



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	3
CloudFormationテンプレートの取得	3
スキャンタイプの設定	4
追加のタグとパーミッションの追加	6
レビュー	7

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。

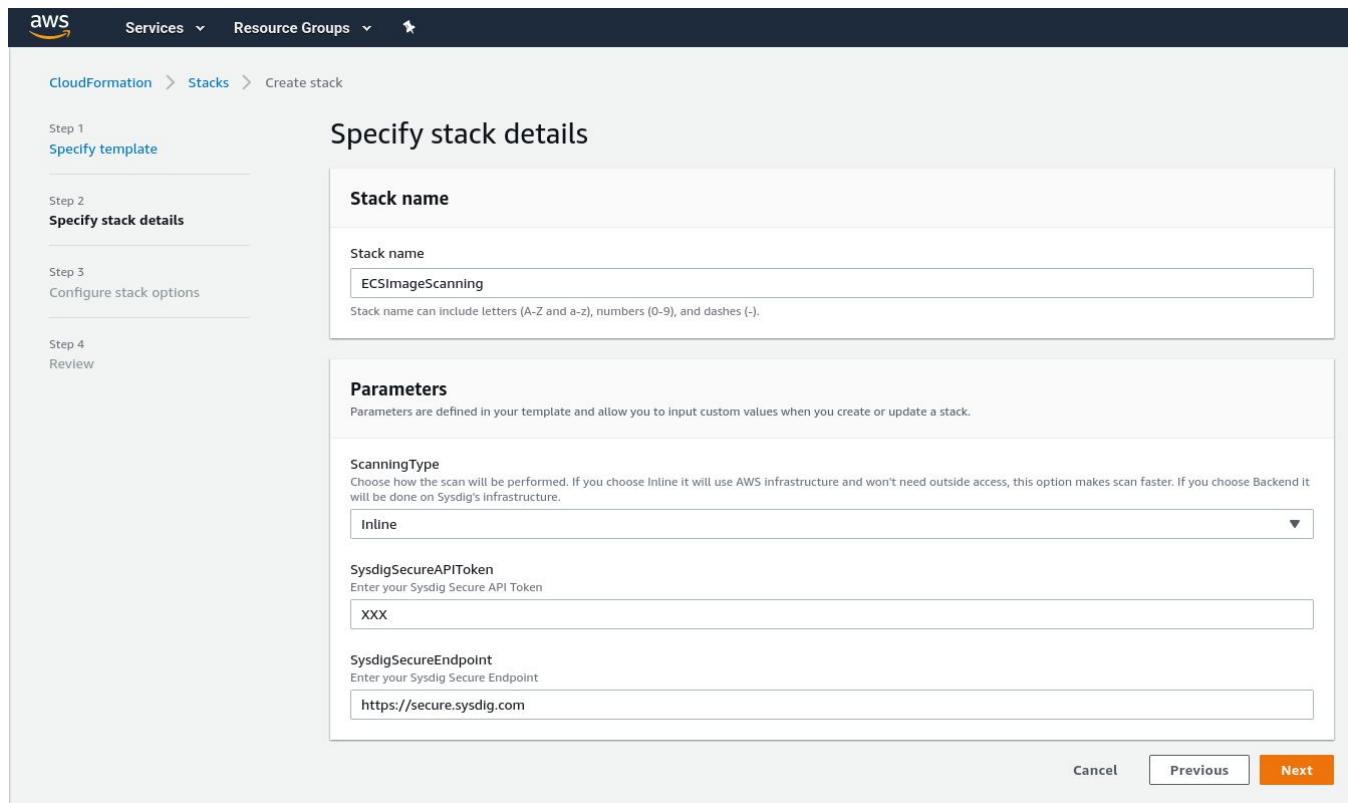
CloudFormationテンプレートの取得

[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。

The screenshot shows the AWS CloudFormation 'Create stack' wizard. The top navigation bar includes 'Services' and 'Resource Groups'. The main title is 'Create stack' under 'Step 1 Specify template'. A sidebar on the left lists steps: Step 1 'Specify template' (selected), Step 2 'Specify stack details', Step 3 'Configure stack options', and Step 4 'Review'. The main content area is titled 'Prerequisite - Prepare template' and contains a 'Prepare template' section with the note: 'Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.' It features three radio button options: 'Template is ready' (selected), 'Use a sample template', and 'Create template in Designer'. Below this is the 'Specify template' section, which says: 'A template is a JSON or YAML file that describes your stack's resources and properties.' It includes a 'Template source' section with the note: 'Selecting a template generates an Amazon S3 URL where it will be stored.' It shows 'Amazon S3 URL' selected and a URL input field containing 'https://cf-templates-secure-scanning-ecs.s3.amazonaws.com/ecs-image-scanning.template'. There is also an 'Upload a template file' option and a 'View in Designer' link. At the bottom right are 'Cancel' and 'Next' buttons.

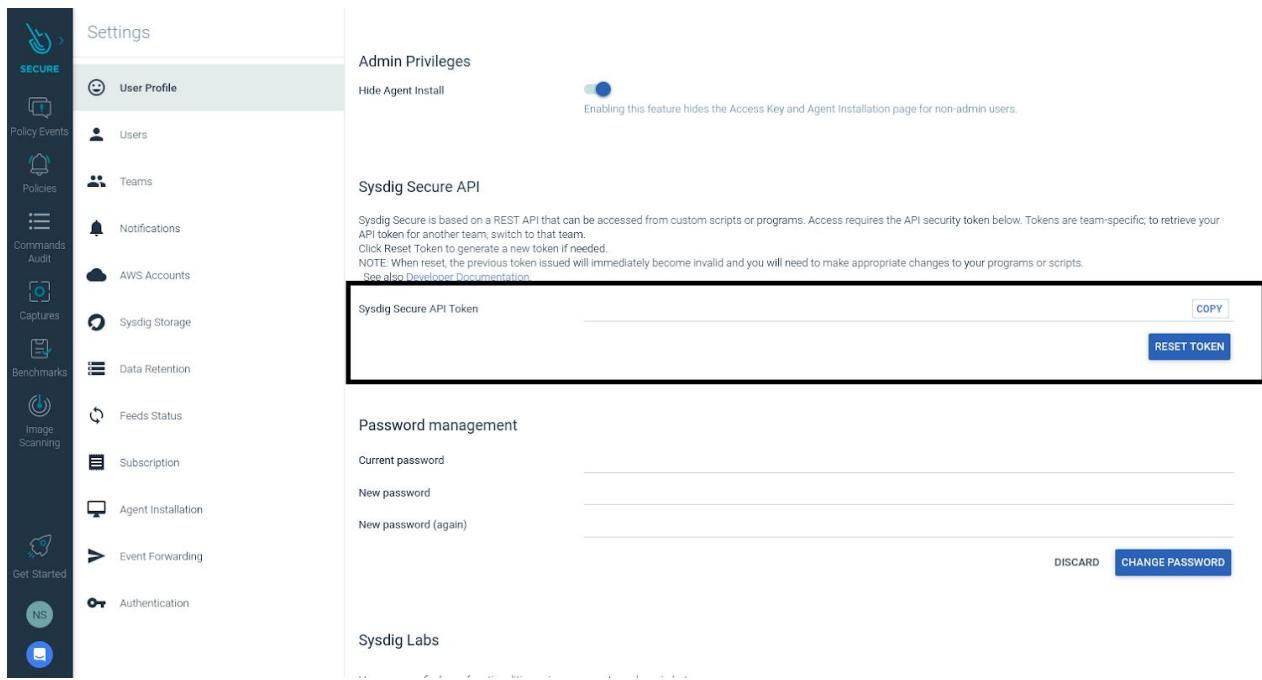
スキャンタイプの設定



The screenshot shows the 'Specify stack details' step of the AWS CloudFormation 'Create stack' wizard. The left sidebar lists steps: Step 1 (Specify template), Step 2 (Specify stack details, currently selected), Step 3 (Configure stack options), and Step 4 (Review). The main area is titled 'Specify stack details' and contains two sections: 'Stack name' and 'Parameters'. In the 'Stack name' section, the name 'ECSImageScanning' is entered into the input field, with a note below stating 'Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-)'. In the 'Parameters' section, there are three fields: 'ScanningType' (set to 'Inline'), 'SysdigSecureAPIToken' (containing placeholder text 'Enter your Sysdig Secure API Token' and the value 'XXX'), and 'SysdigSecureEndpoint' (containing placeholder text 'Enter your Sysdig Secure Endpoint' and the value 'https://secure.sysdig.com'). At the bottom right are 'Cancel', 'Previous', and 'Next' buttons, with 'Next' being highlighted.

設定するパラメータは3つあります。

- ScanningType : インライൻ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。



The screenshot shows the 'Settings' page in the Sysdig Secure interface. On the left, there's a sidebar with various icons and labels: SECURE (highlighted), Policy Events, Policies, Commands Audit, Captures, Benchmarks, Image Scanning, Get Started, NS, and a blue square icon. The main content area has a header 'Settings' and a sub-header 'Admin Privileges'. It includes a toggle switch for 'Hide Agent Install' which is set to 'On'. Below this is a section for 'Sysdig Secure API' with a note about its REST API nature and team-specific tokens. It features a text input field for the 'Sysdig Secure API Token' with a 'COPY' button and a 'RESET TOKEN' button. Underneath is a 'Password management' section with fields for 'Current password', 'New password', and 'New password (again)'. Buttons for 'DISCARD' and 'CHANGE PASSWORD' are at the bottom. At the very bottom, there's a 'Sysdig Labs' section with some small text and icons.

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

The screenshot shows the AWS CloudFormation 'Create stack' interface. The top navigation bar includes the AWS logo, Services dropdown, Resource Groups dropdown, and a star icon. The breadcrumb path is 'CloudFormation > Stacks > Create stack'. On the left, a vertical sidebar lists steps: Step 1 'Specify template', Step 2 'Specify stack details', Step 3 'Configure stack options' (which is selected and highlighted in blue), and Step 4 'Review'. The main content area is titled 'Configure stack options'. It contains two sections: 'Tags' and 'Permissions'. The 'Tags' section allows adding key-value pairs, with a table for 'Key' and 'Value' and a 'Add tag' button. To the right of the table is a vertical 'Remove' button. The 'Permissions' section allows choosing an IAM role, with a dropdown menu set to 'Sample-role-name' and a 'Remove' button. Below these sections is the 'Advanced options' section, which includes 'Stack policy', 'Rollback configuration', 'Notification options', and 'Stack creation options'. At the bottom right are 'Cancel', 'Previous', and 'Next' buttons.

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

The screenshot shows the AWS CloudFormation console interface for creating a new stack. The top navigation bar includes the AWS logo, Services dropdown, Resource Groups dropdown, and a star icon.

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。