

Amazon Managed Service for Prometheus (AMP) ハンズオン

2021/10/31

シニアエバンジェリスト 亀田

Amazon Managed Service for Prometheus (AMP)はコンテナの高い可用性と安全性、およびコンテナに対するマネージドモニタリングを提供するサービスです。Prometheus との互換性を持ち Amazon SNS と連携したアラートを提供することも可能です。

Amazon Managed Service for Grafana (AMG) を先に起動しておき、最終的に AMP が取得したデータを可視化することがこのハンズオンのゴールです。

1. AMG の起動

<https://github.com/harunobukameda/Amazon-Managed-Service-for-Grafana>

をハンズオンシナリオを先に完了させてください。

その際、手順 17 番で Prometheus にチェックをつけておいてください。

2. Cloud9 の起動

AWS が提供する IDE である Cloud9 を起動するため、マネージメントコンソールで Cloud9 にアクセスし、[Create environment]をおします

3. 適当な名前を付け[Next Step]をおします

Name environment

Environment name and description

Name

The name needs to be unique per user. You can update it at any time in your environment settings.

Limit: 60 characters

Description - *Optional*

This will appear on your environment's card in your dashboard. You can update it at any time in your environment settings.

Write a short description for your environment

Limit: 200 characters

Cancel

Next step

4. [Instance Type]で[t3.small]を選びます。

Instance type


- ☐ t2.micro (1 GiB RAM + 1 vCPU)
Free-tier eligible. Ideal for educational users and exploration.
- ☒ t3.small (2 GiB RAM + 2 vCPU)
Recommended for small-sized web projects.
- ☐ m5.large (8 GiB RAM + 2 vCPU)
Recommended for production and general-purpose development.
- ☐ Other instance type
Select an instance type.

t3.nano


5. デフォルト VPC が使えない場合は、適当な VPC と Public Subnet を選びますが、デフォルト VPC が使える場合、そのまま[Next Step]をおします

▼ Network settings (advanced)

Network (VPC)
Launch your EC2 instance into an existing Amazon Virtual Private Cloud (VPC) or create a new one. To allow the AWS Cloud9 environment to connect to its EC2 instance, attach an internet gateway (IGW) to your new VPC.

vpc-5e977a3a (default)  [Create new VPC](#)

Subnet
Select a public subnet in which the EC2 instance is created. (For a private subnet, you must create an environment that connects to its instance via Systems Manager.)

No preference (default subnet in any Availability Zone)  [Create new subnet](#)

No tags associated with the resource.

[Add new tag](#)
You can add 50 more tags.

[Cancel](#) [Previous step](#) [Next step](#)

6. 次の確認画面では、そのまま[Create environment]をおします

7. しばらくするとターミナルにアクセスが可能になります。

8. Cloud9 用 IAM ロールの作成と設定。

IAM のマネージメントコンソールに行き、左ペインから[ロール]をクリックします

9. [ロールの作成]をおします

10. [EC2]を選び[次のステップ]をおします

ロールの作成

1 2 3 4

信頼されたエンティティの種類を選択

 AWS サービス EC2、Lambda、およびその他	 別の AWS アカウント お客様またはサードパーティに属しています	 ウェブ ID Cognito または任意の OpenID プロバイダ	 SAML 2.0 フェデレーション 企業ディレクトリ
--	---	--	--

AWS のサービスによるアクションの代行を許可します。 [詳細はこちら](#)

ユースケースの選択

一般的なユースケース

EC2

Allows EC2 instances to call AWS services on your behalf.

Lambda

Allows Lambda functions to call AWS services on your behalf.

11. [Administrator Access]を選び[次のステップ]をおします

ロールの作成

1 2 3 4

▼ Attach アクセス権限ポリシー

新しいロールにアタッチするポリシーを 1 つ以上選択します。

ポリシーの作成

36 件の結果を表示中

ポリシーのフィルタ

admin

ポリシー名	次として使用
<input checked="" type="checkbox"/> AdministratorAccess	Permissions policy (14)

12. タグはそのまま[次のステップ]をおします

13. 名前に[ecsworkshop-admin]を付け[ロールの作成]をおします。(名前はメモっておいてください)

ロールの作成

1 2 3 4

確認

以下に必要な情報を指定してこのロールを見直してから、作成してください。

ロール名*

英数字と「+,-,@,_,」を使用します。最大 64 文字。

ロールの説明

Allows EC2 instances to call AWS services on your behalf.

最大 1000 文字。英数字と「+,-,@,_,」を使用します。

信頼されたエンティティ AWS のサービス: ec2.amazonaws.com

ポリシー AdministratorAccess

アクセス権限の境界 アクセス権限の境界が設定されていません

追加されたタグはありません。

* 必須

キャンセル

戻る

ロールの作成

14. EC2 のマネージメントコンソールから Cloud9 用インスタンスを特定します。(先ほど Cloud9 につけた名前がついています)

インスタンスの作成

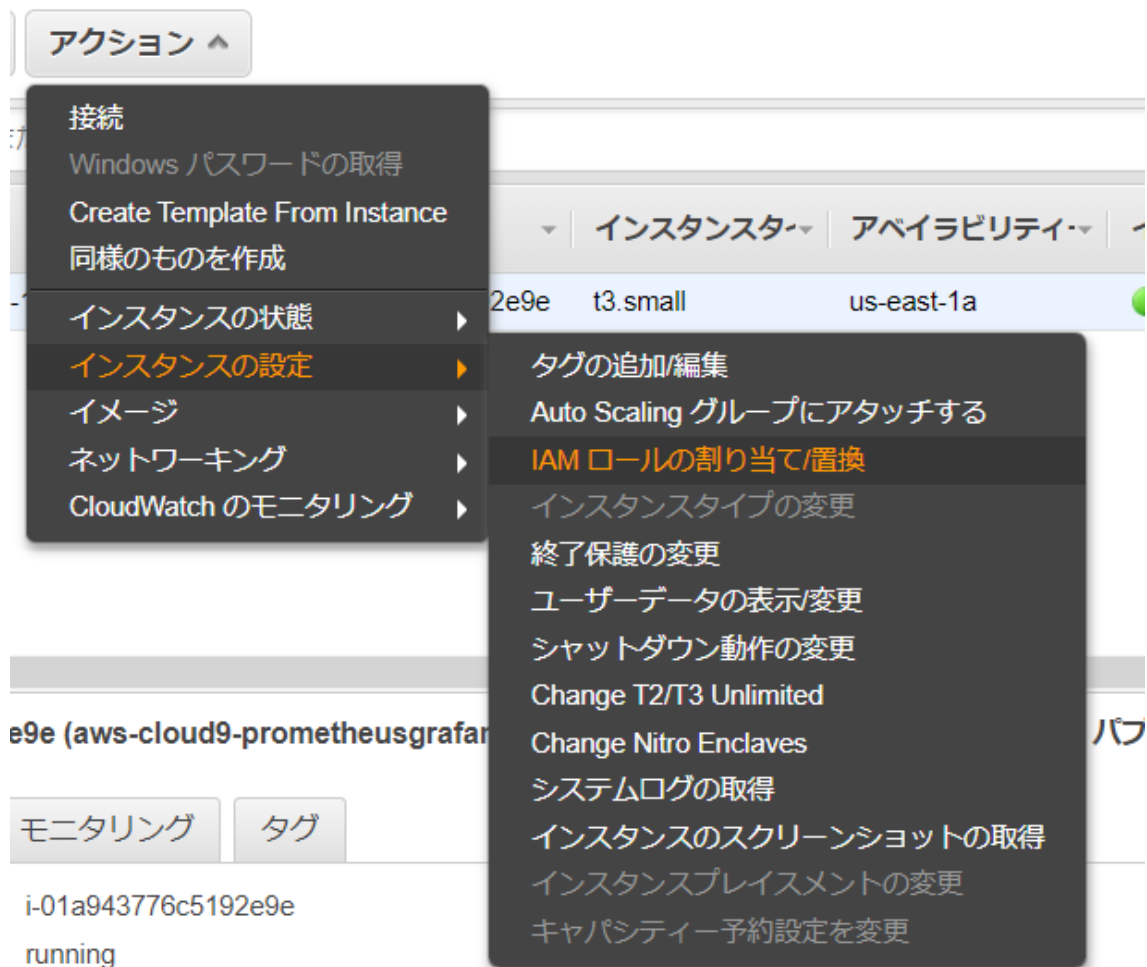
接続

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

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	インスタンスのステータス	ステータスチェック
aws-cloud9-prometheus-grafana-1c502cb63f084...	i-01a943776c5192e9e	t3.small	us-east-1a	running	2/2 のチェ...

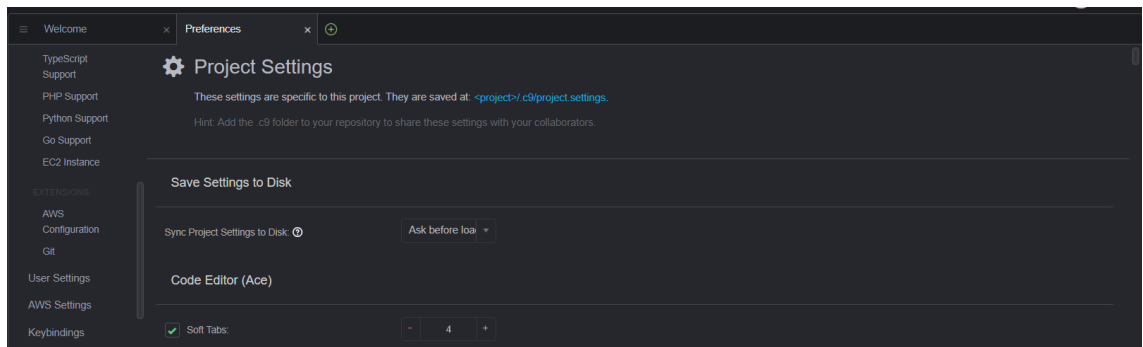
15. [アクション]→[インスタンスの設定]→[IAM ロールの割り当て/置換]を選びます



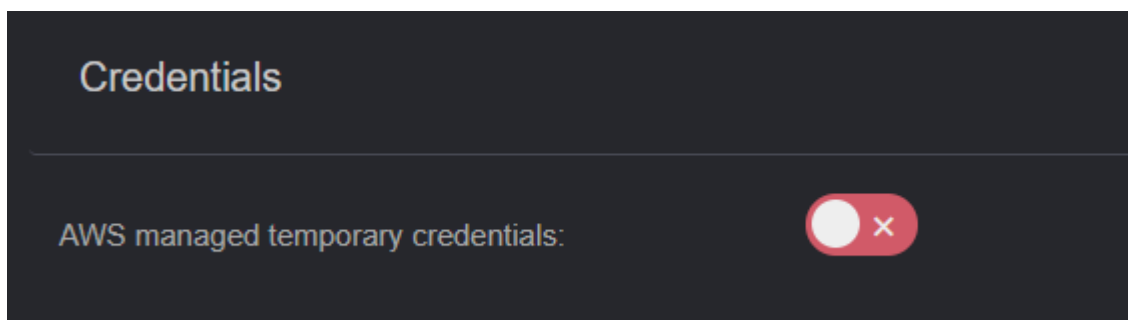
16. 先程作成した IAM ロールを選び[適用]をおします



17. Cloud9 の画面に戻り、右上歯車マークをクリックし、画面左の[AWS Settings]を選びます



18. Credential をオフにします（緑から赤に変更）



19. 以下を実行し、仮の AWS クレデンシャルを削除します
- ```
rm -vf ${HOME}/.aws/credentials
```
20. 以下を実行し jq をインストールします。jq は json を取り扱う用のコマンドが利用可能となるツールです
- ```
sudo yum install -y jq
```
21. コピペ用コマンド 1 番を実行します。作業リージョンを明示的に aws cli にセットします
22. コピペ用コマンド 2 番を実行し、リージョンが正しくセットされていることを確認します

```
ec2-user:~/environment $ test -n "$AWS_REGION" && echo AWS_REGION is "$AWS_REGION" || echo AWS_REGION is not set
AWS_REGION is us-east-1
```

作業しているリージョンは Grafana, Prometheus がサポートされていればどこでも大丈夫です（東京やバージニア北部等）

23. コマンド 3 番を実行し。Bash プロファイルにもリージョンと AWS アカウント ID をセットしておきます
24. コマンド 4 番を実行し、IAM ロールが正しくセットされているかを確認します。[IAM role VALID]を表示されたら作業続行してください。Not VALID の場合、どこかが失敗していますので、作成した IAM ロールの名前、Cloud9 用 EC2 インスタンスに付与された IAM ロールの名前を確認してください。
25. コマンド 5 番を実行して Cloud9 のストレージ容量を増やします（一時的に再起動しま

す)

[検証環境の構築]

これから可視化を行うための検証環境（ECS）を起動していきます。起動には AWS CDK を利用します。

26. コマンド 6 番を実行し、git からサンプルレポジトリを clone し、Python の仮想マシンを作成。AWS CDK の実行に必要な環境の設定、ブートストラップ（初期設定作業）を行います。（CDK により CloudFormation スタックが実行されます。）

```
✓ Environment aws://294963776963/us-east-1 bootstrapped.
*****
*** Newer version of CDK is available [1.130.0] ***
*** Upgrade recommended (npm install -g aws-cdk) ***
*****
```

[AMP ワークスペースの作成]

ワークスペースとは、Prometheus のメトリクスを保存したり照会したりするための論理的な空間です。ワークスペースは、更新、リスト、記述、削除などの管理や、メトリクスの取り込みと照会を許可するためのきめ細かなアクセス・コントロールをサポートしています。ワークスペースは、自分のアカウントの各リージョンに 1 つ以上のワークスペースを持つことができます。

27. コマンド 7 番を実行し、AMP のワークスペースを作成します

```
{
  "status": {
    "statusCode": "CREATING"
  },
  "workspaceId": "ws-814d7d7a-7d5f-4af4-a781-ab0983317316",
  "arn": "arn:aws:aps:us-east-1:294963776963:workspace/ws-814d7d7a-7d5f-4af4-a781-ab0983317316"
}
```

28. [CREATING]と表示されていますので、マネージメントコンソールで AMP にアクセスして、作成が完了していることを確認してから次の作業に進みます。

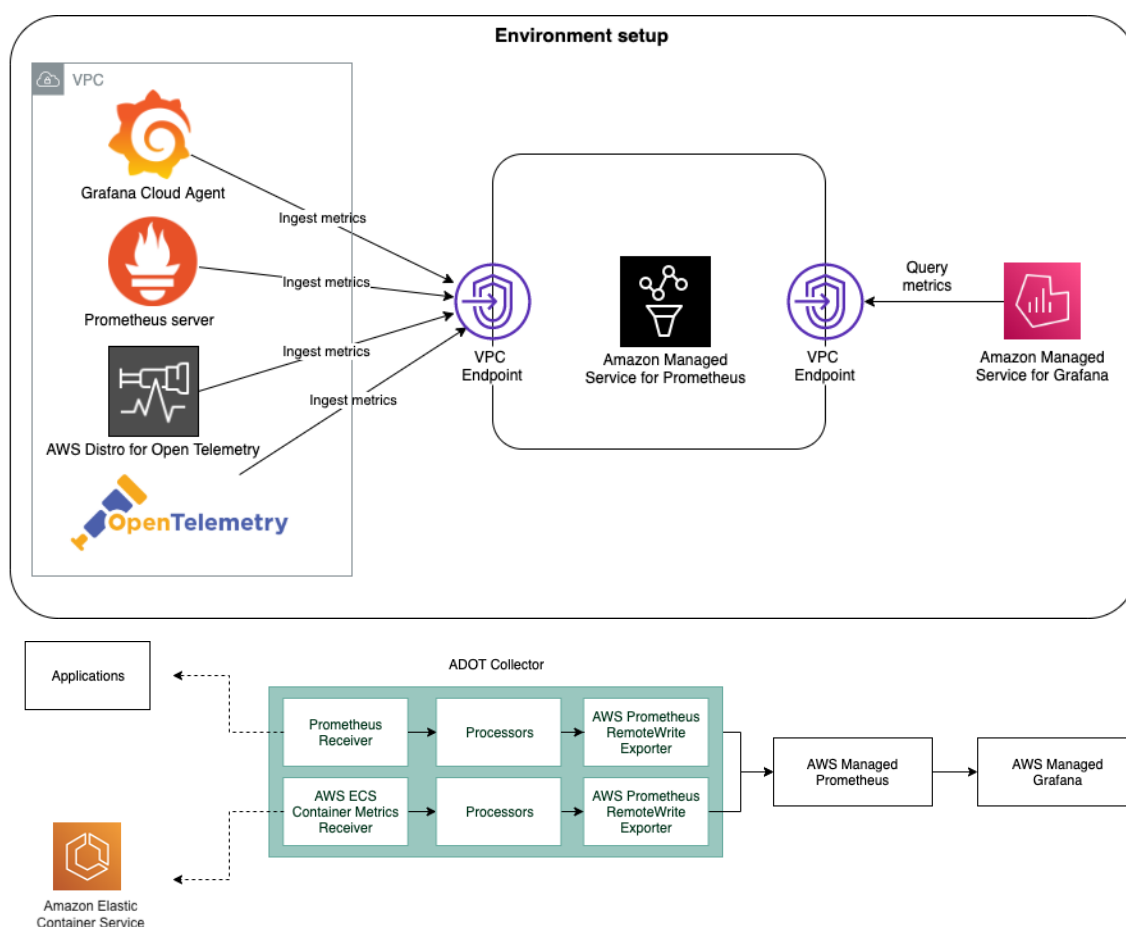
Amazon Prometheus > WorkSpaces

WorkSpaces (1) 情報 リフレッシュ 編集 削除 ワークスペースを作成する

Workspace エイリアス	Workspace ID	作成日	ステータス
ecs-workshop	ws-814d7d7a-7d5f-4af4-a781-ab0983317316	2021-10-31T12:21:06.101Z	Active

[スクレイピング処理と Receiver]

収集されたデータはスクレイピング（フォーマット整形）されたのち、ワークスペースに投入されクエリ言語（PromQL）での処理が可能となります。このため、データをワークスペースに投入する前にスクレイピングを行うモジュールの起動が必要です。このハンズオンでは、アプリケーションからのスクレイピングに Prometheus Receiver を使用し、インフラストラクチャ・メトリクス（AWS ECS Container Metrics）のスクレイピングに AWS ECS Container Metrics Receiver を使用します。Receiver を構成し、AWS Prometheus Remote Write Exporter を使用して、各環境で動作している Exporter からメトリクスがエクスポートされ、Receiver を介してワークスペースにインジェスト（挿入）されます。

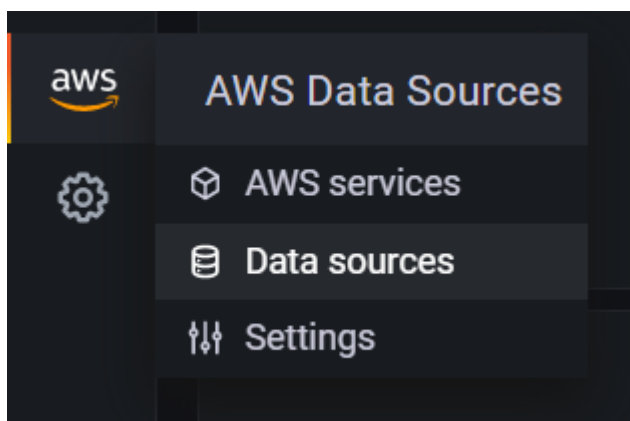


29. コマンド 8 番を実行して、Exporter と連携先ワークスペースの設定などをおこないます
30. コマンド 9 番を実行し、環境構築用 Cfn テンプレートを作成します
31. コマンド 10 番を実行し、デプロイを行います。デプロイには時間がかかりますので、終了するまで待ちます。その間に AMG に管理者権限でログインしておいてください。コマンドプロンプトが操作可能になったら構築が完了しています。

[AMG でデータの可視化]

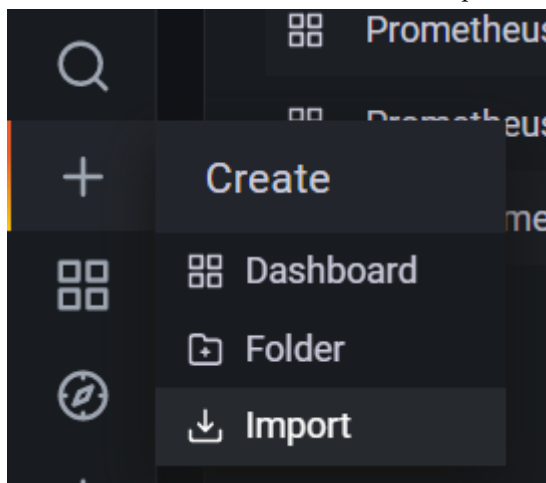
今までの手順で、ECS→AMP のデータ連携が完了しており、可視化の準備が整っていますので、次に AMP→AMG のフローを作成しダッシュボードを作成します。

32. AMG の画面左ペインの [Data sources] を選びます



33. [Service] から Prometheus を選び、作業中のリージョンを指定すると、自動で AMP のワークスペース ID が出てきますので、チェックをつけて [Add 1 data source] をおします

34. 再度左ペインから [+] をおして、[Import] を選びます



35. [Upload JSON file] を選らんで、[AMP_ECS_Task_Monitoring.json] をアップロードします。その後ドロップダウンで Prometheus のワークスペース ID を指定して [Import] をおします

Options

Name

ECS Task Monitoring

Folder

General

Unique identifier (UID)
The unique identifier (UID) of a dashboard can be used to uniquely identify a dashboard between multiple Grafana installs. The UID allows having consistent URLs for accessing dashboards so changing the title of a dashboard will not break any bookmarked links to that dashboard.

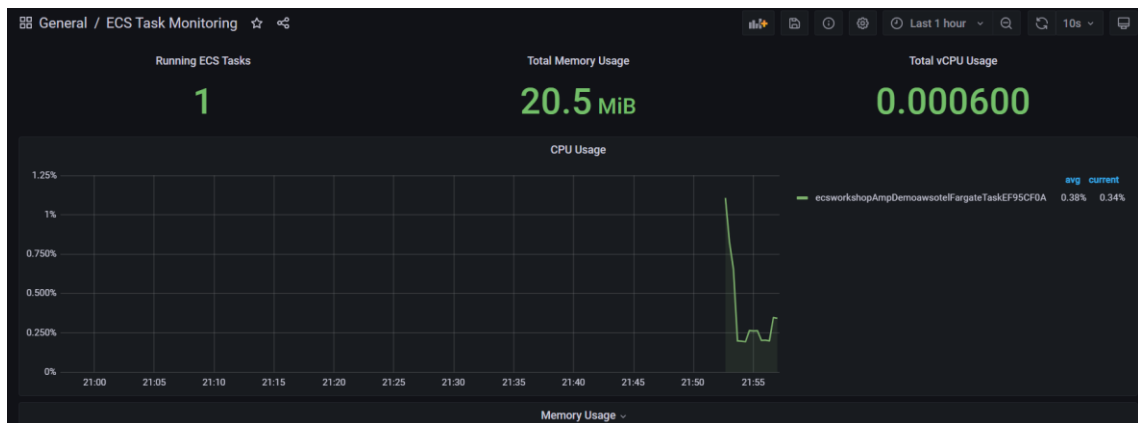
DnWHgZ3Gk Change uid

Prometheus ws-647c2794-32a4-4ded-95e1-59bc7ecd633c

Prometheus ws-814d7d7a-7d5f-4af4-a781

Import Cancel

36. 以下のように可視化されたダッシュボードが表示されます



おつかれさまでした！

削除は以下をお願いします

- ・ `cdk destroy -f` （CDK すでに別システムで使っている方は、明示的に名前を指定してください）（`[cdk list]`で一覧を確認できます）
- ・ CDK 用 S3 バケット
- ・ `aws amp delete-workspace --workspace-id $AMP_WORKSPACE_ID`
- ・ AMG ハンズオンの削除手順
 - # 先に SSO を消すと Grafana が消せなくなるので注意してください。
- ・ CloudWatch ロググループ

