

Cloud Native PostgreSQL の概要

EDBセールスエンジニア

吉野孝太郎



なぜKubernetes なのか？



containers

コンパイル済のソフトウェアのコードを、実行時に必要な依存関係とともに、パッケージ化

開発からデプロイメントまでの スピードアップ

- ソフトウェアを基盤となるインフラから切り離し、異なるクラウド環境や、OS環境でのデプロイメントを容易にする
- OSイメージが含まれていないため、従来のハードウェア環境や、仮想マシン環境（VM）より、少ないシステムリソースで済む



kubernetes

ソフトウェア管理のオーケストレーションを行い
インフラをより効率的に活用するためのコンテナ
管理システム

コンテナ技術のポテンシャルを 実際の運用に導入

- 共有インフラ上で、コンテナ化されたアプリケーションのデプロイ、スケーリング、管理を自動化
- より少ないリソースでITを管理し、コストを削減
- 使いやすさと移植性を実現
- スケーラビリティとモジュール性を強化しており、アプリをより復元力のある、パフォーマンスの高いものにする

ビジネスで、コンテナを大規模に
導入して利用したい場合



すべてのコンテナを自動的に
追跡、スケジュール管理、
オーケストレーションするための
ソリューションが必要



EDB と Kubernetes



- Kubernetes Certified Service Provider (KCSP)
 - このステータスに到達する最初のPostgreSQL会社



- Silver Member of CNCF & Linux Foundation



- Red Hat Certified Kubernetes Operators
 - Cloud Native PostgreSQL (PostgreSQL Operator)
 - Cloud Native BDR (BDR Operator)



Cloud Native PostgreSQL (CNP)



Cloud Native PostgreSQL と BDR

Kubernetesネイティブの EDB 製品

- Operators for Kubernetes
 - KubernetesのようにGO言語で書かれた
 - Kubernetes向けに設計
 - Kubernetes API serverと完全に統合
 - 従来の外部ツールは不要
 - ※Repmgr, Patroni, Stolon, Failover Manager
- コンテナイメージ
 - PostgreSQL 10, 11, 12, 13
 - EDB Postgres Advanced 10, 11, 12, 13
 - BDR (3.6 on 2ndQPostgres in Q1/2021)

Kubernetes オペレーター

Kubernetes コントローラを拡張し、複雑なアプリケーションの動作を定義します。

- Kubernetesオペレーターは、プログラマ的な方法でオペレーターの作業を自動化します
- PostgreSQL クラスターは複雑なアプリケーションです。
 - デプロイとコンフィグ
 - 障害の検出とフェールオーバー
 - アップデートとスイッチオーバー
 - バックアップとリカバリ
- Kubernetesのネイティブコンポーネントと機能に依存：
 - セルフヒーリング, 高可用性, スケーラビリティ, リソース制御, アクセス制限, ...
 - 宣言的かつ完全に自動化

コンテナイメージ

すべてのコンテナイメージは RedHat UBI 8 に基づいています

- Operator コンテナイメージ
 - EDB Limited Use License
- Application コンテナイメージ(PostgreSQL)
 - PostgreSQL:
 - The Postgres License (OSS)
 - GNU GPL 3 (Barman Cloud)
 - EDB Postgres Advanced Server:
 - EDB Limited Use License

ターゲット環境

Kubernetes環境ならどこでも実行可能！

- Private Cloud :
 - Kubernetes 1.16+
 - OpenShift 4.5+
- Public Cloud
 - Microsoft Azure (AKS) – リリース済！
 - Amazon Web Services (EKS) - 2021/Q3 (7-9月期)
 - Google Cloud (GKS) - 2021/Q4 (10-12月期)

評価／トライアル

Operator with PostgreSQL

- 試用ライセンスキーは不要
- 30日 以降の調整の試みなし
 - 各 Postgres クラスターの作成から

Operator with EDB Postgres Advanced

- 試用ライセンスキーが必要
- 有効期限 = ライセンス要求から 60日
- 有効期限後に調整の試みなし

トライアルライセンスキーの取得

<https://cloud-native.enterprisedb.com>

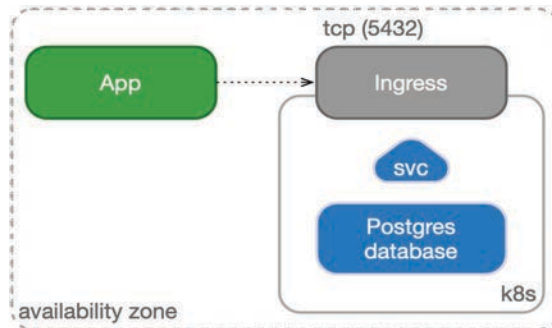
ユースケース

次の分類は、アプリケーションが存在する場所に基づいています。

ケース1: フルKubernetes化



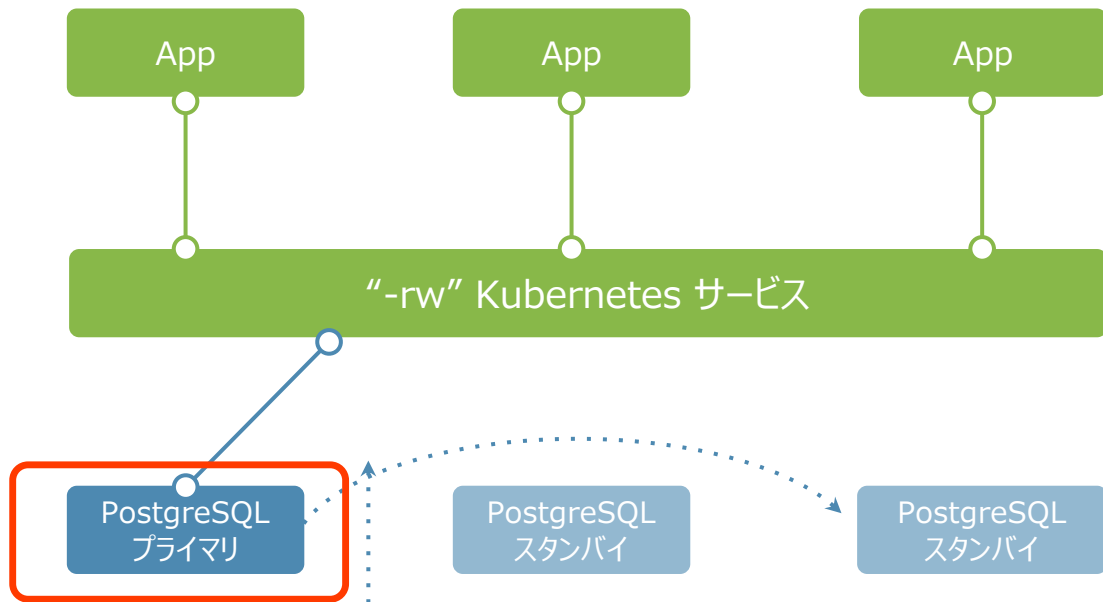
ケース2: レガシーシステムがKubernetesの外



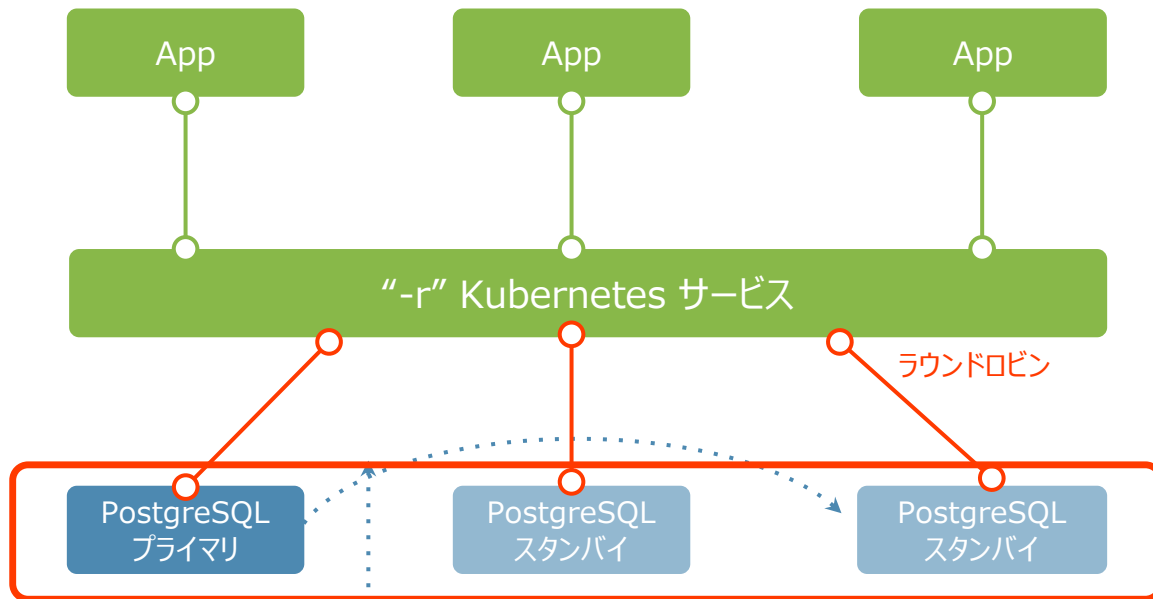
PostgreSQLクラスタ アーキテクチャ

- 1台の PostgreSQL プライマリ
- 任意の数のホット スタンバイ
 - PostgreSQLネイティブ ストリーミング レプリケーション
 - Async (default) and Sync (quorum-based)
 - HA構成には1台以上必要
 - pg_rewindの透過的なサポート
- 3 つの Kubernetes サービスをアプリに提供:
 - -rw suffix (読み取り/書き込みワークロード)
 - -r suffix (読み取りワークロード)
 - -ro suffix (プライマリを除く読み取りワークロード- in 1.1.0)

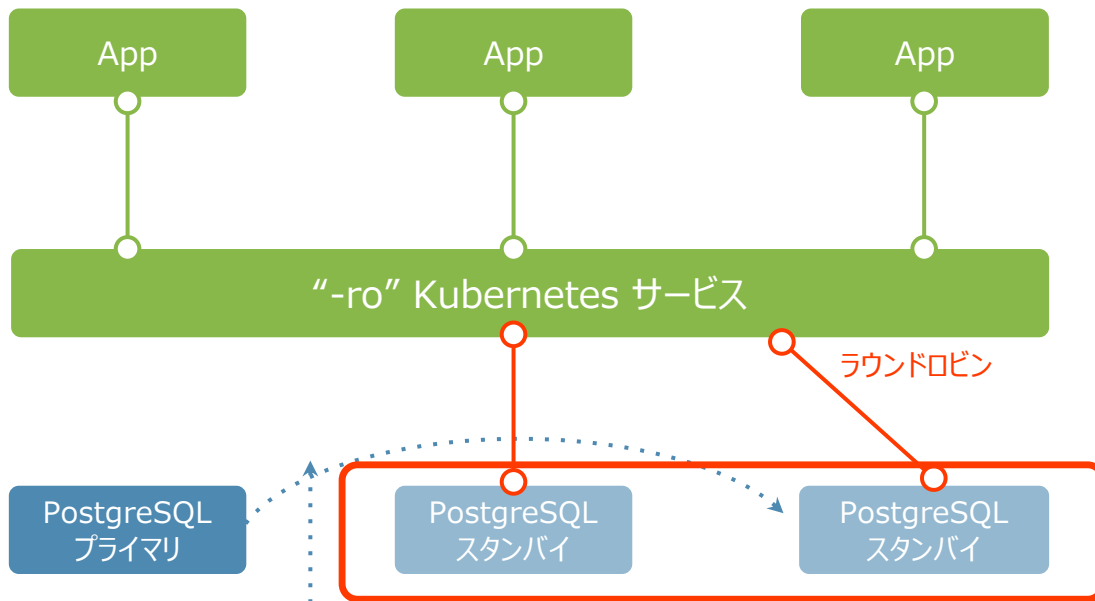
Read-writeワークロード("-rw" service)



Readワークロード("-r" service)



Readワークロード("-ro" service)



クラスタ管理

- セルフヒーリング
 - 死活と読み取りの監視
 - プライマリのフェールオーバー
 - レプリカの自動作成
- プライマリの切り替え(スイッチオーバー)
 - 選択したスタンバイのプロモート
- ロールングアップデート
- スケールアップ/ダウン

ストレージ管理

- 永続ボリューム のサポート (PVC)
 - PVCの自動生成
 - PVC テンプレートのサポート
 - 同じクラスター内のポッドのストレージの再利用
- ストレージクラスの動的プロビジョニング
 - Azure (default, managed-premium), AWS(gp2, io1, st1, sc1), Google(standard)
- 選択の自由
 - Local storage (デフォルト)
 - Network storage

ローリングアップデート

- ダウンタイムのないローリングアップデート
 - 以下の順序で自動更新
 1. 最初に、スタンバイ群が1台ずつアップデートされる
 2. その後、プライマリがスイッチオーバーされる
 3. 最後に古いプライマリがアップデートされる
 - supervised / unsupervised
- トリガーされる時:
 - オペレータのアップデート
 - PostgreSQL のマイナーアップデート
 - 設定の変更で再起動が必要な場合にもトリガー
- レプリカセットまたはステートフルセットを使用しなかった理由の一つ

セキュリティ

- 4Cセキュリティモデル
 - Cloud, Cluster, Container, Code
- ポッドセキュリティポリシーとセキュリティコンテキスト
 - コンテナとボリュームアクセスにroot権限は不要
- TLS 暗号化コネクション
- PostgreSQLシークレットの作成
- 静的コード分析
 - Linters と カバレッジスキャン

TLS (SSL) サポート

- ネイティブで完全に自動化
 - オペレータの証明機関
 - 各 Postgres クラスターの証明機関
- TLS コネクションがデフォルトで有効
 - TLS 証明書に基づくクライアント認証

継続的なバックアップ

- スケジュールとオンデマンド
- オブジェクト ストアのサポート(現在S3互換のみ)
 - Public clouds (AWSでサポート)
 - Private clouds (e.g. MinIO)
- Barman Cloud に依存
 - barman-cloud-wal-archive
 - archive_commandを経由したWAL配送
 - barman-cloud-backup
 - スケジュール／オンデマンドのバックアップコマンド

リカバリ

- バックアップから新しいクラスターを作成する
- base backup レストア
 - Full or PITR
- バックアップWALファイルをプルおよび再生
- Barman Cloud に依存
 - barman-cloud-restore
 - base backup からのリストア
 - barman-cloud-wal-restore
 - オンデマンドのWALのプル

リソース管理

- Podリソース制御
 - CPU とメモリの要求と制限 (スケジュール時のみ適用)
- Podアフィニティーwith nodeSelector
 - Podを展開する場所
- Podアンチアフィニティーpolicies
 - Podを展開しない場所
- Pod Disruption Budget
 - PostgreSQL グループで同時中断を制限する
 - Kubernetes ノードの制御メンテナンスウィンドウ

カスタム リソース定義(CRD)

- “Cluster” リソース
 - Kubernetes コントローラの拡張
- “instances” パラメータ
 - クラスタ内の PostgreSQL インスタンスの数
 - ホットスタンバイレプリカ数 = instances - 1
 - RPO=0 の非同期および同期レプリケーションをサポート

クラスタのデプロイメント

- 宣言型の構成
 - “kubectl” - Kubernetesの公式クライアントコマンドラインツール
 - YAML マニフェストファイル
 - Infrastructure as Code (IaC)
- クラスタの作成／更新と削除
 - `kubectl apply -f cluster-example.yaml`
 - `kubectl delete -f cluster-example.yaml`

マニフェストファイル最小 (yamlファイル)

```
apiVersion: postgresql.k8s.enterprisedb.io/v1
kind: Cluster
metadata:
  name: cluster-example
spec:
  instances: 3
  imageName: quay.io/enterprisedb/postgresql:13.2
storage:
  size: 1Gi
```

各種マニフェストファイルのサンプル

https://www.enterprisedb.com/docs/kubernetes/cloud_native_postgresql/samples/

同期レプリケーション

```
apiVersion: postgresql.k8s.enterprisedb.io/v1
kind: Cluster
metadata:
  name: cluster-example
spec:
  instances: 3
  minSyncReplicas: 1
  maxSyncReplicas: 2
  :
```

※ $0 \leq \text{minSyncReplicas} \leq \text{maxSyncReplicas} < \text{instances}$

PostgreSQLの設定

```
apiVersion: postgresql.k8s.enterprisedb.io/v1
kind: Cluster
metadata:
  name: cluster-example
spec:
  instances: 3
  postgresql:
    parameters:
      max_worker_processes: "60"
  pg_hba:
    - host all all all md5
  :
```

EDB Postgres Advanced Server

```
apiVersion: postgresql.k8s.enterprisedb.io/v1
kind: Cluster
metadata:
  name: cluster-example
spec:
  instances: 3
  imageName: quay.io/enterprisedb/edb-postgres-advanced:13.2
  licenseKey: <ここにライセンスキーを貼付け>
  :
```

トライアルライセンスキーの取得

<https://cloud-native.enterprisedb.com>



ロードマップ

Q3

さまざまなデータセンターのk8sクラスター間でレプリケーションをストリーミングして、災害リカバリと地理的に分散したアーキテクチャをサポート

監査機能

追加でサポートされるプラットフォーム：

- Rancher
- EKS

Q4

コネクションプーリングのサポート

ロジカルレプリケーションのサポート

双方向レプリケーションのサポート

オペレーターによるメジャーバージョンアップ

追加でサポートされるプラットフォーム：

- GKE
- Linux on Power
- Linux on Z

マーケットプレイスの可用性

- RedHat
- 米政府-国防総省

2022年以降

異なるデータセンターのk8sクラスター間での双方向レプリケーション

すでに利用可能なデフォルトのメトリックに基づくサンプルのGrafanaダッシュボード

オペランドのリソース使用量（CPU / メモリ）を報告するオペレーター

スマートなデフォルトと自動チューニング

pgAdminオペレーター

【Kubernetes×PostgreSQL】をその手に！

最先端のPostgreSQLユーザーエクスペリエンスを
いち早くご体験ください！

- EDBのお問い合わせ先
<https://edbjapan.com/contact/>
- Cloud Native PostgreSQLのマニュアル
英語版
https://www.enterprisedb.com/docs/kubernetes/cloud_native_postgresql/
日本語版（ユーザ登録の必要あり）
<https://edbjapan.com/manual/cnp-210509/>