

FUJITSU Enterprise Postgres 12 for Kubernetes



Reference Guide

Preface

Purpose of this document

This document is a reference, and explains parameter.

Intended readers

This document is aimed at people who manage and operate.

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 Custom Resource Parameters](#)

Explains the parameter.

Abbreviations

The following abbreviations are used in this manual:

Full Name	Abbreviations
FUJITSU Software Enterprise Postgres for Kubernetes FUJITSU Software Enterprise Postgres	FEP or FUJITSU Enterprise Postgres
Transparent Data Encryption	TDE
Custom Resource	CR
Custom Resource Definition	CRD
Persistent Volume	PV

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 ("IBM") in the U.S. and other countries.

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.

Issue date and version

Edition 4.0: October 2022
Edition 3.0: November 2021
Edition 2.0: April 2021
Edition 1.0: March 2021

Copyright

Copyright 2021-2022 FUJITSU LIMITED

Contents

Chapter 1 Custom Resource Parameters.....	1
1.1 FEPCluster Parameter.....	1
1.2 Custom Resource Parameters.....	9
1.2.1 FEPCluster Custom Resource Parameters.....	9
1.2.2 FEP Cluster Configuration	14
1.2.3 FEPConfig Child Custom Resource Parameters.....	14
1.2.4 FEPUser Child Custom Resource Parameters.....	17
1.2.5 FEPCert Child Custom Resource Parameters.....	20
1.2.6 FEPCert Child Custom Resource Parameters.....	20
1.2.7 FEPCluster Child Custom Resource Parameters.....	21
1.2.8 FEPCluster Custom Resource Parameters.....	23
1.2.9 FEPCluster Custom Resource Parameters.....	25
1.2.10 FEPCluster Custom Resource Parameters.....	29
1.2.10.1 FEPCluster Specific Operation Details.....	31

Chapter 1 Custom Resource Parameters

This chapter explains the parameter.

1.1 FEPCluster Parameter

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

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

Initial configuration and subsequent changes to FEP Cluster are done through FEP Cluster CR.

Field	Default	Details
metadata.name	new-fep	Name for the Cluster. FEP server container will use this value for Patroni scope. e.g. new-fep
spec.fep.customAnnotation.allDeployments	{ } (*)	Contents under this are optional. User can remove { } and add multiple key-value pairs. All of these pair will be added to annotations of FEP statefulSet and FEP Pods. If left at default, no annotation is added to Pods and statefulSets
spec.fep.image.image	<omitted>	FEP server container image to be used quay.io/fujitsu/fujitsu-enterprise-postgres-12-server:ubi8-12-1.1 It is optional. Image line is omitted by default. In such a case, it will pick up URL of image from operator container environment. If you specify the image, Operator will take that image to deploy fep container
spec.fep.image.pullPolicy	IfNotPresent	
spec.fep.mcSpec.limits	cpu: 500m memory: 700Mi	
spec.fep.mcSpec.requests	cpu: 200m memory: 512Mi	
spec.fep.sysExtraLogging	false	To turn extra debugging on, set value to true It can be turned on/off at any time
spec.fep.instances	1	Number of nodes in the cluster, including both Master and Replicas. In Example CR, it is kept at 1 for certification. However, user can change it to 3 for 1 master and 2 replicas.
spec.fep.servicePort	27500	TCP port for FEP master service
spec.fep.syncMode	off	Replication Mode:

Field	Default	Details
		off - async replication on - sync replication
spec.fep.forceSsl	true	Controls that the communication to the server should only be via SSL. Changes are reflected in pg_hba.conf
spec.fep.podAntiAffinity	false	Defines that all the pods should not run on same worker node
spec.fep.podDisruptionBudget	false	Allows to maintain minimum number of pods of an application even when some nodes are voluntarily drained for say, maintenance
spec.fep.usePodName		Setting this key to true will make internal POD communication, both Patroni and Postgres to use hostname, instead of IP address. This is important for TLS as the hostname of the POD is predictable and can be used to create Server Certificate, whereas IP address is unpredictable and cannot be used to create Certificate. There is no negative effect setting this key to true even if TLS (i.e. Server Certificate) is not used.
spec.fep.patroni.tls.certificateName		This points to Kubernetes TLS secret that contains the certificate for Patroni. The certificate itself is stored in the key tls.crt. This field is optional. When this key is set, the Operator will ignore the value in systemCertificates
spec.fep.patroni.tls.caName		This points to Kubernetes configmap that contains additional CA for Patroni to verify client. The CA is stored in the key ca.crt. This field is optional.
spec.fep.postgres.tls.certificateName		This points to Kubernetes TLS secret that contains the certificate for Postgres. The certificate itself is stored in the key tls.crt. This field is optional. When this value is set, Operator will ignore the value in systemCertificates
spec.fep.postgres.tls.caName		This points to Kubernetes configmap that contains additional CA for Postgres to verify client. The CA is stored in the key ca.crt. This field is optional.
spec.fepChildCrVal.backup.image.image	<omitted>	FEP backup container image to be used quay.io/fujitsu/fujitsu-enterprise-postgres-12-backup:ubi8-12-1.1' It is optional. Image line is omitted by default. In such a case, it will pick up URL of image from operator container environment.

Field	Default	Details
		If you specify the image, Operator will take that image to deploy backup container
spec.fepChildCrVal.backup.image.pull Policy	IfNotPresent	
spec.fepChildCrVal.backup.mcSpec.limits	cpu: 0.2 memory: "300Mi"	
spec.fepChildCrVal.backup.mcSpec.requests	cpu: 0.1 memory: "200Mi"	
spec.fepChildCrVal.backup.pgbackrest Params	[global] repo1-retention-full=7 repo1-retention-full-type=time log-path=/database/log/backup	" " When nothing is specified, and the parameter set in pgbackrest.conf is described from the line below.
spec.fepChildCrVal.backup.schedule.num	2	Number of schedules to set The maximum number of backup schedules is 5.
spec.fepChildCrVal.backup.schedule.schedule1.schedule	15 0 * * 0	Backup <i>schedule</i> in cron format. The date and time is UTC time.
spec.fepChildCrVal.backup.schedule.schedule1.type	full	full: Perform a full backup (Back up the contents of the database cluster). incr - Perform an incremental backup (Back up only the database cluster files that were changed to the last backup migration).
spec.fepChildCrVal.backup.schedule.schedule2.schedule	15 0 * * 1-6	Backup schedule in cron format. The date and time is UTC time.
spec.fepChildCrVal.backup.schedule.schedule2.type	incr	full: Perform a full backup (Back up the contents of the database cluster). incr - Perform an incremental backup (Back up only the database cluster files that were changed to the last backup migration).
spec.fepChildCrVal.customPgAudit	[output] logger = 'auditlog' log_directory = '/database/log/audit' log_truncate_on_rotation = on log_filename = 'pgaudit-%a.log' log_rotation_age = 1d log_rotation_size = 0 [rule]	PgAudit file content
spec.fepChildCrVal.customPgHba	# define pg_hba custom rules here to be merged with default rules.	Entries to be inserted into pg_hba.conf

Field	Default	Details
	# TYPE DATABASE USER ADDRESS METHOD	
spec.fepChildCrVal.customPgParams	<pre># define custom postgresql.conf parameters below to override defaults. # Current values are as per default FEP deployment shared_preload_libraries='pgx_datamas king,pg_prewarm,pg_stat_statements' session_preload_libraries='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_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</pre>	Postgres configuration in postgresql.conf

Field	Default	Details
	<pre>log_min_messages = WARNING log_destination = stderr # wal_archive parameters in default fep installation archive_mode = on archive_command = 'pgbackrest -- stanza=backupstanza --config=/ database/userdata/pgbackrest.conf archive-push %p' wal_level = replica max_wal_senders = 12 wal_keep_segments = 64 track_activities = on track_counts = on</pre>	
spec.fepChildCrVal.storage.dataVol.size	2Gi (**)	Size of data volume. Data volume must be specified
spec.fepChildCrVal.storage.dataVol.storageClass	<omitted> (*)	StorageClass for data volume: When this line is omitted, the PV created will use default storage class in the Kubernetes cluster
spec.fepChildCrVal.storage.dataVol.accessModes	<omitted> (*)	accessModes for data volume: Specified as an array of accessModes e.g. [ReadWriteMany] If omitted, it will be treated as [ReadWriteOnce]
spec.fepChildCrVal.storage.walVol.size	1200Mi (**)	Size of WAL volume. WAL volume must be specified
spec.fepChildCrVal.storage.walVol.storageClass	<omitted> (*)	StorageClass for WAL volume: When this line is omitted, the PV created will use default storage class in the Kubernetes cluster
spec.fepChildCrVal.storage.walVol.accessModes	<omitted> (*)	accessModes for WAL volume: Specified as an array of accessModes e.g. [ReadWriteMany] If omitted, it will be treated as [ReadWriteOnce]
spec.fepChildCrVal.storage.tablespaceVol.size	512Mi (**)	Size of tablespace volume. This volume is optional and can be omitted
spec.fepChildCrVal.storage.tablespaceVol.storageClass	<omitted> (*)	StorageClass for tablespace volume: When this line is omitted, the PV created will use default storage class in the Kubernetes cluster

Field	Default	Details
spec.fepChildCrVal.storage.tablespaceVol.accessModes	<omitted> (*)	accessModes for tablespace volume: Specified as an array of accessModes e.g. [ReadWriteMany] If omitted, it will be treated as [ReadWriteOnce]
spec.fepChildCrVal.storage.archivewalVol.size	1Gi (*)	Size of archivewal volume. This volume is optional and can be omitted
spec.fepChildCrVal.storage.archivewalVol.storageClass	<omitted> (*)	StorageClass for Archived WAL volume: When this line is omitted, the PV created will use default storage class in the Kubernetes cluster When the number of instance is more than 1 and backup is not done on S3, both archivewalVol and backupVol must be hosted on Shared storage such as NFS with respective storageClass
spec.fepChildCrVal.archivewalVol.accessModes	<omitted> (*)	accessModes for Archived WAL volume: Specified as an array of accessModes e.g. [ReadWriteMany] If omitted, it will be treated as [ReadWriteOnce] When the number of instance is more than 1 and backup is not done on S3, both archivewalVol and backupVol must be hosted on Shared storage such as NFS with accessMode set to [ReadWriteMany]
spec.fepChildCrVal.logVol.size	1Gi (*)	Size of log volume. This volume is optional and can be omitted
spec.fepChildCrVal.logVol.storageClass	<omitted> (*)	StorageClass for log volume: When this line is omitted, the PV created will use default storage class in the Kubernetes cluster
spec.fepChildCrVal.logVol.accessModes	<omitted> (*)	accessModes for log volume: Specified as an array of accessModes e.g. [ReadWriteMany] If omitted, it will be treated as [ReadWriteOnce]
spec.fepChildCrVal.backupVol.size	2Gi (*)	Size of backup volume. This volume is optional and can be omitted
spec.fepChildCrVal.backupVol.storageClass	<omitted>	StorageClass for backup volume:

Field	Default	Details
	(*)	<p>When this line is omitted, the PV created will use default storage class in the Kubernetes cluster</p> <p>When the number of instance is more than 1 and backup is not done on S3, both archivalVol and backupVol must be hosted on Shared storage such as NFS with respective storageClass</p>
spec.fepChildCrVal.backupVol.accessModes	<omitted> (*)	<p>accessModes for backup volume:</p> <p>Specified as an array of accessModes e.g. [ReadWriteMany]</p> <p>If omitted, it will be treated as [ReadWriteOnce]</p> <p>When the number of instance is more than 1 and backup is not done on S3, both archivalVol and backupVol must be hosted on Shared storage such as NFS with accessMode set to [ReadWriteMany]</p>
spec.fepChildCrVal.sysUsers.pgAdminPassword	admin-password	Password for user "postgres"
spec.fepChildCrVal.sysUsers.pgdb	mydb (*)	Database to be created during provisioning
spec.fepChildCrVal.sysUsers.pguser	mydbuser (*)	Database user to be created during provisioning
spec.fepChildCrVal.sysUsers.pgpassword	mydbpassword	Password for database user pguser
spec.fepChildCrVal.sysUsers.pgrepluser	repluser (*)	Database user for replication
spec.fepChildCrVal.sysUsers.pgreplpassword	repluserpwd	Password for database user repluser
spec.fepChildCrVal.sysUsers.tdepassphrase	tde-passphrase	TDE keystore passphrase
spec.fepChildCrVal.sysUsers.pgRewindUser	rewind_user	Database user for Rewind
spec.fepChildCrVal.sysUsers.pgRewindUserPassword	rewind_password	Password for database user rewinduser
spec.fepChildCrVal.sysUsers.pgAdminTls.certificateName		This points to Kubernetes TLS secret that contains the certificate of Postgres user "postgres". Patroni will use this for certificate authentication. The certificate itself is stored in the key tls.crt. This field is optional.
spec.fepChildCrVal.sysUsers.pgAdminTls.caName		This points to Kubernetes configmap that contains additional CA the client use to verify a server certificate. The CA is stored in the key ca.crt. This field is optional.

Field	Default	Details
spec.fepChildCrVal.sysUsers.pgAdminTls.sslMode	prefer	Specify the type of TLS negotiation with the server. <ul style="list-style-type: none"> - disable - allow - prefer - require - verify-ca - verify-full
spec.fepChildCrVal.sysUsers.pgreplUserTls.certificateName		This points to Kubernetes TLS secret that contains the certificate of Postgres user “repluser”. Patroni will use this for certificate authentication. The certificate itself is stored in the key tls.crt. This field is optional.
spec.fepChildCrVal.sysUsers.pgreplUserTls.caName		This points to Kubernetes configmap that contains additional CA the client use to verify a server certificate. The CA is stored in the key ca.crt. This field is optional.
spec.fepChildCrVal.sysUsers.pgreplUserTls.sslMode	prefer	Specify the type of TLS negotiation with the server. <ul style="list-style-type: none"> - disable - allow - prefer - require - verify-ca - verify-full
spec.fepChildCrVal.sysUsers.pgRewindUserTls.certificateName		This points to Kubernetes TLS secret that contains the certificate of Postgres user “rewinduser”. Patroni will use this for certificate authentication. The certificate itself is stored in the key tls.crt. This field is optional.
spec.fepChildCrVal.sysUsers.pgRewindUserTls.caName		This points to Kubernetes configmap that contains additional CA the client use to verify a server certificate. The CA is stored in the key ca.crt. This field is optional.
spec.fepChildCrVal.sysUsers.pgRewindUserTls.sslMode	prefer	Specify the type of TLS negotiation with the server. <ul style="list-style-type: none"> - disable - allow - prefer - require - verify-ca

Field	Default	Details
		- verify-full
spec.fepChildCrVal.systemCertificates.key		Use spec.fep.postgres.tls specification instead.
spec.fepChildCrVal.systemCertificates.crt		Use spec.fep.postgres.tls specification instead.
spec.fepChildCrVal.systemCertificates.caert		Use spec.fep.postgres.tls specification instead.

Note

- (*) - These parameters can be specified only at creation time and should not be changed. Any change to these parameters will be ignored and will not have any effect on FEP cluster functioning.
- (**)- The storage volumes size can be increased provided underlying storage supports the operation. Optional volumes can be specified only at initial FEP cluster creation. If an optional volume is added later, operator will ignore it and no action will be taken.
- User should do or remove unsupported CR changes manually.
- spec.fep.postgres.tls CR specification should be used instead of spec.fepChildCrVal.systemCertificates. The lateral spec can still be used, however spec.fep.postgres.tls gives better flexibility to control MTLs access of the cluster.
- Either spec.fep.postgres.tls specification (old specification) or spec.fepChildCrVal.systemCertificates should be used. They should not be used interchangeable.
- Server certificate specified under spec.fep.postgres.tls can be rotated by changing the secret and executing reload (e.g. using FEPAction); however for others specified in the CR, it is required to do restart of the PoDs

While in running state - following value will dynamically appear in the FEPCluster to reflect the cluster status

Field name	Details
fepClusterReady	Will be true or false to reflect if the whole cluster is ready. Kubernetes cluster information is fetched to check number of instances 'READY' & 'RUNNING' is equal to number of Configured instances.

1.2 Custom Resource Parameters

This section explains the Custom Resource Parameters.

1.2.1 FEPCluster Custom Resource Parameters

Category	Details
CRD Name	FEPCluster
Definition	<pre> apiVersion: apiextensions.k8s.io/v1beta1 kind: CustomResourceDefinition metadata: name: FEPClusters.fep.fujitsu.io spec: group: fep.fujitsu.io names: kind: FEPCluster </pre>

Category	Details
	listKind: FEPClusterList plural: fepclusters singular: fepcluster shortNames: - fac scope: Namespaced conversion: strategy: None subresources: status: {} versions: - name: v2 served: true storage: true
Operations	Create: kubectl create fepcluster (or kubectl create -f fepcluster.yaml) Delete: kubectl delete fepcluster (or kubectl delete fepcluster <clusername>) Update: kubectl patch fepcluster (or kubectl apply -f fepcluster.yaml) List: kubectl get fepcluster

FEPCluster CR Example

```

apiVersion: fep.fujitsu.io/v2
kind: FEPCluster
metadata:
  name: new-fep
  namespace: new-fep
spec:
  fep:
    forceSsl: true
    image:
      image: 'quay.io/fujitsu/fujitsu-enterprise-postgres-12-server:ubi8-12-1.1'
      pullPolicy: IfNotPresent
    mcSpec:
      limits:
        cpu: 500m
        memory: 700Mi
      requests:
        cpu: 200m
        memory: 512Mi
    podAntiAffinity: true
    podDisruptionBudget: true
    instances: '3'
    servicePort: 27500
    syncMode: 'on'
    sysExtraLogging: false
  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'
log_truncate_on_rotation = on
log_filename = 'pgaudit-%a.log'
log_rotation_age = 1d
log_rotation_size = 0
[rule]

customPgHba: |
# define pg_hba custom rules here to be merged with default rules.
# TYPE      DATABASE      USER      ADDRESS      METHOD

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
pgx_global_metacache = 10MB

# 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 = 'pgbackrest --stanza=backupstanza --config=/database/userdata/pgbackrest.conf
archive-push %p'
wal_level = replica

```

```

max_wal_senders = 10
wal_keep_segments = 64
wal_sender_timeout = 60s

backup:
  image:
    image: 'quay.io/fujitsu/fujitsu-enterprise-postgres-12-backup:ubi8-12-1.1'
    pullPolicy: IfNotPresent
  mcSpec:
    limits:
      cpu: 200m
      memory: 300Mi
    requests:
      cpu: 100m
      memory: 200Mi
  pgbackrestParams: |
    # define custom pgbackrest.conf parameters below to override defaults.
    [global]
    rep1-retention-full = 30
    rep1-retention-full-type = time
  preScript: " "
  postScript: " "
  schedule:
    num: 2
  schedule1:
    schedule: "15 0 * * 0"
    type: "full"
  schedule2:
    schedule: "15 0 * * 1-6"
    type: "incr"
  schedule3:
    schedule: " "
    type: " "
  schedule4:
    schedule: " "
    type: " "
  schedule5:
    schedule: " "
    type: " "

storage:
  dataVol:
    size: 2Gi
  tablespaceVol:
    size: 512Mi
  walVol:
    size: 1200Mi
  archivewalVol:
    size: 1Gi
  backupVol:
    size: 2Gi
  logVol:
    size: 1Gi

sysUsers:
  pgAdminPassword: admin-password
  pgdb: mydb
  pgpassword: mydbpassword
  pguser: mydbuser
  pgrepluser: repluser
  pgreplpassword: repluserpwd
  tdepassphrase: tde-passphrase

```


systemCertificates:

key: |-

```
-----BEGIN RSA PRIVATE KEY-----  
MIIEpAIBAAKCAQEAvhL4D/01Lmm/Ry3nu+jgLodLYEEg0wqMxhsyPRb43paWSF1p  
gX1CNAPz1Etns4LVGSd6n7TqV73MfZ41NHpuVtjwVTS6wtf7dQj7bbKewQCDF5bK  
QpekP5HAv/5uQ4Bx154FppJvmmMX6CtUBm9ici8X7M1GrPQ5uir7k j8SrUkSpXdkp  
wqyuEufvbenayCI8KapBcTAsRIMjWufWngriln4b8ZYiVh0mcHLrX8HWTmQJvqBh  
91aEwgn/KItPwQVp8dcZlilt+H6gBECd6n4q0/v1x0J2MoVK63Q+zZ7Y3ox5qSNN  
+/Kgacht916AcEzIoJ52pa4vneLwErKX6kJMRwIDAQABAoIBAF2vH9FRr1q4CGyR  
6vwlZfj776z7rOAYPRaP5Q0zO2sKsfvrBhOq12yn3fdj0bMq8zm4ubnqA+9HP31S  
72eUSLpJmirZGIxcDYFPVfUSbN6JKMF0Z9M+snSXzZCfTqMHPB19LcLsJh0sq+Q  
GYD1HRPpe2bqBARoCDIesK0j9IVRNitWOzZCarj1zjlyNSS4vPaEjAySW/XxuRzi  
A5smx2zXVm55+FjJpc2+H4Q+Rd+0AdLKrRAOyGCLMG3X5iYgwBTjzRKmdHJoIsnI  
em+kJYxChSaJFK+2uzJ1+L1W9d+7CtEdxIyMKxv1TaF79agzJI7MvotGGvnuLaTP  
KTTOAEcGYEA6h5h/OP9oB+1WM4xhQAmtnpwOhoQPKjMAYI0XZfzWMKBrzEKKk8p  
klbZIM24xUzMSb/hKvcqcraxYN21IUmgCDspbu0xMG6vNzqjAH0TtK8HhYOihhK1  
hGVV3vToTeJns3SL391IedhCOgVx1bPkHDS61V97Hdd9WIanp/8RwECgYEAz9bC  
A+aMbe3+1xLaoQ2j+54QaE/TbP+bbuP6Rc1H8OP1C1ZEPT1p3I4+mAlTyMq8Reit  
4CmSvvpHWXpOHNnVVCyhHerWCySxyV5Mcp33RARX5xN109TTJEgqoH2daTieM/KY6  
rakqerh7cwSGX0IXcB+N00ApBs7Bjph2g3FNm0cCgYEAjneot2TiLTO+fmkTd1UN  
OdQuU9wJH5a0dmKOjTnvat8KXdrqzYm4GpJa4qt12xn1t1oVjBawDz6dxW11M  
g+vEne0XFtr0Iw66rIxwlm5AjH37Q81LDdNCPBJtSVjr1Ui41BDZMRWFVg8tWZ25  
N7OAlfsqYUCmu8tUWZ0PvweCgYA7xefGd2erteaiTCnUZ7fhhXPYjAKiNmDdY3N2  
37Lw9J5kxEq0i2/4KjF0M7n0GaVNHNXNIEyBQJAEwyrXD/5FXx5LfqPIN1Blm2H  
PgF95/QNSPz6CFRLfUeAvtVvsotXyFBEIXHBYd7bLG4c6mJ9YkzqUQjURL7pplu  
8AcBwQKBqQC149QxQsbnaK1tQsYG5e+vo49GBjrpA7HeZDGq5oJGShAIMqOJSuv  
t+dwgflOxAW65jKBH6hNqVLF4xdZPV6Ka2BHNCPCGK7b0rwwQVvyjplM14dgIhPN6  
tNZgz3cDtHwb3VCHN3APGLcIZDazZbjOMqLWBq/euhdcLnyuB9jBww==  
-----END RSA PRIVATE KEY-----
```

crt: |-

```
-----BEGIN CERTIFICATE-----  
MIIEHjCCAwagAwIBAgIJANroZLqsw8hNMA0GCSqGSIb3DQEBCwUAMBYxWDASBGNV  
BAMMCzEwLjEzMS4wLjk5MB4XDTEwMTEwODE0MzUyNl0XDTQ4MDMyNjE0MzUyNl0w  
aDELMAKGA1UEBhMCOTExFzA8bGZyYXN0dHJhMQ0wCwYDVQQHDARQ  
dw51MRAwDgYDVQQkADGdWppdHN1MQwwCgYDVQQLDANDT0UxYFZASBGNVBAMMCzEw  
LjEzMS4wLjk5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvhL4D/01  
Lmm/Ry3nu+jgLodLYEEg0wqMxhsyPRb43paWSF1pgX1CNAPz1Etns4LVGSd6n7Tq  
V73MfZ41NHpuVtjwVTS6wtf7dQj7bbKewQCDF5bKQpekP5HAv/5uQ4Bx154FppJv  
mMX6CtUBm9ici8X7M1GrPQ5uir7k j8SrUkSpXdkpwwqyuEufvbenayCI8KapBcTAs  
RIMjWufWngriln4b8ZYiVh0mcHLrX8HWTmQJvqBh91aEwgn/KItPwQVp8dcZlilt  
+H6gBECd6n4q0/v1x0J2MoVK63Q+zZ7Y3ox5qSNN+/Kgacht916AcEzIoJ52pa4v  
neLwErKX6kJMRwIDAQABo4IBGzCCARcwrGyDVR0jBD8wPYAUtx0d+PZMXgb1RMKW  
4eogmLURjGhGqQYMBYxWDASBGNVBAMMCzEwLjEzMS4wLjk5ggkAtVepKtIe4D4w  
CQYDVR0TBAIwADALBgNVHQ8EBAMCBAwHQYDVR0LBBYwFAYIKwYBBQUHAWEGCCsG  
AQUFBwMCMIGVbgNVHREegY0wgYqCCmt1YmVybmV0ZXOCmt1YmVybmV0ZXMuZGVm  
YXVsdIIWaz3ViZXJuZXRlcy5kZWZhdWx0LnN2Y4Iea3ViZXJuZXRlcy5kZWZhdWx0  
LnN2Yy5jbHVzdGVygiRrdWJlcm5ldGVzLmR1ZmFlbHQuZjZjLmNsdXN0ZXIubG9j  
YWyHBAQDAGOHkweVVKwDQYJKoZIhvcNAQELBQADggEBADBIpMWGoIdMARIpoFE/  
f3Iwq2VMwr/NBg8ZgQd817+IIHooMP+1/nj2juy7enyrlFPIqRvhXADBkvZthro2  
4c+1bDbEbW0HqdUnRWwwBEeillxq4m6voWXXIA+At7fdiK7Dr7fo2OX5ndgW1Tw  
btXCoqdUee/m9EgvHLmOLhuI3E1654zP6FVB2r1XN/oXeEzefPE18VqSvk7eZ/hr  
adqpK3yt31LeFVQzqfXzcOxOCM7Bt0txVNN4a9NwBoF8abaHxVoKI3rZlxQFpkn+  
RCHx6QtaVDnLJ8jlykXcv8i7Qz+3Nwh0zszl3aM8rt3Pd+PRjC9VGg5kXBMORZi2  
xuo=  
-----END CERTIFICATE-----
```

ca.crt: |-

```
-----BEGIN CERTIFICATE-----  
MIIC/zCCAeegAwIBAgIJALVXqSrSHuA+MA0GCSqGSIb3DQEBCwUAMBYxWDASBGNV  
BAMMCzEwLjEzMS4wLjk5MB4XDTEwMTEwODE0MzUyOV0XDTQ4MDMyNjE0MzUyOV0w  
FjEUMBIgALUEAwLMTAuMTMxLjAuOTkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw  
ggEKAoIBAQLD7F1I69s5QY+NaZMEHVv4cksMdxsNerSdBpZaHaTVLSGod5SeqK8  
EGL0NPua2KccjZRitDLdYx8F1TrPqTie9N7QleDoiLi2AMrP8DEykGA304JtOXzs  
yGGwmodgdqJORhcwmYEFiKej6483Ahy3bXORG4WbmouId1Ou7CmrH6VXTcP8sgmc  
-----END CERTIFICATE-----
```

```

OLEEc9n33C/Ymwl1ggJk6fM/ysZKSic2wiePFPVo86tXJ5k8pRpGJZfGfGJ80Idx
EEyWlr7GRnNm1ZQVD7A4meNarA14Bc/6b/uBtL+WySW7wvqUIua+e4Sp1X4mMbj8
IqZLEzsGvaKpDFT02+jQiVqMCD80G2jHAgMBAAGjUDBOMB0GA1UdDgQWBBS3HR34
9kxeBvVEwPbh6hqcYhSuMTAfBgNVHSMEGDAWgBS3HR349kxeBvVEwPbh6hqcYhSu
MTAMBgNVHRMEBTADAQH/MA0GCSqGSIB3DQEBCwUAA4IBAQAiXOC/idXXeygT8UzH
k3biEs3iRwajDALWVONOpnj8q75F4zIaGhCKvU/kfdOg9cwVy3GJq5+1LhR8qtC
5o5iOhtS+XqyDXiv52Xe+GyY6GvtVUMd/KSHSInF2xgPUDInWdgqnFHC5bwNF2r8
yxHuNzUzEuu9xVzaqi7Wxk8t+uiktS4GgtcK94Zk8EkAxfnQe5PGa2i jcoF90whX
OCmhcT1CBXu4jgO3kfnuJ8E3A3gaN5I+VnqvvnPxpbg3G0mMhxr3pruTuCOBGqFM
CUDBzqNBD5wezjJImdnvS50LGx1CKgelrxP2NAmzblgMAms7XZfKxa51Tszaeqna
wuC4
-----END CERTIFICATE-----

```

It should also be noted that all the passwords / passphrase and certificates will be masked after the creation of the CR. This includes

- Also, initial pgAdminPassword: admin-password
- pgpassword: mydbpassword
- pgreplpassword: repluserpwd
- tdepassphrase: tde-passphrase
- certificate.key
- certificate.crt
- certificate.cacrt

Values of child CRs at the time of initial deployment of cluster, are stored in FEPCluster under fepChildCrVals, e.g. for Server certificates, Configuration of FEP, User details.

All fields for FEPCluster CR and its child CRs should be managed through FEPCluster CR only. Operator will reflect the changes to respective child CR to be processed. The fields that not allowed to change will not be reflected from parent to child CR and hence will not have any affect.

1.2.2 FEP Cluster Configuration

Configuration of all aspects of FEP Cluster is done through FEPCluster CR only.

All fields for FEPCluster CR and its child CRs should be managed through FEPCluster CR only. Operator will reflect the changes to respective child CR to be processed. The fields that not allowed to change will not be reflected from parent to child CR and hence will not have any affect. Refer to "1.1 FEPCluster Parameter" for details.

All child CRs are marked as internal objects in RedHat OCP and will not appear on console. However, it can be checked on command line using oc or kubectl commands.

Following table shows Child CRs of FEPCluster CR and respective sections in parent CR related to given child CR.

Configuration changes are made in these sections will update allowable fields only in corresponding child CR.

Child CR Name	Relevant sections in FEP Cluster CR
FEPBackup	spec.fepChildCrVal.backup
FEPcert	spec.fepChildCrVal.systemCertificates
FEPConfig	spec.fepChildCrVal.customPgAudit spec.fepChildCrVal.customPgHba spec.fepChildCrVal.customPgParams
FEPUser	spec.fepChildCrVal.sysUsers
FEPVolume	spec.fepChildCrVal.storage

1.2.3 FEPConfig Child Custom Resource Parameters

Name	Details
CRD Name	FEPCConfig
Definition	<p>apiVersion: apiextensions.k8s.io/v1beta1</p> <p>kind: CustomResourceDefinition</p> <p>metadata:</p> <p>name: fepconfigs.fep.fujitsu.io</p> <p>spec:</p> <p>group: fep.fujitsu.io</p> <p>names:</p> <p>kind: FEPCConfig</p> <p>listKind: FEPCConfigList</p> <p>plural: fepconfigs</p> <p>singular: fepconfig</p> <p>scope: Namespaced</p> <p>conversion:</p> <p>strategy: None</p> <p>subresources:</p> <p>status: {}</p> <p>versions:</p> <p>- name: v1</p> <p>served: true</p> <p>storage: true</p>
Operations	<p>Create: will be done by FEPCluster CR</p> <p>Edit: kubectl edit fepconfig</p> <p>Update: kubectl patch fepconfig</p> <p>List: kubectl get fepcluster</p>

Field	Default	Details
metadata.name	<same-as-in-FEPCluster>	This value is inherited from parent FEPCluster CR
metadata.namespace	<same-as-in-FEPCluster>	This value is inherited from parent FEPCluster CR
spec.customPgAudit	All line specified in spec.fepChildCrVal.customPg Audit of FEPCluster CR	Audit rules can be updated in this section. Requires restart. Note: initial values inherited once only at start. Changes to FEPCConfig directly
spec.customPgHba	All line specified in spec.fepChildCrVal.customPg Hba of FEPCluster CR	pg_hba rules can be added in this section Note: Inherited once at start. Changes to FEPCConfig directly
spec.customPgParams	All line specified in	All postgres parameters are listed here to overwrite defaults.

Field	Default	Details
	spec.fepChildCrVal.customPgParams of FEPCluster CR	Note: Inherited once at start. Changes to FEPCluster CR directly

Example of FEPCluster CR created

```

apiVersion: fep.fujitsu.io/v1
kind: FEPCluster
metadata:
  name: new-fep-19ncfg
  namespace: cfg-expt
spec:
  sysExtraLogging: false
  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'
    log_truncate_on_rotation = on
    log_filename = 'pgaudit-%a.log'
    log_rotation_age = 1d
    log_rotation_size = 0
    [rule]
  customPgHba: |
    # define pg_hba custom rules here to be merged with default rules.
    # TYPE      DATABASE      USER      ADDRESS      METHOD
  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 = 20
    max_connections = 100
    work_mem = 1MB
    maintenance_work_mem = 20MB
    shared_buffers = 128MB
    effective_cache_size = 384MB
    checkpoint_completion_target = 0.8
    pgx_global_metacache = 10MB
    temp_buffers = 10MB

    # 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
wal_level = replica
max_wal_senders = 10
wal_keep_segments = 64
wal_sender_timeout = 60s

```

1.2.4 FEPUser Child Custom Resource Parameters

Name	Details
CRD Name	FEPUser
Definition	apiVersion: apiextensions.k8s.io/v1beta1 kind: CustomResourceDefinition metadata: name: fepusers.fep.fujitsu.io spec: group: fep.fujitsu.io names: kind: FEPUser listKind: FEPUserList plural: fepusers singular: fepuser scope: Namespaced conversion: strategy: None subresources: status: {} versions: - name: v1 served: true storage: true
Operations	Create: will be done by FEPCluster CR with data in fepChildCrVal Edit: kubectl edit fepuser Update: kubectl patch fepuser

Name	Details
	List: kubectl get fepuser

Field	Default	Details
metadata.name	<same-as-in-FEPCluster>	This value is inherited from parent FEPCluster CR
metadata.namespace	<same-as-in-FEPCluster>	This value is inherited from parent FEPCluster CR
spec.pgAdminPassword	spec.fepChildCrVal.users.pgAdminPassword of FEPCluster CR	postgres superuser password. Masked once secret is created/changed Note: initial values inherited once only at start. Changes to FEPUser directly
spec.pgdb	spec.fepChildCrVal.users.pgdb of FEPCluster CR	Name of a user database Note: Created once only at start. Cannot be changed
spec.pgpassword	spec.fepChildCrVal.users.pgpassword of FEPCluster CR	Password for superuser for user database pgdb. Masked once secret is created/changed Note: initial values inherited once only at start. Changes to FEPUser directly
spec.pguser	spec.fepChildCrVal.users.pguser of FEPCluster CR	Name of a user database Note: Created once only at start. Cannot be changed
spec.pgrepluser	spec.fepChildCrVal.users.pgrepluser of FEPCluster CR	Name of a database user for replication
spec.pgreplpassword	spec.fepChildCrVal.users.pgreplpassword of FEPCluster CR	Password for pgrepluser
spec.tdepasphrase	spec.fepChildCrVal.users.tdepasphrase of FEPCluster CR	Passphrase for encrypting/decrypting keystore file which contains the TDE encryption key
spec.pgRewindUser	rewind_user	Database user for Rewind
spec.pgRewindUserPassword	rewind_password	Password for database user rewinduser
spec.pgAdminTls.certificateName	<secret-name>	Name of Kubernetes secret that contains the certificate in tls.crt and private key in tls.key for “postgres” 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.
spec.pgAdminTls.caName	<configmap-name>	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.
spec.pgAdminTls.sslMode	verify-full	For MTLS, this value must be set to verify-full. If only TLS is required, this can be set to verify-ca or prefer.
spec.pgrepluserTls.certificateName	<secret-name>	Name of Kubernetes secret that contains the certificate in tls.crt and private key in tls.key for “repluser” user. For MTLS Postgres communication, this key must be defined. The private key cannot be password protected. When using

Field	Default	Details
		cert-manager, the secret also contains the CA bundle in ca.crt.
spec.pgrepluserTls.caName	<configmap-name>	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.
spec.pgrepluserTls.sslMode	verify-full	For MTLS, this value must be set to verify-full. If only TLS is required, this can be set to verify-ca or prefer.
spec.pgRewindUserTls.certificateName	<secret-name>	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.
spec.pgRewindUserTls.caName	<configmap-name>	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.
spec.pgRewindUserTls.sslMode	verify-full	For MTLS, this value must be set to verify-full. If only TLS is required, this can be set to verify-ca or prefer.

Example of FEPUser CR created

```

apiVersion: fep.fujitsu.io/v1
kind: FEPUser
metadata:
  name: new-fep-19n
  namespace: testswatiprject
spec:
  pgAdminPassword: '*****'
  pgdb: mydb
  pgpassword: '*****'
  pgreplpassword: '*****'
  pgrepluser: repluser
  pguser: mydbuser
  tdepassphrase: '*****'
  sysExtraLogging: false
  pgRewindUser: rewind_user
  pgRewindUserPassword: rewind_password
  pgAdminTls:
    certificateName: admin-client-certs-secret
    caName: admin-ssl-rootcert-configmap
    sslMode: prefer
  pgrepluserTls:
    certificateName: repluser-client-certs-secret
    caName: repluser-ca-name-configmap
    sslMode: prefer
  pgRewindUserTls:
    certificateName: rewinduser-client-certs-secret
    caName: rewinduser-ca-name-configmap
    sslMode: prefer

```



Note

- Password and Passphrase are masked in output from CR. The original values can still be found in the respective Kubernetes secrets and configmaps.

- TDE is enabled by default with given tdepassphrase and must have a value.
- TDE is enabled by using the key tdepassphrase with the desired passphrase. Do not remove this key once TDE is enabled. Otherwise, the database may go into a crash loop. If the Cluster is running on Async Replication and a failover/switchover occurred during the crash loop, there could be data lost. The team is looking at preventing the deletion of this passphrase from Operator even if customer tries to remove it in customer resource.
- Database users and their passwords managed by the FEPUUser CR should not be changed in the SQL interface. Inconsistencies with the information managed by the operator can cause problems with operator operation. If you make changes in the SQL interface, use the SQL interface again to restore the original state.

1.2.5 FEVolume Child Custom Resource Parameters

FEVolume CR created

```
spec:
  archivalVol:
    size: 1Gi
  backupVol:
    size: 2Gi
  dataVol:
    size: 2Gi
  logVol:
    size: 1Gi
  tablespaceVol:
    size: 512Mi
  walVol:
    size: 1Gi
  selectedVolList:
  - name: data
  - name: tablespace
  - name: wal
  - name: log
  sysExtraLogging: false
```

1.2.6 FEPCert Child Custom Resource Parameters

Below is an example CR for certificates to be used by FEP server container

```
apiVersion: fep.fujitsu.io/v1
kind: FEPCert
metadata:
  name: new-fep
  namespace: ansible-operator-poc
spec:
  key: |-
    -----BEGIN RSA PRIVATE KEY-----
    MIIEowIBAAKCAQEAA4AI33yvHZws+jta6qpV6wzJqF8odIfTIpCfbrVcUUtLFKJ1I
    2e4SceTKi6O3C/I1XuvWlpng5IO65+fQQL006z1/AuQT78YUn/Wlm9x1aHVsv4AN
    B5JWWqD0jrRT3o7nRPGXfilabP0rGE2mJJcVR9nExJ3IeaktgT3sb8YlXvtchyYp
    mjdbfxabTz07ig0+6/cwKoRRxOK8Uf7f5euE0cI/490J6r5Rs4lgD8sIQNCUFlTF
    YvmAH7gcdssSFBt8NPLUATHEsoFmlW0DKCJWNhTLOht+s6L/1zwTHLjPG2pdkg6W
    dgmu5H2pDml8CDNLDv98Aj7i+I5SRKKcVP1nuQIDAQABAoIBAFPPQYK1Ozw/+BA0b
    yMIUpdctIMb/54CR/xR0mVw1DbSjigNVPjHUQvB8Y1B2FAITQObgJO06bAv0QdWN
    Rb0/v/yYiNJDFjaLjaIAH1O/2+oWrXbFaZqgpVDJhB+e1xaZr2x7XGxm+p925k30
    16pvIRY+I8JRKvZiV1VZHwL/R3JOtPr++xMZtLVjVOI+f+ySjQ+TZHuAjm49EKxj
    cEmmJ28b7QcziXsvKy00f+zbqLIBKXQdZAFU5eEr1BsDRXdRW+KfOXIvftuy4BJZ
    vOkt+VghEvF/qysswL4+6IAO6tpuYnnM0Y2d3s0GoWpKtCqK0MekYKzL/WmtCjNs
    9hodJtECgYEA5EWyhEOf4u0Ke5TDp697UCUvXLoOR58FDe/S8XNvScn29jjOkqIg
    OMoqo9xAkJTNTzqn5Uudt1x/pgM2Nx1PLFi jrC0zQLX3SoOO2ryDd9Wni7YKtN16
    KJqa536WeZu2OEbuAZ+S3GALVylRPeTNPnUOmKnF06DjDUGzLNCzy10CgYEA+zfw
    952DWuz1U0Z4wvAEqqcgUKXPKrkTXV/iUnjkDkrLYVr0ZofDNTXrdH1+UedFmaOC
```



```
cieZn6DNhcdz5tKtyysGMH3g/qs9PfoGungvcXsy0Egk0413x1jc8TTCLqXZXyAQ
HMsx51n+R58oncPtzYSUOr9qQ6PbC2CstTbFJA0CgYEAjGEsUliAB/jknfEzjXjG
PdhQUxb8Vye864Az2lah9t/kJzFyIAziAeqZ5GE7t247AGFTBRTHHI8e1Qoemi3P
Wbc9GVIBfsl1IYbcIDpUIYrKPEP805QEXtoNLxXTFgAjRGKiVY87spjCAJ+W2ZhO
e/1it5GYXfgQCYQA2yuBmOUCgYANRkr2YR1axaCk+N1Su6oTdmPu6M5x7PNQE7O
OtMaKjua9lppvIzFGAdMDUteoeEAE7ZR1xnwfB6PDLUpJdIYAqgr1YfPt8qkjaZ
Tv56yZ7CwL0pbF8m6nqwRrZoDp1wwraEvvvxFKFKGY/k3kCHlpTakdjEoDjn3gDi
RnWeVQKBgCEneMSzucei5LRppRtRaJw/Bt1l8q1PMLX3W7dxQ3cLwpmL0n0m51Fp
PIZ44zYK8R6fu4+/sSrlfaIgr86Ugeufp6YNxyNROKxUGza5vDIu5OfwtWtBeg+UK
Z81LWNdX6pp7WMu jmF3H1DrkKbauYMUkZ4UxUYtelgHERMePIxwb
-----END RSA PRIVATE KEY-----
```

crt: |-

```
-----BEGIN CERTIFICATE-----
MIIDUTCCAjmGAWIBAgIRAMocW3qMoHrD6qRvMppMkMwDQYJKoZIhvcNAQELBQAw
NzEQMA4GA1UECgwHRnVqaXRzdTEjMCEGAlUEAwwaRkVQIFJvb3QgQ0EgZm9yIETl
YmVybmV0ZXMwHhcNMjEwMjM2MDQzMjM2WmcNMjEwMjM2MDQzMjM2WjA/MRAwDgYD
VQQKEwdGdWppdHN1MSswKQYDVQDEYjGVUUpJVFNVIEVudGVycHJpc2UgUG9zdGdy
ZXMGU2VydmVyMjEwMjM2MDQzMjM2WmcNMjEwMjM2MDQzMjM2WjA4I33yvH
Zws+jta6qpV6wzJqF8odIFtIpcFbrVcUUtLfkjLI2e4SceTKi603C/I1XuvWlpng
5IO65+fQQL006z1/AuQT78YUn/Wlm9x1aHVsv4ANB5JWWqDOjrRT3o7nRPGXfila
bP0rGE2mJcVR9nEXj3IeaktgT3sb8YlXvtchyYpmjdbfxabTz07ig0+6/cwKoRR
xOK8Uf7f5euE0ci/490J6r5Rs4lgD8sIQNCUFLTFYvmAH7gcdsssFBt8NPLUATHE
soFmlW0DKCJWNhTLOht+s6L/1zwTHLjPG2pdkG6WdgmU5H2pDml8CDNLDv98Aj7i
+I5SRKKcVPlnuQIDAQABo1AwTjAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUH
AwIwDAYDVROTAQH/BAIwADAFBgNVHSMEGDAWgBQcwrrUO0u+FhIUuVdrDRCQRsI6
ZjANBgkqhkiG9w0BAQsFAAOCAQEAm5dxBoI9pScOCvRachg4CprdrRDSJb9K6yB3O
nCAxm47iHeXnY3WlnI388kHu8DU704ba1tJbGs3KY9KzioPk43pU12jWk01onoF
+mTDjx/Ef1cYWA9r5q/LtgTa6Q2sxv4O2x67QW82aAnaxO34dV5zWCPIvAoovZBV
HRT+Bgcg3r2vD1RGKK2n1laYJtWh01SZubam+VttdZ/vbM9oOJctxmImEtBXjkY
KteePdQtLL5o03JhyXWyrshCq+HmMkF2Kgy8gvydGcP4eLQdBWcW40LcnVq6UjT
0kJycJEKngMvademq1ZWHGaiYB7hyT6GhgIcHUJ2cKrPgbehlQ==
-----END CERTIFICATE-----
```

ca.crt: |-

```
-----BEGIN CERTIFICATE-----
MIIDTzCCAjegAWIBAgIUySsQ8I74US5g+1+Z7CHuaDgkZnEwDQYJKoZIhvcNAQEL
BQAwNzEQMA4GA1UECgwHRnVqaXRzdTEjMCEGAlUEAwwaRkVQIFJvb3QgQ0EgZm9y
IETlYmVybmV0ZXMwHhcNMjEwMjM2MDQzMjM2WmcNMjEwMjM2MDQzMjM2WjA3MRAw
DgYDVQQKDAkdWppdHN1MSswIYQYDVQDDbGRVAgUm9vdCBDQSBmb3Igs3ViZXJv
ZXRlc3CCASIdQYJKoZIhvcNAQEBBQADgGEPADCCAQoCggEBAMs97gUF0xkUzCgL
7MiiDju9ySr/zIwjcYU7jA9ML+SLmftMs3HtcYbAmSntqI+MDSBR/FAJTOoytuT
pV+mCFcGj2YAjdpliHPeNcUpbryy4YMChF3+MovkIwGCksxo5rhiWhGmoBYpA48P
4Xe8SP1zqMzhFvNeKzyiUhvjutS2Y1Ss381sTaurFPx64vQ2PaC54XzdwMptXtpb
tYmWSzCpJWwxZ6lF3vitdA2w0tnBWNyctAd0+RIM/fvArxiIqseAux9t0uogm5to
lRihvekuxOpXBPEqtIYQ4j9XUW2JH8vUDnzPkPvjrq+A3Ug8OyyfGvRw7+VYXozu
c4aP7P0CAwEAANtMFewHQYDVR0OBBYEFBzCutQ7S74WEhS5V2sNEJBGyLpmMB8G
A1UdIwQYMBaAFBzCutQ7S74WEhS5V2sNEJBGyLpmMA8GA1UdEwEB/wQFMAMBaf8w
DQYJKoZIhvcNAQELBQADggEBAMDwD85RAaWEBptFgZKw+9xEUylvcZaonAu1qc
T342XTueyAugxkC1lHwdCGgGS34VyctfMGqj4AW6pA2ez4tLrbOps4DmV4sw8uBL
8pgRDgflY3ob9FEg2wa0hmrwX9jH5Bt4vySUE2785uPaqaspT2UNTbXs85BUIIT
sKId2Rtil6an281Z81wyWVI6Jm2D4MG0mbsiGcTPlCtdg/Ul jvDYmXlAvd4vNh1
k9hDal3TgDqJKgKdTIcmZoNqdpEVgFc00h9AEUy5AuLqxHq60dLfZ6ESGP1MI7Lm
i4PzYbCnBmOe+7TnHcPSyrnehs66Ik+oifrd82eYS7vKjFw=
-----END CERTIFICATE-----
```



Note

This approach of specifying FEP Certs is getting deprecated. Should follow Secrets as referred in section to configure Certs for Server, Patroni and Users.

1.2.7 FEPBackup Child Custom Resource Parameters

Name	Details
CRD Name	FEPBackup
Definition	apiVersion: apiextensions.k8s.io/v1beta1 kind: CustomResourceDefinition metadata: name: febackup.fep.fujitsu.io spec: group: fep.fujitsu.io names: kind: FEPBackup listKind: FEPBackupList plural: febackups singular: febackup scope: Namespaced conversion: strategy: None subresources: status: {} versions: - name: v1 served: true storage: true
Operations	Create: will be done by FEPCluster CR Edit: kubectl edit febackup Update: kubectl patch febackup List: kubectl get febackup

Field	Default	Details
apiVersion	fep.fujitsu.io/v1	Fixed
kind	FEPBackup	Fixed
metadata.name	<clustername>	Enter the CR name.
spec.pgbackrestParams	" "	" " It is fixed, and the parameter set in pgbackrest.conf is described from the line below.
spec.schedule.num	Integer	Number of schedules to set The maximum number of backup schedules is 5.
spec.scheduleN.schedule	-	Write the date and time of the Nth schedule in cron format. The date and time is UTC time.
spec.scheduleN.type	full/incr	full: Perform a full backup (Back up the contents of the database cluster).

Field	Default	Details
		incr — Perform an incremental backup (Back up only the database cluster files that were changed to the last backup migration).
spec.preScript	" "	This parameter must specify a default value.
spec.postScript	" "	This parameter must specify a default value.

Example of FEPBackup CR created

```

apiVersion: fep.fujitsu.io/v1
kind: FEPBackup
metadata:
  name: fepcluster-backup
spec:
  schedule:
    num : 2
  schedule1:
    schedule : "0 0 1 * *"
    type : "full"
  schedule2:
    schedule : "0 0 1-6 * *"
    type : "incr"
  preScript: " "
  postScript: " "
  pgbackrestParams: |
    # define custom pgbackrest.conf parameters below to override defaults.
    [global]
    rep1-retention-full = 30
    rep1-retention-full-type = time
...

```

1.2.8 FEPRestore Custom Resource Parameters

Name	Details
CRD Name	FEPRestore
Definition	<pre> apiVersion: apiextensions.k8s.io/v1beta1 kind: CustomResourceDefinition metadata: name: feprestore.fep.fujitsu.io spec: group: fep.fujitsu.io names: kind: FEPRestore listKind: FEPRestoreList plural: feprestores singular: feprestore cope: Namespaced conversion: strategy: None </pre>

Name	Details
	subresources: status: {} versions: - name: v1 served: true storage: true
Operations	Create: kubectl create feprestore Edit: kubectl edit feprestore Update: kubectl patch feprestore List: kubectl get feprestore

Field	Default	Details
apiVersion	fep.fujitsu.io/v1	Fixed
kind	FEPRestore	Fixed
metadata.name	-	Enter the CR name.
spec.image	<current-released-image>	FEP restore container image to be used quay.io/fujitsu/fujitsu-enterprise-postgres-12-restore:ubi8-12-1.1 It is optional. Image is left blank by default. In such a case, it will pick up URL of image from operator container environment. If you specify the image, Operator will take that image to deploy container
spec.imagePullPolicy	IfNotPresent	
spec.mcSpec.limits	cpu: 0.2 memory: "300Mi"	
spec.mcSpec.requests	cpu: 0.1 memory: "200Mi"	
spec.fromFEPcluster	<from_clustername>	The name of the FEPcluster from which to restore
spec.toFEPcluster	<to_clustername>	Name of the FEPcluster to restore to The exact restore destination volume is retrieved from FEPcluster
spec.restoretype	latest/PITR	latest - Restore Latest State PITR - Date-Time Restore
spec.restoredate	-	If spec.restoretype is PITR, specify the day of PITR (UTC) in YYYY-MM-DD format Example) 2020-11-25
spec.restoretime	-	If spec.restoretype is PITR, specifies the PITR time (UTC) in HH: MM: SS format Example) 02:50:43

Example of FEPRestore CR created

```
apiVersion: fep.fujitsu.io/v1
kind: FEPRestore
metadata:
  name: feprestore
spec:
  mcSpec:
    limits:
      cpu: 200m
      memory: 300Mi
    requests:
      cpu: 100m
      memory: 200Mi
  fromFEPcluster: fepcluster1
  toFEPcluster: fepcluster2
  restoreType: latest
  imagePullPolicy: IfNotPresent
```

Example of Point-In-Time-Recovery using FEPRestore CR

```
apiVersion: fep.fujitsu.io/v1
kind: FEPRestore
metadata:
  name: feprestore
spec:
  mcSpec:
    limits:
      cpu: 300m
      memory: 700Mi
    requests:
      cpu: 200m
      memory: 512Mi
  fromFEPcluster: fepclusterA
  toFEPcluster: fepclusterB
  restoreType: PITR
  restoreDate: 2020-11-25
  restoreTime: 02:50:43
  imagePullPolicy: IfNotPresent
```

1.2.9 FEPPgpool2 Custom Resource Parameters

Equivalent Kubernetes command: `kubectl create FEPPgpool2`

This operation will create a PGPool2 with supplied information.

Field	Default	Details
apiVersion	fep.fujitsu.io/v1	Fixed
kind	FEPPgpool2	Fixed
metadata.name	-	List the name of the FEP Pgpool2 container.
metadata.namespace	-	Specify the namespace of the environment where you want to deploy the operator.
spec.image	<current-released-image>	FEPPgpool2 container image to be used quay.io/fujitsu/fujitsu-enterprise-postgres-12-pgpool2:ubi8-12-1.1 It is optional.

Field	Default	Details
		Image is left blank by default. In such a case, it will pick up URL of image from operator container environment. If you specify the image, Operator will take that image to deploy container.
spec.count	2	List the number of FEP Pgpool2 containers to create.
spec.serviceport	9999	Describes the TCP port for connecting to the FEP Pgpool2 container.
spec.statusport	9898	Identifies the TCP port for connecting to the PCP process.
spec.limits.cpu	400m	List the number of CPUs (restriction) to allocate to resources.limits.cpu.
spec.limits.memory	512Mi	Specifies the memory size (restriction) to allocate to resources.limits.memory.
spec.requests.cpu	200m	List the number of CPUs (request) to allocate to resources.requests.cpu.
spec.requests.memory	256Mi	Specifies the memory size (request) to allocate to resources.requests.memory
spec.fepclustername	new-fep	Enter the FEPCluster name to connect to.
spec.customhba		If you want to use pool_hba.conf, describe what pool_hba.conf should contain from the line below.
spec.customparams	listen_addresses = '*' pcp_listen_addresses = '*' num_init_children = 32 reserved_connections = 0 enable_pool_hba = off allow_clear_text_frontend_auth = off authentication_timeout = 80 backend_weight0 = 1 backend_weight1 = 1 backend_flag0 = 'ALWAYS_MASTER' backend_flag1 = 'ALLOW_TO_FAILOVER' connection_cache = on max_pool = 4 listen_backlog_multiplier = 2 serialize_accept = off child_life_time = 300 client_idle_limit = 0 child_max_connections = 0 connection_life_time = 0 reset_query_list = 'ABORT; DISCARD ALL'	" " and the Pgpool-II parameters. Refer to " Pgpool-II parameters " for detail.

Field	Default	Details
	client_min_messages = info log_min_messages = debug1 log_statement = on log_per_node_statement = on log_client_messages = on log_hostname = on log_connections = on log_line_prefix = '%t: pid %p: ' load_balance_mode = on ignore_leading_white_space = on white_function_list = " black_function_list = 'currval,lastval,nextval,setval' black_query_pattern_list = " database_redirect_preference_list = " app_name_redirect_preference_list = " allow_sql_comments = off disable_load_balance_on_write = 'transaction' statement_level_load_balance = on connect_timeout = 10000 sr_check_period = 0 sr_check_user = 'postgres' delay_threshold = 0 log_standby_delay = 'none' ssl = on ssl_ciphers = 'HIGH:MEDIUM:+3DES:!aNULL' ssl_prefer_server_ciphers = off ssl_ecdh_curve = 'prime256v1' ssl_dh_params_file = " relcache_expire = 0 relcache_size = 256 check_temp_table = catalog check_unlogged_table = on enable_shared_relcache = on	

Field	Default	Details
	relcache_query_target = master	
spec.custompcp	" "	If you use the pcp command, " " and the contents of pcp.conf from the line below.
spec.customsslkey	" "	If you want to do it, " " and the Beethoven key content in the line below.
spec.customsslcert	" "	If you want to do it, " " and the contents of the public x 509 certificate from the line below.
spec.customsslca	" "	If you want to do it, " " and the following lines describe the contents of the CA root certificate in PEM format.
spec.customlogsize	100 Mi	Specifies the persistent volume size for log output.
spec.storageclassname		Specifies the storage class for log output.

Pgpool-II parameters

The parameters that can be specified are shown in the table below. For details on the parameters, refer to the Pgpool-II manual.

Category	Parameter name (Specified format)	Restart required after change
Connection settings	listen_addresses (string)	Y
	pcp_listen_addresses (string)	Y
	num_init_children (integer)	Y
	reserved_connections (integer)	Y
Authentication settings	enable_pool_hba (boolean)	
	allow_clear_text_frontend_auth (boolean)	
	authentication_timeout (integer)	
Backend settings	backend_weight0 (floating point)	
	backend_weight1 (floating point)	
	backend_flag0	
	backend_flag1	
Connection pooling	connection_cache (boolean)	Y
	max_pool (integer)	Y
	listen_backlog_multiplier (integer)	Y
	serialize_accept (boolean)	Y
	child_life_time (integer)	Y
	client_idle_limit (integer)	
	child_max_connections (integer)	Y
	connection_life_time (integer)	Y
reset_query_list (string)		
Error reporting and log acquisition	client_min_messages (enum)	
	log_min_messages (enum)	
	log_statement (boolean)	
	log_per_node_statement (boolean)	

Category	Parameter name (Specified format)	Restart required after change
	log_client_messages (boolean)	
	log_hostname (boolean)	
	log_connections (boolean)	
	log_error_verbosity (enum)	
	log_line_prefix (string)	
Load sharing settings	load_balance_mode (boolean)	Y
	ignore_leading_white_space (boolean)	
	white_function_list (string)	
	black_function_list (string)	
	black_query_pattern_list (string)	
	database_redirect_preference_list (string)	
	app_name_redirect_preference_list (string)	
	allow_sql_comments (boolean)	
	disable_load_balance_on_write (string)	Y
	statement_level_load_balance (boolean)	
Health check	connect_timeout (integer)	
Streaming replication check	sr_check_period (integer)	
	sr_check_user (string)	
	sr_check_password (string)	
	sr_check_database (string)	
	delay_threshold (integer)	
	log_standby_delay (string)	
Secure Socket Layer (SSL)	ssl (boolean)	Y
	ssl_ciphers (string)	Y
	ssl_prefer_server_ciphers (boolean)	Y
	ssl_ecdh_curve (string)	Y
	ssl_dh_params_file (string)	Y
Other parameters	relcache_expire (integer)	Y
	relcache_size (integer)	Y
	enable_shared_relcache (boolean)	Y
	relcache_query_target (enum)	
	check_temp_table (enum)	
	check_unlogged_table (boolean)	

1.2.10 FEPAAction Custom Resource Parameters

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

Specify parameters in the format described below.

Custom resource spec	Change effect
.spec.targetClusterName	Must specify target FEP Cluster name within namespace mentioned in metadata.
.spec.targetPgpool2Name	Must specify target FEPPgpool2 name within namespace mentioned in metadata when using pgpool2_restart.
.spec.fepAction.type	Must specify action type. Supported action types are: restart reload list switchover failover pgpool2_restart
.spec.fepAction.args	Must specify arguments needed for given action. For details of args corresponding to each action refer to " 1.2.10.1 FEPAction Specific Operation Details ".
.spec.sysExtraLogging	To turn extra debugging on, set value to true. It can be turned on/off at any time.

After execution of FEPAction CR, status is reflected in fepStatus field that is dynamically inserted in current FEPAction CR as needed. fepStatus field used for FEPAction CR are described here

fepStatus (with possible values)	Remarks
fepActionStatus:	fepStatus is inserted at the top of FEPAction CR
fepActionCondition: Success Failure	This flag is inserted in fepAction CR to reflect success or failure of requested action
fepActionResult: > "details"	The result contains verbose details corresponding to the specific action been executed. Should be noted that it is either plain text of HTTP output.
processedTimestamp: <time stamp>	Denotes time of action execution by the Operator

```

apiVersion: fep.fujitsu.io/v1
kind: FEPAction
fepActionStatus:
  fepActionCondition: Success
metadata:
  name: new-fep-reload-action
  namespace: myns
spec:
  fepAction:
    args:
      - new-fep-sts-0
      - new-fep-sts-1
    type: reload
  sysExtraLogging: false
  targetClusterName: new-fep

```

Note

Please do not use the FEPAction to perform a switchover or restart while executing backup. Failed to get the backup.

1.2.10.1 FEPAction Specific Operation Details

Action type - reload

The reload action will manually reload the FEP database on the targeted FEPCluster.

“reload” action type expects users to specify the name of individual FEP pods that they want to run the database reload operation on. They specify that in the args section under the FEPAction CR spec as below :

```
spec:
  fepAction:
    args:
      - nf-131851-sts-0
      - nf-131851-sts-1
    type: reload
  targetClusterName: nf-131851
```

Action type - restart

The restart action will manually restart the FEP database on the targeted FEPCluster.

“restart” action type expects users to specify the name of individual FEP pods that they want to run the database restart operation on. They specify that in the args section under the FEPAction CR spec as below:

```
spec:
  fepAction:
    args:
      - nf-131851-sts-0
      - nf-131851-sts-1
    type: restart
  targetClusterName: nf-131851
```

Action type - list

The list action will return the status of the targeted FEPCluster.

“list” action type expects users to specify just the target cluster name to list the details of the same. Looks like below:

```
spec:
  fepAction:
    type: list
  targetClusterName: nf-131851
```

Action type - switchover

The switchover action performs a manually switchover of the current leader/primary database from one pod to another pod of the targeted FEPCluster.

“switchover” action type expects users to specify the name of the current leader/primary pod that they want to switchover from. They specify that in the args section under the FEPAction CR spec as below:

```
spec:
  fepAction:
    args:
      - nf-131851-sts-2
    type: switchover
  targetClusterName: nf-131851
```

Here, nf-131851-sts-2 is the current primary.

Action type - failover

The failover action performs a manually failover of the current primary database from one pod to another pod of the targeted FEPCluster. The difference between switchover and failover is that, switchover expects the primary database is running at the time whereas failover can force switchover of primary role from a non-responding pod to another pod. Note that failover is a disruptive action and may cause data lost.

“failover” action type expects users to specify the names of the candidate pods that they want to failover to. They specify that in the args section under the FEPACTION CR spec as below:

```
spec:
  fepAction:
    args:
      - nf-131851-sts-1
      - nf-131851-sts-2
    type: failover
  targetClusterName: nf-131851
```

Here, nf-131851-sts-1 and nf-131851-2 are the candidate pods to failover to. In this example, the current primary pod would be nf-131851-sts-0.

Action type - pgpool2_restart

“pgpool2_restart” action type expects users to specify the name of individual FEPPgpool2 resource that they want to restart operation on. They specify that in the targetPgpool2Name section under the FEPACTION CR spec as below:

```
spec:
  fepAction:
    type: pgpool2_restart
  targetPgpool2Name: nf-131851-pgpool2
```