




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コンテナがスポンサー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 console interface for creating a stack. The breadcrumb navigation is 'CloudFormation > Stacks > Create stack'. The left sidebar shows a progress indicator with four steps: Step 1 (Specify template), Step 2 (Specify stack details), Step 3 (Configure stack options), and Step 4 (Review). The main content area is titled 'Create stack' and contains two sections: 'Prerequisite - Prepare template' and 'Specify template'. In the 'Prerequisite' section, the 'Template is ready' radio button is selected. In the 'Specify template' section, the 'Amazon S3 URL' radio button is selected, and the 'Amazon S3 URL' field contains the text 'https://cf-templates-secure-scanning-ecs.s3.amazonaws.com/ecs-image-scanning.template'. Below this field, the 'S3 URL' is displayed as 'https://cf-templates-secure-scanning-ecs.s3.amazonaws.com/ecs-image-scanning.template'. At the bottom right, there are 'Cancel' and 'Next' buttons.

スキャンタイプの設定

The screenshot shows the AWS CloudFormation console interface for creating a stack. The breadcrumb navigation is 'CloudFormation > Stacks > Create stack'. The left sidebar shows four steps: Step 1 'Specify template', Step 2 'Specify stack details' (which is the active step), Step 3 'Configure stack options', and Step 4 'Review'. The main content area is titled 'Specify stack details' and contains two sections: 'Stack name' and 'Parameters'. In the 'Stack name' section, the text 'Stack name' is followed by a text input field containing 'ECSImageScanning'. Below the input field, a note states: 'Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-)'. The 'Parameters' section is titled 'Parameters' and includes a sub-section 'ScanningType' with a description: 'Choose how the scan will be performed. If you choose Inline it will use AWS infrastructure and won't need outside access, this option makes scan faster. If you choose Backend it will be done on Sysdig's infrastructure.' Below this is a dropdown menu with 'Inline' selected. The next parameter is 'SysdigSecureAPIToken' with the instruction 'Enter your Sysdig Secure API Token' and an input field containing 'XXX'. The final parameter is 'SysdigSecureEndpoint' with the instruction 'Enter your Sysdig Secure Endpoint' and an input field containing 'https://secure.sysdig.com'. At the bottom right of the form, there are three buttons: 'Cancel', 'Previous', and 'Next'.

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。

Settings

Admin Privileges

Hide Agent Install Enabling this feature hides the Access Key and Agent Installation page for non-admin users.

Sysdig Secure API

Sysdig Secure is based on a REST API that can be accessed from custom scripts or programs. Access requires the API security token below. Tokens are team-specific, to retrieve your API token for another team, switch to that team. Click Reset Token to generate a new token if needed.
NOTE: When reset, the previous token issued will immediately become invalid and you will need to make appropriate changes to your programs or scripts.
[See also Developer Documentation](#)

Sysdig Secure API Token COPY RESET TOKEN

Password management

Current password

New password

New password (again)

DISCARD CHANGE PASSWORD

Sysdig Labs

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 console interface for the 'Configure stack options' step. The breadcrumb trail is 'CloudFormation > Stacks > Create stack'. The left sidebar shows four steps: 'Step 1 Specify template', 'Step 2 Specify stack details', 'Step 3 Configure stack options' (which is the active step), and 'Step 4 Review'. The main content area is titled 'Configure stack options' and contains three sections: 'Tags', 'Permissions', and 'Advanced options'. The 'Tags' section has a table with columns for 'Key' and 'Value', and a 'Remove' button. The 'Permissions' section has a dropdown for 'IAM role name' and a 'Remove' button. The 'Advanced options' section has four expandable sections: 'Stack policy', 'Rollback configuration', 'Notification options', and 'Stack creation options'. At the bottom right, there are 'Cancel', 'Previous', and 'Next' buttons.

aws Services Resource Groups

CloudFormation > Stacks > Create stack

Step 1
Specify template

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review

Configure stack options

Tags

You can specify tags (key-value pairs) to apply to resources in your stack. You can add up to 50 unique tags for each stack. [Learn more](#)

Key	Value	Remove
		R e m o v e

Add tag

Permissions

Choose an IAM role to explicitly define how CloudFormation can create, modify, or delete resources in the stack. If you don't choose a role, CloudFormation uses permissions based on your user credentials. [Learn more](#)

IAM role - optional
Choose the IAM role for CloudFormation to use for all operations performed on the stack.

IAM role name Remove

Advanced options

You can set additional options for your stack, like notification options and a stack policy. [Learn more](#)

- Stack policy**
Defines the resources that you want to protect from unintentional updates during a stack update.
- Rollback configuration**
Specify alarms for CloudFormation to monitor when creating and updating the stack. If the operation breaches an alarm threshold, CloudFormation rolls it back. [Learn more](#)
- Notification options**
- Stack creation options**

Cancel Previous Next

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。