

新入社員は見た！ ChatworkにおけるEKSの運用と取り組み

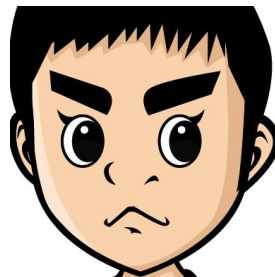


Chatwork株式会社

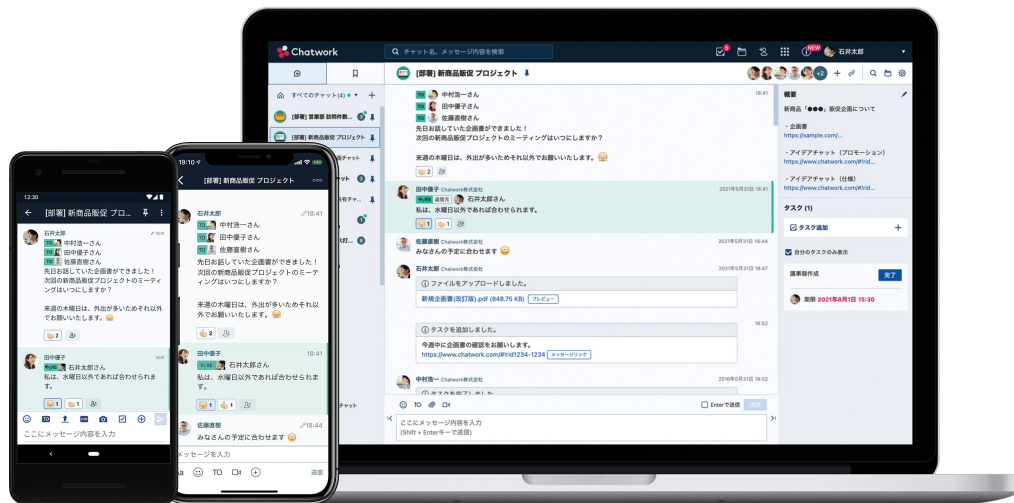
2022年08月04日 SRE部 古屋 啓介

新入社員紹介

- 古屋 啓介
 - Chatwork株式会社 プロダクト本部 SRE部
 - 2022年2月入社
- 入社時のスペック
 - AWS: 3年の実務経験（主にWebアプリ）、資格1x冠
 - Kubernetes(EKS): 実務経験なし、CKA取得済み



Chatworkとは



効率的に情報共有できる
グループチャット



仕事の見える化ができる
タスク管理

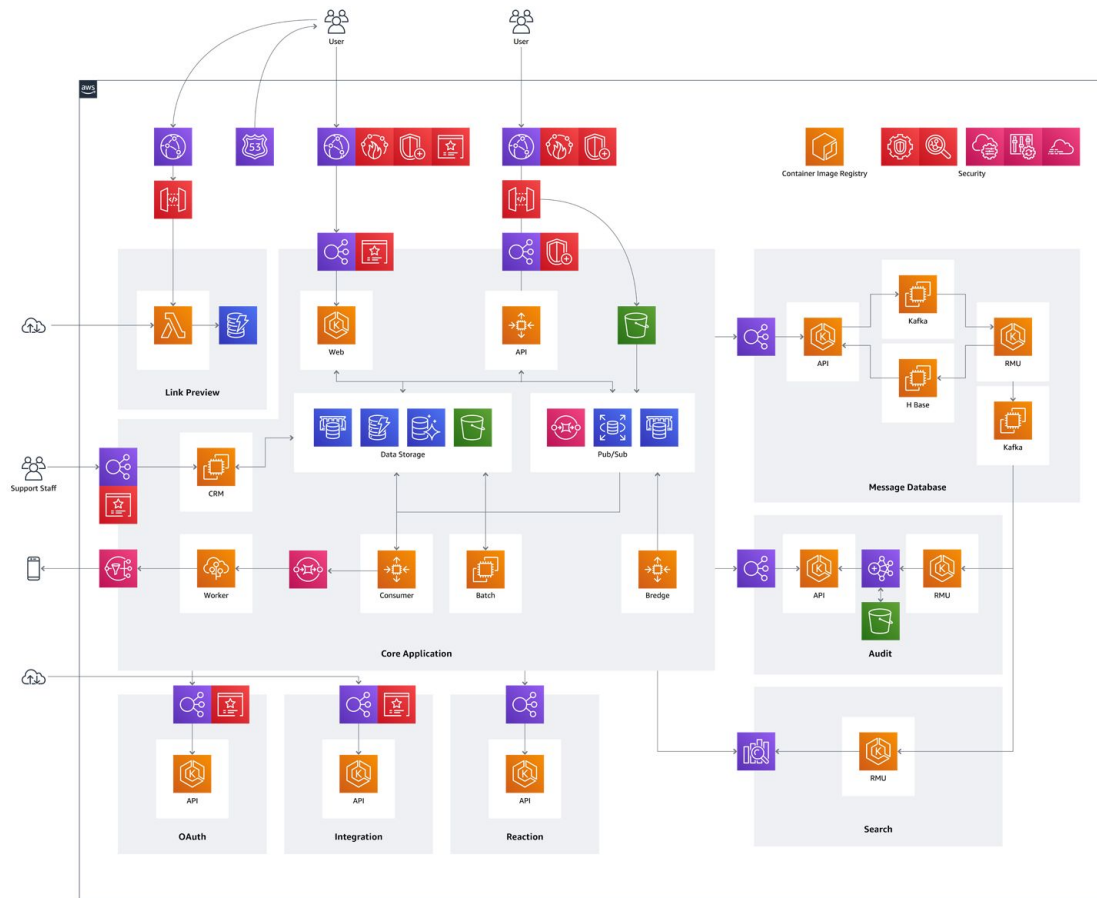


見落としがなくなる
ファイル管理

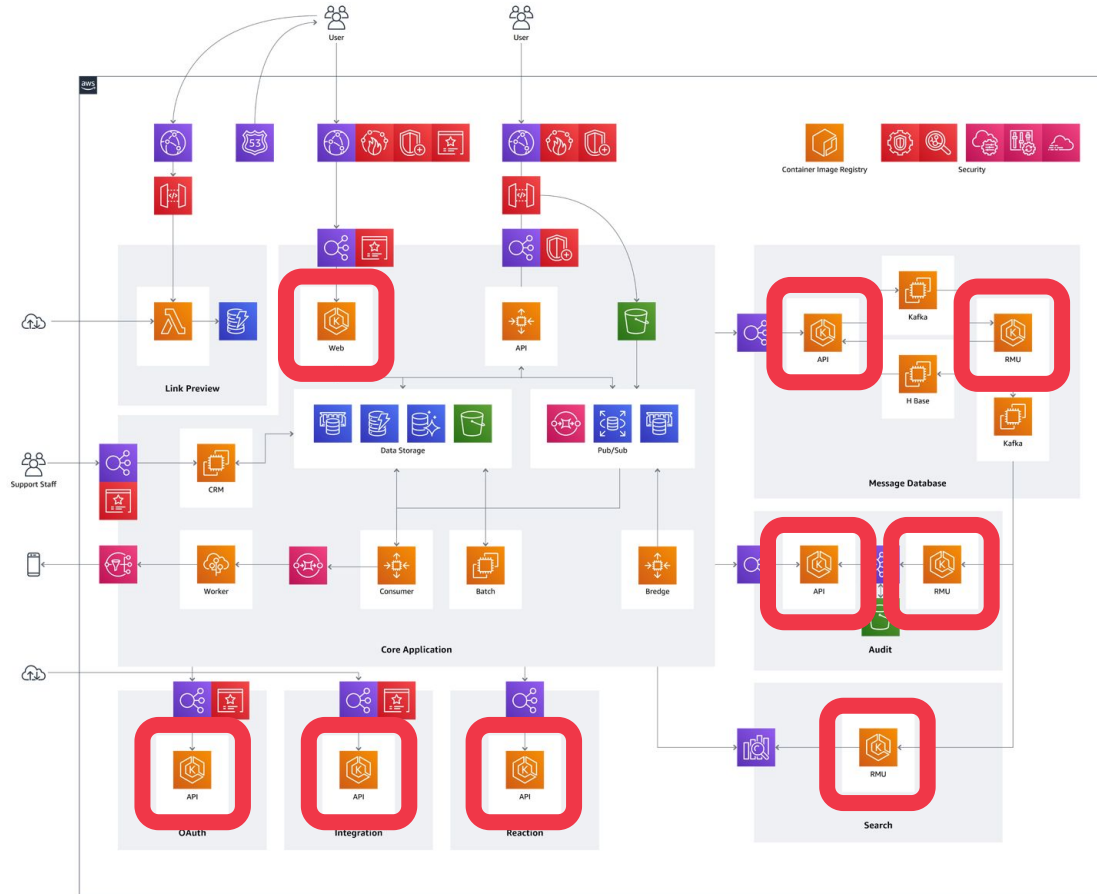


いつでも会議ができる
ビデオ/音声通話

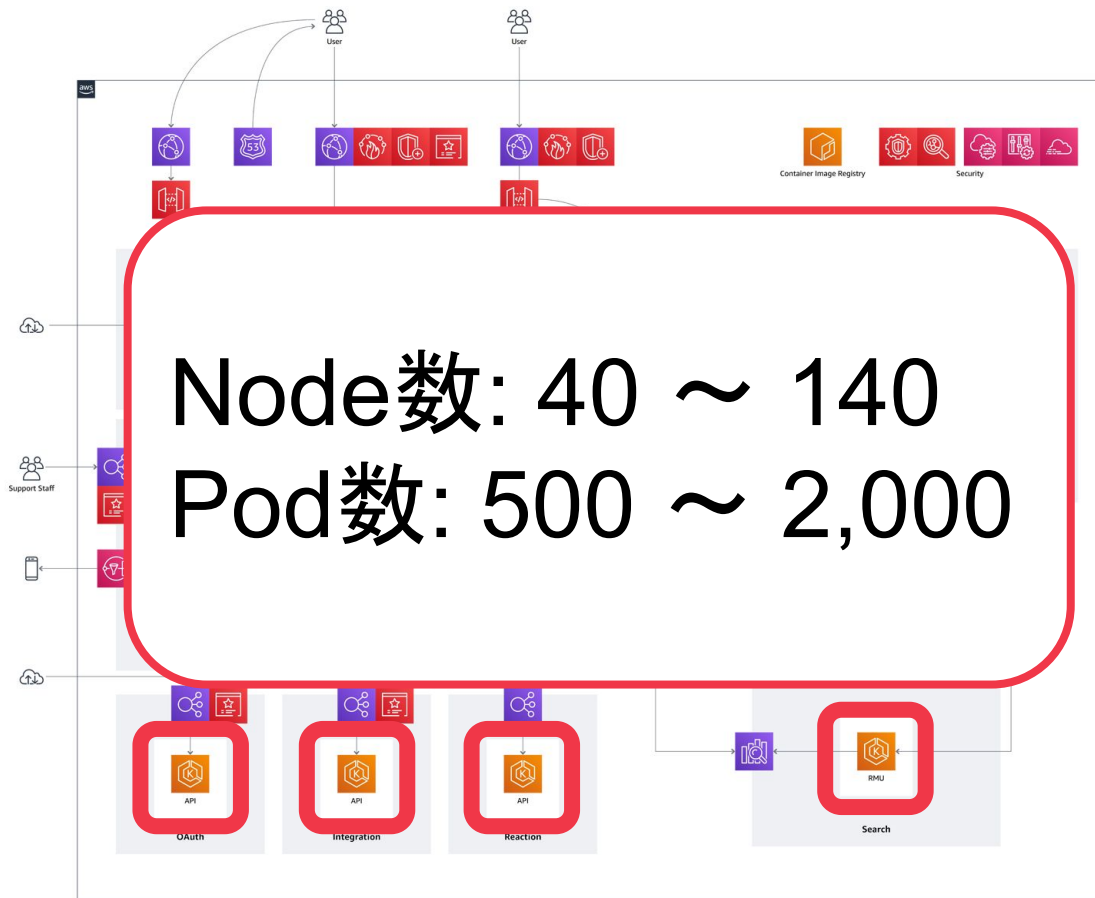
Chatworkの構成 (ざっくり)



Chatworkの構成 (ざっくり)

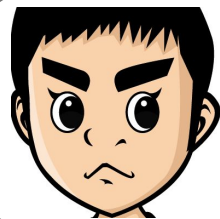


Chatworkの構成（ざっくり）



新入社員は思った

マニフェスト構成は？



EKSのバージョンアップ
どうしてるんやろ...

これどうやって
アプリのデプロイ
してるんやろ...

AGENDA

アジェンダ

- 1 ArgoCDによるGitOps
- 2 EKS1.22へのアップグレード
- 3 ChatworkのEKSを支えるツールたち
- 4 一歩先の運用（妄想と理想）

1

ArgoCDによるGitOps

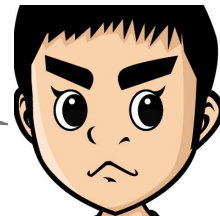
オリエンテーションにて



MGR

本番のArgoCDログインできるようにしよか

GitOpsといえば、ArgoCDですね～
(本番のArgoCDとか怖くて触りたくないけど)

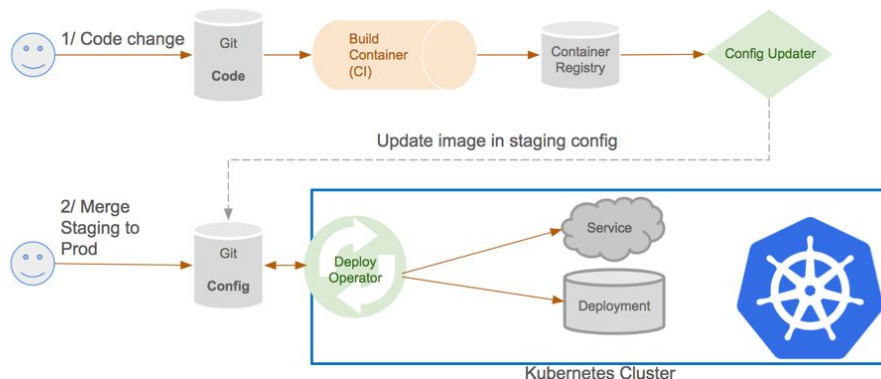


GitOpsとArgoCD (1/2)

- GitOps

- Kubernetesクラスタ管理・アプリケーションデリバリの手法
- Gitですべてを管理し、Git⇔クラスタ&アプリの状態を同期
- アプリのCI/CDとマニフェストのCI/CDが分離され柔軟な運用が可能

Example GitOps Pipeline



<https://www.weave.works/technologies/gitops/>

GitOpsとArgoCD (2/2)

- ArgoCD
 - GitOpsを実現するためのOSS
 - 定期的にGitを見て、クラスタとアプリをGit通りに自動同期する
 - Chatworkでは手動同期で運用中
 - 特にクラスタ構築時にアプリ同士の依存関係があるため
 - diffで最終チェックしてから適用したい



GitOps with ArgoCDがないとき/あるとき

- ないとき

kubectl apply... っと



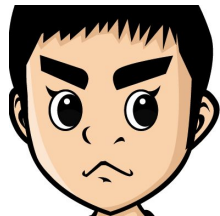
**人 or CIツールに強い権限が必要
クラスタ・アプリがGitの状態と同一である保証がない**

- あるとき



**権限はクラスタ内部に閉じる
クラスタ・アプリはGitの状態が常に正となる**

自己学習中



GitにChatworkのすべて
(のマニフェスト)があるってことかあ
マニフェストはどこで/どうやって
管理されてるんやろか

あ？ え？ dockerfileのリポジトリがあって？
helm Chartのリポジトリがあって？
helmfileのリポジトリ？



沼

helmとhelmfile (1/2)

- helm
 - Kubernetesのパッケージ管理OSS
 - いろんなアプリケーションのマニフェストがChartという単位で公開されている
 - Chartは雛形のみを提供し、細かいパラメータは変数として与えられる
 - **Chatworkが管理しているpublicなCharts/dockerfileリポジトリもアリマス**
 - 細々したマニフェストを自分で用意する必要なし
 - 例：いくつかパラメータを指定しつつfluentdのDaemonSetをサクッとデプロイ

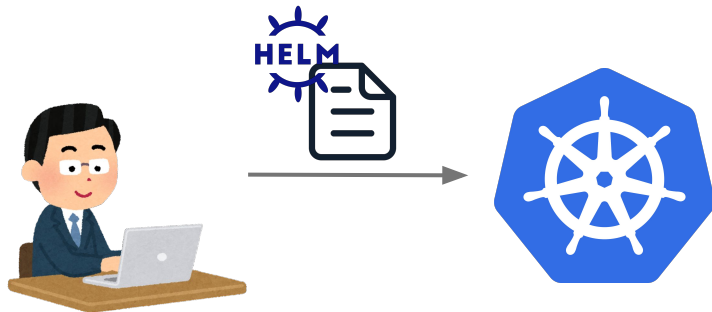


helmとhelmfile (2/2)

- helmfile

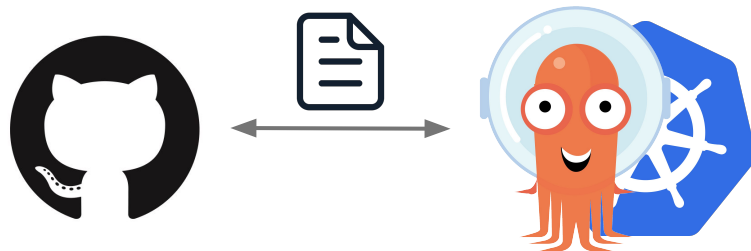
- helmをさらに宣言的/環境別に管理するためのOSS
 - helmコマンドをyamlファイルで管理できる → GitOpsとの相性が良い
 - 環境という概念があり、開発/ステージング/本番の切り替えが容易になる

helmの場合



**helm installコマンド
のポチポチが必要**

helmfileの場合



**helmコマンドをyaml化して
GitOps!**

(余談) 個人的に面白いなと思ったhelm Chart

- slime Chart
 - アプリを動かすのに最低限必要な雛形を提供するChart
 - deployment + service + ingress
 - 公式のChartがないものをhelmfile運用できる
 - 似たようなのでraw Chartというのものもあるけど自由度が高すぎる

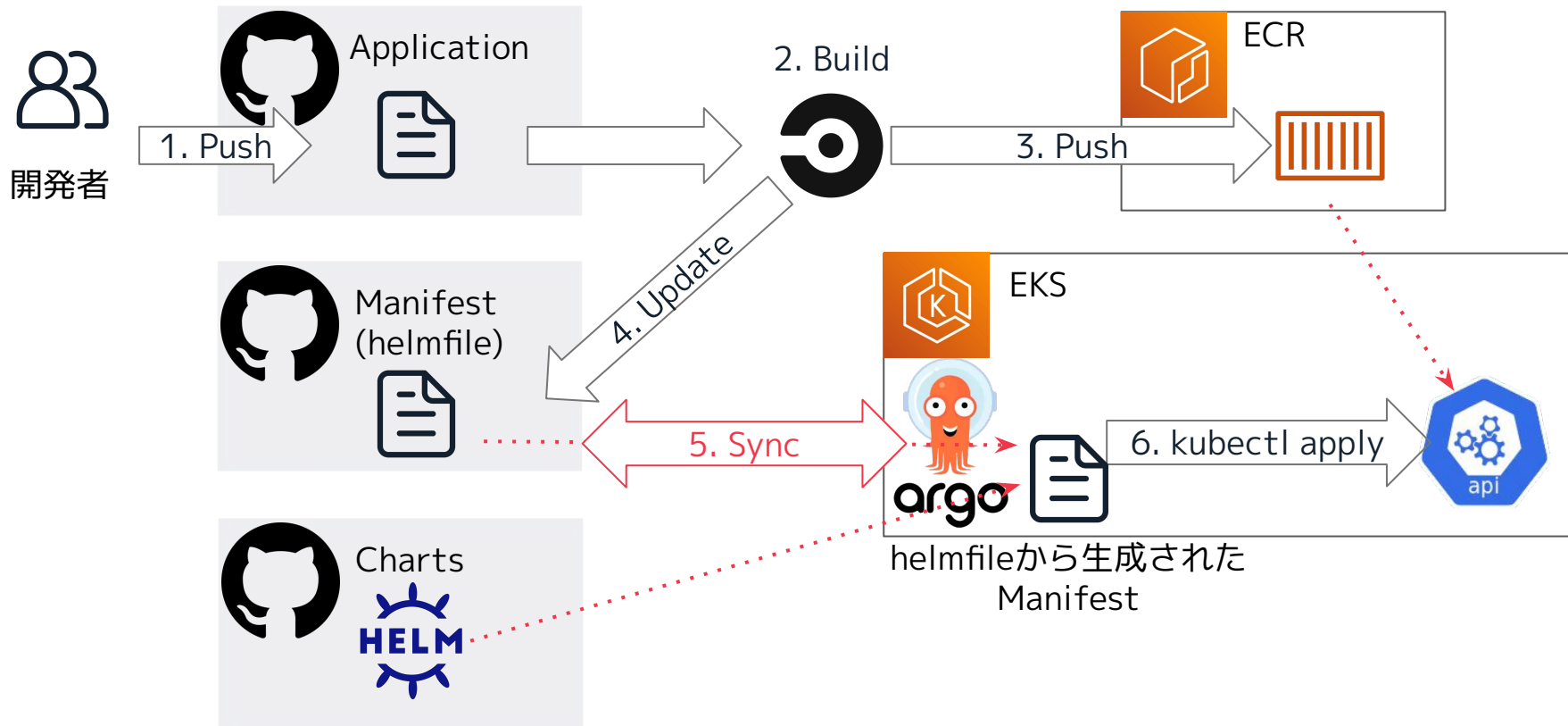
slime

(👁️) < Not my bad slime

(👁️) < I will transform into anything

↑readmeのこれがすき

実際のデプロイフロー



新入社員が感動したポイント

- リリースはmasterマージとArgoCDでSyncするだけ
 - 簡単・はやい
- 開発チーム内で完結
 - 開発とリリースの速度を落とさない「あるべき姿」
- バチバチに構造化されたマニフェストたち
 - helmfileに最適化されまくっている（逆に新人には読み解きづらいことも...）

2

EKS1.22へのアップグレード

AWSさんEKS1.22対応お疲れ様でした

Amazon Web Services ブログ

Amazon EKS が Kubernetes 1.22 のサポートを開始

by Soto Sugita | on 07 APR 2022 | in [Amazon Elastic Kubernetes Service](#), [Containers](#) | [Permalink](#) | [Share](#)

この記事は [Amazon EKS now supports Kubernetes 1.22](#) (記事公開日: 2022 年 4 月 4 日) を翻訳したものです。

Amazon Elastic Kubernetes Service (Amazon EKS) チームは、Kubernetes 1.22 のサポートを発表できることを嬉しく思います。 [Amazon EKS](#)、[Amazon EKS Distro](#)、そして [Amazon EKS Anywhere](#) は、Kubernetes バージョン 1.22 を実行できるようになりました。アップストリームプロジェクトのこのリリースのテーマは、"Reaching New Peaks" です。リリースリードの [Savitha Raghunathan](#) によると、このリリースのテーマは彼女が次のように説明したことによります: "パンデミックとバーンアウトにもかかわらず、Kubernetes 1.22 はあらゆるリリースの中で最も多くの機能拡張が行われました。" このリリースでは、かなりの数の API の変更、Kubernetes のリリース頻度の変更、その他多くのアップデートが行われています。このリリースをより優れたクラウドネイティブエコシステムにもたらすために、アップストリームの [Kubernetes 1.22 リリースチーム](#) が行ってきたすべての作業に感謝します。



Kubernetes 1.22: Reaching New Peaks ロゴ

<https://aws.amazon.com/jp/blogs/news/amazon-eks-now-supports-kubernetes-1-22/>

ChatworkのEKSアップグレード基本方針

- 基本的に毎回あげる
 - が、あまりにスパンが短い場合はスキップすることもある
 - 実は1.21にあげておらず1.20から1.22へ...
 - 1.22へは移行完了済み、次（1.23）は8月？
- Blue/Greenで切り替える
 - 新規クラスタを構築して無停止でアプリを載せ替えていく

事前準備

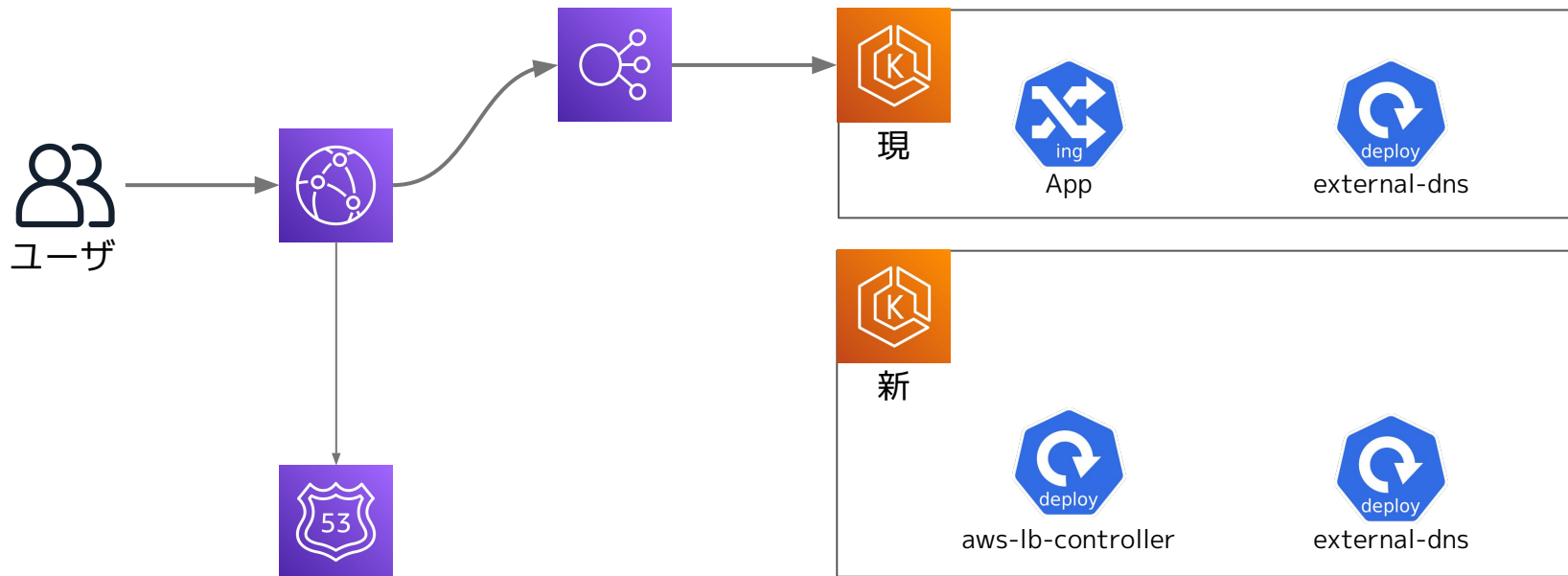
- Kubernetes的/EKS的な変更内容の確認と修正
 - 廃止になったAPI versionはないか、など...
 - 必要であればhelm Chartの修正
- 社内への説明会
 - 開発メンバへも修正点を共有する

クラスタの構築

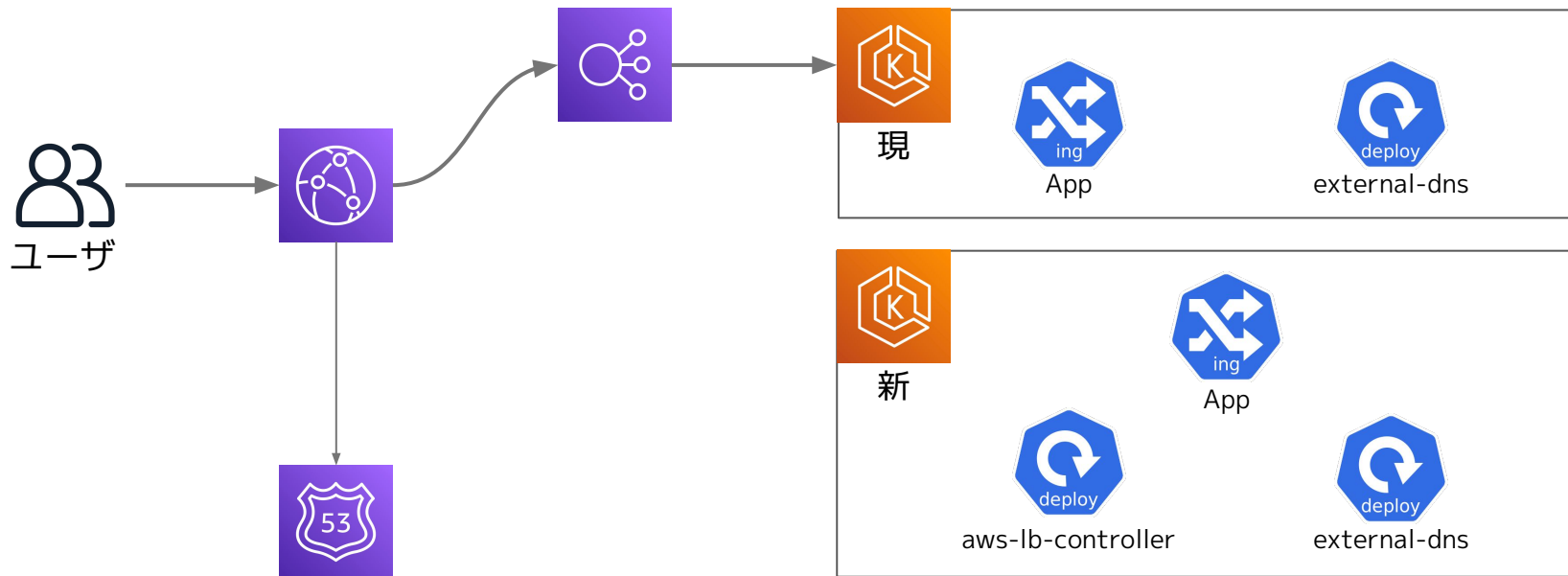
- achlis (eksctlのwrapper) でEKSクラスタ諸々をデプロイ
 - eksctlで利用する設定ファイルを自動生成したりなど
 - 詳しくは「Chatwork achlis」で検索！
- SRE部管轄のアプリをArgoCD経由でデプロイ
 - 管理系、ログ・監視系など



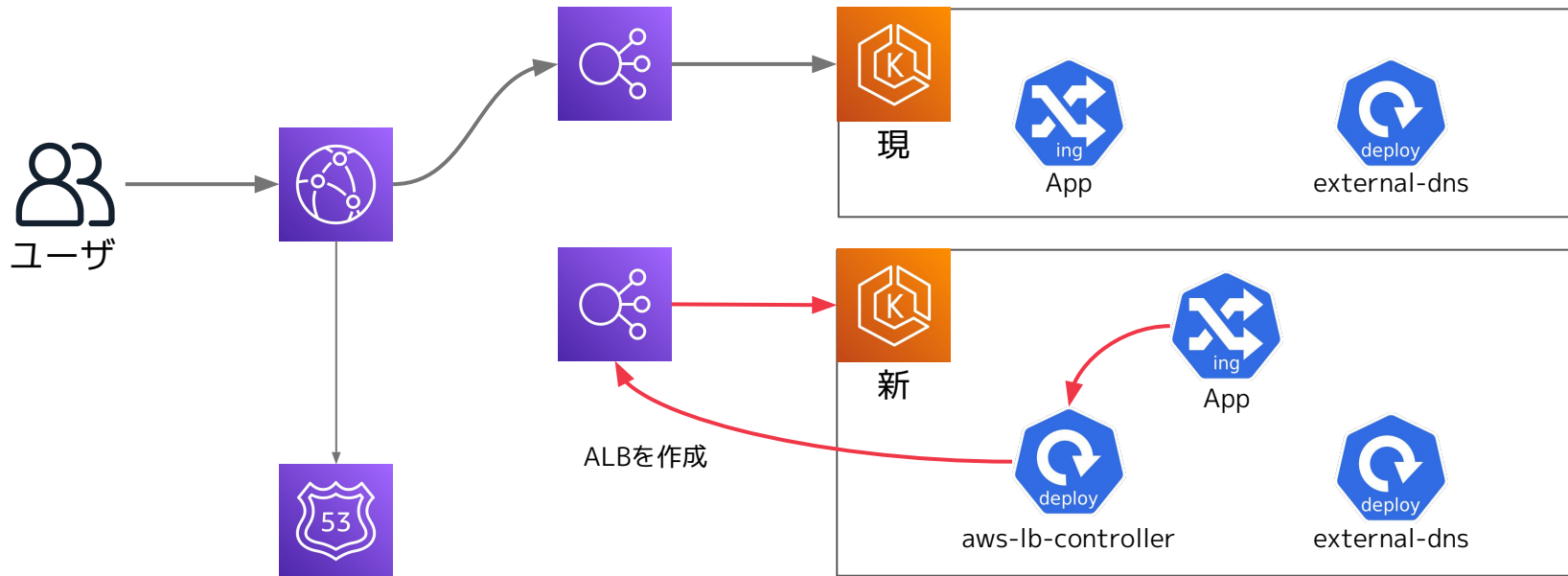
新クラスタへの切り替え (1/8)



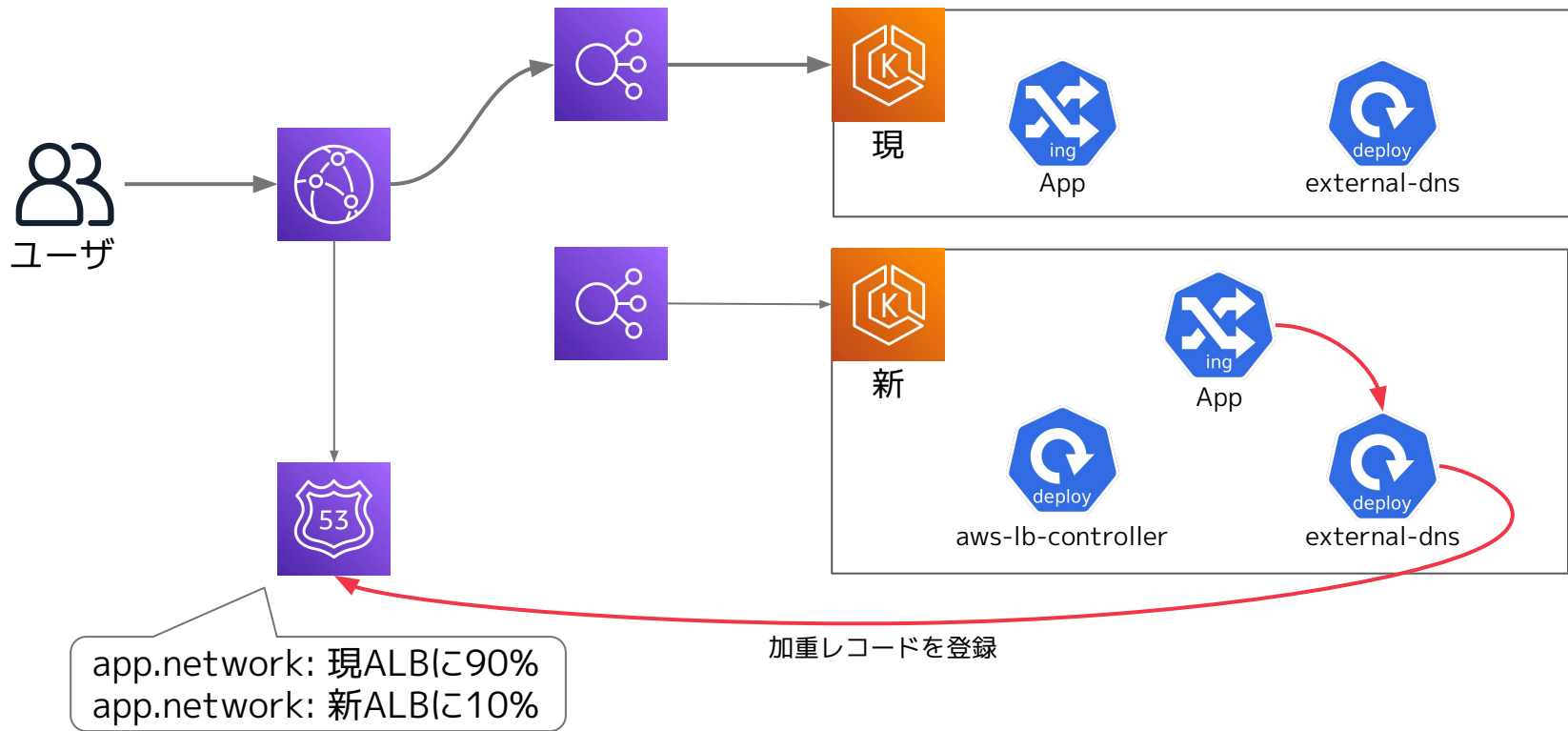
新クラスタへの切り替え (2/8)



新クラスタへの切り替え (3/8)



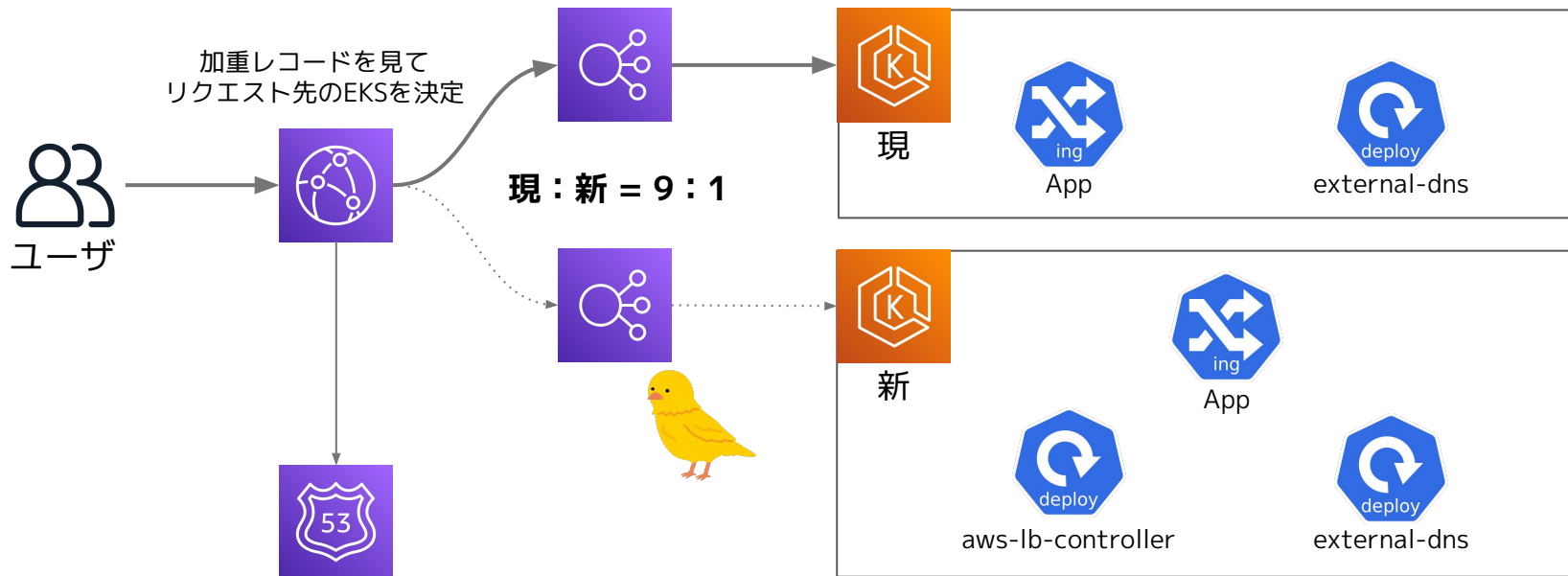
新クラスタへの切り替え (4/8)



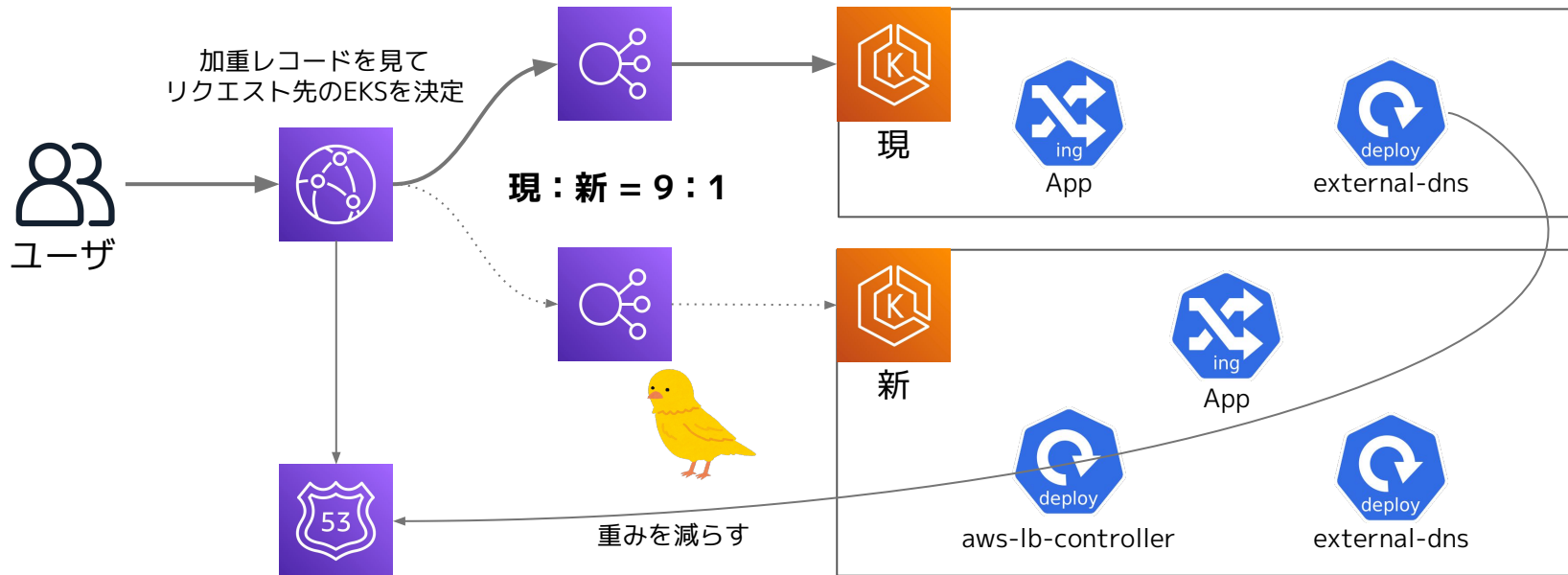
ポイント

- 外からの通信だけでなくアプリ間通信もALBを経由
 - 通信先アプリがどこにいてもALBにあてたFQDNでアクセスできれば問題なし
- external-dnsによるDNS登録とルーティング制御
 - Route53に加重レコードを自動で登録してくれる

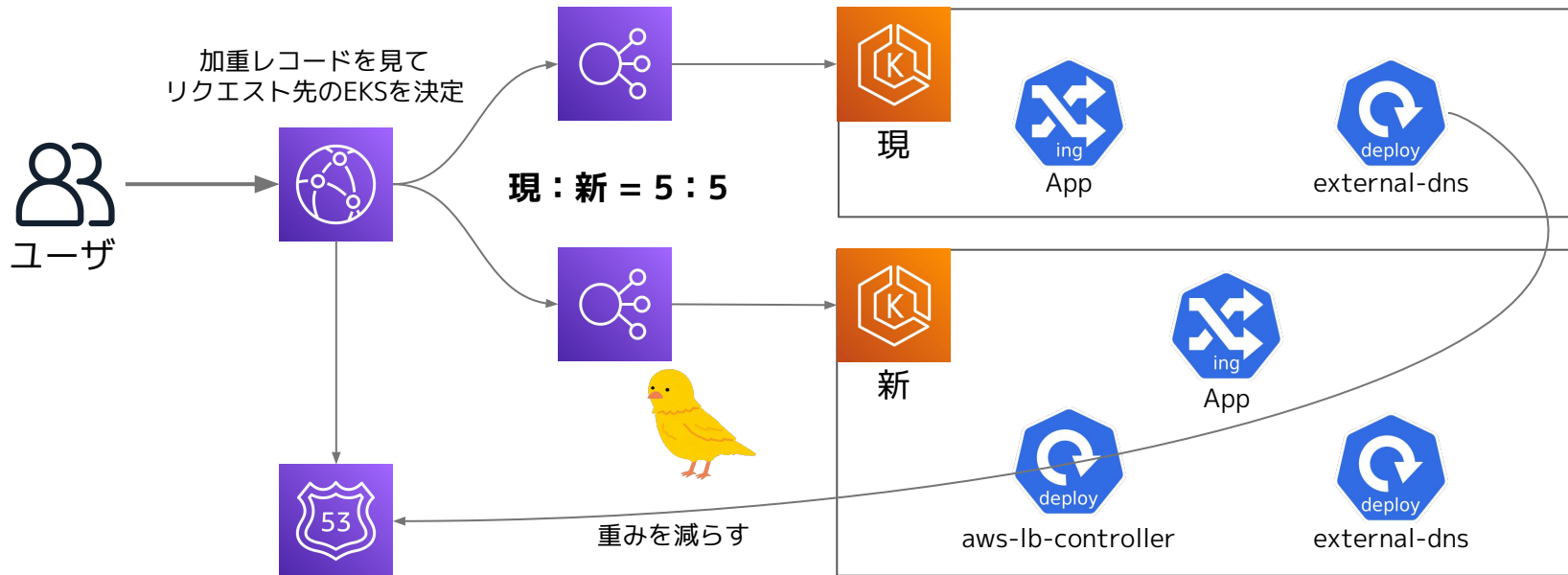
新クラスタへの切り替え (5/8)



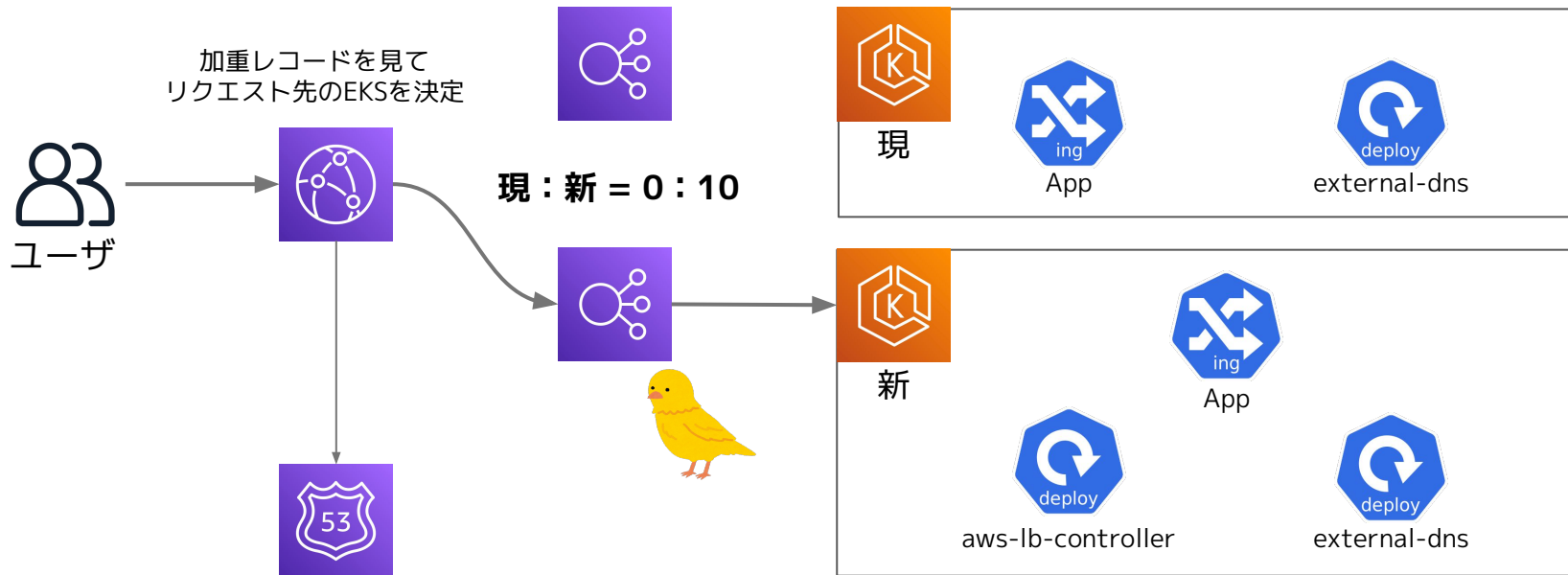
新クラスタへの切り替え (6/8)



新クラスタへの切り替え (7/8)



新クラスタへの切り替え (8/8)



新入社員が感動したポイント

- アプリがデプロイ可能なクラスタの構築は2, 3コマンドで完了
 - ArgoCDポチポチはありつつも手順がまとまっており誰でも実行可能
- アプリの移行は開発チーム内で完結
 - こちらもSRE部関与なしで移行してもらえる
- 営業時間中に無停止かつ数回のデプロイで移行可能
 - 危なげなく無事故で移行完了

3

ChatworkのEKSを支えるツールたち

ピックアップ1: external-dns

- 特徴
 - Route53にレコードを自動で登録
- 使い方
 - ingressにannotationをちよろっと書くだけ
 - 例: external-dns.alpha.kubernetes.io/hostname: hogehoge.com
- 嬉しいポイント
 - マニフェスト内で完結するため、AWS権限のない開発者でも自由に操作ができる

ピックアップ2: aws-secret-operator

- 特徴
 - AWS Secrets Managerに保管したクレデンシャルをもとにSecretを作成
- 使い方
 - AWS Secrets Managerにクレデンシャルを保存
 - AWSSecretカスタムリソースで読み込み
- 嬉しいポイント
 - GitHub上に機密情報を置かなくてよい = GitOpsと相性が良い
- その他
 - Secrets Store CSI Driverは使いにくかったらしい（2021年検証時）
 - 検証時はGAなりたてで一部αだったり、Chartも微妙だったり
 - IAM権限がアプリPodに必要なのかOperatorに必要なのかも運用次第

ピックアップ3: aws-node-termination-handler

- 特徴

- Spotインスタンス終了を検知してpodをdrainしてくれる

- 使い方

- DaemonSetをインストールするだけ
 - SQSとか作らないとだめだけどより高機能なDeployment版も

- 嬉しいポイント

- Spot活用しているSelf-Managed Node Groupでpodを安全に退避できる
 - Managed Node Groupでは最初から入っている

- (余談) ChatworkではSelf-Managed Node Groupで運用中

- Managed Node Groupにしたいけど...
 - kubelet extra configを触りたい
 - 作成時にタグ付けしたい (cluster-autoscalerのため)

AWSさんお願いします

issueもあります

<https://github.com/aws/containers-roadmap/issues/608>

詳細はこちら

- 2020年版ですがあまり変わってないので
 - 「Chatwork Kubernetes ツール」で検索！



2020-12-23

ChatworkのKubernetesを支えるツールたち (2020年版)

SRE Kubernetes

こんにちは。SRE部坂本です。毎年最低1回はフルマラソンに出ています。2020年はあえなく参加できずに終わりました。2月にギリギリ行われたハーフマラソンではなんとか90分切り(89分台)を達成し、今年は3時間10分以内を目指してただけに残念ですが、仕方ありません。

特に部活等で走っていたわけでもなく、トラックの大会に参加するのはやや抵抗があり、年間の走行距離ぐらいしか目標がなく、これを書いている12月中旬で2591kmとなっています。昨年が2724kmだったので、なんとか更新したいなーというのが今の気持ちです。

さて、Chatworkでは2016年からKubernetesを導入しております。EKSもない時代ですので、[kube-aws](#)というツールを利用してEC2にホスティングして運用していましたが、今年EKSに移行しました。

AWS 導入事例：Chatwork 株式会社 | AWS

ビジネスチャットツール「Chatwork」を運営する Chatwork 株式会社。2011年3月のリリース以来、サービス基盤にアマゾンウェブサービス (AWS) を採用し、アーキテクチャを進化させてきま...

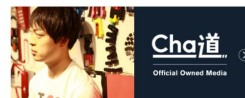


ビジネスチャット「[Chatwork](#)」のエンジニアとデザイナーのブログです。

＋ 読者になる

検索

記事を検索



@Chatwork_devさんをフォロー

メンバー

ピックアップ4: OPA Gatekeeper

- 特徴
 - Open Policy Agentという仕組みに則りマニフェストやリソースの検査を行う
 - 例：特定のラベルを付与してないとデプロイさせない
- 使い方
 - インストールする
 - Regoに則ったPolicyをもつカスタムリソース（Constraint）を作成する
- Gatekeeperを使うにあたってのポイント
 - CIの時点でOPAでvalidationを行うためにConftestを活用
 - ConftestとPolicyを共有するためにKonstraintを活用

4

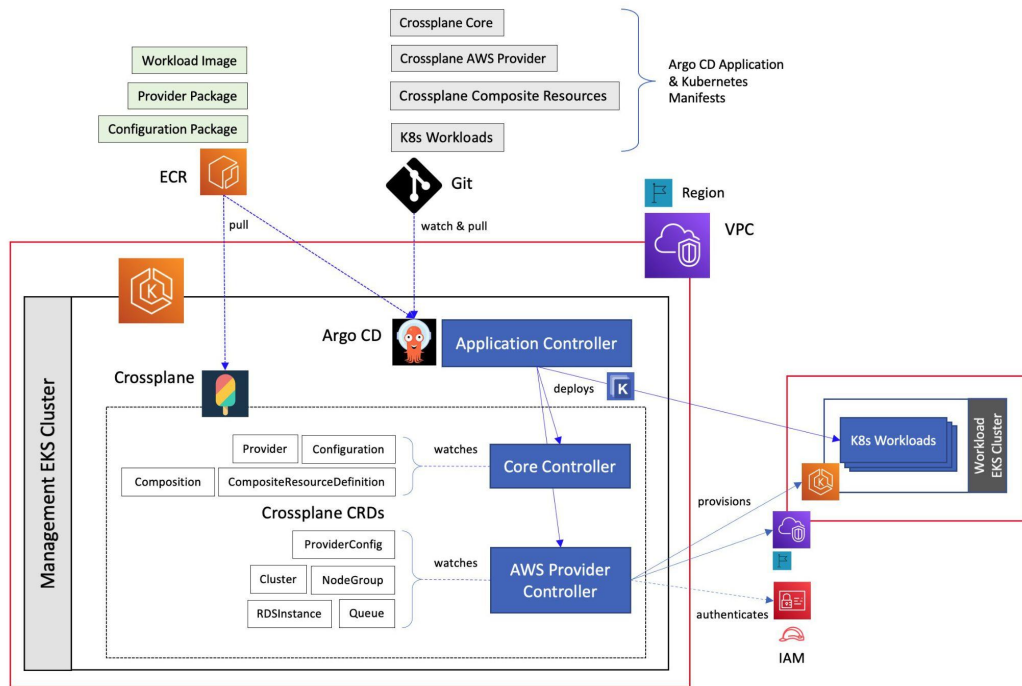
一步先の運用（妄想と理想）

achlis (eksctlのwrapper) の課題

- 実行には作業者ローカルに強い権限が必要
 - ローカルでの実行を想定
- 複数環境（開発/ステー징/本番）作るのしんどい
 - なるべく簡単に作れるようになってるとはいえ
 - 別プロジェクト分も含めて7環境作る必要アリ

妄想: EKSでEKSを作る世界

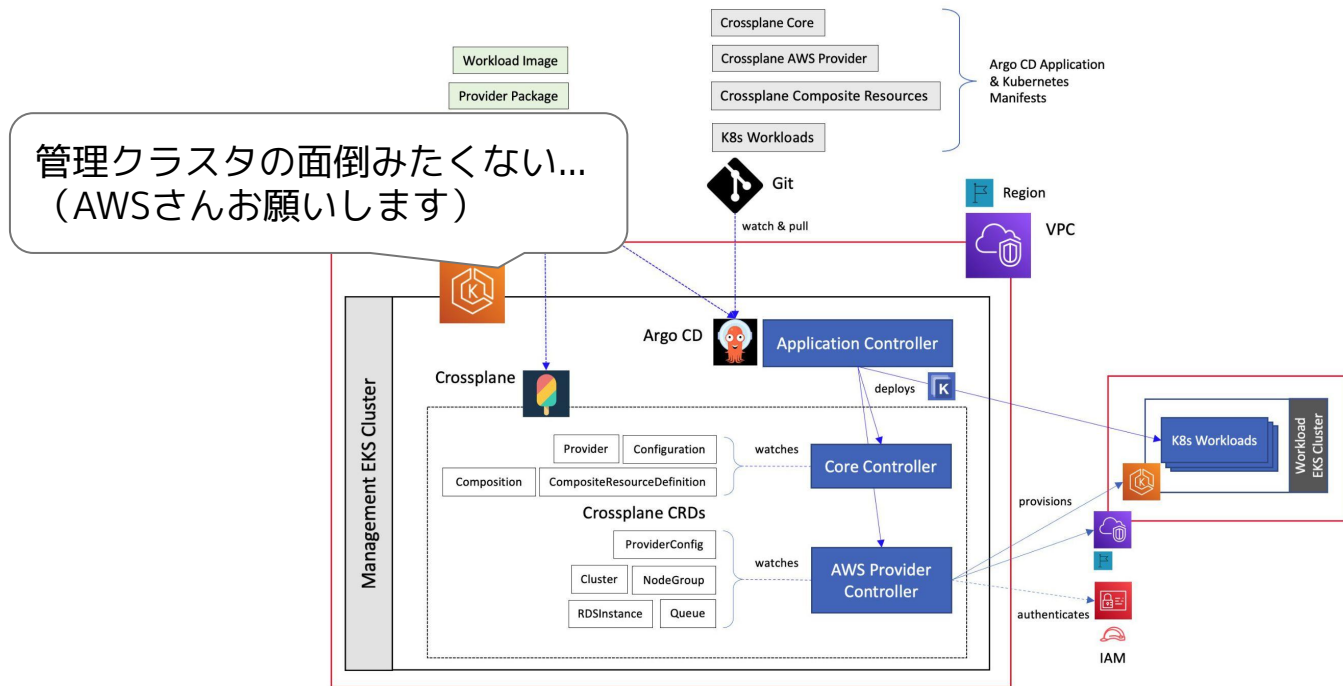
- Crossplane x ArgoCD



<https://aws.amazon.com/jp/blogs/containers/gitops-model-for-provisioning-and-bootstrapping-amazon-eks-clusters-using-crossplane-and-argo-cd/>

妄想: EKSでEKSを作る世界

- Crossplane x ArgoCD



<https://aws.amazon.com/jp/blogs/containers/gitops-model-for-provisioning-and-bootstrapping-amazon-eks-clusters-using-crossplane-and-argo-cd/>

理想: EKSでEKSを作る世界

1. 新クラスタのマニフェストを作成してArgoCDでSyncする
 - ローカルに強い権限が不要
2. 現クラスタが新クラスタを自動構築
 - 管理クラスタは利用せず、稼働中のクラスタのみで完結させる
3. 新クラスタでArgoCDが管理系ツールを自動デプロイ
 - 「あとはアプリを載せるだけ」のクラスタを「宣言的」に構築完了！

理想: EKSでEKSを作る世界

1. 新クラスタのマニフェストを作成してArgoCDでSyncする
 - ローカルに強い権限が不要
2. 現クラスタが新クラスタを自動管理する
 - 管理UIは利用せず、稼働中のクラスタで完結させる
3. 新クラスタがArgoCDが管理系ツールを自動デプロイする
 - 「コンテナイメージを載せるだけ」のクラスタで「宣言的」に構築完了!



Crossplane



HashiCorp
Terraform

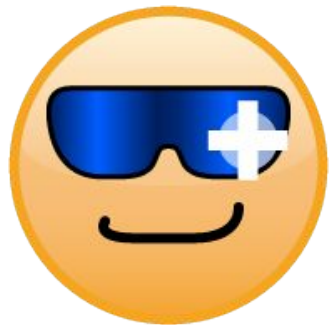
AGENDA

アジェンダ

- 1 ArgoCDによるGitOps
- 2 EKS1.22へのアップグレード
- 3 ChatworkのEKSを支えるツールたち
- 4 一歩先の運用（妄想と理想）

まとめ

- 2022年最新のChatworkにおけるEKS運用についてのお話
 - GitOps、アップグレード戦略、便利ツール
- ベストプラクティスに沿うことで安定した運用を実現
 - 開発者によるGitOpsや無停止でのアップグレードなど
- まだまだ改善やっていき
 - ゆくゆくはEKSでEKSを作る世界へ



宣伝: 採用募集



募集職種一覧

どんなSaaSよりも利用時間が長いビジネスチャット。
日本中のビジネスのやり取りが集中するこの希有な場で、あなたはどんなイノベーションを起こしますか。

エンジニア <input type="checkbox"/>	PM・デザイナー <input type="checkbox"/>	セールス <input type="checkbox"/>
マーケティング <input type="checkbox"/>	事業開発 <input type="checkbox"/>	事業戦略・事業企画 <input type="checkbox"/>
コーポレート/その他 <input type="checkbox"/>	オープンポジション <input type="checkbox"/>	

2022. 10. 08 Sat.

CfP募集中!!!



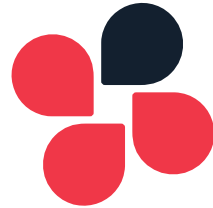
note <https://note.com/jawsdays/>

twitter @jawsdays

facebook www.facebook.com/jawsug

Let's have fun together!

働くをもっと楽しく、創造的に



Chatwork