amazon web services | Partner Network

AUTHORIZED GOVERNMENT PARTNER
ADVANCED CONSULTING PARTNER
CHANNEL PARTNER

stackArmor

Guide to Creating an IAM Role with CloudFormation for stackArmor Threat Scanner

Please contact:
stackArmor
1775 Tysons Blvd, 6th floor
Tysons VA 22102
solutions@stackarmor.com
www.stackArmor.com

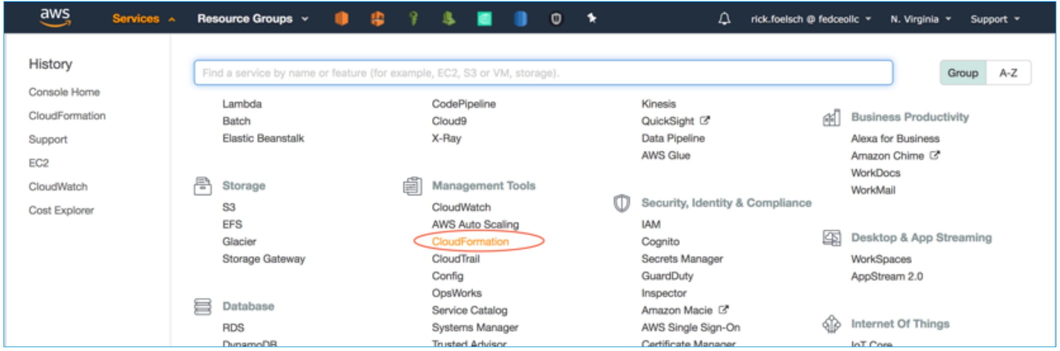
The information in this document is the property of stackArmor (FedCEO LLC) and may not be copied or redistributed without written permission. This document contains data that shall not be disclosed by the Customer and shall not be duplicated, used, or disclosed—in whole or in part—for any reason other than to evaluate this document. This restriction does not limit the Customer's right to use the information contained in this document if it is obtained from another source without restriction. This restriction is in force for all data contained on all pages of this document.

Purpose

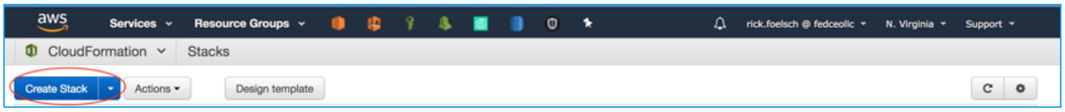
This document is a guide to creating an IAM role using AWS CloudFormation to allow access to stackArmor's Threat Scanner.

Steps

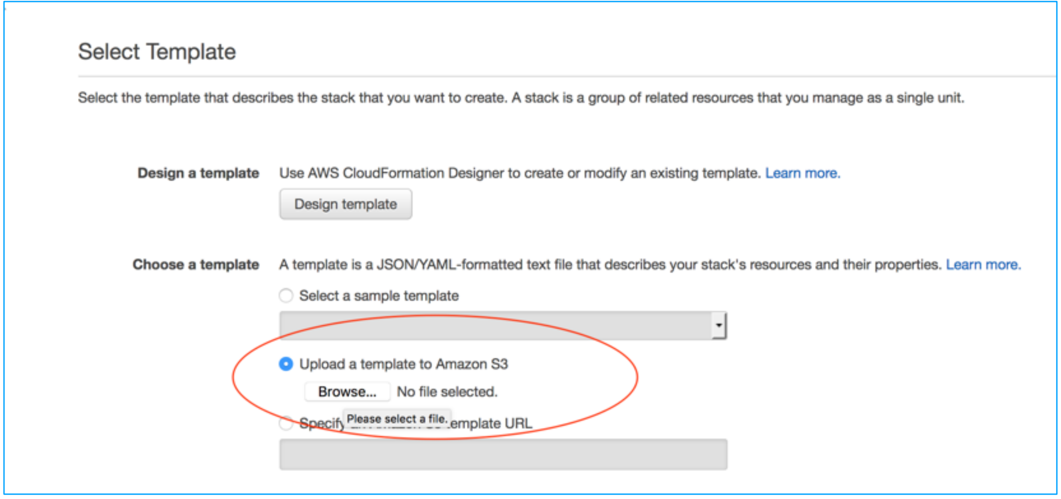
1. Login to your AWS account and go to the CloudFormation service.



2. Click the "Create Stack" button



3. Select the "Upload a template to Amazon S3" radio button, click the browse button and choose the provided stackArmor-TA-IAMRole.json file.



Select Template

Select the template that describes the stack that you want to create. A stack is a group of related resources that you manage as a single unit.

Design a template Use AWS CloudFormation Designer to create or modify an existing template. Learn more.

Choose a template A template is a JSON/YAML-formatted text file that describes your stack's resources and their properties. Learn more.

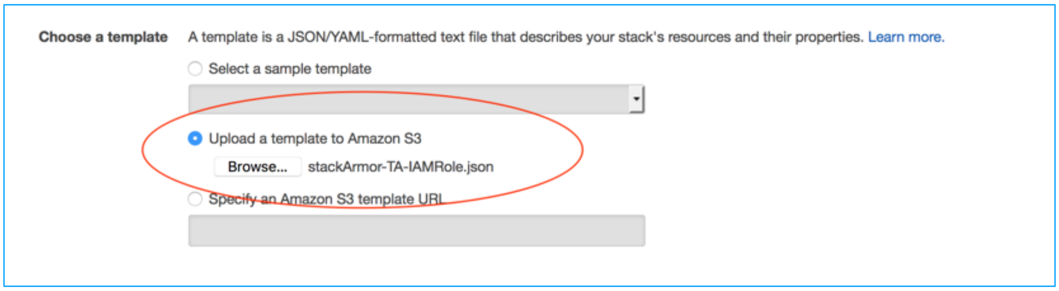
○ Select a sample template

● Upload a template to Amazon S3

No file selected.

Please select a file.

○ Specify an Amazon S3 template URL



Choose a template A template is a JSON/YAML-formatted text file that describes your stack's resources and their properties. Learn more.

○ Select a sample template

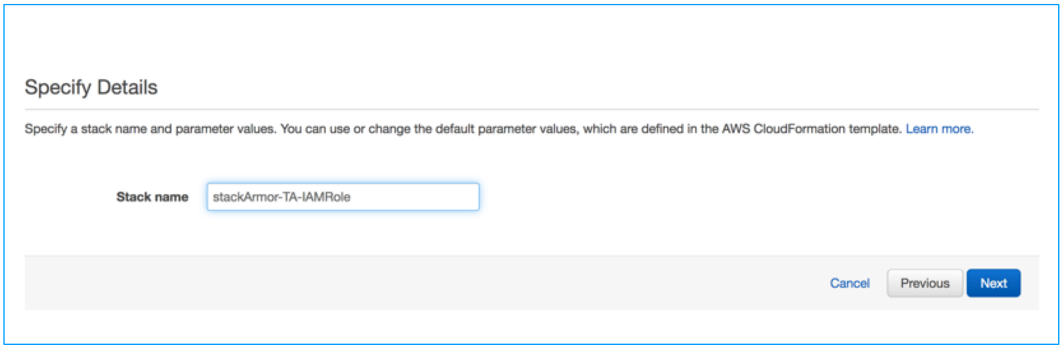
● Upload a template to Amazon S3

stackArmor-TA-IAMRole.json

○ Specify an Amazon S3 template URL

4. Click the “Next” button

5. In the “Stack name” textbox enter “stackArmor-TA-IAMRole” and click the “Next” button

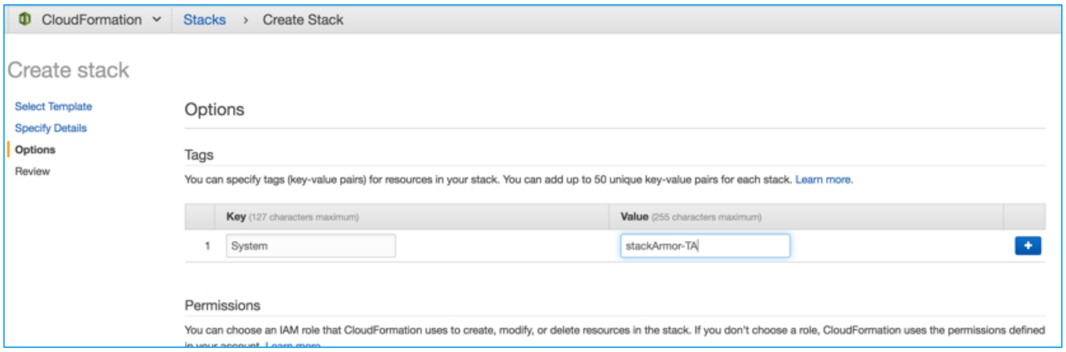


Specify Details

Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. Learn more.

Stack name: stackArmor-TA-IAMRole

6. In the “Options -> Tags” view/section enter “System” for the key and “stackArmor-TA” for the value



Options

Tags

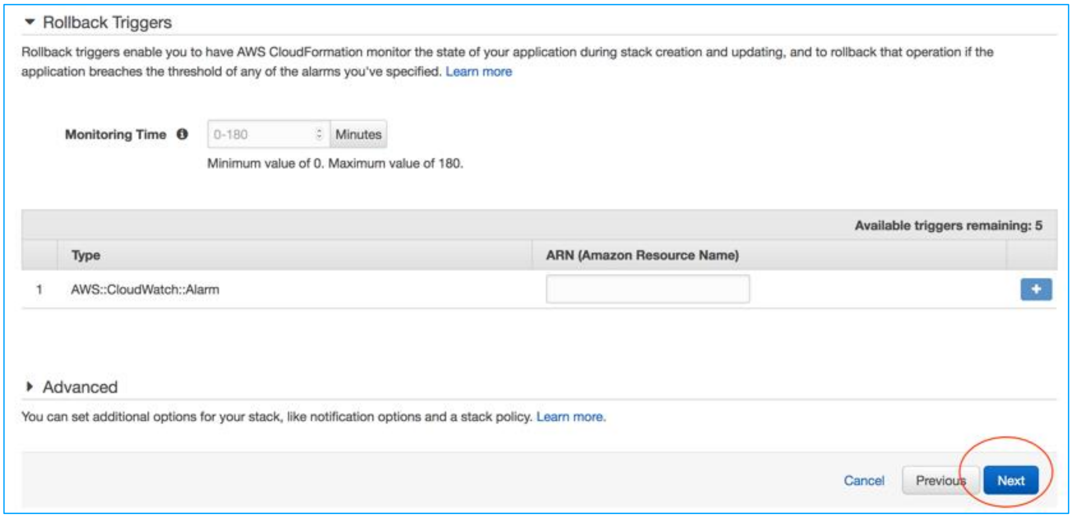
You can specify tags (key-value pairs) for resources in your stack. You can add up to 50 unique key-value pairs for each stack. Learn more.

	Key (127 characters maximum)	Value (255 characters maximum)
1	System	stackArmor-TA

Permissions

You can choose an IAM role that CloudFormation uses to create, modify, or delete resources in the stack. If you don't choose a role, CloudFormation uses the permissions defined in your account. Learn more.

7. Scroll down, leave the rest to the defaults and click the “Next” button



Rollback Triggers

Rollback triggers enable you to have AWS CloudFormation monitor the state of your application during stack creation and updating, and to rollback that operation if the application breaches the threshold of any of the alarms you've specified. Learn more

Monitoring Time: 0-180 Minutes

Minimum value of 0. Maximum value of 180.

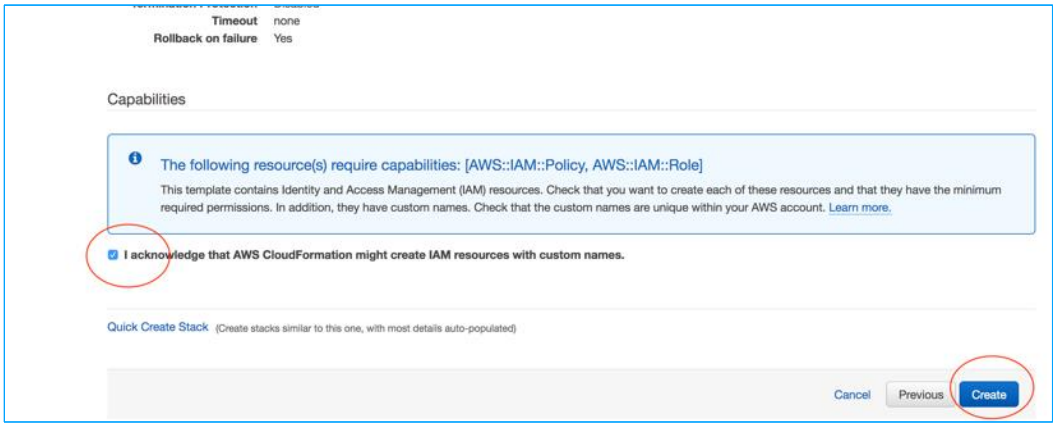
Available triggers remaining: 5

	Type	ARN (Amazon Resource Name)
1	AWS::CloudWatch::Alarm	

Advanced

You can set additional options for your stack, like notification options and a stack policy. Learn more.

8. In the final view check the checkbox labeled “I acknowledge that AWS CloudFormation might create IAM resources with custom names.” and click the “Create” button.



Timeout	none
Rollback on failure	Yes

Capabilities

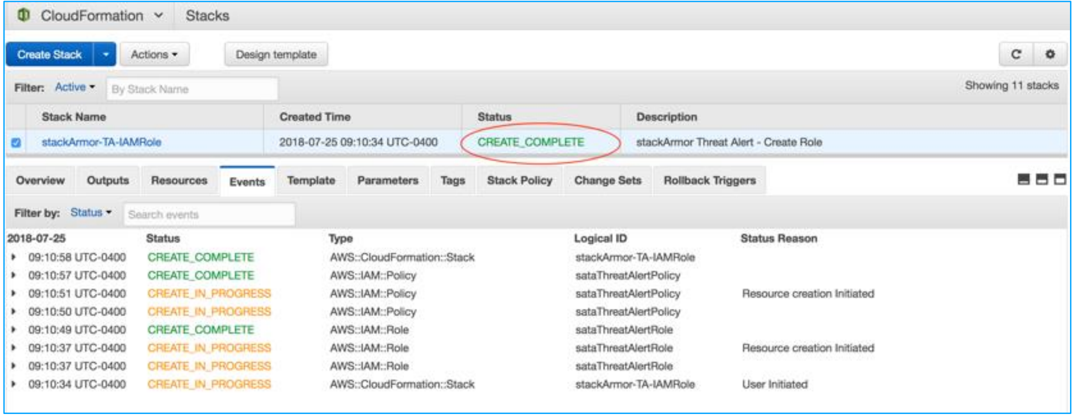
The following resource(s) require capabilities: [AWS::IAM::Policy, AWS::IAM::Role]

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.

Quick Create Stack (Create stacks similar to this one, with most details auto-populated)

9. Go back to the main CloudFormation dashboard to monitor the creation of the resource[s]. When successfully done the status will say “CREATE_COMPLETE”



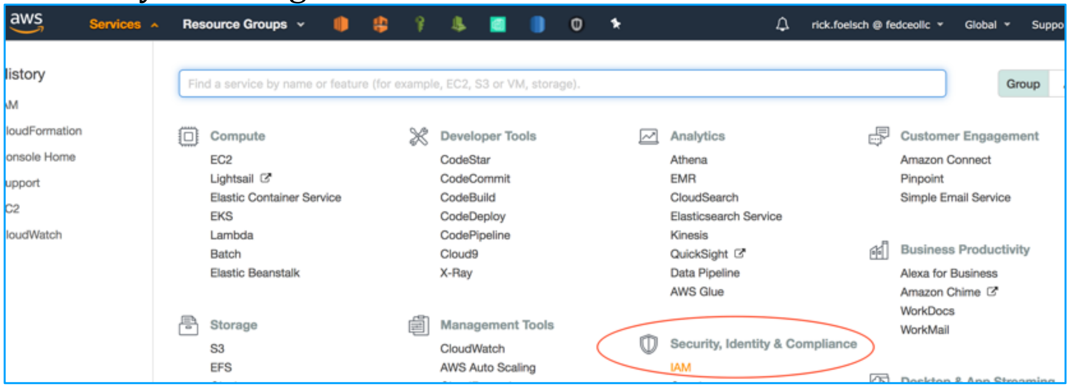
Filter: Active By Stack Name Showing 11 stacks

Stack Name	Created Time	Status	Description
stackArmor-TA-IAMRole	2018-07-25 09:10:34 UTC-0400	CREATE_COMPLETE	stackArmor Threat Alert - Create Role

Filter by: Status Search events

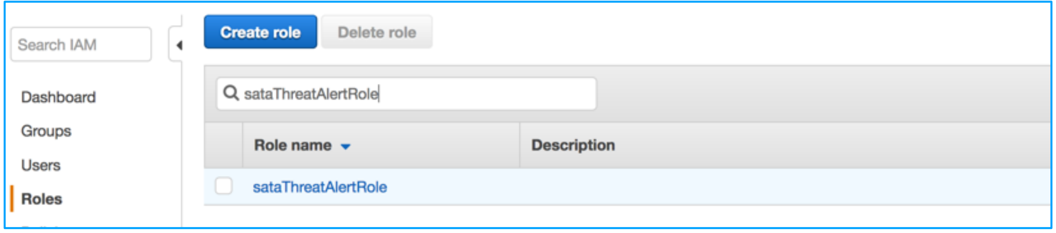
2018-07-25	Status	Type	Logical ID	Status Reason
09:10:58 UTC-0400	CREATE_COMPLETE	AWS::CloudFormation::Stack	stackArmor-TA-IAMRole	
09:10:57 UTC-0400	CREATE_COMPLETE	AWS::IAM::Policy	sataThreatAlertPolicy	
09:10:51 UTC-0400	CREATE_IN_PROGRESS	AWS::IAM::Policy	sataThreatAlertPolicy	Resource creation Initiated
09:10:50 UTC-0400	CREATE_IN_PROGRESS	AWS::IAM::Policy	sataThreatAlertPolicy	
09:10:49 UTC-0400	CREATE_COMPLETE	AWS::IAM::Role	sataThreatAlertRole	
09:10:37 UTC-0400	CREATE_IN_PROGRESS	AWS::IAM::Role	sataThreatAlertRole	Resource creation Initiated
09:10:37 UTC-0400	CREATE_IN_PROGRESS	AWS::IAM::Role	sataThreatAlertRole	
09:10:34 UTC-0400	CREATE_IN_PROGRESS	AWS::CloudFormation::Stack	stackArmor-TA-IAMRole	User Initiated

10. To verify further go to the IAM service



11. Next click the “Roles” link in the left-side menu

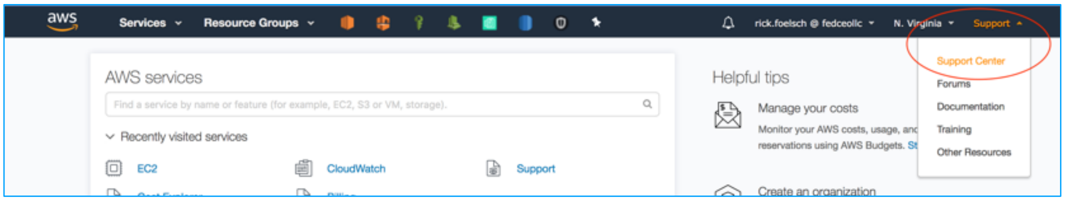
12. In the search textbox enter “sataThreatAlertRole” and verify the result displays



sataThreatAlertRole

	Role name	Description
□	sataThreatAlertRole	

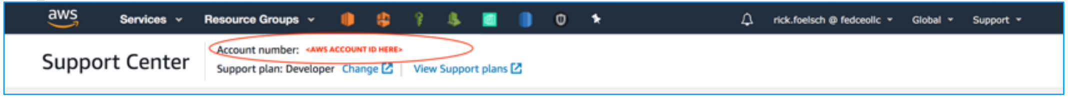
13. Next in the top menu bar click the “Support” link and then click the “Support Center” link.



Manage your costs

Monitor your AWS costs, usage, and reservations using AWS Budgets.

14. Lastly, find your AWS Account ID and provide it to your stackArmor representative



Account number: <AWS ACCOUNT ID HERE>

Support plan: Developer