Implementation Guide

Automations for AWS Firewall Manager

Automations for AWS Firewall Manager: Implementation Guide

Table of Contents

Centrally configure, manage, and audit firewall rules with Automations for AWS Firewall Manager

The Automations for AWS Firewall Manager solution helps you centrally configure, manage, and audit firewall rules across your accounts and applications in AWS Organizations. This solution uses AWS Firewall Manager to automatically define and deploy a set of managed rules for AWS WAF and audit checks for Amazon Virtual Private Cloud (Amazon VPC) security groups across your AWS accounts from a single place. If you use AWS Shield Advanced, this solution optionally provides you with one-click automations to set up and configure application layer distributed denial of service (DDoS) protection, proactive event response, and health-based detection.

The process for defining policies and configuring rule sets in Firewall Manager can be challenging and time consuming. To help simplify this process, this solution deploys a set of AWS managed firewall rules and security group audit checks for you. Managed firewall rules provide a set of preconfigured rules to protect web applications running on Amazon CloudFront, Application Load Balancer, and Amazon API Gateway. Security group audit checks continuously monitor and detect overly permissive security group rules to protect your Amazon VPC resources and improve your firewall posture. You can also customize the default Firewall Manager rules deployed by the solution to fit your needs, as described in the Customization guide.

This implementation guide provides an overview of the Automations for AWS Firewall Manager solution, its reference architecture and components, considerations for planning the deployment, and configuration steps for deploying the solution to the Amazon Web Services (AWS) Cloud.

The intended audience for using this solution's features and capabilities in their environment includes solution architects, business decision makers, DevOps engineers, data scientists, and cloud professionals.

Use this navigation table to quickly find answers to these questions:

If you want to . . .	Read . . .
Know the cost for running this solution. The cost to run the solution in the US East (N. Virginia) Region, **excluding automations for Shield Advanced**, is approximately:	Cost

If you want to . . .	Read . . .
• **$1,733.00 per month** for a small organization • **$18,951.00 per month** for a large organization The cost to run the solution in the US East (N. Virginia) Region, **including deployment of the automations for Shield Advanced**, is approximately: • **$938.82 per month** for a small organization • **$3,352.76 per month** for a large organization **Note** Costs are lower when including the automations for Shield Advanced because your Shield Advanced subscription includes many of the features of this solution, such as AWS WAF policies.	
Understand the security considerations for this solution. This solution uses Parameter Store, a capability of AWS Systems Manager, to initiate create, read, update, and delete (CRUD) operations to the Firewall Manager policies.	Security
Know how to plan for quotas for this solution.	Quotas

If you want to . . .	Read . . .
Know which AWS Regions support this solution.	Supported AWS Regions
View or download the AWS CloudForm ation template included in this solution to automatically deploy the infrastructure resources (the "stack") for this solution.	AWS CloudFormation template
Access the source code and optionally use the AWS Cloud Development Kit (AWS CDK) to deploy the solution.	GitHub repository

Features and benefits for Automations for AWS Firewall Manager

The solution provides the following features:

Optional integration with AWS Shield Advanced

Existing AWS Shield Advanced customers can use this solution's automations to enable Shield Advanced features at scale, across your AWS Organization, without the added complexity of manual configuration. These automations include:

- Setting up health-based detection for your Shield-protected resources
- Enabling proactive Event Response from the Shield Response Team (SRT)
- Deploying DDoS protection with Firewall Manager policies

Shield Advanced customers can also choose to deploy any or all of the automations for Shield Advanced AWS CloudFormation templates as necessary, without the need to deploy the main Firewall Manager template provided by this solution.

If you aren't a Shield Advanced subscriber, you can still use the Firewall Manager automations provided in the solution.

Integration with AWS Organizations

You can optionally deploy the supplemental AWS CloudFormation template included in this solution into an AWS Organizations management account to configure the Firewall Manager prerequisites for this solution automatically. For example:

- Checking that all features for AWS Organizations are activated
- Designating an account as the admin account for Firewall Manager
- Enabling AWS Config across an AWS Organization

Automated onboarding process

This solution automates the onboarding process for Firewall Manager and sets up baseline rules and audit checks for AWS Organizations. You can restrict policies for specific organizational units (OUs), Regions, or tagged resources within your AWS Organizations account. When you modify the installed Parameter Store parameters, this solution updates and deploys the policies to the specified resources.

Use cases for for Automations for AWS Firewall Manager

This solution is intended for customers seeking to manage a consistent security posture across their entire AWS Organization by leveraging key features of Firewall Manager and Shield. This solution enables central configuration, management, and auditing of firewall rules across all AWS Organizations accounts and resources. It also offers operational integration with Shield Advanced. The following are key use cases for this solution.

Align AWS WAF, DNS, and security group policies across your organization

There might be situations where you want to manage multiple Firewall Manager policy configurations across different accounts and organizations. You can use this solution to apply one policy configuration to a subset of OUs in one or multiple Regions, and then apply the same or a different policy to another subset of OUs, all from the same place.

Streamline compliance tasks when onboarding new AWS accounts

The solution automates the process of applying Firewall Manager policies to new accounts in AWS Organizations. As soon as a new account is onboarded, the solution ensures that it inherits all existing security configurations and compliance policies, eliminating the need for manual setup and reducing the risk of security gaps.

Simplify the deployment of Shield Advanced features

For Shield Advanced customers, this solution enables the deployment and configuration of key Shield features, including health-based detection, proactive event response, and DDoS protection. Furthermore, the solution provides Shield Advanced customers the capability to centrally configure and implement DDoS protection across all accounts within their AWS Organization.

Create compliance reports for network policies

You can use this solution to create compliance reports that outline security group policies that you have enabled across accounts and resources. Reports are exportable in `0csv` format.

Concepts and definitions for Automations for AWS Firewall Manager

This section describes key concepts and defines terminology specific to this solution:

Amazon Route 53 health check

Amazon Route 53 health checks monitor the health and performance of your web applications, web servers, and other resources. A health check can monitor the status of other health checks; this type of health check is known as a *calculated health check*. The health check that does the monitoring is the *parent health check*, and the health checks that are monitored are *child health checks*.

distributed denial of service (DDoS)

A DDoS attack is an attack in which multiple compromised systems try to flood a target with traffic. A DDoS attack can prevent legitimate end users from accessing the target services and can cause the target to crash due to overwhelming traffic volume.

Firewall Manager policy

Set of security rules that replicates across your AWS Organization.

Shield Response Team (SRT)

The SRT are security engineers who specialize in DDoS event response and provide added support for Shield Advanced customers.

Note

For a general reference of AWS terms, see the AWS Glossary.

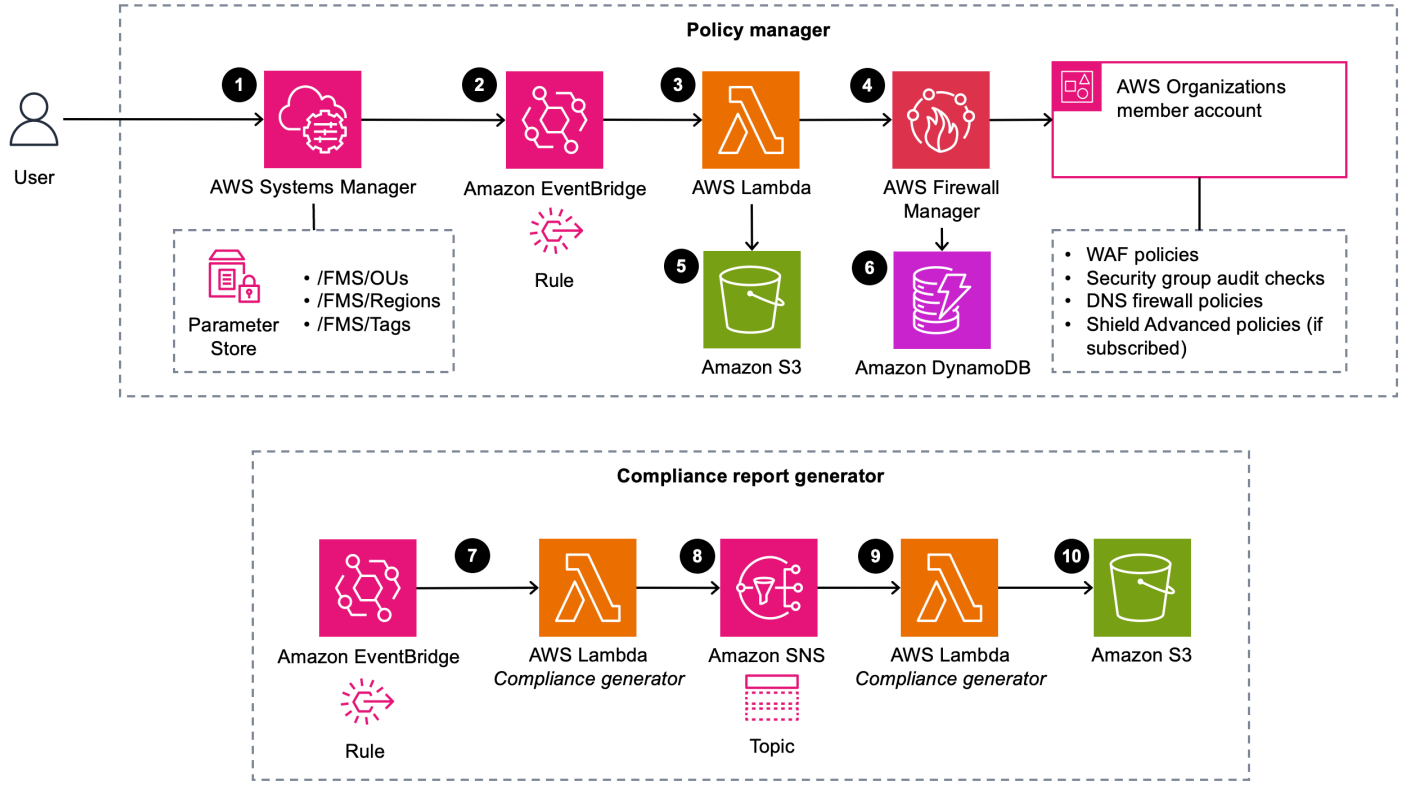
Architecture overview

This section provides the reference implementation architecture diagrams for the components deployed with this solution.

Architecture diagram (Primary stack)

Deploying this solution's Primary stack with the default parameters deploys the following components in your AWS account.

Architecture diagram. Descriptive text follows.



> **Note**
>
> AWS CloudFormation resources are created from AWS Cloud Development Kit (AWS CDK) constructs.

The architecture can be grouped into two separate workflows: policy manager and compliance report generator.

Policy manager

When the `aws-fms-automations` CloudFormation template deploys, an AWS Systems Manager Parameter Store containing three parameters is created, each with default values. The parameters that are created include **/FMS/OUs**, **/FMS/Regions**, and **/FMS/Tags**.

The high-level process flow for the solution components deployed with the CloudFormation template is as follows:

1. You can update these parameters using Systems Manager:
   - For the **/FMS/OUs** parameter, add organizational unit IDs to apply policies and rule sets to multiple OUs.
   - For the **/FMS/Regions** parameter, specify AWS Region names.
   - For the **/FMS/Tags** parameter, create *inclusion* and *exclusion* tags and add tags to specific resources within accounts to indicate resources for which policies and rule sets should be applied or not applied respectively. For information about setting up Parameter Store parameters, refer to Scenarios for setting up the Systems Manager parameters.
2. An Amazon EventBridge rule uses an event pattern to capture the Systems Manager parameter update event.
3. An EventBridge rule invokes an AWS Lambda function.
4. The Lambda function installs a set of predefined Firewall Manager security policies across the user-specified OUs. The policies include an AWS WAF web access control list (ACL) consisting of AWS-managed rule sets and Amazon VPC security group audit policies. Additionally, if you have a subscription to Shield Advanced, this solution deploys policies to protect eligible resources with Shield.
5. The `PolicyManager` Lambda function fetches the policy manifest file from the Amazon Simple Storage Service (Amazon S3) bucket and uses the manifest file to create Firewall Manager security policies.
6. Lambda saves policies metadata in the Amazon DynamoDB table.

For a complete list of policies and rule sets that are installed, refer to the List of policies and rule sets.

Compliance report generator

When the CloudFormation stack deploys, it creates a time-based EventBridge rule, a Lambda function, an Amazon Simple Notification Service (Amazon SNS) topic, and an S3 bucket.

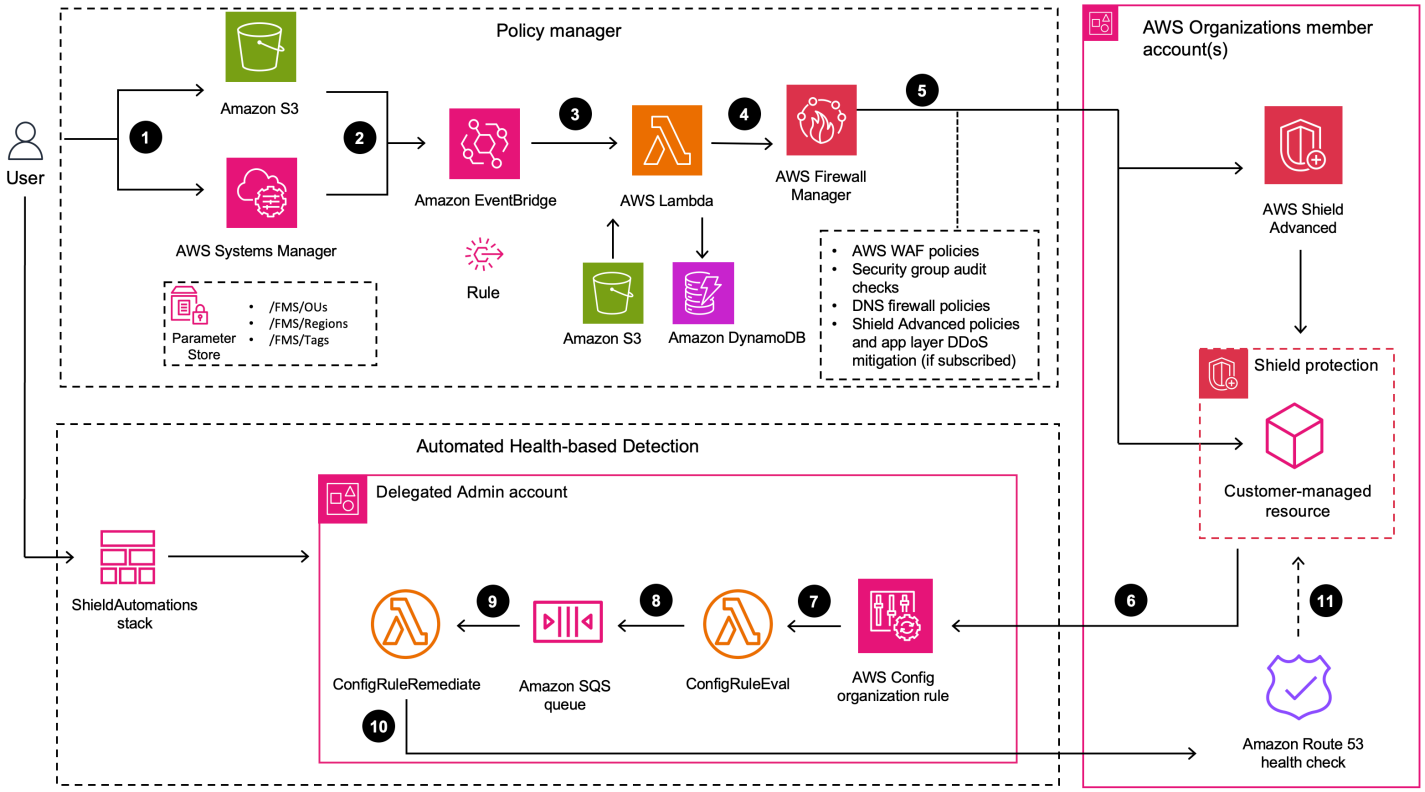
The high-level process flow for the solution components deployed with the CloudFormation template is as follows:

1. A time-based EventBridge rule invokes the `ComplianceGenerator` Lambda function.
2. The `ComplianceGenerator` Lambda function fetches Firewall Manager policies in each Region and publishes the list of policy IDs in the Amazon SNS topic.
3. The Amazon SNS topic invokes the `ComplianceGenerator` Lambda function with the payload `{PolicyId: string, Region: string}`.
4. The `ComplianceGenerator` Lambda function generates a compliance report for each of the policies and uploads the report in CSV format in an S3 bucket.

Architecture diagram (with automations for Shield Advanced)

Deploying all of the solution's stacks with the default parameters deploys the following components in your AWS account.

Depicted below: Automations for AWS Firewall Manager solution architecture with Shield Advanced Automations



Automations for AWS Firewall Manager solution architecture with Shield Advanced Automations

The high-level process flow for the automations for Shield Advanced feature of the solution includes workflows for both the policy manager and automated health-based detection.

Policy manager

1. (Optional) Update the Parameter Store parameters created by the `aws-fms-automations` template with your desired values. The parameters that are created include **/FMS/OUs**, **/FMS/Regions**, and **/FMS/Tags**.

   > **Note**
   >
   > If you have already set up Shield Advanced protections for your AWS resources, you can skip this step.

2. The stack follows steps 2-5 for the **Policy manager** in the Architecture diagram (Primary stack) section to create Firewall Manager security policies. This includes Shield Advanced policies for Shield Advanced customers.

Automated health-based detection

When the aws-fms-shield-automations template is deployed, the stack creates an organization AWS Config rule, two Lambda functions, and an Amazon Simple Queue Service (Amazon SQS) queue in the account where the template is deployed.

6. After deployment, the automated health-based detection workflow runs automatically. The organization AWS Config rule captures existing Shield Advanced protections across your AWS Organization. You can create these Shield Advanced protections automatically through the Firewall Manager security policies deployed by this solution, or manually using the Shield console. The following are all Shield Advanced-protected resource types supported for automated health-based detection:
   a. Amazon Elastic Compute Cloud (Amazon EC2) Elastic IP addresses (with attachments to EC2 instances or Network Load Balancers)
   b. Application Load Balancers
   c. Classic Load Balancers

d. Network Load Balancers

e. CloudFront distributions

Shield Advanced doesn't create protections for Network Load Balancers directly. To protect a Network Load Balancer, you must first attach the Network Load Balancer to an Elastic IP address, and create a protection for that Elastic IP address instead. For more information, see List of resources that AWS Shield Advanced protects.

> **Important**
>
> The network interface used to attach a Network Load Balancer to an Elastic IP address must have the following in its description for automated health-based detection to create an Amazon Route 53 health check for the resource: `net/network-load-balancer-name/network-load-balancer-resource-id`. This is the default description when Network Load Balancers are attached to an Elastic IP address.

7. Shield Advanced protections captured by the organization Config rule are sent to the `ConfigRuleEval` Lambda function for evaluation. This Lambda function determines whether or not the protection has Route 53 health checks associated with it.
8. If there are no Route 53 health checks associated with the Shield Advanced protection, the solution publishes a message to the Amazon SQS queue requesting that health checks be created for the protection.
9. The `ConfigRuleRemediate` Lambda function reads messages from the Amazon SQS queue.
10. The `ConfigRuleRemediate` Lambda function creates a calculated Route 53 health check based on the type of resource that the Shield Advanced protection protects.
11. The `ConfigRuleRemediate` Lambda function associates the Route 53 health check created in step 10 with the Shield Advanced protection being evaluated.

This flow runs continuously for all accounts in your AWS Organization that aren't excluded during CloudFormation template deployment. You can exclude accounts by providing a comma delimited list for the **Excluded Accounts** parameter when deploying the Shield Advanced Automations stack.

> **Note**
>
> You are responsible for maintaining the Route 53 health checks created by the solution for your Shield Advanced protections. Ensure that you keep the health checks up-to-date with

the resources that they are monitoring. For more information, see Health-based detection using health checks with Shield Advanced and Route 53.

Architecture details

This section describes the components and AWS services that make up this solution and the architecture details on how these components work together.

AWS services in this solution

AWS service	Description
AWS CloudFormation	**Core.** Deploys the AWS resources for this solution.
AWS Config	**Core.** Used natively by Firewall Manager. Additionally, this solution's automations for Shield Advanced create AWS Config rules to evaluate and remediate Shield Advanced protections.
Amazon DynamoDB	**Core.** Stores metadata for this solution. The solution uses this metadata to perform create, update, and delete actions on policies.
AWS Firewall Manager	**Core.** Automatically deploys a set of managed rules for AWS WAF and audit checks for VPC security groups across your AWS accounts.
AWS Organizations	**Core.** Helps you centrally manage your accounts. This solution sets up baseline rules and audit checks for AWS Organizations.
Amazon S3	**Core.** Stores the policy manifest and compliance reports.
Amazon CloudWatch	**Supporting.** CloudWatch metric alarms are created by automations for Shield Advanced and used to configure Route 53 health checks for health-based detection.

AWS service	Description
Amazon EventBridge	**Supporting.** Invokes Lambda functions for this solution when Parameter Store for OUs, Regions, and tags are updated.
AWS Lambda	**Supporting.** Initiates prerequisite checks and the installation of policies and rule sets in OUs for Firewall Manager.
Amazon SNS	**Supporting.** Invokes the `Complianc eGenerator` Lambda function, and optionally sends email notifications regarding errors that require manual intervention.
Amazon SQS	**Supporting.** Invokes the `ConfigRul eRemediate` Lambda function.
AWS Systems Manager	**Supporting.** Stores the solution's configura tion parameters.
AWS Shield	**Optional.** AWS Shield Advanced protections are modified to enable health-based detection .

AWS Lambda functions

This solution uses Lambda functions to initiate prerequisite checks and the installation of policies and rule sets in OUs for Firewall Manager.

This solution uses the following Lambda functions:

- `PreReqManager` - This Lambda function checks and validates the following:
  - The prerequisite stack is deployed in the AWS Organizations primary account
  - The AWS Organizations all features option is activated
  - There is a delegated admin account assigned for Firewall Manager
  - Trusted access is activated between AWS Organizations and CloudFormation StackSets

- AWS Config is activated across AWS Organizations for all member accounts

You can access log information for this Lambda function by following these instructions:

1. Sign in to the Amazon CloudWatch console.
2. Select **Logs** from the navigation menu, then **Log groups**.
3. Select the log group named: /aws/lambda/*<Stack-Name>*-xxx-PreReqManager-xxx.

- `PolicyManager` - This Lambda function is responsible for managing Firewall Manager policies, such as creating, updating, and deleting the policies. The Lambda function fetches the policy manifest file from the S3 bucket and uses it to create Firewall Manager security policies. The manifest file can be modified at any time per requirement for policy configuration. The changes in the policy manifest are picked up with the next policy update event. The function saves policy metadata in the DynamoDB table.

You can access log information for this Lambda function by following these instructions:

1. Sign in to the Amazon CloudWatch console.
2. Select **Logs** from the navigation menu, then **Log groups**.
3. Select the log group named: /aws/lambda/*<Stack-Name>*-xxx-PolicyManager-xxx.

- `ComplianceGenerator` - This Lambda function generates compliance reports for audit purposes. The reports are generated in CSV format and staged in an S3 bucket.
  1. Sign in to the Amazon CloudWatch console.
  2. Select **Logs** from the navigation menu, then **Log groups**.
  3. Select the log group named: /aws/lambda/*<Stack-Name>*-xxx-ComplianceGenerator-xxx.
- `ConfigRuleEval` - This Lambda function is invoked by the organization AWS Config rule deployed by the `aws-fms-shield-automations` template. It handles custom evaluation of resources for the AWS Config rule by validating the Shield Advanced protection and determining whether or not it has Route 53 health checks associated with it.
- `ConfigRuleRemediate` - This Lambda function reads messages published to the Amazon SQS queue deployed by the `aws-fms-shield-automations` template. It creates Route 53 health checks and associates them with Shield Advanced protections.

AWS CloudFormation StackSets

This solution uses service-managed CloudFormation StackSets with service-managed permissions to use AWS Config across the AWS Organization.

> **Note**
>
> The amount of time to turn on AWS Config depends on the number of member accounts and Regions under consideration. For example, in testing, it took approximately 90 minutes to turn on AWS Config across 6 accounts and 16 Regions for 2 OUs.

AWS Firewall Manager integration

This solution automatically installs policies and rule sets for Firewall Manager. By default, AWS WAF, security group, and Amazon Route 53 Domain Name System (DNS) Firewall security policies are installed. Additionally, if you have a subscription to Shield Advanced, Shield policies are also installed with application layer DDoS mitigation set to Count mode by default for applicable resources.

Firewall Manager policies are configured with auto-remediation activated for AWS WAF and Shield Advanced policies. If you want to customize policy deployment or another aspect of the solution, refer to the README.md file in the GitHub repository.

AWS Shield Advanced integration

This solution provides automations for Shield Advanced subscribers to configure three features of AWS Shield Advanced: proactive event response, application layer DDoS mitigation, and health-based detection.

Proactive event response

You can enable proactive event response in one click across an AWS Organization by using the `aws-fms-proactive-event-response` CloudFormation template. You can deploy this template as a service-managed StackSet to an AWS Organization to enable this feature for all your associated accounts. This template also provides the option to grant the SRT access to your accounts to act on your behalf.

Application layer DDoS mitigation

Application layer DDoS mitigation is enabled in Count mode by default when the following are true:

- You deploy Firewall Manager security policies using this solution's default `policy_manifest.json` file
- You have an active AWS Shield Advanced subscription

These policies deploy after you configure the Parameter Store parameters to your desired values. You can choose to modify the default count mode configured by the Firewall Manager policies deployed by this solution by editing the `policy_manifest.json` file stored in Amazon S3. For more information, refer to the Customization guide.

Health-based detection

You can automate health-based detection setup with the `aws-fms-shield-automations` template, which uses AWS Config rules and custom Lambda functions to create Amazon Route 53 health checks for existing Shield Advanced protections. The solution will also create health checks for Shield Advanced protections created after this solution is deployed. We recommend reviewing the caveats for application layer DDoS mitigation.

AWS Systems Manager Parameter Store

Parameter Store stores the solution's configuration parameters. You can use these parameters to specify OUs, Regions, and tags_._ The Parameter Store parameters allow you to easily extend policies and rule sets to multiple OUs and Regions. These parameters also allow you to specify inclusion and exclusion tags and apply these tags to specific resources in your accounts.

Additionally, administrators can view and modify the solution's parameters in one centralized location. You can add, edit, and remove parameter values to modify their selection across OUs, Regions, and tags. Corresponding Firewall Manager policies are updated automatically.

Amazon EventBridge

This solution uses the Amazon EventBridge rule to invoke Lambda functions when updates are made to Parameter Store for OUs, Regions, and tags. When the Lambda functions are initiated, policies and rule sets are installed in OUs and Regions (as updated by the user).

Amazon S3

The solution creates two S3 buckets in your account. One bucket stages the policy manifest file, and the other bucket is used by the `ComplianceGenerator` Lambda function to save compliance reports.

AWS Config

Firewall Manager natively uses AWS Config to create and maintain security policies. Additionally, the `aws-fms-shield-automations` CloudFormation template creates an organization AWS Config rule that does the following:

- Detects Shield Advanced protections across an AWS Organization
- Remediates protections that don't have health-based detection configured

Amazon SNS

The solution creates Amazon SNS topics and provides the option to subscribe to these topics during template deployment. When you provide your email address for the **Email Address** template parameter, you receive notifications by email regarding problems that can't be resolved without manual intervention, such as reaching service quotas. This parameter is included in both the Primary and Shield Advanced Automations stacks.

Amazon Route 53

The automations deployed by the `aws-fms-shield-automations` CloudFormation template creates and associates Route 53 health checks with your Shield Advanced protections, including the following:

- Calculated health checks to be associated directly with Shield Advanced protections.
- Child health checks that are attached to the calculated health checks. These child health checks are based on CloudWatch metrics that are configured during deployment.

Amazon DynamoDB

This solution uses DynamoDB to save metadata created from Firewall Manager policies. The metadata is used to update and delete policies across specified OUs and Regions. The following is sample metadata from a Firewall Manager policy.

```
{
"LastUpdatedAt": "2020-09-10T19:18:33.719Z",
"PolicyId": "abcd1234-ab12-cd34-b99b-ab01cde2fg34",
"PolicyName": "FMS-Shield-01",
"PolicyUpdateToken": "1:AbCde1fGH2iJKLM34nO5PQ==",
"Region": "Global"
}
```

Important

Do not delete this table. It is used to perform create, update, and delete actions on the policies.

Plan your deployment

This section describes the cost, security, Regions, and other considerations prior to deploying the solution.

Supported AWS Regions

The following sections specify which Regions each non-prerequisites stack of this solution is available in.

Region support for the Primary stack

Important

Although AWS Organizations and Firewall Manager are available globally, both AWS services use a specific Region as their data plane (for example, US East (N. Virginia) for the commercial AWS Regions). As a result, the service clients for these AWS services must be created with the appropriate endpoint for the Region. These Regions are as follows:

- US East (N. Virginia) for the commercial AWS Regions
- AWS GovCloud (US-West) for the AWS GovCloud (US) Regions
- China (Ningxia) for the China Regions

Deploying in another AWS Region will work, but if there are AWS Organizations service control policies or custom firewall rules restricting traffic from transmitting out of the Region, then these APIs will fail. If you have restrictions in place, then we recommend deploying the solution in one of the Regions listed previously.

The solution's Primary stack is available in the following Regions. For the most current availability of AWS services by Region, see the AWS Regional Services List.

AWS Region	
US East (N. Virginia)	China (Beijing)

AWS Region	
US East (Ohio)	China (Ningxia)
US West (Northern California)	Europe (Frankfurt)
US West (Oregon)	Europe (Ireland)
Africa (Cape Town)	Europe (London)
Asia Pacific (Hong Kong)	Europe (Milan)
Asia Pacific (Hyderabad)	Europe (Paris)
Asia Pacific (Jakarta)	Europe (Spain)
Asia Pacific (Melbourne)	Europe (Stockholm)
Asia Pacific (Mumbai)	Europe (Zurich)
Asia Pacific (Osaka)	Middle East (Bahrain)
Asia Pacific (Seoul)	Middle East (UAE)
Asia Pacific (Singapore)	South America (São Paulo)
Asia Pacific (Sydney)	AWS GovCloud (US-East)
Asia Pacific (Tokyo)	AWS GovCloud (US-West)
Canada (Central)	

Region support for the Shield Advanced Automations stack

You can deploy the `aws-fms-shield-automations` template in the following Regions to enable Shield Advanced health-based detection.

Important

If you want to enable health-based detection for global resources, including CloudFront distributions, you must deploy the stack in one of the following Regions:

- US East (N. Virginia) for the commercial AWS Regions
- AWS GovCloud (US-West) for the AWS GovCloud (US) Regions

Shield Advanced uses these Regions as their data plane for global resources. Therefore, AWS Config won't create configuration items for global resources in Regions other than the ones previously listed. Recording for the `AWS::Shield::Protection` resource type can only be enabled in these Regions. For all other Regions, you only need to enable recording for the `AWS::ShieldRegional::Protection` resource type. If you want to enable health-based detection for regional resources, you can deploy the stack in the following Regions. For the most current availability of AWS services by Region, see the AWS Regional Services List.

AWS Region	
US East (N. Virginia)	Asia Pacific (Tokyo)
US East (Ohio)	Canada (Central)
US West (Northern California)	Europe (Frankfurt)
US West (Oregon)	Europe (Ireland)
Asia Pacific (Jakarta)	Europe (London)
Asia Pacific (Melbourne)	Europe (Paris)
Asia Pacific (Mumbai)	Europe (Stockholm)
Asia Pacific (Seoul)	South America (São Paulo)
Asia Pacific (Singapore)	AWS GovCloud (US-East)
Asia Pacific (Sydney)	AWS GovCloud (US-West)

Region support for the Proactive Event Response stack

The solution's Proactive Event Response stack is available in the following Regions. For the most current availability of AWS services by Region, see the AWS Regional Services List.

AWS Region	
US East (N. Virginia)	Asia Pacific (Tokyo)
US East (Ohio)	Canada (Central)
US West (Northern California)	Europe (Frankfurt)
US West (Oregon)	Europe (Ireland)
Africa (Cape Town)	Europe (London)
Asia Pacific (Hong Kong)	Europe (Paris)
Asia Pacific (Malaysia)	Europe (Stockholm)
Asia Pacific (Mumbai)	Middle East (Bahrain)
Asia Pacific (Seoul)	Middle East (UAE)
Asia Pacific (Singapore)	South America (São Paulo)
Asia Pacific (Sydney)	

Cost

You are responsible for the cost of the AWS services used while running this solution. The following cost estimates are based on specific assumptions. You can reduce the cost to fit your needs by restricting the scope of your Firewall Manager policies with the Systems Manager parameters, or by customizing the default policies deployed by the solution.

As of this revision, the cost to run the solution in the US East (N. Virginia) Region, **excluding automations for Shield Advanced**, is approximately:

- **$1,733.00 per month** for a small organization

- **$18,951.00 per month** for a large organization

The cost to run the solution in the US East (N. Virginia) Region, **including deployment of the automations for Shield Advanced**, is approximately:

- **$938.82 per month** for a small organization
- **$3,352.76 per month** for a large organization

> **Note**
>
> These cost estimations don't include the monthly subscription cost of Shield Advanced. For more information, refer to AWS Shield Advanced pricing.
> Costs are lower when including the automations for Shield Advanced because your Shield Advanced subscription includes many of the features of this solution, such as AWS WAF policies.

These costs are for the resources shown in the Sample cost tables. The total cost to run this solution depends on the following:

- Number of policies installed
- Number of accounts managed
- Number of rule sets and web ACLs installed
- Number and invocation duration of Lambda functions
- Number of EventBridge events published
- Number of Shield protections configured

We recommend creating a budget through AWS Cost Explorer to help manage costs. Prices are subject to change. For full details, see the pricing webpage for each AWS service used in this solution.

Sample cost tables

The following tables provide a sample cost breakdown for deploying this solution with the default parameters in the US East (N. Virginia) Region for one month.

Cost per month for a small organization - Primary stack

Assumptions:

- Accounts: 12 accounts across 2 OUs
- Number of AWS Regions: 3
- Subscription to AWS Shield Advanced: No
- Number of policies: 13
  - CloudFront global policy: AWS WAF global policy (*$100 7 1 global policy*)
  - Regional policies:
    - AWS WAF Regional policy (*$100 x 3 Regions*)
    - Security group content audit policy (*$100 x 3 Regions*)
    - Security group usage audit policy (*$100 x 3 Regions*)
    - DNS Firewall policy (*$100 x 3 Regions*)

> **Note**
>
> The following cost estimate doesn't account for a subscription to AWS Shield Advanced. With the Shield Advanced subscription, the AWS WAF protection policy cost and the AWS WAF web ACL and rules cost are included. For additional information, refer to the AWS Firewall Manager pricing page.

Components	Quantity	Accounts	$/month [USD]	Monthly Total [USD]
AWS Firewall Manager				
Policies	13	N/A	$100.00	**$1,300.00**
AWS WAF web ACL	4	12	$5.00	**$240.00**
AWS WAF rules	4 x 4	12	$1.00	**$192.00**

Components	Quantity	Accounts	$/month [USD]	Monthly Total [USD]
Other AWS services*				
Other*	N/A	12	less than $1.00	**$1.00**
			Total:	**$1,733.00**
* Other AWS services include Lambda, Amazon SNS, EventBridge, CloudFormation StackSets, AWS Config, Route 53 Resolver DNS Firewall, Parameter Store, X-Ray, DynamoDB, and Amazon S3.				

Cost per month for a small organization - Automations for Shield Advanced

Assumptions:

- Includes all costs for a small organization deploying the automations for Shield Advanced templates
- Costs for AWS WAF protection policies, web ACLs, and rules are included in an Shield Advanced subscription, so they are excluded from this calculation. For additional information, refer to AWS Firewall Manager pricing.
- Accounts: 12 accounts
- Number of AWS Regions: 1

- Subscription to Shield Advanced: Yes
- Number of regional Shield Advanced protections: 20
- Number of global Shield Advanced protections: 2

Cost details:

- AWS Config continuous recording: Enabled for Shield Advanced protections
  - Configuration items (*$0.003 per configuration item x 22 Shield Advanced protections x 2 configuration changes*)
  - AWS Config rule evaluations (*$0.001 per rule evaluation x 22 Shield Advanced protections x 2 configuration changes*)
- Route 53 health checks (*$0.50 per health check per month x 3 health checks x 22 Shield Advanced protections*)
- CloudWatch metric alarms (*$0.10 per alarm metric x 22 Shield Advanced protections x 2 metric alarms*)
- Lambda:
  - Function requests (*$0.20 per 1M requests x (44 configuration item evaluations + 22 remediations + 30 time-based evaluations)*)
  - Function duration (*$0.0000000167 per 1ms x 150,000 ms x 96 invocations*)

> **Note**
>
> The following cost estimate only accounts for AWS Config continuous recording costs related to Shield Advanced resource types. These costs might vary depending on the type of recording enabled and the resources being recorded by AWS Config in your accounts. For additional information, refer to the AWS Config pricing page.

Components	Quantity	Pricing (USD)	Monthly Total (USD)
AWS Config			
Configuration items	22	$0.003 per configuration item delivered	**$0.132**

Components	Quantity	Pricing (USD)	Monthly Total (USD)
AWS Config rule evaluations	44	$0.001 per rule evaluation	**$0.044**
Route 53			
Health checks	66	$0.50 per health check per month	**$33.00**
CloudWatch			
Metric alarms	44	$0.10 per alarm metric per month	**$4.40**
Amazon SQS			
FIFO queue	1	First 1 million requests/month are free $0.50 per million requests thereafter	AWS Free Tier
Lambda			
Function duration	150,000 ms	$0.0000000167 per 1 ms	**$0.24**
Function requests	96	$0.20 per 1M requests	AWS Free Tier
X-Ray			
Tracing	~100 traces recorded with default 5% sampling rate	$0.000005 per trace	**< $ 0.01**
		Total	**$37.82**

Cost per month for a large organization - Primary stack

Assumptions:

- Accounts: 150 accounts across 20 OUs
- Number of AWS Regions: 10
- Subscription to AWS Shield Advanced: No
- Number of policies: 41
  - Global policy: AWS WAF global policy ($100 x 1 global policy)
  - Regional policies:
    - AWS WAF Regional policy (*$100 x 10 AWS Regions*)
    - Security group content audit policy (*$100 x 10 Regions*)
    - Security group usage audit policy (*$100 x 10 Regions*)
    - DNS Firewall policy (*$100 x 10 Regions*)

> **Note**
>
> The following cost estimate doesn't account for a subscription to AWS Shield Advanced. With the Shield Advanced subscription, the AWS WAF protection policy cost and the AWS WAF web ACL and rules cost are included. For additional information, refer to the AWS Firewall Manager pricing page.

Components	Quantity	Accounts	$/month [USD]	Monthly Total [USD]
AWS Firewall Manager				
Policies	41	N/A	$100.00	**$4,100.00**
AWS WAF web ACL	11	150	$5.00	**$8,250.00**
AWS WAF rules	4 x 11	150	$1.00	**$6,600.00**

Components	Quantity	Accounts	$/month [USD]	Monthly Total [USD]
* Other AWS services*				
Other*	N/A	150	less than $1.00	**$1.00**
			Total:	**$18,951.00**
*Other AWS services include Lambda, Amazon SNS EventBridge, CloudFormation StackSets, AWS Config, Route 53 Resolver DNS Firewall, Parameter Store, X-Ray, DynamoDB, and Amazon S3.				

Cost per month for a large organization - Automations for Shield Advanced

Assumptions:

- Includes all costs for a small organization deploying the automations for Shield Advanced templates.
- Costs for AWS WAF protection policies, web ACLs, and rules are included in a Shield Advanced subscription, so they are excluded from this calculation. For additional information, refer to Firewall Manager pricing.
- Accounts: 150 accounts
- Number of AWS Regions: 1

- Subscription to Shield Advanced: Yes
- Number of regional Shield Advanced protections: 200
- Number of global Shield Advanced protections: 5

Cost details:

- AWS Config continuous recording: Enabled for Shield Advanced protections
  - Configuration items (*$0.003 per configuration item x 205 Shield Advanced protections x 2 configuration changes*)
  - AWS Config rule evaluations (*$0.001 per rule evaluation x 205 Shield Advanced protections x 2 configuration changes*)
- Route 53 health checks (*$0.50 per health check per month x 3 health checks x 205 Shield Advanced protections*)
- CloudWatch metric alarms (*$0.10 per alarm metric x 205 Shield Advanced protections x 2 metric alarms*)
- Lambda:
  - Function requests (*$0.20 per 1M requests x (410 configuration item evaluations + 205 remediations + 30 time-based evaluations)*)
  - Function duration (*$0.0000000167 per 1 ms x 150,000 ms x 645 invocations*)

> **Note**
>
> The following cost estimate only accounts for AWS Config continuous recording costs related to Shield Advanced resource types. These costs might vary depending on the type of recording enabled and the resources being recorded by AWS Config in your accounts. For additional information, refer to the AWS Config pricing page.

Components	Quantity	Pricing [USD]	Monthly Total [USD]
AWS Config			
Configuration items	205	$0.003 per configuration item delivered	**$0.23**

Components	Quantity	Pricing [USD]	Monthly Total [USD]
AWS Config rule evaluations	410	$0.001 per rule evaluation	**$0.41**
Route 53			
Health checks	615	$0.50 per health check per month	**$307.50**
CloudWatch			
Metric alarms	410	$0.10 per alarm metric per month	**$41.00**
Amazon SQS			
FIFO queue	1	First 1 million requests/month are free $0.50 per million requests thereafter	AWS Free Tier
Lambda			
Function duration	150,000 ms	$0.0000000167 per 1 ms	**$1.62**
Function requests	645	$0.20 per 1M requests	AWS Free Tier
X-Ray			
Tracing	~650 traces recorded with default 5% sampling rate	$0.000005 per trace	**< $ 0.01**
		Total	**$351.76**

Security

When you build systems on AWS infrastructure, security responsibilities are shared between you and AWS. This shared responsibility model reduces your operational burden because AWS operates, manages, and controls the components, including the host operating system, the virtualization layer, and the physical security of the facilities in which the services operate. For more information about AWS security, visit AWS Cloud Security.

IAM roles

AWS Identity and Access Management (IAM) roles allow customers to assign granular access policies and permissions to services and users on the AWS Cloud. This solution creates IAM roles that grant the solution's Lambda functions access to create Regional resources. If you choose to deploy the automations for Shield Advanced, the solution creates additional IAM roles to allow the solution's Lambda functions to assume roles in other accounts within your AWS Organization. These roles grant the Lambda functions access to modify Shield Advanced protections, create Route 53 health checks, and create CloudWatch metric alarms.

Permissions required by the Prerequisite stack

The appropriate IAM permissions are required to fulfill the prerequisites. These permissions include allowing trusted access for AWS services with AWS Organizations, creating and deleting stack set instances to configure AWS Config in member accounts, configuring the Firewall Manager admin, and recording Lambda events in CloudWatch Logs.

Permissions required by the Primary stack

The following IAM permissions are required for the solution to automatically maintain Firewall Manager security policies:

- Creating and deleting Firewall Manager policies for AWS WAF, Shield, VPC Security Groups, and DNS Firewall
- Reading and writing DynamoDB tables with policy metadata
- Reading Systems Manager parameter information
- Recording Lambda events in CloudWatch Logs
- Publishing to the solution's Amazon SNS topic
- Reading and writing to X-Ray

Additionally, the `ComplianceGenerator` Lambda function needs permission to describe all Firewall Manager policies, generate compliance reports, and upload them in an S3 bucket.

Permissions required by the Automations for Shield Advanced Prerequisite stack

The appropriate IAM permissions are required to enable Shield Advanced health-based detection. These permissions are deployed to member accounts in your AWS Organization and include:

- Creating and deleting Route 53 health checks
- Creating and deleting CloudWatch metric alarms
- Modifying Shield Advanced protections
- Reading and writing evaluations in AWS Config

Permissions required by the Automations for Shield Advanced stacks

The appropriate IAM permissions are required for the solution to enable Shield Advanced health-based detection across an AWS Organization. These permissions include:

- Assuming the cross-account IAM role created by the `aws-fms-shield-automations-prereq` stack in your AWS Organization's member accounts
- Reading and writing to the solution's Amazon SQS queue
- Publishing to the solution's Amazon SNS topic
- Retrieving the state of your account's Shield Advanced subscription
- Reading and writing to X-Ray

Additionally, the `aws-fms-proactive-event-response` stack deploys an IAM role with service-managed permissions if you choose to grant permissions for the SRT to access accounts in your AWS Organization. These permissions are required to enable SRT support. For more information see the AWSShieldDRTAccessPolicy.

AWS Systems Manager Parameter Store

This solution uses Parameter Store to initiate create, read, update, and delete (CRUD) operations to the Firewall Manager policies. Systems Manager parameters created by this solution must be secured. Access should only be granted to a specific principal or user. An unexpected user that has access to these parameters can cause undesirable Firewall Manager policy operations, such

as deleting policies. Such operations could be initiated across several member accounts in AWS Organizations.

By default, an IAM user or role must be explicitly authorized to perform an action on the Systems Manager parameters created by the solution. Unless a user receives explicit permission to access these Systems Manager parameters, changes cannot be made to update Firewall Manager security policies. Additionally, you can use *explicit deny* to prevent further access to these resources as shown in the following example policy. This example policy can be assigned to users to prevent access to the DynamoDB table and Systems Manager parameters resources.

```
{
 "Version": "2012-10-17",
 "Statement": [{
 "Action": [
 "dynamodb:*"
 ],
 "Resource": "arn:aws:dynamodb:<region>:<account-id>:table/<table-name>",
 "Effect": "Deny",
 "Sid": "FMSDDBSecure"
 },
 {
 "Action": "ssm:*"
 "Resource": [
 "arn:aws:ssm:<region>:<account-id>:parameter/FMS/OUs",
 "arn:aws:ssm:<region>:<account-id>:parameter/FMS/Regions",
 "arn:aws:ssm:<region>:<account-id>:parameter/FMS/Tags"
 ],
 "Effect": "Deny",
 "Sid": "FMSSSMSecure"
 }
 ]
}
```

Quotas

Service quotas, also referred to as limits, are the maximum number of service resources or operations for your AWS account.

Quotas for AWS services in this solution

Make sure you have sufficient quotas for each of the services implemented in this solution. For more information, see AWS service quotas.

Use the following links to go to the page for that service. To view the service quotas for all AWS services in the documentation without switching pages, view the information in the Service endpoints and quotas page in the PDF instead.

AWS CloudFormation quotas

Your AWS account has AWS CloudFormation quotas that you should be aware of when launching the stack in this solution. By understanding these quotas, you can avoid limitation errors that would prevent you from deploying this solution successfully. For more information, see AWS CloudFormation quotas in the in the *AWS CloudFormation User's Guide*.

Deploy the solution

This solution uses AWS CloudFormation templates and stacks to automate its deployment. The CloudFormation template specifies the AWS resources included in this solution and their properties. The CloudFormation stack provisions the resources that are described in the template.

Deployment process overview

Follow the step-by-step instructions in this section to configure and deploy the solution into your account.

Before you launch the solution, review the cost, architecture, network security, and other considerations discussed earlier in this guide.

Time to deploy: Approximately ten minutes

Step 1: (Optional) Install the prerequisite template

Step 2. Launch the Primary stack

Step 3: Add and manage Firewall Manager policies

Step 4: (Optional) Install the Shield Advanced Automations Prerequisite template

Step 5: (Optional) Launch the Shield Advanced Automations stack

Step 6: (Optional) Launch the Proactive Event Response stack

Important

This solution includes an option to send anonymized operational metrics to AWS. We use this data to better understand how customers use this solution and related services and products. AWS owns the data gathered through this survey. Data collection is subject to the AWS Privacy Notice.

To opt out of this feature, download the template, modify the AWS CloudFormation mapping section, and then use the AWS CloudFormation console to upload your updated template and deploy the solution. For more information, see the Anonymized data collection section of this guide.

AWS CloudFormation templates

You can download the CloudFormation templates for this solution before deploying them.

> **Note**
>
> AWS CloudFormation resources are created from AWS CDK constructs.
> If you have previously deployed this solution, see Update the solution for update instructions.

The following tables compares the CloudFormation templates. **Main stacks** table to see the Prerequisite stack and the Primary stack. **Optional stacks with Shield Advanced automations** table to see the Shield Advanced Automations Prerequisite stack, Shield Advanced Automations stack, and Proactive Event Response stack.

Main stacks

Stack name	What to use it for	Where to deploy	How to deploy
(Optional) Prerequisite stack: `aws-fms-prereq.template` View template	Use this template to install the prerequisites necessary for the Primary stack. These include setting up a Firewall Manager administrator account, enabling AWS Config, and enabling AWS Organizations with all features.	Deploy once, in a single Region. Deploy into your AWS Organization's management account. If you have delegated an account other than your AWS Organization's management account as the Firewall Manager admin, deploy into that delegated Firewall Manager admin account.	CloudFormation stack

Stack name	What to use it for	Where to deploy	How to deploy
Primary stack: `aws-fms-automations.template` View template	Use this template to launch the Automations for AWS Firewall Manager solution. The default configuration deploys the core and supporting services, and you can customize the template to meet your specific needs.	Deploy once, in a single Region. Deploy into your AWS Organization's management account. If you have delegated an account other than your AWS Organization's management account as the Firewall Manager admin, deploy into that delegated Firewall Manager admin account.	CloudFormation stack

Optional stacks with Shield Advanced Automations

Stack name	What to use it for	Where to deploy	How to deploy
(Optional) Shield Advanced Automations Prerequisite stack: `aws-fms-shield-automations-prereq.template` View template	Use this template to install the prerequisites necessary for the Shield Advanced Automations stack. This stack deploys the IAM roles necessary for Lambda functions in the Shield Advanced Automations stack to create Route 53 health checks, set up	Deploy into either your AWS Organization's management account or an account you have delegated as an admin for CloudFormation StackSets. The stack must be deployed to all member accounts in the Organization as a service-managed StackSet. The	StackSet with service-managed permissions (recommended - deploys to all accounts in your AWS Organization) CloudFormation Stack (optional - deploys only to specific account)

Stack name	What to use it for	Where to deploy	How to deploy
	CloudWatch metric alarms, and modify Shield Advanced protections.	stack should only be deployed in a single Region. Deploy to the same Region where you plan to deploy the Shield Advanced Automations stack. **Note** When deploying to the entire AWS Organization, the organization management account is not included. If you want to enable Shield Advanced health-based detection or proactive engagement in your management account, deploy to	

Stack name	What to use it for	Where to deploy	How to deploy
		this account separately.	
(Optional) Shield Advanced Automations stack: `aws-fms-shield-automations.template` View template	Use this template to launch the Shield Advanced Automations stack. This stack enables Shield Advanced health-based detection across your AWS Organization. This stack deploys two Lambda functions, an Amazon SQS queue, and an AWS Config organization rule.	Deploy into either your AWS Organization's management account or an account you have delegated as an admin for AWS Config. We recommend setting up a delegated admin for AWS Config. For more information, refer to Set up an organization-wide aggregator in AWS Config using a delegated administrator account, omitting the steps to setup an aggregator. You can deploy this stack in any supported Region where you have Shield Advanced protections set up.	CloudFormation stack

Stack name	What to use it for	Where to deploy	How to deploy
(Optional) Proactive Event Response stack: `aws-fms-proactive-event-response.template` View template	Use this template to launch the Proactive Event Response stack. This stack enables Shield Advanced proactive engagement in each account where it is deployed. It also provides the option to grant the SRT permissions to act on your behalf.	Deploy in a single Region, for each account where you want to enable proactive engagement. **Note** When deploying to the entire AWS Organization, the organization management account is not included. If you want to enable Shield Advanced health-based detection or proactive engagement in your management account, deploy to this account separately.	StackSet with service-managed permissions (recommended - deploys to all accounts in your AWS Organization) CloudFormation Stack (optional - deploys only to specific account)

Prerequisites for Automations for AWS Firewall Manager

This section describes the prerequisites you must meet before launching each stack.

> **Important**
>
> To deploy the automations for Shield Advanced CloudFormation templates, you must already be subscribed to Shield Advanced. All accounts in your AWS Organization where you wish to enable health-based detection or proactive event response must also be subscribed to Shield Advanced, in addition to the account where the stacks are deployed.

If you don't have Firewall Manager configured in your AWS Organizations primary account, then you must deploy the solution's prerequisite template first. Deploy this template in the AWS Organizations management account with the AWS Organizations all features option activated prior to deploying the template.

For more information, refer to Step 1: (Optional) Install the Prerequisite template.

Prerequisites for the Shield Advanced Automations stack

Before deploying the `aws-fms-shield-automations` CloudFormation template, you must first do the following:

1. Subscribe all accounts in your AWS Organization, to which you deploy the stack, to Shield Advanced.
2. Deploy the Shield Advanced Automations Prerequisite template (`aws-fms-shield-automations-prereq.template`). We recommend deploying this prerequisite template to all member accounts in your AWS Organization by using CloudFormation service-managed StackSets.
3. Enable AWS Config recording for AWS::Shield::Protection and AWS::ShieldRegional::Protection resource types in all accounts in your AWS Organization where you want to enable Shield Advanced health-based detection.

Prerequisites for the Proactive Event Response stack

Before deploying the `aws-fms-proactive-event-response` CloudFormation template, you must first do the following:

1. Subscribe all accounts in your AWS Organization, to which you deploy the stack, to the following:
   a. Either the Business Support plan or the Enterprise Support plan
   b. Shield Advanced
2. Associate a Route 53 health check with any resource that you want to protect with proactive engagement. For more information on configuring proactive event response, refer to Setting up proactive engagement for the SRT to contact you directly in the *AWS WAF, AWS Firewall Manager, and AWS Shield Advanced Developer Guide*.

You don't need to deploy a prerequisite template prior to deploying the `aws-fms-proactive-event-response` template.

Service-managed StackSets

Before deploying stacks using service-managed StackSets, you must first do the following:

1. Enable all features in AWS Organizations
2. Activate trusted access with AWS Organizations

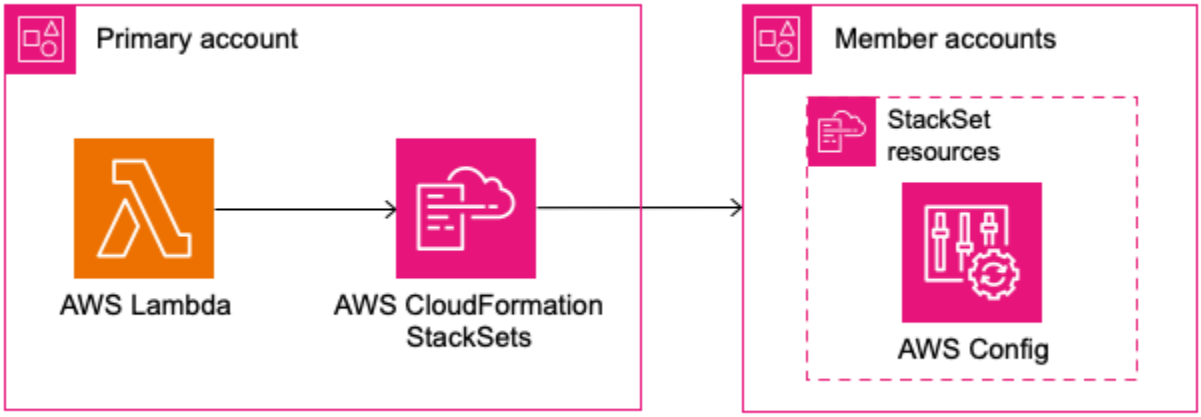
These actions can only be performed by an account administrator in your organization's management account. For more information, refer to Activate trusted access for stack sets with Organizations in the *AWS CloudFormation User Guide*.

Step 1: (Optional) Launch the Prerequisite template

> **Important**
>
> If Firewall Manager is already configured in your AWS Organizations management account, proceed to Step 2: Launch the Primary stack. Otherwise, if you want to use this template to enable AWS Config, you can enter the account ID you have designated as the Firewall Manager admin.

Installing the Firewall Manager prerequisite template in an AWS Organizations primary account with the default parameters builds the following environment in the AWS Cloud.

Architecture: Prerequisites



When the template is deployed in an AWS Organizations primary account, a Lambda function checks for the following prerequisites:

1. The **AWS Organizations All Features** function is activated.
2. The AWS Firewall Manager admin is configured.
3. Optional: AWS Config is activated.

> **Note**
>
> This check is done when you activate AWS Config (set to `Yes`) during deployment of the prerequisite template. See Step 1a: Launch the prerequisite stack for more information.

The Lambda function installs the prerequisites. If there are errors during prerequisite installation, a stack rollback occurs with an error message.

Step 1a. Launch the prerequisite stack

This automated AWS CloudFormation template deploys the Firewall Manager prerequisite template in the AWS Cloud.

View template

aws-fms-prereq.template - Use this template to launch the solution prerequisite template. The

default configuration deploys Lambda functions, CloudFormation StackSets, and AWS Config resources.

> **Note**
>
> You are responsible for the cost of the AWS services used while running this solution. For more details, visit the Cost section in this guide, and refer to the pricing webpage for each AWS service used in this solution.

1. Sign in to the AWS Management Console and select the button to launch the `aws-fms-prereq.template` CloudFormation template.

   Launch solution

2. The template launches in the US East (N. Virginia) Region by default. To launch the solution in a different AWS Region, use the Region selector in the console navigation bar.

   > **Note**
   >
   > Although AWS Organizations and Firewall Manager are available globally, both AWS services use the US East (N. Virginia) Region as their data plane. See Supported AWS Regions for more information.

3. On the **Create stack** page, verify that the correct template URL is in the **Amazon S3 URL** text box and choose **Next**.
4. On the **Specify stack details** page, assign a name to your solution stack. For information about naming character limitations, see IAM and AWS STS quotas, name requirements, and character limits in the *AWS Identity and Access Management User Guide*.
5. Under **Parameters**, review the parameters for this solution template and modify them as necessary. This solution uses the following default values.

Parameter	Default	Description
FMS Admin Account ID	*<Requires input>*	Add your Firewall Manager service admin account ID, if you have already configure

Parameter	Default	Description
		d your Firewall Manager admin account. Otherwise , specify an AWS Organizat ions member account ID that you want as designate d Firewall Manager admin account.
Enable Config	`Yes`	Activate AWS Config across the organization for the resources required by Firewall Manager. If you already have AWS Config activated, select No.

6. Choose **Next**.
7. On the **Configure stack options** page, choose **Next**.
8. On the **Review and create** page, review and confirm the settings. Select the box acknowledging that the template will create IAM resources.
9. Choose **Submit** to deploy the stack.

   You can view the status of the stack in the AWS CloudFormation Console in the **Status** column. You should receive a CREATE_COMPLETE status in approximately 10 minutes.

> **Note**
>
> When installing the prerequisite template, you have the option to designate a separate account in your organization as the Firewall Manager administrator account. If you select this option, you must manually install the `aws-fms-automations` template in the designated account after installing the prerequisite template in your AWS Organizations management account.

Step 1b. Manually activate AWS Firewall Manager (optional)

Use the following procedure to activate AWS Firewall Manager in AWS Organizations.

1. Activate **AWS Organizations All Features**.
2. Activate **AWS Config** on all Organizations member accounts.
3. Designate a member account as **Firewall Manager Admin**.

For additional information to enable Firewall Manager, refer to AWS Firewall Manager prerequisites in the *AWS WAF, AWS Firewall Manager, and AWS Shield Advanced Developer Guide*.

Step 2: Launch the Primary stack

Follow the step-by-step instructions in this section to configure and deploy the solution into your account.

Time to deploy: Approximately three minutes

1. Sign in to the AWS Management Console and select the button to launch the `aws-fms-automations.template` CloudFormation template.

   Launch solution

2. The template launches in the US East (N. Virginia) Region by default. To launch the solution in a different AWS Region, use the Region selector in the console navigation bar.

   > **Note**
   >
   > Although AWS Organizations and Firewall Manager are available globally, both AWS services use the US East (N. Virginia) Region as their data plane. See Supported AWS Regions for more information.

3. On the **Create stack** page, verify that the correct template URL is in the **Amazon S3 URL** text box and choose **Next**.
4. On the **Specify stack details** page, assign a name to your solution stack. For information about naming character limitations, see IAM and AWS STS quotas, name requirements, and character limits in the *AWS Identity and Access Management User Guide*.

5. Under **Parameters**, review the parameters for this solution template and modify them as necessary. This solution uses the following default values.

Parameter	Default	Description
Email Address	*<Requires input>*	Enter an email address where you want to receive notifications regarding problems that cannot be resolved without manual intervention. If you don't want to receive notifications, leave this parameter blank.
Compliance Reporting	Yes	Choose Yes or No based on your preference for generating compliance reports for your Firewall Manager security policies.

6. Select **Next**.
7. On the **Configure stack options** page, choose **Next**.
8. On the **Review** page, review and confirm the settings. Select the boxes acknowledging that the template will create IAM resources and an auto-expand capability.
9. Choose **Create stack** to deploy the stack.

   You can view the status of the stack in the AWS CloudFormation console in the **Status** column. You should receive a CREATE_COMPLETE status in approximately three minutes.

> **Note**
>
> In addition to the primary Lambda functions, this solution includes the `solution-helper` Lambda function, which runs only during initial configuration or when resources are updated or deleted.

When you run this solution, you will notice both Lambda functions in the AWS console. Only the primary functions are regularly active. However, you must not delete the `solution-helper` function, as it is necessary to manage associated resources.

Step 3: Add and manage Firewall Manager policies

You can add Firewall Manager policies across multiple OUs and Regions for your business needs. Using Systems Manager parameters, you can manage Regions and OUs where the policies get created or deleted, and you can manage the resources under scope using the **Tag** parameter. Use the following procedure to update each parameter:

1. Sign in to the AWS Systems Manager console.
2. On navigation menu, under **Application Management**, select **Parameter Store**.
3. Select the parameter to update and choose **Edit**.
4. Update the value.
5. Choose **Save changes**.

You can update these parameters at any time and as many times as needed to meet your use cases and preferences for setting up your OUs, Regions, and tags. These parameters have the following format:

- `/FMS/<PolicyID>/OUs: <StringList>`
- `/FMS/<PolicyID>/Regions: <StringList>`
- `/FMS/<PolicyID>/Tags: <String>`

For examples on updating these parameters, refer to Scenarios for setting up the Systems Manager parameters.

Access the Systems Manager Parameter Store history

Use the following steps to identify the person that invoked a change to the parameters in Parameter Store:

1. Sign in to the AWS Systems Manager console.

2. On the navigation menu, under **Application Management**, select **Parameter Store**.
3. Select the parameter and choose **View Details**.
4. Choose **History**.

> **Note**
>
> If you want to customize the default policies or want different policies being applied to different OUs and Regions, refer to the Customization guide. This section describes how you can use `aws-fms-policy.template` to apply a different set of policies to different OUs or Regions.

Step 4: (Optional) Launch the Shield Advanced Automations Prerequisite stack

> **Important**
>
> Before launching the Shield Advanced Automations Prerequisite stack as a service-managed StackSet, you must first enable trusted access with AWS Organizations. For more information, refer to Activate trusted access for stack sets with Organizations in the *AWS CloudFormation User Guide*.

Follow the step-by-step instructions in this section to configure and deploy the Shield Advanced Automations Prerequisite template into your account. This template is deployed as a service-managed StackSet to member accounts in your AWS Organization.

Time to deploy: Approximately five minutes

1. Sign in to the AWS Management Console and select the button to launch the `aws-fms-shield-automations-prereq.template` CloudFormation template. Since this template is deployed as a service-managed StackSet, you must sign in using the Organization's management account or a delegated administrator account in your AWS Organization.

   Launch solution

2. On the **Choose a template** page, verify that the correct template URL is in the **Amazon S3 URL** text box. Choose **Next**.
3. On the **Specify StackSet details** page, assign a name to your solution StackSet. For information about naming character limitations, see IAM and AWS STS quotas in the *AWS Identity and Access Management User Guide*.
4. Select **Next**.
5. On the **Configure StackSet options** page, choose your preferred execution configuration, then choose **Next**.
6. On the **Set deployment options** page under **Add stacks to stack set,** choose **Deploy new stacks**.
7. Under **Deployment targets**, choose where you would like to deploy the StackSet. We recommend choosing **Deploy to organization** if you want to enable Shield Advanced health-based detection across your AWS Organization.
8. Under **Auto-deployment options**, choose how you would like to handle automatic deployments. We recommend choosing **Activated** for **Automatic Deployment** and **Delete stacks** for **Account removal behavior**.
9. Under **Specify regions**, choose the Region where you would like to deploy the StackSet. You must deploy in the same Region where you plan to deploy the Shield Advanced Automations stack. We recommend deploying in a single Region to start.
10. Under **Deployment options**, choose your preferred deployment concurrency. We recommend keeping the default settings, which restrict deployment to a single concurrent account with strict failure tolerance.
11. Select **Next**.
12. On the **Review** page, review and confirm the settings. Select the boxes acknowledging that the template creates IAM resources.
13. Choose **Create stack** to deploy the stack.

You can view the status of the StackSet in the AWS CloudFormation console on the **StackSets** page. You should receive a CREATE_COMPLETE status in approximately five minutes, depending on how many accounts the StackSet is deployed to.

Note

In addition to the primary Lambda functions, this solution includes the `solution-helper` Lambda function, which runs only during initial configuration or when resources are updated or deleted.
When you run this solution, you will notice both Lambda functions in the AWS Management Console. Only the primary functions are regularly active. However, you must not delete the `solution-helper` function, as it is necessary to manage associated resources.

Step 5: (Optional) Launch the Shield Advanced Automations stack

Important

Before deploying the Shield Advanced Automations stack, ensure that you have enabled AWS Config recording for `AWS::Shield::Protection` and `AWS::ShieldRegional::Protection` resource types for all accounts in your AWS Organization where you want to enable Shield Advanced health-based detection. For more information, see Region support for the Shield Advanced Automations stack.

Follow the step-by-step instructions in this section to configure and deploy the Shield Advanced Automations stack into your account.

Time to deploy: Approximately 15 minutes

1. Sign in to the AWS Management Console and select the button to launch the `aws-fms-shield-automations.template` CloudFormation template. You must deploy this template from your AWS Organizations management account or a delegated admin for AWS Config. We recommend registering a member account in your organization as a delegated admin for AWS Config.

   Launch solution

2. The template launches in the US East (N. Virginia) Region by default. To launch the solution in a different AWS Region, use the Region selector in the console navigation bar.
3. On the **Create stack** page, verify that the correct template URL is in the **Amazon S3 URL** text box. Choose **Next**.
4. On the **Specify stack details** page, assign a name to your solution stack. For information about naming character limitations, see IAM and AWS STS quotas in the *AWS Identity and Access Management User Guide*.
5. Under **Parameters**, review the parameters for this solution template and modify them as necessary. This solution uses the following default values.

Parameter	Required	Default	Description
Email Address	No	N/A	The email address where you want to receive notifications regarding problems that can't be resolved without manual intervention.
Excluded Accounts	No	N/A	A comma delimited list of accounts that you want to exclude from having health-based detection enabled. We recommend adding your AWS Organization's management account ID unless you have deployed the Shield Advanced Automations Prerequisite stack to

Parameter	Required	Default	Description
			your management account directly.
CloudWatch metric configurations for Elastic IPs			
CPUUtilization Metric Threshold	Yes	`85`	Threshold for the CPUUtilization CloudWatch metric used to monitor the health of EC2 instances attached to your Shieldpro tected Elastic IP addresses.
CPUUtilization Metric Statistic	Yes	`Average`	Statistic for the CPUUtilization CloudWatch metric used to monitor the health of EC2 instances attached to your Shield-pr otected Elastic IP addresses.
NetworkIn Metric Threshold	Yes	`1000`	Threshold for the NetworkIn CloudWatch metric used to monitor the health of EC2 instances attached to your Shield-pr otected Elastic IP addresses.

Parameter	Required	Default	Description
NetworkIn Metric Statistic	Yes	`Sum`	Statistic for the NetworkIn CloudWatch metric used to monitor the health of EC2 instances attached to your Shield-protected Elastic IP addresses.
CloudWatch metric configurations for Network Load Balancers			
ActiveFlowCount Metric Threshold	Yes	`1000`	Threshold for the ActiveFlowCount CloudWatch metric used to monitor the health of Network Load Balancers attached to your Shield-protected Elastic IP addresses.
ActiveFlowCount Metric Statistic	Yes	`Average`	Statistic for the ActiveFlowCount CloudWatch metric used to monitor the health of Network Load Balancers attached to your Shield-protected Elastic IP addresses.

Parameter	Required	Default	Description
NewFlowCount Metric Threshold	Yes	`1000`	Threshold for the NewFlowCount CloudWatch metric used to monitor the health of Network Load Balancers attached to your Shield-protected Elastic IP addresses.
NewFlowCount Metric Statistic	Yes	`Sum`	Statistic for the NewFlowCount CloudWatch metric used to monitor the health of Network Load Balancers attached to your Shield-protected Elastic IP addresses.
CloudWatch metric configurations for Elastic Load Balancing			
HTTPCode_ ELB_4XX_Count Metric Threshold	Yes	`1000`	Threshold for the HTTPCode_ ELB_4XX_Count CloudWatch metric used to monitor the health of Shield-pr otected Elastic Load Balancing.

Parameter	Required	Default	Description
HTTPCode_ ELB_4XX_Count Metric Statistic	Yes	Sum	Statistic for the HTTPCode_ ELB_4XX_Count CloudWatch metric used to monitor the health of Shield-pr otected Elastic Load Balancing.
HTTPCode_ ELB_5XX_Count Metric Threshold	Yes	1000	Threshold for the HTTPCode_ ELB_5XX_Count CloudWatch metric used to monitor the health of Shield-pr otected Elastic Load Balancing.
HTTPCode_ ELB_5XX_Count Metric Statistic	Yes	Sum	Statistic for the HTTPCode_ ELB_5XX_Count CloudWatch metric used to monitor the health of Shield-pr otected Elastic Load Balancing.
CloudWatch metric configurations for CloudFront distribut ions			

Parameter	Required	Default	Description
4xxErrorRate Metric Threshold	Yes	`0.05`	Threshold for the 4xxErrorRate CloudWatch metric used to monitor the health of Shield-protected CloudFront distributions.
4xxErrorRate Metric Statistic	Yes	`Average`	Statistic for the 4xxErrorRate CloudWatch metric used to monitor the health of Shield-protected CloudFront distributions.
5xxErrorRate Metric Threshold	Yes	`0.05`	Threshold for the 5xxErrorRate CloudWatch metric used to monitor the health of Shield-protected CloudFront distributions.
5xxErrorRate Metric Statistic	Yes	`Average`	Statistic for the 5xxErrorRate CloudWatch metric used to monitor the health of Shield-protected CloudFront distributions.

6. Select **Next**.
7. On the **Configure stack options** page, choose **Next**.

8. On the **Review** page, review and confirm the settings. Select the boxes acknowledging that the template creates IAM resources.
9. Choose **Create stack** to deploy the stack.

You can view the status of the stack in the AWS CloudFormation console in the **Status** column. You should receive a CREATE_COMPLETE status in approximately three minutes.

> **Note**
>
> In addition to the primary Lambda functions, this solution includes the `solution-helper` Lambda function, which runs only during initial configuration or when resources are updated or deleted.
> When you run this solution, you will notice both Lambda functions in the AWS Management Console. Only the primary functions are regularly active. However, you must not delete the `solution-helper` function, as it is necessary to manage associated resources.

Step 6: (Optional) Launch the Proactive Event Response stack

> **Important**
>
> Before launching the Proactive Event Response stack as a service-managed StackSet, you must first enable trusted access with AWS Organizations. For more information, refer to Activate trusted access for stack sets with Organizations in the *AWS CloudFormation User Guide*.

Follow the step-by-step instructions in this section to configure and deploy the Shield Automations prerequisite template into your account. This template is deployed as a service-managed StackSet to member accounts in your AWS Organization.

Time to deploy: Approximately five minutes

1. Sign in to the AWS Management Console and select the button to launch the `aws-fms-proactive-event-response.template` CloudFormation template. Since this template

is deployed as a service-managed StackSet, you must sign in using the Organization's management account or a delegated administrator account in your AWS Organization.

Launch solution

2. On the **Choose a template** page, verify that the correct template URL is in the **Amazon S3 URL** text box. Choose **Next**.
3. On the **Specify StackSet details** page, assign a name to your solution StackSet. For information about naming character limitations, see IAM and AWS STS quotas in the *AWS Identity and Access Management User Guide*.
4. Under **Parameters**, review the parameters for this solution template and modify them as necessary. This solution uses the following default values.

Parameter	Required	Default	Description
Emergency Contact Phone Number	Yes	N/A	The phone number where you want the SRT to contact you in case of emergencies.
Emergency Contact Email Address	Yes	N/A	The email address where you want the SRT to contact you in case of emergencies.
Grant SRT (Shield Response Team) Account Access	Yes	No	Choose if you would like to grant the SRT access to accounts where this stack is deployed. This allows the SRT to make Shield Advanced and AWS WAF API calls on your behalf and to

Parameter	Required	Default	Description
			access your AWS WAF logs. For more informati on, see Granting access for the SRT in the *AWS WAF, AWS Firewall Manager, and AWS Shield Advanced Developer Guide*.

5. Select **Next**.
6. On the **Configure StackSet options** page, choose your preferred execution configuration, then choose **Next**.
7. On the **Set deployment options** page under **Add stacks to stack set**, choose **Deploy new stacks**.
8. Under **Deployment targets**, choose where you want to deploy the StackSet. We recommend choosing **Deploy to organization** if you want to enable Shield Advanced proactive engagement across your AWS Organization.

> **Important**
>
> All accounts where you choose to deploy the stack must be subscribed to either the Business Support plan or the Enterprise Support plan, in addition to Shield Advanced. For more information, refer to Setting up proactive engagement for the SRT to contact you directly in the *AWS WAF, AWS Firewall Manager, and AWS Shield Advanced Developer Guide*.

9. Under **Auto-deployment options**, choose how you would like to handle automatic deployments. We recommend choosing **Deactivated** for **Automatic Deployment** and **Delete stacks** for **Account removal behavior**.
10. Under **Specify regions**, choose the Region where you want to deploy the StackSet. You should only deploy the stack in a single Region. This activates the proactive engagement feature globally.

11. Under **Deployment options**, choose your preferred deployment concurrency. We recommend keeping the default settings which restrict deployment to a single concurrent account with strict failure tolerance.
12. Select **Next**.
13. On the **Review** page, review and confirm the settings. Select the boxes acknowledging that the template creates IAM resources.
14. Choose **Create stack** to deploy the stack.

You can view the status of the StackSet in the AWS CloudFormation console on the **StackSets** page. You should receive a CREATE_COMPLETE status in approximately five minutes, depending on how many accounts the StackSet is deployed to.

> **Note**
>
> In addition to the primary Lambda functions, this solution includes the `solution-helper` Lambda function, which runs only during initial configuration or when resources are updated or deleted.
> When you run this solution, you will notice both Lambda functions in the AWS Management Console. Only the primary functions are regularly active. However, you must not delete the `solution-helper` function, as it is necessary to manage associated resources.

Update the solution

If you have previously deployed the solution, follow this procedure to update the solution's Primary CloudFormation stack to get the latest version of the solution's framework.

1. Sign in to the AWS CloudFormation console, select your existing Automations for AWS Firewall Manager CloudFormation stack, and select **Update**.
2. Select **Replace current template**.
3. Under **Specify template**:
   a. Select **Amazon S3 URL**.
   b. Copy the link of the latest template.
   c. Paste the link in the **Amazon S3 URL** box.
   d. Verify that the correct template URL shows in the **Amazon S3 URL** text box, and choose **Next**. Choose **Next** again.
4. Under **Parameters**, review the parameters for the template and modify them as necessary. For details about the parameters, see Step 2: Launch the Primary stack.
5. Choose **Next**.
6. On the **Configure stack options** page, choose **Next**.
7. On the **Review** page, review and confirm the settings. Select the box acknowledging that the template creates IAM resources.
8. Choose **View change set** and verify the changes.
9. Choose **Update stack** to deploy the stack.

You can view the status of the stack in the AWS CloudFormation console in the **Status** column. You should receive a UPDATE_COMPLETE status in approximately three minutes.

Review updated default security policies

If you have previously deployed the solution, we recommend reviewing changes made to the default Firewall Manager security policies deployed by the solution.

> **Note**
>
> Updating the CloudFormation stack doesn't update the policies in the S3 bucket created by the solution. To update the policies, you must manually retrieve, modify, and re-upload the `policy_manifest.json` file with your desired configurations.

To update the default Firewall Manager security policies, follow these steps:

1. Sign in to the Amazon S3 console.
2. Choose the *<Stack-Name>*-*<xx>*-policymanifestbucket-*<xx>* S3 bucket.
3. Choose the `policy_manifest.json` file in the bucket.
4. Download the manifest file.
5. Review updates made to the default security policies in the solution's GitHub repository. If you want to apply updates to your own policies, copy and paste them into your `policy_manifest.json` file.
6. Upload the modified manifest file in the same S3 bucket.
7. The Firewall Manager policies automatically update to reflect the changes made in Step 5.

Troubleshooting

This section provides troubleshooting instructions when deploying the solution.

Before addressing the following common errors, you can adjust the level of detail in the CloudWatch Logs. For more details, refer to Amazon CloudWatch logs insights.

The AWS Config errors and Other errors resolution sections provide instructions to mitigate known errors. If these instructions don't address your issue, Contact Support provides instructions for opening an Support case for this solution.

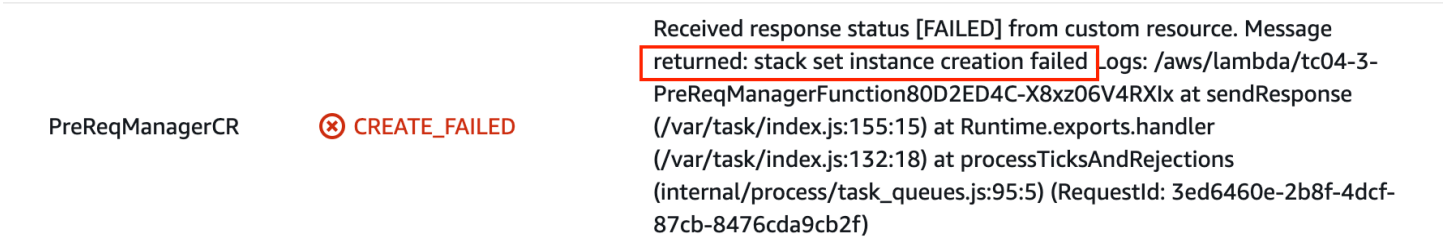
AWS Config errors

This section addresses known errors with AWS Config when deploying or using this solution.

Problem: Enabling AWS Config in the prerequisite stack doesn't work

The following error occurs when you deploy solution's `aws-fms-prereq.template` CloudFormation template with the **Enable Config** parameter set to `Yes`.

Screenshot showing CREATE_FAILED status with error message returned:stack set instance creation failed.

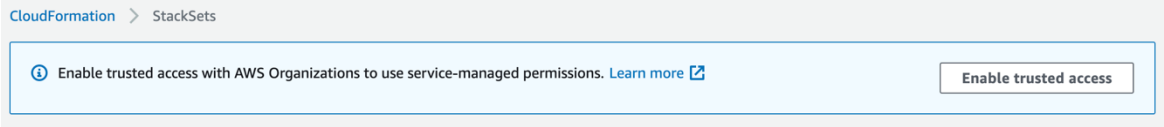


Reason: Trusted access for CloudFormation StackSets can **only** be enabled using the AWS CloudFormation console. Refer to Enabling trusted access with AWS CloudFormation Stacksets in the *AWS Organizations User Guide*.

Resolution

1. Sign in to the AWS CloudFormation console.
2. From the navigation menu, choose **StackSets**.
3. Choose **Activate trusted access**. Providing a registered delegated administrator is optional.

CloudFormation StackSets message: Activate trusted access with AWS Organizations to use service-managed permissions.



4. Deploy the `aws-fms-prereq.template` again.

Problem: Activating AWS Config using CloudFormation StackSets fails when creating the configuration recorder

The following error occurs in the StackSets console:

Example error text with ResourceStatusReason:Failed to put configuration recorder.

ResourceLogicalId:ConfigRecorder, ResourceType:AWS::Config::ConfigurationRecorder, ResourceStatusReason:Failed to put configuration recorder 'StackSet-FMS-EnableConfig-CloudFront-2765adb1-71a9-4a3e-9bbb-535c4efdf35e-ConfigRecorder-1V0GK1MU9SVGJ' because maximum number of configuration recorders: 1 is reached. (Service: AmazonConfig; Status Code: 400; Error Code: MaxNumberOfConfigurationRecordersExceededException; Request ID: 4d48abd6-380a-4037-ab8e-51f239d203cc; Proxy: null).

Reason: Each AWS Region supports only one configuration recorder. CloudFormation StackSets will fail to create a stack instance in the account and Region if the recorder already exists. This happens when you're using AWS Config in that Region, or you used it in the past. For additional information, refer to Configuration Recorder in the *AWS Config Developer Guide*.

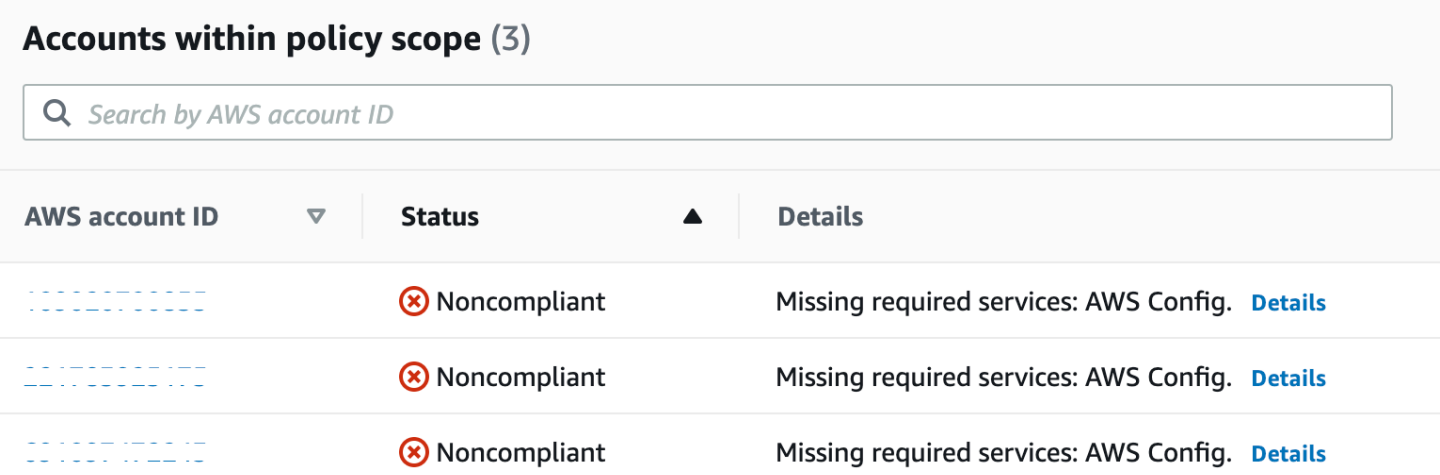
Resolution

Activate AWS Config in the appropriate Region and ensure that the necessary resource types are included in the recording group. For additional information, refer to Enable AWS Config in the *AWS WAF, AWS Firewall Manager, and AWS Shield Advanced Developer Guide*.

Problem: AWS Config isn't activated in member accounts

When AWS Config isn't activated in member accounts, you see following error message in your Firewall Manager console:

Screenshot showing Noncompliant status for AWS accounts.



Resolution

If you're using this solution's prerequisite template to activate AWS Config, then this is a transient issue. It takes time for AWS Config to activate and propagate across AWS Organizations accounts. Allow some time for the update to complete its processing. If you are not using this solution's prerequisite template, then access the individual accounts to activate AWS Config manually. For more information, refer to Enable AWS Config in the *AWS WAF, AWS Firewall Manager, and AWS Shield Advanced Developer Guide*.

Other errors

This section addresses other known errors when deploying or using this solution.

Problem: The FMS admin account-id isn't displayed in the Firewall Manager console

The Firewall Manager settings don't reflect the Admin account ID provided in the CloudFormation stack.

Resolution

It might take up to five minutes for the changes to update in the console.

Problem: The CloudFormation StackSets instance displays as Outdated

The CloudFormation StackSets instance displays an **Outdated** status.

Screenshot showing OUTDATED status for AWS Regions.

eu-west-1	OUTDATED	User initiated operation
eu-west-2	OUTDATED	User initiated operation
eu-west-3	OUTDATED	User initiated operation
sa-east-1	OUTDATED	User initiated operation
us-east-2	OUTDATED	User initiated operation
us-west-1	OUTDATED	User initiated operation
us-west-2	OUTDATED	User initiated operation

Resolution

The **Outdated** status is temporary. Allow more time for the CloudFormation StackSets to update to a final state after the StackSets operation completes. Creating StackSets instances across multiple accounts and Regions is a time-intensive process. For example, for 6 accounts in approximately 18 Regions, it takes about 90 minutes to complete the StackSets operation.

Problem: InternalErrorException when creating a policy in Firewall Manager

Firewall Manager fails to create policies due to `InternalErrorException`.

Example error showing "code": "InternalErrorExeception".

```
2020-09-10T13:47:18.041-04:0...  [ERROR] [fmsHelper/putPolicy] {"message":null,"code":"InternalErrorException","time":"2020-09-10
[ERROR] [fmsHelper/putPolicy]
{
    "message": null,
    "code": "InternalErrorException",
    "time": "2020-09-10T17:47:18.041Z",
    "requestId": "b8c75083-ec51-4cc0-a92c-5135abb1faf1",
    "statusCode": 400,
    "retryable": false,
    "retryDelay": 80.23010098902039
}
```

```
2020-09-10T13:47:18.041-04:0...  [ERROR] [PolicyManager/saveShieldPolicy-Regional] failed to save policy
[ERROR] [PolicyManager/saveShieldPolicy-Regional] failed to save policy
```

Resolution

This issue is transient in nature, and invoking the Lambda function again fixes the issue. For example, after updating the **/FMS/Regions** parameter, follow the steps to invoke the update again. Use the following steps to invoke the event again:

1. Sign in to the AWS Systems Manager console.
2. On the navigation menu, under **Application Management**, select **Parameter Store**.
3. Select the **/FMS/Regions** parameter and choose **Edit**.
4. Keep the default value and choose **Save changes**.

This invokes the `policyManager` Lambda function again using the same value. The Firewall Manager policy should successfully create.

Problem: Throttling exception with AWS APIs

AWS APIs throttling can occur if the solution is handling large number of Firewall Manager policies and AWS accounts. The following error is logged in CloudWatch logs:

CloudWatch log error

```
[ERROR] [ComplianceGenerator/getComplianceDetails] ThrottlingException: Rate
exceeded
```

Resolution

The Lambda functions include a `MAX_ATTEMPTS` environment variable, which you can adjust to fix this issue. The `MAX_ATTEMPTS` variable controls how many times the solution attempts to retry an API request.

Contact Support

If you have AWS Developer Support, AWS Business Support, or AWS Enterprise Support, you can use the Support Center to get expert assistance with this solution. The following sections provide instructions.

Create case

1. Sign in to Support Center.
2. Choose **Create case**.

How can we help?

1. Choose **Technical**.
2. For **Service**, select **Solutions**.
3. For **Category**, select **Other Solutions**.
4. For **Severity**, select the option that best matches your use case.
5. When you enter the **Service**, **Category**, and **Severity**, the interface populates links to common troubleshooting questions. If you can't resolve your question with these links, choose **Next step: Additional information**.

Additional information

1. For **Subject**, enter text summarizing your question or issue.
2. For **Description**, describe the issue in detail.
3. Choose **Attach files**.
4. Attach the information that AWS Support needs to process the request.

Help us resolve your case faster

1. Enter the requested information.
2. Choose **Next step: Solve now or contact us**.

Solve now or contact us

1. Review the **Solve now** solutions.
2. If you can't resolve your issue with these solutions, choose **Contact us**, enter the requested information, and choose **Submit**.

Uninstall the solution

You can uninstall this solution from the AWS Management Console or by using the AWS Command Line Interface (AWS CLI).

Before uninstalling the solution, complete the following steps for each deployed stack to ensure that the Firewall Manager security policies are deleted before the stack deletion:

1. Sign in to the AWS Systems Manager console.
2. On the navigation menu, under **Application Management**, select **Parameter Store**.
3. Select the **/FMS/<Policy-Id>/OU** parameter and choose **Edit**.
4. Change the value to `delete` and choose **Save changes**.

All other resources deployed by this solution are automatically deleted when you delete each respective stack. Only custom defined rules are not automatically deleted.

Using the AWS Management Console

1. Sign in to the CloudFormation console.
2. On the **Stacks** page, select this solution's installation stack.
3. Choose **Delete**.

Using AWS Command Line Interface

Determine whether the AWS CLI is available in your environment. For installation instructions, see What Is the AWS Command Line Interface in the *AWS CLI User Guide*. After confirming that the AWS CLI is available, run the following command.

```
$ aws cloudformation delete-stack --stack-name <installation-stack-name>
```

> **Note**
>
> This solution supports a complete deletion of the stack and all resources deployed by the solution. Only custom defined rules and an S3 bucket with compliance reports are left behind.

Deleting the Amazon S3 buckets

This solution is configured to retain the solution-created S3 buckets for storing compliance reports and Firewall Manager policies to prevent accidental data loss. After uninstalling the solution, you can manually delete these S3 buckets if you don't need to retain the data. Follow these steps to delete the Amazon S3 bucket.

1. Sign in to the Amazon S3 console.
2. Choose **Buckets** from the left navigation pane.
3. Locate the *<stack-name>* S3 buckets.
4. Select the S3 bucket and choose **Delete**.

To delete the S3 bucket using AWS CLI, run the following command:

```
$ aws s3 rb s3://<bucket-name> --force
```

Deleting Route 53 health checks

Route 53 health checks created by the Shield Advanced Automations stack aren't automatically deleted when you delete the Shield Advanced Automations stack. This is because these resources are created dynamically by the solution's Lambda functions. Follow these steps to delete the health checks created by the solution:

1. Sign in to the Amazon Route 53 health checks console.
2. Enter `calculated` in the **Search** bar.
3. Choose a health check to open the **Info** tab.
4. Under **Health checks to monitor**, confirm that the name of the **CloudWatch Alarm** begins with `FMS-Shield-`. This confirms that both child health checks are created by the solution.
5. For each child health check, choose **Delete Health Check**.
6. For each parent health check, choose **Delete Health Check**.

Deleting CloudWatch metric alarms

CloudWatch metric alarms created by the Shield Advanced Automations stack aren't automatically deleted when you delete the Shield Advanced Automations stack. This is because these resources

are created dynamically by the solution's Lambda functions. Follow these steps to delete the health checks created by the solution:

Follow these steps to delete the CloudWatch metric alarms created by the solution:

1. Sign in to the AWS CloudWatch Alarms console.
2. Enter `FMS-Shield` in the **Search** bar.
3. **Select** all the alarms that you want to delete.
4. Choose **Actions**.
5. Choose **Delete**.

Use the solution

This section provides a user guide for using the AWS solution.

Set up the Systems Manager parameters

This solution uses three Systems Manager parameters to initiate creating, updating, and deleting Firewall Manager policies. Review the following scenarios for guidance to set up the following Systems Manager tasks:

- Create policies across two OUs and five AWS Regions
- Delete tags from policies
- Delete Regional policies
- Delete all policies

Each of the parameters is a *StringList* type. Use commas to separate each string.

Create policies across OUs and Regions

Use the following steps to create policies across two OUs and five AWS Regions with the scope of policies restricted to a certain tag value.

> **Note**
>
> For this example, we use the following values to represent variables:
>
> - OUs: `ou-xxxx-y1y1y1y1,ou-yyyy-x2x2x2x2`
> - Regions: `us-east-1,us-east-2,us-west-1,us-west-2,eu-west-1`
> - Tag: `{"ResourceTags": [{"Key":"Environment","Value":"Prod"}],"ExcludeResourceTags":false}`

1. Sign in to the AWS Systems Manager console.
2. On the navigation menu, under **Application Management**, select **Parameter Store**.
3. Update the **/FMS/OUs** parameter:

   a. Select the **/FMS/OUs** parameter and choose **Edit**.
   b. Update the parameter with the OU values. For this example, we use: `ou-xxxx-y1y1y1y1,ou-yyyy-x2x2x2x2`.
   c. This action creates the Global AWS WAF and AWS Shield Advanced policies.
4. Update the **/FMS/Regions** parameter:
   a. Select the **/FMS/Regions** parameter and choose **Edit**.
   b. Update the **/FMS/Regions** parameter with the chosen Regions. For this example, we use: `us-east-1,us-east-2,us-west-1,us-west-2,eu-west-1`.
   c. This action creates the Regional policies (one AWS WAF, one AWS Shield, and two Security Groups).
5. Update the **/FMS/Tags** parameter:
   a. Select the **/FMS/Tags** parameter and choose **Edit**.
   b. Update the **/FMS/Tags** parameter with the tag value. For this example, we use: `{"ResourceTags": [{"Key":"Environment","Value":"Prod"}],"ExcludeResourceTags":false}`.
   c. This action updates all policies with the provided tag value.

The solution creates Firewall Manager after you complete these steps. Two global policies and four Regional policies should be in each of the selected Regions. In this scenario, 22 total policies are created, using the following formula:

(4 Regional policies × 5 Regions) + 2 global policies

Delete tags from policies

To delete tags from the policies, complete the following steps:

1. Sign in to the AWS Systems Manager console.
2. On the navigation menu, under **Application Management**, select **Parameter Store**.
3. Select the **/FMS/Tags** parameter and choose **Edit**.
4. Update the **/FMS/Tags** parameter using the following value: delete

This action updates all policies and removes the applied tags.

Delete Regional policies

To delete all Regional policies, complete the following steps:

1. Sign in to the AWS Systems Manager console.
2. On the navigation menu, under **Application Management**, select **Parameter Store**.
3. Select the **/FMS/Regions** parameter and choose **Edit**.
4. Update the **/FMS/Regions** parameter using the following value: delete

This action deletes all Regional policies.

Delete policies

To delete all policies, complete the following steps:

1. Sign in to the AWS Systems Manager console.
2. On the navigation menu, under **Application Management**, select **Parameter Store**.
3. Select the **/FMS/OUs** parameter and choose **Edit**.
4. Update the **/FMS/OUs** parameter using the following value: delete

> **Note**
>
> The policy metadata is stored in the DynamoDB table. Don't delete this table while you're using the solution.

Access compliance reports

The `aws-fms-compliance.template` CloudFormation template deploys infrastructure needed to generate compliance reports on the Firewall Manager policies. This generates the following reports:

- **Account Compliance Report** - This report lists all member accounts in scope of the policy and their compliance status. You can find this report the S3 bucket with naming schema *<timestamp>*_account_compliance_*<policy-id>*.

Example account compliance report with COMPLIANCE_STATUS.

MEMBER_ACCOUNT	COMPLIANCE_STATUS
[redacted]	COMPLIANT
[redacted]	COMPLIANT
[redacted]	{"AWSCONFIG":"Cannot create config rule resource for member account [redacted]. Please ensure AWS Config Recorder is enabled and the Config resource limits are not exceeded."}

- **Resource Violation Report** - This report lists all AWS resources in member accounts in scope of that policy, that are in violation of compliance. You can find this report can be in the S3 bucket with naming schema *<timestamp>*_resource_violator_*<policy-id>*.

Example resource violation report with VIOLATION_REASON.

MEMBER_ACCOUNT	RESOURCE_ID	RESOURCE_TYPE	VIOLATION_REASON
[redacted]	[redacted]	AWS::EC2::SecurityGroup	RESOURCE_VIOLATES_AUDIT_SECURITY_GROUP
[redacted]	[redacted]	AWS::EC2::SecurityGroup	RESOURCE_VIOLATES_AUDIT_SECURITY_GROUP

The S3 bucket that includes the reports has public access blocked, is encrypted, and has version turned on. Additionally, we recommend the following:

- Turning on multi-factor authentication (MFA) on object deletion for this bucket
- Ensuring that users don't gain elevated privileges to view or delete these reports (following the least privilege design principles).

For more information, refer to Configuring MFA delete in the *Amazon S3 User Guide*.

View health checks created by Automations for Shield Advanced

The `aws-fms-shield-automations` CloudFormation template deploys infrastructure needed to automatically create Route 53 health checks and associate them with existing Shield Advanced protections in your AWS Organization. Follow these steps to view a health check associated with a particular Shield Advanced protection:

1. Sign in to the AWS Shield console.
2. On the navigation menu, under **AWS Shield**, select **Protected resources**.
3. Select the resource that you want to view.
4. Select **Edit**.
5. Select **Next**.
6. Select the dropdown menu under **Associated Health Check**. Copy the highlighted **resource ID**.

7. Sign in to the Route 53 health checks console.
8. Paste the **resource ID** into the **Search** bar.
9. Choose the Route 53 health check to view.

Alternatively, you can view the health checks associated with a particular Shield Advanced protection by using the Shield Advanced DescribeProtection API.

> **Note**
>
> Health checks created by the solution are labeled as undefined in the AWS Shield console until you assign a name to them manually in the Route 53 health check console.

Set up CloudWatch Logs insights

This solution logs error, warning, informational, and debugging messages for the Lambda functions. To choose the type of messages to log, locate the applicable function in the AWS Lambda console and change the **LOG_LEVEL** environment variable to the applicable type of message. For further instructions on how to change the variable, see Using Lambda environment variables in the *AWS Lambda Developer Guide*.

The following table lists the types of log levels you can choose from.

Level	Description
ERROR	Logs include information on anything that causes an operation to fail.
WARNING	Logs include information on anything that con potentially cause inconsistencies in the function but might not necessarily cause the operation to fail. Logs also include ERROR messages.
INFO	Logs include high-level information about how the function is operating. Logs also include ERROR and WARNING messages.

Level	Description
DEBUG	Logs include information that might be helpful when debugging a problem with the function. Logs also include ERROR, WARNING, and INFO messages.

You can adjust the log levels to troubleshoot the issues identified in Troubleshooting.

View CloudWatch Logs insights

The following CloudWatch Logs insights queries are added to your account when you deploy the solution. To view and use these queries, access your saved queries from the CloudWatch console.

Alternatively, you can complete the following steps to use the queries manually.

Policy Manager

1. Navigate to the Amazon CloudWatch console.
2. On the navigation menu, under **Logs**, choose **Insights**.
3. On the **Logs Insights** page, choose the **Logs** tab.
4. Select **/aws/lambda/*<xxxx>*-PolicyStack-PolicyManager-*<xxxx>*** . This log group contains the log events related to policy creation, updates, and deletions.
5. Copy one of the following sample queries and paste it into the query field:
   - To identify error events:

     ```
     fields @timestamp, @level
     |sort @timestamp desc
     |filter level = "ERROR"
     ```

   - To identify policy create success events:

     ```
     fields @timestamp, @level, @message
     |sort @timestamp desc
     |filter message like "successfully put policy"
     ```

   - To identify policy create fail events:

```
fields @timestamp, @message
|sort @timestamp desc
|filter message like "encountered error putting policy"
```

6. Select a time preference and choose **Run query**. Save these queries for future use.

Automations for Shield Advanced

1. Navigate to the Amazon CloudWatch Logs console.
2. On the navigation menu, under **Logs**, choose **Logs Insights**.
3. On the **Logs Insights** page, choose the **Logs** tab.
4. Select **/aws/lambda/*<xxxx>*-FMS-ShieldAutomations-ConfigRuleRemediate-*<xxxx>*** . This log group contains the log events related to Route 53 health check creation and association.
5. Select **/aws/lambda/*<xxxx>*-FMS-ShieldAutomations-ConfigRuleEval-*<xxxx>*** to view log events related to evaluation of your organization's Shield Advanced protections.
6. Copy one of the following sample queries and paste it into the query field:
   - To identify error events:

```
fields @timestamp, @level
|sort @timestamp desc
|filter level = "ERROR"
```

   - To identify successful health check create events:

```
fields @timestamp, @message
|sort @timestamp desc
|filter message like "Created Route53 Health Check"
```

   - To identify successful remediation events:

```
fields @timestamp, @message
|sort @timestamp desc
|filter message like "Remediation successful for Shield Protection"
```

   - To identify successful associations of health checks with Shield Advanced protections:

```
fields @timestamp, @message
|sort @timestamp desc
```

```
|filter message like "Associated calculated Health Check"
```

7. Select a time preference and choose **Run query**. Save these queries for future use.

Each CloudWatch log has an associated X-Ray trace ID. To view the X-Ray trace for a particular function invocation, paste the X-Ray trace ID in the **X-Ray traces** tab of the CloudWatch console.

Developer guide

This section provides the source code for the solution, a list of policies and rule sets, and additional customizations.

Source code

Visit our GitHub repository to download the source files for this solution and to share your customizations with others.

The AWS CDK generates the solution templates. See the README.md file for additional information.

List of policies and rule sets

This section describes the policies and rule sets used with this solution.

Centralized WAF managed rules automation

To support Firewall Manager, this solution installs AWS Managed Rules for AWS WAF. You can scope your accounts based on either OUs or resource tags.

The solution installs the following AWS Managed Rules:

- **Core Rule Set (CRS)- web ACL capacity unit (WCU) 700** - This group contains rules that are generally applicable to web applications. This group provides protection against exploitation of a wide range of vulnerabilities, including those described in Open Worldwide Application Security Project (OWASP) publications.
- **Amazon IP reputation list-WCU 25** - This group contains rules that are based on Amazon threat intelligence. This list is useful if you want to block sources associated with bots or other threats.
- **Known Bad Inputs (KBI)-WCU 200** - This group contains rules that allow you to block request patterns that are known to be not valid and are associated with exploitation or discovery of vulnerabilities. These inputs help reduce the risk of an unintended entity discovering a vulnerable application.
- **SQL-WCU 200** - This group contains rules that allow you to block request patterns associated with exploitation of SQL databases, like SQL injection attacks. These rules help prevent remote injection of unauthorized queries.

By default, any findings based on these rules are auto-remediated by Firewall Manager. You can change this setting to remediate manually by updating the selection in the solution's manifest file.

Centralized security group audit checks

In Firewall Manager, this solution installs pre-configured audit checks for VPC security groups in your Amazon EC2 instances across your accounts from a central admin account. You can scope the accounts based on either OUs or resource tags. The solution provides for auditing and cleanup of unused and redundant security groups.

By default, findings based on these rules are not auto-remediated by Firewall Manager.

Centralized DDoS protection enablement

If you are subscribed to Shield Advanced, then you can use its rules and policies to protect from centralized DDoS attacks. For CloudFront distributions and Application Load Balancers, the default Shield Advanced policies deployed by the solution enable application layer DDoS mitigation in Count mode.

By default, findings based on these rules are auto-remediated by Firewall Manager. You can choose to change this setting to remediate manually by updating the selection in the solution's manifest file.

Centralized DNS Firewall rules automation

To support centralized management of DNS Firewall rules, the solution installs pre-configured DNS Firewall rule group in each Region. The DNS Firewall rule group uses AWS Managed Domain Lists.

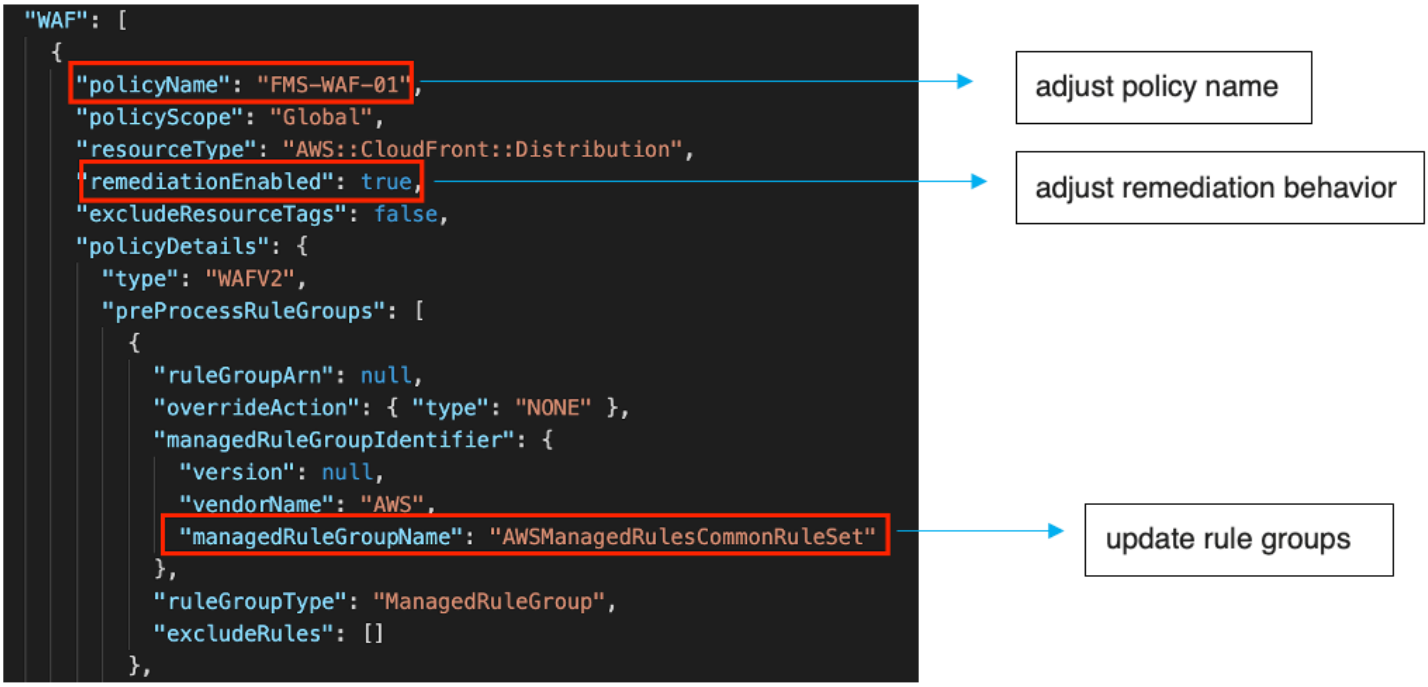
For more details, refer to Route 53 Resolver DNS Firewall in the *Amazon Route 53 Developer Guide*.

Policy manifest file

This solution uses a JSON manifest file to create Firewall Manager policies. When you deploy this solution, the manifest file is copied to an S3 bucket (*<Stack-Name>*-*<xx>*-policymanifestbucket-*<xx>*) in your account.

The manifest file is a set of opinionated defaults for the policies. If these defaults aren't suitable for your use case, you can adjust the configurations in the manifest by using the following sample policy manifest.

Example policy manifest where you adjust policyName remediationEnabled, and managedRuleGroupName.



Manifest schema

Review the following schema details and definitions before updating the manifest file for your use case.

```
{
 "default": {
 "<Policy-Type>": <Policy-Object>
 }
}
```

- **default** - Manifest root key. **Do not** change.
- **Policy-Type** - Firewall Manager policies supported by the solution. The following list provides the supported types.
  - `"WAF_GLOBAL"`
  - `"WAF_REGIONAL"`
  - `"SHIELD_GLOBAL", "SHIELD_REGIONAL"`
  - `"SECURITY_GROUPS_USAGE_AUDIT"`
  - `"SECURITY_GROUPS_CONTENT_AUDIT"`

- `"DNS_FIREWALL"`
- **Policy-Object**
  - **policyName** -The name of the Firewall Manager policy.
  - **policyDetails** - Details about the policy that are specific to the service type, in JSON format. For details on different policy types, refer to Security service policy data.
  - **resourceType** - The type of resource protected by or in scope of the policy. This is in the format shown in AWS resource and property types reference.
  - **resourceTypeList** - A list of **resourceType**.
  - **remediationEnabled** - Indicates if the policy should be automatically applied to new resources and if the policy findings should be automatically remediated.

For further details on customizing the solution, refer to the README.md file in the GitHub repository.

Recovering data

Policy metadata stored by the solution could be accidentally deleted or overwritten. You can restore this data to an existing backup by enabling service-level recovery by default:

1. **Restore S3 objects** - The **Policy Manifest** S3 bucket deployed by the Primary solution stack has S3 versioning enabled by default. You can use versioning to restore objects that have been deleted or overwritten. See Restoring previous versions in the *Amazon Simple Storage Service User Guide* for instructions on how to restore objects to a previous state.
2. **Restore DynamoDB data** - The **Policy Table** DynamoDB table deployed by the Primary stack has point-in-time recovery (PITR) enabled by default. You can use PITR to restore the table to an existing backup. See Restoring a DynamoDB table to a point in time in the *Amazon DynamoDB User Guide* for instructions on how to restore the table to a previous state.

Customization guide

This section provides customization instructions and examples for this solution.

Change the encryption at-rest method to use custom keys

All AWS resources deployed by the solution use default service-managed encryption. For example, Amazon S3 managed keys (SSE-S3) are used to encrypt the S3 buckets created by the Primary CloudFormation stack. You can modify the encryption method used for any AWS service deployed by the solution by using the AWS Management Console or API. The following resources provide instructions on how to modify the solution's resources to use your own custom encryption keys:

- **DynamoDB** - Bring your own encryption keys to Amazon DynamoDB
- **Amazon S3** - AWS KMS Keys in the *Amazon Simple Storage Service User Guide*

Change the log retention period

By default, the solution employs log retention periods of one year or one week, depending on the log group. You can customize the retention period of any log group created by the solution to fit your needs. See Change log data retention in CloudWatch Logs in the *Amazon CloudWatch Logs User Guide* for detailed instructions on modifying log retention periods.

Change the default Firewall Manager security policy configuration

This solution deploys Firewall Manager security policies with default configurations. However, you can change policy settings or apply different policies to different OUs and Regions.

To change the default Firewall Manager security policy configuration, follow these steps after deploying the solution.

1. Sign in to the Amazon S3 console.
2. Choose the *<Stack-Name>*-*<xx>*-policymanifestbucket-*<xx>* S3 bucket.
3. Choose the `policy_manifest.json` file in the bucket.
4. Download the manifest file and make adjustments to the default settings in the policy manifest. For more information, refer to Policy manifest file.
5. Upload the updated manifest file in the same location.
6. The Firewall Manager policies automatically update to reflect the changes made in Step 4.

Apply different policies to different OUs and Regions

To apply different policies to different OUs and Regions, follow these steps.

1. Use aws-fms-policy.template to launch additional resources needed to support different policies for different OUs and Regions. You can launch this template multiple times for as many policy configurations as needed.
2. Provide following stack parameter values:

Parameter	Default	Description
Policy Identifier	*<Optional input>*	A unique identifier for the policies.
Policy Table	*<Optional input>*	DynamoDB table where policy metadata will be saved. This table is created as part of Primary template deployment.
UUID	*<Optional input>*	Universally unique identifier (UUID) for stack deployment. The UUID is created as part of Primary template deployment. **Note** You can leave this parameter blank if you don't want to send an anonymized metric to the solution's endpoint.
Metric Queue	*<Optional input>*	Amazon Simple Queue Service (Amazon SQS) queue to send anonymized metrics to the solution endpoint. The queue is created as part of Primary template deploymen

Parameter	Default	Description
		t. NOTE: You can leave this parameter blank if you don't want to send an anonymized metric to the solution's endpoint.

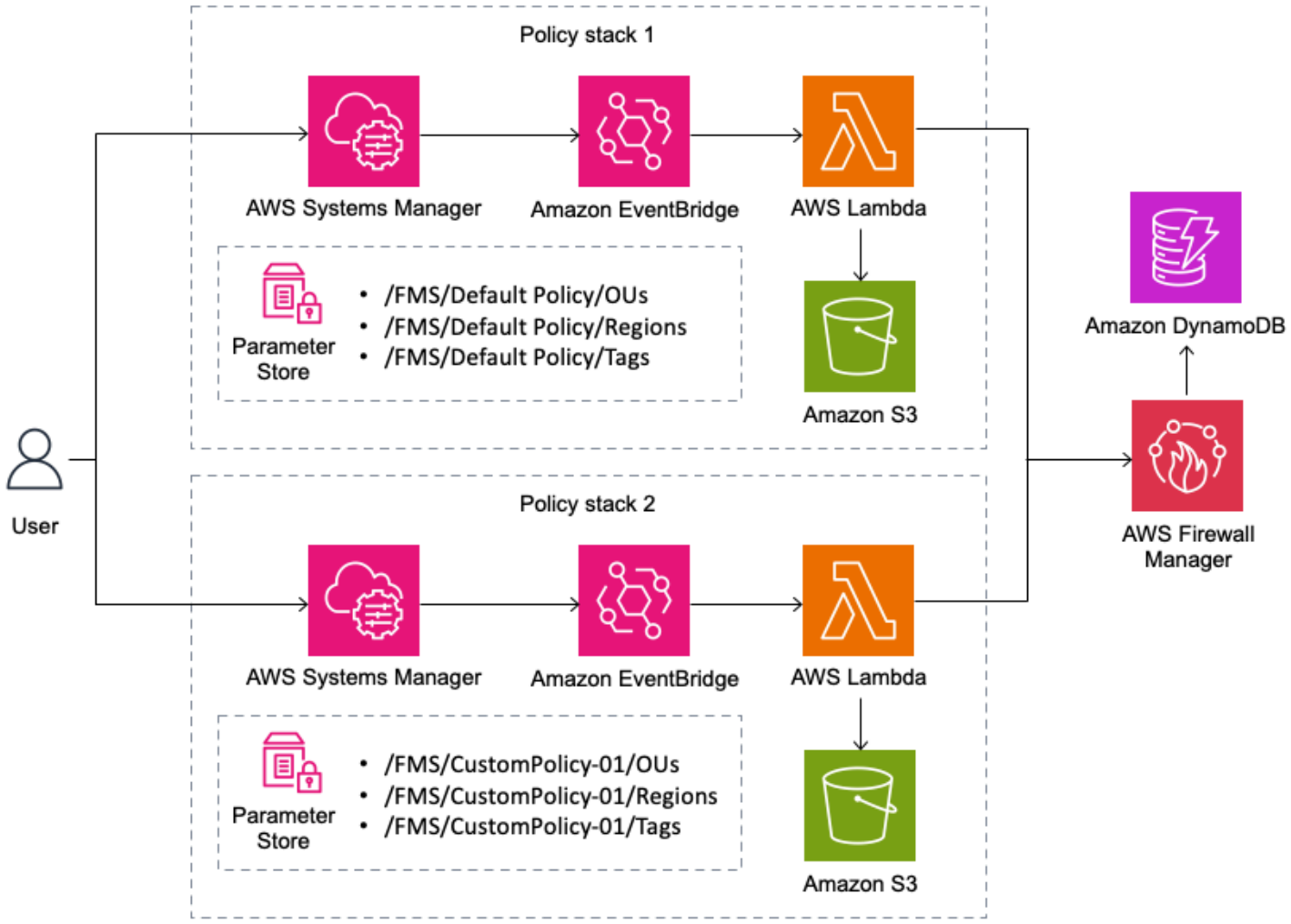
> **Note**
>
> **Policy Table**, **UUID**, and **Metric Queue** are created as part of the primary stack deployment. You can review their values by checking the Outputs section of the primary deployed stack. Ensure that you provide the same value as given in the **Outputs** section of the primary deployed stack.

3. After the deployment succeeds, three more Parameter Stores are added in the Systems Manager console, as well as one more *<Stack-Name>*-*<xx>*-policymanifestbucket-*<xx>* bucket in the Amazon S3 console.

You can adjust these Parameter Store values. If you adjust them, the solution creates a Firewall Manager policy accordingly.

The policy configuration is managed by the `policy_manifest.json` file from the manifest bucket. You can update the `policy_manifest.json` file at any time. See Policy manifest file for more information.

Architecture showing two policy stacks feeding into Firewall Manager and DynamoDB.



You can create as many policy stacks for different policy configurations as needed and apply them to different OUs and Regions.

Example policy customization scenarios

For details on policy manifest schema, refer to Policy manifest file. You can configure the policy manifest in any number of ways. The following examples are some common scenarios.

Change policy auto-remediation behavior

All the policies have a default remediation behavior in the policy manifest file. You can adjust this as `true` or `false` per your requirements.

```
"remediationEnabled": false
```

Add AWS WAF Bot Control rule group

You can customize the **WAF Global** or **WAF Regional** policy in the manifest file to add AWS managed WAF Bot Control rule group. You can update the `preProcessRuleGroups` or `postProcessRuleGroups` section in the WAF policy as follows:

```
"postProcessRuleGroups": [{
 "ruleGroupArn": null,
 "overrideAction": {
 "type": "NONE"
 },
 "managedRuleGroupIdentifier": {
 "version": null,
 "vendorName": "AWS",
 "managedRuleGroupName": "AWSManagedRulesBotControlRuleSet"
 },
 "ruleGroupType": "ManagedRuleGroup",
 "excludeRules": []
}]
```

For more information about the AWS WAF Bot Control managed rule group, refer to AWS Managed Rules rule groups list in the *AWS WAF, AWS Firewall Manager, and AWS Shield Advanced Developer Guide*.

Deploy specific policy types

You can deploy a selection of Firewall Manager policy from the supported policies:

- `WAF_GLOBAL`
- `WAF_REGIONAL`
- `SHIELD_GLOBAL`
- `SHIELD_REGIONAL`
- `SECURITY_GROUPS_USAGE_AUDIT`
- `SECURITY_GROUPS_CONTENT_AUDIT`
- `DNS_FIREWALL`

Each Firewall Manager policy type has a JSON object defined in the manifest schema that controls the policy configuration. You can remove this JSON object from the manifest file if you don't need a specific policy.

If the policy has already been created by the solution, use the following steps to delete a specific policy type:

1. Delete the deployed FMS policy type.
   a. Sign in to the AWS Firewall Manager console, using the admin account.
   b. Identify the policy to be deleted.
   c. Select the policy and choose **Delete**.
   d. Chose **Delete all policy resources** in the pop-up window, and choose **Delete.**
2. Update the policy manifest file in the S3 bucket. For more information, refer to Policy manifest file.
3. Update Parameter Store parameters. For more information, refer to Step 3. Add and manage Firewall Manager policies.

Reference

This section includes information about an optional feature for collecting unique metrics for this solution, pointers to related resources, and a list of builders who contributed to this solution.

Anonymized data collection

This solution includes an option to send anonymized operational metrics to AWS. We use this data to better understand how customers use this solution and related services and products. When invoked, the following information is collected and sent to AWS:

- **Solution ID** - The AWS solution identifier
- **Unique ID (UUID)** - Randomly generated, unique identifier for each deployment
- **Timestamp** - Data-collection timestamp
- **Solution Version** - Version of the solution being used
- **Organizational Unit size** - The size of OUs where Firewall Manager policies are deployed
- **Policy Region** - The Region where Firewall Manager policies are created
- **Event** - Whether Firewall Manager policies are being created or updated
- **Policy Type** - The type of Firewall Manager policy being deployed
- **Count of compliance reports generated** - The number of compliance reports generated by the solution

AWS owns the data gathered through this survey. Data collection is subject to the Privacy Notice. To opt out of this feature, complete the following steps before launching the AWS CloudFormation template.

1. Download the `aws-fms-prereq.template` AWS CloudFormation templates to your local hard drive.
2. Open the AWS CloudFormation template with a text editor.
3. Modify the AWS CloudFormation template mapping section from:

```
"Mappings": {
 "PolicyStackMap": {
 "Metric": {
 "SendAnonymousMetric": "Yes"
```

```
},
```

to

```
"Mappings": {
 "PolicyStackMap": {
 "Metric": {
 "SendAnonymousMetric": "No"
},
```

4. Sign in to the AWS CloudFormation console.
5. Select **Create stack**.
6. On the **Create stack** page, **Specify template** section, select **Upload a template file**.
7. Under **Upload a template file**, choose **Choose file** and select the edited template from your local drive.
8. Choose **Next** and follow the steps in Launch the stack in the Deploy the solution section of this guide.

Other AWS WAF solution and resources

- AWS WAF Security Automations solution

Contributors

- Garvit Singh
- Rakshana Balakrishnan
- Aijun Peng
- William Quan
- Nikhil Reddy
- Ryan Garay
- Aaron Schuetter

Revisions

Publication date: *September 2020*

Visit the CHANGELOG.md in our GitHub repository to track version-specific improvements and fixes.

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents AWS current product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers, or licensors. AWS products or services are provided "as is" without warranties, representations, or conditions of any kind, whether express or implied. AWS responsibilities and liabilities to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.