

AWSドキュメント 自動化のススメ

～ それなりにいい感じのドキュメント～

高江洲 祐治(たかえす ゆうじ)

たかえす ゆうじ

- サーバークラス大阪 技術4課
- 趣味は、お酒とマラソン
- 好きな言語

Ruby

Python, Golang あたりは勉強中)

- 好きなAWSサービス

S3 (Lambda等のServerlessやりたい気持ち)

早速ですが

こんなのを作りました

sgdoc

<https://github.com/yusabana/sgdoc>

セキュリティグループの設定をマークダウンとして出力するドキュメント自動化ツール

※現状はプロトタイプレベルのサンプル実装

実行方法

shared credentialsや環境変数でアクセストークン・シークレットを設定しておく

- `$ gem install sgdoc`
- `$ sgdoc > security_groups.md`

security_groups.md

Inbound

Protocol	Port	Source	%Description
----	----	----	----
tcp	3306	10.10.0.0/16	
tcp	3306	10.20.0.0/16	

Outbound

Protocol	Port	Destination	%Description
----	----	----	----
all	all	0.0.0.0/0	

...略

マークダウンツールで表示(Backlog)

構成管理ツールYambdaで出力したドキュメントっぽい

rds-launch-wizard

Group ID	Description	Tags
sg-0376330e	Created from the RDS Management Console	

Inbound

Protocol	Port	Source	%Description
tcp	3306	10.10.0.0/16	
tcp	3306	10.20.0.0/16	

Outbound

Protocol	Port	Destination	%Description
all	all	0.0.0.0/0	

Instances references

Instance Name	Instance ID	Security Groups
myTestVPC_1	i-06027227-4ca0130	maintenance, TestELB-quick-create-1, default
myTESTVPC_NAT_instance_sample	i-04200130020000008	maintenance

なぜ作ったか(本日は話すこと)

- 構成管理ツールのYambdaとは
- 運用フェーズの現状と課題
- マネジメントコンソールつらい問題
- AWSドキュメント化ツールの展望

構成管理ツールのYambdaとは

- どんなもの

設計・構築支援するサーバーワークス社内ツール

AWS環境の標準化と構築のスピードアップ

- 自動生成

設定パラメータの **ドキュメント(マークダウン)** を自動生成

構築自動化のための **CloudFormationテンプレート** を自動生成

Yambdaは おもに 初期構築 に特化した 標準化/自動化の構成管理

初期構築は品質を維持して大幅に効率化できている

運用フェーズの現状と課題

- 運用開始後に追加構築などでYambdaが余り活用ができていない
- マネジメントコンソールで設定変更することが結構ある
 - セキュリティグループ1つ追加する...
 - インスタンスタイプの変更...
- 設定パラメータのドキュメント(マークダウン)を手で加筆修正している
 - 引き継ぎ案件だとそもそもドキュメント修正忘れてしまったり...

rds-launch-wizard

Group ID	Description	Tags
sg-0074e00e	Created from the RDS Management Console	

Inbound

Protocol	Port	Source	%Description
tcp	3306	10.0.0.0/16	
tcp	3306	10.20.0.0/16	

Outbound

Protocol	Port	Destination	%Description
all	all	0.0.0.0/0	

Instances references

Instance Name	Instance ID	Security Groups
myTestVPC_1	i-00037a2274e30f130	maintenance, TestELB-quick-create-1, default
myTESTVPC_NAT_instance_sample	i-04200214020090228	maintenance

設定パラメータのドキュメント

- お客さんと認識合わせのために必要最低限のAWS設定値情報
- 運用する上で変更がありそうな設定情報
- 細かい設定値すべては網羅しなくてもよいので、確認しやすいよう一覧性のある表示

rds-launch-wizard

Group ID	Description	Tags
sg- XXXXXXXXXX	Created from the RDS Management Console	

Inbound

Protocol	Port	Source	%Description
tcp	3306	10.10.0.0/16	
tcp	3306	10.20.0.0/16	

それなりの情報をいい感じに

Outbound

Protocol	Port	Destination	%Description
all	all	0.0.0.0/0	

ブラウザの文字列検索もできる

Instances references

Instance Name	Instance ID	Security Groups
myTestVPC_1	i- XXXXXXXXXX	maintenance, TestELB-quick-create-1, default
myTESTVPC_NAT_instance_sample	i- XXXXXXXXXX	maintenance

"マネジメントコンソールでいいんじゃないね??"

そうなんだけど...

マネジメントコンソールつらい 問題

EC2から関連しているセキュリティグループを確認

EC2 ダッシュボード

イベント
タグ
レポート
制限

インスタンス
インスタンス
スポットリクエスト
リザーブドインスタンス
専有ホスト

イメージ
AMI
バンドルタスク

ELASTIC BLOCK STORE
ボリューム
スナップショット

ネットワーク & セキュリティ
セキュリティグループ
Elastic IP
プレースメントグループ
キーペア
ネットワークインターフェイス

ロードバランシング
ロードバランサー
ターゲットグループ

AUTO SCALING
起動設定
Auto Scaling グループ

SYSTEMS MANAGER

インスタンスの作成 接続 アクション

タグや属性によるフィルター、またはキーワードによる検索

3 個中 1 ~ 3

Name	インスタンス ID	インスタンスタイプ	アベイラビリティゾーン	インスタンスステータス	ステータスチェック	アラームのステータス	パブリック DNS
myTESTVPC_NAT_instance...	i-0e63f72f274ea8fb0	t2.nano	ap-northeast-1a	stopped		なし	
myTestVPC_1	i-0e63f72f274ea8fb0	t2.micro	ap-northeast-1a	running	2/2 のチェ...	なし	ec2-13-112-135...
myTestVPC2_1	i-0e63f72f274ea8fb0	t2.nano	ap-northeast-1a	stopped		なし	

選択して

インスタンス: i-0e63f72f274ea8fb0 (myTestVPC_1) パブリック DNS: ec2-13-112-135-183.ap-northeast-1.compute.amazonaws.com

マウスで引き上げたりして

説明 ステータスチェック モニタリング タグ

インスタンス ID	i-0e63f72f274ea8fb0	パブリック DNS (IPv4)	ec2-13-112-135-183.ap-northeast-1.compute.amazonaws.com
インスタンスの状態	running	IPv4 パブリック IP	13.112.135.183
インスタンスタイプ	t2.micro	IPv6 IP	-
Elastic IP		プライベート DNS	ip-10-10-1-225.ap-northeast-1.compute.internal
アベイラビリティゾーン	ap-northeast-1a	プライベート IP	10.10.1.225
セキュリティグループ	maintenance, TestELB-quick-create-1, default. インバウンドルールの表示	セカンダリプライベート IP	
予定されているイベント	予定されているイベントはありません	VPC ID	vpc-24106e5b
AMI ID	myTest1-rhel (ami-6e988e09)	サブネット ID	subnet-b5f4fcc3
プラットフォーム	-	ネットワークインターフェイス	eth0

セキュリティグループをひとつずつみる

セキュリティグループの詳細

EC2 ダッシュボード

イベント
タグ
レポート
制限

インスタンス
インスタンス
スポットリクエスト
リザーブドインスタンス
専用ホスト

イメージ
AMI
バンドルタスク

ELASTIC BLOCK STORE
ボリューム
スナップショット

ネットワーク & セキュリティ
セキュリティグループ

Elastic IP
プレースメントグループ
キーペア
ネットワークインターフェイス

ロードバランシング
ロードバランサー
ターゲットグループ

セキュリティグループの作成 アクション

グループ ID : sg-5977ab3f フィルターを追加

1 個中 1 ~ 1

Name	グループ ID	グループ名	VPC ID	説明
maintenance	sg-5977ab3f	maintenance	vpc-3f106a5b	Allow SSH inbound traffic

インバウンド・アウトバウンド切り替えたりして必要な情報を確認する

セキュリティグループ: sg-5977ab3f

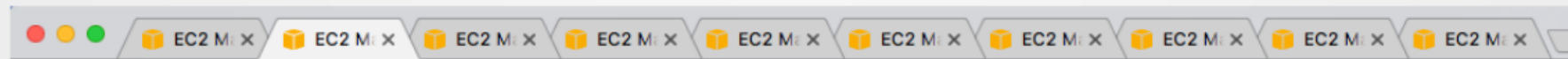
説明 インバウンド アウトバウンド タグ

編集

タイプ	プロトコル	ポート範囲	ソース
HTTP	TCP	80	0.0.0.0/0
SSH	TCP	22	10.20.0.0/16
すべての ICMP - IPv4	すべて	該当なし	10.20.0.0/16

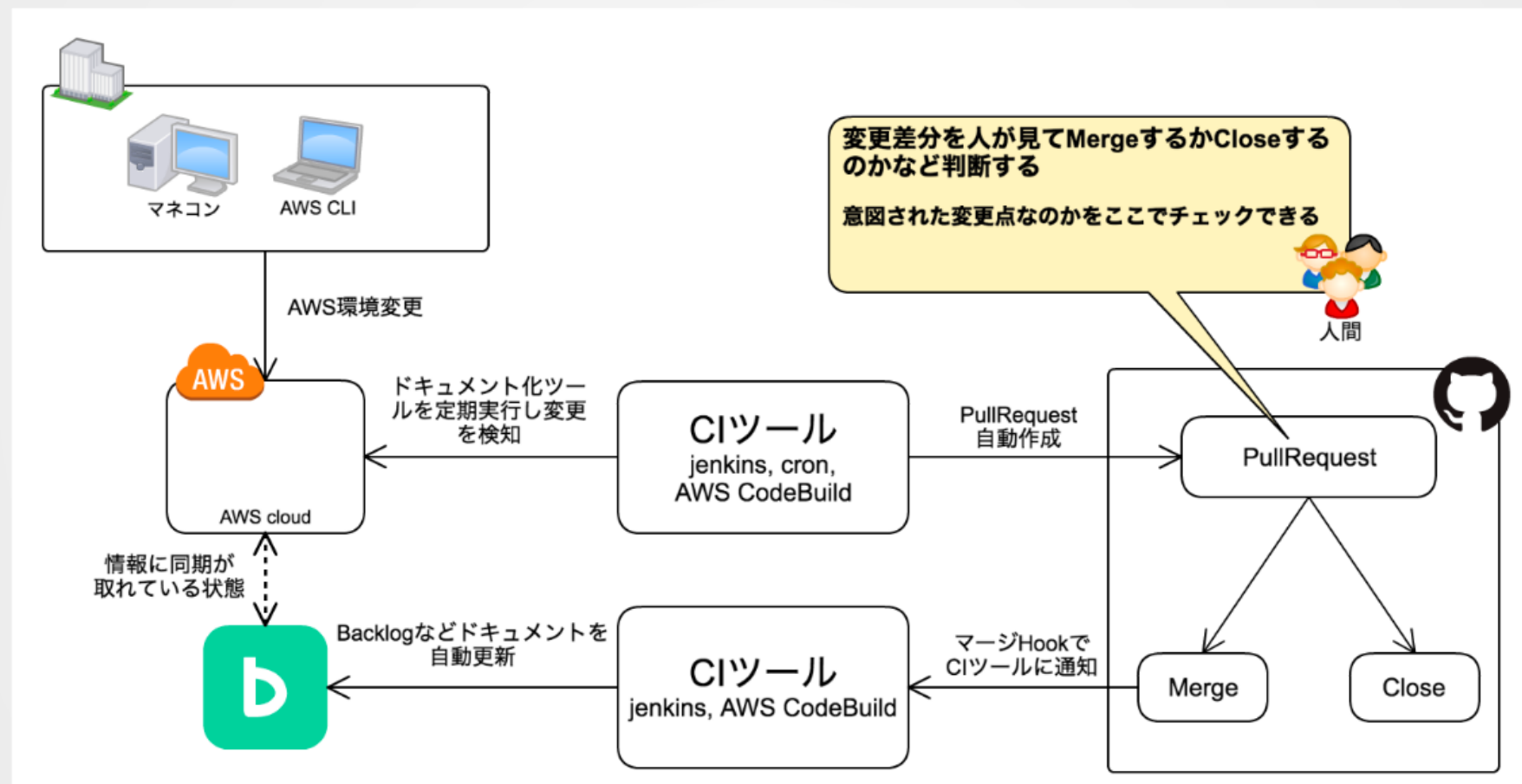
最終的にこうなってしまう... 🙇

増えていくタブ... 結局わからなくなってしまう



AWSドキュメント化ツールの 展望

こんなこともできるかも



今後やっていきたいこと

- SecurityGroupだけでなく色々なAWSサービスに対応
各種AWSの情報をそれなりにいい感じに一覧できる
- sgdocは捨てるかも、、新たなツールと名前でOSSとしてやって
いけたらと思う
- CloudAutomatorやポータルとかに組み込めたりもするかも

ありがとうございました。

一緒にやっていく人募集中