VERSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>openshiftcluster1-cmfv8-master-0</td>
<td>Ready</td>
<td>master</td>
<td>370d</td>
<td>v1.19.0+4c3480d</td>
</tr>
<tr>
<td>openshiftcluster1-cmfv8-master-1</td>
<td>Ready</td>
<td>master</td>
<td>370d</td>
<td>v1.19.0+4c3480d</td>
</tr>
<tr>
<td>openshiftcluster1-cmfv8-master-2</td>
<td>Ready</td>
<td>master</td>
<td>370d</td>
<td>v1.19.0+4c3480d</td>
</tr>
</tbody>
</table>

$ oc describe nodes openshiftcluster1-cmfv8-master-0 | grep IP

InternalIP: 10.0.2.8
An example of verifying the service resource for the FEP pgpool2 container.

```bash
$ oc get all
```

Check where the resource type is Service (Begin with "svc/").

You can also see this with the `oc get svc` command. The following is an example.

```bash
$ oc get svc
```

<table>
<thead>
<tr>
<th>NAME</th>
<th>TYPE</th>
<th>CLUSTER-IP</th>
<th>EXTERNAL-IP</th>
<th>PORT(S)</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>svc-feppgpool2-feppgpool2</td>
<td>NodePort</td>
<td>172.30.248.12</td>
<td>&lt;none&gt;</td>
<td>9999: 30537/TCP, 9998: 30489/TCP</td>
<td>2m5s</td>
</tr>
</tbody>
</table>

This is an example of accessing the FEP pgpool2 container.

```bash
$ psql -h 10.0.2.8 -p 30537 -c "show pool_nodes"
```

### 5.2 Configuration Change

This section describes changes to the FEPCluster configuration.

#### List FEPCluster

Equivalent Kubernetes command: `kubectl get FEPClusters (-A)`

This operation will list all FEPClusters in a namespace, or if the `-A` option is specified, will list all FEPClusters in all namespace.

Default output format:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>.metadata.name</td>
<td>Name of Cluster</td>
</tr>
<tr>
<td>AGE</td>
<td>Elapsed time</td>
<td>Indicates the amount of time that has elapsed since the cluster was created</td>
</tr>
</tbody>
</table>

Example)

```bash
# kubectl get fepclusters -A
```

<table>
<thead>
<tr>
<th>NAMESPACE</th>
<th>NAME</th>
<th>AGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>namespace1</td>
<td>ns1fep1</td>
<td>21h</td>
</tr>
<tr>
<td>namespace2</td>
<td>ns2fep2</td>
<td>22h</td>
</tr>
</tbody>
</table>

#### Update FEPCluster

Equivalent Kubernetes command: `kubectl apply -f <new_spec>`

Operations that can be performed here.

<table>
<thead>
<tr>
<th>Custom Resource spec</th>
<th>Change effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>.spec.fep.instances: $n</td>
<td>Increase the number of nodes in the cluster to $n.</td>
</tr>
</tbody>
</table>
This will impact behavior for values in fep section only. All other values except spec.fepChildCrVal.backup.image.image must be changed from respective child CR.

**Delete FEPCluster**

Equivalent Kubernetes command: `kubectl delete FEPCluster <cluster_name>`

This operation will remove the FEPCluster by the cluster_name and all Child CRs (FEPVolume, FEPConfig, FEPCert & FEPUser) & resources associated with it.

---

**Note**

Deleting a FEPCluster will delete all PV associated with the cluster, including backup and archived WAL volumes (except when using pre-made PV or AWS S3). This is an unrecoverable action.

---

### 5.3 FEPCluster Resource Change

#### 5.3.1 Changing CPU and Memory Allocation Resources

Describes how to change the CPU and memory resources assigned to a pod created by a FEPCluster.

This allows you to scale the pod vertically through custom resources.

To modify CPU and memory resources, modify the `spec.fep.mcSpec` section of the FEPCluster custom resource and apply your changes.

When the changes are applied, restart the replica server with the new resource settings. If there are multiple replica servers, restart them one at a time. When all replica servers are restarted, one of them is promoted to the new master server due to a switchover. Then restart the container image on the original master server. This allows you to change resource settings for all servers with minimal disruption.

*1) Modifying this section scales up the FEP server container. For information about other container resource sections, refer to “FEPCluster Parameters” in the Reference.

#### 5.3.2 Resizing PVCs

Describes how to resize a PVC assigned to a pod created by a FEPCluster.

This allows you to increase the size of the volume allocated to the pod through custom resources.

To change the PVC size, modify the size of each volume in the `spec.fepChildCrVal.storage` section of the FEPCluster custom resource and apply the change. These changes apply to all PVCs assigned to the pod created by the FEPCluster.

---

**Note**

- PVC resizing is extensible only.
- You can resize a PVC only if the StorageClass supports dynamic resizing.
- If the StorageClass does not support resizing PVCs, use the FEPRestore custom resource to create a new FEPCluster to resize the PVC. For more information, refer to "FEPRestore Custom Resource Parameters" in the Reference.

---

### 5.4 FEPPGPool2 Configuration Change

This section describes changes to the FEPPGPool2 configuration.

**List FEPPGPool2**

Equivalent Kubernetes command: `kubectl get FEPPGPool2 (-A)`
This operation will list all FEPPGPool2 in a namespace, or if the -A option is specified, will list all FEPPGPool2 in all namespaces.

Default output format:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>.metadata.name</td>
<td>Name of pgpool2</td>
</tr>
</tbody>
</table>

Example)

```
# kubectl get feppgpool2 -A

NAMESPACE   NAME
namespace1   fep1-pgpool2
namespace2   fep2-pgpool2
```

Delete FEPPGPool2

Equivalent Kubernetes command: kubectl delete FEPPGPool2 <pgpool2_name>

This operation will remove the FEPPGPool2 by the pgpool2_name.

Update FEPPGPool2

Equivalent Kubernetes command: kubectl apply -f <new_spec>

Specify updated parameters in the format described in "2.3.4 Deploying Pgpool-II and Connect to FEPCluster from Operator". Only the following parameters would change for Operations that can be performed here.

<table>
<thead>
<tr>
<th>Custom Resource spec</th>
<th>Change Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>.spec.count: n</td>
<td>Increase the number of nodes in the cluster to n.</td>
</tr>
<tr>
<td>.spec.serviceport</td>
<td>Change the TCP port for connecting to the Pgpool-II.</td>
</tr>
<tr>
<td>.spec.statusport</td>
<td>Change the TCP port for connecting to the PCP process.</td>
</tr>
<tr>
<td>.spec.limits.cpu</td>
<td>Change limits of cpus.</td>
</tr>
<tr>
<td>.spec.limits.memory</td>
<td>Change limits of memory.</td>
</tr>
<tr>
<td>.spec.requests.cpu</td>
<td>Change requests of cpus.</td>
</tr>
<tr>
<td>.spec.requests.memory</td>
<td>Change requests of memory.</td>
</tr>
<tr>
<td>.spec.fepclustername</td>
<td>Change fepcluster to connect.</td>
</tr>
<tr>
<td>.spec.customhba</td>
<td>Change pool_hba.conf file.</td>
</tr>
<tr>
<td>.spec.customparams</td>
<td>Change pgpool2 parameters</td>
</tr>
<tr>
<td>.spec.custompcp</td>
<td>Change pcp.conf file.</td>
</tr>
<tr>
<td>.spec.customsslkey</td>
<td>Change key content</td>
</tr>
<tr>
<td>.spec.customsslcert</td>
<td>Change the contents of the public x 509 certificate.</td>
</tr>
<tr>
<td>.spec.customsslcacert</td>
<td>Change the contents of the CA root certificate in PEM format.</td>
</tr>
</tbody>
</table>

Some of the customparams parameters, customhba and custompcp, require a restart of pgpool2.

Equivalent Kubernetes command: Kubectl apply -f <new_spec>

"pgpool2_restart" action type expects users to specify the name of the pgpool2 that they want to restart from.

Specify the metadata.Name of the FEPPGPool2 CR in the targetPgpool2Name section of the FEPAction CR, as below:

```
spec:
  targetPgpool2Name: fep1-pgpool2
```
When updating FEPPGPool2, the Pod of FEPPGPool2 is restarted. If configured with more than one FEPPGpool2, they are rebooted sequentially. The application should be designed to reconnect the connection because the connection being connected is broken.

5.5 Scheduling Backup from Operator

**Operational status confirm**

Information about the backup can be found by running the command in the FEP backup container, as shown in the example below.

```bash
$ oc exec pod/fepserver-XXXXX -c FEPbackup -- pgbackrest info

stanza: fepbackup
status: ok
cipher: none

db (current)
  wal archive min/max (12-1): 000000010000000000000001/000000010000000000000005
  full backup: 20201125-025043F
    wal start/stop: 000000010000000000000003 / 000000010000000000000003
    database size: 31.7MB, backup size: 31.7MB
    repository size: 3.9MB, repository backup size: 3.9MB

  incr backup: 20201125-025043F_20201125-025600I
    timestamp start/stop: 2020-11-25 02:56:00 / 2020-11-25 02:56:02
    wal start/stop: 000000010000000000000005 / 000000010000000000000005
    database size: 31.7MB, backup size: 24.3KB
    repository size: 3.9MB, repository backup size: 619B
    backup reference list: 20201125-025043F
```

**Update FEPBackup**

Equivalent Kubernetes command: kubectl apply -f <new_spec>

Specify updated parameters in the format described in "2.3.5 Scheduling Backup from Operator". Only following parameters would change for Operations that can be performed here.

<table>
<thead>
<tr>
<th>Custom Resource spec</th>
<th>Change Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>spec.schedule.num</td>
<td>Change the Number of Registered Backup Schedules</td>
</tr>
<tr>
<td>spec.scheduleN.schedule</td>
<td>Change the scheduled backup time</td>
</tr>
<tr>
<td>spec.scheduleN.type</td>
<td>Change the scheduled backup type</td>
</tr>
<tr>
<td>spec.pgBackrestParams</td>
<td>Change pgBackRest parameters</td>
</tr>
<tr>
<td>spec.scheduleN.repo</td>
<td>If you specified more than one repository for spec.pgBackrestParams, select the repository in which to store the backup data. The default is 1.</td>
</tr>
</tbody>
</table>

**Note**

- Changes made during the backup are reflected from the next backup.
Changes to the backup schedule do not affect the application.

If you perform any of the following update operations, be sure to obtain a backup after the update.

- When the master encryption key is updated with `pgx_set_master_key`
- When the encryption passphrase for transparent data encryption is updated (can be updated by the `tdeppassphrase` parameter of `FEPCluster CR`)

5.6 Configure MTLS Setting

5.6.1 Certification Rotation

All certificates are bounded by the time limit. At certain time, it needs to be renewed. We recommend to renew the certificate when it reaches 3/4 of its life cycle or as soon as possible if it is compromised. When a certificate is renewed, we need to rotate it inside the FEP server container. At the moment, FEP server container does not support automatic certificate rotation. Depending on which certificate has renewed, there are different procedures to handle that.

**Patroni Certificate Rotation**

When Patroni certificate is renewed, we have to re-deploy each and every Pod for FEP server container to pick up the new certificate. There is a down time on `FEPCluster`.

**FEP Server Certificate Rotation**

When FEP Server certificate is renewed, we can use `FEPAction CR` to trigger a reload of the database and FEP server will pick up the new certificate with no interruption to service.

**Client certificate Rotation**

When any of the client certificate is renewed, FEP server container internally will use the new certificate next time it establishes a connection to FEP server. However, to avoid any unexpected interruption to service, it is recommended to re-deploy each and every Pod as soon as possible.

5.7 Monitoring

Monitoring is collecting historic data points that you then use to generate alerts (for any anomalies), to optimize databases and lastly to be proactive in case something goes wrong (for example, a failing database).

There are five key reasons to monitor FEP database.

1. **Availability**

   It is a very simple equation that if you do not have a database in running, your application will not work. If the application is critical, it directly affects on users and the organization.

2. **System Optimization**

   Monitoring helps to identify the system bottlenecks and according to the user can make changes to your system to see if it resolves the problem or not. To put this into perspective, there may be a situation where users see a very high load on the system. And figured out that there is a host parameter that can be set to a better value.

3. **Identify Performance Problems**

   Proactive monitoring can help you to identify future performance problems. From the database side, it could be related to bloating, slow running queries, table and index statistics, or the vacuum being unable to catch up.

4. **Business Process Improvement**

   Every database user has a different need and priority. Knowing the system (load, user activity, etc.) helps you to prioritize customer tasks, reporting, or downtime. Monitoring helps to make business process improvement.
5. Capacity Planning

More user or application growth means more system resources. It leads to key questions: Do you need more disk space? Do you need a new read replica? Do you need to scale your database system vertically? Monitoring helps you to understand your current system utilization—and if you have data, points spread over a few weeks or months, it helps to forecast system scaling needs.

This article describes monitoring and alerting operations using OpenShift's standard Pod alive monitoring, resource monitoring and database statistics provided by the FEP Exporter.

### 5.7.1 Monitoring FEP Operator and Operands

The monitoring of FEP operators and operands are achieved by Prometheus' standard alive and resource monitoring.

<table>
<thead>
<tr>
<th>Metrics name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alive monitoring</td>
<td>Can monitor Pod status</td>
</tr>
<tr>
<td>Resource monitoring</td>
<td>You can monitor the following resource status</td>
</tr>
<tr>
<td></td>
<td>- CPU Usage</td>
</tr>
<tr>
<td></td>
<td>- CPU Quota</td>
</tr>
<tr>
<td></td>
<td>- Memory Usage</td>
</tr>
<tr>
<td></td>
<td>- Memory Quota</td>
</tr>
<tr>
<td></td>
<td>- Current Network Usage</td>
</tr>
<tr>
<td></td>
<td>- Receive Bandwidth</td>
</tr>
<tr>
<td></td>
<td>- Transmit Bandwidth</td>
</tr>
<tr>
<td></td>
<td>- Rate of Received Packets</td>
</tr>
<tr>
<td></td>
<td>- Rate of Transmitted Packets</td>
</tr>
<tr>
<td></td>
<td>- Rate of Received Packets Dropped</td>
</tr>
<tr>
<td></td>
<td>- Rate of Transmitted Packets Dropped</td>
</tr>
</tbody>
</table>

By setting alert rules based on these monitoring items, operators and operands can be monitored. For the setting method, refer to the appendix in the Reference.

If an error is detected by monitoring the operator's alive, it can be dealt with by recreating the Pod.

If resource monitoring detects an error, consider allocating more resources to the Operator or Operands.

Check the Operator Hub or Red Hat Operator Catalog page to see which version you are currently using, which can be updated, and to check for security vulnerabilities.

### 5.7.2 Monitoring FEP Server

Monitoring and alerts system leverages standard GAP stack (Grafana, Alert manager, Prometheus) deployed on OCP and Kubernetes. GAP stack must be there before FEP operator & FEPCluster can be deployed.

Prometheus is a condensed way to store time-series metrics. Grafana provides a flexible and visually pleasing interface to view graphs of FEP metrics stored in Prometheus.

Together they let store large amounts of metrics that user can slice and break down to see how the FEP database is behaving. They also have a strong community around them to help deal with any usage and setup issues.

The Prometheus acts as storage and a polling consumer for the time-series data of FEP container. Grafana queries Prometheus to displaying informative and very pretty graphs.

If Prometheus rules are defined, it also evaluates rules periodically to fire alerts to Alert manager if conditions are met. Further Alert manager can be integrated with external systems like email, slack, SMS or back-office to take action on alerts raised.
Metrics from FEP Cluster(s) is collected by Prometheus through optional components deployed using FEP Exporter with default set of metrics and corresponding Prometheus rules to raise alerts. User may extend or overwrite metrics by defining their custom metrics queries and define their custom Prometheus rules for alerting.

5.7.2.1 Architecture

Block diagram of monitoring FEP server is as follows.

- FEPExporter CR is managed by FEP Operator
- When FEPExporter CR is created, FEP operator creates following kubernetes objects:
  - ConfigMap that contains default and custom queries to collect metrics from database cluster from each node
  - Secret containing JDBC URL for all FEPCluster nodes to connect and request metrics. This string contains authentication details as well to make JDBC connection.
  - Prometheus rules corresponding to default alert rules
  - ServiceMonitor for Prometheus to discover FEPExporter service
  - FEPExporter container using FEPExporter image to scrape metrices from all FEPCluster nodes

**Note**

- Alert Manager integration to back-office to send mail / message / raising ticket is done by user based on their environment
- Grafana installation and integration is done by user. Use the Grafana Operator provided by OperatorHub.
- Grafana dashboard is created by user based on their requirements and design.

5.7.2.2 Default Server Metrics Monitoring

By default FEPExporter scrapes some useful metrics for server.

Once FEPExporter is running, user can check the collected metrics under Openshift->Monitoring->Metrics submenu.

There are 2 levels of default server metrics defined by FEP Exporter
**Type Details**

<table>
<thead>
<tr>
<th>Type</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default mandatory</td>
<td>Are collected by FEP Exporter. These are kept enabled by default by FEP Exporter and cannot be disabled by end user.</td>
</tr>
<tr>
<td>Default useful</td>
<td>Useful focused metrics for health and performance metrics. Can be disabled by end user.</td>
</tr>
</tbody>
</table>

**Default mandatory metrics**

These metrics are either from basic statistics view of the database or FEP Exporter own metrics;

Various metrics under this category are

<table>
<thead>
<tr>
<th>Metrics name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>pg_stat_bgwriter_*</td>
<td>Maps to view in Statistic Collector</td>
</tr>
<tr>
<td>pg_stat_database_*</td>
<td>Maps to view in Statistic Collector</td>
</tr>
<tr>
<td>pg_stat_database_conflicts_*</td>
<td>Maps to view in Statistic Collector</td>
</tr>
<tr>
<td>pg_stat_archiver_*</td>
<td>Maps to view in Statistic Collector</td>
</tr>
<tr>
<td>pg_stat_activity_*</td>
<td>Maps to view in Statistic Collector</td>
</tr>
<tr>
<td>pg_stat_replication_*</td>
<td>Maps to view in Statistic Collector</td>
</tr>
<tr>
<td>pg_replication_slots_*</td>
<td>Maps to System Catalog pg_replication_slots</td>
</tr>
<tr>
<td>pg_settings_*</td>
<td>Maps to System Catalog pg_settings</td>
</tr>
<tr>
<td>pg_locks_*</td>
<td>Maps to System Catalog pg_locks</td>
</tr>
<tr>
<td>pg_exporter_*</td>
<td>Exposes exporter metrics:</td>
</tr>
<tr>
<td></td>
<td>- last_scrape_duration_seconds (Duration of the last scrape of metrics from PostgresSQL)</td>
</tr>
<tr>
<td></td>
<td>- scrapes_total (Total number of times PostgresSQL was scraped for metrics)</td>
</tr>
<tr>
<td></td>
<td>last_scrape_error (Whether the last scrape of metrics from PostgresSQL resulted in an error; 1 for error &amp; 0 for success)</td>
</tr>
<tr>
<td>pg_*</td>
<td>Exposes exporter metrics</td>
</tr>
<tr>
<td></td>
<td>- pg_up ( set to 1 if the connection to service is success, 0 otherwise )</td>
</tr>
<tr>
<td></td>
<td>- pg_static ( can be used to fetch label short_version / version containing postgres server version information )</td>
</tr>
</tbody>
</table>

**Default useful metrics**

There are certain useful queries which are additionally added to evaluate the health of the Database system.

<table>
<thead>
<tr>
<th>Metrics name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>pg_capacity_connection_*</td>
<td>Metrics on connections e.g. txns running for 1 hour</td>
</tr>
<tr>
<td>pg_capacity_schema_*</td>
<td>Metrics on disk space of schema</td>
</tr>
<tr>
<td>pg_capacity_tblspace_*</td>
<td>Metrics on disk space of tablespace</td>
</tr>
<tr>
<td>pg_capacity_tblvacuum_*</td>
<td>Metrics on tables without vacuum for days</td>
</tr>
<tr>
<td>pg_capacity_longtx_*</td>
<td>Number of transactions running longer than 5 minutes</td>
</tr>
<tr>
<td></td>
<td>Review the information and consider SQL tuning and resource enhancements.</td>
</tr>
<tr>
<td>pg_performance_locking_detail_*</td>
<td>Details of processes in blocked state</td>
</tr>
<tr>
<td>pg_performance_locking_*</td>
<td>Number of processes in blocked state</td>
</tr>
</tbody>
</table>
### Metrics name

<table>
<thead>
<tr>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>pg_replication_*</td>
</tr>
<tr>
<td>Replication lag behind master in seconds</td>
</tr>
<tr>
<td>Provides the ability to check for the most current data in a reference replica</td>
</tr>
<tr>
<td>To solve the problem, it is necessary to consider measures such as increasing network resources and reducing the load</td>
</tr>
<tr>
<td>pg_postmaster_*</td>
</tr>
<tr>
<td>Time at which postmaster started</td>
</tr>
<tr>
<td>pg_stat_user_tables_*</td>
</tr>
<tr>
<td>Important statistics from pg_stat_user_tables</td>
</tr>
<tr>
<td>pg_statio_user_tables_*</td>
</tr>
<tr>
<td>Important statistics from pg_statio_user_tables</td>
</tr>
<tr>
<td>pg_database_*</td>
</tr>
<tr>
<td>Database size</td>
</tr>
<tr>
<td>If the database runs out of space, database restore is required</td>
</tr>
<tr>
<td>pg_stat_statements_*</td>
</tr>
<tr>
<td>Statistics of SQL statements executed by server</td>
</tr>
<tr>
<td>pg_capacity_tblbloat_*</td>
</tr>
<tr>
<td>Fetched bloat in tables</td>
</tr>
<tr>
<td>pg_tde_encrypted_*</td>
</tr>
<tr>
<td>Presence or absence of transparent data encryption in the tablespace and the number of tables and indexes stored</td>
</tr>
<tr>
<td>pg_password_valid_*</td>
</tr>
<tr>
<td>Database Role Password Validity Period</td>
</tr>
<tr>
<td>pg_not_set_password_valid_*</td>
</tr>
<tr>
<td>Number of database roles with no password expiration</td>
</tr>
</tbody>
</table>

---

**Note**

You can tune the intervals and thresholds at which information is gathered by changing the values specified in the information gathering query. For more information, refer to the queries in the appendix of the Reference Guide, and make your own settings.

Refer an example below.

---

### 5.7.2.3 Default Alerts

There are few basic alert rules which are setup by the FEP Operator as below

<table>
<thead>
<tr>
<th>Alert rule</th>
<th>Alert Level</th>
<th>Condition persistence</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ContainerHighCPUUsage</td>
<td>Warning</td>
<td>5 mins</td>
<td>FEP server container/POD CPU usage is exceeding 80% of the resource limits</td>
</tr>
</tbody>
</table>
### Alert Rule Description

<table>
<thead>
<tr>
<th>Alert rule</th>
<th>Alert Level</th>
<th>Condition persistence</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ContainerHighRAMUsage</td>
<td>Warning</td>
<td>30 mins</td>
<td>FEP server container/Pod memory usage is exceeding 80% of the resource limits</td>
</tr>
<tr>
<td>PVCLowDiskSpace</td>
<td>Warning</td>
<td>5 mins</td>
<td>A FEP PVC (volume) has less than 10% disk available</td>
</tr>
<tr>
<td>ContainerDisappeared</td>
<td>Warning</td>
<td>60 seconds</td>
<td>FEP server container/Pod has disappeared since last 60 seconds</td>
</tr>
<tr>
<td>PostgresqlDown</td>
<td>Error</td>
<td>-</td>
<td>FEP server apparently went down or not accessible</td>
</tr>
<tr>
<td>PostgresqlTooManyConnections</td>
<td>Warning</td>
<td>-</td>
<td>FEP server container/Pod connection usage is beyond 90% of its available capacity</td>
</tr>
<tr>
<td>PostgresqlRolePasswordCloseExpierd</td>
<td>Warning</td>
<td>-</td>
<td>A Postgresql role exists with a password expiration of less than 7 days</td>
</tr>
<tr>
<td>PostgresqlRolePasswordExpired</td>
<td>Warning</td>
<td>-</td>
<td>A Postgresql role exists with an expired password</td>
</tr>
</tbody>
</table>

**The alerts are based on statistics/metrics. If a platform statistics are incorrect, it may raise an incorrect alarm.**

E.g. if the Storage Driver is not showing correct metrics for bytes usage for a PV, system may end up raising incorrect alarm of PVCLowDiskSpace. This behaviour can be seen with NFS storage.

You can configure any alert by adding alert rules to other monitoring items.

### 5.7.2.4 Graphical user interface

User can build their custom dashboard using default and custom metrics.

An example Grafana dashboard screenshot is shown below.

![Grafana Dashboard Screenshot](image)

### 5.7.3 Monitoring FEP Backup

You can view information about the backed-up data and the status of the backup process in the FEP server tables and system views.

Backup information is updated when the automatic backup process completes or when backup data is deleted as specified by retention.

The following tables and views are added. The tables and views to be added are created under the fep_exporter schema in the postgres database on the FEP server.
### 5.7.3.1 pgbackrest_info_backup view

Contains one line per backup for information about the state of the backup.

<table>
<thead>
<tr>
<th>Column</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>label</td>
<td>text</td>
<td>Information identifying the backup</td>
</tr>
<tr>
<td>type</td>
<td>text</td>
<td>Full: full backup, incr: incremental backup</td>
</tr>
<tr>
<td>prior</td>
<td>text</td>
<td>Label of the backup that should be applied first (For incremental backups only)</td>
</tr>
<tr>
<td>database_size</td>
<td>bigint</td>
<td>Database size</td>
</tr>
<tr>
<td>database_size_comp</td>
<td>bigint</td>
<td>Database size (After Compression)</td>
</tr>
<tr>
<td>backup_size</td>
<td>bigint</td>
<td>Backup size</td>
</tr>
<tr>
<td>backup_size_comp</td>
<td>bigint</td>
<td>Backup size (After Compression)</td>
</tr>
<tr>
<td>archive_start</td>
<td>text</td>
<td>Range of WALs required for restore (Start)</td>
</tr>
<tr>
<td>archive_stop</td>
<td>text</td>
<td>Range of WALs required for restore (End)</td>
</tr>
<tr>
<td>backup_start</td>
<td>timestamp with timezone</td>
<td>Backup Start Time</td>
</tr>
<tr>
<td>backup_stop</td>
<td>timestamp with timezone</td>
<td>Backup End Time</td>
</tr>
<tr>
<td>backup_exec_time</td>
<td>interval</td>
<td>The duration of the backup</td>
</tr>
</tbody>
</table>

### 5.7.4 Monitoring FEP PGPool2

Information about pgpool2 activity and replication status can be found in the FEP server table and in the system view.

The pgpool2 statistics are updated according to the schedule specified in the parameter.

The tables and views that have been added are described below. The tables and views to be added are created under the fep_exporter schema in the postgres database on the FEP server.

<table>
<thead>
<tr>
<th>Table/View name</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>pgpool2_stat_load_balance</td>
<td>Load Balance Information in pgpool2</td>
</tr>
<tr>
<td>pgcluster_stat_replication</td>
<td>Replication State</td>
</tr>
<tr>
<td>pgpool2_stat_conn_pool</td>
<td>Connection Pool State for pgpool2</td>
</tr>
<tr>
<td>pgpool2_stat_sql_command</td>
<td>SQL Command Statistics</td>
</tr>
</tbody>
</table>

### 5.7.4.1 pgpool2_stat_load_balance view

Contains one row for MasterService and one row for ReplicaService.

<table>
<thead>
<tr>
<th>Column</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>node_id</td>
<td>integer</td>
<td>database node id (0 or 1)</td>
</tr>
<tr>
<td>status</td>
<td>text</td>
<td>status (up or down)</td>
</tr>
<tr>
<td>lb_weight</td>
<td>double precision</td>
<td>load-balancing weight</td>
</tr>
<tr>
<td>role</td>
<td>text</td>
<td>role (primary or standby)</td>
</tr>
<tr>
<td>last_status_change</td>
<td>timestamp with timezone</td>
<td>last status change time</td>
</tr>
</tbody>
</table>
5.7.4.2 pgpool2_stat_conn_pool view

Indicates the state of the connection pool. Contains connection pool information for each pcpool2 instance.

<table>
<thead>
<tr>
<th>Column</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pgpool2_node_id</td>
<td>integer</td>
<td>pgpool2 node id (0 - the number of pgpool2 instance -1)</td>
</tr>
<tr>
<td>pool_pid</td>
<td>integer</td>
<td>The PID of the displayed Pgpool-II process</td>
</tr>
<tr>
<td>start_time</td>
<td>timestamp with timezone</td>
<td>The timestamp of when this process was launched</td>
</tr>
<tr>
<td>pool_id</td>
<td>integer</td>
<td>The pool identifier (should be between 0 and max_pool - 1)</td>
</tr>
<tr>
<td>backend_id</td>
<td>integer</td>
<td>The backend identifier (should be between 0 and the number of configured backends minus one)</td>
</tr>
<tr>
<td>role</td>
<td>text</td>
<td>role (primary or standby)</td>
</tr>
<tr>
<td>database</td>
<td>text</td>
<td>The database name for this process's pool id connection</td>
</tr>
<tr>
<td>username</td>
<td>text</td>
<td>The user name for this process's pool id connection</td>
</tr>
<tr>
<td>create_time</td>
<td>timestamp with timezone</td>
<td>The creation time and date of the connection</td>
</tr>
<tr>
<td>majorversion</td>
<td>integer</td>
<td>The protocol version numbers used in this connection</td>
</tr>
<tr>
<td>minorversion</td>
<td>integer</td>
<td>The protocol version numbers used in this connection</td>
</tr>
<tr>
<td>pool_counter</td>
<td>integer</td>
<td>Counts the number of times this pool of connections (process) has been used by clients</td>
</tr>
<tr>
<td>pool_connected</td>
<td>boolean</td>
<td>True (1) if a frontend is currently using this backend</td>
</tr>
</tbody>
</table>

5.7.4.3 pgpool2_stat_sql_command view

Represents SQL command statistics.

<table>
<thead>
<tr>
<th>Column</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>node_id</td>
<td>integer</td>
<td>The backend identifier (should be between 0 and the number of configured backends minus one)</td>
</tr>
<tr>
<td>role</td>
<td>text</td>
<td>role (primary or standby)</td>
</tr>
<tr>
<td>select_cnt</td>
<td>integer</td>
<td>The numbers of SQL command: SELECT</td>
</tr>
<tr>
<td>insert_cnt</td>
<td>integer</td>
<td>The numbers of SQL command: INSERT</td>
</tr>
<tr>
<td>update_cnt</td>
<td>integer</td>
<td>The numbers of SQL command: UPDATE</td>
</tr>
<tr>
<td>delete_cnt</td>
<td>integer</td>
<td>The numbers of SQL command: DELETE</td>
</tr>
<tr>
<td>ddl_cnt</td>
<td>integer</td>
<td>The numbers of SQL command: DDL</td>
</tr>
<tr>
<td>other_cnt</td>
<td>integer</td>
<td>The numbers of SQL command: others</td>
</tr>
<tr>
<td>panic_cnt</td>
<td>integer</td>
<td>The numbers of failed commands</td>
</tr>
<tr>
<td>fatal_cnt</td>
<td>integer</td>
<td>The numbers of failed commands</td>
</tr>
<tr>
<td>error_cnt</td>
<td>integer</td>
<td>The numbers of failed commands</td>
</tr>
</tbody>
</table>

5.8 Event Notification

The eventing mechanism introduced, is to enable operator to raise customized Kubernetes events. The custom events will be raised during the creation of custom resources. Currently following events are raised.
5.8.1 Events raised

- **fepcluster** - During FEPCluster CR creation
  - Event is raised when FEPVolume CR creation is initiated and when FEPVolume CR creation initiation fails.
  - Event is raised when FEPConfig CR creation is initiated and when FEPConfig CR creation initiation fails.
  - Event is raised when FEPUser CR creation is initiated and when FEPUser CR creation initiation fails.
  - Event is raised when FEPCert CR creation is initiated and when FEPCert CR creation initiation fails.
  - Event is raised when Statefulset creation is successful and Statefulset creation fails.
  - Event is raised when PDB creation is successful and when PDB creation fails.
  - Event is raised when FEPBackup CR creation is initiated and when FEPBackup CR creation initiation fails.

---

Please note the following child CR events are raised as part of Create FEP Cluster

- **fepcert** - During FEPCert CR creation
  - Event is raised when FEPCert CR creation is successful, when FEPCert CR fails annotating FEPCluster and when FEPCert CR creation fails.

- **fepconfig** - During FEPConfig CR creation
  - Event is raised when FEPConfig CR creation is successful, when FEPConfig CR fails annotating FEPCluster and when FEPConfig CR creation fails.

- **fepvolume** - During FEPVolume CR creation
  - Event is raised when FEPVolume CR creation is successful, when FEPVolume CR fails annotating FEPCluster and when FEPVolume CR creation fails.

- **fepbackup** - During FEPBackup CR creation
  - Event is raised when FEPBackup cronjob1 creation is successful and when FEPBackup cronjob1 creation fails.
  - Event is raised when FEPBackup cronjob2 creation is successful and when FEPBackup cronjob2 creation fails.
  - Event is raised when FEPBackup cronjob3 creation is successful and when FEPBackup cronjob3 creation fails.
  - Event is raised when FEPBackup cronjob4 creation is successful and when FEPBackup cronjob4 creation fails.
  - Event is raised when FEPBackup cronjob5 creation is successful and when FEPBackup cronjob5 creation fails.

- **feppgpool2** - During FEPPgPool2 CR creation
  - Event is raised when FEPPgPool2 CR creation is successful and when FEPPgPool2 CR creation fails.
  - Event is raised when FEPPgPool2Cert CR creation is initiated and when FEPPgPool2Cert CR creation initiation fails.

---

Please note the following child CR event are raised as part of Create FEP PgPool2

- **feppgpool2cert** - During FEPPgPool2Cert CR creation
  - Event is raised when FEPPgPool2Cert CR creation is successful, when FEPPgPool2Cert CR fails annotating FEPPgPool2 and when FEPPgPool2Cert CR creation fails.

- **feprestore** - During FEPRestore CR creation
  - Event is raised when FEPRestore CR creation is successful and when FEPRestore CR creation fails.

5.8.2 Events that Occur when Custom Resources are Updated

If the "sysExtraEvent" parameter is specified in the custom resource, an event will be generated when changes to FEPCluster, FEPLogging, FEPExporter are detected, or when the changes are applied successfully/failed.

Refer to "Operator operation event notification" in "Reference" for information about events that occur.
5.8.3 Viewing the Custom Events

The custom events can be viewed on CLI as well as the Openshift console

On CLI

Executing the command

```
kubectl get events
```

OR

```
oc get events
```

Following is a snippet of the events output as shown when the above command is executed.

On openshift console

For the specific project/namespace the custom events can be viewed along with Kubernetes events under the events as shown in the following screenshot.

5.9 Scaling Replicas

5.9.1 Automatic Scale Out

Automatic scale out occurs when the average CPU utilization or number of connections of the DB container exceeds the threshold.

The maximum number of replica containers, excluding the master container, is 15.

If the load decreases after the number of replicas increases due to a temporary increase in load, the number of replicas will remain increased. Perform manual scale in if necessary.

Specify `spec.fepChildCrVal.autoscale.scaleout` in FEPClusterCR when you want to perform Automatic scale out. Refer to "FEPCluster Parameters" in the Reference for information about the values to specify.

```
$ oc edit fepcluster <FEPClusterCR name>
```
5.9.2 Manual Scale In/Out

To manually scale in or out of a FEPCluster, edit the "spec.fep.instances" in FEPClusterCR.

The value must be between 1 and 16. (Number of instances with one master)

```
$ oc edit fepcluster <FEPClusterCR name>
```

---

**Note**

- Do not scale in from two to one replica instance when the syncMode is 'on'. Update SQL cannot be executed.
- Any database connections to the replica Pod that are deleted during a scale in will be forced to disconnect.

---

5.10 Backing Up to Object Storage

Describes how to store backup data in object storage.

5.10.1 Pre-creation of Resources

5.10.1.1 Storing CA Files (Root Certificates)

If you want to use a non-default root certificate for object storage connections, register it in ConfigMap.

```
$ oc create configmap storage-cacert --from-file=ca.crt=storage-ca.pem -n my-namespace
```

5.10.1.2 Storing Repository Key

When using the parameter (repo-gcs-key) of pgBackRest, register the GCS repository key in Secret.

```
$ oc create secret generic storage-key-secret --from-file=key.json=storage-key.json -n my-namespace
```

5.10.2 Defining a FEPCluster Custom Resource

List the backup settings under spec.fepChildCrVal.backup in the FEPCluster custom resource.

Specify the object storage for the backup data in pgbackrestParams. Refer to "2.3.5 Scheduling Backup from Operator" for possible values for pgbackrestParams.

Specify the ConfigMap name created in "5.10.1.1 Storing CA Files (Root Certificates)" for caName.

FEPCluster Custom Resource Example: Only Object Storage Used for Backup Repository

```yaml
apiVersion: fep.fujitsu.io/v2
kind: FEPCluster
metadata:
  ...
spec:
  fepChildCrVal:
    backup:
      pgbackrestParams: |
        repol-type=s3
        repol-path=/backup/cluster1
        repol-s3-bucket=sample-bucket
        repol-s3-endpoint=s3.ap-northeast-1.amazonaws.com
        repol-s3-region=ap-northeast-1
        repol-storage-ca-file=/pgbackrest/storage-certs/ca.crt
        pgbackrestKeyParams: |
        repol-s3-key=SAMPLEKEY
        repol-s3-key-secret=SAMPLESECRET
```
If the persistent volume and object storage specified in spec.fepChildeCrVal.storage.backupVol are to be used together in the backup repository, specify the object storage setting after "repo2".

If "repo1" is not defined, a permanent volume is automatically designated as the storage destination for the backup volume.

FEPCluster Custom Resource Example: When using object storage and PV

```yaml
... spec:
  fepChildeCrVal:
    backup:
      pgbackrestParams: |
        repo2-type=s3
        repo2-path=/backup/cluster1
        repo2-s3-bucket= sample-bucket
        repo2-s3-endpoint=s3.ap-northeast-1.amazonaws.com
        repo2-s3-region=ap-northeast-1
        repo2-storage-ca-file=/pgbackrest/storage-certs/ca.crt
      pgbackrestKeyParams: |
        repo2-s3-key=SAMPLEKEY
        repo2-s3-key-secret=SAMPLESECRET
      caName:
        - storage-cacert
...```

When using object storage GCS as a backup repository, specify as follows.
For repoKeySecretName, specify the Secret created in "5.10.1.2 Storing Repository Key". Also, specify service for gcs-key-type.

FEPCluster Custom Resource Example: When using GCS as a backup repository

```yaml
apiVersion: fep.fujitsu.io/v1
kind: FEPCluster
metadata:
  ... spec:
    fepChildeCrVal:
      backup:
        pgbackrestParams: |
          repo1-type=gcs
          repo1-path=/backup-ct/test2
          repo1-gcs-bucket=dbaas-gcs
          repo1-gcs-endpoint=localhost
          repo1-storage-ca-file=/pgbackrest/storage-certs/ca.crt
          repo1-gcs-key=/pgbackrest/storage-keys/key.json
          repo1-gcs-key-type=service
        caName:
          - storage-cacert
        repoKeySecretName:
          - storage-key-secret
...```

5.11 Disaster Recovery

By using OSS (pg_backrest) functionality to store backup data in object storage, data can be migrated to a database cluster in a different OCP environment.
Even if it is difficult to operate in an OCP environment with a database cluster due to a disaster, it is possible to continue operating in a different OCP environment.

### 5.11.1 Disaster Recovery Prerequisites

The configuration diagram of the pod placement and backup repository, which are prerequisites for the backup feature for performing disaster recovery, is shown below.

In FEPCluster, to get a backup, specify the object storage as the backup data storage destination with `spec.fepChildCrVal.backup.pgbackrestParams`.

Specify object storage that is in an area that is considered safe for the scope of the expected disaster.

---

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>The definition of the FEPCluster custom resource is not inherited when performing disaster recovery.</td>
</tr>
<tr>
<td>We recommend that you save your production site FEPCluster custom resource definitions in case of a disaster.</td>
</tr>
</tbody>
</table>

### 5.11.2 Performing Disaster Recovery

Describes the procedure for restoring to an OCP environment different from the restore source using the backup data stored in the object storage.

#### 5.11.2.1 Pre-creation of Resources

##### 5.11.2.1.1 Storing CA Files (Root Certificates)

If you want to use a non-default root certificate for object storage connections, register it in ConfigMap.

```
$ oc create configmap storage-cacert --from-file=ca.crt=storage-ca.pem -n my-namespace
```

##### 5.11.2.1.2 Storing Repository Key

When using the parameter (repo-gcs-key) of pgBackRest, register the GCS repository key in Secret.

```
$ oc create secret generic storage-key-secret --from-file=key.json=storage-key.json -n my-namespace
```

#### 5.11.2.2 Defining a FEPCluster Custom Resource

In addition to the FEPCluster settings, specify the Restore settings below.

FEPCluster Custom Resource Example

```yaml
apiVersion: fep.fujitsu.io/v1
description: FEPCluster
kind: FEPCluster
```
When using object storage GCS as a backup repository, specify as follows.

For repoKeySecretName, specify the Secret created in "5.11.2.1.2 Storing Repository Key". Also, specify service for gcs-key-type.

<table>
<thead>
<tr>
<th>Field</th>
<th>Default</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>spec.fepChildCrVal.restore</td>
<td></td>
<td>Define when restoring by specifying the backup data stored in the object storage.</td>
</tr>
<tr>
<td>spec.fepChildCrVal.restore.pgbackrestParams</td>
<td></td>
<td>Optional</td>
</tr>
</tbody>
</table>

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>repo1-type=gcs</td>
<td></td>
<td>Specify the object storage where the backup data is stored.</td>
</tr>
<tr>
<td>repo1-path=/backup-ct/test2</td>
<td></td>
<td>If you want to use a root certificate other than the default, specify the following: repo1-storage-ca-path=/pgbackrest/storage-certs/&lt;file name&gt;</td>
</tr>
<tr>
<td>repo1-gcs-bucket=dbaas-gcs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>repo1-gcs-endpoint=localhost</td>
<td></td>
<td></td>
</tr>
<tr>
<td>repo1-storage-ca-file=/pgbackrest/storage-certs/ca.crt</td>
<td></td>
<td></td>
</tr>
<tr>
<td>repo1-gcs-key=/pgbackrest/storage-key/key.json</td>
<td></td>
<td></td>
</tr>
<tr>
<td>repo1-gcs-key-type=service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>caName: storage-cacert</td>
<td></td>
<td></td>
</tr>
<tr>
<td>repoKeySecretName: storage-key-secret</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Default</td>
<td>Details</td>
</tr>
<tr>
<td>-------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>spec.fepChildCrVal.restore.pgbkrestKeyParams</td>
<td></td>
<td>Optional&lt;br&gt;&quot;[]&quot; is fixed, and the following lines specify the parameters to set in pgbackrest.conf. The value described by this parameter is masked with ****. Specify the parameter you want to mask, such as a password.</td>
</tr>
<tr>
<td>spec.fepChildCrVal.restore.caName</td>
<td></td>
<td>Optional&lt;br&gt;Specify when you use a CA file other than the system default.&lt;br&gt;Specify the name of the created ConfigMap in list format.&lt;br&gt;The specified ConfigMap will be mounted in /pgbackrest/storage-certs.</td>
</tr>
<tr>
<td>spec.fepChildCrVal.restore.mcS pec.limits</td>
<td>cpu: 200m&lt;br&gt;memory: 300Mi</td>
<td>Optional&lt;br&gt;CPU and memory allocated to the container performing the restore.</td>
</tr>
<tr>
<td>spec.fepChildCrVal.restore.mcS pec.requests</td>
<td>cpu: 100m&lt;br&gt;memory: 200Mi</td>
<td>Optional&lt;br&gt;CPU and memory allocated to the container performing the restore.</td>
</tr>
<tr>
<td>spec.fepChildCrVal.restore.restoretype</td>
<td>latest</td>
<td>Optional&lt;br&gt;Restore Type (latest or PITR)</td>
</tr>
<tr>
<td>spec.fepChildCrVal.restore.redate</td>
<td></td>
<td>Optional&lt;br&gt;Specify the date to restore when spec.fepChildCrVal.restore.restoretype is &quot;PITR&quot;.</td>
</tr>
<tr>
<td>spec.fepChildCrVal.restore.reftime</td>
<td></td>
<td>Optional&lt;br&gt;Specify the time to restore when spec.fepChildCrVal.restore.restoretype is &quot;PITR&quot;.</td>
</tr>
<tr>
<td>spec.fepChildCrVal.restore.image</td>
<td></td>
<td>Optional&lt;br&gt;Image of the container to perform the restore.&lt;br&gt;It is omitted by default. In this case, the URL for image is obtained from the operator container environment.</td>
</tr>
<tr>
<td>spec.fepChildCrVal.restore.imag ePullPolicy</td>
<td>IfNotPresent</td>
<td>Optional</td>
</tr>
</tbody>
</table>

### 5.12 Operation of Transparent Data Encryption Using Key Management System

**5.12.1 Updating Custom Resource Parameters**

When using a newly generated master encryption key in your key management system, update the FEPCluster custom resource fepChildCrVal.sysTde.tdek.targetKeyId to the ID of the new master encryption key. The operator will automatically re-enable TDE when this value is updated.

Also, if the credentials for connecting with the key management system are updated, update the corresponding values in the FEPCluster custom resource. The operator automatically performs a keystore open when the credentials are updated.

When re-enabling TDE or opening the keystore is completed, the following event will be notified.

```bash
# When re-enabling TDE
$ kubectl get event
LAST SEEN   TYPE    REASON                     OBJECT                     MESSAGE
- 121 -
```
If the process fails, review the parameters defined in the FEP Cluster custom resource and re-enter the correct values.

If only the contents of the Secret or ConfigMap that stores the credentials are updated and the custom resource is not modified, open the keystore using the FEPAction custom resource described in "5.12.2 Update Credentials".

### 5.12.2 Update Credentials

If the credentials in the key management system are updated, update the contents of the corresponding Secret or ConfigMap. If there are no changes to the values specified in the FEP cluster custom resource, apply the FEPAction custom resource to update the credentials used by FEP.

Example) Definition example of FEPAction custom resource

```yaml
apiVersion: fep.fujitsu.io/v1
kind: FEPAction
metadata:
  name: new-fep-action
spec:
sysExtraLogging: false
targetClusterName: nf-131851
fepAction:
type: open_tde_masterkey
```

### 5.12.3 Encrypting a Tablespace

If you create an encrypted tablespace, configure the encryption algorithm in runtime parameters. For example, to create a tablespace named secure_tablespace using AES with a 256-bit key length as the encryption algorithm, define:

```sql
-- Specify the encryption algorithm for the tablespace to be created below
SET tablespace_encryption_algorithm = 'AES256';
CREATE TABLESPACE secure_tablespace LOCATION '/database/tablespaces/tbspace1';
-- Specify that the tablespace to be created below is not to be encrypted
SET tablespace_encryption_algorithm = 'none';
```

```
CREATE TABLESPACE tbs_tst_new LOCATION '/database/tablespaces/tbspace1' WITH (tablespace_encryption_algorithm = 'AES256');
```

Checking for encrypted tablespaces

You can check which tablespaces are encrypted by executing the following SQL.

```sql
SELECT spcname, spcencalgo FROM pg_tablespace ts, pgx_tablespaces tsx WHERE ts.oid = tsx.spcid;
```

### 5.12.4 Backup/Restore

In case the FEP cluster is damaged or lost, backups should be made at the following times:

- When the cluster is first created
- When the master encryption key is changed
When you use the FEPRestore custom resource to create a cluster restored from backup, the restored cluster is restored with the master encryption key at the time the backup was taken on the source cluster (where the backup was created from).

If a newer master encryption key is specified in sysTde.tdek.targetKeyId than when the source FEPCluster was backed up, the value will be carried over to the restore destination FEPCluster custom resource, and the operator automatically re-enables TDE with the new master encryption key after data recovery.

Also, update the authentication information to the key management system before executing the restore. If your credentials are not up-to-date, FEP will not be able to connect to the key management service and restore your data.

If you mistakenly update the information for connecting to the key management system under sysTde.tdek.kmsDefinition after building FEPCluster, FEP will not be able to refer to the key management system when restoring data. Before executing the restore process, confirm that the correct values are described in the FEPCluster custom resource.

### 5.12.5 Changing Key Management System Definitions

Modify the parameters under spec.fepChildCrVal.sysTde.tdek.kmsDefinition in the FEPCluster custom resource if you want to add or change the connection information to the key management system.

If you make any of the following changes, the replica server will be restarted with the new parameters. If there are multiple replica servers, they are restarted one at a time. When all replica servers are restarted, one of them is promoted to the new master server due to a switchover. The original master server's container image is then restarted. This allows you to change the definition of the key management system for all servers with minimal disruption.

- Add a new key management system definition
- Delete an existing key management system definition
- Change the order of key management system definitions
- Add, Delete, or rename ConfigMap or Secret resources that you specify as credentials

If you make changes that require a restart, temporarily disable the automatic scale out feature for the database before making the changes. The automatic scale out feature can be disabled with the spec.fepChildCrVal.autoscale.scaleout.policy parameter of the FEPCluster custom resource.

You cannot rename the ConfigMap/Secret resource that you currently specify as the credential for the key management system you are using as the keystore.

### 5.13 Confidential Management Support Feature

#### 5.13.1 Enabling Confidential Management Support Feature

When building FEPCluster, the extension "pgx_confidential_management_support" of the confidential management support feature was installed and set up in the following database.

- template1
- postgres
- Database specified in spec.fepChildCrVal.sysUsers.pgdb

In addition, when creating a confidential administrator role (spec.fepChildCeVal.sysUsers.pgSecurityUser), this role is assigned the following functions necessary for executing confidential management support feature.

- CREATE ROLE
- SELECT, INSERT, UPDATE, and DELETE privileges on all tables included in the extension

Therefore, immediately after FEPCluster is built, database objects can be managed by the confidential management support feature in a database in which the extension "pgx_confidential_management_support" is installed or in a database created from template1.

Refer to "Confidential Management Support" in the Fujitsu Enterprise Postgres Security Operation Guide for details on how to operate the security management support function.
Refer to "Tables Used by Confidential Management Support Feature" in the Fujitsu Enterprise Postgres Security Operation Guide for tables included in the extension.

In addition, if a database role other than the confidential administrator role needs to operate the confidential management support feature, such as by preparing a database role for each schema that manages database objects using the confidential management support feature, the confidential management support feature assigns the following privileges to the database role.

- CREATE ROLE
- SELECT, INSERT, UPDATE, and DELETE privileges on all tables included in the extension

When using the confidential management support feature to manage database objects created by other users, it is necessary to grant ownership of the database objects to the database role that operates the confidential management support feature.

Example) When giving ownership of the table "security_table" to the confidential administrator user "security_user"

```sql
ALTER TABLE security_table OWNER TO security_user;
```

The owner of the database object can be confirmed using the PostgreSQL meta-command "\d".

### 5.13.2 Monitoring Confidential Management Support Feature

You can forward pgAudit's audit logs to Elasticsearch using the FEP logging feature.

Analyze the transferred audit log and monitor for changes in privileges on database objects by unintended users.

For the FEP log feature, please refer to "4.9 FEP Logging".
Chapter 6 Maintenance Operations

This chapter describes the maintenance operation after deploying the container.

6.1 Minor Version Upgrade

Minor FEP version upgrade is done by replacing the image in FEPCluster customer resource with a new one. For the procedure, refer to "Minor Version Upgrade" in the Overview.

Update information can be found in the Red Hat catalog to see if a new FEP database server container has been released.

Upgrades are rolling updated, so you can localize downtime, but it is recommended that you avoid running during business hours as connected applications will result in connection errors.

Note

The upgrade process will cause an outage on the cluster for the duration to upgrade both Master and Sync Replica. If there is no Sync Replica in the cluster, the outage is limited to the length of time to upgrade the Master (or actually the failover time required to take another replica been promoted by patroni).

6.2 Cluster Master Switchover

You can switch a master instance to a replica instance in the event of a master instance performance failure or planned node maintenance.

Specify "switchover" for the action type of the FEPAction CR to update FEPAction CR.

Equivalent Kubernetes command: kubectl apply -f <new_spec>

The "switchover" action type requires the user to specify the name of the target cluster on which to perform the switchover. The args section is not needed for switchovers, as FEPAction internally identifies the pod to switch from and promotes a new master pod.

```yaml
spec:
  fepAction:
    type: switchover
    targetClusterName: new-fep
```

Refer to "FEPAction Custom Resource Parameters" in the Reference for more information on parameters.

6.3 Perform PITR and the Latest Backup Restore from Operator

It can be used to restore a database to a specific location due to an application failure or to prepare a duplicate database for production.

Restore process can restore data by creating a CR (FEPRestore CR) for the restore as follows:

```bash
oc create -f [Custom Resource Files]
```

Example)

```bash
$oc create -f config/samples/postgres_v1_restore.yaml
```

There are two methods of restoring: restoring data to an existing FEPCluster or restoring data to a new FEPCluster.

When restoring to an existing FEPCluster, information such as the FEPCluster name, IP address, and various settings remain the same.

If you restore to a new FEPCluster, the FEPCluster name is the one you specified in CR and the new IP address is also given. If the setting value is not specified, the new cluster will inherit the settings from the restore source cluster, but you can change the settings to create a new cluster by specifying them in CR.

6.3.1 Setting Item

Refer to "FEP Restore Custom Resource Parameters" in the Reference for the items to be set in a custom resource file.
6.3.2 After Restore

Switching connections to the new cluster

The restore creates a new FEPCluster. If necessary, you need to set up Pgpool-II and change the access point of the application to the new cluster or the new Pgpool-II.

Backup data of the destination cluster

PITR restores to the pre-restore time are not possible, because the backup of the destination cluster begins after the restore completes.

6.4 Major Version Upgrade

Describes the procedure for upgrading the major version of the operator and FEP container.

A major version upgrade of a FEP builds a new major version of the FEP in the same Namespace as the previous major version of the FEP. At this time, by defining the "spec.fepChildCrVal.upgrade" field in FEPClusterCR, the operator creates the upgrade execution container. The upgrade execution container uses the previous version of FEP Cluster specified in “spec.fepChildCrVal.upgrade.sourceCluster” as the data source FEPCluster and migrates the data to the newly created FEPCluster.

6.4.1 Pre-work on the Data Source FEP Cluster

Stop the running business application before executing the major version upgrade.

Next, edit "spec.fepChildCrVal.customPgHba" of the data source FEPCluster Custom Resource to allow the connection of the upgrade execution container.

The addresses that are allowed to connect are specified as follows:

```
<fep>-upgrade-pod.<fep>-upgrade-headless-svc.<namespace>.svc.cluster.local
```

<fep> specifies the name of the newly created FEPCluster Custom Resource.

The authentication method can be either trust/md5/cert.

Example of Editing a FEPCluster Custom Resource in a Data Source:

```
apiVersion: fep.fujitsu.io/v2
kind: FEPCluster
metadata:
  name: source-fep
  namespace: my-namespace
spec:
  fepChildCrVal:
    customPgHba: |
      host all all destination-fep-upgrade-pod. destination-fep-upgrade-headless-svc. my-namespace.svc.cluster.local trust
...
```

6.4.2 Operator Upgrade

Describes the instructions for upgrading the operator.

Note

After an operator upgrade, any custom resource configuration changes you defined in the previous version are not reflected in the container.

6.4.2.1 Uninstalling the Old Operator

Uninstall the old operator.
Select "Uninstall Operator" from "Operators"> "Installed Operators"> "Fujitsu Enterprise Postgres <Old version> Operator"> Actions.

6.4.2.2 Installing a New Version of the Operator

Refer to "Chapter 3 Operator Installation" to install the new version of the operator.

6.4.3 Major Version Upgrade of FEP

6.4.3.1 Creating a New FEPCluster CR

Refer to the Reference to define a new major version of the FEPCluster custom resource. At this time, allow the running upgrade container to connect as you did in "6.4.1 Pre-work on the Data Source FEP Cluster".

In addition, a major version upgrade of FEP is performed by defining the "spec.fepChildCrVal.upgrade" field, as in the following example of defining a FEPCluster custom resource.

The upgrade execution container uses PV to store dump files retrieved from the FEPCluster of the data source.

If you have not enabled the automatic PV provisioning feature in your Kubernetes environment, create a PV for the upgrade in addition to the new PV for the FEPCluster before creating the FEPCluster custom resource.

Also, edit "spec.fepChildCrVal.customPgHba" to allow the connection of the upgrade execution container, as in "6.4.1 Pre-work on the Data Source FEP Cluster".

Example of Defining a FEPCluster Custom Resource to Perform an Upgrade:

```
apiVersion: fep.fujitsu.io/v2
kind: FEPCluster
metadata:
  name: destination-fep
  namespace: my-namespace
spec:
  fep:
    ...
  fepChildCrVal:
    upgrade
    sourceCluster: source-fep-cluster
    storage:
      size: 8Gi
    customPgHba:
      host  all  all  destination-fep-upgrade-pod.destination-fep-upgrade-headless-svc.my-namespace.svc.cluster.local  trust
    ...
```

FEPCluster Custom Resource Fields "spec.fepChildCrVal.upgrade"

<table>
<thead>
<tr>
<th>Field</th>
<th>Default</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>spec.fepChildCrVal.upgrade</td>
<td>Optional</td>
<td>When this field is defined, a major version upgrade is performed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>However, if spec.fepChildCrVal.restore is defined, the FEPCluster build stops.</td>
</tr>
<tr>
<td>spec.fepChildCrVal.upgrade.sourceCluster</td>
<td></td>
<td>Specify the FEPCluster CR name of the data migration source.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Be sure to specify spec.fepChildCrVal.upgrade when defining it.</td>
</tr>
<tr>
<td>Field</td>
<td>Default</td>
<td>Details</td>
</tr>
<tr>
<td>-------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>spec.fepChildCrVal.upgrade.mcSpec.limits</td>
<td></td>
<td>Optional Specify the maximum number of resources allocated to the upgrade execution container.</td>
</tr>
<tr>
<td>spec.fepChildCrVal.upgrade.mcSpec.requests</td>
<td></td>
<td>Optional Specify the lower limit of resources allocated to the upgrade execution container.</td>
</tr>
<tr>
<td>spec.fepChildCrVal.upgrade.image</td>
<td></td>
<td>Optional If omitted, the URL of the image is obtained from the operator container environment.</td>
</tr>
<tr>
<td>spec.fepChildCrVal.upgrade.imagePullPolicy</td>
<td>IfNotPresent</td>
<td>Optional Specify the pull policy for the container image. <code>Always</code>, <code>IfNotPresent</code>, <code>Never</code></td>
</tr>
<tr>
<td>spec.fepChildCrVal.upgrade.source.pgAdminTls.certificateName</td>
<td></td>
<td>Optional If the data source FEPCluster used &quot;cert&quot; as the authentication method for the Upgrade Execution Container, use the secret certificate that defines <code>spec.fepChildCrVal.sysUsers.pgAdminTls.certificateName</code> for the data source FEPCluster. If the above parameter is not defined, it points to the Kubernetes TLS secret containing the certificate of the Postgres user &quot;postgres&quot; in the data source. Refer to &quot;4.7.1 Manual Certificate Management&quot; for information about creating secrets.</td>
</tr>
<tr>
<td>spec.fepChildCrVal.upgrade.destination.pgAdminTls.certificateName</td>
<td></td>
<td>Optional If the newly created FEPCluster used the &quot;cert&quot; authentication method for the running upgrade container, use the secret certificate that defines the <code>spec.fepChildCrVal.sysUsers.pgAdminTls.certificateName</code> of the newly created FEPCluster. If the above parameter is not defined, it points to the</td>
</tr>
</tbody>
</table>
Field | Default | Details
---|---|---

| Kubernetes TLS secret containing the certificate of the newly created Postgres user "postgres". Refer to "4.7.1 Manual Certificate Management" for information about creating secrets. |

| spec.fepChildCrVal.upgrade.storage | Optional | Defines storage for storing dump files. |

| spec.fepChildCrVal.upgrade.storage.storageClass | Optional | If omitted, the default storage class of the operating environment will be used. |

| spec.fepChildCrVal.upgrade.storage.size | 2Gi | Optional | Specify the size of the storage to store the dump file. |

| spec.fepChildCrVal.upgrade.storage.accessModes | ReadWriteOnce | Optional | Storage access mode for storing dump files As an array of access modes. e.g. [ReadWriteMany] If omitted, it is treated as [ReadWriteOnce]. |

---

**Note**

Connect to the database and run the following SQL to check the size of the database in advance:

```sql
$ SELECT pg_size_pretty(sum(pg_database_size(datname))) AS dbsize FROM pg_database;
```

Since the pg_dumpall command used in the upgrade execution container outputs the database data as an SQL command, the file actually created is as follows.

For example, the integer type 2147483647 is 4 bytes for database data.

However, this is 10 bytes because SQL commands output them as strings. Therefore, make sure that the storage (PV) for dump files has sufficient disk space.

---

### 6.4.3.2 Verifying FEP Major Upgrade Complete

If you migrate your data to the new FEPCluster and the FEP major version upgrade is successful, the following event will be output:

```bash
$ kubectl get event
LAST SEEN  TYPE    REASON               OBJECT                                     MESSAGE
164m       Normal  SuccessfulFepUpgrade fepupgrade/<Name of the new FEPClusterCR> <namespace>, Successfully FEP Upgrade
```

In addition, the following annotation will be added to YAML in FEPClusterCR:
When a major upgrade of FEP fails, an event similar to the following is output:

```
$ kubectl get event
LAST SEEN   TYPE     REASON            OBJECT                                     MESSAGE
164m        Warning  FailedFepUpgrade  fepupgrade/<Name of the new FEPClusterCR> <namespace>, Error/Failure in FEP Upgrade
```

Obtain the Kubernetes resource information listed in the OBJECT column, review the output messages, and then recreate the new FEPCluster custom resource.

```
$ kubectl describe fepupgrade/<Name of the new FEPClusterCR>
```

### 6.4.4 Updating Each Custom Resource

Describes the procedures for each custom resource used to operate the FEPCluster for the data source after the major FEP upgrade is complete.

After this process is complete, resume the suspended business applications.

#### 6.4.4.1 Removing a FEPClusterCR for a Data Source

Delete the FEPCluster for the data source.

For the Openshift GUI console:

From "Operators" > "Installed Operators" > "Fujitsu Enterprise Postgres < New version > Operator" > "FEPCluster" > "FEPCluster name to delete" > Actions, select "Delete FEPCluster".

#### 6.4.4.2 FEPPgpool2

Re-create FEPPgpool2 to match the version of the client with the version of the upgraded FEP.

#### 6.4.4.3 FEPExporter Built in Standalone Mode

Edit the FEPExporter custom resource "spec.fepExporter.fepClusterList" to specify the new version of the FEPCluster custom resource.

Refer to "FEPExporter Custom Resource" in the Reference for more information about the parameters.

### 6.5 Assigned Resources for Operator Containers

The following resources are allocated by default to the operator containers provided by this product.

```
resources:
limits:
  cpu: 2
  memory: 1536Mi
requests:
```

---

```yaml
apiVersion: fep.fujitsu.io/v2
kind: FEPCluster
metadata:
  annotations:
  - FEPUpgradeDone: true
  name: destination-fep-cluster
  namespace: my-namespace
spec:
...
```
If there is only one FEPCluster custom resource managed by an operator, it can be operated with the resource assigned by default. However, when deploying and operating multiple FEPCluster custom resources, change the assigned resource of the operator container.

**Note**

If you have changed the resource, the resource value will revert to the default value after the operator version upgrade. Therefore, change the resource again after upgrading the operator.

### 6.5.1 How to Change Assigned Resources

Describes how to change the resources assigned to an operator container.

When updating resources assigned to an operator container, the operator container is recreated. At this time, the operation of already built containers such as FEPCluster will not stop.

How you change the allocated resources depends on how the operator was installed.

#### 6.5.1.1 When installing using OperatorHub

If you are using an operator installed from OperatorHub To change the resources assigned to the operator container, edit the ClusterServiceVersion (CSV).

Editing the CSV "spec.install.spec.deployments[0].spec.template.spec.containers[0].resources" will recreate the operator container and apply the specified resources.

**When editing CSV from the OCP GUI console**

Click [Installed Operators] in the menu item under Operators and select the installed operator. On the [YAML] tab, edit the specified part of the allocation resource and click [Save].

#### When editing CSV from the CUI console using the OC client

Check the CSV name of the installed operator with the “oc get” command.

```
$ oc get csv
NAME                 DISPLAY                                               VERSION REPLACES PHASE
fujitsu-enterprise-postgres-operator.v4.1.5  Fujitsu Enterprise Postgres Operator 4.1.5 Succeeded
```
6.5.1.2 When installing using Helm Chart or RancherUI

If the operator is installed using Helm Chart or RancherUI, edit the deployment of the operator container to change the resources assigned to the operator container.

Editing the Deployment's "spec.template.spec.containers[0].resources" will recreate the operator container and apply the specified resources.

Edit the Deployment "fep-ansible-operator" with the "kubectl edit" command.

```
$ kubectl get deployment fep-ansible-operator
NAME                   READY   UP-TO-DATE   AVAILABLE   AGE
fep-ansible-operator   1/1     1            1           2m10s
$ kubectl edit deployment fep-ansible-operator
```

6.6 Using SUPERUSER Privilege

6.6.1 CREATE EXTENSION

When executing the CREATE EXTENSION command to install external extensions for PostgreSQL, there are extensions that can only be installed by SUPERUSER. To install such extensions we make use of the FEPAction custom resource.

By specifying "create_extension" in spec.fepAction.type of FEPAction custom resource, CREATE EXTENSION can be executed for the specified FEPCluster container.

Please refer to the Reference for how to use.

6.6.2 Change Password of SUPERUSER

To update the password of SUPERUSER "postgres", specify update_admin_password for fepActionType of the FEPAction custom resource.

Recreate the password with a random value and update it.

Please refer to the Reference for how to use.

6.6.3 Using SUPERUSER

If SUPERUSER privileges are required for database operation, you can obtain the password for SUPERUSER "postgres" by following the steps below.

1. Get the base64-encoded password from the Secret with the same name as the FEPCluster custom resource name.

   Example) When the FEPCluster custom resource name is new-fep

   ```
   $ kubectl get -o yaml secret new-fep | grep PG_ADMIN_PASSWORD
   PG_ADMIN_PASSWORD: YWRtaW4tcGFzc3dvcmQ=
   ```

2. Decode the obtained password.

   ```
   $ echo YWRtaW4tcGFzc3dvcmQ= | base64 -d
   admin-password
   ```
In order to prevent SUPERUSER from being used by a third party, please set Kubernetes Role permissions to the Secret so that only the database administrator can refer it.
Chapter 7 Abnormality

This chapter describes the actions to take when an error occurs in the database or an application, while FEP is operating.

Depending on the type of error, recover from the backed-up material, reserve capacity, check the operator log, and check the FEP log.

7.1 Handling of Data Abnormalities

Recover the database cluster from the backup immediately prior to failure in any of the following cases:

- A hardware failure occurs on the data storage disk or the backup data storage disk.
- If the data on the disk is logically corrupted and the database does not work correctly
- Data corruption caused by user error

Refer to "6.3 Perform PITR and the Latest Backup Restore from Operator" for restore instructions.

7.2 Handling when the Capacity of the Data Storage Destination or Transaction Log Storage Destination is Insufficient

If you run out of space in the data storage location, first check if there are any unnecessary files on the disk, and then delete them so that you can continue working.

If deleting unnecessary files does not solve the problem, you may need to migrate the data to a larger disk.

Use a backup restore to migrate data.

7.3 What to do when the Capacity of the Backup Data Storage Area is Insufficient

If you run out of space in the backup data destination, first check the disk for unnecessary files, and then delete the unnecessary files. Or reduce the backup retention generation.

7.4 Handling Access Abnormalities When Instance Shutdown Fails

If an instance fails to start or stop, refer to the Operator log and the FEP log to determine the cause.

For checking the operator log and the FEP log, refer to "7.5 Collection of Failure Investigation Information".

7.5 Collection of Failure Investigation Information

If the cause of the trouble that occurred during the construction or operation of the environment is not identified, information for the initial investigation is collected.

I will explain how to collect information for the initial investigation.

- Product log
- Operator log

Product log

FEP log

Get into the container and collect the log.

The log location is specified by log_directory in the custom resource FEP Clusterspec.startupValues.customPgParam parameter. The default is/database/log.
Pgpool-II log

Get into the container and collect the log.
The log location is /var/log/pgpool/pool.log.

Operator log

Check the operator log as follows.

Verification Example

```
$ oc get po
NAME                                     READY   STATUS    RESTARTS   AGE
fep-ansible-operator-7dc5fd9bf7-4 smzk   1/1     Running   0          20m
```

How to check the log

```
$ oc logs pod fep-ansible-operator-7dc5fd9bf7-4 smzk -c manager
```

The log will be output to the console. Please check the file output by redirection.
Appendix A  Quantitative Values and Limitations

A.1 Quantitative Values

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

A.2 Limitations

Note

If you log in to a container and edit the configuration file directly, restarting the container may undo your changes.

If you want to change the settings, modify the custom resource files as described in "5.2 Configuration Change" and reapply. Depending on the parameters to be changed, the container may be redeployed. Refer to "5.2 Configuration Change" for details of the parameters.

Unavailable FEP features

Since FEP server container is based on other components (like UBI and Patroni), there are certain limitations that doesn’t allow it to be 100% functionally capable to VM based server instance. The known limitations are as below.

<table>
<thead>
<tr>
<th>No</th>
<th>Limitation</th>
<th>Reason for Limitation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Crypto Express cards are not supported</td>
<td>IBM LinuxOne doesn’t support CryptoExpress cards in Openshift container platform at this stage.</td>
<td>FEP TDEz extension cannot be used on LinuxOne Openshift environment. However, User can still use TDE on both LinuxOne Openshift environment as well as Azure (x86) Openshift environment.</td>
</tr>
</tbody>
</table>

Fixed parameter

Some parameters cannot be changed. Refer to "2.3.5.2 Parameters that cannot be Set".

FEP features that needs to be set when using

Refer to "2.3.7 FEP Unique Feature Enabled by Default".
Appendix B Adding Custom Annotations to FEPCluster Pods using Operator

This section describes instructions for adding custom annotations to a FEPCluster pod.

1. In YAML view of the Create FEPCluster section, add custom annotations as below and then click on Create.
2. Both the Statefulset and its resulting pods will be annotated with your provided annotations: archivewalVol and backupVol must be ReadWriteMany.
Appendix C  Utilize Shared Storage

Explains how to build a FEPCluster when using shared storage.

Use a disk where PV accessModes can specify ReadWriteMany.

This chapter shows an example of using NFS as PV in static provisioning.

C.1  Creating a StorageClass

Create a StorageClass.

In the OCP WebGUI screen, click “StorageClass” in the main menu “Storage”, then press “Create Storage Class” > “Edit YAML” and edit YAML to create the StorageClass.

If you are using the CLI, create a yaml file and create a StorageClass with the following command:

$ oc create -f <file_name>.yaml

YAML definitions are created with reference to the following samples.

Example)

```yaml
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: < StorageClass Name >
provisioner: kubernetes.io/no-provisioner
reclaimPolicy: Delete
volumeBindingMode: WaitForFirstConsumer
```

C.2  Creating a PersistentVolume

Create as many PersistentVolumes (PV) as you need.

On the Web GUI screen, click “PersistentVolumes” in the main menu “Storage”, click “Create PersistentVolume”, and edit YAML to create PV.

If you are using the CLI, create a yaml file and create a PV using the following command:

$ oc create -f <file_name>.yaml

YAML definitions are created with reference to the following samples.

The StorageClass name specifies the StorageClass created in "C.1 Creating a StorageClass".

Assign a different NFS directory for each PV.

In addition, accessModes is ReadWriteMany.

Example)

```yaml
apiVersion: v1
kind: PersistentVolume
metadata:
  name: < PV name >
spec:
  capacity:
    storage: < Capacity Required ex.8Gi >
  accessModes:
  - ReadWriteMany
  persistentVolumeReclaimPolicy: Retain
  mountOptions:
  - hard
  nfs:
```
C.3 Creating FEPCluster

Specifies that ReadWriteMany PV is used in the YAML definition in step 4 of "4.1 Deploying FEPCluster using Operator".

In spec.fepChildCRVal.storage, specify the StorageClass and AccessModes of the PV created in "C.2 Creating a PersistentVolume". The "spec.fepChildCRVal.storage.<Volume Type>.size" should be less than or equal to the PV allocated.

Example) Using PV created by archivewalVol and backupVol

```yaml
apiVersion: fep.fujitsu.io/v2
kind: FEPCluster
metadata:
  name: t3-fep
spec:
  - Suppress -
    fepChildCrVal:
      storage:
        archivewalVol:
          size: < Capacity Required ex. 8Gi >
          storageClass: <StorageClass name created in C.1 Creating a StorageClass*> 
          accessModes:
            - "ReadWriteMany"
        backupVol:
          size: < Capacity Required ex. 8Gi >
          storageClass: <StorageClass name created in C.1 Creating a StorageClass*> 
          accessModes:
            - "ReadWriteMany"
  - Suppress -
```

path: < NFS directory path (Assign a different directory for each PV) ex. /nfs/pv >
server: < IP address of the NFS server ex. 192.168.1.10> 
storageClassName: < StorageClass name created in "C.1 Creating a StorageClass" >
Appendix D  Key Management System Available for Transparent Data Encryption

Describes the key management system available for transparent data encryption.

D.1  KMIP Server

Refer to "To Connect to a key Management System Using the KMIP Protocol" in the Fujitsu Enterprise Postgres Installation and Setup Guide for Server for KMIP server requirements.

D.2  AWS Key Management Service

D.2.1  Available Services

By using the AWS KMS adapter, you can use encryption keys on the Key Management Service (hereafter referred to as AWS KMS) provided by AWS. There is no region restriction as long as it is a region supported by AWS KMS.

D.2.2  Available AWS KMS Keys

The KMS key's key spec must be "symmetric". "asymmetric" keys cannot be used. Also, the KMS key usage must be ENCRYPT_DECRYPT.

D.2.3  Required Privileges

For the KMS key to be used, the following operations must be permitted for the user accessing AWS KMS.

- Encrypt
- Decrypt
- DescribeKey

D.2.4  Key ID

The following can be specified as key IDs for the TDE key management system linkage feature.

- Key ARN

D.3  Azure Key Management Service

D.3.1  Available Services

Accessible via Azure's Key Vault API using the Azure KMS Adapter, and a key management service is available that allows you to use symmetric keys.

See

Refer to below for key management services for which symmetric keys are available.

Refer to below for Azure key management services.
https://learn.microsoft.com/en-us/azure/security/fundamentals/key-management#azure-key-management-services
D.3.2 Available Keys
A symmetric key is available.

D.3.3 Available Algorithms
The following algorithms are available during encryption/decryption operations.
- A256GCM

D.3.4 Key Operation
For the key to be used, the following operations must be permitted for the user who accesses Azure's key management service.
- encrypt
- decrypt
- get

D.3.5 Key ID
The following can be specified as key IDs for the TDE key management system linkage feature.
- Key object identifier

D.3.6 Sign In
Sign in to Azure using your service principal. You will need your application ID, tenant ID, and credentials to sign in.

See
Refer to below for service principals.