sysdig

AWSアカウントに Fargate Scanningを デプロイする

本文の内容は、Deploying Fargate Scanning in your AWS account(https://sysdiglabs.github.io/ecs-image-scanning/install.html）を元に日本語に翻訳・再構成した内容となっております。

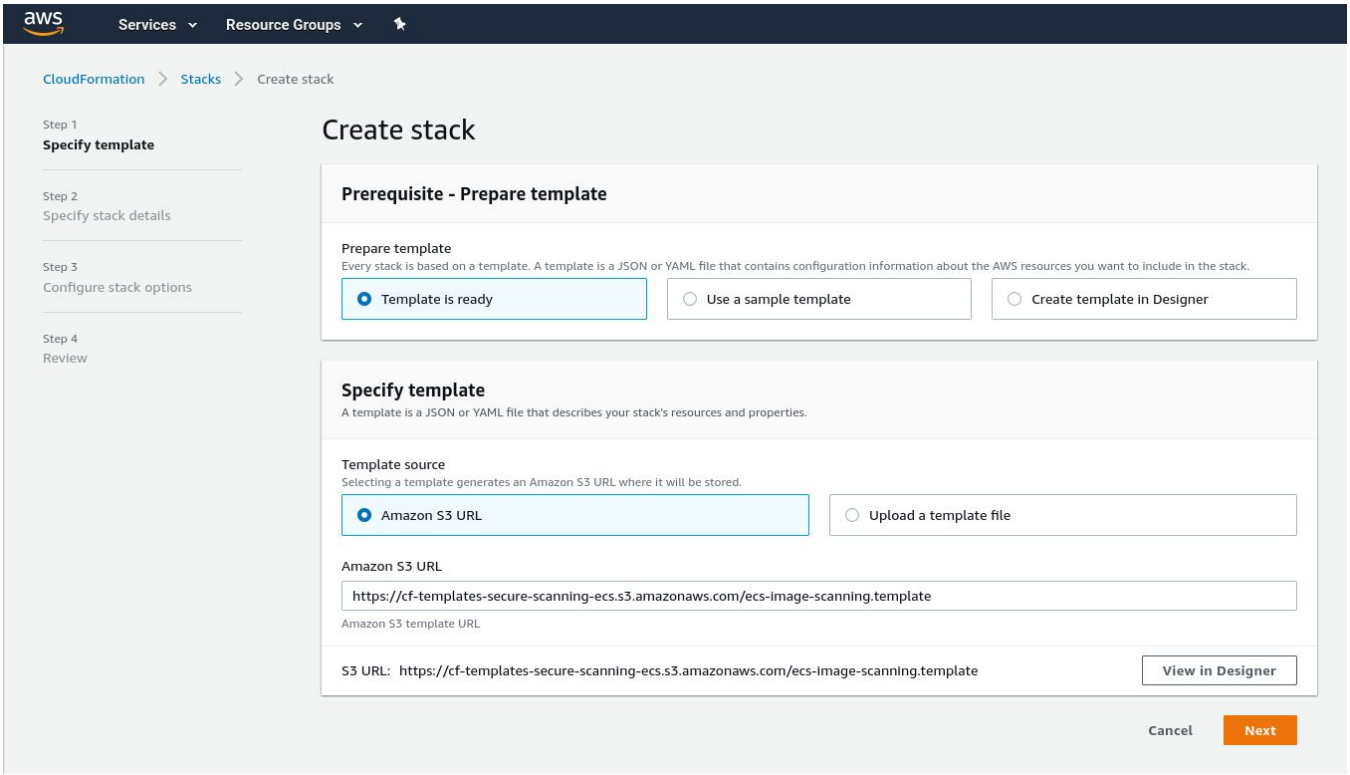
はじめに

このガイドでは、Sysdig SecureのFargate Scanning機能をAWSアカウントにデプロイする方法を説明します。これはCloudFormationテンプレートを使用してパッケージ化されているため、この機能をデプロイするにはわずか4回のクリックで済みます。

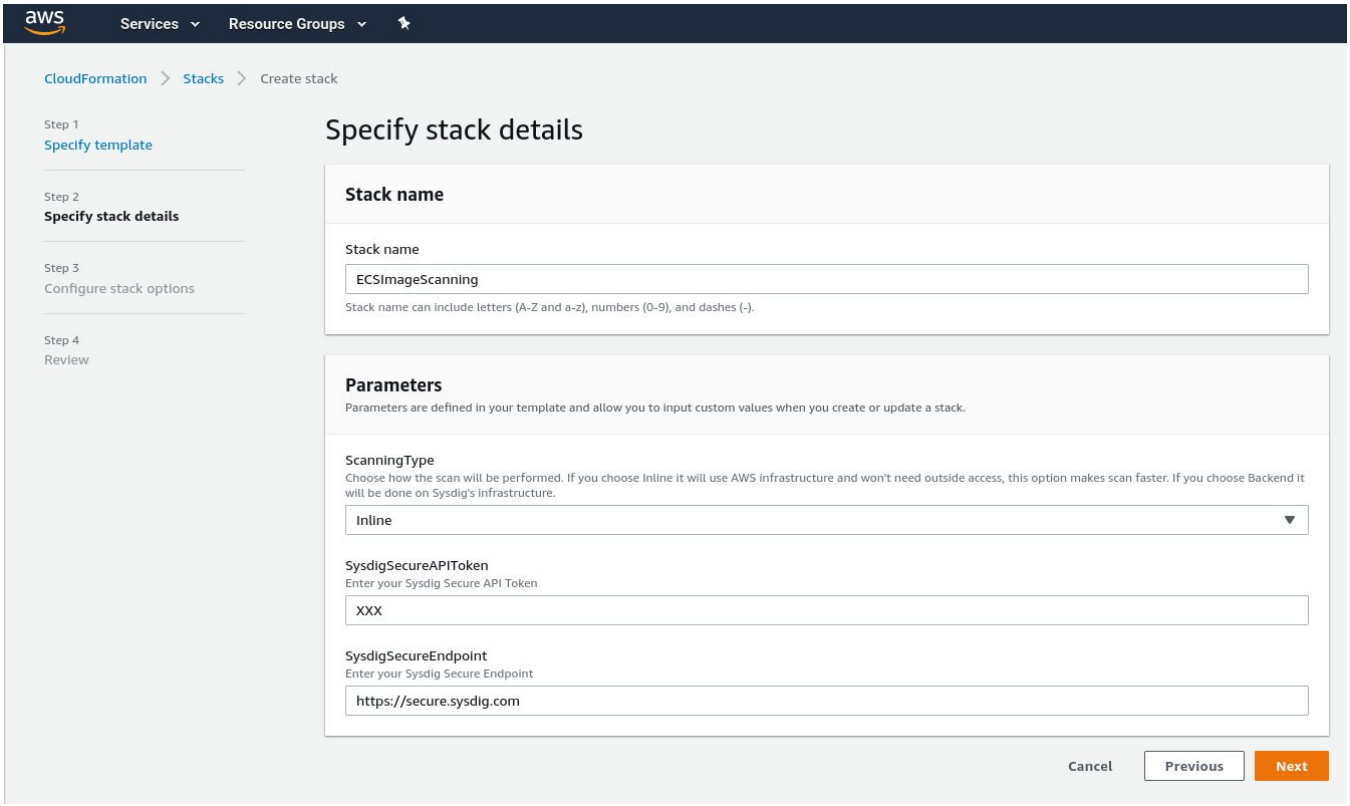
CloudFormationテンプレートの取得

このリンクを使用してデプロイすることができます。

ECSコンテナがスポーンされるのと同じアベイラビリティゾーンにデプロイするようにしてください。他のアベイラビリティゾーンにデプロイされているECSクラスタからイベントを受信することはできません。

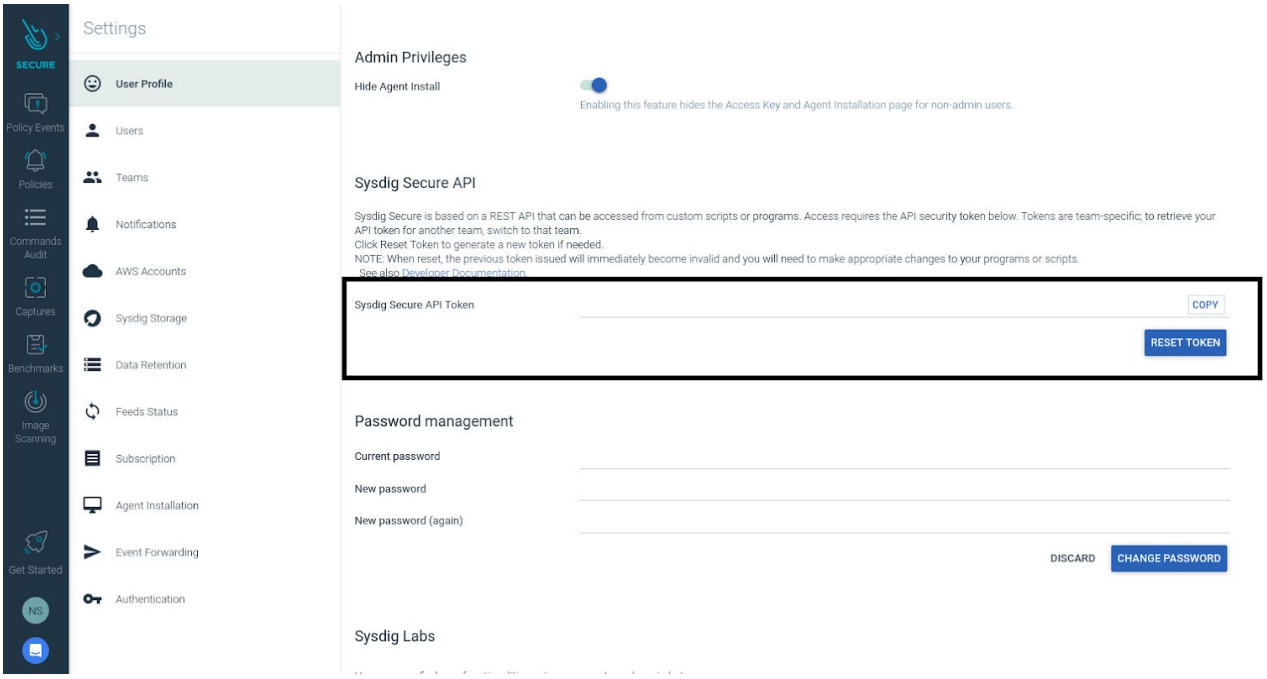


スキャンタイプの設定



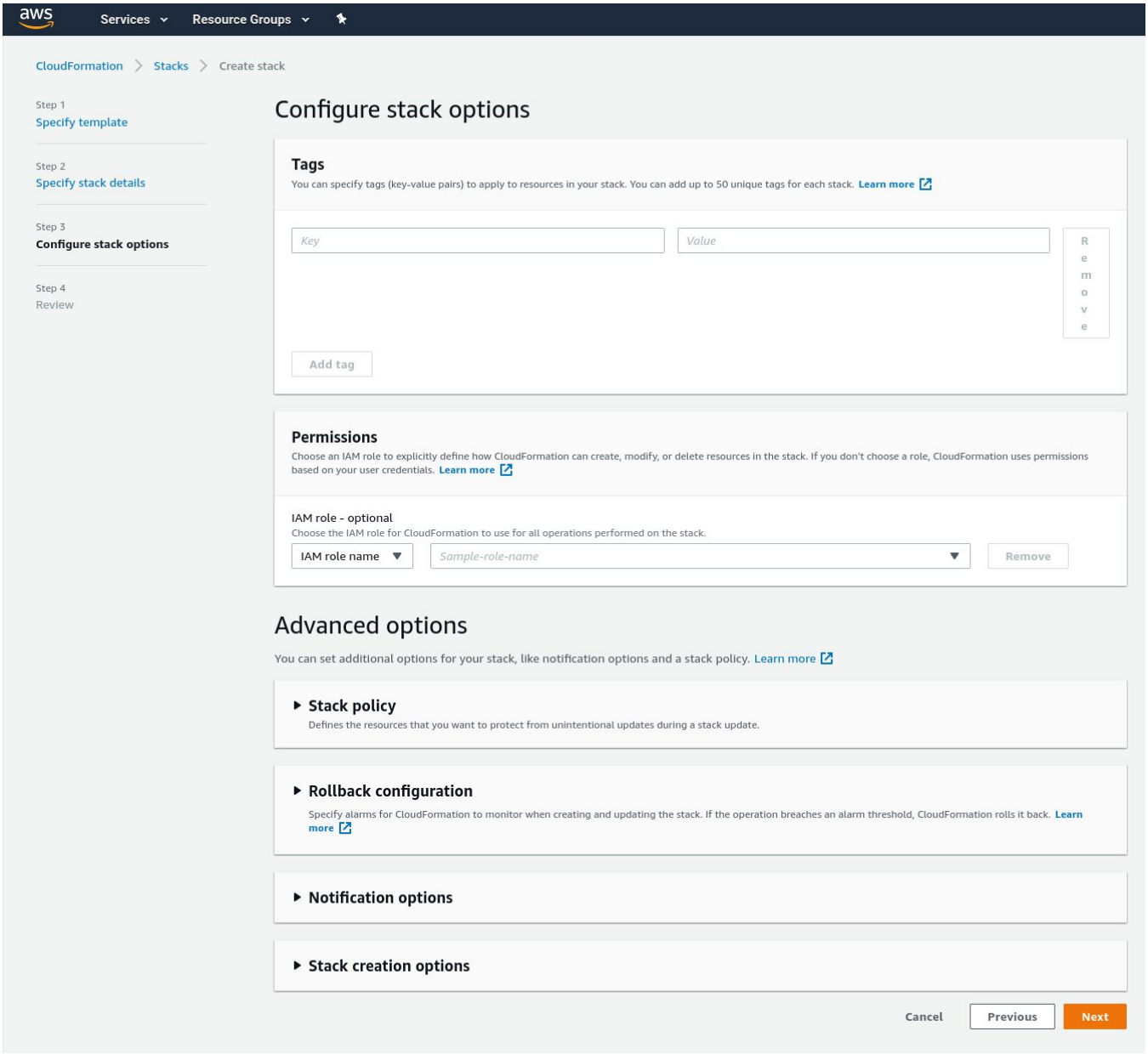
設定するパラメータは3つあります。

- ScanningType：インラインスキャンはAWSインフラストラクチャ上でイメージをスキャンします。バックエンドはSysdigのインフラストラクチャ上で行います。
- SysdigSecureAPIToken.：Secure API Tokenが必要です。



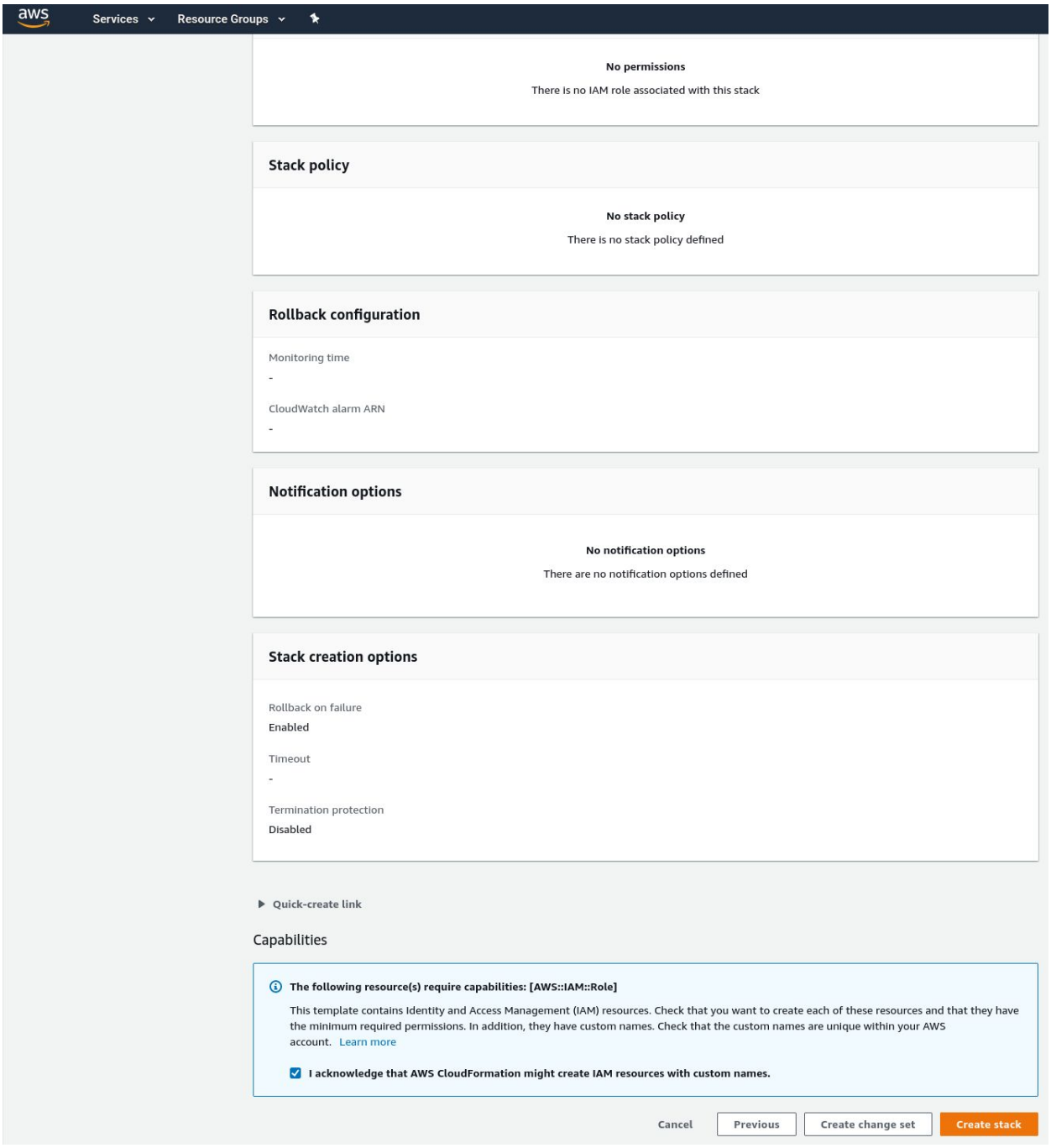
SysdigSecureEndpoint： オンプレミスデプロイメントを使用している場合は、Secure が配備されているアドレスを指すようにこの url を調整してください。

追加のタグとパーミッションの追加



このステップでは、必要に応じていくつかの余分なタグやパーミッションを追加することができます。

レビュー


aws
Services
Resource Groups
No permissions
There is no IAM role associated with this stack
Stack policy
No stack policy
There is no stack policy defined
Rollback configuration
Monitoring time
-
CloudWatch alarm ARN
-
Notification options
No notification options
There are no notification options defined
Stack creation options
Rollback on failure
Enabled
Timeout
-
Termination protection
Disabled
Quick-create link
Capabilities
The following resource(s) require capabilities: [AWS::IAM::Role]
This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have the minimum required permissions. In addition, they have custom names. Check that the custom names are unique within your AWS account. Learn more
I acknowledge that AWS CloudFormation might create IAM resources with custom names.
Cancel
Previous
Create change set
Create stack

最後のステップでは、以前に紹介したすべてのパラメータを確認することができ、最小特権の原則を尊重しながらスキャンを実行するための専用のIAMロールを作成する限り、チェックボックスを承認する必要があります。

その後、次へをクリックして、スタックが正常にデプロイされていることを確認してください。